Citrix ADC 13.1

Machine translated content

Disclaimer

Contents

Notas de la versión de Citrix ADC

October 5, 2021

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

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

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

> **Nota**
>
> - Las etiquetas [n.º XXXXXX] de las descripciones de problemas son identificadores de seguimiento internos utilizados por el equipo de Citrix ADC.
> - Estas notas de la versión no documentan las correcciones relacionadas con la seguridad. Para obtener una lista de correcciones y avisos relacionados con la seguridad, consulte el boletín de seguridad de Citrix.

Notas de la versión de Citrix ADC 13.1—27.59

August 11, 2022

Este documento de notas de la versión describe las mejoras y los cambios, los problemas resueltos y conocidos que existen para la versión 13.1—27.59 de Citrix ADC.

Notas

Este documento de notas de la versión no incluye correcciones relacionadas con la seguridad. Para obtener una lista de correcciones y avisos relacionados con la seguridad, consulte el boletín de seguridad de Citrix.

Novedades

Las mejoras y los cambios que están disponibles en las compilaciones 13.1—27.59.

Autenticación, autorización y auditoría

Permitir a los usuarios usar la configuración de Intune NAC v2 con las nuevas API de Microsoft Graph

Ahora puede usar la configuración de Intune NAC v2 con las nuevas API de Microsoft Graph en lugar de las API de AAD Graph obsoletas.

Para obtener más información, consulte https://docs.citrix.com/en-us/citrix-gateway/current-release/microsoft-intune-integration.html. y https://docs.citrix.com/en-us/citrix-gateway/current-release/microsoft-intune-integration/extended-support-for-azure-ad-graph.html..

[NSAUTH-11897]

Administración de bots

StyleBook para la administración de WAF y bots en dispositivos Citrix Gateway

Ahora puede configurar las directivas WAF y BOT para los dispositivos Citrix Gateway a fin de proteger la página de inicio de sesión de Gateway. Ya están disponibles dos nuevos libros de estilos predeterminados para la administración de WAF y bots en dispositivos Citrix Gateway:

- Protección de sitios de inicio de sesión de StyleBook para Citrix Gateway mediante WAF y BOT
- Protección de sitios de inicio de sesión de StyleBook para Citrix Gateway mediante WAF y BOT con infracciones de seguridad de WAF y BOT

Para usar el StyleBook predeterminado para la administración de WAF o bots en la puerta de enlace, vaya a Aplicaciones > Configuración > StyleBooks. Escriba el nombre del StyleBook en el campo de búsqueda y presione la tecla Entrar. Para obtener más información, consulte https://docs.citrix.com/en-us/citrix-application-delivery-management-software/current-release/stylebooks/how-to-use-default-stylebooks.html%23to-create-a-configuration-from-a-default-stylebook

[NSBOT-755]

Habilitación de la función de detección de bots para todos los derechos premium de Citrix ADC

La función de detección de bots junto con las comprobaciones de firma y reputación de IP ahora está habilitada de forma predeterminada para todos los derechos premium de Citrix ADC.

Puede ver el tráfico de bots que llega a su entorno y la acción realizada por el dispositivo Citrix ADC. Además, el dispositivo ADC captura la siguiente información de tráfico de bots en los mensajes de registro SNMP:

- Número de bots detectados

- Las dos principales categorías de bots detectadas
- La ubicación donde puede encontrar más detalles sobre los bots detectados

Para obtener más información, consulte Detección de bots.

[NSBOT-752]

Citrix Web App Firewall

Habilitar firmas nuevas automáticamente

Ahora puede seleccionar **Habilitar nuevas firmas automáticamente** para permitir que las nuevas reglas predeterminadas de firmas WAF se habiliten automáticamente después de una actualización.

[NSWAF-8825]

Campos confidenciales en un perfil WAF

Ahora puede agregar campos confidenciales en un perfil WAF. Estos campos están enmascarados y no se capturan en los registros de ADC cuando se produce una infracción. Anteriormente, puede agregar estos campos solo con la configuración.

[NSWAF-8525]

Compatibilidad con palabras clave personalizadas para la carga útil HTML

Puede agregar las palabras clave que quiera y comprobar si estas palabras clave configuradas están presentes en la carga útil HTML. Si se detectan las palabras clave configuradas en las solicitudes entrantes, puede configurar el dispositivo Citrix ADC para bloquear las solicitudes, actualizar los registros o aumentar los contadores de registros.

Con esta función, puede agregar palabras clave que no están cubiertas en las comprobaciones de inyección de SQL e inyección de comandos y, por lo tanto, reducir los falsos positivos.

[NSWAF-8520]

Enfoque basado en gramáticas para la detección de inyección de comandos en cargas útiles HTML

La solución NextGen Citrix Web App Firewall ahora se ha mejorado para admitir el enfoque basado en gramáticas para la detección de inyección de comandos. Este enfoque reduce los falsos positivos en las cargas HTML.

Anteriormente, solo se admitía el enfoque basado en patrones.

[NSWAF-8270]

Redes

Ahora, puede usar el puerto NSIP:8080 en Citrix ADC CPX para la configuración del servidor virtual. Anteriormente, este puerto estaba reservado y no estaba disponible para la configuración del usuario.

[NSNET-25399]

Soporte de túneles de Ginebra en una configuración de clúster

Los túneles de Geneve ahora se admiten en una configuración de clúster de dispositivos Citrix ADC.

[NSNET-24773]

Mejoras para incluir el nivel de gravedad al enviar mensajes SNMP Trap

El dispositivo Citrix ADC VPX ahora incluye el nivel de gravedad en los mensajes de captura SNMP como un enlace variable. Utilice el siguiente comando con la opción **severityInfoInTrap**:

- **set snmp option -severityInfoInTrap ENABLED**

Cuando esta opción está habilitada, el nivel de gravedad de la captura se incluye en el mensaje de captura SNMP.

[NSNET-21603]

Plataforma

Soporte de direcciones IPv6 para la alta disponibilidad de Citrix ADC en AWS

El par de alta disponibilidad de Citrix ADC VPX ahora admite direcciones IPv6 en la misma zona de disponibilidad de AWS. Anteriormente, solo se admitían direcciones IPv4.

[NSPLAT-16672]

Interfaz de usuario

Microsoft dejó de desarrollador el explorador Internet Explorer a partir de junio de 2022. Para obtener más información, consulte https://support.microsoft.com/en-us/windows/internet-explorer-help-23360e49-9cd3-4dda-ba52-705336cc0de2.

A partir de la versión 13.1 27.x de Citrix ADC, el dispositivo Citrix ADC ya no admite Internet Explorer para acceder a su GUI.

Al acceder a la GUI de Citrix ADC mediante Internet Explorer, el dispositivo Citrix ADC muestra un mensaje de que Internet Explorer no es compatible. También recomienda una lista de exploradores compatibles para acceder a la GUI.

[NSUI-18224]

Solicitud de confirmación para habilitar o inhabilitar una función en la GUI de Citrix ADC

La GUI de Citrix ADC ahora le pide que confirme la operación cuando habilite o inhabilite una función de Citrix ADC en la GUI. La solicitud de confirmación impide la activación o desactivación accidental de una función de Citrix ADC.

[NSUI-18098]

Problemas resueltos

Los problemas que se abordan en las compilaciones 13.1—27.59.

Autenticación, autorización y auditoría

No se pueden reescribir directivas para dispositivos de punto final como `/logon/LogonPoint/Resources/List and /cgi/Resources/List`.

[NSHELP-29488]

Dispositivo Citrix ADC SDX

La configuración de la zona horaria de la máquina virtual de Citrix Service no funciona como se esperaba.

[NSHELP-32114]

En un dispositivo Citrix ADC SDX, se detecta un mayor uso de memoria debido al alto volumen de procesamiento de datos SNMP.

[NSHELP-30222]

La aplicación SNMP walk que se ejecuta en el dispositivo Citrix ADC SDX para SDX-ROOT-MIB::xenTable lleva más tiempo del esperado.

[NSHELP-30085]

Citrix Gateway

A veces, los usuarios no pueden acceder a los marcadores en el modo VPN sin cliente avanzado.

[NSHELP-30939]

El dispositivo Citrix Gateway configurado en modo Proxy ICA para la conexión de audio UDP podría bloquearse debido a daños en la memoria.

[NSHELP-30919]

El lanzamiento de la aplicación ICA falla en las siguientes condiciones:

- La función Directiva de seguridad de contenido (CSP) está habilitada.
- El usuario inicia sesión desde un explorador, pero usa la aplicación Citrix Workspace para iniciar la aplicación.

[NSHELP-30534]

El dispositivo Citrix Gateway puede bloquearse durante el análisis de canales cuando HDX Insight está habilitado y NSAP está inhabilitado.

[NSHELP-30029]

Gateway Insight informa de un error de autenticación falso incluso antes de que el usuario envíe las credenciales para el inicio de sesión cuando la regla de autenticación está configurada para que coincida con una de las solicitudes del flujo de inicio de sesión.

[NSHELP-29313]

El inicio de la aplicación falla después de introducir las credenciales si el perfil de sesión contiene el FQDN de StoreFront. Aparece el siguiente error.

“Error interno del servidor Http/1.1 43531”

Con esta solución, los clientes pueden introducir el FQDN en lugar de la dirección WI del perfil de sesión en IP.

[NSHELP-26671]

Citrix Web App Firewall

Los registros de `No user-agent header action` y `multi user-agent header action` pueden usar incorrectamente el mensaje de registro de la comprobación de reputación de IP.

[NSHELP-31935]

Un dispositivo Citrix ADC puede bloquearse mientras procesa las búsquedas de firmas de BOT con servidores DNS lentos.

[NSHELP-31642]

El dispositivo Citrix ADC puede bloquearse si el scripting entre sitios está habilitado en la regla de firma.

[NSHELP-31617]

Equilibrio de carga

En algunos casos, el estado del servicio no está sincronizado con el estado del monitor.

[NSHELP-31747]

El dispositivo Citrix ADC se bloquea durante la eliminación del servidor de nombres si se cumplen las siguientes condiciones:

- El servidor DNS y el servidor de nombres están configurados en la misma dirección IP y puerto.
- La directiva de escucha está establecida en el servidor DNS.

[NSHELP-31142]

Un dispositivo Citrix ADC puede bloquearse durante la configuración limpia si hay entradas de persistencia y se configura una gran cantidad de servidores virtuales de equilibrio de carga ficticios y servidores virtuales de grupo.

[NSHELP-30051]

La creación de un servicio virtual comodín falla si existe una configuración de WIHOME sin resolver en el dispositivo Citrix ADC.

[NSHELP-25627]

Otros

En un dispositivo Citrix ADC, cuando se agrega un disco duro adicional al dispositivo, se crea un enlace para el archivo `/var/nslog` en la carpeta de cierres inesperados `/var/crash/nslog`. Los archivos `newnslog` disponibles en la carpeta crash no se recopilan en la carpeta del recopilador generada por asistencia técnica.

[NSHELP-31354]

El dispositivo Citrix ADC SWG puede bloquearse cuando la memoria asignada a un recurso no se libera, lo que provoca un uso elevado de la memoria incluso cuando no hay tráfico.

[NSHELP-31290]

En una configuración de clúster de Citrix ADC con la autenticación del sistema de clave pública configurada, se observa el siguiente problema:

- VTYSH no muestra la información de todos los nodos del clúster en el coordinador de configuración de clústeres (CCO).

[NSHELP-28762]

Plataforma

En la plataforma SDX 26000 (SDX 26100-100G, 26160-100G, 26200-100G, 26250-100G), el número máximo de núcleos de CPU que se pueden asignar a una sola instancia VPX se cambia de 26 a 25 núcleos de CPU.

[NSPLAT-21233]

La licencia BYOL no se puede aplicar a una instancia Citrix ADC VPX que se ejecute en la plataforma en la nube de ALI.

[NSHELP-31546]

SSL

El dispositivo Citrix ADC SDX se bloquea cuando se asignan unidades criptográficas a una instancia VPX y se habilita la configuración jumbo.

[NSHELP-30950]

Un dispositivo Citrix ADC puede bloquearse en las siguientes situaciones:

- Un monitor de equilibrio de carga de tipo SSL y el servicio SSL tienen el mismo nombre
- Se cambia el nombre de un servicio SSL
- Se elimina un monitor de equilibrio de carga

[NSHELP-30445]

Si la interceptación SSL está habilitada y los servidores DNS no devuelven una respuesta DNS válida, se bloquea el acceso al sitio web.

[NSHELP-30201]

Un dispositivo Citrix ADC se bloquea cuando se producen las siguientes condiciones:

- Un par de claves de certificado RSA predeterminado está enlazado a un servicio interno.
- Un par de claves de certificado no RSA está enlazado al mismo servicio.
- Se produce la sincronización de HA.

[NSHELP-30084]

Sistema

El dispositivo Citrix ADC se bloquea cuando el dispositivo Citrix ADM administrador tiene una MTU de red superior a 1500.

[NSHELP-30835]

Un dispositivo Citrix ADC con la configuración de medición del lado del cliente puede dañar una variable y provocar un error de carga de la página en las siguientes condiciones:

- La respuesta HTTP contiene una variable javascript de más de 2000 bytes.

[NSHELP-30026]

En un dispositivo Citrix ADC, si desvincula las directivas globales avanzadas predeterminadas y guarda la configuración, los cambios no se reflejan en el siguiente reinicio.

[NSHELP-19867]

El dispositivo Citrix ADC descarta paquetes que contienen encabezados HTTP personalizados con un carácter de punto en el campo del nombre del encabezado. Esta acción se produce porque el parámetro allowOnlyWordCharactersAndHyphen está habilitado de forma predeterminada en el perfil HTTP predeterminado.

De 13.1-27.x y posteriores, el parámetro allowOnlyWordCharactersAndHyphen en el conjunto de perfiles HTTP predeterminado está inhabilitado de forma predeterminada. Sin embargo, Citrix recomienda mantener este parámetro habilitado para mejorar la seguridad.

[NSBASE-16722]

Interfaz de usuario

No puede desvincular miembros de grupos de servicios de equilibrio de carga mediante la GUI en Citrix ADC versión 13.0 versión 85.15 build.

[NSHELP-31474]

La página **Sistema > Diagnósticos** de la GUI de Citrix ADC no muestra los detalles de la página para los clientes con una licencia Advanced.

[NSHELP-31330]

Es posible que el registro de un seguimiento de paquetes no funcione como se esperaba en una partición de administración.

[NSHELP-31321]

La reconexión al dispositivo Citrix ADC falla con el siguiente error cuando `CTRL+C` se introduce mientras se ejecuta el comando `show run` en la interfaz CLI:

- `Invalid username or password`

Este problema se produce si los caracteres de la clave y la contraseña son los mismos.

[NSHELP-30817]

Debido a una secuencia de instalación de actualización incorrecta, se produce el siguiente problema en el dispositivo Citrix ADC.

- La imagen del núcleo se actualiza primero y, tras unos pocos pasos, se copian las claves de cifrado. Entre estos pasos, se produce una falla y el dispositivo ADC presenta una nueva imagen. Las claves de cifrado que faltan en la nueva imagen provocan un error de descifrado y una falta de configuración.

[NSHELP-30755]

Problemas conocidos

Los problemas que existen en las versiones 13.1—27.59.

AppFlow

HDX Insight no informa de un error de inicio de aplicación causado por un usuario que intenta iniciar una aplicación o un escritorio a los que el usuario no tiene acceso.

[NSINSIGHT-943]

Autenticación, autorización y auditoría

Un dispositivo Citrix ADC no autentica los intentos de inicio de sesión con contraseñas duplicadas y evita los bloqueos de cuentas.

[NSHELP-563]

LoginSchema de DualAuthPushOrOTP.xml no aparece correctamente en la pantalla del editor de esquemas de inicio de sesión de la GUI de Citrix ADC.

[NSAUTH-6106]

El perfil proxy ADFS se puede configurar en una implementación de clúster. El estado de un perfil proxy se muestra incorrectamente en blanco al ejecutar el siguiente comando.
`show adfsproxyprofile <profile name>`

Solución alternativa:

Conéctese al Citrix ADC activo principal del clúster y ejecute el comando `show adfsproxyprofile <profile name>`. Mostraría el estado del perfil de proxy.

[NSAUTH-5916]

La página Configurar servidor LDAP de autenticación de la GUI de Citrix ADC deja de responder si sigue los pasos siguientes:

- Se abre la opción Probar accesibilidad LDAP.
- Las credenciales de inicio de sesión no válidas se rellenan y envían.
- Las credenciales de inicio de sesión válidas se rellenan y envían.

Solución alternativa:

Cierre y abra la opción Probar accesibilidad de LDAP.

[NSAUTH-2147]

Almacenamiento en caché

Es posible que un dispositivo Citrix ADC se bloquee si la función Almacenamiento en caché integrado está habilitada y el dispositivo tiene poca memoria.

[NSHELP-22942]

Dispositivo Citrix ADC SDX

En un dispositivo Citrix ADC SDX, si el CLAG se crea en una NIC Mellanox, la MAC de CLAG cambia cuando se reinicia la instancia VPX. El tráfico a la instancia VPX se detiene tras el reinicio porque la tabla MAC tiene la antigua entrada MAC de CLAG.

[NSSVM-4333]

En un dispositivo Citrix ADC SDX, la lista de redes VLAN permitidas no se actualiza con el valor correcto para las interfaces Mellanox asignadas a una instancia de Citrix ADC VPX.

[NSHELP-31849]

Al actualizar un dispositivo Citrix SDX, aunque la versión del hipervisor sea la misma para la versión actual y la actualizada de SDX, se notifica el siguiente evento incorrecto en la GUI de Management Service:

No coinciden las versiones del SVM y el hipervisor

[NSHELP-31769]

La instalación de un certificado SSL en un dispositivo Citrix ADC SDX falla si el nombre del certificado o el nombre de la clave contienen algún espacio.

[NSHELP-31711]

En un dispositivo Citrix ADC SDX, las instancias de ADC no alcanzan su capacidad máxima al configurar el modo de asignación de rendimiento en ráfagas.

[NSHELP-27477]

Las caídas de paquetes se observan en una instancia VPX alojada en un dispositivo Citrix ADC SDX si se cumplen las siguientes condiciones:

- El modo de asignación de rendimiento está en ráfaga.
- Existe una gran diferencia entre el rendimiento y la capacidad máxima de ráfaga.

[NSHELP-21992]

Citrix Gateway

Las conexiones directas a los recursos fuera del túnel establecido por Citrix Secure Access pueden fallar si se produce un retraso o una congestión significativos.

[NSHELP-31598]

Cuando se configura AlwaysOn, se produce un error en el túnel de usuario debido al número de versión incorrecto (1.1.1.1) en el archivo aoservice.exe.

[NSHELP-30662]

Los usuarios no pueden conectarse al dispositivo Citrix Gateway después de cambiar el parámetro "networkAccessOnVPNFailure" siempre en el perfil de "fullAccess" a "onlyToGateway".

[NSHELP-30236]

La página principal de la puerta de enlace no se muestra inmediatamente después de que el plug-in de puerta de enlace establezca el túnel VPN correctamente. Para solucionar este problema, se introduce el siguiente valor de registro.

\HKLM\Software\Citrix\Secure Access Client\SecureChannelResetTimeoutSeconds
Tipo: DWORD

De forma predeterminada, este valor de registro no se establece ni se agrega. Cuando el valor de `SecureChannelResetTimeoutSeconds` es 0 o no se agrega, la solución para gestionar el retraso no funciona, que es el comportamiento predeterminado. El administrador debe configurar este registro en el cliente para habilitar la corrección (es decir, mostrar la página de inicio inmediatamente después de que el plug-in de puerta de enlace establezca correctamente el túnel VPN).

[NSHELP-30189]

El cliente VPN de Windows no respeta la alerta de "notificación de cierre SSL" del servidor y envía la solicitud de inicio de sesión de transferencia en la misma conexión.

[NSHELP-29675]

En algunos casos, el código de validación del servidor falla cuando se confía en el certificado del servidor. Como resultado, los usuarios finales no pueden acceder a la puerta de enlace.

[NSHELP-28942]

Es posible que observe algunas direcciones IP internas de Citrix en el archivo rdx.js.

[NSHELP-28682]

La autenticación de certificados de cliente falla para Citrix SSO para macOS si no hay certificados de cliente en el llavero de macOS.

[NSHELP-28551]

A veces, se desactiva la sesión de un usuario en Citrix Gateway en unos segundos cuando se establece el tiempo de espera por inactividad del cliente.

[NSHELP-28404]

No se puede desvincular una directiva de autorización clásica mediante la interfaz gráfica de usuario. Sin embargo, puede usar la CLI para desvincular la directiva Autenticación, autorización y autorización de auditoría.

Con esta corrección, ahora puede desvincular la directiva de autorización mediante la interfaz gráfica de usuario.

[NSHELP-27064]

El complemento EPA para Windows no utiliza el proxy configurado del equipo local y se conecta directamente al servidor de puerta de enlace.

[NSHELP-24848]

Gateway Insight no muestra información precisa sobre los usuarios de VPN.

[NSHELP-23937]

El complemento VPN no establece el túnel después del inicio de sesión de Windows, si se cumplen las siguientes condiciones:

- El dispositivo Citrix Gateway está configurado para la función Always On
- El dispositivo está configurado para la autenticación basada en certificados con autenticación de dos factores `off`

[NSHELP-23584]

A veces, al navegar por los esquemas, aparece el mensaje de error `Cannot read property 'type 'of undefined`.

[NSHELP-21897]

Si quiere utilizar la funcionalidad Always On VPN antes de iniciar sesión en Windows, se recomienda actualizar a Citrix Gateway 13.0 o posterior. Esto le permite aprovechar las mejoras adicionales introducidas en la versión 13.0 que no están disponibles en la versión 12.1.

[CGOP-19355]

El error de inicio de la aplicación debido a un tíquet de STA no válido no se informa en Gateway Insight.

[CGOP-13621]

El informe Gateway Insight muestra incorrectamente el valor `Local` en lugar de `SAML` en el campo Tipo de autenticación para los errores de SAML.

[CGOP-13584]

En una configuración de alta disponibilidad, durante la conmutación por error de Citrix ADC, el recuento de SR aumenta en lugar del recuento de conmutación por error en Citrix ADM.

[CGOP-13511]

Cuando se inicia una conexión ICA desde un receptor MAC versión 19.6.0.32 o Citrix Virtual Apps and Desktops versión 7.18, la función HDX Insight se inhabilita.

[CGOP-13494]

Cuando la función EDT Insight está habilitada, a veces los canales de audio pueden fallar durante una discrepancia de red.

[CGOP-13493]

Al aceptar conexiones de host local desde el explorador web, el cuadro de diálogo Aceptar conexión para macOS muestra el contenido en inglés independientemente del idioma seleccionado.

[CGOP-13050]

El texto `Home Page` de la página de inicio de la aplicación Citrix SSO > aparece cortado para algunos idiomas.

[CGOP-13049]

Aparece un mensaje de error al agregar o modificar una directiva de sesión desde la GUI de Citrix ADC.

[CGOP-11830]

En Outlook Web App (OWA) 2013, al hacer clic en **Opciones**, en el menú Configuración, aparece el cuadro de diálogo **Error crítico**. Además, la página deja de responder.

[CGOP-7269]

Citrix Web App Firewall

Un dispositivo Citrix ADC puede bloquearse mientras procesa las búsquedas de firmas de BOT con servidores DNS lentos.

[NSHELP-31642]

El dispositivo Citrix ADC puede bloquearse si el scripting entre sitios está habilitado en la regla de firma.

[NSHELP-31617]

Equilibrio de carga

En una configuración de alta disponibilidad, es posible que las sesiones de suscriptor del nodo principal no se sincronicen con el nodo secundario. Este es un caso raro.

[NSLB-7679]

En algunos casos, el estado del servicio no está sincronizado con el estado del monitor.

[NSHELP-31747]

El dispositivo Citrix ADC puede bloquearse y volcar el núcleo si se cumplen las siguientes condiciones:

- La proximidad estática o RTT se utiliza como método de equilibrio de carga principal o de respaldo.
- La persistencia de la dirección IP de origen está habilitada

[NSHELP-31735]

El formato serviceGroupName de la captura `entityofs` del grupo de servicios es el siguiente: `<service(group)name>?<ip/DBS>?<port>`

En el formato de captura, el grupo de servicios se identifica mediante una dirección IP o un nombre y puerto de DBS. El signo de interrogación (?) se utiliza como separador. Citrix ADC envía la captura con el signo de interrogación (?). El formato aparece igual en la GUI de Citrix ADM. Este es el comportamiento esperado.

[NSHELP-28080]

En algunos casos, los servidores enlazados a un grupo de servicios muestran un valor de cookie no válido. Puede ver el valor correcto de la cookie en los registros de seguimiento.

[NSHELP-21196]

Otros

Cuando se produce una sincronización forzada en una configuración de alta disponibilidad, el dispositivo ejecuta el comando `set urlfiltering parameter` en el nodo secundario.
Como resultado, el nodo secundario omite cualquier actualización programada hasta la siguiente hora programada mencionada en el parámetro `TimeOfDayToUpdateDB`.

[NSSWG-849]

El registro de la lista AlwaysOnAllow no funciona como se esperaba si el valor del registro es superior a 2000 bytes.

[NSHELP-31836]

En un dispositivo Citrix ADC, cuando se agrega un disco duro adicional al dispositivo, se crea un enlace para el archivo `/var/nslog` en la carpeta de cierres inesperados `/var/crash/nslog`. Los archivos `newnslog` disponibles en la carpeta crash no se recopilan en la carpeta del recopilador generada por asistencia técnica.

Solución alternativa:

Recopila los archivos newnslog que faltan manualmente.

[NSHELP-31354]

Un dispositivo Citrix ADC puede reiniciarse debido al estancamiento de la CPU de administración si se produce un problema de conectividad con el proveedor externo de filtrado de URL.

[NSHELP-22409]

Redes

En un dispositivo Citrix ADC BLX compatible con DPDK, las VLAN etiquetadas no son compatibles con los puertos NIC DPDK Intel i350. Esto se observa, ya que es un problema conocido presente en el controlador DPDK.

[NSNET-25299]

Es posible que un dispositivo Citrix ADC BLX con DPDK no se reinicie si se cumplen todas las condiciones siguientes:

- El dispositivo Citrix ADC BLX se asigna con un número bajo de `hugepages`. Por ejemplo, 1G.
- El dispositivo Citrix ADC BLX se asigna con una gran cantidad de procesos de trabajo. Por ejemplo, 28.

El problema se registra como un mensaje de error en `/var/log/ns.log`:

- `BLX-DPDK:DPDK Mempool could Not be Initialized for PE-x`

Nota: x es un número <= número de procesos de trabajo.

Solución alternativa:

Asigne un número elevado de `hugepages` y, a continuación, reinicie el dispositivo.

[NSNET-25173]

Es posible que un dispositivo Citrix ADC BLX con DPDK no se reinicie si se cumple la siguiente condición:

- Al dispositivo Citrix ADC BLX se le asigna una gran cantidad de `hugepages`. Por ejemplo, 16 GB.

El problema se registra como un mensaje de error en `/var/log/ns.log`:

- `EAL: rte_mem_virt2phy(): cannot open /proc/self/pagemap: Too many open files`

Solución alternativa:

Use una de las siguientes soluciones para este problema:

- Aumente el límite de archivos abiertos en el host Linux mediante el uso del comando `ulimit` o la modificación del archivo `limits.conf`.
- Reduzca el número de `hugepages` asignadas.

[NSNET-24727]

Un dispositivo Citrix ADC BLX en modo DPDK puede tardar un poco más en reiniciarse debido a la funcionalidad de facilidad de DPDK.

[NSNET-24449]

Las siguientes operaciones de interfaz no son compatibles con las interfaces `X710 10G (i40e)` de Intel en un dispositivo Citrix ADC BLX con DPDK:

- Disable
- Enable
- Reset

[NSNET-16559]

La instalación de un dispositivo Citrix ADC BLX podría fallar en un host Linux basado en Debian (versión 18 y posteriores de Ubuntu) con el siguiente error de dependencia:

```
The following packages have unmet dependencies: blx-core-libs:i386 :
PreDepends: libc6:i386 (>= 2.19)but it is not installable
```

Solución alternativa:

Ejecute los siguientes comandos en la CLI del host Linux antes de instalar un dispositivo Citrix ADC BLX:

- dpkg — agregar arquitectura i386
- actualización apt-get
- apt-get dist-upgrade
- apt-get install libc6:i386

[NSNET-14602]

En algunos casos de conexiones de datos FTP, el dispositivo Citrix ADC solo realiza operaciones NAT y no procesamiento TCP en los paquetes para la negociación TCP MSS. Como resultado, la MTU de interfaz óptima no está configurada para la conexión. Esta configuración de MTU incorrecta provoca la fragmentación de los paquetes y afecta al rendimiento de la CPU.

[NSNET-5233]

Cuando se cambia un límite de memoria de la partición de administración en el dispositivo Citrix ADC, el límite de memoria intermedia TCP se establece automáticamente en el nuevo límite de memoria de la partición de administración.

[NSHELP-21082]

Plataforma

La conmutación por error de alta disponibilidad no funciona en las nubes de AWS y GCP. La CPU de administración puede alcanzar su capacidad del 100% en las nubes de AWS y GCP, y en Citrix ADC VPX en las instalaciones. Ambos problemas se producen cuando se cumplen las siguientes condiciones:

1. Durante el primer arranque del dispositivo Citrix ADC, no guarda la contraseña solicitada.

2. Posteriormente, reinicie el dispositivo Citrix ADC.

[NSPLAT-22013]

Cuando actualiza de compilaciones 13.0/12.1/11.1 a una versión 13.1 o baja de una compilación 13.1 a 13.0/12.1/11.1, algunos paquetes python no se instalan en los dispositivos Citrix ADC. Este problema se ha solucionado en las siguientes versiones de Citrix ADC:

- 13.1-4.x
- 13.0-82.31 y posteriores
- 12.1-62.21 y posteriores

Los paquetes python no se instalan cuando se degrada la versión de Citrix ADC de la versión 13.1-4.x a cualquiera de las siguientes versiones:

- Cualquier compilación 11.1
- 12.1-62.21 y anteriores
- 13.0-81.x y anteriores

[NSPLAT-21691]

En una configuración de clúster en un dispositivo Citrix ADC SDX, hay una discordancia de CLAG MAC en el segundo nodo y CLIP si se cumplen las siguientes condiciones:

- El CLAG se crea en una NIC Mellanox.
- Agrega otra instancia VPX al clúster y a la configuración de CLAG.

Como resultado, el tráfico a la instancia VPX se detiene.

[NSPLAT-21049]

En una configuración de clúster en un dispositivo Citrix ADC SDX, el primer nodo se cae debido a una discordancia de direcciones MAC en la tabla CLIP y MAC, si se cumplen las siguientes condiciones:

- El CLAG se crea en una NIC Mellanox.
- Quita el segundo nodo del clúster.

[NSPLAT-21042]

Al eliminar una configuración de escalabilidad automática o un conjunto de escalas de VM de un grupo de recursos de Azure, elimine la configuración del perfil de nube correspondiente de la instancia de Citrix ADC. Utilice el comando `rm cloudprofile` para borrar el perfil.

[NSPLAT-4520]

En una configuración de alta disponibilidad en Azure, al iniciar sesión en el nodo secundario a través de la GUI, aparece la pantalla de usuario por primera vez (FTU) para la configuración del perfil de nube de escalabilidad automática.
Solución temporal: omita la pantalla e inicie sesión en el nodo principal para crear el perfil de nube. El perfil de la nube siempre debe configurarse en el nodo principal.

[NSPLAT-4451]

A partir de la versión 13.1 de Citrix ADC, el dispositivo Citrix ADC no se inicia en un hipervisor ESXi con más de 8 interfaces de red VMXNET3.

[NSHELP-31266]

Directivas

Las conexiones pueden bloquearse si el tamaño de los datos de procesamiento es mayor que el tamaño de búfer TCP predeterminado configurado.Solución temporal: establezca el tamaño del búfer TCP en el tamaño máximo de los datos que deben procesarse.

[NSPOLICY-1267]

SSL

En un clúster heterogéneo de dispositivos Citrix ADC SDX 22000 y Citrix ADC SDX 26000, se produce una pérdida de configuración de entidades SSL si se reinicia el dispositivo SDX 26000.

Solución alternativa:

1. En el CLIP, inhabilite SSLv3 en todas las entidades SSL nuevas y existentes, como servidores virtuales, servicios, grupos de servicios y servicios internos. Por ejemplo, `set ssl vserver <name> -SSL3 DISABLED`.
2. Guarde la configuración.

[NSSSL-9572]

No se puede agregar un objeto de Azure Key Vault si ya se ha agregado un objeto de autenticación de Azure Key Vault.

[NSSSL-6478]

Puede crear varias entidades de la aplicación Azure con el mismo ID de cliente y secreto de cliente. El dispositivo Citrix ADC no devuelve ningún error.

[NSSSL-6213]

El siguiente mensaje de error incorrecto aparece al quitar una clave HSM sin especificar KEYVAULT como tipo HSM.
ERROR: Actualización de crl inhabilitada

[NSSSL-6106]

La actualización automática de claves de sesión aparece incorrectamente como inhabilitada en una dirección IP de clúster. (Esta opción no se puede desactivar).

[NSSSL-4427]

Aparece `Warning: No usable ciphers configured on the SSL vserver/service,,` un mensaje de advertencia incorrecto, si intenta cambiar el protocolo o el cifrado SSL en el perfil SSL.

[NSSSL-4001]

Un tíquet de sesión caducado se respeta en un nodo que no es de CCO y en un nodo de alta disponibilidad después de una conmutación por error de alta disponibilidad. [NSSSL-3184, NSSSL-1379, NSSSL-1394]

Un dispositivo Citrix ADC puede bloquearse en las siguientes situaciones:

- Un monitor de equilibrio de carga de tipo SSL y el servicio SSL tienen el mismo nombre
- Se cambia el nombre de un servicio SSL
- Se elimina un monitor de equilibrio de carga

[NSHELP-30445]

Sistema

El valor MAX_CONCURRENT_STREAMS se establece en 100 de forma predeterminada si el dispositivo no recibe el marco de configuración max_concurrent_stream del cliente.

[NSHELP-21240]

Los contadores mptcp_cur_session_without_subflow disminuyen incorrectamente a un valor negativo en lugar de cero.

[NSHELP-10972]

En una implementación de clúster, si ejecuta un comando `force cluster sync` en un nodo que no es de CCO, el archivo ns.log contiene entradas de registro duplicadas. [NSBASE-16304, NSGI-1293]

Cuando instala Citrix ADM en un clúster de Kubernetes, no funciona según lo esperado porque es posible que los procesos necesarios no aparezcan.

Solución temporal: reinicie el pod de administración.

[NSBASE-15556]

La IP del cliente y la IP del servidor se invierten en el registro SkipFlow de HDX Insight cuando se configura el tipo de transporte LogStream para Insight

[NSBASE-8506]

Interfaz de usuario

Para la función Reescritura de MQTT, no puede eliminar una expresión mediante el Editor de expresiones en la GUI.

Solución alternativa:

Use el comando de acción add o edit de tipo MQTT a través de la CLI.

[NSUI-18049]

En la GUI de Citrix ADC, el enlace `Help` presente debajo de la ficha `Dashboard` no funciona.

[NSUI-14752]

El asistente Crear/Supervisar CloudBridge Connector podría dejar de responder o no configurar un conector de cloudbridge.

Solución alternativa:

Configure los conectores cloudbridge agregando perfiles IPsec, túneles IP y reglas PBR mediante la GUI o CLI de Citrix ADC.

[NSUI-13024]

Si crea una clave ECDSA mediante la interfaz gráfica de usuario, no se muestra el tipo de curva.

[NSUI-6838]

En una configuración de alta disponibilidad, las sesiones de usuario VPN se desconectan si se cumple la siguiente condición:

- Si se realizan dos o más operaciones de failover manual de alta disponibilidad sucesivas cuando la sincronización de alta disponibilidad está en curso.

Solución alternativa:

Realice una conmutación por error manual de alta disponibilidad sucesiva solo después de que se haya completado la sincronización de alta disponibilidad (ambos nodos están en estado de sincronización correcta).

[NSHELP-25598]

En una configuración de alta disponibilidad de los dispositivos Citrix ADC BLX, es posible que el nodo principal deje de responder bloqueando cualquier solicitud de CLI o API.

Solución alternativa:

Reinicie el nodo principal.

[NSCONFIG-6601]

Si usted (administrador del sistema) realiza todos los pasos siguientes en un dispositivo Citrix ADC, es posible que los usuarios del sistema no inicien sesión en el dispositivo Citrix ADC degradado.

1. Actualice el dispositivo Citrix ADC a una de las compilaciones:
    - 13.0 52.24 compilación
    - 12.1 57,18 compilación

- 11.1 65.10 compilación

2. Agregar un usuario del sistema o cambiar la contraseña de un usuario del sistema existente y guardar la configuración, y
3. Rebaja la versión del dispositivo Citrix ADC a cualquier versión anterior.

Para mostrar la lista de estos usuarios del sistema mediante la CLI:
En el símbolo del sistema, escriba:

```
query ns config -changedpassword [-config <full path of the configuration file (ns.conf)>]
```

Solución alternativa:

Para solucionar este problema, utilice una de las siguientes opciones independientes:

- Si el dispositivo Citrix ADC aún no se ha rebajado (paso 3 de los pasos mencionados anteriormente), revierta la versión del dispositivo Citrix ADC con un archivo de configuración del que se ha creado previamente una copia de seguridad (ns.conf) de la misma compilación de la versión.
- Cualquier administrador del sistema cuya contraseña no se haya cambiado en la compilación actualizada puede iniciar sesión en la compilación degradada y actualizar las contraseñas de otros usuarios del sistema.
- Si ninguna de las opciones anteriores funciona, el administrador del sistema puede restablecer las contraseñas de usuario del sistema.

Para obtener más información, consulte https://docs.citrix.com/en-us/citrix-adc/13/system/ns-ag-aa-intro-wrapper-con/ns-ag-aa-reset-default-amin-pass-tsk.html

[NSCONFIG-3188]

Notas de la versión de Citrix ADC 13.1-24.38

July 27, 2022

Este documento de notas de la versión describe las mejoras y los cambios, los problemas resueltos y conocidos que existen para la versión 13.1-24.38 de Citrix ADC.

Notas

Este documento de notas de la versión no incluye correcciones relacionadas con la seguridad. Para obtener una lista de correcciones y avisos relacionados con la seguridad, consulte el boletín de seguridad de Citrix.

Las compilaciones 13.1-24.38 y posteriores abordan las vulnerabilidades de seguridad descritas en https://support.citrix.com/article/CTX457836.

Novedades

Las mejoras y los cambios que están disponibles en la compilación 13.1-24.38.

Equilibrio de carga

Soporte de conmutación por error de conexión para el modo INC de alta disponibilidad

Citrix ADC ahora admite la conmutación por error de conexión para el modo INC de alta disponibilidad cuando se cumplen todas las condiciones siguientes:

- El tipo de servicio de servidor virtual es ANY.
- El modo es DSR (MAC, IPTUNNEL o TOS).
- USIP está habilitado en los servicios enlazados al servidor virtual.

[NSLB-9121]

Soporte para registros de la CAA

El dispositivo Citrix ADC ahora admite la adición de registros de autorización de la entidad de certificación (CAA). El registro CAA es un tipo de registro del Sistema de nombres de dominio (DNS) que permite a los propietarios del dominio especificar qué entidad de certificación (CA) puede emitir certificados SSL para el dominio.

Esta mejora proporciona una capa adicional de protección a su presencia en la web. No tener registros de la CAA puede provocar un riesgo de seguridad, ya que cualquiera puede generar una solicitud de firma de certificado (CSR) para el dominio y obtener la firma del certificado por cualquier CA.

[NSLB-9007]

Plataforma

En la plataforma Citrix ADC SDX 8015, la versión de administración de luces apagadas (LOM) se actualiza de 3.21 a 3.56.

En las plataformas Citrix ADC SDX 14000, SDX 14000-40G, SDX 14000-40S y SDX 14000-FIPS, la versión LOM se actualiza de 4.08 a 4.14.

[NSPLAT-23416]

Compatibilidad con Autoscale de backend de Citrix ADC en Azure con VMSS en todos los grupos de recursos

La instancia de Citrix ADC VPX ahora admite el Autoescalado de fondo de Azure en todos los grupos de recursos en los siguientes casos:

La instancia de Azure VMSS y Citrix ADC VPX se implementan en la misma red virtual de Azure.
La instancia de Azure VMSS y Citrix ADC VPX se implementan en diferentes redes virtuales de Azure que están en la misma suscripción de Azure. Estas dos redes virtuales deben estar conectadas mediante la función de emparejamiento de redes virtuales de Azure.

Esta función le permite segregar las aplicaciones y los recursos de red en diferentes grupos de recursos.

Anteriormente, Autoscale de back-end de Citrix ADC en Azure solo funcionaba si la instancia de VMSS y Citrix ADC VPX se implementaban en el mismo grupo de recursos.

[NSPLAT-16664]

Sistema

Suscribir contadores en el recopilador de métricas

El dispositivo Citrix ADC ahora admite una opción para suscribir contadores en el recopilador de métricas.
El recopilador de métricas admite la exportación de datos de análisis de series temporales cada 30 segundos en diferentes formatos, como AVRO, formato Prometheus y formato Influx DB. El recopilador de métricas admite la actualización dinámica de contadores, lo que le permite agregar los contadores necesarios a un archivo de esquema. Puede configurar el nombre del archivo de esquema mediante la interfaz CLI. El recopilador de métricas lee los nombres de los contadores del archivo de esquema y los exporta.

Anteriormente, el recopilador de métricas solo permitía exportar un conjunto predefinido de contadores en tiempo de compilación. Cualquier cambio en la lista de contadores requería una actualización de la compilación.
Para obtener más información, consulte https://docs.citrix.com/en-us/citrix-adc/current-release/ns-ag-appflow-intro-wrapper-con/ns-ag-appflow-config-tsk.html.

[NSBASE-11595]

Interfaz de usuario

Configurar alertas de caducidad de licencias de Citrix ADC

Ahora puede configurar el dispositivo Citrix ADC para que realice las siguientes operaciones de alerta durante un número específico de días antes de que caduque una licencia de Citrix ADC:

- Muestra un anuncio de alerta de caducidad de licencia en la GUI de Citrix ADC.
- Envía capturas SNMP que contienen la información de caducidad de la licencia a intervalos regulares a los oyentes de capturas configurados si la alarma SNMP `NS_LICENSE_EXPIRY` está habilitada.

[NSCONFIG-6360]

Problemas resueltos

Los problemas que se abordan en la compilación 13.1-24.38.

Autenticación, autorización y auditoría

En una configuración de puerta de enlace unificada, en raras ocasiones se le puede presentar una página de inicio de sesión nuevo al acceder a los servicios detrás de la puerta de enlace unificada, incluso después de que la autenticación se haya realizado correctamente.

[NSHELP-31148, NSHELP-27994]

El SSO basado en formularios falla para los servidores backend que envían parámetros de clave-valor en la consulta de URL.

[NSHELP-30975]

El dispositivo Citrix ADC puede bloquearse debido a una gran asignación de memoria debido a la falta de una URL de destino en la configuración de OAuth.

[NSHELP-30963]

Es posible que experimentes problemas intermitentes con la autenticación RADIUS al usar Chrome en modo incógnito.

[NSHELP-30944]

El módulo Autenticación, autorización y auditoríaD del dispositivo Citrix ADC puede bloquearse debido a una longitud de contraseña entrante faltante o incorrecta del motor de paquetes a Autenticación, autorización y auditoríaD.

[NSHELP-30911]

El dispositivo Citrix ADC se bloquea durante la operación de inserción de nFactor.

[NSHELP-30577]

Puede haber un error intermitente al conectarse al servidor de Exchange de Outlook a través de la aplicación Outlook debido a la adición incorrecta de encabezados por parte del dispositivo Citrix ADC.

[NSHELP-30555]

El dispositivo Citrix ADC puede bloquearse debido a daños en la memoria en caso de que se produzca un error de comunicación de núcleo a núcleo.

[NSHELP-30275]

El inicio de sesión único falla durante una sesión de autenticación cuando se activa el evento de cambio de contraseña. Este problema solo se produce si el parámetro persistentLogin attempts está habilitado.

[NSHELP-28085]

En algunos casos, se muestra un mensaje de error `invalid credentials` durante el proceso de autenticación RADIUS. El error aparece cuando se accede al dispositivo Citrix ADC desde un dispositivo cliente mediante el explorador Google Chrome.

[NSHELP-27113]

Cuando un dispositivo Citrix ADC realiza una búsqueda de grupos LDAP anidada, se pierde parte de la información de los grupos del directorio activo debido a un comportamiento no válido del dispositivo Citrix ADC. El dispositivo ADC toma un valor incorrecto incluso cuando el parámetro `groupSearchSubAttribute` está configurado correctamente.

[NSHELP-26316]

El dispositivo Citrix ADC descarga el núcleo cuando NOAUTH se configura como primer factor y Negotiate como el factor posterior en el flujo de autenticación basado en 401.

[NSHELP-25203]

Dispositivo Citrix ADC SDX

En una GUI de Citrix ADC SDX, mostrar los servidores NTP puede congelar la interfaz de usuario si el archivo de configuración NTP (ntp.conf) solo tiene espacios en alguna de las líneas.

[NSHELP-31530]

En un dispositivo Citrix ADC SDX con NIC Mellanox, modificar el rendimiento de una instancia VPX que tiene NIC Mellanox reinicia la instancia VPX.

[NSHELP-31305]

Después de actualizar un dispositivo Citrix ADC SDX a la versión 13.1 compilación 21.50 o posterior, el descifrado SSL y la comparación de MAC pueden fallar. Como resultado, es posible que vea fallas de protocolo de enlace SSL, inestabilidad del estado de VPX, falta de disponibilidad de la GUI de la instancia VPX y caídas de aplicaciones y servidores virtuales.

Nota: Este problema se observa en las plataformas SDX 8900, SDX 15000, SDX 15000-50G, SDX 26000 y SDX 26000-50S.

[NSHELP-31672]

Citrix Gateway

En raras ocasiones, el dispositivo Citrix ADC configurado con el servidor virtual VPN puede fallar después de iniciar sesión correctamente en Citrix Gateway.

[NSHELP-31481]

En una configuración de DTLS de ICA, el dispositivo Citrix Gateway se bloquea al procesar el tíquet de STA.

[NSHELP-31211]

El dispositivo Citrix ADC registra incorrectamente el mensaje `UDPFLOWSTAT` que indica que el tráfico como `Allowed` es el tráfico UDP denegado por una directiva de autorización.

[NSHELP-29542]

Se observa una pérdida de memoria en un dispositivo Citrix ADC cuando se configura un proxy saliente.

[NSHELP-29234]

La página Sesión de usuarios activos no muestra todas las sesiones de usuario activas a menos que el número de entradas se cambie a 2000 por página.

Con esta solución, se agrega un nuevo enlace `All user session` (Citrix Gateway -> Supervisar conexiones > Todas las sesiones de usuario) en la interfaz de usuario de administración que enumera todas las sesiones y conexiones de los usuarios.

[NSHELP-29151]

El resultado del comando `show vpn icaConnection` no muestra correctamente los números de serie de las conexiones ICA. Este problema se produce porque el número de serie se restablece arbitrariamente cuando `show vpn icaconnection` se ejecuta.

[NSHELP-25646]

Citrix Web App Firewall

Una directiva de Web App Firewall se puede guardar dos veces en el archivo configuration (`ns.conf`).

[NSHELP-30899]

En la inyección de SQL de WAF que contiene una comilla (comilla simple, comilla doble o marca inversa), la cotización de apertura y cierre debe estar presente para marcar el patrón como un ataque. Sin embargo, cuando hay un comentario en el patrón, no se requiere la cotización de cierre.

[NSHELP-30379]

Equilibrio de carga

El prefijo de ámbito no se establece correctamente cuando ECS está habilitado en el dispositivo ADC y no se encuentra la ubicación. Este problema provoca la creación de una entrada de persistencia incorrecta. La entrada de persistencia incorrecta se crea en función de la dirección IP de LDNS en lugar de la dirección IP de ECS recibida en la solicitud del método GSLB no estático basado en proximidad.

[NSHELP-30846]

En un caso poco común de condiciones de carrera, el motor de paquetes puede fallar con el volcado de memoria cuando se presenta la siguiente configuración en el dispositivo Citrix ADC:

- El servidor virtual GSLB está configurado con la persistencia basada en la dirección IP de origen y el registro DNS está habilitado en el perfil DNS enlazado al servicio ADNS.
- El servidor de equilibrio de carga de DNS está configurado sin el registro de DNS habilitado en el perfil de DNS.

[NSHELP-29791]

Otros

La interfaz de usuario de jQuery del portal se actualiza de 1.12.1 a 1.13.1 para solucionar la vulnerabilidad descrita en los boletines de seguridad: CVE-2021-41182, CVE-2021-41183 y CVE-2021-41184.

[NSHELP-30209]

Redes

En un host Linux basado en Debian (Ubuntu versión 18 y posteriores), un dispositivo Citrix ADC BLX siempre se implementa en modo compartido independientemente de la configuración del archivo de configuración BLX()/`etc/blx/blx.conf`. Este problema se produce porque `mawk`, que está presente de forma predeterminada en los sistemas Linux basados en Debian, no ejecuta algunos de los comandos awk presentes en el archivo `blx.conf`.

[NSNET-14603]

En una configuración NAT44 a gran escala, el dispositivo Citrix ADC puede bloquearse mientras recibe tráfico SIP por el siguiente motivo:

- Las entradas de mapeo y filtrado LSN no están presentes en el dispositivo.

[NSHELP-30225]

El dispositivo Citrix ADC puede bloquearse si desvincula un conjunto de datos de una regla de ACL cuando algunos paquetes coinciden con la regla de ACL.

[NSHELP-30221]

En una configuración NAT44 a gran escala, el dispositivo Citrix ADC puede bloquearse mientras recibe tráfico SIP por el siguiente motivo:

- El recuento de referencias de sesión no es cero al eliminar una entrada de filtrado.

[NSHELP-29348]

Plataforma

En un dispositivo Citrix ADC SDX con imagen de paquete único (SBI) y VPX versiones 13.1-24.x o posteriores, se admite la implementación activa-activa mediante VRRP en NIC de Fortville. Esta implementación no se admite en el modo L2.

Los siguientes puntos se aplican a la implementación:

- Citrix recomienda eliminar la configuración de VRID del servicio de administración antes de actualizar o degradar la instancia VPX asociada. Agregue la configuración de VRID desde Management Service una vez finalizada la operación de actualización o degradación.
- Si no sigue la recomendación anterior, debe volver a detectar manualmente las instancias VPX desde Management Service para habilitar la convergencia de VRRP.

[NSHELP-30670]

La conmutación por error de alta disponibilidad para la instancia de Citrix ADC VPX en la nube de GCP y AWS falla cuando la contraseña de un nodo RPC contiene un carácter especial.

[NSHELP-28600]

Directivas

En algunos casos, un dispositivo Citrix ADC puede bloquearse cuando se utiliza una acción de asignación con la operación de borrado de una variable de AppExpert.

[NSHELP-29766]

SSL

Un dispositivo FIPS Citrix ADC MPX/SDX 14000 puede bloquearse debido al uso continuo de API para operaciones de cifrado, por parte de aplicaciones internas como SAML, durante un período de tiempo.

[NSHELP-27952]

Sistema

El recopilador REST está inactivo incluso cuando el parámetro AppFlow `TimeSeriesOverNSIP` está habilitado.

[NSHELP-30759]

En un dispositivo Citrix ADC, se observa un problema de latencia en las transacciones HTTP/2 si se cumplen las siguientes condiciones:

- La configuración SSL HTTP/2 está habilitada en el servicio de back-end
- El servicio no admite el protocolo HTTP/2.

[NSHELP-30020]

El dispositivo Citrix ADC informa de una falsa alarma SNMP en los contadores de inundación SYN del servicio.

[NSHELP-28710, NSHELP-28713]

Interfaz de usuario

Si se actualiza un dispositivo Citrix ADC configurado con licencias agrupadas, es posible que el dispositivo se reinicie con una configuración parcial.

[NSHELP-30926]

En un dispositivo Citrix ADC, el enlace de la directiva de caché para anular el global o el global predeterminado mediante la interfaz GUI falla con el siguiente error:

- Falta el argumento obligatorio.

Este error no se ve al vincular la directiva de caché mediante la interfaz CLI.

[NSHELP-30826]

El filtro de búsqueda no está disponible para la clave 'Nombre' en la página Administrar certificados > CSR de la GUI de Citrix ADC.

[NSHELP-30274]

Problemas conocidos

Los problemas que existen en la versión 13.1-24.38.

AppFlow

HDX Insight no informa de un error de inicio de aplicación causado por un usuario que intenta iniciar una aplicación o un escritorio a los que el usuario no tiene acceso.

[NSINSIGHT-943]

Autenticación, autorización y auditoría

Un dispositivo Citrix ADC no autentica los intentos de inicio de sesión con contraseñas duplicadas y evita los bloqueos de cuentas.

[NSHELP-563]

LoginSchema de DualAuthPushOrOTP.xml no aparece correctamente en la pantalla del editor de esquemas de inicio de sesión de la GUI de Citrix ADC.

[NSAUTH-6106]

El perfil proxy ADFS se puede configurar en una implementación de clúster. El estado de un perfil proxy se muestra incorrectamente en blanco al ejecutar el siguiente comando.
`show adfsproxyprofile <profile name>`

Solución alternativa:

Conéctese al Citrix ADC activo principal del clúster y ejecute el comando `show adfsproxyprofile <profile name>`. Mostraría el estado del perfil de proxy.

[NSAUTH-5916]

La página Configurar servidor LDAP de autenticación de la GUI de Citrix ADC deja de responder si sigue los pasos siguientes:

- Se abre la opción Probar accesibilidad LDAP.
- Las credenciales de inicio de sesión no válidas se rellenan y envían.
- Las credenciales de inicio de sesión válidas se rellenan y envían.

Solución alternativa:

Cierre y abra la opción Probar accesibilidad de LDAP.

[NSAUTH-2147]

Almacenamiento en caché

Es posible que un dispositivo Citrix ADC se bloquee si la función Almacenamiento en caché integrado está habilitada y el dispositivo tiene poca memoria.

[NSHELP-22942]

Dispositivo Citrix ADC SDX

En un dispositivo Citrix ADC SDX, si el CLAG se crea en una NIC Mellanox, la MAC de CLAG cambia cuando se reinicia la instancia VPX. El tráfico a la instancia VPX se detiene tras el reinicio porque la tabla MAC tiene la antigua entrada MAC de CLAG.

[NSSVM-4333]

La instalación de un certificado SSL en un dispositivo Citrix ADC SDX falla si el nombre del certificado o el nombre de la clave contienen algún espacio.

[NSHELP-31711]

En un dispositivo Citrix ADC SDX, las instancias de ADC no alcanzan su capacidad máxima al configurar el modo de asignación de rendimiento en ráfagas.

[NSHELP-27477]

Las caídas de paquetes se observan en una instancia VPX alojada en un dispositivo Citrix ADC SDX si se cumplen las siguientes condiciones:

- El modo de asignación de rendimiento está en ráfaga.
- Existe una gran diferencia entre el rendimiento y la capacidad máxima de ráfaga.

[NSHELP-21992]

Citrix Gateway

Cuando se configura AlwaysOn, se produce un error en el túnel de usuario debido al número de versión incorrecto (1.1.1.1) en el archivo aoservice.exe.

[NSHELP-30662]

Los usuarios no pueden conectarse al dispositivo Citrix Gateway después de cambiar el parámetro "networkAccessOnVPNFailure" siempre en el perfil de "fullAccess" a "onlyToGateway".

[NSHELP-30236]

La página principal de la puerta de enlace no se muestra inmediatamente después de que el plug-in de puerta de enlace establezca el túnel VPN correctamente. Para solucionar este problema, se introduce el siguiente valor de registro.
\HKLM\Software\Citrix\Secure Access Client\SecureChannelResetTimeoutSeconds
Tipo: DWORD

[NSHELP-30189]

El cliente VPN de Windows no respeta la alerta de "notificación de cierre SSL" del servidor y envía la solicitud de inicio de sesión de transferencia en la misma conexión.

[NSHELP-29675]

En algunos casos, el código de validación del servidor falla cuando se confía en el certificado del servidor. Como resultado, los usuarios finales no pueden acceder a la puerta de enlace.

[NSHELP-28942]

Es posible que observe algunas direcciones IP internas de Citrix en el archivo rdx.js.

[NSHELP-28682]

La autenticación de certificados de cliente falla para Citrix SSO para macOS si no hay certificados de cliente en el llavero de macOS.

[NSHELP-28551]

A veces, se desactiva la sesión de un usuario en Citrix Gateway en unos segundos cuando se establece el tiempo de espera por inactividad del cliente.

[NSHELP-28404]

No se puede desvincular una directiva de autorización clásica mediante la interfaz gráfica de usuario. Sin embargo, puede usar la CLI para desvincular la directiva Autenticación, autorización y autorización de auditoría.

Con esta corrección, ahora puede desvincular la directiva de autorización mediante la interfaz gráfica de usuario.

[NSHELP-27064]

El complemento EPA para Windows no utiliza el proxy configurado del equipo local y se conecta directamente al servidor de puerta de enlace.

[NSHELP-24848]

Gateway Insight no muestra información precisa sobre los usuarios de VPN.

[NSHELP-23937]

El complemento VPN no establece un túnel después del inicio de sesión de Windows si se cumplen las siguientes condiciones:

- El dispositivo Citrix Gateway está configurado para la función Always On
- El dispositivo está configurado para la autenticación basada en certificados con autenticación de dos factores `off`

[NSHELP-23584]

A veces, al navegar por los esquemas, aparece el mensaje de error `Cannot read property 'type 'of undefined`.

[NSHELP-21897]

Si quiere utilizar la funcionalidad Always On VPN antes de iniciar sesión en Windows, se recomienda actualizar a Citrix Gateway 13.0 o posterior. Esto le permite aprovechar las mejoras adicionales introducidas en la versión 13.0 que no están disponibles en la versión 12.1.

[CGOP-19355]

El error de inicio de la aplicación debido a un tíquet STA no válido no se informa en Gateway Insight.

[CGOP-13621]

El informe Gateway Insight muestra incorrectamente el valor `Local` en lugar de `SAML` en el campo Tipo de autenticación para los errores de SAML.

[CGOP-13584]

En una configuración de alta disponibilidad, durante la conmutación por error de Citrix ADC, el recuento de SR aumenta en lugar del recuento de conmutación por error en Citrix ADM.

[CGOP-13511]

Cuando se inicia una conexión ICA desde un receptor MAC versión 19.6.0.32 o Citrix Virtual Apps and Desktops versión 7.18, la función HDX Insight se inhabilita.

[CGOP-13494]

Cuando la función EDT Insight está habilitada, a veces los canales de audio pueden fallar durante una discrepancia de red.

[CGOP-13493]

Al aceptar conexiones de host local desde el explorador web, el cuadro de diálogo Aceptar conexión para macOS muestra el contenido en inglés independientemente del idioma seleccionado.

[CGOP-13050]

El texto `Home Page` de la página de inicio de la aplicación Citrix SSO > aparece cortado para algunos idiomas.

[CGOP-13049]

Aparece un mensaje de error al agregar o modificar una directiva de sesión desde la GUI de Citrix ADC.

[CGOP-11830]

En Outlook Web App (OWA) 2013, al hacer clic en **Opciones**, en el menú Configuración, aparece el cuadro de diálogo **Error crítico**. Además, la página deja de responder.

[CGOP-7269]

Equilibrio de carga

En una configuración de alta disponibilidad, es posible que las sesiones de suscriptor del nodo principal no se sincronicen con el nodo secundario. Este es un caso raro.

[NSLB-7679]

El formato serviceGroupName de la captura `entityofs` del grupo de servicios es el siguiente: `<service(group)name>?<ip/DBS>?<port>`

En el formato de captura, el grupo de servicios se identifica mediante una dirección IP o un nombre y puerto de DBS. El signo de interrogación (?) se utiliza como separador. Citrix ADC envía la captura

con el signo de interrogación (?). El formato aparece igual en la GUI de Citrix ADM. Este es el comportamiento esperado.

[NSHELP-28080]

En algunos casos, los servidores enlazados a un grupo de servicios muestran un valor de cookie no válido. Puede ver el valor correcto de la cookie en los registros de seguimiento.

[NSHELP-21196]

Otros

Cuando se produce una sincronización forzada en una configuración de alta disponibilidad, el dispositivo ejecuta el comando `set urlfiltering parameter` en el nodo secundario.
Como resultado, el nodo secundario omite cualquier actualización programada hasta la siguiente hora programada mencionada en el parámetro `TimeOfDayToUpdateDB`.

[NSSWG-849]

Un dispositivo Citrix ADC puede reiniciarse debido al estancamiento de la CPU de administración si se produce un problema de conectividad con el proveedor externo de filtrado de URL.

[NSHELP-22409]

Redes

En un dispositivo Citrix ADC BLX compatible con DPDK, las VLAN etiquetadas no son compatibles con los puertos NIC DPDK Intel i350. Esto se observa, ya que es un problema conocido presente en el controlador DPDK.

[NSNET-25299]

Es posible que un dispositivo Citrix ADC BLX con DPDK no se reinicie si se cumplen todas las condiciones siguientes:

- El dispositivo Citrix ADC BLX se asigna con un número bajo de `hugepages`. Por ejemplo, 1G.
- El dispositivo Citrix ADC BLX se asigna con una gran cantidad de procesos de trabajo. Por ejemplo, 28.

El problema se registra como un mensaje de error en `/var/log/ns.log`:

- `BLX-DPDK:DPDK Mempool could Not be Initialized for PE-x`

Nota: x es un número <= número de procesos de trabajo.

Solución alternativa:

Asigne un número elevado de `hugepages` y, a continuación, reinicie el dispositivo.

[NSNET-25173]

Es posible que un dispositivo Citrix ADC BLX con DPDK no se reinicie si se cumple la siguiente condición:

- Al dispositivo Citrix ADC BLX se le asigna una gran cantidad de hugepages. Por ejemplo, 16 GB.

El problema se registra como un mensaje de error en /var/log/ns.log:

- EAL: rte_mem_virt2phy(): cannot open /proc/self/pagemap: Too many open files

Solución alternativa:

Use una de las siguientes soluciones para este problema:

- Aumente el límite de archivos abiertos en el host Linux mediante el uso del comando ulimit o la modificación del archivo limits.conf.
- Reduzca el número de hugepages asignadas.

[NSNET-24727]

Un dispositivo Citrix ADC BLX en modo DPDK puede tardar un poco más en reiniciarse debido a la funcionalidad de facilidad de DPDK.

[NSNET-24449]

Las siguientes operaciones de interfaz no son compatibles con las interfaces X710 10G (i40e) de Intel en un dispositivo Citrix ADC BLX con DPDK:

- Disable
- Enable
- Reset

[NSNET-16559]

La instalación de un dispositivo Citrix ADC BLX podría fallar en un host Linux basado en Debian (versión 18 y posteriores de Ubuntu) con el siguiente error de dependencia:

```
The following packages have unmet dependencies: blx-core-libs:i386 :
PreDepends: libc6:i386 (>= 2.19)but it is not installable
```

Solución alternativa:

Ejecute los siguientes comandos en la CLI del host Linux antes de instalar un dispositivo Citrix ADC BLX:

- dpkg — agregar arquitectura i386
- actualización apt-get
- apt-get dist-upgrade
- apt-get install libc6:i386

[NSNET-14602]

En algunos casos de conexiones de datos FTP, el dispositivo Citrix ADC solo realiza operaciones NAT y no procesamiento TCP en los paquetes para la negociación TCP MSS. Como resultado, la MTU de interfaz óptima no está configurada para la conexión. Esta configuración de MTU incorrecta provoca la fragmentación de los paquetes y afecta al rendimiento de la CPU.

[NSNET-5233]

Cuando se cambia un límite de memoria de la partición de administración en el dispositivo Citrix ADC, el límite de memoria intermedia TCP se establece automáticamente en el nuevo límite de memoria de la partición de administración.

[NSHELP-21082]

Plataforma

La conmutación por error de alta disponibilidad no funciona en las nubes de AWS y GCP. La CPU de administración puede alcanzar su capacidad del 100% en las nubes de AWS y GCP, y en Citrix ADC VPX en las instalaciones. Ambos problemas se producen cuando se cumplen las siguientes condiciones:

1. Durante el primer arranque del dispositivo Citrix ADC, no guarda la contraseña solicitada.
2. Posteriormente, reinicie el dispositivo Citrix ADC.

[NSPLAT-22013]

Cuando actualiza de compilaciones 13.0/12.1/11.1 a una versión 13.1 o baja de una compilación 13.1 a 13.0/12.1/11.1, algunos paquetes python no se instalan en los dispositivos Citrix ADC. Este problema se ha solucionado en las siguientes versiones de Citrix ADC:

- 13.1-4.x
- 13.0-82.31 y posteriores
- 12.1-62.21 y posteriores

Los paquetes python no se instalan cuando se degrada la versión de Citrix ADC de la versión 13.1-4.x a cualquiera de las siguientes versiones:

- Cualquier compilación 11.1
- 12.1-62.21 y anteriores
- 13.0-81.x y anteriores

[NSPLAT-21691]

En una configuración de clúster en un dispositivo Citrix ADC SDX, hay una discordancia de CLAG MAC en el segundo nodo y CLIP si se cumplen las siguientes condiciones:

- El CLAG se crea en una NIC Mellanox.
- Agrega otra instancia VPX al clúster y a la configuración de CLAG.

Como resultado, el tráfico a la instancia VPX se detiene.

[NSPLAT-21049]

En una configuración de clúster en un dispositivo Citrix ADC SDX, el primer nodo se cae debido a una discordancia de direcciones MAC en la tabla CLIP y MAC, si se cumplen las siguientes condiciones:

- El CLAG se crea en una NIC Mellanox.
- Quita el segundo nodo del clúster.

[NSPLAT-21042]

Al eliminar una configuración de escalabilidad automática o un conjunto de escalas de VM de un grupo de recursos de Azure, elimine la configuración del perfil de nube correspondiente de la instancia de Citrix ADC. Utilice el comando `rm cloudprofile` para borrar el perfil.

[NSPLAT-4520]

En una configuración de alta disponibilidad en Azure, al iniciar sesión en el nodo secundario a través de la GUI, aparece la pantalla de usuario por primera vez (FTU) para la configuración del perfil de nube de escalabilidad automática.
Solución temporal: omita la pantalla e inicie sesión en el nodo principal para crear el perfil de nube. El perfil de la nube siempre debe configurarse en el nodo principal.

[NSPLAT-4451]

A partir de la versión 13.1 de Citrix ADC, el dispositivo Citrix ADC no se inicia en un hipervisor ESXi con más de 8 interfaces de red VMXNET3.

[NSHELP-31266]

Directivas

Las conexiones pueden bloquearse si el tamaño de los datos de procesamiento es mayor que el tamaño de búfer TCP predeterminado configurado.Solución temporal: establezca el tamaño del búfer TCP en el tamaño máximo de los datos que deben procesarse.

[NSPOLICY-1267]

SSL

En un clúster heterogéneo de dispositivos Citrix ADC SDX 22000 y Citrix ADC SDX 26000, se produce una pérdida de configuración de entidades SSL si se reinicia el dispositivo SDX 26000.

Solución alternativa:

1. En el CLIP, inhabilite SSLv3 en todas las entidades SSL nuevas y existentes, como servidores virtuales, servicios, grupos de servicios y servicios internos. Por ejemplo, `set ssl vserver <name> -SSL3 DISABLED`.

2. Guarde la configuración.

[NSSSL-9572]

No se puede agregar un objeto de Azure Key Vault si ya se ha agregado un objeto de autenticación de Azure Key Vault.

[NSSSL-6478]

Puede crear varias entidades de la aplicación Azure con el mismo ID de cliente y secreto de cliente. El dispositivo Citrix ADC no devuelve ningún error.

[NSSSL-6213]

El siguiente mensaje de error incorrecto aparece al quitar una clave HSM sin especificar KEYVAULT como tipo HSM.
ERROR: Actualización de crl inhabilitada

[NSSSL-6106]

La actualización automática de claves de sesión aparece incorrectamente como inhabilitada en una dirección IP de clúster. (Esta opción no se puede desactivar).

[NSSSL-4427]

Aparece `Warning: No usable ciphers configured on the SSL vserver/service,,` un mensaje de advertencia incorrecto, si intenta cambiar el protocolo o el cifrado SSL en el perfil SSL.

[NSSSL-4001]

Un tíquet de sesión caducado se respeta en un nodo que no es de CCO y en un nodo de alta disponibilidad después de una conmutación por error de alta disponibilidad. [NSSSL-3184, NSSSL-1379, NSSSL-1394]

En los dispositivos con certificación FIPS MPX 8900 y MPX 15000, la ejecución del tráfico ECDHE puede provocar una pérdida de memoria.

[NSHELP-30744]

Sistema

El valor MAX_CONCURRENT_STREAMS se establece en 100 de forma predeterminada si el dispositivo no recibe el marco de configuración max_concurrent_stream del cliente.

[NSHELP-21240]

Los contadores mptcp_cur_session_without_subflow disminuyen incorrectamente a un valor negativo en lugar de cero.

[NSHELP-10972]

En una implementación de clúster, si ejecuta un comando `force cluster sync` en un nodo que no es de CCO, el archivo ns.log contiene entradas de registro duplicadas. [NSBASE-16304, NSGI-1293]

Cuando instala Citrix ADM en un clúster de Kubernetes, no funciona según lo esperado porque es posible que los procesos necesarios no aparezcan.

Solución alternativa: reinicie el pod de administración.

[NSBASE-15556]

La IP del cliente y la IP del servidor se invierten en el registro SkipFlow de HDX Insight cuando el tipo de transporte LogStream se configura para Insight.

[NSBASE-8506]

El dispositivo Citrix ADC descarta paquetes que contienen encabezados HTTP personalizados con un punto (“. “) en el campo del nombre del encabezado. Esta acción se produce porque el parámetro `allowOnlyWordCharactersAndHyphen` está habilitado de forma predeterminada en el perfil HTTP predeterminado.

Solución temporal: Inhabilite `allowOnlyWordCharactersAndHyphen` en el perfil HTTP predeterminado. Sin embargo, Citrix recomienda mantenerla habilitada.

[NSBASE-16722]

Interfaz de usuario

Para la función Reescritura de MQTT, no puede eliminar una expresión mediante el Editor de expresiones en la GUI.

Solución alternativa:

Use el comando de acción add o edit de tipo MQTT a través de la CLI.

[NSUI-18049]

En la GUI de Citrix ADC, el enlace `Help` presente debajo de la ficha `Dashboard` no funciona.

[NSUI-14752]

El asistente Crear/Supervisar CloudBridge Connector podría dejar de responder o no configurar un conector de cloudbridge.

Solución alternativa:

Configure los conectores de cloudbridge agregando perfiles IPSec, túneles IP y reglas PBR mediante la GUI o la CLI de Citrix ADC.

[NSUI-13024]

Si crea una clave ECDSA mediante la interfaz gráfica de usuario, no se muestra el tipo de curva.

[NSUI-6838]

En una configuración de alta disponibilidad, las sesiones de usuario VPN se desconectan si se cumple la siguiente condición:

- Si se realizan dos o más operaciones de failover manual de alta disponibilidad sucesivas cuando la sincronización de alta disponibilidad está en curso.

Solución alternativa:

Realice una conmutación por error manual de alta disponibilidad sucesiva solo después de que se haya completado la sincronización de alta disponibilidad (ambos nodos están en estado de sincronización correcta).

[NSHELP-25598]

En una configuración de alta disponibilidad de los dispositivos Citrix ADC BLX, es posible que el nodo principal deje de responder bloqueando cualquier solicitud de CLI o API.

Solución alternativa:

Reinicie el nodo principal.

[NSCONFIG-6601]

Si usted (administrador del sistema) realiza todos los pasos siguientes en un dispositivo Citrix ADC, es posible que los usuarios del sistema no inicien sesión en el dispositivo Citrix ADC degradado.

1. Actualice el dispositivo Citrix ADC a una de las compilaciones:

- 13.0 52.24 compilación
- 12.1 57,18 compilación
- 11.1 65.10 compilación

1. Agregar un usuario del sistema o cambiar la contraseña de un usuario del sistema existente y guardar la configuración, y
2. Rebaja la versión del dispositivo Citrix ADC a cualquier versión anterior.

Para mostrar la lista de estos usuarios del sistema mediante la CLI:
En el símbolo del sistema, escriba:

```
query ns config -changedpassword [-config <full path of the configuration file (ns.conf)>]
```

Solución alternativa:

Para solucionar este problema, utilice una de las siguientes opciones independientes:

- Si el dispositivo Citrix ADC aún no se ha rebajado (paso 3 de los pasos mencionados anteriormente), revierta la versión del dispositivo Citrix ADC con un archivo de configuración del que se ha creado previamente una copia de seguridad (ns.conf) de la misma compilación de la versión.

- Cualquier administrador del sistema cuya contraseña no se haya cambiado en la compilación actualizada puede iniciar sesión en la compilación degradada y actualizar las contraseñas de otros usuarios del sistema.
- Si ninguna de las opciones anteriores funciona, el administrador del sistema puede restablecer las contraseñas de usuario del sistema.

Para obtener más información, consulte https://docs.citrix.com/en-us/citrix-adc/13/system/ns-ag-aa-intro-wrapper-con/ns-ag-aa-reset-default-amin-pass-tsk.html

[NSCONFIG-3188]

Notas

July 8, 2022

Este documento de notas de la versión describe las mejoras y los cambios, los problemas resueltos y conocidos que existen para la versión de Citrix ADC, compilación 13.1-21.50.

Este documento de notas de la versión no incluye correcciones relacionadas con la seguridad. Para obtener una lista de correcciones y avisos relacionados con la seguridad, consulte el boletín de seguridad de Citrix.

Las compilaciones 13.1-21.50 y posteriores abordan las vulnerabilidades de seguridad descritas en https://support.citrix.com/article/CTX457048.

Novedades

Las mejoras y los cambios que están disponibles en las compilaciones 13.1-21.50.

Administración de bots

Técnica de límite de velocidad de bots basada en la ubicación geográfica del usuario

La técnica de detección de límite de velocidad de bots ahora le permite limitar el bot de tráfico en función de la ubicación geográfica del usuario. En esta configuración, puede establecer un nombre de país como un valor similar al de la URL o al nombre de la cookie. De esta manera, puede aplicar una limitación de tarifa diferente para diferentes países. Anteriormente, la técnica de detección podía limitar el tráfico solo en función de la dirección IP, la sesión o la URL del cliente.

[NSBOT-753]

Técnica mejorada de huellas dactilares del dispositivo (DFP) para la detección de exploradores sin cabeza

Un hacker puede acceder a los recursos del servidor a través de un explorador sin cabeza automatizando procesos como la creación de cuentas de varios usuarios, la reserva de boletos, el desguace de precios, el relleno de credenciales, los ataques de hilado de boletos, etc.

La técnica de detección de huellas dactilares del dispositivo (DFP) en un perfil de bot ahora se ha mejorado con inteligencia para detectar bots sin cabeza y controladores web. Para mitigar el tráfico de bots de exploradores sin cabeza, debe habilitar la opción Detección de explorador sin cabeza junto con la función de detección de huellas dactilares del dispositivo.

[NSBOT-747]

Citrix Web App Firewall

Relajación detallada para los ataques de inyección de comandos JSON

El dispositivo Citrix ADC ahora le permite configurar una relajación detallada para los ataques de inyección de comandos JSON.

[NSWAF-8511]

Relajación pormenorizada para los ataques de scripting de sitios JSON

El dispositivo Citrix ADC ahora le permite configurar una relajación detallada para los ataques de scripting de sitios JSON.

[NSWAF-8510]

Relajación pormenorizada para los ataques de inyección JSON SQL

El dispositivo Citrix ADC ahora le permite configurar una relajación pormenorizada para los ataques de inyección JSON SQL.

[NSWAF-8509]

Equilibrio de carga

Mensajes de error de API de estado deseado mejorados

El mensaje de error que se muestra cuando la dirección IP de un miembro del grupo de servicios ya está asociada a otras entidades de Citrix ADC, como el servidor virtual de CS, se mejora. El motivo del fallo se aclara ahora en el mensaje de error. Anteriormente, el motivo del error en el mensaje de error no estaba claro.

[NSLB-9005]

La API de estado deseado admite la reutilización de direcciones IP y nombres de servidores existentes

La API de estado deseado ahora admite la vinculación de miembros del grupo de servicios a un grupo de servicios, incluso si la dirección IP de un miembro del grupo de servicios coincide con un servidor existente. La dirección IP y el nombre del servidor existente se reutilizan mientras se vincula al miembro del grupo de servicios.

Anteriormente, cuando la dirección IP coincidía, la vinculación de los miembros del grupo de servicios a un grupo de servicios no tenía éxito.

[NSLB-9004]

Redes

Compatibilidad con enlaces basados en CIDR en conjuntos de datos IPv4 para ACL extendidas

La ACLS extendida ahora admite conjuntos de datos IPv4 que contienen rangos de direcciones IPv4 especificados en la notación CIDR.

[NSNET-24452]

Compatibilidad de escalado del lado de recepción de software para el dispositivo Citrix ADC BLX en modo DPDK

Un dispositivo Citrix ADC BLX en modo DPDK y configurado con una mayor cantidad de motores de paquetes, no admite un puerto NIC con un número menor de colas de envío (Tx) y recepción (Rx).

Un dispositivo Citrix ADC BLX en modo DPDK no usa un puerto NIC si se cumplen las dos condiciones siguientes:

- El dispositivo tiene un puerto NIC que admite un número limitado de colas de envío (Tx) y colas de recepción (Rx). Por ejemplo, 7.
- El dispositivo está configurado con un número mayor de motores de paquetes. Por ejemplo, 28.

Para resolver este problema, a partir de la compilación 13.1 21.x, el dispositivo Citrix ADC BLX utiliza el ajuste de escala del lado de recepción (RSS) para distribuir de manera eficiente los paquetes recibidos en los puertos NIC en varios motores de paquetes.

El módulo RSS de software asigna un par lógico de colas Rx y Tx a cada puerto NIC. A continuación, el par de colas se mapea al motor de paquetes PE-0.

Para cada paquete en la cola Rx de un puerto NIC, el PE-0 selecciona un motor de paquetes mediante un algoritmo hash RSS. A continuación, PE-0 envía el paquete al motor de paquetes seleccionado para su procesamiento. Una vez finalizado el procesamiento del paquete, PE-0 envía el paquete a la cola Tx del puerto NIC.

[NSNET-23133]

Configurar el servicio GUI HTTP interno mediante la GUI de Citrix ADC, la CLI de Citrix ADC o las API de Citrix ADC NITRO

En un dispositivo Citrix ADC, `/etc/httpd.conf` es el archivo de configuración para el servicio GUI HTTP interno que administra las conexiones a la GUI de Citrix ADC.

En lugar de usar el archivo `httpd.conf` para configurar el servicio GUI HTTP interno, ahora puede usar la GUI de Citrix ADC, la CLI de Citrix ADC o las API de Citrix ADC NITRO. Por ejemplo, puede usar la CLI de Citrix ADC para modificar la cantidad máxima de clientes que pueden conectarse al servicio HTTP interno a la vez.

El servicio GUI HTTP interno tiene el siguiente formato de nombre: `nshttpd-gui-<loop back IP address>-80`

Use las operaciones de comandos del servicio Citrix ADC para configurar el servicio GUI HTTP interno.

[NSNET-20350]

Plataforma

Compatibilidad con la plataforma Citrix ADC MPX 9100

Esta versión admite la plataforma Citrix ADC MPX 9100. Incluye los modelos MPX 9110, MPX 9120 y MPX9130. Para obtener más información, consulte Citrix ADC MPX 9100.

[NSPLAT-23308]

Compatibilidad con la plataforma Citrix ADC SDX 9100

Esta versión admite la plataforma Citrix ADC SDX 9100. Incluye los modelos SDX 9120 y SDX 9130. Para obtener más información, consulte Citrix ADC SDX 9100.

[NSPLAT-23299]

Mejore el rendimiento de SSL-TPS en las nubes de AWS y GCP

Puede obtener un mejor rendimiento de SSL-TPS en las nubes de AWS y GCP si distribuye los pesos del motor de paquetes (PE) por igual. Para hacerlo, ejecute el siguiente comando en la CLI de Citrix ADC para establecer el modo PE:

```
set cpuparam pemode [CPUBOUND | Default]
```

En una nube de Azure, los pesos de PE se distribuyen equitativamente de forma predeterminada. Esta función no mejora el rendimiento de las instancias de Azure.

[NSPLAT-22570]

Compatibilidad con la actualización 3c de VMware ESXi 7.0 en la instancia de Citrix ADC VPX

La instancia de Citrix ADC VPX ahora admite la actualización 3c de la versión 7.0 de VMware ESXi (compilación 19193900).

[NSPLAT-22468]

SSL

Ver detalles de la utilización de chips SSL en plataformas Citrix ADC

A partir de la versión 13.1 compilación 21.x, se agregan contadores para ver más detalles sobre la utilización de chips SSL en plataformas MPX y SDX que se suministran con chips Intel Coleto y plataforma MPX 9100 (Lewisburg). En plataformas no compatibles, estos contadores muestran un valor de 0.0.

Para obtener más información, consulte Compatibilidad con plataformas basadas en chips SSL Intel Coleto y Lewisberg.

[NSSSL-10996]

Compatibilidad con certificados y cifrados ECDSA con DTLS

Los certificados y cifrados ECDSA ahora se pueden usar en entidades DTLS, como servidores y servicios virtuales.

[NSSSL-9535]

Sistema

Mejoras relacionadas con el envío de detalles del cliente en el encabezado de opción TCP

- El dispositivo Citrix ADC ahora inserta la dirección IP del cliente en el paquete ACK final del apretón de manos de tres vías además del primer paquete de datos. Anteriormente, el dispositivo enviaba la dirección IP del cliente solo en el primer paquete de datos.
- El dispositivo Citrix ADC ahora admite el envío de puertos de cliente en la opción TCP para la configuración del modo de inserción. Se ha introducido un parámetro `Send Client Port in Tcp Option` (`sendClientPortInTcpOption`) en el perfil TCP para habilitar o inhabilitar esta función.

[NSBASE-15635]

Problemas resueltos

Los problemas que se abordan en la compilación 13.1-21.50.

Autenticación, autorización y auditoría

El dispositivo Citrix ADC puede bloquearse si se produce un error al actualizar el par de claves de certificado SSL que se utiliza en la configuración de SAML. Para solucionar este problema, puede desvincular el certificado, actualizarlo y volver a vincularlo.

[NSHELP-30270]

Los usuarios no pueden iniciar sesión en el dispositivo Citrix ADC si la solicitud de inicio de sesión que utiliza SAML contiene caracteres de espacio en blanco distintos de ‘’ (comillas simples). Con esta corrección, se permiten todos los caracteres de espacio en blanco.

[NSHELP-29773]

Al enviar una solicitud AS_REQ para un usuario delegado, que forma parte del SSO de KCD, el dispositivo Citrix ADC selecciona un tipo de cifrado con la siguiente prioridad cuando el controlador de dominio (DC) publica todos los tipos de cifrado.

1. ETYPE_ARCFOUR_HMAC_MD5
2. ETYPE_AES128_CTS_HMAC_SHA1_96
3. ETYPE_AES256_CTS_HMAC_SHA1_96En lugar de
4. ETYPE_AES256_CTS_HMAC_SHA1_96
5. ETYPE_AES128_CTS_HMAC_SHA1_96
6. ETYPE_ARCFOUR_HMAC_MD5

[NSHELP-28681]

A veces, la autenticación puede fallar cuando se utilizan Autenticación, autorización y auditing.login.Password.

[NSHELP-28101]

El dispositivo Citrix ADC podría entrar en un bucle SSO con el servidor backend y provocar la acumulación de memoria si se cumplen las dos condiciones siguientes.

- El dispositivo ADC realiza una negociación y autenticaciones de SSO NTLM con el servidor backend.
- El servidor backend no puede realizar ambas autenticaciones.

[NSHELP-27757]

El dispositivo Citrix ADC puede bloquearse cuando la sincronización de la sesión y la configuración de la clave se produce entre la tarjeta controladora principal y la secundaria.

[NSHELP-26891]

Dispositivo Citrix ADC SDX

Aparece un mensaje incorrecto cuando la instalación limpia falla porque la partición de fábrica no tiene suficiente espacio.

[NSHELP-30136]

El campo plano anterior de la página Agregar nodo de clúster ya no es obligatorio a menos que se cumpla una de las siguientes condiciones:

- El grupo de nodos ya existe para los clústeres de capa 3.
- Es un clúster de capa 2.

[NSHELP-29701]

Citrix Gateway

Los usuarios del cliente VPN no pueden cerrar sesión correctamente si SAML y EPA están configurados como los factores sucesivos en una autenticación nFactor. Con esta corrección, los usuarios pueden cerrar sesión sin ningún problema.

[NSHELP-30193]

En una configuración de VPN SSL y GSLB de Citrix ADC, se observa una pérdida de memoria mientras se maneja una conexión ICA DTLS. Como resultado, la conexión se cae y la memoria se acumula.

[NSHELP-30182]

El inicio de PCoIP Apps and Desktops falla cuando se inicia desde un explorador y `VMware client missing` se muestra el mensaje de error. Este problema se produce porque el protocolo `vmware-view` no se agrega a la lista de protocolos permitidos.

[NSHELP-30062]

La exploración de la EPA para verificar el último análisis completo del sistema del antivirus falla en macOS.

[NSHELP-29571]

El túnel completo de Citrix Gateway VPN no funciona como se esperaba si la respuesta binaria está habilitada. Como resultado, la cookie de la NSAAC está dañada. Con esta corrección, la respuesta binaria funciona en los plug-ins VPN anteriores. Sin embargo, Citrix recomienda usar el último complemento de VPN que sea compatible con la respuesta JSON.

[NSHELP-28729]

Equilibrio de carga

Un dispositivo Citrix ADC con particiones puede volcar el núcleo mientras procesa un paquete de solicitud DNS con un encabezado adicional (EDNS).

[NSHELP-30796]

En una implementación de DNS con escalabilidad automática, los miembros en el estado TROFS no detectan ni responden a los errores de verificación de estado.

[NSHELP-29628]

El dispositivo Citrix ADC podría bloquearse al vincular la directiva de reescritura al servidor virtual de equilibrio de carga si se cumplen las siguientes condiciones:

1. La evaluación de la segunda expresión sobrescribe las variables de estado de la directiva de la primera expresión que está en curso.
2. Las variables de estado de la directiva DETERMINE_SERVICES se sobrescriben mediante la regla definida por el servidor virtual de equilibrio de carga.

[NSHELP-29449]

El tiempo de respuesta del monitor que se muestra al ejecutar el comando *show service* a veces es incorrecto.

[NSHELP-28994]

Los mensajes de reintento de SMPP se envían a todos los nodos de un clúster incluso cuando la solicitud se realiza correctamente. Este caso provoca un alto consumo de memoria en el dispositivo Citrix ADC.

[NSHELP-28332]

Redes

Al actualizar un dispositivo Citrix ADC BLX a la versión 13.1 compilación 17.x, es posible que el dispositivo no se inicie.

[NSNET-25002]

La instalación de un dispositivo Citrix ADC BLX en un host Linux basado en RHEL falla si el módulo python `jsonschema` está ausente en el host.

[NSNET-24638]

La actualización de un dispositivo Citrix ADC BLX con DPDK falla si se cumplen todas las condiciones siguientes:

- El dispositivo Citrix ADC BLX se ejecuta en un host Linux basado en Debian

- La actualización se realiza desde Citrix ADC versión 13.0 compilación 82.x o anterior a la versión 13.1 compilación 17.x.

[NSNET-24622]

Al configurar una regla de ACL de ICMP después de configurar una regla de ACL de TCP con la configuración del puerto, se puede observar el siguiente problema:

- El dispositivo Citrix ADC agrega incorrectamente la misma configuración de puerto de la ACL TCP a la ACL ICMP también.

[NSHELP-31114]

La modificación de una dirección IP privada en una regla INAT mediante la GUI falla si se cumple la siguiente condición:

- La conmutación por error de conexión está habilitada en la regla INAT.

[NSHELP-30792]

En la consola serie de un dispositivo Citrix ADC, es posible que el indicador VTYSH o el símbolo del shell no muestren ningún resultado.

[NSHELP-30446]

La modificación de un perfil de red que ya tiene un conjunto de IP vinculado a él puede fallar con el siguiente error:

- `IP set is already bound to the network profile`

[NSHELP-29363]

En una configuración NAT44 a gran escala, el dispositivo Citrix ADC puede bloquearse mientras recibe tráfico SIP por el siguiente motivo:

- Los recuentos de referencia de filtrado y mapeo son distintos de cero para el módulo LSN del dispositivo.

[NSHELP-28842]

Plataforma

No se puede acceder a la consola serie de una instancia de Citrix ADC VPX alojada en la nube de Azure cuando la máquina virtual se encuentra en las primeras etapas del arranque.

[NSPLAT-23010]

Durante la conmutación por error de alta disponibilidad de Citrix ADC VPX, el movimiento de la dirección IP elástica en la nube de AWS falla si configura un IPset sin vincular el IPset a ninguna dirección IP.

[NSHELP-29425]

SSL

El conjunto de cifrado RC4 falla durante un protocolo de enlace SSL con un mensaje `Illegal parameter error`.

[NSSSL-11463]

El dispositivo Citrix ADC se bloquea cuando la interceptación SSL está habilitada y hay varias solicitudes paralelas para acceder a un servidor backend con un certificado caducado.

[NSHELP-29520]

En una configuración de clúster, es posible que se observen los siguientes problemas:

- Falta el comando para el par de claves de certificado predeterminado vinculado a los servicios internos SSL del CLIP. Sin embargo, si actualiza desde una versión anterior, es posible que tenga que vincular el par de claves de certificado predeterminado a los servicios internos SSL afectados en el CLIP.
- Discrepancia de configuración entre el CLIP y los nodos del comando set predeterminado para los servicios internos.
- Falta el comando default cipher bind para las entidades SSL en el resultado del comando show running config ejecutado en un nodo. La omisión es solo un problema de visualización y no tiene ningún impacto funcional. El enlace se puede ver con el comando show ssl `<entity> <name>`.

[NSHELP-25764]

Sistema

El dispositivo Citrix ADC se bloquea si se produce alguna de las siguientes condiciones:

- La acción syslog se configura con el nombre de dominio y usted borra la configuración mediante la GUI o la CLI.
- La sincronización de alta disponibilidad se produce en el nodo secundario. [NSHELP-30987, NSHELP-28121, NSHELP-29843]

Todos los paquetes de datos reenviados desde un dispositivo Citrix ADC no tienen el valor TTL configurado, sino que tienen el valor enviado por el cliente o el servidor.

[NSHELP-30683]

El dispositivo Citrix ADC no puede reenviar algunos de los paquetes de datos no HTTP a los servidores back-end.

[NSHELP-30192]

En ciertos casos, el dispositivo Citrix ADC no reenvía algunos paquetes HTTP al servidor back-end, si se cumple la siguiente condición:

- Si una función Citrix ADC clona internamente paquetes HTTP.

[NSHELP-29958]

El dispositivo Citrix ADC puede agregar incorrectamente una dirección IPv4 a un registro de AppFlow relacionado con una transacción IPv6.

[NSHELP-29261]

Un dispositivo Citrix ADC podría bloquearse al reproducir una respuesta fragmentada del módulo ICAP al cliente.

[NSHELP-28788]

La falla de Pitboss ocurre cuando se hace un bucle de una gran cantidad de paquetes en la cola de retransmisión.

[NSHELP-26071]

Algunos mensajes SYSLOG se eliminan al iniciar sesión en un servidor SYSLOG externo mediante el protocolo TCP.

[NSHELP-24522]

En ciertos casos, la captura de paquetes nstrace pierde todos los paquetes si aplica el filtro basado en dirección IP.

[NSHELP-23483]

Interfaz de usuario

Es posible que el filtrado de caché no funcione según lo esperado en la GUI de Citrix ADC.

[NSHELP-30392]

Cuando se configura un dispositivo Citrix ADC para usar un servidor de autenticación externo, puede haber un retraso en la ejecución de los comandos stat, independientemente del parámetro RBAOnResponse configurado para inhabilitarse globalmente. El parámetro se puede inhabilitar desde la GUI o la CLI.

[NSHELP-30289]

La GUI de Citrix ADC no procesa las llamadas RAPI, lo que hace que algunos componentes de la GUI dejen de responder.

[NSHELP-30231]

En algunos casos, es posible que no pueda cargar claves SSL desde la ficha Claves SSL en la GUI de Citrix ADC.

[NSHELP-28870]

La respuesta de la API para una solicitud GET de NITRO con un filtro puede contener información adicional aunque no se mencione en el filtro.

[NSHELP-28598]

La carga y adición de un archivo de lista de revocación de certificados (CRL) produce un error en la configuración de una partición de administración.

[NSHELP-20988]

Problemas conocidos

Los problemas que existen en la versión 13.1-21.50.

AppFlow

HDX Insight no informa de un error de inicio de aplicación causado por un usuario que intenta iniciar una aplicación o un escritorio a los que el usuario no tiene acceso.

[NSINSIGHT-943]

Autenticación, autorización y auditoría

Un dispositivo Citrix ADC no autentica los intentos de inicio de sesión con contraseñas duplicadas y evita los bloqueos de cuentas.

[NSHELP-563]

LoginSchema de DualAuthPushOrOTP.xml no aparece correctamente en la pantalla del editor de esquemas de inicio de sesión de la GUI de Citrix ADC.

[NSAUTH-6106]

El perfil proxy ADFS se puede configurar en una implementación de clúster. El estado de un perfil proxy se muestra incorrectamente en blanco al ejecutar el siguiente comando.
`show adfsproxyprofile <profile name>`

Solución temporal:

Conéctese al Citrix ADC activo principal del clúster y ejecute el comando `show adfsproxyprofile <profile name>`. Mostraría el estado del perfil de proxy.

[NSAUTH-5916]

La página Configurar servidor LDAP de autenticación de la GUI de Citrix ADC deja de responder si sigue los pasos siguientes:

- Se abre la opción Probar accesibilidad LDAP.

- Las credenciales de inicio de sesión no válidas se rellenan y envían.
- Las credenciales de inicio de sesión válidas se rellenan y envían.

Solución temporal:

Cierre y abra la opción Probar accesibilidad de LDAP.

[NSAUTH-2147]

Almacenamiento en caché

Es posible que un dispositivo Citrix ADC se bloquee si la función Almacenamiento en caché integrado está habilitada y el dispositivo tiene poca memoria.

[NSHELP-22942]

Dispositivo Citrix ADC SDX

En un dispositivo Citrix ADC SDX, si el CLAG se crea en una NIC Mellanox, la MAC de CLAG cambia cuando se reinicia la instancia VPX. El tráfico a la instancia VPX se detiene tras el reinicio porque la tabla MAC tiene la antigua entrada MAC de CLAG.

[NSSVM-4333]

En un dispositivo Citrix ADC SDX con NIC Mellanox, modificar el rendimiento de una instancia VPX que tiene NIC Mellanox reinicia la instancia VPX.

[NSHELP-31305]

En un dispositivo Citrix ADC SDX, las instancias de ADC no alcanzan su capacidad máxima al configurar el modo de asignación de rendimiento en ráfagas.

[NSHELP-27477]

Las caídas de paquetes se observan en una instancia VPX alojada en un dispositivo Citrix ADC SDX si se cumplen las siguientes condiciones:

- El modo de asignación de rendimiento está en ráfaga.
- Existe una gran diferencia entre el rendimiento y la capacidad máxima de ráfaga.

[NSHELP-21992]

Después de actualizar un dispositivo Citrix ADC SDX a la versión 13.1 compilación 21.50 o posterior, el descifrado SSL y la comparación de MAC pueden fallar. Como resultado, es posible que vea fallas de protocolo de enlace SSL, inestabilidad del estado de VPX, falta de disponibilidad de la GUI de la instancia VPX y caídas de aplicaciones y servidores virtuales.

Nota: Este problema se observa en las plataformas SDX 8900, SDX 15000, SDX 15000-50G, SDX 26000 y SDX 26000-50S.

[NSHELP-31672]

Citrix Gateway

En algunos casos, Citrix Secure Access para macOS interrumpe las conexiones debido a problemas con algunos protocolos no DNS que utilizan el puerto 53, como STUN.

[NSHELP-31004]

Cuando se configura AlwaysOn, se produce un error en el túnel de usuario debido al número de versión incorrecto (1.1.1.1) en el archivo aoservice.exe.

[NSHELP-30662]

Los usuarios no pueden conectarse al dispositivo Citrix Gateway después de cambiar el parámetro “networkAccessOnVPNFailure” siempre en el perfil de “fullAccess” a “onlyToGateway”.

[NSHELP-30236]

El cliente VPN de Windows no respeta la alerta de “notificación de cierre SSL” del servidor y envía la solicitud de inicio de sesión de transferencia en la misma conexión.

[NSHELP-29675]

En algunos casos, el código de validación del servidor falla cuando se confía en el certificado del servidor. Como resultado, los usuarios finales no pueden acceder a la puerta de enlace.

[NSHELP-28942]

La autenticación de certificados de cliente falla para Citrix SSO para macOS si no hay certificados de cliente en el llavero de macOS.

[NSHELP-28551]

A veces, se desactiva la sesión de un usuario en Citrix Gateway en unos segundos cuando se establece el tiempo de espera por inactividad del cliente.

[NSHELP-28404]

No se puede desvincular una directiva de autorización clásica mediante la interfaz gráfica de usuario. Sin embargo, puede usar la CLI para desvincular la directiva Autenticación, autorización y autorización de auditoría.

Con esta corrección, ahora puede desvincular la directiva de autorización mediante la interfaz gráfica de usuario.

[NSHELP-27064]

En una configuración de alta disponibilidad, las sesiones de usuario VPN se desconectan si se cumple la siguiente condición:

- Si se realizan dos o más operaciones de failover manual de alta disponibilidad sucesivas cuando la sincronización de alta disponibilidad está en curso.

Solución temporal:

Realice una conmutación por error manual de alta disponibilidad sucesiva solo después de que se haya completado la sincronización de alta disponibilidad (ambos nodos están en estado de sincronización correcta).

[NSHELP-25598]

El complemento EPA para Windows no utiliza el proxy configurado del equipo local y se conecta directamente al servidor de puerta de enlace.

[NSHELP-24848]

Gateway Insight no muestra información precisa sobre los usuarios de VPN.

[NSHELP-23937]

El complemento VPN no establece un túnel después del inicio de sesión de Windows si se cumplen las siguientes condiciones:

- El dispositivo Citrix Gateway está configurado para la función Always On
- El dispositivo está configurado para la autenticación basada en certificados con autenticación de dos factores `off`

[NSHELP-23584]

A veces, al navegar por los esquemas, aparece el mensaje de error `Cannot read property 'type 'of undefined`.

[NSHELP-21897]

Si quiere utilizar la funcionalidad Always On VPN antes de iniciar sesión en Windows, se recomienda actualizar a Citrix Gateway 13.0 o posterior. Esto le permite aprovechar las mejoras adicionales introducidas en la versión 13.0 que no están disponibles en la versión 12.1.

[CGOP-19355]

El error de inicio de la aplicación debido a un tíquet de STA no válido no se informa en Gateway Insight.

[CGOP-13621]

El informe Gateway Insight muestra incorrectamente el valor `Local` en lugar de `SAML` en el campo Tipo de autenticación para los errores de SAML.

[CGOP-13584]

En una configuración de alta disponibilidad, durante una conmutación por error de Citrix ADC, el recuento de SR aumenta en lugar del recuento de fallas en Citrix ADM.

[CGOP-13511]

Cuando se inicia una conexión ICA desde un receptor MAC versión 19.6.0.32 o Citrix Virtual Apps and Desktops versión 7.18, la función HDX Insight se inhabilita.

[CGOP-13494]

Cuando la función EDT Insight está habilitada, a veces los canales de audio pueden fallar durante una discrepancia de red.

[CGOP-13493]

Al aceptar conexiones de host local desde el explorador web, el cuadro de diálogo Aceptar conexión para macOS muestra el contenido en inglés independientemente del idioma seleccionado.

[CGOP-13050]

El texto `Home Page` de la página de inicio de la aplicación Citrix SSO > aparece cortado para algunos idiomas.

[CGOP-13049]

Aparece un mensaje de error al agregar o modificar una directiva de sesión desde la GUI de Citrix ADC.

[CGOP-11830]

En Outlook Web App (OWA) 2013, al hacer clic en **Opciones**, en el menú Configuración, aparece el cuadro de diálogo **Error crítico**. Además, la página deja de responder.

[CGOP-7269]

Equilibrio de carga

En una configuración de alta disponibilidad, es posible que las sesiones de suscriptor del nodo principal no se sincronicen con el nodo secundario. Este es un caso raro.

[NSLB-7679]

El formato serviceGroupName de la captura `entityofs` del grupo de servicios es el siguiente: `<service(group)name>?<ip/DBS>?<port>`

En el formato de captura, el grupo de servicios se identifica mediante una dirección IP o un nombre y puerto de DBS. El signo de interrogación (`?`) se utiliza como separador. Citrix ADC envía la captura con el signo de interrogación (`?`). El formato aparece igual en la GUI de Citrix ADM. Este es el comportamiento esperado.

[NSHELP-28080]

Otros

Cuando se produce una sincronización forzada en una configuración de alta disponibilidad, el dispositivo ejecuta el comando `set urlfiltering parameter` en el nodo secundario.

Como resultado, el nodo secundario omite cualquier actualización programada hasta la siguiente hora programada mencionada en el parámetro `TimeOfDayToUpdateDB`.

[NSSWG-849]

Un dispositivo Citrix ADC puede reiniciarse debido al estancamiento de la CPU de administración si se produce un problema de conectividad con el proveedor externo de filtrado de URL.

[NSHELP-22409]

Redes

En un dispositivo Citrix ADC BLX compatible con DPDK, las VLAN etiquetadas no son compatibles con los puertos NIC DPDK Intel i350. Esto se observa, ya que es un problema conocido presente en el controlador DPDK.

[NSNET-25299]

Es posible que un dispositivo Citrix ADC BLX con DPDK no se reinicie si se cumplen todas las condiciones siguientes:

- El dispositivo Citrix ADC BLX se asigna con un número bajo de `hugepages`. Por ejemplo, 1G.
- El dispositivo Citrix ADC BLX se asigna con una gran cantidad de procesos de trabajo. Por ejemplo, 28.

El problema se registra como un mensaje de error en `/var/log/ns.log`:

- `BLX-DPDK:DPDK Mempool could Not be Initialized for PE-x`

Nota: x es un número <= número de procesos de trabajo.

Solución temporal:

Asigne un número elevado de `hugepages` y, a continuación, reinicie el dispositivo.

[NSNET-25173]

Es posible que un dispositivo Citrix ADC BLX con DPDK no se reinicie si se cumple la siguiente condición:

- Al dispositivo Citrix ADC BLX se le asigna una gran cantidad de `hugepages`. Por ejemplo, 16 GB.

El problema se registra como un mensaje de error en `/var/log/ns.log`:

- `EAL: rte_mem_virt2phy(): cannot open /proc/self/pagemap: Too many open files`

Solución temporal:

Use una de las siguientes soluciones para este problema:

- Aumente el límite de archivos abiertos en el host Linux mediante el uso del comando `ulimit` o la modificación del archivo `limits.conf`.
- Reduzca el número de `hugepages` asignadas.

[NSNET-24727]

Un dispositivo Citrix ADC BLX en modo DPDK puede tardar un poco más en reiniciarse debido a la funcionalidad de facilidad de DPDK.

[NSNET-24449]

Las siguientes operaciones de interfaz no son compatibles con las interfaces `X710 10G (i40e)` de Intel en un dispositivo Citrix ADC BLX con DPDK:

- Disable
- Enable
- Reset

[NSNET-16559]

La instalación de un dispositivo Citrix ADC BLX podría fallar en un host Linux basado en Debian (versión 18 y posteriores de Ubuntu) con el siguiente error de dependencia:

```
The following packages have unmet dependencies: blx-core-libs:i386 :
PreDepends: libc6:i386 (>= 2.19)but it is not installable
```

Solución temporal:

Ejecute los siguientes comandos en la CLI del host Linux antes de instalar un dispositivo Citrix ADC BLX:

- dpkg — agregar arquitectura i386
- actualización apt-get
- apt-get dist-upgrade
- apt-get install libc6:i386

[NSNET-14602]

En algunos casos de conexiones de datos FTP, el dispositivo Citrix ADC solo realiza operaciones NAT y no procesamiento TCP en los paquetes para la negociación TCP MSS. Como resultado, la MTU de interfaz óptima no está configurada para la conexión. Esta configuración de MTU incorrecta provoca la fragmentación de los paquetes y afecta al rendimiento de la CPU.

[NSNET-5233]

Cuando se cambia el límite de memoria de una partición de administración en el dispositivo Citrix ADC, el límite de memoria de almacenamiento en búfer TCP se establece automáticamente en el límite de memoria nueva de la partición de administración.

[NSHELP-21082]

Plataforma

La conmutación por error de alta disponibilidad no funciona en las nubes de AWS y GCP. La CPU de administración puede alcanzar su capacidad del 100% en las nubes de AWS y GCP, y en Citrix ADC VPX en las instalaciones. Ambos problemas se producen cuando se cumplen las siguientes condiciones:

1. Durante el primer arranque del dispositivo Citrix ADC, no guarda la contraseña solicitada.
2. Posteriormente, reinicie el dispositivo Citrix ADC.

[NSPLAT-22013]

Cuando actualiza de compilaciones 13.0/12.1/11.1 a una versión 13.1 o baja de una compilación 13.1 a 13.0/12.1/11.1, algunos paquetes python no se instalan en los dispositivos Citrix ADC. Este problema se ha solucionado en las siguientes versiones de Citrix ADC:

- 13.1-4.x
- 13.0—82.31 y posteriores
- 12.1—62.21 y posteriores

Los paquetes python no se instalan cuando se degrada la versión de Citrix ADC de la versión 13.1-4.x a cualquiera de las siguientes versiones:

- Cualquier compilación 11.1
- 12.1—62.21 y anteriores
- 13.0-81.x y anteriores

[NSPLAT-21691]

En una configuración de clúster en un dispositivo Citrix ADC SDX, hay una discordancia de CLAG MAC en el segundo nodo y CLIP si se cumplen las siguientes condiciones:

- El CLAG se crea en una NIC Mellanox.
- Agrega otra instancia VPX al clúster y a la configuración de CLAG.

Como resultado, el tráfico a la instancia VPX se detiene.

[NSPLAT-21049]

En una configuración de clúster en un dispositivo Citrix ADC SDX, el primer nodo se apaga debido a una falta de coincidencia de direcciones MAC en la tabla CLIP y MAC, si se cumplen las siguientes condiciones:

- El CLAG se crea en una NIC Mellanox.
- Quita el segundo nodo del clúster.

[NSPLAT-21042]

Al eliminar una configuración de escalabilidad automática o un conjunto de escalas de VM de un grupo de recursos de Azure, elimine la configuración del perfil de nube correspondiente de la instancia de Citrix ADC. Utilice el comando `rm cloudprofile` para borrar el perfil.

[NSPLAT-4520]

En una configuración de alta disponibilidad en Azure, al iniciar sesión en el nodo secundario a través de la GUI, aparece la pantalla de usuario por primera vez (FTU) para la configuración del perfil de nube de escalabilidad automática.
Solución alternativa: omita la pantalla e inicie sesión en el nodo principal para crear el perfil de nube. El perfil de nube debe estar siempre configurado en el nodo principal.

[NSPLAT-4451]

A partir de la versión 13.1 de Citrix ADC, el dispositivo Citrix ADC no se inicia en un hipervisor ESXi con más de 8 interfaces de red VMXNET3.

[NSHELP-31266]

Directivas

Las conexiones pueden bloquearse si el tamaño de los datos de procesamiento es mayor que el tamaño de búfer TCP predeterminado configurado.Solución alternativa: establezca el tamaño del búfer TCP en un tamaño máximo de datos que deben procesarse.

[NSPOLICY-1267]

En algunos casos, un dispositivo Citrix ADC puede bloquearse cuando se utiliza una acción de asignación con la operación de borrado de una variable de AppExpert.

[NSHELP-29766]

SSL

En un clúster heterogéneo de dispositivos Citrix ADC SDX 22000 y Citrix ADC SDX 26000, se produce una pérdida de configuración de entidades SSL si se reinicia el dispositivo SDX 26000.

Solución temporal:

1. En el CLIP, inhabilite SSLv3 en todas las entidades SSL nuevas y existentes, como servidores virtuales, servicios, grupos de servicios y servicios internos. Por ejemplo, `set ssl vserver <name> -SSL3 DISABLED`.
2. Guarde la configuración.

[NSSSL-9572]

No se puede agregar un objeto de Azure Key Vault si ya se ha agregado un objeto de autenticación de Azure Key Vault.

[NSSSL-6478]

Puede crear varias entidades de la aplicación Azure con el mismo ID de cliente y secreto de cliente. El dispositivo Citrix ADC no devuelve ningún error.

[NSSSL-6213]

El siguiente mensaje de error incorrecto aparece al quitar una clave HSM sin especificar KEYVAULT como tipo HSM.
ERROR: Actualización de crl inhabilitada

[NSSSL-6106]

La actualización automática de claves de sesión aparece incorrectamente como inhabilitada en una dirección IP de clúster. (Esta opción no se puede desactivar).

[NSSSL-4427]

Aparece `Warning: No usable ciphers configured on the SSL vserver/service,,` un mensaje de advertencia incorrecto, si intenta cambiar el protocolo o el cifrado SSL en el perfil SSL.

[NSSSL-4001]

Un tíquet de sesión caducado se respeta en un nodo que no es de CCO y en un nodo de alta disponibilidad después de una conmutación por error de alta disponibilidad.

[NSSSL-3184, NSSSL-1379, NSSSL-1394]

En los dispositivos con certificación FIPS MPX 8900 y MPX 15000, la ejecución del tráfico ECDHE puede provocar una pérdida de memoria.

[NSHELP-30744]

Sistema

El valor MAX_CONCURRENT_STREAMS se establece en 100 de forma predeterminada si el dispositivo no recibe el marco de configuración max_concurrent_stream del cliente.

[NSHELP-21240]

Los contadores mptcp_cur_session_without_subflow disminuyen incorrectamente a un valor negativo en lugar de cero.

[NSHELP-10972]

En una implementación de clúster, si ejecuta el comando `force cluster sync` en un nodo que no es de CCO, el archivo ns.log contiene entradas de registro duplicadas. [NSBASE-16304, NSGI-1293]

Cuando instala Citrix ADM en un clúster de Kubernetes, no funciona según lo esperado porque es posible que los procesos necesarios no aparezcan.

Solución alternativa: reinicie el pod de administración.

[NSBASE-15556]

La IP del cliente y la IP del servidor se invierten en el registro HDX Insight SkipFlow cuando el tipo de transporte de LogStream está configurado para Insight.

[NSBASE-8506]

El dispositivo Citrix ADC descarta paquetes que contienen encabezados HTTP personalizados con un punto (“. “) en el campo del nombre del encabezado. Esta acción se produce porque el parámetro `allowOnlyWordCharactersAndHyphen` está habilitado de forma predeterminada en el perfil HTTP predeterminado.

Solución temporal: Inhabilite `allowOnlyWordCharactersAndHyphen` en el perfil HTTP predeterminado. Sin embargo, Citrix recomienda mantenerla habilitada.

[NSBASE-16722]

Interfaz de usuario

Para la función Reescritura de MQTT, no puede eliminar una expresión mediante el Editor de expresiones en la GUI.

Solución temporal:

Use el comando de acción add o edit de tipo MQTT a través de la CLI.

[NSUI-18049]

En la GUI de Citrix ADC, el enlace `Help` presente debajo de la ficha `Dashboard` no funciona.

[NSUI-14752]

El asistente Crear/Supervisar CloudBridge Connector podría dejar de responder o no configurar un conector de cloudbridge.

Solución temporal:

Configure los conectores de cloudbridge agregando perfiles IPSec, túneles IP y reglas PBR mediante la GUI o la CLI de Citrix ADC.

[NSUI-13024]

Si crea una clave ECDSA mediante la interfaz gráfica de usuario, no se muestra el tipo de curva.

[NSUI-6838]

En una configuración de alta disponibilidad de los dispositivos Citrix ADC BLX, es posible que el nodo principal deje de responder bloqueando cualquier solicitud de CLI o API.

Solución temporal:

Reinicie el nodo principal.

[NSCONFIG-6601]

Si usted (administrador del sistema) realiza todos los pasos siguientes en un dispositivo Citrix ADC, es posible que los usuarios del sistema no inicien sesión en el dispositivo Citrix ADC degradado.

1. Actualice el dispositivo Citrix ADC a una de las compilaciones:

- 13.0 52.24 compilación
- 12.1 57,18 compilación
- 11.1 65.10 compilación

1. Agregar un usuario del sistema o cambiar la contraseña de un usuario del sistema existente y guardar la configuración, y
2. Rebaja la versión del dispositivo Citrix ADC a cualquier versión anterior.

Para mostrar la lista de estos usuarios del sistema mediante la CLI:
En el símbolo del sistema, escriba:

```
query ns config -changedpassword [-config <full path of the configuration file (ns.conf)>]
```

Solución temporal:

Para solucionar este problema, utilice una de las siguientes opciones independientes:

- Si el dispositivo Citrix ADC aún no se ha degradado (paso 3 de los pasos mencionados anteriormente), degrade el dispositivo Citrix ADC mediante un archivo de configuración del que se realizó una copia de reserva (ns.conf) de la misma versión.
- Cualquier administrador del sistema cuya contraseña no se haya cambiado en la compilación actualizada puede iniciar sesión en la compilación degradada y actualizar las contraseñas de otros usuarios del sistema.
- Si ninguna de las opciones anteriores funciona, el administrador del sistema puede restablecer las contraseñas de usuario del sistema.

Para obtener más información, consulte Cómo restablecer la contraseña del administrador raíz (nsroot).

[NSCONFIG-3188]

Notas de la versión de Citrix ADC 13.1-17.42

June 22, 2022

Este documento de notas de la versión describe las mejoras y los cambios, los problemas resueltos y conocidos que existen para la versión de Citrix ADC, compilación 13.1-17.42.

Notas

Este documento de notas de la versión no incluye correcciones relacionadas con la seguridad. Para obtener una lista de correcciones y avisos relacionados con la seguridad, consulte el boletín de seguri-

dad de Citrix.

Novedades

Las mejoras y los cambios que están disponibles en las compilaciones 13.1-17.42.

Administración de bots

Compatibilidad con direccionamiento IPv6

La administración de bots de Citrix ADC ahora admite el direccionamiento del protocolo de Internet versión 6 (IPv6) para las técnicas de detección de bots.

[NSBOT-690]

Citrix Gateway

Propagación de bits DF para EDT en Citrix Gateway

El dispositivo Citrix Gateway ahora admite la aplicación de bits DF para la función EDT Path Maximum Transmission Unit Discovery (PMTUD). La función de descubrimiento de MTU de ruta ayuda a determinar dinámicamente la unidad de transmisión máxima (MTU) al establecer una sesión de EDT. La aplicación de bits DF evita la fragmentación de EDT que puede provocar una degradación del rendimiento o la imposibilidad de establecer una sesión.

En versiones anteriores, Citrix Gateway admitía MTUD de ruta EDT, pero no admitía la aplicación de bits DF.

[CGOP-18438]

Citrix Web App Firewall

Soporte mejorado para el aprendizaje de múltiples infracciones de scripts de sitios (XSS)

El proceso de aprendizaje de Citrix Web App Firewall ahora se ha mejorado para reducir los falsos positivos en los ataques de scripts de sitios.

Con el aprendizaje habilitado, puede aprender todas las infracciones en una solicitud y, potencialmente, aplicar relajación a todas las etiquetas/atributos/patrones a la vez. Anteriormente, solo podía denunciar una infracción a la vez y debía repetir el proceso para varias infracciones.

Por ejemplo, si hay 15 etiquetas personalizadas en una carga útil, cada una de las cuales resulta en una infracción, puede aplicar una relajación para la primera infracción y ejecutar la solicitud para marcar otra etiqueta personalizada como infracción. El proceso debe repetirse para aplicar una relajación a todas las etiquetas personalizadas una por una.

[NSWAF-7545]

Equilibrio de carga

Opción para habilitar o inhabilitar miembros del grupo de servicios LB y GSLB Autoscale

Ahora puede habilitar o inhabilitar directamente miembros específicos de un grupo de servicios de Autoscale LB o GSLB (basado en DNS). Por lo tanto, la administración de un grupo de servicios de Autoscale LB o GSLB (basado en DNS) ahora es más fácil.

Anteriormente, tenía que habilitar o inhabilitar todo un grupo de servicios LB o GSLB Autoscale para habilitar o inhabilitar a un miembro individual. Solo los grupos de servicios que no son de escalabilidad automática tenían la opción de habilitar o inhabilitar a un miembro individual.

[NSLB-8109]

Redes

Mejoras en las estadísticas de ISSU

Las dos mejoras siguientes se agregan a las estadísticas de ISSU:

- Se ha agregado una opción `dumpsession` (`Dump Session`) a la operación `show migration` para mostrar la lista de conexiones existentes que el nodo principal anterior está sirviendo actualmente. La operación show migration con la opción `dumpsession` debe ejecutarse solo en el nuevo nodo principal.
- La operación show migration (sin ninguna opción) ahora muestra la siguiente información adicional relacionada con la operación de migración ISSU:
- Número total de conexiones que se procesan como parte de la operación de migración de ISSU
- Número de conexiones restantes que se están procesando como parte de la operación de migración de ISSU

Para obtener más información, consulte https://docs.citrix.com/en-us/citrix-adc/current-release/upgrade-downgrade-citrix-adc-appliance/issu-high-availability.html .

[NSNET-23577]

Supervisar el uso de puertos en un dispositivo Citrix ADC para conexiones back-end mediante SNMP

Puede usar la alarma SNMP `PORT-ALLOC-EXCEED` para supervisar el uso de puertos en un dispositivo Citrix ADC para conexiones back-end.

La alarma SNMP `PORT-ALLOC-EXCEED` incluye los parámetros `high-threshold` y `normal-threshold`, que especifican el total de puertos asignados de las direcciones IP propiedad de Citrix

como porcentajes. Por ejemplo, si el parámetro `high-threshold` se establece en 90, el dispositivo Citrix ADC genera y envía mensajes de captura cuando ocurre el siguiente evento:

- cuando el porcentaje de asignación de puertos supera el 90 por ciento en cualquiera de las direcciones IP propiedad de Citrix ADC para las conexiones back-end

Las alertas SNMP lo ayudan a decidir la necesidad de más direcciones IP propiedad de Citrix si los puertos libres disponibles están a punto de agotarse.

[NSNET-21719]

Compatibilidad con el protocolo GENEVE

Un dispositivo Citrix ADC ahora admite el protocolo Generic Network Virtualization Encapsulation (GENEVE) como se define en RFC 8926.

La virtualización de servidores y la arquitectura de computación en la nube han aumentado la demanda de redes de capa 2 aisladas en un centro de datos. El límite de VLAN de 4094 ha demostrado ser inadecuado y se introdujeron protocolos de encapsulación como VXLAN y NVGRE para superar esta limitación.

Estos protocolos difieren principalmente en la implementación del plano de control. El protocolo GENEVE no define las especificaciones para el plano de control. El protocolo deja que la implementación defina las especificaciones del plano de control.

El protocolo GENEVE es una tecnología de encapsulación que tiene como objetivo crear redes superpuestas de capa 2 sobre la infraestructura de capa 3 mediante la encapsulación de tramas de capa 2 en paquetes UDP. Cada VLAN se identifica mediante un identificador único de 24 bits denominado VNID. Solo dentro del mismo ID de segmento (VNID) pueden comunicarse entre sí.

Un dispositivo Citrix ADC admite la encapsulación GENEVE en el puerto UDP 6081.

[NSNET-21717]

Configurar el acceso SSH al host Linux que ejecuta un dispositivo Citrix BLX en modo dedicado

De forma predeterminada, el acceso SSH a un host Linux que ejecuta el dispositivo Citrix BLX en modo dedicado no se puede realizar a través de las interfaces dedicadas del dispositivo.

Puede configurar el acceso SSH al host Linux a través de las interfaces dedicadas del dispositivo Citrix ADC BLX. Esta función es útil en un host Linux de interfaz única que ejecuta un dispositivo Citrix BLX en modo dedicado.

Puede configurar el acceso SSH directo al host Linux en cualquiera de los siguientes tipos:

- Proporcione acceso SSH en el puerto 9022 de Citrix ADC IP (NSIP) del dispositivo Citrix ADC BLX.
  - `<Citrix ADC IP address (NSIP)>:9022`

- Defina una nueva dirección IP en la subred de Citrix ADC IP (NSIP) y proporcione acceso SSH en el puerto 22. - <**new** IP address on the Citrix ADC IP address (NSIP)subnet >:22
  Además, se puede acceder a todos los demás puertos del host Linux mediante la nueva dirección IP. Por ejemplo, ahora se puede acceder a un servidor rsyslog que se ejecuta en el host Linux en el puerto 514/UDP en el puerto 514 de la nueva dirección IP.

[NSNET-21586]

Implementación simplificada de un dispositivo Citrix ADC BLX con puertos DPDK

El procedimiento para implementar un dispositivo Citrix ADC BLX con puertos DPDK se ha simplificado con las siguientes mejoras:

- El dispositivo Citrix ADC BLX ahora usa bibliotecas compiladas con la versión 20.11.1 de DPDK. El dispositivo carga automáticamente el módulo kernel VFIO de DPDK en el host Linux.
- El parámetro dpdk-config se ha eliminado del archivo de configuración (blx.conf) de Citrix ADC BLX. El parámetro worker-processes existente ahora también se aplica al dispositivo Citrix ADC BLX con puertos DPDK. worker-processes especifica la cantidad de motores de paquetes para un dispositivo Citrix ADC BLX. En otras palabras, ahora worker-processes es un parámetro común para el dispositivo Citrix ADC BLX, independientemente de su modo (compartido, dedicado o DPDK). Si worker-process no está configurado, el dispositivo Citrix ADC BLX está configurado con 1 motor de paquetes de forma predeterminada.
- El parámetro interfaces ahora especifica los puertos NIC compatibles con DPDK además de los puertos NIC que no son DPDK. El dispositivo Citrix ADC BLX detecta automáticamente los puertos NIC compatibles con DPDK (si los hay) de la lista de puertos especificados en el parámetro interfaces. A continuación, el dispositivo vincula los puertos NIC compatibles con DPDK detectados al módulo VFIO DPDK en el host Linux. Después de iniciar el dispositivo Citrix ADC BLX, los puertos NIC DPDK y no DPDK se agregan automáticamente como parte del dispositivo.
- El parámetro dpdk-non-uio-intf, que especifica los puertos NIC de Mellanox enlazados a DPDK, se ha eliminado del archivo de configuración (blx.conf) de Citrix ADC BLX. El parámetro interfaces ahora especifica los puertos NIC Mellanox que se utilizarán como puertos DPDK en el dispositivo Citrix ADC BLX. Antes de especificar los puertos NIC Mellanox para el dispositivo Citrix ADC BLX, las bibliotecas DPDK OFED de Mellanox y los módulos del kernel deben instalarse en el host Linux. El dispositivo Citrix ADC BLX detecta automáticamente los puertos NIC Mellanox especificados y los inicializa en modo DPDK. Después de iniciar el dispositivo Citrix ADC BLX, los puertos NIC Mellanox enlazados a DPDK se agregan como parte del dispositivo.
- Se ha introducido un nuevo parámetro total-hugepage-mem en el archivo de configuración (blx.conf) de Citrix ADC BLX para configurar hugepages para DPDK en el host Linux. El parámetro total-hugepage-mem especifica el tamaño de hugepages en MB o GB (por

ejemplo, 1024 MB y 2 GB).

- Al actualizar un dispositivo Citrix ADC BLX con puertos DPDK, el módulo de actualización convierte automáticamente las configuraciones existentes al nuevo formato en el archivo de configuración (`blx.conf`) de Citrix ADC BLX.

[NSNET-20524]

Supervisar los puertos libres disponibles en un dispositivo Citrix ADC para una nueva conexión back-end

Para la comunicación con los servidores físicos u otros dispositivos del mismo nivel, el dispositivo Citrix ADC utiliza una dirección IP propiedad de Citrix como dirección IP de origen. El dispositivo Citrix ADC mantiene un conjunto de sus direcciones IP y selecciona dinámicamente una dirección IP mientras se conecta con un servidor. En función de la subred en la que se coloque el servidor físico, el dispositivo decide qué dirección IP se va a utilizar. Este grupo de direcciones se utiliza para enviar sondeos de tráfico y monitorizar.

Puede mostrar el número total de puertos libres disponibles en las direcciones IP propiedad de Citrix ADC para una nueva conexión back-end. Esta información lo ayuda a decidir la necesidad de más direcciones IP propiedad de Citrix si los puertos gratuitos disponibles están a punto de agotarse.

Puede proporcionar la siguiente información para que el dispositivo Citrix ADC calcule la cantidad total de puertos libres disponibles para una nueva conexión back-end:

- Dirección IP propiedad de Citrix (opcional)
- Dirección IP de destino
- Puerto de destino
- Protocolo TCP o no TCP

[NSNET-20410]

Plataforma

Soporte para configuraciones de Citrix ADC VPX en el primer arranque del dispositivo Citrix ADC en el hipervisor KVM

Ahora puede aplicar las configuraciones de Citrix ADC VPX durante el primer arranque del dispositivo Citrix ADC en el hipervisor KVM. Por lo tanto, la configuración de un cliente en una instancia VPX se puede configurar en mucho menos tiempo.

[NSPLAT-21571]

Excluir la carpeta nstrace de las particiones administrativas de Citrix ADC durante la operación de copia

En un dispositivo Citrix ADC con particiones de administración, se excluye la operación de copia de seguridad de la carpeta nstrace. Esto reduce el tamaño general de la copia de seguridad de Citrix ADC sin perder datos importantes.

[NSPLAT-21433]

Directivas

Compatibilidad con la notación de subred CIDR en direcciones IPv4 e IPv6 para el conjunto de datos de directivas

Los conjuntos de datos de directivas para direcciones IPv4 e IPv6 ahora permiten que el valor enlazado sea subredes mediante la notación CIDR (por ejemplo, a.b.c.d/n). La notación CIDR especifica la dirección y el rango de la subred. Anteriormente, no había ninguna opción para agregar subredes en los conjuntos de datos de directivas.

Para obtener más información, consulte https://docs.citrix.com/en-us/citrix-adc/current-release/appexpert/pattern-sets-data-seta/configuring-data-sets.html

[NSPOLICY-3828]

SSL

Inhabilitar los protocolos no seguros en los servicios SSL front-end en un dispositivo Citrix ADC

Los análisis de seguridad estándar pueden desencadenar una alerta de protocolos no seguros en los servicios SSL front-end creados de forma predeterminada cuando se inicia un dispositivo Citrix ADC. Para evitar este tipo de alertas, estos protocolos ahora están inhabilitados de forma predeterminada en los servicios SSL front-end cuando se inician los dispositivos. Algunos ejemplos de protocolos no seguros son SSLv3, TLv1 y TLSv1.1.

Cuando se habilita el perfil SSL predeterminado, se crea un nuevo perfil SSL en el que se inhabilitan estos protocolos. Este nuevo perfil está vinculado a los servicios SSL front-end (ns_default_ssl_profile_internal_frontend_service). Este perfil se puede modificar.

[NSSSL-9985]

Compatibilidad con certificados firmados mediante los algoritmos RSASSA-PSS

Todas las plataformas Citrix ADC ahora admiten certificados firmados con los algoritmos RSASSA-PSS. Estos algoritmos se admiten en la validación de rutas de certificados X.509.

[NSSSL-9289]

Problemas resueltos

Los problemas que se abordan en la compilación 13.1-17.42.

Autenticación, autorización y auditoría

El dispositivo Citrix ADC se bloquea si la URL de ADFSPIP se establece en tipo `http://`. ADFSPIP solo admite tipos de URL `https://`.

[NSHELP-29838]

El dispositivo Citrix ADC puede bloquearse durante un flujo de IdP SAML, si hay un retraso significativo en el procesamiento de la solicitud.

[NSHELP-29789]

No se pueden reescribir directivas para dispositivos de punto final como `/logon/LogonPoint/Resources/List and /cgi/Resources/List`.

[NSHELP-29488]

En casos excepcionales, el dispositivo Citrix ADC puede bloquearse debido a una posición de registro incorrecta.

[NSHELP-29267]

Un dispositivo Citrix ADC configurado para autenticarse mediante el proveedor de servicios OAuth no se puede configurar con ‘client-secrete_post‘ para autenticarse con IDP tokenEndPoint.

Con esta corrección, el método de autenticación `client_secret_basic` se agrega a la función de proveedor de servicios OAuth de ADC cuando se comunica con el extremo de token del IDP.

[NSHELP-28945]

Es posible que un dispositivo Citrix ADC no responda cuando la autenticación SAML esté en curso y se utilicen certificados X.509 de un tamaño de 1800 bytes o más en la autenticación SAML.

[NSHELP-28608]

La expresión Authentication, authorization and auditing.user.attribute puede dar un valor vacío en el dispositivo Citrix ADC de varios núcleos cuando la contraseña del usuario se cambia al expirar.

[NSHELP-28419]

El dispositivo Citrix ADC, cuando se configura como una parte de confianza de OAuth, no agrega la información del campo “correo electrónico” y “nombre de usuario” extraída del token de ID al atributo hash de la sesión de autenticación, autorización y auditoría.

[NSHELP-28262]

Cuando se configuran los metadatos SAML, se observa una pérdida de memoria con los certificados SSL.

[NSHELP-27846]

Cuando un usuario realiza un cierre de sesión de SAML, el cierre de sesión no se produce de inmediato y se muestra el siguiente mensaje de error:

```
Unsupported mechanisms found in Assertion; Please contact your administrator
.
```

Este error se observa porque el IDP que configuró el cliente utiliza una técnica de codificación de URL diferente para codificar el parámetro del algoritmo de firma en la respuesta. Esta corrección ahora admite la codificación del parámetro del algoritmo de firma en una respuesta SAML mediante varias técnicas de codificación de URL.

[NSHELP-27621]

A veces, si se configura nFactor, se registra una dirección IP incorrecta en el mensaje de cierre de sesión.

[NSHELP-26692]

El dispositivo Citrix ADC se bloquea si se cumplen las dos condiciones siguientes.

- La OTP de correo electrónico está configurada
- El servidor de correo electrónico no responde o hay un problema de red con el servidor de correo electrónico

[NSHELP-26137]

En una configuración de alta disponibilidad, el dispositivo Citrix ADC se bloquea cuando se inicia una sincronización forzada.

[NSAUTH-11876]

Intune NAC v2 no es compatible con Android 11 y versiones posteriores.

[NSAUTH-11872]

Los administradores no pueden usar la herramienta de conectividad LDAP o RADIUS si la contraseña contiene un cierto carácter especial o si los argumentos contienen un espacio.

[NSAUTH-11322]

Administración de bots

Cuando el desafío de CAPTCHA está en curso, la administración de bots de Citrix ADC no respeta el valor configurado establecido por el usuario para los reintentos de CAPTCHA.

[NSBOT-801]

Llamar a casa

El registro de CallHome puede fallar para los dispositivos Citrix ADC MPX que utilizan licencias agrupadas. El registro falla porque CallHome utiliza un número de serie incorrecto para registrar los dispositivos en el servidor de soporte de Citrix.

[NSHELP-28667]

Dispositivo Citrix ADC SDX

Cuando restaura un dispositivo Citrix ADC SDX desde la copia de seguridad, la cadena de comandos de la CLI no se restaura.

[NSHELP-30238]

En un dispositivo Citrix ADC SDX 115xx, la restauración de una VPX asignada con una gran cantidad de núcleos de CPU (de 3 a 5 núcleos) puede fallar si la copia de seguridad del dispositivo contiene tres o más instancias.

[NSHELP-30135]

En un dispositivo Citrix ADC SDX, el valor predeterminado para activar la alarma en la alerta `Hypervisor Disk Usage High` aumenta al 98 por ciento.

[NSHELP-29688]

Cuando el valor de velocidad de la interfaz es superior a 4 Gbps, se devuelve un valor incorrecto debido a un desbordamiento de enteros.

[NSHELP-29658]

En casos excepcionales, el inventario de ADC no se produce en un dispositivo Citrix ADC SDX.

[NSHELP-29607]

En un dispositivo Citrix ADC SDX, Management Service no envía notificaciones de syslog o correo electrónico si las fallas de la fuente de alimentación, el voltaje o el disco se producen más de una vez.

[NSHELP-29443]

Citrix Gateway

Los usuarios no pueden iniciar el complemento de la EPA ni el complemento de VPN después de actualizar a las versiones del explorador Chrome 98 o Edge 98. Para solucionar este problema, lleve a cabo lo siguiente:

1. Para la actualización del complemento de VPN, los usuarios finales deben conectarse mediante el cliente VPN por primera vez para obtener la solución en sus máquinas. En los intentos de

inicio de sesión posteriores, los usuarios pueden elegir el explorador o el complemento para conectarse.

2. Para el caso de uso exclusivo de la EPA, los usuarios finales no tendrán el cliente VPN para conectarse a la puerta de enlace. En este caso, lleve a cabo lo siguiente:

   a) Conéctese a la puerta de enlace mediante un explorador.
   b) Espere a que aparezca la página de descarga y descargue el archivo nsepa_setup.exe.
   c) Después de la descarga, cierre el explorador e instale el archivo nsepa_setup.exe.
   d) Reinicie el cliente.

[NSHELP-30641]

En una configuración de alta disponibilidad con configuración TCP SYSLOG, un nodo puede bloquearse durante la conmutación por error de alta disponibilidad o durante la operación de configuración clara.

[NSHELP-29251]

En la página del portal de Citrix Gateway, el icono de **enlace de proxy RDP** no cambia con el tema del portal de RFWebUI.

[NSHELP-28974]

Después de actualizar el dispositivo Citrix Gateway a la versión 13.0, la configuración de proxy en el perfil de sesión no funciona según lo previsto. La conexión de proxy se omite para el proxy NS no HTTP configurado.

Ejemplo:
add vpn sessionAction-proxy NS -httpProxy 192.0.2.0:24 -sslProxy 192.0.2.0:24

En este ejemplo, -httpProxy funciona según lo previsto, pero -sslProxy no funciona.

[NSHELP-28640]

El dispositivo Citrix Gateway se bloquea mientras se procesa STA en audio DTLS porque la memoria asignada no se restablece.

[NSHELP-28432]

El dispositivo Citrix ADC registra los mensajes obsoletos relacionados con el proceso VPND que están en desuso.

[NSHELP-28163]

El acceso a StoreFront a través de un servidor virtual VPN falla si se accede a StoreFront a través de un servidor virtual de equilibrio de carga de respaldo.

[NSHELP-27852]

El dispositivo Citrix Gateway puede bloquearse al volver a conectarse a una sesión ICA existente.

[NSHELP-27441]

No se puede desvincular una directiva de autorización clásica mediante la interfaz gráfica de usuario. Sin embargo, puede usar la CLI para desvincular la directiva Autenticación, autorización y autorización de auditoría.

Con esta corrección, ahora puede desvincular la directiva de autorización mediante la interfaz gráfica de usuario.

[NSHELP-27064]

Citrix Web App Firewall

Una actualización a la versión 2.9.12 de la biblioteca XML provoca que los archivos XML relacionados con la firma WAF se rompan durante el análisis.

[NSWAF-8662]

La protección de inyección de comandos JSON aparece `Not blocked` en el mensaje ns.log, incluso si el módulo Web App Firewall bloqueó la solicitud HTTP.

[NSHELP-29709]

Se muestra el mensaje de registro de Web App Firewall, `BAD URL` para infracciones de atributos de URL de scripts de sitios (XSS), y el término `Bad URL` no está claro a qué categoría pertenece (como etiqueta, patrón o atributo).

[NSHELP-29358]

La URL de publicación de huella digital del dispositivo bot puede fallar si la directiva de administración de bots está habilitada en un servidor virtual de equilibrio de carga de tipo SSL.

[NSHELP-29198]

El ID de firma de Web App Firewall 1048 bloquea la carga de la página de Citrix Gateway.

[NSHELP-29113]

Un dispositivo Citrix ADC podría bloquearse si se habilitan los siguientes módulos:

- Web App Firewall con comprobaciones de seguridad avanzadas.
- Appqoe.

[NSHELP-28251]

Equilibrio de carga

Cuando un miembro del grupo de servicios DNS de tipo Autoscale está en estado TROFS y si el mismo miembro se agrega nuevamente al grupo, el estado de este miembro no se propaga.

[NSHELP-29493]

La sincronización incremental falla para los comandos `add dns action` y `add location` con expresiones de directiva que contienen caracteres comodín.

[NSHELP-29301]

Algunos miembros del grupo de servicios no se eliminan de la lista de grupos de servicios de Autoscale cuando hay un conflicto entre los registros DNS resueltos dinámicamente y los miembros enlazados estáticamente. Este problema lleva a la corrupción de la memoria.

[NSHELP-28949]

El estado del grupo de servicios que se muestra en los comandos show y stat es incoherente.

[NSHELP-28931]

En casos excepcionales, es posible que falte la configuración de la base de datos de ubicaciones en el archivo de configuración (ns.conf).

[NSHELP-28570]

Los monitores de tipo SQL u Oracle se bloquean cuando el par envía una solicitud para restablecer la conexión existente.

[NSHELP-28478]

En una implementación habilitada para la persistencia, se almacena un servidor virtual incorrecto durante el guardado del contexto.

[NSHELP-28342]

La configuración de persistencia para un grupo LB se pierde después de una conmutación por error de HA o cuando se reinicia el dispositivo Citrix ADC.

[NSHELP-28071]

El estado configurado del monitor predeterminado se muestra como inhabilitado incluso cuando el monitor predeterminado está enlazado a un servicio.

[NSHELP-27669]

Otros

El siguiente problema se produce después de actualizar el dispositivo a la versión 12.1 de Citrix ADC compilación 63.22:

- Es posible que la API de búsqueda de extensiones no funcione después de la actualización.

[NSHELP-29860]

Redes

Un dispositivo Citrix ADC puede bloquearse si se cumplen todas las condiciones siguientes:

- Se configura una ruta de equilibrio de carga en un dominio de tráfico del dispositivo.
- Se realiza una operación de configuración clara en el dispositivo.

[NSNET-23847]

En una configuración NAT44 a gran escala, el dispositivo Citrix ADC puede bloquearse mientras recibe tráfico SIP por el siguiente motivo:

- El módulo LSN no encuentra el servicio mientras disminuye el recuento de referencias o elimina el servicio.

[NSHELP-29134]

En una implementación NAT44 a gran escala, el dispositivo Citrix ADC puede bloquearse al recibir tráfico SIP por el siguiente motivo:

- El módulo LSN accedió a la ubicación de memoria de un servicio ya eliminado.

[NSHELP-28815]

En un dispositivo Citrix ADC con un número par de motores de paquetes (PE), el dispositivo muestra incorrectamente el estado de las interfaces activas como inactivas de un conjunto de interfaces redundantes (canales LR). Este problema no afecta a ninguna funcionalidad del dispositivo Citrix ADC.

[NSHELP-28099]

Es posible que el dispositivo Citrix ADC no genere mensajes de captura SNMP `coldStart` después de un reinicio en frío.

[NSHELP-27917]

Plataforma

El comando `ntpdate` se bloquea y provoca un volcado de memoria.

[NSHELP-29649]

SSL

Un dispositivo Citrix ADC MPX 7500 se bloquea si se utiliza un conjunto de cifrado EXPORT.

[NSSSL-11294]

En casos excepcionales, es posible que se produzca un bloqueo durante el procesamiento de DTLS en las siguientes plataformas:

- MPX 5900

- MPX/SDX 8900
- MPX/SDX 15000
- MPX/SDX 15000-50G
- MPX/SDX 26000
- MPX/SDX 26000-50
- MPX/SDX 26000-100G

[NSHELP-29538]

En una configuración de alta disponibilidad, el tipo de certificado no se sincroniza correctamente entre los nodos principal y secundario.

[NSHELP-27589]

En una implementación de VPN, el dispositivo Citrix ADC selecciona una sesión SSL para reutilizar la sesión de la memoria caché para comunicarse con el servidor proxy o back-end. Lo hace sin hacer coincidir el SNI recibido del cliente con el SNI presente en la sesión en caché.

Como resultado, el SNI no se envía o se envía un SNI diferente en función de los datos almacenados en caché.

[NSHELP-27439]

Sistema

Se observa una pérdida de memoria en un dispositivo Citrix ADC al borrar la memoria asignada para los recursos del Sistema de prevención de intrusiones (IPS).

[NSHELP-29992]

Las operaciones de configuración que asocian perfiles SSL y claves de certificado SSL con un servidor virtual HTTP QUIC pueden fallar en una implementación de clúster de Citrix ADC.

[NSHELP-29655]

Se produce un error en una segunda solicitud en la misma conexión de cliente si se cumplen las siguientes condiciones:

- clientSideMeasurements está habilitado
- Se recibe la solicitud HEAD.

[NSHELP-29353]

En algunos casos, un dispositivo Citrix ADC puede bloquearse en las siguientes condiciones:

- Se utilizan tramas jumbo TCP.
- La persistencia se configura en un servidor virtual de equilibrio de carga TCP.

[NSHELP-29162]

Un dispositivo Citrix ADC se bloquea si se cumplen las siguientes condiciones:

- La opción de medidas del lado del cliente está habilitada en la acción AppFlow.
- Los encabezados de los fragmentos caen en el límite del paquete.

[NSHELP-29049]

Un dispositivo Citrix ADC restablece una conexión si el tamaño del proceso HTTP (una o varias solicitudes) supera los 128 KB. El problema se produce porque el tamaño del proceso está limitado a 128 KB.

[NSHELP-28846]

Un sistema de prevención de intrusiones (IPS) de Citrix ADC observa un problema con la directiva de reescritura al insertar o modificar datos si se cumple la siguiente condición:

- El dispositivo Citrix ADC envía paquetes de datos al servidor IPS antes de que se abra la conexión del servidor back-end.

[NSHELP-28496]

En una configuración de alta disponibilidad, la sincronización de alta disponibilidad de las configuraciones de la partición de administración falla en el nodo secundario por la siguiente razón:

- Problemas de memoria bajos causados por las enormes cargas de configuración en el nodo secundario

[NSHELP-28409]

Cuando un cliente restablece una conexión con varios flujos TCP, no se envía el registro de transacciones del lado del servidor, lo que hace que falten registros L4 para esos flujos de datos.

[NSHELP-28281]

En una conexión TCP, el dispositivo Citrix ADC puede descartar un paquete FIN, recibido de un servidor, en lugar de reenviarlo al cliente si se cumplen todas las condiciones siguientes:

- El almacenamiento en búfer TCP está habilitado.
- El servidor envía el paquete FIN y el paquete de datos por separado.

[NSHELP-27274]

En una configuración de clúster, el comando `set ratecontrol` solo funciona después de reiniciar el dispositivo Citrix ADC.

[NSHELP-21811]

Cuando un dispositivo Citrix ADC recibe un paquete TCP desordenado con el indicador FIN establecido, se pueden observar los siguientes problemas:

- El dispositivo Citrix ADC envía un SACK incorrecto, que indica que el dispositivo recibió un paquete TCP desordenado de 2 bytes en lugar de 1 byte.
- El dispositivo Citrix ADC no reconoce el paquete TCP FIN al recibir paquetes TCP en orden.

[NSBASE-15735]

Interfaz de usuario

Puede desvincular accidentalmente un certificado SSL porque no se solicita confirmación. Con esta corrección, cuando el usuario hace clic en un certificado vinculado, solicita una confirmación antes de desvincular un certificado.

[NSUI-17897]

La modificación de una regla RNAT basada en ACL, que ya tiene habilitada la conmutación por error de conexión, mediante la GUI de Citrix ADC puede producir el siguiente error:

- `Invalid argument value [connfailover]`

[NSHELP-29243]

Al configurar o comprobar los certificados SSL mediante la GUI de Citrix ADC, es posible que aparezca el error `Directory doesn't exist`. Este problema se produce cuando existe un nombre de archivo con dos puntos consecutivos (`..`) en la carpeta **SSL**/`nsconfig`/`ssl`.

[NSHELP-28589]

En una configuración de alta disponibilidad, la sincronización de alta disponibilidad podría fallar para un enlace de conjunto de patrones de directivas integrado, si el conjunto de patrones de directivas integrado se modificó en el nodo principal.

[NSHELP-28460]

Al anular la selección de la opción segura para el nodo RPC en la GUI de ADC, aparece el siguiente mensaje de error:

Falta el requisito previo del argumento [validateCert, segure==Yes]

[NSHELP-28239]

Cuando el usuario intenta cambiar el tamaño de página de una lista en las vistas del panel lateral, la página se distorsiona.

[NSHELP-28220]

Se introduce incorrectamente un carácter de barra invertida adicional si se utilizan caracteres especiales en los argumentos de algunos comandos SSL, como `create ssl rsakey` y `create ssl cert`.

[NSHELP-27378]

el comando ping o ping6 con la opción interface (-I) puede fallar con el siguiente error:

- **`interface`** `option not supported`

[NSHELP-26962]

Problemas conocidos

Los problemas que existen en la versión 13.1-17.42.

AppFlow

HDX Insight no informa de un error de inicio de aplicación causado por un usuario que intenta iniciar una aplicación o un escritorio a los que el usuario no tiene acceso.

[NSINSIGHT-943]

Autenticación, autorización y auditoría

Un dispositivo Citrix ADC no autentica los intentos de inicio de sesión con contraseñas duplicadas y evita los bloqueos de cuentas.

[NSHELP-563]

LoginSchema de DualAuthPushOrOTP.xml no aparece correctamente en la pantalla del editor de esquemas de inicio de sesión de la GUI de Citrix ADC.

[NSAUTH-6106]

El perfil proxy ADFS se puede configurar en una implementación de clúster. El estado de un perfil proxy se muestra incorrectamente en blanco al ejecutar el siguiente comando.
`show adfsproxyprofile <profile name>`

Solución temporal:

Conéctese al Citrix ADC activo principal del clúster y ejecute el comando `show adfsproxyprofile <profile name>`. Mostraría el estado del perfil de proxy.

[NSAUTH-5916]

La página Configurar servidor LDAP de autenticación de la GUI de Citrix ADC deja de responder si sigue los pasos siguientes:

- Se abre la opción Probar accesibilidad LDAP.
- Las credenciales de inicio de sesión no válidas se rellenan y envían.
- Las credenciales de inicio de sesión válidas se rellenan y envían.

Solución temporal:

Cierre y abra la opción Probar accesibilidad de LDAP.

[NSAUTH-2147]

Almacenamiento en caché

Es posible que un dispositivo Citrix ADC se bloquee si la función Almacenamiento en caché integrado está habilitada y el dispositivo tiene poca memoria.

[NSHELP-22942]

Dispositivo Citrix ADC SDX

En un dispositivo Citrix ADC SDX, si el CLAG se crea en una NIC Mellanox, la MAC de CLAG cambia cuando se reinicia la instancia VPX. El tráfico a la instancia VPX se detiene tras el reinicio porque la tabla MAC tiene la antigua entrada MAC de CLAG.

[NSSVM-4333]

En un dispositivo Citrix ADC SDX, las instancias de ADC no alcanzan su capacidad máxima al configurar el modo de asignación de rendimiento en ráfagas.

[NSHELP-27477]

Las caídas de paquetes se observan en una instancia VPX alojada en un dispositivo Citrix ADC SDX si se cumplen las siguientes condiciones:

- El modo de asignación de rendimiento está en ráfaga.
- Existe una gran diferencia entre el rendimiento y la capacidad máxima de ráfaga.

[NSHELP-21992]

Citrix Gateway

En algunos casos, el código de validación del servidor falla cuando se confía en el certificado del servidor. Como resultado, los usuarios finales no pueden acceder a la puerta de enlace.

[NSHELP-28942]

En una configuración de alta disponibilidad de Citrix Gateway, el nodo secundario podría bloquearse si Gateway Insight está habilitado.

[NSHELP-28856]

La autenticación de certificados de cliente falla para Citrix SSO para macOS si no hay certificados de cliente en el llavero de macOS.

[NSHELP-28551]

A veces, se desactiva la sesión de un usuario en Citrix Gateway en unos segundos cuando se establece el tiempo de espera por inactividad del cliente.

[NSHELP-28404]

En una configuración de alta disponibilidad, las sesiones de usuario VPN se desconectan si se cumple la siguiente condición:

- Si se realizan dos o más operaciones de failover manual de alta disponibilidad sucesivas cuando la sincronización de alta disponibilidad está en curso.

Solución temporal:

Realice una conmutación por error manual de alta disponibilidad sucesiva solo después de que se haya completado la sincronización de alta disponibilidad (ambos nodos están en estado de sincronización correcta).

[NSHELP-25598]

El complemento EPA para Windows no utiliza el proxy configurado del equipo local y se conecta directamente al servidor de puerta de enlace.

[NSHELP-24848]

Gateway Insight no muestra información precisa sobre los usuarios de VPN.

[NSHELP-23937]

El complemento VPN no establece un túnel después del inicio de sesión de Windows si se cumplen las siguientes condiciones:

- El dispositivo Citrix Gateway está configurado para la función Always On
- El dispositivo está configurado para la autenticación basada en certificados con autenticación de dos factores `off`

[NSHELP-23584]

A veces, al navegar por los esquemas, aparece el mensaje de error `Cannot read property 'type 'of undefined`.

[NSHELP-21897]

Si quiere utilizar la funcionalidad Always On VPN antes de iniciar sesión en Windows, se recomienda actualizar a Citrix Gateway 13.0 o posterior. Esto le permite aprovechar las mejoras adicionales introducidas en la versión 13.0 que no están disponibles en la versión 12.1.

[CGOP-19355]

El error de inicio de la aplicación debido a un tíquet STA no válido no se informa en Gateway Insight.

[CGOP-13621]

El informe Gateway Insight muestra incorrectamente el valor `Local` en lugar de `SAML` en el campo **Tipo de autenticación** para los errores de SAML.

[CGOP-13584]

En una configuración de alta disponibilidad, durante la conmutación por error de Citrix ADC, el recuento de SR aumenta en lugar del recuento de conmutación por error en Citrix ADM.

[CGOP-13511]

Al aceptar conexiones de host local desde el explorador web, el cuadro de diálogo **Aceptar conexión** para macOS muestra el contenido en inglés independientemente del idioma seleccionado.

[CGOP-13050]

El texto `Home Page` de la **aplicación Citrix SSO > Página de inicio** se corta para algunos idiomas.

[CGOP-13049]

Aparece un mensaje de error al agregar o modificar una directiva de sesión desde la GUI de Citrix ADC.

[CGOP-11830]

En Outlook Web App (OWA) 2013, al hacer clic en **Opciones** en el menú **Configuración**, se muestra un cuadro de diálogo **Error crítico**. Además, la página deja de responder.

[CGOP-7269]

En una implementación de clúster, si ejecuta un comando `force cluster sync` en un nodo que no es de CCO, el archivo ns.log contiene entradas de registro duplicadas.

[CGOP-6794]

Equilibrio de carga

En una configuración de alta disponibilidad, es posible que las sesiones de suscriptor del nodo principal no se sincronicen con el nodo secundario. Este es un caso raro.

[NSLB-7679]

El formato serviceGroupName de la captura `entityofs` del grupo de servicios es el siguiente: `<service(group)name>?<ip/DBS>?<port>`

En el formato de captura, el grupo de servicios se identifica mediante una dirección IP o un nombre y puerto de DBS. El signo de interrogación (?) se utiliza como separador. Citrix ADC envía la captura con el signo de interrogación (?). El formato aparece igual en la GUI de Citrix ADM. Este es el comportamiento esperado.

[NSHELP-28080]

Otros

Cuando se produce una sincronización forzada en una configuración de alta disponibilidad, el dispositivo ejecuta el comando `set urlfiltering parameter` en el nodo secundario.

Como resultado, el nodo secundario omite cualquier actualización programada hasta la siguiente hora programada mencionada en el parámetro `TimeOfDayToUpdateDB`.

[NSSWG-849]

Un dispositivo Citrix ADC puede reiniciarse debido al estancamiento de la CPU de administración si se produce un problema de conectividad con el proveedor externo de filtrado de URL.

[NSHELP-22409]

Redes

Es posible que un dispositivo Citrix ADC BLX con DPDK no se reinicie si se cumplen todas las condiciones siguientes:

- El dispositivo Citrix ADC BLX se asigna con un número bajo de `hugepages`. Por ejemplo, 1G.
- El dispositivo Citrix ADC BLX se asigna con una gran cantidad de procesos de trabajo. Por ejemplo, 28.

El problema se registra como un mensaje de error en `/var/log/ns.log`:

- `BLX-DPDK:DPDK Mempool could Not be Initialized for PE-x`

Nota: x es un número <= número de procesos de trabajo.

Solución temporal:

Asigne un número elevado de `hugepages` y, a continuación, reinicie el dispositivo.

[NSNET-25173]

Es posible que un dispositivo Citrix ADC BLX con DPDK no se reinicie si se cumple la siguiente condición:

- Al dispositivo Citrix ADC BLX se le asigna una gran cantidad de `hugepages`. Por ejemplo, 16 GB.

El problema se registra como un mensaje de error en `/var/log/ns.log`:

- `EAL: rte_mem_virt2phy(): cannot open /proc/self/pagemap: Too many open files`

Solución temporal:

Use una de las siguientes soluciones para este problema:

- Aumente el límite de archivos abiertos en el host Linux mediante el uso del comando `ulimit` o la modificación del archivo `limits.conf`.
- Reduzca el número de `hugepages` asignadas.

[NSNET-24727]

Un dispositivo Citrix ADC BLX en modo DPDK puede tardar un poco más en reiniciarse debido a la funcionalidad de facilidad de DPDK.

[NSNET-24449]

Tras una actualización de la versión 13.0 61.x del dispositivo Citrix ADC BLX a la versión 13.0 64.x, se pierde la configuración del archivo de configuración BLX. El archivo de configuración de BLX se restablece a los valores predeterminados.

[NSNET-17625]

Las siguientes operaciones de interfaz no son compatibles con las interfaces `X710 10G (i40e)` de Intel en un dispositivo Citrix ADC BLX con DPDK:

- Disable
- Enable
- Reset

[NSNET-16559]

En un host Linux basado en Debian (Ubuntu versión 18 y posteriores), un dispositivo Citrix ADC BLX siempre se implementa en modo compartido independientemente de la configuración del archivo de configuración BLX()`/etc/blx/blx.conf`. Este problema se produce porque `mawk`, que está presente de forma predeterminada en los sistemas Linux basados en Debian, no ejecuta algunos de los comandos `awk` presentes en el archivo `blx.conf`.

Solución temporal:

Instale `gawk` antes de instalar un dispositivo Citrix ADC BLX. Puede ejecutar el siguiente comando en la CLI del host de Linux para instalar `gawk`:

- apt-get install gawk

[NSNET-14603]

La instalación de un dispositivo Citrix ADC BLX podría fallar en un host Linux basado en Debian (versión 18 y posteriores de Ubuntu) con el siguiente error de dependencia:

```
The following packages have unmet dependencies: blx-core-libs:i386 :
PreDepends: libc6:i386 (>= 2.19)but it is not installable
```

Solución temporal:

Ejecute los siguientes comandos en la CLI del host Linux antes de instalar un dispositivo Citrix ADC BLX:

- dpkg — agregar arquitectura i386
- actualización apt-get
- apt-get dist-upgrade
- apt-get install libc6:i386

[NSNET-14602]

En algunos casos de conexiones de datos FTP, el dispositivo Citrix ADC solo realiza operaciones NAT y no procesamiento TCP en los paquetes para la negociación TCP MSS. Como resultado, la MTU de interfaz óptima no está configurada para la conexión. Esta configuración de MTU incorrecta provoca la fragmentación de los paquetes y afecta al rendimiento de la CPU.

[NSNET-5233]

Cuando se cambia un límite de memoria de la partición de administración en el dispositivo Citrix ADC, el límite de memoria intermedia TCP se establece automáticamente en el nuevo límite de memoria de la partición de administración.

[NSHELP-21082]

Plataforma

La conmutación por error de alta disponibilidad no funciona en las nubes de AWS y GCP. La CPU de administración puede alcanzar su capacidad del 100% en las nubes de AWS y GCP, y en Citrix ADC VPX en las instalaciones. Ambos problemas se producen cuando se cumplen las siguientes condiciones:

1. Durante el primer arranque del dispositivo Citrix ADC, no guarda la contraseña solicitada.
2. Posteriormente, reinicie el dispositivo Citrix ADC.

[NSPLAT-22013]

Cuando actualiza de compilaciones 13.0/12.1/11.1 a una versión 13.1 o baja de una compilación 13.1 a 13.0/12.1/11.1, algunos paquetes python no se instalan en los dispositivos Citrix ADC. Este problema se ha solucionado en las siguientes versiones de Citrix ADC:

- 13.1-4.x
- 13.0—82.31 y posteriores
- 12.1—62.21 y posteriores

Los paquetes python no se instalan cuando se degrada la versión de Citrix ADC de la versión 13.1-4.x a cualquiera de las siguientes versiones:

- Cualquier compilación 11.1
- 12.1—62.21 y anteriores
- 13.0-81.x y anteriores

[NSPLAT-21691]

En una configuración de clúster en un dispositivo Citrix ADC SDX, hay una discordancia de CLAG MAC en el segundo nodo y CLIP si se cumplen las siguientes condiciones:

- El CLAG se crea en una NIC Mellanox.
- Agrega otra instancia VPX al clúster y a la configuración de CLAG.

Como resultado, el tráfico a la instancia VPX se detiene.

[NSPLAT-21049]

En una configuración de clúster en un dispositivo Citrix ADC SDX, el primer nodo se cae debido a una discordancia de direcciones MAC en la tabla CLIP y MAC, si se cumplen las siguientes condiciones:

- El CLAG se crea en una NIC Mellanox.
- Quita el segundo nodo del clúster.

[NSPLAT-21042]

Cuando elimina una configuración de Autoscale o un conjunto de escala de VM de un grupo de recursos de Azure, elimine la configuración de perfil de nube correspondiente de la instancia de Citrix ADC. Utilice el comando `rm cloudprofile` para borrar el perfil.

[NSPLAT-4520]

En una configuración de alta disponibilidad en Azure, al iniciar sesión en el nodo secundario a través de la GUI, aparece la pantalla de usuario por primera vez (FTU) para la configuración del perfil en la nube de Autoscale.
Solución alternativa: omita la pantalla e inicie sesión en el nodo principal para crear el perfil de nube. Configure siempre el perfil de nube en el nodo principal.

[NSPLAT-4451]

La conmutación por error de alta disponibilidad para la instancia de Citrix ADC VPX en la nube de GCP y AWS falla cuando la contraseña de un nodo RPC contiene un carácter especial.

[NSHELP-28600]

Directivas

Las conexiones pueden bloquearse si el tamaño de los datos de procesamiento es mayor que el tamaño de búfer TCP predeterminado configurado.Solución alternativa: establezca el tamaño del búfer TCP en el tamaño máximo de los datos que deben procesarse.

[NSPOLICY-1267]

SSL

En un clúster heterogéneo de dispositivos Citrix ADC SDX 22000 y Citrix ADC SDX 26000, se produce una pérdida de configuración de entidades SSL si se reinicia el dispositivo SDX 26000.

Solución temporal:

1. En el CLIP, inhabilite SSLv3 en todas las entidades SSL nuevas y existentes, como servidores virtuales, servicios, grupos de servicios y servicios internos. Por ejemplo, `set ssl vserver <name> -SSL3 DISABLED`.

2. Guarde la configuración.

[NSSSL-9572]

No se puede agregar un objeto de Azure Key Vault si ya se ha agregado un objeto de autenticación de Azure Key Vault.

[NSSSL-6478]

Puede crear varias entidades de la aplicación Azure con el mismo ID de cliente y secreto de cliente. El dispositivo Citrix ADC no devuelve ningún error.

[NSSSL-6213]

El siguiente mensaje de error incorrecto aparece cuando se quita una clave de HSM sin especificar Key Vault como el tipo de HSM.
ERROR: Actualización de crl inhabilitada

[NSSSL-6106]

La actualización automática de claves de sesión aparece incorrectamente como inhabilitada en una dirección IP de clúster. (Esta opción no se puede desactivar).

[NSSSL-4427]

Aparece `Warning: No usable ciphers configured on the SSL vserver/service,,` un mensaje de advertencia incorrecto, si intenta cambiar el protocolo o el cifrado SSL en el perfil SSL.

[NSSSL-4001]

Un tíquet de sesión caducado se respeta en un nodo que no es de CCO y en un nodo de alta disponibilidad después de una conmutación por error de alta disponibilidad.

[NSSSL-3184]

Sistema

El valor MAX_CONCURRENT_STREAMS se establece en 100 de forma predeterminada si el dispositivo no recibe el marco de configuración **max_concurrent_stream** del cliente.

[NSHELP-21240]

Los contadores mptcp_cur_session_without_subflow disminuyen incorrectamente a un valor negativo en lugar de cero.

[NSHELP-10972]

Se observa un problema al generar los informes PCI DSS en la GUI de Citrix ADC (Navegación: **Sistema > Informes > Generar informe PCI DSS**).

[NSBASE-16225]

La IP del cliente y la IP del servidor se invierten en el registro SkipFlow de HDX Insight cuando se configura el tipo de transporte LogStream para Insight

[NSBASE-8506]

El dispositivo Citrix ADC descarta paquetes que contienen encabezados HTTP personalizados con un punto (“. “) en el campo del nombre del encabezado. Esta acción se produce porque el parámetro `allowOnlyWordCharactersAndHyphen` está habilitado de forma predeterminada en el perfil HTTP predeterminado.

Solución temporal: Inhabilite `allowOnlyWordCharactersAndHyphen` en el perfil HTTP predeterminado. Sin embargo, Citrix recomienda mantenerla habilitada.

[NSBASE-16722]

Interfaz de usuario

Para la función Reescritura de MQTT, no puede eliminar una expresión mediante el Editor de expresiones en la GUI.

Solución temporal:

Use el comando de acción add o edit de tipo MQTT a través de la CLI.

[NSUI-18049]

En la GUI de Citrix ADC, el enlace `Help` presente debajo de la ficha `Dashboard` no funciona.

[NSUI-14752]

El asistente Crear/Supervisar CloudBridge Connector podría dejar de responder o no configurar un conector de cloudbridge.

Solución temporal:

Configure los conectores cloudbridge agregando perfiles IPsec, túneles IP y reglas PBR mediante la GUI o CLI de Citrix ADC.

[NSUI-13024]

Si crea una clave ECDSA mediante la interfaz gráfica de usuario, no se muestra el tipo de curva.

[NSUI-6838]

La carga y adición de un archivo de lista de revocación de certificados (CRL) produce un error en la configuración de una partición de administración.

[NSHELP-20988]

Al revertir la versión 13.0-71.x de un dispositivo Citrix ADC a una versión anterior, es posible que algunas API de NITRO no funcionen debido a los cambios en los permisos de archivo.

Solución temporal:

Cambie el permiso de `/nsconfig/ns.conf` a 644.

[NSCONFIG-4628]

Si usted (administrador del sistema) realiza todos los pasos siguientes en un dispositivo Citrix ADC, es posible que los usuarios del sistema no inicien sesión en el dispositivo Citrix ADC degradado.

1. Actualice el dispositivo Citrix ADC a una de las compilaciones:
    - 13.0 52.24 compilación
    - 12.1 57,18 compilación
    - 11.1 65.10 compilación
2. Agregar un usuario del sistema o cambiar la contraseña de un usuario del sistema existente y guardar la configuración, y
3. Rebaja la versión del dispositivo Citrix ADC a cualquier versión anterior.

Para mostrar la lista de estos usuarios del sistema mediante la CLI:
En el símbolo del sistema, escriba:

```
query ns config -changedpassword [-config <full path of the configuration file (ns.conf)>]
```

Solución temporal:

Para solucionar este problema, utilice una de las siguientes opciones independientes:

1. Si el dispositivo Citrix ADC aún no se ha rebajado (paso 3 de los pasos mencionados anteriormente), revierta la versión del dispositivo Citrix ADC con un archivo de configuración del que se ha creado previamente una copia de seguridad (ns.conf) de la misma compilación de la versión.
2. Cualquier administrador del sistema cuya contraseña no se haya cambiado en la compilación actualizada puede iniciar sesión en la compilación degradada y actualizar las contraseñas de otros usuarios del sistema.
3. Si ninguna de las opciones anteriores funciona, el administrador del sistema puede restablecer las contraseñas de usuario del sistema.

Para obtener más información, consulte https://docs.citrix.com/en-us/citrix-adc/13/system/ns-ag-aa-intro-wrapper-con/ns-ag-aa-reset-default-amin-pass-tsk.html

[NSCONFIG-3188]

Notas de la versión de Citrix ADC 13.1-12.51

June 22, 2022

Este documento de notas de la versión describe las mejoras y los cambios, los problemas resueltos y conocidos que existen para la versión de Citrix ADC, compilaciones 13.1-12.51.

La compilación 13.1—12.51 reemplaza a la compilación 13.1—12.50.

Esta compilación también incluye una solución para el siguiente problema: NSWAF-8668.

Notas

Este documento de notas de la versión no incluye correcciones relacionadas con la seguridad. Para obtener una lista de correcciones y avisos relacionados con la seguridad, consulte el boletín de seguridad de Citrix.

Novedades

Las mejoras y los cambios que están disponibles en las compilaciones 13.1-12.51.

Autenticación, autorización y auditoría

Compatibilidad con las últimas versiones de las API NAC de Intune

La compatibilidad de Citrix Gateway para el control de acceso a redes (NAC) de Intune ahora se ha mejorado para las últimas versiones de las API NAC de Intune.

[NSAUTH-9722]

Compatibilidad con la implementación activa-activa de GSLB para la autenticación nFactor mediante proxy de conexión

Ahora se ha agregado compatibilidad para la implementación activa-activa de GSLB para la autenticación nFactor mediante el proxy de conexión. Esta compatibilidad se aplica tanto a Citrix Gateway como a los casos de autenticación, autorización y auditoría.
Actualmente, si se configuran varios factores en la autenticación nFactor y si la puerta de enlace está configurada para GSLB, la autenticación podría romperse si la solicitud del cliente llega a diferentes sitios GSLB.

Por ejemplo, si LDAP se configura como primer factor y RADIUS se configura como segundo factor, la autenticación podría romperse en el siguiente caso.

- La solicitud del cliente para LDAP aterriza en el sitio 1 de GSLB.
- La solicitud de Radius llega al sitio 2 de GSLB.
  El proxy de conexión ahora se usa para enrutar la solicitud a los sitios GSLB correctos para completar la autenticación y servir el tráfico.

[NSAUTH-7141]

Dispositivo Citrix ADC SDX

En un dispositivo Citrix ADC SDX, Management Service sondea las instancias de Citrix ADC en segundo plano en busca de operaciones, como certificados SSL, funciones de red y auditoría de configuración. Ahora puede habilitar y inhabilitar este sondeo en función de sus requisitos. La desactivación de este sondeo mejora el rendimiento de las instancias de Management Service y ADC.

[NSSVM-4991]

Citrix Web App Firewall

Registro detallado para comprobaciones de seguridad JSON (SQL, CMD y XSS)

El dispositivo Citrix ADC ahora le permite configurar el parámetro de nivel de registro detallado para los detalles de las infracciones de registro, como el patrón, la carga útil del patrón y los detalles del encabezado HTTP para las comprobaciones de seguridad de JSON. Los detalles del registro se envían al servidor Citrix ADM para fines de supervisión y solución de problemas. El mensaje de registro verboso no se almacena en el archivo ns.log.

[NSWAF-8269]

Directivas de registro de auditoría obsoletas de Web App Firewall Classic

Para vincular de forma global las directivas de Web App Firewall, ahora `APPFW_GLOBAL` se puede configurar un nuevo tipo de enlace global en los comandos `bind audit syslogGlobal` y `bind audit nslogGlobal`. Las directivas de registro de auditoría enlazadas globales se evalúan en el contexto de registro de Web App Firewall.

[NSWAF-406]

Equilibrio de carga

Función de directiva de reescritura para el protocolo MQTT

La función de reescritura ahora es compatible con el protocolo MQTT. Puede configurar la directiva de reescritura para que tome medidas en función de los parámetros de las solicitudes del cliente MQTT y las respuestas del servidor.

[NSLB-8661]

Orden prioritario de servicios

La función de orden de prioridad para los servicios le permite priorizar el orden de los servicios o grupos de servicios en función de las preferencias de selección de equilibrio de carga. Ahora puede

configurar el orden de selección de servicios cuando vincula los servicios o grupos de servicios a los servidores virtuales LB o GSLB. Se agrega un nuevo parámetro, -order <number>, a los comandos bind para configurar la preferencia de selección de servicios.

De forma predeterminada, el número de pedido más bajo tiene la prioridad más alta. Sin embargo, puede diferir este comportamiento de selección predeterminado. Con los nuevos comandos de acción y directiva de LB, ahora puede configurar el orden de selección de servicios en función del tráfico de clientes entrante.

La función de orden de prioridad para los servicios imita el comportamiento de la funcionalidad de la cadena de servidores virtuales principal y de reserva con menos comandos de configuración.

[NSLB-8039]

Redes

Inserte la dirección IP del cliente en el encabezado externo del túnel IP para configurar el equilibrio de carga sin sesión

En una configuración de equilibrio de carga sin sesión con la siguiente configuración, el dispositivo Citrix ADC encapsulador utiliza una dirección SNIP en lugar de la dirección IP del cliente como IP de origen en el encabezado externo del túnel IP.

- Servidor virtual de equilibrio de carga:
- modo de redirección (m): túnel IP
- sin sesión: habilitado
- Parámetro global del túnel IP:
- usar la dirección IP de origen del cliente (useClientSourceIP): habilitado

Sin embargo, en algunos casos, el desencapsulador de túnel (un Citrix ADC back-end o un servidor back-end) debe conocer la dirección IP del cliente.

Para cumplir con este requisito, el dispositivo Citrix ADC encapsulador ahora usa la dirección IP del cliente como la IP de origen en el encabezado externo del túnel IP.

Para obtener más información, consulte Configurar el equilibrio de carga en modo DSR mediante IP sobre IP.

[NSNET-21804]

Plataforma

La imagen de VMware ESXi se inicia hasta la versión 13 de hardware virtual

Cuando implementa una instancia de Citrix ADC VPX desde la imagen de VMware ESXi (12.1 en adelante), de forma predeterminada, la máquina virtual presenta la versión de hardware 13.

[NSPLAT-21416]

Compatibilidad con el controlador Intel Ethernet series X710 y XL710 en Citrix Hypervisor

Ahora puede configurar una instancia de Citrix ADC VPX que se ejecute en Citrix Hypervisor mediante la virtualización de E/S de raíz única (SR-IOV) con las siguientes NIC:

- Intel X710 10G
- Intel XL710 40G

[NSPLAT-21410]

Implemente un par de alta disponibilidad VPX mediante direcciones IP privadas con una VPC compartida de AWS

Ahora puede implementar un par de alta disponibilidad VPX con direcciones IP privadas en diferentes zonas de AWS con nubes privadas virtuales (VPC) compartidas de AWS. El uso compartido de VPC permite que varias cuentas de AWS creen sus recursos de aplicaciones en VPC compartidas y administradas de forma centralizada. Puede crear instancias de Citrix ADC VPX en una VPC compartida de AWS. La VPC compartida reduce la cantidad de VPC que se crean y administran, a la vez que se usan cuentas separadas para la facturación y el control de acceso.

[NSPLAT-21401]

SSL

Nueva expresión para detectar malware basado en la huella digital SSL JA3

Se agrega una nueva expresión SSL, CLIENT.SSL.JA3_FINGERPRINT, que ayuda a identificar cualquier solicitud maliciosa al comparar la solicitud con la huella digital JA3 configurada.

Ejemplo:

```
add ssl policy ja3_pol -rule "CLIENT.SSL.JA3_FINGERPRINT.EQ(bb4c15a90e93a25ddc1627439
)"-action reset
```

[NSSSL-10156]

Compatibilidad con paquetes de certificados en clúster

Los paquetes de certificados ahora se admiten en una configuración de clúster.

[NSSSL-9854]

Compatibilidad con el paquete de certificados SSL

La función de paquete de certificados se ha mejorado para tratar el paquete como una entidad. Por lo tanto, no es necesario crear archivos para cada certificado intermedio. Ahora, dos paquetes de certificados pueden compartir parte de la cadena de certificados intermedia. También puede agregar un par de claves de certificado con el mismo certificado y clave de servidor que también forma parte de un paquete de certificados. La eliminación del paquete de certificados también se simplifica.

Anteriormente, al agregar un paquete de certificados, se agregaron varios comandos en la configuración. No puede agregar otro paquete de certificados si dos paquetes comparten un certificado intermedio común. La eliminación también era un proceso manual.

[NSSSL-9425]

Sistema

Los comandos relacionados con la inyección html se eliminaron en la versión 13.1. Este cambio elimina todo el código de backend.

[NSBASE-14742]

Problemas resueltos

Los problemas que se abordan en la compilación 13.1-12.51.

Autenticación, autorización y auditoría

El dispositivo Citrix ADC se bloquea si se configura la OTP de correo electrónico.

[NSHELP-29312]

La herramienta de cifrado OTP nativa no permite caracteres especiales en el nombre del dispositivo.

[NSHELP-28795]

Cuando inicia sesión en el dispositivo Citrix ADC, aparece un campo de contraseña en blanco cuando se cumplen las dos condiciones siguientes.

- Se configura la autenticación de dos factores Duo
- Se utiliza el tema del portal RFwebUI

[NSHELP-27868]

Se deniega el acceso a un servicio si se cumplen las siguientes condiciones:

- El servicio está enlazado a un servidor virtual de autenticación.
- La autenticación 401 se configura en el servicio y en el servidor virtual al que está enlazado el servicio.

[NSHELP-26903]

En un caso poco frecuente, el nodo secundario en una configuración de alta disponibilidad puede bloquearse si se cumple la siguiente condición.

- `aaa groups` y/o `aaa users` están configurados en el dispositivo Citrix ADC.

[NSHELP-26732]

Si la contraseña de administrador para los servicios LDAP, RADIUS o TACACS contiene el carácter de comillas dobles (“), el dispositivo Citrix ADC lo elimina durante la comprobación de `Test Connectivity`, lo que provoca un error de conexión.

[NSHELP-23630]

Dispositivo Citrix ADC SDX

En las plataformas Citrix ADC SDX 14000-40G, 15000 y 15000-50G, se produce un error al configurar la velocidad de la interfaz mediante la CLI.

[NSHELP-29388]

Cuando cambia el perfil en una instancia de ADC alojada en la plataforma Citrix ADC SDX, es posible que observe algunas entradas adicionales para el comando `save config` en el archivo de registros.

[NSHELP-29343]

En un dispositivo Citrix ADC SDX, un agente SNMP que se ejecuta en Management Service devuelve un código de error incorrecto para los OID inexistentes.

[NSHELP-29209]

Los datos de la tabla de eventos ADC ahora se pueden ordenar en las páginas si el número total de registros de datos es inferior a 5000.

[NSHELP-29170]

Citrix Gateway

El dispositivo Citrix ADC podría bloquearse si se configura la EPA y no hay suficiente memoria disponible.

[NSHELP-28329]

El directorio /var/NetScaler/logon/LogonPoint/custom/ no se crea después de una actualización si el directorio no estaba presente inicialmente.

[NSHELP-28223]

Es posible que vea una línea adicional para los registros NS_AUDITLOG_STR* en el archivo ns_aaa_json.c.

[NSHELP-28160]

El registro de DNS no funciona después de que se establece la conexión VPN.

Para solucionar este problema, debe habilitar la perilla nsapimgr, nsapimgr_wr.sh -ys call=toggle_vpn_configured_

[NSHELP-27760]

A veces, durante el inicio de sesión de transferencia, las subredes IP de intranet se muestran incorrectamente en el lado del cliente.

[NSHELP-26904]

La latencia ICA de una sesión se registra incorrectamente como 64 000 ms en Citrix Director cuando la latencia L7 está habilitada. La latencia L7 se activa cuando el mando de `nsapimgr enable_ica_l7_latency` está ajustado a 1.

[NSHELP-23459]

El archivo de registros de Gateway Insight se inunda con el siguiente mensaje cuando los usuarios inician sesión en el dispositivo Citrix Gateway y acceden a las aplicaciones ICA.

```
GwInsight: Func=ns_aaa_copy_email_id_to_vpn_record input hash_attrs_len is
 zero Oct 25 23:01:31 <local0.err> 10.217.24.1Oct 25 23:01:31 <local0.err
> 10.217.24.101 10/26/2021:06:01:31 GMT NSGWTHDR 0-PPE-0 : default SSLVPN
 Message 10491736 0 : GwInsight: Func=ns_aaa_copy_email_id_to_vpn_record
input hash_attrs_len is zero
```

[CGOP-19685]

La función de marcadores empresariales del portal de Citrix Gateway solo admite los siguientes protocolos. Todos los demás marcadores están bloqueados. `http://`, `https://`, `rdp://` y `ftp://`.

[CGOP-19543]

Citrix Web App Firewall

Si utiliza firmas WAF, después de actualizar la compilación, debe actualizar todas las firmas WAF, incluidas las firmas predeterminadas, a la versión más reciente. A continuación, vuelva a habilitar las reglas de firma requeridas.

[NSWAF-8668]

En algunos casos, un dispositivo Citrix ADC puede bloquearse cuando las URL de captura se generan automáticamente en el sistema de administración de bots.

[NSHELP-29339]

Equilibrio de carga

El grupo de servicios GSLB no puede gestionar las actualizaciones del monitor debido a la falta de un valor ENUM en los comandos fallidos.

[NSHELP-29050]

El dispositivo Citrix ADC se bloquea al intentar liberar memoria asignada en una partición diferente de la que se está liberando.

[NSHELP-29038]

Si hay un registro DNS de tipo ZONE disponible para el dominio principal, la consulta del dominio secundario con un registro NS existente da como resultado un registro SOA del dominio principal en lugar del registro NS del dominio secundario.

[NSHELP-28793]

Es posible que el dispositivo Citrix ADC no responda a una consulta de dominio GSLB con una dirección IP de servicio GSLB esperada, si el servidor virtual GSLB se configura de la siguiente manera:
Tipo de persistencia: Dirección IP de origen
Algoritmo de equilibrio de carga: Proximidad estática
Método de equilibrio de carga de seguridad: Tiempo de ida y vuelta (RTT)

[NSHELP-28668]

El estado del grupo de servicios de Autoscale basado en dominio GSLB o equilibrio de carga permanece INACTIVO si usa un puerto comodín.

[NSHELP-28548]

El último mensaje de respuesta se muestra incorrectamente para los monitores enlazados a grupos de servicios GSLB.

[NSHELP-28393]

El valor cookieTimeout se establece incorrectamente durante la operación GET, lo que provoca un error en la operación de actualización del servidor virtual de CS.

[NSHELP-27979]

Un dispositivo Citrix ADC puede fallar al manejar la sonda de monitor para el tipo de monitor mysql, lo que eventualmente lleva a un reinicio del sistema.

[NSHELP-27953]

Otros

La instancia CPX de Citrix ADC, que se ejecuta en un sistema Linux con arquitectura de 64 bits y 1 TB de almacenamiento de archivos, puede cargar archivos de certificados y claves ahora.

[NSHELP-28986]

La coincidencia del patrón del conjunto de URL falla para los dominios estándar IDNA2008.

[NSHELP-28902]

Cuando el reenvío basado en Mac (MBF) está habilitado para VXLAN, no se establecía la sesión TCP con estado.

[NSHELP-27125]

Redes

La actualización de un dispositivo Citrix ADC que tiene particiones de administración puede provocar alguna pérdida de configuración si se cumple la siguiente condición:

- Si toda la memoria del sistema disponible se asigna a particiones de administración.

[NSNET-23031]

LIMITACIONES -

La VLAN ID 2 está reservada para uso interno

VLAN ID 2 está reservado para uso interno para implementaciones en el modo puente y ninguno. Citrix ADC CPX vincula todas las interfaces, excepto la 0/1, a la VLAN ID 2 y la MTU (unidades máximas de transmisión) de la VLAN ID 2 se establece igual a la MTU de la interfaz eth0. Si quiere configurar la VLAN y vincular la interfaz con ella, establezca la MTU en la VLAN como la MTU de la interfaz configurada en Linux, si la MTU de la interfaz es inferior a 1500 bytes.

[NSNET-22807]

Un dispositivo Citrix ADC BLX en modo DPDK podría bloquearse si se configura un perfil de Firewall de aplicaciones web con comprobaciones de protección de seguridad avanzadas.

[NSNET-22654]

El dispositivo Citrix ADC puede bloquearse al crear una sonda de monitor para el servicio relacionado si se cumplen las siguientes condiciones:

- Un perfil de red con un conjunto de IP que tiene al menos una dirección IPv4 y ninguna dirección IPv6. El perfil de red está enlazado a un monitor, que se establece en un servicio IPv6.
- Un perfil de red con un conjunto de IP que tiene al menos una dirección IPv6 y ninguna dirección IPv4. El perfil de red está enlazado a un monitor, que se establece en un servicio IPv4.

[NSHELP-29382]

En un dispositivo Citrix ADC, las conexiones de datos FTP pasivas pueden perderse después de un error de asignación de memoria.

[NSHELP-26522]

Plataforma

Las instancias de Citrix ADC VPX que usan el controlador VMXNET3 pueden bloquearse de forma aleatoria si la instancia se ejecuta en una de las siguientes compilaciones de Citrix ADC:

- Citrix ADC 13.1 compilación 4.x
- Citrix ADC 13.1 compilación 9.x

[NSHELP-29120]

Directivas

Un dispositivo Citrix ADC puede bloquearse con las siguientes condiciones:

- Una acción de mensaje de auditoría se configura con la expresión del generador de cadenas con una o más funciones REGEX aplicadas al cuerpo de una solicitud.
- Un perfil de Application Firewall configurado con la opción Streaming habilitada.

Por ejemplo: HTTP.REQ.BODY(10000000).REGEX_SELECT(re/name=[^\r\n]*[\r\n]+/).

[NSHELP-27895]

SSL

Un dispositivo Citrix ADC se bloquea al procesar una solicitud HTTP si la acción de directiva se establece en `Forward` para una directiva que ya está enlazada en el punto de enlace de la solicitud.

[NSHELP-29115]

Un dispositivo Citrix ADC se bloquea si se siguen los siguientes pasos:

1. Se agrega un monitor de tipo SSL.
2. Un par de claves de certificado está vinculado al monitor.
3. Se quita el monitor.
4. Se agrega otro monitor con el mismo nombre.
5. Se actualiza el par de claves de certificado.

[NSHELP-28666]

Ahora se muestran todas las direcciones IP de un certificado SAN. Anteriormente, solo se mostraba la última dirección IP de SAN de todas las direcciones IP del certificado de SAN.

[NSHELP-27336]

El protocolo de enlace SSL falla si utiliza cifrados DH con un HSM externo.

[NSHELP-25307]

Sistema

Cuando un dispositivo Citrix ADC recibe una trama GOWAY HTTP/2 de un cliente, restablece incorrectamente todas las transmisiones con un ID de transmisión mayor que el ID prometido (último identificador de transmisión iniciado por el par).

[NSHELP-29328]

En Citrix ADM, el agente ADM puede informar de un uso elevado de memoria debido a un problema en el agente ADM.

[NSHELP-29285]

El dispositivo Citrix ADC se bloquea cuando se cumplen todas las condiciones siguientes:

- Una acción de inspección de contenido, con una dirección IP de servidor, utiliza los datos internos de un servicio si ya está configurado.
- Como resultado, los datos internos del servicio también se eliminan cuando se elimina la acción de CI.
- Cuando se elimina el servicio real, el dispositivo Citrix ADC intenta acceder y eliminar los datos internos ya eliminados.

[NSHELP-28293]

En un dispositivo Citrix ADC con particiones de administración, es posible que la utilidad `nstrace` no se ejecute correctamente en una partición no predeterminada

[NSBASE-15738]

En una configuración de clúster, un nodo con prioridad de CCO se desconecta de Open vSwitch (OVS) debido a problemas de red. Cuando el nodo se vuelve a unir a la configuración del clúster, no recibe la cookie SYN más reciente.

[NSBASE-14419]

Interfaz de usuario

Las instancias de ADC en un modo de clúster configuradas con capacidad agrupada disminuyen. Este problema ocurre cuando se configura un nombre de host en los nodos del clúster y si los nodos tardan más en conectarse al servidor de licencias ADM durante el arranque.

[NSHELP-28613]

La GUI de Citrix ADC puede generar incorrectamente un paquete de asistencia técnica en clúster de un solo nodo en lugar de todos los nodos del clúster.

[NSHELP-28606]

La generación de un paquete de asistencia técnica en clúster mediante la GUI de Citrix ADC puede fallar con un error.

[NSHELP-28586]

En una interfaz CLI de Citrix ADC, las opciones para vincular comandos no se completan automáticamente si presiona la tecla <Tab> mientras escribe el comando en el símbolo del sistema.

Por ejemplo, escriba el siguiente comando y, al usar la tecla <Tab>, los objetos no se rellenan automáticamente.

```
bind authentication vserver <authvservername> -policy <Tab>.
```

En este caso, el servidor virtual de autenticación se puede vincular a varios tipos de objetos, como la directiva de radio, la directiva de Idappolicy, la directiva de certificados, la directiva de TACAS, la directiva de autenticación avanzada, etc.

[NSCONFIG-6340]

Problemas conocidos

Los problemas que existen en las versiones 13.1-12.51.

AppFlow

HDX Insight no informa de un error de inicio de aplicación causado por un usuario que intenta iniciar una aplicación o un escritorio a los que el usuario no tiene acceso.

[NSINSIGHT-943]

Autenticación, autorización y auditoría

En algunos casos, se observa una pérdida de memoria en un dispositivo Citrix ADC si la funcionalidad SSO se usa con un servidor proxy.

[NSHELP-27744]

Un dispositivo Citrix ADC no autentica los intentos de inicio de sesión con contraseñas duplicadas y evita los bloqueos de cuentas.

[NSHELP-563]

LoginSchema de DualAuthPushOrOTP.xml no aparece correctamente en la pantalla del editor de esquemas de inicio de sesión de la GUI de Citrix ADC.

[NSAUTH-6106]

El perfil proxy ADFS se puede configurar en una implementación de clúster. El estado de un perfil proxy se muestra incorrectamente en blanco al ejecutar el siguiente comando.

```
show adfsproxyprofile <profile name>
```


Solución temporal:

Conéctese al Citrix ADC activo principal del clúster y ejecute el comando `show adfsproxyprofile <profile name>`. Mostraría el estado del perfil de proxy.

[NSAUTH-5916]

La página Configurar servidor LDAP de autenticación de la GUI de Citrix ADC deja de responder si sigue los pasos siguientes:

- Se abre la opción Probar accesibilidad LDAP.
- Las credenciales de inicio de sesión no válidas se rellenan y envían.
- Las credenciales de inicio de sesión válidas se rellenan y envían.

Solución temporal:

Cierre y abra la opción Probar accesibilidad de LDAP.

[NSAUTH-2147]

Almacenamiento en caché

Es posible que un dispositivo Citrix ADC se bloquee si la función Almacenamiento en caché integrado está habilitada y el dispositivo tiene poca memoria.

[NSHELP-22942]

Dispositivo Citrix ADC SDX

En un dispositivo Citrix ADC SDX, si el CLAG se crea en una NIC Mellanox, la MAC de CLAG cambia cuando se reinicia la instancia VPX. El tráfico a la instancia VPX se detiene tras el reinicio porque la tabla MAC tiene la antigua entrada MAC de CLAG.

[NSSVM-4333]

En un dispositivo Citrix ADC SDX, las instancias de ADC no alcanzan su capacidad máxima al configurar el modo de asignación de rendimiento en ráfagas.

[NSHELP-27477]

Las caídas de paquetes se observan en una instancia VPX alojada en un dispositivo Citrix ADC SDX si se cumplen las siguientes condiciones:

- El modo de asignación de rendimiento está en ráfaga.
- Existe una gran diferencia entre el rendimiento y la capacidad máxima de ráfaga.

[NSHELP-21992]

Citrix Gateway

En algunos casos, el código de validación del servidor falla cuando se confía en el certificado del servidor. Como resultado, los usuarios finales no pueden acceder a la puerta de enlace.

[NSHELP-28942]

A veces, después de desconectar la VPN, el solucionador de DNS no resuelve los nombres de host porque los sufijos DNS se eliminan durante la desconexión de la VPN.

[NSHELP-28848]

La autenticación de certificados de cliente falla para Citrix SSO para macOS si no hay certificados de cliente en el llavero de macOS.

[NSHELP-28551]

A veces, se desactiva la sesión de un usuario en Citrix Gateway en unos segundos cuando se establece el tiempo de espera por inactividad del cliente.

[NSHELP-28404]

Es posible que el complemento de Windows se bloquee durante la autenticación.

[NSHELP-28394]

El complemento EPA para Windows no utiliza el proxy configurado del equipo local y se conecta directamente al servidor de puerta de enlace.

[NSHELP-24848]

Gateway Insight no muestra información precisa sobre los usuarios de VPN.

[NSHELP-23937]

El complemento VPN no establece un túnel después del inicio de sesión de Windows si se cumplen las siguientes condiciones:

- El dispositivo Citrix Gateway está configurado para la función Always On
- El dispositivo está configurado para la autenticación basada en certificados con autenticación de dos factores `off`

[NSHELP-23584]

A veces, al navegar por los esquemas, aparece el mensaje de error `Cannot read property 'type 'of undefined`.

[NSHELP-21897]

Si quiere utilizar la funcionalidad Always On VPN antes de iniciar sesión en Windows, se recomienda actualizar a Citrix Gateway 13.0 o posterior. Esto le permite aprovechar las mejoras adicionales introducidas en la versión 13.0 que no están disponibles en la versión 12.1.

[CGOP-19355]

El error de inicio de la aplicación debido a un tíquet STA no válido no se informa en Gateway Insight.

[CGOP-13621]

El informe Gateway Insight muestra incorrectamente el valor en `Local` lugar de `SAML` en el campo Tipo de autenticación para los errores de SAML.

[CGOP-13584]

En una configuración de alta disponibilidad, durante la conmutación por error de Citrix ADC, el recuento de SR aumenta en lugar del recuento de conmutación por error en Citrix ADM.

[CGOP-13511]

Al aceptar conexiones de host locales desde el explorador, el cuadro de diálogo Aceptar conexión para macOS muestra el contenido en inglés, independientemente del idioma seleccionado.

[CGOP-13050]

El texto `Home Page` de la aplicación Citrix SSO > Página de inicio se corta en algunos idiomas.

[CGOP-13049]

Aparece un mensaje de error al agregar o modificar una directiva de sesión desde la GUI de Citrix ADC.

[CGOP-11830]

En Outlook Web App (OWA) 2013, al hacer clic en **Opciones** en el menú Configuración, se muestra un cuadro de diálogo **Error crítico**. Además, la página deja de responder.

[CGOP-7269]

En una implementación de clúster, si ejecuta un comando `force cluster sync` en un nodo que no es de CCO, el archivo ns.log contiene entradas de registro duplicadas.

[CGOP-6794]

Equilibrio de carga

En una configuración de alta disponibilidad, es posible que las sesiones de suscriptor del nodo principal no se sincronicen con el nodo secundario. Este es un caso raro.

[NSLB-7679]

El formato serviceGroupName de la captura `entityofs` del grupo de servicios es el siguiente: `<service(group)name>?<ip/DBS>?<port>`

En el formato de captura, el grupo de servicios se identifica mediante una dirección IP o un nombre y puerto de DBS. El signo de interrogación (`?`) se utiliza como separador. Citrix ADC envía la captura

con el signo de interrogación (?). El formato aparece igual en la GUI de Citrix ADM. Este es el comportamiento esperado.

[NSHELP-28080]

Otros

Cuando se produce una sincronización forzada en una configuración de alta disponibilidad, el dispositivo ejecuta el comando `set urlfiltering parameter` en el nodo secundario.
Como resultado, el nodo secundario omite cualquier actualización programada hasta la siguiente hora programada mencionada en el parámetro `TimeOfDayToUpdateDB`.

[NSSWG-849]

Un dispositivo Citrix ADC puede reiniciarse debido al estancamiento de la CPU de administración si se produce un problema de conectividad con el proveedor externo de filtrado de URL.

[NSHELP-22409]

Redes

Tras una actualización de la versión 13.0 61.x del dispositivo Citrix ADC BLX a la versión 13.0 64.x, se pierde la configuración del archivo de configuración BLX. El archivo de configuración de BLX se restablece a los valores predeterminados.

[NSNET-17625]

Las siguientes operaciones de interfaz no son compatibles con las interfaces `X710 10G (i40e)` de Intel en un dispositivo Citrix ADC BLX con DPDK:

- Disable
- Enable
- Reset

[NSNET-16559]

En un host Linux basado en Debian (Ubuntu versión 18 y posteriores), un dispositivo Citrix ADC BLX siempre se implementa en modo compartido independientemente de la configuración del archivo de configuración BLX()`/etc/blx/blx.conf`. Este problema se produce porque `mawk`, que está presente de forma predeterminada en los sistemas Linux basados en Debian, no ejecuta algunos de los comandos awk presentes en el archivo `blx.conf`.

Solución temporal:

Instale `gawk` antes de instalar un dispositivo Citrix ADC BLX. Puede ejecutar el siguiente comando en la CLI del host de Linux para instalar `gawk`:

- apt-get install gawk

[NSNET-14603]

La instalación de un dispositivo Citrix ADC BLX podría fallar en un host Linux basado en Debian (versión 18 y posteriores de Ubuntu) con el siguiente error de dependencia:

```
The following packages have unmet dependencies: blx-core-libs:i386 :
PreDepends: libc6:i386 (>= 2.19)but it is not installable
```

Solución temporal:

Ejecute los siguientes comandos en la CLI del host Linux antes de instalar un dispositivo Citrix ADC BLX:

- dpkg — agregar arquitectura i386
- actualización apt-get
- apt-get dist-upgrade
- apt-get install libc6:i386

[NSNET-14602]

En algunos casos de conexiones de datos FTP, el dispositivo Citrix ADC solo realiza operaciones NAT y no procesamiento TCP en los paquetes para la negociación TCP MSS. Como resultado, la MTU de interfaz óptima no está configurada para la conexión. Esta configuración de MTU incorrecta provoca la fragmentación de los paquetes y afecta al rendimiento de la CPU.

[NSNET-5233]

En una configuración de alta disponibilidad, en el caso de que la versión de alta disponibilidad no coincida entre ambos nodos, las rutas dinámicas no se sincronizan con el nodo secundario. No se puede acceder al nodo secundario si su accesibilidad depende de las rutas dinámicas.

Como solución, las rutas dinámicas se sincronizan con el nodo secundario incluso en caso de que la versión de alta disponibilidad no coincida.

[NSHELP-28326]

Cuando se cambia un límite de memoria de la partición de administración en el dispositivo Citrix ADC, el límite de memoria intermedia TCP se establece automáticamente en el nuevo límite de memoria de la partición de administración.

[NSHELP-21082]

Plataforma

La conmutación por error de alta disponibilidad no funciona en las nubes de AWS y GCP. La CPU de administración puede alcanzar su capacidad del 100% en las nubes de AWS y GCP, y en Citrix ADC VPX en las instalaciones. Ambos problemas se producen cuando se cumplen las siguientes condiciones:

1. Durante el primer arranque del dispositivo Citrix ADC, no guarda la contraseña solicitada.

2. Posteriormente, reinicie el dispositivo Citrix ADC.

[NSPLAT-22013]

Cuando actualiza de compilaciones 13.0/12.1/11.1 a una versión 13.1 o baja de una compilación 13.1 a 13.0/12.1/11.1, algunos paquetes python no se instalan en los dispositivos Citrix ADC. Este problema se ha solucionado en las siguientes versiones de Citrix ADC:

- 13.1-4.x
- 13.0-82.31 y posteriores
- 12.1-62.21 y posteriores

Los paquetes python no se instalan cuando se degrada la versión de Citrix ADC de la versión 13.1-4.x a cualquiera de las siguientes versiones:

- Cualquier compilación 11.1
- 12.1-62.21 y anteriores
- 13.0-81.x y anteriores

[NSPLAT-21691]

El aprovisionamiento de una instancia VPX con la versión 12.0 XVA falla en un dispositivo Citrix ADC SDX que ejecuta la versión 13.1.

Solo se admiten las versiones 12.1 y posteriores de VPX. Actualice la versión VPX antes de actualizar el SBI a la versión 13.1.

[NSPLAT-21442]

En una configuración de clúster en un dispositivo Citrix ADC SDX, hay una discordancia de CLAG MAC en el segundo nodo y CLIP si se cumplen las siguientes condiciones:

- El CLAG se crea en una NIC Mellanox.
- Agrega otra instancia VPX al clúster y a la configuración de CLAG.

Como resultado, el tráfico a la instancia VPX se detiene.

[NSPLAT-21049]

En una configuración de clúster en un dispositivo Citrix ADC SDX, el primer nodo se cae debido a una discordancia de direcciones MAC en la tabla CLIP y MAC, si se cumplen las siguientes condiciones:

- El CLAG se crea en una NIC Mellanox.
- Quita el segundo nodo del clúster.

[NSPLAT-21042]

Al eliminar una configuración de escalabilidad automática o un conjunto de escalas de VM de un grupo de recursos de Azure, elimine la configuración del perfil de nube correspondiente de la instancia de Citrix ADC. Utilice el comando `rm cloudprofile` para borrar el perfil.

[NSPLAT-4520]

En una configuración de alta disponibilidad en Azure, al iniciar sesión en el nodo secundario a través de la GUI, aparece la pantalla de usuario por primera vez (FTU) para la configuración del perfil de nube de escalabilidad automática.
Solución alternativa: omita la pantalla e inicie sesión en el nodo principal para crear el perfil de nube. El perfil de la nube siempre debe configurarse en el nodo principal.

[NSPLAT-4451]

Directivas

Las conexiones pueden bloquearse si el tamaño de los datos de procesamiento es mayor que el tamaño de búfer TCP predeterminado configurado.Solución alternativa: establezca el tamaño del búfer TCP en el tamaño máximo de los datos que deben procesarse.

[NSPOLICY-1267]

SSL

En un clúster heterogéneo de dispositivos Citrix ADC SDX 22000 y Citrix ADC SDX 26000, se produce una pérdida de configuración de entidades SSL si se reinicia el dispositivo SDX 26000.

Solución temporal:

1. En el CLIP, inhabilite SSLv3 en todas las entidades SSL nuevas y existentes, como servidores virtuales, servicios, grupos de servicios y servicios internos. Por ejemplo, `set ssl vserver <name> -SSL3 DISABLED`.
2. Guarde la configuración.

[NSSSL-9572]

El comando Actualizar no está disponible para los siguientes comandos de adición:

- agregar aplicación azure
- add azure keyvault
- agregar ssl certkey con la opción hsmkey

[NSSSL-6484]

No se puede agregar un objeto de Azure Key Vault si ya se ha agregado un objeto de autenticación de Azure Key Vault.

[NSSSL-6478]

Puede crear varias entidades de la aplicación Azure con el mismo ID de cliente y secreto de cliente. El dispositivo Citrix ADC no devuelve ningún error.

[NSSSL-6213]

El siguiente mensaje de error incorrecto aparece al quitar una clave HSM sin especificar KEYVAULT como tipo HSM.
ERROR: Actualización de crl inhabilitada

[NSSSL-6106]

La actualización automática de claves de sesión aparece incorrectamente como inhabilitada en una dirección IP de clúster. (Esta opción no se puede desactivar).

[NSSSL-4427]

Aparece `Warning: No usable ciphers configured on the SSL vserver/service,,` un mensaje de advertencia incorrecto, si intenta cambiar el protocolo o el cifrado SSL en el perfil SSL.

[NSSSL-4001]

Un tíquet de sesión caducado se respeta en un nodo que no es de CCO y en un nodo de alta disponibilidad después de una conmutación por error de alta disponibilidad.

[NSSSL-3184]

Sistema

El valor MAX_CONCURRENT_STREAMS se establece en 100 de forma predeterminada si el dispositivo no recibe el marco de configuración max_concurrent_stream del cliente.

[NSHELP-21240]

Los contadores mptcp_cur_session_without_subflow disminuyen incorrectamente a un valor negativo en lugar de cero.

[NSHELP-10972]

Al procesar grandes flujos de tráfico de gRPC, la ventana anunciada por TCP aumenta exponencialmente, lo que lleva a un uso elevado de memoria.

[NSBASE-15447]

La IP del cliente y la IP del servidor se invierten en el registro SkipFlow de HDX Insight cuando el tipo de transporte LogStream se configura para Insight.

[NSBASE-8506]

Interfaz de usuario

Para la función Reescritura de MQTT, no puede eliminar una expresión mediante el Editor de expresiones en la GUI.

Solución temporal:

Use el comando de acción add o edit de tipo MQTT a través de la CLI.

[NSUI-18049]

En la GUI de Citrix ADC, el enlace `Help` presente debajo de la ficha `Dashboard` no funciona.

[NSUI-14752]

El asistente Crear/Supervisar CloudBridge Connector podría dejar de responder o no configurar un conector de cloudbridge.

Solución temporal:

Configure los conectores de cloudbridge agregando perfiles IPSec, túneles IP y reglas PBR mediante la GUI o la CLI de Citrix ADC.

[NSUI-13024]

Si crea una clave ECDSA mediante la interfaz gráfica de usuario, no se muestra el tipo de curva.

[NSUI-6838]

En una configuración de alta disponibilidad, las sesiones de usuario VPN se desconectan si se cumple la siguiente condición:

- Si se realizan dos o más operaciones de failover manual de alta disponibilidad sucesivas cuando la sincronización de alta disponibilidad está en curso.

Solución temporal:

Realice una conmutación por error manual de alta disponibilidad sucesiva solo después de que se haya completado la sincronización de alta disponibilidad (ambos nodos están en estado de sincronización correcta).

[NSHELP-25598]

Al cambiar una versión 13.0-71.x de un dispositivo Citrix ADC a una versión anterior, es posible que algunas API de Nitro no funcionen debido a los cambios en los permisos del archivo.

Solución temporal:

Cambie el permiso de `/nsconfig/ns.conf` a 644.

[NSCONFIG-4628]

Si usted (administrador del sistema) realiza todos los pasos siguientes en un dispositivo Citrix ADC, es posible que los usuarios del sistema no inicien sesión en el dispositivo Citrix ADC degradado.

1. Actualice el dispositivo Citrix ADC a una de las compilaciones:

- 13.0 52.24 compilación
- 12.1 57,18 compilación

- 11.1 65.10 compilación

1. Agregar un usuario del sistema o cambiar la contraseña de un usuario del sistema existente y guardar la configuración, y
2. Rebaja la versión del dispositivo Citrix ADC a cualquier versión anterior.

Para mostrar la lista de estos usuarios del sistema mediante la CLI:
En el símbolo del sistema, escriba:

```
query ns config -changedpassword [-config <full path of the configuration file (ns.conf)>]
```

Solución temporal:

Para solucionar este problema, utilice una de las siguientes opciones independientes:

- Si el dispositivo Citrix ADC aún no se ha rebajado (paso 3 de los pasos mencionados anteriormente), revierta la versión del dispositivo Citrix ADC con un archivo de configuración del que se ha creado previamente una copia de seguridad (ns.conf) de la misma compilación de la versión.
- Cualquier administrador del sistema cuya contraseña no se haya cambiado en la compilación actualizada puede iniciar sesión en la compilación degradada y actualizar las contraseñas de otros usuarios del sistema.
- Si ninguna de las opciones anteriores funciona, el administrador del sistema puede restablecer las contraseñas de usuario del sistema.

Para obtener más información, consulte https://docs.citrix.com/en-us/citrix-adc/13/system/ns-ag-aa-intro-wrapper-con/ns-ag-aa-reset-default-amin-pass-tsk.html

[NSCONFIG-3188]

Notas de la versión de Citrix ADC 13.1-9.60

June 22, 2022

Este documento de notas de la versión describe las mejoras y los cambios, los problemas resueltos y conocidos que existen para la versión 13.1 a 9.60 de Citrix ADC.

Notas

Este documento de notas de la versión no incluye correcciones relacionadas con la seguridad. Para obtener una lista de correcciones y avisos relacionados con la seguridad, consulte el boletín de seguridad de Citrix.

Novedades

Las mejoras y los cambios que están disponibles en las compilaciones 13.1-9.60.

Administración de bots

Compatibilidad con el protocolo IPv6 para la reputación de IP

La función de reputación de IP de Citrix Web App Firewall ahora admite el protocolo IPv6 para la configuración de directivas y la protección de seguridad mejorada contra direcciones IP incorrectas que envían solicitudes no deseadas.

Las siguientes categorías de amenazas son compatibles con el protocolo IPv6.

- Fuentes de spam
- Exploits de Windows
- Ataques web
- Botnets
- Escáneres
- Denegación de servicio
- Reputación
- Phishing
- Proxy
- Red
- Proveedores de nube
- Amenazas móviles
- Proxy Tor

[NSBOT-585]

Categorías de proveedores de servicios en la nube pública de Webroot para firmas de bots

La detección de bots de Citrix basada en la técnica de reputación de IP se ha mejorado para detectar si un cliente entrante es una dirección IP de nube pública. La función de reputación de IP debe habilitarse con la configuración de la función de administración de bots. El dispositivo Citrix ADC puede usar las categorías de proveedores de servicios de nube pública de Webroot para validar la dirección IP del cliente con la base de datos de direcciones IP del proveedor de servicios en la nube para la evaluación de directivas.

A continuación se presentan los tipos de nube pública que se pueden enlazar a un perfil de bot.

- AWS
- GCP
- Azure

- Oracle
- IBM
- Salesforce

[NSBOT-50]

Dispositivo Citrix ADC SDX

Compatibilidad para restaurar un dispositivo SDX con una licencia agrupada

Se agrega funcionalidad para restaurar un dispositivo Citrix ADC SDX que utiliza una licencia agrupada. La página de licencias también se ha mejorado. Ahora puede agregar y modificar licencias desde esa página.

Para obtener más información, consulte https://docs.citrix.com/en-us/sdx/current-release/configuring-management-service/backup-restore.html%23restore-the-appliance

[NSSVM-4750]

Los usuarios ahora pueden modificar los perfiles de administración, en un dispositivo Citrix ADC SDX, para aplicar las nuevas credenciales en las instancias de ADC.

Para obtener más información, consulte https://docs.citrix.com/en-us/sdx/current-release/provision-netscaler-instances.html%23update-an-admin-profile

[NSSVM-4409]

Los registros de la partición de fábrica ahora se incluyen en el paquete “techsupport” para capturar cualquier historial de restablecimiento de fábrica.

[NSSVM-2190]

Citrix Gateway

Análisis de la EPA en busca de direcciones MAC incluidas en la lista de permitidos

Puede configurar un análisis de EPA para direcciones MAC incluidas en la lista de permitidos sin tener que enumerar todas las direcciones IP en la expresión. En su lugar, puede usar conjuntos de patrones para esta configuración. Antes de la versión 13.1 de Citrix ADC, todas las direcciones MAC incluidas en la lista de permitidos debían especificarse como parte de una expresión de la EPA.

[CGOP-17928]

Citrix Web App Firewall

Compatibilidad con protección de seguridad adicional

Se agregan dos nuevos contadores de relajación para admitir las siguientes comprobaciones de seguridad adicionales. Los datos se utilizan para rastrear relajaciones obsoletas en la configuración.

- Protección por tipo de contenido
- Protección contra inyección JSON Cmd

[NSWAF-6950]

Redes

Nuevas licencias locales basadas en suscripciones y ancho de banda para los dispositivos Citrix ADC BLX

Las siguientes licencias locales basadas en suscripción basadas en ancho de banda ya están disponibles para los dispositivos Citrix ADC BLX.

- Suscripción a Citrix ADC VPX/BLX 10 Mbps Standard, Advanced, Premium Edition
- Suscripción a Citrix ADC VPX/BLX 100 Gbps Standard, Advanced, Premium Edition

Para obtener más información, consulte https://docs.citrix.com/en-us/citrix-adc-blx/current-release/licensing-blx.html

[NSNET-21527]

Compatibilidad con recopiladores de métricas en dispositivos Citrix ADX BLX

Los dispositivos Citrix ADX BLX ahora admiten la función de recopilador de métricas de Citrix ADC.

[NSNET-15095]

Plataforma

Compatibilidad con las configuraciones de Citrix ADC VPX en el primer arranque del dispositivo Citrix ADC en el hipervisor VMware ESX

Ahora puede aplicar las configuraciones de Citrix ADC VPX durante el primer arranque del dispositivo Citrix ADC en el hipervisor VMware ESX. De este modo, en ciertos casos, se pone en marcha una configuración específica o una instancia VPX en mucho menos tiempo.

Para obtener más información, consulte https://docs.citrix.com/en-us/citrix-adc/current-release/deploying-vpx/install-vpx-on-esx/apply-preboot-userdata-on-esx-vpx.html

[NSPLAT-21021]

Compatibilidad con la actualización 1d de VMware ESX 7.0 en la instancia de Citrix ADC VPX

La instancia de Citrix ADC VPX ahora admite la actualización 1d de VMware ESX versión 7.0 (compilación 17551050).

[NSPLAT-19667]

Directivas

Expresión de directiva para devolver la ruta URL con el sufijo eliminado

El Citrix ADC ahora admite una nueva expresión de directiva, `HTTP.REQ.URL.STRIP_SUFFIX` que devuelve la ruta URL con el sufijo eliminado.

Ejemplo:

URL: /testsite/file5.html

HTTP.REQ.URL.STRIP_SUFFIX devuelve el texto como `/testsite/file5`

[NSPOLICY-825]

Sistema

Compatibilidad con TCP multitrayecto versión 1

El dispositivo Citrix ADC ahora admite la versión 1 de TCP multiruta (MPTCP), además de la compatibilidad existente para la versión 0 de MPTCP. La compatibilidad con MPTCP versión 1 cumple con RFC 8684.

Para obtener más información, consulte https://docs.citrix.com/en-us/citrix-adc/current-release/system/tcp-configurations.html

[BASE 9237]

Compatibilidad con el monitor de estado gRPC

Un dispositivo Citrix ADC ahora admite un monitor de estado de gRPC para sondear el estado de gRPC del servidor. El monitor de estado de gRPC comprueba el estado general del servicio de gRPC o el estado de un servicio en particular.

El protocolo de comprobación de estado se implementa configurando los parámetros gRPC, gRPCHealthCheck, gRPCStatusCode y gRPCServiceName en la configuración del monitor HTTP2. Un cliente que implementa el protocolo consulta al servidor por su estado (correcto, no correcto, desconocido o servicio no implementado) y el servidor responde con un mensaje de estado.

[NSBASE-6455]

Interfaz de usuario

Licencias de entrada y salida de Citrix ADC BLX

Puede asignar licencias a los dispositivos Citrix ADC BLX a petición desde Citrix Application Delivery Management (ADM). El software ADM almacena y administra las licencias, que tienen un marco de licencias que proporciona un aprovisionamiento de licencias escalable y automatizado.

Un dispositivo Citrix ADC BLX puede extraer la licencia de Citrix ADM cuando se implementa un dispositivo Citrix ADC BLX. Cuando se quita o se destruye un dispositivo Citrix ADC BLX, el dispositivo vuelve a comprobar su licencia del software Citrix ADM.

Para obtener más información, consulte https://docs.citrix.com/en-us/citrix-adc-blx/current-release/licensing-blx.html

[NSCONFIG-5777]

Uso de herramientas de automatización NITRO

Citrix ADM service connect ahora captura el uso de herramientas de automatización como Ansible, Terraform o NITRO SDK.

[NSCONFIG-4515]

Problemas resueltos

Los problemas que se abordan en la compilación 13.1-9.60.

Autenticación, autorización y auditoría

Un dispositivo Citrix ADC puede bloquearse si se cumplen las siguientes condiciones.

1. El dispositivo está bajo presión de memoria.
2. El registro de auditoría está habilitado y se establece como nivel INFO.
3. La autenticación del usuario está en curso.

[NSHELP-29053]

Si se configura un dispositivo Citrix ADC para el atributo de cookie `SameSite` y el atributo de dominio para la autenticación, la autenticación falla. Esto ocurre porque el valor del atributo de cookie `SameSite` y el atributo de dominio no están separados por punto y coma.

[NSHELP-28971]

Un dispositivo Citrix ADC puede bloquearse si se cumplen las siguientes condiciones.

1. El dispositivo está bajo presión de memoria.

2. SAML se configura como uno de los métodos de autenticación.

[NSHELP-28855]

Se devuelve una URL de cierre de sesión (`/cgi/tmlogout`) incorrecta cuando un servidor virtual VPN se configura como SP SAML. El problema ocurre porque se genera una URL de cierre de sesión incorrecta en los metadatos SAML.

[NSHELP-28726]

En algunos casos, en un entorno multinúcleo, un explorador cliente no puede acceder a los recursos detrás de un servidor virtual de autenticación, autorización y auditing-TM.

[NSHELP-28474]

En una configuración de alta disponibilidad de Citrix ADC, se muestran algunos comandos de autenticación durante la configuración de la CLI como resultado de un problema de sincronización.

[NSHELP-28448]

Si el SSO de formulario está habilitado, el dispositivo Citrix ADC responde a una solicitud de credenciales del servidor back-end agregando un formulario junto con el encabezado de tipo de contenido. Esta adición conduce a encabezados duplicados si ya hay uno presente.

[NSHELP-28405]

El dispositivo Citrix ADC arroja un error de validación del servidor si se utiliza el esquema de inicio de sesión `DualAuthOrPush.xml`.

[NSHELP-28063]

`SameSite` los atributos de cookie no se agregan a las cookies de autenticación si un dispositivo Citrix ADC está configurado para la autenticación basada en 401.

[NSHELP-27764]

En algunos casos, se muestra un mensaje de error `invalid credentials` durante el proceso de autenticación RADIUS. El error aparece cuando se accede al dispositivo Citrix ADC desde un dispositivo cliente mediante el explorador Google Chrome.

[NSHELP-27113]

El dispositivo Citrix ADC puede bloquearse durante la extracción de grupos de Active Directory si el nombre completo de un grupo extraído es NULL.

[NSHELP-26899]

Se rellena un nombre de dominio SSO incorrecto para el usuario que inició sesión si se usa Autenticación, autorización y auditoría.USUARIO.DOMINIO en la expresión.

[NSHELP-26443]

En algunos casos, se observa una fuga de NSB en un dispositivo Citrix ADC cuando la funcionalidad de SSO se usa con un servidor proxy.

[NSHELP-25492]

Almacenamiento en caché

Se envía una información de encabezado adicional en la respuesta de la memoria caché si el parámetro `insertAge` está habilitado en el comando `set cache contentGroup`.

[NSHELP-27772]

Un dispositivo Citrix ADC puede bloquearse si los valores de los parámetros `Max_age` y `s_maxage` no se establecen dinámicos en el bloque de control de la memoria caché.

[NSHELP-27758]

Un dispositivo Citrix ADC puede bloquearse si se cumplen las siguientes condiciones:

- El dispositivo sirve contenido desde su caché integrada.
- El contenido en caché se vuelve a validar.
- La nueva solicitud llega a ADC desde diferentes clientes para el mismo objeto almacenado en caché.

[NSHELP-22596]

Dispositivo Citrix ADC SDX

En un dispositivo Citrix ADC SDX, el sistema no está bajo gracia, la alarma se genera continuamente en lugar de solo una vez cuando la licencia SDX no está bajo el período de gracia.

[NSHELP-28740]

Management Service en un dispositivo Citrix ADC SDX muestra la velocidad de la interfaz para los administradores SNMP en Kbps/Mbps en lugar de bits por segundo.

[NSHELP-28724]

Las cadenas de comunidad de los destinos de capturas SNMP v2 se enmascaran en un dispositivo Citrix ADC SDX.

[NSHELP-28625]

En un dispositivo Citrix ADC SDX, puede modificar el rendimiento de una instancia VPX incluso después del período de gracia de la licencia agrupada (30 días).

[NSHELP-28553]

Debido a una actualización en la versión de Python, la carga del SDK de Python del servicio de administración puede fallar debido a errores de sintaxis.

[NSHELP-27897]

En un dispositivo Citrix ADC SDX, el valor predeterminado para activar la alarma en `Hypervisor Disk Usage High` se incrementa al 98%.

[NSHELP-27854]

En un dispositivo Citrix ADC SDX, se muestra una interfaz que forma parte de un canal de administración junto con el canal de administración si se cumple esta secuencia de condiciones:

1. La instancia VPX forma parte de un clúster.
2. Se crea el canal de gestión.

[NSHELP-27487]

Citrix Gateway

Los bits de licencia SSL VPN no están configurados para VPX en GCP Marketplace. Como resultado, los suscriptores de Marketplace no pueden usar SSL VPN en GCP.

[NSHELP-29107]

Un dispositivo Citrix ADC puede bloquearse mientras procesa el tráfico UDP.

[NSHELP-28802]

El dispositivo Citrix ADC puede bloquearse durante el inicio de sesión de la VPN si una directiva de AppFlow con la regla HTTP está enlazada a Citrix Gateway.

[NSHELP-28705]

Es posible que la página de inicio de sesión de Citrix Gateway no se cargue para los usuarios de 3G/con anclaje a red.

[NSHELP-28367]

En raras ocasiones, el dispositivo Citrix Gateway podría bloquearse durante el inicio de sesión de transferencia cuando se accede a una sesión liberada.

[NSHELP-28022]

El dispositivo Citrix ADC se bloquea al procesar el tráfico de carga útil de seguridad encapsulante (ESP) entrante y no se encuentra la asociación de seguridad (SA).

[NSHELP-27991]

Es posible que observe problemas con el inicio de sesión de transferencia si SAML se configura como el último factor en la autenticación nFactor y también se configura el EPA clásico.

[NSHELP-27983]

El dispositivo Citrix ADC puede bloquearse si se cumplen las dos condiciones siguientes.

- El dispositivo se implementa para el modo proxy ICA.
- La función Gateway Insight para el flujo de ICA está habilitada.

[NSHELP-27982]

En casos excepcionales, la página del portal de Citrix Gateway no muestra el botón **Descargar** para el complemento EPA en el explorador Internet Explorer.

[NSHELP-27849]

El dispositivo Citrix Gateway puede bloquearse si se bloquea la sincronización y se modifica la configuración de la directiva de conmutación de contenido.

[NSHELP-27570]

Un dispositivo Citrix ADC puede bloquearse mientras procesa el tráfico UDP.

[NSHELP-27536]

El archivo de marcadores personales de los usuarios no se puede copiar de un dispositivo Citrix Gateway a otro dispositivo.

[NSHELP-27389]

El dispositivo Citrix Gateway puede bloquearse si se establece una opción de cliente VPN desconocida en la directiva de sesión.

[NSHELP-27380]

En ocasiones, el dispositivo Citrix Gateway puede bloquearse al acceder a una ubicación de memoria no válida.

[NSHELP-27343]

El dispositivo Citrix Gateway se reinicia de forma inesperada debido a la inundación de mensajes de registro SSL VPN en el archivo local ns.log cuando se habilita Gateway Insight.

[NSHELP-27040]

La localización del portal de Citrix Gateway no es compatible con el explorador Internet Explorer.

[NSHELP-26822]

La GUI de Citrix Gateway muestra el mensaje `Invalid IP or Port` al modificar un perfil de sesión de VPN.

[NSHELP-26722]

La salida de `show audit messages` no muestra los registros más recientes si modifica el servidor syslog en los parámetros syslog globales.

[NSHELP-19430]

Citrix Web App Firewall

El motor de aprendizaje de Citrix Web App Firewall aprende las reglas de formato de campo solo cuando se observa una infracción.

[NSWAF-7677]

Un dispositivo Citrix ADC puede bloquearse si se cumplen las siguientes condiciones:

- El proxy de cookie de Web App Firewall está habilitado.
- La cookie de sesión y la cookie persistente tienen el mismo nombre.

[NSHELP-28181]

Equilibrio de carga

Si los valores de los parámetros de los comandos relacionados con el monitor de usuario y el monitor integrado tienen un espacio entre el texto, el valor del parámetro se corta y el texto que sigue al espacio se ignora.

Ejemplo:

```
add lb monitor ftp_user USER -scriptName nsftp.pl -scriptArgs `file=
    test.txt;username=NS user;password=test123` -dispatcherIP 127.0.0.1
    -dispatcherPort 3013`
<!--NeedCopy-->
```

En este ejemplo, el nombre de usuario se establece como `NS user` pero solo `NS` se envía y el texto posterior se corta debido al espacio.

[NSLB-8915]

Los sitios VPX principal y secundario se bloquearon tras configurar el grupo de servicios GSLB con Autoscale habilitado.

[NSHELP-28530]

Un dispositivo Citrix ADC en una configuración de alta disponibilidad pierde conectividad porque la memoria NSB no se libera después de enviar la respuesta HTTP durante la supervisión de la sonda HTTP.

[NSHELP-28466]

A veces, en un sistema con varios PE, los grupos basados en el dominio no se recuperan al estado UP después de algunos errores en el sistema. Este problema se debe a una condición de carrera entre la CLI y los monitores internos.

[NSHELP-27965]

En algunos casos, un dispositivo Citrix ADC puede bloquearse cuando se emite el comando show running configuration.

[NSHELP-27815]

En una configuración de clúster, cuando uno o más nodos pasan al estado `DOWN`, es posible que el nodo de seguridad no pueda unirse al grupo de nodos del clúster. Este error provoca que algunas funciones de Citrix ADC fallen.

[NSHELP-27664]

Es posible que un dispositivo Citrix ADC no inserte un identificador de paquete adecuado en las respuestas, cuando se reciben solicitudes RADIUS procesadas. Debido a este problema, el cliente recibe una respuesta no válida.

[NSHELP-27391]

La configuración de GSLB podría perderse parcialmente si se cumplen las siguientes condiciones:

- Se reinicia el dispositivo Citrix ADC.
- El servicio ADNS está configurado con la misma dirección IP que el sitio GSLB remoto.

[NSHELP-26816]

Cuando se configura una gran cantidad de servicios GSLB en varios sitios GSLB que tienen una latencia de red alta, es posible que el estado de los servicios GSLB no se actualice en el sitio GSLB remoto.

[NSHELP-23799]

Otros

El comando `add URLF categorization` no actualiza la base de datos, lo que provoca un error interno.

[NSSWG-1315]

El dispositivo Citrix ADC puede bloquearse tras reanudar el procesamiento si se cumplen las siguientes condiciones:

- Se utiliza la función de proxy de reenvío SSL.
- La información de protocolo para una solicitud de proxy de reenvío SSL se recibe en múltiples paquetes asíncronos. El dispositivo detiene el procesamiento de paquetes y lo reanuda después de recibir todos los detalles del protocolo para la solicitud.

[NSHELP-28447]

Cuando un dispositivo en línea envía un mensaje personalizado seguido de un restablecimiento, el dispositivo Citrix ADC restablece la conexión antes de reenviar la respuesta del dispositivo en línea al cliente.

[NSHELP-27676]

Redes

La instancia de Citrix ADC VPX puede bloquearse si se cumplen las siguientes condiciones:

- Hay un número elevado de conexiones de datos FTP.
- Se produce una conmutación por error en el dispositivo Citrix ADC.
- Se borra una conexión NATPCB del lado del cliente o del servidor.

[NSHELP-27816]

En una configuración de alta disponibilidad, la dirección SNIP habilitada para enrutamiento dinámico no se expone a VTYSH al reiniciar si se cumple la siguiente condición:

- Una dirección SNIP habilitada para enrutamiento dinámico está enlazada a la VLAN compartida en una partición no predeterminada.

Como parte de la solución, el dispositivo Citrix ADC ahora no permite vincular una dirección SNIP habilitada para enrutamiento dinámico a la VLAN compartida en una partición no predeterminada

[NSHELP-24000]

Plataforma

La instancia de Citrix ADC VPX en la nube de AWS se bloquea durante el reinicio en caliente del dispositivo Citrix ADC.

[NSPLAT-21979]

Una instancia de Citrix ADC VPX con la versión de software 13.1 compilación 4.43 no admite la familia de instancias C5n en la nube de AWS.

[NSPLAT-21451]

En la instancia de Citrix ADC VPX en la nube de Azure y en el servidor Microsoft Hyper-V, en ciertas situaciones, pueden producirse caídas de paquetes de congestión en el lado de transmisión de la interfaz virtual de Hyper-V. Estas caídas de paquetes pueden detener las transmisiones del dispositivo Citrix ADC.

[NSHELP-28375]

En las plataformas Citrix ADC MPX 5900 y MPX 8900, aparece un número de plataforma incorrecto en la pantalla LCD.

[NSHELP-28207]

El estado de la plataforma SDX aparece como DESCONOCIDO en la consola LOM. Esto es solo un problema de visualización y no tiene ningún impacto funcional.

[NSHELP-20009]

Directivas

Un Citrix ADC puede bloquearse si el tipo de servicio FIX se usa en el modo Capa 2 y Capa 3.

[NSHELP-28468]

Un dispositivo Citrix ADC puede bloquearse si la expresión MATCHES() se usa en el protocolo no basado en TCP.

[NSHELP-26062]

SSL

La adición de un par de claves de certificado puede fallar debido a un error en la asignación de memoria. Como resultado, la búsqueda del par de claves de certificado de CA falla y el dispositivo se bloquea.

[NSHELP-28197]

La renegociación del protocolo de manos SSL puede fallar en las plataformas Citrix ADC MPX, si se configuran directivas asíncronas en el servidor virtual SSL.

[NSHELP-27870]

El dispositivo Citrix ADC no acepta una respuesta de OCSP si no tiene el encabezado HTTP de longitud de contenido.

[NSHELP-27039]

El nombre del certificado de CA que emitió la CRL se corta en 32 caracteres, aunque el nombre de la clave de certificado puede tener hasta 64 caracteres. Este problema se produce porque el campo CRL tiene un límite de 32 caracteres.

[NSHELP-26986]

En un dispositivo FIPS Citrix ADC MPX/SDX 14000, es posible que vea pérdidas de memoria al usar la configuración de EDT con un tamaño de datagrama EDT > 1 K.

[NSHELP-25375]

Sistema

Cuando se registra una instancia de Citrix ADC en Citrix ADM, los errores de asignación de puertos se ven en los contadores ADC.

[NSHELP-28779]

Después de actualizar a Citrix ADC versión 13.0, compilación 64-x, y posteriores, se reciben demasiados registros de advertencias con un mensaje `Unexpected data received from the server on probe connection for SSL_BRIDGE service type - Server..`

[NSHELP-28656]

Un dispositivo Citrix ADC con la versión 13.0, compilación 82.x, y posteriores podría bloquearse si `ns mode pmtud` está habilitado y se usan particiones.

[NSHELP-28068]

Si el tamaño del encabezado recibido es mayor que el tamaño máximo de la tabla de encabezados, el dispositivo restablece el tamaño de la tabla como cero. Como resultado, las solicitudes HTTP2 fallan después de algunas solicitudes.

[NSHELP-27977]

El puntero del recopilador de AppFlow al que hace referencia el perfil de análisis está dañado.

[NSHELP-27924]

Si ADM tiene transacciones pendientes en la cola, informa aleatoriamente de una alerta crítica para el uso elevado de memoria.

[NSHELP-27913]

El tiempo de espera zombie TCP vacía las conexiones activas del servidor o del cliente debido al tiempo de espera de medio cierre en el lado más rápido de la conexión.

[NSHELP-27502]

La opción TCP de encadenamiento de conexiones se agrega a las conexiones RPC de Citrix ADC. El problema provoca un problema de interoperabilidad con la comunicación de los sitios GSLB.

[NSHELP-27417]

El aumento de las retransmisiones de paquetes se observa en las implementaciones de clúster MPTCP en la nube pública si el conjunto de enlaces está inhabilitado.

[NSHELP-27410]

Un dispositivo Citrix ADC podría enviar un paquete TCP no válido junto con opciones TCP como bloques SACK, marca de tiempo y ACK de datos MPTCP en conexiones MPTCP.

[NSHELP-27179]

El cliente NSWL ocasionalmente registra datos varias veces desde el motor de paquetes (PE-0), mientras que se omiten los registros de otros motores de paquetes.

[NSHELP-27138]

Un dispositivo Citrix ADC puede bloquearse si se cumplen las siguientes condiciones:

- Al gestionar los registros de metadatos de Logstream.
- La función AppFlow está habilitada.

[NSHELP-26942]

Se observa una discrepancia en los registros de Logstream en el dispositivo Citrix ADC y el cargador de datos.

[NSHELP-25796]

Interfaz de usuario

Para un servidor virtual, al modificar cualquier parámetro en **Configuración de tráfico** en la GUI de Citrix ADC (versión 13.1 compilación 4.43), aparece el siguiente mensaje de error:

`Invalid argument [pq]`

[NSHELP-29492]

Se observa el siguiente problema si se realiza alguna operación que lee el archivo `ns.conf`. Por ejemplo, `show ns saved config`.

- El proceso HTTPD puede congelarse y provocar que la GUI y la API de NITRO se vuelvan inaccesibles.

[NSHELP-28249]

Cuando anula la selección de la opción segura para un nodo RPC en la GUI de ADC, aparece el siguiente mensaje de error:

Falta el requisito previo del argumento [validateCert, segure==Yes]

[NSHELP-28239]

En una configuración de clúster, las entidades únicas o globales con dos o más contraseñas pueden fallar en un nodo durante un proceso de sincronización de configuración por el siguiente motivo:

- Si se omite la primera contraseña de la secuencia, el descifrado de contraseña posterior falla en el nodo de sincronización. El descifrado falla porque busca la clave local de CCO, que no está presente en el nodo de sincronización.

[NSHELP-28035]

Después de actualizar una configuración de alta disponibilidad o una configuración de clúster a la versión 13.0 compilación 74.14 o posterior, la sincronización de la configuración podría fallar por la siguiente razón:

- Tanto las claves `ssh_host_rsa_key` privadas como las públicas son un par incorrecto.

[NSHELP-27834]

En una configuración de alta disponibilidad, un dispositivo Citrix ADC puede bloquearse durante un proceso de autenticación de usuario del sistema si se cumple la siguiente condición:

- El cálculo del hash de la contraseña tarda más en perder cinco latidos del corazón.

[NSHELP-27066]

Los detalles de las estadísticas del servidor de equilibrio de carga están desalineados en el panel de la GUI de Citrix ADC.

[NSHELP-20752]

Al desvincular la URL que limita la velocidad de un perfil de bot, se produce un error interno en la base de datos.

[NSCONFIG-6231]

El dispositivo Citrix ADC devuelve `Zero` de forma incorrecta algunos de los parámetros GSLB y estadísticas en las llamadas a la API NITRO.

[NSCONFIG-6104]

Un dispositivo Citrix ADC habilitado en el modo de color de la CLI muestra los mensajes de texto de éxito de la CLI en color blanco en lugar de mostrarlos en color verde.

[NSCONFIG-5689]

Si un dispositivo Citrix ADC BLX tiene licencia mediante Citrix ADM, es posible que se produzca un error en las licencias tras actualizar el dispositivo a la versión 13.0 compilación 83.x.

[NSCONFIG-4834]

Optimización de vídeo

Es posible que un dispositivo Citrix ADC se bloquee debido a un error en la asignación de memoria con la función de optimización de vídeo habilitada.

[NSHELP-28752]

Problemas conocidos

Los problemas que existen en la versión 13.1-9.60.

AppFlow

HDX Insight no informa de un error de inicio de aplicación causado por un usuario que intenta iniciar una aplicación o un escritorio a los que el usuario no tiene acceso.

[NSINSIGHT-943]

Autenticación, autorización y auditoría

En casos excepcionales, el dispositivo Citrix ADC puede bloquearse debido a una posición de registro incorrecta.

[NSHELP-29267]

La expresión Authentication, authorization and auditing.user.attribute puede dar un valor vacío en un dispositivo Citrix ADC de varios núcleos cuando la contraseña del usuario se cambia al expirar.

[NSHELP-28419]

En algunos casos, se observa una pérdida de memoria en un dispositivo Citrix ADC si la funcionalidad SSO se usa con un servidor proxy.

[NSHELP-27744]

El dispositivo Citrix ADC se bloquea si se cumplen las dos condiciones siguientes.

- La OTP de correo electrónico está configurada
- El servidor de correo electrónico no responde o hay un problema de red con el servidor de correo electrónico

[NSHELP-26137]

Un dispositivo Citrix ADC no autentica los intentos de inicio de sesión con contraseñas duplicadas y evita los bloqueos de cuentas.

[NSHELP-563]

LoginSchema de DualAuthPushOrOTP.xml no aparece correctamente en la pantalla del editor de esquemas de inicio de sesión de la GUI de Citrix ADC.

[NSAUTH-6106]

El perfil proxy ADFS se puede configurar en una implementación de clúster. El estado de un perfil proxy se muestra incorrectamente en blanco al ejecutar el siguiente comando.
`show adfsproxyprofile <profile name>`

Solución temporal:

Conéctese al Citrix ADC activo principal del clúster y ejecute el comando `show adfsproxyprofile <profile name>`. Mostraría el estado del perfil de proxy.

[NSAUTH-5916]

La página Configurar servidor LDAP de autenticación de la GUI de Citrix ADC deja de responder si sigue los pasos siguientes:

- Se abre la opción Probar accesibilidad LDAP.
- Las credenciales de inicio de sesión no válidas se rellenan y envían.
- Las credenciales de inicio de sesión válidas se rellenan y envían.

Solución temporal:

Cierre y abra la opción Probar accesibilidad de LDAP.

[NSAUTH-2147]

Almacenamiento en caché

Es posible que un dispositivo Citrix ADC se bloquee si la función Almacenamiento en caché integrado está habilitada y el dispositivo tiene poca memoria.

[NSHELP-22942]

Call Home

El registro de Call Home puede fallar para los dispositivos Citrix ADC MPX que utilizan licencias agrupadas. El registro falla porque Call Home utiliza un número de serie incorrecto para registrar los dispositivos en el servidor de asistencia de Citrix.

[NSHELP-28667]

Dispositivo Citrix ADC SDX

En un dispositivo Citrix ADC SDX, si el CLAG se crea en una NIC Mellanox, la MAC de CLAG cambia cuando se reinicia la instancia VPX. El tráfico a la instancia VPX se detiene tras el reinicio porque la tabla MAC tiene la antigua entrada MAC de CLAG.

[NSSVM-4333]

En un dispositivo Citrix ADC SDX, Management Service no envía notificaciones de syslog o correo electrónico si las fallas de la fuente de alimentación, el voltaje o el disco se producen más de una vez.

[NSHELP-29443]

En un dispositivo Citrix ADC SDX, las instancias de ADC no alcanzan su capacidad máxima al configurar el modo de asignación de rendimiento en ráfagas.

[NSHELP-27477]

Las caídas de paquetes se observan en una instancia VPX alojada en un dispositivo Citrix ADC SDX si se cumplen las siguientes condiciones:

- El modo de asignación de rendimiento está en ráfaga.
- Existe una gran diferencia entre el rendimiento y la capacidad máxima de ráfaga.

[NSHELP-21992]

Citrix Gateway

Cuando el túnel dividido se establece en la resolución `Reverse`, DNS para los dominios de intranet falla.

[NSHELP-29371]

En una configuración de alta disponibilidad con configuración TCP SYSLOG, un nodo puede bloquearse durante la conmutación por error de alta disponibilidad o durante la operación de configuración clara.

[NSHELP-29251]

En la página del portal de Citrix Gateway, el icono del **enlace de proxy RDP** no cambia con el tema del portal de RfWebUI.

[NSHELP-28974]

En algunos casos, el código de validación del servidor falla cuando se confía en el certificado del servidor. Como resultado, los usuarios finales no pueden acceder a la puerta de enlace.

[NSHELP-28942]

A veces, después de desconectar la VPN, el solucionador de DNS no resuelve los nombres de host porque los sufijos DNS se eliminan durante la desconexión de la VPN.

[NSHELP-28848]

Después de actualizar el dispositivo Citrix Gateway a la versión 13.0, la configuración de proxy en un perfil de sesión no funciona según lo previsto. La conexión de proxy se omite para el proxy NS no HTTP configurado.

Ejemplo:

```
add vpn sessionAction-proxy NS -httpProxy 192.0.2.0:24 -sslProxy 192.0.2.0:24
```

En este ejemplo, -httpProxy funciona según lo previsto, pero -sslProxy no funciona.

[NSHELP-28640]

La autenticación de certificados de cliente falla para Citrix SSO para macOS si no hay certificados de cliente en el llavero de macOS.

[NSHELP-28551]

A veces, se desactiva la sesión de un usuario en Citrix Gateway en unos segundos cuando se establece el tiempo de espera por inactividad del cliente.

[NSHELP-28404]

Es posible que el complemento de Windows se bloquee durante la autenticación.

[NSHELP-28394]

El acceso a StoreFront a través de un servidor virtual VPN falla si se accede a StoreFront a través de un servidor virtual de equilibrio de carga de respaldo.

[NSHELP-27852]

El dispositivo Citrix Gateway puede bloquearse al volver a conectarse a una sesión ICA existente.

[NSHELP-27441]

No se puede desvincular una directiva de autorización clásica mediante la interfaz gráfica de usuario. Sin embargo, puede usar la CLI para desvincular la directiva Autenticación, autorización y autorización de auditoría.

Con esta corrección, ahora puede desvincular la directiva de autorización mediante la interfaz gráfica de usuario.

[NSHELP-27064]

El dispositivo Citrix ADC se bloquea si se produce alguna de las siguientes condiciones:

- La acción syslog se configura con el nombre de dominio y usted borra la configuración mediante la GUI o la CLI.
- La sincronización de alta disponibilidad se produce en el nodo secundario.

Solución temporal:

Cree una acción syslog con la dirección IP del servidor syslog en lugar del nombre de dominio del servidor syslog.

[NSHELP-25944]

En una configuración de alta disponibilidad, las sesiones de usuario VPN se desconectan si se cumple la siguiente condición:

- Si se realizan dos o más operaciones de failover manual de alta disponibilidad sucesivas cuando la sincronización de alta disponibilidad está en curso.

Solución temporal:

Realice una conmutación por error manual de alta disponibilidad sucesiva solo después de que se haya completado la sincronización de alta disponibilidad (ambos nodos están en estado de sincronización correcta).

[NSHELP-25598]

El complemento EPA para Windows no utiliza el proxy configurado del equipo local y se conecta directamente al servidor de puerta de enlace.

[NSHELP-24848]

Gateway Insight no muestra información precisa sobre los usuarios de VPN.

[NSHELP-23937]

El complemento VPN no establece un túnel después del inicio de sesión de Windows si se cumplen las siguientes condiciones:

- El dispositivo Citrix Gateway está configurado para la función Always On
- El dispositivo está configurado para la autenticación basada en certificados con autenticación de dos factores `off`

[NSHELP-23584]

A veces, al navegar por los esquemas, aparece el mensaje de error `Cannot read property 'type 'of undefined`.

[NSHELP-21897]

Si quiere utilizar la funcionalidad Always On VPN antes de iniciar sesión en Windows, se recomienda actualizar a Citrix Gateway 13.0 o posterior. Esto le permite aplicar las mejoras adicionales introducidas en la versión 13.0 que no están disponibles en la versión 12.1.

[CGOP-19355]

El error de inicio de la aplicación debido a un tíquet de STA no válido no se informa en Gateway Insight.

[CGOP-13621]

El informe Gateway Insight muestra incorrectamente el valor `Local` en lugar de `SAML` en el campo Tipo de autenticación para los errores de SAML.

[CGOP-13584]

En una configuración de alta disponibilidad, durante la conmutación por error de Citrix ADC, el recuento de SR aumenta en lugar del recuento de conmutación por error en Citrix ADM.

[CGOP-13511]

Al aceptar conexiones de host local desde el explorador web, el cuadro de diálogo **Aceptar conexión** para macOS muestra el contenido en inglés independientemente del idioma seleccionado.

[CGOP-13050]

El texto `Home Page` de la **aplicación Citrix SSO > Página de inicio** se corta para algunos idiomas.

[CGOP-13049]

Aparece un mensaje de error al agregar o modificar una directiva de sesión desde la GUI de Citrix ADC.

[CGOP-11830]

En Outlook Web App (OWA) 2013, al hacer clic en **Opciones** en el menú **Configuración**, se muestra un cuadro de diálogo **Error crítico**. Además, la página deja de responder.

[CGOP-7269]

En una implementación de clúster, si ejecuta un comando `force cluster sync` en un nodo que no es de CCO, el archivo ns.log contiene entradas de registro duplicadas.

[CGOP-6794]

Citrix Web App Firewall

La URL de publicación de huella digital del dispositivo bot puede fallar si la directiva de administración de bots está habilitada en un servidor virtual de equilibrio de carga de tipo SSL.

[NSHELP-29198]

Un dispositivo Citrix ADC podría bloquearse si se habilitan los siguientes módulos:

- Web App Firewall con comprobaciones de seguridad avanzadas.
- Appqoe.

[NSHELP-28251]

Equilibrio de carga

En una configuración de alta disponibilidad, es posible que las sesiones de suscriptor del nodo principal no se sincronicen con el nodo secundario. Este es un caso raro.

[NSLB-7679]

La sincronización incremental falla para los comandos `add dns action` y `add location` con expresiones de directiva que contienen caracteres comodín.

[NSHELP-29301]

El estado del grupo de servicios que se muestra en los comandos show y stat es incoherente.

[NSHELP-28931]

Si hay un registro DNS de tipo ZONE disponible para el dominio principal, la consulta del dominio secundario con un registro NS existente da como resultado un registro SOA del dominio principal en lugar del registro NS del dominio secundario.

[NSHELP-28793]

El formato serviceGroupName de la captura `entityofs` del grupo de servicios es el siguiente: `<service(group)name>?<ip/DBS>?<port>`

En el formato de captura, el grupo de servicios se identifica mediante una dirección IP o un nombre y puerto de DBS. El signo de interrogación (?) se utiliza como separador. Citrix ADC envía la captura con el signo de interrogación (?). El formato aparece igual en la GUI de Citrix ADM. Este es el comportamiento esperado.

[NSHELP-28080]

Otros

Cuando se produce una sincronización forzada en una configuración de alta disponibilidad, el dispositivo ejecuta el comando `set urlfiltering parameter` en el nodo secundario.
Como resultado, el nodo secundario omite cualquier actualización programada hasta la siguiente hora programada mencionada en el parámetro `TimeOfDayToUpdateDB`.

[NSSWG-849]

La instancia CPX de Citrix ADC, que se ejecuta en un sistema Linux con arquitectura de 64 bits y 1 TB de almacenamiento de archivos, puede cargar archivos de certificados y claves ahora.

[NSHELP-28986]

Un dispositivo Citrix ADC puede reiniciarse debido al estancamiento de la CPU de administración si se produce un problema de conectividad con el proveedor externo de filtrado de URL.

[NSHELP-22409]

Redes

Un dispositivo Citrix ADC puede bloquearse si se cumplen todas las condiciones siguientes:

- Se configura una ruta de equilibrio de carga en un dominio de tráfico del dispositivo.
- Se realiza una operación de configuración clara en el dispositivo.

[NSNET-23847]

Tras una actualización de la versión 13.0 61.x del dispositivo Citrix ADC BLX a la versión 13.0 64.x, se pierde la configuración del archivo de configuración BLX. El archivo de configuración de BLX se restablece a los valores predeterminados.

[NSNET-17625]

Las siguientes operaciones de interfaz no son compatibles con las interfaces `X710 10G (i40e)` de Intel en un dispositivo Citrix ADC BLX con DPDK:

- Disable
- Enable
- Reset

[NSNET-16559]

En un host Linux basado en Debian (Ubuntu versión 18 y posteriores), un dispositivo Citrix ADC BLX siempre se implementa en modo compartido independientemente de la configuración del archivo de configuración BLX()`/etc/blx/blx.conf`. Este problema se produce porque `mawk`, que está presente de forma predeterminada en los sistemas Linux basados en Debian, no ejecuta algunos de los comandos `awk` presentes en el archivo `blx.conf`.

Solución temporal:

Instale gawk antes de instalar un dispositivo Citrix ADC BLX. Puede ejecutar el siguiente comando en la CLI del host de Linux para instalar gawk:

- apt-get install gawk

[NSNET-14603]

La instalación de un dispositivo Citrix ADC BLX podría fallar en un host Linux basado en Debian (versión 18 y posteriores de Ubuntu) con el siguiente error de dependencia:

```
The following packages have unmet dependencies: blx-core-libs:i386 :
PreDepends: libc6:i386 (>= 2.19)but it is not installable
```

Solución temporal:

Ejecute los siguientes comandos en la CLI del host Linux antes de instalar un dispositivo Citrix ADC BLX:

- dpkg --add-architecture i386
- apt-get update
- apt-get dist-upgrade
- apt-get install libc6:i386

[NSNET-14602]

En algunos casos de conexiones de datos FTP, el dispositivo Citrix ADC solo realiza operaciones NAT y no procesamiento TCP en los paquetes para la negociación TCP MSS. Como resultado, la MTU de interfaz óptima no está configurada para la conexión. Esta configuración de MTU incorrecta provoca la fragmentación de los paquetes y afecta al rendimiento de la CPU.

[NSNET-5233]

En una configuración NAT44 a gran escala, el dispositivo Citrix ADC puede bloquearse mientras recibe tráfico SIP por el siguiente motivo:

- El módulo LSN no encuentra el servicio mientras disminuye el recuento de referencias o elimina el servicio.

[NSHELP-29134]

Cuando se cambia el límite de memoria de una partición de administración en el dispositivo Citrix ADC, el límite de memoria de almacenamiento en búfer TCP se establece automáticamente en el nuevo límite de memoria de la partición de administración.

[NSHELP-21082]

Plataforma

La conmutación por error de alta disponibilidad no funciona en las nubes de AWS y GCP. La CPU de administración puede alcanzar su capacidad del 100% en las nubes de AWS y GCP, y en Citrix ADC VPX en las instalaciones. Ambos problemas se producen cuando se cumplen las siguientes condiciones:

1. Durante el primer arranque del dispositivo Citrix ADC, no guarda la contraseña solicitada.
2. A continuación, reinicie el dispositivo Citrix ADC.

[NSPLAT-22013]

Cuando actualiza de compilaciones 13.0/12.1/11.1 a una versión 13.1 o baja de una compilación 13.1 a 13.0/12.1/11.1, algunos paquetes python no se instalan en los dispositivos Citrix ADC. Este problema se ha solucionado en las siguientes versiones de Citrix ADC:

- 13.1-4.x
- 13.0—82.31 y posteriores
- 12.1—62.21 y posteriores

Los paquetes python no se instalan cuando se degrada la versión de Citrix ADC de la versión 13.1-4.x a cualquiera de las siguientes versiones:

- Cualquier compilación 11.1
- 12.1—62.21 y anteriores
- 13.0-81.x y anteriores

[NSPLAT-21691]

El aprovisionamiento de una instancia VPX con la versión 12.0 XVA falla en un dispositivo Citrix ADC SDX que ejecuta la versión 13.1.

Solo se admiten las versiones 12.1 y posteriores de VPX. Actualice la versión VPX antes de actualizar el SBI a la versión 13.1.

[NSPLAT-21442]

En una configuración de clúster en un dispositivo Citrix ADC SDX, hay una discordancia de CLAG MAC en el segundo nodo y CLIP si se cumplen las siguientes condiciones:

- El CLAG se crea en una NIC Mellanox.
- Agrega otra instancia VPX al clúster y a la configuración de CLAG.

Como resultado, el tráfico a la instancia VPX se detiene.

[NSPLAT-21049]

En una configuración de clúster en un dispositivo Citrix ADC SDX, el primer nodo se apaga debido a una falta de coincidencia de direcciones MAC en la tabla CLIP y MAC, si se cumplen las siguientes condiciones:

- El CLAG se crea en una NIC Mellanox.

- Quita el segundo nodo del clúster.

[NSPLAT-21042]

Cuando elimina una configuración de Autoscale o un conjunto de escala de VM de un grupo de recursos de Azure, elimine la configuración de perfil de nube correspondiente de la instancia de Citrix ADC. Utilice el comando `rm cloudprofile` para borrar el perfil.

[NSPLAT-4520]

En una configuración de alta disponibilidad en Azure, al iniciar sesión en el nodo secundario a través de la GUI, aparece la pantalla de usuario por primera vez (FTU) para la configuración del perfil en la nube de Autoscale.
Solución alternativa: omita la pantalla e inicie sesión en el nodo principal para crear el perfil de nube. El perfil de nube debe estar siempre configurado en el nodo principal.

[NSPLAT-4451]

Las instancias de Citrix ADC VPX que usan el controlador VMXNET3 pueden bloquearse de forma aleatoria si la instancia se ejecuta en una de las siguientes compilaciones de Citrix ADC:

- Citrix ADC 13.1 compilación 4.x
- Citrix ADC 13.1 compilación 9.x

[NSHELP-29120]

Directivas

Las conexiones pueden bloquearse si el tamaño de los datos de procesamiento es superior al tamaño del búfer TCP predeterminado configurado.Solución alternativa: Establezca el tamaño del búfer TCP en el tamaño máximo de los datos que se deben procesar.

[NSPOLICY-1267]

SSL

En un clúster heterogéneo de dispositivos Citrix ADC SDX 22000 y Citrix ADC SDX 26000, se produce una pérdida de configuración de entidades SSL si se reinicia el dispositivo SDX 26000.

Solución temporal:

1. En el CLIP, inhabilite SSLv3 en todas las entidades SSL nuevas y existentes, como servidores virtuales, servicios, grupos de servicios y servicios internos. Por ejemplo, `set ssl vserver <name> -SSL3 DISABLED`.
2. Guarde la configuración.

[NSSSL-9572]

No se puede agregar un objeto de Azure Key Vault si ya se ha agregado un objeto de autenticación de Azure Key Vault.

[NSSSL-6478]

Puede crear varias entidades de la aplicación Azure con el mismo ID de cliente y secreto de cliente. El dispositivo Citrix ADC no devuelve ningún error.

[NSSSL-6213]

El siguiente mensaje de error incorrecto aparece al quitar una clave HSM sin especificar KEYVAULT como tipo HSM.
ERROR: Actualización de crl inhabilitada

[NSSSL-6106]

La actualización automática de claves de sesión aparece incorrectamente como inhabilitada en una dirección IP de clúster. (Esta opción no se puede desactivar).

[NSSSL-4427]

Aparece `Warning: No usable ciphers configured on the SSL vserver/service,,` un mensaje de advertencia incorrecto, si intenta cambiar el protocolo o el cifrado SSL en el perfil SSL.

[NSSSL-4001]

Un tíquet de sesión caducado se respeta en un nodo que no es de CCO y en un nodo de alta disponibilidad después de una conmutación por error de alta disponibilidad.

[NSSSL-3184]

En una configuración de alta disponibilidad, el tipo de certificado no se sincroniza correctamente entre los nodos principal y secundario.

[NSHELP-27589]

Sistema

Cuando un dispositivo Citrix ADC recibe una trama HTTP/2 GOWAY de un cliente, restablece incorrectamente todas las transmisiones con un ID de transmisión mayor que el ID prometido (último identificador de transmisión iniciado por pares).

[NSHELP-29328]

El encabezado X-Forwarder no se agrega a algunas solicitudes enviadas desde el dispositivo Citrix ADC al servidor back-end.

[NSHELP-29142]

Un dispositivo Citrix ADC se bloquea si se cumplen las siguientes condiciones:

- La opción de medidas del lado del cliente está habilitada en la acción AppFlow.
- Los encabezados de los fragmentos caen en el límite del paquete.

[NSHELP-29049]

En una configuración de alta disponibilidad, la sincronización de alta disponibilidad de las configuraciones de la partición de administración falla en el nodo secundario por la siguiente razón:

- Problemas de memoria bajos causados por las enormes cargas de configuración en el nodo secundario

[NSHELP-28409]

En una conexión TCP, el dispositivo Citrix ADC puede descartar un paquete FIN, recibido de un servidor, en lugar de reenviarlo al cliente si se cumplen todas las condiciones siguientes:

- El almacenamiento en búfer TCP está habilitado.
- El servidor envía el paquete FIN y el paquete de datos por separado.

[NSHELP-27274]

La falla de Pitboss ocurre cuando se hace un bucle de una gran cantidad de paquetes en la cola de retransmisión.

[NSHELP-26071]

El valor MAX_CONCURRENT_STREAMS se establece en 100 de forma predeterminada si el dispositivo no recibe el marco de configuración max_concurrent_stream del cliente.

[NSHELP-21240]

Los contadores mptcp_cur_session_without_subflow disminuyen incorrectamente a un valor negativo en lugar de cero.

[NSHELP-10972]

En un dispositivo Citrix ADC con particiones de administración, es posible que la utilidad `nstrace` no se ejecute correctamente en una partición no predeterminada

[NSBASE-15738]

Al procesar grandes flujos de tráfico de gRPC, la ventana anunciada por TCP aumenta exponencialmente, lo que lleva a un uso elevado de memoria.

[NSBASE-15447]

La IP del cliente y la IP del servidor se invierten en el registro HDX Insight SkipFlow cuando el tipo de transporte de LogStream está configurado para Insight.

[NSBASE-8506]

Interfaz de usuario

En la GUI de Citrix ADC, el enlace `Help` presente debajo de la ficha `Dashboard` no funciona.

[NSUI-14752]

El asistente Crear/Supervisar CloudBridge Connector podría dejar de responder o no configurar un conector de cloudbridge.

Solución temporal:

Configure los conectores cloudbridge agregando perfiles IPsec, túneles IP y reglas PBR mediante la GUI o CLI de Citrix ADC.

[NSUI-13024]

Si crea una clave ECDSA mediante la interfaz gráfica de usuario, no se muestra el tipo de curva.

[NSUI-6838]

Al configurar o comprobar los certificados SSL mediante la GUI de Citrix ADC, es posible que aparezca el error `Directory doesn't exist`. Este problema se produce cuando hay un nombre de archivo con dos puntos consecutivos (`..`) en la carpeta SSL `/nsconfig/ssl`.

Solución temporal:

Elimina o mueve estos archivos de la carpeta `/nsconfig/ssl`.

[NSHELP-28589]

En una configuración de alta disponibilidad, la sincronización de alta disponibilidad podría fallar para un enlace de conjunto de patrones de directivas integrado, si el conjunto de patrones de directivas integrado se modificó en el nodo principal.

[NSHELP-28460]

Cuando el usuario intenta cambiar el tamaño de página de una lista en las vistas del panel lateral, la página se distorsiona.

[NSHELP-28220]

El comando ping o ping6 con la opción interface (-I) puede fallar con el siguiente error:

- `interface option not supported`

[NSHELP-26962]

La carga y adición de un archivo de lista de revocación de certificados (CRL) produce un error en la configuración de una partición de administración.

[NSHELP-20988]

Al revertir la versión 13.0-71.x de un dispositivo Citrix ADC a una versión anterior, es posible que algunas API de NITRO no funcionen debido a los cambios en los permisos de archivo.

Solución temporal:

Cambie el permiso de `/nsconfig/ns.conf` a 644.

[NSCONFIG-4628]

Si usted (administrador del sistema) realiza todos los pasos siguientes en un dispositivo Citrix ADC, es posible que los usuarios del sistema no inicien sesión en el dispositivo Citrix ADC degradado.

1. Actualice el dispositivo Citrix ADC a una de las compilaciones:
    - 13.0 52.24 compilación
    - 12.1 57,18 compilación
    - 11.1 65.10 compilación
2. Agregar un usuario del sistema o cambiar la contraseña de un usuario del sistema existente y guardar la configuración, y
3. Rebaja la versión del dispositivo Citrix ADC a cualquier versión anterior.

Para mostrar la lista de estos usuarios del sistema mediante la CLI:
En el símbolo del sistema, escriba:

```
query ns config -changedpassword [-config <full path of the configuration file (ns.conf)>]
```

Solución temporal:

Para solucionar este problema, utilice una de las siguientes opciones independientes:

- Si el dispositivo Citrix ADC aún no se ha degradado (paso 3 de los pasos mencionados anteriormente), degrade el dispositivo Citrix ADC mediante un archivo de configuración del que se realizó una copia de reserva (ns.conf) de la misma versión.
- Cualquier administrador del sistema cuya contraseña no se haya cambiado en la compilación actualizada puede iniciar sesión en la compilación degradada y actualizar las contraseñas de otros usuarios del sistema.
- Si ninguna de las opciones anteriores funciona, el administrador del sistema puede restablecer las contraseñas de usuario del sistema.

Para obtener más información, consulte https://docs.citrix.com/en-us/citrix-adc/13/system/ns-ag-aa-intro-wrapper-con/ns-ag-aa-reset-default-amin-pass-tsk.html

[NSCONFIG-3188]

Notas de la versión de Citrix ADC 13.1-4.44

June 22, 2022

Este documento de notas de la versión describe las mejoras y los cambios, los problemas solucionados y conocidos que existen para la versión de Citrix ADC, compilaciones 13.1 a 4.44.

Notas

- Este documento de notas de la versión no incluye correcciones relacionadas con la seguridad. Para obtener una lista de correcciones y consejos relacionados con la seguridad, consulte el boletín de seguridad de Citrix.
- El agente Citrix Secure Access (anteriormente conocido como complemento de Citrix Gateway para Windows) compilación 21.9.1.2 y posteriores contiene la corrección para https://support.citrix.com/article/CTX341455. El plug-in de Citrix Gateway para Windows compilación 21.9.1.2 se incluye en la compilación 13.1—4.44 de Citrix ADC.
- Las compilaciones 13.1 a 4.44 y versiones posteriores abordan las vulnerabilidades de seguridad descritas en https://support.citrix.com/article/CTX330728.
- La compilación 4.44 reemplaza a la compilación 4.43.
- Esta compilación también incluye una solución para el siguiente problema: NSHELP-29519.

Novedades

Las mejoras y los cambios que están disponibles en las compilaciones 13.1-4.44.

Autenticación, autorización y auditoría

Se admite el desplazamiento del dominio raíz al dominio de árbol para la autenticación de SSO Kerberos

Ahora se admite el desplazamiento del dominio raíz al dominio de árbol durante la autenticación de SSO Kerberos para el servidor de fondo del dispositivo Citrix ADC. Para obtener más información, consulte https://docs.citrix.com/en-us/citrix-adc/current-release/aaa-tm/single-sign-on-types/kerberos-single-sign-on/setup-citrix-adc-single-sign-on.html.

[NSAUTH-9836]

Administración de bots

Registro verboso para la administración de bots de Citrix ADC

Si el tráfico entrante se identifica como bot, el dispositivo Citrix ADC ahora le permite configurar la funcionalidad de registro detallado del bot para registrar detalles adicionales del encabezado HTTP, como dirección de dominio, URL, encabezado de agente de usuario y encabezado de cookie. Los detalles del registro se envían al servidor ADM con fines de supervisión y solución de problemas. El mensaje de registro verboso no se almacena en el archivo ns.log.

Para obtener más información, consulte https://docs.citrix.com/en-us/citrix-adc/current-release/bot-management/bot-detection.html

[NSBOT-273]

Dispositivo Citrix ADC SDX

Mejoras en la página de formación de clústeres en un dispositivo Citrix ADC SDX

Los siguientes cambios se realizan en la interfaz gráfica de usuario de la página `Add Node to Cluster`. El sistema ahora solicita al usuario que agregue una dirección SNIP mientras agrega un nuevo nodo a un clúster. Estas mejoras abordan los problemas de seguridad de la comprobación estricta de la dirección IP de origen.

- Ahora se proporciona un campo opcional para SNIP.
- También se proporciona un botón `Add` para crear SNIP dinámicamente mientras se agrega un nodo a la dirección IP del clúster (CLIP).

[NSSVM-4170]

Un administrador de Citrix ADC SDX ahora puede desbloquear a un usuario antes de que caduque el intervalo de bloqueo. El bloqueo no se aplica si un usuario inicia sesión en Management Service a través de la consola. El intervalo de bloqueo también cambia de segundos a minutos. Valor mínimo = 1 minuto. Valor máximo = 30 minutos.

Para desbloquear a un usuario mediante la interfaz gráfica de usuario:

1. Vaya a **Configuración > Sistema > Administración de usuarios > Usuarios**.
2. Seleccione el usuario que quiere desbloquear.
3. Haga clic en **Desbloquear**.**Para desbloquear a un usuario mediante la CLI:**

En el símbolo del sistema, escriba:

```
set systemuser id=`<ID>` unlock=true
<!--NeedCopy-->
```

[NSSVM-4144]

Citrix Gateway

Más idiomas disponibles

El portal de usuarios de Citrix Gateway ya está disponible en los idiomas ruso, coreano y chino (tradicional).

[CG-17095]

Compatibilidad con la autenticación OAuth-OpenID Connect para Gateway Insight

Citrix Gateway Insight ahora informa de eventos relacionados con la autenticación de OAuth-OpenID Connect (inicios de sesión de usuario correctos y fallidos).

Para obtener más información, consulte https://docs.citrix.com/en-us/citrix-application-delivery-management-software/current-release/analytics/gateway-insight.html

[CGP-16907]

Citrix Web App Firewall

Extracción de direcciones IP del cliente mediante una expresión de directiva avanzada

El dispositivo Citrix ADC utiliza una expresión de directiva avanzada para extraer la dirección IP del cliente de un encabezado de solicitud HTTP, cuerpo de solicitud y URL de solicitud. El valor extraído se envía al servidor de ADM para el registro de auditoría, la información de seguridad y el cálculo de la geolocalización del cliente.

Para obtener más información, consulte https://docs.citrix.com/en-us/citrix-adc/current-release/bot-management/bot-detection.html

[NSWAF-7260]

Habilitar opción para el mecanismo de detección de TPS BOT

La opción Habilitar ahora está disponible para cada regla de detección de bots TPS en la configuración del perfil de bot. De forma predeterminada, el valor es ON.

Para obtener más información, consulte https://docs.citrix.com/en-us/citrix-adc/current-release/bot-management/bot-detection.html

[NSHELP-25777]

Equilibrio de carga

Compatibilidad con la redirección HTTP a HTTPS en servidores virtuales de conmutación de contenido

Los servidores virtuales de conmutación de contenido del tipo de servicio SSL ahora admiten la redirección del tráfico HTTP. Dos nuevos parámetros: `HttpsRedirectUrl` y `RedirectFromPort` se agregan al comando `add cs vserver`. Todo el tráfico HTTP que llega al puerto especificado en el parámetro `RedirectFromPort` se redirige a la URL especificada en el parámetro `HttpsRedirectUrl`. Si `HttpsRedirectUrl` no está configurado, el tráfico HTTP se redirige al valor del encabezado del host en la solicitud HTTP entrante.

Para obtener más información, consulte https://docs.citrix.com/en-us/citrix-adc/current-release/ssl/how-to-articles/ssl-config-https-vserver-to-accept-http-traffic.html

[NSLB-8224]

Compatibilidad para sincronizar el comando save config con sitios GSLB remotos

Ahora puede sincronizar el comando `save ns config` con sitios GSLB remotos. Para habilitar esta funcionalidad, se agrega un nuevo parámetro `GSLBSyncSaveConfigCommand` al comando `set gslb parameter`. Una vez habilitado `GSLBSyncSaveConfigCommand`, el comando `save ns config` se trata como otro comando de GSLB y se sincroniza con sitios GSLB remotos. Debe habilitar la opción `AutomaticConfigSync` para sincronizar el comando `save ns config`.

Para obtener más información, consulte https://docs.citrix.com/en-us/citrix-adc/current-release/global-server-load-balancing/synchronizing-configuration-in-gslb-setup/real-time-synchronization.html

[NSLB-7831]

Compatibilidad con argumentos de script seguros para monitores de usuario

Se agrega un nuevo parámetro, `-secureargs`, al comando `add lb monitor`. Este parámetro almacena los argumentos de script en un formato cifrado en lugar de en formato de texto sin formato. Puede proteger los datos confidenciales relacionados con los scripts del monitor de usuario mediante este parámetro, por ejemplo, nombre de usuario y contraseña. Citrix recomienda utilizar el parámetro `-secureargs` en lugar del parámetro `-scriptargs` para cualquier dato confidencial relacionado con los scripts. Si elige utilizar ambos parámetros a la vez, el script especificado en `-scriptname` debe aceptar los argumentos en el orden: `<scriptargs> <secureargs>`. Es decir, debe especificar los primeros parámetros `<scriptargs>` y el resto de los parámetros en `<secureargs>` manteniendo el orden definido para los argumentos. Los argumentos seguros solo se aplican al despachador interno.

Para obtener más información, consulte https://docs.citrix.com/en-us/citrix-adc/current-release/load-balancing/load-balancing-custom-monitors/configure-user-monitor.html

[NSLB-6314]

Redes

Compatibilidad con conjuntos de datos de tipo numérico para ACL ampliadas

El dispositivo Citrix ADC ahora admite el conjunto de datos de tipo numérico para las ACL extendidas. Puede utilizar el conjunto de datos de tipo numérico para especificar el puerto de origen o el puerto de destino, o ambos para una regla de ACL ampliada.

[NSNET-20235]

Compatibilidad con RHI para una dirección VIP vinculada a un conjunto de IP

Un dispositivo Citrix ADC anuncia una dirección VIP vinculada a un conjunto de IP como ruta del kernel si se cumplen todas las condiciones siguientes:

- La dirección VIP tiene la opción `host route` activada.
- El IPset está enlazado a una configuración, por ejemplo, servidores virtuales de equilibrio de carga de varias IP.

[NSNET-20209]

Compatibilidad con el registro de Citrix ADC CPX con ADM mediante montajes de volúmenes

Citrix ADC CPX ahora admite el registro en Citrix ADM mediante montajes de volúmenes a través de Kubernetes ConfigMaps y Secret. Citrix ADC CPX inicia el registro con el agente ADM con los detalles de configuración derivados de los montajes de volumen que se encuentran en el sistema de archivos de Citrix ADC CPX.

[NSNET-19058]

Plataforma

Compatibilidad con la actualización 2a de VMware ESX 7.0 en la instancia de Citrix ADC VPX

La instancia de Citrix ADC VPX ahora admite la actualización 2a de VMware ESX versión 7.0 (compilación 17867351).

Para obtener más información, consulte https://docs.citrix.com/en-us/citrix-adc/current-release/deploying-vpx/supported-hypervisors-features-limitations.html

[NSPLAT-20104]

Compatibilidad con procesadores AMD para instancia Citrix ADC VPX en ESXi

La instancia Citrix ADC VPX del hipervisor VMware ESXi ahora admite procesadores AMD. Para obtener más información, consulte https://docs.citrix.com/en-us/citrix-adc/current-release/deploying-vpx/install-vpx-on-esx.html

[NSPLAT-17853]

Compatibilidad con la suscripción a Citrix ADC VPX 5000 en Azure Marketplace

El plan de suscripción Citrix ADC VPX 5000 ahora es compatible con Azure Marketplace. Este plan basado en suscripción ofrece las siguientes licencias:

- Estándar
- Avanzado
- Premium

Para obtener más información, consulte https://docs.citrix.com/en-us/citrix-adc/current-release/deploying-vpx/deploy-vpx-on-azure.html#citrix-adc-vpx-licensing

[NSPLAT-13663]

Directivas

Compatibilidad con campos de encabezado IP en expresiones de directivas avanzadas

La expresión de directiva avanzada ahora permite obtener los siguientes campos de encabezado de un paquete IP.

- DSCP
- ECN
- TTL
- Versión
- Identificación
- Longitud del encabezado
- suma de comprobación de encabezado
- Opciones
- Payload

[NSPOLICY-2441]

Eliminación de funciones obsoletas de Citrix ADC versión 13.1 en adelante

Ahora se han eliminado numerosas funciones obsoletas y ya no se pueden configurar en un dispositivo Citrix ADC.

que incluye:

- La función Filtro (también conocida como filtrado de contenido o CF): acciones, directivas y vinculación.
- Las funciones SPDY, conexión segura (SC), cola prioritaria (PQ), denegación de servicio HTTP (DoS) e inyección de HTML.
- Directivas clásicas para SSL, cambio de contenido, redirección de caché, compresión y firewall de aplicaciones.

- Los parámetros `url` y `domain` de las directivas de conmutación de contenido.
- Expresiones clásicas en reglas de persistencia de equilibrio de cargas.
- El parámetro `pattern` de las acciones de reescritura.
- El parámetro `bypassSafetyCheck` de las acciones de reescritura.
- `SYS.EVAL_CLASSIC_EXPR` en Expresiones avanzadas.
- Entidad de configuración `patclass`.
- `HTTP.REQ.BODY` sin argumentos en las expresiones avanzadas.
- Prefijos Q y S en expresiones avanzadas.
- Parámetro `policyType` para la configuración del parámetro cmp. (Comando `set cmp parameter` de la CLI)

Como ya se ha documentado, puede usar la herramienta `nspepi` para la conversión. Debe ejecutar la herramienta en un dispositivo Citrix ADC versión 13.0 o 12.1.

Para obtener más información, consulte https://docs.citrix.com/en-us/citrix-adc/current-release/appexpert/policies-and-expressions/introduction-to-policies-and-exp/classic-policy-deprecation-faq.html

Además, si quiere utilizar la versión más reciente de las herramientas para migrar de la configuración clásica a la avanzada y de los dominios de tráfico a las particiones de administración, consulte https://github.com/citrix/ADC-scripts

[NSPOLICY-186]

Sistema

Ver las estadísticas de QUIC bridge

El comando puente QUIC `stat` ahora proporciona un resumen detallado de las estadísticas del puente QUIC.

[NSBASE-13883]

Eliminación de funciones obsoletas en Citrix ADC 13.1 en adelante

Las siguientes funciones obsoletas y sus configuraciones ya no son compatibles y se quitan del dispositivo Citrix ADC:

- Conexión segura (SC)
- Colas prioritarias (PQ)
- Protección HTTP DoS (HDOSP)
- `HTMLInjection`

Como alternativa, Citrix recomienda utilizar AppQoE para SureConnect, Priority Queueing y HTTP DoS Protection y usar mediciones del lado del cliente para `HTMLInjection`.

Para obtener más información, consulte https://docs.citrix.com/en-us/citrix-adc/current-release/appexpert/policies-and-expressions/introduction-to-policies-and-exp/classic-policy-deprecation-faq.html

[NSBASE-13780]

Interfaz de usuario

Compatibilidad con API por lotes para llamadas NITRO

El dispositivo Citrix ADC ahora admite la API de `batchapi`. La API de `batchapi` puede gestionar varias llamadas NITRO en una sola solicitud y, por lo tanto, minimizar el tráfico de red. Puede realizar las siguientes operaciones mediante `batchapi`:

- Puede utilizar la API por lotes para crear, actualizar y eliminar varios recursos heterogéneos simultáneamente.
- Puede usar la API por lotes para obtener varios recursos heterogéneos.

[NSCONFIG-4061]

Problemas resueltos

Los problemas que se abordan en las compilaciones 13.1 a 4.44.

Autenticación, autorización y auditoría

Al enlazar un monitor LDAP a un servicio, el monitor se desactiva porque el dispositivo Citrix ADC envía una contraseña incorrecta al active directory.

[NSHELP-27961]

En un AD de varias cascadas, la cuenta de un usuario no se bloquea si no se encuentra a un usuario en la última cascada.

[NSHELP-27948]

Cuando se configura un dispositivo Citrix ADC para la autenticación SAML, el dispositivo vuelca el núcleo al utilizar un certificado que no sea RSA.

[NSHELP-27813]

En algunos casos, es posible que un dispositivo Citrix ADC se bloquee al gestionar la solicitud de autenticación de determinados usuarios cuando se configura el acceso basado en roles.

[NSHELP-27655]

Los usuarios no pueden iniciar sesión a través de la aplicación Citrix Workspace si Azure AD está configurado como proveedor de identidad de OAuth en el servidor virtual de autenticación de Citrix ADC.

[NSHELP-27462]

En algunos casos, la autenticación SAML falla con la aplicación Workspace si se accede a la aplicación mediante StoreFront.

[NSHELP-27338]

En algunos casos, una solicitud HTTP POST a un servidor virtual Authentication, authorization and Auditing-TM se procesa incorrectamente si la solicitud no tiene una cookie de autenticación. El cuerpo POST se pierde durante el procesamiento.

[NSHELP-27227]

El dispositivo Citrix ADC se bloquea con frecuencia al procesar el tráfico basado en autenticación, autorización y auditing-TM y 401 LB.

[NSHELP-27094]

En algunos casos, un dispositivo Citrix ADC se bloquea al realizar la autenticación de usuario para Citrix Gateway y Autenticación, autorización y auditoría: implementación administrada por tráfico.

[NSHELP-26555]

Al introducir una OTP incorrecta, aparece un mensaje de error `Email Auth failed. No further action to continue`.

[NSHELP-26400]

En algunos casos, el comando Vincular autenticación, autorización y grupo de auditoría puede fallar si el nombre de la directiva es más largo que el nombre de la aplicación de la intranet.

[NSHELP-25971]

Un dispositivo Citrix ADC configurado como proveedor de identidad (IdP) SAML corta el estado de retransmisión del proveedor de servicios (SP) si contiene comillas.

[NSHELP-20131]

La comprobación de conectividad de red falla debido a un problema de descifrado de contraseñas. Sin embargo, la funcionalidad de autenticación funciona bien.

[NSAUTH-10216]

Administración de bots

En el mecanismo de detección de bots de transacciones por segundo (TPS), el servidor de aplicaciones back-end devuelve una respuesta 304 durante la recuperación de respuestas tras el desafío CAPTCHA.

[NSBOT-626]

Almacenamiento en caché

En una configuración de alta disponibilidad, la sincronización de alta disponibilidad falla en la configuración del parámetro de caché `memLimit` durante una conmutación por error de alta disponibilidad.

[NSHELP-28428]

En una configuración de alta disponibilidad, el nodo principal se bloquea después de acceder a un puntero NULL en lugar de a un objeto almacenado en caché.

[NSHELP-26967]

Dispositivo Citrix ADC SDX

En un dispositivo Citrix ADC SDX, la restauración de instancias podría fallar si la instancia se creó con la versión de software 13.0-76.x o anterior.

[NSHELP-28429]

En un dispositivo Citrix ADC SDX, Management Service informa sobre el uso incorrecto de datos de las instancias ADC.

[NSHELP-28208]

En un dispositivo Citrix ADC SDX, no se puede cambiar el mensaje de CLI en la consola de Management Service.

[NSHELP-28030]

En un dispositivo Citrix ADC SDX, Management Service puede reportar un uso elevado de memoria de alrededor del 80% debido al aumento de los trabajos y programadores que se ejecutan en el inventario.

[NSHELP-27805]

En un dispositivo Citrix ADC SDX, la actualización puede fallar si los archivos del sistema (snmpd.conf y ntp.conf) contienen caracteres de retorno de carro.

[NSHELP-27713]

En un dispositivo Citrix ADC SDX, Management Service puede reportar un uso elevado de memoria de alrededor del 80% debido al aumento de los trabajos y programadores que se ejecutan en el inventario.

[NSHELP-27396]

Citrix Gateway

Los usuarios pueden observar un error en el inicio de la sesión RDP cuando hay una actualización a la última versión.

[NSHELP-29519]

Aparece un mensaje de error al intentar modificar los atributos CSS de un tema personalizado.

[NSHELP-28648]

El inicio de sesión en Citrix Workspace falla si las directivas de respuesta que pueden entrar en un estado bloqueado durante la evaluación están vinculadas al servidor virtual.

[NSHELP-27819]

Al acceder al dispositivo Citrix Gateway mediante la VPN sin cliente, se puede generar un volcado de memoria.

[NSHELP-27653]

Es posible que el dispositivo Citrix Gateway se bloquee al procesar el tráfico UDP iniciado por el servidor.

[NSHELP-27611]

Los usuarios pueden ver los buzones de correo de otros usuarios cuando inician sesión en Microsoft Outlook. Como solución alternativa, inhabilite la multiplexación.

[NSHELP-27538]

Un dispositivo Citrix ADC podría bloquearse si los comandos relacionados con EDT, como `clearconfig`, `kill ica connection` o `stop dtls listener` son procesados por el dispositivo.

[NSHELP-27398]

Es posible que el dispositivo Citrix Gateway se bloquee al procesar el tráfico UDP.

[NSHELP-27317]

El dispositivo Citrix Gateway se bloquea cuando una directiva de syslog está vinculada a un servidor virtual y se modifica la acción syslog correspondiente.

[NSHELP-27171]

Los registros de Citrix ADC pueden estar inundados con el mensaje de registro `GwInsight: Func =ns_sslvpn_send_app_launch_fail_record Appflow policy evaluation has failed` cuando Gateway Insight está habilitado.

[NSHELP-26750]

El dispositivo Citrix Gateway se bloquea al intentar borrar la configuración si se cumplen las dos condiciones siguientes:

- Un perfil SSL y un par de claves de certificado están enlazados al monitor TCP predeterminado.
- El mismo monitor TCP predeterminado está vinculado a una acción syslog.

[NSHELP-26685]

Al introducir el FQDN como proxy en la página Crear perfil de tráfico de Citrix Gateway, aparece el mensaje `Invalid Proxy Value`.

[NSHELP-26613]

Al crear un perfil de cliente RDP mediante la GUI de Citrix ADC, aparece un mensaje de error cuando se cumplen las siguientes condiciones:

- Se ha configurado una clave previamente compartida (PSK) predeterminada.
- Intenta modificar el temporizador de validez de la cookie de RDP en el campo Validez de cookies de RDP (segundos).

[NSHELP-25694]

El OID SNMP envía un conjunto incorrecto de conexiones actuales al servidor virtual VPN.

[NSHELP-25596]

El dispositivo Citric ADC se bloquea cuando varios clientes de plug-ins VPN utilizan certificados X.509 de un tamaño de 1800 bytes o más para configurar un túnel.

[NSHELP-25195]

Si cambia el nombre de un servidor virtual VPN vinculado a un servidor STA, el estado del servidor STA aparece DESACTIVADO cuando ejecuta el comando show.

[NSHELP-24714]

En raras ocasiones, el dispositivo Citrix Gateway podría bloquearse si la dirección IP (IIP) de la intranet está habilitada y hay conexiones iniciadas por el servidor a la dirección IIP.

[NSHELP-23819]

El resultado del comando `show tunnel global` incluye nombres de directivas avanzadas. Anteriormente, el resultado no mostraba los nombres de directivas avanzadas.

Ejemplo:

Nueva salida:

```
> show tunnel global
Policy Name: ns_tunnel_nocmp Priority: 0

Policy Name: ns_adv_tunnel_nocmp Type: Advanced policy
Priority: 1
Global bindpoint: REQ_DEFAULT

Policy Name: ns_adv_tunnel_msdocs Type: Advanced policy
```



```
Priority: 100
Global bindpoint: RES_DEFAULT
Done
>
<!--NeedCopy-->
```

Salida anterior:

```
> show tunnel global
Policy Name: ns_tunnel_nocmp Priority: 0 Disabled

Advanced Policies:

Global bindpoint: REQ_DEFAULT
Number of bound policies: 1

Done
<!--NeedCopy-->
```

[NSHELP-23496]

Si ha configurado la contabilidad RADIUS para el evento de inicio/detención ICA, el ID de sesión de la solicitud de cuentas RADIUS para el inicio de ICA se muestra como todos ceros.

[NSHELP-22576]

Citrix Web App Firewall

En una configuración de clúster de Citrix ADC, uno de los nodos se bloquea si uno o más nodos se actualizan desde la versión 12.0, 12.1 o 13.0 compilación 52.x o versiones anteriores de Citrix ADC. El bloqueo se produce debido a una incompatibilidad en el formato y el tamaño de las cookie de Web App Firewall.

[NSWAF-7689]

En Web App Firewall, el parámetro `Cookie-transformation` divide los valores de cookie del lado de respuesta si tiene una coma como delimitador.

[NSHELP-28411]

Un dispositivo Citrix ADC podría bloquearse si se observan infracciones de inyección de comandos en un orden específico y si se cumplen las siguientes condiciones:

- Hay varias cookies presentes en la solicitud
- `URLDecodeRequestCookies` la función está desactivada

[NSHELP-28365]

Un dispositivo Citrix ADC puede mostrar un uso elevado de memoria al analizar respuestas HTTP con el atributo Samesite y la función Firewall de aplicaciones web habilitadas.

[NSHELP-27722]

La función de secuestro de cookie tiene una funcionalidad limitada para el explorador Internet Explorer porque los exploradores Internet Explorer no reutilizan las conexiones SSL. Debido a la limitación, se envían varios redireccionamientos para una solicitud, lo que ocasionará un error `MAX REDIRECTS EXCEEDED` en el explorador Internet Explorer.

[NSHELP-27193]

Tras una actualización a Citrix ADC versión 13.0 compilación 76.29 y con la función Carga de archivos habilitada en el dispositivo, se observa el siguiente problema:

- Las comprobaciones de protección de scripts SQL y entre sitios bloquean el proceso de carga de archivos de todas las aplicaciones web.

[NSHELP-27140]

Equilibrio de carga

En una configuración de GSLB, el estado de los servicios remotos no se actualiza después de borrar las estadísticas del sitio de GSLB. Como solución alternativa, vuelva a borrar las estadísticas en el mismo sitio de GSLB. A continuación, se actualiza el estado de los servicios remotos.

[NSHELP-28169]

En una configuración de alta disponibilidad, el nodo secundario podría bloquearse si se cumplen las siguientes condiciones:

- La cantidad de memoria física de ambos nodos es diferente entre sí.
- Las sesiones de datos no se sincronizan correctamente.

[NSHELP-26503]

En una configuración de clúster, la dirección IP del servicio GSLB no se muestra en la GUI cuando se accede a través de enlaces de servidor virtual GSLB. Esto es solo un problema de visualización y no afecta a la funcionalidad.

[NSHELP-20406]

Otros

Un dispositivo Citrix ADC agrega información adicional de nivel 2 cuando se crea un túnel o servidores virtuales de tipo de servicio (TOS).

[NSHELP-27825]

Redes

Después de actualizar un dispositivo Citrix ADC BLX (versión 13.0 compilación 82.x) que se ejecuta en un host Linux basado en Debian, SSH no funciona según lo previsto en el modo compartido.

[NSNET-23020]

Después de actualizar un dispositivo Citrix ADC BLX a la versión 13.1 compilación 4.x, es posible que el firewall de aplicaciones web bloquee incorrectamente una solicitud que no tiene encabezado de tipo de contenido.

[NSNET-21415]

En un dispositivo Citrix ADC BLX, es posible que NSVLAN enlazada con interfaces `non-dpdk` etiquetadas no funcione según lo esperado. NSVLAN enlazado con interfaces `non-dpdk` no etiquetadas funciona bien.

[NSNET-18586]

En un dispositivo Citrix ADC, la capa de controladores internos puede utilizar un búfer de datos incorrecto que provoque daños en los datos, lo que a su vez provoca que el dispositivo se bloquee.

[NSHELP-27858]

Problema solucionado:

Citrix ADC CPX implementado como sidecar y conectado a varias redes no pudo elegir la dirección IP de origen correcta para la subred de destino.

[NSHELP-27810]

En una configuración de alta disponibilidad, la sincronización de alta disponibilidad puede fallar en las configuraciones del perfil WAF y del archivo de ubicación.

[NSHELP-27546]

Los bucles de paquetes se observan en una configuración de equilibrio de carga si se cumplen todas las condiciones siguientes:

- El servidor virtual está configurado para escuchar en el puerto 80 y el parámetro de conmutación por error de conexión (`connfailover`) se establece en sin estado.
- El servidor virtual recibe dos paquetes de solicitud que tienen:
  - Puerto de origen = 80
  - Puerto de destino = número distinto de 80
  - Dirección IP de destino = dirección IP (VIP) del servidor virtual

[NSHELP-22431]

Plataforma

`Failed to create target instance` aparece un mensaje de error en la consola de GCP incluso cuando no creas ninguna instancia de destino. Este problema se produce cuando no tiene el permiso de IAM `compute.targetInstances.get` en su cuenta de servicio de GCP. A partir de esta versión, Citrix ADC VPX crea instancias de destino solo para las máquinas virtuales que utilizan la función VIP Scaling.

[NSPLAT-20952]

El dispositivo Citrix ADC genera alertas de límite de velocidad de paquetes falsos por segundo (PPS) incluso antes de que el dispositivo Citrix ADC alcance su límite de PPS para la licencia.

[NSHELP-26935]

Directivas

La variable NS con ámbito global no funciona para el tráfico HTTP/2.

[NSHELP-27095]

SSL

En una configuración de clúster, cuando dos certificados instalados son emisores de un certificado de servidor que tiene la extensión AIA de OCSP, el dispositivo deja de estar disponible si quita el certificado del servidor.

[NSHELP-28058]

En una configuración de alta disponibilidad, la actualización automática de CRL falla de forma intermitente si se cumplen las dos condiciones siguientes:

- Los archivos se sincronizan del nodo principal al nodo secundario.
- El archivo CRL se está descargando del servidor CRL al mismo tiempo.

[NSHELP-27435]

En un dispositivo Citrix ADC, se registra una notificación de caducidad de certificado falso al día siguiente cuando se agrega un par de claves de certificado con -expiryMonitor habilitado.

[NSHELP-27348]

En una base de datos de clúster, el enlace no se actualiza correctamente si enlaza una directiva SSL a un servidor virtual en el punto de enlace de saludo del cliente varias veces y con distintas prioridades. Como resultado, aparece un error al quitar la directiva incluso después de haberla desvinculado del servidor virtual.

[NSHELP-27301]

El dispositivo Citrix ADC se bloquea durante el reinicio si se cambia el nombre del certificado integrado (`ns-server-certificate`) en el archivo de configuración.

[NSHELP-26858]

En una configuración de clúster, es posible que se observen los siguientes problemas:

- Falta el comando para el par de claves de certificado predeterminado vinculado a los servicios internos SSL del CLIP. Sin embargo, si actualiza desde una versión anterior, es posible que tenga que vincular el par de claves de certificado predeterminado a los servicios internos SSL afectados en el CLIP.
- Discrepancia de configuración entre el CLIP y los nodos del comando set predeterminado para los servicios internos.
- Falta el comando default cipher bind para las entidades SSL en el resultado del comando show running config ejecutado en un nodo. La omisión es solo un problema de visualización y no tiene ningún impacto funcional. El enlace se puede ver mediante el comando `show ssl <entity> <name>`.

[NSHELP-25764]

Sistema

Es posible que un dispositivo Citrix ADC se bloquee con una respuesta ICAP OPTIONS. El problema se produce cuando el valor de encabezado permitido contiene un valor distinto de 204.

[NSHELP-27879]

En AppFlow, el recuento de bytes de capa 4 para los registros de flujo no coincide con las transacciones del servidor virtual HTTP. El valor de recuento es inferior al valor de recuento de bytes del servidor virtual de capa 7.

[NSHELP-27495]

El contador tcpCurClientConn muestra un valor alto si el dispositivo Citrix ADC está registrado en Citrix ADM.

[NSHELP-27463]

Es posible que un dispositivo Citrix ADC se bloquee cuando la función AppFlow se inhabilita y se vuelve a habilitar.

[NSHELP-27236]

En raras ocasiones, un dispositivo Citrix ADC podría enviar números de secuencia TCP SACK incorrectos al cliente al reenviarlo desde el servidor backend. El problema se produce si la opción ACK selectiva de TCP (SACK) está habilitada en un perfil TCP.

[NSHELP-24875]

Un dispositivo Citrix ADC puede bloquearse cuando una directiva con la expresión `HTTP.REQ.*` está enlazada al punto de enlace RESPONSE del servidor virtual `HTTP_QUIC`. El problema no se produce si vincula la misma directiva a un servidor virtual de tipo HTTP o SSL junto con un servidor virtual `HTTP_QUIC`.

[NSBASE-14612]

Interfaz de usuario

En la GUI de Compression Policy Manager, no se puede enlazar una directiva de compresión a un protocolo HTTP especificando un punto de enlace y un tipo de conexión pertinentes.

[NSUI-17682]

Al obtener el contenido de cualquier archivo de una instancia de ADC mediante el comando `show systemfile`, aparece un mensaje de error de error de descarga en la consola de ADC. El problema se produce si el contenido del archivo comienza con bytes NULL.

[NSHELP-28227]

La inundación de SYSLOG `admautoregd` provoca una clasificación y un diagnóstico erróneos de la definición de recursos del cliente
(CRD) debido a un problema interno del sistema (falta el archivo binario de Python).

Corrección: Dejar de supervisar el proceso `admautoregd` después de 30 minutos si el binario python sigue faltando.

[NSHELP-28185]

Es posible que se pierda la configuración si una instancia VPX en AWS, configurada con KEK, se actualiza a Citrix ADC versión 13.0 compilación 76.x o posterior. Todos los datos confidenciales cifrados mediante KEK fallan si la configuración se carga después de reiniciar.

[NSHELP-28010]

Se introduce incorrectamente una barra diagonal inversa adicional si se utilizan caracteres especiales en los argumentos de algunos comandos SSL, como `create ssl rsakey` y `create ssl cert`.

[NSHELP-27378]

En una configuración de alta disponibilidad, la sincronización de alta disponibilidad o la propagación de alta disponibilidad pueden fallar si se cumple alguna de las siguientes condiciones:

- La contraseña del nodo RPC tiene caracteres especiales.
- La contraseña del nodo RPC tiene 127 caracteres (caracteres máximos permitidos).

[NSHELP-27375]

La herramienta `nsconfigaudit` podría fallar si el tamaño del archivo de configuración de entrada es muy grande.

[NSHELP-27263]

No se puede enlazar un servicio o un grupo de servicios a un servidor virtual de equilibrio de carga prioritario mediante la GUI de Citrix ADC.

[NSHELP-27252]

La funcionalidad de generación de informes podría dejar de funcionar si el reloj del sistema se actualiza en un dispositivo Citrix ADC.

[NSHELP-25435]

En un dispositivo Citrix ADC VPX, una operación de configuración de capacidad puede fallar tras agregar un servidor de licencias. El problema se produce porque los componentes relacionados con Flexera tardan más en inicializarse debido al gran número de licencias admitidas de tipo check-in y check-out (CICO)

[NSHELP-23310]

La llamada GET de la API de NITRO `botprofile_logexpression_binding` no devuelve ninguna respuesta si la expresión de registro está enlazada a un perfil de bot.

[NSCONFIG-5490]

En una configuración de clúster, cuando vincula un perfil de Web App Firewall con reglas específicas y, a continuación, con reglas `non-fine-graned` a la misma URL, las reglas específicas se eliminan de la base de datos. Como resultado, solo se muestran las reglas no específicas en la dirección IP del clúster.

[NSCONFIG-5389]

Problemas conocidos

Los problemas que existen en las versiones 13.1 a 4.44.

AppFlow

HDX Insight no informa de un error de inicio de aplicación causado por un usuario que intenta iniciar una aplicación o un escritorio a los que el usuario no tiene acceso.

[NSINSIGHT-943]

Autenticación, autorización y auditoría

Se devuelve una URL de cierre de sesión (`/cgi/tmlogout`) incorrecta cuando un servidor virtual VPN se configura como SP SAML. El problema ocurre porque se genera una URL de cierre de sesión incorrecta en los metadatos SAML.

[NSHELP-28726]

En algunos casos, se observa una pérdida de memoria en un dispositivo Citrix ADC si la funcionalidad SSO se usa con un servidor proxy.

[NSHELP-27744]

En un caso poco frecuente, el nodo secundario en una configuración de alta disponibilidad puede bloquearse si se cumple la siguiente condición.

- `aaa groups` o `aaa users` o ambos se configuran en el dispositivo Citrix ADC.

[NSHELP-26732]

Un dispositivo Citrix ADC no autentica los intentos de inicio de sesión con contraseñas duplicadas y evita los bloqueos de cuentas.

[NSHELP-563]

LoginSchema de DualAuthPushOrOTP.xml no aparece correctamente en la pantalla del editor de esquemas de inicio de sesión de la GUI de Citrix ADC.

[NSAUTH-6106]

El perfil proxy ADFS se puede configurar en una implementación de clúster. El estado de un perfil proxy se muestra incorrectamente en blanco al ejecutar el siguiente comando.
`show adfsproxyprofile <profile name>`

Solución temporal:

Conéctese al Citrix ADC activo principal del clúster y ejecute el comando `show adfsproxyprofile <profile name>`. Mostraría el estado del perfil de proxy.

[NSAUTH-5916]

La página Configurar servidor LDAP de autenticación de la GUI de Citrix ADC deja de responder si sigue los pasos siguientes:

- Se abre la opción Probar accesibilidad LDAP.
- Las credenciales de inicio de sesión no válidas se rellenan y envían.
- Las credenciales de inicio de sesión válidas se rellenan y envían.

Solución temporal:

Cierre y abra la opción Probar accesibilidad de LDAP.

[NSAUTH-2147]

Almacenamiento en caché

Es posible que un dispositivo Citrix ADC se bloquee si la función Almacenamiento en caché integrado está habilitada y el dispositivo tiene poca memoria.

[NSHELP-22942]

Dispositivo Citrix ADC SDX

En un dispositivo Citrix ADC SDX, se produce un error al crear una instancia de ADC con la imagen XVA de la versión 12.0 del software. Como resultado, no se puede acceder a la instancia.

[NSHELP-28408]

En un dispositivo Citrix ADC SDX, las instancias de ADC no alcanzan su capacidad máxima al configurar el modo de asignación de rendimiento en ráfagas.

[NSHELP-27477]

Las caídas de paquetes se observan en una instancia VPX alojada en un dispositivo Citrix ADC SDX si se cumplen las siguientes condiciones:

- El modo de asignación de rendimiento está en ráfaga.
- Existe una gran diferencia entre el rendimiento y la capacidad máxima de ráfaga.

[NSHELP-21992]

Citrix Gateway

A veces, después de desconectar la VPN, el solucionador de DNS no resuelve los nombres de host porque los sufijos DNS se eliminan durante la desconexión de la VPN.

[NSHELP-28848]

Después de actualizar el dispositivo Citrix Gateway a la versión 13.0, la configuración de proxy en el perfil de sesión no funciona según lo previsto. La conexión de proxy se omite para el proxy NS no HTTP configurado.

Ejemplo:
add vpn sessionAction -proxy NS -httpProxy 192.0.2.0:24 -sslProxy 192.0.2.0:24

En este ejemplo, -httpProxy funciona según lo previsto, pero -sslProxy no funciona.

[NSHELP-28640]

La autenticación de certificados de cliente falla para Citrix SSO para macOS si no hay certificados de cliente en el llavero de macOS.

[NSHELP-28551]

A veces, se desactiva la sesión de un usuario en Citrix Gateway en unos segundos cuando se establece el tiempo de espera por inactividad del cliente.

[NSHELP-28404]

Es posible que el complemento de Windows se bloquee durante la autenticación.

[NSHELP-28394]

El dispositivo Citrix ADC se bloquea si se produce alguna de las siguientes condiciones:

- La acción syslog se configura con el nombre de dominio y usted borra la configuración mediante la GUI o la CLI.
- La sincronización de alta disponibilidad se produce en el nodo secundario.

Solución temporal:

Cree una acción syslog con la dirección IP del servidor syslog en lugar del nombre de dominio del servidor syslog.

[NSHELP-25944]

El complemento EPA para Windows no utiliza el proxy configurado del equipo local y se conecta directamente al servidor de puerta de enlace.

[NSHELP-24848]

Gateway Insight no muestra información precisa sobre los usuarios de VPN.

[NSHELP-23937]

El complemento VPN no establece el túnel después del inicio de sesión de Windows si se cumplen las siguientes condiciones:

- El dispositivo Citrix Gateway está configurado para la función Always On
- El dispositivo está configurado para la autenticación basada en certificados con autenticación de dos factores `off`

[NSHELP-23584]

A veces, al navegar por los esquemas, aparece el mensaje de error `Cannot read property 'type 'of undefined`.

[NSHELP-21897]

El error de inicio de la aplicación debido a un tíquet de STA no válido no se informa en Gateway Insight.

[CGOP-13621]

El informe Gateway Insight muestra incorrectamente el valor `Local` en lugar de `SAML` en el campo **Tipo de autenticación** para los errores de SAML.

[CGOP-13584]

En una configuración de alta disponibilidad, durante la conmutación por error de Citrix ADC, el recuento de SR aumenta en lugar del recuento de conmutación por error en Citrix ADM.

[CGOP-13511]

Al aceptar conexiones de host local desde el explorador web, el cuadro de diálogo **Aceptar conexión** para macOS muestra el contenido en inglés independientemente del idioma seleccionado.

[CGOP-13050]

El texto `Home Page` de la **aplicación Citrix SSO > Página de inicio** se corta para algunos idiomas.

[CGOP-13049]

Aparece un mensaje de error al agregar o modificar una directiva de sesión desde la GUI de Citrix ADC.

[CGOP-11830]

En Outlook Web App (OWA) 2013, al hacer clic en **Opciones** en el menú **Configuración**, se muestra un cuadro de diálogo **Error crítico**. Además, la página deja de responder.

[CGOP-7269]

En una implementación de clúster, si ejecuta un comando `force cluster sync` en un nodo que no es de CCO, el archivo ns.log contiene entradas de registro duplicadas.

[CGOP-6794]

Citrix Web App Firewall

El ID de firma de Web App Firewall 1048 bloquea la carga de la página de Citrix Gateway.

[NSHELP-29113]

Equilibrio de carga

En una configuración de alta disponibilidad, es posible que las sesiones de suscriptor del nodo principal no se sincronicen con el nodo secundario. Este es un caso raro.

[NSLB-7679]

El grupo de servicios GSLB no puede gestionar las actualizaciones del monitor debido a la falta de un valor ENUM en los comandos fallidos.

[NSHELP-29050]

Es posible que el dispositivo Citrix ADC no responda a una consulta de dominio GSLB con una dirección IP de servicio GSLB esperada, si el servidor virtual GSLB se configura de la siguiente manera:
Tipo de persistencia: Dirección IP de origen
Algoritmo de equilibrio de carga: Proximidad estática
Método de equilibrio de carga de seguridad: Tiempo de ida y vuelta (RTT)

[NSHELP-28668]

Los sitios VPX principal y secundario se bloquearon tras configurar el grupo de servicios GSLB con Autoscale habilitado.

Solución alternativa:
No agregue los servidores virtuales ficticio, como el servidor virtual de conmutación de contenido, al agregar un servicio GSLB o vincular un puerto IP a un grupo de servicios GSLB.

[NSHELP-28530]

Un dispositivo Citrix ADC en una configuración de alta disponibilidad pierde conectividad porque la memoria NSB no se libera después de enviar la respuesta HTTP durante la supervisión de la sonda HTTP.

[NSHELP-28466]

El formato serviceGroupName de la captura `entityofs` del grupo de servicios es el siguiente: `<service(group)name>?<ip/DBS>?<port>`

En el formato de captura, el grupo de servicios se identifica mediante una dirección IP o un nombre y puerto de DBS. El signo de interrogación (?) se utiliza como separador. Citrix ADC envía la captura con el signo de interrogación (?). El formato aparece igual en la GUI de Citrix ADM. Este es el comportamiento esperado.

[NSHELP-28080]

Otros

Cuando se produce una sincronización forzada en una configuración de alta disponibilidad, el dispositivo ejecuta el comando `set urlfiltering parameter` en el nodo secundario.
Como resultado, el nodo secundario omite cualquier actualización programada hasta la siguiente hora programada mencionada en el parámetro `TimeOfDayToUpdateDB`.

[NSSWG-849]

La coincidencia del patrón del conjunto de URL falla para los dominios estándar IDNA2008.

[NSHELP-28902]

Cuando el reenvío basado en Mac (MBF) está habilitado para VXLAN, no se establecía la sesión TCP con estado.

[NSHELP-27125]

Un dispositivo Citrix ADC puede reiniciarse debido al estancamiento de la CPU de administración si se produce un problema de conectividad con el proveedor externo de filtrado de URL.

[NSHELP-22409]

Redes

Un dispositivo Citrix ADC BLX en modo DPDK podría bloquearse si se configura un perfil de Firewall de aplicaciones web con comprobaciones de protección de seguridad avanzadas.

Solución temporal:

Elimine la configuración de protección de seguridad avanzada para WAF.

[NSNET-22654]

Tras una actualización de la versión 13.0 61.x del dispositivo Citrix ADC BLX a la versión 13.0 64.x, se pierde la configuración del archivo de configuración BLX. El archivo de configuración de BLX se restablece a los valores predeterminados.

[NSNET-17625]

Las siguientes operaciones de interfaz no son compatibles con las interfaces `X710 10G (i40e)` de Intel en un dispositivo Citrix ADC BLX con DPDK:

- Disable
- Enable
- Reset

[NSNET-16559]

En un host Linux basado en Debian (Ubuntu versión 18 y posteriores), un dispositivo Citrix ADC BLX siempre se implementa en modo compartido independientemente de la configuración del archivo de configuración BLX()`/etc/blx/blx.conf`. Este problema se produce porque `mawk`, que está presente de forma predeterminada en los sistemas Linux basados en Debian, no ejecuta algunos de los comandos `awk` presentes en el archivo `blx.conf`.

Solución temporal:

Instale `gawk` antes de instalar un dispositivo Citrix ADC BLX. Puede ejecutar el siguiente comando en la CLI del host de Linux para instalar `gawk`:

- apt-get install gawk

[NSNET-14603]

La instalación de un dispositivo Citrix ADC BLX podría fallar en un host Linux basado en Debian (versión 18 y posteriores de Ubuntu) con el siguiente error de dependencia:

```
The following packages have unmet dependencies: blx-core-libs:i386 :
PreDepends: libc6:i386 (>= 2.19)but it is not installable
```

Solución temporal:

Ejecute los siguientes comandos en la CLI del host Linux antes de instalar un dispositivo Citrix ADC BLX:


```
- dpkg --add-architecture i386
- apt-get update
- apt-get dist-upgrade
- apt-get install libc6:i386
<!--NeedCopy-->
```

[NSNET-14602]

En algunos casos de conexiones de datos FTP, el dispositivo Citrix ADC solo realiza operaciones NAT y no procesamiento TCP en los paquetes para la negociación TCP MSS. Como resultado, la MTU de interfaz óptima no está configurada para la conexión. Esta configuración de MTU incorrecta provoca la fragmentación de los paquetes y afecta al rendimiento de la CPU.

[NSNET-5233]

En una implementación NAT a gran escala de dos dispositivos Citrix ADC en una configuración de alta disponibilidad, es posible que IPsec ALG no funcione correctamente si la configuración de alta disponibilidad tiene la opción `stayprimary` o `staysecondary` configurada.

[NSNET-1646]

Cuando se cambia el límite de memoria de una partición de administración en el dispositivo Citrix ADC, el límite de memoria de almacenamiento en búfer TCP se establece automáticamente en el nuevo límite de memoria de la partición de administración.

[NSHELP-21082]

En una configuración de alta disponibilidad (HA), si se inhabilita ARP gratuito (GARP), es posible que el enrutador de subida no dirija el tráfico al nuevo primario tras una conmutación por error de alta disponibilidad.

[NSHELP-20796]

Plataforma

Cuando actualiza de compilaciones 13.0/12.1/11.1 a una versión 13.1 o baja de una compilación 13.1 a 13.0/12.1/11.1, algunos paquetes python no se instalan en los dispositivos Citrix ADC. Este problema se ha solucionado en las siguientes versiones de Citrix ADC:

- 13.1-4.x
- 13.0—82.31 y posteriores
- 12.1—62.21 y posteriores

Los paquetes python no se instalan cuando se degrada la versión de Citrix ADC de la versión 13.1-4.x a cualquiera de las siguientes versiones:

- Cualquier compilación 11.1
- 12.1-62.21 y anteriores
- 13.0-81.x y anteriores

[NSPLAT-21691]

El aprovisionamiento de una instancia VPX con la versión 12.0 XVA falla en un dispositivo Citrix ADC SDX que ejecuta la versión 13.1.

Solo se admiten las versiones 12.1 y posteriores de VPX. Actualice la versión VPX antes de actualizar el SBI a la versión 13.1.

[NSPLAT-21442]

Al eliminar una configuración de escalabilidad automática o un conjunto de escalas de VM de un grupo de recursos de Azure, elimine la configuración del perfil de nube correspondiente de la instancia de Citrix ADC. Utilice el comando `rm cloudprofile` para borrar el perfil.

[NSPLAT-4520]

En una configuración de alta disponibilidad en Azure, al iniciar sesión en el nodo secundario a través de la GUI, aparece la pantalla de usuario por primera vez (FTU) para la configuración del perfil de nube de escalabilidad automática.
Solución alternativa: omita la pantalla e inicie sesión en el nodo principal para crear el perfil de nube. El perfil de la nube siempre debe configurarse en el nodo principal.

[NSPLAT-4451]

Las instancias de Citrix ADC VPX que usan el controlador VMXNET3 pueden bloquearse de forma aleatoria si la instancia se ejecuta en una de las siguientes compilaciones de Citrix ADC:

- Citrix ADC 13.1 compilación 4.x
- Citrix ADC 13.1 compilación 9.x

[NSHELP-29120]

Directivas

Las conexiones pueden bloquearse si el tamaño de los datos de procesamiento es mayor que el tamaño de búfer TCP predeterminado configurado.Solución alternativa: establezca el tamaño del búfer TCP en un tamaño máximo de datos que deben procesarse.

[NSPOLICY-1267]

SSL

En un clúster heterogéneo de dispositivos Citrix ADC SDX 22000 y Citrix ADC SDX 26000, se produce una pérdida de configuración de entidades SSL si se reinicia el dispositivo SDX 26000.

Solución temporal:

1. En el CLIP, inhabilite SSLv3 en todas las entidades SSL nuevas y existentes, como servidores virtuales, servicios, grupos de servicios y servicios internos. Por ejemplo, `set ssl vserver <name> -SSL3 DISABLED`.
2. Guarde la configuración.

[NSSSL-9572]

El comando Actualizar no está disponible para los siguientes comandos de adición:

```
- add azure application
- add azure keyvault
- add ssl certkey with hsmkey option
<!--NeedCopy-->
```

[NSSSL-6484]

No se puede agregar un objeto de Azure Key Vault si ya se ha agregado un objeto de autenticación de Azure Key Vault.

[NSSSL-6478]

Puede crear varias entidades de la aplicación Azure con el mismo ID de cliente y secreto de cliente. El dispositivo Citrix ADC no devuelve ningún error.

[NSSSL-6213]

El siguiente mensaje de error incorrecto aparece al eliminar una clave HSM sin especificar `KEYVAULT` como el tipo de HSM.
ERROR: `crl refresh disabled`

[NSSSL-6106]

La actualización automática de claves de sesión aparece incorrectamente como inhabilitada en una dirección IP de clúster. (Esta opción no se puede desactivar).

[NSSSL-4427]

Aparece `Warning: No usable ciphers configured on the SSL vserver/service,,` un mensaje de advertencia incorrecto, si intenta cambiar el protocolo o el cifrado SSL en el perfil SSL.

[NSSSL-4001]

Un tíquet de sesión caducado se respeta en un nodo que no es de CCO y en un nodo de alta disponibilidad después de una conmutación por error de alta disponibilidad.

[NSSSL-3184]

Un dispositivo Citrix ADC se bloquea al procesar una solicitud HTTP si la acción de directiva se establece en `Forward` para una directiva que ya está enlazada en el punto de enlace de la solicitud.

[NSHELP-29115]

Sistema

Se observa una fuga en la ventana TCP cuando un dispositivo Citrix ADC procesa tramas de encabezado HTTP/2.

[NSHELP-28475]

Cuando un cliente restablece una conexión con varios flujos TCP, no se envía el registro de transacciones del lado del servidor, lo que hace que falten registros L4 para esos flujos de datos.

[NSHELP-28281]

En una configuración de clúster, el comando `set ratecontrol` solo funciona después de reiniciar el dispositivo Citrix ADC.

Solución temporal:

Use el comando `nsapimgr_wr.sh -ys icmp_rate_threshold=<new value>`.

[NSHELP-21811]

El valor MAX_CONCURRENT_STREAMS se establece en 100 de forma predeterminada si el dispositivo no recibe el marco de configuración max_concurrent_stream del cliente.

[NSHELP-21240]

Los contadores mptcp_cur_session_without_subflow disminuyen incorrectamente a un valor negativo en lugar de cero.

[NSHELP-10972]

La IP del cliente y la IP del servidor se invierten en el registro HDX Insight SkipFlow cuando el tipo de transporte de LogStream está configurado para Insight.

[NSBASE-8506]

Interfaz de usuario

En la GUI de Citrix ADC, el enlace `Help` presente debajo de la ficha `Dashboard` no funciona.

[NSUI-14752]

El asistente Crear/Supervisar CloudBridge Connector podría dejar de responder o no configurar un conector de cloudbridge.

Solución temporal:

Configure los conectores cloudbridge agregando perfiles IPsec, túneles IP y reglas PBR mediante la GUI o CLI de Citrix ADC.

[NSUI-13024]

Si crea una clave ECDSA mediante la interfaz gráfica de usuario, no se muestra el tipo de curva.

[NSUI-6838]

Se observa el siguiente problema si se realiza alguna operación que lee el archivo `ns.conf`. Por ejemplo, `show ns saved config`.

- El proceso HTTPD puede congelarse y provocar que la GUI y la API de NITRO se vuelvan inaccesibles.

[NSHELP-28249]

En una configuración de alta disponibilidad, las sesiones de usuario VPN se desconectan si se cumple la siguiente condición:

- Si se realizan dos o más operaciones de failover manual de alta disponibilidad sucesivas cuando la sincronización de alta disponibilidad está en curso.

Solución temporal:

Realice una conmutación por error manual de alta disponibilidad sucesiva solo después de que se haya completado la sincronización de alta disponibilidad (ambos nodos están en estado de sincronización correcta).

[NSHELP-25598]

La carga y adición de un archivo de lista de revocación de certificados (CRL) produce un error en la configuración de una partición de administración.

[NSHELP-20988]

Al revertir la versión 13.0-71.x de un dispositivo Citrix ADC a una versión anterior, es posible que algunas API de NITRO no funcionen debido a los cambios en los permisos de archivo.

Solución temporal:

Cambie el permiso de `/nsconfig/ns.conf` a 644.

[NSCONFIG-4628]

Si usted (administrador del sistema) realiza todos los pasos siguientes en un dispositivo Citrix ADC, es posible que los usuarios del sistema no inicien sesión en el dispositivo Citrix ADC degradado.

1. Actualice el dispositivo Citrix ADC a una de las compilaciones:
    - 13.0 52.24 compilación
    - 12.1 57,18 compilación

- 11.1 65.10 compilación

2. Agregar un usuario del sistema o cambiar la contraseña de un usuario del sistema existente y guardar la configuración, y
3. Rebaja la versión del dispositivo Citrix ADC a cualquier versión anterior.

Para mostrar la lista de estos usuarios del sistema mediante la CLI:
En el símbolo del sistema, escriba:

```
query ns config -changedpassword [-config <full path of the configuration file (ns.conf)>]
```

Solución temporal:

Para solucionar este problema, utilice una de las siguientes opciones independientes:

- Si el dispositivo Citrix ADC aún no se ha degradado (paso 3 de los pasos mencionados anteriormente), degrade el dispositivo Citrix ADC mediante un archivo de configuración del que se realizó una copia de reserva (ns.conf) de la misma versión.
- Cualquier administrador del sistema cuya contraseña no se haya cambiado en la compilación actualizada puede iniciar sesión en la compilación degradada y actualizar las contraseñas de otros usuarios del sistema.
- Si ninguna de las opciones anteriores funciona, el administrador del sistema puede restablecer las contraseñas de usuario del sistema.

Para obtener más información, consulte Cómo restablecer la contraseña del administrador raíz.

[NSCONFIG-3188]

Cualquiera de las siguientes operaciones de actualización de Citrix ADC puede provocar un error de inicio de sesión en las cuentas de usuario del sistema local:

- desde la compilación de Citrix ADC 13.0-83.x a la compilación de Citrix ADC 13.1-4.x
- desde la compilación 12.1-63.x de Citrix ADC a la compilación 13.1-4.x de Citrix ADC
- desde la compilación de Citrix ADC 12.1-63.x a la compilación de Citrix ADC 13.0-82.x

Este problema solo se observa en las cuentas de usuario del sistema local que cumplen alguna de las siguientes condiciones:

- la contraseña de usuario se cambió para la cuenta del sistema local en la compilación de Citrix ADC (13.0-83.x o 12.1-63.x) antes de realizar la operación de actualización.
- la cuenta de usuario del sistema local se agregó en la compilación de Citrix ADC (13.0-83.x o 12.1-63.x) antes de realizar la operación de actualización.

Solución temporal:

Un administrador del sistema puede restablecer la contraseña de las cuentas de usuario del sistema local que enfrentan el problema de error de inicio de sesión.

Para obtener más información, consulte Cómo restablecer la contraseña del administrador raíz.

[NSCONFIG-5650]

Cómo empezar con Citrix ADC

July 8, 2022

En este tema se describen las funciones básicas y los detalles de configuración de un dispositivo Citrix ADC. Los administradores de sistemas y redes que instalan y configuran los equipos de red pueden consultar el contenido.

Comprensión de Citrix ADC

El dispositivo Citrix ADC es un conmutador de aplicación que realiza análisis de tráfico específico de la aplicación para distribuir, optimizar y proteger de manera inteligente el tráfico de red de capa 4 y capa 7 (L4 a L7) para aplicaciones web. Por ejemplo, la carga de un dispositivo Citrix ADC equilibra las decisiones sobre solicitudes HTTP individuales en lugar de conexiones TCP de larga duración. La función de equilibrio de carga ayuda a ralentizar la falla de un servidor con menos interrupciones para los clientes. Las funciones del ADC se pueden clasificar en términos generales como:

1. Conmutación de datos
2. Seguridad de firewall
3. Optimización
4. Infraestructura
5. Flujo de paquetes
6. Limitación del sistema

Conmutación de datos

Cuando se implementa frente a los servidores de aplicaciones, un Citrix ADC garantiza una distribución óptima del tráfico mediante la forma en que dirige las solicitudes de los clientes. Los administradores pueden segmentar el tráfico de aplicaciones en función de la información en el cuerpo de una solicitud HTTP o TCP y en función de la información del encabezado de nivel 4 a 7, como la URL, el tipo de datos de la aplicación o la cookie. Numerosos algoritmos de equilibrio de carga y amplias comprobaciones de estado del servidor mejoran la disponibilidad de las aplicaciones al garantizar que las solicitudes de los clientes se dirijan a los servidores apropiados.

Seguridad de firewall

La seguridad y la protección de Citrix ADC protegen las aplicaciones web de los ataques de la capa de aplicaciones. Un dispositivo ADC permite solicitudes de clientes legítimas y puede bloquear solicitudes maliciosas. Proporciona defensas integradas contra los ataques de denegación de servicio (DoS) y admite funciones que protegen contra aumentos repentinos legítimos en el tráfico de aplicaciones que de otro modo abrumaría a los servidores. Un firewall integrado disponible protege las aplicaciones web de los ataques de la capa de aplicación, incluidos los ataques de desbordamiento de búfer, los intentos de inyección de SQL, los ataques de scripts entre sitios y más. Además, el firewall proporciona protección contra el robo de identidad al proteger la información corporativa confidencial y los datos confidenciales de los clientes.

Optimización

La optimización descarga las operaciones que consumen muchos recursos, como el procesamiento de Secure Sockets Layer (SSL), la compresión de datos, el mantenimiento activo del cliente, el almacenamiento en búfer TCP y el almacenamiento en caché de contenido estático y dinámico de los servidores. Esto mejora el rendimiento de los servidores en la comunidad de servidores y, por lo tanto, acelera las aplicaciones. Un dispositivo ADC admite varias optimizaciones TCP transparentes que mitigan los problemas causados por la alta latencia y los enlaces de red congestionados. De este modo, se acelera la entrega de aplicaciones sin requerir cambios de configuración en los clientes o servidores.

Infraestructura

Una directiva define detalles específicos del filtrado y la administración del tráfico en un Citrix ADC. Consta de dos partes: la expresión y la acción. La expresión define los tipos de solicitudes con las que coincide la directiva. La acción indica al dispositivo ADC qué debe hacer cuando una solicitud coincide con la expresión. Por ejemplo, la expresión podría coincidir con un patrón de URL específico para un ataque de seguridad con la configuración para eliminar o restablecer la conexión. Cada directiva tiene una prioridad y las prioridades determinan el orden en que se evalúan las directivas.

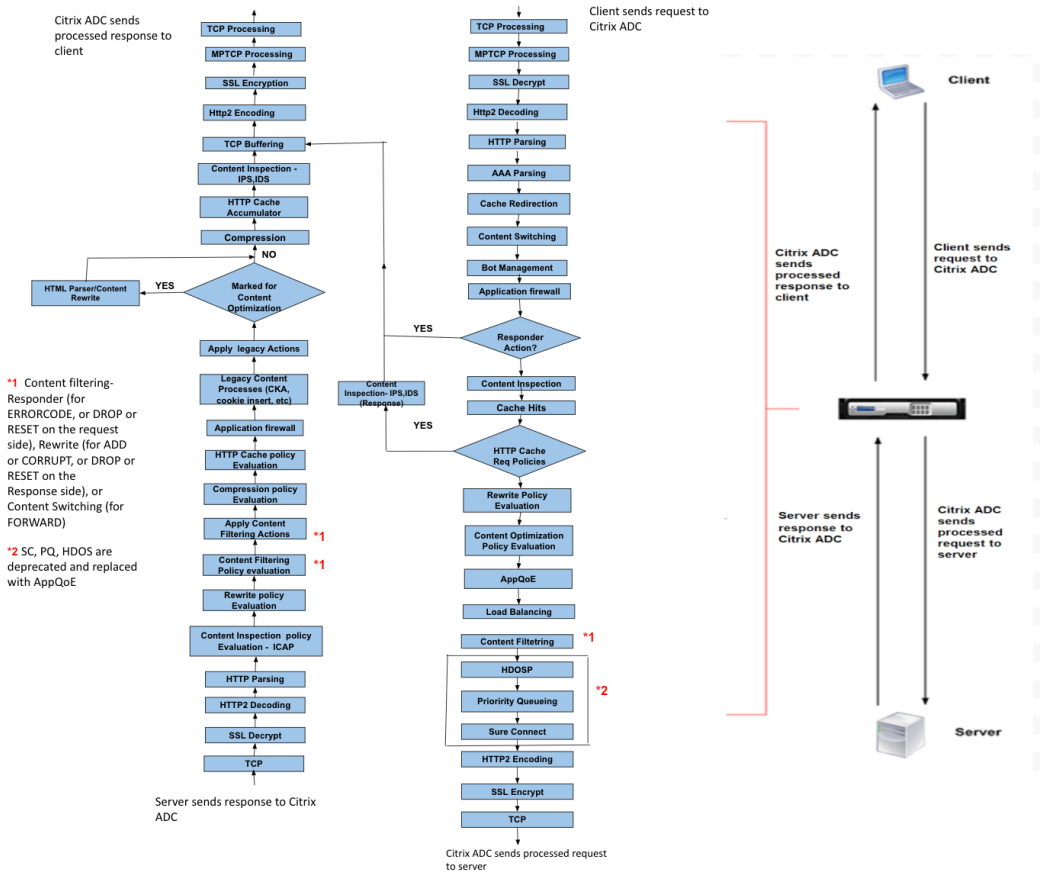
Cuando un dispositivo ADC recibe tráfico, la lista de directivas apropiada determina cómo procesar el tráfico. Cada directiva de la lista contiene una o más expresiones, que juntas definen los criterios que debe cumplir una conexión para que coincida con la directiva.

Para todos los tipos de directivas, excepto la reescritura, el dispositivo implementa solo la primera directiva que tiene una coincidencia de solicitud. Para las directivas de reescritura, el dispositivo ADC evalúa las directivas en orden y realiza las acciones asociadas en el mismo orden. La prioridad de las directivas es importante para obtener los resultados que quiere.

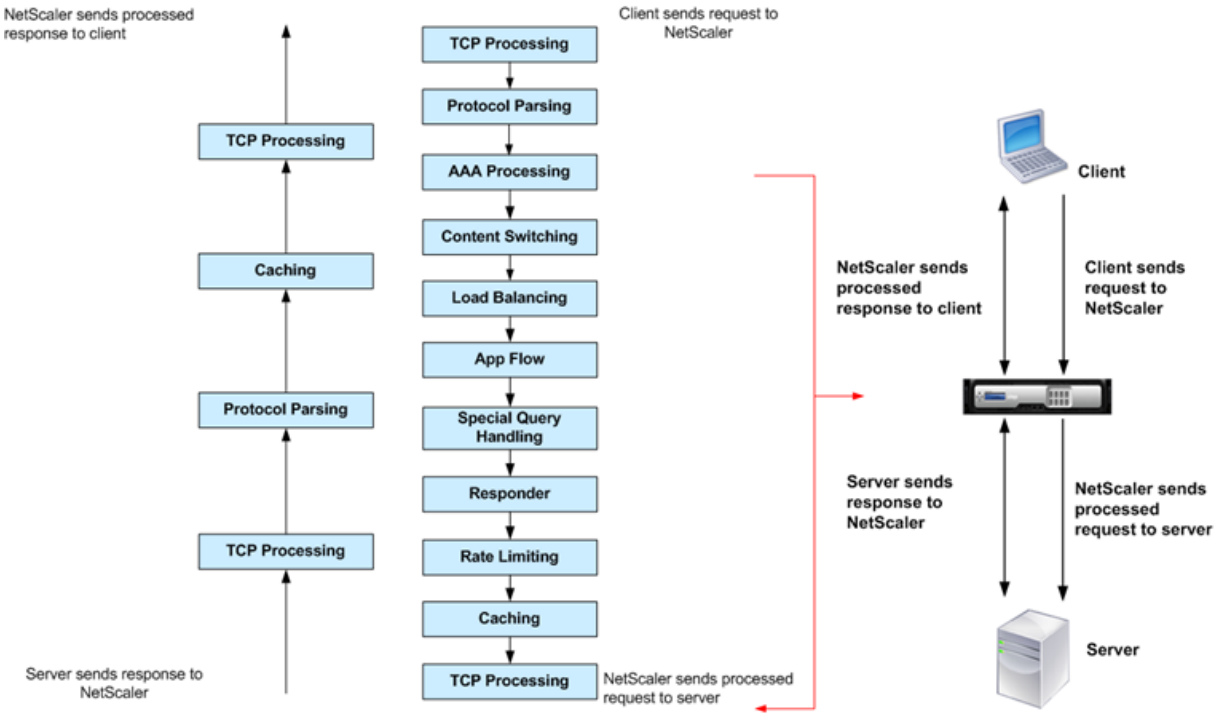
Flujo de paquetes

En función de los requisitos, puede elegir configurar varias funciones. Por ejemplo, puede elegir configurar tanto la compresión como la descarga SSL. Como resultado, un paquete saliente puede comprimirse y luego cifrarse antes de enviarse al cliente.

En la siguiente ilustración se muestra el flujo de paquetes HTTP2 en el dispositivo Citrix ADC.



En la siguiente ilustración se muestra el flujo de procesamiento de consultas de flujo de datos en el dispositivo Citrix ADC. DataStream es compatible con bases de datos MySQL y MS SQL. Para obtener información sobre la función DataStream, consulte DataStream.



> **Nota:** Si el tráfico es para un servidor virtual de conmutación de contenido, el dispositivo evalúa las directivas en el siguiente orden:
>
> 1. vinculado a la anulación global.
> 2. vinculado al servidor virtual de equilibrio de carga.
> 3. vinculado al servidor virtual de conmutación de contenido.
> 4. vinculado al valor predeterminado global.
>
> De esta manera, si una regla de directiva es verdadera y gotopriorityexpression es END, detendremos una mayor evaluación de la directiva.
> En la conmutación de contenido, si no se selecciona ningún servidor virtual de equilibrio de carga o se enlaza al servidor virtual de conmutación de contenido, evaluamos las directivas de respuesta vinculadas solo al servidor virtual de conmutación de contenido.

Limitación del sistema

Existen limitaciones del sistema para cada función de Citrix ADC al instalar el software Citrix ADC 9.2 o posterior. Para obtener más información, consulte el artículo de Citrix, CTX118716.

¿Dónde cabe un dispositivo Citrix ADC en la red?

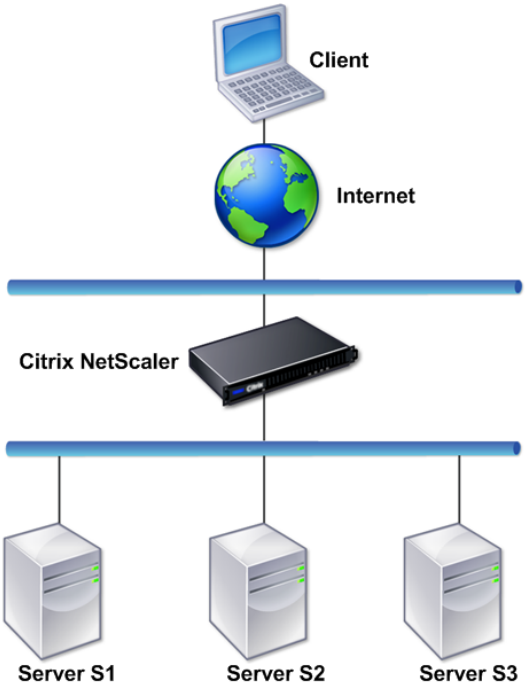
August 20, 2021

Un dispositivo Citrix ADC reside entre los clientes y los servidores, de modo que las solicitudes del cliente y las respuestas del servidor pasan a través de él. En una instalación típica, los servidores virtuales configurados en el dispositivo proporcionan puntos de conexión que los clientes utilizan para acceder a las aplicaciones detrás del dispositivo. En este caso, el dispositivo posee direcciones IP públicas asociadas a sus servidores virtuales, mientras que los servidores reales están aislados en una red privada. También es posible operar el dispositivo en modo transparente como un puente L2 o enrutador L3, o incluso combinar aspectos de estos y otros modos.

Modos de implementación física

Un dispositivo Citrix ADC que reside lógicamente entre clientes y servidores se puede implementar en cualquiera de los dos modos físicos: En línea y en un brazo. En el modo en línea, se conectan varias interfaces de red a diferentes segmentos Ethernet y el dispositivo se coloca entre los clientes y los servidores. El dispositivo tiene una interfaz de red independiente para cada red cliente y una interfaz de red independiente para cada red de servidor. El dispositivo y los servidores pueden existir en diferentes subredes en esta configuración. Es posible que los servidores estén en una red pública y que los clientes accedan directamente a los servidores a través del dispositivo, con la aplicación transparente de las funciones L4-L7. Normalmente, los servidores virtuales (descritos más adelante) se configuran para proporcionar una abstracción de los servidores reales. La siguiente ilustración muestra una implementación en línea típica.

Ilustración 1. Implementación en línea



En el modo de un brazo, solo se conecta una interfaz de red del dispositivo a un segmento Ethernet. En este caso, el dispositivo no aísla los lados cliente y servidor de la red, sino que proporciona acceso a las aplicaciones a través de servidores virtuales configurados. El modo de un brazo puede simplificar los cambios de red necesarios para la instalación de Citrix ADC en algunos entornos.

Para ver ejemplos de implementación en línea (de dos brazos) y de un brazo, consulte Descripción de las topologías de red comunes.

Citrix ADC como dispositivo L2

Se dice que un dispositivo Citrix ADC que funciona como dispositivo L2 funciona en modo L2. En el modo L2, el dispositivo ADC reenvía paquetes entre interfaces de red cuando se cumplen todas las condiciones siguientes:

- Los paquetes están destinados a la dirección MAC (Media Access Control) de otro dispositivo.
- La dirección MAC de destino se encuentra en una interfaz de red diferente.
- La interfaz de red es miembro de la misma LAN virtual (VLAN).

De forma predeterminada, todas las interfaces de red son miembros de una VLAN predefinida, VLAN 1. Las solicitudes y respuestas del Protocolo de resolución de direcciones (ARP) se reenvían a todas las

interfaces de red que son miembros de la misma VLAN. Para evitar la conexión de bucles en puente, el modo L2 debe inhabilitarse si otro dispositivo L2 funciona en paralelo con el dispositivo Citrix ADC.

Para obtener información sobre cómo interactúan los modos L2 y L3, consulte Modos de reenvío de paquetes.

Para obtener información sobre cómo configurar el modo L2, consulte la sección “Habilitar y inhabilitar el modo de capa 2” en los modos de reenvío de paquetes.

Citrix ADC como dispositivo de reenvío de paquetes

Un dispositivo Citrix ADC puede funcionar como dispositivo de reenvío de paquetes, y este modo de operación se denomina modo L3. Con el modo L3 habilitado, el dispositivo reenvía los paquetes de unidifusión recibidos destinados a una dirección IP que no pertenece al dispositivo, si hay una ruta al destino. El dispositivo también puede enrutar paquetes entre VLAN.

En ambos modos de operación, L2 y L3, el dispositivo generalmente descarta paquetes que se encuentran en:

- Marcos de multidifusión
- Marcos de protocolo desconocidos destinados a la dirección MAC de un dispositivo (no IP y no ARP)
- Protocolo de árbol de expansión (a menos que BridgeBPDU esté activado)

Para obtener información sobre cómo interactúan los modos L2 y L3, consulte Modos de reenvío de paquetes.

Para obtener información sobre cómo configurar el modo L3, consulte Modos de reenvío de paquetes.

Cómo se comunica un dispositivo Citrix ADC con clientes y servidores

August 20, 2021

Normalmente, un dispositivo Citrix ADC se implementa frente a una comunidad de servidores y funciona como un proxy TCP transparente entre clientes y servidores, sin necesidad de ninguna configuración del lado del cliente. Este modo básico de operación se denomina tecnología de conmutación de solicitudes y es el núcleo de la funcionalidad de Citrix ADC. La conmutación de solicitudes permite a un dispositivo multiplexar y descargar las conexiones TCP, mantener las conexiones persistentes y administrar el tráfico en el nivel de solicitud (capa de aplicación). Esto es posible porque el dispositivo puede separar la solicitud HTTP de la conexión TCP en la que se entrega la solicitud.

Según la configuración, es posible que el dispositivo procese el tráfico antes de reenviar la solicitud a un servidor. Por ejemplo, si el cliente intenta obtener acceso a una aplicación segura en el servidor, el dispositivo puede realizar el procesamiento SSL necesario antes de enviar tráfico al servidor.

Para facilitar el acceso eficaz y seguro a los recursos del servidor, un dispositivo utiliza un conjunto de direcciones IP conocidas colectivamente como direcciones IP propiedad de Citrix ADC. Para administrar el tráfico de red, debe asignar direcciones IP propiedad de Citrix ADC a entidades virtuales que se convierten en los bloques de creación de la configuración. Por ejemplo, para configurar el equilibrio de carga, debe crear servidores virtuales para recibir solicitudes de cliente y distribuirlas a los servicios, que son entidades que representan las aplicaciones de los servidores.

Descripción de las direcciones IP propiedad de Citrix ADC

Para funcionar como proxy, un dispositivo Citrix ADC utiliza una variedad de direcciones IP. Las direcciones IP clave propiedad de Citrix ADC son:

- Dirección IP deCitrix ADC (NSIP)

  La dirección NSIP es la dirección IP para la administración y el acceso general al sistema al propio dispositivo, y para la comunicación entre dispositivos en una configuración de alta disponibilidad.

- Dirección IP (VIP) del servidorvirtual

  Una dirección VIP es la dirección IP asociada a un servidor virtual. Es la dirección IP pública a la que se conectan los clientes. Un dispositivo que administra un amplio rango de tráfico puede tener varias direcciones IP virtuales configuradas.

- Dirección IP de subred (SNIP)

  Se utiliza una dirección SNIP en la administración de conexiones y la supervisión del servidor. Puede especificar varias direcciones SNIP para cada subred. Las direcciones SNIP se pueden enlazar a una VLAN.

- Conjunto deIP

  Un conjunto de IP es un conjunto de direcciones IP, que se configuran en el dispositivo como SNIP. Un conjunto de IP se identifica con un nombre significativo que ayuda a identificar el uso de las direcciones IP contenidas en él.

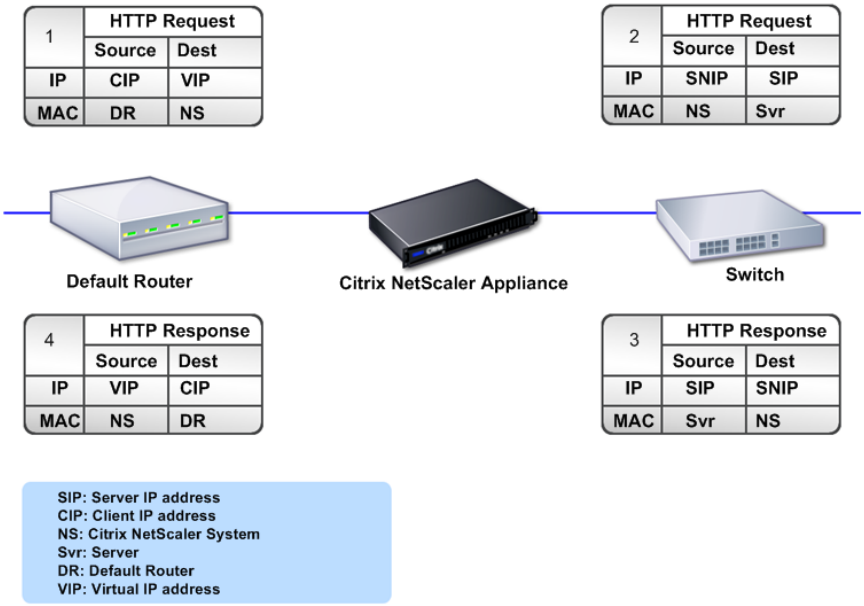
- Perfil de red

  Un perfil de red (o perfil de red) contiene una dirección IP o un conjunto de IP. Un perfil de red puede vincularse al equilibrio de carga o al cambio de contenido de servidores virtuales, servicios, grupos de servicios o monitores. Durante la comunicación con servidores físicos o compañeros, el dispositivo utiliza las direcciones especificadas en el perfil como direcciones IP de origen.

Cómo se administran los flujos de tráfico

Dado que un dispositivo Citrix ADC funciona como un proxy TCP, traduce las direcciones IP antes de enviar paquetes a un servidor. Cuando configura un servidor virtual, los clientes se conectan a una dirección VIP en el dispositivo Citrix ADC en lugar de conectarse directamente a un servidor. Según lo determinado por la configuración del servidor virtual, el dispositivo selecciona un servidor adecuado y envía la solicitud del cliente a ese servidor. De forma predeterminada, el dispositivo utiliza una dirección SNIP para establecer conexiones con el servidor, como se muestra en la ilustración siguiente.

Ilustración 1. Conexiones basadas en servidores virtuales



En ausencia de un servidor virtual, cuando un dispositivo recibe una solicitud, reenvía la solicitud de forma transparente al servidor. Esto se llama el modo transparente de operación. Cuando funciona en modo transparente, un dispositivo traduce las direcciones IP de origen de las solicitudes de cliente entrantes a la dirección SNIP, pero no cambia la dirección IP de destino. Para que este modo funcione, el modo L2 o L3 debe configurarse adecuadamente.

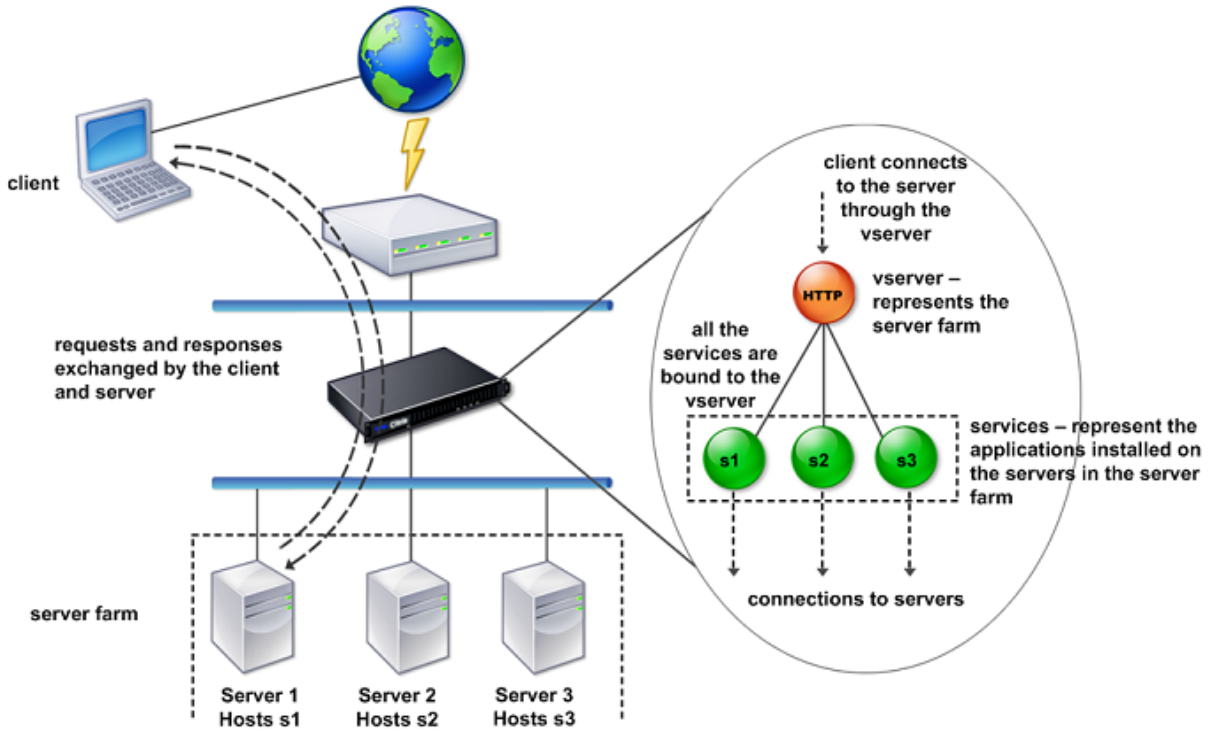
En los casos en que los servidores necesitan la dirección IP del cliente real, el dispositivo puede configurarse para modificar el encabezado HTTP insertando la dirección IP del cliente como un campo adicional o configurado para usar la dirección IP del cliente en lugar de una dirección SNIP para las conexiones a los servidores.

Bloques de construcción de la gestión del tráfico

La configuración de un dispositivo Citrix ADC se genera normalmente con una serie de entidades virtuales que sirven como bloques de creación para la administración del tráfico. El enfoque de bloques de construcción ayuda a separar los flujos de tráfico. Las entidades virtuales son abstracciones, que normalmente representan direcciones IP, puertos y controladores de protocolo para procesar el tráfico. Los clientes acceden a aplicaciones y recursos a través de estas entidades virtuales. Las entidades más utilizadas son servidores y servicios virtuales. Los servidores virtuales representan grupos de servidores en una comunidad de servidores o una red remota, y los servicios representan aplicaciones específicas en cada servidor.

La mayoría de las funciones y configuraciones de tráfico se habilitan a través de entidades virtuales. Por ejemplo, puede configurar un dispositivo para comprimir todas las respuestas del servidor a un cliente conectado al conjunto de servidores a través de un servidor virtual determinado. Para configurar el dispositivo para un entorno concreto, debe identificar las funciones adecuadas y, a continuación, elegir la combinación adecuada de entidades virtuales para entregarlas. La mayoría de las entidades se entregan a través de una cascada de entidades virtuales enlazadas entre sí. En este caso, las entidades virtuales son como bloques que se ensamblan en la estructura final de una aplicación entregada. Puede agregar, quitar, modificar, enlazar, habilitar e inhabilitar las entidades virtuales para configurar las entidades. En la siguiente ilustración se muestran los conceptos tratados en esta sección.

Ilustración 2. Cómo funcionan los bloques de construcción de la gestión del tráfico

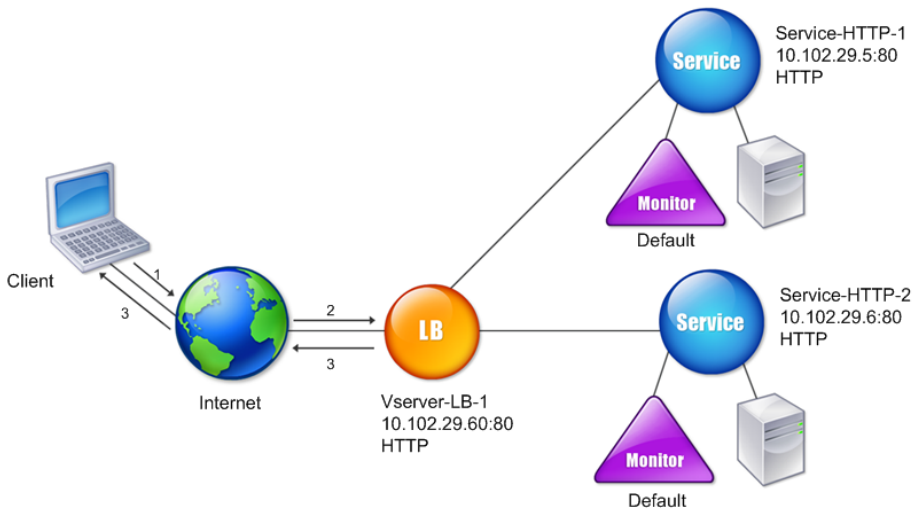


Una configuración simple de equilibrio de carga

En el ejemplo que se muestra en la siguiente ilustración, el dispositivo Citrix ADC está configurado para funcionar como equilibrador de carga. Para esta configuración, debe configurar entidades virtuales específicas para el equilibrio de carga y vincularlas en un orden específico. Como equilibrador de carga, un dispositivo distribuye las solicitudes de cliente entre varios servidores y, por lo tanto, optimiza la utilización de los recursos.

Los componentes básicos de una configuración típica de equilibrio de carga son los servicios y los servidores virtuales de equilibrio de carga. Los servicios representan a las aplicaciones en los servidores. Los servidores virtuales abstraen los servidores proporcionando una única dirección IP a la que se conectan los clientes. Para asegurarse de que las solicitudes de cliente se envían a un servidor, debe vincular cada servicio a un servidor virtual. Es decir, debe crear servicios para cada servidor y enlazar los servicios a un servidor virtual. Los clientes utilizan la dirección VIP para conectarse a un dispositivo Citrix ADC. Cuando el dispositivo recibe solicitudes de cliente enviadas a la dirección VIP, las envía a un servidor determinado por el algoritmo de equilibrio de carga. El equilibrio de carga utiliza una entidad virtual denominada monitor para realizar un seguimiento de si un servicio configurado específico (servidor más aplicación) está disponible para recibir solicitudes.

Ilustración 3. Servidor virtual, servicios y monitores de equilibrio de carga



Además de configurar el algoritmo de equilibrio de carga, puede configurar varios parámetros que afectan el comportamiento y el rendimiento de la configuración de equilibrio de carga. Por ejemplo, puede configurar el servidor virtual para mantener la persistencia en función de la dirección IP de origen. A continuación, el dispositivo dirige todas las solicitudes de cualquier dirección IP específica al mismo servidor.

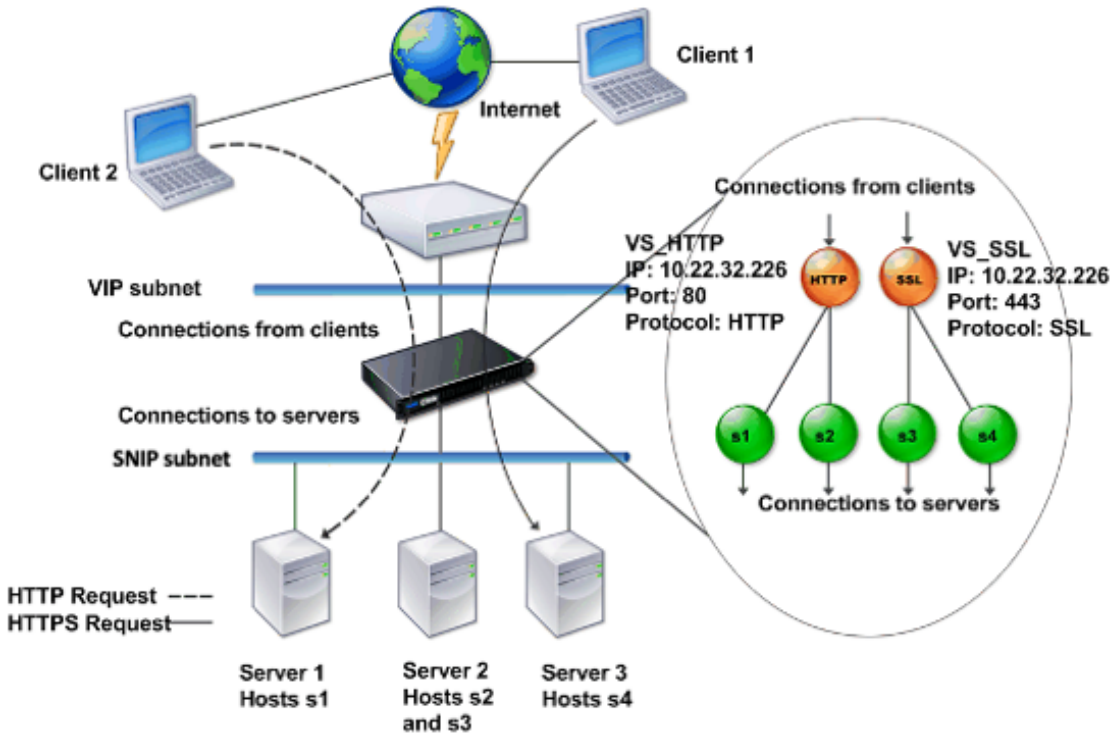
Descripción de los servidores virtuales

Un servidor virtual es una entidad Citrix ADC denominada que los clientes externos pueden usar para acceder a aplicaciones alojadas en los servidores. Se representa mediante un nombre alfanumérico, una dirección IP virtual (VIP), un puerto y un protocolo. El nombre del servidor virtual es solo de importancia local y está diseñado para facilitar la identificación del servidor virtual. Cuando un cliente intenta acceder a aplicaciones en un servidor, envía una solicitud a la dirección IP virtual en lugar de enviarla a la dirección IP del servidor físico. Cuando el dispositivo recibe una solicitud en la dirección VIP, finaliza la conexión en el servidor virtual y utiliza su propia conexión con el servidor en nombre del cliente. La configuración de puerto y protocolo del servidor virtual determina las aplicaciones que representa el servidor virtual. Por ejemplo, un servidor web se puede representar mediante un servidor virtual y un servicio cuyo puerto y protocolo se establecen en 80 y HTTP, respectivamente. Varios servidores virtuales pueden usar la misma dirección VIP pero diferentes protocolos y puertos.

Los servidores virtuales son puntos para entregar funciones. La mayoría de las funciones, como la compresión, el almacenamiento en caché y la descarga de SSL, normalmente están habilitadas en un servidor virtual. Cuando el dispositivo recibe una solicitud en una dirección VIP, elige el servidor virtual apropiado por el puerto en el que se recibió la solicitud y su protocolo. A continuación, el dispositivo procesa la solicitud según corresponda para las funciones configuradas en el servidor virtual.

En la mayoría de los casos, los servidores virtuales funcionan en conjunto con los servicios. Puede enlazar varios servicios a un servidor virtual. Estos servicios representan las aplicaciones que se ejecutan en servidores físicos en una comunidad de servidores. Una vez que el dispositivo procesa las solicitudes recibidas en una dirección VIP, las reenvía a los servidores según lo determinado por el algoritmo de equilibrio de carga configurado en el servidor virtual. La siguiente ilustración ilustra estos conceptos.

Imagen 4. Múltiples servidores virtuales con una única dirección VIP



La ilustración anterior muestra una configuración que consta de dos servidores virtuales con una dirección VIP común pero puertos y protocolos diferentes. Cada uno de los servidores virtuales tiene dos servicios vinculados a él. Los servicios s1 y s2 están enlazados a VS_HTTP y representan las aplicaciones HTTP en el servidor 1 y el servidor 2. Los servicios s3 y s4 están enlazados a VS_SSL y representan las aplicaciones SSL en el servidor 2 y el servidor 3 (el servidor 2 proporciona aplicaciones HTTP y SSL). Cuando el dispositivo recibe una solicitud HTTP en la dirección VIP, procesa la solicitud según lo especificado por la configuración de VS_HTTP y la envía al servidor 1 o al servidor 2. Del mismo modo, cuando el dispositivo recibe una solicitud HTTPS en la dirección VIP, la procesa según lo especificado por la configuración de VS_SSL y la envía al servidor 2 o al servidor 3.

Los servidores virtuales no siempre se representan mediante direcciones IP, números de puerto o protocolos específicos. Se pueden representar mediante comodines, en cuyo caso se conocen como servidores virtuales comodines. Por ejemplo, cuando configura un servidor virtual con un comodín en lugar de un VIP, pero con un número de puerto específico, el dispositivo intercepta y procesa todo el tráfico conforme a ese protocolo y destinado al puerto predefinido. Para los servidores virtuales con comodines en lugar de VIPs y números de puerto, el dispositivo intercepta y procesa todo el tráfico conforme al protocolo.

Los servidores virtuales pueden agruparse en las siguientes categorías:

- Servidor virtual de equilibrio de carga

  Recibe y redirige solicitudes a un servidor apropiado. La elección del servidor apropiado se

basa en cuál de los diversos métodos de equilibrio de carga configura el usuario.

- Servidor virtual de redirección de caché

  Redirige las solicitudes de cliente de contenido dinámico a los servidores de origen y las solicitudes de contenido estático a los servidores de caché. Los servidores virtuales de redirección de caché a menudo funcionan junto con los servidores virtuales de equilibrio de carga.

- Servidor virtual de conmutación de contenido

  Dirige el tráfico a un servidor en función del contenido solicitado por el cliente. Por ejemplo, puede crear un servidor virtual de conmutación de contenido que dirija todas las solicitudes de los clientes de imágenes a un servidor que solo sirve imágenes. Los servidores virtuales de conmutación de contenido suelen funcionar conjuntamente con los servidores virtuales de equilibrio de carga.

- Servidor virtual de red privada virtual (VPN)

  Descifra el tráfico en túnel y lo envía a aplicaciones de intranet.

- Servidor virtual SSL

  Recibe y descifra el tráfico SSL y, a continuación, redirige a un servidor apropiado. Elegir el servidor adecuado es similar a elegir un servidor virtual de equilibrio de carga.

Descripción de los servicios

Los servicios representan aplicaciones en un servidor. Aunque los servicios se combinan normalmente con servidores virtuales, en ausencia de un servidor virtual, un servicio puede administrar el tráfico específico de la aplicación. Por ejemplo, puede crear un servicio HTTP en un dispositivo Citrix ADC para representar una aplicación de servidor web. Cuando el cliente intenta tener acceso a un sitio web alojado en el servidor web, el dispositivo intercepta las solicitudes HTTP y crea una conexión transparente con el servidor web.

En el modo de solo servicio, un dispositivo funciona como proxy. Termina las conexiones de cliente, utiliza una dirección SNIP para establecer una conexión con el servidor y traduce las direcciones IP de origen de las solicitudes de cliente entrantes a una dirección SNIP. Aunque los clientes envían solicitudes directamente a la dirección IP del servidor, el servidor las ve como procedentes de la dirección SNIP. El dispositivo traduce las direcciones IP, los números de puerto y los números de secuencia.

Un servicio también es un punto para aplicar funcionalidades. Considere el ejemplo de aceleración SSL. Para utilizar esta función, debe crear un servicio SSL y enlazar un certificado SSL al servicio. Cuando el dispositivo recibe una solicitud HTTPS, descifra el tráfico y lo envía, en texto sin formato, al servidor. Solo se puede configurar un conjunto limitado de funciones en el caso de solo servicio.

Los servicios utilizan entidades llamadas monitores para realizar un seguimiento del estado de las aplicaciones. Cada servicio tiene un monitor predeterminado, que se basa en el tipo de servicio, vin-

culado a él. Según lo especificado por la configuración configurada en el monitor, el dispositivo envía sondeos a la aplicación a intervalos regulares para determinar su estado. Si los sondeos fallan, el dispositivo marca el servicio como inactivo. En tales casos, el dispositivo responde a las solicitudes del cliente con un mensaje de error adecuado o redirige la solicitud según lo determinado por las directivas de equilibrio de carga configuradas.

Introducción a la línea de productos Citrix ADC

April 5, 2022

La línea de productos Citrix ADC optimiza la entrega de aplicaciones a través de Internet y redes privadas, combinando la seguridad, la optimización y la administración del tráfico a nivel de aplicaciones en un único dispositivo integrado. Puede instalar un dispositivo Citrix ADC en su sala de servidores y enrutar todas las conexiones a sus servidores administrados a través de él. Las funciones de Citrix ADC que habilita y las directivas que establece se aplican al tráfico entrante y saliente.

Un dispositivo Citrix ADC se puede integrar en cualquier red como complemento de los equilibradores de carga, los servidores, las cachés y los firewalls existentes. No requiere software adicional del lado del cliente o del servidor y se puede configurar mediante las utilidades de configuración de GUI y CLI basadas en web de Citrix ADC.

Este tema incluye las siguientes secciones:

- Plataformas de hardware Citrix ADC
- Ediciones Citrix ADC
- Versiones compatibles en hardware ADC
- Exploradores Web compatibles

Plataformas de hardware Citrix ADC

El hardware de Citrix ADC está disponible en una variedad de plataformas que tienen una variedad de especificaciones de hardware:

Plataforma de hardware Citrix ADC MPX

Plataforma de hardware Citrix ADC SDX

Ediciones Citrix ADC

El sistema operativo Citrix ADC está disponible en tres ediciones:

- Estándar
- Avanzado

- Premium

Las ediciones Standard y Advanced tienen funciones limitadas disponibles. Se requieren licencias de función para todas las ediciones.

Para obtener más información sobre las ediciones del software Citrix ADC, consulte la hoja de datos de Citrix ADC Editions.

Para obtener información sobre cómo obtener e instalar licencias, consulte Licencias.

Versiones admitidas en hardware Citrix ADC

Consulte las siguientes tablas matriciales de compatibilidad para todas las plataformas de hardware Citrix ADC y las versiones de software compatibles con estas plataformas:

Matriz de compatibilidad de hardware y software de Citrix ADC MPX

Tabla de compatibilidad entre hardware y software de Citrix ADC SDX

Exploradores compatibles

Para acceder a la GUI de Citrix ADC, su estación de trabajo debe tener un explorador web compatible.

En la siguiente tabla se enumeran los exploradores compatibles para la GUI de NetScaler versión 12.0, 12.1 y 13.0:

Sistema operativo	Explorador web	Versiones
Windows 7 y versiones posteriores	Internet Explorer	11, Edge y versiones posteriores
Windows 7 y versiones posteriores	Mozilla Firefox	45 y posteriores
Windows 7 y versiones posteriores	Chrome	60 y posteriores
MAC	Mozilla Firefox	45 y posteriores
MAC	Safari	10.1.1 y posteriores

Las versiones de exploradores web compatibles para Citrix ADC 11.1 son las siguientes:

Sistema operativo	Explorador web	Versiones
Windows 7 y versiones posteriores	Internet Explorer	8, 9, 10, 11, borde

Sistema operativo	Explorador web	Versiones
Windows 7 y versiones posteriores	Mozilla Firefox	45 y posteriores
Windows 7 y versiones posteriores	Chrome	60 y posteriores
MAC	Mozilla Firefox	45 y posteriores
MAC	Safari	10.1.1 y posteriores

Instalar el hardware

January 12, 2021

Antes de instalar un dispositivo Citrix ADC, revise la lista de comprobación previa a la instalación.

Para utilizar el dispositivo SDX, debe realizar las tareas siguientes siguiendo las instrucciones que se indican en los recursos proporcionados en la tabla. Completar las tareas en la secuencia dada.

Tarea

Descripción

1. Leer seguridad, advertencias, advertencias y otra información

   Lea la información de precaución y peligro que necesita saber, antes de instalar el producto.

2. Para preparar la instalación

   Desempaquete el dispositivo y asegúrese de que todas las piezas fueron entregadas, prepare el sitio y el bastidor y siga las precauciones básicas de seguridad eléctrica antes de instalar el nuevo dispositivo.

3. Instalar el hardware

   Monte el dispositivo en rack, instale transceptores (si está disponible) y conecte el dispositivo a la red y a una fuente de alimentación.

4. Configure el dispositivo.

   Configure la configuración inicial del dispositivo Citrix ADC mediante la interfaz gráfica de usuario o la consola serie.

   Siga los pasos que se indican en las siguientes documentaciones para completar estas tareas:

   - Documentación de hardware de Citrix ADC MPX
   - Documentación de hardware de Citrix ADC SDX

Acceder a un dispositivo Citrix ADC

August 20, 2021

Un dispositivo Citrix ADC tiene una interfaz de línea de comandos (CLI) y una GUI. La GUI incluye una utilidad de configuración para configurar el dispositivo y una utilidad estadística, denominada Dashboard. Para el acceso inicial, todos los dispositivos se envían con la dirección IP de Citrix ADC (NSIP) predeterminada de 192.168.100.1 y la máscara de subred predeterminada de 255.255.0.0. Puede asignar un nuevo NSIP y una máscara de subred asociada durante la configuración inicial.

Si encuentra un conflicto de dirección IP al implementar varias unidades Citrix ADC, compruebe las siguientes causas posibles:

- ¿Ha seleccionado un NSIP que es una dirección IP ya asignada a otro dispositivo de la red?
- ¿Asignó el mismo NSIP a varios dispositivos Citrix ADC?
- El NSIP es accesible en todos los puertos físicos. Los puertos de un dispositivo Citrix ADC son puertos de host, no puertos de switch.

En la siguiente tabla se resumen los métodos de acceso disponibles.

Método Access	Port	¿Se requiere dirección IP predeterminada? (S/N)
CLI	Consola	N
CLI y GUI	Ethernet	S

Interfaz de línea de comandos

Acceda a la CLI localmente conectando una estación de trabajo al puerto de la consola o conectándose de forma remota a través del shell seguro (SSH) desde cualquier estación de trabajo de la misma red.

Inicie sesión en la interfaz de línea de comandos a través del puerto de consola

El dispositivo dispone de un puerto de consola para conectarse a una estación de trabajo. Para iniciar sesión en el dispositivo, necesita un cable cruzado serie y una estación de trabajo con un programa de emulación de terminales.

Para iniciar sesión en la CLI a través del puerto de consola, siga estos pasos:

1. Conecte el puerto de la consola a un puerto serie de la estación de trabajo. Para obtener más información, consulte Conectar el cable de la consola.
2. En la estación de trabajo, inicie HyperTerminal o cualquier otro programa de emulación de terminal. Si no aparece el mensaje de inicio de sesión, es posible que tenga que presionar ENTRAR

una o varias veces para mostrarlo.

3. En Nombre de usuario, escriba `nsroot`. En Contraseña, escriba `nsroot` y, si la contraseña no funciona, intente escribir el número de serie del dispositivo. El código de barras del número de serie está disponible en la parte posterior del dispositivo.

Inicie sesión en la interfaz de línea de comandos mediante SSH

El protocolo SSH es el método de acceso remoto preferido para acceder a un dispositivo de forma remota desde cualquier estación de trabajo en la misma red. Puede usar SSH versión 1 (SSH1) o SSH versión 2 (SSH2).

Si no tiene un cliente SSH en funcionamiento, puede descargar e instalar cualquiera de los siguientes programas de cliente SSH:

- PuTTY

  Software de código abierto compatible con múltiples plataformas. Disponible en:

  http://www.chiark.greenend.org.uk/~sgtatham/putty/

- `Vandyke` Software SecureCRT

  Software comercial compatible con la plataforma Windows. Disponible en:

  http://www.vandyke.com/products/securecrt/

Estos programas son probados por el equipo de Citrix ADC, que ha verificado que funcionan correctamente con un dispositivo Citrix ADC. Es posible que otros programas también funcionen correctamente, pero no se han probado.

Para comprobar que el cliente SSH está instalado correctamente, utilícelo para conectarse a cualquier dispositivo de la red que acepte conexiones SSH.

Para iniciar sesión en un dispositivo Citrix ADC mediante un cliente SSH, siga estos pasos:

1. En su estación de trabajo, inicie el cliente SSH.
2. Para la configuración inicial, utilice la dirección IP predeterminada (NSIP), que es 192.168.100.1. Para el acceso posterior, utilice el NSIP que se asignó durante la configuración inicial. Seleccione SSH1 o SSH2 como protocolo.
3. En Nombre de usuario, escriba `nsroot`. En Contraseña, escriba `nsroot` y, si la contraseña no funciona, intente escribir el número de serie del dispositivo. El código de barras del número de serie está disponible en la parte posterior del dispositivo. Por ejemplo.

```
1 login as: nsroot
2
3
```



```
Using keyboard-interactive authentication.

Password:

Last login: Tue Jun 16 10:37:28 2009 from 10.102.29.9



Done

>

<!--NeedCopy-->
```

GUI de Citrix ADC

> **Importante:**
>
> Se requiere un par de claves de certificado para el acceso HTTPS a la GUI de Citric ADC. En el ADC, un par de certificados y claves se vincula automáticamente a los servicios internos. En un dispositivo MPX o SDX, el tamaño de clave predeterminado es 1024 bytes y, en una instancia VPX, el tamaño de clave predeterminado es 512 bytes. Sin embargo, la mayoría de los exploradores hoy en día no aceptan una clave que sea inferior a 1024 bytes. Como resultado, el acceso HTTPS a la utilidad de configuración VPX está bloqueado.

Además, si una licencia no está presente en un dispositivo MPX cuando se inicia y agrega una licencia más tarde y reinicia el dispositivo, es posible que pierda el enlace de certificado.

Citrix recomienda instalar un par de claves de certificado de al menos 1024 bytes en el dispositivo para tener acceso HTTPS a la GUI. Además, instale una licencia adecuada antes de iniciar el dispositivo.

La GUI incluye una utilidad de configuración y una utilidad estadística, denominada Dashboard, a la que se accede a través de una estación de trabajo conectada a un puerto Ethernet del dispositivo.

Los requisitos del sistema para la estación de trabajo que ejecuta la GUI son los siguientes:

- Para estaciones de trabajo basadas en Windows, un procesador Pentium 166 MHz o más rápido.
- Para estaciones de trabajo basadas en Linux, una plataforma Pentium que ejecute el kernel Linux v2.2.12 o superior y la `glibc` versión 2.12—11 o posterior. Se requiere un mínimo de 32 MB de RAM y se recomienda 48 MB de RAM. La estación de trabajo debe admitir el modo de color

de 16 bits, los administradores de ventanas KDE y KWM utilizados conjuntamente, con pantallas configuradas en hosts locales.
- Para estaciones de trabajo basadas en Solaris, Sun que ejecute Solaris 2.6, Solaris 7 u Solaris 8.

Su estación de trabajo debe tener un explorador web compatible para acceder a la utilidad de configuración y al Panel de control.

Se admiten los siguientes exploradores.

Sistema operativo: Windows 7.

Explorador: Internet Explorer (versión 9, 10 y 11), Mozilla Firefox (versión 3.6.25 y superior), Google Chrome (última).

Sistema operativo: Windows de 64 bits

Explorador: Internet Explorer (versión 8, 9, 10 y 11), Google Chrome (versión más reciente)

Sistema operativo:
Explorador MAC: Mozilla Firefox (versión 3.6.25 y superior), Safari (versión 5.1.3 y superior), Google Chrome (versión más reciente)

Utilizar la GUI de Citrix ADC

Una vez que inicie sesión en la utilidad de configuración, puede configurar el dispositivo a través de una interfaz gráfica que incluya ayuda sensible al contexto.

Para iniciar sesión en la GUI, siga estos pasos:

1. Abra su explorador web e introduzca la IP de Citrix ADC (NSIP) como dirección HTTP. Si aún no ha configurado la configuración inicial, introduzca el NSIP predeterminado (http://192.168.100.1). Aparecerá la página Inicio de sesión de Citrix.

   Nota: Si tiene dos dispositivos Citrix ADC en una configuración de alta disponibilidad, no acceda a la GUI introduciendo la dirección IP del dispositivo Citrix ADC secundario. Si lo hace y utiliza la GUI para configurar el dispositivo secundario, los cambios de configuración no se aplicarán al dispositivo Citrix ADC principal.

2. En el cuadro de texto Nombre de usuario, escriba `nsroot`.
3. En el cuadro de texto Contraseña, escriba la contraseña administrativa asignada a la `nsroot` cuenta durante la configuración inicial y haga clic en **Iniciar sesión**. Si la contraseña no funciona, intente escribir el número de serie del dispositivo. El código de barras del número de serie está disponible en la parte posterior del dispositivo.

   Para acceder a la ayuda en línea, selecciona Ayuda en el menú Ayuda en la esquina superior derecha.

Utilizar la utilidad estadística

Dashboard, la utilidad estadística, es una aplicación basada en explorador que muestra gráficos y tablas en las que puede supervisar el rendimiento de un dispositivo Citrix ADC.

Para iniciar sesión en el panel, siga estos pasos:

1. Abra su explorador web e introduzca el NSIP como una dirección HTTP. Aparecerá la página Inicio de sesión de Citrix.
2. En el cuadro de texto Nombre de usuario, escriba `nsroot`.
3. En el cuadro de texto Contraseña, escriba la contraseña administrativa asignada a la `nsroot` cuenta durante la configuración inicial. Si la contraseña no funciona, intente escribir el número de serie del dispositivo. El código de barras del número de serie está disponible en la parte posterior del dispositivo.

Configurar el ADC por primera vez

January 12, 2021

Para obtener información sobre la configuración inicial de un dispositivo Citrix ADC MPX, consulte Configuración inicial de un dispositivo Citrix MPX.

Para obtener información sobre la configuración inicial de un dispositivo Citrix SDX, consulte Configuración inicial de un dispositivo Citrix SDX.

API de NITRO

Puede utilizar la API NITRO para configurar el dispositivo Citrix ADC. NITRO expone su funcionalidad a través de interfaces de transferencia de estado representacional (REST). Por lo tanto, las aplicaciones NITRO se pueden desarrollar en cualquier lenguaje de programación. Además, para las aplicaciones que deben desarrollarse en Java o.NET o Python, las API de NITRO se exponen a través de bibliotecas relevantes que se empaquetan como kits de desarrollo de software (SDK) independientes. Para obtener más información, consulte API de NITRO.

Proteja su implementación de Citrix ADC

October 5, 2021

Para mantener la seguridad durante el ciclo de vida de implementación del dispositivo Citrix ADC, Citrix recomienda tener en cuenta los siguientes aspectos de seguridad:

- Seguridad física
- Seguridad del dispositivo
- Seguridad de red
- Administración y Gestión

Diferentes implementaciones pueden requerir diferentes consideraciones de seguridad. Las directrices de implementación segura de Citrix ADC proporcionan orientación general de seguridad para ayudarle a decidir sobre una implementación segura adecuada en función de sus requisitos de seguridad específicos.

Para obtener más información sobre las directrices para implementar de forma segura el dispositivo Citrix ADC, consulte Directrices de implementación segura de Citrix ADC.

Configurar alta disponibilidad

August 20, 2021

Puede implementar dos dispositivos Citrix ADC en una configuración de alta disponibilidad, donde una unidad acepta conexiones y administra servidores de forma activa, mientras que la unidad secundaria supervisa la primera. El dispositivo Citrix ADC que acepta activamente conexiones y administra los servidores se denomina unidad principal y la otra unidad secundaria en una configuración de alta disponibilidad. Si hay una falla en la unidad primaria, la unidad secundaria se convierte en la primaria y comienza a aceptar conexiones activamente.

Cada dispositivo Citrix ADC en un par de alta disponibilidad supervisa el otro mediante el envío de mensajes periódicos, denominados mensajes de latido o comprobaciones de estado, para determinar el estado o el estado del nodo del mismo nivel. Si falla la comprobación de estado de una unidad primaria, la unidad secundaria reintenta la conexión durante un período de tiempo específico. Para obtener más información sobre la alta disponibilidad, consulte Alta disponibilidad. Si un reintento no se realiza correctamente al final del período de tiempo especificado, la unidad secundaria se hará cargo de la unidad principal en un proceso denominado conmutación por error. La siguiente ilustración muestra dos configuraciones de alta disponibilidad, una en modo de un brazo y la otra en modo de dos brazos.

Ilustración 1. Alta disponibilidad en modo de un brazo

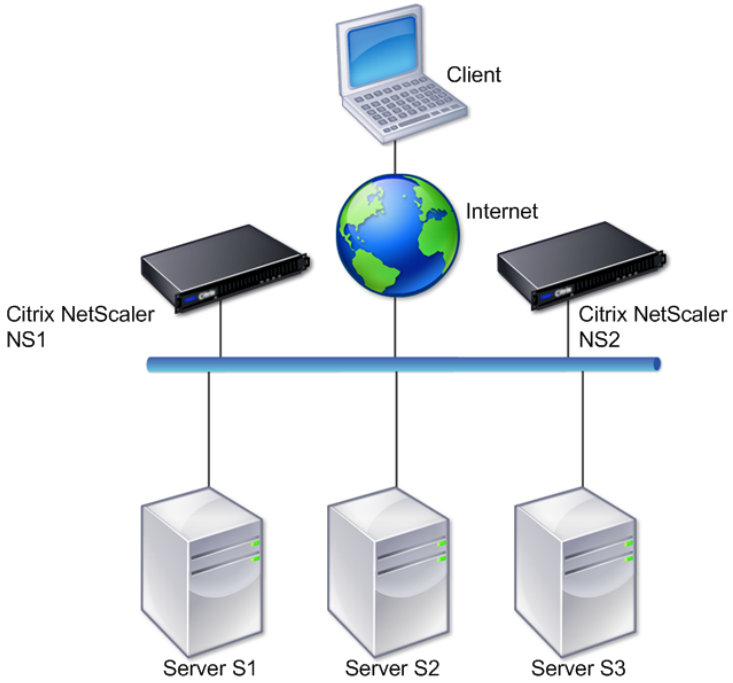
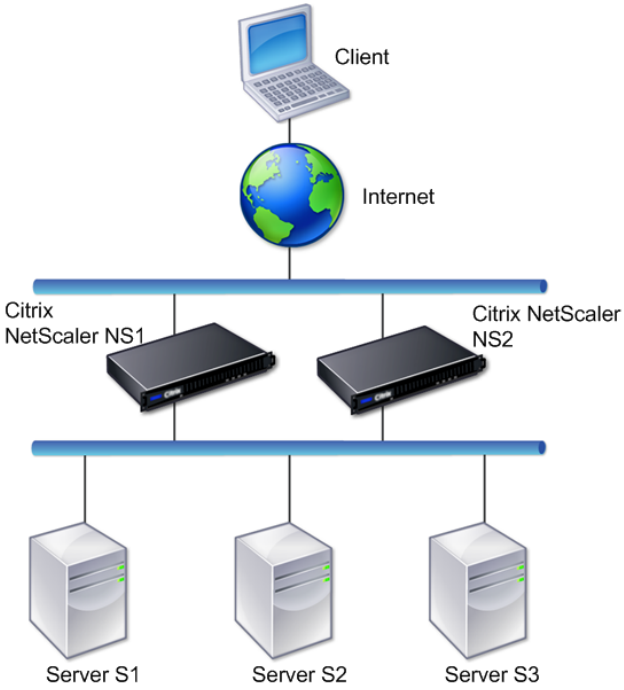


Ilustración 2. Alta disponibilidad en modo de dos brazos



En la configuración de un brazo, tanto NS1 como NS2 y los servidores S1, S2 y S3 están conectados al switch.

En la configuración de dos brazos, NS1 y NS2 están conectados a dos switches. Los servidores S1, S2 y S3 están conectados al segundo conmutador. El tráfico entre el cliente y los servidores pasa a través de NS1 o NS2.

Para configurar un entorno de alta disponibilidad, configure un dispositivo ADC como primario y otro como secundario. Realice las siguientes tareas en cada uno de los dispositivos ADC:

- Agregue un nodo.
- Inhabilite la supervisión de alta disponibilidad para las interfaces no utilizadas.

Agregar un nodo

Un nodo es una representación lógica de un dispositivo Citrix ADC del mismo nivel. Identifica la unidad del mismo nivel por ID y NSIP. Un dispositivo utiliza estos parámetros para comunicarse con el par y realizar un seguimiento de su estado. Cuando agrega un nodo, las unidades principal y secundaria intercambian mensajes de latido de forma asíncrona. El identificador de nodo es un número entero que no debe ser mayor que 64.

A través de CLI

Para agregar un nodo mediante la interfaz de línea de comandos, siga estos pasos:

En el símbolo del sistema, escriba los siguientes comandos para agregar un nodo y compruebe que se ha agregado el nodo:

- add HA node <id> <IPAddress>
- show HA node <id>

  Ejemplo

```
add HA node 0 10.102.29.170
 Done
> show HA node 0
1)      Node ID:      0
        IP:   10.102.29.200 (NS200)
        Node State: UP
        Master State: Primary
        SSL Card Status: UP
        Hello Interval: 200 msecs
        Dead Interval: 3 secs
        Node in this Master State for: 1:0:41:50 (days:hrs:min:
           sec)
<!--NeedCopy-->
```

A través de GUI

Para agregar un nodo mediante la GUI, siga estos pasos:

1. Vaya a **Sistema** > **Alta disponibilidad**.
2. Haga clic en **Agregar** en la ficha **Nodos**.
3. En la página **Crear nodo HA**, en el cuadro de texto **Dirección IP del nodo remoto**, escriba la dirección NSIP (por ejemplo, 10.102.29.170) del nodo remoto.
4. Asegúrese de que la casilla de verificación **Configurar sistema remoto para participar en la instalación de alta disponibilidad** está activada. Proporcione las credenciales de inicio de sesión del nodo remoto en los cuadros de texto en **Credenciales de inicio de sesión del sistema remoto**.
5. Active la casilla de verificación **Desactivar el monitor de alta disponibilidad en interfaces o canales que están desactivados** para inhabilitar el monitor de alta disponibilidad en interfaces que están inactivas.

Compruebe que el nodo agregado aparezca en la lista de nodos de la ficha Nodos.

Inhabilitar la supervisión de alta disponibilidad para interfaces no utilizadas

El monitor de alta disponibilidad es una entidad virtual que supervisa una interfaz. Debe inhabilitar el monitor para las interfaces que no están conectadas o que se utilizan para el tráfico. Cuando el monitor está habilitado en una interfaz cuyo estado es DOWN, el estado del nodo se convierte en NO UP. En una configuración de alta disponibilidad, un nodo principal que entra en un estado NOTO UP puede provocar una conmutación por error de alta disponibilidad. Una interfaz está marcada como DOWN en las siguientes condiciones:

- La interfaz no está conectada
- La interfaz no funciona correctamente
- El cable que conecta la interfaz no funciona correctamente

A través de CLI

Para inhabilitar el monitor de alta disponibilidad para una interfaz no utilizada mediante la interfaz de línea de comandos, siga estos pasos:

En el símbolo del sistema, escriba los siguientes comandos para inhabilitar el monitor de alta disponibilidad para una interfaz no utilizada y compruebe que está inhabilitada:

- set interface <id> -haMonitor OFF
- mostrar interfaz <id>

  Ejemplo

```
> set interface 1/8 -haMonitor OFF
 Done
> show interface 1/8
        Interface 1/8 (Gig Ethernet 10/100/1000 MBits) #2
        flags=0x4000 <ENABLED, DOWN, down, autoneg, 802.1q>
        MTU=1514, native vlan=1, MAC=00:d0:68:15:fd:3d, downtime
           238h55m44s
        Requested: media AUTO, speed AUTO, duplex AUTO, fctl OFF,
                  throughput 0

        RX: Pkts(0) Bytes(0) Errs(0) Drops(0) Stalls(0)
        TX: Pkts(0) Bytes(0) Errs(0) Drops(0) Stalls(0)
        NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0)
           Muted(0)
        Bandwidth thresholds are not set.
<!--NeedCopy-->
```


Cuando el monitor de alta disponibilidad está inhabilitado para una interfaz no utilizada, la salida del comando show interface para esa interfaz no incluye “HAMON.”

A través de GUI

Para inhabilitar el monitor de alta disponibilidad para interfaces no utilizadas mediante la GUI, siga estos pasos:

1. Vaya a Sistema > Red > Interfaces.
2. Seleccione la interfaz para la que debe inhabilitarse el monitor.
3. Haga clic en Abrir. Aparecerá el cuadro de diálogo Modificar interfaz.
4. En Supervisión de alta disponibilidad, seleccione la opción OFF.
5. Haga clic en Aceptar.
6. Verifique que, cuando se selecciona la interfaz, “HA Monitoring: OFF” aparezca en los detalles de la parte inferior de la página.

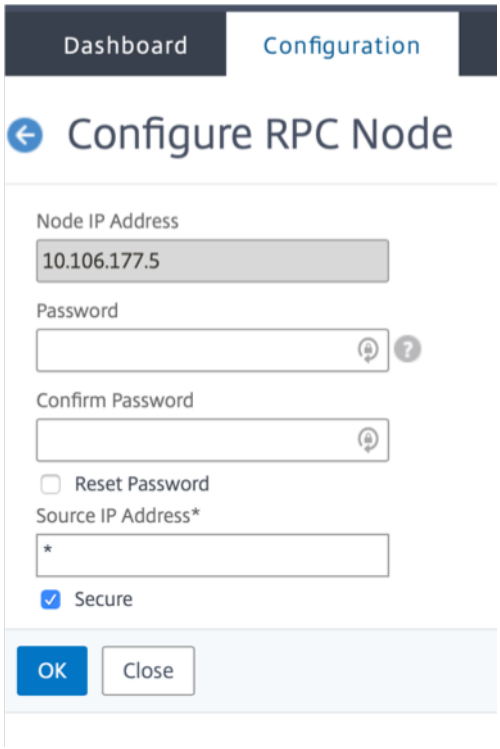
Cambiar una contraseña de nodo RPC

January 12, 2021

Para comunicarse con otros dispositivos Citrix ADC, cada dispositivo requiere conocimientos sobre los demás dispositivos, incluido el modo de autenticarse en el dispositivo Citrix ADC. Los nodos RPC son entidades internas del sistema utilizadas para la comunicación de información de configuración y sesión de sistema a sistema. Existe un nodo RPC en cada dispositivo Citrix ADC y almacena información, como las direcciones IP del otro dispositivo Citrix ADC y las contraseñas utilizadas para la autenticación. El dispositivo Citrix ADC que se pone en contacto con el otro dispositivo Citrix ADC comprueba la contraseña dentro del nodo RPC.

Para cambiar una contraseña de nodo RPC mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **Red** > **RPC**.
2. En el panel **RPC**, seleccione el nodo y, a continuación, haga clic en **Modificar**.
3. En **Configurar nodo RPC**, escriba la nueva contraseña.
4. En **Dirección IP de origen, escriba la dirección**IP del nodo existente que se utilizará para comunicarse con el nodo del sistema del mismo nivel.



5. Seleccione **Secure** y, a continuación, haga clic en **Aceptar**.

> **Nota**
>
> Para mejorar la seguridad, Citrix recomienda habilitar la opción **Secure** en nodos RPC. Cuando se habilita la opción **Secure**, el dispositivo cifra toda la comunicación RPC enviada desde un nodo ADC a otros nodos ADC, protegiendo así la comunicación RPC. Esta comunicación segura utiliza el número de puerto 3008. Si el firewall entre los nodos ADC bloquea el número de puerto 3008, desbloquee y continúe. De lo contrario, la sincronización de configuración y la propagación de la configuración podrían fallar.

Para cambiar una contraseña de nodo RPC mediante la CLI

En la línea de comandos, escriba los siguientes comandos:

```
set ns rpcNode <IPAddress> {
 -password }
  [-secure ( YES | NO )]
show ns rpcNode
<!--NeedCopy-->
```

Ejemplo:


```
> set ns rpcNode 192.0.2.4 -password mypassword -secure YES
 Done
> show rpcNode
.
.
.
 IPAddress:  192.0.2.4 Password:  d336004164d4352ce39e
     SrcIP:  *           Secure:  ON
Done
>

<!--NeedCopy-->
```

Configurar un dispositivo FIPS por primera vez

December 2, 2021

> **Nota**
>
> - Las preguntas frecuentes sobre FIPS se pueden encontrar aquí: Preguntas frecuentes sobre FIPS.

Se requiere un par de claves de certificado para el acceso HTTPS a la utilidad de configuración y para las llamadas seguras a procedimientos remotos. Los nodos RPC son entidades internas del sistema utilizadas para la comunicación de información de configuración y sesión de sistema a sistema. Existe un nodo RPC en cada dispositivo. Este nodo almacena la contraseña, que se compara con la proporcionada por el dispositivo de contacto. Para comunicarse con otros dispositivos Citrix ADC, cada dispositivo requiere conocimiento de los demás dispositivos, incluido cómo autenticarse en el otro dispositivo. Los nodos RPC conservan esta información, que incluye las direcciones IP de los demás dispositivos Citrix ADC y las contraseñas utilizadas para autenticarse en cada uno.

En un dispositivo virtual de dispositivo Citrix ADC MPX, un par de claves de certificado se enlaza automáticamente a los servicios internos. En un dispositivo FIPS, se debe importar un par de claves de certificado en el módulo de seguridad de hardware (HSM) de una tarjeta FIPS. Para hacerlo, debe configurar la tarjeta FIPS, crear un par de claves de certificado y vincularlo a los servicios internos.

Configurar HTTPS seguro mediante la CLI

Para configurar HTTPS seguro mediante la CLI, siga estos pasos

1. Inicialice el módulo de seguridad de hardware (HSM) en la tarjeta FIPS del dispositivo. Para obtener información sobre la inicialización del HSM, consulte Configurar el HSM.

2. Si el dispositivo forma parte de una configuración de alta disponibilidad, habilite la SIM. Para obtener información sobre cómo habilitar la SIM en los dispositivos primario y secundario, consulte Configurar dispositivos FIPS en una configuración de alta disponibilidad.
3. Importe la clave FIPS en el HSM de la tarjeta FIPS del dispositivo. En el símbolo del sistema, escriba:

   ```
   import ssl fipskey serverkey -key ns-server.key -inform PEM
   ```

4. Agregue un par de claves de certificado. En el símbolo del sistema, escriba:

   ```
   add certkey server -cert ns-server.cert -fipskey serverkey
   ```

5. Enlace la clave de certificado creada en el paso anterior a los siguientes servicios internos. En el símbolo del sistema, escriba:

   ```
   bind ssl service nshttps-127.0.0.1-443 -certkeyname server
   ```

   ```
   bind ssl service nshttps-::11-443 -certkeyname server
   ```

Configurar HTTPS seguro mediante la GUI

Para configurar HTTPS seguro mediante la GUI, siga estos pasos:

1. Inicialice el módulo de seguridad de hardware (HSM) en la tarjeta FIPS del dispositivo. Para obtener información sobre la inicialización del HSM, consulte Configurar el HSM.
2. Si el dispositivo forma parte de una configuración de alta disponibilidad, habilite el sistema de información seguro (SIM). Para obtener información sobre cómo habilitar la SIM en los dispositivos primario y secundario, consulte Configurar dispositivos FIPS en una configuración de alta disponibilidad.
3. Importe la clave FIPS en el HSM de la tarjeta FIPS del dispositivo. Para obtener más información sobre la importación de una clave FIPS, consulte la sección Importar una clave FIPS existente.
4. Vaya a **Administración del tráfico > SSL > Certificados**.
5. En el panel de detalles, haga clic en Instalar.
6. En el cuadro de diálogo Instalar certificado, escriba los detalles del certificado.
7. Haga clic en Crear y, a continuación, en Cerrar.
8. Vaya a **Traffic Management > Load Balancing > Services**.
9. En el panel de detalles, en la ficha Acción, haga clic en Servicios internos.
10. Seleccione `nshttps-127.0.0.1-443` en la lista y, a continuación, haga clic en Abrir.
11. En la ficha Configuración de SSL, en el panel Disponible, seleccione el certificado creado en el paso 7, haga clic en Agregar y, a continuación, haga clic en Aceptar.

12. Seleccione `nshttps-::11-443` en la lista y, a continuación, haga clic en Abrir.
13. En la ficha Configuración de SSL, en el panel Disponible, seleccione el certificado creado en el paso 7, haga clic en Agregar y, a continuación, haga clic en Aceptar.
14. Haga clic en Aceptar.

Configurar RPC segura mediante la CLI

Para configurar RPC segura mediante la CLI, siga estos pasos:

1. Inicialice el módulo de seguridad de hardware (HSM) en la tarjeta FIPS del dispositivo. Para obtener información sobre la inicialización del HSM, consulte Configurar el HSM.
2. Habilite el sistema de información segura (SIM). Para obtener información sobre cómo habilitar la SIM en los dispositivos primario y secundario, consulte Configurar dispositivos FIPS en una configuración de alta disponibilidad.
3. Importe la clave FIPS en el HSM de la tarjeta FIPS del dispositivo. En el símbolo del sistema, escriba:

   ```
   import ssl fipskey serverkey -key ns-server.key -inform PEM
   ```

4. Agregue un par de claves de certificado. En el símbolo del sistema, escriba:

   ```
   add certkey server -cert ns-server.cert -fipskey serverkey
   ```

5. Enlace el par de claves de certificado a los siguientes servicios internos. En el símbolo del sistema, escriba:

   ```
   bind ssl service nsrpcs-127.0.0.1-3008 -certkeyname server
   bind ssl service nskrpcs-127.0.0.1-3009 -certkeyname server
   bind ssl service nsrpcs-::1l-3008 -certkeyname server
   ```

6. Habilite el modo RPC seguro. En el símbolo del sistema, escriba:

   ```
   set ns rpcnode \<IP address\> -secure YES
   ```

   Para obtener más información sobre cómo cambiar la contraseña de un nodo RPC, consulte Cambiar una contraseña de nodo RPC.

Configurar RPC seguro mediante la interfaz gráfica de usuario

Para configurar RPC segura mediante la GUI, siga estos pasos:

1. Inicialice el módulo de seguridad de hardware (HSM) en la tarjeta FIPS del dispositivo. Para obtener información sobre la inicialización del HSM, consulte Configurar el HSM.

2. Habilite el sistema de información segura (SIM). Para obtener información sobre cómo habilitar la SIM en los dispositivos primario y secundario, configure los dispositivos FIPS en una configuración de alta disponibilidad.
3. Importe la clave FIPS en el HSM de la tarjeta FIPS del dispositivo. Para obtener más información sobre la importación de una clave FIPS, la sección Importar una clave FIPS existente.
4. Vaya a **Administración del tráfico > SSL > Certificados**.
5. En el panel de detalles, haga clic en Instalar.
6. En el cuadro de diálogo Instalar certificado, escriba los detalles del certificado.
7. Haga clic en Crear y, a continuación, en Cerrar.
8. Vaya a **Traffic Management > Load Balancing > Services**.
9. En el panel de detalles, en la ficha Acción, haga clic en Servicios internos.
10. Seleccione nsrpcs-127.0.0.1-3008 de la lista y, a continuación, haga clic en Abrir.
11. En la ficha Configuración de SSL, en el panel Disponible, seleccione el certificado creado en el paso 7, haga clic en Agregar y, a continuación, haga clic en Aceptar.
12. Seleccione nskrpcs-127.0.0.1-3009 de la lista y, a continuación, haga clic en Abrir.
13. En la ficha Configuración de SSL, en el panel Disponible, seleccione el certificado creado en el paso 7, haga clic en Agregar y, a continuación, haga clic en Aceptar.
14. Seleccione `nsrpcs-::11-3008` en la lista y, a continuación, haga clic en Abrir.
15. En la ficha Configuración de SSL, en el panel Disponible, seleccione el certificado creado en el paso 7, haga clic en Agregar y, a continuación, haga clic en Aceptar.
16. Haga clic en Aceptar.
17. Vaya a **Sistema > Red > RPC**.
18. En el panel de detalles, seleccione la dirección IP y haga clic en Abrir.
19. En el cuadro de diálogo Configurar nodo RPC, seleccione Secure.
20. Haga clic en Aceptar.

Topologías de red comunes

August 20, 2021

Como se describe en la sección “Modo de implementación física” de ¿Dónde cabe un dispositivo Citrix ADC en la red?, puede implementar el dispositivo Citrix ADC ya sea en línea entre los clientes y los servidores o en modo de un solo brazo. El modo en línea utiliza una topología de dos brazos, que es el tipo de implementación más común.

Configurar una topología común de dos brazos

En una topología de dos brazos, una interfaz de red está conectada a la red del cliente y otra interfaz de red está conectada a la red del servidor, lo que garantiza que todo el tráfico fluya a través del

dispositivo. Esta topología puede requerir que vuelva a conectar el hardware y también puede provocar un tiempo de inactividad momentáneo. Las variaciones básicas de la topología de dos brazos son varias subredes, normalmente con el dispositivo en una subred pública y los servidores en una subred privada, y el modo transparente, con el dispositivo y los servidores en la red pública.

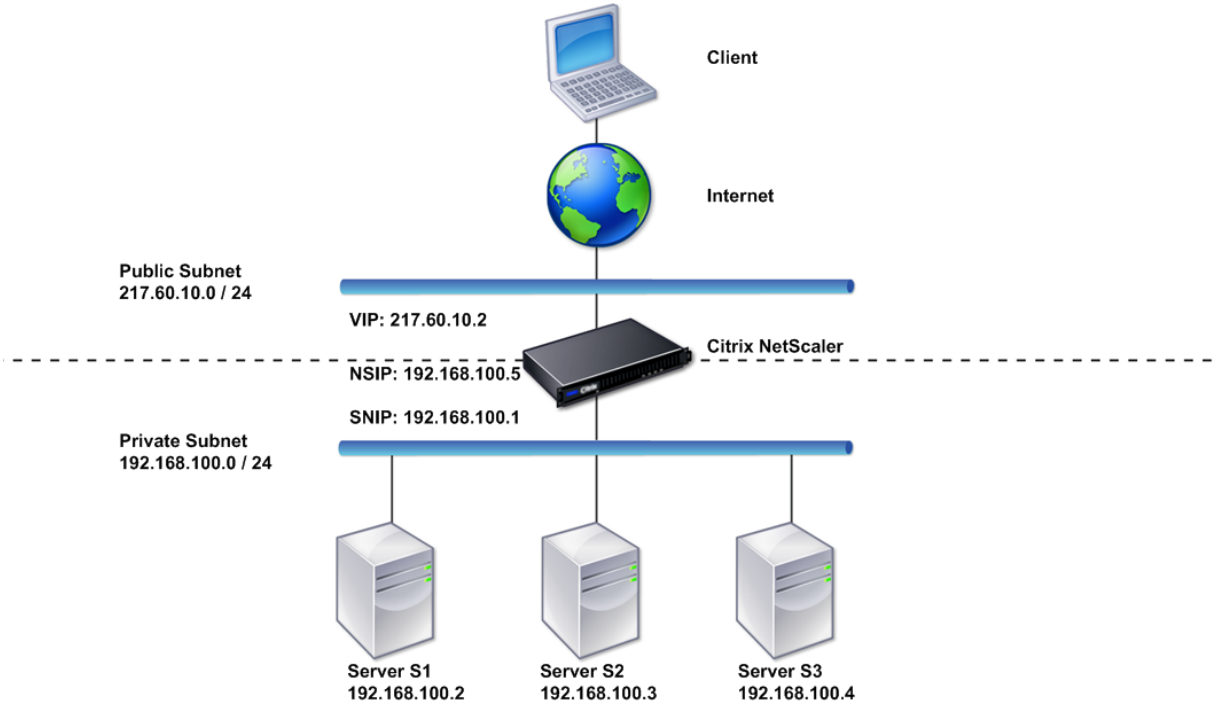
Configurar una topología simple de subred múltiple de dos brazos

Una de las topologías más utilizadas tiene el dispositivo Citrix ADC en línea entre los clientes y los servidores, con un servidor virtual configurado para gestionar las solicitudes del cliente. Esta configuración se utiliza cuando los clientes y servidores residen en diferentes subredes. En la mayoría de los casos, los clientes y servidores residen en subredes públicas y privadas, respectivamente.

Por ejemplo, considere un dispositivo implementado en modo de dos brazos para administrar servidores S1, S2 y S3, con un servidor virtual de tipo HTTP configurado en el dispositivo y con servicios HTTP ejecutándose en los servidores. Los servidores se encuentran en una subred privada y se configura un SNIP en el dispositivo para comunicarse con los servidores. La opción Usar SNIP (USNIP) debe estar habilitada en el dispositivo para que utilice el SNIP en lugar del MIP.

Como se muestra en la siguiente ilustración, el VIP está en la subred pública 217.60.10.0, y el NSIP, los servidores y el SNIP están en la subred privada 192.168.100.0/24.

Ilustración 1. Diagrama de topología para el modo de dos brazos, varias subredes



Para implementar un dispositivo Citrix ADC en modo de dos brazos con varias subredes, siga estos pasos:

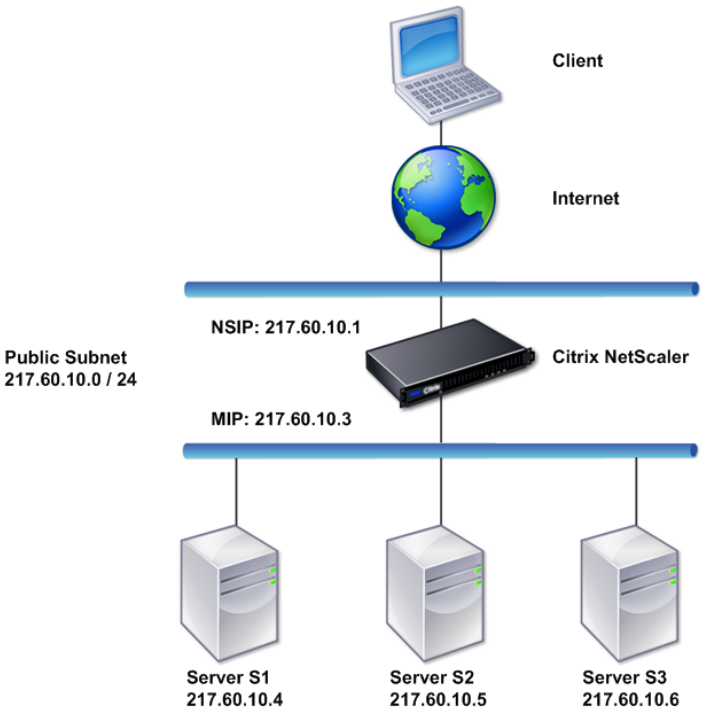
1. Configure el NSIP y la puerta de enlace predeterminada, como se describe en Configuración de la dirección IP de NetScaler (NSIP).
2. Configure el SNIP, tal y como se describe en Configuración de direcciones IP de subred.
3. Habilite la opción USNIP, como se describe en la sección Para habilitar o inhabilitar el modo USNIP .
4. Configure el servidor virtual y los servicios, tal como se describe en la sección Creación de un servidor virtual y en la sección Configuración de servicios .
5. Conecte una de las interfaces de red a una subred privada y la otra interfaz a una subred pública.

Configurar una topología transparente simple de dos brazos

Utilice el modo transparente si los clientes necesitan acceder a los servidores directamente, sin ningún servidor virtual que intervenga. Las direcciones IP del servidor deben ser públicas porque los clientes necesitan poder acceder a ellas. En el ejemplo que se muestra en la siguiente ilustración, se coloca un dispositivo Citrix ADC entre el cliente y el servidor, por lo que el tráfico debe pasar a través del dispositivo. Debe habilitar el modo L2 para conectar los paquetes en puente. El NSIP y MIP se

encuentran en la misma subred pública, 217.60.10.0/24.

Ilustración 2. Diagrama de topología para modo transparente de dos brazos



Para implementar un dispositivo Citrix ADC en modo transparente de dos brazos, siga estos pasos

1. Configure el NSIP y la puerta de enlace predeterminada, como se describe en Configuración de la dirección IP de NetScaler (NSIP).
2. Habilite el modo L2, tal y como se describe en Habilitación y desactivación del modo de capa 2.
3. Configure la Gateway predeterminada de los servidores administrados como MIP.
4. Conecte las interfaces de red a los puertos apropiados del conmutador.

Configurar topologías comunes de un brazo

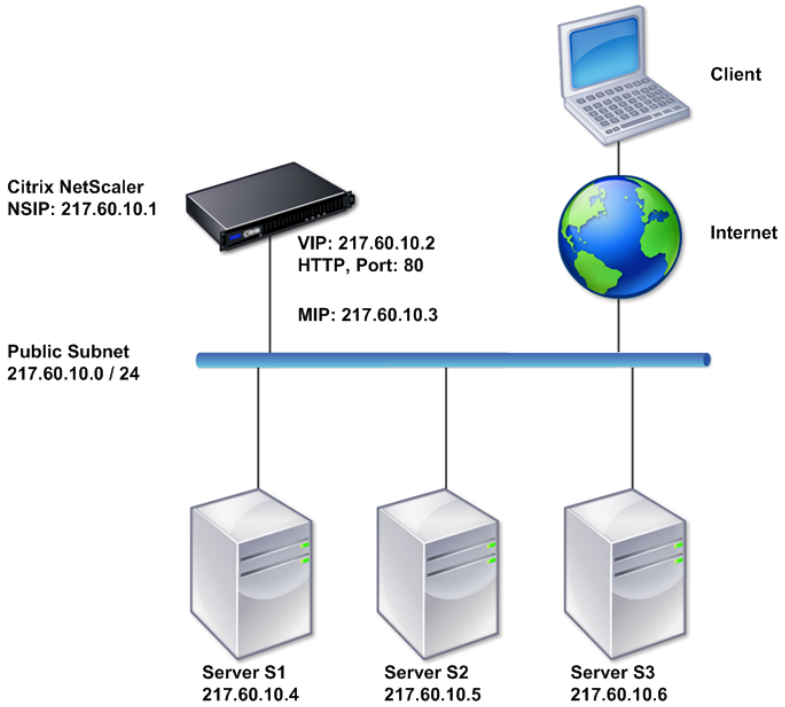
Las dos variaciones básicas de la topología de un brazo son con una sola subred y con varias subredes.

Configurar una topología de subred simple de un solo brazo

Puede utilizar una topología de un brazo con una sola subred cuando los clientes y servidores residen en la misma subred. Por ejemplo, considere un dispositivo Citrix ADC implementado en modo de un brazo para administrar los servidores S1, S2 y S3. Se configura un servidor virtual de tipo HTTP en un

dispositivo ADC y los servicios HTTP se ejecutan en los servidores. Como se muestra en la siguiente ilustración, la dirección IP de Citrix ADC (NSIP), la dirección IP asignada (MIP) y las direcciones IP del servidor se encuentran en la misma subred pública, 217.60.10.0/24.

Ilustración 3. Diagrama de topología para modo de un brazo, subred única



Para implementar un dispositivo Citrix ADC en modo de un brazo con una sola subred, siga estos pasos:

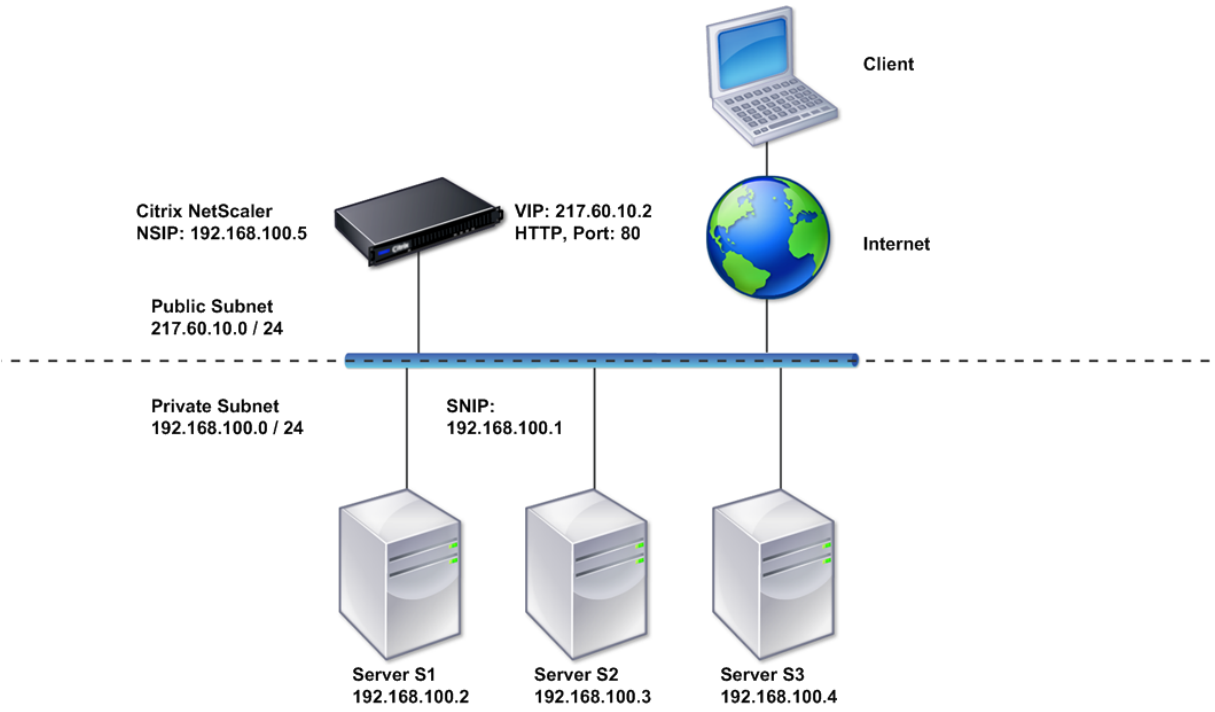
1. Configure el NSIP y la puerta de enlace predeterminada, como se describe en, tal y como se describe en Configuración de la dirección IP de Citrix ADC (NSIP).
2. Configure el servidor virtual y los servicios, tal como se describe en la sección Creación de un servidor virtual y en la sección Configuración de servicios .
3. Conecte una de las interfaces de red al conmutador.

Configurar una topología simple de subred múltiple de un brazo

Puede utilizar una topología de un brazo con varias subredes cuando los clientes y servidores residen en las diferentes subredes. Por ejemplo, considere un dispositivo Citrix ADC implementado en modo de un brazo para administrar los servidores S1, S2 y S3, con los servidores conectados para conmutar SW1 en la red. Se configura un servidor virtual de tipo HTTP en el dispositivo y los servicios HTTP

se ejecutan en los servidores. Estos tres servidores se encuentran en la subred privada, por lo que se configura una dirección IP de subred (SNIP) para comunicarse con ellos. La opción Usar dirección IP de subred (USNIP) debe estar habilitada para que el dispositivo utilice el SNIP en lugar de un MIP. Como se muestra en la siguiente ilustración, la dirección IP virtual (VIP) está en la subred pública 217.60.10.0/24; las direcciones NSIP, SNIP y IP del servidor están en la subred privada 192.168.100.0/24.

Imagen 4. Diagrama de topología para el modo de un brazo, varias subredes



Para implementar un dispositivo Citrix ADC en modo de un brazo con varias subredes, siga estos pasos:

1. Configure el NSIP y la puerta de enlace predeterminada, como se describe en Configuración de la dirección IP de NetScaler (NSIP).
2. Configure el SNIP y habilite la opción USNIP, tal como se describe en Configuración de direcciones IP de subred.
3. Configure el servidor virtual y los servicios, tal como se describe en la sección Creación de un servidor virtual y en la sección Configuración de servicios .
4. Conecte una de las interfaces de red al conmutador.

Configuración de administración del sistema

August 20, 2021

Una vez establecida la configuración inicial, puede configurar opciones para definir el comportamiento del dispositivo Citrix ADC y facilitar la administración de conexiones. Tiene una serie de opciones para manejar solicitudes y respuestas HTTP. Los modos de redirección, conexión en puente y reenvío basados en MAC están disponibles para gestionar paquetes no dirigidos al dispositivo Citrix ADC. Puede definir las funciones de las interfaces de red y agregar las interfaces. Para evitar problemas de temporización, puede sincronizar el reloj Citrix con un servidor de protocolo de hora de red (NTP). El dispositivo Citrix ADC puede funcionar en varios modos DNS, incluso como un servidor de nombres de dominio autorizado (ADNS). Puede configurar SNMP para la administración del sistema y personalizar el registro syslog de eventos del sistema. Antes de la implementación, compruebe que la configuración está completa y correcta.

Configuración del sistema

February 16, 2021

La configuración de la configuración del sistema incluye tareas básicas como la configuración de puertos HTTP para habilitar la conexión keep-alive y la descarga del servidor, establecer el número máximo de conexiones para cada servidor y establecer el número máximo de solicitudes por conexión. Puede habilitar la inserción de direcciones IP de cliente para situaciones en las que una dirección IP de proxy no es adecuada, y puede cambiar la versión de la cookie HTTP.

También puede configurar un dispositivo Citrix ADC para que abra conexiones FTP en un rango controlado de puertos en lugar de puertos efímeros para conexiones de datos. Esto mejora la seguridad, ya que abrir todos los puertos del firewall no es seguro. Puede establecer el rango entre 1.024 y 64,000.

Antes de la implementación, revise las listas de verificación para verificar su configuración. Para configurar los parámetros HTTP y el intervalo de puertos FTP, utilice la GUI de Citrix ADC.

Puede modificar los tipos de parámetros HTTP descritos en la tabla siguiente.

Tipo de parámetro: Información del puerto HTTP

Especifica: Los puertos HTTP del servidor web utilizados por los servidores administrados. Si especifica los puertos, el dispositivo realiza la conmutación de solicitud para cualquier solicitud de cliente que tenga un puerto de destino que coincida con un puerto especificado.

> Nota: Si una solicitud de cliente entrante no está destinada a un servicio o un servidor virtual configurado específicamente en el dispositivo, el puerto de destino de la solicitud debe coincidir con uno de los puertos HTTP configurados globalmente. Esto permite que el dispositivo realice la conexión keep-alive y la descarga del servidor.

Tipo de parámetro: Límites

Especifica: El número máximo de conexiones a cada servidor administrado y el número máximo de solicitudes enviadas a través de cada conexión. Por ejemplo, si establece Conexiones máximas en 500 y el dispositivo administra tres servidores, puede abrir un máximo de 500 conexiones a cada uno de los tres servidores. De forma predeterminada, el dispositivo puede crear un número ilimitado de conexiones a cualquiera de los servidores que administra. Para especificar un número ilimitado de solicitudes por conexión, establezca Máximo de solicitudes en 0.

> Nota: Si utiliza el servidor HTTP Apache, debe establecer conexiones máximas iguales al valor del parámetro MaxClients en el archivo httpd.conf de Apache. Establecer este parámetro es opcional para otros servidores web.

Tipo de parámetro: Inserción de IP de cliente

Especifica: Habilitar/inhabilitar la inserción de la dirección IP del cliente en el encabezado de solicitud HTTP. Puede especificar un nombre para el campo de encabezado en el cuadro de texto adyacente. Cuando un servidor web administrado por un dispositivo recibe una dirección IP de subred, el servidor la identifica como la dirección IP del cliente. Algunas aplicaciones necesitan la dirección IP del cliente para fines de registro o para determinar dinámicamente el contenido que va a servir el servidor web.

Puede habilitar la inserción de la dirección IP del cliente real en la solicitud de encabezado HTTP enviada desde el cliente a uno, algunos o todos los servidores administrados por el dispositivo. A continuación, puede acceder a la dirección insertada mediante una modificación menor del servidor (mediante un módulo Apache, una interfaz ISAPI o una interfaz NSAPI).

Tipo de parámetro: Versión de cookie

Especifica: La versión de la cookie HTTP que se va a utilizar cuando la persistencia de COOKIEINSERT está configurada en un servidor virtual. El valor predeterminado, la versión 0, es el tipo más común en Internet. Alternativamente, puede especificar la versión 1.

Tipo de parámetro: Solicitudes/Respuestas

Especifica: Opciones para manejar ciertos tipos de solicitudes y habilitar/inhabilitar el registro de respuestas de error HTTP.

Tipo de parámetro: Inserción de encabezado de servidor

Especifica: Inserte un encabezado de servidor en las respuestas HTTP generadas por Citrix ADC.

Para configurar los parámetros HTTP mediante la GUI, siga estos pasos:

1. En el panel de navegación, expanda **Sistema**y, a continuación, haga clic en **Configuración**.
2. En el panel de detalles, en **Configuración**, haga clic en **Cambiar parámetros HTTP**.
3. En el cuadro de diálogo **Configurar parámetros HTTP**, especifique los valores para algunos o todos los parámetros que aparecen bajo los encabezados enumerados en la tabla anterior.
4. Haga clic en **Aceptar**.

Para establecer el intervalo de puertos FTP mediante la GUI, siga estos pasos:

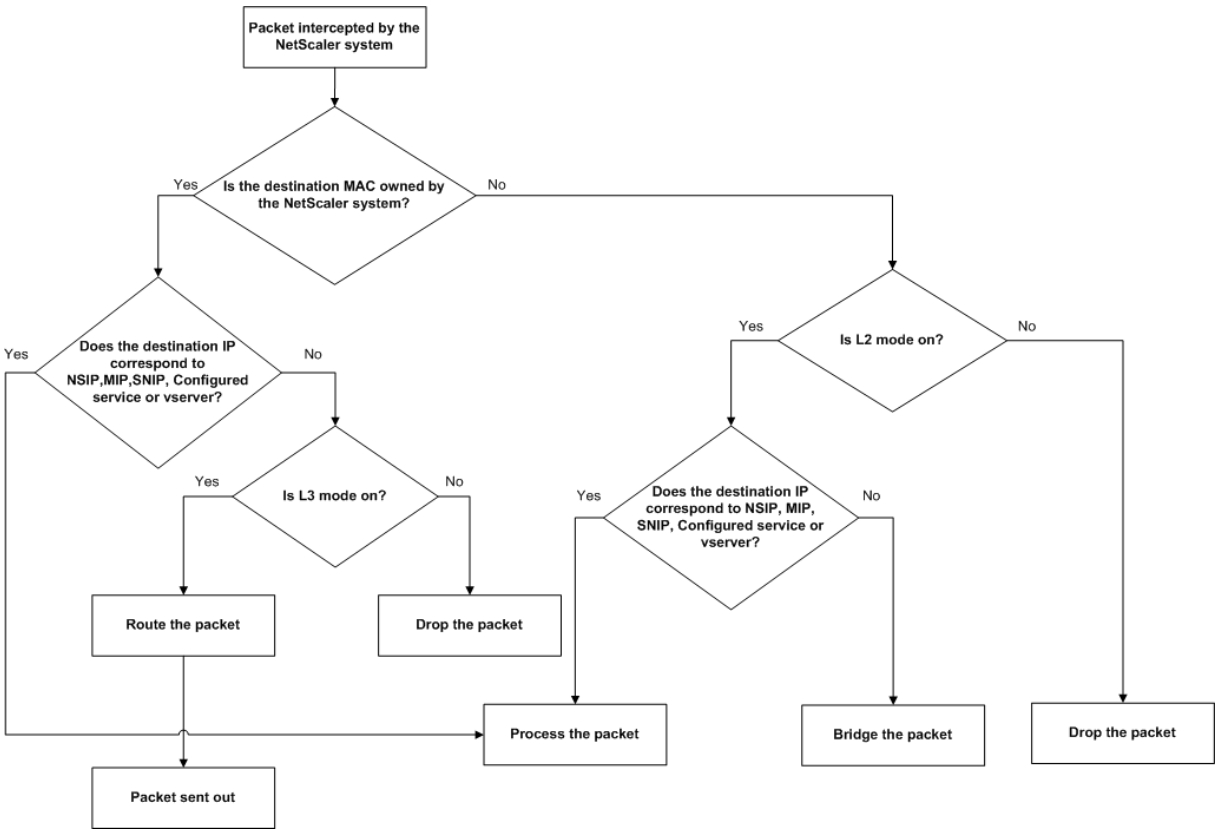
1. En el panel de navegación, expanda **Sistema** y, a continuación, haga clic en **Configuración**
2. En el panel de detalles, en **Configuración**, haga clic en **Cambiar la configuración global del sistema**.
3. En **Rango de puertos FTP,** en los cuadros de texto **Puerto inicial** y **Puerto final**, escriba los números de puerto más bajos y más altos, respectivamente, para el rango que quiera especificar (por ejemplo, 5000 y 6000).
4. Haga clic en **Aceptar**.

Modos de reenvío de paquetes

April 5, 2022

El dispositivo Citrix ADC puede enrutar o conectar paquetes que no están destinados a una dirección IP propiedad del dispositivo (es decir, la dirección IP no es el NSIP, un MIP, un SNIP, un servicio configurado o un servidor virtual configurado). De forma predeterminada, el modo L3 (redirección) está habilitado y el modo L2 (puente) está inhabilitado, pero puede cambiar la configuración. El siguiente diagrama de flujo muestra cómo el dispositivo evalúa los paquetes y los procesa, enruta, conecta o elimina.

Ilustración 1. Interacción entre los modos de capa 2 y capa 3



Un dispositivo puede usar los siguientes modos para reenviar los paquetes que recibe:

- Modo de capa 2 (L2)
- Modo de capa 3 (L3)
- Modo de reenvío basado en MAC

Habilitar y inhabilitar el modo de capa 2

El modo de capa 2 controla la función de reenvío (puente) de capa 2. Puede usar este modo para configurar un dispositivo Citrix ADC para que se comporte como un dispositivo de capa 2 y conecte los paquetes que no están destinados a él. Cuando este modo está habilitado, los paquetes no se reenvían a ninguna de las direcciones MAC, porque los paquetes pueden llegar a cualquier interfaz del dispositivo y cada interfaz tiene su propia dirección MAC.

Con el modo de capa 2 inhabilitado (que es el valor predeterminado), el dispositivo descarta paquetes que no están destinados a una de sus direcciones MAC. Si se instala otro dispositivo de capa 2 en paralelo con el dispositivo, el modo de capa 2 debe estar inhabilitado para evitar bucles de conexión en puente (capa 2). Puede usar la utilidad de configuración o la línea de comandos para habilitar el modo de capa 2.

Nota: El dispositivo no admite el Spanning Tree Protocol. Para evitar bucles, si habilita el modo L2, no conecte dos interfaces del dispositivo al mismo dominio de transmisión.

Para habilitar o inhabilitar el modo de capa 2 mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para habilitar/inhabilitar el modo de capa 2 y verificar que se haya habilitado/inhabilitado:

- enable ns mode <Mode>
- disable ns mode <Mode>
- mostrar modo ns

Ejemplos

```
    > enable ns mode l2
    Done
    > show ns mode

    Mode Acronym Status
    ------- ------- ------
    1) Fast Ramp FR ON
    2) Layer 2 mode L2 ON
    .
    .
    .
    Done
    >

    > disable ns mode l2
    Done
    > show ns mode

    Mode Acronym Status
    ------- ------- ------
    1) Fast Ramp FR ON
    2) Layer 2 mode L2 OFF
    .
    .
    .
    Done
    >
<!--NeedCopy-->
```

Para habilitar o inhabilitar el modo de capa 2 mediante la interfaz gráfica de usuario

1. En el panel de navegación, expanda **Sistema** y, a continuación, haga clic en **Configuración**.
2. En el panel de detalles, en **Modos** y **funciones**, haga clic en **Configurar modos**.

3. En el cuadro de diálogo **Configurar modos**, para habilitar el modo de capa 2, marque la casilla **Modo de capa 2**. Para inhabilitar el modo Capa 2, desactive la casilla de verificación.
4. Haga clic en **Aceptar**. El mensaje **¿Habilitar los modos de activación/desactivación?** aparece en el panel de detalles.
5. Haga clic en **Sí**.

Habilitar y inhabilitar el modo de capa 3

El modo de capa 3 controla la función de reenvío de capa 3. Puede utilizar este modo para configurar un dispositivo Citrix ADC para ver su tabla de redirección y reenviar paquetes que no están destinados a él. Con el modo de capa 3 habilitado (que es el predeterminado), el dispositivo realiza búsquedas en la tabla de rutas y reenvía todos los paquetes que no están destinados a ninguna dirección IP propiedad del dispositivo. Si inhabilita el modo de capa 3, el dispositivo descarta estos paquetes.

Habilitar o inhabilitar el modo de capa 3 mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para habilitar/inhabilitar el modo de capa 3 y verificar que se haya habilitado/inhabilitado:

- enable ns mode <Mode>
- disable ns mode <Mode>
- mostrar modo ns

Ejemplos

```
> enable ns mode l3
Done
> show ns mode

Mode Acronym Status
------- ------- ------
1) Fast Ramp FR ON
2) Layer 2 mode L2 OFF
.
.
.
9) Layer 3 mode (ip forwarding) L3 ON
.
.
.
Done
```



```
17      >
18
19      > disable ns mode l3
20      Done
21      > show ns mode
22
23      Mode Acronym Status
24      ------- ------- ------
25      1) Fast Ramp FR ON
26      2) Layer 2 mode L2 OFF
27      .
28      .
29      .
30      9) Layer 3 mode (ip forwarding) L3 OFF
31      .
32      .
33      .
34      Done
35      >
36  <!--NeedCopy-->
```

Habilitar o inhabilitar el modo de capa 3 mediante la interfaz gráfica de usuario

1. En el panel de navegación, expanda **Sistema** y, a continuación, haga clic en **Configuración**.
2. En el panel de detalles, en **Modos y funciones**, haga clic en **Configurar modos**.
3. En el cuadro de diálogo **Configurar modos**, para habilitar el modo de capa 3, marque la casilla **Modo de capa 3 (reenvío de IP)**. Para inhabilitar el modo Capa 3, desactive la casilla de verificación.
4. Haga clic en **Aceptar**. El mensaje **¿Habilitar los modos de activación/desactivación?** aparece en el panel de detalles.
5. Haga clic en **Sí**.

Habilitar y inhabilitar el modo de reenvío basado en

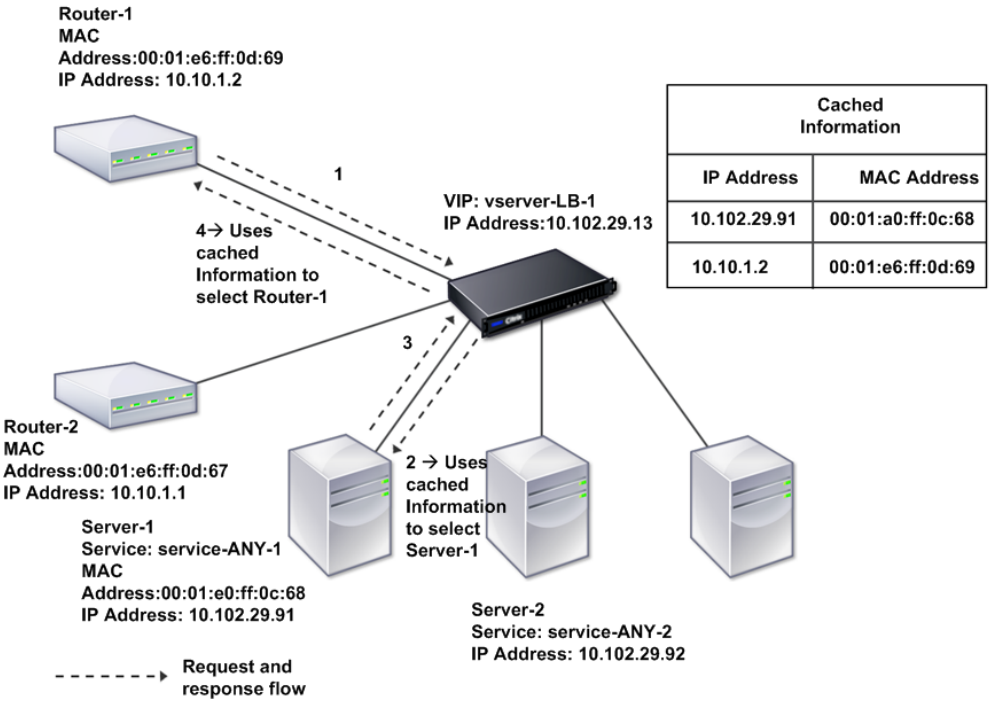
Puede usar el reenvío basado en MAC para procesar el tráfico de manera más eficiente y evitar búsquedas de múltiples rutas o ARP al reenviar paquetes, ya que el dispositivo Citrix ADC recuerda la dirección MAC del origen. Para evitar varias búsquedas, el dispositivo almacena en caché la dirección MAC de origen de cada conexión para la que realiza una búsqueda ARP y devuelve los datos a la misma dirección MAC.

El reenvío basado en MAC es útil cuando se utilizan dispositivos VPN porque el dispositivo garantiza que todo el tráfico que fluye a través de una VPN en particular pase a través del mismo dispositivo

VPN.

La siguiente ilustración muestra el proceso de reenvío basado en Mac.

Ilustración 2. Proceso de reenvío basado en MAC



Cuando el reenvío basado en MAC está habilitado, el dispositivo almacena en caché la dirección MAC de:

- El origen (un dispositivo de transmisión, como un enrutador, un firewall o un dispositivo VPN) de la conexión entrante.
- El servidor que responde a las solicitudes.

Cuando un servidor responde a través de un dispositivo, el dispositivo establece la dirección MAC de destino del paquete de respuesta en la dirección en caché, lo que garantiza que el tráfico fluya de manera simétrica y, a continuación, reenvía la respuesta al cliente. El proceso omite las funciones de búsqueda en la tabla de rutas y de búsqueda ARP. Sin embargo, cuando un dispositivo inicia una conexión, utiliza las tablas de ruta y ARP para la función de búsqueda. Para habilitar el reenvío basado en MAC, use la utilidad de configuración o la línea de comandos.

Algunas implementaciones requieren que las rutas de entrada y salida fluyan a través de enrutadores diferentes. En estas situaciones, el reenvío basado en MAC rompe el diseño de la topología. Para un sitio de equilibrio de carga de servidor global (GSLB) que requiera que las rutas entrantes y salientes

fluyan a través de enrutadores diferentes, debe inhabilitar el reenvío basado en MAC y utilizar el enrutador predeterminado del dispositivo como enrutador saliente.

Con el reenvío basado en MAC inhabilitado y la conectividad de capa 2 o capa 3 habilitada, una tabla de rutas puede especificar enrutadores separados para las conexiones salientes y entrantes. Para inhabilitar el reenvío basado en MAC, use la utilidad de configuración o la línea de comandos.

Habilitar o inhabilitar el reenvío basado en MAC mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para habilitar/inhabilitar el modo de reenvío basado en MAC y verificar que se haya habilitado/inhabilitado:

- <enable ns mode <Mode>
- <disable ns mode <Mode>
- <show ns mode
  Ejemplo

  “‘ pre codeblock

  ```
  enable ns mode mbf
  Done
  show ns mode
  ```

  ```
  1   Mode                          Acronym           Status
  2   -------                       -------           ------   1)  Fast
      Ramp                     FR                ON   2)  Layer 2
      mode                  L2                OFF   .   .   .   6)
      MAC-based forwarding        MBF               ON   .   .   .
        Done  >
  ```

  ```
  disable ns mode mbf
  Done
  show ns mode
  ```

  ```
  1   Mode                          Acronym           Status
  2   -------                       -------           ------   1)  Fast
      Ramp                     FR                ON   2)  Layer 2
      mode                  L2                OFF   .   .   .   6)
      MAC-based forwarding        MBF               OFF   .   .   .
         Done  >  <!--NeedCopy--> ```
  ```


Para habilitar o inhabilitar el reenvío basado en MAC mediante la interfaz gráfica de usuario

1. En el panel de navegación, expanda **Sistema** y, a continuación, haga clic en **Configuración**.
2. En el panel de detalles, en el grupo **Modos y funciones**, haga clic en **Configurar modos**.
3. En el cuadro de diálogo **Configurar modos**, para habilitar el modo de reenvío basado en MAC, seleccione la casilla **Reenvío basado en MAC**. Para inhabilitar el modo de reenvío basado en MAC, desactive la casilla de verificación.
4. Haga clic en **Aceptar**. El mensaje **¿Habilitar los modos de activación/desactivación?** aparece en el panel de detalles.
5. Haga clic en **Sí**.

Interfaces de red

August 20, 2021

Las interfaces Citrix ADC están numeradas en notación de ranura/puerto. Además de modificar las funciones de las interfaces individuales, puede configurar LAN virtuales para restringir el tráfico a grupos específicos de hosts. También puede agregar enlaces en canales de alta velocidad.

LAN virtuales

El dispositivo Citrix ADC admite el puerto (capa 2) y las LAN virtuales (VLAN) etiquetadas IEEE802.1Q. Las configuraciones de VLAN son útiles cuando se necesita restringir el tráfico a determinados grupos de estaciones. Puede configurar una interfaz de red para que pertenezca a varias VLAN mediante el etiquetado IEEE 802.1q.

Puede enlazar las VLAN configuradas a subredes IP. El dispositivo ADC (si está configurado como el enrutador predeterminado para los hosts de las subredes) realiza el reenvío de IP entre estas VLAN.

El dispositivo Citrix ADC admite los siguientes tipos de VLAN.

- VLAN predeterminada

  De forma predeterminada, las interfaces de red de un dispositivo Citrix ADC se incluyen en una única VLAN basada en puertos como interfaces de red sin etiquetas. Esta VLAN predeterminada posee un VID de 1 y existe de forma permanente. No se puede eliminar y su VID no se puede cambiar.

- VLAN basadas en puertos

  Un conjunto de interfaces de red que comparten un dominio de difusión de capa 2 común y exclusivo definen la pertenencia a una VLAN basada en puerto. Puede configurar varias VLAN basadas en puertos. Cuando agrega una interfaz a una VLAN nueva como miembro sin etiqueta, se elimina automáticamente de la VLAN predeterminada.

- VLAN etiquetada

  Una interfaz de red puede ser un miembro etiquetado o no etiquetado de una VLAN. Cada interfaz de red es un miembro sin etiquetas de una sola VLAN (su VLAN nativa). La interfaz de red sin etiquetas reenvía las tramas de la VLAN nativa como tramas sin etiquetas. Una interfaz de red etiquetada puede formar parte de más de una VLAN. Cuando configure el etiquetado, asegúrese de que ambos extremos del vínculo tengan la configuración de VLAN coincidente. Puede utilizar la utilidad de configuración para definir una VLAN etiquetada (nsvlan) que pueda tener cualquier puerto enlazado como miembros etiquetados de la VLAN. La configuración de esta VLAN requiere un reinicio del dispositivo ADC y, por lo tanto, debe realizarse durante la configuración inicial de la red.

Vincular canales agregados

La agregación de enlaces combina datos entrantes de varios puertos en un único enlace de alta velocidad. La configuración del canal agregado de vínculos aumenta la capacidad y la disponibilidad del canal de comunicación entre un dispositivo Citrix ADC y otros dispositivos conectados. Un enlace agregado también se conoce como canal.

Cuando una interfaz de red está enlazada a un canal, los parámetros del canal tienen prioridad sobre los parámetros de la interfaz de red Una interfaz de red puede estar vinculada a un solo canal. La vinculación de una interfaz de red a un canal agregado de enlace cambia la configuración de la VLAN. Es decir, la vinculación de interfaces de red a un canal las elimina de las VLAN a las que pertenecían originalmente y las agrega a la VLAN predeterminada. Sin embargo, puede enlazar el canal a la VLAN antigua o a una nueva. Por ejemplo, si tiene interfaces de red enlazadas 1/2 y 1/3 a una VLAN con ID 2 y, a continuación, las vincula para vincular el canal agregado LA/1, las interfaces de red se mueven a la VLAN predeterminada, pero puede vincularlas a VLAN 2.

Nota: También puede utilizar el Protocolo de control de agregación de enlaces (LACP) para configurar la agregación de enlaces. Para obtener más información, consulte Configuración de la agregación de vínculos mediante el protocolo de control de agregación de vínculos.

Sincronización de relojes

April 5, 2022

Puede configurar el dispositivo Citrix ADC para que sincronice su reloj local con un servidor de Protocolo de hora de red (NTP). Esto garantiza que su reloj tenga la misma configuración de fecha y hora que los demás servidores de la red. NTP utiliza el puerto 123 del Protocolo de datagramas de usuario (UDP) como capa de transporte. Agregue servidores NTP en el archivo de configuración NTP para que el dispositivo reciba actualizaciones periódicas de estos servidores.

Si no tiene un servidor NTP local, puede encontrar una lista de servidores NTP públicos de acceso abierto en el sitio oficial de NTP en http://www.ntp.org.

Para configurar la sincronización del reloj en su dispositivo, siga estos pasos:

1. Inicie sesión en la línea de comandos e introduzca el comando shell.
2. En el símbolo del shell, copie el archivo ntp.conf del directorio /etc al directorio /nsconfig. Si el archivo ya existe en el directorio /nsconfig, asegúrese de eliminar las siguientes entradas del archivo ntp.conf:

   ```
   restrict localhost

   restrict 127.0.0.2
   ```

   Estas entradas solo son obligatorias si desea ejecutar el dispositivo como un servidor horario. Sin embargo, esta función no se admite en el dispositivo Citrix ADC.
3. Modifique /nsconfig/ntp.conf escribiendo la dirección IP del servidor NTP deseado en el servidor del archivo y restrinja las entradas.
4. Cree un archivo llamado rc.netscaler en el directorio /nsconfig, si el archivo aún no existe en el directorio.
5. Modifique /nsconfig/rc.netscaler agregando la siguiente entrada: `/bin/sh /etc/ntpd_ctl full_start`.

   Esta entrada inicia el servicio ntpd y comprueba el archivo ntp.conf.

   Si no desea sincronizar forzosamente la hora cuando hay una gran diferencia, puede establecer la fecha manualmente y luego iniciar ntpd nuevamente. Puede comprobar la diferencia horaria entre el dispositivo y el servidor de tiempo ejecutando el siguiente comando en el shell:

   ```
   1 ntpdate -q <IP address or domain name of the NTP server>
   2 <!--NeedCopy-->
   ```

6. Reinicie el dispositivo para habilitar la sincronización del reloj.

   Nota: Si desea iniciar la sincronización horaria sin reiniciar el dispositivo, introduzca uno de los siguientes comandos en el símbolo del sistema de comandos:

   ```
   1 /usr/sbin/ntpd -c /nsconfig/ntp.conf -g -p /var/run/ntpd.pid -l /
       var/log/ntpd.log &
   2
   3 or
   4
   ```



```
5 /bin/sh /etc/ntpd_ctl full_start
6
7 <!--NeedCopy-->
```

Configuración de DNS

July 8, 2022

Puede configurar un dispositivo Citrix ADC para que funcione como un servidor de nombres de dominio autoritativo (ADNS), un servidor proxy DNS, un solucionador final o un reenviador. Puede agregar registros de recursos DNS, como registros SRV, registros AAAA, registros A, registros MX, registros NS, registros CNAME, registros PTR y registros SOA. Además, el dispositivo puede equilibrar la carga en los servidores DNS externos.

Una práctica común es configurar un dispositivo como reenviador. Para esta configuración, debe agregar servidores de nombres externos. Después de agregar los servidores externos, debe comprobar que la configuración es correcta.

Puede agregar, quitar, habilitar o inhabilitar servidores de nombres externos. Puede crear un servidor de nombres especificando su dirección IP o puede configurar un servidor virtual existente como servidor de nombres.

Al agregar servidores de nombres, puede especificar direcciones IP o direcciones IP virtuales (VIP). Si utiliza direcciones IP, el dispositivo equilibra la carga de las solicitudes a los servidores de nombres configurados por turnos. Si usa direcciones VIP, puede especificar cualquier método de equilibrio de carga.

Agregar un servidor de nombres mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para agregar un servidor de nombres y verificar la configuración:

- <add dns nameServer \<IP\>
- <show dns nameServer \<IP\>

Ejemplo

```
1 > add dns nameServer 10.102.29.10
2  Done
3 > show dns nameServer 10.102.29.10
4 1)       10.102.29.10  -  State: DOWN
```



```
5    Done
6
7   <!--NeedCopy-->
```

Agregar un servidor de nombres mediante la GUI

1. Vaya a **Administración del tráfico** > **DNS** > **Servidores de nombres**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En el cuadro de diálogo **Crear servidor de nombres**, seleccione **Dirección IP**.
4. En el cuadro de texto **Dirección IP**, escriba la dirección IP del servidor de nombres (por ejemplo, 10.102.29.10). Si piensa agregar un servidor de nombres externo, desmarque la casilla **Local**.
5. Haga clic en **Crear** y, a continuación, en **Cerrar**.
6. Compruebe que el servidor de nombres que ha agregado aparece en el panel **Servidores de nombres**.

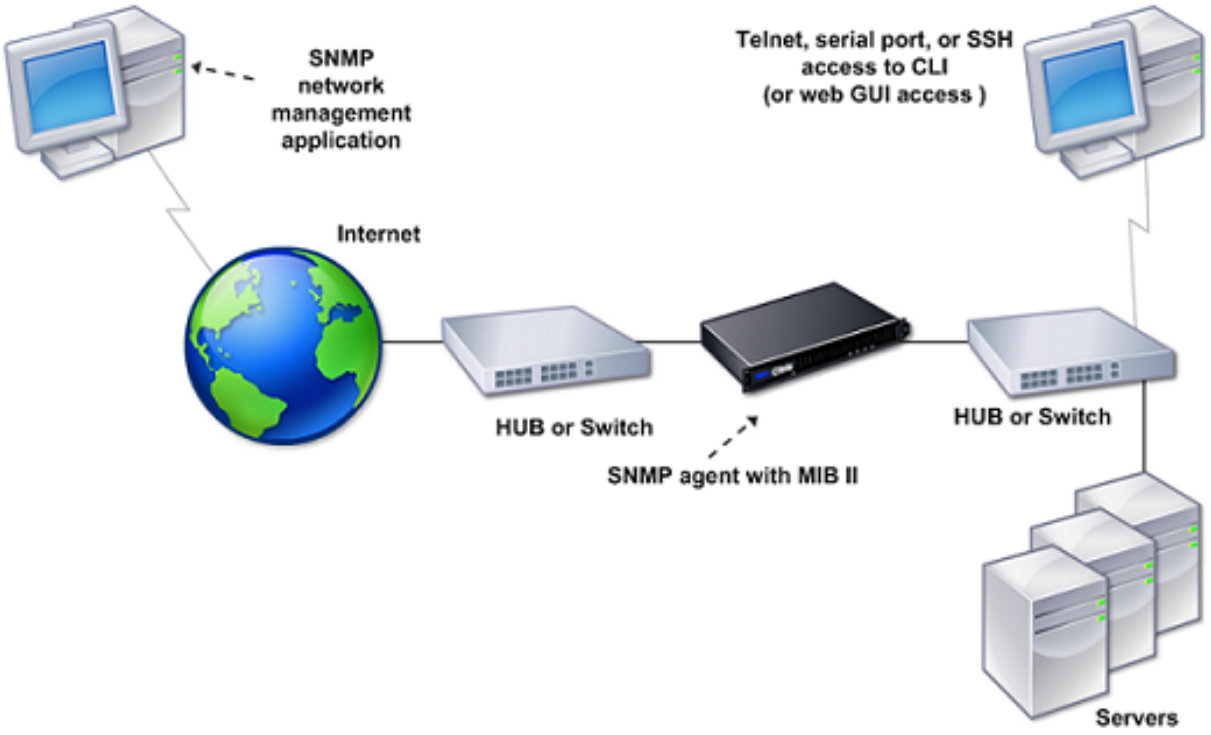
Configuración SNMP

August 20, 2021

La aplicación de administración de red Simple Network Management Protocol (SNMP), que se ejecuta en un equipo externo, consulta al agente SNMP en el dispositivo Citrix ADC. El agente busca en la base de información de administración (MIB) los datos solicitados por la aplicación de administración de red y los envía a la aplicación.

La supervisión SNMP utiliza mensajes de captura y alarmas. Los mensajes de capturas SNMP son eventos asincrónicos que genera el agente para señalar condiciones anormales, que se indican mediante alarmas. Por ejemplo, si quiere que se le informe cuando la utilización de la CPU es superior al 90%, puede configurar una alarma para esa condición. En la siguiente ilustración se muestra una red con un dispositivo Citrix ADC que tiene SNMP habilitado y configurado.

Ilustración 1. SNMP en el dispositivo Citrix ADC



El agente SNMP de un dispositivo Citrix ADC admite SNMP versión 1 (SNMPv1), SNMP versión 2 (SNMPv2) y SNMP versión 3 (SNMPv3). Dado que funciona en modo bilingüe, el agente puede manejar consultas SNMPv2, como Get-Bulk, y consultas SNMPv1. El agente SNMP también envía capturas compatibles con SNMPv2 y admite tipos de datos SNMPv2, como counter64. Los administradores SNMPv1 (programas de otros servidores que solicitan información SNMP del dispositivo ADC) utilizan el archivo NS-MIB-smiv1.mib al procesar consultas SNMP. Los administradores SNMPv2 utilizan el archivo NS-MIB-smiv2.mib.

El dispositivo Citrix ADC admite las siguientes MIB específicas de la empresa:

- Subconjunto de grupos MIB-2 estándar. Proporciona grupos MIB-2 SYSTEM, IF, ICMP, UDP y SNMP.
- Una MIB de empresa del sistema. Proporciona configuración y estadísticas específicas del sistema.

Para configurar SNMP, especifique qué administradores pueden consultar el agente SNMP, agregar detectores de capturas SNMP que recibirán los mensajes de captura SNMP y configurar alarmas SNMP.

Agregar administradores SNMP

Puede configurar una estación de trabajo que ejecute una aplicación de administración que cumpla con las versiones 1, 2 o 3 de SNMP para acceder a un dispositivo. Tal estación de trabajo se llama administrador SNMP. Si no especifica un administrador SNMP en el dispositivo, el dispositivo acepta consultas SNMP de todas las direcciones IP de la red y responde a ellas. Si configura uno o varios admin-

istradores SNMP, el dispositivo acepta y responde a las consultas SNMP solo desde esas direcciones IP específicas. Al especificar la dirección IP de un administrador SNMP, puede utilizar el parámetro máscara de red para conceder acceso desde subredes completas. Puede agregar un máximo de 100 administradores o redes SNMP. Para agregar un administrador SNMP mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para agregar un administrador SNMP y verificar la configuración:

```
add snmp manager <IPAddress> ... [-netmask <netmask>]
show snmp manager <IPAddress>
```

Ejemplo:

```
1 add snmp manager 10.102.29.5 -netmask 255.255.255.255
2 Done
3 show snmp manager 10.102.29.5
4 10.102.29.5 255.255.255.255
5 Done
6 <!--NeedCopy-->
```

Para agregar un administrador SNMP mediante la GUI:

1. En el panel de navegación, expanda **Sistema**, **SNMP** y, a continuación, haga clic en **Administradores**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En el cuadro de diálogo **Agregar Administrador SNMP**, en el cuadro de texto **Dirección IP**, escriba la dirección IP de la estación de trabajo que ejecuta la aplicación de administración (por ejemplo, 10.102.29.5).
4. Haga clic en **Crear** y, a continuación, en **Cerrar**.
5. Compruebe que el administrador SNMP que agregó aparezca en la sección **Detalles** de la parte inferior del panel.

Agregar detectores de capturas SNMP

Después de configurar las alarmas, debe especificar el detector de captura al que el dispositivo enviará los mensajes de captura. Además de especificar parámetros como la dirección IP y el puerto de destino de la escucha de captura, puede especificar el tipo de captura (genérico o específico) y la versión SNMP.

Puede configurar un máximo de 20 detectores de captura para recibir capturas genéricas o específicas.

Para agregar una escucha de captura SNMP mediante la CLI

En el símbolo del sistema, escriba el siguiente comando para agregar una captura SNMP y compruebe que se ha agregado:

- `add snmp trap specific <IP>`
- `show snmp trap`

Ejemplo:

```
Trap type: SPECIFIC
Destination IP: 10.102.29.3
TD: 0
Destination Port: 162
Source IP: NetScaler IP
Version: V2
Min-Severity: -
AllPartition: DISABLED
Community: public
<!--NeedCopy-->
```

Para agregar un detector de capturas SNMP mediante la interfaz gráfica de usuario

1. En el panel de navegación, expanda Sistema, expanda **SNMP** y, a continuación, haga clic en **Capturas**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En el cuadro de diálogo **Crear destino de captura SNMP**, en el cuadro de texto **Dirección IP de destino**, escriba la dirección IP (por ejemplo, 10.102.29.3).
4. Haga clic en **Create** y, luego, en **Close**.
5. Compruebe que la captura SNMP que agregó aparece en la sección **Detalles** en la parte inferior del panel.

Configurar alarmas SNMP

Las alarmas se configuran para que el dispositivo genere un mensaje de captura cuando se produce un evento correspondiente a una de las alarmas. La configuración de una alarma consiste en habilitar la alarma y establecer el nivel de gravedad en el que se genera una trampa. Existen cinco niveles de gravedad: Crítico, Mayor, Menor, Advertencia e Informativo. Una captura solo se envía cuando la gravedad de la alarma coincide con la gravedad especificada para la captura.

Algunas alarmas están habilitadas de forma predeterminada. Si inhabilita una alarma SNMP, el dispositivo no generará mensajes de captura cuando se produzcan los eventos correspondientes. Por

ejemplo, si inhabilita la alarma SNMP con error de inicio de sesión, el dispositivo no generará un mensaje de captura cuando se produzca un error de inicio de sesión.

Para habilitar o inhabilitar una alarma mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para habilitar o inhabilitar una alarma y compruebe que se ha habilitado o inhabilitado:

- set snmp alarm <trapName> [-state ENABLED | DISABLED]
- show snmp alarm <trapName>

  Ejemplo

```
set snmp alarm LOGIN-FAILURE -state ENABLED
Done
show snmp alarm LOGIN-FAILURE
Alarm Alarm Threshold Normal Threshold Time State Severity Logging
----- --------------- ---------------- ---- -------- --------- --------
LOGIN-FAILURE N/A N/A N/A ENABLED - ENABLED
Done
<!--NeedCopy-->
```

Para establecer la gravedad de la alarma mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para establecer la gravedad de la alarma y compruebe que la gravedad se ha establecido correctamente:

- set snmp alarm <trapName> [-severity <severity>]
- show snmp alarm <trapName>

Ejemplo:

```
set snmp alarm LOGIN-FAILURE -severity Major
Done
show snmp alarm LOGIN-FAILURE
Alarm Alarm Threshold Normal Threshold Time State Severity Logging
----- --------------- ---------------- ---- -------- --------- --------
LOGIN-FAILURE N/A N/A N/A ENABLED Major ENABLED
Done
<!--NeedCopy-->
```


Para configurar alarmas mediante la interfaz gráfica de usuario

1. En el panel de navegación, expanda **Sistema**, expanda SNMPy, a continuación, haga clic en **Alarmas**.
2. En el panel de detalles, seleccione una alarma (por ejemplo, LOGIN-FAILURE) y, a continuación, haga clic en **Abrir**.
3. En el cuadro de diálogo **Configurar alarma SNMP**, para habilitar la alarma, seleccione Activado en la lista desplegable **Estado**. Para desactivar la alarma, seleccione Inhabilitado.
4. En la lista desplegable **Gravedad**, seleccione una opción de gravedad (por ejemplo, Mayor).
5. Haga clic en **Aceptar** y, a continuación, haga clic en **Cerrar**.
6. Compruebe que los parámetros de la alarma SNMP configurada estén correctamente configurados viendo la sección **Detalles** en la parte inferior del panel.

Verificar la configuración

January 12, 2021

Una vez que haya terminado de configurar el sistema, complete las siguientes listas de comprobación para verificar la configuración.

Lista de comprobación de configuración

- La compilación que se ejecuta es:
- No existen problemas de incompatibilidad. (Los problemas de incompatibilidad se documentan en las notas de la versión de la compilación).
- Los ajustes del puerto (velocidad, dúplex, control de flujo, supervisión) son los mismos que el puerto del conmutador.
- Se han configurado suficientes direcciones IP de SNIP para admitir todas las conexiones del lado del servidor durante las horas punta.
  - El número de direcciones IP de SNIP configuradas es:__
  - El número esperado de conexiones simultáneas de servidor es:
    [] 62.000 [] 124.000 [] Otro____

Lista de comprobación de configuración de topología

Las rutas se han utilizado para resolver servidores en otras subredes.

Las rutas introducidas son:

_____

- Si el dispositivo Citrix ADC se encuentra en una topología público-privada, se ha configurado NAT inversa.
- La configuración de conmutación por error (alta disponibilidad) configurada en el dispositivo ADC se resuelve en una configuración de uno o dos brazos. Todas las interfaces de red no utilizadas se han inhabilitado:

  _____

- Si el dispositivo ADC se coloca detrás de un equilibrador de carga externo, la directiva de equilibrio de carga del equilibrador de carga externo no es la “conexión mínima”.

  La directiva de equilibrio de carga configurada en el equilibrador de carga externo es:

  _____

- Si el dispositivo ADC se coloca frente a un firewall, el tiempo de espera de la sesión en el firewall se establece en un valor superior o igual a 300 segundos.

  Nota: El tiempo de espera de conexión inactiva TCP en un dispositivo Citrix ADC es de 360 segundos. Si el tiempo de espera del firewall también se establece en 300 segundos o más, el dispositivo puede realizar la multiplexación de conexiones TCP de manera efectiva porque las conexiones no se cerrarán antes.

  El valor configurado para el tiempo de espera de la sesión es: _____

Lista de comprobación de configuración del servidor

- “Keep-Alive” se ha habilitado en todos los servidores.

  El valor configurado para el tiempo de espera de mantenimiento vivo es: _____
- La Gateway predeterminada se ha establecido en el valor correcto. (La Gateway predeterminada debe ser un dispositivo Citrix ADC o un enrutador ascendente.) La Gateway predeterminada es:

  _____

- La configuración del puerto del servidor (velocidad, dúplex, control de flujo, supervisión) es la misma que la configuración del puerto del conmutador.

  _____

- Si se utiliza Microsoft® Internet Information Server, el almacenamiento en búfer está habilitado en el servidor.
- Si se utiliza un servidor Apache, el parámetro MaxConn (número máximo de conexiones) se configura en el servidor y en el dispositivo Citrix ADC.

  El valor MaxConn (número máximo de conexiones) que se ha establecido es:

- Si se utiliza Netscape Enterprise Server, las solicitudes máximas por parámetro de conexión se establecen en el dispositivo Citrix ADC. El número máximo de solicitudes por valor de conexión que se ha establecido es:

Lista de comprobación de configuración de funciones de software

- ¿Es necesario desactivar la función de modo Capa 2? (Inhabilite si otro dispositivo de capa 2 funciona en paralelo con un dispositivo Citrix ADC).

  Motivo para habilitar o inhabilitar:

- ¿Es necesario desactivar la función de reenvío basada en Mac? (Si la dirección MAC utilizada por el tráfico de retorno es diferente, debe inhabilitarse).

  Motivo para habilitar o inhabilitar:

- ¿Es necesario inhabilitar la reutilización basada en host? (¿Hay alojamiento virtual en los servidores?)

  Motivo para habilitar o inhabilitar:

- ¿Es necesario cambiar la configuración predeterminada de la función de protección contra sobretensiones?

  Motivo para cambiar o no cambiar:

Lista de comprobación de acceso

- Las direcciones IP del sistema se pueden hacer ping desde la red del lado del cliente.
- Las direcciones IP del sistema se pueden hacer ping desde la red del lado del servidor.
- Los servidores administrados se pueden hacer ping a través del Citrix ADC.
- Los hosts de Internet se pueden hacer ping desde los servidores administrados.
- Se puede acceder a los servidores administrados a través del explorador.
- Se puede acceder a Internet desde servidores administrados mediante el explorador.
- Se puede acceder al sistema mediante SSH.
- El acceso de administrador a todos los servidores administrados está funcionando.

> Nota: Cuando utilice la utilidad ping, asegúrese de que el servidor con ping tiene ICMP ECHO habilitado o que el ping no se realizará correctamente.

Lista de comprobación del firewall

Se han cumplido los siguientes requisitos de firewall:

- UDP 161 (SNMP)
- UDP 162 (captura SNMP)
- TCP/UDP 3010 (GUI)
- HTTP 80 (GUI)
- TCP 22 (SSH)

Tráfico de equilibrio de carga en un dispositivo Citrix ADC

August 20, 2021

La función de equilibrio de carga distribuye las solicitudes de los clientes en varios servidores para optimizar la utilización de los recursos. En un caso real con un número limitado de servidores que proporcionan servicio a un gran número de clientes, un servidor puede sobrecargarse y degradar el rendimiento de la comunidad de servidores. Un dispositivo Citrix ADC utiliza criterios de equilibrio de carga para evitar cuellos de botella al reenviar cada solicitud de cliente al servidor más adecuado para gestionar la solicitud cuando llegue.

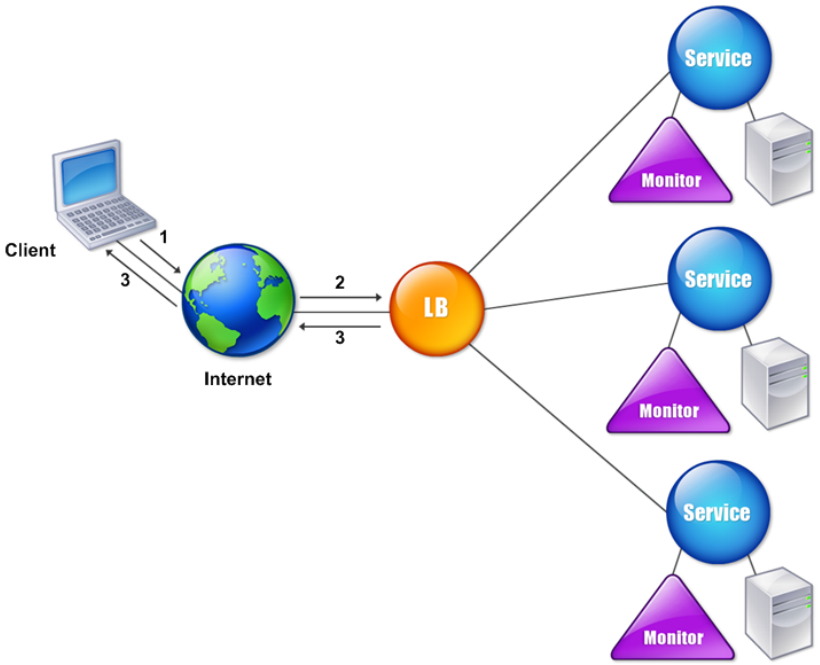
Para configurar el equilibrio de carga, debe definir un servidor virtual para proxy de varios servidores en una comunidad de servidores y equilibrar la carga entre ellos.

Cuando un cliente inicia una conexión con el servidor, un servidor virtual termina la conexión del cliente e inicia una nueva conexión con el servidor seleccionado, o reutiliza una conexión existente con el servidor, para realizar el equilibrio de carga. La función de equilibrio de carga proporciona administración del tráfico desde la capa 4 (TCP y UDP) hasta la capa 7 (FTP, HTTP y HTTPS).

El dispositivo Citrix ADC utiliza varios algoritmos, denominados métodos de equilibrio de carga, para determinar cómo distribuir la carga entre los servidores. El método de equilibrio de carga predeterminado es el método Least Connections.

Una implementación típica de equilibrio de carga consta de las entidades descritas en la siguiente ilustración.

Ilustración 1. Arquitectura de equilibrio de carga



Las entidades funcionan de la siguiente manera:

- **Servidor virtual**. Entidad representada por una dirección IP, un puerto y un protocolo. La dirección IP de servidor virtual (VIP) suele ser una dirección IP pública. El cliente envía solicitudes de conexión a esta dirección IP. El servidor virtual representa un banco de servidores.
- **Servicio**. Una representación lógica de un servidor o una aplicación que se ejecuta en un servidor. Identifica la dirección IP del servidor, un puerto y un protocolo. Los servicios se vinculan con servidores virtuales.
- **Objeto de servidor**. Entidad representada por una dirección IP. El objeto de servidor se crea al crear un servicio. La dirección IP del servicio se toma como nombre del objeto de servidor. También puede crear un objeto de servidor y, a continuación, crear servicios mediante el objeto de servidor.
- **Monitor**. Entidad que realiza un seguimiento del estado de los servicios. El dispositivo sondea periódicamente los servidores mediante el monitor vinculado a cada servicio. Si un servidor no responde dentro de un tiempo de espera de respuesta especificado y falla el número especificado de sondeos, el servicio se marca como DOWN. A continuación, el dispositivo realiza el equilibrio de carga entre los servicios restantes.

Equilibrio de carga

August 20, 2021

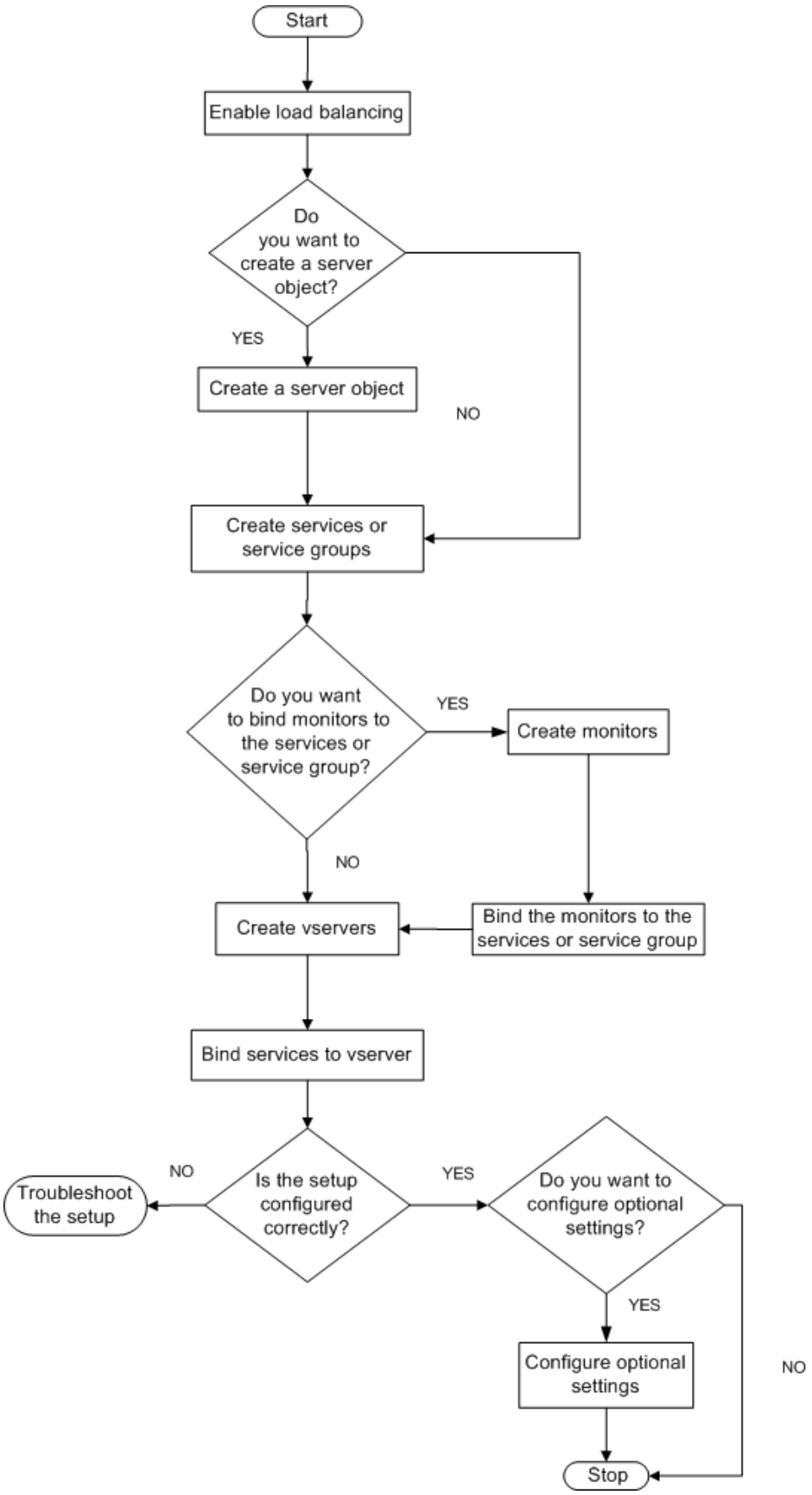
Para configurar el equilibrio de carga, primero debe crear servicios. A continuación, crea servidores virtuales y vincula los servicios a los servidores virtuales. De forma predeterminada, el dispositivo Citrix ADC vincula un monitor a cada servicio. Después de vincular los servicios, verifique su configuración asegurándose de que todos los ajustes sean correctos.

> Nota: Después de implementar la configuración, puede mostrar estadísticas que muestren el rendimiento de las entidades de la configuración. Utilice la utilidad estadística o el <vserverName> comando
> stat lb vserver.

Opcionalmente, puede asignar pesos a un servicio. A continuación, el método de equilibrio de carga utiliza el peso asignado para seleccionar un servicio. Sin embargo, para empezar, puede limitar las tareas opcionales a la configuración de algunas opciones básicas de persistencia, para las sesiones que deben mantener una conexión a un servidor determinado, y algunas opciones básicas de protección de configuración.

El siguiente diagrama de flujo ilustra la secuencia de las tareas de configuración.

Ilustración 1. Secuencia de tareas para configurar el equilibrio de carga



Habilitar equilibrio de carga

Antes de configurar el equilibrio de carga, asegúrese de que la función de equilibrio de carga está habilitada.

Para habilitar el equilibrio de carga mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para habilitar el equilibrio de carga y compruebe que está habilitado:

- habilitar función lb
- show feature

Ejemplo

“‘ pre codeblock

```
enable feature lb
Done
show feature
```

```
1   Feature                  Acronym          Status
2   -------                  -------          ------   1)  Web
       Logging               WL               OFF   2)  Surge
       Protection         SP               OFF   3)  Load Balancing
                 LB               ON   .   .   .   9)  SSL
       Offloading            SSL              ON   .   .   .  Done
       <!--NeedCopy--> ```
```

Para habilitar el equilibrio de carga mediante la interfaz gráfica de usuario

1. En el panel de navegación, expanda Sistemay, a continuación, haga clic en Configuración.
2. En el panel de detalles, en Modos y funciones, haga clic en Cambiar funciones básicas.
3. En el cuadro de diálogo Configurar funciones básicas, active la casilla Equilibrio de carga y, a continuación, haga clic en Aceptar.
4. ¿En las funciones Activar/Desactivar?, haga clic en Sí.

Configurar servicios y un servidor virtual

Cuando haya identificado los servicios que quiere equilibrar la carga, puede implementar la configuración inicial de equilibrio de carga creando los objetos de servicio, creando un servidor virtual de equilibrio de carga y vinculando los objetos de servicio al servidor virtual.

Para implementar la configuración inicial de equilibrio de carga mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para implementar y verificar la configuración inicial:

- <add service <name> <IPaddress> <serviceType> <port>
- <add lb vserver <vServerName> <serviceType> [<IPaddress> <port>]
- <bind lb vserver <name> <serviceName>
- <show service bindings <serviceName>

  Ejemplo

```
> add service service-HTTP-1 10.102.29.5 HTTP 80
 Done
> add lb vserver vserver-LB-1 HTTP 10.102.29.60 80
 Done
> bind lb vserver vserver-LB-1 service-HTTP-1
 Done
> show service bindings service-HTTP-1
    service-HTTP-1 (10.102.29.5:80) - State : DOWN

      1)      vserver-LB-1 (10.102.29.60:80) - State : DOWN
 Done
<!--NeedCopy-->
```

Para implementar la configuración inicial de equilibrio de carga mediante la interfaz gráfica de usuario

1. Acceda a Administración del tráfico > Equilibrio de carga.
2. En el panel de detalles, en Introducción, haga clic en Asistente para equilibrio de carga y siga las instrucciones para crear una configuración básica de equilibrio de carga.
3. Vuelva al panel de navegación, expanda Equilibrio de carga y, a continuación, haga clic en Servidores virtuales.
4. Seleccione el servidor virtual que configuró y compruebe que los parámetros mostrados en la parte inferior de la página estén configurados correctamente.
5. Haga clic en Abrir.
6. Compruebe que cada servicio está enlazado al servidor virtual confirmando que la casilla de verificación Activo está activada para cada servicio en la ficha Servicios.

Parámetros de persistencia

August 11, 2022

Debe configurar la persistencia en un servidor virtual si quiere mantener los estados de las conexiones en los servidores representados por ese servidor virtual (por ejemplo, las conexiones utilizadas en el comercio electrónico). A continuación, el dispositivo utiliza el método de equilibrio de carga configurado para la selección inicial de un servidor, pero reenvía a ese mismo servidor todas las solicitudes posteriores del mismo cliente.

Si se configura la persistencia, anula los métodos de equilibrio de carga una vez que se ha seleccionado el servidor. Si la persistencia configurada se aplica a un servicio que está inactivo, el dispositivo utiliza los métodos de equilibrio de carga para seleccionar un nuevo servicio y el nuevo servicio se vuelve persistente para las solicitudes posteriores del cliente. Si el servicio seleccionado está en estado Fuera de servicio, continúa atendiendo las solicitudes pendientes, pero no acepta solicitudes ni conexiones nuevas. Una vez transcurrido el período de cierre, se cierran las conexiones existentes. En la tabla siguiente se enumeran los tipos de persistencia que puede configurar.

Tipo de persistencia	Conexiones persistentes
IP de origen, ID de sesión SSL, regla, DESTIP, SRCIPDESTIP	250K*
CookieInsert, URL pasiva, ID de servidor personalizado	Límite de memoria. En el caso de CookieInsert, si el tiempo de espera no es 0, se permite cualquier número de conexiones hasta que esté limitado por la memoria.

El * en la tabla anterior se hace referencia a lo siguiente:

El motor de paquetes predeterminado es de 250 000 sesiones por núcleo. Para configurar 1 millón de entradas de sesión por motor de paquetes, ejecute el siguiente comando:

```
set lb parameter -sessionsthreshold <1000000*number of PE>
```

Para un sistema 3 PE, ejecute el siguiente comando:

```
set lb parameter -sessionsthreshold 3000000
```

Tabla 1. Limitaciones en la cantidad de conexiones persistentes simultáneas

Si la persistencia configurada no se puede mantener debido a la falta de recursos en un dispositivo, se utilizan los métodos de equilibrio de carga para la selección del servidor. La persistencia se mantiene durante un período de tiempo configurado, según el tipo de persistencia. Algunos tipos de persistencia son específicos de ciertos servidores virtuales. En la tabla siguiente se muestra la relación.

TypeHeader de persistencia 1	HTTP	HTTPS	TCP	UDP/IP	SSL_Bridge
IP de origen	SÍ	SÍ	SÍ	SÍ	SÍ
CookieInsert	SÍ	SÍ	NO	NO	NO
ID de sesión SSL	NO	SÍ	NO	NO	SÍ
URL pasiva	SÍ	SÍ	NO	NO	NO
ID de servidor personal-izado	SÍ	SÍ	NO	NO	NO
Rule	SÍ	SÍ	NO	NO	NO
SRCIPDESTIP	N/D	N/D	SÍ	SÍ	N/D
DESTIP	N/D	N/D	SÍ	SÍ	N/D

Tabla 2. Tipos de persistencia disponibles para cada tipo de servidor virtual

También puede especificar la persistencia para un grupo de servidores virtuales. Cuando habilita la persistencia en el grupo, las solicitudes del cliente se dirigen al mismo servidor seleccionado, independientemente del servidor virtual del grupo que reciba la solicitud del cliente. Cuando transcurre el tiempo configurado para la persistencia, se puede seleccionar cualquier servidor virtual del grupo para las solicitudes de clientes entrantes.

Dos tipos de persistencia de uso común son la persistencia basada en cookies y la persistencia basada en los ID de servidor en las URL.

Configurar la persistencia en función de las cookies

Cuando habilita la persistencia basada en cookies, el dispositivo Citrix ADC agrega una cookie HTTP en el campo de **encabezado Set-Cookie** de la respuesta HTTP. La cookie contiene información sobre el servicio al que se deben enviar las solicitudes HTTP. El cliente almacena la cookie y la incluye en todas las solicitudes posteriores, y el ADC la usa para seleccionar el servicio para esas solicitudes. Puede usar este tipo de persistencia en servidores virtuales de tipo HTTP o HTTPS.

El dispositivo Citrix ADC inserta la cookie <NSC_XXXX>= <ServiceIP> <ServicePort>

Donde:

- <<NSC_XXXX> es el ID del servidor virtual que se deriva del nombre del servidor virtual.

- <<ServiceIP> es el valor hexadecimal de la dirección IP del servicio.
- <<ServicePort> es el valor hexadecimal del puerto del servicio.

El ADC cifra ServiceIP y ServicePort cuando inserta una cookie y los descifra cuando recibe una cookie.

Nota: Si el cliente no tiene permiso para almacenar la cookie HTTP, las solicitudes posteriores no tienen la cookie HTTP y no se respeta la persistencia.

De forma predeterminada, el dispositivo ADC envía la cookie HTTP versión 0, de conformidad con la especificación de Netscape. También puede enviar la versión 1, de conformidad con RFC 2109.

Puede configurar un valor de tiempo de espera para la persistencia que se base en las cookies HTTP. Tenga en cuenta lo siguiente:

- Si se utiliza la versión 0 de la cookie HTTP, el dispositivo Citrix ADC inserta la hora universal coordinada (GMT) absoluta de la caducidad de la cookie (el atributo expires de la cookie HTTP), calculada como la suma de la hora GMT actual en un dispositivo ADC y el valor del tiempo de espera.
- Si se utiliza una cookie HTTP versión 1, el dispositivo ADC inserta un tiempo de caducidad relativo (atributo Max-Age de la cookie HTTP). En este caso, el software cliente calcula la fecha de caducidad real.

Nota: La mayoría del software cliente instalado actualmente (exploradores web Microsoft Internet Explorer y Netscape) comprende la versión 0 de la cookie HTTP; sin embargo, algunos proxies HTTP entienden la versión 1 de la cookie HTTP.

Si establece el valor de tiempo de espera en 0, el dispositivo ADC no especifica la hora de caducidad, independientemente de la versión de la cookie HTTP utilizada. El tiempo de caducidad depende entonces del software del cliente, y dichas cookies no son válidas si se cierra el software. Este tipo de persistencia no consume ningún recurso del sistema. Por lo tanto, puede admitir un número ilimitado de clientes persistentes.

Un administrador puede cambiar la versión de la cookie HTTP.

Para cambiar la versión de la cookie HTTP mediante la CLI

En el símbolo del sistema, escriba;

```
set ns param [-cookieversion ( 0 | 1 )]
<!--NeedCopy-->
```

Ejemplo:


```
set ns param -cookieversion 1
<!--NeedCopy-->
```

Para cambiar la versión de la cookie HTTP mediante la GUI

1. Vaya a **Sistema > Configuración**.
2. En el panel de detalles, haga clic en Cambiar parámetros HTTP.
3. En el cuadro de diálogo Configurar parámetros HTTP, en Cookie, seleccione Versión 0 o Versión 1.

Nota: Para obtener información sobre los parámetros, consulte Configurar la persistencia basada en cookies.

Para configurar la persistencia basada en cookies mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para configurar la persistencia basada en cookies y verificar la configuración:

```
set lb vserver <name> -persistenceType COOKIEINSERT

show lb vserver <name>
<!--NeedCopy-->
```

Ejemplo:

```
set lb vserver vserver-LB-1 -persistenceType COOKIEINSERT
Done
show lb vserver vserver-LB-1
    vserver-LB-1 (10.102.29.60:80) - HTTP   Type: ADDRESS
    .
    .
    .
    Persistence: COOKIEINSERT (version 0)
    Persistence Timeout: 2 min
    .
    .
    .
 Done
<!--NeedCopy-->
```


Para configurar la persistencia basada en cookies mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. En el panel de detalles, seleccione el servidor virtual para el que quiere configurar la persistencia (por ejemplo, vServer-LB-1) y, a continuación, haga clic en Abrir.
3. En el cuadro de diálogo Configurar servidor virtual (equilibrio de carga), en la ficha Método y persistencia, en la lista Persistencia, seleccione COOKIEINSERT.
4. En el cuadro de texto Tiempo límite (min), escriba el valor del tiempo de espera (por ejemplo, 2).
5. Haga clic en Aceptar.
6. Compruebe que el servidor virtual para el que configuró la persistencia esté correctamente configurado seleccionando el servidor virtual y consultando la sección Detalles en la parte inferior del panel.

Configurar la persistencia en función de los ID de servidor en las URL

El dispositivo Citrix ADC puede mantener la persistencia en función de los ID de servidor en las URL. En una técnica llamada persistencia pasiva de URL, el ADC extrae el ID del servidor de la respuesta del servidor y lo incrusta en la consulta de URL de la solicitud del cliente. El ID del servidor es una dirección IP y el puerto se especifica como un número hexadecimal. El ADC extrae el ID del servidor de las solicitudes posteriores del cliente y lo utiliza para seleccionar el servidor.

La persistencia pasiva de URL requiere configurar una expresión de carga útil o una expresión de infraestructura de directiva que especifique la ubicación del ID del servidor en las solicitudes de cliente. Para obtener más información sobre las expresiones, consulte Configuración y referencia de directivas.

Nota: Si el ID del servidor no se puede extraer de las solicitudes del cliente, la selección del servidor se basa en el método de equilibrio de carga.

Ejemplo: Expresión de carga útil

La expresión URLQUERY contiene sid= configura el sistema para extraer el ID del servidor de la consulta de URL de una solicitud de cliente, después de hacer coincidir el token sid=. Por lo tanto, una solicitud con la URL `http://www.citrix.com/index.asp?\\&sid;=c0a864100050` se dirige al servidor con la dirección IP 10.102.29.10 y el puerto 80.

El valor de tiempo de espera no afecta a este tipo de persistencia, que se mantiene mientras se pueda extraer el ID del servidor de las solicitudes del cliente. Este tipo de persistencia no consume ningún recurso del sistema, por lo que puede acomodar un número ilimitado de clientes persistentes.

> Nota: Para obtener información sobre los parámetros, consulte Equilibrio de carga.

Para configurar la persistencia basada en los ID de servidor en las direcciones URL mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para configurar la persistencia en función de los ID de servidor en las URL y verificar la configuración:

```
set lb vserver <name> -persistenceType URLPASSIVE

<show lb vserver <name>
<!--NeedCopy-->
```

Ejemplo:

```
set lb vserver vserver-LB-1 -persistenceType URLPASSIVE
Done
show lb vserver vserver-LB-1
    vserver-LB-1 (10.102.29.60:80) - HTTP   Type: ADDRESS
    .
    .
    .
    Persistence: URLPASSIVE
    Persistence Timeout: 2 min
    .
    .
    .
Done
<!--NeedCopy-->
```

Para configurar la persistencia en función de los ID de servidor en las URL mediante la interfaz gráfica de usuario

1. Vaya a Administración del tráfico > Equilibrio de carga > Servidores virtuales.
2. En el panel de detalles, seleccione el servidor virtual para el que quiere configurar la persistencia (por ejemplo, vServer-LB-1) y, a continuación, haga clic en Abrir.
3. En el cuadro de diálogo Configurar servidor virtual (equilibrio de carga), en la ficha Método y persistencia, en la lista Persistencia, seleccione URLPASSIVE.
4. En el cuadro de texto Tiempo límite (min), escriba el valor del tiempo de espera (por ejemplo, 2).
5. En el cuadro de texto Regla, introduzca una expresión válida. También puede hacer clic en Configurar junto al cuadro de texto Regla y utilizar el cuadro de diálogo Crear expresión para crear

una expresión.

6. Haga clic en Aceptar.
7. Compruebe que el servidor virtual para el que configuró la persistencia esté correctamente configurado seleccionando el servidor virtual y consultando la sección Detalles en la parte inferior del panel.

Configurar funciones para proteger la configuración de equilibrio de carga

August 20, 2021

Puede configurar la redirección de URL para proporcionar notificaciones de errores de funcionamiento del servidor virtual, y puede configurar servidores virtuales de copia de seguridad para que se haga cargo si un servidor virtual principal no está disponible.

Configurar redirección de URL

Puede configurar una dirección URL de redirección para comunicar el estado del dispositivo en caso de que un servidor virtual de tipo HTTP o HTTPS esté inactivo o inhabilitado. Esta URL puede ser un vínculo local o remoto. El dispositivo utiliza la redirección HTTP 302.

Las redirecciones pueden ser URL absolutas o URL relativas. Si la URL de redirección configurada contiene una URL absoluta, la redirección HTTP se envía a la ubicación configurada, independientemente de la URL especificada en la solicitud HTTP entrante. Si la dirección URL de redirección configurada contiene solo el nombre de dominio (URL relativa), la redirección HTTP se envía a una ubicación después de agregar la dirección URL entrante al dominio configurado en la dirección URL de redirección.

Nota: Si un servidor virtual de equilibrio de carga está configurado tanto con un servidor virtual de copia de seguridad como con una URL de redirección, el servidor virtual de copia de seguridad tiene prioridad sobre la URL de redirección. En este caso, se utiliza una redirección cuando los servidores virtuales principales y de copia de seguridad están inactivos.

Para configurar un servidor virtual para redirigir las solicitudes de cliente a una URL mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para configurar un servidor virtual para redirigir las solicitudes de cliente a una dirección URL y verificar la configuración:

```
1 set lb vserver <name> -redirectURL <URL>
```



```
2
3 show lb vserver <name>
4 <!--NeedCopy-->
```

Ejemplo:

```
1     > set lb vserver vserver-LB-1 -redirectURL <http://www.newdomain.
         com/mysite/maintenance>
2      Done
3     > show lb vserver vserver-LB-1
4         vserver-LB-1 (10.102.29.60:80) - HTTP   Type: ADDRESS
5         State: DOWN
6         Last state change was at Wed Jun 17 08:56:34 2009 (+666 ms)
7         .
8         .
9         .
10        Redirect URL: <http://www.newdomain.com/mysite/maintenance>
11        .
12        .
13        .
14     Done
15    >
16 <!--NeedCopy-->
```

Para configurar un servidor virtual para redirigir las solicitudes de cliente a una URL mediante la interfaz gráfica de usuario

1. Vaya a Administración del tráfico > Equilibrio de carga > Servidores virtuales.
2. En el panel de detalles, seleccione el servidor virtual para el que quiere configurar la redirección de URL (por ejemplo, VServer-LB-1) y, a continuación, haga clic en Abrir.
3. En el cuadro de diálogo Configurar servidor virtual (equilibrio de carga), en la ficha Opciones avanzadas, en el cuadro de texto Redirigir dirección URL, escriba la dirección URL (por ejemplo,`http://www.newdomain.com/mysite/maintenance`) y, a continuación, haga clic en Aceptar.
4. Compruebe que la dirección URL de redirección configurada para el servidor aparece en la sección Detalles en la parte inferior del panel.

Configurar servidores virtuales de backup

Si el servidor virtual principal está inactivo o inhabilitado, el dispositivo puede dirigir las conexiones o las solicitudes de cliente a un servidor virtual de copia de seguridad que reenvía el tráfico del cliente

a los servicios. El dispositivo también puede enviar un mensaje de notificación al cliente en relación con la interrupción o mantenimiento del sitio. El servidor virtual de copia de seguridad es un proxy y es transparente para el cliente.

Puede configurar un servidor virtual de copia de seguridad al crear un servidor virtual o al cambiar los parámetros opcionales de un servidor virtual existente. También puede configurar un servidor virtual de copia de seguridad para un servidor virtual de copia de seguridad existente, creando así un servidor virtual de copia de seguridad en cascada. La profundidad máxima de los servidores virtuales de backup en cascada es 10. El dispositivo busca un servidor virtual de copia de seguridad que esté activo y accede a ese servidor virtual para entregar el contenido.

Puede configurar la redirección de URL en el principal para su uso cuando los servidores virtuales principal y de copia de seguridad estén inactivos o hayan alcanzado sus umbrales para gestionar solicitudes.

Nota: Si no existe ningún servidor virtual de copia de seguridad, aparecerá un mensaje de error, a menos que el servidor virtual esté configurado con una dirección URL de redirección. Si se configuran tanto un servidor virtual de copia de seguridad como una dirección URL de redirección, el servidor virtual de copia de seguridad tiene prioridad.

Para configurar un servidor virtual de copia de seguridad mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para configurar un servidor de copia de seguridad y verifique la configuración:

```
set lb vserver <name> [-backupVserver <string>]

show lb vserver <name>
<!--NeedCopy-->
```

Ejemplo:

```
    > set lb vserver vserver-LB-1 -backupVserver vserver-LB-2
     Done
    > show lb vserver vserver-LB-1
        vserver-LB-1 (10.102.29.60:80) - HTTP   Type: ADDRESS
        State: DOWN
        Last state change was at Wed Jun 17 08:56:34 2009 (+661 ms)
        .
        .
        .
```



```
10          Backup: vserver-LB-2
11          .
12          .
13          .
14       Done
15      >
16  <!--NeedCopy-->
```

Para configurar un servidor virtual de copia de seguridad mediante la interfaz gráfica de usuario

1. Vaya a Administración del tráfico > Equilibrio de carga > Servidores virtuales.
2. En el panel de detalles, seleccione el servidor virtual para el que quiere configurar el servidor virtual de copia de seguridad (por ejemplo, VServer-LB-1) y, a continuación, haga clic en Abrir.
3. En el cuadro de diálogo Configurar servidor virtual (equilibrio de carga), en la ficha Avanzadas, en la lista Servidor virtual de copia de seguridad, seleccione el servidor virtual de copia de seguridad (por ejemplo, VServer-LB-2 y, a continuación, haga clic en Aceptar.
4. Compruebe que el servidor virtual de copia de seguridad configurado aparezca en la sección Detalles en la parte inferior del panel.

   Nota: Si el servidor principal se desactiva y vuelve a activarse y quiere que el servidor virtual de copia de seguridad funcione como servidor principal hasta que restablezca explícitamente el servidor virtual principal, active la casilla de verificación Inhabilitar primario cuando está caído.

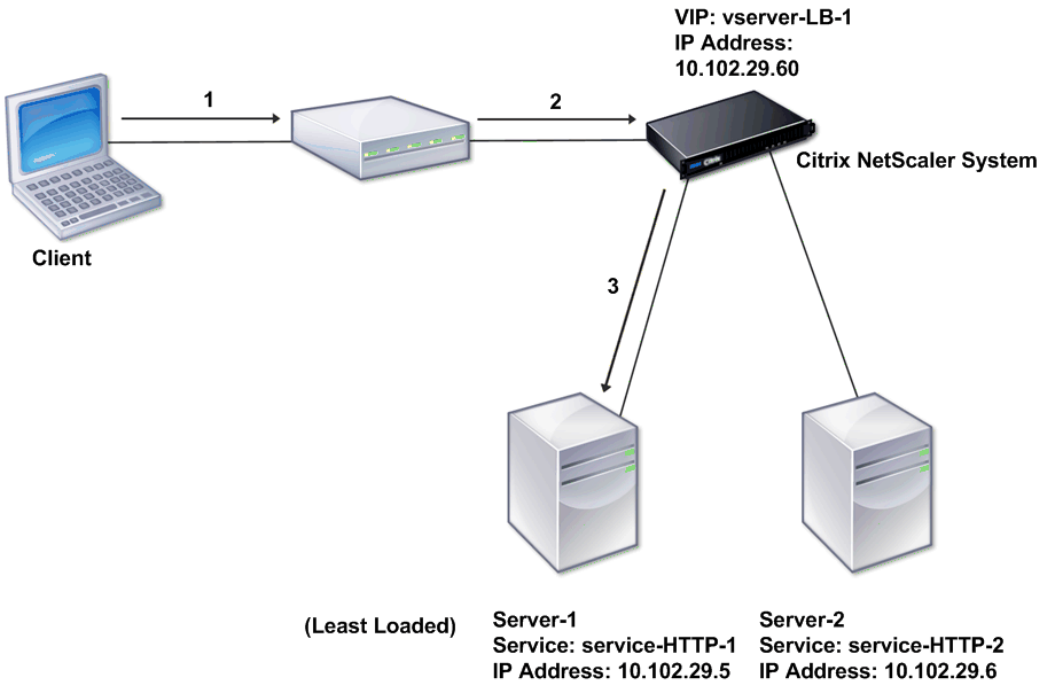
Un caso típico de equilibrio de carga

August 20, 2021

En una configuración de equilibrio de carga, los dispositivos Citrix ADC se ubican lógicamente entre el cliente y la comunidad de servidores, y administran el flujo de tráfico hacia los servidores.

La siguiente ilustración muestra la topología de una configuración básica de equilibrio de carga.

Ilustración 1. Topología básica de equilibrio de carga

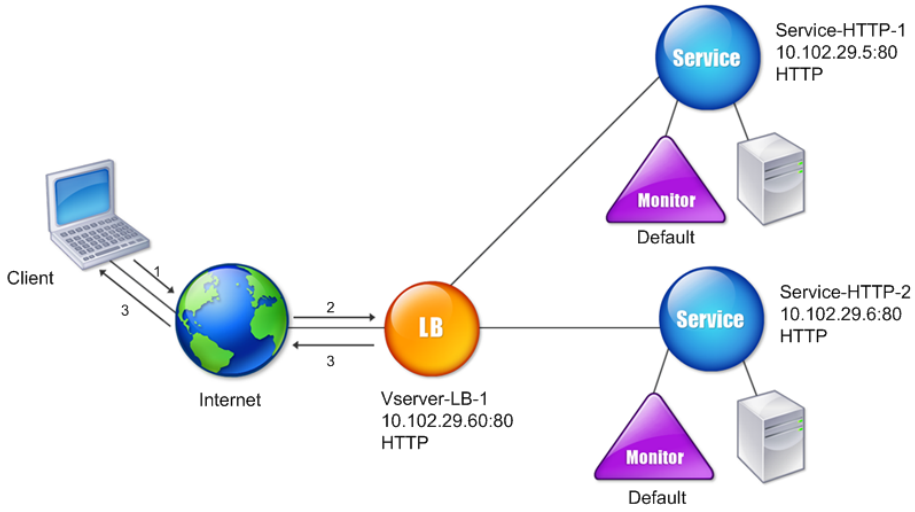


El servidor virtual selecciona el servicio y lo asigna para atender las solicitudes del cliente. Considere el caso de la ilustración anterior, donde los servicios Service-HTTP-1 y Servicio-HTTP-2 se crean y vinculan al servidor virtual denominado Servidor-LB-1. Virtual Server-LB-1 reenvía la solicitud del cliente a Service-HTTP-1 o Servicio-HTTP-2. El sistema selecciona el servicio para cada solicitud mediante el método de equilibrio de carga de Least Connections. En la siguiente tabla se detallan los nombres y los valores de las entidades básicas que se deben configurar en el sistema.

Cuadro 1 Valores de parámetros de configuración LB

En la siguiente ilustración se muestran los valores de muestra de equilibrio de carga y los parámetros necesarios que se describen en la tabla anterior.

Ilustración 2. Modelo de entidad de equilibrio de carga



En las tablas siguientes se enumeran los comandos utilizados para configurar esta configuración de equilibrio de carga mediante la interfaz de línea de comandos.

Tarea	Comando
Para habilitar el equilibrio de carga	habilitar función lb
Para crear un servicio denominado Service-HTTP-1	add service service-HTTP-1 10.102.29.5 HTTP 80
Para crear un servicio denominado Service-HTTP-2	add service service-HTTP-2 10.102.29.6 HTTP 80
Para crear un servidor virtual denominado VServer-LB-1	add lb vserver vserver-lb-1 HTTP 10.102.29.60 80
Para enlazar un servicio denominado Service-HTTP-1 a un servidor virtual denominado VServer-LB-1	bind lb vserver vServer-LB-1 Servicio-HTTP-1

Tarea	Comando
Para enlazar un servicio denominado Service-HTTP-2 a un servidor virtual denominado VServer-LB-1	bind lb vserver vServer-LB-1 Servicio-HTTP-2

Tabla 2. Tareas de configuración iniciales

Para obtener más información sobre las tareas de configuración iniciales, consulte Configuración del equilibrio de carga básico.

Tarea	Comando
Para ver las propiedades de un servidor virtual denominado VServer-LB-1	show lb vserver vserver-lb-1
Para ver las estadísticas de un servidor virtual denominado VServer-LB-1	stat lb vserver vserver-LB-1
Para ver las propiedades de un servicio denominado Service-HTTP-1	show service service-http-1
Para ver las estadísticas de un servicio denominado Service-HTTP-1	servicio stat servicio-HTTP-1
Para ver los enlaces de un servicio denominado Service-HTTP-1	show service bindings Service-HTTP-1

Tabla 3. Tareas de verificación

Tarea	Comando
Para configurar la persistencia en un servidor virtual denominado VServer-LB-1	set lb vserver vServer-lb-1 -PersistenceType SOURCEIP -PersistenceMask 255.255.255.255 -timeout 2
Para configurar la persistencia de COOKIEINSERT en un servidor virtual denominado VServer-LB-1	set lb vserver vServer-lb-1 -persistenceType COOKIEINSERT
Para configurar la persistencia URLPassive en un servidor virtual denominado VServer-LB-1	set lb vserver vServer-lb-1 -PersistenceType URLPASSIVE

Tarea	Comando
Para configurar un servidor virtual para redirigir la solicitud del cliente a una dirección URL en un servidor virtual denominado VServer-LB-1	set lb vserver vServer-lb-1 -redirectURL`http://www.newdomain.com/mysite/maintenance`
Para establecer un servidor virtual de copia de seguridad en un servidor virtual denominado VServer-LB-1	set lb vserver vserver-lb-1 -backupvserver vserver-lb-2

Tabla 4. Tareas de personalización

Para obtener más información sobre la configuración de la persistencia, consulte Selección y configuración de los parámetros de persistencia. Para obtener información sobre la forma de configurar un servidor virtual de modo que se redirija la solicitud de cliente a una URL y la forma de establecer un servidor virtual de respaldo, consulte Configuración de funcionalidades para proteger la configuración de equilibrio de carga.

Caso de uso: Cómo forzar las opciones de cookie Secure y HttpOnly para sitios web que utilizan el dispositivo Citrix ADC

October 5, 2021

Los administradores web pueden forzar el Secure o HttpOnly, o ambos indicadores del ID de sesión y las cookies de autenticación generadas por las aplicaciones web. Puede modificar los encabezados de Set-cookie para incluir estas dos opciones mediante un servidor virtual de equilibrio de carga HTTP y reescritura de directivas en un dispositivo Citrix ADC.

- **HttpOnly**: Esta opción de una cookie hace que los exploradores web devuelvan la cookie mediante únicamente el protocolo HTTP o HTTPS. Los métodos que no son HTTP, como las referencias de document.cookie JavaScript, no pueden acceder a la cookie. Esta opción ayuda a evitar el robo de cookies debido a los scripts entre sitios.

  > NOTA
  >
  > No puede utilizar la opción HttpOnly cuando una aplicación web requiere acceso al contenido de las cookies mediante un script del lado del cliente, como JavaScript o un applet Java del lado del cliente. Puede utilizar el método mencionado en este documento para reescribir solo las cookies generadas por el servidor y no las cookies generadas por el dis-

> positivo Citrix ADC. Por ejemplo, AppFirewall, persistencia, cookies de sesión VPN, etc.

- **Seguro** : esta opción en una cookie hace que los exploradores web devuelvan solo el valor de la cookie cuando la transmisión está cifrada por SSL. Esta opción se puede utilizar para evitar el robo de cookies a través del espionaje de conexión.

> NOTA
>
> El siguiente procedimiento no se aplica a los servidores virtuales VPN.

Para configurar el dispositivo Citrix ADC para forzar los indicadores Secure y HttpOnly para un servidor virtual HTTP existente mediante la CLI

1. Crea una acción de reescritura.

   Este ejemplo está configurado para establecer indicadores Secure y HttpOnly. Si falta alguno de ellos, modifíquelo según sea necesario para otras combinaciones.

```
1 add rewrite action act_cookie_Secure replace_all http.RES.
     full_Header ""Secure; HttpOnly; path=/"" -search "regex(re!(
     path=/\\; Secure; HttpOnly)|(path=/\\; Secure)|(path=/\\;
     HttpOnly)|(path=/)!)"
2 <!--NeedCopy-->
```

   Esta directiva reemplaza todas las instancias de “path=/”, “path=/; Secure”, “path=/; Secure; HttpOnly” y “path=/; HttpOnly” por “Secure; HttpOnly; path=/”. Esta expresión regular (regex) falla si las mayúsculas no coinciden.

2. Cree una directiva de reescritura para desencadenar la acción.

```
1 add rewrite policy rw_force_secure_cookie "http.RES.HEADER("Set-
     Cookie").EXISTS" act_cookie_Secure
2 <!--NeedCopy-->
```

3. Vincule la directiva de reescritura al servidor virtual que quiere proteger. Si se utiliza la opción `Secure`, se debe utilizar un servidor virtual SSL.

```
1 bind lb vserver mySSLVServer -policyName rw_force_secure_cookie -
     priority 100 -gotoPriorityExpression NEXT -type RESPONSE
2 <!--NeedCopy-->
```


Ejemplos:

En el ejemplo siguiente se muestra la cookie antes de configurar el indicador HttpOnly.

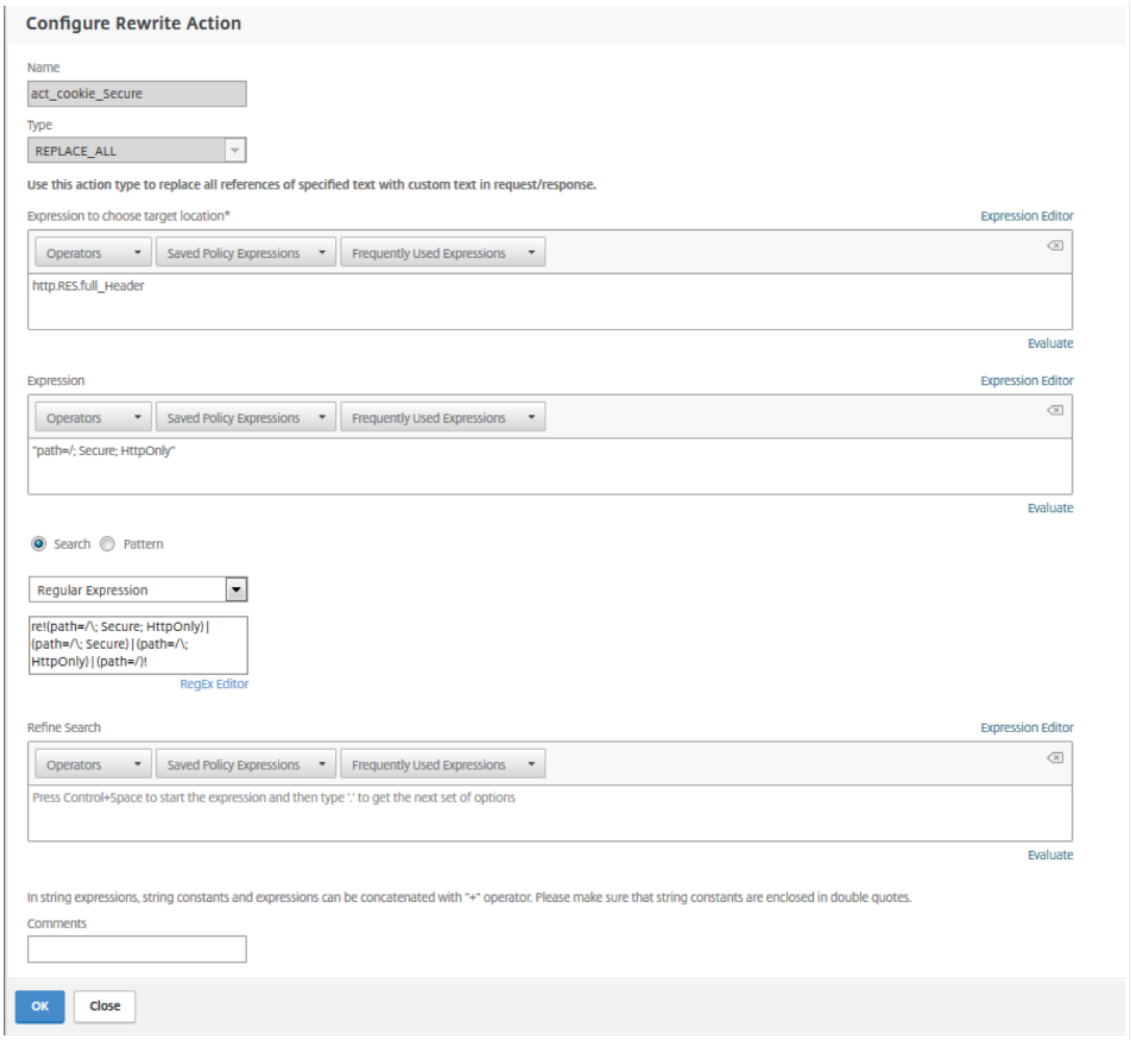
```
1 Set-Cookie: CtxsAuthId=C5614491; path=/Citrix/ProdWeb
2 <!--NeedCopy-->
```

En el ejemplo siguiente se muestra la cookie después de configurar el indicador HttpOnly.

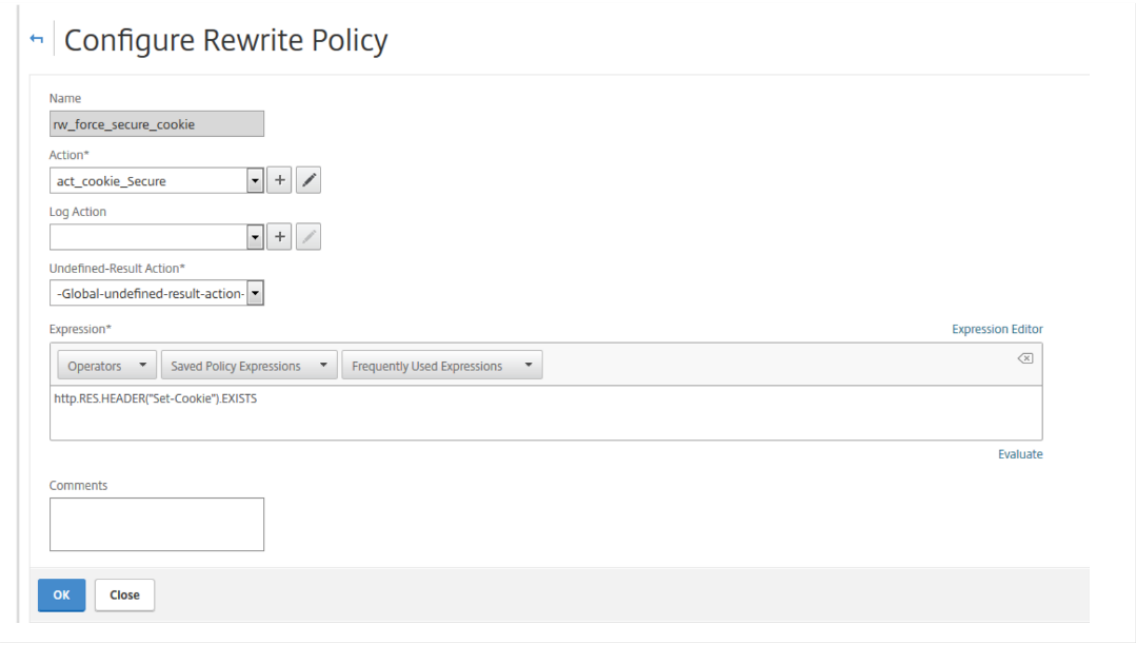
```
1 Set-Cookie: CtxsAuthId=C5614491; Secure; HttpOnly; path=/Citrix/ProdWeb
     /
2 <!--NeedCopy-->
```

Para configurar el dispositivo Citrix ADC para forzar los indicadores Secure y HttpOnly para un servidor virtual HTTP existente mediante la GUI

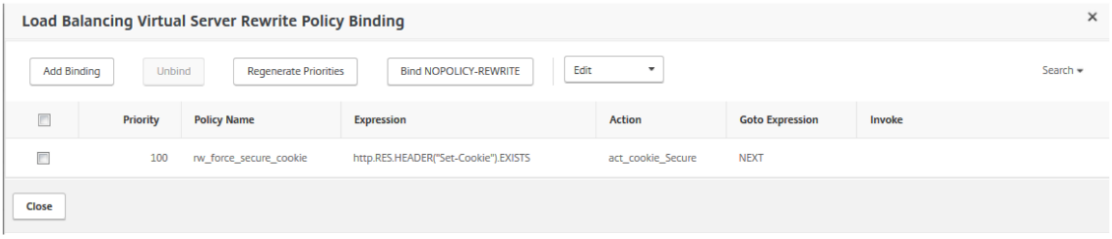
1. Vaya a **AppExpert > Reescritura > Acciones**y haga clic en **Agregar** para agregar una nueva acción de reescritura.



2. Vaya a **AppExpert > Reescritura > Directivas**y haga clic en **Agregar** para agregar una nueva directiva de reescritura.



3. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**y, a continuación, vincule la directiva de reescritura (respuesta) al servidor virtual SSL correspondiente.



Acelere el tráfico equilibrado de carga mediante compresión

October 5, 2021

La compresión es un medio popular de optimizar el uso del ancho de banda y la mayoría de los exploradores web admiten datos comprimidos. Si habilita la función de compresión, el dispositivo Citrix ADC intercepta las solicitudes de los clientes y determina si el cliente puede aceptar contenido comprimido. Tras recibir la respuesta HTTP del servidor, el dispositivo examina el contenido para determinar si es comprimible. Si el contenido es comprimible, el dispositivo lo comprime, modifica el encabezado de respuesta para indicar el tipo de compresión realizada y reenvía el contenido comprimido al cliente.

La compresión de Citrix ADC es una función basada en directivas. Una directiva filtra las solicitudes y las respuestas para identificar las respuestas que se van a comprimir y especifica el tipo de compresión que se aplicará a cada respuesta. El dispositivo proporciona varias directivas integradas

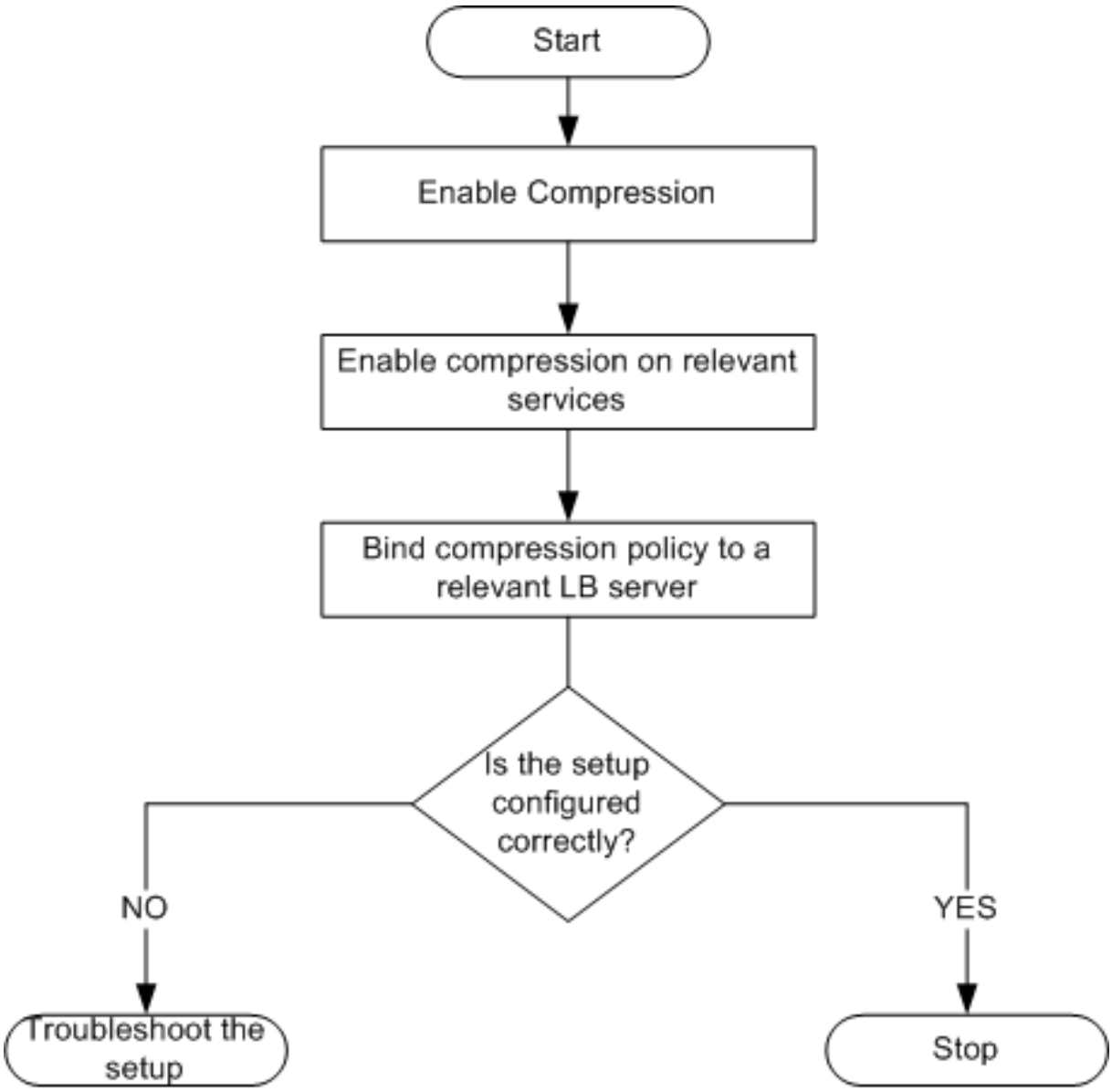
para comprimir tipos MIME comunes, como text/html, text/plain, text/xml, text/css, text/rtf, application/msword, application/vnd.ms-excel y application/vnd.ms-powerpoint. También puede crear directivas personalizadas. El dispositivo no comprime tipos MIME comprimidos como aplicaciones o secuencias de octetos, binario, bytes ni formatos de imagen comprimidos como GIF y JPEG.

Para configurar la compresión, debe habilitarla globalmente y en cada servicio que proporcionará las respuestas que quiera comprimir. Si ha configurado servidores virtuales para el equilibrio de carga o la conmutación de contenido, debe vincular las directivas a los servidores virtuales. De lo contrario, las directivas se aplican a todo el tráfico que pasa por el dispositivo.

secuencia de tareas de configuración de compresión

El siguiente diagrama de flujo muestra la secuencia de tareas para configurar la compresión básica en una configuración de equilibrio de carga.

Ilustración 1. Secuencia de tareas para configurar la compresión



> Nota: Los pasos de la ilustración anterior suponen que el equilibrio de carga ya se ha configurado.

Habilitar compresión

De forma predeterminada, la compresión no está habilitada. Debe habilitar la función de compresión para permitir la compresión de las respuestas HTTP que se envían al cliente.

Para habilitar la compresión mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para habilitar la compresión y verificar la configuración:

- habilitar función ns CMP
- función show ns

```
    > enable ns feature CMP



    Done

    > show ns feature



           Feature                        Acronym              Status

           -------                        -------              ------

    1)     Web Logging                    WL                   ON

    2)     Surge Protection               SP                   OFF

    .

    7) Compression Control CMP ON

       .

    Done
<!--NeedCopy-->
```


Para habilitar la compresión mediante la interfaz gráfica de usuario

1. En el panel de navegación, expanda Sistemay, a continuación, haga clic en Configuración.
2. En el panel de detalles, en Modos y funciones, haga clic en Cambiar funciones básicas.
3. En el cuadro de diálogo Configure Basic Features, seleccione la casilla de verificación Compression y, a continuación, haga clic en OK.
4. En el cuadro de diálogo Enable/Disable Feature(s)?, haga clic en Yes.

Configurar servicios para comprimir datos

Además de habilitar la compresión de forma global, debe habilitarla en cada servicio que entregue archivos para comprimirlos.

Para habilitar la compresión en un servicio mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para habilitar la compresión en un servicio y compruebe la configuración:

- set service <name>-CMP SÍ
- servicio de espectáculos <name>

```
> show service SVC_HTTP1

SVC_HTTP1 (10.102.29.18:80) - HTTP

State: UP

Last state change was at Tue Jun 16 06:19:14 2009 (+737 ms)

Time since last state change: 0 days, 03:03:37.200

Server Name: 10.102.29.18

Server ID : 0   Monitor Threshold : 0

Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
```



```
23
24
25 Use Source IP: NO
26
27
28 Client Keepalive(CKA): NO
29
30
31 Access Down Service: NO
32
33
34 TCP Buffering(TCPB): NO
35
36
37 HTTP Compression(CMP): YES
38
39
40 Idle timeout: Client: 180 sec   Server: 360 sec
41
42
43 Client IP: DISABLED
44
45
46 Cacheable: NO
47
48
49 SC: OFF
50
51
52 SP: OFF
53
54
55 Down state flush: ENABLED
56
57 1)      Monitor Name: tcp-default
58
59
60 State: DOWN     Weight: 1
61
62
63 Probes: 1095    Failed [Total: 1095 Current: 1095]
64
65
66 Last response: Failure - TCP syn sent, reset received.
67
```



```
68
69 Response Time: N/A
70
71
72 Done
73
74 <!--NeedCopy-->
```

Para habilitar la compresión en un servicio mediante la interfaz gráfica de usuario

1. Vaya a Traffic Management -> Load Balancing -> Services.
2. En el panel de detalles, seleccione el servicio para el que quiere configurar la compresión (por ejemplo, Service-HTTP-1) y, a continuación, haga clic en Abrir.
3. En la ficha Advanced, en Settings, seleccione la casilla de verificación Compression y, a continuación, haga clic en OK.
4. Compruebe que, cuando se selecciona el servicio, aparece Compresión HTTP (CMP): ON en la sección **Detalles** de la parte inferior del panel.

Enlazar una directiva de compresión a un servidor virtual

Si vincula una directiva a un servidor virtual, la directiva solo la evalúan los servicios asociados a ese servidor virtual. Puede enlazar directivas de compresión a un servidor virtual desde el cuadro de diálogo Configurar servidor virtual (equilibrio de carga) o desde el cuadro de diálogo Administrador de directivas de compresión. En este tema se incluyen instrucciones para enlazar directivas de compresión a un servidor virtual de equilibrio de carga mediante el cuadro de diálogo Configurar servidor virtual (equilibrio de carga).

Para enlazar o desenlazar una directiva de compresión a un servidor virtual mediante la línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para enlazar o desvincular una directiva de compresión a un servidor virtual de equilibrio de carga y compruebe la configuración:

- (bind|unbind) lb vserver <name>-policyName <string>
- mostrar servidor lb <name>

Ejemplo:

```
1 > bind lb vserver lbvip -policyName ns_cmp_msapp
2 Done
3 > showlbserverlbvip
```



```
4
5  lbvip(8.7.6.6:80)-HTTPType:ADDRESS
6  State:UP
7  LaststatechangewasatThuMay2805:37:212009(+685ms)
8  Timesincelaststatechange:19days,04:26:50.470
9  EffectiveState:UP
10 ClientIdleTimeout:180sec
11 Downstateflush:ENABLED
12 DisablePrimaryVserverOnDown:DISABLED
13 PortRewrite:DISABLED
14 No.ofBoundServices:1(Total)1(Active)
15 ConfiguredMethod:LEASTCONNECTION
16 CurrentMethod:RoundRobin,Reason:Boundservice'sstatechangedtoUP
17 Mode:IP
18 Persistence:NONE
19 VserverIPandPortinsertion:OFF
20 Push:DISABLEDPushVServer:
21 PushMultiClients:NO
22 PushLabelRule:
23
24 BoundServiceGroups:
25 1)GroupName:Service-Group-1
26
27 1)Service-Group-1(10.102.29.252:80)-HTTPState:UPWeight:1
28
29 1)Policy:ns_cmp_msappPriority:0
30
31 Done
32
33 <!--NeedCopy-->
```

Para enlazar o desvincular una directiva de compresión a un servidor virtual de equilibrio de carga mediante la interfaz gráfica de usuario

1. Vaya a Administración del tráfico > Equilibrio de carga > Servidores virtuales.
2. En el panel de detalles, seleccione el servidor virtual al que quiere enlazar o desenlazar una directiva de compresión (por ejemplo, vServer-LB-1) y, a continuación, haga clic en Abrir.
3. En el cuadro de diálogo Configurar servidor virtual (equilibrio de carga), en la ficha Directivas, haga clic en Compresión.
4. Lleve a cabo una de las siguientes acciones:
   - Para enlazar una directiva de compresión, haga clic en Insertar directiva y, a continuación, seleccione la directiva que quiere enlazar al servidor virtual.

- Para desenlazar una directiva de compresión, haga clic en el nombre de la directiva que quiere desvincular del servidor virtual y, a continuación, haga clic en Desvincular directiva.

5. Haga clic en OK.

Tráfico seguro con equilibrio de carga mediante SSL

October 5, 2021

La función de descarga SSL de Citrix ADC mejora de forma transparente el rendimiento de los sitios web que realizan transacciones SSL. Al descargar las tareas de cifrado y descifrado SSL de uso intensivo de la CPU del servidor web local al dispositivo, la descarga SSL garantiza la entrega segura de las aplicaciones web sin la penalización de rendimiento que se produce cuando el servidor procesa los datos SSL. Una vez que se descifra el tráfico SSL, todos los servicios estándar pueden procesarlo. El protocolo SSL funciona a la perfección con varios tipos de datos HTTP y TCP y proporciona un canal seguro para las transacciones que utilizan dichos datos.

Para configurar SSL, primero debe habilitarlo. A continuación, configura los servicios HTTP o TCP y un servidor virtual SSL en el dispositivo y vincula los servicios al servidor virtual. También debe agregar un par de claves de certificado y vincularlo al servidor virtual SSL. Si utiliza servidores de Outlook Web Access, debe crear una acción para habilitar la compatibilidad con SSL y una directiva para aplicarla. Un servidor virtual SSL intercepta el tráfico cifrado entrante y lo descifra mediante un algoritmo negociado. A continuación, el servidor virtual SSL reenvía los datos descifrados a las demás entidades del dispositivo para su procesamiento adecuado.

Para obtener información detallada sobre la descarga SSL, consulte Descarga y aceleración de SSL.

Secuencia de tareas de configuración SSL

Para configurar SSL, primero debe habilitarlo. A continuación, debe crear un servidor virtual SSL y servicios HTTP o TCP en el dispositivo Citrix ADC. Por último, se debe enlazar un certificado SSL válido y los servicios configurados al servidor virtual SSL.

Un servidor virtual SSL intercepta el tráfico cifrado entrante y lo descifra mediante un algoritmo negociado. A continuación, el servidor virtual SSL reenvía los datos descifrados a las demás entidades del dispositivo Citrix ADC para su procesamiento adecuado.

El siguiente diagrama de flujo muestra la secuencia de tareas para configurar una configuración básica de descarga de SSL.

Ilustración 1. Secuencia de tareas para configurar la descarga de SSL

Habilitar descarga SSL

En primer lugar, habilite la función SSL. Puede configurar entidades basadas en SSL en el dispositivo sin habilitar la función SSL, pero no funcionarán hasta que habilite SSL.

Habilitar SSL mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para habilitar la descarga SSL y compruebe la configuración:

```
-  enable ns feature SSL
-  show ns feature
<!--NeedCopy-->
```

Ejemplo:

```
> enable ns feature ssl

Done


> show ns feature


Feature Acronym Status


------- ------- ------


1) Web Logging WL ON


2) SurgeProtection SP OFF


3) Load Balancing LB ON . . .


 9) SSL Offloading SSL ON


```



```
10) Global Server Load Balancing GSLB ON . .


Done >
<!--NeedCopy-->
```

Habilitar SSL mediante la interfaz gráfica de usuario

Siga estos pasos:

1. En el panel de navegación, expanda **Sistema**y, a continuación, haga clic en **Configuración**.
2. En el panel de detalles, en **Modos y funciones**, haga clic en **Cambiar funciones básicas**.
3. Active la casilla **Descarga SSL** y, a continuación, haga clic en **Aceptar**.
4. ¿En la (s) **función (s) activar/desactivar (s)?** cuadro de mensaje, haga clic en **Sí**.

Crear servicios HTTP

Un servicio del dispositivo representa una aplicación de un servidor. Una vez configurados, los servicios están inhabilitados hasta que el dispositivo puede llegar al servidor de la red y supervisar su estado. En este tema se describen los pasos para crear un servicio HTTP.

Nota: Para el tráfico TCP, realice los siguientes procedimientos, pero cree servicios TCP en lugar de servicios HTTP.

Agregar un servicio HTTP mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para agregar un servicio HTTP y compruebe la configuración:

```
-  add service <name> (<IP> | <serverName>) <serviceType> <port>
-  show service <name>
<!--NeedCopy-->
```

Ejemplo:

```
> add service SVC_HTTP1 10.102.29.18 HTTP 80


 Done

```



```
> show service SVC_HTTP1

        SVC_HTTP1 (10.102.29.18:80) - HTTP

        State: UP

        Last state change was at Wed Jul 15 06:13:05 2009

        Time since last state change: 0 days, 00:00:15.350

        Server Name: 10.102.29.18

        Server ID : 0   Monitor Threshold : 0

        Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits

        Use Source IP: NO

        Client Keepalive(CKA): NO

        Access Down Service: NO

        TCP Buffering(TCPB): NO

        HTTP Compression(CMP): YES

        Idle timeout: Client: 180 sec   Server: 360 sec

        Client IP: DISABLED

```



```
51
52          Cacheable: NO
53
54
55          SC: OFF
56
57
58          SP: OFF
59
60
61          Down state flush: ENABLED
62
63
64
65
66
67  1)      Monitor Name: tcp-default
68
69
70                  State: UP       Weight: 1
71
72
73                  Probes: 4       Failed [Total: 0 Current: 0]
74
75
76                  Last response: Success - TCP syn+ack received.
77
78
79                  Response Time: N/A
80
81
82   Done
83  <!--NeedCopy-->
```

Agregar un servicio HTTP mediante la interfaz gráfica de usuario

Siga estos pasos:

1. Vaya a **Administración del tráfico > Descarga SSL > Servicios**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En el cuadro de diálogo **Crear servicio**, escriba el nombre del servicio, la dirección IP y el puerto (por ejemplo, SVC_HTTP1, 10.102.29.18 y 80).
4. En la lista **Protocolo**, seleccione el tipo de servicio (por ejemplo, HTTP).

5. Haga clic en **Crear**y, a continuación, en **Cerrar**. El servicio HTTP configurado aparece en la página Servicios.
6. Compruebe que los parámetros configurados están correctamente configurados seleccionando el servicio y visualizando la sección Detalles en la parte inferior del panel.

Agregar un servidor virtual basado en SSL

En una configuración básica de descarga de SSL, el servidor virtual SSL intercepta el tráfico cifrado, lo descifra y envía los mensajes de texto sin cifrar a los servicios vinculados al servidor virtual. La descarga del procesamiento SSL de uso intensivo de la CPU en el dispositivo permite que los servidores back-end procesen un mayor número de solicitudes.

Agregar un servidor virtual basado en SSL mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para crear un servidor virtual basado en SSL y compruebe la configuración:

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

> **Precaución:** Para garantizar conexiones seguras, debe vincular un certificado SSL válido al servidor virtual basado en SSL antes de habilitarlo.

Ejemplo:

```
> add lb vserver vserver-SSL-1 SSL 10.102.29.50 443
  Done


  > show lb vserver vserver-SSL-1


  vserver-SSL-1 (10.102.29.50:443) - SSL Type: ADDRESS


  State: DOWN[Certkey not bound] Last state change was at Tue Jun 16
     06:33:08 2009 (+176 ms)


  Time since last state change: 0 days, 00:03:44.120
```



```
15
16
17    Effective State: DOWN Client Idle Timeout: 180 sec
18
19
20    Down state flush: ENABLED
21
22
23    Disable Primary Vserver On Down : DISABLED
24
25
26    No. of Bound Services : 0 (Total) 0 (Active)
27
28
29    Configured Method: LEASTCONNECTION Mode: IP
30
31
32    Persistence: NONE
33
34
35    Vserver IP and Port insertion: OFF
36
37
38    Push: DISABLED Push VServer: Push Multi Clients: NO Push Label Rule:
          Done
39  <!--NeedCopy-->
```

Agregar un servidor virtual basado en SSL mediante la interfaz gráfica de usuario

Siga estos pasos:

1. Vaya a **Administración del tráfico > Descarga SSL > Servidores virtuales**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En el cuadro de diálogo **Crear servidor virtual (descarga SSL)**, escriba el nombre del servidor virtual, la dirección IP y el puerto.
4. En la lista **Protocolo**, seleccione el tipo de servidor virtual, por ejemplo, SSL.
5. Haga clic en **Crear**y, a continuación, en **Cerrar**.
6. Compruebe que los parámetros configurados están correctamente configurados seleccionando el servidor virtual y visualizando la sección Detalles en la parte inferior del panel. El servidor virtual está marcado como DOWN porque el par de claves de certificado y los servicios no se han vinculado a él.

> **Precaución:** Para garantizar conexiones seguras, debe vincular un certificado SSL válido al servidor virtual basado en SSL antes de habilitarlo.

Enlazar servicios al servidor virtual SSL

Tras descifrar los datos entrantes, el servidor virtual SSL reenvía los datos a los servicios vinculados al servidor virtual.

La transferencia de datos entre el dispositivo y los servidores se puede cifrar o en texto sin cifrar. Si la transferencia de datos entre el dispositivo y los servidores está cifrada, toda la transacción estará segura de extremo a extremo. Para obtener más información sobre cómo configurar el sistema para la seguridad integral, consulte Descarga y aceleración SSL.

Enlazar un servicio a un servidor virtual mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para enlazar un servicio al servidor virtual SSL y compruebe la configuración:

```
-  bind lb vserver <name> <serviceName>
-  show lb vserver <name>
<!--NeedCopy-->
```

Ejemplo:

```
> bind lb vserver vserver-SSL-1 SVC_HTTP1



  Done


  > show lb vserver vserver-SSL-1 vserver-SSL-1 (10.102.29.50:443) -
     SSL Type:

  ADDRESS State: DOWN[Certkey not bound]

  Last state change was at Tue Jun 16 06:33:08 2009 (+174 ms)

```



```
17
18    Time since last state change: 0 days, 00:31:53.70
19
20
21    Effective State: DOWN Client Idle
22
23
24    Timeout: 180 sec
25
26
27    Down state flush: ENABLED Disable Primary Vserver On Down :
28
29
30    DISABLED No. of Bound Services : 1 (Total) 0 (Active)
31
32
33    Configured Method: LEASTCONNECTION Mode: IP Persistence: NONE Vserver
          IP and
34
35
36    Port insertion: OFF Push: DISABLED Push VServer: Push Multi Clients:
         NO Push Label Rule:
37
38
39
40
41
42    1) SVC_HTTP1 (10.102.29.18: 80) - HTTP
43
44
45    State: DOWN Weight: 1
46
47
48    Done
49  <!--NeedCopy-->
```

Enlazar un servicio a un servidor virtual mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Descarga SSL > Servidores virtuales**.
2. En el panel de detalles, seleccione un servidor virtual y haga clic en **Open**.
3. En la ficha **Servicios**, en la columna **Activo**, seleccione las casillas de verificación situadas junto a los servicios que quiere enlazar al servidor virtual seleccionado.
4. Haga clic en **OK**.

5. Compruebe que el contador Número de servicios vinculados de la sección Detalles de la parte inferior del panel se incrementa en función del número de servicios vinculados al servidor virtual.

Agregar un par de claves de certificado

Un certificado SSL es un elemento integral del proceso de intercambio de claves SSL y de cifrado/descifrado. El certificado se utiliza durante un enlace SSL para establecer la identidad del servidor SSL. Puede utilizar un certificado SSL válido existente que tenga en el dispositivo Citrix ADC o puede crear su propio certificado SSL. El dispositivo admite certificados RSA de hasta 4096 bits.

Se admiten certificados ECDSA con las curvas siguientes:

- prime256v1 (P_256 en el ADC)
- secp384r1 (P_384 en el ADC)
- secp521r1 (P_521 en el ADC; solo compatible con VPX)
- secp224r1 (P_224 en el ADC; solo compatible con VPX)

> **Nota:** Citrix recomienda utilizar un certificado SSL válido emitido por una entidad emisora de certificados de confianza. Los certificados no válidos y los certificados de creación propia no son compatibles con todos los clientes SSL.

Para poder usar un certificado para el procesamiento SSL, debes emparejarlo con su clave correspondiente. El par de claves de certificado se vincula al servidor virtual y se utiliza para el procesamiento SSL.

Agregar un par de claves de certificado mediante la CLI

> **Nota:** Para obtener información sobre la creación de un par de claves de certificado ECDSA, consulte Crear un par de claves de certificado ECDSA.

En el símbolo del sistema, escriba los siguientes comandos para crear un par de claves de certificado y verificar la configuración:

```
1 -  add ssl certKey <certkeyName> -cert <string> [-key <string>]
2 -  show sslcertkey <name>
3 <!--NeedCopy-->
```

Ejemplo:

```
1 > add ssl certKey CertKey-SSL-1 -cert ns-root.cert -key ns-root.key
2
```



```
 Done


> show sslcertkey CertKey-SSL-1


   Name: CertKey-SSL-1 Status: Valid,


   Days to expiration:4811 Version: 3


   Serial Number: 00 Signature Algorithm: md5WithRSAEncryption Issuer:
      C=US,ST=California,L=San


   Jose,O=Citrix ANG,OU=NS Internal,CN=de fault


   Validity Not Before: Oct 6 06:52:07 2006 GMT Not After : Aug 17
      21:26:47 2022 GMT


   Subject: C=US,ST=California,L=San Jose,O=Citrix ANG,OU=NS Internal,
      CN=d efault Public Key


   Algorithm: rsaEncryption Public Key


   size: 1024


 Done
<!--NeedCopy-->
```

Agregar un par de claves de certificado mediante la interfaz gráfica de usuario

Siga estos pasos:

1. Vaya a **Administración del tráfico > SSL > Certificados**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En el cuadro de diálogo **Instalar certificado**, en el cuadro de texto Nombre del par de claves de certificado, escriba un nombre para el par de claves de certificado que quiere agregar, por

ejemplo, Certkey-SSL-1.

4. En **Detalles**, en Nombre de archivo de certificado, haga clic en **Examinar (dispositivo)** para buscar el certificado. Tanto el certificado como la clave se almacenan en la carpeta /nsconfig/ssl/ del dispositivo. Para utilizar un certificado presente en el sistema local, seleccione Local.
5. Seleccione el certificado que quiera usar y, a continuación, haga clic en **Seleccionar**.
6. En Nombre de archivo de clave privada, haga clic en **Examinar (dispositivo)** para buscar el archivo de clave privada. Para utilizar una clave privada presente en el sistema local, seleccione Local.
7. Selecciona la clave que quieres usar y haga clic en **Seleccionar**. Para cifrar la clave utilizada en el par de claves de certificado, escriba la contraseña que se utilizará para el cifrado en el cuadro de texto Contraseña.
8. Haga clic en **Instalar**.
9. Haga doble clic en el par de claves de certificado y, en la ventana Detalles del certificado, compruebe que los parámetros se han configurado correctamente y guardado.

Enlazar un par de claves de certificado SSL al servidor virtual

Después de emparejar un certificado SSL con su clave correspondiente, vincule el par de claves de certificado al servidor virtual SSL para que se pueda utilizar para el procesamiento SSL. Las sesiones seguras requieren establecer una conexión entre el equipo cliente y un servidor virtual basado en SSL del dispositivo. El procesamiento SSL se lleva a cabo en el tráfico entrante en el servidor virtual. Por lo tanto, antes de habilitar el servidor virtual SSL en el dispositivo, debe vincular un certificado SSL válido al servidor virtual SSL.

Enlazar un par de claves de certificado SSL a un servidor virtual mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para enlazar un par de claves de certificado SSL a un servidor virtual y compruebe la configuración:

```
- bind ssl vserver <vServerName> -certkeyName <string>
- show ssl vserver <name>
<!--NeedCopy-->
```

Ejemplo:

```
> bind ssl vserver Vserver-SSL-1 -certkeyName CertKey-SSL-1

Done

```



```
> show ssl vserver Vserver-SSL-1

    Advanced SSL configuration for VServer Vserver-SSL-1:

    DH: DISABLED

    Ephemeral RSA: ENABLED Refresh Count: 0

    Session Reuse: ENABLED Timeout: 120 seconds

    Cipher Redirect: ENABLED

    SSLv2 Redirect: ENABLED

    ClearText Port: 0

    Client Auth: DISABLED

    SSL Redirect: DISABLED

    Non FIPS Ciphers: DISABLED

    SSLv2: DISABLED SSLv3: ENABLED TLSv1: ENABLED

1) CertKey Name: CertKey-SSL-1 Server Certificate
```



```
50
51 1) Cipher Name: DEFAULT
52
53
54    Description: Predefined Cipher Alias
55
56
57 Done
58 <!--NeedCopy-->
```

Enlazar un par de claves de certificado SSL a un servidor virtual mediante la interfaz gráfica de usuario

Siga estos pasos:

1. Vaya a **Administración del tráfico > Descarga SSL > Servidores virtuales**.
2. Seleccione el servidor virtual al que quiere enlazar el par de claves de certificado, por ejemplo, vServer-SSL-1 y haga clic en Abrir.
3. En el cuadro de diálogo **Configurar servidor virtual (descarga SSL)**, en la ficha **Configuración SSL**, en **Disponible**, seleccione el par de claves de certificado que quiere enlazar al servidor virtual. A continuación, haga clic en **Agregar**.
4. Haga clic en **OK**.
5. Compruebe que el par de claves de certificado que ha seleccionado aparece en el área Configurado.

Configurar compatibilidad con el acceso web de Outlook

Si utiliza servidores Outlook Web Access (OWA) en el dispositivo Citrix ADC, debe configurar el dispositivo para que inserte un campo de encabezado especial, FRONT-END-HTTPS: ON, en las solicitudes HTTP dirigidas a los servidores OWA, de modo que los servidores generen vínculos URL `https://` en lugar de `http://`.

Nota: Solo puede habilitar la compatibilidad de OWA para servidores y servicios virtuales SSL basados en HTTP. No se puede aplicar a los servidores y servicios virtuales SSL basados en TCP.

Para configurar la compatibilidad con OWA, haga lo siguiente:

- Cree una acción SSL para habilitar la compatibilidad con OWA.
- Cree una directiva SSL.
- Enlace la directiva al servidor virtual SSL.

Crear una acción SSL para habilitar la compatibilidad con OWA

Para poder habilitar la compatibilidad con Outlook Web Access (OWA), debe crear una acción SSL. Las acciones SSL están vinculadas a directivas SSL y se activan cuando los datos entrantes coinciden con la regla especificada por la directiva.

Crear una acción SSL para habilitar el soporte de OWA mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para crear una acción SSL que permita la compatibilidad con OWA y compruebe la configuración:

```
-  add ssl action <name> -OWASupport ENABLED
-  show SSL action <name>
<!--NeedCopy-->
```

Ejemplo:

```
    > add ssl action Action-SSL-OWA -OWASupport enabled



    Done

    > show SSL action Action-SSL-OWA

    Name: Action-SSL-OWA

    Data Insertion Action: OWA

    Support: ENABLED

    Done
<!--NeedCopy-->
```


Crear una acción SSL para habilitar la compatibilidad con OWA mediante la interfaz gráfica de usuario

Siga estos pasos:

1. Vaya a **Administración del tráfico > SSL > Directivas**.
2. En el panel de detalles, en la ficha **Acciones**, haga clic en **Agregar**.
3. En el cuadro de diálogo **Crear acción SSL**, en el cuadro de texto Nombre, escriba Action-SSL-OWA.
4. En Outlook Web Access, seleccione **Habilitado**.
5. Haga clic en **Crear**y, a continuación, en **Cerrar**.
6. Compruebe que Action-SSL-OWA aparezca en la página **Acciones SSL** .

Crear directivas SSL

Las directivas SSL se crean mediante la infraestructura de directivas. Cada directiva SSL tiene vinculada una acción SSL y la acción se lleva a cabo cuando el tráfico entrante coincide con la regla que se ha configurado en la directiva.

Crear una directiva SSL mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para configurar una directiva SSL y verifique la configuración:

```
-  add ssl policy <name> -rule <expression> -reqAction <string>
-  show ssl policy <name>
<!--NeedCopy-->
```

Ejemplo:

```
> add ssl policy-SSL-1 -rule ns_true -reqaction Action-SSL-OWA

Done

> show ssl policy-SSL-1

Name: Policy-SSL-1 Rule: ns_true

Action: Action-SSL-OWA Hits: 0

Policy is bound to following entities
```



```
12
13 1) PRIORITY : 0
14
15 Done
16 <!--NeedCopy-->
```

Crear una directiva SSL mediante la interfaz gráfica de usuario

Siga estos pasos:

1. Vaya a **Administración del tráfico > SSL > Directivas**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En el cuadro de diálogo **Crear directiva SSL**, en el cuadro de texto Nombre, escriba el nombre de la directiva SSL (por ejemplo, Policy-SSL-1).
4. En **Solicitar** acción, seleccione la acción SSL configurada que quiere asociar a esta directiva (por ejemplo, Action-SSL-OWA). La expresión general ns_true aplica la directiva a todo el tráfico de enlace SSL correcto. Sin embargo, para filtrar respuestas específicas, puede crear directivas con un nivel más alto de detalle. Para obtener más información sobre la configuración de expresiones de directivas granulares, consulte Acciones y directivas SSL.
5. En **Expresiones con nombre**, elija la expresión general integrada ns_true y haga clic en **Agregar expresión**. La expresión ns_true aparece ahora en el cuadro de texto Expresión.
6. Haga clic en **Crear**y, a continuación, en **Cerrar**.
7. Compruebe que la directiva está configurada correctamente seleccionándola y visualizando la sección Detalles en la parte inferior del panel.

Enlazar la directiva SSL al servidor virtual SSL

Después de configurar una directiva SSL para Outlook Web Access, vincule la directiva a un servidor virtual que interceptará el tráfico entrante de Outlook. Si los datos entrantes coinciden con alguna de las reglas configuradas en la directiva SSL, la directiva se desencadena y se lleva a cabo la acción asociada a ella.

Enlazar una directiva SSL a un servidor virtual SSL mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para enlazar una directiva SSL a un servidor virtual SSL y compruebe la configuración:

```
1 -  bind ssl vserver <vServerName> -policyName <string>
2 -  show ssl vserver <name>
3 <!--NeedCopy-->
```


Ejemplo:

```
> bind ssl vserver Vserver-SSL-1 -policyName Policy-SSL-1

 Done

> show ssl vserver Vserver-SSL-1

Advanced SSL configuration for VServer Vserver-SSL-1:

DH: DISABLED

Ephemeral RSA: ENABLED

Refresh Count: 0

Session Reuse: ENABLED

Timeout: 120 seconds

Cipher Redirect: ENABLED

SSLv2 Redirect: ENABLED

ClearText Port: 0

Client Auth: DISABLED

SSL Redirect: DISABLED

Non FIPS Ciphers: DISABLED

SSLv2: DISABLED SSLv3: ENABLED TLSv1: ENABLED

1) CertKey Name: CertKey-SSL-1 Server Certificate

1) Policy Name: Policy-SSL-1 Priority: 0

1) Cipher Name: DEFAULT Description: Predefined Cipher Alias

Done
<!--NeedCopy-->
```


Enlazar una directiva SSL a un servidor virtual SSL mediante la interfaz gráfica de usuario

Siga estos pasos:

1. Vaya a **Administración del tráfico > Descarga SSL > Servidores virtuales**.
2. En el panel de detalles, seleccione el servidor virtual (por ejemplo, vServer-SSL-1) y, a continuación, haga clic en **Abrir**.
3. En el cuadro de diálogo **Configurar servidor virtual (descarga SSL)**, haga clic en **Insertar directiva**y, a continuación, seleccione la directiva que quiere enlazar al servidor virtual SSL. Si lo quiere, puede hacer doble clic en el campo Prioridad y escribir un nuevo nivel de prioridad.
4. Haga clic en **OK**.

Funciones de un vistazo

August 20, 2021

Las funciones de Citrix ADC se pueden configurar de forma independiente o en combinación para satisfacer necesidades específicas. Aunque algunas funciones se ajustan a más de una categoría, las numerosas funciones de Citrix ADC generalmente se pueden clasificar como funciones de administración de tráfico y conmutación de aplicaciones, funciones de aceleración de aplicaciones, funciones de seguridad de aplicaciones y funciones de firewall y seguridad de aplicaciones, así como una función de visibilidad de aplicaciones.

Para comprender el orden en que las funciones realizan su procesamiento, consulte la sección Orden de procesamiento de funciones .

Funciones de gestión del tráfico y conmutación de aplicaciones

January 31, 2022

A continuación se muestran las funciones de gestión del tráfico y conmutación de aplicaciones.

Descarga SSL

Descarga de forma transparente el cifrado y el descifrado SSL de los servidores web, lo que libera recursos del servidor para atender las solicitudes de contenido. SSL supone una pesada carga para el rendimiento de una aplicación y puede hacer que muchas medidas de optimización sean ineficaces. La descarga de SSL y la aceleración permiten aplicar todos los beneficios de la tecnología Citrix Request Switching al tráfico SSL, lo que garantiza la entrega segura de aplicaciones web sin degradar el rendimiento del usuario final.

Para obtener más información, consulte Descarga y aceleración de SSL.

Listas de control de acceso

Compara los paquetes entrantes con las listas de control de acceso (ACL). Si un paquete coincide con una regla de ACL, la acción especificada en la regla se aplica al paquete. De lo contrario, se aplica la acción predeterminada (ALLOW) y el paquete se procesa normalmente. Para que el dispositivo compare los paquetes entrantes con las ACL, debe aplicar las ACL. Todas las ACL están habilitadas de forma predeterminada, pero debe aplicarlas para que el dispositivo Citrix ADC compare los paquetes entrantes con ellas. Si no es necesario que una ACL forme parte de la tabla de búsqueda, pero debe conservarse en la configuración, debe inhabilitarse antes de que se apliquen las ACL. Un dispositivo ADC no compara los paquetes entrantes con ACL inhabilitadas.

Para obtener más información, consulte Lista de control de acceso.

Equilibrio de carga

Las decisiones de equilibrio de carga se basan en una variedad de algoritmos, como round robin, menos conexiones, menor ancho de banda ponderado, menos paquetes ponderados, tiempo de respuesta mínimo y hash basado en URL, IP de origen de dominio o IP de destino. Se admiten los protocolos TCP y UDP, por lo que el dispositivo Citrix ADC puede equilibrar la carga de todo el tráfico que utiliza esos protocolos como operador subyacente (por ejemplo, HTTP, HTTPS, UDP, DNS, NNTP y tráfico de firewall general). Además, el dispositivo ADC puede mantener la persistencia de la sesión según la IP de origen, la cookie, el servidor, el grupo o la sesión SSL. Permite a los usuarios aplicar la verificación ampliada de contenido (ECV) personalizada a servidores, cachés, firewalls y otros dispositivos de infraestructura para garantizar que estos sistemas funcionan correctamente y proporcionan el contenido adecuado a los usuarios. También puede realizar comprobaciones de estado mediante ping, TCP o URL HTTP, y el usuario puede crear monitores basados en scripts Perl.
Para proporcionar una optimización de WAN a gran escala, los dispositivos CloudBridge implementados en los centros de datos se pueden equilibrar la carga mediante dispositivos Citrix ADC. El ancho de banda y el número de sesiones simultáneas se pueden mejorar significativamente.

Para obtener más información, consulte Equilibrio de carga.

Dominios de tráfico

Los dominios de tráfico proporcionan una forma de crear particiones ADC lógicas en un único dispositivo Citrix ADC. Le permiten segmentar el tráfico de red para distintas aplicaciones. Puede utilizar dominios de tráfico para crear varios entornos aislados cuyos recursos no interactúan entre sí. Una aplicación que pertenece a un dominio de tráfico específico se comunica solo con entidades y procesa el tráfico dentro de ese dominio. El tráfico perteneciente a un dominio de tráfico no puede cruzar los

límites de otro dominio de tráfico. Por lo tanto, puede utilizar direcciones IP duplicadas en el dispositivo siempre y cuando las direcciones no se dupliquen en el mismo dominio.

Para obtener más información, consulte Dominios de tráfico.

Traducción de direcciones de red

La traducción de direcciones de red (NAT) implica la modificación de las direcciones IP de origen y/o destino, y/o los números de puerto TCP/UDP, de los paquetes IP que pasan por el dispositivo Citrix ADC. La activación de NAT en el dispositivo mejora la seguridad de su red privada y la protege de una red pública como Internet, modificando las direcciones IP de origen de la red cuando los datos pasan por el dispositivo Citrix ADC.

El dispositivo Citrix ADC admite los siguientes tipos de traducción de direcciones de red:

INAT: En NAT entrante (INAT), una dirección IP (normalmente pública) configurada en el dispositivo Citrix ADC escucha las solicitudes de conexión en nombre de un servidor. En el caso de un paquete de solicitud recibido por el dispositivo en una dirección IP pública, el ADC reemplaza la dirección IP de destino por la dirección IP privada del servidor. En otras palabras, el dispositivo actúa como proxy entre los clientes y el servidor. La configuración de INAT incluye reglas INAT, que definen una relación 1:1 entre la dirección IP del dispositivo Citrix ADC y la dirección IP del servidor.

RNAT: En la traducción inversa de direcciones de red (RNAT), para una sesión iniciada por un servidor, el dispositivo Citrix ADC reemplaza la dirección IP de origen de los paquetes generados por el servidor por una dirección IP (tipo SNIP) configurada en el dispositivo. De este modo, el dispositivo evita la exposición de la dirección IP del servidor en cualquiera de los paquetes generados por el servidor. Una configuración de RNAT implica una regla RNAT, que especifica una condición. El dispositivo realiza el procesamiento RNAT en los paquetes que coinciden con la condición.

Traducción sin estado de NAT46: El NAT46 sin estado permite la comunicación entre redes IPv4 e IPv6, mediante la traducción de paquetes IPv4 a IPv6 y viceversa, sin mantener ninguna información de sesión en el dispositivo Citrix ADC. Una configuración NAT46 sin estado incluye una regla INAT IPv4-IPv6 y un prefijo IPv6 NAT46.

Traducción con estado de NAT64: La función NAT64 con estado permite la comunicación entre clientes IPv4 y servidores IPv6 a través de la traducción de paquetes IPv6 a IPv4, y viceversa, al tiempo que mantiene la información de sesión en el dispositivo Citrix ADC. Una configuración NAT64 con estado implica una regla NAT64 y un prefijo NAT64 IPv6.

Para obtener más información, consulte Configuración de la traducción de direcciones de red.

Compatibilidad con TCP de rutas múltiples

Los dispositivos Citrix ADC admiten TCP multiruta (MPTCP). MPTCP es una extensión de protocolo TCP/IP que identifica y utiliza varias rutas disponibles entre hosts para mantener la sesión TCP. Debe

habilitar MPTCP en un perfil TCP y vincularlo a un servidor virtual. Cuando MPTCP está habilitado, el servidor virtual funciona como una Gateway MPTCP y convierte las conexiones MPTCP con los clientes en conexiones TCP que mantiene con los servidores.

Para obtener más información, consulte MPTCP (TCP de múltiples rutas).

Conmutación de contenido

Determina el servidor al que se va a enviar la solicitud en función de las directivas de conmutación de contenido configuradas. Las reglas de directivas se pueden basar en la dirección IP, la URL y los encabezados HTTP. Esto permite que las decisiones de conmutación se basen en las funciones del usuario y del dispositivo, como quién es el usuario, qué tipo de agente se está usando y qué contenido solicitó el usuario.

Para obtener más información, consulte Cambio de contenido.

Equilibrio de carga global del servidor (GSLB)

Amplía las capacidades de administración del tráfico de NetScaler para incluir sitios de Internet distribuidos y empresas globales. Independientemente de que las instalaciones se distribuyan en varias ubicaciones de red o en varios clústeres en una sola ubicación, NetScaler mantiene la disponibilidad y distribuye el tráfico entre ellas. Toma decisiones de DNS inteligentes para evitar que los usuarios sean enviados a un sitio que está caído o sobrecargado. Cuando se habilita el método GSLB basado en proximidad, NetScaler puede tomar decisiones de equilibrio de carga en función de la proximidad del servidor DNS local (LDNS) del cliente en relación con diferentes sitios. El principal beneficio del método GSLB basado en proximidad es un tiempo de respuesta más rápido resultante de la selección del sitio más cercano disponible.

Para obtener más información, consulte Equilibrio de carga global del servidor.

Redirección dinámica

Permite a los routers obtener información de topología, rutas y direcciones IP de los routers vecinos de forma automática. Cuando se habilita la redirección dinámica, el proceso de redirección correspondiente escucha las actualizaciones de ruta y anuncia las rutas. Los procesos de redirección también se pueden colocar en modo pasivo. Los protocolos de redirección permiten a un router ascendente equilibrar la carga del tráfico a servidores virtuales idénticos alojados en dos unidades NetScaler independientes mediante la técnica Equal Cost Multipath.

Para obtener más información, consulte Configuración de rutas dinámicas.

Equilibrio de carga de enlaces

Equilibra la carga de varios enlaces WAN y proporciona conmutación por error de enlaces, lo que optimiza aún más el rendimiento de la red y garantiza la continuidad del negocio. Garantiza que las conexiones de red sigan siendo altamente disponibles mediante la aplicación de controles de estado y control de tráfico inteligentes para distribuir el tráfico de forma eficiente entre los routers ascendentes. Identifica el mejor enlace WAN para redirigir el tráfico entrante y saliente en función de las directivas y las condiciones de red, y protege las aplicaciones contra fallos de WAN o de enlace a Internet al proporcionar detección rápida de fallos y conmutación por error.

Para obtener más información, consulte Equilibrio de carga de vínculos.

Optimización TCP

Puede utilizar perfiles TCP para optimizar el tráfico TCP. Los perfiles TCP definen la forma en que los servidores virtuales NetScaler procesan el tráfico TCP. Los administradores pueden utilizar los perfiles TCP integrados o configurar perfiles personalizados. Tras definir un perfil TCP, puede vincularlo a un único servidor virtual o a varios servidores virtuales.

Algunas de las principales funciones de optimización que pueden habilitar los perfiles TCP son:

- TCP keep-alive: comprueba el estado operativo de los pares en intervalos de tiempo especificados para evitar que se rompa el enlace.
- Reconocimiento selectivo (SACK): mejora el rendimiento de la transmisión de datos, especialmente en redes largas y gruesas (LFN).
- Escalado de ventana TCP: Permite la transferencia eficiente de datos a través de redes largas de grasa (LFN).

Para obtener más información sobre los perfiles TCP, consulte Configuración de perfiles TCP.

Conector CloudBridge

La función Citrix NetScaler CloudBridge Connector, una parte fundamental del marco de trabajo de Citrix OpenCloud, es una herramienta que se utiliza para crear un centro de datos ampliado en la nube. OpenCloud Bridge le permite conectar uno o más dispositivos Citrix ADC o dispositivos virtuales NetScaler en la nube a su red sin necesidad de volver a configurar la red. Las aplicaciones alojadas en la nube parecen ejecutarse en una red empresarial contigua. El objetivo principal de OpenCloud Bridge es permitir a las empresas trasladar sus aplicaciones a la nube a la vez que se reducen los costes y el riesgo de fallo de las aplicaciones. Además, OpenCloud Bridge aumenta la seguridad de la red en entornos de nube. Un puente OpenCloud es un puente de red de capa 2 que conecta un dispositivo Citrix ADC o un dispositivo virtual NetScaler en una instancia de nube a un dispositivo Citrix ADC o a un dispositivo virtual NetScaler de su LAN. La conexión se realiza a través de un túnel que utiliza el protocolo Genérico Encapsulación de redirección (GRE). El protocolo GRE proporciona un mecanismo

para encapsular paquetes de una amplia variedad de protocolos de red que se reenvían a través de otro protocolo. A continuación, se utiliza el conjunto de protocolos de seguridad de Protocolo Internet (IPSec) para proteger la comunicación entre los pares en OpenCloud Bridge.

Para obtener más información, consulte CloudBridge.

DataStream

La función NetScaler DataStream proporciona un mecanismo inteligente para el cambio de solicitudes en el nivel de la base de datos mediante la distribución de solicitudes en función de la consulta SQL que se envía.

Cuando se implementa frente a servidores de bases de datos, NetScaler garantiza una distribución óptima del tráfico desde los servidores de aplicaciones y los servidores web. Los administradores pueden segmentar el tráfico según la información de la consulta SQL y en función de los nombres de base de datos, nombres de usuario, conjuntos de caracteres y tamaño de paquete.

Puede configurar el equilibrio de carga para cambiar las solicitudes de acuerdo con los algoritmos de equilibrio de carga, o puede elaborar los criterios de conmutación configurando el cambio de contenido para tomar una decisión basada en los parámetros de consulta SQL, como el nombre de usuario, los nombres de bases de datos y los parámetros de comandos. Puede configurar más monitores para realizar un seguimiento de los estados de los servidores de bases de datos.

La infraestructura de directivas avanzada del dispositivo Citrix ADC incluye expresiones que se pueden utilizar para evaluar y procesar las solicitudes. Las expresiones avanzadas evalúan el tráfico asociado a los servidores de bases de datos MySQL. Puede utilizar expresiones basadas en solicitudes (expresiones que empiezan por MYSQL.CLIENT y MYSQL.REQ) en directivas avanzadas para tomar decisiones de cambio de solicitud en el punto de enlace del servidor virtual de conmutación de contenido y en las expresiones basadas en respuestas (expresiones que comienzan por MYSQL.RES) para evaluar las respuestas del servidor al usuario monitores de estado configurados.

> Nota: DataStream es compatible con bases de datos MySQL y MS SQL.

Para obtener más información, consulte DataStream.

Funciones de aceleración de aplicaciones

August 20, 2021

- AppCompress

  Utiliza el protocolo de compresión gzip para proporcionar compresión transparente para archivos HTML y de texto. La relación de compresión típica de 4:1 produce una reducción de

hasta un 50% en los requisitos de ancho de banda fuera del centro de datos. También resulta en una mejora significativa del tiempo de respuesta del usuario final, ya que reduce la cantidad de datos que se deben entregar al explorador del usuario.

- Redirección de caché

  Administra el flujo de tráfico a un proxy inverso, proxy transparente o comunidad de caché de proxy de reenvío. Inspecciona todas las solicitudes e identifica las solicitudes que no se pueden almacenar en caché y las envía directamente a los servidores de origen a través de conexiones persistentes. Al redirigir de forma inteligente las solicitudes que no se pueden almacenar en caché a los servidores web de origen, el dispositivo Citrix ADC libera recursos de caché y aumenta las tasas de aciertos de caché, al tiempo que reduce el consumo general de ancho de banda y los retrasos de respuesta para estas solicitudes.

  Para obtener más información, consulte Redirección de caché.

- AppCache

  Ayuda a optimizar el contenido web y la entrega de datos de aplicaciones al proporcionar un rápido almacenamiento en caché web compatible con HTTP/1.1 y HTTP/1.0 en memoria para contenido estático y dinámico. Esta memoria caché integrada almacena los resultados de las solicitudes de aplicación entrantes incluso cuando una solicitud entrante está protegida o los datos comprimidos, y luego reutiliza los datos para satisfacer las solicitudes posteriores de la misma información. Al servir datos directamente desde la memoria caché integrada, el dispositivo puede reducir los tiempos de regeneración de páginas al eliminar la necesidad de canalizar solicitudes de contenido estático y dinámico al servidor.

  Para obtener más información, consulte Almacenamiento en caché integrado.

- Almacenamiento en búfer TCP

  Buffers la respuesta del servidor y la entrega al cliente a la velocidad del cliente, descargando el servidor más rápido y mejorando así el rendimiento de los sitios web.

Funciones de firewall y seguridad de aplicaciones

February 19, 2022

A continuación se muestran las funciones de seguridad y firewall.

Defensa contra ataques de denegación de servicio (DoS)

Detecta y detiene los ataques de denegación de servicio distribuido (DDoS) maliciosos y otros tipos de ataques maliciosos antes de que lleguen a los servidores, lo que evita que afecten al rendimiento

de la red y las aplicaciones. El dispositivo Citrix ADC identifica a los clientes legítimos y aumenta su prioridad, lo que hace que los clientes sospechosos no puedan consumir un porcentaje desproporcionado de recursos y paralizar su sitio. El dispositivo proporciona protección a nivel de aplicación contra los siguientes tipos de ataques maliciosos:

- Los ataques de inundación SYN
- Ataques de pipeline
- Ataques lágrima
- Los ataques terrestres
- Ataques frágiles
- Ataques de conexión zombie

El dispositivo se defiende de forma agresiva contra este tipo de ataques impidiendo la asignación de recursos del servidor para estas conexiones. Esto aísla a los servidores de la abrumadora cantidad de paquetes asociados a estos eventos.

El dispositivo también protege los recursos de red de los ataques basados en ICMP mediante la limitación de velocidad ICMP y la inspección agresiva de paquetes ICMP. Realiza un reensamblaje IP sólido, elimina una variedad de paquetes sospechosos y mal formados y aplica Listas de control de acceso (ACL) al tráfico del sitio para mayor protección.

Para obtener más información, consulte Protección contra denegación de servicio HTTP.

Filtrado de contenido

Proporciona protección contra ataques maliciosos para sitios web de nivel 7. El dispositivo inspecciona cada solicitud entrante según reglas configuradas por el usuario basadas en encabezados HTTP y realiza la acción configurada por el usuario. Las acciones pueden incluir restablecer la conexión, soltar la solicitud o enviar un mensaje de error al explorador del usuario. Esto permite al dispositivo detectar solicitudes no deseadas y reduce la exposición de los servidores a los ataques.

Esta función también puede analizar las solicitudes HTTP GET y POST y filtrar las firmas incorrectas conocidas, lo que le permite defender sus servidores contra ataques basados en HTTP.

Para obtener más información, consulte Filtrado de contenido.

Responder

Funciona como un filtro avanzado y se puede utilizar para generar respuestas desde el dispositivo al cliente. Algunos usos comunes de esta función son la generación de respuestas de redirección, respuestas definidas por el usuario y restablecimientos.

Para obtener más información, consulte Respondedor.

Reescribe

Modifica los encabezados HTTP y el cuerpo del texto. Puede utilizar la función de reescritura para agregar encabezados HTTP a una solicitud o respuesta HTTP, modificar encabezados HTTP individuales o eliminar encabezados HTTP. También permite modificar el cuerpo HTTP en solicitudes y respuestas.

Cuando el dispositivo recibe una solicitud o envía una respuesta, comprueba si hay reglas de reescritura y, si existen reglas aplicables, las aplica a la solicitud o respuesta antes de transmitirlas al servidor web o al equipo cliente.

Para obtener más información, consulte Reescritura.

Protección contra picos de tensión

Regula el flujo de solicitudes de los usuarios a los servidores y controla el número de usuarios que pueden acceder simultáneamente a los recursos de los servidores, lo que pone en cola cualquier solicitud adicional una vez que los servidores hayan alcanzado su capacidad. Al controlar la velocidad a la que se pueden establecer conexiones, el dispositivo impide que las sobretensiones en las solicitudes se transfieran a los servidores, evitando así la sobrecarga del sitio.

Para obtener más información, consulte Protección contra sobretensiones.

Citrix Gateway

Citrix Gateway es una solución de acceso seguro a las aplicaciones que proporciona a los administradores controles detallados de directivas y acciones a nivel de aplicación para proteger el acceso a las aplicaciones y los datos, a la vez que permite a los usuarios trabajar desde cualquier lugar. Proporciona a los administradores de TI un único punto de control y herramientas para ayudar a garantizar el cumplimiento de las normativas y los niveles más altos de seguridad de la información dentro y fuera de la empresa. Al mismo tiempo, proporciona a los usuarios un único punto de acceso (optimizado para funciones, dispositivos y redes) a las aplicaciones empresariales y los datos que necesitan. Esta combinación única de capacidades ayuda a maximizar la productividad de la fuerza de trabajo móvil actual.

Para obtener más información, consulte Citrix Gateway.

Firewall de aplicaciones

Protege las aplicaciones del uso indebido por parte de hackers y malware, como ataques de scripts entre sitios, ataques de desbordamiento de búfer, ataques de inyección SQL y navegación forzada, filtrando el tráfico entre cada servidor web protegido y los usuarios que se conectan a cualquier sitio web de ese servidor web. El firewall de la aplicación examina todo el tráfico en busca de pruebas

de ataques a la seguridad del servidor web o mal uso de los recursos del servidor web, y toma las medidas adecuadas para evitar que estos ataques tengan éxito.

Para obtener más información, consulte Firewall de aplicaciones.

Función de visibilidad de aplicaciones

August 20, 2021

- Citrix Application Delivery Management

  Citrix Application Delivery Management (ADM) es un recopilador de alto rendimiento que proporciona visibilidad integral de la experiencia del usuario en el tráfico Web y HDX (ICA). Recopila registros HTTP e ICA AppFlow generados por los dispositivos Citrix ADC y rellena los informes analíticos que cubren las estadísticas de la capa 3 a la capa 7. Citrix ADM proporciona un análisis detallado de los últimos cinco minutos de datos en tiempo real y de los datos históricos recopilados durante la última hora, un día, una semana y un mes.

  El panel analítico HDX (ICA) le permite profundizar desde usuarios de HDX, aplicaciones, escritorios e incluso desde información a nivel de puerta de enlace. Del mismo modo, el análisis HTTP proporciona una vista general de las aplicaciones web, las direcciones URL a las que se accede, las direcciones IP del cliente y las direcciones IP del servidor, y otros paneles. El administrador puede profundizar e identificar los puntos problemáticos desde cualquiera de estos paneles, según corresponda en el caso de uso.

- Visibilidad mejorada de las aplicaciones mediante AppFlow

  El dispositivo Citrix ADC es un punto central de control para todo el tráfico de aplicaciones en el centro de datos. Recopila información de flujo y nivel de sesión de usuario valiosa para aplicaciones de supervisión del rendimiento de las aplicaciones, análisis e inteligencia empresarial. AppFlow transmite esta información mediante el formato de Internet Protocol Flow Information Export (IPFIX), que es un estándar abierto de Internet Engineering Task Force (IETF) definido en RFC 5101. IPFIX (la versión estandarizada de NetFlow de Cisco) se utiliza ampliamente para supervisar la información de flujo de red. AppFlow define nuevos elementos de información para representar la información de nivel de aplicación.

  Con UDP como protocolo de transporte, AppFlow transmite los datos recopilados, denominados *registros de flujo*, a uno o más recopiladores IPv4. Los recopiladores agregan los registros de flujo y generan informes históricos o en tiempo real.

  AppFlow proporciona visibilidad en el nivel de transacción para flujos HTTP, SSL, TCP y SSL_TCP. Puede muestrear y filtrar los tipos de flujo que quiere supervisar.

Para limitar los tipos de flujos a supervisar, mediante el muestreo y el filtrado del tráfico de aplicaciones, puede habilitar AppFlow para un servidor virtual. AppFlow también puede proporcionar estadísticas para el servidor virtual.

También puede habilitar AppFlow para un servicio específico, que represente un servidor de aplicaciones, y supervisar el tráfico a ese servidor de aplicaciones.

Para obtener más información, consulte AppFlow.

- Stream Analytics

  El rendimiento de su sitio web o aplicación depende de qué tan bien se optimice la entrega del contenido solicitado con más frecuencia. Técnicas como el almacenamiento en caché y la compresión ayudan a acelerar la entrega de servicios a los clientes, pero debe poder identificar los recursos que se solicitan con mayor frecuencia y, a continuación, almacenar en caché o comprimir esos recursos. Puede identificar los recursos utilizados con más frecuencia agregando estadísticas en tiempo real sobre el tráfico de sitios web o aplicaciones. Estadísticas como la frecuencia con la que se accede a un recurso en relación con otros recursos y la cantidad de ancho de banda que consumen esos recursos ayudan a determinar si esos recursos deben almacenarse en caché o comprimirse para mejorar el rendimiento del servidor y la utilización de la red. Estadísticas como los tiempos de respuesta y el número de conexiones simultáneas a la aplicación le ayudan a determinar si debe mejorar los recursos del lado del servidor.

  Si el sitio web o la aplicación no cambia con frecuencia, puede utilizar productos que recopilan datos estadísticos, y luego analizar manualmente las estadísticas y optimizar la entrega de contenido. Sin embargo, si no quiere realizar optimizaciones manuales, o si su sitio web o aplicación es de naturaleza dinámica, necesita una infraestructura que no solo pueda recopilar datos estadísticos, sino que también pueda optimizar automáticamente la entrega de recursos en función de las estadísticas. En el dispositivo Citrix ADC, esta funcionalidad se proporciona mediante la función Stream Analytics. La función funciona en un único dispositivo Citrix ADC y recopila estadísticas de tiempo de ejecución basadas en los criterios definidos. Cuando se utiliza con directivas Citrix ADC, la función también le proporciona la infraestructura que necesita para la optimización automática del tráfico en tiempo real.

  Para obtener más información, consulte Action Analytics.

Soluciones Citrix ADC

January 19, 2021

Las soluciones Citrix ADC simplifican la tarea de configurar configuraciones implementadas con frecuencia. Compruebe este espacio de vez en cuando para obtener soluciones adicionales.

Esta sección incluye las siguientes soluciones.

- Configuración de Citrix ADC para Citrix Virtual Apps and Desktops
- Preferencia de zona alimentada de Equilibrio de carga de servidor global (GSLB)
- Compatibilidad con Anycast en Citrix ADC
- Implemente una plataforma de publicidad digital en AWS con Citrix ADC
- Mejorar el análisis de Clickstream en AWS mediante Citrix ADC
- Citrix ADC en una nube privada administrada por Microsoft Windows Azure Pack y Cisco ACI

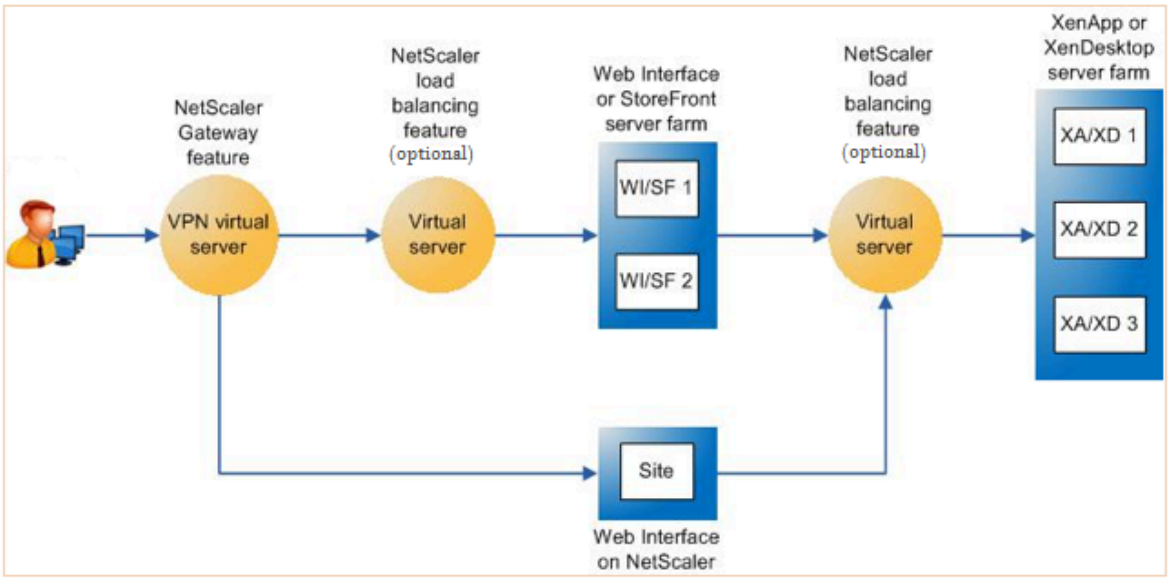
Configuración de Citrix ADC para Citrix Virtual Apps and Desktops

August 20, 2021

Un dispositivo Citrix ADC puede proporcionar acceso remoto seguro y equilibrado de carga a sus aplicaciones Citrix Virtual Apps and Desktops. Puede utilizar la función de equilibrio de carga de Citrix ADC para distribuir el tráfico en el servidor Citrix Virtual Apps and Desktops. Puede utilizar la función Citrix Gateway para proporcionar acceso remoto seguro a los servidores.

Citrix ADC también puede acelerar y optimizar el flujo de tráfico y ofrecer funciones de visibilidad útiles para implementaciones de Citrix Virtual Apps and Desktops.

Ilustración 1. Dispositivo Citrix ADC en la configuración de Citrix Virtual Apps and Desktops



La ilustración anterior muestra los componentes involucrados en esta implementación:

- **NetScaler Gateway.** Proporciona la dirección URL para el acceso de los usuarios y proporciona seguridad mediante la autenticación de los usuarios.
- **Servidor virtual de equilibrio de carga de Citrix ADC.** La carga equilibra el tráfico de los servidores de la Interfaz Web o StoreFront. También puede implementar un servidor virtual de equilibrio de carga frente a los servidores Citrix Virtual Apps y Desktop para equilibrar la carga de componentes clave, como XML Broker y el servidor de Desktop Delivery Controller (DDC).
- **Interfaz Web o StoreFront o Interfaz Web en Citrix ADC.** Proporciona la interfaz a través de la cual puede acceder a las aplicaciones.

  Nota: Interfaz Web en Citrix ADC (WionNS) es una personalización del producto Web Interface, alojado en el dispositivo Citrix ADC.
- **Citrix Virtual Apps and Desktops.** Proporciona las aplicaciones a las que los usuarios desean acceder.

Para configurar Citrix ADC para Citrix Virtual Apps and Desktops mediante la GUI de Citrix ADC

Requisitos previos

- Los servidores Citrix Virtual Apps y Desktop están configurados y disponibles.
- Interfaz Web, StoreFront o Interfaz Web en los servidores Citrix ADC están configurados y disponibles.
- Tiene conocimientos prácticos de Citrix Gateway, Citrix ADC, Citrix Virtual Apps and Desktops StoreFront/Web Interface/Web Interface en Citrix ADC.
- Asegúrese de haber configurado un servidor virtual y un servicio y enlazado el servicio al servidor virtual. Para obtener más información, consulte:
  - Balance de carga XenDesktop
  - Equilibrio de carga XenApp

Procedimiento:

1. Inicie sesión en el dispositivo Citrix ADC y, en la ficha **Configuración**, haga clic en **XenApp y XenDesktop**.
2. En el panel **Detalles**, haga clic en **Introducción**. Si la configuración existe en Citrix ADC, haga clic en el enlace **Modificar** correspondiente a cada una de las secciones que quiera modificar.
3. Seleccione el producto (StoreFront, Interfaz Web o Interfaz Web en Citrix ADC) que en su implementación proporciona la interfaz para acceder a las aplicaciones Citrix Virtual Apps and Desktops.
4. Configure el acceso remoto seguro.
   a) En la sección **Configuración de NetScaler Gateway**, especifique los detalles del servidor virtual VPN y haga clic en **Continuar**.

b) En la sección **Certificado de servidor**, elija un certificado existente o instale un certificado nuevo y haga clic en **Continuar**.

c) En la sección **Autenticación**, configure el mecanismo de autenticación principal que se va a utilizar y especifique los detalles del servidor o utilice un servidor existente y haga clic en **Continuar**.

d) En la sección **StoreFront**, especifique los detalles del servidor que proporciona la interfaz para acceder a las aplicaciones y haga clic en **Continuar**.

e) Puede utilizar una de las siguientes opciones como servidor StoreFront.

   i. Servidor virtual LB que apunta a varios servidores SF.
   ii. Interfaz Web o servidor StoreFront accesible directamente desde el dispositivo Citrix ADC.
   iii. Interfaz Web en Citrix ADC.

5. Haga clic en **Listo** para completar la configuración.

Preferencia de zona alimentada de Equilibrio de carga de servidor global (GSLB)

August 20, 2021

La preferencia de zona con tecnología GSLB es una función que integra Citrix Virtual Apps and Desktops, StoreFront y Citrix ADC para proporcionar a los clientes acceso al centro de datos más optimizado según la ubicación del cliente.

En una implementación distribuida de Citrix Virtual Apps and Desktops, es posible que StoreFront no seleccione un centro de datos óptimo cuando hay varios recursos equivalentes disponibles en varios centros de datos. En tales casos, StoreFront selecciona aleatoriamente un centro de datos. Puede enviar la solicitud a cualquiera de los servidores Citrix Virtual Apps and Desktops de cualquier centro de datos, independientemente de la proximidad al cliente que realiza la solicitud.

La dirección IP del cliente se examina cuando llega una solicitud HTTP al dispositivo Citrix Gateway. La dirección IP del cliente real se utiliza para crear la lista de preferencias del centro de datos que se reenvía a StoreFront. Si el dispositivo Citrix ADC está configurado para insertar el encabezado de preferencia de zona, StoreFront 3.5 o posterior puede utilizar la información proporcionada por el dispositivo para reordenar la lista de controladores de entrega y conectarse a un Controller de entrega óptimo en la misma zona que el cliente. StoreFront selecciona el servidor virtual VPN de puerta de enlace óptimo para la zona del centro de datos seleccionada, agrega esta información al archivo ICA con las direcciones IP adecuadas y la envía al cliente. StoreFront intenta iniciar aplicaciones alojadas

en los controladores de entrega preferidos del centro de datos antes de intentar ponerse en contacto con controladores equivalentes en otros centros de datos.

Para obtener más información sobre la configuración de esta solución, haga clic aquí.

Para ver una descripción de vídeo sobre la solución de preferencias de zona alimentada por GSLB, haga clic en https://www.youtube.com/watch?v=Y8DELum0Xp0.

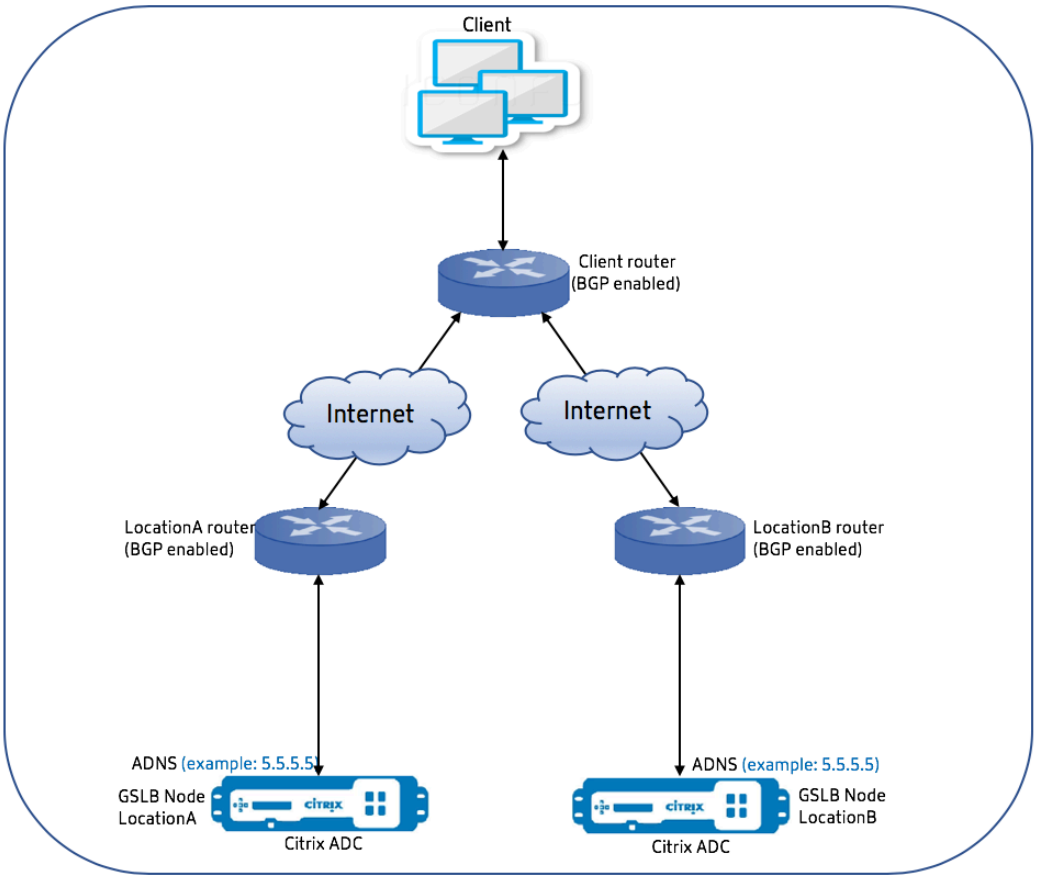
Compatibilidad con Anycast en Citrix ADC

August 20, 2021

Anycast es un tipo de red donde un conjunto de servidores comparte una dirección IP. La solicitud del cliente se dirige al servidor topográficamente más cercano en función de sus tablas de redirección. Esta redirección reduce los problemas de latencia, garantiza una alta disponibilidad y minimiza el tiempo de inactividad.

Citrix ADC admite la red Anycast con funciones de equilibrio de carga global de servidores (GSLB) y DNS.

El siguiente diagrama ilustra un diagrama de topología de Anycast en Citrix ADC.



Anycast GSLB Negro

La función Citrix ADC GSLB proporciona equilibrio de carga entre sitios distribuidos globalmente junto con recuperación ante desastres y garantiza la disponibilidad continua de las aplicaciones.

Durante una interrupción, GSLB proporciona recuperación ante desastres inmediata al enrutar el tráfico al centro de datos más cercano o al mejor rendimiento. Sin embargo, GSLB no puede controlar lo siguiente:

- Cómo se enruta el tráfico DNS a nodos GSLB en diferentes ubicaciones geográficas.
- Cuánta latencia se agrega mientras las consultas DNS se enrutan a los nodos GSLB.

En una configuración típica de GSLB, cada centro de datos tiene un nodo GSLB configurado con el servidor de nombres de dominio autoritativo (ADNS) específico del sitio para recibir consultas DNS. El ADNS de cada sitio está configurado como servidor de nombres en el solucionador DNS. A medida que aumenta el número de nodos GSLB, el número de registros del servidor de nombres también aumenta. En tales casos, si hay una falla de un centro de datos, LDNS tiene que volver a intentar la resolución con un servidor de nombres diferente. Este reintento se agrega a la latencia en la resolución DNS.

Además, cada vez que se agrega un nodo GSLB, se deben actualizar los registros del servidor de nombres.

Para superar estos inconvenientes, puede usar Anycast ADNS. En Anycast ADNS, se utiliza una única dirección IP ADNS para todos los nodos GSLB y el tráfico DNS se enruta a nodos GSLB mediante redirección dinámica.

Por ejemplo, si un sitio GSLB está DESCONECTADO, la tabla de redirección se actualiza y se quita la ruta a este sitio. Como resultado, Las consultas DNS no se envían a los sitios que están ABAJO. Como resultado, no hay reintentos.

Si se agrega un nuevo nodo GSLB, al nuevo nodo se le asigna la misma dirección IP de ADN. El redirección dinámica actualiza automáticamente las tablas de redirección con rutas a nuevos sitios basados en los algoritmos de redirección. Por lo tanto, no es necesario actualizar los registros del servidor de nombres DNS. El implementación de nuevos sitios GSLB se hace más simple y más rápido con Anycast.

Cómo configurar una dirección IP de ADNS en modo Anycast

Habilite la redirección de host en la IP de ADNS en un dispositivo Citrix ADC y establezca el nivel adecuado de inyección de estado de ruta (RHI). Principalmente, no habría ningún servidor virtual en la IP de ADNS y, por lo tanto, el nivel RHI debe seleccionarse como NONE. Al habilitar la ruta del host en la IP de ADNS, se convierte en una ruta del kernel. A continuación, puede habilitar la redirección dinámica de elección y configurar el protocolo de redirección para redistribuir las rutas del núcleo.

Configuración IP de ADNS: Ejemplo

En el símbolo del sistema, escriba;

```
add service adns_public 5.5.5.5 ADNS 53

set ip 5.5.5.5 -hostRoute ENABLED -vserverRHILevel ALL_VSERVERS
<!--NeedCopy-->
```

Configuración de BGP en el sitio GSLB: Ejemplo

```
Site1#sh run
!
hostname Site1
!
log syslog
```



```
log record-priority
!
ns route-install bgp
!
interface lo0
 ip address 127.0.0.1/8
 ipv6 address fe80::1/64
 ipv6 address ::1/128
!
interface vlan0
 ip address 10.102.148.94/25
 ipv6 address fe80::e84c:f4ff:fe74:4588/64
!
interface vlan2
 ip address 172.18.30.15/24
!
router bgp 5
 redistribute kernel -----> redistributing the kernel routes
 neighbor 172.18.30.30 remote-as 4
 neighbor 172.18.30.30 advertisement-interval 1
 neighbor 172.18.30.30 timers 4 16
!
End

Site1#
<!--NeedCopy-->
```

Tabla de redirección de sitios GSLB: Ejemplo

```
Site1#sh ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, I - Intranet
       * - candidate default

K       5.5.5.5/32 via 0.0.0.0 ---------------------------------------->
    Kernel Route for ADNS
C       10.102.148.0/25 is directly connected, vlan0
C       127.0.0.0/8 is directly connected, lo0
B       172.18.10.0/24 [20/0] via 172.18.30.30, vlan2, 01w5d22h
```



```
B       172.18.20.0/24 [20/0] via 172.18.30.30, vlan2, 01w5d22h
C       172.18.30.0/24 is directly connected, vlan2
B       192.168.3.0/24 [20/0] via 172.18.30.30, vlan2, 01w5d22h
B       192.168.5.0/24 [20/0] via 172.18.30.30, vlan2, 01w5d22h
B       192.168.10.0/24 [20/0] via 172.18.30.30, vlan2, 01w5d22h

Gateway of last resort is not set
Site1#
<!--NeedCopy-->
```

DNS Anycast

Puede usar Anycast DNS para servidores virtuales proxy DNS en Citrix ADC. Cuando hay varios servidores de nombres DNS configurados, el solucionador DNS responde en función del método round robin. Por ejemplo, si el solucionador no recibe ninguna respuesta del primer servidor, cambia al segundo servidor después de que caduque el valor de tiempo de espera configurado. El cambio del primer servidor al segundo servidor aumenta la latencia en la resolución DNS. Si los resolvers DNS están configurados con Anycast, entonces esta latencia se puede eliminar.

Configuración DNS: Ejemplo

En el símbolo del sistema, escriba;

```
add lb vserver dns DNS 5.5.5.50 53

set ip 5.5.5.50 -hostRoute ENABLED -vserverRHILevel ALL_VSERVERS
<!--NeedCopy-->
```

Implemente una plataforma de publicidad digital en AWS con Citrix ADC

August 20, 2021

Con la naturaleza cambiante de las plataformas digitales, una amplia gama de aplicaciones publicitarias están disponibles. Por ejemplo, redes sociales, correo directo, vídeos, banners, pops, intersticiales, medios enriquecidos, etc. Los anunciantes están adoptando redes de publicidad de vídeo a un ritmo rápido, lo que representa casi el 40% del tráfico publicitario. Pero con un mayor uso de móviles por parte de los usuarios modernos, la publicación de anuncios de vídeo en la plataforma móvil ha experimentado un aumento considerable.

Las plataformas de publicidad digital se enfrentan a varios desafíos. Algunos de los desafíos son:

- Amenazas
- Altos costes operativos
- Hay una amplia gama de dispositivos disponibles para enviar tráfico a través de Internet. Los diferentes protocolos para la comunicación en tiempo real plantean los siguientes desafíos:
  - WebRTC
  - Transmisión adaptativa
  - UDP para vídeo, donde WebRTC utiliza UDP sobre HTTP

Para hacer frente al comportamiento complejo de las plataformas publicitarias, la solución Citrix ADC, con su conjunto completo de funciones y funciones bien integradas con AWS, proporciona un acceso instantáneo, seguro y fiable al inventario de anuncios digitales, en cualquier lugar y en cualquier momento. Citrix ADC desempeña un papel fundamental en la entrega de SaaS y aplicaciones web para plataformas digitales.

Integración de plataformas de publicidad digital con Citrix ADC

Descripción general de la plataforma de publicidad digital

La plataforma de publicidad digital consta de los siguientes componentes clave:

- Intercambio de anuncios
- Red publicitaria
- Plataforma del lado de la demanda (DSP)
- Plataforma lateral de suministro (SSP)
- Sistemas de licitación en tiempo real (RTB)

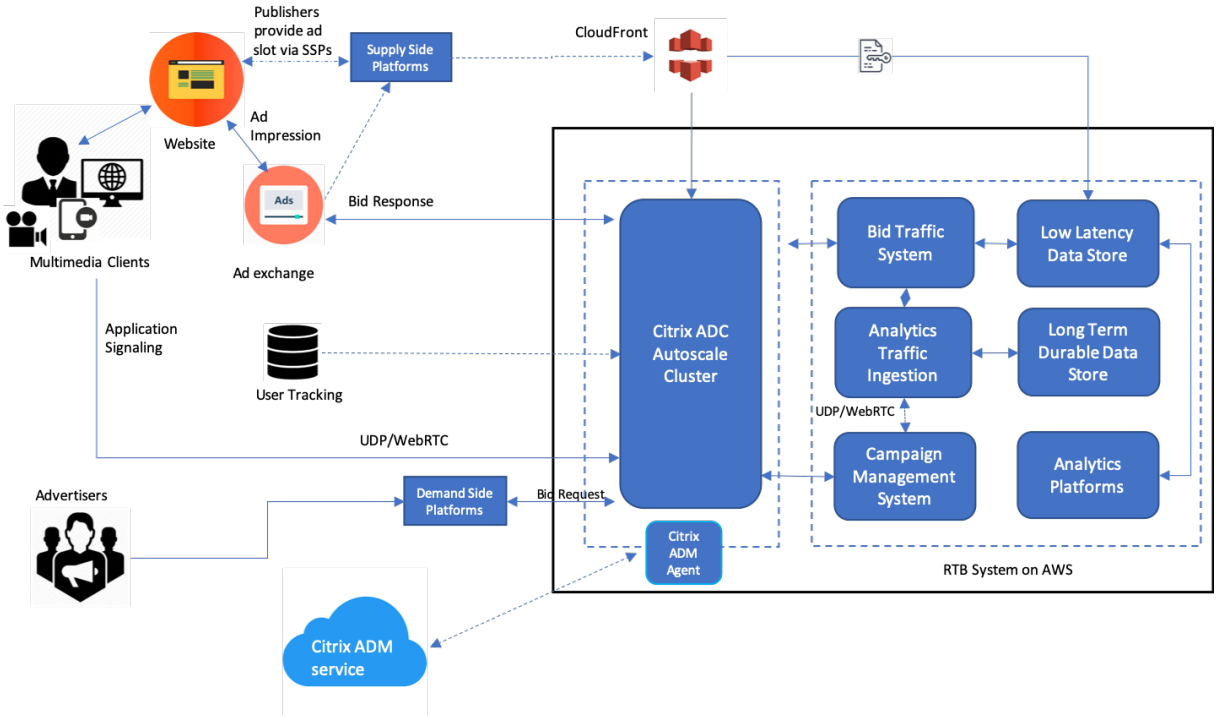
Una visión general del proceso seguido en un sistema publicitario es el siguiente.

- La primera transacción ocurre cuando el usuario visita el sitio web.
- Esto activa una solicitud de puja/anuncio (incluida la información demográfica del usuario) que se envía al servidor de anuncios o al editor que se pone en contacto con un intercambio de anuncios.
- Los editores de anuncios envían la solicitud de anuncio a un intercambio de anuncios a través de SSP.
- El Ad Exchange envía esta solicitud y los datos adjuntos a DSP indicando que hay una solicitud de impresión o anuncio disponible. Por lo tanto, varios anunciantes pueden enviar pujas automáticamente en tiempo real para publicar sus anuncios.
- Mientras tanto, los anunciantes deben configurar sus campañas en DSP. Utilice la información sobre el usuario de Data Management Platform (DMP) para evaluar la cantidad que están dispuestos a pagar por entregar un anuncio al usuario.
- Los DSP envían estas pujas en tiempo real en cada impresión de anuncio porque se envían al intercambio de anuncios.

- Cualquiera que sea el pujador que más puje dentro de un período de tiempo establecido por el Ad Exchange o los SSP, obtiene un espacio publicitario de los editores para publicar sus anuncios. De lo contrario, pierden la oportunidad de obtener el anuncio adecuado para su demográfico clave.

Cómo se integra la plataforma de publicidad digital con Citrix ADC

El siguiente diagrama ilustra cómo los diferentes componentes de la plataforma publicitaria se comunican con Citrix ADC y Citrix Application Delivery Management (ADM) para publicar anuncios en línea.



Cómo contribuye Citrix ADC

En el proceso de publicación de anuncios, la solución Citrix ADC ayuda a gestionar y procesar la afluencia inconsistente del tráfico de pujas. Actúa como punto de entrada para todo el tráfico para garantizar la escalabilidad y la disponibilidad en todas las zonas de disponibilidad. Para satisfacer la naturaleza elástica del tráfico publicitario, se implementa en un grupo de escalado automático frente a aplicaciones web y servidores de bases de datos.

La plataforma publicitaria de AWS con la solución Citrix ADC le permite obtener el rendimiento en tiempo real, la alta escalabilidad y la alta disponibilidad en todo el mundo. Puede comprar y vender anuncios multimedia enriquecidos, vídeo, móviles y nativos en tiempo real. Reduce el coste operativo general y la latencia implicados en la ejecución de una plataforma de publicidad. Es el proxy de mejor rendimiento con las completas capacidades de eliminar correctamente los servidores back-end

durante la escala automática, la multiplexación de conexiones y garantizar que el tráfico del usuario final nunca se vea afectado. Citrix ADC admite el equilibrio de carga de los protocolos HTTP, UDP, WebRTC y RTSP que se utilizan en las plataformas publicitarias.

Citrix ADC encaja de forma coherente en el entorno de AWS con los siguientes atributos clave:

- Cambio de contenido: cambie a la plataforma correcta según el nombre del host.
- Protección de seguridad: utilice la funcionalidad del firewall de aplicaciones web (WAF), la limitación de velocidad (a través de la IP del cliente) y la protección contra ataques DDoS.
- Escalado automático del tráfico front-end y back-end.
- Visibilidad de extremo a extremo y detección de anomalías en todos los dispositivos ADC mediante el uso de ADM.
- Baja latencia.

Cómo contribuye Citrix ADM

Citrix ADC utiliza Citrix ADM para superar los siguientes desafíos a los que se enfrentan las plataformas de publicidad digital:

- Identificar las desviaciones de tendencia respecto al rendimiento esperado
- Análisis del rendimiento de aplicaciones en tiempo real
- Supervisión de la capacidad

Ventajas de la integración de plataformas publicitarias con Citrix ADC y ADM

La solución Citrix ADC ofrece las siguientes capacidades y beneficios a un proveedor de plataformas de publicidad digital.

Bajo coste

- Integrada con el servicio AWS Autoscaling, la instancia de Citrix ADC VPX puede ampliar o reducir sus recursos front-end y back-end automáticamente. Esto proporciona una configuración de cero toque que atiende a la elasticidad de las plataformas publicitarias.
- Consolidación de la entrega de todo tipo de tráfico desde un único punto.

Para obtener más información sobre el escalado automático de AWS, consulte Agregar el servicio back-end de AWS Autoscaling.

Alta disponibilidad

- Si una zona de disponibilidad deja de estar disponible, Citrix ADC aplica su capacidad de tolerancia a fallos para detectar automáticamente los servidores de otra zona de disponibilidad, sin interrupción del tráfico.

- Además, finaliza con gracia los servidores evitando la pérdida de conexiones de cliente.

Para obtener más información, consulte Cómo funciona la alta disponibilidad en AWS.

Análisis del rendimiento de las aplicaciones

El análisis inteligente de Citrix ADM y el análisis del rendimiento de las aplicaciones garantizan:

- Obtenga visibilidad de los problemas (anomalías de respuesta del servidor, errores 5XX, etc.) que afectan a la experiencia del usuario final.
- Alerta al administrador para que tome medidas correctivas inmediatamente.

Para obtener más información, consulte Indicadores de rendimiento para análisis de aplicaciones.

Seguridad de firewall enriquecida

La mayoría de las vulnerabilidades de seguridad comunes se producen en aplicaciones web y no en redes. Es vital proteger sus aplicaciones web contra accesos no autorizados, como bots, robos de datos y ataques de capas de aplicaciones.

Citrix ADC proporciona seguridad integral e integrada de nivel 4 a nivel 7 que incluye:

- Web App Firewall (WAF) para proteger sus aplicaciones web, identificar y mitigar los robots maliciosos con firmas de bot actualizadas periódicamente y detección basada en el comportamiento.
- Limitación de tarifas para evitar que una plataforma publicitaria se abrume.

Para obtener más información, consulte Citrix Web App Firewall.

Seleccione el tipo de instancia de AWS adecuado para la plataforma publicitaria

Elija el tipo de instancia de AWS adecuado para ADC en función de los dos factores siguientes:

- Número de usuarios que acceden simultáneamente a la plataforma publicitaria.
- Número medio de usuarios en la plataforma.

Citrix ADC se puede implementar en varias instancias EC2, que incluyen c5, c5n, m5, etc. Para plataformas publicitarias, utilice los siguientes tipos de instancias de AWS:

- c5 o c5n es apropiado para manejar el tráfico pesado SSL.
- c5.large puede manejar hasta 1000 SSL TPS.

Para obtener más información, consulte Matriz de soporte de VPX-AWS.

Mejora de la analítica de flujo de clics en AWS mediante Citrix ADC

October 5, 2021

Los clientes acceden cada vez más a los productos de la empresa a través de diversas aplicaciones, como aplicaciones móviles, aplicaciones SaaS, etc. Por lo tanto, las aplicaciones pueden convertirse en una mina terrestre de los datos de experiencia del cliente. Para realizar un seguimiento del comportamiento de los clientes en línea, las empresas centradas en el cliente crean perfiles basados en datos para cada uno de sus clientes utilizando estos datos de comportamiento del cliente.

Un flujo de clics es una secuencia o secuencia de eventos que representan acciones del usuario (clics) en un sitio web o una aplicación móvil. Sin embargo, el alcance de la secuencia de clics va más allá de los clics. Incluye búsquedas de productos, impresiones, compras y cualquier evento de este tipo que pueda ser relevante para la empresa. El mero hecho de recopilar y almacenar los datos de la experiencia del cliente no tiene mucho valor. Es necesario distribuir los datos altamente complejos sin problemas a los proveedores adecuados en el momento adecuado. Las empresas pueden obtener valor de los datos y tomar decisiones conscientes rápidamente para mejorar sus estrategias. Por lo tanto, las empresas utilizan cada vez más el análisis de secuencias de clics para obtener información sobre el recorrido de la experiencia del cliente de las aplicaciones.

Este documento le proporciona una buena comprensión de por qué los datos de Clickstream son de suma importancia, cómo se recopilan, almacenan, distribuyen y transforman en análisis útiles y procesables.

Citrix ADC se integra con Citrix ADM y agrega valor a los servicios de AWS como Amazon Kinesis Data Firehose para equipar a las empresas con la mejor solución de análisis de su clase que gira en torno a los flujos de clics de los usuarios.

Esta solución Citrix ADC le ayuda a resolver problemas empresariales complejos de forma eficiente y con extrema sencillez. Citrix ADC y AWS Kinesis ayudan a capturar los problemas del flujo de trabajo mal diseñado. Citrix ADM ayuda a capturar problemas relacionados con el rendimiento de la red y las aplicaciones web mediante la aplicación de filtros pertinentes. La combinación de Citrix ADC con Citrix ADM y AWS Kinesis le ayuda a administrar y analizar la enorme afluencia de datos de secuencias de clics en cada fase. Esta solución es de alta disponibilidad, escalable, robusta y garantiza que la entrega sea continua y segura. Por lo tanto, puede obtener información procesable.

¿Por qué las empresas optan por el análisis Clickstream?

Las empresas optan por la secuencia de clics principalmente para comprender cómo interactúan los usuarios con la aplicación y para obtener información sobre cómo mejorar los objetivos de la aplicación. Clickstream Analytics es un caso de uso de recuperación de información que realiza un

seguimiento del comportamiento del usuario, los hábitos de navegación, etc. El análisis de clickstream le proporciona información sobre:

- En qué enlace hacen clic sus clientes con más frecuencia y en qué momento.
- ¿Dónde estaba el visitante antes de llegar a mi sitio web?
- ¿Cuánto tiempo pasó el visitante en cada página?
- ¿Cuándo y dónde hizo clic el visitante en el botón “atrás” del explorador web?
- ¿Qué artículos agregó (o eliminó) el visitante a su carrito de compras?
- ¿De qué página salió el visitante de mi sitio web?

Servicio de análisis para gestionar los datos de Clickstream mediante Amazon Kinesis

Puede utilizar Amazon Kinesis para realizar análisis de flujos de clics. Amazon kinesis habilita el análisis de secuencias de clics con los siguientes servicios:

- Firehose de datos de Amazon Kinesis
- Análisis de datos de Amazon Kinesis
- Streams de datos de Amazon Kinesis

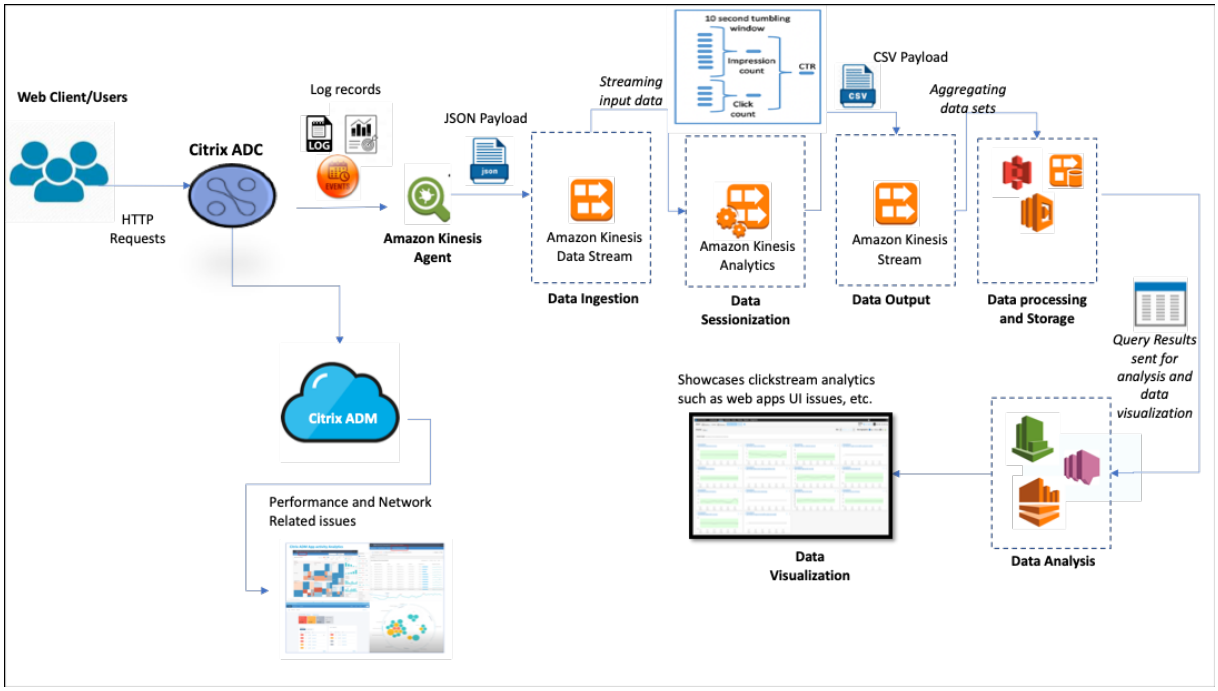
Con Amazon Kinesis, puede recopilar y analizar sus enormes conjuntos de datos a cualquier escala. AWS Kinesis puede gestionar datos de diversas fuentes, tales como:

- Aplicaciones móviles y web (por ejemplo, juegos, comercio electrónico)
- Dispositivos IoT
- Aplicaciones de redes sociales
- Servicios de trading financiero
- Servicios geoespaciales

Cómo habilita Citrix ADC el análisis de secuencias de clics

La solución Citrix ADC recopila y proporciona información de forma segura sobre las actividades de los usuarios, como los sitios web visitados, el ancho de banda utilizado y el flujo de navegación. Las empresas analizan estos datos de flujo de clics continuo y de alto rendimiento para corroborar la eficacia de lo siguiente:

- Diseño del sitio
- Campañas de marketing
- Nuevas funciones de aplicación



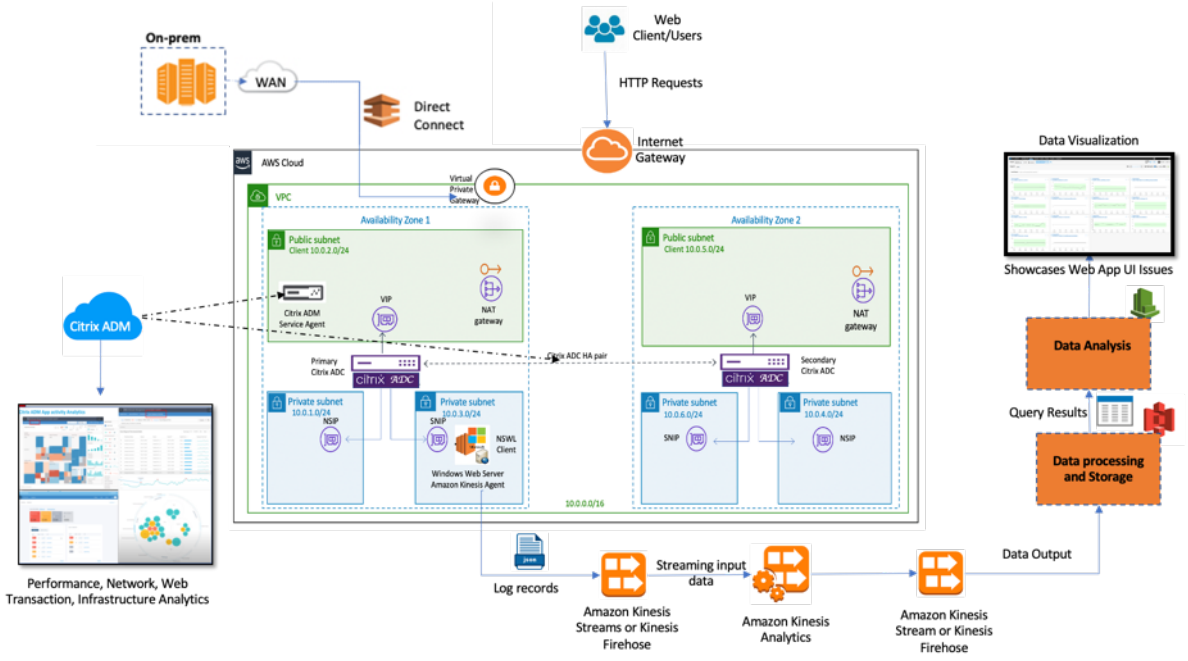
Con la capacidad de Citrix ADC de proporcionar una protección de red resistente para entornos empresariales, el coste del servidor se reduce de forma múltiple al descargar tareas de uso intensivo de cómputo y ejecutar sesiones con estos datos. De este modo, ayuda a las empresas a identificar eventos en tiempo real con alta disponibilidad, seguridad y baja latencia siempre.

Para obtener información sobre la configuración, consulte Configurar la solución Citrix ADC para el análisis de flujo de clics.

Cómo Citrix ADC y Citrix ADM complementan el entorno de AWS

El siguiente diagrama ilustra el flujo de trabajo de usuario de extremo a extremo para realizar análisis de secuencias de clics en la infraestructura de AWS. Este diagrama le ayuda a comprender los siguientes procesos:

- Cómo interactúa el usuario con Citrix ADC
- Cómo captura Citrix ADC las acciones de los usuarios y genera datos de secuencia de clics
- Cómo se entregan los datos de secuencias de clics a los servicios de AWS (Amazon Kinesis)
- Cómo procesa Amazon Kinesis los registros de datos y los almacena para producir análisis de secuencias de clics significativas



Citrix ADC se integra perfectamente en el entorno de AWS y Citrix ADM, lo que ayuda a las empresas a ser compatibles con el volumen variable y la naturaleza diversa de los datos del flujo de clics. Proporciona servicios para cargar y analizar el conocimiento de streaming con sencillez. También puede crear aplicaciones de conocimiento de streaming personalizadas para deseos especializados.

Amazon Kinesis

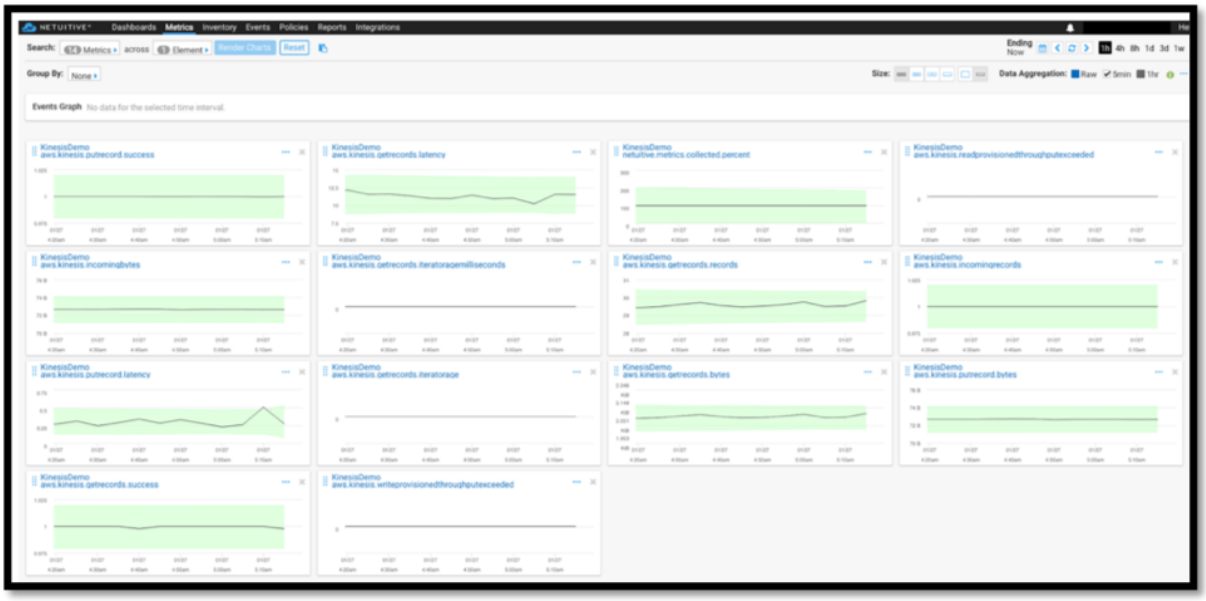
El entorno de AWS cuenta con diferentes servicios que realizan análisis de los eventos de usuario, registros y métricas capturados por Citrix ADC. Los datos pueden ser flujos de clics en sitios web, transacciones financieras, fuentes de redes sociales, registros de TI y eventos de seguimiento de ubicación.

- Amazon Kinesis Data Streams realiza análisis en casos que implican una transmisión de datos en tiempo real escalable y duradera que puede capturar de forma continua GB de datos por segundo de varias fuentes.
- Amazon Kinesis Data Analytics se puede utilizar en casos con menor latencia entre la generación de sesiones porque lleva menos tiempo agregar varios conjuntos de datos.
- Amazon Kinesis Agent para Microsoft Windows recopila, analiza, filtra y transmite los datos de entrada a los flujos de datos de Kinesis.
- Una vez que los datos estén en la nube, puede implementar el procesamiento de datos exacto para obtener los resultados que quiere. Por ejemplo, puede utilizar esta información en Amazon Quick Sight, que es una herramienta de visualización que se utiliza para crear cuadros de mando.

El panel de control de AWS Kinesis proporciona las siguientes ofertas:

- Muestra problemas de interfaz de usuario de aplicaciones web

- Visualizaciones casi en tiempo real de métricas de uso web, como eventos por hora, recuento de visitantes y referencias.
- Análisis de sesión



Análisis de Citrix ADM

Al utilizar Citrix ADM con Citrix ADC, puede obtener una vista única de todos los entornos empresariales. Los registros capturados de Citrix ADC se introducen en Citrix ADM, que trata sus aplicaciones individuales como una sola entidad. Puede obtener información valiosa y solucionar problemas de forma eficaz con las siguientes capacidades de ADM:

- Análisis inteligente
- Análisis de transacciones web
- Detección de anomalías
- Problemas relacionados con el rendimiento y la red

El siguiente panel de servicios de ADM le ayuda a obtener información valiosa para solucionar los problemas de forma eficaz.

Cómo se correlaciona Citrix ADM con los análisis de Clickstream

Los datos de análisis de secuencias de clics se pueden correlacionar con el análisis de ADM para describir, predecir y mejorar el rendimiento de la aplicación.

Para obtener más información sobre Citrix ADM, consulte Citrix ADM

Por ejemplo, una organización al analizar sus registros observa que la mayoría de los usuarios están abandonando sus sitios. Pero para encontrar la causa raíz de este comportamiento de usuario, necesitan averiguar qué parte de su aplicación funciona mal. Con los datos de análisis de secuencias de clics y el análisis de ADM, puede obtener la siguiente información para analizar el motivo por el que los usuarios abandonan un sitio:

- ¿Está abandonando el usuario debido a la latencia, errores 5xx?
- ¿Hay algún error de apretón de manos SSL?
- ¿Hay alguna parte de la aplicación que tenga problemas de rendimiento o de red?
- ¿Hay un error 404 o el tiempo de carga de la página tarda una eternidad en responder, y así sucesivamente?
- ¿Los clientes se enfrentan a anomalías en la respuesta del servidor?

El servicio Citrix ADM proporciona Web Insights que permite a los administradores de TI acelerar la resolución de problemas con las siguientes funciones:

- Proporciona supervisión integrada y en tiempo real de todas las aplicaciones web que proporciona Citrix ADC.
- Obtenga una visión holística del rendimiento de la aplicación, el tiempo de trabajo, la latencia y el comportamiento habitual del usuario mediante herramientas de observabilidad (como el gráfico de servicio global).
- Realice análisis inteligentes para comprender las anomalías en la respuesta del servidor.
- La información sobre SSL contribuye a resolver los errores 5xx y 4xx.
- Para mantener registros de todas las sesiones web que incluyen:
  - Registros detallados de cada transacción web
  - Capacidad de búsqueda para encontrar registros relevantes
  - Capacidad para aislar a un usuario final de ADC frente a Problema ADC-to-server

Tipos de datos exportados por ADC para análisis Clickstream

Citrix ADC captura las distintas fuentes que generan diversas formas de datos, que son las siguientes:

- Registros del servidor web

  La función de registro del servidor web envía registros de solicitudes HTTP y HTTPS a un sistema cliente para su almacenamiento y recuperación. Estos registros contienen una gran cantidad de datos, lo cual es difícil de comprender y le da sentido. Las herramientas analíticas ayudan a comprenderlas y aportarles valor. Para obtener información detallada sobre la configuración, consulte la **sección Configuración del registro web** de este documento.

- Syslogs

  El uso principal de los syslogs es para la administración de sistemas. La supervisión proactiva de syslog da sus frutos porque reduce significativamente el tiempo de inactividad de los servidores y otros dispositivos de su infraestructura. Syslog identifica los problemas críticos de la red y los informa de forma proactiva.

- Registros de acceso

  Los registros de acceso almacenan información sobre los sucesos ocurridos en el servidor web. Por ejemplo, cuando alguien visita su sitio web, se registra y almacena un registro para proporcionar al administrador del servidor web información como la dirección IP del visitante, las páginas que estaba viendo, los códigos de estado y el explorador utilizado. Acceder a los registros puede resultar abrumador, si no hay conocimientos adecuados para entenderlos.
  Puede programar su sistema para que se integre con:

  - Citrix ADC para una entrega perfecta
  - Kinesis para obtener información procesable que resulta útil para las empresas

- Registros de auditoría

La función Registro de auditoría permite registrar los estados y la información de estado de Citrix ADC recopilada por varios módulos del kernel y en los daemons de nivel de usuario.

- Registros de errores

  El archivo de registros de errores ayuda a los administradores a proporcionar más información sobre un error específico que se ha producido en el servidor web.

Configurar la solución Citrix ADC para el análisis de secuencias de clics

La función de registro del servidor web le permite enviar registros de solicitudes HTTP y HTTPS a un sistema cliente para su almacenamiento y recuperación.

Para configurar Citrix ADC para el registro del servidor web, debe:

- Habilitar función de registro web
- Configure el tamaño del búfer para almacenar temporalmente las entradas de registro porque el servidor de registros web se ejecuta en Citrix ADC.

Para configurar el registro del servidor web mediante CLI:

1. Habilite la función de registro del servidor web.

```
enable ns feature WL
<!--NeedCopy-->
```

2. [Opcional] Modificar/configurar el tamaño del búfer para almacenar la información registrada.

```
set ns weblogparam -bufferSizeMB 60
<!--NeedCopy-->
```

3. Instale el cliente de registro web (NSWL) de Citrix ADC. Para obtener más información, consulte Instalación del cliente de registro web (NSWL) de Citrix ADC
4. Instale el cliente NSWL en Windows realizando las siguientes operaciones en el sistema donde descargó el paquete.
   a) Extraiga y< release number >< build number > copie el archivo nswl_win–.zip del paquete en un sistema Windows en el que quiera instalar el cliente NSWL.
   b) En el sistema Windows, descomprima el archivo en un directorio (denominado < NSWL-HOME>). Se extraen bin, samples y otros directorios.
   c) En el símbolo del sistema, ejecute el siguiente comando desde el < NSWL-HOME > directorio\ bin:


```
nswl -install -f < path of the log.conf file >\log.conf
<!--NeedCopy-->
```

> **Nota:**
>
> Para desinstalar el cliente NSWL, en el símbolo del sistema, ejecute el siguiente comando desde el < NSWL-HOME > directorio\ bin:

```
nswl -remove
<!--NeedCopy-->
```

5. Después de instalar el cliente NSWL, configure el cliente NSWL mediante el ejecutable NSWL. Estas configuraciones se almacenan en el archivo de configuración del cliente NSWL (log.conf).

   Ejecute los siguientes comandos desde el directorio en el que se encuentra el ejecutable de NSWL:

```
\ns\bin
<!--NeedCopy-->
```

6. En el archivo de configuración del cliente NSWL (log.conf), agregue la dirección IP de Citrix ADC (NSIP) desde la que el cliente NSWL recopila los registros ejecutando lo siguiente en el símbolo del sistema del cliente:

```
nswl -addns -f < Path to the configuration(log.conf) file >\log.
    conf
<!--NeedCopy-->
```

7. Introduzca el NSIP (dirección IP) del dispositivo Citrix ADC, el nombre de usuario `nsroot` y la contraseña como “el ID de instancia/la contraseña establecida” para que:

   - El cliente NSWL se conecta al ADC después de agregar la dirección IP de NetScaler (NSIP) al archivo de configuración de NSWL
   - ADC almacena en búfer las entradas del registro de solicitudes HTTP y HTTPS antes de enviarlas al cliente.
   - El cliente puede filtrar las entradas (modificando el archivo log.conf) antes de almacenarlas.

> Nota
>
> Cambie la contraseña predeterminada de Citrix ADC y, a continuación, continúe con la configuración. Escriba el siguiente comando para cambiar la contraseña:

```
set system user nsroot -password <your password>
<!--NeedCopy-->
```

Configuración del agente de Amazon Kinesis

Realice los siguientes pasos en la consola web de AWS para configurar el agente de Amazon Kinesis:

1. Cree un archivo de configuración (appsettings.json) e impleméntelo. Los archivos de configuración definen conjuntos de fuentes, sumideros y tuberías que conectan fuentes con sumideros, junto con transformaciones opcionales.

   El siguiente ejemplo es un archivo de `appsettings.json` configuración completo que configura Kinesis Agent para transmitir los sucesos del registro de aplicaciones de Windows a Kinesis Data Firehose.

```
{

"Sources": [
    {

        "Id": "NSWLog",
        "SourceType": "DirectorySource",
        "Directory": "C:\Users\Administrator\Downloads\nswl_win
           -13.0-52.24\bin",
        "FileNameFilter": "*.log"
        "RecordParser": "TimeStamp",
        "TimestampFormat": "yyyy-MM-dddd HH:mm:ss.ffff", //
           Optional parameter required only by the timestamp
           record parser
        "TimeZoneKind": "UTC", //Local or UTC
        "SkipLines": 0 //Skip a number of lines at the beginning
           of each file
     }

    ],
"Sinks": [
    {
```



```
19
20          "Id": "ApplicationLogKinesisFirehoseSink",
21          "SinkType": "KinesisFirehose",
22          "StreamName": "Delivery-ik-logs",
23          "AccessKey": "Your Access Key",
24          "SecretKey": "YourSecretKey",
25          "Region": "ap-south-1"
26       }
27
28      ],
29  "Pipes": [
30      {
31
32      "Id": "ApplicationLogSourceToApplicationLogKinesisFirehoseSink
            ",
33      "SourceRef": "ApplicationLogSource",
34      "SinkRef": "ApplicationLogKinesisFirehoseSink"
35       }
36
37      ],
38  "Telemetrics":
39      {
40
41      "off": "true"
42       }
43
44   }
45
46  <!--NeedCopy-->
```

2. Configure un agente de Kinesis en las fuentes de datos para recopilar datos y enviarlos continuamente a Amazon Kinesis Firehose/Kinesis Data Analytics. Para obtener más información, consulte Introducción a Amazon Kinesis Agent para Microsoft Windows.
3. Cree un flujo de entrega de datos de extremo a extremo con Amazon Kinesis Firehose. El flujo de entrega transmite sus datos desde el agente al destino. El destino incluye Amazon Kinesis Analytics, Amazon Redshift, el servicio Amazon Elasticsearch y Amazon S3. Para el origen, elija **PUT directo u otras fuentes** para crear un flujo de entrega de Kinesis Data Firehose.
4. Procese los datos de registro entrantes mediante consultas SQL de Amazon Kinesis Analytics.
5. Cargue los datos procesados de Kinesis Analytics en Amazon Elasticsearch Service para indexar los datos.
6. Analice y visualice los datos procesados mediante herramientas de visualización, como Kibana y AWS QuickInsight Services.

Referencias

- Ver y exportar mensajes de syslog
- Citrix Networking para multinube híbrida
- Escritura en AWK Kinesis Data Streams con Kinesis Agent

Citrix ADC en una nube privada administrada por Microsoft Windows Azure Pack y Cisco ACI

August 20, 2021

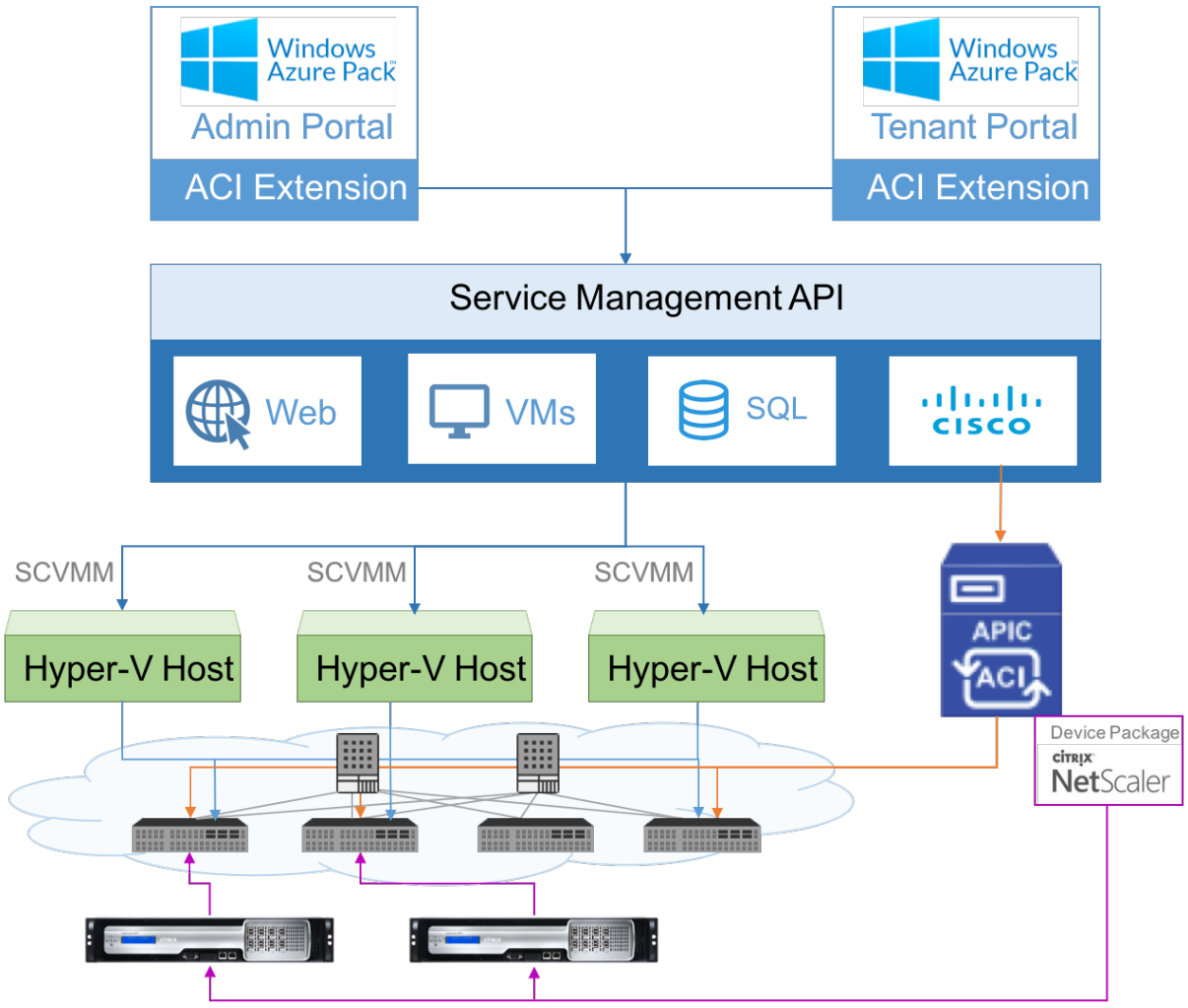
Puede utilizar un dispositivo Citrix ADC para equilibrar la carga en una nube privada administrada a través de Microsoft Windows Azure Pack. La red para la nube privada se automatiza mediante Cisco ACI y Citrix ADC.

Esta solución implica muchos puntos de integración, como Windows Azure Pack (WAP) a Cisco APIC, Cisco APIC a System Center Virtual Machine Manager (SCVMM) y Cisco APIC a Citrix ADC. Como arrendatario en la nube privada, puede habilitar NAT, aprovisionar servicios de red y agregar un equilibrador de carga.

WAP admite portales de arrendatarios y administradores donde un administrador puede realizar tareas administrativas como registro ACI, rango VIP, asociación de dispositivos Citrix ADC con nube de máquina virtual, creación de cuentas de usuario de arrendatarios. Los arrendatarios pueden iniciar sesión en el portal de arrendatarios WAP y configurar la red, los dominios de puente y la redirección y reenvío virtuales (VRF), y utilizar las funciones de equilibrio de carga de Citrix ADC y RNAT.

> **Importante**
>
> - En esta solución, el dispositivo Citrix ADC solo proporciona equilibrio de carga básico.
> - Los arrendatarios pueden implementar varias direcciones VIP con diferentes puertos para la misma red, pero deben asegurarse de que la combinación IP y puertos sea única.
> - El paquete de dispositivos Citrix ADC solo admite la implementación de contexto único. Cada arrendatario obtiene una instancia de Citrix ADC dedicada.
> - WAP admite dispositivos Citrix ADC MPX y dispositivos virtuales Citrix ADC VPX, incluidas las instancias Citrix ADC VPX implementadas en la plataforma Citrix ADC SDX.

La siguiente ilustración proporciona una descripción general de la solución:



Requisitos previos

Asegúrese de que:

- Tiene conocimientos conceptuales sobre los componentes ACI de Cisco y los ADC de Citrix.
  - Para obtener más información acerca de Cisco ACI y sus componentes, consulte la documentación del producto en: http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html.
  - Para obtener más información acerca de los ADC de Citrix, consulte la documentación del producto Citrix ADC en http://docs.citrix.com/.
- Todos los componentes requeridos de Cisco ACI, incluido Cisco APIC en el centro de datos, están configurados y configurados. Para obtener más información acerca de Cisco ACI y sus componentes, consulte la documentación del producto en: http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html.

- Sabe cómo integrar Cisco ACI con Microsoft Windows Azure Pack. Consulte la documentación del producto en: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/2-x/virtualization/b_ACI_Virtualization_Guide_2_2_1.html.
- Tiene conocimientos conceptuales de Microsoft Windows Azure Pack. Consulte la documentación del producto en: https://www.microsoft.com/en-in/cloud-platform/windows-azure-pack.
- Ha instalado el software Citrix ADC versión 11.1 o posterior.
- Los ADC de Citrix se configuran en Cisco ACI, de modo que se puedan administrar mediante Cisco APIC.
- Desde Cisco APIC, asegúrese de que:
  - Se establece la conectividad de administración de Cisco APIC a Citrix ADC.
  - Puede cargar el paquete del dispositivo Citrix ADC versión *11.1—52.3* y registrar el dispositivo Citrix ADC en Cisco ACI mediante Cisco APIC.
  - Configure el dispositivo Citrix ADC en el arrendatario común de Cisco APIC y asegúrese de que no haya fallas en Cisco APIC.
  - Ha configurado todas las configuraciones específicas de APIC como, grupo de VLAN, L3outServiceSdom, L3extout, grupo de recursos. Para obtener más información, consulte la *documentación de Cisco*.

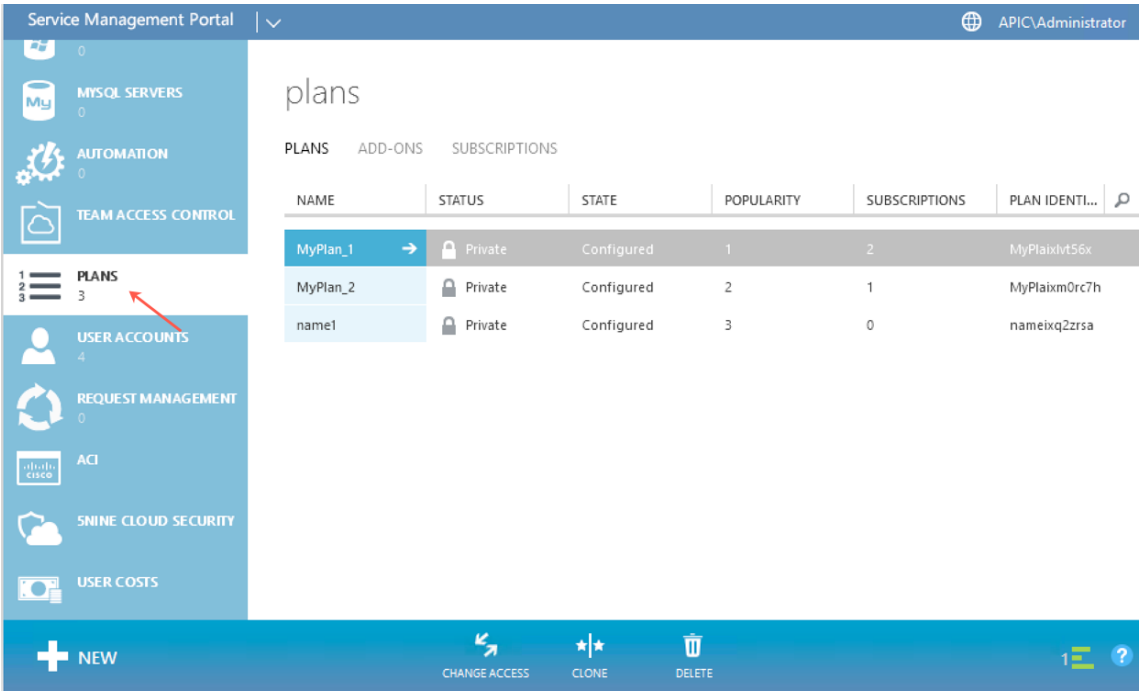
Creación de un equilibrador de carga de Citrix ADC en un plan en Service Management Portal (Portal de administración)

January 12, 2021

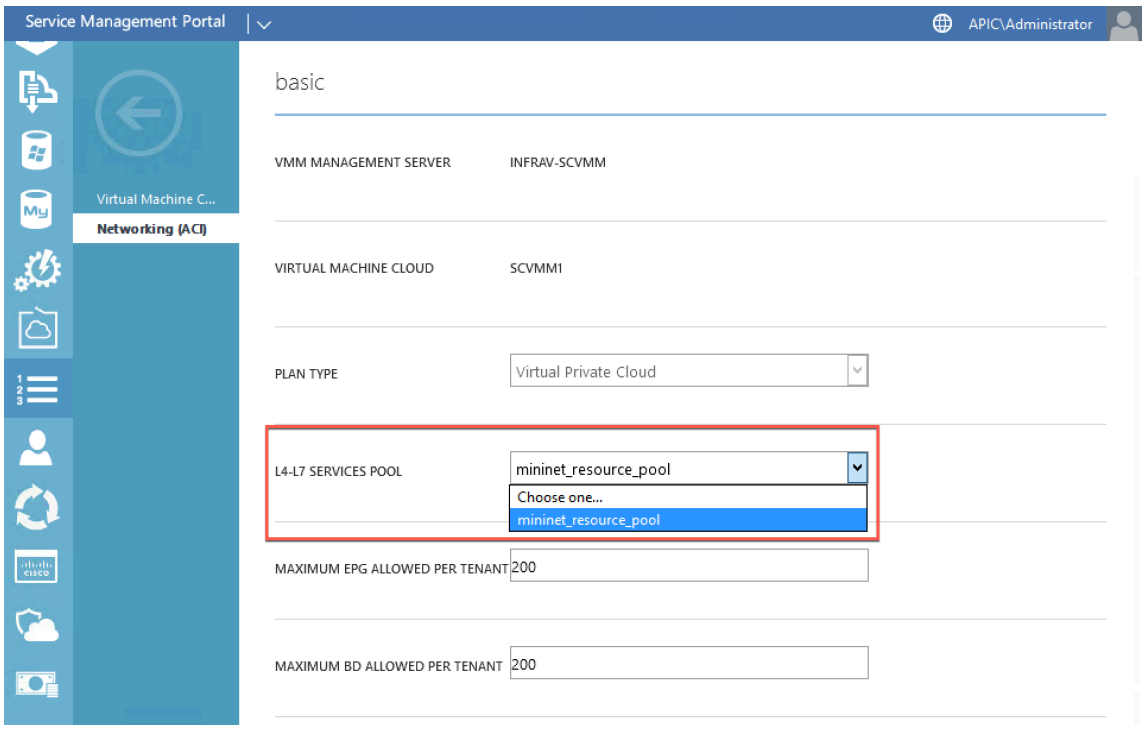
El Portal de administración de servicios en WAP permite a un administrador registrar Cisco APIC con WAP y también crear un plan de alojamiento. Como parte del plan, puede especificar el rango VIP, asociar el equilibrador de carga de Citrix ADC con el plan y crear cuentas de usuario de arrendatarios.

Para crear un equilibrador de carga de Citrix ADC en un plan en el Portal de administración:

1. Inicie sesión en el Portal de administración de servicios (Portal de administración).
2. En el panel de navegación, seleccione **PLANES**.



3. En el panel de planes, seleccione el plan que quiere agregar un equilibrador de carga.
4. En el panel del plan seleccionado, seleccione **Redes (ACI)**.
5. En el panel **Redes (ACI)**, en la lista desplegable **L4-L7 SERVICE POOL**, seleccione el grupo de recursos L4-L7 que había creado en Cisco APIC.



6. Cree una cuenta de usuario de arrendatario y asocie el usuario con el plan que ha creado.

Configuración de un equilibrador de carga de Citrix ADC mediante el Portal de administración de servicios (portal de arrendatarios)

August 20, 2021

En WAP, una vez que el arrendatario crea el dominio de puente (BD), el VRF y una red, el arrendatario puede configurar un equilibrador de carga de Citrix ADC a través del Portal de administración de servicios (portal de arrendatarios).

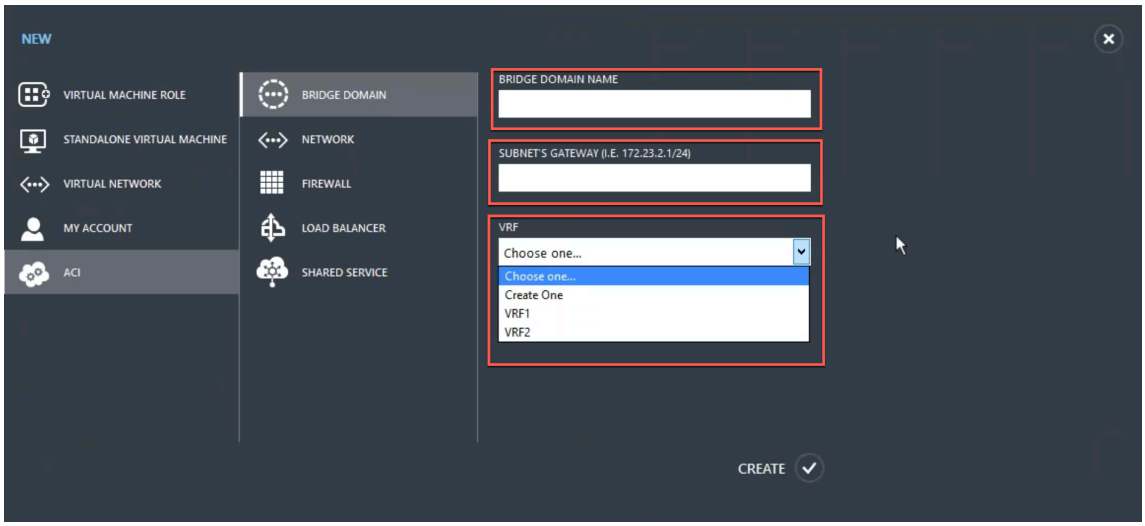
Para configurar el equilibrador de carga de Citrix ADC en el Portal de administración de servicios (portal de arrendatarios)

1. Inicie sesión en el Portal de administración de servicios (portal de arrendatarios).
2. Cree un dominio de puente y VRF, de la siguiente manera:

   a. En el panel de navegación, seleccione **ACI**.

   b. Haga clic en **NUEVO**.

   c. En el panel **NUEVO**, seleccione **BRIDGE DOMAIN**.



   d. En el campo **BRIDGE DOMAIN**, introduzca el nombre de dominio del puente (por ejemplo, BD01).

   e. (Opcional) En el campo **GATEWAY** DE SUBNET, introduzca la Gateway de la subred (por ejemplo, 192.168.1.1/24).

   f. En el campo **VRF**, seleccione un VRF que ya forme parte de la suscripción o seleccione **Crear uno** para crear un VRF.

   g. Haga clic en **CREATE**.

3. Cree una red y asociarla con el dominio de puente que creó. Haga lo siguiente:

a. En el panel de navegación, seleccione **ACI**.

b. Haga clic en **NUEVO**.

c. En el panel **NUEVO**, seleccione **RED**.

d. En el campo **NOMBRE DE LA RED**, introduzca el nombre de la red (por ejemplo, S01).

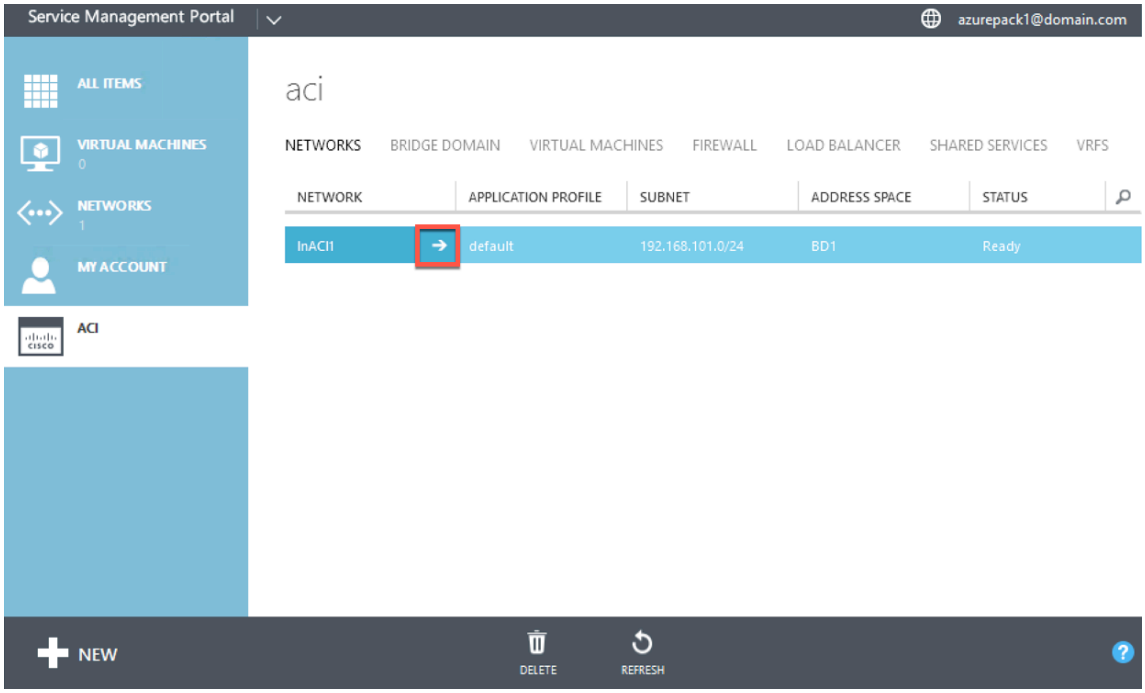
e. En la lista desplegable **BRIDGE DOMAIN**, seleccione el dominio de puente que ha creado. (por ejemplo, BD01).

f. En el campo **GATEWAY** de la subred, introduzca la dirección de la Gateway de la subred (por ejemplo, 172.23.2.1/24).

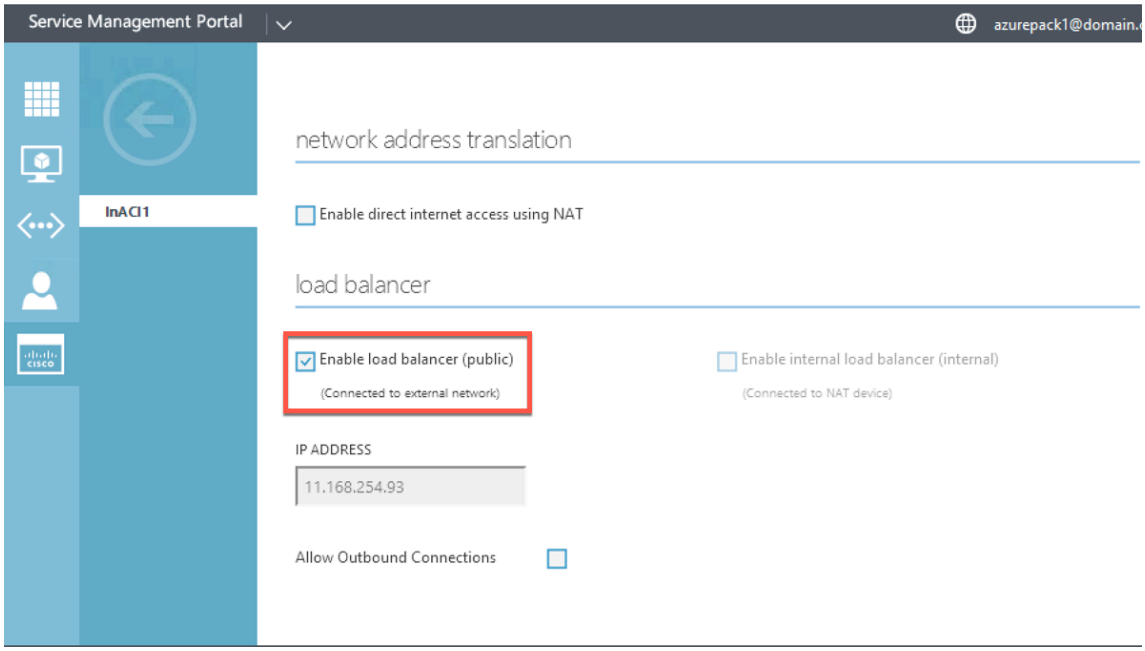
g. (Opcional) En el campo **DNS SERVER IP/IPS**, introduzca los detalles del servidor DNS.

h. Haga clic en **CREATE**.

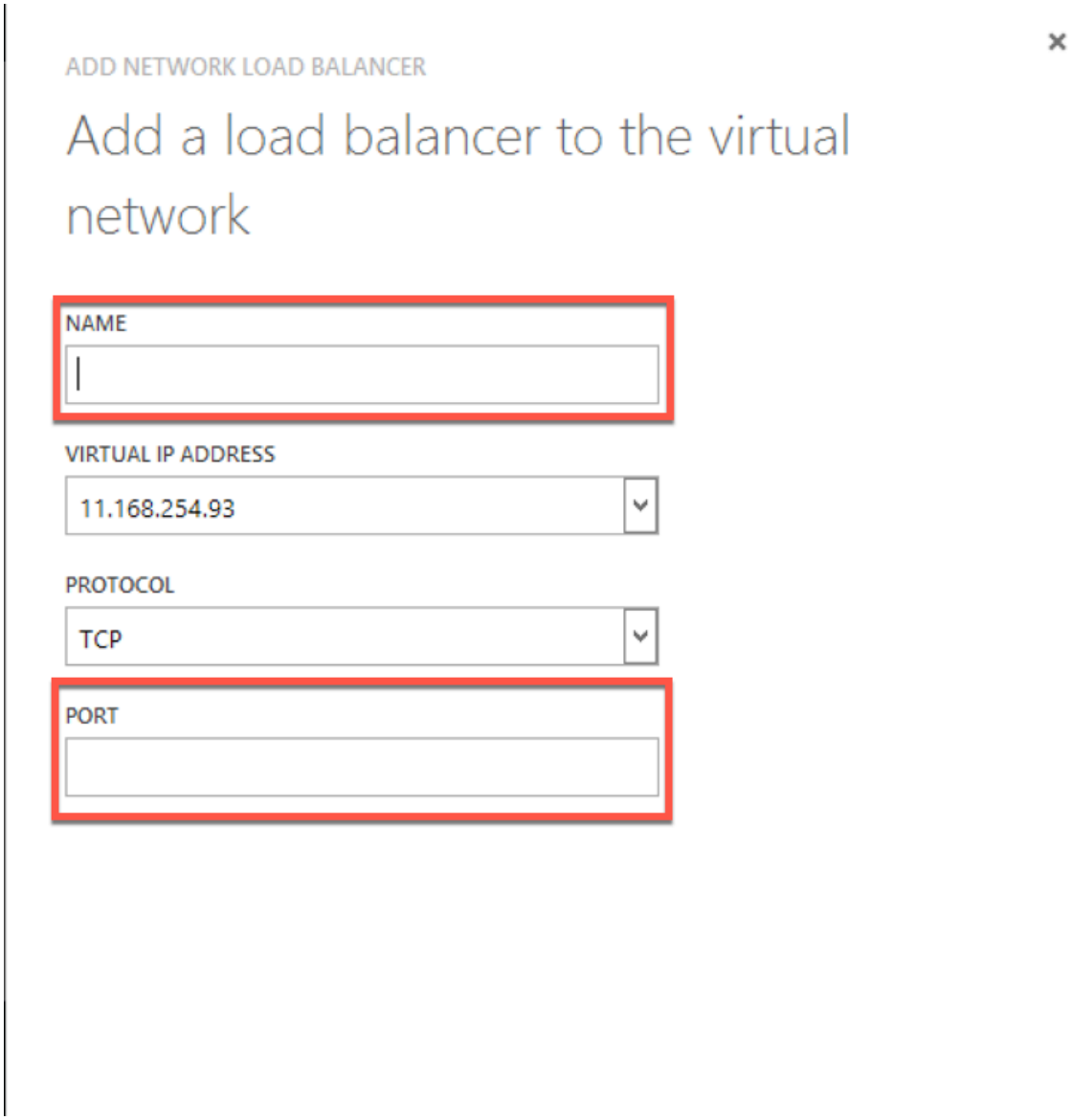
4. En el panel **ACI**, seleccione **NETDES**.



5. Haga doble clic en la red que ha creado. A continuación, en el panel de red, seleccione **Habilitar equilibrador de carga (público)**. En el campo **Dirección IP**, se asigna automáticamente un VIP desde el rango VIP que el administrador configuró en el Portal de administración. Para obtener más información, consulte Creación de un balanceador de carga de Citrix ADC en un plan en el portal de administración de servicios (Admin Portal).
6. Haga doble clic en la red que ha creado. A continuación, en el panel de red, seleccione **Habilitar equilibrador de carga (público)**. En el campo **Dirección IP**, se asigna automáticamente un VIP desde el rango VIP que el administrador configuró en el Portal de administración. Para obtener más información, consulte Creación de un balanceador de carga de Citrix ADC en un plan en el portal de administración de servicios (Admin Portal).



7. En el panel de red, seleccione la ficha **Equilibradores de carga** y haga clic en **ADD**.



8. En el panel **ADD NETWORK LOAD BALANCER**, haga lo siguiente:

   a. En el campo **NAME**, introduzca el nombre del equilibrador de carga.

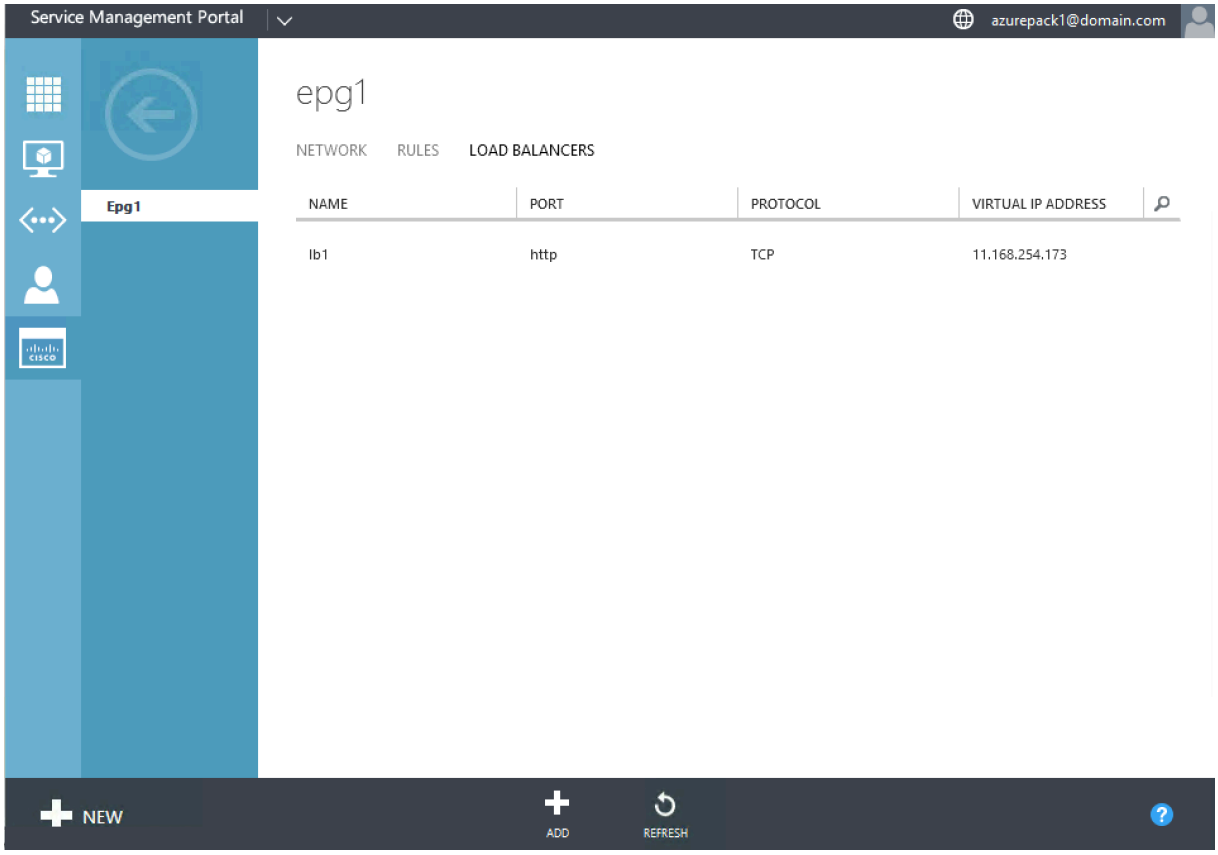
   b. Opcionalmente, en el campo **DIRECCIÓN IP VIRTUAL**, asigne al equilibrador de carga una dirección VIP del rango VIP definido anteriormente.

   c. Si lo quiere, en el campo **PROTOCOLO**, seleccione **TCP**.

   d. En el campo **PORT**, introduzca el número de puerto.

9. Haga clic en **CREATE**.

   El equilibrador de carga de Citrix ADC se muestra en la ficha **LOAD BALANCERS** y el equilibrador de carga de Citrix ADC está listo para la ruta de datos.



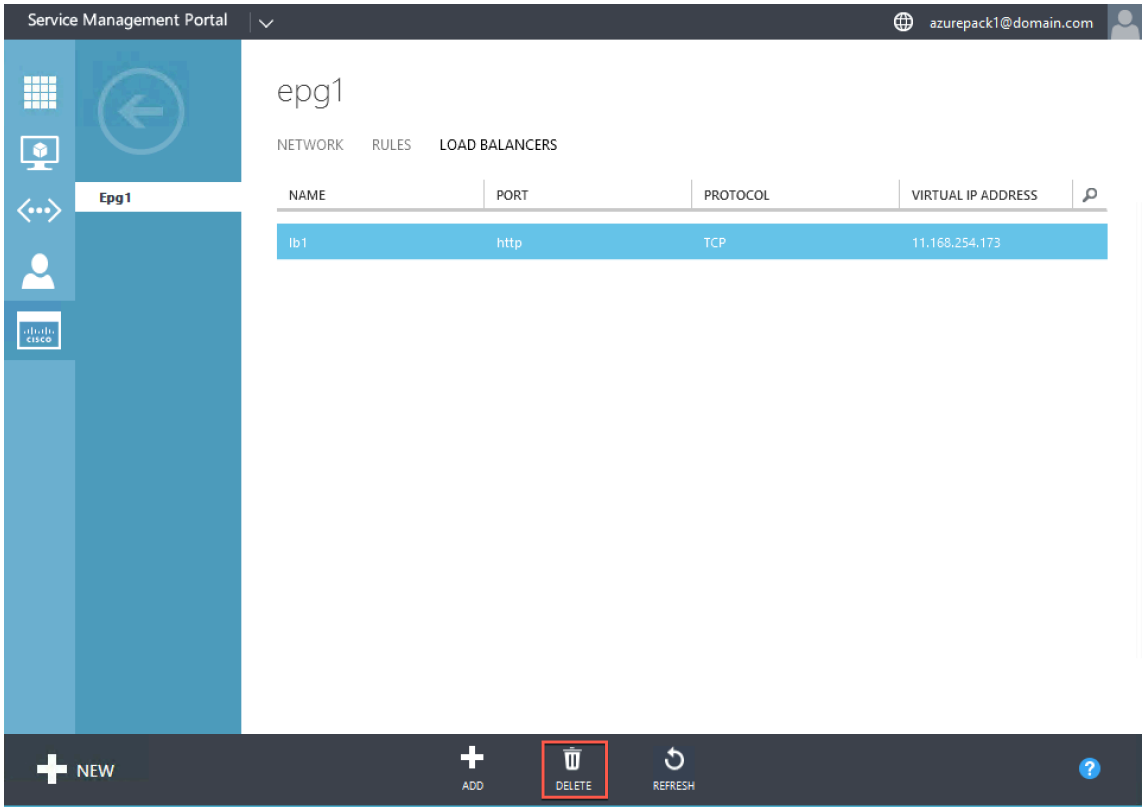
Eliminación de un equilibrador de carga de Citrix ADC de la red

January 12, 2021

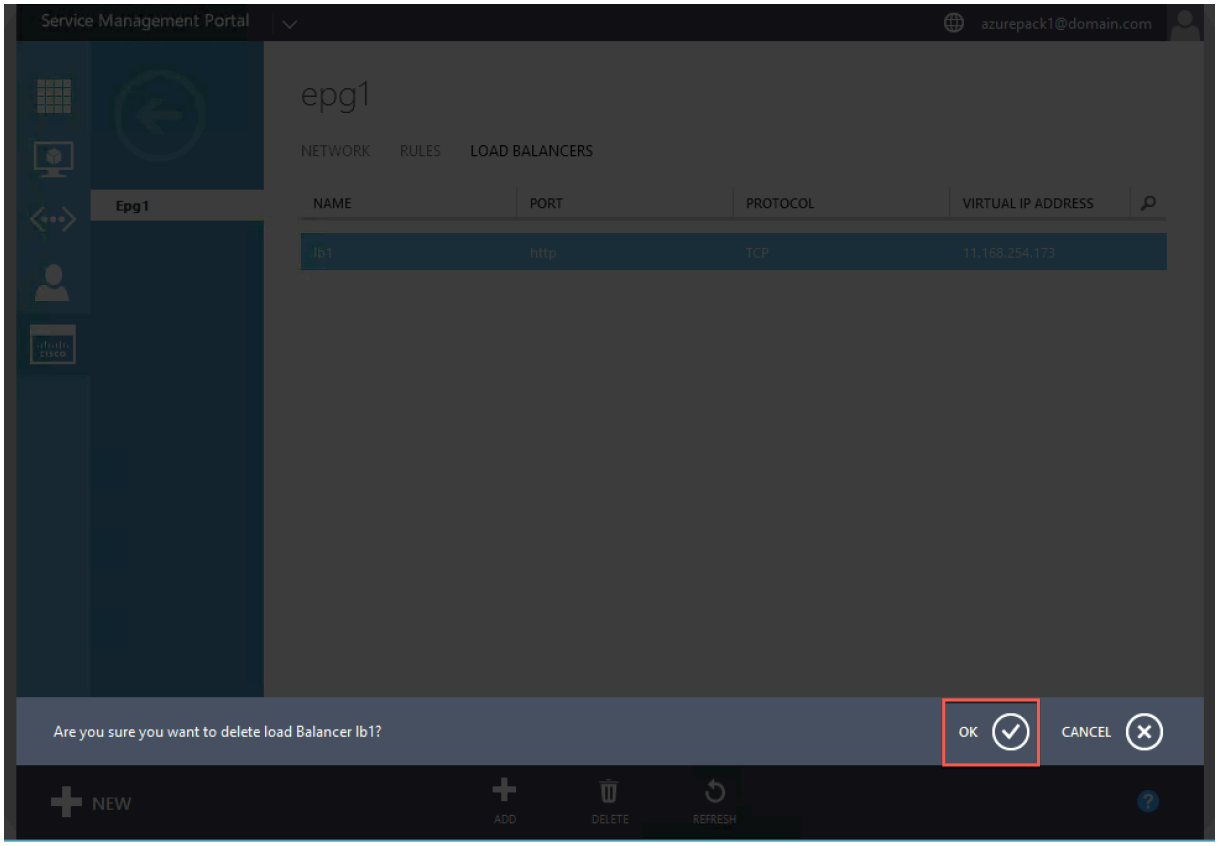
Mediante el Portal de administración de servicios (portal de arrendatarios), desde la red, puede eliminar el equilibrador de carga de Citrix ADC que creó.

Para eliminar un equilibrador de carga de Citrix ADC de la red:

1. Inicie sesión en el Portal de administración de servicios (portal de arrendatarios).
2. En el panel de navegación, seleccione **ACI**.
3. En el panel **ACI**, en la ficha **REDES**, haga clic en la red que creó.
4. En el panel de la red seleccionada, seleccione el equilibrador de carga de Citrix ADC y haga clic en **SUPR**.



5. Haga clic en **Aceptar** para eliminar el equilibrador de carga de Citrix ADC.



Solución nativa de Citrix Cloud para microservicios basada en Kubernetes

August 20, 2021

A medida que las empresas se transforman para innovar más rápido y acercarse a los clientes, están rediseñando su proceso interno y rompiendo los límites dentro de su organización. Están eliminando los silos para reunir los conjuntos de habilidades correctos en el mismo equipo. Uno de los objetivos es crear y entregar aplicaciones de software con velocidad, agilidad y eficiencia. A este respecto, un número creciente de empresas está adoptando arquitecturas modernas de aplicaciones basadas en microservicios.
Mediante una arquitectura de microservicios, puede crear aplicaciones como conjuntos de servicios no acoplados que se pueden implementar, actualizar y escalar de forma independiente.

Cloud nativo es un enfoque que se basa en la arquitectura de microservicios para crear e implementar aplicaciones con los siguientes atributos clave:

- Implementa aplicaciones como microservicios o contenedores no acoplados.
- Implica un grado muy alto de automatización

- Implementa procesos ágiles de DevOps y flujos de trabajo de entrega continua
- Se centra en las API para la interacción y la colaboración

¿Cómo ayuda Kubernetes en el viaje nativo de la nube?

Para proporcionar los niveles deseados de agilidad y estabilidad, las aplicaciones nativas de la nube requieren altos niveles de automatización de infraestructura, seguridad, redes y supervisión. Necesita un sistema de orquestación de contenedores que pueda administrar de manera eficiente los contenedores a gran escala. Kubernetes se ha convertido en la plataforma más popular para la implementación y la orquestación de contenedores. Kubernetes abstrae la compleja tarea de ejecutar, implementar y administrar contenedores de desarrolladores y operadores, y programa automáticamente contenedores entre un clúster de nodos. Kubernetes y el ecosistema de la base de computación nativa en la nube (CNCF) le ayudan a crear una plataforma para soluciones nativas de la nube.

Algunos de los beneficios clave del uso de Kubernetes:

- Simplifica la implementación de aplicaciones ya sea infraestructura local, híbrida o de nube pública
- Acelera el desarrollo y la implementación de aplicaciones
- Aumenta la agilidad, flexibilidad y escalabilidad de las aplicaciones

¿Qué es la solución nativa de Citrix Cloud?

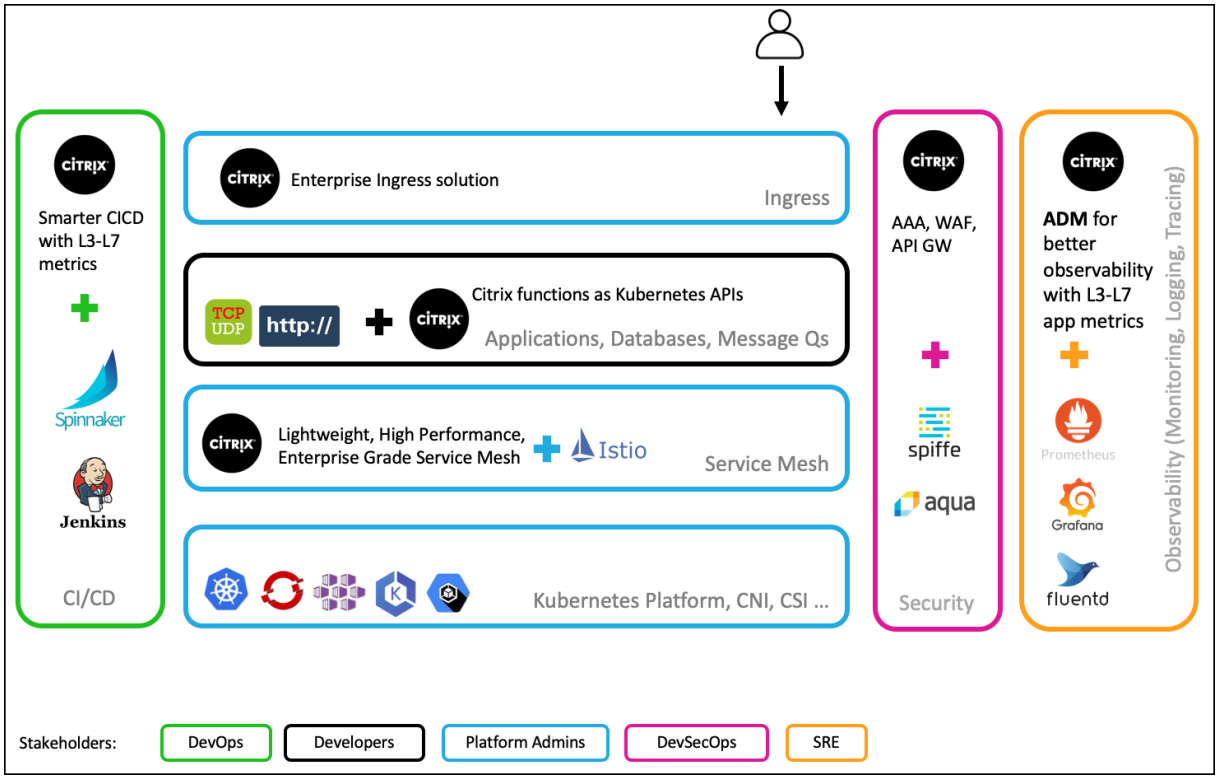
Para maximizar los beneficios del uso de Kubernetes en producción, debe integrar Kubernetes con varias herramientas, componentes de origen proveedor y código abierto. Garantizar la fiabilidad y la seguridad de nivel de producción para sus aplicaciones nativas en la nube es un reto al que se enfrentan muchas organizaciones.
Como proveedor de ADC Citrix líderes en la industria, Citrix ofrece una solución nativa de Citrix en la nube para abordar los desafíos en un entorno de producción de Kubernetes.

La solución nativa de Citrix Cloud aprovecha la administración avanzada del tráfico, la observabilidad y las funciones de seguridad integrales de los ADC de Citrix para garantizar la fiabilidad y seguridad de nivel empresarial. Puede proporcionar visibilidad completa del tráfico de aplicaciones en su entorno de Kubernetes, generar retroalimentación inmediata y ayudar a obtener información significativa sobre el rendimiento de las aplicaciones.

En la siguiente tabla se enumeran los requisitos clave de las diferentes partes interesadas durante la implementación de una solución Ingress.

Interesados	Función de trabajo	Necesidades
Administradores de plataformas	Garantizar la disponibilidad de los clústeres de Kubernetes	Formas más sencillas de administrar aplicaciones implementadas en varios clústeres, operaciones y administración del ciclo de vida de la plataforma
DevOps	Acelere la implementación de aplicaciones en producción	Integración con el proceso de CI/CD, soporte para técnicas de implementación como Canary y azul-verde para una implementación más rápida
Desarrolladores	Desarrollar y probar microservicios	Formas de introducir tráfico en el clúster de Kubernetes, rastreo y depuración, limitación de velocidad para aplicaciones y autenticación para aplicaciones
IEES	Garantizar la disponibilidad de las aplicaciones para cumplir con los acuerdos de nivel de servicio	Telemetría avanzada para aplicaciones e infraestructura
SECOPs	Garantizar el cumplimiento de seguridad	Tráfico de entrada seguro, protección de API, malla de servicio para una comunicación segura entre microservicios dentro del clúster de Kubernetes

En el siguiente diagrama se explica la solución nativa de Citrix Cloud y cómo aborda los diversos desafíos a los que se enfrentan las partes interesadas en su viaje nativo a la nube.



La solución nativa de Citrix Cloud ofrece las siguientes ventajas clave:

- Proporciona una solución avanzada de Kubernetes Ingress que satisface las necesidades de desarrolladores, SRE, DevOps y administradores de redes o clústeres.
- Elimina la necesidad de reescribir aplicaciones heredadas basadas en el tráfico TCP o UDP mientras se mueven a un entorno Kubernetes.
- Protege las aplicaciones con directivas de Citrix ADC expuestas como API de Kubernetes.
- Ayuda a implementar microservicios de alto rendimiento para el tráfico Norte-Sur y el tráfico Este-Oeste.
- Proporciona una vista todo en uno de todos los microservicios mediante el gráfico de servicios de Citrix ADM.
- Permite una solución más rápida de problemas de microservicios en diferentes tipos de tráfico, incluidos TCP, UDP, HTTP, HTTPS y SSL.
- Protege las API.
- Automatiza el proceso de CI/CD para implementaciones Canary.
- Proporciona integraciones de forma lista para usar con herramientas de código abierto CNCF.

Para obtener más información sobre los diferentes componentes de la solución nativa de Citrix Cloud, consulte los siguientes vínculos:

- Solución Kubernetes Ingress
- Malla de servicio
- Soluciones para la observabilidad

- Gateway API para Kubernetes

Solución Kubernetes Ingress

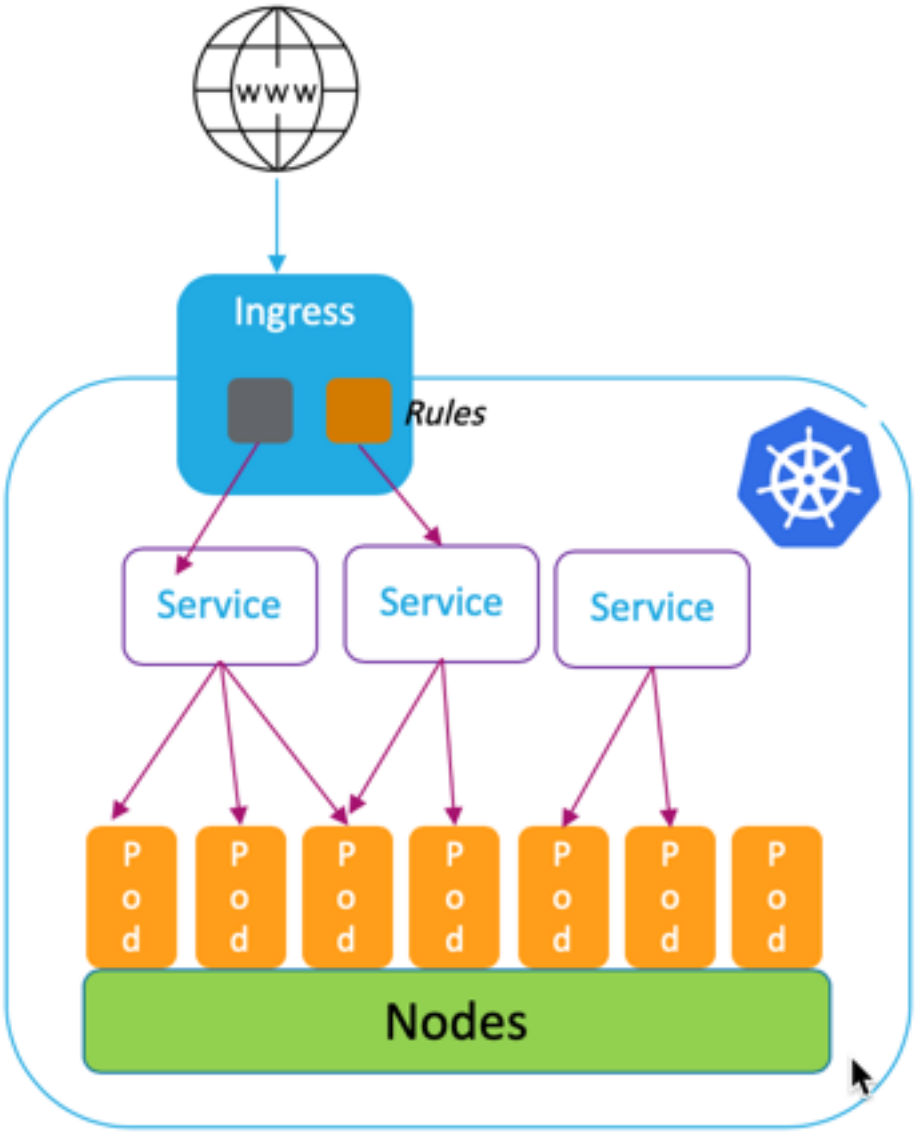
August 20, 2021

En este tema se ofrece una visión general de la solución Kubernetes Ingress proporcionada por Citrix y se explican los beneficios.

¿Qué es Kubernetes Ingress?

Cuando ejecuta una aplicación dentro de un clúster de Kubernetes, debe proporcionar una forma para que los usuarios externos tengan acceso a las aplicaciones desde fuera del clúster de Kubernetes. Kubernetes proporciona un objeto llamado Ingress que proporciona la forma más efectiva de exponer varios servicios mediante una dirección IP estable. Un objeto Kubernetes Ingress siempre está asociado con uno o más servicios y actúa como un punto de entrada único para que los usuarios externos accedan a los servicios que se ejecutan dentro del clúster.

El siguiente diagrama explica cómo funciona la entrada de Kubernetes.



La implementación de Kubernetes Ingress consta de los siguientes componentes:

- **Recurso Ingress**. Un recurso Ingress permite definir reglas para acceder a las aplicaciones desde fuera del clúster.
- **Controller de entrada**. Un controlador Ingress es una aplicación implementada dentro del clúster que interpreta las reglas definidas en la entrada. El controlador Ingress convierte las reglas de Ingress en instrucciones de configuración para una aplicación de equilibrio de carga integrada con el clúster. El equilibrador de carga puede ser una aplicación de software que se ejecuta dentro del clúster de Kubernetes o un dispositivo de hardware que se ejecuta fuera del clúster.

- **Dispositivo de entrada**. Un dispositivo Ingress es una aplicación de equilibrio de carga como Citrix ADC CPX, VPX o MPX que realiza el equilibrio de carga de acuerdo con las instrucciones de configuración proporcionadas por el controlador Ingress.

¿Qué es la solución Kubernetes Ingress de Citrix?

En esta solución, Citrix proporciona una implementación del Controller Kubernetes Ingress para administrar y enrutar el tráfico al clúster de Kubernetes mediante ADC de Citrix (Citrix ADC CPX, VPX o MPX). El Citrix ingress controller integra Citrix ADC con su entorno de Kubernetes y configura Citrix ADC CPX, VPX o MPX de acuerdo con las reglas de entrada.

Las soluciones estándar de Kubernetes Ingress proporcionan equilibrio de carga solo en la capa 7 (tráfico HTTP o HTTPS). Algunas veces, necesita exponer muchas aplicaciones heredadas que dependen de TCP o UDP o aplicaciones y necesitan una forma de equilibrar la carga de esas aplicaciones. La solución Citrix Kubernetes Ingress proporciona compatibilidad con tráfico TCP, TCP-SSL y UDP, además de la entrada HTTP o HTTPS estándar. Además, funciona sin problemas en múltiples nubes o centros de datos locales.

Citrix ADC proporciona directivas de administración de tráfico de nivel empresarial, como directivas de reescritura y respuesta, para equilibrar eficazmente el tráfico en la capa 7. Sin embargo, Kubernetes Ingress carece de tales directivas de gestión del tráfico de nivel empresarial. Con la solución Kubernetes Ingress de Citrix, puede aplicar directivas de reescritura y respuesta para el tráfico de aplicaciones en un entorno de Kubernetes mediante CRD proporcionados por Citrix.

La solución Kubernetes Ingress de Citrix también admite la implementación Canary automatizada para su proceso de aplicaciones CI/CD. En esta solución, Citrix ADC se integra con la plataforma Spinnaker y sirve de fuente para proporcionar métricas precisas para analizar la implementación Canary mediante Kayenta. Tras analizar las métricas, Kayenta genera una puntuación agregada para Canary y decide promocionar o fallar la versión Canary. También puede regular la distribución del tráfico a la versión Canary mediante la infraestructura de directivas de Citrix ADC.

En la siguiente tabla se resumen los beneficios que ofrece la solución Ingress de Citrix sobre Kubernetes Ingress.

Funciones	Kubernetes Ingress	Solución Ingress de Citrix
Compatibilidad con HTTP y HTTPS	Sí	Sí
Redirección de URL	Sí	Sí
TLS	Sí	Sí
Equilibrio de carga	Sí	Sí
TCP, TCP-SSL	No	Sí

Funciones	Kubernetes Ingress	Solución Ingress de Citrix
UDP	No	Sí
HTTP/2	Sí	Sí
Soporte automatizado de implementación Canary con herramientas CI/CD	No	Sí
Compatibilidad con la aplicación de directivas de reescritura y respuesta de Citrix ADC	No	Sí
Autenticación (Autorización abierta (OAuth), TLS mutua (MTL))	No	Sí
Compatibilidad con la aplicación de directivas de limitación de velocidad de Citrix	No	Sí

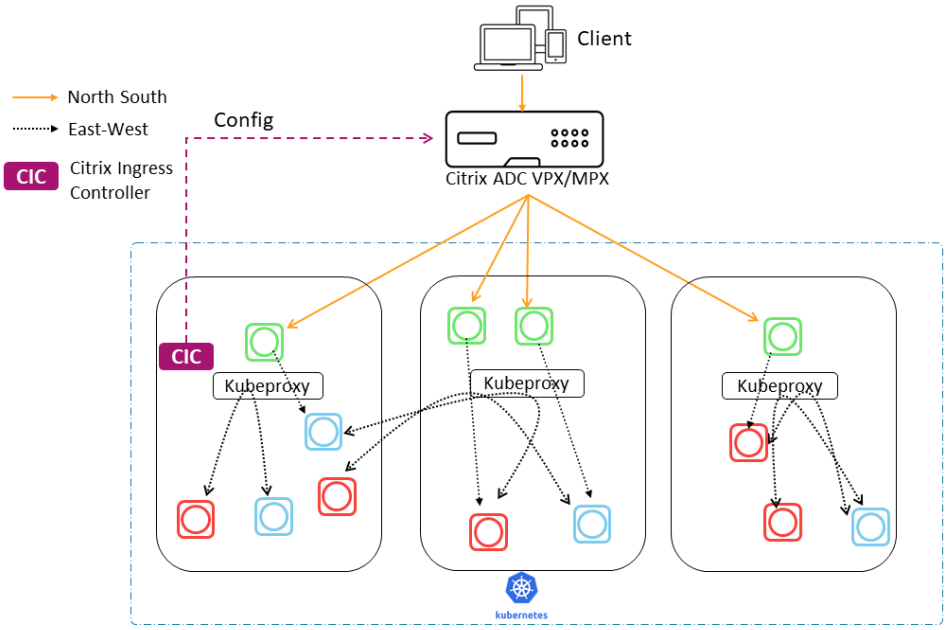
Opciones de implementación para la solución Kubernetes Ingress

La solución Kubernetes Ingress de Citrix le proporciona una arquitectura flexible en función de cómo quiera administrar sus ADC de Citrix y su entorno de Kubernetes.

Ingress unificado (nivel único)

En una arquitectura de Ingress unificada (un solo nivel), un dispositivo Citrix MPX o VPX implementado fuera del clúster de Kubernetes se integra con el entorno de Kubernetes mediante el Citrix ingress controller. El Citrix ingress controller se implementa como pod en el clúster de Kubernetes y automatiza la configuración de Citrix ADC en función de los cambios realizados en los microservicios o los recursos de Ingress. El dispositivo Citrix ADC realiza funciones como equilibrio de carga, terminación TLS y optimizaciones de protocolos HTTP o TCP en el tráfico entrante y, a continuación, enruta el tráfico al microservicio correcto dentro de un clúster de Kubernetes. Esta arquitectura se adapta mejor a casos en los que el mismo equipo administra la plataforma Kubernetes y otra infraestructura de red, incluidos los controladores de entrega de aplicaciones (ADC).

El siguiente diagrama muestra una implementación que utiliza la arquitectura de Ingress unificada.



Una solución unificada de ingreso proporciona los siguientes beneficios clave:

- Proporciona una forma de ampliar las capacidades de su infraestructura Citrix ADC existente al entorno Kubernetes
- Le permite aplicar directivas de administración de tráfico para el tráfico entrante
- Proporciona una arquitectura simplificada adecuada para equipos de DevOps conocedores de la red
- Soporta multitenancy

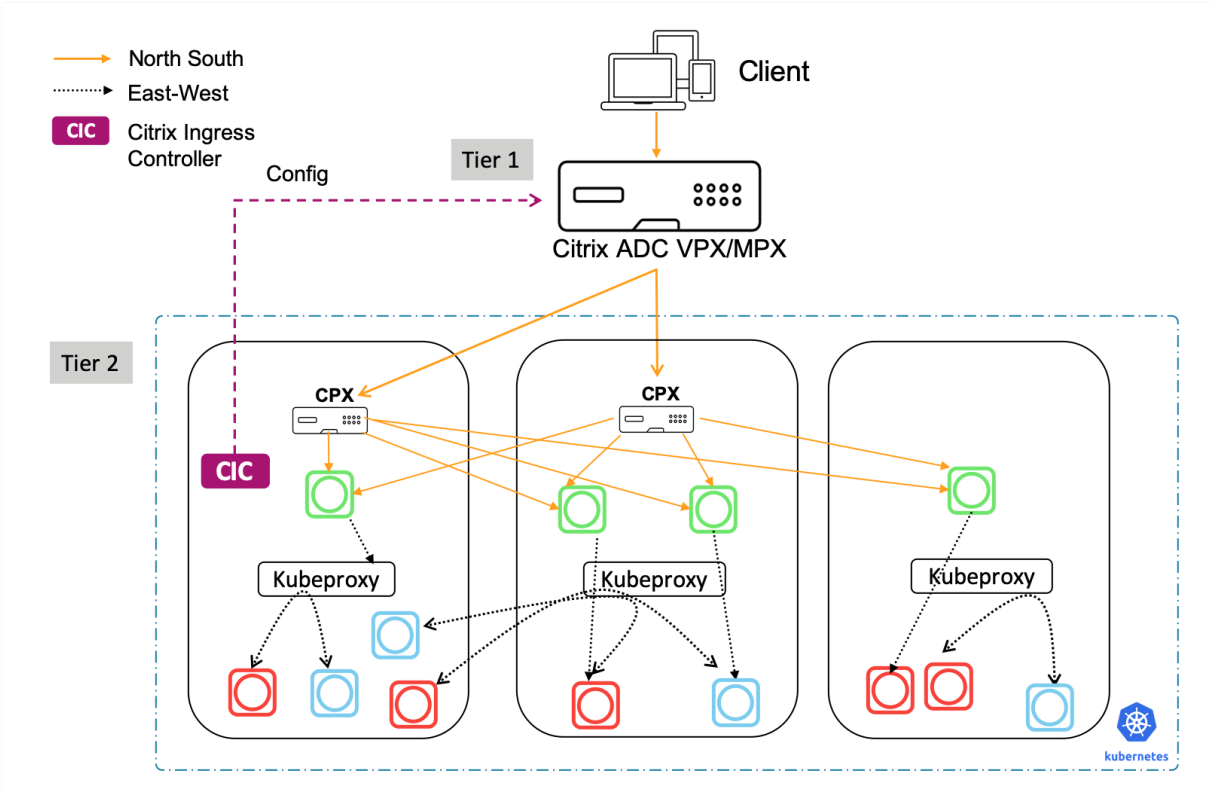
Ingreso de dos niveles

En una arquitectura de dos niveles, Citrix ADC (MPX o VPX) implementado fuera del clúster de Kubernetes actúa en el nivel 1 y la carga equilibra el tráfico Norte-Sur con CPX de Citrix ADC que se ejecutan dentro del clúster. Citrix ADC CPX actúa en el nivel 2 y realiza el equilibrio de carga para microservicios dentro del clúster de Kubernetes.

En casos en los que equipos independientes administran la plataforma Kubernetes y la infraestructura de red, la arquitectura de doble nivel es la más adecuada.

Los equipos de redes utilizan Citrix ADC de nivel 1 para casos de uso como GSLB, terminación TLS en la plataforma de hardware y equilibrio de carga TCP. Los equipos de plataformas de Kubernetes pueden usar Citrix ADC (CPX) de nivel 2 para el equilibrio de carga de la capa 7 (HTTP/HTTPS), TLS mutuo y la observabilidad o supervisión de microservicios. El Citrix ADC (CPX) de nivel 2 puede tener una versión de software diferente de la versión de Citrix ADC de nivel 1 para acomodar las capacidades recién disponibles.

El siguiente diagrama muestra una implementación con arquitectura de dos niveles.



Una entrada de dos niveles proporciona los siguientes beneficios clave:

- Garantiza una alta velocidad de desarrollo de aplicaciones para desarrolladores o equipos de plataformas
- Permite aplicar directivas de administración de tráfico impulsadas por desarrolladores para microservicios dentro del clúster de Kubernetes
- Permite escalar y multitenancy en la nube

Para obtener más información, consulte la documentación del Citrix ingress controller.

Introducción

Para empezar a utilizar la solución Kubernetes Ingress de Citrix, puede probar los siguientes ejemplos:

- Equilibrio de carga Tráfico de entrada con Citrix ADC CPX en Minikube
- Equilibrio de carga del tráfico de entrada Norte-Sur mediante el proxy CPX de Citrix ADC
- Equilibrio de carga tráfico de microservicios Este-Oeste mediante el proxy CPX de Citrix ADC
- Sumérgete en las funciones de Kubernetes con Citrix ADC CPX

Malla de servicio

August 20, 2021

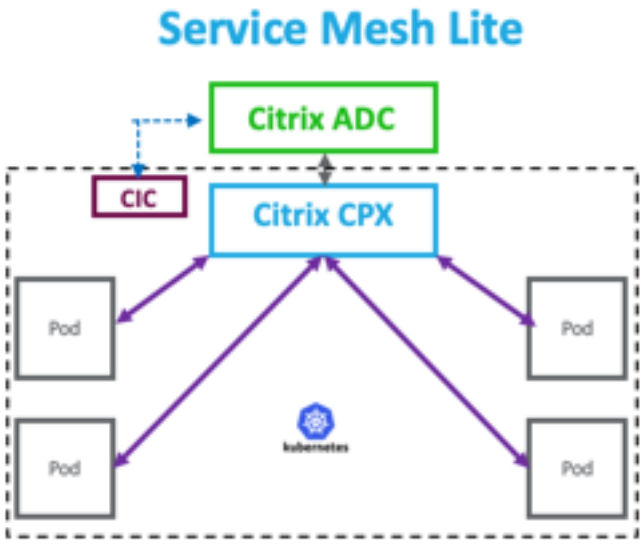
Una malla de servicio es una capa de infraestructura para gestionar la comunicación de servicio a servicio para aplicaciones nativas de la nube que utilizan API. Proporciona una forma de conectar, proteger y supervisar sus microservicios. Citrix ofrece dos soluciones para satisfacer sus requisitos de malla de servicio:

- Malla de servicio lite
- Malla de servicio (integración de Citrix ADC con Istio)

Malla de servicio lite

Una implementación completa de malla de servicio es compleja y requiere una curva de aprendizaje pronunciada. Si busca una implementación simplificada de una malla de servicios con beneficios similares, Citrix ofrece una solución denominada service mesh lite con menor complejidad. En esta solución, un dispositivo Citrix ADC CPX se ejecuta como equilibrador de carga centralizado en el clúster de Kubernetes y equilibra la carga el tráfico Este-Oeste entre los microservicios. Citrix ADC CPX aplica directivas para el tráfico entrante y entre contenedores.

El siguiente diagrama muestra una arquitectura de Service Mesh Lite.



Para obtener información, consulte la documentación de service mesh lite.

Malla de servicio (integración de Citrix ADC con Istio)

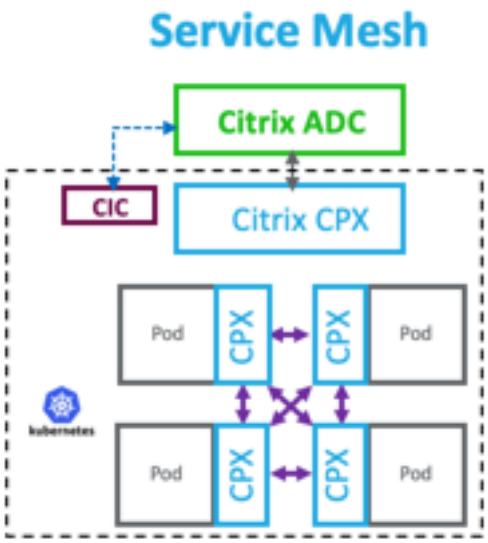
Citrix proporciona una solución de malla de servicio mediante la integración de Citrix ADC con Istio. Istio, una malla de servicio de código abierto e independiente de la plataforma, es una de las implementaciones de malla de servicio más populares. Al integrar Citrix ADC con Istio, puede aprovechar las funciones de Citrix ADC para proteger y optimizar el tráfico de las aplicaciones en la malla de servicio.

Citrix ADC se puede integrar con Istio de las siguientes maneras:

- Citrix ADC MPX, VPX o CPX como puerta de enlace de ingreso de Istio a la malla de servicio para exponer el tráfico al clúster de Kubernetes.
- Citrix ADC CPX como proxy sidecar con contenedores de aplicaciones en la malla de servicio para controlar la comunicación entre aplicaciones.

Puede utilizar la integración de forma independiente o puede combinar ambas formas para tener una solución unificada de plano de datos.

El siguiente diagrama muestra una arquitectura de malla de servicio.



La malla de servicio es ideal para aplicaciones altamente seguras y también ofrece las siguientes ventajas.

- Ofrece una gestión de tráfico de grano fino (modularizado) por contenedor
- Garantiza una mayor observabilidad, análisis y seguridad (TLS mutua) gracias a la implementación de sidecar

- Permite la implementación Canary automatizada para cada contenedor con Citrix ADC CPX integrado
- Admite portabilidad en la nube
- Permite descargar algunas de las funciones realizadas por las aplicaciones al sidecar
- Proporciona menor latencia de sidecar
- Proporciona integraciones con herramientas de código abierto
- Ofrece escalabilidad

Para obtener más información, consulte la integración de Citrix ADC con la documentación de Istio.

Soluciones para la observabilidad

August 20, 2021

En una arquitectura basada en microservicios, la visibilidad de las comunicaciones de servicio a servicio es fundamental para construir una arquitectura eficiente y resistente. Las formas tradicionales de registro y supervisión no son capaces de abordar los desafíos de una arquitectura de microservicios. Las soluciones de observabilidad de Citrix le proporcionan la posibilidad de ver lo que está sucediendo cuando sus servicios interactúan entre sí y obtener información significativa sobre su sistema.

Citrix ofrece las siguientes soluciones para satisfacer las necesidades de observabilidad de su arquitectura de microservicios:

- Gráfico de servicios y análisis de Citrix ADM
- Exportador de observabilidad Citrix ADC

Gráfico de servicios y análisis de Citrix ADM

Citrix Application Delivery Management (ADM) es una solución de administración centralizada que proporciona visibilidad y automatización en toda la empresa para los trabajos de administración que deben ejecutarse en varias instancias.

En una arquitectura de microservicios, la solución de problemas es difícil porque una única solicitud de usuario final puede abarcar varios microservicios.

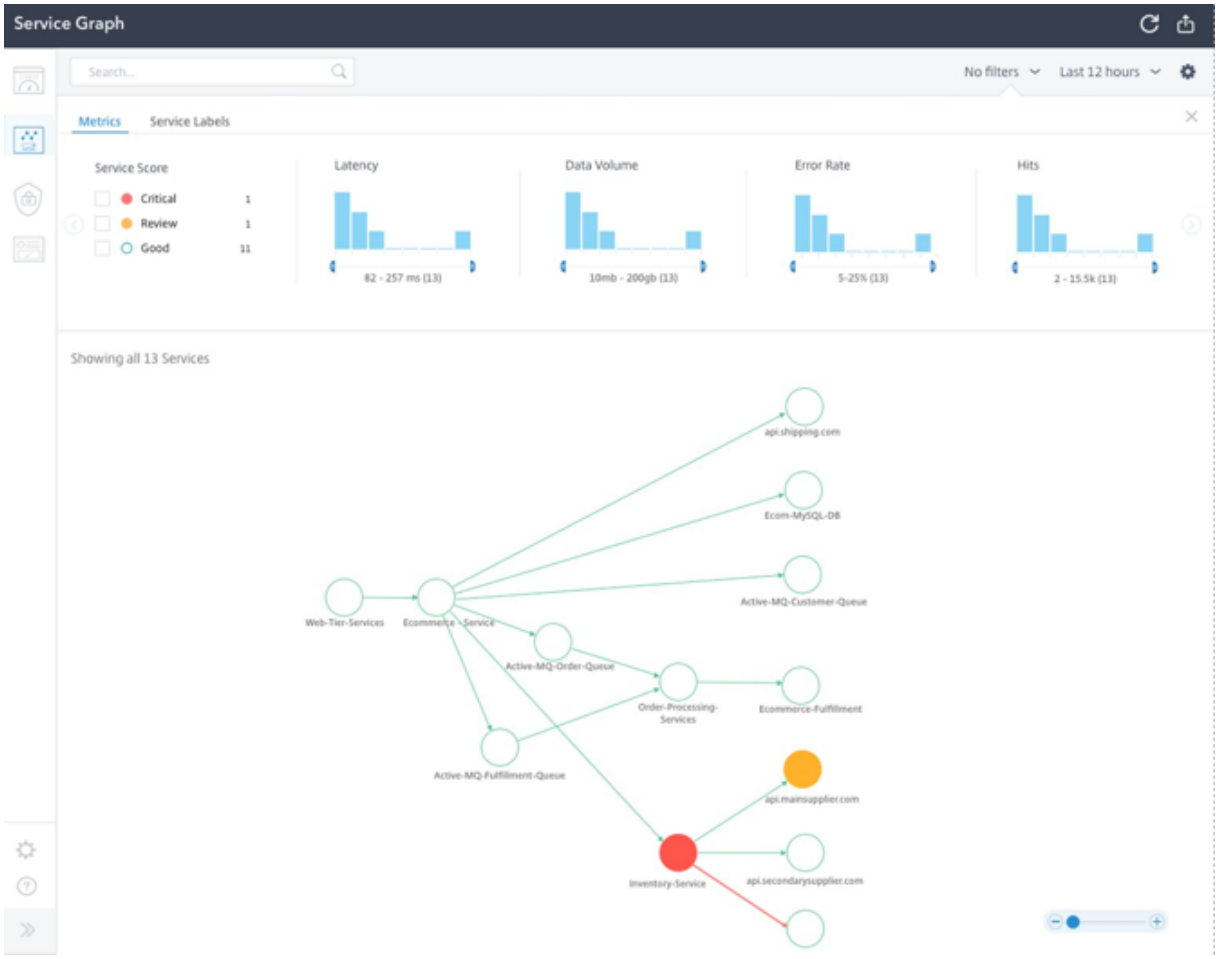
El gráfico de servicios y el análisis de Citrix ADM proporcionan visibilidad de las interacciones entre microservicios y ayudan a identificar y solucionar problemas en función de diversas métricas, como latencia y errores HTTP.

Citrix ADM también proporciona análisis avanzados basados en métricas y registros de transacciones recopilados de Citrix ADC.

La solución Citrix ADM ofrece las siguientes ventajas:

- Proporciona un único panel de vidrio para aplicaciones en contenedores, locales o en la nube
- Proporciona una mejor observabilidad y solución de problemas más rápida para microservicios
- Admite la implementación Canary

El siguiente diagrama muestra un gráfico de servicio de ejemplo para una aplicación que contiene varios microservicios.



Para obtener más información sobre cómo configurar el gráfico de servicios y análisis de Citrix ADM, consulte el gráfico de servicio y la documentación de Analytics .

Exportador de observabilidad Citrix ADC

El exportador de observabilidad Citrix ADC es un contenedor que recopila métricas y transacciones de Citrix ADC y los transforma en formatos adecuados (como JSON, AVRO) para endpoints compatibles. Puede exportar los datos recopilados por el exportador de observabilidad Citrix ADC al extremo deseado. Al analizar los datos, puede obtener información valiosa a nivel de microservicios para aplicaciones representadas por los ADC de Citrix.

Compatibilidad con seguimiento distribuido

Los trazadores distribuidos le permiten visualizar el flujo de datos entre sus microservicios y le ayudan a identificar los cuellos de botella en su arquitectura de microservicios. OpenTracing es una especificación y un conjunto estándar de API para diseñar e implementar el rastreo distribuido.

El exportador de observabilidad de Citrix implementa el seguimiento distribuido para Citrix ADC y actualmente admite Zipkin como trazador distribuido.

Puede mejorar el análisis de rastros mediante Elasticsearch y Kibana con Zipkin. Elasticsearch proporciona retención a largo plazo de los datos de seguimiento. Kibana le permite obtener una visión mucho más profunda de los datos proporcionando una herramienta para explorar y visualizar mensajes de registro.

Recopilación de transacciones y soporte de transmisión

El exportador de observabilidad de Citrix ADC admite recopilar transacciones y transmitirlas a endpoints. Actualmente, el exportador de observabilidad Citrix ADC admite Elasticsearch y Kafka como puntos finales de transacción.

Para obtener más información, consulte la documentación del exportador de observabilidad de Citrix ADC.

Habilitar análisis mediante anotaciones en el archivo YAML de la Citrix ingress controller

Puede habilitar los análisis mediante el perfil de análisis que se define como una anotación inteligente en Ingress o servicio de configuración de tipo LoadBalancer. Puede definir los parámetros específicos que debe supervisar especificándolos en la configuración de Ingress o servicio de la aplicación. Para obtener más información sobre cómo habilitar los análisis mediante anotaciones, consulte Analytics mediante anotaciones.

Gateway API para Kubernetes

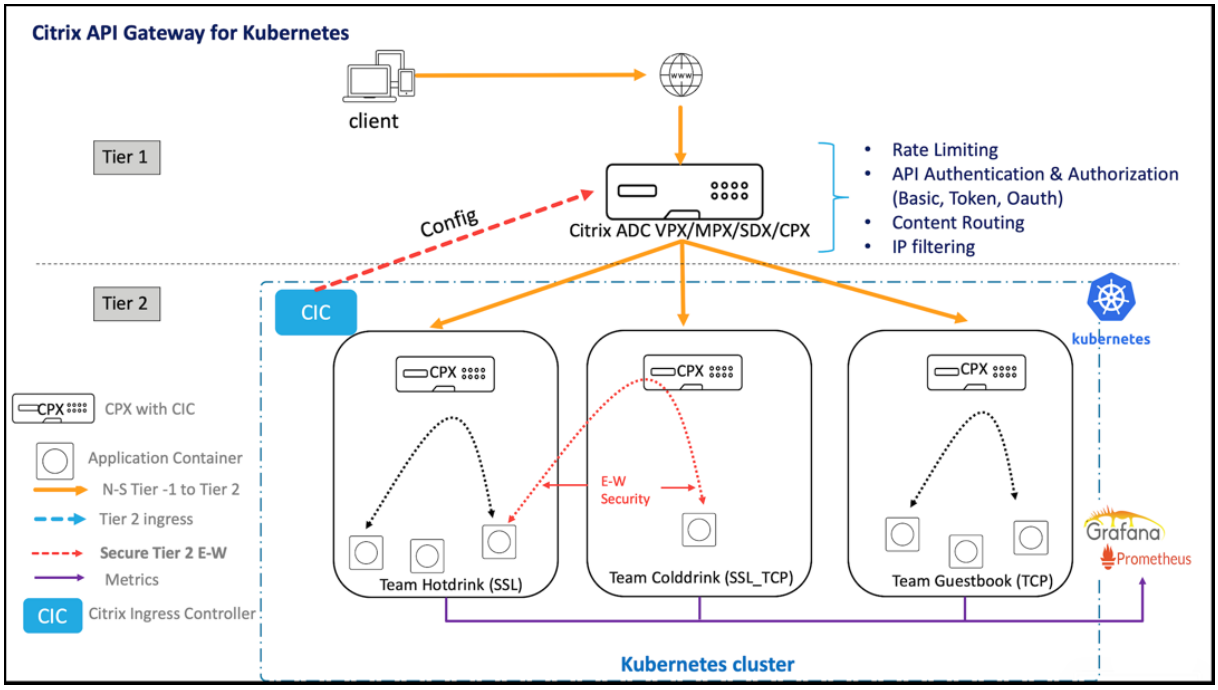
August 20, 2021

Una Gateway API actúa como el único punto de entrada para sus API y garantiza un acceso seguro y confiable a múltiples API y microservicios en su sistema.

Citrix proporciona una Gateway API de nivel empresarial para el tráfico de API Norte-Sur en el clúster de Kubernetes. La puerta de enlace
API se integra con Kubernetes a través del controlador Ingress de Citrix y el Citrix ADC (Citrix ADC MPX,

VPX o CPX) implementado como la puerta de enlace de entrada para implementaciones locales o en la nube.

El siguiente diagrama muestra una topología de dos niveles para la Gateway de API.



Con la Gateway API que ofrece Citrix, puede realizar las siguientes funcionalidades:

- Aplicar directivas de autenticación
- Tasa límite de acceso a los servicios
- Redirección avanzada de contenido
- Transformación flexible e integral de transacciones HTTP mediante las directivas de reescritura y respuesta
- Aplicar directivas de firewall de aplicaciones web

¿Cómo funciona la Gateway de API?

La puerta de enlace API se basa en la puerta de enlace de entrada de Citrix y utiliza extensiones de API de Kubernetes, como definiciones de recursos personalizadas (CRD). Con los CRD, puede configurar automáticamente Citrix ADC y API Gateway en la misma instancia.

Citrix proporciona las siguientes CRD para la Gateway de API:

- Auth CRD
- Límite de velocidad CRD
- CRD de redirección de contenido
- Reescribir y responder CRD
- WAF CRD

Ventajas clave del uso de la Gateway API

A continuación se presentan las ventajas clave de la Gateway API ofrecida por Citrix:

- Utiliza la administración avanzada del tráfico y las funciones de seguridad integrales de Citrix ADC.
- Optimiza las implementaciones mediante la consolidación de varias funciones de red en un solo componente de la puerta de enlace de entrada de Citrix.
- Reduce la complejidad operativa y el coste que implica la implementación de varios componentes.
- Garantiza un mejor rendimiento para el tráfico de las aplicaciones al reducir múltiples saltos de descifrado TCP o TLS mientras utiliza componentes independientes.
- Simplifica la implementación e integración en sus entornos Kubernetes, ya sea mediante el uso directo de YAML o gráficos de timón.

Implementación de la Gateway de API

Para obtener más información sobre cómo configurar las funciones de API Gateway mediante CRD, consulte la documentación del controlador Ingress de Citrix:

- Autenticación
- Limitación de velocidad
- Redirección avanzada de contenido
- Directivas de reescritura y respuesta
- Directivas de firewall de aplicaciones web

Usar Citrix ADM para solucionar problemas de redes nativas de la nube de Citrix

February 19, 2022

Información general

Este documento proporciona información sobre cómo puede usar Citrix ADM para entregar y supervisar aplicaciones de microservicios de Kubernetes. También se sumerge en el uso de la CLI, los gráficos de servicio y el seguimiento para permitir que los equipos de la plataforma y de SRE solucionen los problemas.

Descripción general de rendimiento y latencia de aplicaciones

Cifrado TLS

TLS es un protocolo de cifrado diseñado para proteger las comunicaciones por Internet. Un desafío mutuo TLS es el proceso que inicia una sesión de comunicación que utiliza el cifrado TLS. Durante un protocolo de enlace TLS, las dos partes que se comunican intercambian mensajes para reconocerse mutuamente, verificarse mutuamente, establecer los algoritmos de cifrado que utilizan y ponerse de acuerdo sobre las claves de sesión. Los apretones de manos de TLS son una parte fundamental del funcionamiento de HTTPS.

Apretones de manos TLS vs SSL

SSL (Secure Sockets Layer), fue el protocolo de cifrado original desarrollado para HTTP. TLS (Transport Layer Security) reemplazó a SSL hace algún tiempo. Los apretones de manos SSL ahora se denominan apretones de manos TLS, aunque el nombre "SSL" sigue siendo de uso generalizado.

¿Cuándo se produce un desafío mutuo TLS?

Se produce un desafío mutuo TLS cada vez que un usuario navega a un sitio web a través de HTTPS y el explorador comienza a consultar primero el servidor de origen del sitio web. Un desafío mutuo TLS también ocurre cuando cualquier otra comunicación utiliza HTTPS, incluidas las llamadas a la API y las consultas DNS a través de HTTPS.

Los apretones de manos TLS se producen después de que se ha abierto una conexión TCP mediante un protocolo de enlace TCP.

¿Qué ocurre durante un desafío mutuo de TLS?

- Durante un protocolo de enlace de TLS, el cliente y el servidor juntos hacen lo siguiente:
  - Especifique qué versión de TLS (TLS 1.0, 1.2, 1.3, etc.) usan.
  - Decida qué conjuntos de cifrado (consulte la siguiente sección) que utilizan.
  - Autenticar la identidad del servidor a través de la clave pública del servidor y la firma digital de la entidad de certificación SSL.
  - Genere claves de sesión para usar cifrado simétrico después de que se complete el desafío mutuo.

¿Cuáles son los pasos de un desafío mutuo TLS?

- Los apretones de manos TLS son una serie de datagramas o mensajes intercambiados por un cliente y un servidor. Un desafío mutuo TLS implica varios pasos, ya que el cliente y el servidor intercambian la información necesaria para completar el desafío mutuo y hacer posible una conversación posterior.

Los pasos exactos dentro de un protocolo de enlace TLS varían según el tipo de algoritmo de intercambio de claves utilizado y los conjuntos de cifrado admitidos por ambas partes. El algoritmo de intercambio de claves RSA se usa con mayor frecuencia. Va de la siguiente manera:

1. El mensaje de “saludo del cliente”: el cliente inicia el desafío mutuo enviando un mensaje de “hola” al servidor. El mensaje incluye qué versión de TLS admite el cliente, las suites de cifrado admitidas y una cadena de bytes aleatorios conocida como “cliente aleatorio”.
2. El mensaje de “saludo del servidor”: en respuesta al mensaje de saludo del cliente, el servidor envía un mensaje que contiene el certificado SSL del servidor, el conjunto de cifrado elegido por el servidor y el “servidor aleatorio”, otra cadena aleatoria de bytes que genera el servidor.
3. Autenticación: El cliente verifica el certificado SSL del servidor con la entidad de certificación que lo emitió. Esto confirma que el servidor es quien dice ser y que el cliente interactúa con el propietario real del dominio.
4. El secreto premaestro: El cliente envía una cadena aleatoria más de bytes, el “secreto premaestro”. El secreto premaestro se cifra con la clave pública y el servidor solo puede descifrarlo con la clave privada. (El cliente obtiene la clave pública del certificado SSL del servidor).
5. Clave privada utilizada: el servidor descifra el secreto premaestro.
6. Claves de sesión creadas: tanto el cliente como el servidor generan claves de sesión a partir del cliente aleatorio, el servidor aleatorio y el secreto premaestro. Deben llegar a los mismos resultados.
7. El cliente está listo: el cliente envía un mensaje “finalizado” que se cifra con una clave de sesión.
8. El servidor está listo: el servidor envía un mensaje “finalizado” cifrado con una clave de sesión.
9. Cifrado simétrico seguro: se completa el desafío mutuo y la comunicación continúa utilizando las claves de sesión.

Todos los apretones de manos TLS utilizan cifrado asimétrico (la clave pública y la privada), pero no todos usan la clave privada en el proceso de generación de claves de sesión. Por ejemplo, un desafío mutuo efímero de Diffie-Hellman procede de la siguiente manera:

1. Saludo del cliente: el cliente envía un mensaje de saludo al cliente con la versión del protocolo, el cliente aleatorio y una lista de conjuntos de cifrado.

2. Saludos del servidor: el servidor responde con su certificado SSL, su conjunto de cifrado seleccionado y el servidor de forma aleatoria. A diferencia del protocolo de enlace RSA descrito en la sección anterior, en este mensaje el servidor también incluye lo siguiente (paso 3).

3. Firma digital del servidor: el servidor utiliza su clave privada para cifrar el cliente de forma aleatoria, el servidor de forma aleatoria y su parámetro DH*. Estos datos cifrados funcionan como la firma digital del servidor, lo que establece que el servidor tiene la clave privada que coincide con la clave pública del certificado SSL.

4. Firma digital confirmada: el cliente descifra la firma digital del servidor con la clave pública, verificando que el servidor controla la clave privada y es quien dice ser. Parámetro DH del cliente: el cliente envía su parámetro DH al servidor.

5. El cliente y el servidor calculan el secreto premaestro: en lugar de que el cliente genere el secreto premaestro y lo envíe al servidor, como en un protocolo de enlace RSA, el cliente y el

servidor utilizan los parámetros DH que intercambiaron para calcular un secreto premaestro coincidente por separado.

6. Claves de sesión creadas: Ahora, el cliente y el servidor calculan las claves de sesión a partir del secreto premaestro, el aleatorio del cliente y el aleatorio del servidor, al igual que en un protocolo de enlace RSA.

    - El cliente está listo:
      igual que un desafío mutuo de RSA
    - El servidor está listo
    - Encriptación simétrica segura

    *Parámetro DH: DH significa Diffie-Hellman. El algoritmo Diffie-Hellman utiliza cálculos exponenciales para llegar al mismo secreto de premaster. El servidor y el cliente proporcionan un parámetro para el cálculo y, cuando se combinan, dan como resultado un cálculo diferente en cada lado, con resultados iguales.

Para obtener más información sobre el contraste entre los apretones de manos efímeros de Diffie-Hellman y otros tipos de apretones de manos, y cómo logran el secreto hacia adelante, consulte esta documentación del protocolo TLS.

¿Qué es un conjunto de cifrado?

- Un conjunto de cifrado es un conjunto de algoritmos de cifrado para su uso en el establecimiento de una conexión de comunicaciones segura. (Un algoritmo de cifrado es un conjunto de operaciones matemáticas que se realizan en los datos para hacer que los datos parezcan aleatorios). Hay varios conjuntos de cifrado de uso generalizado, y una parte esencial del desafío mutuo TLS es acordar qué conjunto de cifrado se usa para ese desafío mutuo.

Para empezar, consulte Referencia: documentación del protocolo TLS.

Panel SSL de Citrix Application Delivery Management

Citrix Application Delivery Management (ADM) ahora optimiza todos los aspectos de la administración de certificados por usted. A través de una sola consola, puede establecer directivas automatizadas para garantizar el emisor correcto, la fortaleza de la clave y los algoritmos correctos, al tiempo que mantiene una estrecha ficha sobre los certificados que no se utilizan o que caducan pronto. Para empezar a usar el panel SSL de Citrix ADM y sus funcionalidades, debe comprender qué es un certificado SSL y cómo puede usar Citrix ADM para rastrear sus certificados SSL.

Un certificado Secure Socket Layer (SSL), que forma parte de cualquier transacción SSL, es un formulario de datos digitales (X509) que identifica a una empresa (dominio) o a un individuo. El certificado tiene un componente de clave pública visible para cualquier cliente que quiera iniciar una transacción segura con el servidor. La clave privada correspondiente, que reside de forma segura en el dispositivo

Citrix Application Delivery Controller (ADC), se utiliza para completar el cifrado y descifrado de clave asimétrica (o clave pública).

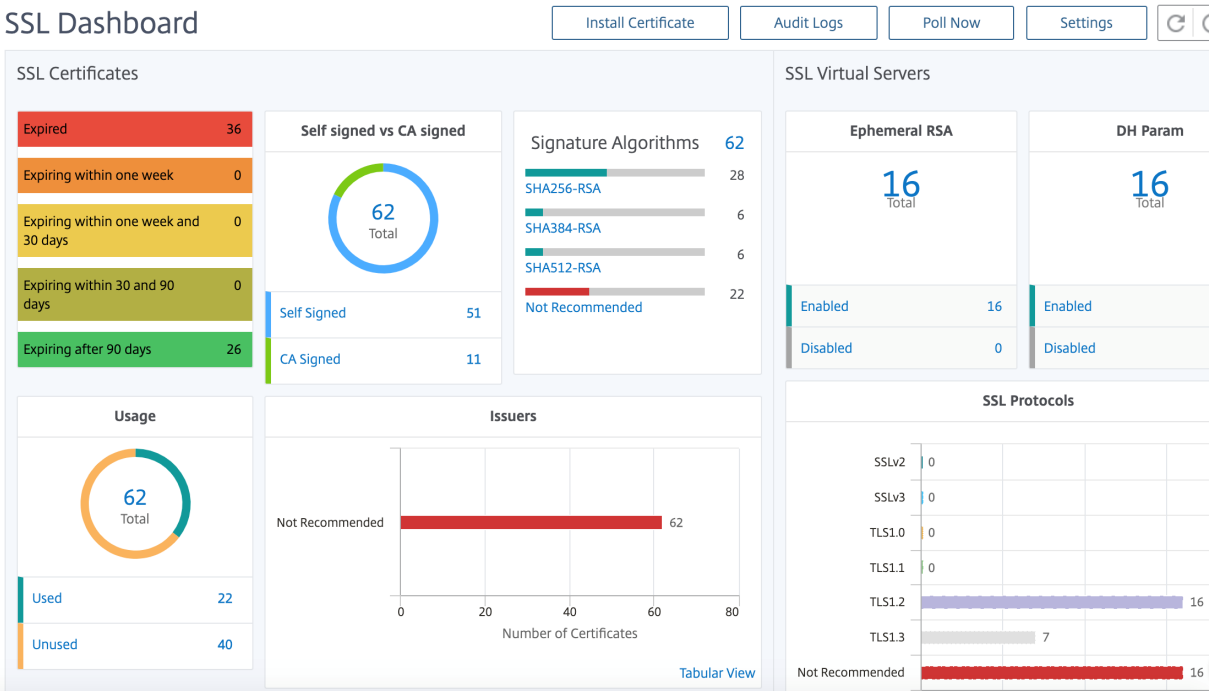
Puede obtener un certificado y una clave SSL de cualquiera de las siguientes maneras:

- De una entidad emisora de certificados (CA) autorizada
- Al generar un nuevo certificado SSL y una clave en el dispositivo Citrix ADC

Citrix ADM proporciona una vista centralizada de los certificados SSL instalados en todas las instancias de Citrix ADC administradas. En el Panel de control SSL, puede ver gráficos que le ayudan a realizar un seguimiento de emisores de certificados, fortalezas clave, algoritmos de firma, certificados caducados o no utilizados, etc. También puede ver la distribución de los protocolos SSL que se ejecutan en sus servidores virtuales y las claves que están habilitadas en ellos.

También puede configurar notificaciones para informarle cuando los certificados están a punto de caducar e incluir información sobre las instancias Citrix ADC que utilizan dichos certificados.

Puede vincular los certificados de una instancia de Citrix ADC a un certificado de CA. Sin embargo, asegúrese de que los certificados que vincula al mismo certificado de CA tienen el mismo origen y el mismo emisor. Después de vincular los certificados a un certificado de CA, puede desvincularlos.



Para empezar, consulte la documentación del panel de SSL.

Integraciones de terceros

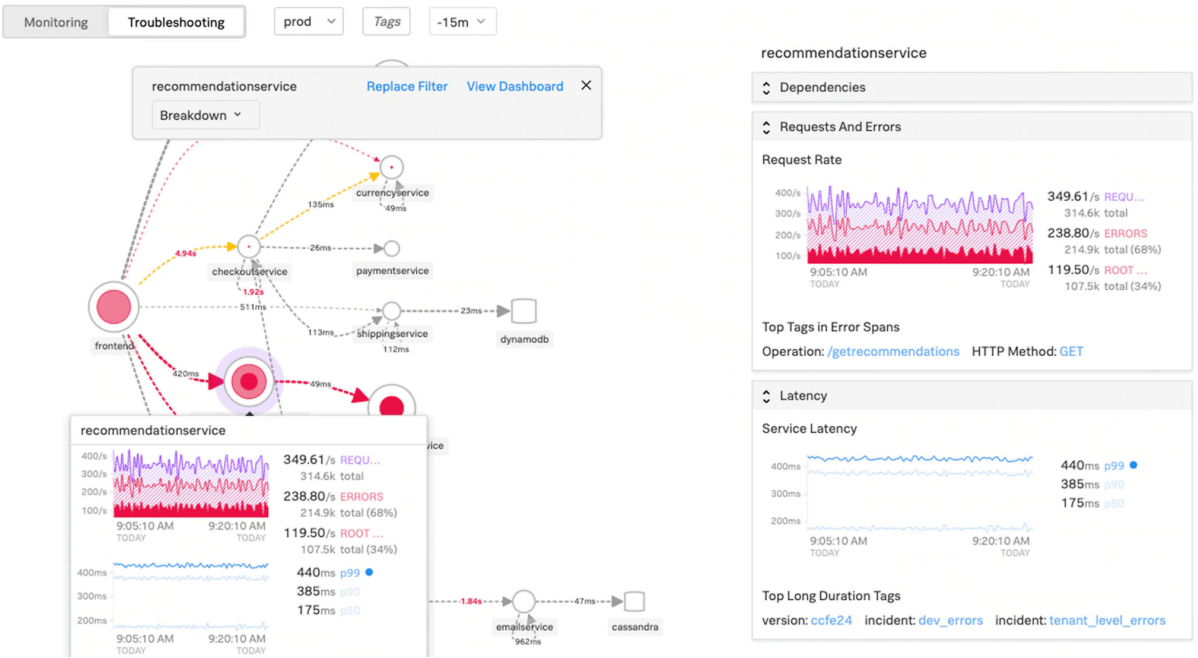
La latencia de la aplicación se mide en milisegundos y puede indicar una de dos cosas según la métrica utilizada. La forma más común de medir la latencia se llama “tiempo de ida y vuelta” (o RTT). El RTT

calcula el tiempo que tarda un paquete de datos en viajar de un punto a otro de la red y para que una respuesta se envíe de vuelta a la fuente. La otra medición se denomina “tiempo hasta el primer byte” (o TTFB), que registra el tiempo que tarda desde el momento en que un paquete sale de un punto de la red hasta el momento en que llega a su destino. El RTT se usa más comúnmente para medir la latencia porque se puede ejecutar desde un solo punto de la red y no requiere que el software de recopilación de datos se instale en el punto de destino (como lo hace TTFB).

Al supervisar el uso y el rendimiento del ancho de banda de la aplicación en tiempo real, el servicio ADM facilita la identificación de problemas y el tratamiento preventivo de posibles problemas antes de que se manifiesten y afecten a los usuarios de su red. Esta solución basada en flujo hace un seguimiento del uso por interfaz, aplicación y conversación, lo que le brinda información detallada sobre la actividad en su red.

Uso de herramientas de Splunk

El rendimiento de la infraestructura y las aplicaciones es interdependiente. Para ver el panorama completo, SignalFx proporciona una correlación perfecta entre la infraestructura de la nube y los microservicios que se ejecutan en la parte superior de la misma. Si su aplicación funciona mal debido a una pérdida de memoria, a un contenedor vecino ruidoso o a cualquier otro problema relacionado con la infraestructura, SignalFx se lo informa. Para completar el panorama, el acceso en contexto a los registros y eventos de Splunk permite una solución de problemas más profunda y un análisis de la causa raíz.



Para obtener más información sobre la APM de microservicios SignalFx y la solución de problemas con Splunk, consulte Splunk para obtener información sobre DevOps.

Compatibilidad con MongoDB

MongoDB almacena los datos en documentos flexibles similares a JSON. Los campos de significado pueden variar de un documento a otro y la estructura de los datos se puede cambiar con el tiempo.

El modelo de documento se asigna a los objetos del código de la aplicación, lo que facilita el trabajo con los datos.

Las consultas bajo demanda, la indexación y la agregación en tiempo real proporcionan formas eficaces de acceder a sus datos y analizarlos.

MongoDB es una base de datos distribuida en su núcleo, por lo que la alta disponibilidad, el escalado horizontal y la distribución geográfica están integradas y son fáciles de usar.

MongoDB está diseñado para satisfacer las demandas de las aplicaciones modernas con una base tecnológica que le permite:

- El modelo de datos de documentos: le presenta la mejor manera de trabajar con datos.
- Un diseño de sistemas distribuidos, que le permite colocar los datos de manera inteligente donde lo desea.
- Una experiencia unificada que le da la libertad de funcionar en cualquier lugar, lo que le permite preparar su trabajo para el futuro y eliminar la dependencia de los proveedores.

Con estas capacidades, puede crear una plataforma de datos operativos inteligente, respaldada por MongoDB. Para obtener más información, consulte la documentación de MongoDB.

Cómo equilibrar la carga del tráfico de entrada a una aplicación basada en TCP o UDP

En un entorno de Kubernetes, un Ingress es un objeto que permite el acceso a los servicios de Kubernetes desde fuera del clúster de Kubernetes. Los recursos estándar de Kubernetes Ingress asumen que todo el tráfico se basa en HTTP y no atiende a protocolos no basados en HTTP, como TCP, TCP-SSL y UDP. Por lo tanto, las aplicaciones críticas basadas en protocolos L7, como DNS, FTP o LDAP, no se pueden exponer mediante Kubernetes Ingress estándar.

La solución estándar de Kubernetes consiste en crear un servicio de tipo LoadBalancer. Consulte Load-Balancer de tipos de servicio en Citrix ADC para obtener más información.

La segunda opción es anotar el objeto de entrada. Citrix ingress controller le permite equilibrar la carga del tráfico de entrada basado en TCP o UDP. Proporciona las siguientes anotaciones que puede usar en la definición de recursos de Kubernetes Ingress para equilibrar la carga del tráfico de entrada basado en TCP o UDP:

- ingress.citrix.com/insecure-service-type: La anotación habilita el equilibrio de carga L4 con TCP, UDP o ANY como protocolo para Citrix ADC.

- ingress.citrix.com/insecure-port: La anotación configura el puerto TCP. La anotación es útil cuando se requiere acceso a microservicios en un puerto no estándar. De forma predeterminada, se configura el puerto 80.

Para obtener más información, consulte Cómo equilibrar la carga del tráfico de entrada a una aplicación basada en TCP o UDP.

Supervise y mejore el rendimiento de sus aplicaciones basadas en TCP o UDP

Los desarrolladores de aplicaciones pueden supervisar de cerca el estado de las aplicaciones basadas en TCP o UDP a través de monitores enriquecidos (como TCP-ECV, UDP-ECV) en Citrix ADC. La ECV (validación de contenido extendida) supervisa la ayuda para verificar si la aplicación devuelve el contenido esperado o no.

Además, el rendimiento de la aplicación se puede mejorar mediante el uso de métodos de persistencia, como la IP de origen. Puede usar estas funciones de Citrix ADC a través de anotaciones inteligentes en Kubernetes. A continuación se muestra un ejemplo de ello:

```
apiVersion: extensions/v1beta1
kind: Ingress
metadata:
    name: mongodb
    annotations:
        ingress.citrix.com/insecure-port:  “80”
        ingress.citrix.com/frontend-ip:  “192.168.1.1”
        ingress.citrix.com/csvserver:  ‘{
  “l2conn” :” on”  }
 ’
        ingress.citrix.com/lbvserver:  ‘{
  “mongodb-svc” :{
  “lbmethod” :” SRCIPDESTIPHASH”  }
  }
 ’
        ingress.citrix.com/monitor:  ‘{
  “mongodbsvc” :{
  “type” :” tcp-ecv”  }
  }
 ’
Spec:
    rules:
    - host: mongodb.beverages.com
      http:
        paths:
```



```
26          - path: /
27            backend:
28              serviceName: mongodb-svc
29              servicePort: 80
30  <!--NeedCopy-->
```

Servicio Citrix Application Delivery Management (ADM)

Citrix ADM Service ofrece las siguientes ventajas:

- **Ágil**: Fácil de operar, actualizar y consumir. El modelo de servicio de Citrix ADM Service está disponible en la nube, lo que facilita la operación, la actualización y el uso de las funciones proporcionadas. La frecuencia de las actualizaciones, combinada con la función de actualización automatizada, mejora rápidamente la implementación de Citrix ADC.
- **Tiempo de obtención de valor** más rápido: Logro de objetivos empresariales más rápido. A diferencia de la implementación local tradicional, puede usar su servicio Citrix ADM con unos pocos clics. No solo ahorra tiempo de instalación y configuración, sino que también evita perder tiempo y recursos en posibles errores.
- **Administración de varios sitios**: Un solo panel de vidrio para instancias en centros de datos de varios sitios. Con Citrix ADM Service, puede administrar y supervisar los ADC de Citrix que se encuentran en varios tipos de implementaciones. Tiene una administración integral para los ADC de Citrix implementados en las instalaciones y en la nube.
- **Eficiencia operativa**: Forma optimizada y automatizada de lograr una mayor productividad operativa. Con Citrix ADM Service, sus costes operativos se reducen al ahorrar tiempo, dinero y recursos en el mantenimiento y actualización de las implementaciones de hardware tradicionales.

Gráfico de servicio para aplicaciones Kubernetes

Con el gráfico de servicio para la función de aplicación nativa de la nube en Citrix ADM, puede:

- Garantice el performance general de las aplicaciones end-to-end
- Identifique los cuellos de botella creados por la interdependencia de los diferentes componentes de sus aplicaciones
- Reúna información sobre las dependencias de los diferentes componentes de sus aplicaciones
- Supervisar los servicios dentro del clúster de Kubernetes
- Supervisar qué servicio tiene problemas
- Comprobar los factores que contribuyen a los problemas de rendimiento
- Ver visibilidad detallada de las transacciones HTTP de servicio
- Analizar las métricas HTTP, TCP y SSL

Al visualizar estas métricas en Citrix ADM, puede analizar la causa raíz de los problemas y realizar las acciones necesarias para solucionar problemas más rápidamente. El gráfico de servicios muestra sus aplicaciones en varios servicios de componentes. Estos servicios que se ejecutan dentro del clúster de Kubernetes pueden comunicarse con varios componentes dentro y fuera de la aplicación.

Para empezar, consulta Configurar el gráfico de servicios.

Gráfico de servicio para aplicaciones web de 3 niveles

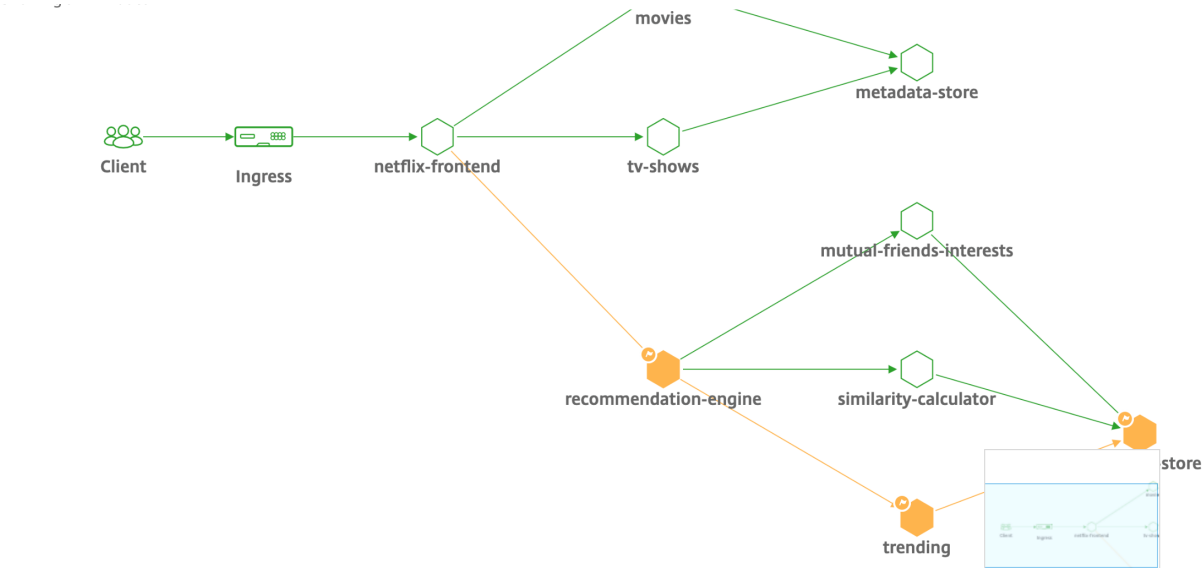
Con la función de gráfico de servicio desde el panel de aplicación, puede ver:

- Detalles sobre cómo se configura la aplicación (con el servidor virtual de conmutación de contenido y el servidor virtual de equilibrio de carga)
  - Para las aplicaciones GSLB, puede ver el centro de datos, la instancia de ADC, los servidores virtuales CS y LB
- Transacciones de extremo a extremo desde el cliente hasta el servicio
- La ubicación desde la que el cliente accede a la aplicación
- El nombre del centro de datos donde se procesan las solicitudes del cliente y las métricas de Citrix ADC del centro de datos asociadas (solo para aplicaciones GSLB)
- Detalles de métricas para clientes, servicios y servidores virtuales
- Si los errores son del cliente o del servicio
- El estado del servicio, como **Crítico**, **Revisión** y **Bueno**. Citrix ADM muestra el estado del servicio según el tiempo de respuesta del servicio y el recuento de errores.
  - **Crítico (rojo)**: Indica cuando el tiempo medio de respuesta del servicio es > 200 ms Y cuenta de errores > 0
  - **Revisión (naranja)**: Indica cuando el tiempo promedio de respuesta del servicio > 200 ms O cuenta de errores > 0
  - **Buena (verde)**: Indica que no hay errores y tiempo medio de respuesta del servicio < 200 ms
- El estado del cliente, como **Crítico**, **Revisión** y **Bueno**. Citrix ADM muestra el estado del cliente según la latencia de la red del cliente y el recuento de errores.
  - **Crítico (rojo)**: Indica cuando la latencia media de la red del cliente > 200 ms Y el número de errores > 0
  - **Revisión (naranja)**: Indica cuando la latencia media de la red del cliente > 200 ms O cuenta de errores > 0
  - **Buena (verde)**: Indica que no hay errores y latencia media de la red del cliente < 200 ms
- El estado del servidor virtual como **Crítico**, **Revisión** y **Bueno**. Citrix ADM muestra el estado del servidor virtual en función de la puntuación de la aplicación.
  - **Crítico (rojo)**: Indica cuando la puntuación de la aplicación es < 40
  - **Revisión (naranja)**: Indica cuando la puntuación de la aplicación está entre 40 y 75
  - **Bueno (verde)**: Indica cuando la puntuación de la aplicación es > 75

Puntos a tener en cuenta:

- En el gráfico de servicio solo se muestran los servidores virtuales de equilibrio de carga, conmutación de contenido y GSLB.
- Si ningún servidor virtual está enlazado a una aplicación personalizada, los detalles no se ven en el gráfico de servicio de la aplicación.
- Puede ver métricas para clientes y servicios en el gráfico de servicios solo si se producen transacciones activas entre servidores virtuales y aplicaciones web.
- Si no hay transacciones activas disponibles entre los servidores virtuales y la aplicación web, solo puede ver los detalles en el gráfico de servicio en función de los datos de configuración, como el equilibrio de carga, la conmutación de contenido, los servidores virtuales GSLB y los servicios.
- Las actualizaciones en la configuración de la aplicación pueden tardar 10 minutos en reflejarse en el gráfico de servicio.

Para obtener más información, consulte Gráfico de servicio para aplicaciones.



Para empezar, consulte la documentación de Service Graph.

Solución de problemas para los equipos Citrix ADC

Analicemos algunos de los atributos más comunes para solucionar problemas en la plataforma Citrix ADC y cómo estas técnicas de solución de problemas se aplican a las implementaciones de nivel 1 para topologías de microservicios.

Citrix ADC tiene una interfaz de línea de comandos (CLI) que muestra los comandos en tiempo real y es útil para determinar las configuraciones en tiempo de ejecución, la estática y la configuración de directivas. Esto se facilita mediante el comando **“SHOW”**.

SHOW: realizar operaciones CLI de ADC:

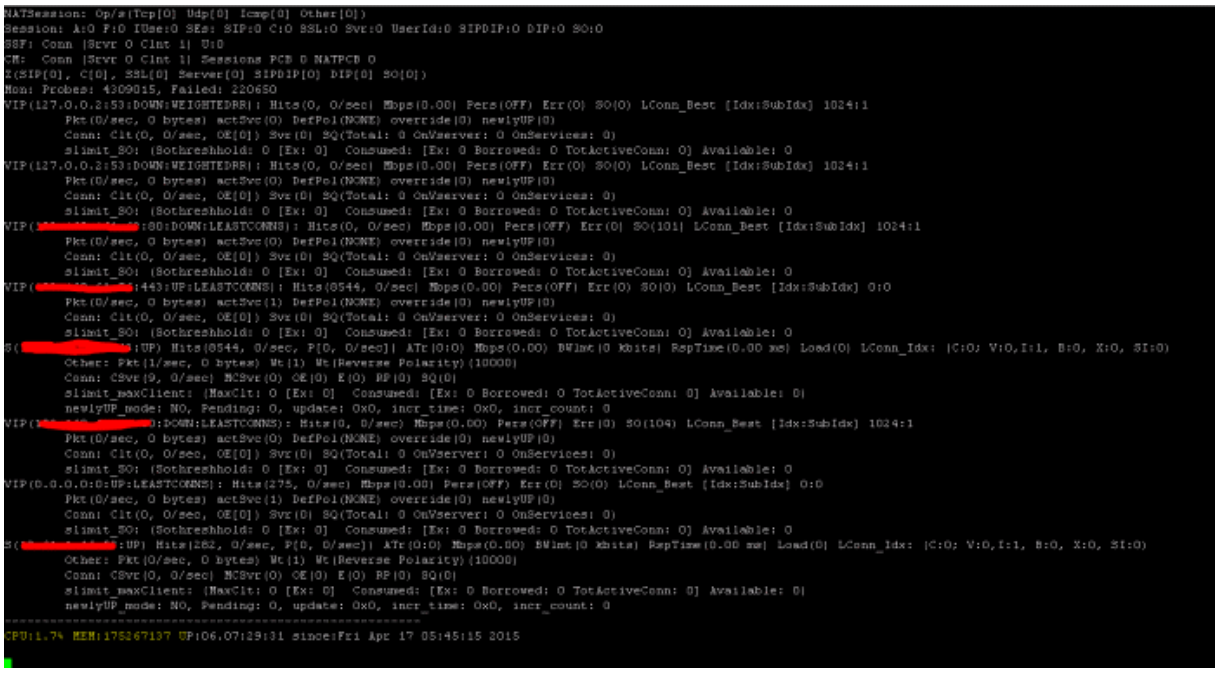

```
>Show running config (-summary -fullValues)

 Ability to search (grep command)
> “sh running config | -i grep vserver”

Check the version.
>Show license
   “sh license”
<!--NeedCopy-->
```

Mostrar estadísticas de SSL

```
>Sh ssl
        System
        Frontend
        Backend
        Encryption
<!--NeedCopy-->
```



Citrix ADC tiene un comando para enumerar las estadísticas de todos los objetos en función de un intervalo de contador de siete (7) segundos. Esto se facilita mediante el comando **“STAT”**.

Telemetría L3-L7 altamente granular de Citrix ADC

- Nivel del sistema: uso de CPU y memoria del ADC.
- Protocolo HTTP: #Requests /Responses, división GET/POST, errores HTTP para N-S y E-W (solo para service mesh lite, sidecar pronto).
- SSL: #Sessions y #Handshakes para tráfico N-S y E-W solo para service mesh lite.
- Protocolo IP: #Packets recibidos/enviados, #Bytes recibidos/enviados, paquetes #Truncated y búsqueda de direcciones #IP.
- Citrix ADC AAA: Sesiones #Active
- Interfaz: paquetes de multidifusión #Total, bytes transferidos #Total y paquetes #Jumbo recibidos/enviados.
- Servidor virtual de equilibrio de carga y servidor virtual de conmutación de contenido: #Packets, #Hits y #Bytes recibidos/enviados.

STAT: realice operaciones CLI de ADC:

```
1 >Statistics
2  “stat ssl”
3 <!--NeedCopy-->
```



```
> stat ns

System overview

Up since        Thu Apr 16 19:45:15 2015
Packet CPU usage (%)                1.60
Management CPU usage (%)            0.80
Memory usage (MB)                    165
InUse Memory (%)                   17.03
Last Transition time Th...015
System state                         UP
Master state                    Primary
# SSL cards UP                         0
# SSL cards present                    0

System Disks                   Used (%) Available
/flash Used (%)                       17      1168
/var Used (%)                         13     11246

Throughput Statistics                    Rate (/s)               Total
Megabits received                                2                288237
Megabits transmitted                             3                345685

TCP Connections                  Client   Server
All client connections              158      272
Established client connections      158      145

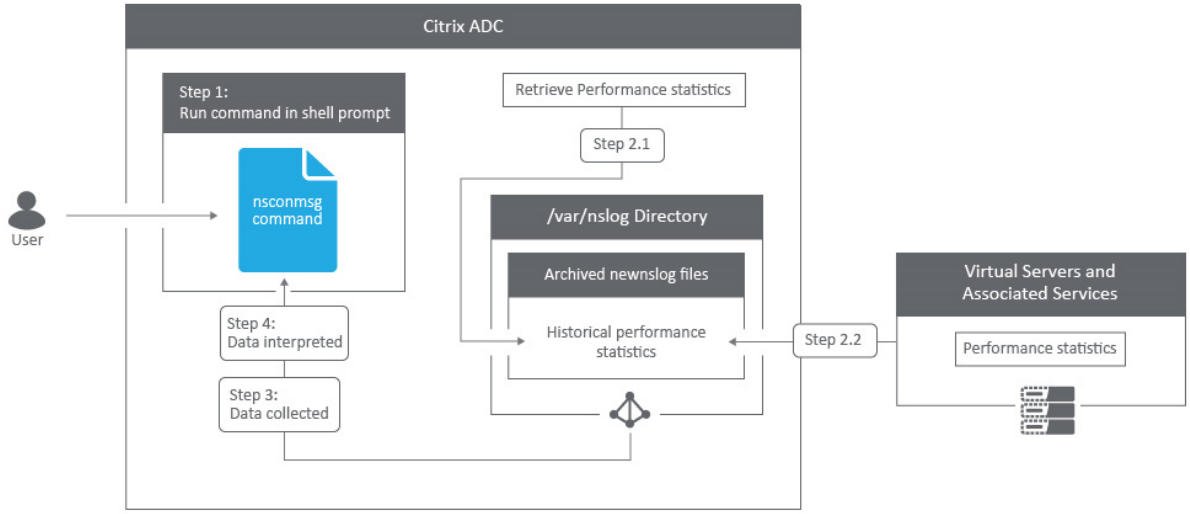
HTTP                                     Rate (/s)               Total
Total requests                                   0                191529
Total responses                                  0                263011
Request bytes received                        7007           1178810535
Response bytes received                     164477          12348432171

SSL                                      Rate (/s)               Total
```

Citrix ADC tiene una estructura de archivo de registros que permite buscar estadísticas y contadores al solucionar errores específicos mediante el comando **“NSCONMSG”**.

NSCONMSG - archivo de registro principal (formato de datos ns)

```
1     Cd/var/nslog
2
3      “Mac Moves”
4     nsconmsg -d current -g nic_err
5  <!--NeedCopy-->
```

Nstcpdump

Se puede utilizar `nstcpdump` para la solución de problemas de bajo nivel. `nstcpdump` recopila información menos detallada que `nstrace`. Abra la CLI de ADC y escriba `shell`. Puede usar filtros con `nstcpdump`, pero no puede usar filtros específicos para los recursos ADC. La salida del volcado se puede ver directamente en la pantalla de la CLI.

CTRL + C: Presione estas teclas simultáneamente para detener un `nstcpdump`.

`nstcpdump.sh dst host x.x.x.x` — Muestra el tráfico enviado al host de destino.

`nstcpdump.sh -n src host x.x.x.x` — Muestra el tráfico del host especificado y no convierte las direcciones IP en nombres (-n).

`nstcpdump.sh host x.x.x.x` — Muestra el tráfico hacia y desde la IP del host especificada.

![`nstcpdump` de ejemplo](/en-us/citrix-adc/media/nstcpdump.png)

NSTRACE: Archivo de seguimiento de paquetes

NSTRACE es una herramienta de depuración de paquetes de bajo nivel para solucionar problemas de redes. Le permite almacenar archivos de captura que puede analizar más a fondo con las herramientas del analizador. Dos herramientas comunes son Network Analyzer y Wireshark.

![El resultado de `nstrace`](/en-us/citrix-adc/media/nstrace.png)

```
> start nstrace -size 0
 Done
> stop nstrace
 Done
```

Una vez que se crea el archivo de captura NSTRACE en /var/nstrace en el ADC, puede importar el archivo de captura en Wireshark para la captura de paquetes y el análisis de red.

SYSCTL: Información detallada del ADC: descripción, modelo, plataforma, CPU, etc

```
    sysctl -a grep hw.physmem

    hw.physmem: 862306304
    netscaler.hw_physmem_mb: 822
<!--NeedCopy-->
```

aaad.debug: Abrir proceso para información de depuración de autenticación

```
process_radius Got RADIUS event
process_radius Received BAD_ACCESS_REJECT for: <username>
process_radius Sending reject.
send_reject_with_code Rejecting with error code 4001.
```

Para obtener más información sobre cómo solucionar problemas de autenticación a través de ADC o ADC Gateway con el módulo aaad.debug, consulte el artículo de asistencia de aaad.debug.

También existe la posibilidad de obtener estadísticas de rendimiento y registros de eventos directamente para el ADC. Para obtener más información al respecto, consulte el documento de asistencia de ADC.

Solución de problemas para los equipos de SRE

Flujos de tráfico de Kubernetes

Norte/sur:

- El tráfico norte/sur es el tráfico que fluye desde el usuario al clúster, a través de la entrada.

Este/oeste:

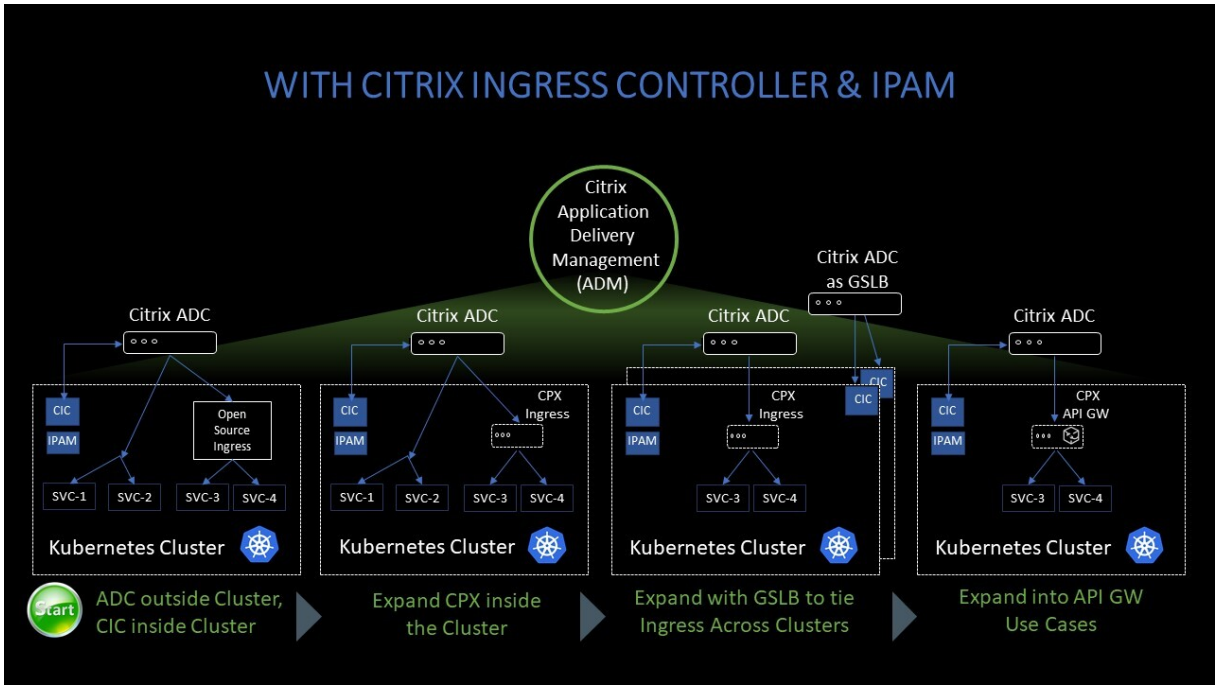
- El tráfico este/oeste es el tráfico que fluye por el clúster de Kubernetes: de servicio a servicio o de servicio a almacén de datos.

Cómo la carga de Citrix ADC CPX equilibra el flujo de tráfico de este a oeste en un entorno de Kubernetes

Después de implementar el clúster de Kubernetes, debe integrar el clúster con ADM proporcionando los detalles del entorno de Kubernetes en ADM. ADM supervisa los cambios en los recursos de Kubernetes, como los servicios, los puntos finales y las reglas de entrada.

Cuando implementa una instancia de ADC CPX en el clúster de Kubernetes, se registra automáticamente en ADM. Como parte del proceso de registro, ADM aprende sobre la dirección IP de la instancia CPX y el puerto en el que puede llegar a la instancia para configurarla mediante las API REST de NITRO.

En esta ilustración se muestra cómo la carga de ADC CPX equilibra el flujo de tráfico de este a oeste en un clúster de Kubernetes.



En este ejemplo,

El nodo 1 y el nodo 2 de los clústeres de Kubernetes contienen instancias de un servicio front-end y un servicio back-end. Cuando las instancias de ADC CPX se implementan en el nodo 1 y el nodo 2, las instancias de ADC CPX se registran automáticamente en ADM. Debe integrar manualmente el clúster de Kubernetes con ADM configurando los detalles del clúster de Kubernetes en ADM.

Cuando un cliente solicita el servicio front-end, la carga de recursos de entrada equilibra la solicitud entre las instancias del servicio front-end en los dos nodos. Cuando una instancia del servicio de front-end necesita información de los servicios de back-end en el clúster, dirige las solicitudes a la instancia de ADC CPX en su nodo. La carga de la instancia CPX de ADC equilibra las solicitudes entre los servicios de back-end del clúster, lo que proporciona un flujo de tráfico de este a oeste.

Gráfico de servicio ADM para aplicaciones

La función de gráfico de servicio de Citrix ADM permite supervisar todos los servicios de una representación gráfica. Esta función también proporciona un análisis detallado y métricas útiles. Puede ver gráficos de servicios para:

- Aplicaciones configuradas en todas las instancias de Citrix ADC
- Aplicaciones Kubernetes
- Aplicaciones web de 3 niveles

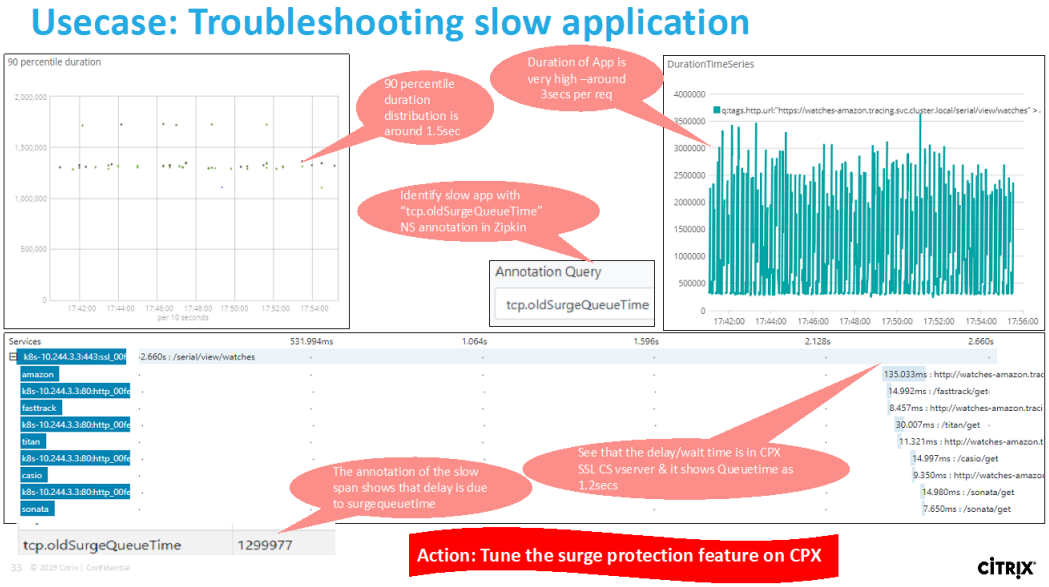
Para empezar, consulte los detalles en el gráfico de servicios.

Ver contadores de aplicaciones de microservicios

El gráfico de servicio también muestra todas las aplicaciones de microservicios que pertenecen a los clústeres de Kubernetes. Sin embargo, el puntero del mouse en un servicio para ver los detalles de las métricas.

Podrá ver lo siguiente:

- El nombre del servicio
- El protocolo utilizado por el servicio como SSL, HTTP, TCP, SSL sobre HTTP
- **Hits**: El número total de hits recibidos por el servicio
- **Tiempo de respuesta del servicio**: El tiempo medio de respuesta tomado del servicio. (Tiempo de respuesta = cliente RTT + petición último byte: Solicitud primer byte)
- **Errores**: El total de errores como 4xx, 5xx, etc.
- **Volumen de datos**: Volumen total de datos procesados por el servicio
- **Espacio de nombres**: El espacio de nombres del servicio
- **Nombre del clúster: Nombre** del clúster en el que está alojado el servicio
- **Errores del servidor SSL**: El total de errores SSL del servicio



Estos contadores y registros de transacciones específicos se pueden extraer a través de Citrix Observability Exporter (COE) mediante una variedad de puntos finales compatibles. Para obtener más información sobre el COE, consulte las siguientes secciones.

Exportador de estadísticas de Citrix ADC

Se trata de un servidor sencillo que extrae las estadísticas de Citrix ADC y las exporta a través de HTTP a Prometheus. Luego, Prometheus se puede agregar como fuente de datos a Grafana para ver las estadísticas de Citrix ADC de forma gráfica.

Para supervisar las estadísticas y los contadores de las instancias de Citrix ADC, `citrix-adc-metric-exporter` se puede ejecutar como contenedor o script. El exportador recopila estadísticas de Citrix ADC, como el total de visitas a un servidor virtual, la tasa de solicitudes HTTP, la tasa de cifrado y descifrado SSL, etc., de las instancias de Citrix ADC y las retiene hasta que el servidor Prometheus extrae las estadísticas y las almacena con una marca de tiempo. A continuación, se puede apuntar a Grafana al servidor Prometheus para obtener las estadísticas, trazarlas, establecer alarmas, crear mapas de calor, generar tablas, etc., según sea necesario para analizar las estadísticas de Citrix ADC.

En estas secciones se proporcionan detalles sobre la configuración del exportador para que trabaje en un entorno como se indica en la ilustración. También se explica una nota sobre qué entidades/métricas de Citrix ADC extrae el exportador de forma predeterminada y cómo modificarlas.

Para obtener más información sobre Exporter for Citrix ADC, consulte el GitHub de Metrics Exporter.

Rastreo distribuido del servicio ADM

En el gráfico de servicio, puede utilizar la vista de rastreo distribuido para:

- Analice el rendimiento general del servicio.
- Visualice el flujo de comunicación entre el servicio seleccionado y sus servicios interdependientes.
- Identificar qué servicio indica errores y solucionar el servicio erróneo
- Permite ver los detalles de las transacciones entre el servicio seleccionado y cada servicio interdependiente.

Requisitos previos para el seguimiento distribuido de ADM

Para ver la información de seguimiento del servicio, debe:

- Asegúrese de que una aplicación mantenga los siguientes encabezados de seguimiento, mientras envía cualquier tráfico este-oeste:

- `x-request-id`
- `x-b3-traceid`
- `x-b3-spanid`
- `x-b3-parentspanid`
- `x-b3-sampled`
- `x-b3-flags`
- `x-ot-span-context`

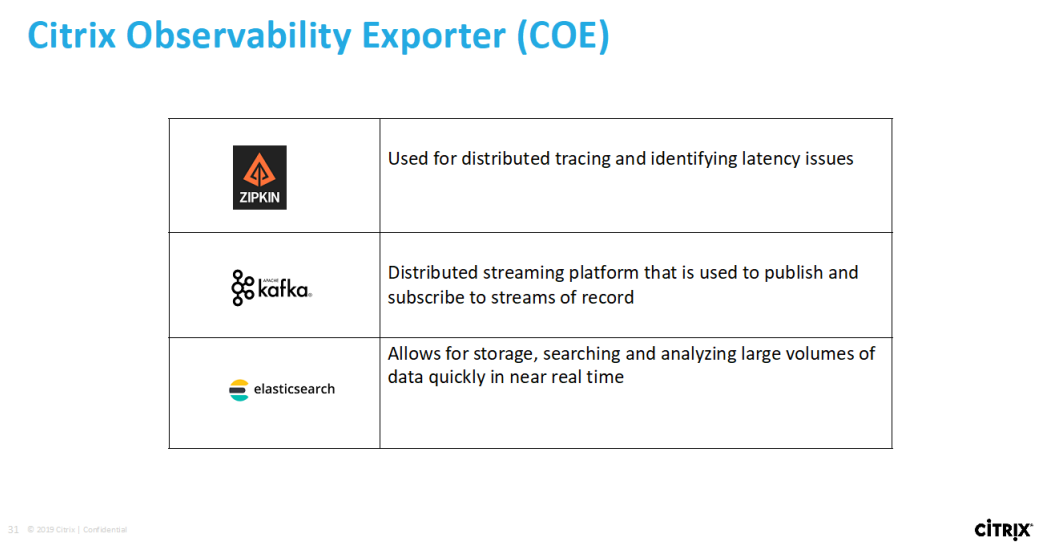
- Actualice el archivo YAML CPX con NS_DISTRIBUTED_TRACING y el valor YES.
  Para empezar, consulte Rastreo distribuido.

Análisis de Citrix ADC Observability Exporter (COE)

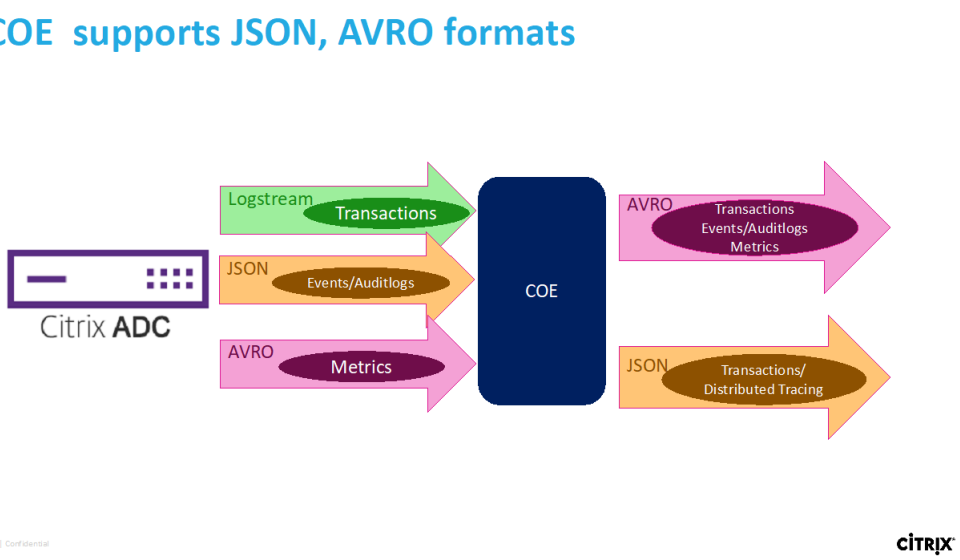
Citrix Observability Exporter es un contenedor que recopila métricas y transacciones de Citrix ADC y las transforma a formatos adecuados (como JSON, AVRO) para los puntos finales compatibles. Puede exportar los datos recopilados por Citrix Observability Exporter al punto final deseado. Al analizar los datos exportados al punto final, puede obtener información valiosa a nivel de microservicios para las aplicaciones proxy de Citrix ADC.

Para obtener más información sobre el COE, consulta el COE GitHub.

COE con Elasticsearch como punto final de la transacción



Cuando se especifica Elasticsearch como el punto de enlace de la transacción, Citrix Observability Exporter convierte los datos a formato JSON. En el servidor de Elasticsearch, Citrix Observability Exporter crea índices de Elasticsearch para cada ADC cada hora. Estos índices se basan en los datos, la hora, el UUID del ADC y el tipo de datos HTTP (http_event o http_error). A continuación, Citrix Observability Exporter carga los datos en formato JSON en índices de búsqueda elástica para cada ADC. Todas las transacciones regulares se colocan en el índice http_event y cualquier anomalía se coloca en el índice http_error.



Función de rastreo distribuido con Zipkin

En una arquitectura de microservicios, una solicitud de un solo usuario final puede abarcar varios microservicios, lo que dificulta el seguimiento de una transacción y la corrección de las fuentes de errores. En tales casos, las formas tradicionales de supervisión del rendimiento no pueden identificar con precisión dónde ocurren las fallas y cuál es la razón detrás de un rendimiento deficiente. Necesita una forma de capturar puntos de datos específicos para cada microservicio que gestiona una solicitud y analizarlos para obtener información valiosa.

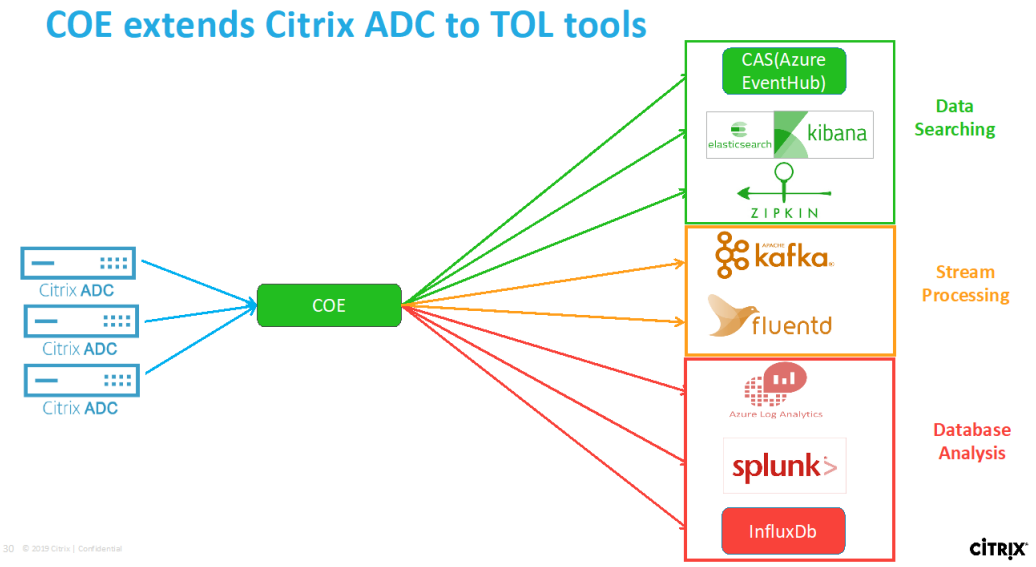
El rastreo distribuido aborda este desafío al proporcionar una forma de rastrear una transacción de extremo a extremo y comprender cómo se maneja en varios microservicios.

OpenTracing es una especificación y un conjunto estándar de API para diseñar e implementar el rastreo distribuido. Los trazadores distribuidos le permiten visualizar el flujo de datos entre sus microservicios y le ayudan a identificar los cuellos de botella en su arquitectura de microservicios.

Citrix ADC Observability Exporter implementa el seguimiento distribuido para Citrix ADC y actualmente admite Zipkin como rastreador distribuido.

Actualmente, puede supervisar el rendimiento a nivel de aplicación mediante Citrix ADC. Con Citrix Observability Exporter con Citrix ADC, puede obtener datos de seguimiento para microservicios de cada aplicación proxy por su Citrix ADC CPX, MPX o VPX.

Para empezar, consulta el Exportador de observabilidad de GitHub.

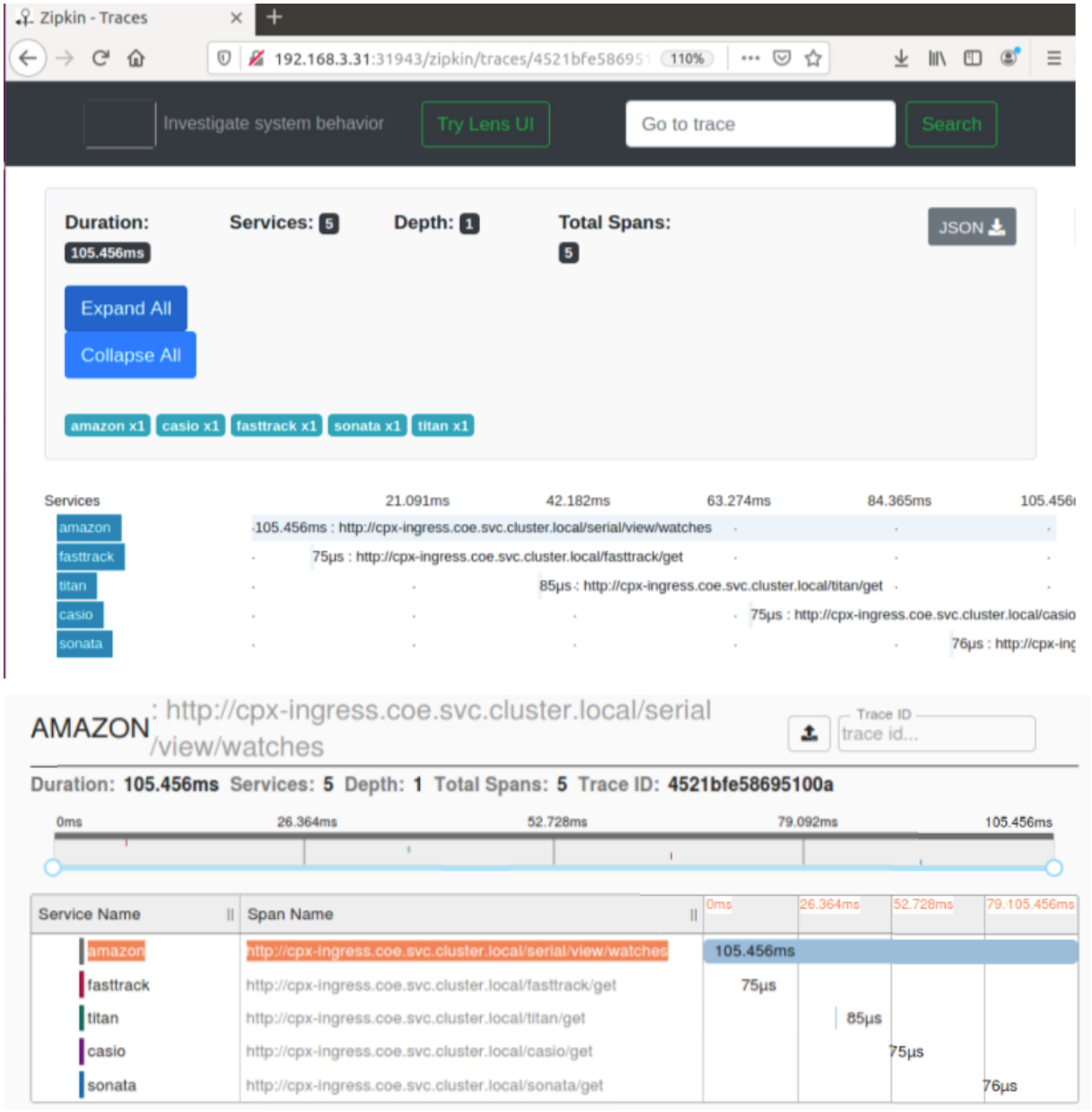


Zipkin para depuración de aplicaciones

Zipkin es un sistema de rastreo distribuido de código abierto basado en el documento de Dapper de Google. Dapper es el sistema de Google para su sistema de rastreo distribuido en producción. Google explica esto en su artículo: "Creamos Dapper para proporcionar a los desarrolladores de Google más información sobre el comportamiento de los sistemas distribuidos complejos". Observar el sistema desde diferentes ángulos es fundamental a la hora de solucionar problemas, especialmente cuando un sistema es complejo y está distribuido.

Los siguientes datos de rastreo de Zipkin identifican un total de 5 intervalos y 5 servicios relacionados con la aplicación de muestra Watches. Los datos de seguimiento muestran los datos de extensión específicos en los 5 microservicios.

Para empezar, consulte Zipkin.



Ejemplo de intervalo de Zipkin que muestra la latencia de la aplicación para la solicitud de carga

Services: amazon

Date Time	Relative Time	Annotation	Address
7/15/2020, 2:14:24 PM		Server Start	10.10.235.179:1719 (amazon)
7/15/2020, 2:14:24 PM	105.456ms	Server Finish	10.10.235.179:1719 (amazon)

Key	Value
component	py_zipkin
http.host	amazon:1719
http.method	GET
http.path	/serial/view/watches
http.url	http://cpx-ingress.coe.svc.cluster.local/serial/view/watches
Local Component	amazon
peer.address	10.10.235.190

Kibana para ver datos

Kibana es una interfaz de usuario abierta que le permite visualizar sus datos de Elasticsearch y navegar por Elastic Stack. Puede hacer lo que quiera, desde hacer un seguimiento de la carga de las consultas hasta comprender la forma en que las solicitudes fluyen

Tanto si es analista como administrador, Kibana hace que sus datos sean procesables al proporcionar las siguientes tres funciones clave:

- **Una plataforma de análisis y visualización de código abierto.** Use Kibana para explorar sus datos de Elasticsearch y, a continuación, crear visualizaciones y paneles atractivos.
- **Una interfaz de usuario para administrar Elastic Stack.** Administre su configuración de seguridad, asigne funciones de usuario, tome instantáneas, acumule sus datos y mucho más, todo desde la comodidad de una interfaz de usuario de Kibana.

- **Un centro centralizado para las soluciones de Elastic.** Desde análisis de registros hasta descubrimiento de documentos y SIEM, Kibana es el portal para acceder a estas y otras capacidades.

Kibana está diseñado para usar Elasticsearch como fuente de datos. Piense en Elasticsearch como el motor que almacena y procesa los datos, con Kibana en la cima.

En la página principal, Kibana proporciona estas opciones para agregar datos:

- Importe datos mediante el visualizador de datos de archivo.
- Configura un flujo de datos a Elasticsearch con nuestros tutoriales integrados. Si no existe un tutorial para sus datos, vaya a Descripción general de Beats para obtener información sobre otros remitentes de datos de la familia Beats.
- Agregue un conjunto de datos de muestra y lleve a Kibana a probarlo sin cargar los datos usted mismo.
- Indexe sus datos en Elasticsearch con las API REST o lasbibliotecas cliente.

Kibana usa un patrón de índice para indicarle qué índices de Elasticsearch explorar. Si carga un archivo, ejecuta un tutorial incorporado o agrega datos de muestra, obtiene un patrón de índice de forma gratuita y es bueno comenzar a explorar. Si carga sus propios datos, puede crear un patrón de índice en Stack Management.

Paso 1: Configurar el patrón de índice para Logstash

Paso 2: Seleccione el índice y genere tráfico para rellenar.

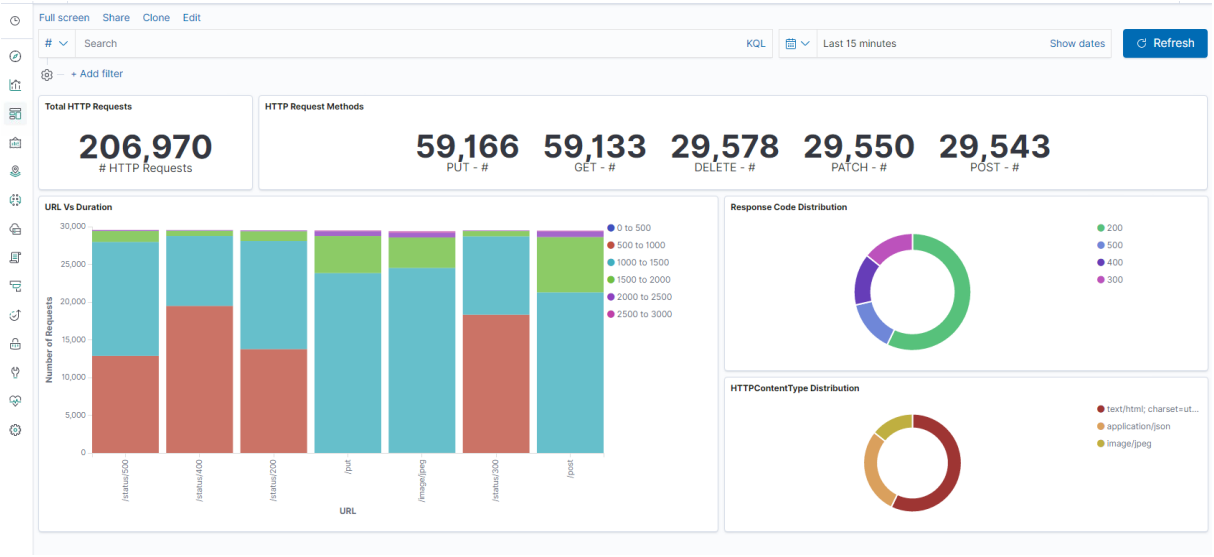
Paso 3: generar la aplicación a partir de los datos no estructurados de las fuentes de registro.

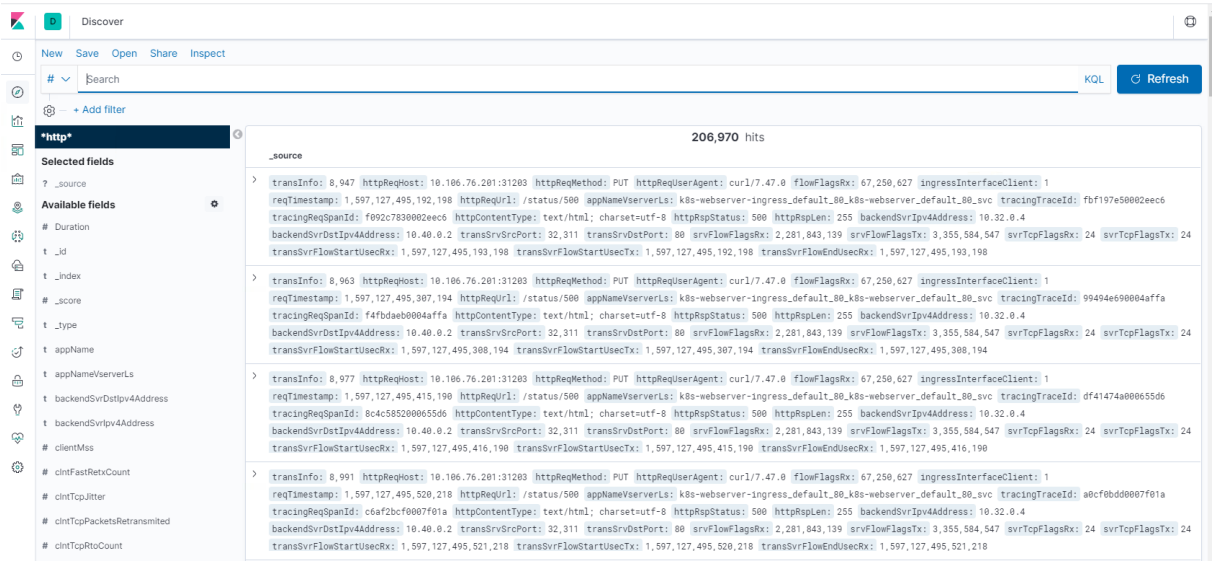
Paso 4: Kibana formatea la entrada de Logstash para crear informes y paneles.

- Intervalo de tiempo
- Vista tabular
- Los recuentos de resultados se basan en la aplicación.
  - Hora IP, agente, Machine.OS, código de respuesta (200), URL
  - Filtrar por valores

Paso 5: Visualice los datos en un informe de agregaciones.

- Agregación de resultados en un informe de gráficos (circular, gráfico, etc.)





Implementar una instancia de Citrix ADC VPX

January 31, 2022

> **Nota**
>
> Citrix ADM Service connect se habilita de forma predeterminada, después de instalar o actualizar Citrix ADC o Citrix Gateway a la versión 13.0 compilación 61.xx y superior. Para obtener más información, consulte Administración de datos y conexión del servicio Citrix ADM.

El producto Citrix ADC VPX es un dispositivo virtual que se puede alojar en una amplia variedad de plataformas de virtualización y nube:

- Citrix Hypervisor
- VMware ESX
- Microsoft Hyper-V
- Linux KVM
- Amazon Web Services
- Microsoft Azure
- Google Cloud Platform

Para obtener más información, consulte la hoja de datos de Citrix ADC VPX.

Para obtener más información sobre el aprovisionamiento de una instancia Citrix ADC VPX en un dispositivo SDX, consulte Aprovisionamiento de instancias Citrix ADC.

Citrix Application Delivery Management para Citrix ADC VPX

El software Citrix Application Delivery Management es una solución de administración centralizada que simplifica las operaciones al proporcionar a los administradores visibilidad en toda la empresa y automatizar los trabajos de administración que deben ejecutarse en varias instancias.

Puede administrar y supervisar instancias Citrix ADC VPX además de otros productos de redes de aplicaciones de Citrix, como Citrix Gateway, Citrix ADC SDX, Citrix ADC CPX y Citrix SD-WAN. Puede utilizar el software de administración de entrega de aplicaciones para administrar, supervisar y solucionar problemas de toda la infraestructura de entrega de aplicaciones global desde una única consola unificada.

Para obtener más información, consulte la documentación de Citrix Application Delivery Management.

Tabla de compatibilidad y pautas de uso

August 11, 2022

En este documento se enumeran los diferentes hipervisores y funciones admitidos en una instancia de Citrix ADC VPX. El documento también describe sus pautas de uso y las limitaciones conocidas.

Tabla 1. Instancia VPX en Citrix Hypervisor

Versión de Citrix Hypervisor	SysID	Modelos VPX
8.2 era compatible con 13.0 64.x y versiones posteriores, 8.0, 7.6, 7.1	450000	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10 G, VPX 15 G, VPX 25 G, VPX 40 G

Tabla 2. Instancia VPX en hipervisor VMware ESXi

Versión ESX	Fecha de lanzamiento de ESX (AAAA/M-M/DD)	Número de compilación de ESX	Versión de Citrix ADC VPX	SysID	Modelos VPX
Actualización 3D de ESXi 7.0	03/29/2022	19482537	A partir de 13.1-27.x	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
Actualización 3c de ESXi 7.0	2022/01/27	19193900	13.1-21.x en adelante	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G

Versión ESX	Fecha de lanzamiento de ESX (AAAA/M-M/DD)	Número de compilación de ESX	Versión de Citrix ADC VPX	SysID	Modelos VPX
Actualización 2d de ESX 7.0	2021/09/14	18538813	13.1-9.x en adelante	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
Actualización 2a de ESX 7.0	2021/04/29	17867351	13.1-4.x en adelante	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
Actualización 1d de ESX 7.0	2021/02/02	17551050	13.0-82.x en adelante	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G

Versión ESX	Fecha de lanzamiento de ESX (AAAA/M-M/DD)	Número de compilación de ESX	Versión de Citrix ADC VPX	SysID	Modelos VPX
Actualización 1c de ESX 7.0	2020/12/17	17325551	13.0-79.x en adelante	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
Actualización 1b de ESX 7.0	2020/10/06	16850804	13.0-76.x en adelante	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
ESXi 7.0b	2020/06/23	16324942	13.0-71.x en adelante	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G

Versión ESX	Fecha de lanzamiento de ESX (AAAA/M-M/DD)	Número de compilación de ESX	Versión de Citrix ADC VPX	SysID	Modelos VPX
ESXi 7.0 GA	2020/04/02	15843807	13.0-71.x en adelante	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
ESXi 6.7 P04	2020/11/19	17167734	A partir de 13.0-67.x	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
ESXi 6.7 P03	2020/08/20	16713306	A partir de 13.0-67.x	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G

Versión ESX	Fecha de lanzamiento de ESX (AAAA/M-M/DD)	Número de compilación de ESX	Versión de Citrix ADC VPX	SysID	Modelos VPX
ESXi 6.7 P02	2020/04/28	16075168	A partir de 13.0-67.x	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
ESXi 6.7 P01	2019/12/05	15160138	A partir de 13.0-67.x	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
ESXi 6.7 Actualización 3	2019/08/20	14320388	13.0-58.x en adelante	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G

Versión ESX	Fecha de lanzamiento de ESX (AAAA/M-M/DD)	Número de compilación de ESX	Versión de Citrix ADC VPX	SysID	Modelos VPX
ESXi 6.7 U2	2019/04/11	13006603	13.0-47.x en adelante	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
ESXi 6.5 GA	2016/11/15	4564106	13.0-47.x en adelante	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
ESXi 6.5 U1g	2018/3/20	7967591	13.0 47.x en adelante	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G

Versión ESX	Fecha de lanzamiento de ESX (AAAA/M-M/DD)	Número de compilación de ESX	Versión de Citrix ADC VPX	SysID	Modelos VPX
Actualización 3 de ESXi 6.0	2017/2/24	5050593	12.0-51.x en adelante	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
Parche 11 de ESXi 6.0 Express	2017/10/5	6765062	12.0-56.x en adelante	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G

Tabla 3. VPX en Microsoft Hyper-V

Versión Hyper-V	SysID	Modelos VPX
2012, 2012 R2, 2016, 2019	450020	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000

Tabla 4. Instancia VPX en KVM genérico

Versión KVM genérica	SysID	Modelos VPX
RHEL 7.4, RHEL 7.5 (a partir de la versión 12.1 50.x de Citrix ADC), RHEL 7.6, RHEL 8.0, Ubuntu 16.04, Ubuntu 18.04, RHV 4.2	450070	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10 G, VPX 15 G. VPX 25G, VPX 40G, VPX 100G

Puntos a tener en cuenta:

Tenga en cuenta los siguientes puntos al utilizar hipervisores KVM.

- La instancia VPX está calificada para las versiones de versión de Hypervisor mencionadas en la tabla 1—4, y no para las versiones de parche de una versión. Sin embargo, se espera que la instancia VPX funcione sin problemas con las versiones de parches de una versión compatible. Si no es así, registre un caso de asistencia para solucionar problemas y depurar.
- Antes de utilizar RHEL 7.6, siga los pasos siguientes en el host KVM:
  1. Modifique /etc/default/grub y agregue ”kvm_intel.preemption_timer=0” a la variable GRUB_CMDLINE_LINUX.
  2. Vuelva a generar grub.cfg con el comando ”## grub2-mkconfig -o /boot/grub2/grub.cfg”.
  3. Reinicie el equipo host.
- Antes de utilizar Ubuntu 18.04, siga los pasos siguientes en el host KVM:
  1. Modifique /etc/default/grub y agregue ”kvm_intel.preemption_timer=0” a la variable GRUB_CMDLINE_LINUX.
  2. Vuelva a generar grub.cfg con el comando ”## grub-mkconfig -o /boot/grub/grub.cfg “.
  3. Reinicie el equipo host.

Tabla 5. Instancia VPX en AWS

Versión AWS	SysID	Modelos VPX
N/D	450040	VPX 10, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX BYOL, VPX 8000, VPX 10G, VPX 15G y VPX 25G solo están disponibles con BYOL con tipos de instancia EC2 (C5, M5 y C5n)

> Nota:
>
> La oferta VPX 25G no ofrece el rendimiento deseado de 25 G en AWS, pero puede ofrecer una tasa de transacciones SSL más alta en comparación con la oferta VPX 15G.

Tabla 6. Instancia VPX en Azure

Versión Azure	SysID	Modelos VPX
N/D	450020	VPX 10, VPX 200, VPX 1000, VPX 3000, VPX BYOL

Tabla 7. Tabla de funciones VPX

	VPX on XenServer		VPX on VMware ESX				VPX on Microsoft Hyper-V	VPX on generic KVM			VPX on AWS	VPX on Azure	VPX on GCP
Features	**PV**	**SR-IOV**	**PV**	**SR-IOV**	**Emulated**	**PCI Passthrough**	**PV**	**PV**	**SR-IOV**	**PCI Passthrough**			
Multi-PE Support	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Clustering Support	Yes	Yes[1]	Yes	Yes[1]	Yes	Yes	Yes	Yes	Yes[1]	Yes	No	No	No
VLAN Tagging	Yes	Yes	Yes	Yes	Yes	Yes	Yes (only on 2012R2)	Yes	Yes	Yes	No	No	No
Detecting Link Events	No[2]	Yes[3]	No[2]	Yes[3]	No[2]	Yes[3]	No[2]	No[2]	Yes[3]	Yes[3]	No[2]	No[2]	No[2]
Interface Parameter Configuration	No	No	No	No	No	Yes	No	No	No	Yes	No	No	No
Static LA	Yes[2]	Yes[3]	Yes[2]	No	Yes[2]	Yes[3]	Yes[2]	Yes[2]	Yes[3]	Yes[3]	No	No	No
LACP	No	Yes[3]	Yes[2]	No	Yes[2]	Yes[3]	No	Yes[2]	Yes[3]	Yes[3]	No	No	No
Static CLAG	No	No	No	No	No	No	No	No	No	No	No	No	No
LACP CLAG	No	No	Yes[2]	No	Yes[2]	Yes[3]	No	Yes[2]	Yes[3]	Yes[3]	No	No	No
Hot-plug	No	No	No	No	No	No	No	No	No	No	Yes	No	No

Los números en superíndice (1, 2, 3) utilizados en la tabla anterior se refieren a los siguientes puntos con la numeración respectiva:

1. La compatibilidad con clústeres está disponible en SRIOV para las interfaces orientadas al cliente y al servidor, y no para el plano posterior.
2. Los eventos de interfaz DOWN no se registran en instancias de Citrix ADC VPX.
3. Para LA estática, es posible que aún se envíe tráfico en la interfaz cuyo estado físico sea DOWN.
4. Para LACP, el dispositivo del mismo nivel conoce el evento DOWN de la interfaz basado en el mecanismo de tiempo de espera de LACP.
    - Tiempo de espera corto: 3 segundos
    - Tiempo de espera prolongado: 90 segundos
5. En el caso de LACP, no comparta interfaces entre máquinas virtuales.
6. Para la redirección dinámica, el tiempo de convergencia depende del Protocolo de redirección, ya que no se detectan eventos de vínculo.
7. La funcionalidad Ruta estática supervisada falla si no vincula monitores a rutas estáticas porque el estado de la ruta depende del estado de la VLAN. El estado de la VLAN depende del estado del vínculo.
8. La detección de fallos parciales no se produce en alta disponibilidad si se produce un error de enlace. Una afección cerebral dividida de alta disponibilidad podría ocurrir si se produce un fallo de enlace.
    - Cuando se genera cualquier evento de enlace (desactivar/habilitar, restablecer) desde una instancia VPX, el estado físico del enlace no cambia. Para LA estática, cualquier tráfico iniciado por el par se elimina en la instancia.
    - Para que funcione la función de etiquetado de VLAN, haga lo siguiente:

    En VMware ESX, establezca el ID de VLAN del grupo de puertos en 1-4095 en el vSwitch del servidor VMware ESX. Para obtener más información sobre la configuración de un ID de VLAN en el vSwitch del servidor VMware ESX, consulte Soluciones VLAN VMware ESX Server 3 802.1Q.

Tabla 8. Exploradores web compatibles

Sistema operativo	Explorador y versiones
Windows 7	Internet Explorer: 8, 9, 10 y 11; Mozilla Firefox 3.6.25 y superior; Google Chrome: 15 y superior
Windows de 64 bits	Internet Explorer: 8, 9; Google Chrome: 15 y superior
MAC	Mozilla Firefox - 12 y superior; Safari - 5.1.3; Google Chrome: 15 y superior

Directrices de uso

Siga estas pautas de uso:

Consulte la sección **Consideraciones sobre la CPU de VMware ESXi** en el documento Prácticas recomendadas de rendimiento para VMware vSphere 6.5. Aquí hay un extracto:

- No se recomienda que las máquinas virtuales con una demanda elevada de CPU o memoria se sitúen en un host o clúster que está sobrecomprometido.
- En la mayoría de los entornos, ESXi permite niveles significativos de compromiso excesivo de CPU sin afectar el rendimiento de la máquina virtual. En un host, puede ejecutar más vCPU que el número total de núcleos de procesador físicos de ese host.
- Si un host ESXi se satura de la CPU, es decir, las máquinas virtuales y otras cargas del host exigen todos los recursos de CPU que tiene el host, las cargas de trabajo sensibles a la latencia podrían no funcionar bien. En este caso, es posible que quiera reducir la carga de la CPU, por ejemplo apagando algunas máquinas virtuales o migrándolas a un host diferente (o permitiendo que DRS las migre automáticamente).
- Citrix recomienda la última versión de compatibilidad de hardware para aprovechar los conjuntos de funciones más recientes del hipervisor ESXi para la máquina virtual. Para obtener más información sobre la compatibilidad de hardware y versiones de ESXi, consulte la documentación de VMware.
- Citrix ADC VPX es un dispositivo virtual de alto rendimiento y sensible a la latencia. Para ofrecer el rendimiento esperado, el dispositivo requiere reserva de vCPU, reserva de memoria y fijación de vCPU en el host. Además, el hipersubproceso debe estar inhabilitado en el host. Si el host no cumple estos requisitos, se producen problemas como conmutación por error de alta disponibilidad, picos de CPU dentro de la instancia VPX, lentitud en el acceso a la CLI VPX, fallo del demonio de pit boss, caídas de paquetes y bajo rendimiento.

Un Hypervisor se considera sobreaprovisionado si se cumple una de las dos condiciones siguientes:

- El número total de núcleos virtuales (vCPU) aprovisionados en el host es mayor que el número total de núcleos físicos (pCPU).
- El número total de máquinas virtuales aprovisionadas consume más VCPU que el número total de pCPU.

  Si una instancia está sobreaprovisionada, es posible que el hipervisor no garantice los recursos reservados (como CPU, memoria y otros) para la instancia debido a los gastos generales de programación del hipervisor, errores o limitaciones con el hipervisor. Este comportamiento puede provocar la falta de recursos de CPU para Citrix ADC y puede provocar los problemas mencionados en el primer punto de **las Directrices de uso**. Como administradores, se recomienda reducir el alquiler en el host para que el número total de vCPU aprovisionadas en el host sea menor o igual al número total de pCPU.

Ejemplo

En el caso del hipervisor ESX, si el parámetro `%RDY%` de una vCPU VPX es mayor que 0 en el resultado del comando `esxtop`, se dice que el host ESX tiene gastos generales de programación, lo que puede causar problemas relacionados con la latencia en la instancia VPX.

En tal situación, reduzca la tenencia en el host para que siempre `%RDY%` vuelva a 0. También puede ponerse en contacto con el proveedor del hipervisor para seleccionar el motivo por el que no se ha respetado la reserva de recursos realizada.

- La adición en caliente solo se admite en las interfaces PV y SRIOV con Citrix ADC en AWS. Las instancias VPX con interfaces ENA no admiten conexión en marcha y el comportamiento de las instancias puede ser impredecible si se intenta conectar en caliente.
- La eliminación en caliente a través de la consola web de AWS o la interfaz CLI de AWS no se admite con las interfaces PV, SRIOV y ENA para Citrix ADC. El comportamiento de las instancias puede ser impredecible si se intenta eliminar en caliente.

Comandos para controlar el uso de la CPU del motor de paquetes

Puede utilizar dos comandos (`set ns vpxparam` y `show ns vpxparam`) para controlar el comportamiento de uso de CPU del motor de paquetes (no administrativo) de las instancias VPX en entornos de hipervisor y nube:

- `set ns vpxparam [-cpuyield (YES | NO | DEFAULT)] [-masterclockcpu1 (YES | NO)]`

  Permitir que cada máquina virtual utilice recursos de CPU que se hayan asignado a otra máquina virtual pero que no se estén usando.

  `Set ns vpxparam` parámetros:

  -cpuyield: Libere o no libere recursos de CPU asignados pero no utilizados.

  - **SÍ**: Permitir que otra máquina virtual utilice recursos de CPU asignados pero no utilizados.
  - **NO**: Reserve todos los recursos de CPU para la máquina virtual a la que se han asignado. Esta opción muestra un porcentaje más alto en entornos de hipervisores y nube para el uso de CPU VPX.
  - **PREDETERMINADO**: No.

  > **Nota**
  >
  > En todas las plataformas Citrix ADC VPX, el uso de vCPU en el sistema host es del 100 por ciento. Escriba el comando `set ns vpxparam -cpuyield YES` para anular este uso.

  Si quiere configurar los nodos de clúster en “yield”, debe realizar las siguientes configuraciones adicionales en CCO:

  - Si se forma un clúster, todos los nodos aparecen con “yield=Default”.
  - Si se forma un clúster mediante los nodos que ya están configurados en “Yield=yes”, los nodos se agregan al clúster mediante el rendimiento “DEFAULT”.

> Nota:
>
> Si quiere establecer los nodos del clúster en “Yield=Sí”, puede configurarlos solo después de formar el clúster, pero no antes de que se forme el clúster.

-masterclockcpu1: Puede mover la fuente de reloj principal de la CPU0 (CPU de administración) a la CPU1. Este parámetro tiene las siguientes opciones:

  - **SÍ**: Permita que la VM mueva la fuente de reloj principal de la CPU0 a la CPU1.
  - **NO**: La máquina virtual utiliza CPU0 para la fuente de reloj principal. De forma predeterminada, CPU0 es la principal fuente de reloj.

- `show ns vpxparam`

  Muestra los parámetros de `vpxparam` actuales.

Otras referencias

- Para obtener productos Citrix Ready, visite Citrix Ready Marketplace.
- Para obtener asistencia sobre los productos Citrix Ready, consulte la página de preguntas frecuentes.
- Para ver las versiones de hardware de VMware ESX, consulte Actualización de VMware Tools.

Optimice el rendimiento de Citrix ADC VPX en VMware ESX, Linux KVM y Citrix Hypervisors

October 5, 2021

El rendimiento de Citrix ADC VPX varía en gran medida según el hipervisor, los recursos del sistema asignados y las configuraciones del host. Para lograr el rendimiento deseado, primero siga las recomendaciones de la hoja de datos de VPX y, a continuación, optimice aún más mediante las prácticas recomendadas que se proporcionan en este documento.

Instancia Citrix ADC VPX en hipervisores VMware ESX

Esta sección contiene detalles sobre las opciones y los ajustes configurables y otras sugerencias que le ayudan a lograr un rendimiento óptimo de la instancia Citrix ADC VPX en hipervisores VMware ESX.

Configuración recomendada en hosts ESX

Para lograr un alto rendimiento para VPX con interfaces de red de paso E1000, VMXNET3, SR-IOV y PCI, siga estas recomendaciones:

- El número total de CPU virtuales (vCPU) aprovisionadas en el host ESX debe ser inferior o igual al número total de CPU físicas (PCPU) del host ESX.
- La afinidad de acceso a memoria no uniforme (NUMA) y la afinidad de CPU deben configurarse para que el host ESX obtenga buenos resultados.

  — Para encontrar la afinidad NUMA de un Vmnic, inicie sesión en el host de forma local o remota y escriba:

```
#vsish -e get /net/pNics/vmnic7/properties | grep NUMA
Device NUMA Node: 0
<!--NeedCopy-->
```

  - Para establecer la afinidad de NUMA y vCPU para una VM, consulte la documentación de VMware.

Citrix ADC VPX con interfaces de red E1000

Realice la siguiente configuración en el host de VMware ESX:

- En el host VMware ESX, cree dos vNIC a partir de un conmutador vNIC. Varias vNIC crean varios subprocesos Rx en el host ESX. Esto aumenta el rendimiento de Rx de la interfaz pNIC.
- Habilite las VLAN en el nivel de grupo de puertos de vSwitch para cada vNIC que haya creado.
- Para aumentar el rendimiento de transmisión de vNIC (Tx), utilice un subproceso Tx independiente en el host ESX por vNIC. Utilice el siguiente comando de ESX:
  - Para la versión 5.5 de ESX:

```
esxcli system settings advanced set -o /Net/NetTxWorldlet -
    i
<!--NeedCopy-->
```


- Para la versión 6.0 de ESX en adelante:

```
esxcli system settings advanced set -o /Net/NetVMTxType  -i 1
<!--NeedCopy-->
```

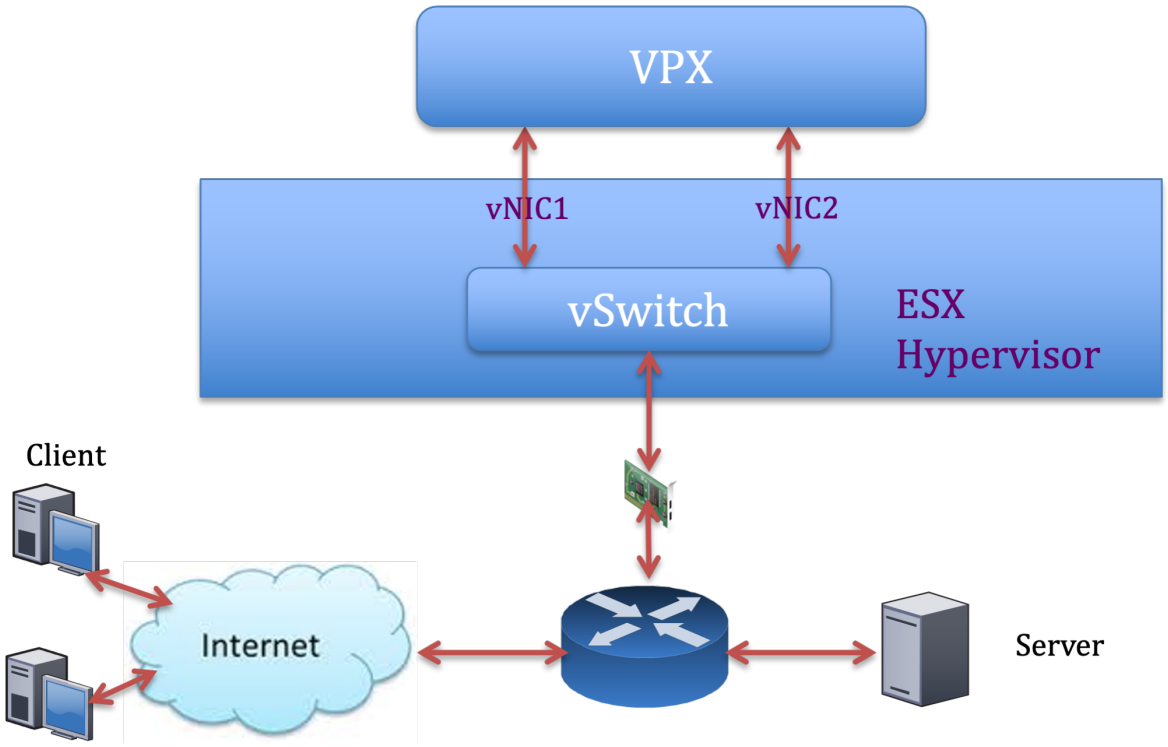
- Para aumentar aún más el rendimiento de vNIC Tx, utilice un subproceso de finalización Tx y una cola de subprocesos Rx por dispositivo (NIC) independientes. Utilice el siguiente comando de ESX:

```
esxcli system settings advanced set -o /Net/
   NetNetqRxQueueFeatPairEnable -i 0
<!--NeedCopy-->
```

> Nota:
>
> Asegúrese de reiniciar el host de VMware ESX para aplicar la configuración actualizada.

Dos vNIC por implementación de pNIC

A continuación se muestra un ejemplo de comandos de topología y configuración para el modelo de implementación **Dos vNIC por pNIC** que ofrece un mejor rendimiento de la red.



Ejemplo de configuración de Citrix ADC VPX:

Para lograr la implementación mostrada en la topología de ejemplo anterior, realice la siguiente configuración en la instancia de Citrix ADC VPX:

- En el lado del cliente, vincule el SNIP (1.1.1.2) a la interfaz de red 1/1 y habilite el modo de etiqueta VLAN.

```
bind vlan 2 -ifnum 1/1  - tagged
bind vlan 2 -IPAddress 1.1.1.2 255.255.255.0
<!--NeedCopy-->
```

- En el lado del servidor, vincule el SNIP (2.2.2.2) a la interfaz de red 1/1 y habilite el modo de etiqueta VLAN.

```
bind vlan 3 -ifnum 1/2  - tagged
bind vlan 3 -IPAddress 2.2.2.2 255.255.255.0
<!--NeedCopy-->
```

- Agregar un servidor virtual HTTP (1.1.1.100) y vincularlo a un servicio (2.2.2.100).

```
add lb vserver v1 HTTP 1.1.1.100 80 -persistenceType NONE -
   Listenpolicy None -cltTimeout 180
add service s1 2.2.2.100 HTTP 80 -gslb NONE -maxClient 0 -maxReq
   0 -cip DISABLED -usip NO -useproxyport YES -sp ON -cltTimeout
   180 -svrTimeout 360 -CKA NO -TCPB NO -CMP NO
bind lb vserver v1 s1
<!--NeedCopy-->
```

> Nota:
>
> Asegúrese de incluir las dos entradas siguientes en la tabla de rutas:
>
> - subred 1.1.1.0/24 con puerta de enlace apuntando a SNIP 1.1.1.2
> - Subred 2.2.2.0/24 con puerta de enlace que apunta a SNIP 2.2.2.2

Citrix ADC VPX con interfaces de red VMXNET3

Para lograr un alto rendimiento para VPX con interfaces de red VMXNET3, realice la siguiente configuración en el host VMware ESX:

- Cree dos vNIC a partir de un vSwitch pNIC. Varias vNIC crean varios subprocesos Rx en el host ESX. Esto aumenta el rendimiento de Rx de la interfaz pNIC.
- Habilite las VLAN en el nivel de grupo de puertos de vSwitch para cada vNIC que haya creado.
- Para aumentar el rendimiento de transmisión de vNIC (Tx), utilice un subproceso Tx independiente en el host ESX por vNIC. Utilice los siguientes comandos de ESX:
  - Para la versión 5.5 de ESX:

```
esxcli system settings advanced set -o /Net/NetTxWorldlet -i
<!--NeedCopy-->
```

  - Para la versión 6.0 de ESX en adelante:

```
 esxcli system settings advanced set -o /Net/NetVMTxType -i 1
 <!--NeedCopy-->
```

En el host de VMware ESX, realice la siguiente configuración:

- En el host VMware ESX, cree dos vNIC a partir de 1 vSwitch pNIC. Varias vNIC crean varios subprocesos Tx y Rx en el host ESX. Esto aumenta el rendimiento Tx y Rx de la interfaz pNIC.
- Habilite las VLAN en el nivel de grupo de puertos de vSwitch para cada vNIC que haya creado.
- Para aumentar el rendimiento de Tx de una vNIC, utilice un subproceso de finalización Tx y una cola de subprocesos Rx por dispositivo (NIC) independientes. Utilice el siguiente comando:

```
esxcli system settings advanced set -o /Net/
   NetNetqRxQueueFeatPairEnable -i 0
<!--NeedCopy-->
```

- Configure una máquina virtual para que use un subproceso de transmisión por vNIC, agregando la siguiente configuración a la configuración de la máquina virtual:

```
ethernetX.ctxPerDev = "1"
<!--NeedCopy-->
```

Para obtener más información, consulte Prácticas recomendadas para el ajuste del rendimiento de las cargas de trabajo de telecomunicaciones y NFV
en vSphere

> Nota:
>
> Asegúrese de reiniciar el host de VMware ESX para aplicar la configuración actualizada.

Puede configurar VMXNET3 como **dos vNIC por implementación de PNIC** . Para obtener más información, consulte Dos vNIC por implementación de PNIC.

Citrix ADC VPX con interfaces de red de paso SR-IOV y PCI

Para lograr un alto rendimiento para VPX con interfaces de red de paso SR-IOV y PCI, consulte Configuración recomendada en hosts ESX.

Instancia Citrix ADC VPX en la plataforma Linux-KVM

Esta sección contiene detalles sobre las opciones y los ajustes configurables, así como otras sugerencias que le ayudarán a lograr un rendimiento óptimo de la instancia Citrix ADC VPX en la plataforma Linux-KVM.

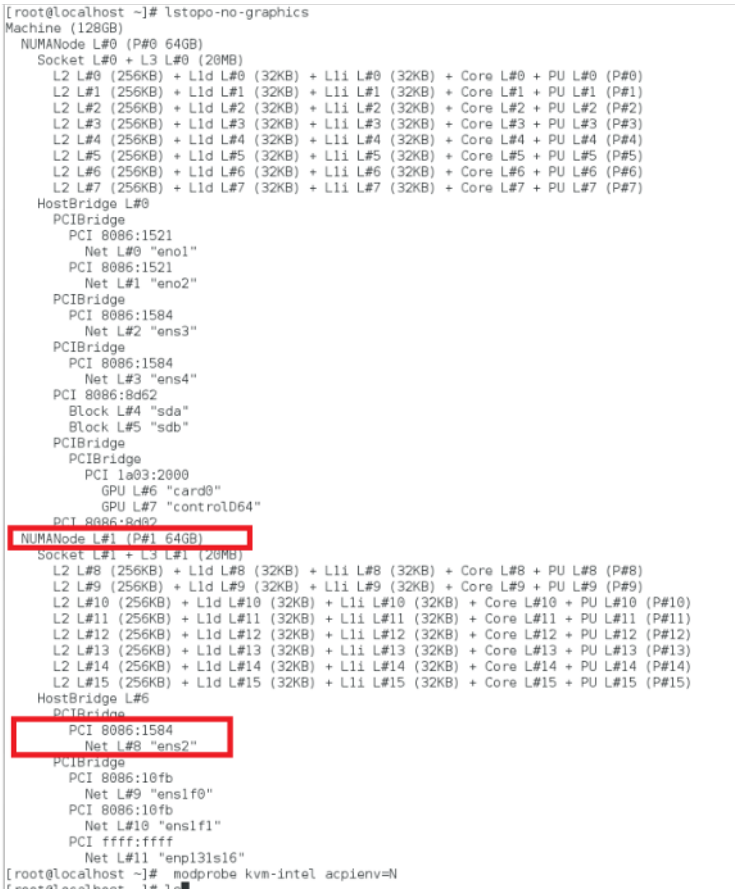
- Configuración de rendimiento para KVM
- Citrix ADC VPX con interfaces de red fotovoltaica
- Interfaces de red de paso de Citrix ADC VPX con SR-IOV y Fortville PCIe

Configuración de rendimiento para KVM

Realice los siguientes ajustes en el host KVM:

Busque el dominio NUMA de la NIC mediante el comando `lstopo`:

Asegúrese de que la memoria del VPX y de la CPU esté fijada en la misma ubicación.
En el siguiente resultado, la NIC 10G “ens2” está vinculada al dominio NUMA #1.



Asigne la memoria VPX del dominio NUMA.

El comando `numactl` indica el dominio NUMA desde el que se asigna la memoria. En el siguiente resultado, se asignan unos 10 GB de RAM desde el nodo NUMA #0.

```
[root@localhost ~]# numactl --hardware
available: 2 nodes (0-1)
node 0 cpus: 0 1 2 3 4 5 6 7
node 0 size: 65429 MB
node 0 free: 55854 MB
node 1 cpus: 8 9 10 11 12 13 14 15
node 1 size: 65536 MB
node 1 free: 52388 MB
node distances:
node   0   1
  0:  10  21
  1:  21  10
[root@localhost ~]#
```

Para cambiar la asignación de nodos NUMA, sigue estos pasos.

1. Modifique el archivo.xml del VPX en el host.


```
/etc/libvirt/qemu/<VPX_name>.xml
<!--NeedCopy-->
```

2. Agrega la siguiente etiqueta:

```
<numatune>
<memory mode="strict" nodeset="1"/>    This is the NUMA domain
   name
</numatune>
<!--NeedCopy-->
```

3. Apaga el VPX.
4. Ejecute este comando:

```
virsh define /etc/libvirt/qemu/<VPX_name>.xml
<!--NeedCopy-->
```

   Este comando actualiza la información de configuración de la máquina virtual con las asignaciones de nodos NUMA.

5. Enciende el VPX. A continuación, compruebe el resultado del comando `numactl -hardware` en el host para ver las asignaciones de memoria actualizadas para el VPX.

```
[root@localhost ~]# numactl --hardware
available: 2 nodes (0-1)
node 0 cpus: 0 1 2 3 4 5 6 7
node 0 size: 65429 MB
node 0 free: 65429 MB
node 1 cpus: 8 9 10 11 12 13 14 15
node 1 size: 65536 MB
node 1 free: 55854 MB
node distances:
node   0   1
  0:  10  21
  1:  21  10
[root@localhost ~]#
```

Anclar vCPU de VPX a núcleos físicos.

- Para ver las asignaciones de vCPU a PCPU de un VPX, escriba el siguiente comando

```
virsh vcpupin <VPX name>
<!--NeedCopy-->
```



```
root@localhost qemu]#  virsh vcpupin NS-VPX-DVR
CPU: CPU Affinity
----------------------------------
  0: 8
  1: 9
  2: 10
  3: 11
```

Las vCPU 0—4 se asignan a los núcleos físicos 8—11.

- Para ver el uso actual de la PCPU, escriba el siguiente comando:

```
mpstat -P ALL 5
<!--NeedCopy-->
```

```
[root@localhost qemu]# mpstat -P ALL 5
Linux 3.10.0-123.el7.x86_64 (localhost.localdomain)     05/17/2016      _x86_64_        (16 CPU)

02:26:20 PM  CPU    %usr   %nice    %sys %iowait    %irq   %soft  %steal  %guest  %gnice   %idle
02:26:25 PM  all    0.24    0.00    1.67    0.00    0.00    0.00    0.00   17.32    0.00   80.78
02:26:25 PM    0    0.20    0.00    1.00    0.00    0.00    0.00    0.00    0.00    0.00   98.80
02:26:25 PM    1    0.20    0.00    0.20    0.00    0.00    0.00    0.00    0.00    0.00   99.60
02:26:25 PM    2    0.20    0.00    0.40    0.00    0.00    0.00    0.00    0.00    0.00   99.40
02:26:25 PM    3    0.00    0.00    0.20    0.00    0.00    0.00    0.00    0.00    0.00   99.80
02:26:25 PM    4    0.20    0.00    0.20    0.00    0.00    0.00    0.00    0.00    0.00   99.60
02:26:25 PM    5    0.60    0.00    0.20    0.00    0.00    0.00    0.00    0.00    0.00   99.20
02:26:25 PM    6    0.40    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00   99.60
02:26:25 PM    7    1.62    0.00    1.42    0.00    0.00    0.00    0.00    0.00    0.00   96.96
02:26:25 PM    8    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00  100.00
02:26:25 PM    9    0.00    0.00    7.60    0.00    0.00    0.00    0.00   92.40    0.00    0.00
02:26:25 PM   10    0.20    0.00    7.00    0.00    0.00    0.00    0.00   92.80    0.00    0.00
02:26:25 PM   11    0.00    0.00    8.60    0.00    0.00    0.00    0.00   91.40    0.00    0.00
02:26:25 PM   12    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00  100.00
02:26:25 PM   13    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00  100.00
02:26:25 PM   14    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00  100.00
02:26:25 PM   15    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00  100.00
```

En este resultado, 8 es CPU de administración y 9-11 son motores de paquetes.

- Para cambiar la fijación de vCPU a PCPU, hay dos opciones.
  - Cámbielo en tiempo de ejecución después de que se inicie el VPX con el siguiente comando:

```
virsh vcpupin <VPX name> <vCPU id>  <pCPU number>
virsh vcpupin NetScaler-VPX-XML 0 8
virsh vcpupin NetScaler-VPX-XML 1 9
virsh vcpupin NetScaler-VPX-XML 2 10
virsh vcpupin NetScaler-VPX-XML 3 11
<!--NeedCopy-->
```

  - Para realizar cambios estáticos en el VPX, modifique el archivo `.xml` como antes con las siguientes etiquetas:

1. Modificar el archivo.xml del VPX en el host

```
/etc/libvirt/qemu/<VPX_name>.xml
<!--NeedCopy-->
```

2. Agrega la siguiente etiqueta:

```
<vcpu placement='static' cpuset='8-11'>4</vcpu>
    <cputune>
        <vcpupin vcpu='0' cpuset='8'/>
        <vcpupin vcpu='1' cpuset='9'/>
        <vcpupin vcpu='2' cpuset='10'/>
        <vcpupin vcpu='3' cpuset='11'/>
    </cputune>
<!--NeedCopy-->
```

3. Apaga el VPX.
4. Actualice la información de configuración de la máquina virtual con las asignaciones de nodos NUMA mediante el siguiente comando:

```
virsh define /etc/libvirt/qemu/ <VPX_name>.xml
<!--NeedCopy-->
```

5. Enciende el VPX. A continuación, compruebe el resultado del comando `virsh vcpupin <VPX name>` en el host para ver la fijación actualizada de la CPU.

Elimine la sobrecarga de interrupción del host.

- Detecte VM_EXITS mediante el comando `kvm_stat`.

  En el nivel del hipervisor, las interrupciones del host se asignan a las mismas PCPU en las que están fijadas las vCPU de la VPX. Esto podría provocar que las vCPU de la VPX se expulsaran periódicamente.

  Para encontrar las salidas de VM realizadas por las máquinas virtuales que ejecutan el host, use el comando `kvm_stat`.

```
[root@localhost ~]# kvm_stat -1  | grep EXTERNAL
kvm_exit(EXTERNAL_INTERRUPT)  1728349 27738
[root@localhost ~]#
```



```
<!--NeedCopy-->
```

Un valor más alto del orden 1+M indica un problema.

Si hay una sola máquina virtual, el valor esperado es de 30 a 100 K. Si hay más de eso, puede indicar que hay uno o más vectores de interrupción del host asignados a la misma PCPU.

- Detecte las interrupciones del host y migre las interrupciones del host.

  Al ejecutar el comando `concatenate` del archivo "/proc/interrupts", muestra todas las asignaciones de interrupción del host. Si una o más IRQ activas se asignan a la misma PCPU, su contador correspondiente aumenta.

  Mueva las interrupciones que se superpongan con las PCPUs de su Citrix ADC VPX a las PCPUs que no se utilicen:

```
echo 0000000f > /proc/irq/55/smp_affinity
0000000f - - > it is a bitmap, LSBs indicates that IRQ 55 can
   only be scheduled on pCPUs 0 - 3
<!--NeedCopy-->
```

- Desactiva el saldo de IRQ.

  Inhabilite el demonio de equilibrio de IRQ para que no se produzca ninguna reprogramación sobre la marcha.

```
service irqbalance stop
service irqbalance show - To check the status
service irqbalance start - Enable if needed
<!--NeedCopy-->
```

  Asegúrese de ejecutar el comando `kvm_stat` para asegurarse de que no haya muchos contadores.

Citrix ADC VPX con interfaces de red fotovoltaica

Puede configurar las interfaces de red de paso de para-virtualización (PV), SR-IOV y PCIe como **dos vNIC por implementación de PNIC** . Para obtener más información, consulte Dos vNIC por implementación de PNIC.

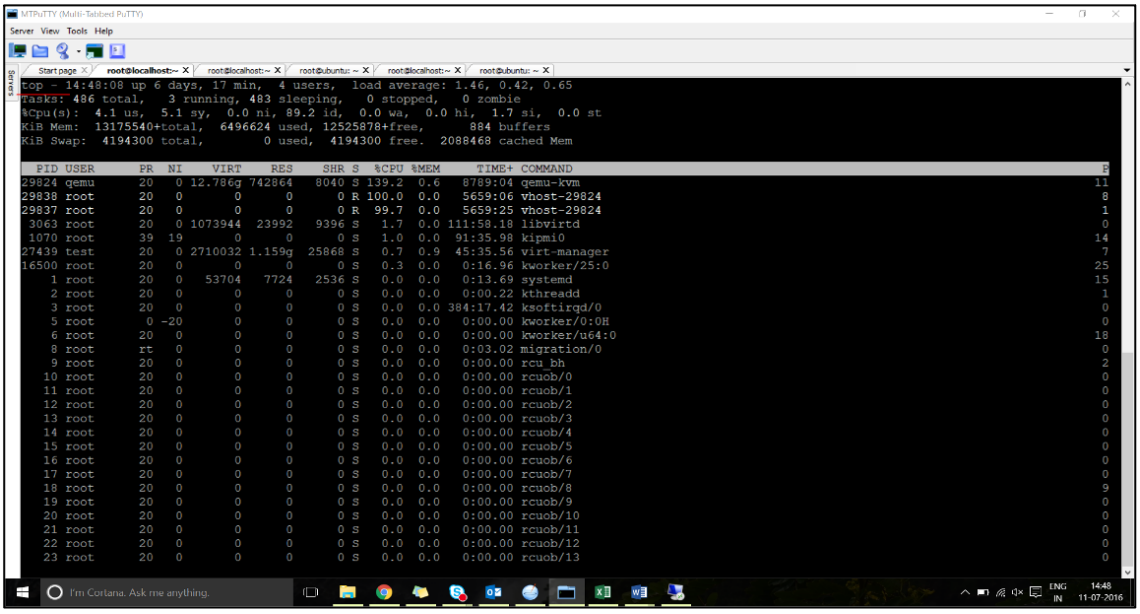
Para obtener un rendimiento óptimo de las interfaces fotovoltaicas (virtio), siga estos pasos:

- Identifique el dominio NUMA al que está vinculada la ranura o NIC PCIe.

- La memoria y la vCPU del VPX deben estar ancladas al mismo dominio NUMA.
- El subproceso vhost debe estar enlazado a las CPU del mismo dominio NUMA.

Enlazar los subprocesos del host virtual a las CPU correspondientes:

1. Una vez iniciado el tráfico, ejecute el comando `top` en el host.



2. Identificar el proceso de host virtual (denominado como `vhost-<pid-of-qemu>`) afinidad.
3. Enlace los procesos vHost a los núcleos físicos del dominio NUMA identificado anteriormente mediante el siguiente comando:

```
taskset -pc <core-id> <process-id>
<!--NeedCopy-->
```

Ejemplo:

```
taskset -pc 12 29838
<!--NeedCopy-->
```

4. Los núcleos del procesador correspondientes al dominio NUMA se pueden identificar con el siguiente comando:

```
[root@localhost ~]# virsh capabilities | grep cpu
<cpu>
    </cpu>
```



```
4           <cpus num='8'>
5               <cpu id='0' socket_id='0' core_id='0' siblings='0'/>
6               <cpu id='1' socket_id='0' core_id='1' siblings='1'/>
7               <cpu id='2' socket_id='0' core_id='2' siblings='2'/>
8               <cpu id='3' socket_id='0' core_id='3' siblings='3'/>
9               <cpu id='4' socket_id='0' core_id='4' siblings='4'/>
10              <cpu id='5' socket_id='0' core_id='5' siblings='5'/>
11              <cpu id='6' socket_id='0' core_id='6' siblings='6'/>
12              <cpu id='7' socket_id='0' core_id='7' siblings='7'/>
13          </cpus>
14
15          <cpus num='8'>
16          <cpu id='8' socket_id='1' core_id='0' siblings='8'/>
17          <cpu id='9' socket_id='1' core_id='1' siblings='9'/>
18          <cpu id='10' socket_id='1' core_id='2' siblings='10'/>
19          <cpu id='11' socket_id='1' core_id='3' siblings='11'/>
20          <cpu id='12' socket_id='1' core_id='4' siblings='12'/>
21          <cpu id='13' socket_id='1' core_id='5' siblings='13'/>
22          <cpu id='14' socket_id='1' core_id='6' siblings='14'/>
23          <cpu id='15' socket_id='1' core_id='7' siblings='15'/>
24          </cpus>
25
26      <cpuselection/>
27      <cpuselection/>
28
29  <!--NeedCopy-->
```

Enlazar el proceso QEMU al núcleo físico correspondiente:

1. Identificar los núcleos físicos en los que se ejecuta el proceso QEMU. Para obtener más información, consulte el resultado anterior.
2. Enlace el proceso QEMU a los mismos núcleos físicos a los que vincula las vCPU mediante el siguiente comando:

```
1 taskset -pc 8-11 29824
2 <!--NeedCopy-->
```

Interfaces de red de paso de Citrix ADC VPX con SR-IOV y Fortville PCIe

Para obtener un rendimiento óptimo de las interfaces de red de paso SR-IOV y Fortville PCIe, siga estos pasos:

- Identifique el dominio NUMA al que está vinculada la ranura o NIC PCIe.
- La memoria y la vCPU del VPX deben estar ancladas al mismo dominio NUMA.

Archivo XML VPX de ejemplo para vCPU y fijación de memoria para Linux KVM:

```
    <domain type='kvm'>
        <name>NetScaler-VPX</name>
        <uuid>138f7782-1cd3-484b-8b6d-7604f35b14f4</uuid>
        <memory unit='KiB'>8097152</memory>
        <currentMemory unit='KiB'>8097152</currentMemory>
        <vcpu placement='static'>4</vcpu>

    <cputune>
        <vcpupin vcpu='0' cpuset='8'/>
        <vcpupin vcpu='1' cpuset='9'/>
        <vcpupin vcpu='2' cpuset='10'/>
        <vcpupin vcpu='3' cpuset='11'/>
    </cputune>

    <numatune>
    <memory mode='strict' nodeset='1'/>
    </numatune>

    </domain>
<!--NeedCopy-->
```

Instancia de Citrix ADC VPX en Citrix Hypervisors

Esta sección contiene detalles sobre las opciones y los ajustes configurables y otras sugerencias que le ayudan a lograr un rendimiento óptimo de la instancia de Citrix ADC VPX en Citrix Hypervisors.

- Configuración de rendimiento de Citrix Hypervisors
- Citrix ADC VPX con interfaces de red SR-IOV
- Citrix ADC VPX con interfaces para-virtualizadas

Configuración de rendimiento de Citrix Hypervisors

Busque el dominio NUMA de la NIC mediante el comando “xl”:

```
xl info -n
<!--NeedCopy-->
```


Anclar vCPU de VPX a núcleos físicos.

```
xl vcpu-pin <Netsclaer VM Name>  <vCPU id>  <physical CPU id>
<!--NeedCopy-->
```

Compruebe la vinculación de las vCPU.

```
xl vcpu-list
<!--NeedCopy-->
```

Asigne más de 8 vCPU a las máquinas virtuales Citrix ADC.

Para configurar más de 8 vCPU, ejecute los siguientes comandos desde la consola de Citrix Hypervisor:

```
xe vm-param-set uuid=your_vms_uuid VCPUs-max=16
xe vm-param-set uuid=your_vms_uuid VCPUs-at-startup=16
<!--NeedCopy-->
```

Citrix ADC VPX con interfaces de red SR-IOV

Para obtener un rendimiento óptimo de las interfaces de red SR-IOV, siga estos pasos:

- Identifique el dominio NUMA al que está vinculada la ranura PCIe o la NIC.
- Anclar la memoria y la vCPU del VPX al mismo dominio NUMA.
- Enlaza la vCPU Domain-0 a la CPU restante.

Citrix ADC VPX con interfaces para-virtualizadas

Para obtener un rendimiento óptimo, se recomiendan dos vNIC por cada pNIC y una vNIC por cada pNIC, como en otros entornos fotovoltaicos.

Para lograr un rendimiento óptimo de las interfaces para-virtualizadas (netfront), siga estos pasos:

- Identifique el dominio NUMA al que está vinculada la ranura PCIe o la NIC.
- Anclar la memoria y la vCPU del VPX al mismo dominio NUMA.
- Enlazar la vCPU Domain-0 a la CPU restante del mismo dominio NUMA.
- Anclar subprocesos Rx/Tx del host de vNIC a vCPU de dominio 0.

Anclar subprocesos de host a vCPU Domain-0:

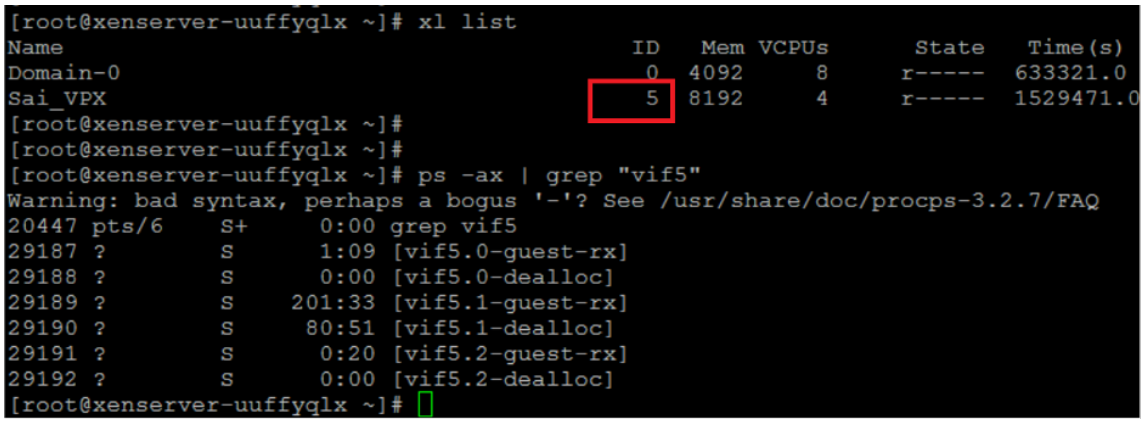
1. Busque Xen-ID del VPX mediante el comando `xl list` del shell de host de Citrix Hypervisor.

2. Identifique los subprocesos de host mediante el siguiente comando:

```
ps -ax | grep vif <Xen-ID>
<!--NeedCopy-->
```

En el siguiente ejemplo, estos valores indican:

- **vif5.0** - Subprocesos de la primera interfaz asignada a VPX en XenCenter (interfaz de administración).
- **vif5.1** - Los hilos de la segunda interfaz asignados a VPX y así sucesivamente.



3. Anclar los subprocesos a las vCPU Domain-0 mediante el siguiente comando:

```
taskset  - pc <core-id> <process-id>
<!--NeedCopy-->
```

Ejemplo:

```
taskset -pc 1 29189
<!--NeedCopy-->
```

Aplicación de configuraciones Citrix ADC VPX en el primer arranque del dispositivo Citrix ADC en la nube

December 2, 2021

Puede aplicar las configuraciones de Citrix ADC VPX durante el primer arranque del dispositivo Citrix ADC en un entorno de nube. Esta etapa se aborda como fase de **prearranque** en este documento. Por lo tanto, en algunos casos, como las licencias agrupadas por ADC, una instancia VPX específica aparece en mucho menos tiempo. Esta función está disponible en Microsoft Azure, la plataforma de Google Cloud y las nubes de AWS.

Qué son los datos de usuario

Cuando aprovisiona una instancia VPX en un entorno de nube, tiene la opción de pasar datos de usuario a la instancia. Los datos de usuario le permiten realizar tareas de configuración automatizadas comunes, personalizar los comportamientos de inicio de las instancias y ejecutar scripts después de que se inicie la instancia. En el primer arranque, la instancia Citrix ADC VPX realiza las siguientes tareas:

- Lee los datos del usuario.
- Interpreta la configuración proporcionada en los datos de usuario.
- Aplica la configuración recién agregada a medida que se inicia.

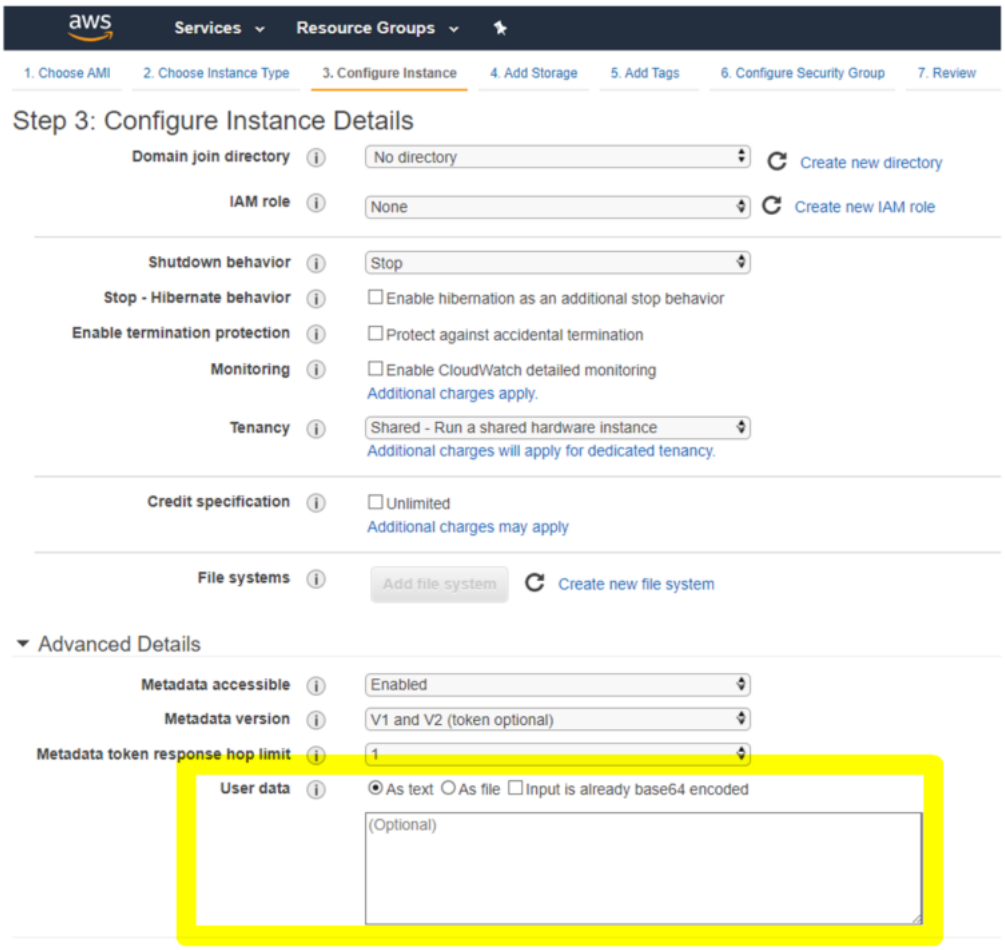
Cómo proporcionar datos de usuario previos al arranque en una instancia de nube

Puede proporcionar datos de usuario de prearranque a la instancia de nube en formato XML. Las distintas nubes tienen interfaces diferentes para proporcionar datos de usuario.

Proporcionar datos de usuario previos al arranque mediante la consola de AWS

Cuando aprovisione una instancia Citrix ADC VPX mediante la consola de AWS, vaya a **Configurar detalles de instancias > Detalles avanzados**y proporcione la configuración de datos de usuario previo al arranque en el campo **Datos de usuario** .

Para obtener instrucciones detalladas sobre cada uno de los pasos, consulte Implementación de una instancia Citrix ADC VPX en AWS mediante la consola web de AWS.
Para obtener más información, consulte la documentación de AWS sobre el lanzamiento de una instancia.



Proporcionar datos de usuario previos al arranque mediante AWS CLI

Escriba el siguiente comando en la CLI de AWS:

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type t2.micro \
    --count 1 \
    --subnet-id subnet-08fc749671b2d077c \
    --key-name MyKeyPair \
    --security-group-ids sg-0b0384b66d7d692f9 \
    --user-data file://my_script.txt
<!--NeedCopy-->
```

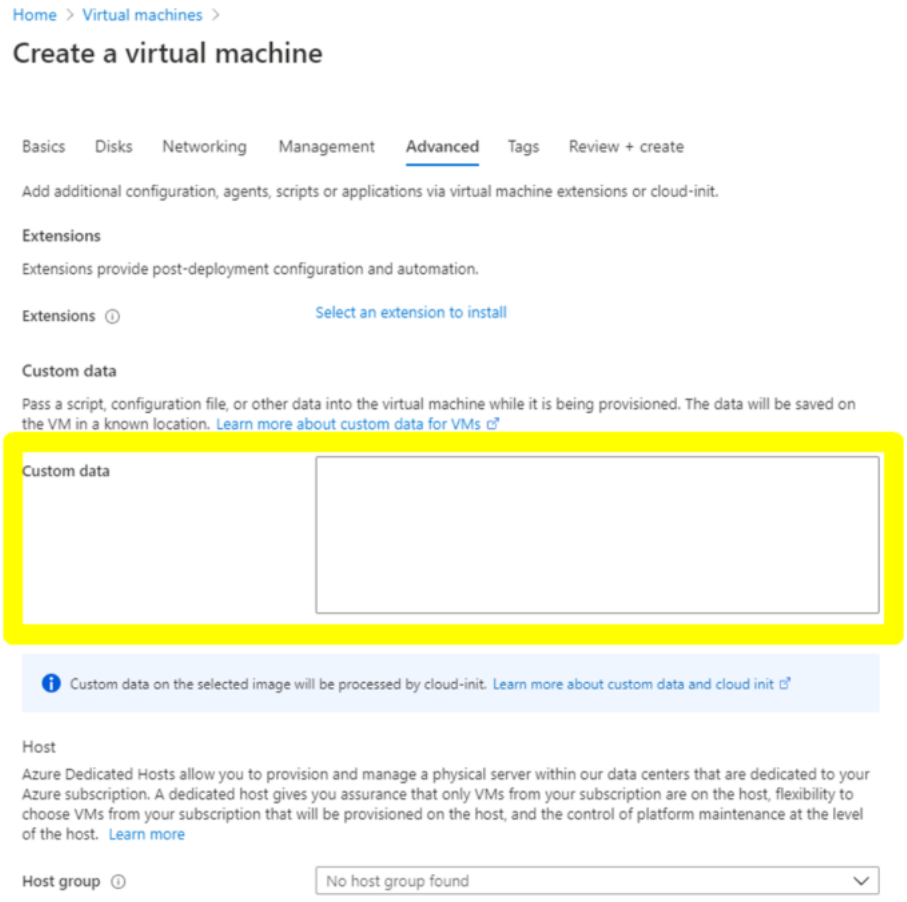
Para obtener más información, consulte la documentación de AWS sobre instancias en ejecución.

Para obtener más información, consulte la documentación de AWS sobre Uso de datos de usuario de

instancias

Proporcionar datos de usuario previos al arranque mediante la consola de Azure

Cuando aprovisione una instancia Citrix ADC VPX mediante la consola de Azure, vaya a **Crear una máquina virtual > ficha Avanzadas** . En el campo **Datos personalizados**, proporcione la configuración de datos de usuario de prearranque.



Proporcionar datos de usuario previos al arranque mediante la CLI de Azure

Escriba el siguiente comando en la CLI de Azure:

```
az vm create \
  --resource-group myResourceGroup \
  --name MyVm \
  --image debian \
  --custom-data MyCloudInitScript.txt \
<!--NeedCopy-->
```


Ejemplo:

```
az vm create --resource-group MyResourceGroup -name MyVm --image debian
    --custom-data MyCloudInitScript.txt
<!--NeedCopy-->
```

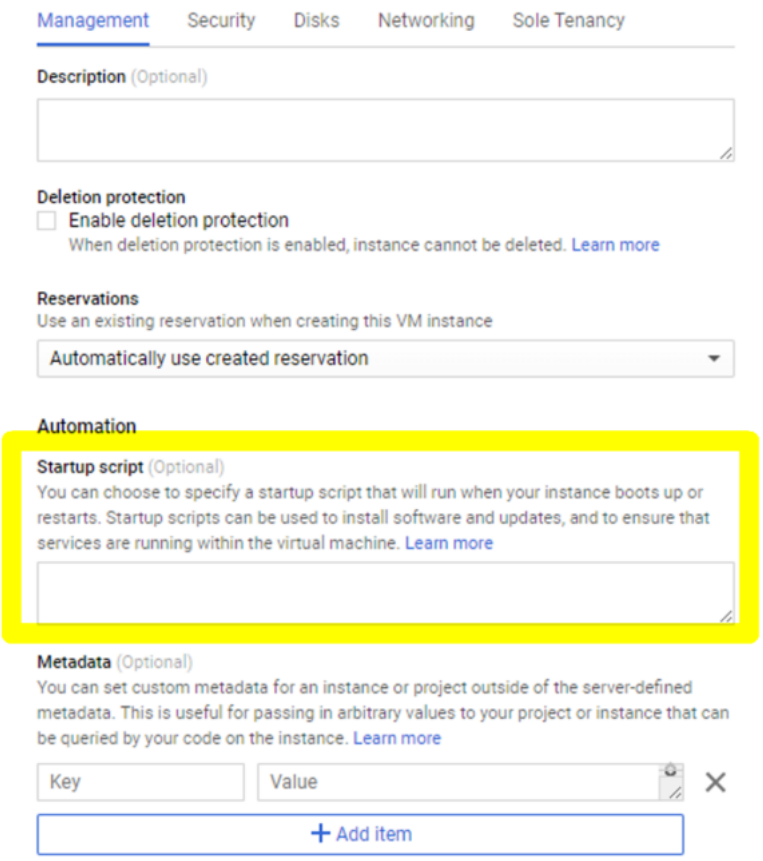
Puede pasar los datos personalizados o la configuración previa al arranque como un archivo al parámetro "—custom-data". En este ejemplo, el nombre de archivo es **MyCloudInitScript.txt**.

Para obtener más información, consulte la documentación de Azure CLI.

Proporcionar datos de usuario previos al arranque mediante la consola de GCP

Cuando aprovisione una instancia Citrix ADC VPX mediante la consola de GCP, complete las propiedades de la instancia. Amplíe **Administración, seguridad, discos, redes, arrendamiento único**. Acceda a la ficha **Administración** . En la sección **Automatización**, proporcione la configuración de datos de usuario de prearranque en el campo **Script de inicio** .

Para obtener información detallada sobre cómo crear la instancia VPX mediante GCP, consulte Implementación de una instancia Citrix ADC VPX en Google Cloud Platform.



Proporcionar datos de usuario de prearranque mediante la CLI de gcloud

Escriba el siguiente comando en la CLI de GCP:

```
gcloud compute instances create INSTANCE_NAMES --metadata-from-file=
    startup-script=LOCAL_FILE_PATH
<!--NeedCopy-->
```

metadata-from-file: Lee el valor o los datos de usuario de un archivo almacenado en el <LOCAL_FILE_PATH>.

Para obtener más información, consulta la documentación de la CLI de gcloud

Formato de datos de usuario de prearranque

Los datos de usuario de prearranque deben proporcionarse a la instancia de nube en formato XML. Los datos de usuario de prearranque de Citrix ADC que proporciona a través de la infraestructura de nube durante el arranque pueden abarcar las cuatro secciones siguientes:

- Configuración de Citrix ADC representada con la etiqueta <NS-CONFIG>.
- Arranque personalizado de Citrix ADC representado con la etiqueta <NS-BOOTSTRAP>.
- Almacenar guiones de usuario en Citrix ADC representados con la etiqueta <NS-SCRIPTS>.
- Configuración de licencias agrupadas representada con la etiqueta <NS-LICENSE-CONFIG>.

Puede proporcionar las cuatro secciones anteriores en cualquier orden dentro de la configuración de prearranque de ADC.
Asegúrese de seguir estrictamente el formato que se muestra en las secciones siguientes mientras proporciona los datos de usuario de prearranque.

> Nota:
>
> La configuración completa de datos de usuario de prearranque debe incluirse en la etiqueta <NS-PRE-BOOT-CONFIG>, tal y como se muestra en los ejemplos siguientes.

Ejemplo 1:

```
<NS-PRE-BOOT-CONFIG>
     <NS-CONFIG>          </NS-CONFIG>
     <NS-BOOTSTRAP>       </NS-BOOTSTRAP>
     <NS-SCRIPTS>         </NS-SCRIPTS>
     <NS-LICENSE-CONFIG>  </NS-LICENSE-CONFIG>
</NS-PRE-BOOT-CONFIG>
<!--NeedCopy-->
```

Ejemplo 2:

```
<NS-PRE-BOOT-CONFIG>
    <NS-LICENSE-CONFIG> </NS-LICENSE-CONFIG>
    <NS-SCRIPTS>        </NS-SCRIPTS>
    <NS-BOOTSTRAP>      </NS-BOOTSTRAP>
    <NS-CONFIG>         </NS-CONFIG>
</NS-PRE-BOOT-CONFIG>
<!--NeedCopy-->
```

Utilice la etiqueta <NS-CONFIG> para proporcionar las configuraciones específicas de Citrix ADC VPX que deben aplicarse a la instancia VPX en la etapa de prearranque.

> NOTA:
>
> La sección <NS-CONFIG> debe tener comandos CLI de ADC válidos. No se verifican los errores sintácticos ni el formato de las CLI.

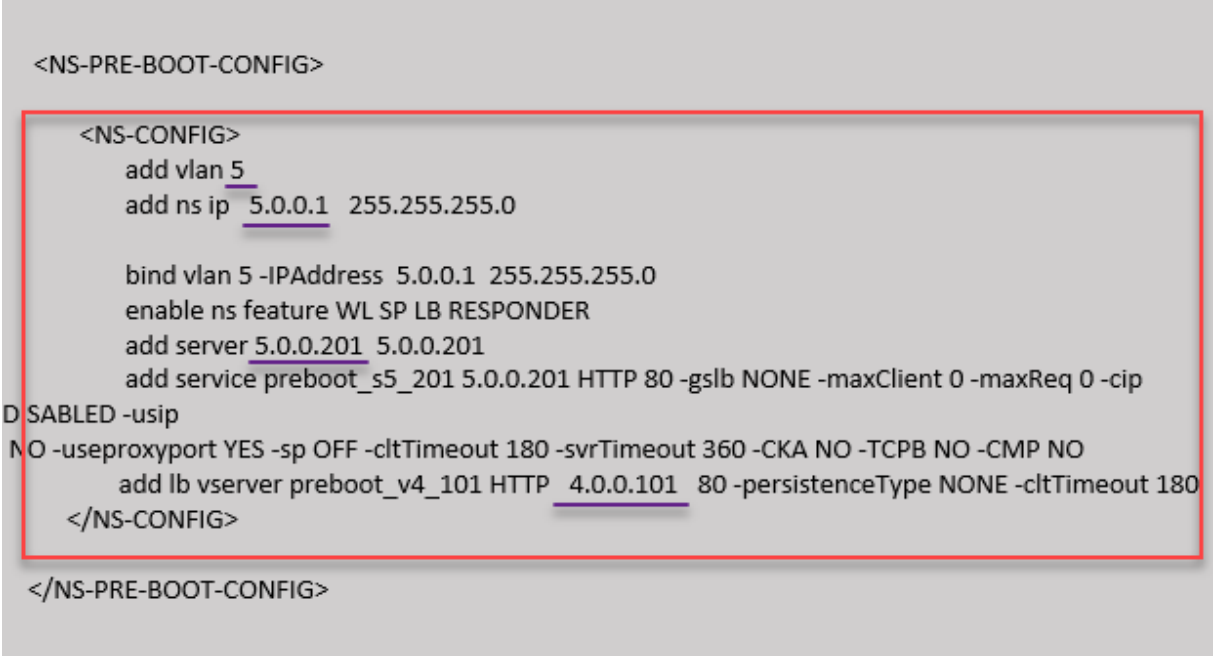
Configuraciones de Citrix ADC

Utilice la etiqueta <NS-CONFIG> para proporcionar las configuraciones específicas de Citrix ADC VPX que deben aplicarse a la instancia VPX en la etapa de prearranque.

> NOTA:
>
> La sección <NS-CONFIG> debe tener comandos CLI de ADC válidos. No se verifican los errores sintácticos ni el formato de las CLI.

Ejemplo:

En el ejemplo siguiente, la sección <NS-CONFIG> contiene los detalles de las configuraciones. Una VLAN de ID '5' está configurada y enlazada al SNIP (5.0.0.1). También se configura un servidor virtual de equilibrio de carga (4.0.0.101).



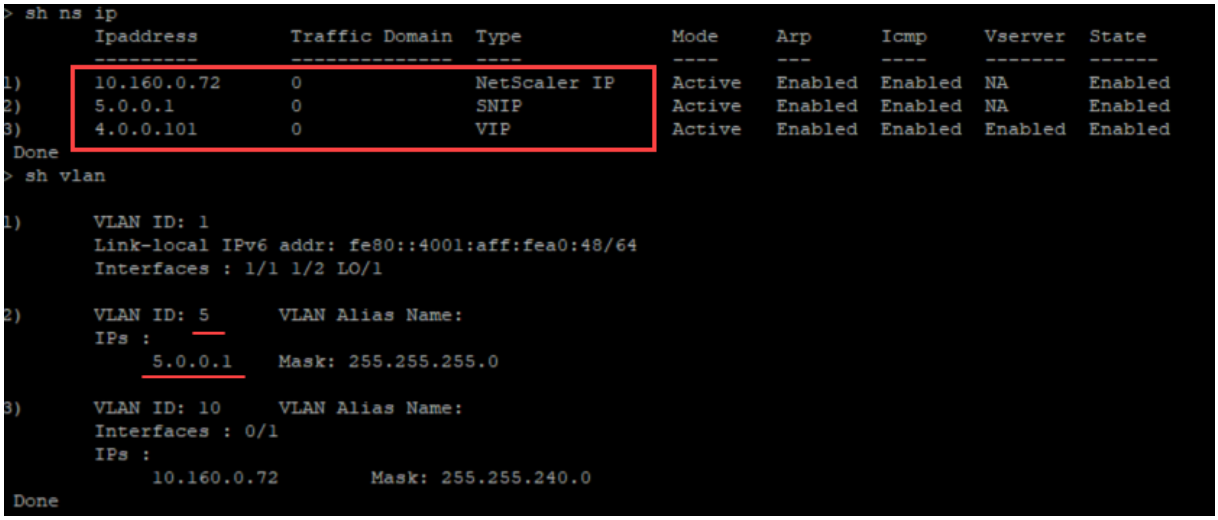
Puede copiar la configuración que se muestra en la captura de pantalla anterior desde aquí:

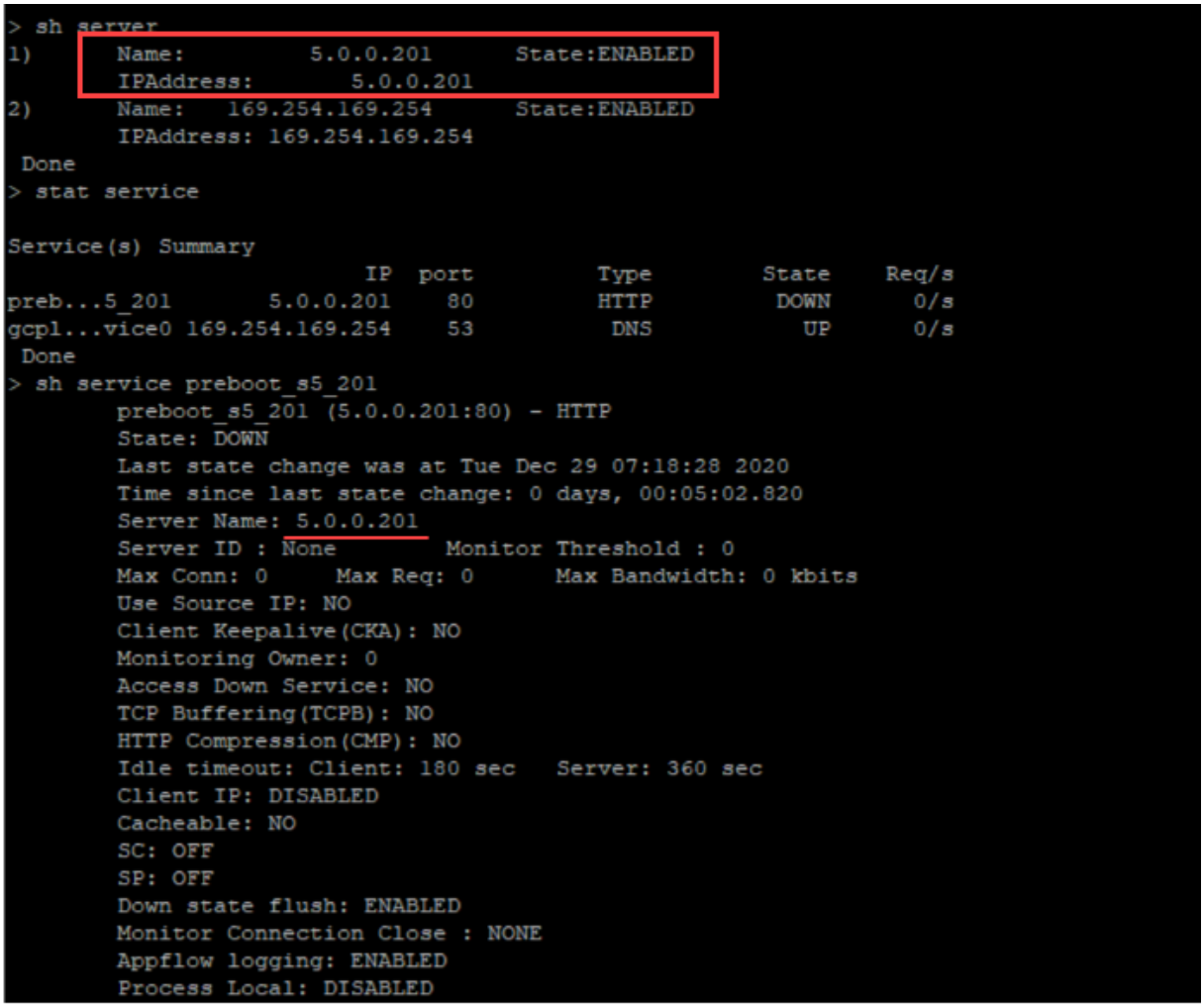
```
<NS-PRE-BOOT-CONFIG>
     <NS-CONFIG>
         add vlan 5
         add ns ip 5.0.0.1 255.255.255.0
         bind vlan 5 -IPAddress 5.0.0.1 255.255.255.0
         enable ns feature WL SP LB RESPONDER
         add server 5.0.0.201 5.0.0.201
         add service preboot_s5_201 5.0.0.201 HTTP 80 -gslb NONE -
            maxClient 0 -maxReq 0 -cip DISABLED -usip
```



```
 9   NO -useproxyport YES -sp OFF -cltTimeout 180 -svrTimeout 360 -CKA NO -
        TCPB NO -CMP NO
10           add lb vserver preboot_v4_101 HTTP 4.0.0.101 80 -
                 persistenceType NONE -cltTimeout 180
11       </NS-CONFIG>
12  </NS-PRE-BOOT-CONFIG>
13  <!--NeedCopy-->
```

La instancia Citrix ADC VPX presenta la configuración aplicada en la sección <NS-CONFIG> como se muestra en las ilustraciones siguientes.





Guiones de usuario

Utilice la etiqueta <NS-SCRIPTS> para proporcionar cualquier script que deba almacenarse y ejecutarse en la instancia de Citrix ADC VPX.

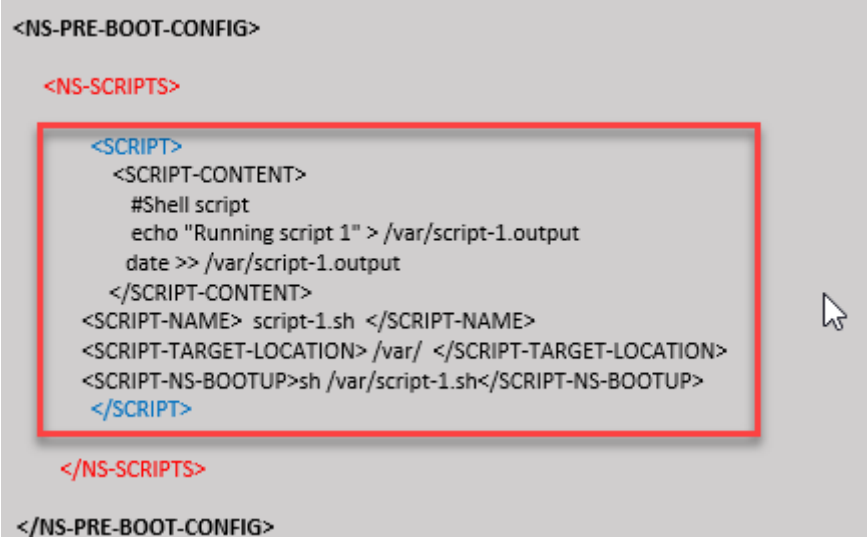
Puede incluir muchos scripts dentro de la etiqueta <NS-SCRIPTS>. Cada guión debe incluirse dentro de la etiqueta <SCRIPT>.
Cada sección <SCRIPT> corresponde a un guión y contiene todos los detalles del guión mediante las siguientes subetiquetas.

- **<SCRIPT-NAME>:** Indica el nombre del archivo de script que debe almacenarse.
- **<SCRIPT-CONTENT>:** Indica el contenido del archivo que debe almacenarse.
- **<SCRIPT-TARGET-LOCATION>:** Indica la ubicación de destino designada en la que debe almacenarse este archivo. Si no se proporciona la ubicación de destino, de forma predeterminada, el archivo o el script se guardan en el directorio "/nsconfig".
- **<SCRIPT-NS-BOOTUP>:** Especifique los comandos que utiliza para ejecutar el script.

- Si utiliza la sección <SCRIPT-NS-BOOTUP>, los comandos proporcionados en la sección se almacenan en "/nsconfig/nsafter.sh ", y los comandos se ejecutan después de que se inicie el motor de paquetes como parte de la ejecución de" nsafter.sh".
- Si no utiliza la sección <SCRIPT-NS-BOOTUP>, el archivo de script se almacena en la ubicación de destino que especifique.

Ejemplo 1:

En este ejemplo, la etiqueta <NS-SCRIPTS> contiene detalles de un único script: script-1.sh. El script "script-1.sh" se guarda en el directorio "/var". El script se rellena con el contenido especificado y se ejecuta con el comando "sh /var/script-1.sh" después de arrancar el motor de paquetes.



Puede copiar la configuración que se muestra en la captura de pantalla anterior desde aquí:

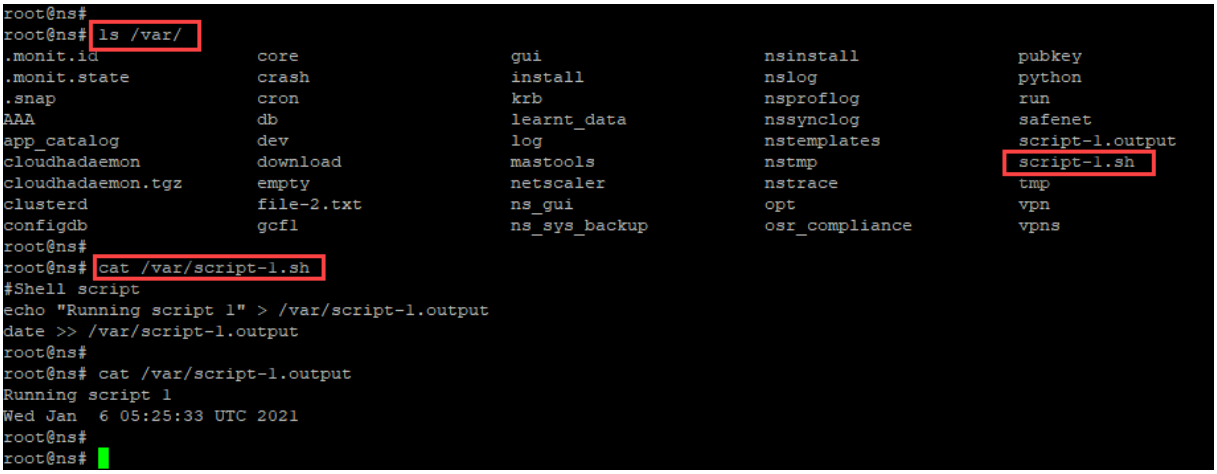
```
<NS-PRE-BOOT-CONFIG>
    <NS-SCRIPTS>
    <SCRIPT>
            <SCRIPT-CONTENT>
                #Shell script
                echo "Running script 1" > /var/script-1.output
                date >> /var/script-1.output
            </SCRIPT-CONTENT>

                <SCRIPT-NAME> script-1.sh </SCRIPT-NAME>
                <SCRIPT-TARGET-LOCATION> /var/ </SCRIPT-TARGET-LOCATION
                    >
                <SCRIPT-NS-BOOTUP>sh /var/script-1.sh</SCRIPT-NS-BOOTUP
                    >
        </SCRIPT>
    </NS-SCRIPTS>
```



```
</NS-PRE-BOOT-CONFIG>
<!--NeedCopy-->
```

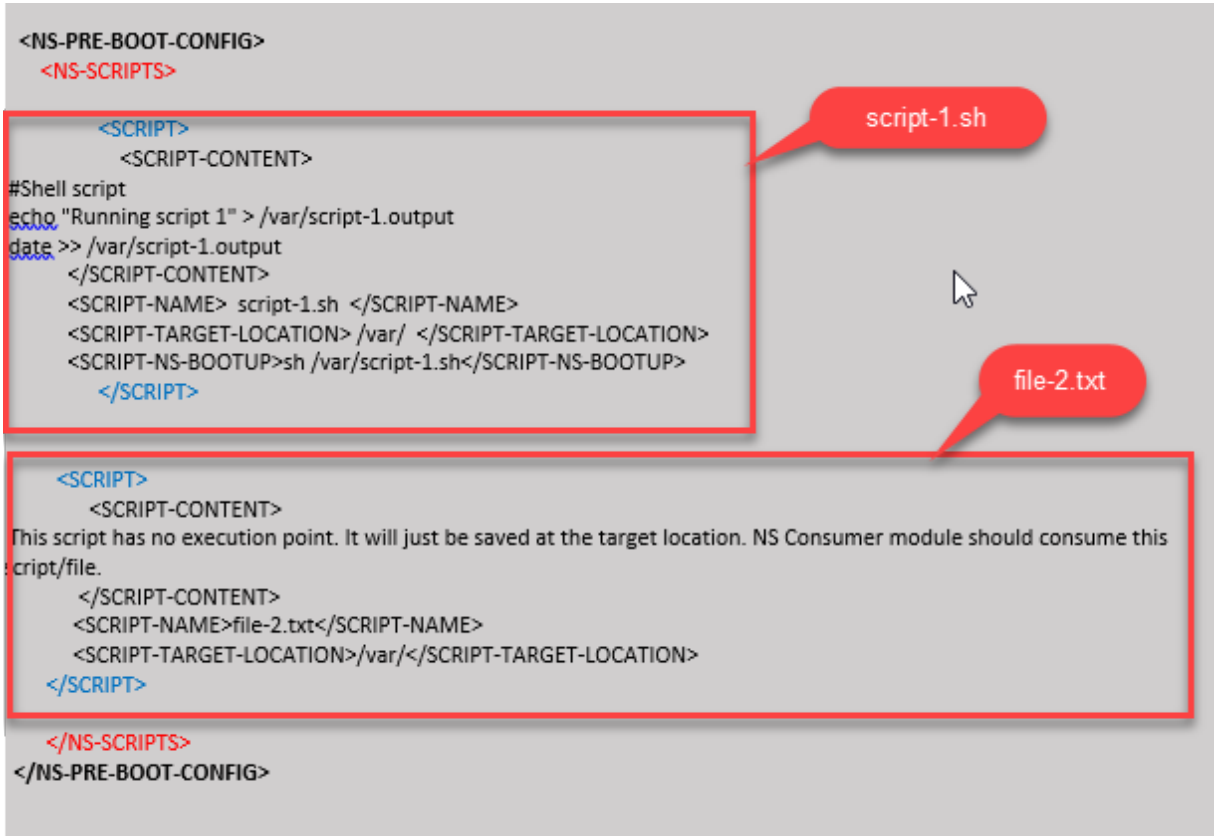
En la siguiente instantánea, puede comprobar que el script “script-1.sh” está guardado en el directorio “/var/”. Se ejecuta el script “Script-1.sh” y el archivo de salida se crea correctamente.



Ejemplo 2:

En el ejemplo siguiente, la etiqueta <NS-SCRIPTS> contiene detalles de dos scripts.

- El primer script se guarda como “script-1.sh” en el directorio “/var”. El script se rellena con el contenido especificado y se ejecuta con el comando “sh /var/script-1.sh” después de arrancar el motor de paquetes.
- El segundo script se guarda como “file-2.txt” en el directorio “/var”. Este archivo se rellena con el contenido especificado. Pero no se ejecuta porque no <SCRIPT-NS-BOOTUP> se proporciona el comando de ejecución de arranque.



Puede copiar la configuración que se muestra en la captura de pantalla anterior desde aquí:

```
<NS-PRE-BOOT-CONFIG>
    <NS-SCRIPTS>
        <SCRIPT>
            <SCRIPT-CONTENT>
               #Shell script
               echo ”Running script 1” > /var/script-1.output
               date >> /var/script-1.output
            </SCRIPT-CONTENT>

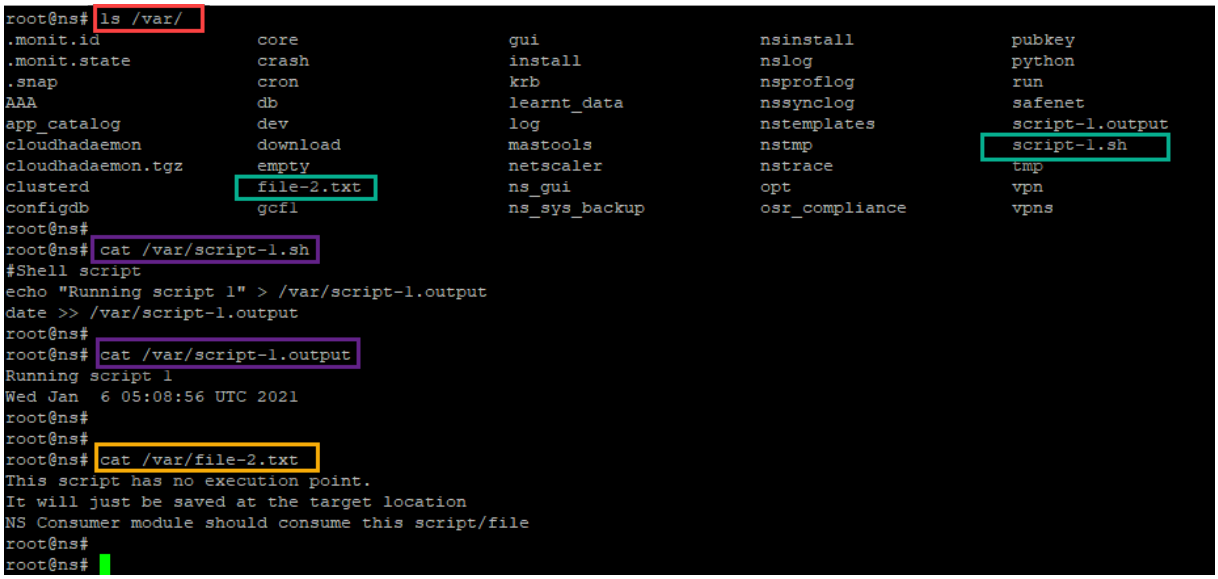
            <SCRIPT-NAME>  script-1.sh  </SCRIPT-NAME>
            <SCRIPT-TARGET-LOCATION> /var/  </SCRIPT-TARGET-LOCATION>
            <SCRIPT-NS-BOOTUP>sh /var/script-1.sh</SCRIPT-NS-BOOTUP>
            </SCRIPT>

        <SCRIPT>
            <SCRIPT-CONTENT>
                This script has no execution point.
                It will just be saved at the target location
                NS Consumer module should consume this script/file
```



```
            </SCRIPT-CONTENT>
            <SCRIPT-NAME>file-2.txt</SCRIPT-NAME>
            <SCRIPT-TARGET-LOCATION>/var/</SCRIPT-TARGET-LOCATION>
        </SCRIPT>
    </NS-SCRIPTS>
</NS-PRE-BOOT-CONFIG>
<!--NeedCopy-->
```

En la siguiente instantánea, puede comprobar que script-1.sh y file-2.txt se crean en el directorio "/var/". Script-1.sh se ejecuta y el archivo de salida se crea correctamente.



Licencias

Utilice la etiqueta <NS-LICENSE-CONFIG> para aplicar licencias agrupadas de Citrix ADC mientras arranca la instancia VPX. Utilice la etiqueta <LICENSE-COMMANDS> dentro de la sección <NS-LICENSE-CONFIG> para proporcionar los comandos de licencia agrupados. Estos comandos deben ser válidos sintácticamente.

Puede especificar los detalles de las licencias agrupadas, como el tipo de licencia, la capacidad y el servidor de licencias en la sección <LICENSE-COMMANDS> mediante los comandos de licencias agrupados estándar. Para obtener más información, consulte Configurar las licencias de capacidad agrupadas de Citrix ADC.

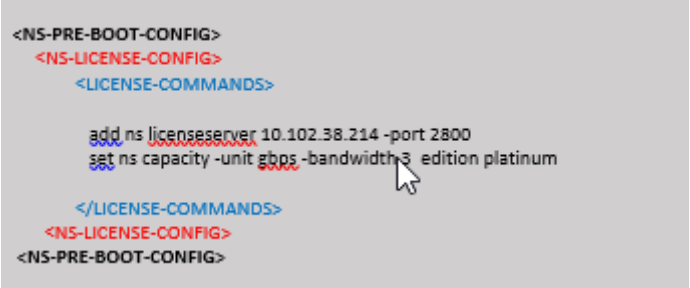
Después de aplicar el <NS-LICENSE-CONFIG>, VPX aparece la edición solicitada al arrancar y VPX intenta extraer las licencias configuradas del servidor de licencias.

- Si la retirada de la licencia se realiza correctamente, el ancho de banda configurado se aplica a VPX.

- Si se produce un error en la retirada de la licencia, la licencia no se recupera del servidor de licencias en un plazo de 10 a 12 minutos aproximadamente. Como resultado, el sistema se reinicia y entra en un estado sin licencia.

Ejemplo:

En el ejemplo siguiente, después de aplicar el <NS-LICENSE-CONFIG>, VPX aparece la edición Premium al arrancar y VPX intenta extraer las licencias configuradas del servidor de licencias (10.102.38.214).



Puede copiar la configuración que se muestra en la captura de pantalla anterior desde aquí:

```
<NS-PRE-BOOT-CONFIG>
   <NS-LICENSE-CONFIG>
        <LICENSE-COMMANDS>
            add ns licenseserver 10.102.38.214 -port 2800
            set ns capacity -unit gbps -bandwidth 3  edition platinum
        </LICENSE-COMMANDS>
    </NS-LICENSE-CONFIG>
</NS-PRE-BOOT-CONFIG>
<!--NeedCopy-->
```

Como se muestra en la siguiente ilustración, puede ejecutar el comando “show license server” y comprobar que el servidor de licencias (10.102.38.214) se ha agregado al VPX.

Bootstrapping

Utilice la etiqueta <NS-BOOTSTRAP> para proporcionar la información de bootstrapping personalizada. Puede utilizar las etiquetas <SKIP-DEFAULT-BOOTSTRAP> y <NEW-BOOTSTRAP-SEQUENCE> dentro de la sección <NS-BOOTSTRAP>. En esta sección se informa al dispositivo Citrix ADC si debe

evitar el arranque predeterminado o no. Si se evita el bootstrapping predeterminado, en esta sección se ofrece la opción de proporcionar una nueva secuencia de bootstrapping.

Configuración de arranque predeterminada

La configuración de arranque predeterminada del dispositivo Citrix ADC sigue estas asignaciones de interfaz:

- **Eth0** - Interfaz de administración con una determinada dirección NSIP.
- **Eth1** - Interfaz orientada al cliente con una determinada dirección VIP.
- **Eth2**: Interfaz orientada al servidor con una determinada dirección SNIP.

Personalizar la configuración bootstrap

Puede omitir la secuencia de arranque predeterminada y proporcionar una nueva secuencia de arranque para la instancia Citrix ADC VPX. Utilice la etiqueta <NS-BOOTSTRAP> para proporcionar la información de bootstrapping personalizada. Por ejemplo, puede cambiar el bootstrapping predeterminado, donde la interfaz de administración (NSIP), la interfaz orientada al cliente (VIP) y la interfaz orientada al servidor (SNIP) siempre se proporcionan en un orden determinado.

En la tabla siguiente se indica el comportamiento de bootstrapping con los distintos valores permitidos en etiquetas <SKIP-DEFAULT-BOOTSTRAP> y <NEW-BOOTSTRAP-SEQUENCE>.

SKIP-DEFAULT-BOOTSTRAP	NEW-BOOTSTRAP-SEQUENCE	Comportamiento bootstrap
SÍ	SÍ	Se omite el comportamiento de bootstrapping predeterminado y se ejecuta una nueva secuencia de arranque personalizada proporcionada en la sección <NS-BOOTSTRAP>.
SÍ	NO	Se omite el comportamiento de arranque predeterminado. Se ejecutan los comandos bootstrap proporcionados en la sección <NS-CONFIG>.

Puede personalizar la configuración de arranque mediante los tres métodos siguientes:

- Proporcionar solo los detalles de la interfaz

- Proporcionar los detalles de la interfaz junto con las direcciones IP y la máscara de subred
- Proporcionar comandos relacionados con el arranque en la sección <NS-CONFIG>

Método 1: arranque personalizado especificando solo los detalles de la interfaz

Se especifican las interfaces de administración, orientadas al cliente y orientadas al servidor, pero no sus direcciones IP y máscaras de subred. Las direcciones IP y las máscaras de subred se completan consultando la infraestructura en la nube.

Ejemplo de arranque personalizado para AWS

Proporciona la secuencia de arranque personalizada como se muestra en el siguiente ejemplo. Para obtener más información, consulte Cómo proporcionar datos de usuario de prearranque en la instancia de nube. La interfaz Eth1 se asigna como interfaz de administración (NSIP), interfaz Eth0 como interfaz de cliente (VIP) e interfaz Eth2 como interfaz de servidor (SNIP). La sección <NS-BOOTSTRAP> contiene solo los detalles de la interfaz y no los detalles de las direcciones IP y las máscaras de subred.

```
<NS-PRE-BOOT-CONFIG>
    <NS-BOOTSTRAP>
        <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
        <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>

        <MGMT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth1 </INTERFACE-NUM>
        </MGMT-INTERFACE-CONFIG>

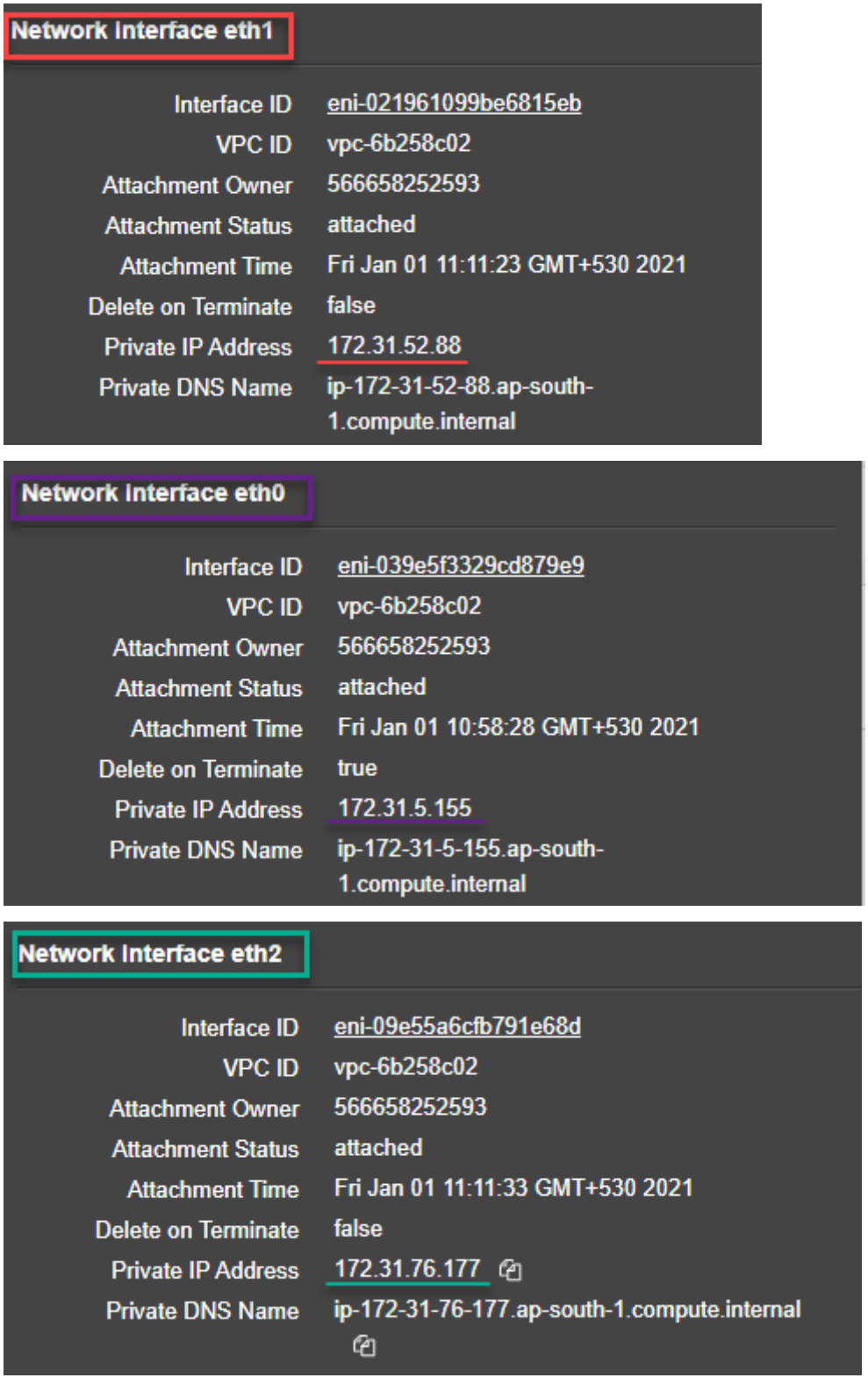
        <CLIENT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth0 </INTERFACE-NUM>
        </CLIENT-INTERFACE-CONFIG>

        <SERVER-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth2 </INTERFACE-NUM>
        </SERVER-INTERFACE-CONFIG>

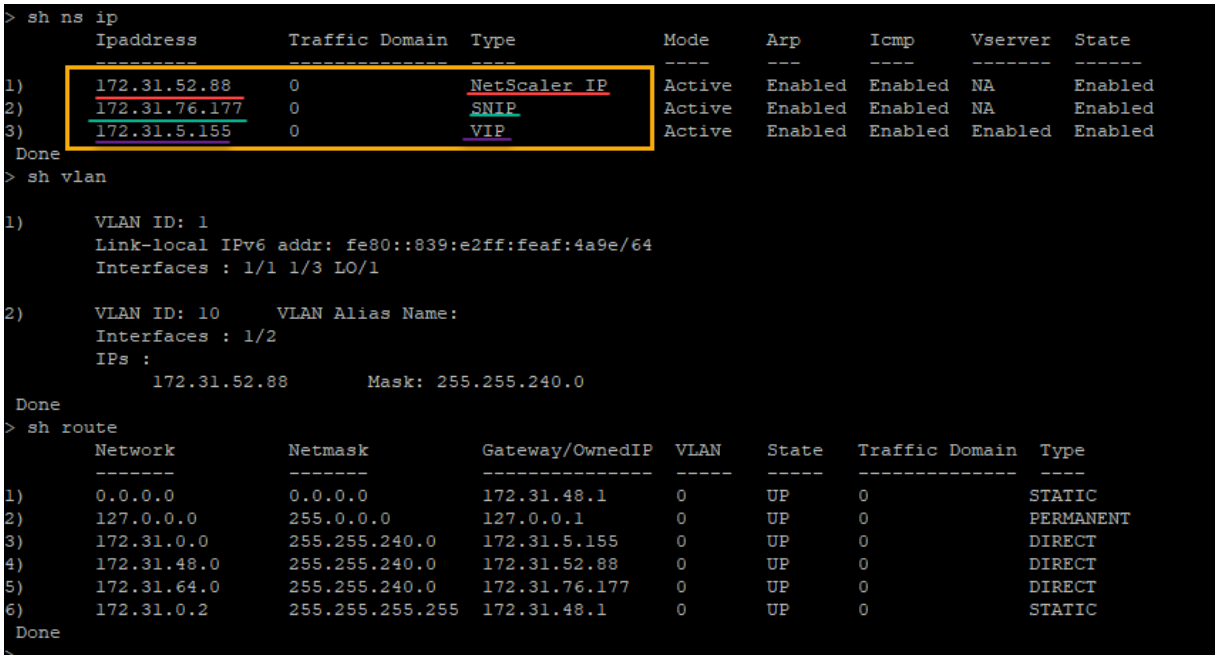
    </NS-BOOT STRAP>
</NS-PRE-BOOT-CONFIG>
```

Después de crear la instancia de VM, en el portal de AWS, puede verificar las propiedades de la interfaz de red de la siguiente manera:

1. Vaya al **portal de AWS > instancias EC2**y seleccione la instancia que ha creado proporcionando la información de arranque personalizada.
2. En la ficha **Descripción**, puede verificar las propiedades de cada interfaz de red como se muestra en las ilustraciones siguientes.



Puede ejecutar el comando `show nsip` en la **CLI de ADC**y verificar las interfaces de red aplicadas a la instancia VPX de ADC durante el primer arranque del dispositivo ADC.



Ejemplo de arranque personalizado para Azure

Proporciona la secuencia de arranque personalizada como se muestra en el siguiente ejemplo. Para obtener más información, consulte Cómo proporcionar datos de usuario de prearranque en la instancia de nube. La interfaz Eth2 se asigna como interfaz de administración (NSIP), interfaz Eth1 como interfaz de cliente (VIP) e interfaz Eth0 como interfaz de servidor (SNIP). La sección <NS-BOOTSTRAP > contiene solo los detalles de la interfaz y no los detalles de las direcciones IP y las máscaras de subred.


```
<NS-PRE-BOOT-CONFIG>

    <NS-BOOTSTRAP>
        <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
        <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>

        <MGMT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth2 </INTERFACE-NUM>
        </MGMT-INTERFACE-CONFIG>

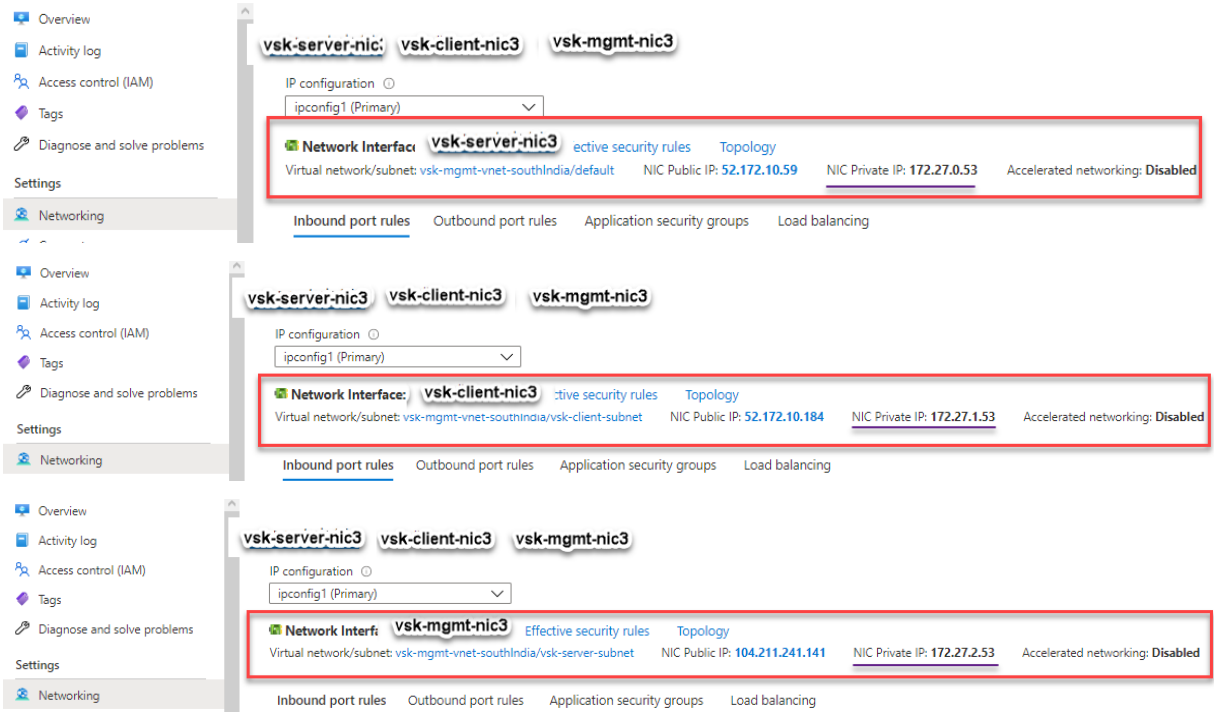
        <CLIENT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth1 </INTERFACE-NUM>
        </CLIENT-INTERFACE-CONFIG>

        <SERVER-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth0 </INTERFACE-NUM>
        </SERVER-INTERFACE-CONFIG>

    </NS-BOOTSTRAP>

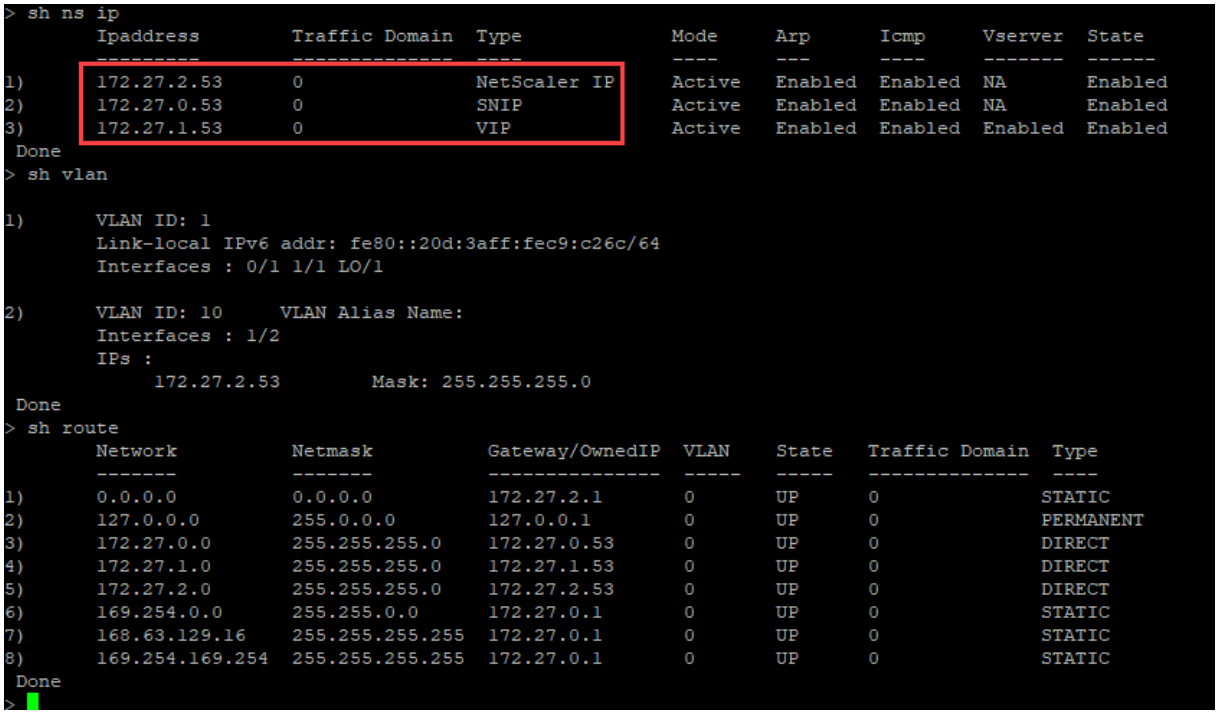
</NS-PRE-BOOT-CONFIG>
```

Puede ver que la instancia Citrix ADC VPX se crea con tres interfaces de red. Vaya al **portal de Azure > Instancia de VM > Redes**y compruebe las propiedades de red de las tres NIC como se muestra en las ilustraciones siguientes.



Puede ejecutar el comando “show nsip” en la CLI de ADC y comprobar que se aplica la nueva secuencia

de arranque especificada en la sección <NS-BOOTSTRAP>. Puede ejecutar el comando “show route” para verificar la máscara de subred.



Ejemplos de bootstrap personalizados para GCP

Proporciona la secuencia de arranque personalizada como se muestra en el siguiente ejemplo. Para obtener más información, consulte Cómo proporcionar datos de usuario de prearranque en la instancia de nube. La interfaz Eth1 se asigna como interfaz de administración (NSIP), interfaz Eth0 como interfaz de cliente (VIP) e interfaz Eth2 como interfaz de servidor (SNIP). La sección <NS-BOOTSTRAP> contiene solo los detalles de la interfaz y no los detalles de las direcciones IP y las máscaras de subred.


```
<NS-PRE-BOOT-CONFIG>
    <NS-BOOTSTRAP>
        <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
        <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>

        <MGMT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth1 </INTERFACE-NUM>
        </MGMT-INTERFACE-CONFIG>

        <CLIENT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth0 </INTERFACE-NUM>
        </CLIENT-INTERFACE-CONFIG>

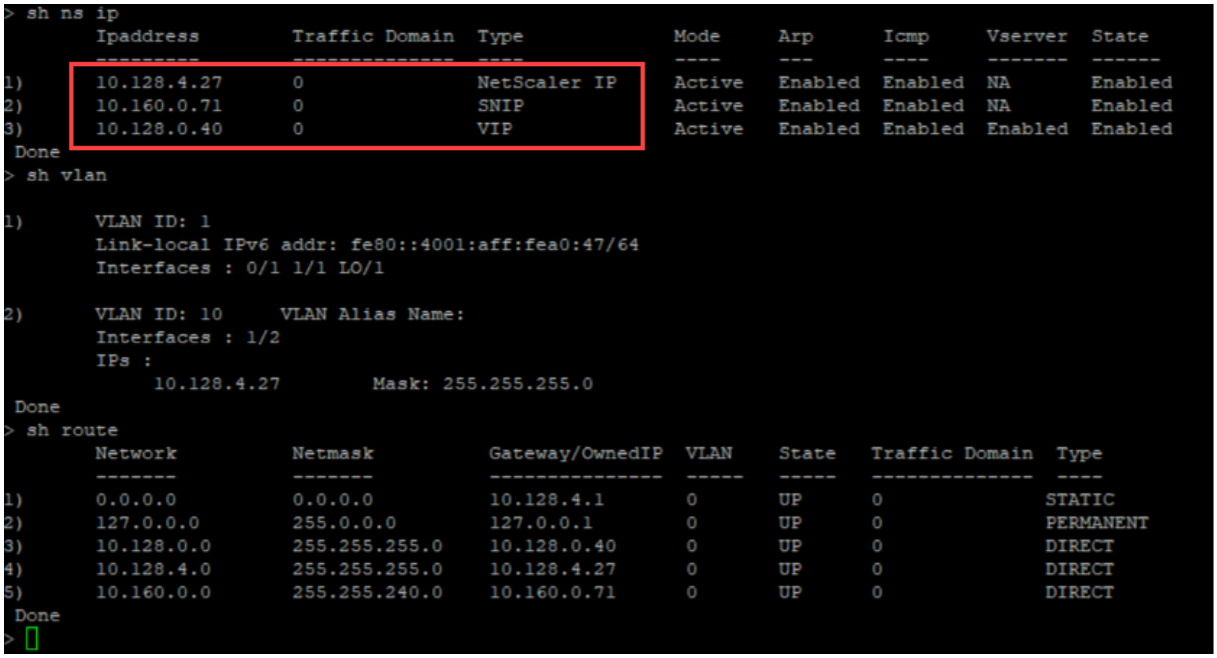
        <SERVER-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth2 </INTERFACE-NUM>
        </SERVER-INTERFACE-CONFIG>

    </NS-BOOT STRAP>
</NS-PRE-BOOT-CONFIG>
```

Después de crear la instancia de VM en el portal de GCP, puede verificar las propiedades de la interfaz de red de la siguiente manera:

1. Seleccione la instancia que ha creado proporcionando la información de arranque personalizada.
2. Vaya a las propiedades de la interfaz de red y compruebe los detalles de la NIC de la siguiente manera

Puede ejecutar el comando `show nsip` en la **CLI de ADC**y verificar las interfaces de red aplicadas a la instancia VPX de ADC durante el primer arranque del dispositivo ADC.



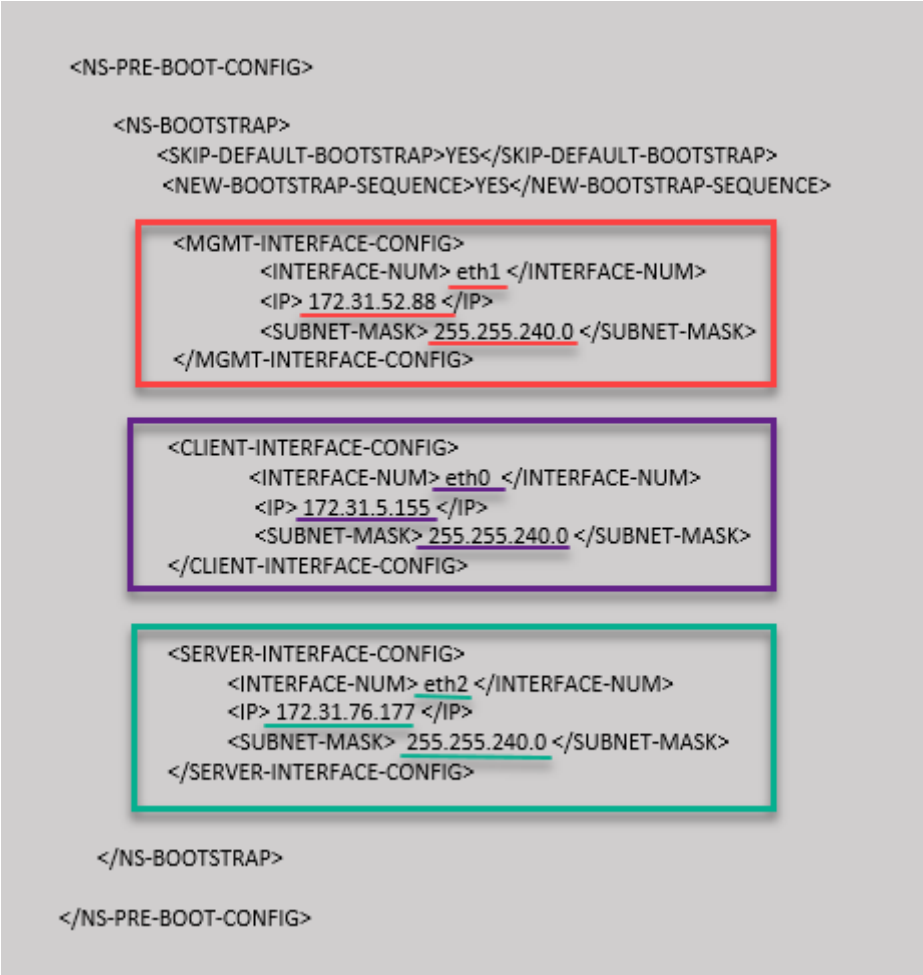
Método 2: arranque personalizado especificando las interfaces, las direcciones IP y las máscaras de subred

Se especifican las interfaces de administración, orientadas al cliente y orientadas al servidor junto con sus direcciones IP y máscara de subred.

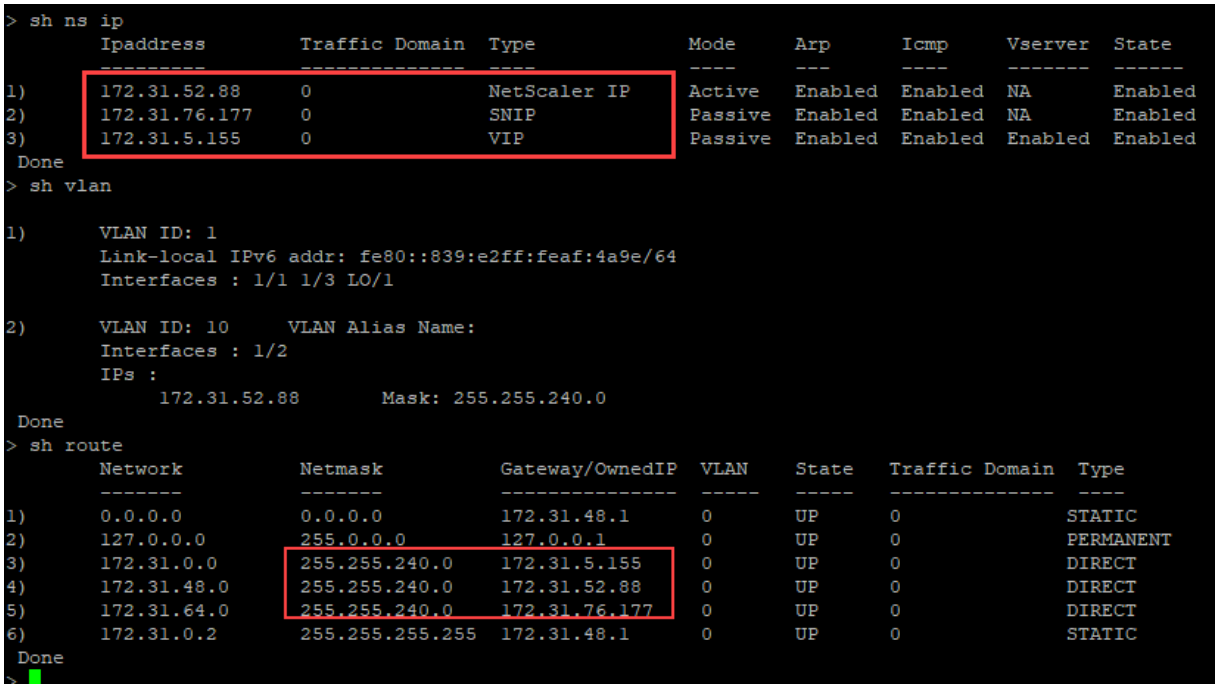
Ejemplos de arranque personalizados para AWS

En el siguiente ejemplo, omite el bootstrap predeterminado y ejecuta una nueva secuencia de arranque para el dispositivo Citrix ADC. Para la nueva secuencia de arranque, especifique los siguientes detalles:

- **Interfaz de administración:** Interfaz - Eth1, NSIP - 172.31.52.88 y máscara de subred - 255.255.240.0
- **Interfaz orientada al cliente:** Interfaz - Eth0, VIP - 172.31.5.155 y máscara de subred - 255.255.240.0.
- **Interfaz orientada al servidor:** Interfaz - Eth2, SNIP - 172.31.76.177 y máscara de subred - 255.255.240.0.



Puede ejecutar el comando `show nsip` en la CLI de ADC y verificar que se haya aplicado la nueva secuencia de arranque especificada en la sección `<NS-BOOTSTRAP>`. Puede ejecutar el comando “show route” para verificar la máscara de subred.



Ejemplo de arranque personalizado para Azure

En el ejemplo siguiente, se menciona una nueva secuencia de arranque para ADC y se omite el bootstrap predeterminado. Proporciona los detalles de la interfaz junto con las direcciones IP y las máscaras de subred de la siguiente manera:

- Interfaz de administración (eth2), NSIP (172.27.2.53) y máscara de subred (255.255.255.0)
- Interfaz orientada al cliente (eth1), VIP (172.27.1.53) y máscara de subred (255.255.255.0)
- Interfaz orientada al servidor (eth0), SNIP (172.27.0.53) y máscara de subred (255.255.255.0)


```
<NS-PRE-BOOT-CONFIG>

    <NS-BOOTSTRAP>
        <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
        <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>

        <MGMT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth2 </INTERFACE-NUM>
            <IP> 172.27.2.53 </IP>
            <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
        </MGMT-INTERFACE-CONFIG>

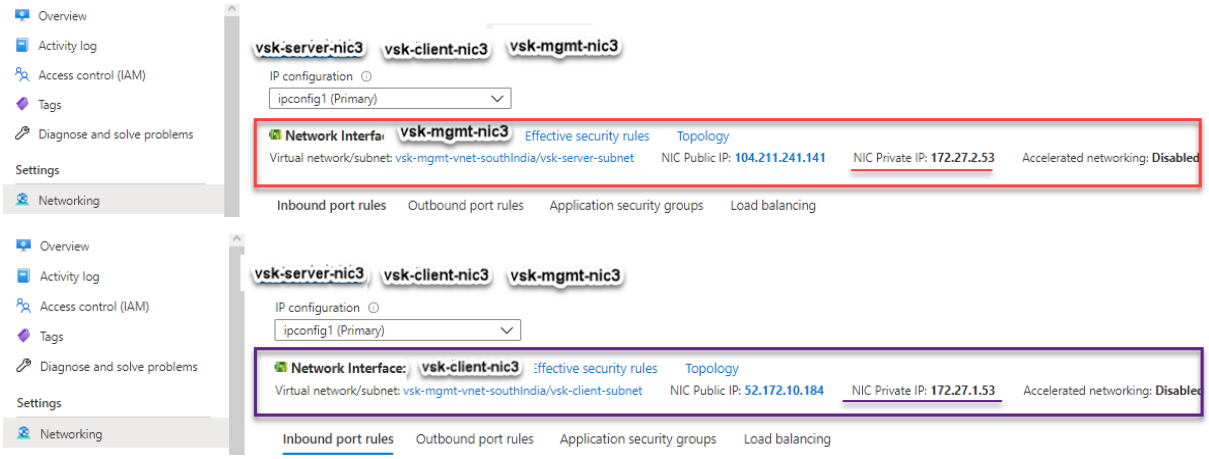
        <CLIENT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth1 </INTERFACE-NUM>
            <IP> 172.27.1.53 </IP>
            <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
            </CLIENT-INTERFACE-CONFIG>

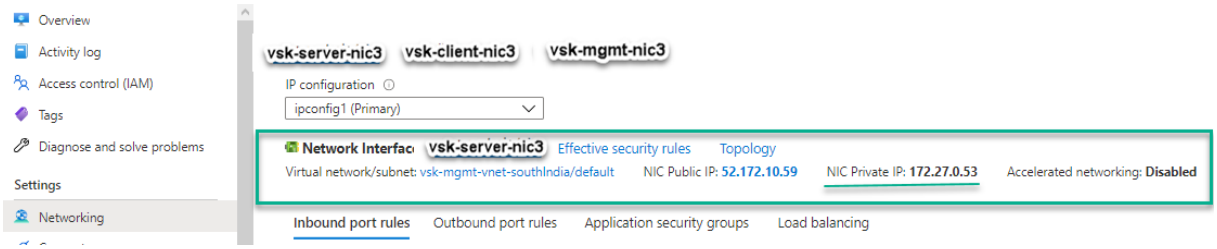
        <SERVER-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth0 </INTERFACE-NUM>
            <IP> 172.27.0.53 </IP>
            <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
        </SERVER-INTERFACE-CONFIG>

    </NS-BOOTSTRAP>

</NS-PRE-BOOT-CONFIG>
```

Puede ver que la instancia Citrix ADC VPX se crea con tres interfaces de red. Vaya al **portal de Azure > Instancia de VM > Redes**y compruebe las propiedades de red de las tres NIC como se muestra en las ilustraciones siguientes.





Puede ejecutar el comando `show nsip` en la CLI de ADC y verificar que se haya aplicado la nueva secuencia de arranque especificada en la sección <NS-BOOTSTRAP>. Puede ejecutar el comando "show route" para verificar la máscara de subred.

```
> sh ns ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----             ----     ---      ----     -------  ------
1)      172.27.2.53      0               NetScaler IP     Active   Enabled  Enabled  NA       Enabled
2)      172.27.0.53      0               SNIP             Active   Enabled  Enabled  NA       Enabled
3)      172.27.1.53      0               VIP              Active   Enabled  Enabled  Enabled  Enabled
 Done
> sh vlan

1)      VLAN ID: 1
        Link-local IPv6 addr: fe80::20d:3aff:fec9:c26c/64
        Interfaces : 0/1 1/1 LO/1

2)      VLAN ID: 10     VLAN Alias Name:
        Interfaces : 1/2
        IPs :
             172.27.2.53        Mask: 255.255.255.0
 Done
> sh route
        Network          Netmask          Gateway/OwnedIP  VLAN    State   Traffic Domain  Type
        -------          -------          ---------------  -----   -----   --------------  ----
1)      0.0.0.0          0.0.0.0          172.27.2.1       0       UP      0               STATIC
2)      127.0.0.0        255.0.0.0        127.0.0.1        0       UP      0               PERMANENT
3)      172.27.0.0       255.255.255.0    172.27.0.53      0       UP      0               DIRECT
4)      172.27.1.0       255.255.255.0    172.27.1.53      0       UP      0               DIRECT
5)      172.27.2.0       255.255.255.0    172.27.2.53      0       UP      0               DIRECT
6)      169.254.0.0      255.255.0.0      172.27.0.1       0       UP      0               STATIC
7)      168.63.129.16    255.255.255.255  172.27.0.1       0       UP      0               STATIC
8)      169.254.169.254  255.255.255.255  172.27.0.1       0       UP      0               STATIC
 Done
```

Ejemplo de bootstrap personalizado para GCP

En el ejemplo siguiente, se menciona una nueva secuencia de arranque para ADC y se omite el bootstrap predeterminado. Proporciona los detalles de la interfaz junto con las direcciones IP y las máscaras de subred de la siguiente manera:

- Interfaz de administración (eth2), NSIP (10.128.4.31) y máscara de subred (255.255.255.0)
- Interfaz orientada al cliente (eth1), VIP (10.128.0.43) y máscara de subred (255.255.255.0)
- Interfaz orientada al servidor (eth0), SNIP (10.160.0.75) y máscara de subred (255.255.255.0)


```
<NS-PRE-BOOT-CONFIG>
   <NS-BOOTSTRAP>
         <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
         <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>
          <MGMT-INTERFACE-CONFIG>
               <INTERFACE-NUM> eth2 </INTERFACE-NUM>
               <IP> 10.128.4.31 </IP>
               <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
           </MGMT-INTERFACE-CONFIG>
          <CLIENT-INTERFACE-CONFIG>
               <INTERFACE-NUM> eth1 </INTERFACE-NUM>
               <IP> 10.128.0.43 </IP>
               <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
          </CLIENT-INTERFACE-CONFIG>
          <SERVER-INTERFACE-CONFIG>
               <INTERFACE-NUM> eth0 </INTERFACE-NUM>
               <IP> 10.160.0.75 </IP>
               <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
          </SERVER-INTERFACE-CONFIG>
   </NS-BOOTSTRAP>
</NS-PRE-BOOT-CONFIG>
```

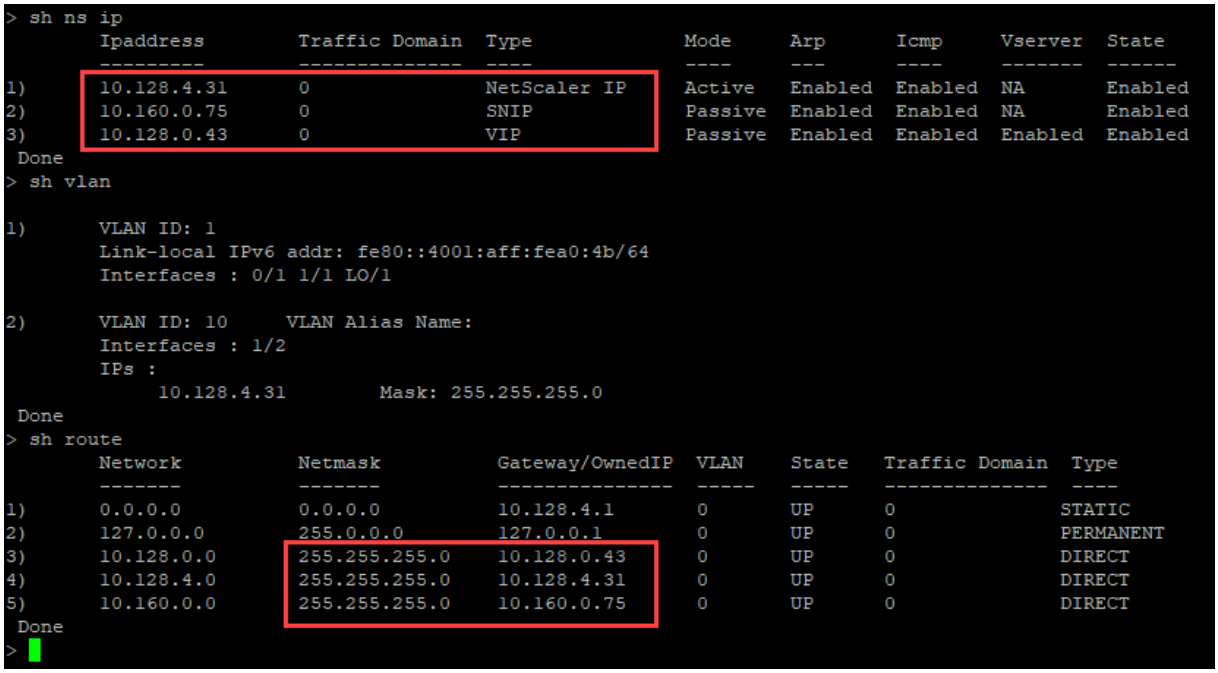
Una vez creada la instancia de VM en el portal de GCP con el bootstrap personalizado, puede verificar las propiedades de la interfaz de red de la siguiente manera:

1. Seleccione la instancia que ha creado proporcionando la información de arranque personalizada.
2. Vaya a las propiedades de la interfaz de red y compruebe los detalles de la NIC de la siguiente manera

Network interfaces

Name	Network	Subnetwork	Primary internal IP	Alias IP ranges	External IP	Network Tier	IP forwarding	Network details
nic0	default	default	vsk-defnw-st-ip1 (10.160.0.75)	–	34.93.216.90 (ephemeral)	Premium	Off	View details
nic1	vsk-vpc-network-1	asia-south1-subnet-1	vsk-vpc-nw1-st-ip1 (10.128.0.43)	–	35.244.40.113 (ephemeral)	Premium		View details
nic2	vsk-vpc-network-2	asia-south1-subnet-5	vsk-nw2-st-ip-1 (10.128.4.31)	–	34.93.202.214 (ephemeral)	Premium		View details

Puede ejecutar el comando `show nsip` en la CLI de ADC y verificar que se haya aplicado la nueva secuencia de arranque especificada en la sección <NS-BOOTSTRAP>. Puede ejecutar el comando “show route” para verificar la máscara de subred.



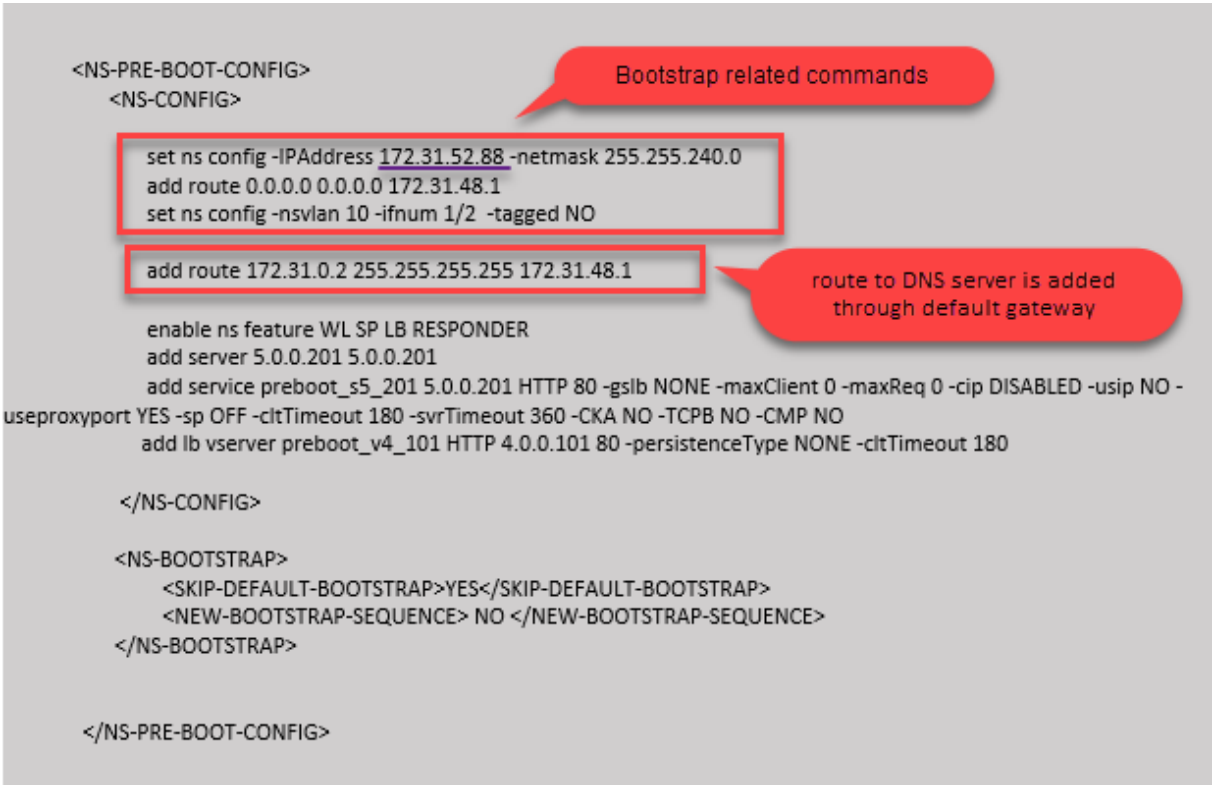
Método 3: Arranque personalizado proporcionando comandos relacionados con el bootstrap en la sección <NS-CONFIG>

Puede proporcionar los comandos relacionados con el arranque en la sección <NS-CONFIG>. En la sección <NS-BOOTSTRAP>, debe especificar <NEW-BOOTSTRAP-SEQUENCE> como "No" para ejecutar los comandos de arranque de la sección <NS-CONFIG>. También debe proporcionar los comandos para asignar NSIP, ruta predeterminada y NSVLAN. Además, proporcione los comandos relevantes para la nube que utiliza.

Antes de proporcionar un arranque personalizado, asegúrese de que su infraestructura en la nube admite una configuración de interfaz concreta.

Ejemplo de arranque personalizado para AWS

En este ejemplo, los comandos relacionados con bootstrap se proporcionan en la sección <NS-CONFIG>. La sección <NS-BOOTSTRAP> indica que se omite el bootstrapping predeterminado y se ejecuta la información de arranque personalizada proporcionada en la sección <NS-CONFIG>. También debe proporcionar los comandos para crear NSIP, agregar una ruta predeterminada y agregar NSVLAN.



Puede copiar la configuración que se muestra en la captura de pantalla anterior desde aquí:

```
<NS-PRE-BOOT-CONFIG>
    <NS-CONFIG>

        set ns config -IPAddress 172.31.52.88 -netmask 255.255.240.0
        add route 0.0.0.0 0.0.0.0 172.31.48.1
        set ns config -nsvlan 10 -ifnum 1/2  -tagged NO
        add route 172.31.0.2 255.255.255.255 172.31.48.1

        enable ns feature WL SP LB RESPONDER
        add server 5.0.0.201 5.0.0.201
        add service preboot_s5_201 5.0.0.201 HTTP 80 -gslb NONE -
            maxClient 0 -maxReq 0 -cip DISABLED -usip NO - useproxyport
            YES -sp OFF -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO
             -CMP NO
        add lb vserver preboot_v4_101 HTTP 4.0.0.101 80 -
            persistenceType NONE -cltTimeout 180

    </NS-CONFIG>

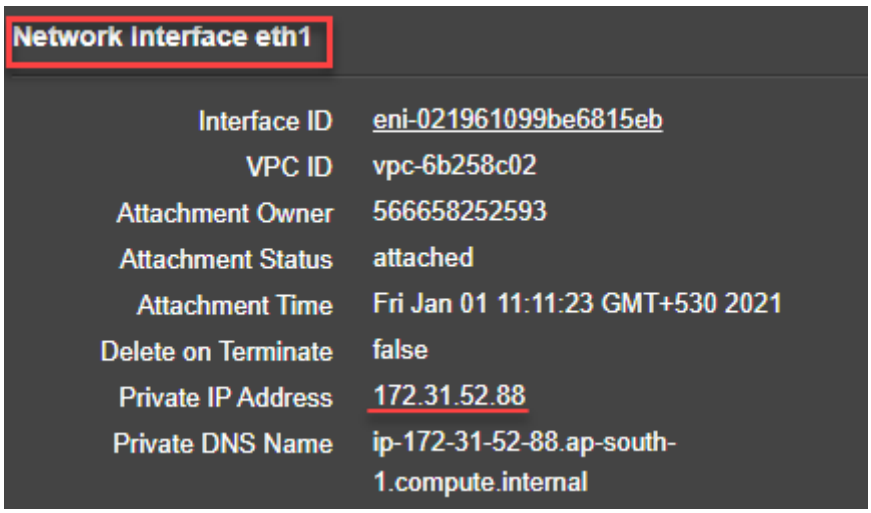
    <NS-BOOTSTRAP>
```

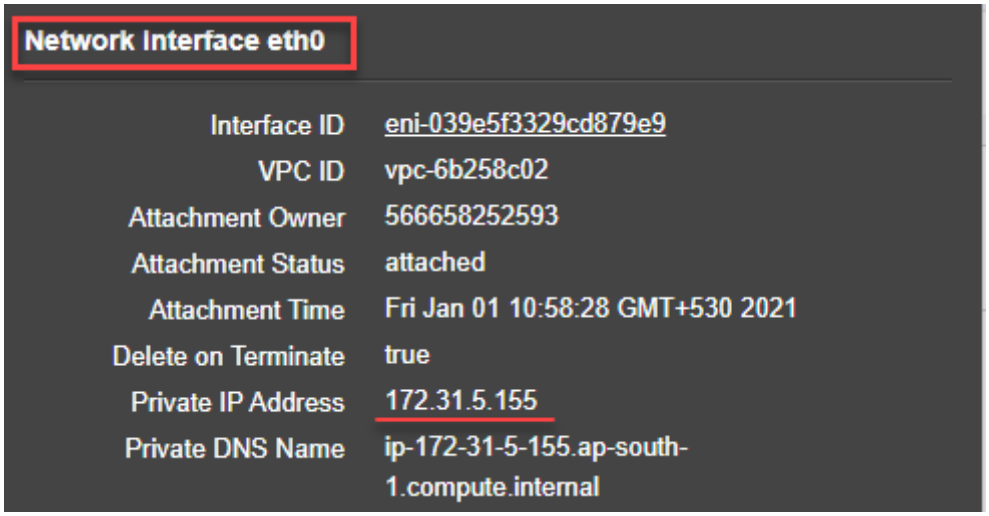


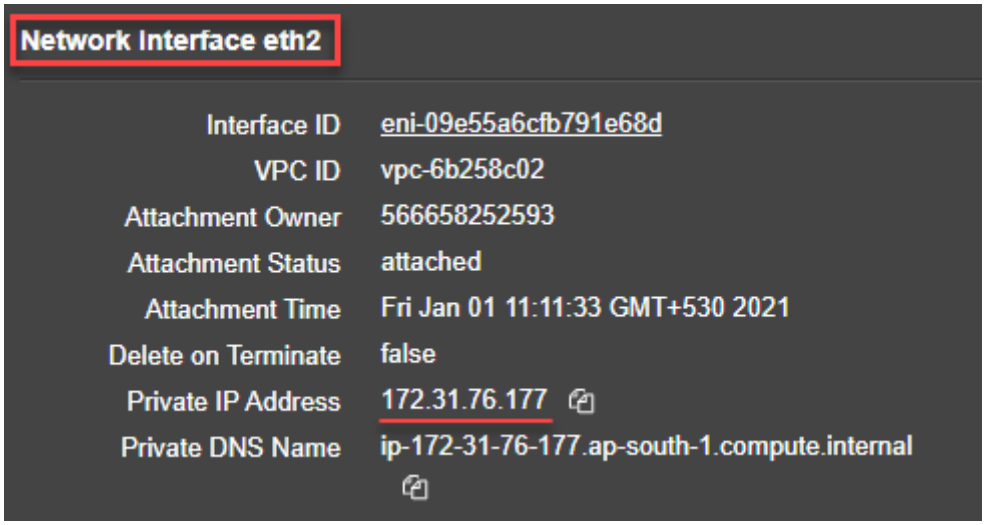
```
17        <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
18        <NEW-BOOTSTRAP-SEQUENCE> NO </NEW-BOOTSTRAP-SEQUENCE>
19       </NS-BOOTSTRAP>
20
21
22  </NS-PRE-BOOT-CONFIG>
23  <!--NeedCopy-->
```

Después de crear la instancia de VM, en el portal de AWS, puede verificar las propiedades de la interfaz de red de la siguiente manera:

1. Vaya al **portal de AWS > instancias EC2**y seleccione la instancia que ha creado proporcionando la información de arranque personalizada.
2. En la ficha **Descripción**, puede verificar las propiedades de cada interfaz de red como se muestra en las ilustraciones siguientes.







Puede ejecutar el comando `show nsip` en la **CLI de ADC**y verificar las interfaces de red aplicadas a la instancia VPX de ADC durante el primer arranque del dispositivo ADC.

```
> sh ns ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----             ----     ---      ----     -------  ------
1)      172.31.52.88     0               NetScaler IP     Active   Enabled  Enabled  NA       Enabled
2)      4.0.0.101        0               VIP              Active   Enabled  Enabled  Enabled  Enabled
 Done
> sh vlan

1)      VLAN ID: 1
        Link-local IPv6 addr: fe80::839:e2ff:feaf:4a9e/64
        Interfaces : 1/1 1/3 LO/1

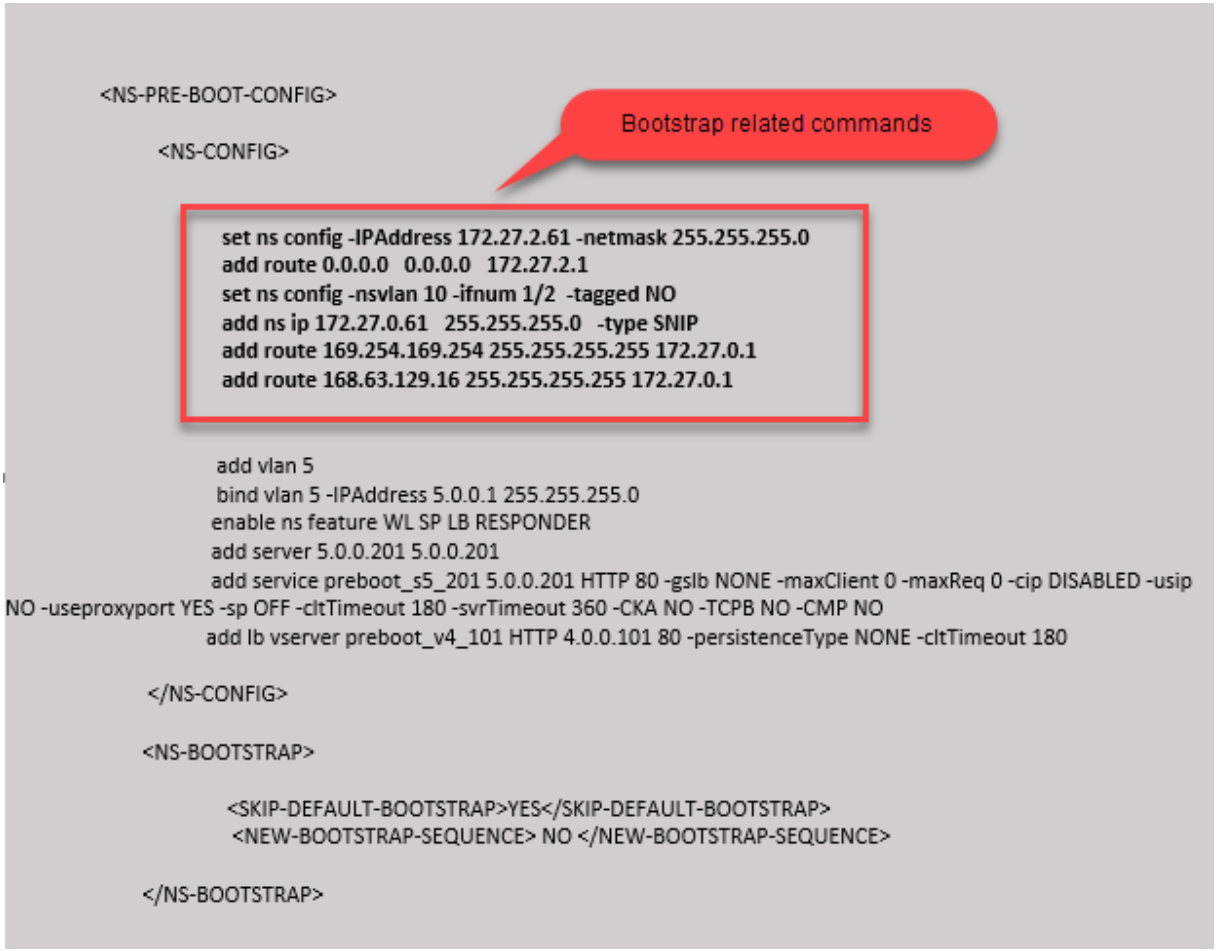
2)      VLAN ID: 10     VLAN Alias Name:
        Interfaces : 1/2
        IPs :
             172.31.52.88       Mask: 255.255.240.0
 Done
> sh route
        Network          Netmask          Gateway/OwnedIP  VLAN    State   Traffic Domain  Type
        -------          -------          ---------------  -----   -----   --------------  ----
1)      0.0.0.0          0.0.0.0          172.31.48.1      0       UP      0               STATIC
2)      127.0.0.0        255.0.0.0        127.0.0.1        0       UP      0               PERMANENT
3)      172.31.48.0      255.255.240.0    172.31.52.88     0       UP      0               DIRECT
4)      172.31.0.2       255.255.255.255  172.31.48.1      0       UP      0               STATIC
 Done
>
```

Ejemplo de arranque personalizado para Azure

En este ejemplo, los comandos relacionados con bootstrap se proporcionan en la sección <NS-CONFIG>. La sección <NS-BOOTSTRAP> indica que se omite el bootstrapping predeterminado y se ejecuta la información de arranque personalizada proporcionada en la sección <NS-CONFIG>.

> Nota:
>
> Para la nube de Azure, el servidor de metadatos de instancias (IMDS) y los servidores DNS solo se puede acceder a través de la interfaz principal (Eth0). Por lo tanto, si la interfaz Eth0 no se

> utiliza como interfaz de administración (NSIP), la interfaz Eth0 debe configurarse al menos como SNIP para el acceso IMDS o DNS al trabajo. También se debe agregar la ruta al extremo IMDS (169.254.169.254) y al extremo DNS (168.63.129.16) a través de la puerta de enlace de Eth0.




```
<NS-PRE-BOOT-CONFIG>

   <NS-CONFIG>

        set ns config -IPAddress 172.27.2.61 -netmask 255.255.255.0
        add route 0.0.0.0   0.0.0.0   172.27.2.1
        set ns config -nsvlan 10 -ifnum 1/2  -tagged NO
        add ns ip 172.27.0.61   255.255.255.0   -type SNIP
        add route 169.254.169.254 255.255.255.255 172.27.0.1
        add route 168.63.129.16 255.255.255.255 172.27.0.1

        add vlan 5
        bind vlan 5 -IPAddress 5.0.0.1 255.255.255.0
        enable ns feature WL SP LB RESPONDER
```



```
        add server 5.0.0.201 5.0.0.201
        add service preboot_s5_201 5.0.0.201 HTTP 80 -gslb NONE -
            maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport
            YES -sp OFF -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO
             -CMP NO
        add lb vserver preboot_v4_101 HTTP 4.0.0.101 80 -
            persistenceType NONE -cltTimeout 180

    </NS-CONFIG>

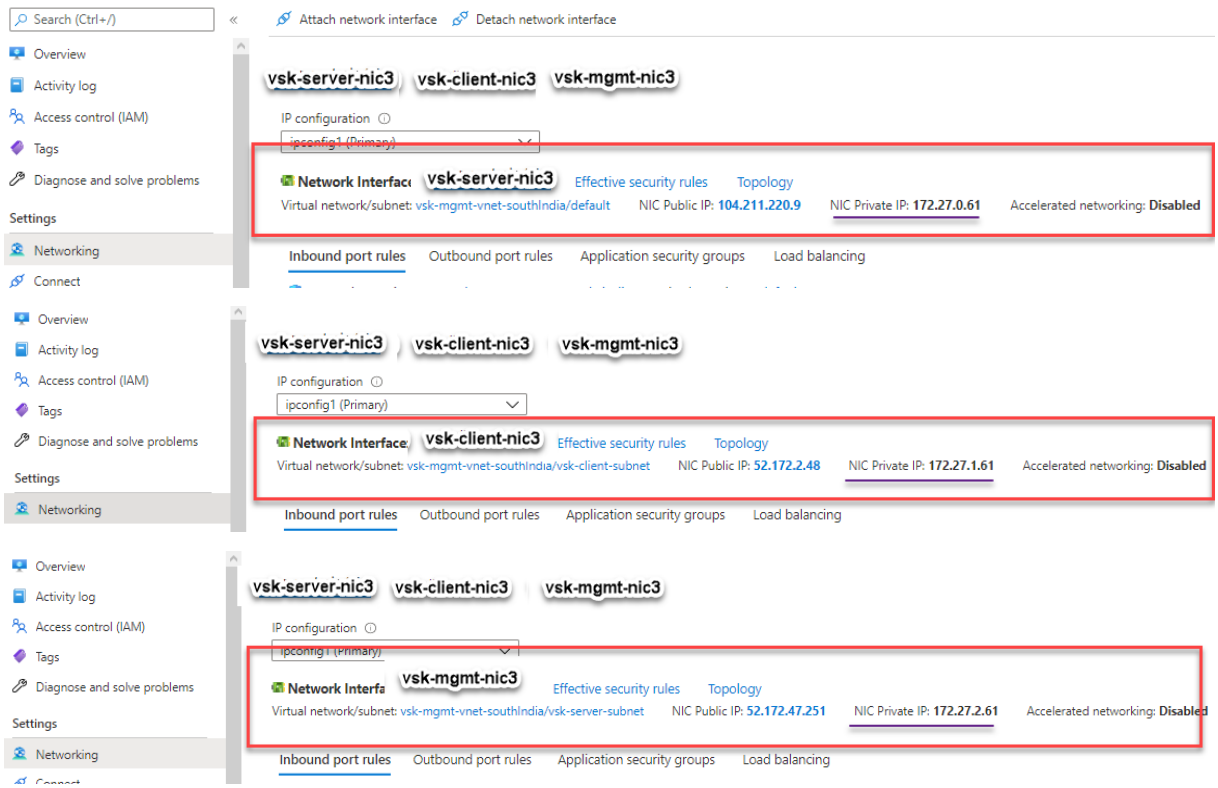
    <NS-BOOTSTRAP>

    <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
    <NEW-BOOTSTRAP-SEQUENCE> NO </NEW-BOOTSTRAP-SEQUENCE>

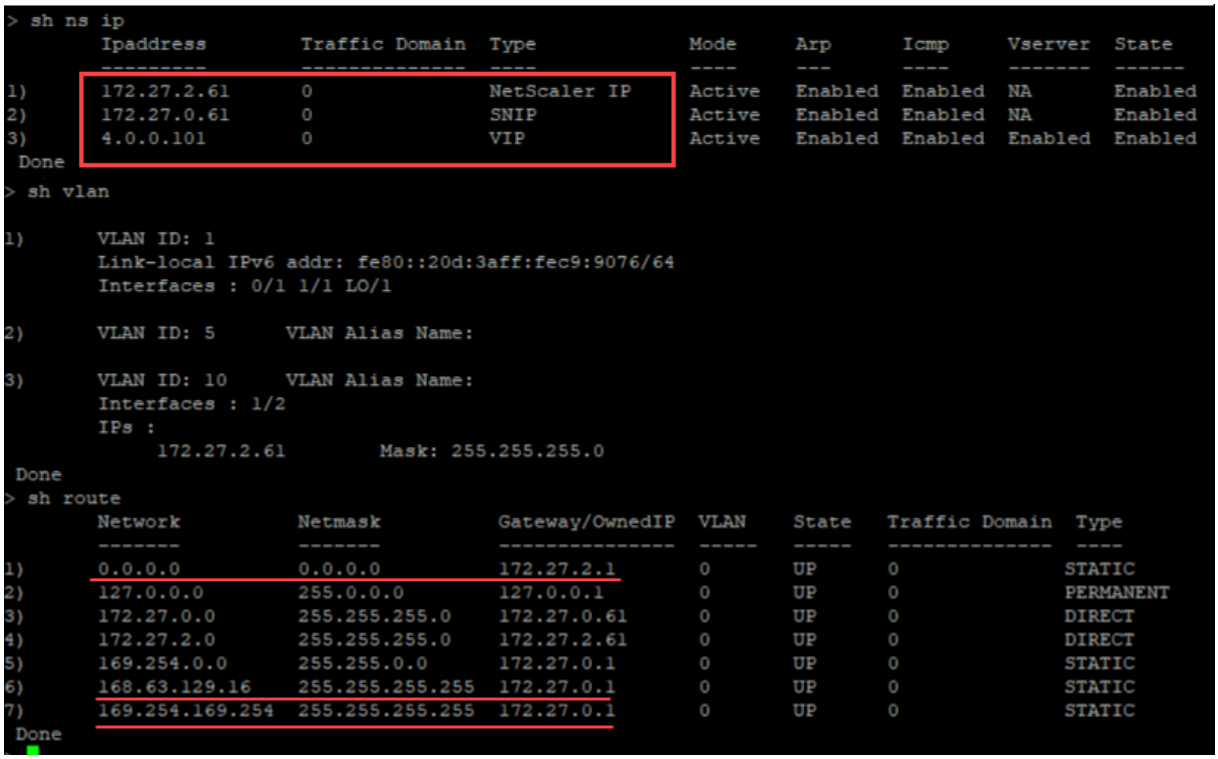
    </NS-BOOTSTRAP>

</NS-PRE-BOOT-CONFIG>
<!--NeedCopy-->
```

Puede ver que la instancia Citrix ADC VPX se crea con tres interfaces de red. Vaya al **portal de Azure > Instancia de VM > Redes**y compruebe las propiedades de red de las tres NIC como se muestra en las ilustraciones siguientes.



Puede ejecutar el comando `show nsip` en la CLI de ADC y verificar que se haya aplicado la nueva secuencia de arranque especificada en la sección <NS-BOOTSTRAP>. Puede ejecutar el comando "show route" para verificar la máscara de subred.



```
> sh ns ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----             ----     ---      ----     -------  -----
1)      172.27.2.61      0               NetScaler IP     Active   Enabled  Enabled  NA       Enabled
2)      172.27.0.61      0               SNIP             Active   Enabled  Enabled  NA       Enabled
3)      4.0.0.101        0               VIP              Active   Enabled  Enabled  Enabled  Enabled
 Done
> sh vlan

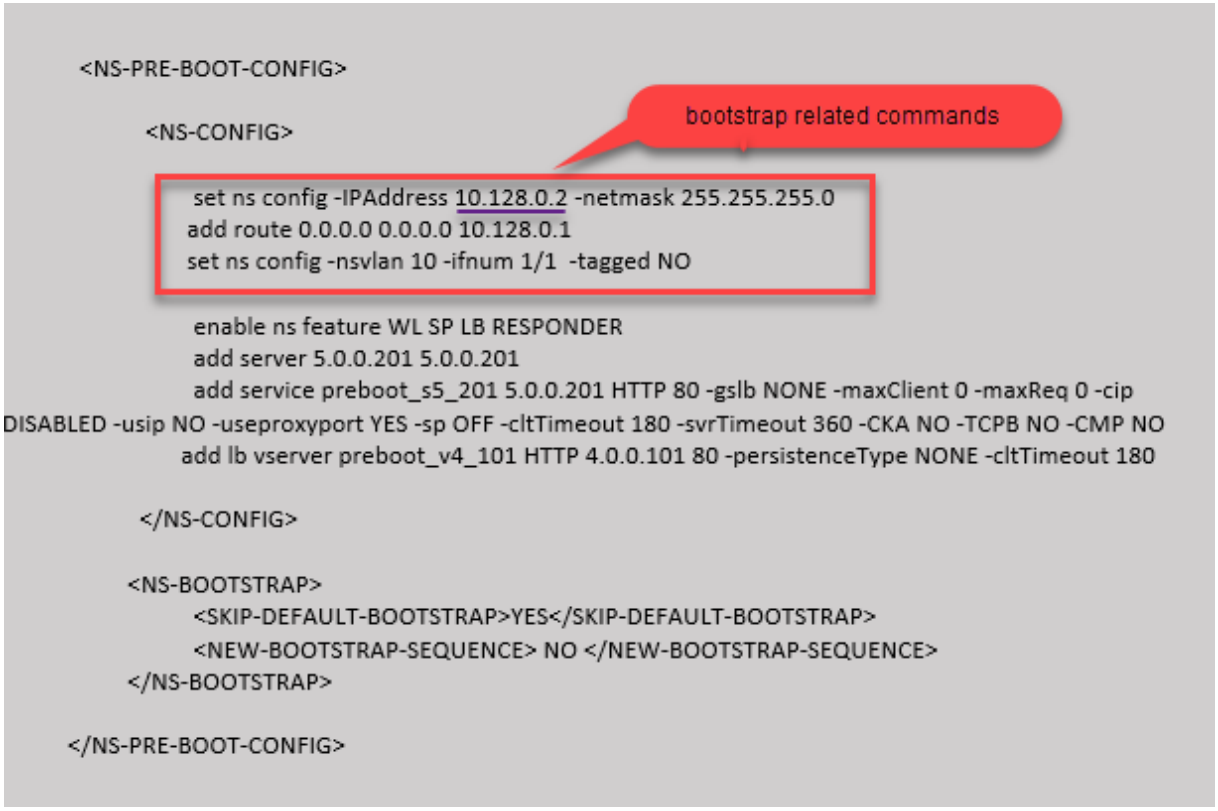
1)      VLAN ID: 1
        Link-local IPv6 addr: fe80::20d:3aff:fec9:9076/64
        Interfaces : 0/1 1/1 LO/1

2)      VLAN ID: 5      VLAN Alias Name:

3)      VLAN ID: 10     VLAN Alias Name:
        Interfaces : 1/2
        IPs :
             172.27.2.61        Mask: 255.255.255.0
 Done
> sh route
        Network          Netmask          Gateway/OwnedIP  VLAN    State   Traffic Domain  Type
        -------          -------          ---------------  -----   -----   --------------  ----
1)      0.0.0.0          0.0.0.0          172.27.2.1       0       UP      0               STATIC
2)      127.0.0.0        255.0.0.0        127.0.0.1        0       UP      0               PERMANENT
3)      172.27.0.0       255.255.255.0    172.27.0.61      0       UP      0               DIRECT
4)      172.27.2.0       255.255.255.0    172.27.2.61      0       UP      0               DIRECT
5)      169.254.0.0      255.255.0.0      172.27.0.1       0       UP      0               STATIC
6)      168.63.129.16    255.255.255.255  172.27.0.1       0       UP      0               STATIC
7)      169.254.169.254  255.255.255.255  172.27.0.1       0       UP      0               STATIC
 Done
```

Ejemplo de bootstrap personalizado para GCP

En este ejemplo, los comandos relacionados con bootstrap se proporcionan en la sección <NS-CONFIG>. La sección <NS-BOOTSTRAP> indica que se omite el bootstrapping predeterminado y se aplica la información de arranque personalizada proporcionada en la sección <NS-CONFIG>.



Puede copiar la configuración que se muestra en la captura de pantalla anterior desde aquí:

```
<NS-PRE-BOOT-CONFIG>

    <NS-CONFIG>

        set ns config -IPAddress 10.128.0.2 -netmask 255.255.255.0
        add route 0.0.0.0 0.0.0.0 10.128.0.1
        set ns config -nsvlan 10 -ifnum 1/1  -tagged NO

        enable ns feature WL SP LB RESPONDER
        add server 5.0.0.201 5.0.0.201
        add service preboot_s5_201 5.0.0.201 HTTP 80 -gslb NONE -
            maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport
            YES -sp OFF -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO
             -CMP NO
        add lb vserver preboot_v4_101 HTTP 4.0.0.101 80 -
            persistenceType NONE -cltTimeout 180

    </NS-CONFIG>

    <NS-BOOTSTRAP>
```

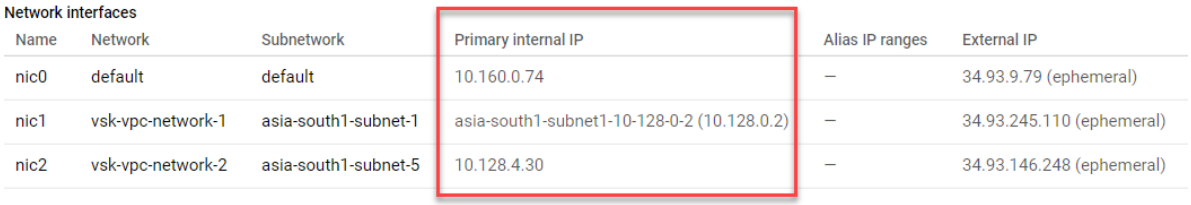


```
        <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
        <NEW-BOOTSTRAP-SEQUENCE> NO </NEW-BOOTSTRAP-SEQUENCE>
    </NS-BOOTSTRAP>

</NS-PRE-BOOT-CONFIG>
<!--NeedCopy-->
```

Una vez creada la instancia de VM en el portal de GCP con el bootstrap personalizado, puede verificar las propiedades de la interfaz de red de la siguiente manera:

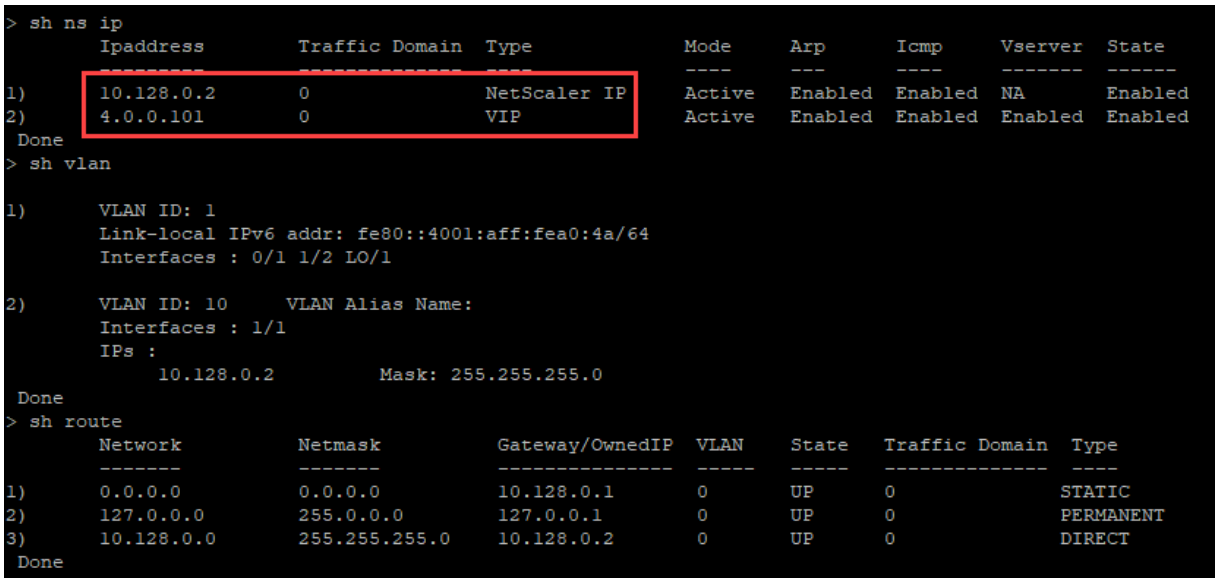
1. Seleccione la instancia que ha creado proporcionando la información de arranque personalizada.
2. Desplácese hasta las propiedades de la interfaz de red y compruebe los detalles de la NIC como se muestra en la ilustración.



Network interfaces

Name	Network	Subnetwork	Primary internal IP	Alias IP ranges	External IP
nic0	default	default	10.160.0.74	–	34.93.9.79 (ephemeral)
nic1	vsk-vpc-network-1	asia-south1-subnet-1	asia-south1-subnet1-10-128-0-2 (10.128.0.2)	–	34.93.245.110 (ephemeral)
nic2	vsk-vpc-network-2	asia-south1-subnet-5	10.128.4.30	–	34.93.146.248 (ephemeral)

Puede ejecutar el comando `show nsip` en la **CLI de ADC**y verificar que las configuraciones proporcionadas en la sección <NS-CONFIG> anterior se apliquen en el primer arranque del dispositivo ADC.



```
> sh ns ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----             ----     ---      ----     -------  -----
1)      10.128.0.2       0               NetScaler IP     Active   Enabled  Enabled  NA       Enabled
2)      4.0.0.101        0               VIP              Active   Enabled  Enabled  Enabled  Enabled
 Done
> sh vlan

1)      VLAN ID: 1
        Link-local IPv6 addr: fe80::4001:aff:fea0:4a/64
        Interfaces : 0/1 1/2 LO/1

2)      VLAN ID: 10     VLAN Alias Name:
        Interfaces : 1/1
        IPs :
             10.128.0.2         Mask: 255.255.255.0
 Done
> sh route
        Network          Netmask          Gateway/OwnedIP  VLAN    State   Traffic Domain  Type
        -------          -------          ---------------  -----   -----   --------------  ----
1)      0.0.0.0          0.0.0.0          10.128.0.1       0       UP      0               STATIC
2)      127.0.0.0        255.0.0.0        127.0.0.1        0       UP      0               PERMANENT
3)      10.128.0.0       255.255.255.0    10.128.0.2       0       UP      0               DIRECT
 Done
```

Impacto de adjuntar y separar NIC en AWS y Azure

AWS y Azure ofrecen la opción de adjuntar una interfaz de red a una instancia y separar una interfaz de red de una instancia. La conexión o desconexión de interfaces podría alterar las posiciones de la interfaz. Por lo tanto, Citrix recomienda que se abstengan de separar interfaces de la instancia VPX de ADC.

Si desconecta o adjunta una interfaz cuando se configura el bootstrapping personalizado, la instancia Citrix ADC VPX reasigna la IP principal de la interfaz recién disponible en la posición de la interfaz de administración como NSIP. Si no hay más interfaces disponibles después de la que desconectó, la primera interfaz se transforma en la interfaz de administración de la instancia VPX de ADC.

Por ejemplo, se presenta una instancia de Citrix ADC VPX con 3 interfaces: Eth0 (SNIP), Eth1 (NSIP) y Eth2 (VIP). Si desactiva la interfaz Eth1 de la instancia, que es una interfaz de administración, ADC configura la siguiente interfaz disponible (Eth2) como interfaz de administración. Por lo tanto, se sigue accediendo a la instancia VPX de ADC a través de la IP principal de la interfaz Eth2. Si Eth2 tampoco está disponible, la interfaz restante (Eth0) se hace la interfaz de administración. Por lo tanto, el acceso a la instancia VPX de ADC sigue existiendo.

Consideremos una asignación diferente de interfaces de la siguiente manera: Eth0 (SNIP), Eth1 (VIP) y Eth2 (NSIP). Si desactiva Eth2 (NSIP), porque no hay nueva interfaz disponible después de Eth2, la primera interfaz (Eth0) se transforma en la interfaz de administración.

Mejore el rendimiento de SSL-TPS en plataformas de nube pública

April 21, 2022

Puede obtener un mejor rendimiento de SSL-TPS en las nubes de AWS y GCP si distribuye los pesos del motor de paquetes (PE) por igual. La activación de esta función puede provocar una ligera caída en el rendimiento de HTTP de entre un 10 y un 12%.

En las nubes de AWS y GCP, las instancias de Citrix ADC VPX con 10 a 16 vCPU no muestran ninguna mejora en el rendimiento porque los pesos de PE se distribuyen por igual de forma predeterminada.

> Nota:
>
> En la nube de Azure, los pesos de PE se distribuyen equitativamente de forma predeterminada. Esta función no mejora el rendimiento de las instancias de Azure.

Configurar el modo PE mediante la CLI de Citrix ADC

Después de configurar el modo PE, debe reiniciar el sistema para que los cambios de configuración surtan efecto.

En el símbolo del sistema, escriba:

```
set cpuparam pemode [CPUBOUND | Default]
<!--NeedCopy-->
```


Cuando el modo PE se establece en CPUBOUND, las ponderaciones PE se distribuyen equitativamente.
Cuando el modo PE se establece en DEFAULT, las ponderaciones PE se establecen en los valores predeterminados.

> Nota:
>
> Este comando es específico del nodo. En una configuración de clúster o de alta disponibilidad, debe ejecutar el comando en cada nodo. Si ejecuta el comando en CLIP, se produce el siguiente error:
> `Operation not permitted on CLIP`

Para mostrar el estado del modo PE configurado, ejecute el siguiente comando:

```
1 show cpuparam
2 <!--NeedCopy-->
```

Ejemplo:

```
1 > show cpuparam
2     Pemode:  CPUBOUND
3  Done
4 <!--NeedCopy-->
```

Aplicar la configuración del modo PE en el primer arranque del dispositivo Citrix ADC en la nube

Para aplicar la configuración del modo PE en el primer arranque del dispositivo Citrix ADC en la nube, debe crear un archivo `/nsconfig/.cpubound.conf` mediante el script personalizado. Para obtener más información, consulte Aplicar configuraciones de Citrix ADC VPX en el primer arranque del dispositivo Citrix ADC en la nube.

Instalar una instancia de Citrix ADC VPX en un servidor desnudo

August 20, 2021

Un bare metal es un servidor físico totalmente dedicado que ofrece aislamiento físico, totalmente integrado en el entorno de nube. También se conoce como servidor de un solo arrendatario. El ar-

rendamiento único le permite evitar el efecto vecino ruidoso. Con solo metal, no sufrirá el efecto del "vecino ruidoso" porque será el único usuario.

Un servidor desnudo instalado con un hipervisor proporciona un conjunto de administración para crear máquinas virtuales en el servidor. El hipervisor no ejecuta aplicaciones de forma nativa. Su propósito es virtualizar sus cargas de trabajo en máquinas virtuales independientes para obtener la flexibilidad y fiabilidad de la virtualización.

Requisitos previos para instalar la instancia de Citrix ADC VPX en servidores básicos

Se debe obtener un servidor desnudo de un proveedor de nube que cumpla con todos los requisitos del sistema para el hipervisor respectivo.

Instale la instancia de Citrix ADC VPX en servidores desnudos

Para instalar instancias de Citrix ADC VPX en un servidor desnudo, primero debe obtener un servidor bare metal con los recursos del sistema adecuados de un proveedor en la nube. En ese servidor, cualquiera de los hipervisores admitidos como Linux KVM, VMware ESX, Citrix Hypervisor o Microsoft Hyper-V debe estar instalado y configurado antes de implementar la instancia de ADC VPX.

Para obtener más información sobre la lista de diferentes hipervisores y funciones compatibles con una instancia Citrix ADC VPX, consulte Matriz de soporte y directrices de uso.

Para obtener más información sobre la instalación de instancias de Citrix ADC VPX en diferentes hipervisores, consulte la documentación correspondiente.

- **Citrix Hypervisor:** consulte Instalación de una instancia Citrix ADC VPX en Citrix Hypervisor.
- **VMware ESX:** consulte Instalación de una instancia de Citrix ADC VPX en VMware ESX.
- **Microsoft Hyper-V:** consulte Instalación de una instancia Citrix ADC VPX en el servidor Microsoft Hyper-V.
- **Plataforma KVM Linux:** consulte Instalación de una instancia Citrix ADC VPX en la plataforma Linux-KVM.

Instalar una instancia de Citrix ADC VPX en Citrix Hypervisor

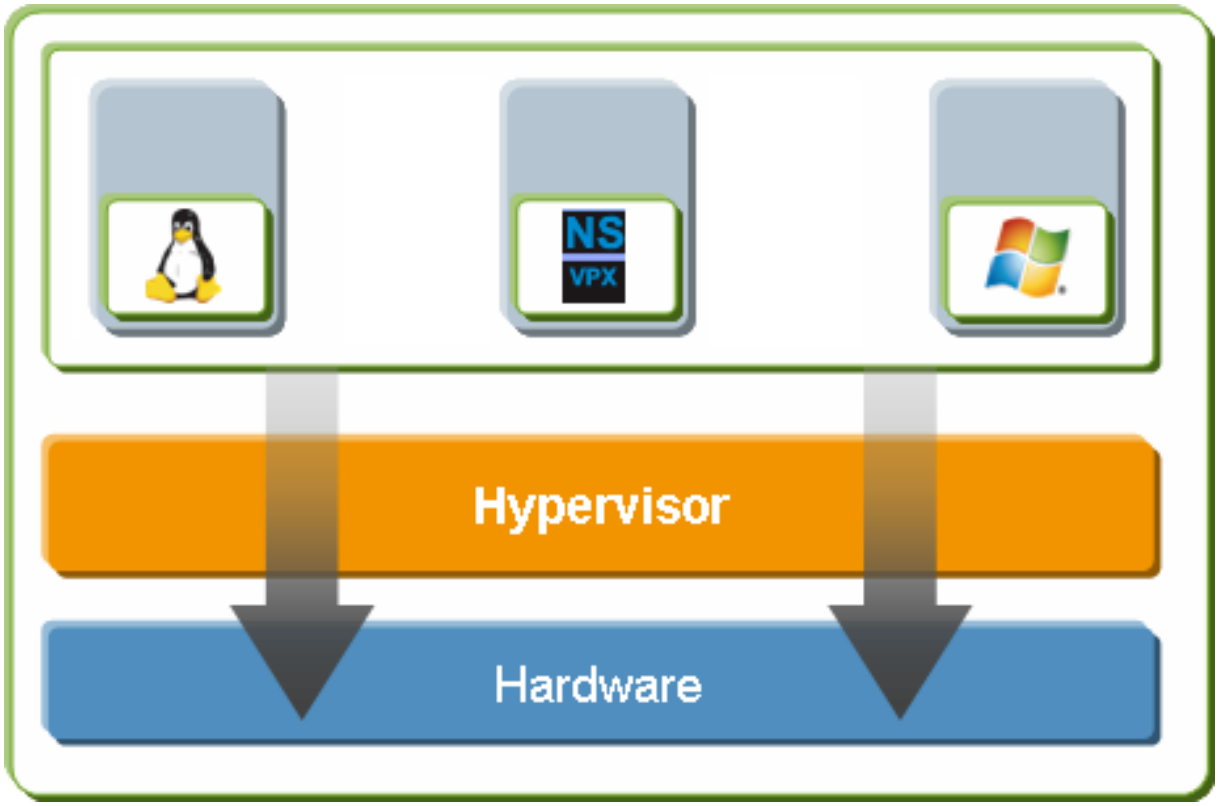
December 2, 2021

Para instalar instancias VPX en Citrix Hypervisor, primero debe instalar el Hypervisor en un equipo con los recursos del sistema adecuados. Para realizar la instalación de la instancia de Citrix ADC VPX, utilice Citrix XenCenter, que debe instalarse en un equipo remoto que pueda conectarse al host del hipervisor a través de la red.

Para obtener más información sobre Hypervisor, consulte la documentación de Citrix Hypervisor.

En la siguiente ilustración se muestra la arquitectura de soluciones sin usar de la instancia de Citrix ADC VPX en Hypervisor.

Ilustración. Una instancia de Citrix ADC VPX en Citrix Hypervisor



Requisitos previos para instalar una instancia de Citrix ADC VPX en Hypervisor

Antes de comenzar a instalar un dispositivo virtual, haga lo siguiente:

- Instale Hypervisor versión 6.0 o posterior en hardware que cumpla los requisitos mínimos.
- Instale XenCenter en una estación de trabajo de administración que cumpla los requisitos mínimos del sistema.
- Obtenga archivos de licencia de dispositivo virtual. Para obtener más información sobre las licencias de dispositivos virtuales, consulte la *Guía de licencias de Citrix ADC VPX* en http://support.citrix.com/article/ctx122426.

Requisitos de hardware de hiper

En la tabla siguiente se describen los requisitos mínimos de hardware para una plataforma Hypervisor que ejecuta una instancia Citrix ADC VPX.

Tabla 1. Requisitos mínimos del sistema para el hipervisor que ejecuta una instancia de nCore VPX

Componente	Requisito
CPU	2 o más CPU x86 de 64 bits con asistencia de virtualización (Intel-VT) habilitada. Para ejecutar la instancia Citrix ADC VPX, la compatibilidad de hardware para la virtualización debe estar habilitada en el host del hipervisor. Asegúrese de que la opción del BIOS para la compatibilidad con la virtualización no esté inhabilitada. Para obtener más información, consulte la documentación del BIOS.
RAM	3 GB
Espacio en disco	Almacenamiento conectado localmente (PATA, SATA, SCSI) con 40 GB de espacio en disco. Nota: La instalación del hipervisor crea una partición de 4 GB para el dominio de control de host del hipervisor. El espacio restante está disponible para la instancia Citrix ADC VPX y otras máquinas virtuales.
NIC	Una NIC de 1 Gbps; recomendada: dos NIC de 1 Gbps

Para obtener información sobre la instalación de Hypervisor, consulte la documentación del hipervisor en http://support.citrix.com/product/xens/.

En la tabla siguiente se enumeran los recursos informáticos virtuales que debe proporcionar Hypervisor para cada dispositivo virtual nCore VPX.

Tabla 2. Recursos informáticos virtuales mínimos necesarios para ejecutar una instancia de nCore VPX

Componente	Requisito
Memoria	2 GB
CPU virtual (vCPU)	2
Interfaces de red virtual	2

> Nota: Para el uso de producción de la instancia de
> Citrix ADC VPX, Citrix recomienda que la prioridad de la CPU (en las propiedades de la máquina virtual) se establezca al nivel más alto para mejorar el comportamiento de programación y la latencia de la red.

requisitos del sistema de XenCenter

XenCenter es una aplicación cliente de Windows. No se puede ejecutar en el mismo equipo que el host del hipervisor. Para obtener más información sobre los requisitos mínimos del sistema y la instalación de XenCenter, consulte los siguientes documentos del hipervisor:

- Requisitos del sistema
- Instalación

Instalar instancias Citrix ADC VPX en Hypervisor mediante XenCenter

Después de instalar y configurar Hypervisor y XenCenter, puede usar XenCenter para instalar dispositivos virtuales en Hypervisor. El número de dispositivos virtuales que puede instalar depende de la cantidad de memoria disponible en el hardware que ejecuta Hypervisor.

Después de utilizar XenCenter para instalar la instancia inicial de Citrix ADC VPX (imagen.xva) en el hipervisor, puede usar el Command Center para aprovisionar la instancia de Citrix ADC VPX. Para obtener más información, consulte la documentación del Centro de comandos.

Para instalar instancias de Citrix ADC VPX en Hypervisor mediante XenCenter, siga estos pasos:

1. Inicie XenCenter en su estación de trabajo.
2. En el menú Servidor, haga clic en Agregar.
3. En el cuadro de diálogo Agregar nuevo servidor, en el cuadro de texto nombre de host, escriba la dirección IP o el nombre DNS del hipervisor al que quiere conectarse.
4. En los cuadros de texto Nombre de usuario y Contraseña, escriba las credenciales de administrador y, a continuación, haga clic en Conectar. El nombre del hipervisor aparece en el panel de navegación con un círculo verde, lo que indica que el hipervisor está conectado.
5. En el panel de navegación, haga clic en el nombre del hipervisor en el que quiere instalar la instancia Citrix ADC VPX.
6. En el menú VM, haga clic en Importar.
7. En el cuadro de diálogo Importar, en el nombre del archivo Importar, vaya a la ubicación en la que guardó el archivo de imagen .xva de instancia VPX de Citrix ADC VPX. Asegúrese de que la opción VM exportada está seleccionada y, a continuación, haga clic en Siguiente.

8. Seleccione el hipervisor en el que quiere instalar el dispositivo virtual y, a continuación, haga clic en Siguiente.
9. Seleccione el repositorio de almacenamiento local en el que quiere almacenar el dispositivo virtual y, a continuación, haga clic en Importar para iniciar el proceso de importación.
10. Puede agregar, modificar o eliminar las interfaces de red virtual según sea necesario. Cuando haya terminado, haga clic en Siguiente.
11. Haga clic en Finish para completar el proceso de importación.

    Nota: Para ver el estado del proceso de importación, haga clic en la ficha **Registro**.
12. Si quiere instalar otro dispositivo virtual, repita los pasos 5 a 11.

> **Nota**
>
> Tras la configuración inicial de la instancia VPX, si quiere actualizar el dispositivo a la última versión de software, consulte Actualización o degradación del software del sistema.

Configurar instancias VPX para que usen interfaces de red de virtualización de E/S de raíz única (SR-IOV)

January 21, 2022

Después de instalar y configurar una instancia de Citrix ADC VPX en XenServer, puede configurar el dispositivo virtual para que use interfaces de red SR-IOV.

Se admiten las siguientes NIC:

- Intel 82599 10G
- Intel X710 10G
- Intel XL710 40G

Limitaciones

XenServer no admite algunas funciones en las interfaces SR-IOV. Las limitaciones de las NIC Intel 82599, Intel X710 e Intel XL710 se enumeran en las siguientes secciones.

Limitaciones de la NIC Intel 82599

La NIC Intel 82599 no admite las siguientes funciones:

- Conmutación del modo L2
- Agrupar en clústeres

- Particionado de administrador [modo VLAN compartida]
- Alta disponibilidad [Activo - modo activo]
- Marcos Jumbo
- Protocolo IPv6 en el entorno de clúster

Limitaciones de las NIC Intel X710 10G e Intel XL710 40G

Las NIC Intel X710 10G e Intel XL710 40G tienen las siguientes limitaciones:

- No se admite la conmutación de modo L2.
- No se admite la partición de administrador (modo VLAN compartida).
- En un clúster, las tramas gigantes no se admiten cuando la NIC XL710 se utiliza como interfaz de datos.
- La lista de interfaces se reordena cuando las interfaces se desconectan y vuelven a conectar
- No se admiten configuraciones de parámetros de interfaz como velocidad, dúplex y negociaciones automáticas.
- Para las NIC Intel X710 10G e Intel XL710 40G, la interfaz aparece como una interfaz 40/x.
- Solo se admiten hasta 16 interfaces SR-IOV Intel X710/XL710 en una instancia VPX.

> Nota:
> Para que las NIC Intel X710 10G e Intel XL710 40G admitan IPv6, habilite el modo de confianza en las funciones virtuales (VF) escribiendo el siguiente comando en el host de XenServer:
>
> ```
> ## ip link set <PNIC> <VF> trust on
> ```
>
> Ejemplo:
>
> ```
> ## ip link set ens785f1 vf 0 trust on
> ```

Requisitos previos para la NIC Intel 82599

En el host de XenServer, asegúrese de que:

- Agregue la NIC (NIC) Intel 82599 al host.
- Bloquear la lista del controlador `ixgbevf` agregando la siguiente entrada al archivo **/etc/modprobe.d/blacklist.conf**:

  lista de prohibidos ixgbevf
- Habilite las funciones virtuales (VF) de SR-IOV agregando la siguiente entrada al archivo **/etc/modprobe.d/ixgbe**:

  opciones ixgbe max_vfs=* <number_of_VFs>*

  donde <*number_VFs*> es el número de VF SR-IOV que quiere crear.
- Compruebe que SR-IOV esté habilitado en el BIOS.

> Nota:
>
> Se recomienda el controlador IXGBE versión 3.22.3.

Asignar VF Intel 82599 SR-IOV a la instancia de Citrix ADC VPX mediante el host XenServer

Para asignar una VF Intel 82599 SR-IOV a una instancia de Citrix ADC VPX, siga estos pasos:

1. En el host de XenServer, utilice el siguiente comando para asignar las VF SR-IOV a la instancia de Citrix ADC VPX:

   xe host-call-plugin plugin=iovirt host-uuid=<*Xen host UUID*> **fn=assign_free_vf args:uuid**=<*NetScaler VM UUID*> **args:ethdev**=<*interface name*> **args:mac=***<Mac addr>*

   Donde:

   - <*Xen host UUID*> es el UUID del host XenServer.
   - <*NetScaler VM UUID*> es el UUID de la instancia Citrix ADC VPX.
   - <*interface name*> es la interfaz para las VF de SR-IOV.
   - <*MAC address*> es la dirección MAC del SR-IOV VF.

   > **Nota**
   >
   > Especifique la dirección MAC que quiere utilizar en el parámetro args:Mac=; si no se especifica, el script `iovirt` genera aleatoriamente y asigna una dirección MAC. Además, si quiere utilizar los VF SR-IOV en modo de agregación de enlaces, asegúrese de especificar la dirección MAC como 00:00:00:00:00:00.

2. Inicie la instancia de Citrix ADC VPX.

Anular la asignación de VF Intel 82599 SR-IOV a la instancia ADC VPX mediante el host XenServer

Si ha asignado un VF SR-IOV incorrecto o si quiere modificar un VF SR-IOV asignado, debe anular la asignación y reasignar los VF SR-IOV a la instancia Citrix ADC VPX.

Para anular la asignación de la interfaz de red SR-IOV asignada a una instancia de Citrix ADC VPX, siga estos pasos:

1. En el host de XenServer, use el siguiente comando para asignar las VF de SR-IOV a la instancia de Citrix ADC VPX y reiniciar la instancia de Citrix ADC VPX:

   xe host-call-plugin plugin=iovirt **host-uuid**=<*Xen_host_UUID*> **fn**=unassign_all **args:uuid**=<*Netscaler_VM_U*

   Donde:

- *<Xen_host_UUID>*: El UUID del host de XenServer.
- *<Netscaler_VM_UUID>*: El UUID de la instancia de Citrix ADC VPX

2. Inicie la instancia de Citrix ADC VPX.

Asignar VF Intel X710/XL710 SR-IOV a la instancia de Citrix ADC VPX mediante el host XenServer

Para asignar una VF Intel X710/XL710 SR-IOV a la instancia de Citrix ADC VPX, siga estos pasos:

1. Ejecute el siguiente comando en el host de XenServer para crear una red.

```
xe network-create name-label=<network-name>
<!--NeedCopy-->
```

Ejemplo:

```
xe network-create name-label=SR-IOV-NIC-18 8ee59b73-7319-6998-cd69
   -b9fa3e8d7503
<!--NeedCopy-->
```

2. Determine el identificador único universal (UUID) de PIF de la NIC en la que se va a configurar la red SR-IOV.

```
xe pif-list

            uuid ( RO)  : e2874343-f1de-1fa7-8fef-98547c348783
            device ( RO): eth18
currently-attached ( RO): true
              VLAN ( RO): -1
      network-uuid ( RO): f865bd85-44dd-b865-ab65-dcd6ae28c16e
<!--NeedCopy-->
```

3. Configure la red como una red SR-IOV. El siguiente comando también devuelve el UUID de la red SR-IOV recién creada:

```
xe network-sriov-create network-uuid=<network-uuid> pif-uuid=<
   physical-pif-uuid>
<!--NeedCopy-->
```


Ejemplo:

```
xe network-sriov-create network-uuid=8ee59b73-7319-6998-cd69-
   b9fa3e8d7503 pif-uuid=e2874343-f1de-1fa7-8fef-98547
   c3487831629b44f-832a-084e-d67d-5d6d314d5e0f
<!--NeedCopy-->
```

Para obtener más información sobre los parámetros de red SR-IOV, ejecute el siguiente comando:

```
[root@citrix-XS82-TOPO ~]# xe network-sriov-param-list uuid=1629
   b44f-832a-084e-d67d-5d6d314d5e0f

               uuid ( RO): 1629b44f-832a-084e-d67d-5d6d314d5e0f
      physical-PIF ( RO): e2874343-f1de-1fa7-8fef-98547c348783
       logical-PIF ( RO): 85d52771-5814-c62d-45fa-f37b536144ff
   requires-reboot ( RO): false
remaining-capacity ( RO): 32
<!--NeedCopy-->
```

4. Cree una interfaz virtual (VIF) y conéctela a la máquina virtual de destino.

```
xe vif-create device=0 mac=b2:61:fc:ae:00:1d network-uuid=8ee59b73
   -7319-6998-cd69-b9fa3e8d7503 vm-uuid=b507e8a6-f5ca-18eb-561d
   -308218a9dd68
3e1e2e58-b2ad-6dc0-61d4-1d149c9c6466
<!--NeedCopy-->
```

> NOTA: El número de índice de NIC de la VM debe comenzar por 0.

Use el siguiente comando para encontrar el UUID de VM:

```
[root@citrix-XS82-TOPO ~]# xe vm-list
uuid ( RO): b507e8a6-f5ca-18eb-561d-308218a9dd68
 name-label ( RW): sai-vpx-1
power-state ( RO): halted
<!--NeedCopy-->
```


Elimine las VF Intel X710/XL710 SR-IOV de la instancia de Citrix ADC mediante el host XenServer

Para quitar una VF Intel X710/XL710 SR-IOV de una instancia de Citrix ADC VPX, siga estos pasos:

1. Copie el UUID del VIF que quiere destruir.
2. Ejecute el siguiente comando en el host de XenServer para destruir el VIF.

```
xe vif-destroy uuid=<vif-uuid>
<!--NeedCopy-->
```

Ejemplo:

```
[root@citrix-XS82-TOPO ~]# xe vif-destroy uuid=3e1e2e58-b2ad-6dc0
   -61d4-1d149c9c6466
<!--NeedCopy-->
```

Configuración de VLAN en la interfaz SR-IOV

> **Importante**
>
> Mientras asigna las VF de SR-IOV a la instancia de Citrix ADC VPX, asegúrese de especificar la dirección MAC 00:00:00:00:00:00 para las VF.

Para utilizar las funciones virtuales de SR-IOV en el modo de agregación de enlaces, debe inhabilitar la comprobación de suplantación de funciones virtuales que haya creado. En el host de XenServer, use el siguiente comando para inhabilitar la comprobación de suplantación:

ip link set <*interface_name*> **vf** <*VF_id*> **spoofchk** off

Donde:

- <interface_name> es el nombre de la interfaz.
- <VF_id> es el identificador de función virtual.

Después de inhabilitar la comprobación de suplantación de todas las funciones virtuales que ha creado, reinicie la instancia de Citrix ADC VPX y configure la agregación de vínculos. Para obtener instrucciones, consulte Configurar la agregación de enlaces.

Configurar VLAN en la interfaz SR-IOV

Puede configurar VLAN en las funciones virtuales SR-IOV, para obtener instrucciones, consulte Configuración de una VLAN.

> **Importante**
>
> Asegúrese de que el host XenServer no contenga la configuración de VLAN para la interfaz de VF.

Instalar una instancia de Citrix ADC VPX en VMware ESX

April 5, 2022

Antes de instalar instancias de Citrix ADC VPX en VMware ESX, asegúrese de que VMware ESX Server esté instalado en una máquina con los recursos del sistema adecuados. Para instalar una instancia de Citrix ADC VPX en VMware ESXi, utilice el cliente VMware vSphere. El cliente o la herramienta deben estar instalados en un equipo remoto que pueda conectarse a VMware ESX a través de la red.

En esta sección se incluyen los temas siguientes:

- Requisitos previos
- Instalación de una instancia de Citrix ADC VPX en VMware ESX

> **Importante**
>
> No puede instalar VMware Tools estándar ni actualizar la versión de VMware Tools disponible en una instancia de Citrix ADC VPX. VMware Tools para una instancia de Citrix ADC VPX se suministra como parte de la versión del software Citrix ADC.

Requisitos previos

Antes de comenzar a instalar un dispositivo virtual, haga lo siguiente:

- Instale VMware ESX en un hardware que cumpla los requisitos mínimos.
- Instale VMware Client en una estación de trabajo de administración que cumpla los requisitos mínimos del sistema.
- Descargue los archivos de configuración del dispositivo Citrix ADC VPX.
- Etiquete los puertos de red físicos de VMware ESX.
- Obtenga archivos de licencias VPX. Para obtener más información sobre las licencias de instancia de Citrix ADC VPX, consulte Descripción general de las licencias.

Requisitos de hardware de VMware ESX

En la tabla siguiente se describen los requisitos mínimos del sistema para los servidores VMware ESX que ejecutan el dispositivo virtual Citrix ADC VPX nCore.

Tabla 1. Requisitos mínimos del sistema para un servidor VMware ESX que ejecuta una instancia Citrix ADC VPX

Componente	Requisito
CPU	2 o más CPU x86 de 64 bits con asistencia de virtualización (Intel-VT) habilitada. Para ejecutar una instancia de Citrix ADC VPX, la compatibilidad de hardware para la virtualización debe estar habilitada en el host VMware ESX. Asegúrese de que la opción BIOS para la función de virtualización no esté inhabilitada. Para obtener más información, consulte la documentación del BIOS. A partir de la versión 13.1 de Citrix ADC, la instancia de Citrix ADC VPX en el hipervisor VMware ESXi admite procesadores AMD.
RAM	3 GB
Espacio en disco	40 GB de espacio en disco disponible
Red	Una NIC (NIC) de 1 Gbps; se recomiendan dos NIC de 1 Gbps

Para obtener información acerca de la instalación de VMware ESX, consulte http://www.vmware.com/.

En la tabla siguiente se enumeran los recursos informáticos virtuales que el servidor VMware ESX debe proporcionar para cada dispositivo virtual VPX nCore.

Tabla 2. Recursos informáticos virtuales mínimos necesarios para ejecutar una instancia de Citrix ADC VPX

Componente	Requisito
Memoria	4 GB
CPU virtual (vCPU)	2
Interfaces de red virtual	En ESX, puede instalar un máximo de 10 interfaces de red virtuales si el hardware VPX se actualiza a la versión 7 o superior.
Espacio en disco	20 GB

> Nota
>
> Esto se suma a cualquier requisito de disco para el Hypervisor.

Para el uso de producción del dispositivo virtual VPX, se debe reservar la asignación de memoria completa. Los ciclos de CPU (en MHz) iguales al menos a la velocidad de un núcleo de CPU del ESX deben reservarse.

Requisitos del sistema cliente de VMware vSphere

VMware vSphere es una aplicación cliente que se puede ejecutar en sistemas operativos Windows y Linux. No se puede ejecutar en la misma máquina que el servidor VMware ESX. En la siguiente tabla se describen los requisitos mínimos del sistema.

Tabla 3. Requisitos mínimos del sistema para la instalación del cliente de VMware vSphere

Componente	Requisito
Sistema operativo	Para conocer los requisitos detallados de VMware, busque el archivo PDF “Tablas de compatibilidad de vSphere” en http://kb.vmware.com/.
CPU	750 MHz; se recomienda 1 gigahercio (GHz) o más rápido
RAM	1 GB. Se recomiendan 2 GB
NIC (NIC)	NIC de 100 Mbps o más rápido

Requisitos del sistema OVF Tool 1.0

OVF Tool es una aplicación cliente que puede ejecutarse en sistemas Windows y Linux. No se puede ejecutar en la misma máquina que el servidor VMware ESX. En la siguiente tabla se describen los requisitos mínimos del sistema.

Tabla 4. Requisitos mínimos del sistema para la instalación de herramientas OVF

Componente	Requisito
Sistema operativo	Para conocer los requisitos detallados de VMware, busque el archivo PDF “Guía del usuario de herramientas OVF” en http://kb.vmware.com/.

Componente	Requisito
CPU	750 MHz como mínimo, se recomienda 1 GHz o más rápido
RAM	1 GB mínimo, 2 GB recomendado
NIC (NIC)	NIC de 100 Mbps o más rápido

Para obtener información sobre la instalación de OVF, busque el archivo PDF “Guía del usuario de la herramienta OVF” en http://kb.vmware.com/.

Descarga de los archivos de configuración de Citrix ADC VPX

El paquete de configuración de instancias Citrix ADC VPX para VMware ESX sigue el estándar de formato Open Virtual Machine (OVF). Puede descargar los archivos desde el sitio web de Citrix. Necesita una cuenta de Citrix para iniciar sesión. Si no tiene una cuenta de Citrix, acceda a la página principal en http://www.citrix.com, haga clic en el **enlace Nuevos usuarios**y siga las instrucciones para crear una cuenta de Citrix.

Una vez iniciada la sesión, navegue por la siguiente ruta desde la página principal de Citrix:

Citrix.com > **Descargas > Citrix ADC > Dispositivos virtuales**.

Copie los siguientes archivos en una estación de trabajo de la misma red que el servidor ESX. Copie los tres archivos en la misma carpeta.

- NSVPX-ESX-<release number>-<build number>-disk1.vmdk (por ejemplo, NSVPX-ESX-13.0-71.44_nc_64-disk1.vmdk)
- NSVPX-ESX-<release number>-<build number>.ovf (por ejemplo, NSVPX-ESX-13.0-71.44_nc_64.ovf)
- NSVPX-ESX-<release number>-<build number>.mf (por ejemplo, NSVPX-ESX-13.0-71.44_nc_64.mf)

Etiquetar los puertos de red físicos de VMware ESX

Antes de instalar un dispositivo virtual VPX, etiqueta todas las interfaces que va a asignar a los dispositivos virtuales, en un formato único, por ejemplo, NS_NIC_1_1, NS_NIC_1_2, etc. En implementaciones grandes, el etiquetado en un formato único ayuda a identificar rápidamente las interfaces asignadas al dispositivo virtual VPX, entre otras interfaces utilizadas por otras máquinas virtuales, como Windows y Linux. Este etiquetado es especialmente importante cuando distintos tipos de máquinas virtuales comparten interfaces.

Para etiquetar los puertos de red físicos del servidor VMware ESX, siga estos pasos:

1. Inicie sesión en el servidor VMware ESX mediante el cliente de vSphere.

2. En el cliente de vSphere, seleccione la ficha Configuración y, a continuación, haga clic en Redes.
3. En la esquina superior derecha, haga clic en Agregar red.
4. En el Asistente para agregar red, en **Tipo de conexión**, seleccione **Máquina virtual** y, a continuación, haga clic en Siguiente.
5. Desplácese por la lista de adaptadores físicos de vSwitch y elija el puerto físico que se asigna a la interfaz 1/1 de los dispositivos virtuales.
6. Introduzca la etiqueta de la interfaz, por ejemplo, **NS_NIC_1_1** como nombre del conmutador virtual asociado a la interfaz 1/1 de los dispositivos virtuales.
7. Haga clic en Siguiente para finalizar la creación de vSwitch. Repita el procedimiento, empezando por el paso 2, para agregar cualquier interfaz adicional que utilizarán los dispositivos virtuales. Etiquete las interfaces secuencialmente en el formato correcto (por ejemplo, NS_NIC_1_2).

Instalar una instancia de Citrix ADC VPX en VMware ESX

Una vez instalado y configurado VMware ESX, puede utilizar el cliente de VMware vSphere para instalar dispositivos virtuales en el servidor VMware ESX. El número de dispositivos virtuales que puede instalar depende de la cantidad de memoria disponible en el hardware que ejecuta VMware ESX.

Para instalar instancias Citrix ADC VPX en VMware ESX mediante VMware vSphere Client, siga estos pasos:

1. Inicie el cliente de VMware vSphere en su estación de trabajo.
2. En el cuadro de texto **Dirección IP/Nombre**, escriba la dirección IP del servidor VMware ESX al que quiere conectarse.
3. En los cuadros de texto **Nombre de usuario** y **Contraseña**, escriba las credenciales de administrador y, a continuación, haga clic en Iniciar sesión.
4. En el menú **Archivo**, haga clic en **Implementar plantilla OVF**.
5. En el cuadro de diálogo **Implementar plantilla de OVF**, en **Implementar desde archivo**, vaya a la ubicación en la que guardó los archivos de configuración de instancias de Citrix ADC VPX, seleccione el archivo .ovf y haga clic en **Siguiente**.
6. Asigne las redes que se muestran en la plantilla OVF del dispositivo virtual a las redes configuradas en el host ESX. Haga clic en **Siguiente** para comenzar a instalar un dispositivo virtual en VMware ESX. Una vez finalizada la instalación, una ventana emergente le informa de que la instalación se ha realizado correctamente.
7. Ya está listo para iniciar la instancia de Citrix ADC VPX. En el panel de navegación, seleccione la instancia de Citrix ADC VPX que ha instalado y, en el menú contextual, seleccione **Encendido**.
8. Después de arrancar la VM, desde la consola, configure las direcciones IP, máscara de red y puerta de enlace de Citrix ADC. Cuando complete la configuración, seleccione la opción **Guardar y salir** en la consola.
9. Si quiere instalar otro dispositivo virtual, repita desde el paso 6.

> **Nota**
>
> De forma predeterminada, la instancia de Citrix ADC VPX utiliza interfaces de red E1000.
>
> Después de la instalación, puede utilizar vSphere client o vSphere Web Client para administrar dispositivos virtuales en VMware ESX.
>
> Para que la función de etiquetado de VLAN funcione, en VMware ESX, establezca el identificador de VLAN del grupo de puertos en All (4095) en el vSwitch del servidor VMware ESX. Para obtener más información acerca de cómo configurar un ID de VLAN en el vSwitch del servidor VMware ESX, consulte http://www.vmware.com/pdf/esx3_vlan_wp.pdf.

Migrar una instancia de Citrix ADC VPX mediante VMware vMotion

Puede migrar una instancia de Citrix ADC VPX mediante VMware vSphere vMotion.

Siga estas pautas de uso:

- VMware no admite la función vMotion en máquinas virtuales configuradas con interfaces PCI Passthrough y SR-IOV.
- Las interfaces compatibles son E1000 y VMXNET3. Para utilizar vMotion en la instancia VPX, asegúrese de que la instancia esté configurada con una interfaz compatible.
- Para obtener más información sobre cómo migrar una instancia mediante VMware vMotion, consulte la documentación de VMware.

Configurar una instancia de Citrix ADC VPX para usar la interfaz de red VMXNET3

August 20, 2021

Después de instalar y configurar la instancia de Citrix ADC VPX en VMware ESX, puede usar el cliente web VMware vSphere para configurar el dispositivo virtual para que use interfaces de red VMXNET3.

Para configurar las instancias de Citrix ADC VPX para que utilicen interfaces de red VMXNET3 mediante VMware vSphere Web Client:

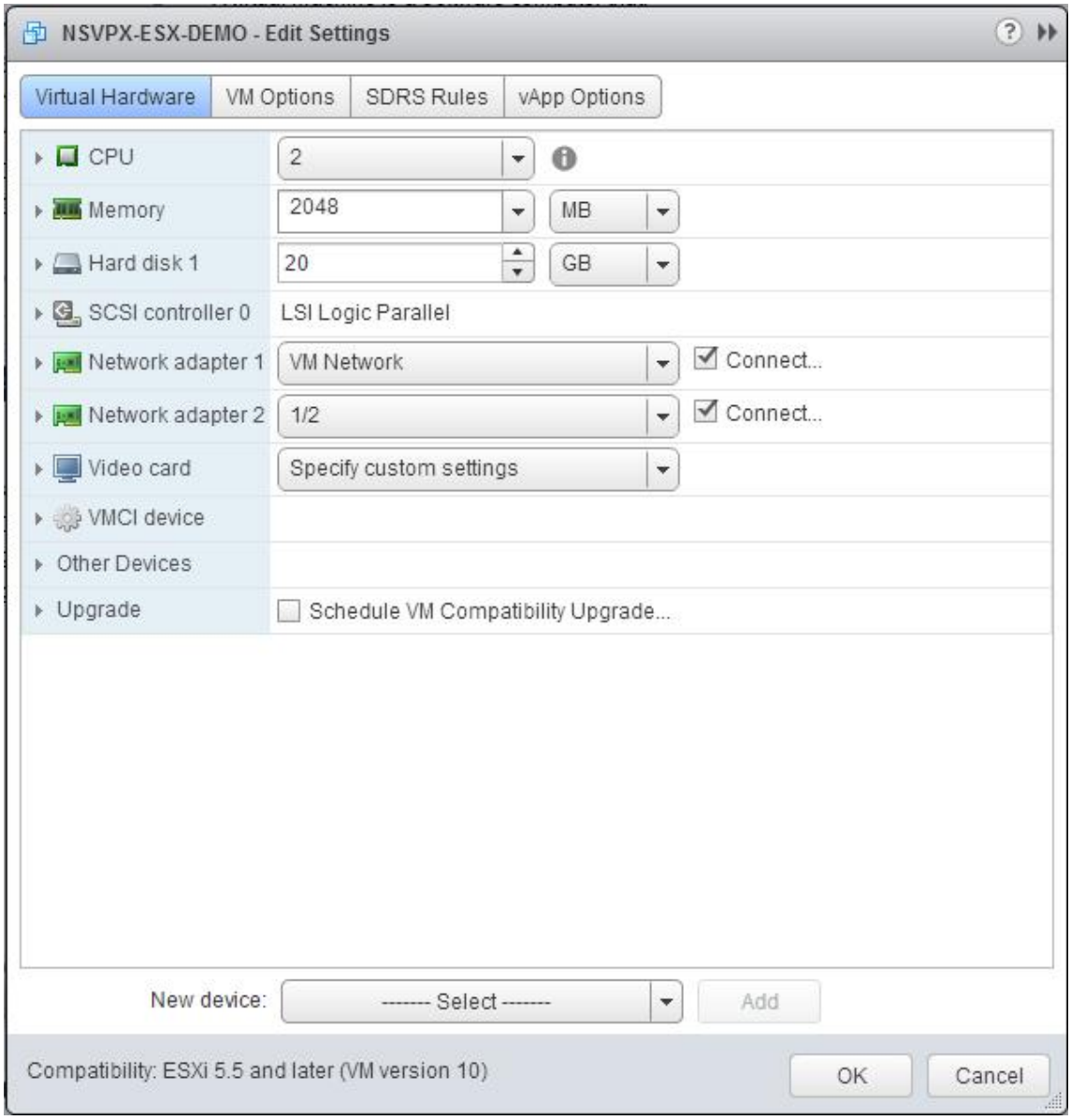
1. En vSphere Web Client, seleccione Hosts and Clusters.
2. Actualice la configuración de compatibilidad de la instancia de Citrix ADC VPX a ESX, de la siguiente manera:

   a. Apague la instancia de Citrix ADC VPX.

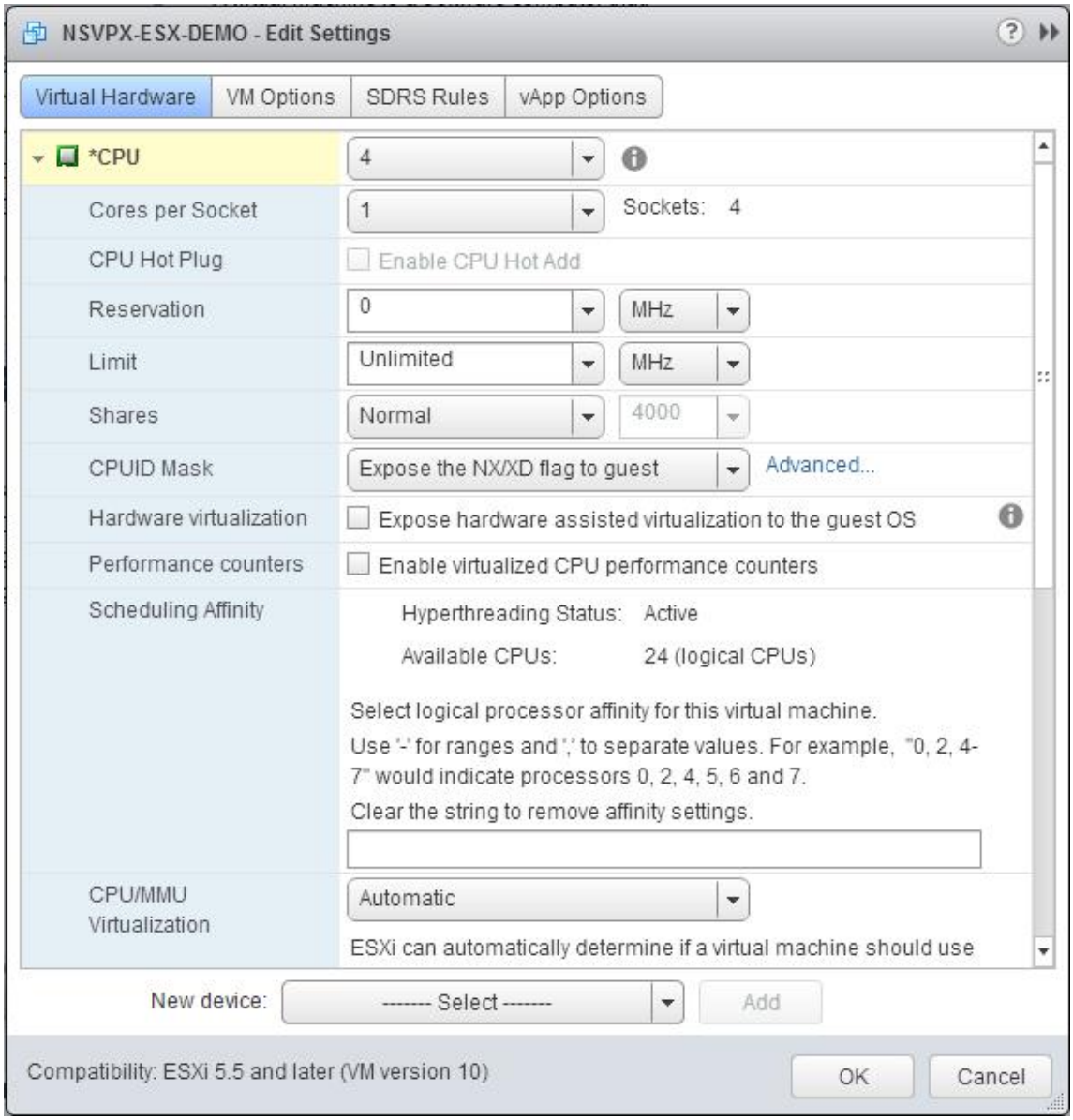
   b. Haga clic con el botón secundario en la instancia de Citrix ADC VPX y seleccione Compatibilidad > Actualizar compatibilidad de VM.

c. En el cuadro de diálogo Configurar compatibilidad de máquinas virtuales, seleccione ESXi 5.5 y versiones posteriores de la lista desplegable Compatible con y haga clic en Aceptar.

3. Haga clic con el botón derecho en la instancia de Citrix ADC VPX y haga clic en Modificar configuración.



4. En el cuadro de <virtual_appliance> diálogo: Modificar configuración, haga clic en la sección CPU.



5. En la sección CPU, actualice lo siguiente:

   - Número de CPU
   - Número de zócalos
   - Reservas
   - Límite
   - Acciones

   Establezca los valores de la siguiente manera:

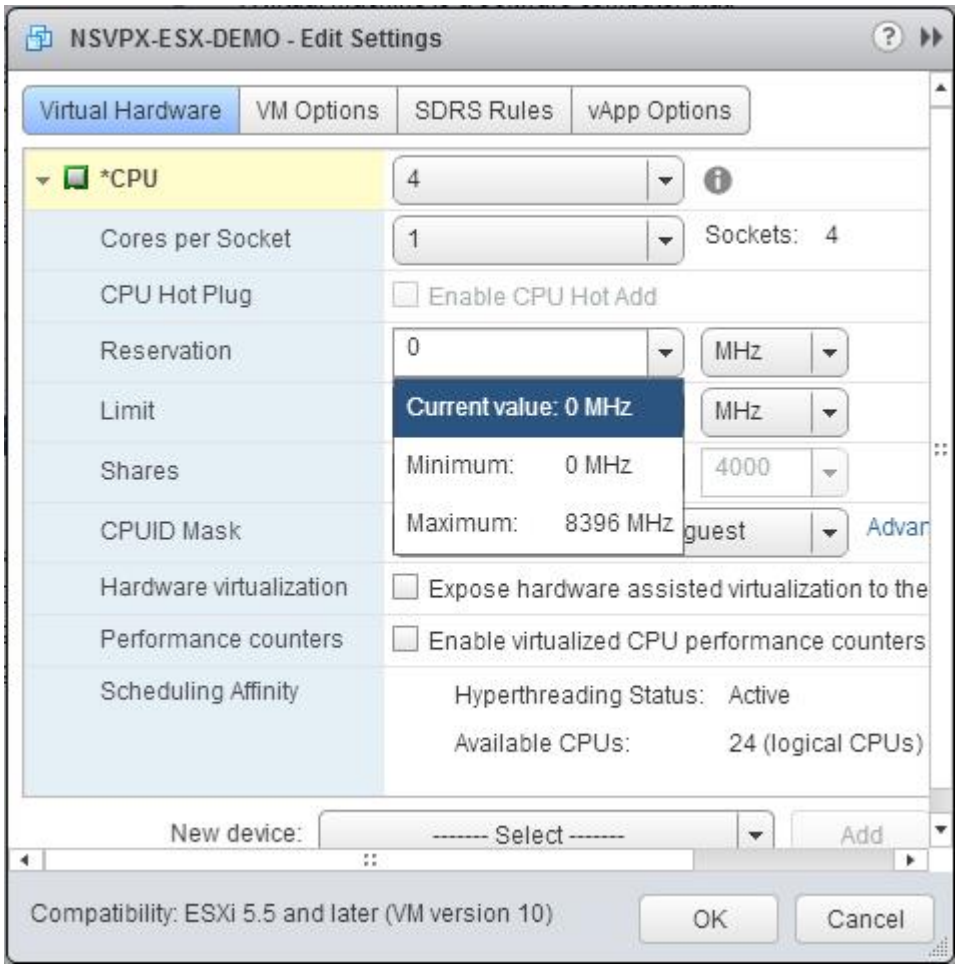
   a. En la lista desplegable CPU, seleccione el número de CPU que quiere asignar al dispositivo virtual.

   b. En la lista desplegable Núcleos por socket, seleccione el número de sockets.

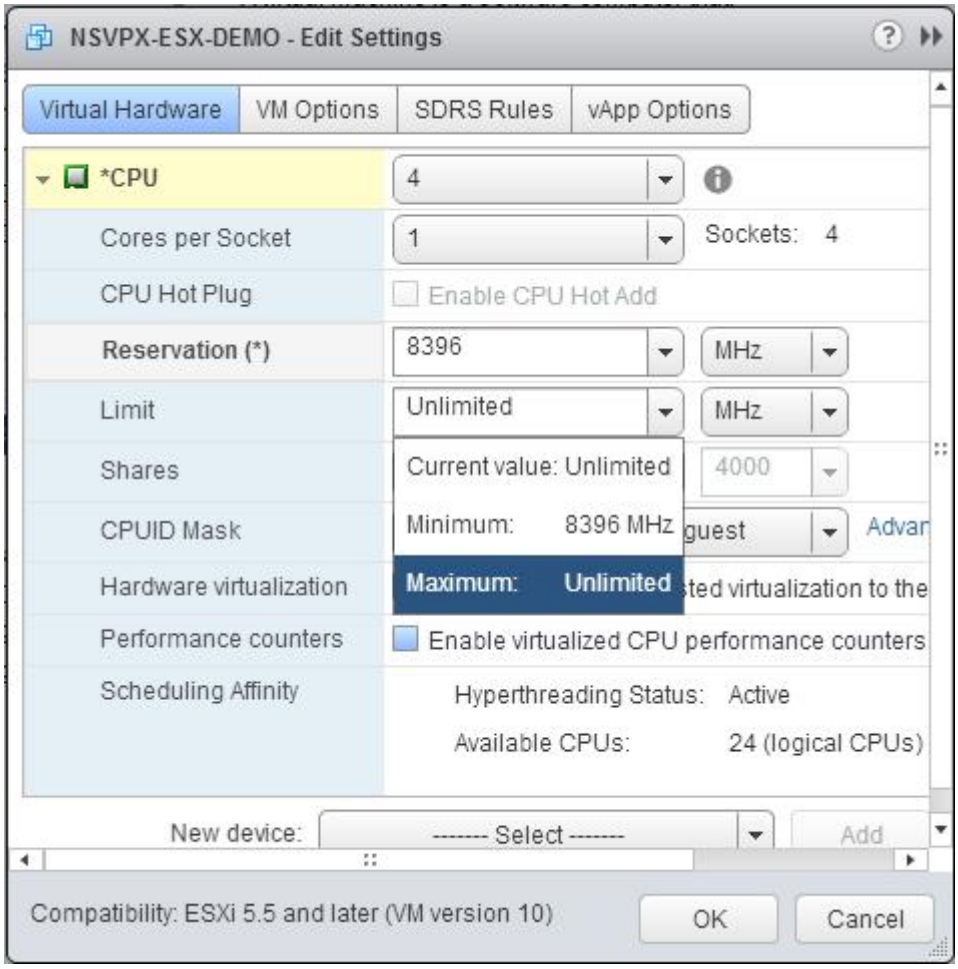
c. (Opcional) En el campo Hot Plug de CPU, active o anule la selección de la casilla Habilitar adición en caliente de CPU.

Nota: Citrix recomienda aceptar el valor predeterminado (inhabilitado).

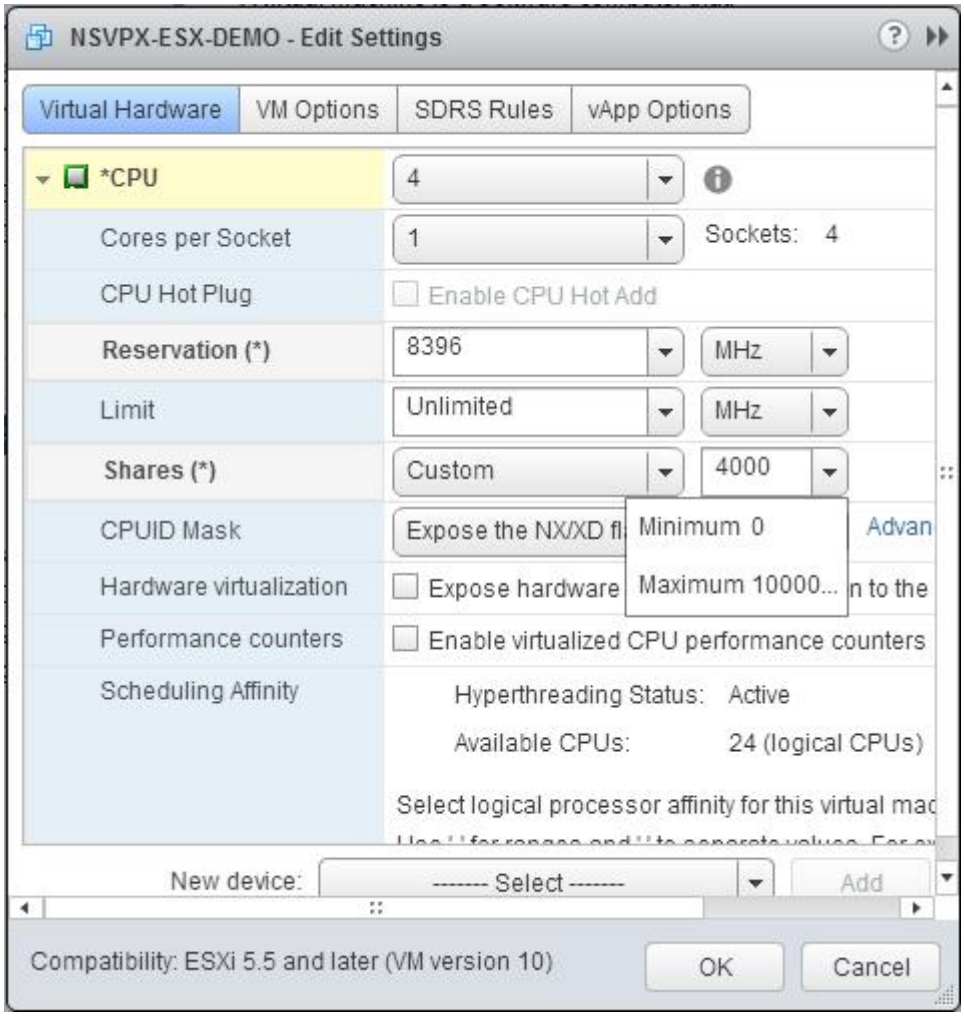
d. En la lista desplegable Reserva, seleccione el número que se muestra como valor máximo.



e. En la lista desplegable Límite, seleccione el número que se muestra como valor máximo.



f. En las listas desplegables Acciones, seleccione Personalizado y el número que se muestra como valor máximo.



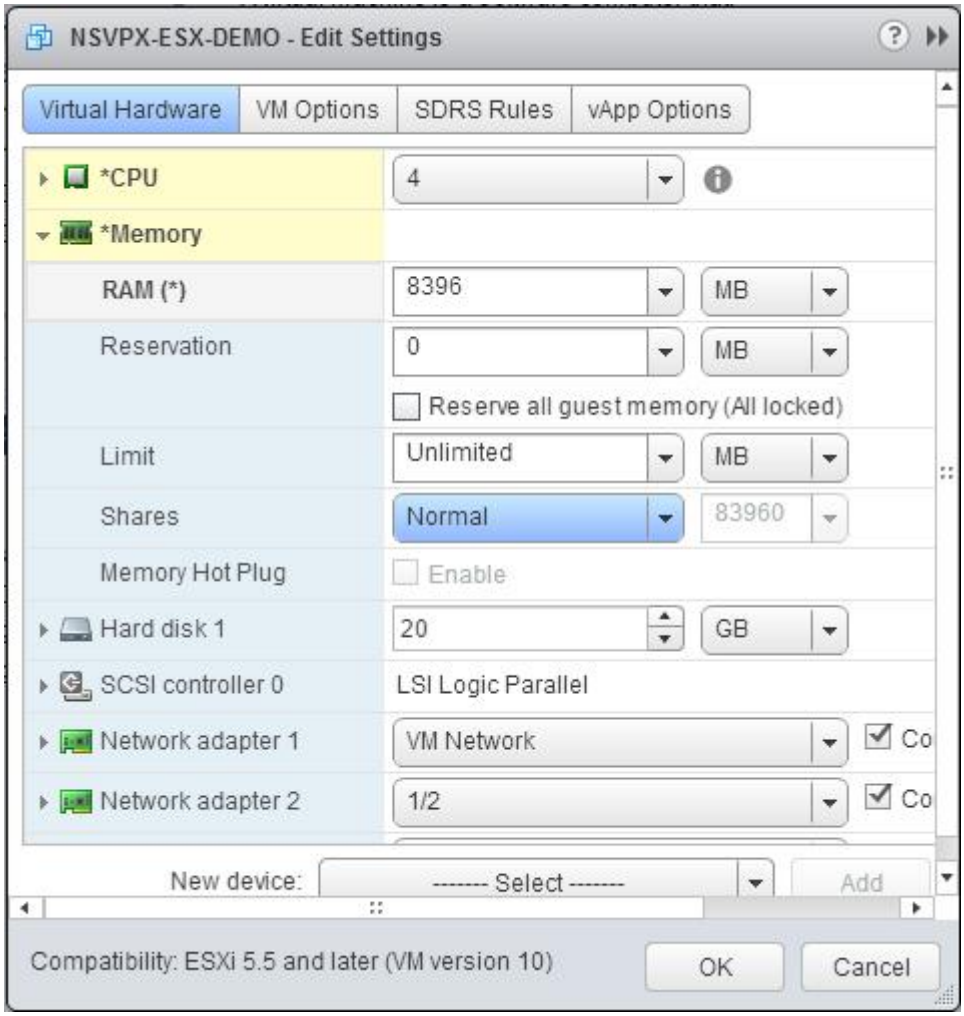
6. En la sección Memoria, actualice lo siguiente:

   - Tamaño de la RAM
   - Reservas
   - Límite
   - Acciones

   Establezca los valores de la siguiente manera:

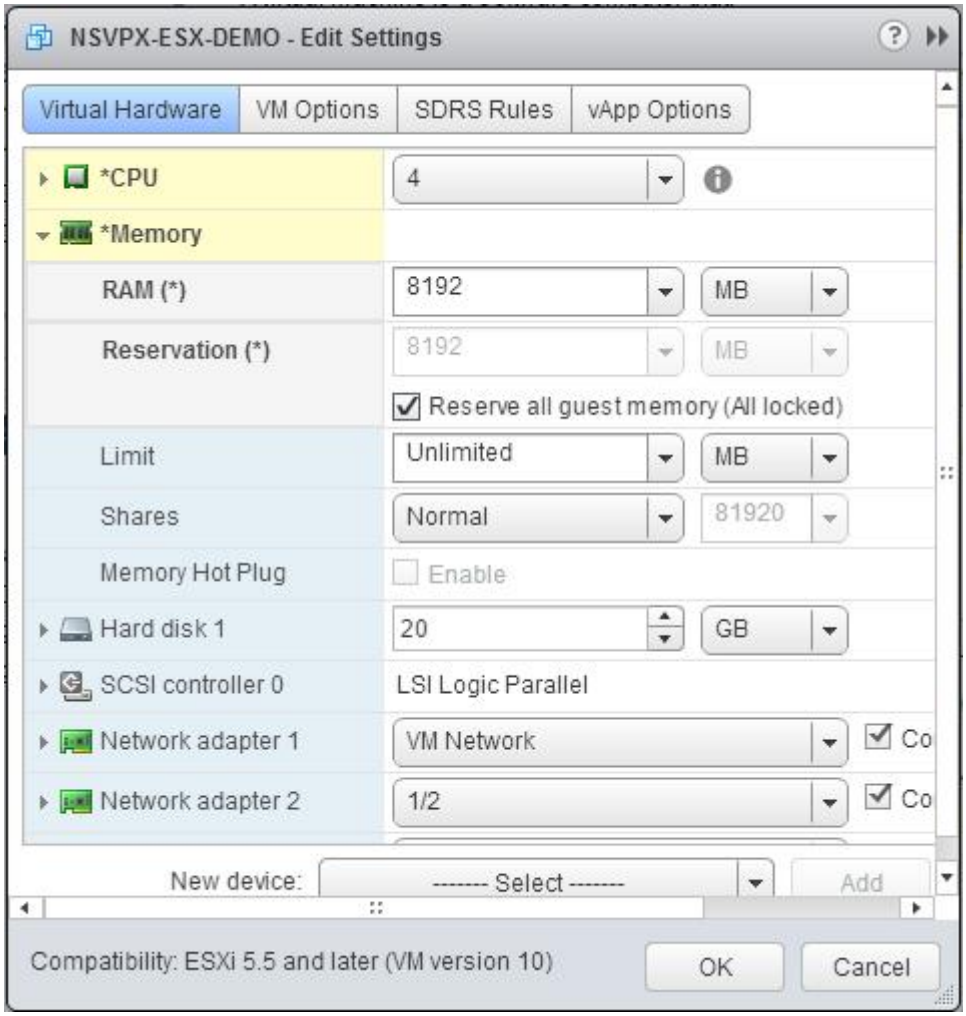
   a. En la lista desplegable RAM, seleccione el tamaño de la RAM. Debe ser el número de vCPU x 2 GB. Por ejemplo, si el número de vCPU es 4, la RAM debe ser de 4 x 2 GB = 8 GB.

   Nota: Para una edición avanzada o Premium del dispositivo Citrix ADC VPX, asegúrese de asignar 4 GB de RAM a cada vCPU. Por ejemplo, si el número de vCPU es 4, entonces RAM = 4 x 4 GB = 16 GB.

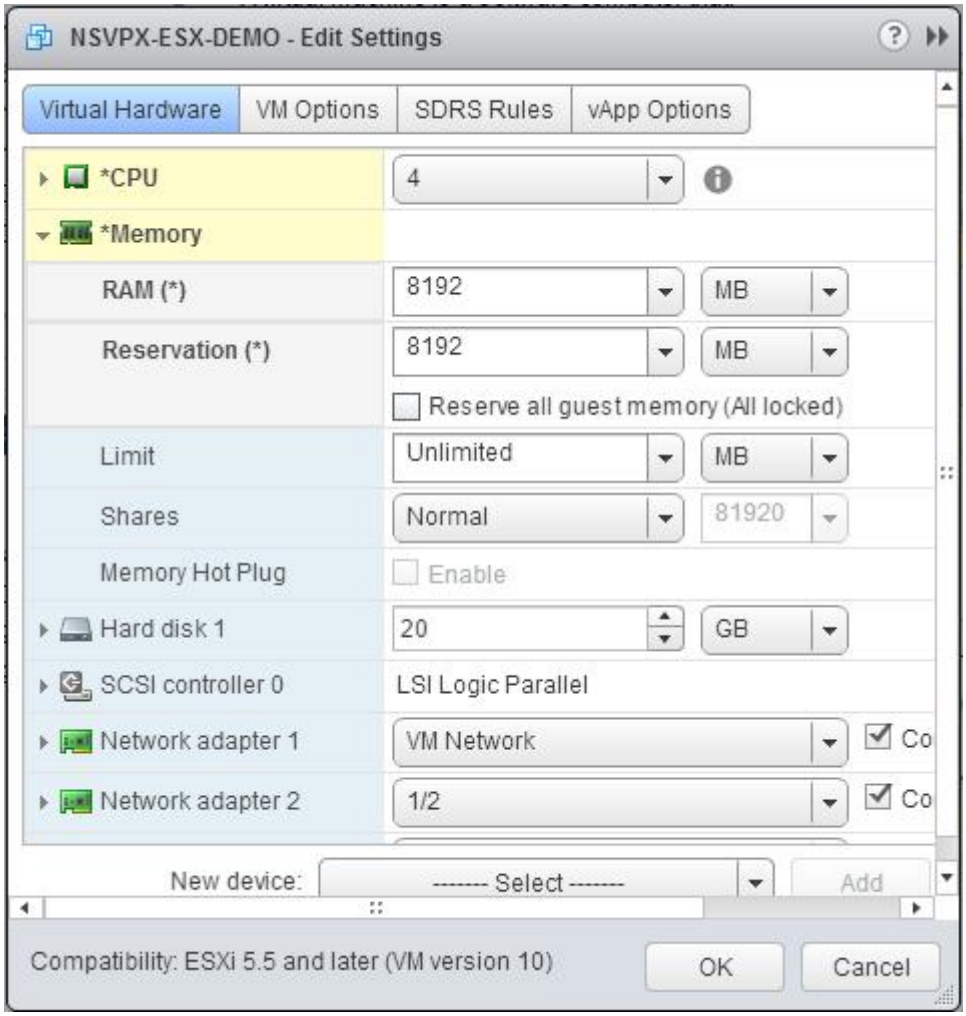


b. En la lista desplegable Reserva, introduzca el valor de la reserva de memoria y active la casilla de verificación Reservar toda la memoria de invitado (Todo bloqueado). La reserva de memoria debe ser el número de vCPU x 2 GB. Por ejemplo, si el número de vCPU es 4, la reserva de memoria debe ser de 4 x 2 GB = 8 GB.

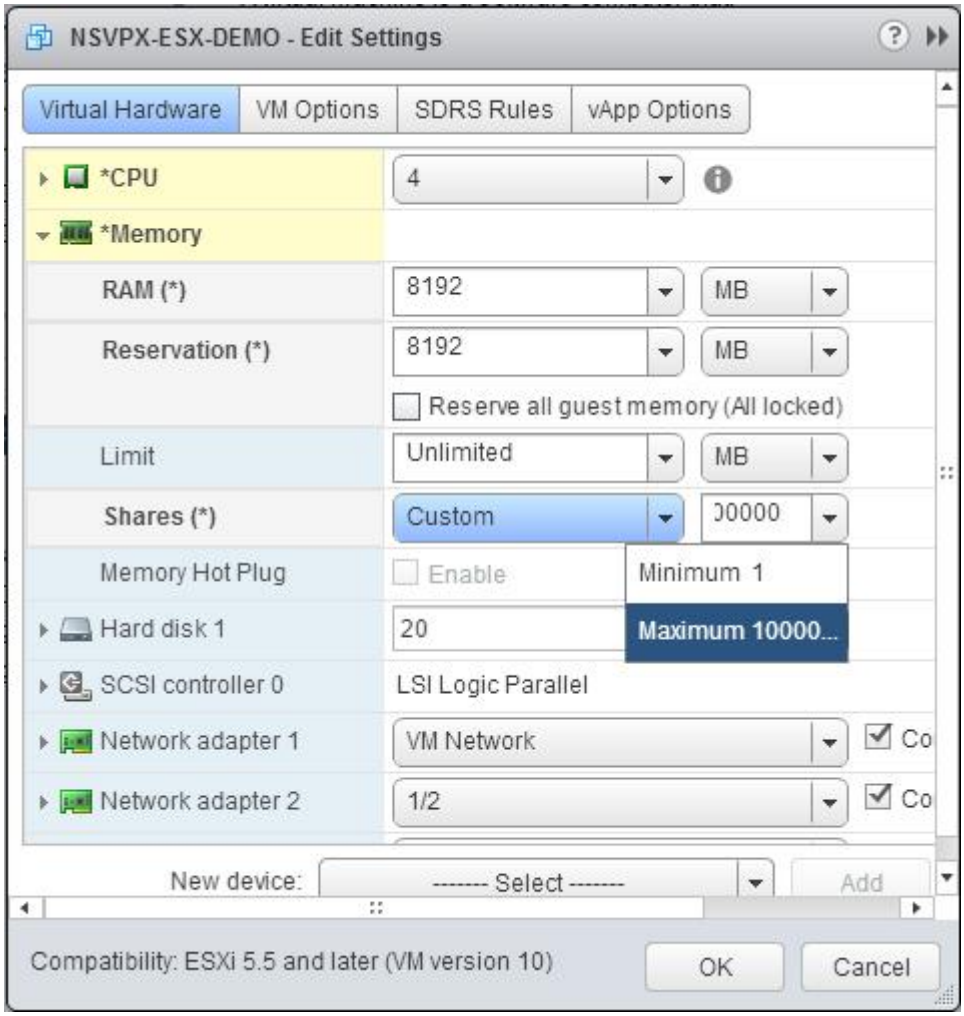
Nota: Para una edición avanzada o Premium del dispositivo Citrix ADC VPX, asegúrese de asignar 4 GB de RAM a cada vCPU. Por ejemplo, si el número de vCPU es 4, entonces RAM = 4 x 4 GB = 16 GB.



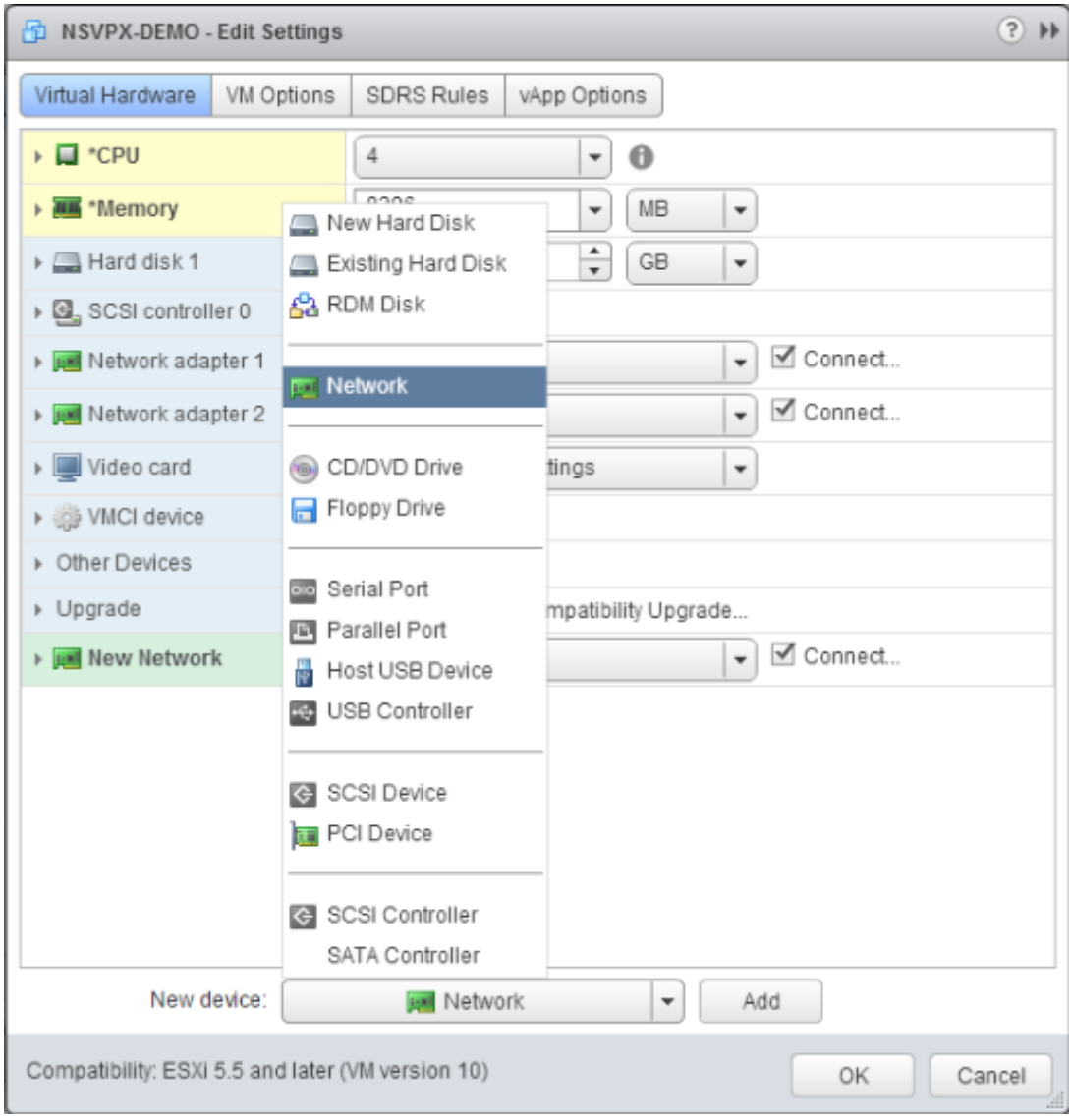
c. En la lista desplegable Límite, seleccione el número que se muestra como valor máximo.



d. En las listas desplegables de recursos compartidos, seleccione Personalizado y el número que se muestra como el valor máximo.



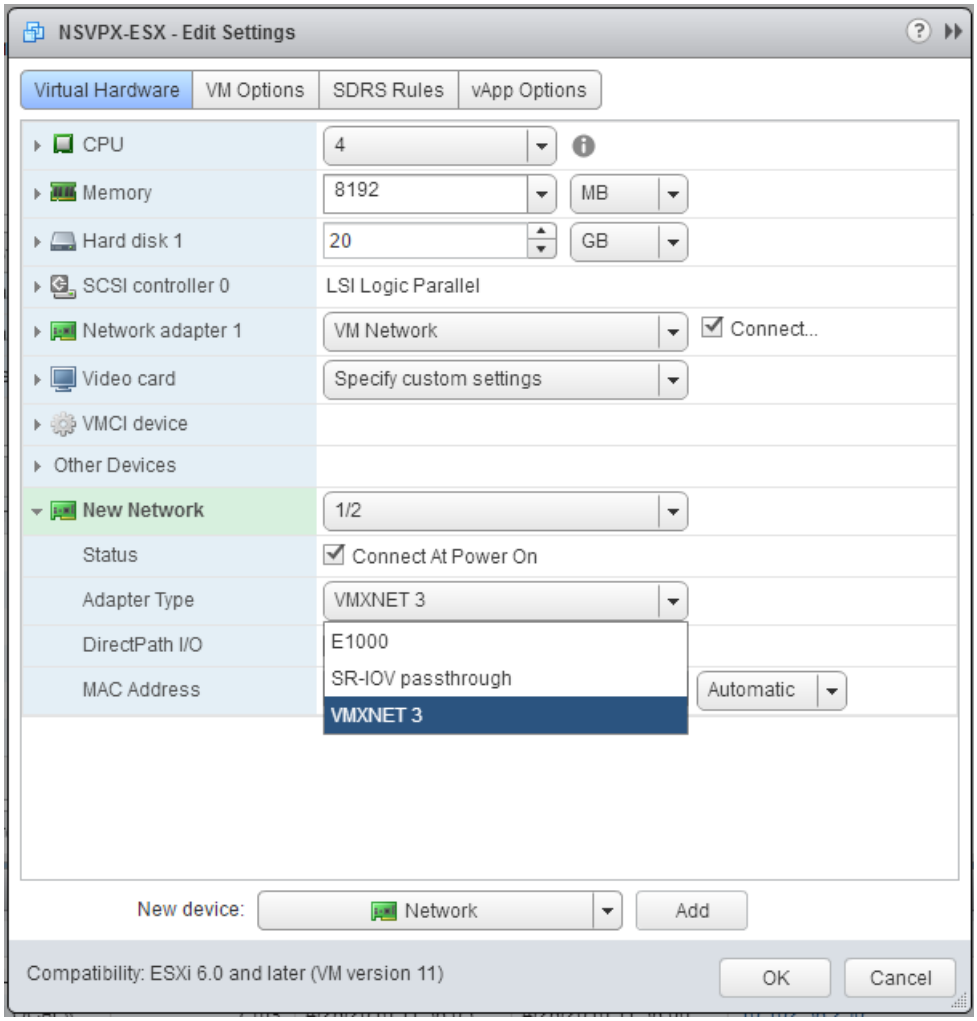
7. Agregue una interfaz de red VMXNET3. En la lista desplegable Nuevo dispositivo, seleccione Red y haga clic en Agregar.



8. En la sección Nueva red, en la lista desplegable, seleccione la interfaz de red y haga lo siguiente:

   a. En la lista desplegable Tipo de adaptador, seleccione VMXNET3.

> **Importante**
>
> La interfaz de red E1000 predeterminada y VMXNET3 no pueden coexistir, asegúrese de quitar la interfaz de red E1000 y utilizar VMXNET3 (0/1) como interfaz de administración.



9. Haga clic en Aceptar.
10. Encienda la instancia de Citrix ADC VPX.
11. Una vez que se enciende la instancia de Citrix ADC VPX, puede utilizar el siguiente comando para verificar la configuración:

    > mostrar resumen de interfaz

El resultado debe mostrar todas las interfaces que ha configurado:

```
> show interface summary
-------------------------------------------------------------------------

      Interface  MTU        MAC                Suffix
-------------------------------------------------------------------------
```



```
5 1     0/1         1500        00:0c:29:89:1d:0e    NetScaler Vir...rface,
      VMXNET3
6 2     1/1         9000        00:0c:29:89:1d:18    NetScaler Vir...rface,
      VMXNET3
7 3     1/2         9000        00:0c:29:89:1d:22    NetScaler Vir...rface,
      VMXNET3
8 4     LO/1        9000        00:0c:29:89:1d:0e    Netscaler Loopback
    interface
```

Nota

Después de agregar una interfaz VMXNET3 y reiniciar el dispositivo Citrix ADC VPX, el hipervisor VMware ESX podría cambiar el orden en que se presenta la NIC al dispositivo VPX. Por lo tanto, es posible que el adaptador de red 1 no permanezca siempre 0/1, lo que provoca la pérdida de conectividad de administración con el dispositivo VPX. Para evitar este problema, cambie la red virtual del adaptador de red en consecuencia.

Se trata de una limitación del hipervisor VMware ESX.

Configurar una instancia de Citrix ADC VPX para utilizar la interfaz de red SR-IOV

August 20, 2021

Después de instalar y configurar la instancia VPX de Citrix ADC en VMware ESX, puede utilizar el cliente web VMware vSphere para configurar el dispositivo virtual de modo que utilice interfaces de red de virtualización (SR-IOV) raíz única de E/S v virtualización (SR-IOV).

Limitaciones

Un Citrix ADC VPX configurado con una interfaz de red SR-IOV tiene las siguientes limitaciones:

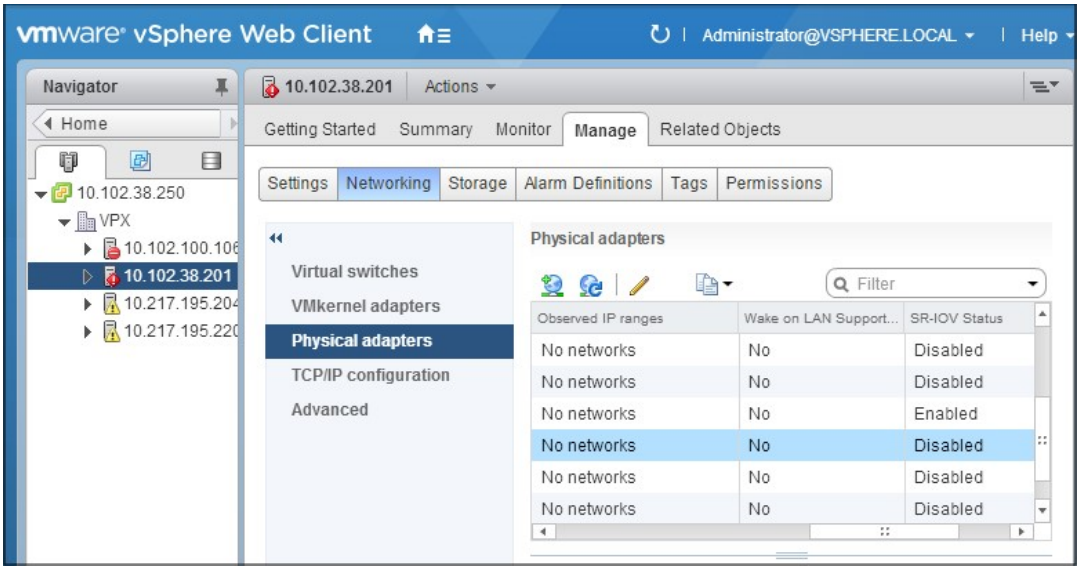
- Las siguientes funciones no se admiten en las interfaces SR-IOV que utilizan la NIC Intel 82599 10G en ESX VPX:
  - Conmutación del modo L2
  - Agregación de enlaces estáticos y LACP
  - Agrupar en clústeres
  - Partición de administrador [modo VLAN compartida]
  - Alta disponibilidad [Activo: Modo activo]
  - Marcos Jumbo
  - IPv6

- Las siguientes funciones no se admiten en la interfaz SR-IOV con una NIC Intel 82599 10G en KVM VPX:
  - Agregación de enlaces estáticos y LACP
  - Conmutación del modo L2
  - Agrupar en clústeres
  - Partición de administrador [modo VLAN compartida]
  - Alta disponibilidad [Activo: Modo activo]
  - Marcos Jumbo
  - IPv6
  - No se admite la configuración de VLAN en el hipervisor para la interfaz VF SR-IOV a través del `ip link` comando

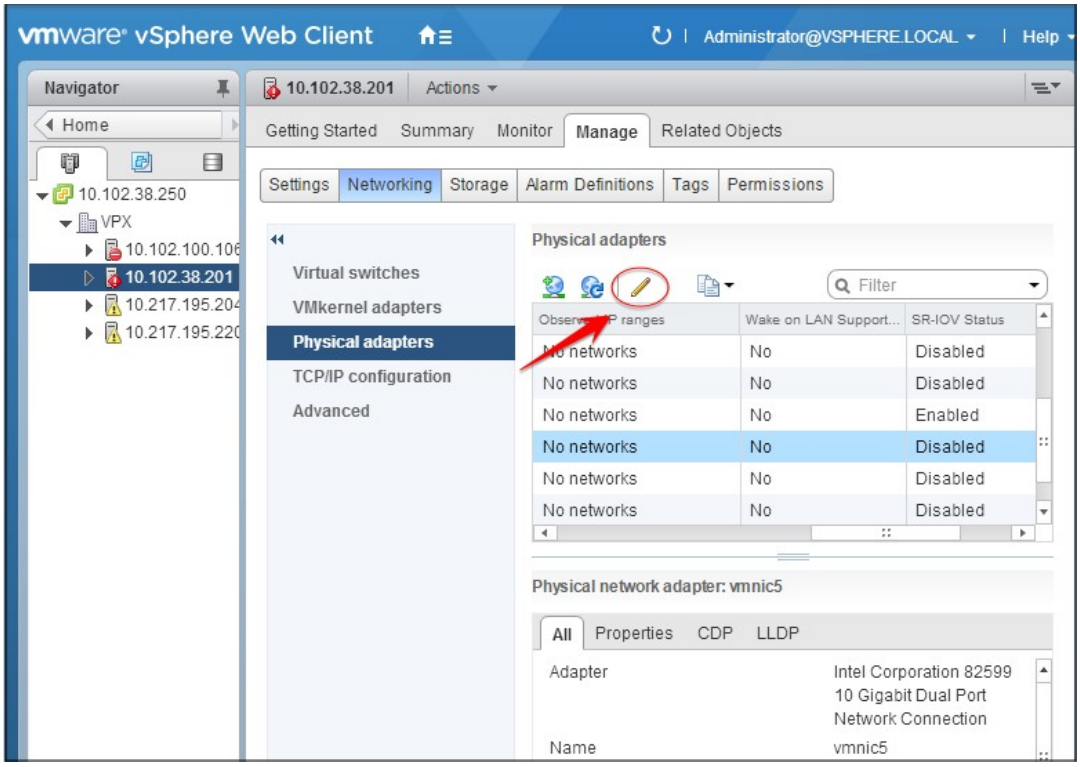
Requisito previo

Asegúrese de que:

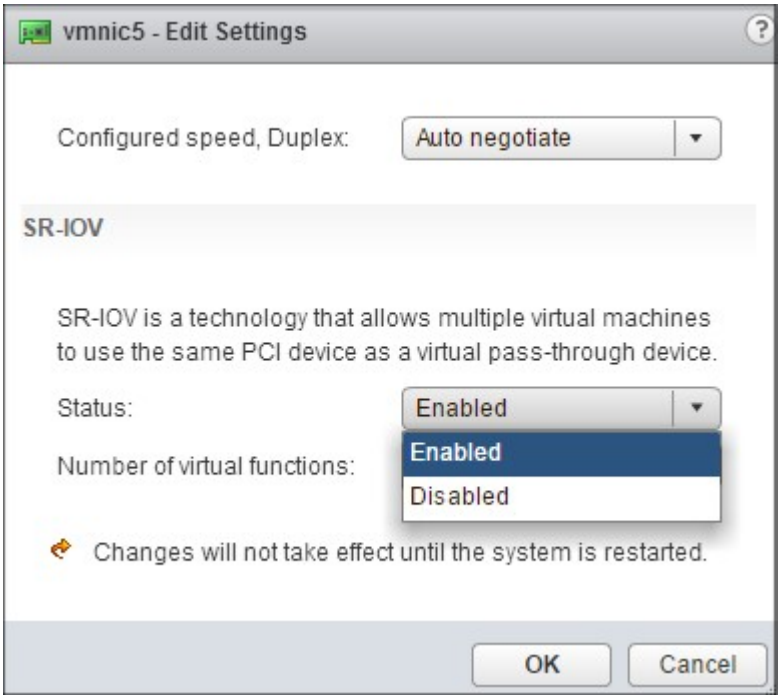
- Agregue la NIC (NIC) Intel 82599 al host ESX. Se recomienda el controlador IXGBE versión 3.7.13.7.14iov.
- Habilite SR-IOV en el adaptador físico del host, de la siguiente manera:
  1. En vSphere Web Client, desplácese hasta Host.
  2. En la ficha **Administrar > Redes**, seleccione **Adaptadores físicos**. El campo Estado SR-IOV muestra si un adaptador físico admite SR-IOV.



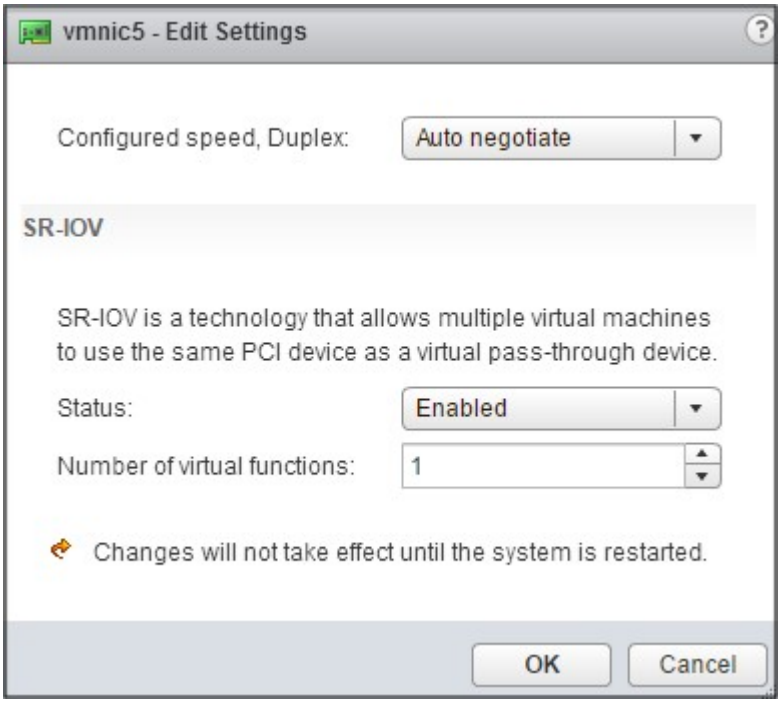
  3. Seleccione el adaptador físico y, a continuación, haga clic en el icono del lápiz para abrir el cuadro de diálogo **Modificar configuración**.



4. En SR-IOV, seleccione **Habilitado** en la lista desplegable **Estado**.



5. En el campo **Número de funciones virtuales**, escriba el número de funciones virtuales que quiere configurar para el adaptador.



6. Haga clic en **Aceptar**.
7. Reinicie el host.

- Cree un conmutador virtual distribuido (DVS) y `Portgroups`. Para obtener instrucciones, consulte la Documentación de VMware.

> **Nota**
>
> Citrix ha calificado la configuración SR-IOV en DVS y `Portgroups` solo.

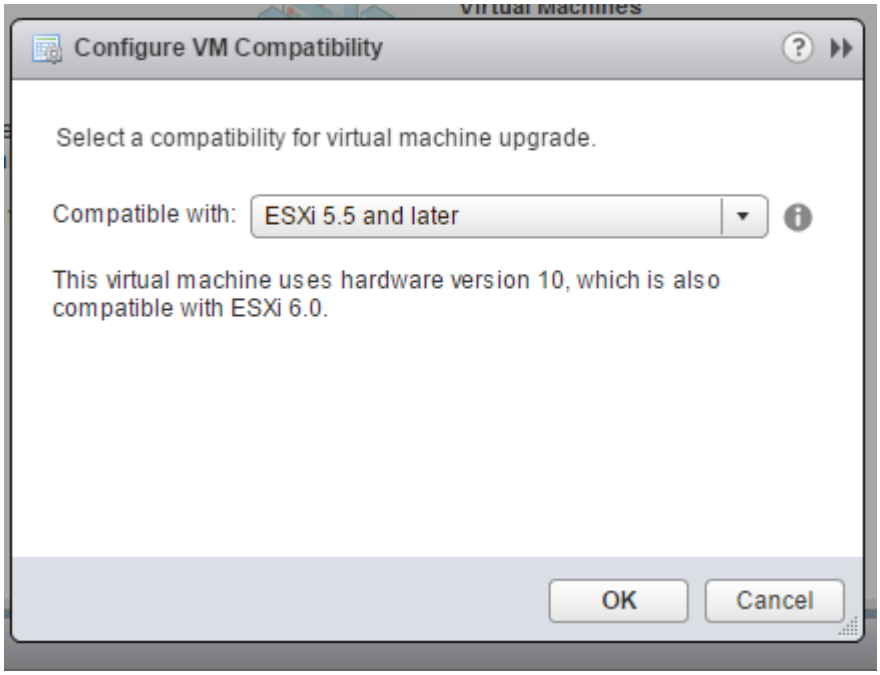
Para configurar instancias de Citrix ADC VPX para que utilicen la interfaz de red SR-IOV mediante VMware vSphere Web Client:

1. En vSphere Web Client, seleccione **Hosts and Clusters**.
2. Actualice la configuración de compatibilidad de la instancia de Citrix ADC VPX a ESX 5.5 o posterior, de la siguiente manera:

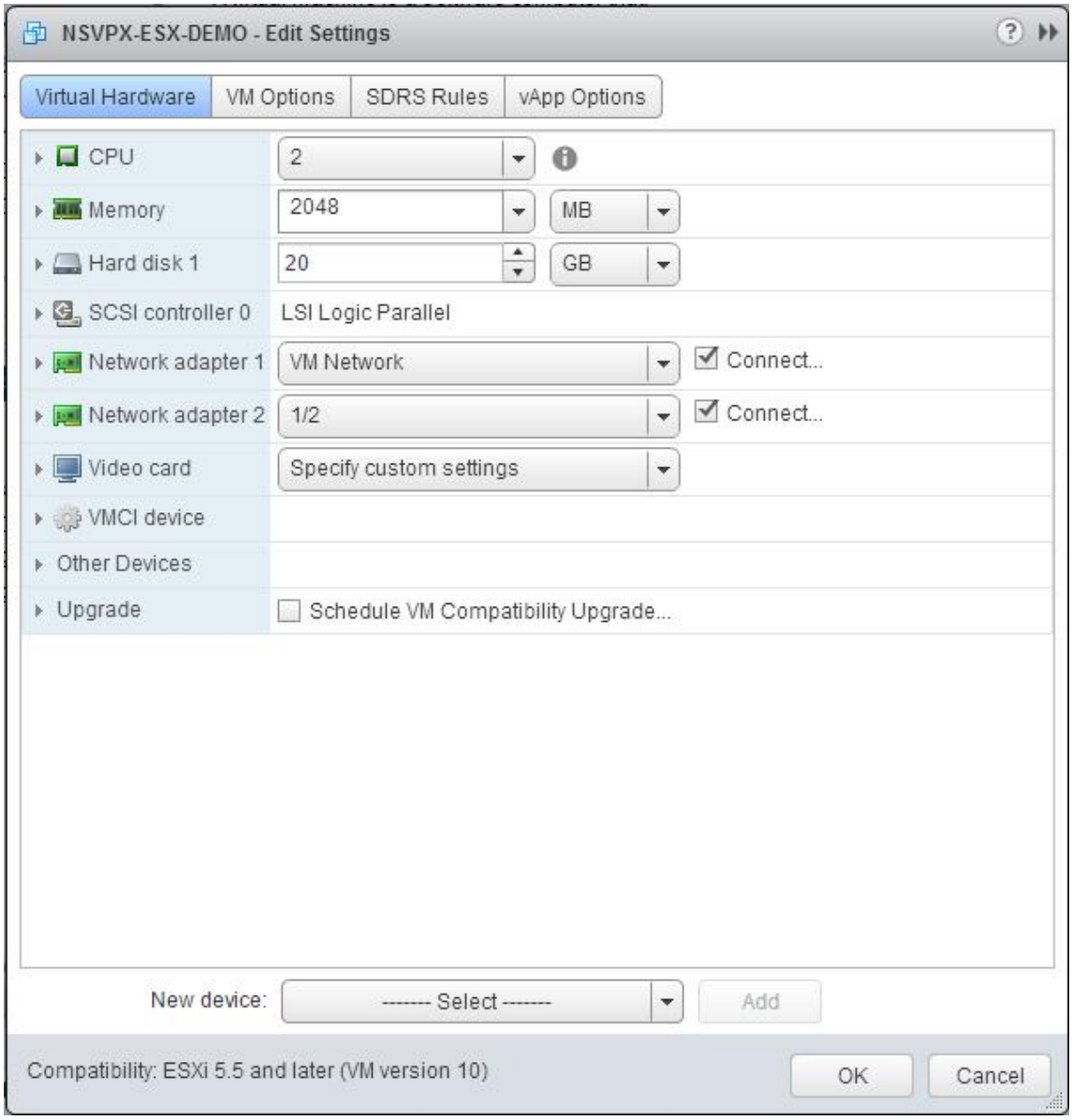
   a. Apague la instancia de Citrix ADC VPX.

   b. Haga clic con el botón secundario en la instancia de Citrix ADC VPX y seleccione **Compatibilidad > Actualizar compatibilidad de VM**.

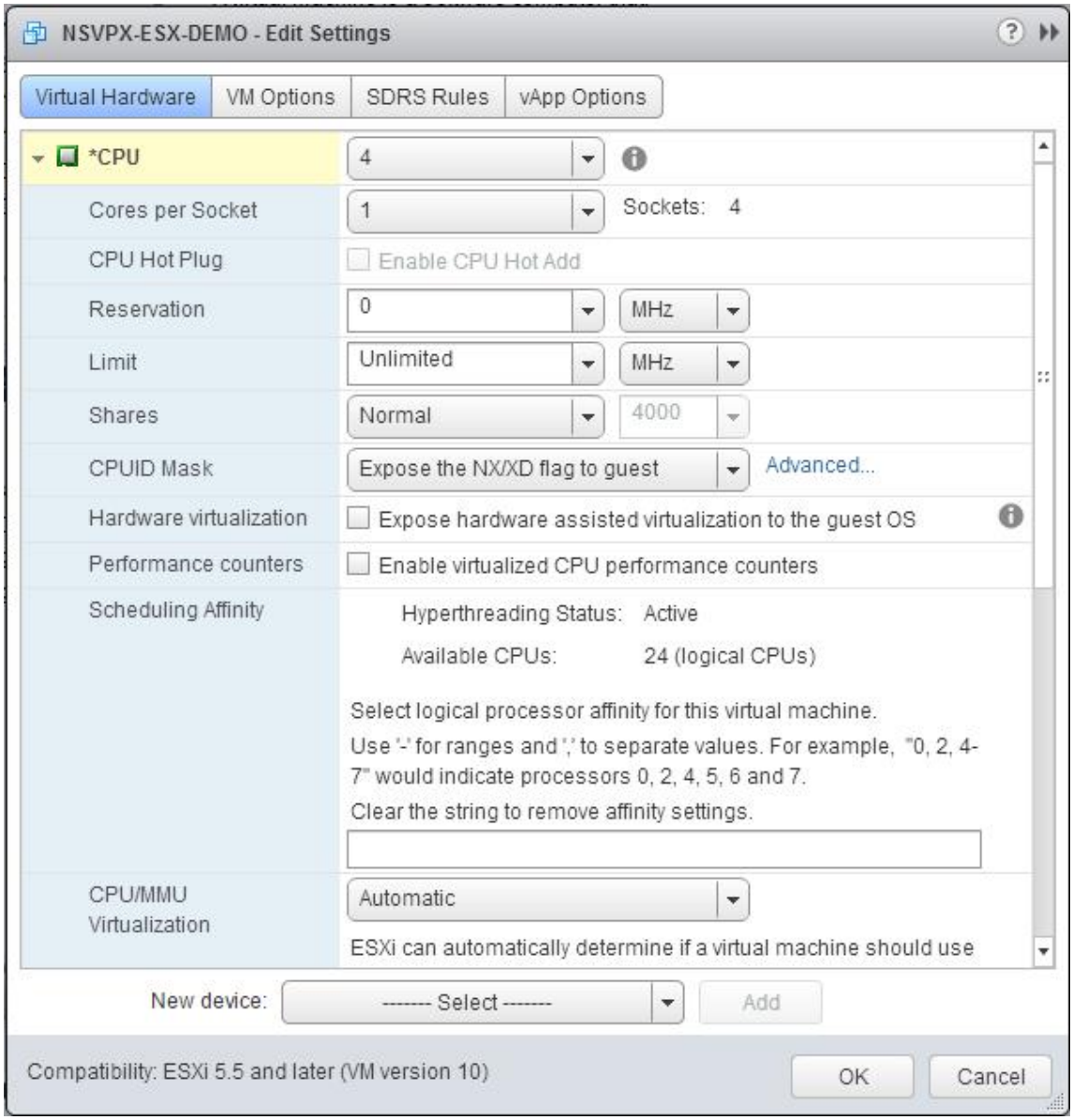
   c. En el cuadro de diálogo **Configurar compatibilidad de máquinas virtuales**, seleccione **ESXi 5.5 y versiones posteriores** de la lista desplegable **Compatible con** y haga clic en **Aceptar**.



3. Haga clic con el botón derecho en la instancia de Citrix ADC VPX y haga clic en **Modificar configuración**.



4. En el cuadro de **<virtual_appliance> diálogo: Modificar configuración, haga clic en la sección **CPU**.



5. En la sección **CPU**, actualice la siguiente configuración:

   - Número de CPU
   - Número de zócalos
   - Reservas
   - Límite
   - Acciones

   Establezca los valores de la siguiente manera:

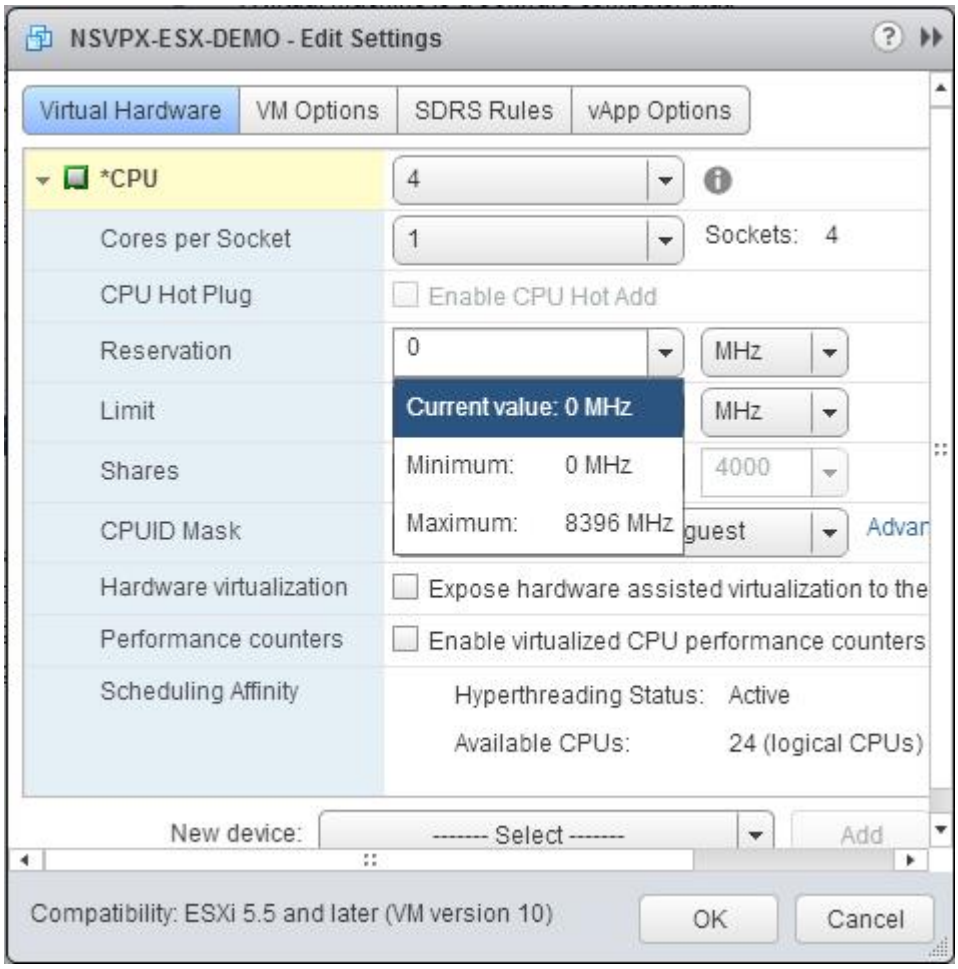
   a. En la lista desplegable **CPU**, seleccione el número de CPU que desea asignar al dispositivo virtual.

   b. En la lista desplegable **Núcleos por socket**, seleccione el número de sockets.

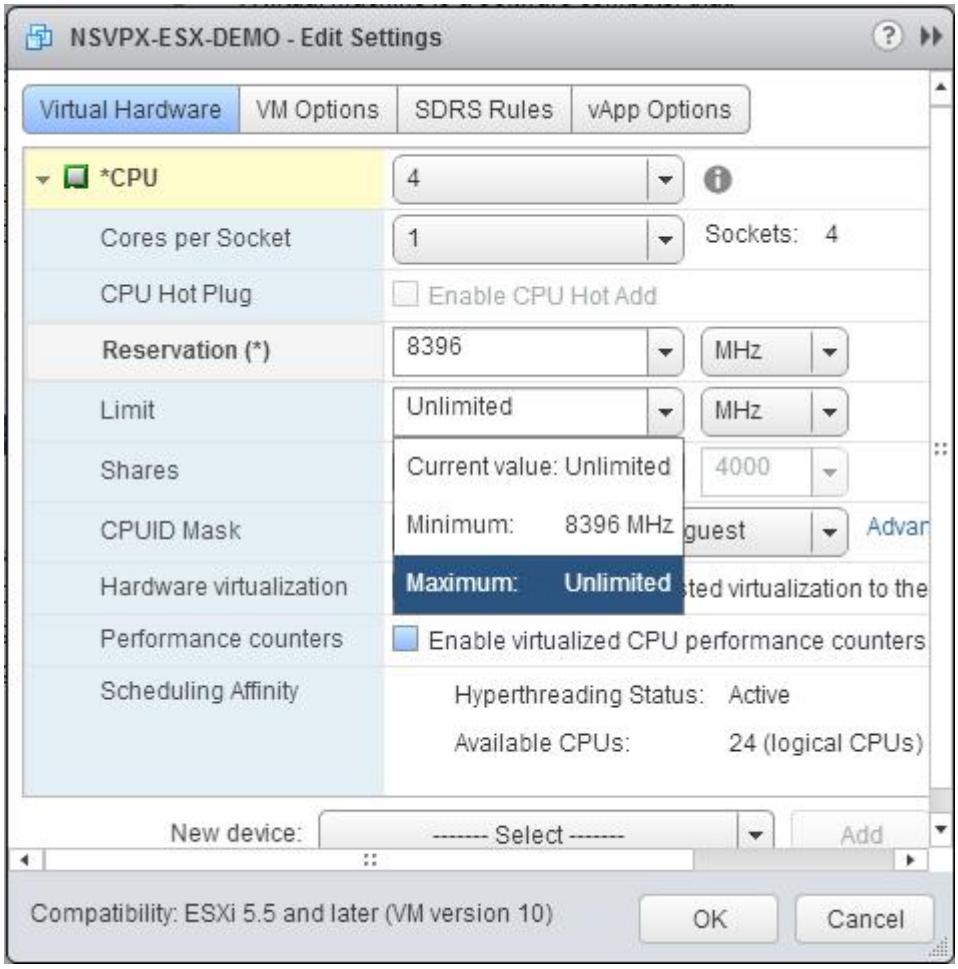
c. (Opcional) En el campo **CPU Hot Plug**, active o desactive la casilla de verificación **Habilitar CPU Hot Add**.

Nota: Citrix recomienda aceptar el valor predeterminado (inhabilitado).

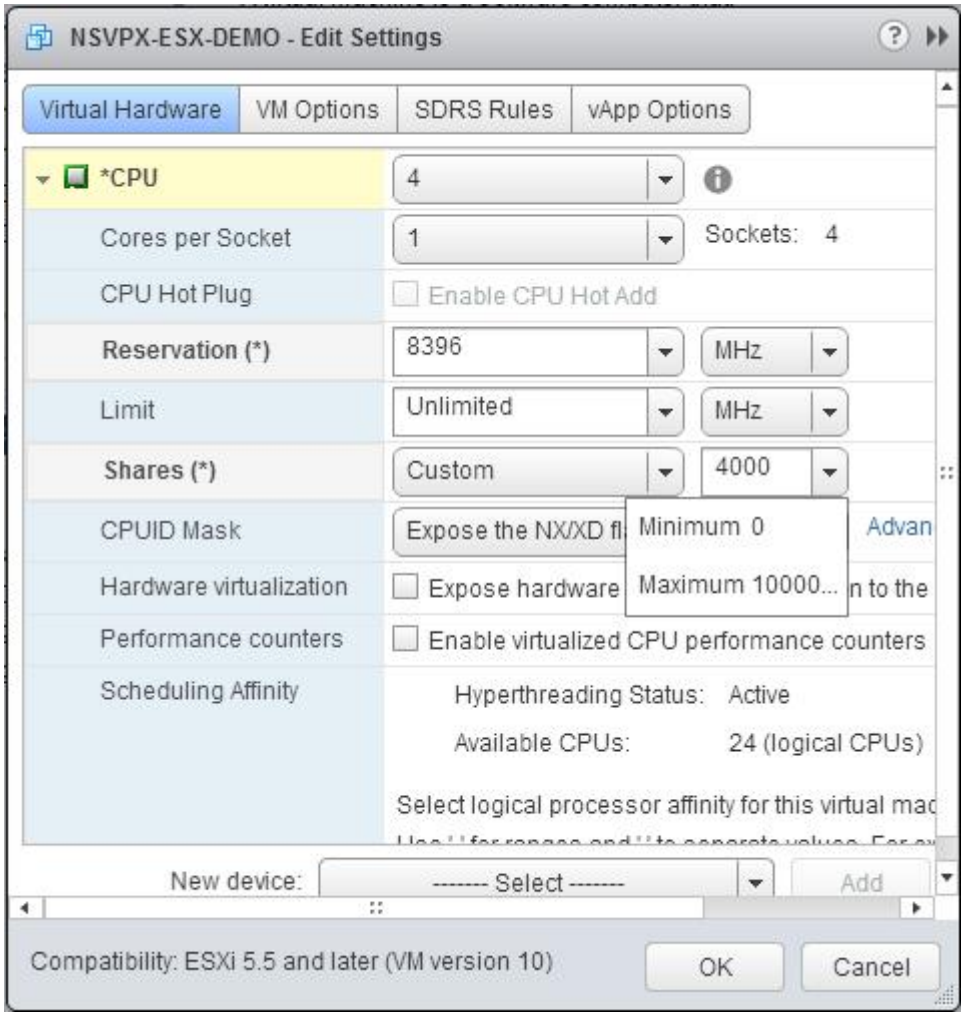
d. En la lista desplegable **Reserva**, seleccione el número que se muestra como valor máximo.



e. En la lista desplegable **Límite**, seleccione el número que se muestra como valor máximo.



f. En las listas desplegables **Acciones**, seleccione **Personalizado** y el número que se muestra como valor máximo.



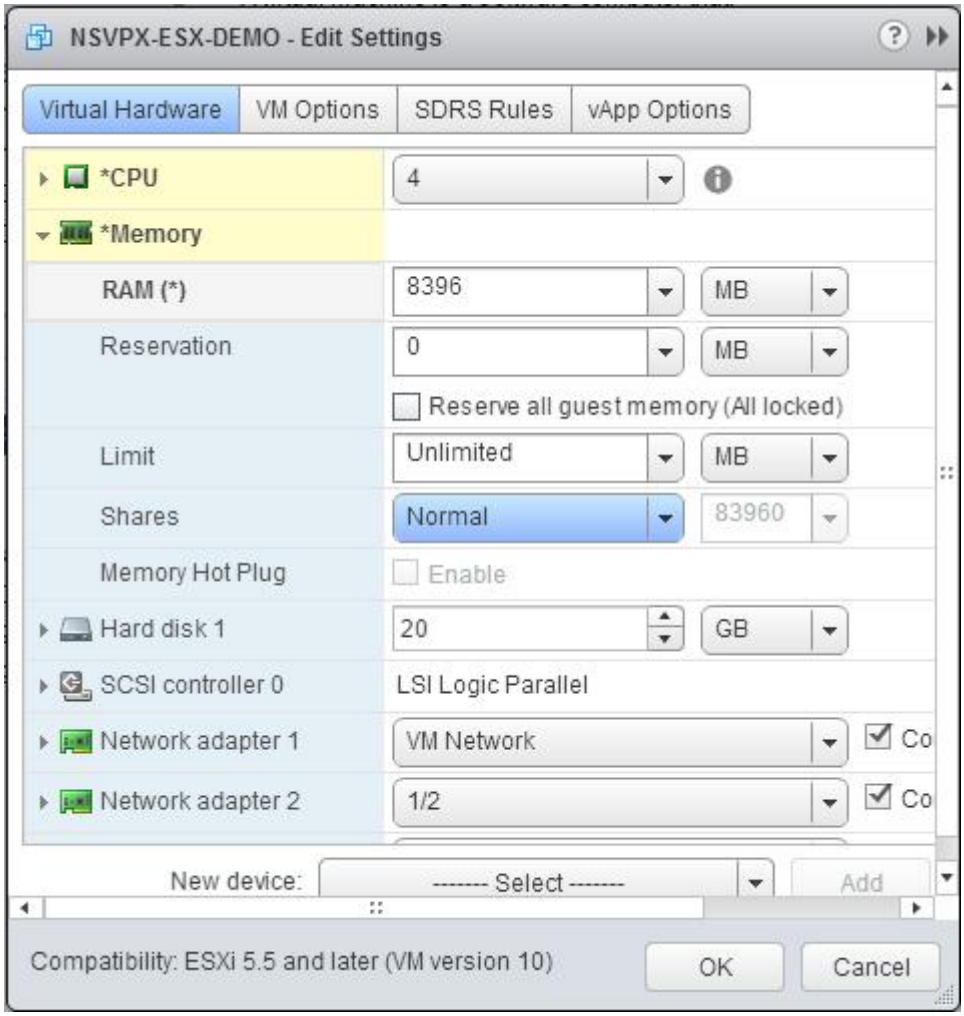
6. En la sección **Memoria**, actualice la siguiente configuración:

   - Tamaño de la RAM
   - Reservas
   - Límite
   - Acciones

   Establezca los valores de la siguiente manera:

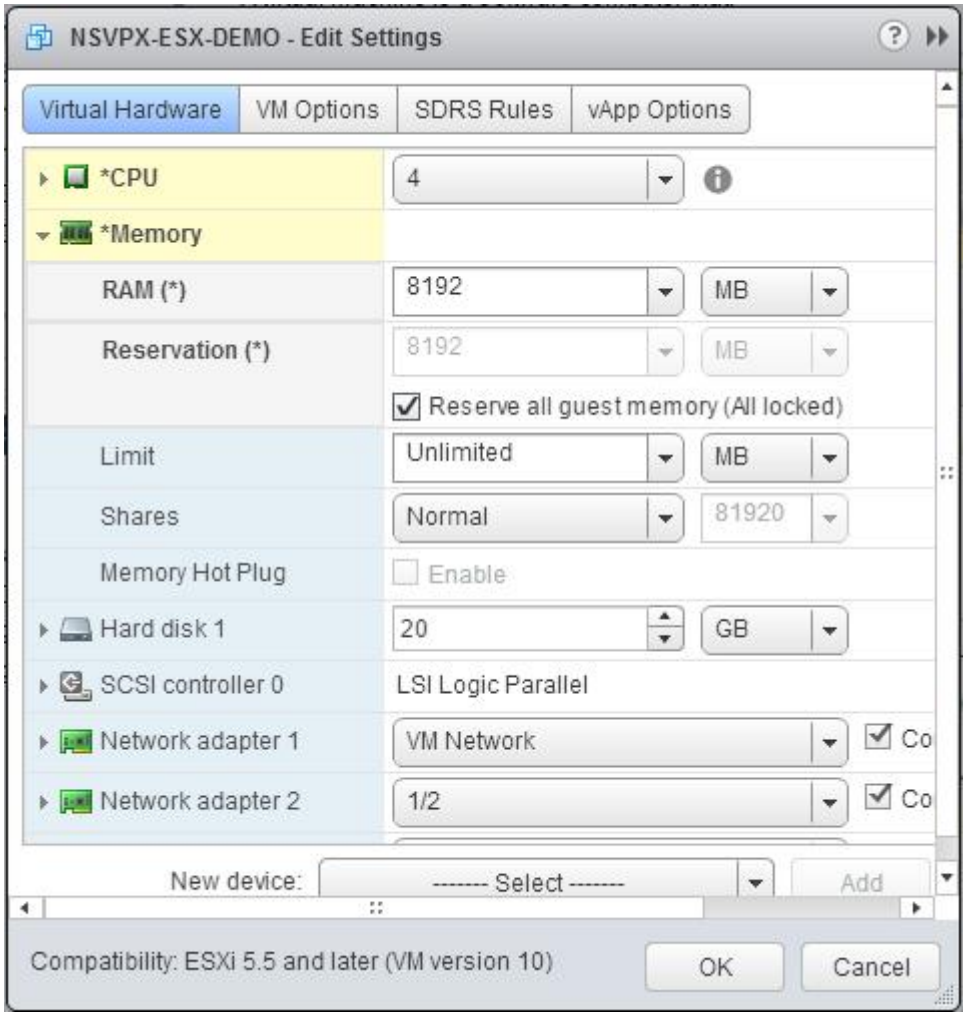
   a. En la lista desplegable **RAM**, seleccione el tamaño de la RAM. Debe ser el número de vCPU x 2 GB. Por ejemplo, si el número de vCPU es 4, entonces RAM = 4 x 2 GB = 8 GB.

   Nota: Para la edición Advanced o Premium del dispositivo Citrix ADC VPX, asegúrese de asignar 4 GB de RAM a cada vCPU. Por ejemplo, si el número de vCPU es 4, entonces RAM = 4 x 4 GB = 16 GB.

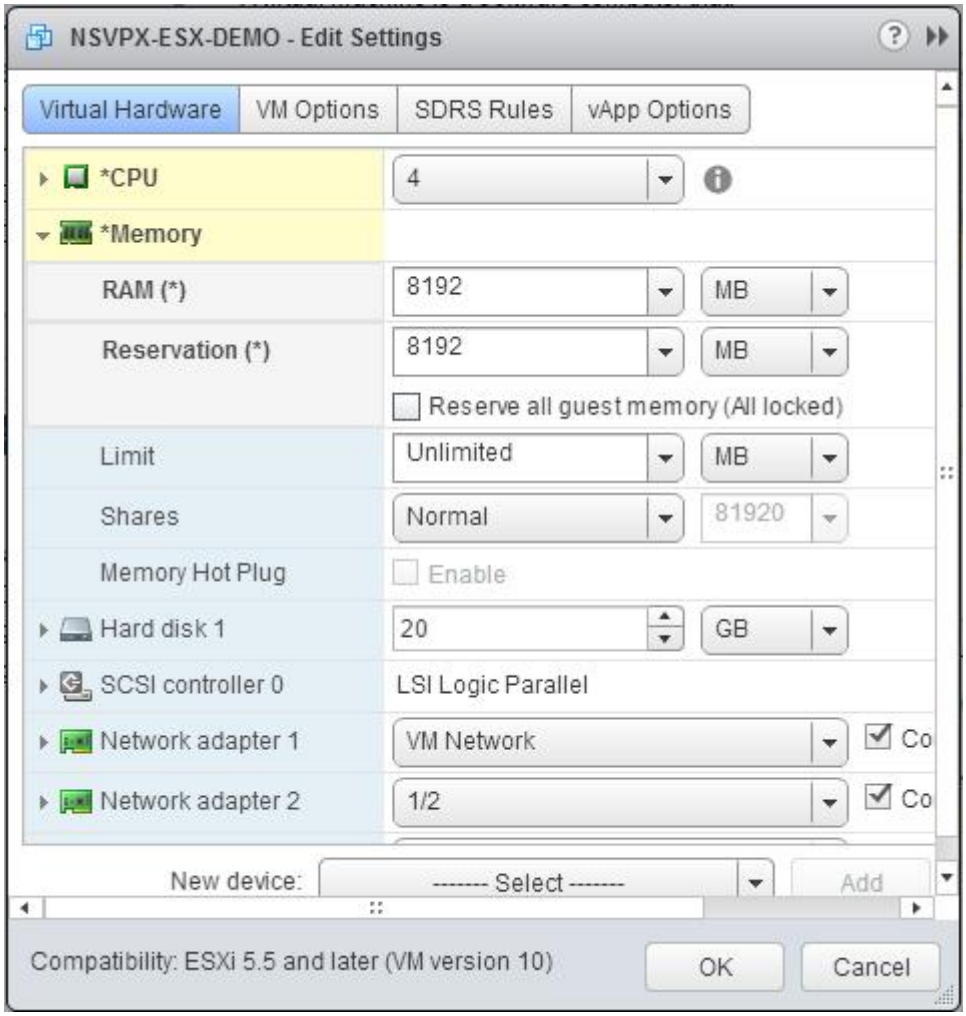


b. En la lista desplegable **Reserva**, introduzca el valor de la reserva de memoria y active la casilla de verificación Reservar **toda la memoria de invitado (Todo bloqueado)**. La reserva de memoria debe ser el número de vCPU x 2 GB. Por ejemplo, si el número de vCPU es 4, la reserva de memoria debe ser de 4 x 2 GB = 8 GB.

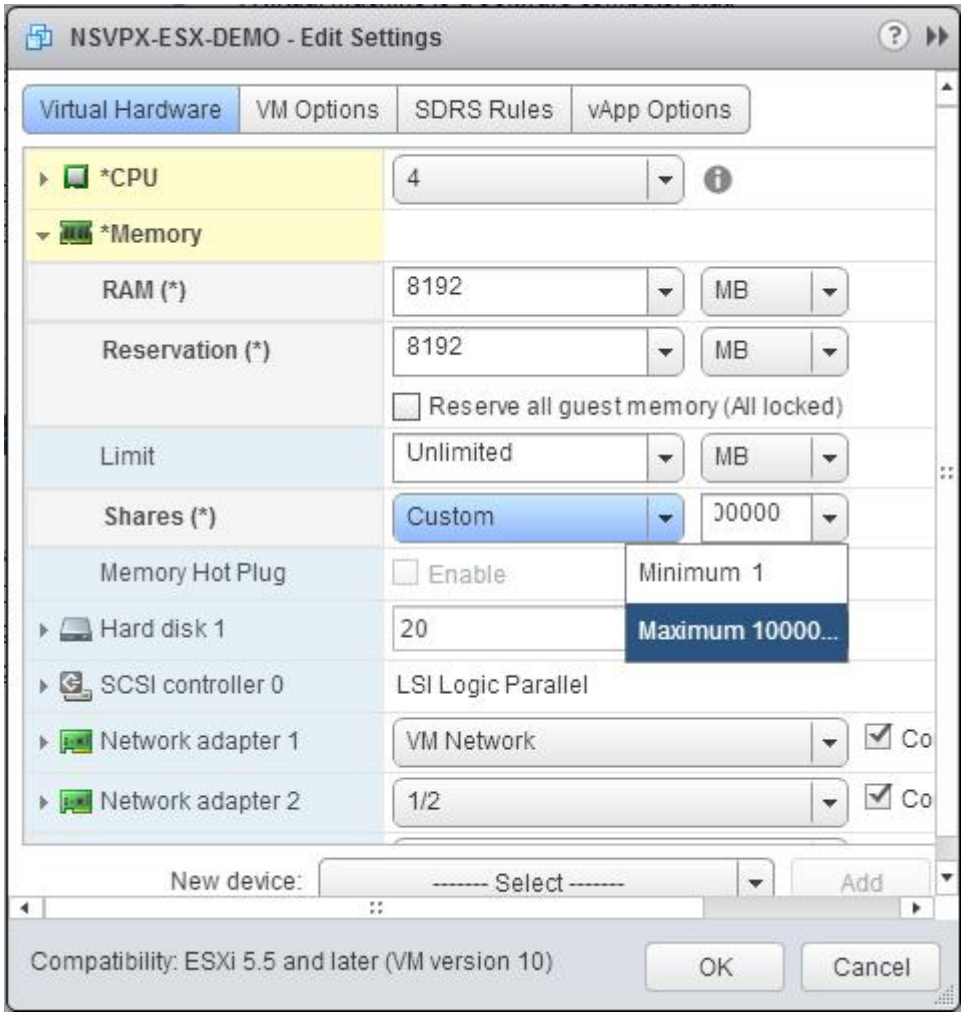
Nota: Para la edición Advanced o Premium del dispositivo Citrix ADC VPX, asegúrese de asignar 4 GB de RAM a cada vCPU. Por ejemplo, si el número de vCPU es 4, entonces RAM = 4 x 4 GB = 16 GB.



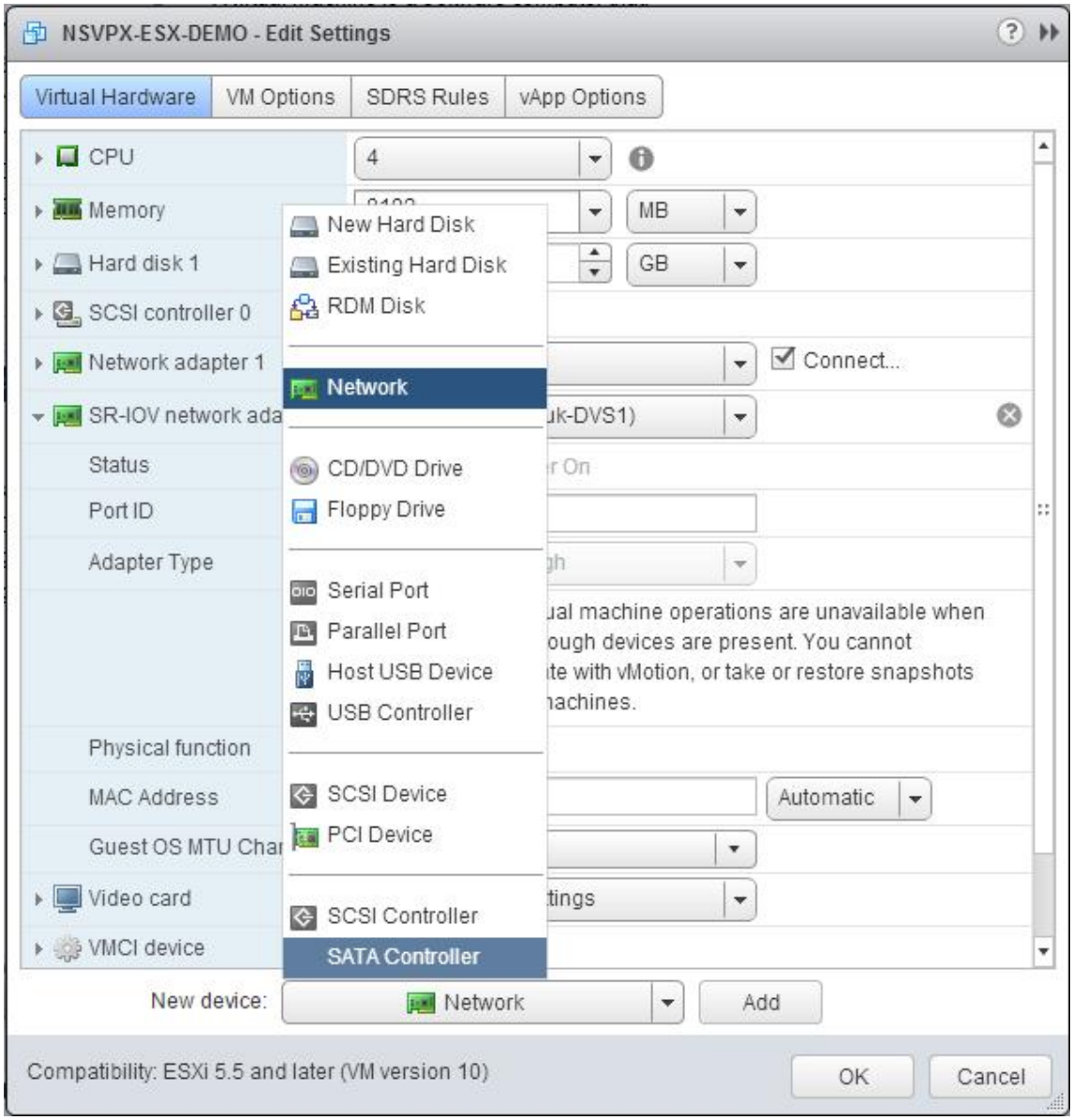
c. En la lista desplegable **Límite**, seleccione el número que se muestra como valor máximo.



d. En las listas desplegables **Acciones**, seleccione **Personalizado** y seleccione el número que se muestra como valor máximo.

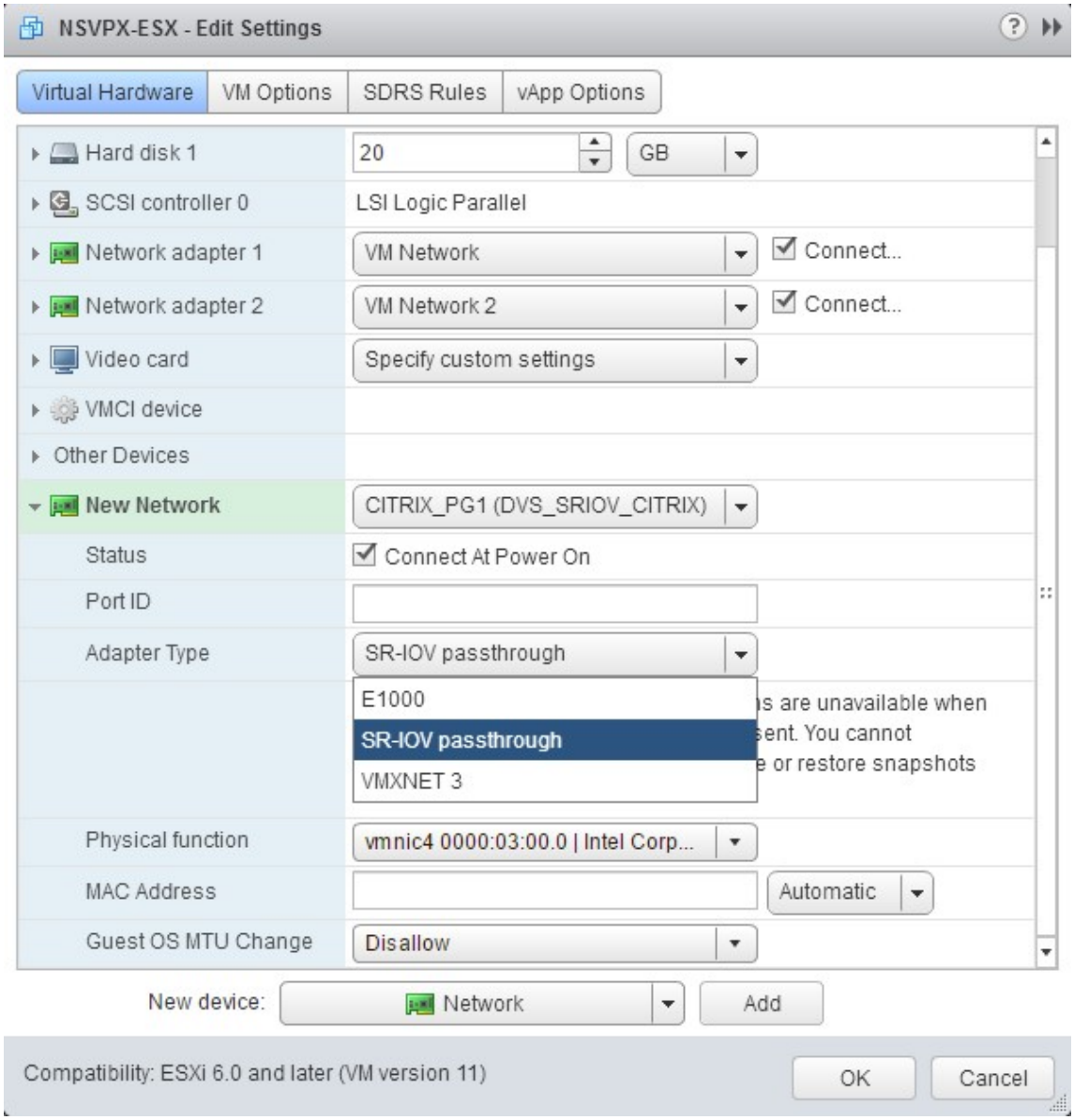


7. Agregue una interfaz de red SR-IOV. En la lista desplegable **Nuevo dispositivo**, seleccione **Red** y haga clic en **Agregar**.

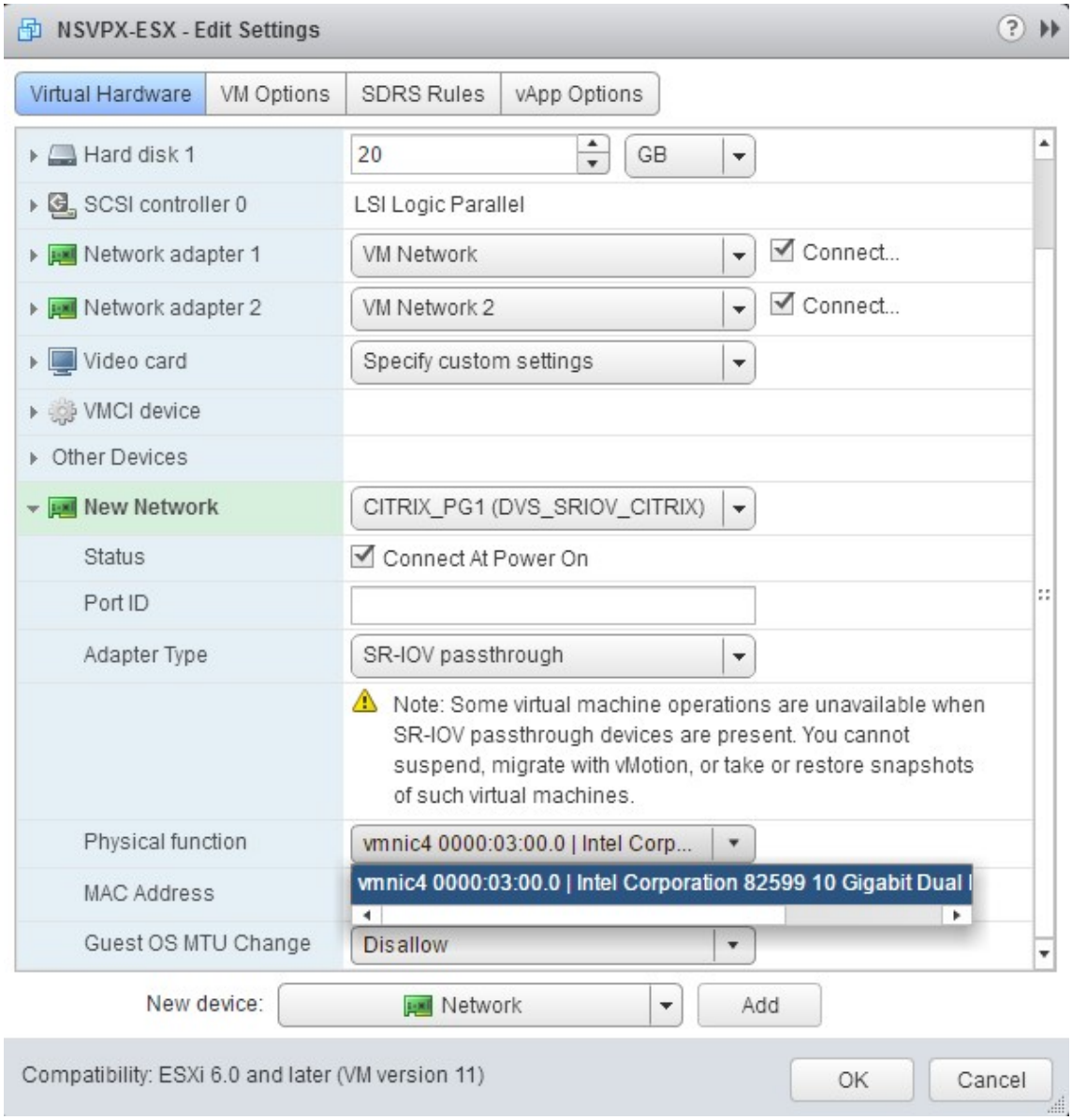


8. En la sección **Nueva red**. En la lista desplegable, seleccione el `Portgroup` que ha creado y haga lo siguiente:

   a. En la lista desplegable **Tipo de adaptador**, seleccione **Passthrough SR-IOV**.



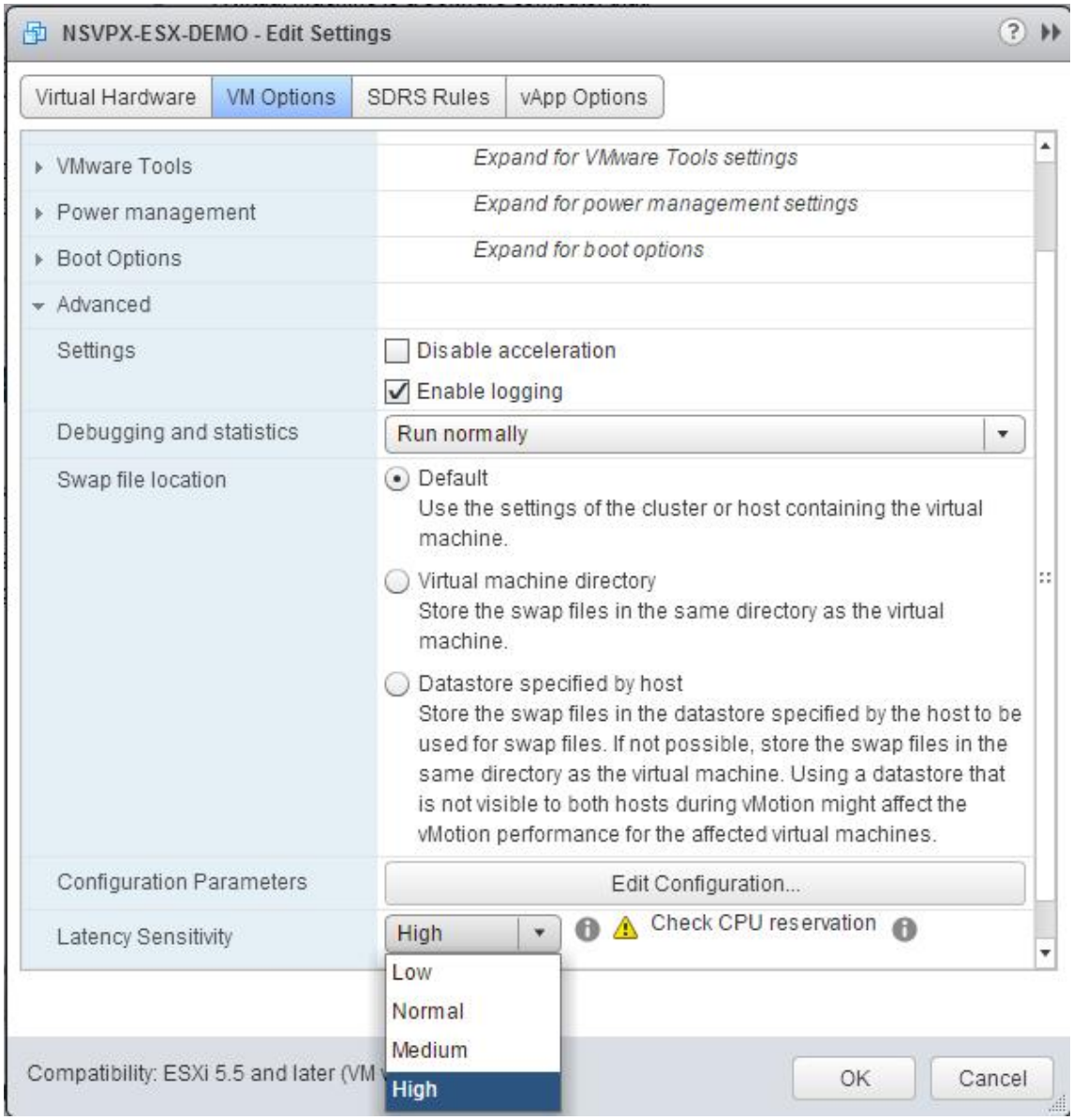
b. En la lista desplegable **Función física**, seleccione el adaptador físico asignado a `Portgroup`.



c. En la lista desplegable **Cambiar MTU del SO invitado**, seleccione **No permitir**.

9. En el ****<virtual_appliance> cuadro de diálogo: Modificar configuración, haga clic en la ficha **Opciones de VM**.

10. En la ficha **Opciones de VM**, seleccione la sección **Avanzadas**. En la lista desplegable **Sensibilidad de latencia**, seleccione **Alta**.



11. Haga clic en **Aceptar**.
12. Encienda la instancia de Citrix ADC VPX.
13. Una vez que se enciende la instancia de Citrix ADC VPX, puede utilizar el siguiente comando para verificar la configuración:

    > mostrar resumen de interfaz

El resultado debe mostrar todas las interfaces que ha configurado:

```
1 > show interface summary
2 ---------------------------------------------------------------------------
```



```
3        Interface  MTU        MAC                Suffix
4 ----------------------------------------------------------------------------

5 1      0/1        1500       00:0c:29:1b:81:0b  NetScaler Virtual
     Interface
6 2      10/1       1500       00:50:56:9f:0c:6f  Intel 82599 10G VF
     Interface
7 3      10/2       1500       00:50:56:9f:5c:1e  Intel 82599 10G VF
     Interface
8 4      10/3       1500       00:50:56:9f:02:1b  Intel 82599 10G VF
     Interface
9 5      10/4       1500       00:50:56:9f:5a:1d  Intel 82599 10G VF
     Interface
10 6     10/5       1500       00:50:56:9f:4e:0b  Intel 82599 10G VF
     Interface
11 7     LO/1       1500       00:0c:29:1b:81:0b  Netscaler Loopback
     interface
12  Done
13 > show inter 10/1
14 1)      Interface 10/1 (Intel 82599 10G VF Interface) #1
15         flags=0xe460 <ENABLED, UP, UP, HAMON, 802.1q>
16         MTU=1500, native vlan=55, MAC=00:50:56:9f:0c:6f, uptime 0
               h21m53s
17         Actual: media FIBER, speed 10000, duplex FULL, fctl NONE,
               throughput 10000
18         LLDP Mode: NONE,                LR Priority: 1024
19
20         RX: Pkts(838020742) Bytes(860888485431) Errs(0) Drops(2527)
               Stalls(0)
21         TX: Pkts(838149954) Bytes(860895860507) Errs(0) Drops(0) Stalls
               (0)
22         NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)
23         Bandwidth thresholds are not set.
24  Done
```

Migración de Citrix ADC VPX de E1000 a las interfaces de red SR-IOV o VMXNET3

August 20, 2021

24 de mayo de 2018

Puede configurar las instancias Citrix ADC VPX de salida que utilizan interfaces de red E1000 para usar interfaces de red SR-IOV o VMXNET3.

Para configurar una instancia Citrix ADC VPX existente para utilizar interfaces de red SR-IOV, consulte Configurar una instancia Citrix ADC VPX para utilizar la interfaz de red SR-IOV.

Para configurar una instancia Citrix ADC VPX existente para que use interfaces de red VMXNET3, consulte Configurar una instancia Citrix ADC VPX para utilizar la interfaz de red VMXNET3.

Configurar una instancia de Citrix ADC VPX para utilizar la interfaz de red de transferencia PCI

August 20, 2021

Información general

Después de instalar y configurar una instancia de Citrix ADC VPX en VMware ESX Server, puede utilizar vSphere Web Client para configurar el dispositivo virtual para utilizar interfaces de red de paso PCI.

La función de transferencia PCI permite a una máquina virtual invitada acceder directamente a dispositivos PCI y PCIe físicos conectados a un host.

Requisitos previos

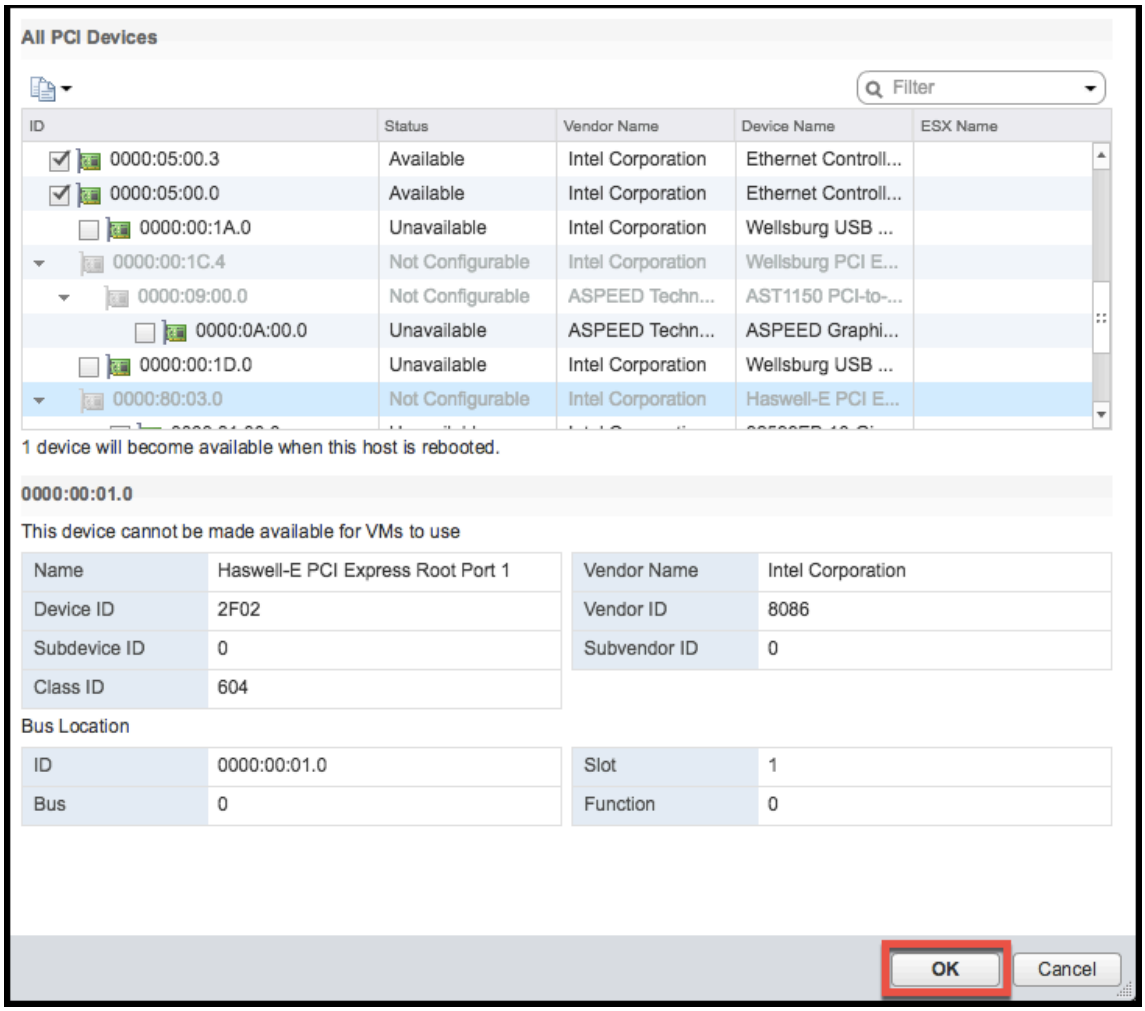
- La versión de firmware de la NIC Intel XL710 en el host es 5.04.
- Un dispositivo de transferencia PCI conectado y configurado en el host
- NIC compatibles:
  - NIC Intel X710 10G
  - NIC Intel XL710 de doble puerto 40G
  - NIC Intel XL710 de un solo puerto 40G

Configurar dispositivos de paso en un host

Antes de configurar un dispositivo PCI de paso en una máquina virtual, debe configurarlo en la máquina host. Siga estos pasos para configurar dispositivos de paso en un host.

1. Seleccione el host en el panel Navigator de vSphere Web Client.
2. Haga clic en **Administrar** > **Configuración** > **Dispositivos PCI**. Se muestran todos los dispositivos de paso disponibles.

3. Haga clic con el botón secundario en el dispositivo que quiere configurar y haga clic en **Modificar**.
4. Aparecerá la ventana **Modificar disponibilidad de dispositivos PCI**.
5. Seleccione los dispositivos que se utilizarán para el paso a través y haga clic en **Aceptar**.

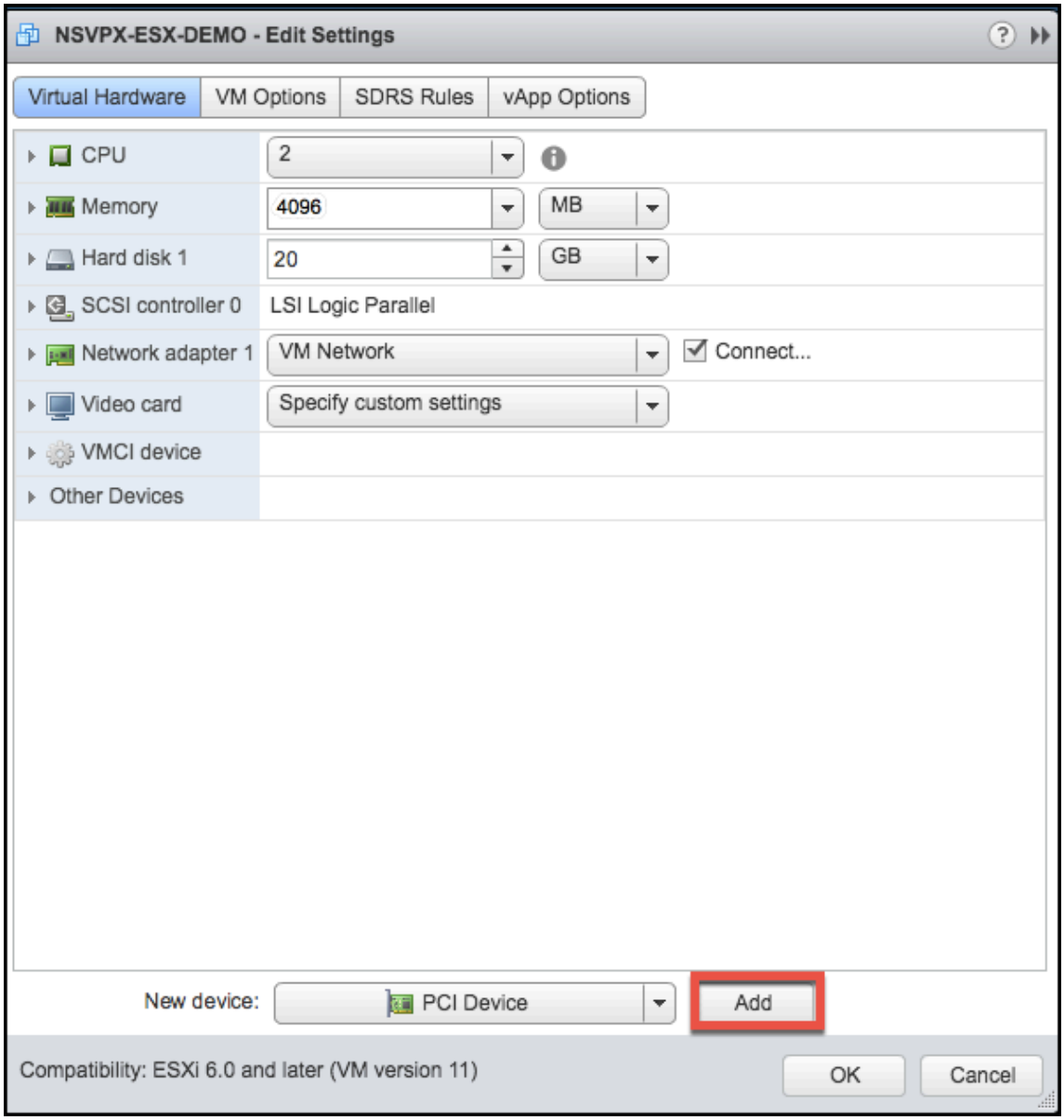


6. Reinicie el equipo host.

Configurar dispositivos de paso en una instancia de Citrix ADC VPX

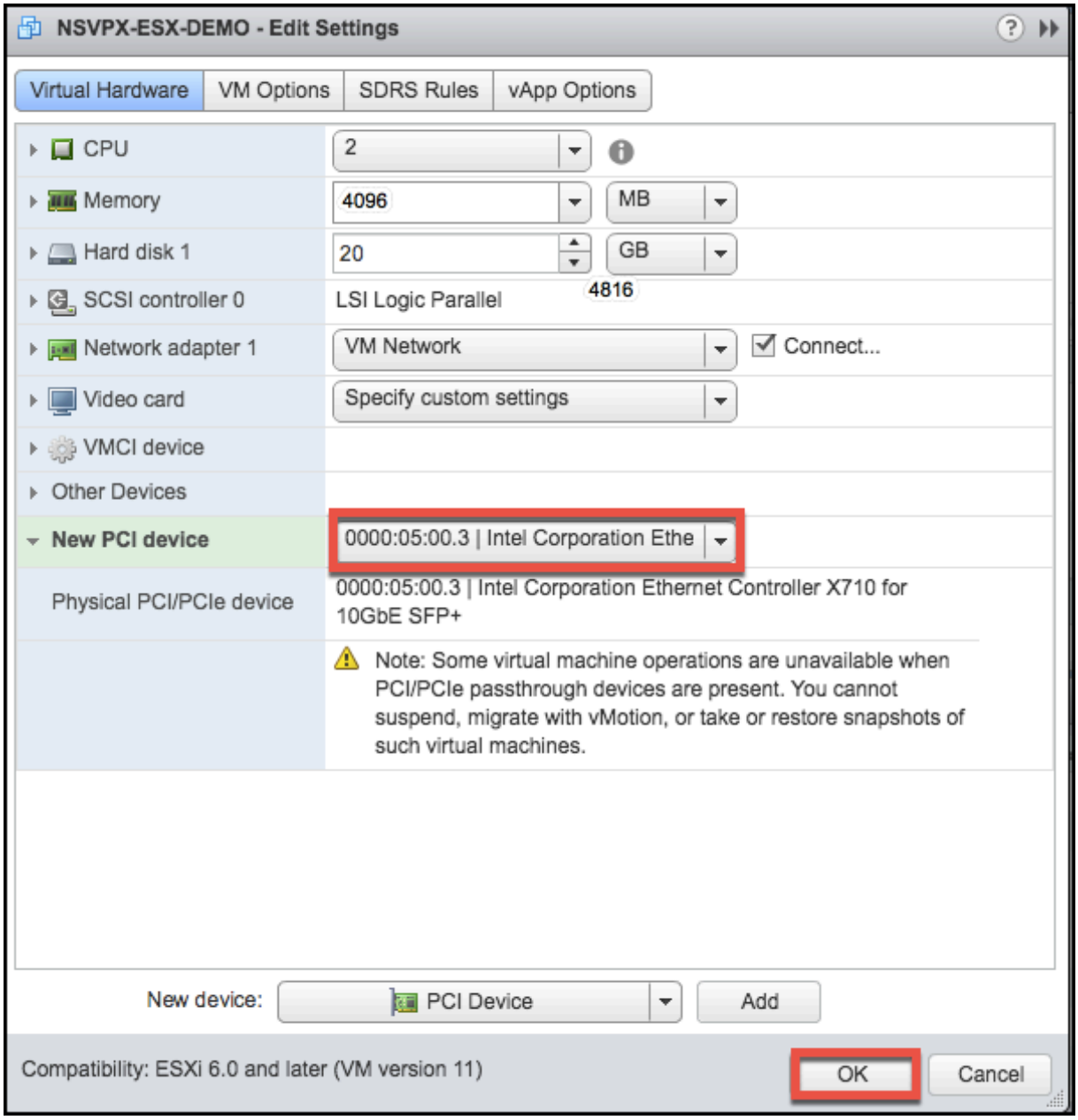
Siga estos pasos para configurar un dispositivo PCI de paso a través en una instancia de Citrix ADC VPX.

1. Apague la máquina virtual.
2. Haga clic con el botón derecho en la máquina virtual y seleccione **Modificar configuración**.
3. En la ficha **Hardware virtual**, seleccione **Dispositivo PCI** en el menú desplegable **Nuevo dispositivo** y haga clic en **Agregar**.



4. Expanda **Nuevo dispositivo PCI** y seleccione el dispositivo de paso a través para conectarse a la máquina virtual en la lista desplegable y haga clic en **Aceptar**.

> **Nota**
>
> La interfaz de red VMXNET3 y la interfaz de red PCI Passthrough no pueden coexistir.



1. Encienda la máquina virtual invitada.

Ha completado los pasos para configurar Citrix ADC VPX para que utilice interfaces de red de transferencia PCI.

Aplicar configuraciones de Citrix ADC VPX en el primer arranque del dispositivo Citrix ADC en el hipervisor VMware ESX

December 2, 2021

Puede aplicar las configuraciones de Citrix ADC VPX durante el primer arranque del dispositivo Citrix ADC en el hipervisor VMware ESX. Por lo tanto, en ciertos casos, se presenta una configuración específica o una instancia VPX en mucho menos tiempo.

Para obtener más información sobre los datos de usuario de prearranque y su formato, consulte Aplicar configuraciones de Citrix ADC VPX en el primer arranque del dispositivo Citrix ADC en la nube.

> Nota:
>
> Para arrancar con los datos de usuario de prearranque en ESX, se debe pasar la configuración de puerta de enlace predeterminada en la sección <NS-CONFIG>. Para obtener más información sobre el contenido de la etiqueta <NS-CONFIG>, consulte [Sample-<NS-CONFIG>-section](apply-preboot-userdata-on-esx-vpx.html#sample-<ns-config>-section).

<NS-CONFIG> Sección de muestra:

```
<NS-PRE-BOOT-CONFIG>

    <NS-CONFIG>
        add route 0.0.0.0 0.0.0.0  10.102.38.1
    </NS-CONFIG>

    <NS-BOOTSTRAP>
            <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
            <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>

        <MGMT-INTERFACE-CONFIG>
                <INTERFACE-NUM> eth0 </INTERFACE-NUM>
                <IP> 10.102.38.216 </IP>
                <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
        </MGMT-INTERFACE-CONFIG>
    </NS-BOOTSTRAP>

</NS-PRE-BOOT-CONFIG>
<!--NeedCopy-->
```

Cómo proporcionar datos de usuario previos al arranque en el hipervisor ESX

Puede proporcionar datos de usuario antes del arranque en el hipervisor ESX de las dos maneras siguientes:

- Uso de CD/DVD ISO
- Uso de la propiedad OVF

Proporcionar datos de usuario mediante CD/DVD ISO

Puede utilizar el cliente de VMware vSphere para inyectar datos de usuario en la VM como una imagen ISO mediante la unidad de CD/DVD.

Siga estos pasos para proporcionar los datos del usuario mediante ISO de CD/DVD:

1. Cree un archivo con un nombre de archivo `userdata` que contenga el contenido de datos de usuario antes del arranque. Para obtener más información sobre el contenido de la etiqueta <NS-CONFIG>, consulte la sección Sample <NS-CONFIG>.

   > Nota: El nombre del archivo debe usarse estrictamente como `userdata`.

2. Guarde el archivo `userdata` en una carpeta y cree una imagen ISO con la carpeta.

   Puede crear una imagen ISO con un archivo `userdata` mediante los dos métodos siguientes:

   - Usar cualquier herramienta de procesamiento de imágenes, como PowerISO.
   - Mediante comandos `mkisofs` en Linux.

   La siguiente configuración de ejemplo muestra cómo generar una imagen ISO con el comando `mkisofs` en Linux.

```
root@ubuntu:~/sai/14jul2021# ls -l total 4
drwxr-xr-x 2 root root 4096 Jul 14 12:32 esx_preboot_userdata
root@ubuntu:~/sai/14jul2021#
root@ubuntu:~/sai/14jul2021# ls -l esx_preboot_userdata/total 4
-rw-r--r-- 1 root root 3016 Jul 14 12:32 userdata
root@ubuntu:~/sai/14jul2021# mkisofs -o esx_preboot_userdata.iso
    ./esx_preboot_userdata
I: -input-charset not specified, using utf-8 (detected in locale
    settings)
Total translation table size: 0
Total rockridge attributes bytes: 0
Total directory bytes: 112
Path table size(bytes): 10
Max brk space used 0
176 extents written (0 MB)
root@ubuntu:~/sai/14jul2021# ls -lh
total 356K
drwxr-xr-x 2 root root 4.0K Jul 14 12:32 esx_preboot_userdata
-rw-r--r-- 1 root root 352K Jul 14 12:34 esx_preboot_userdata.iso

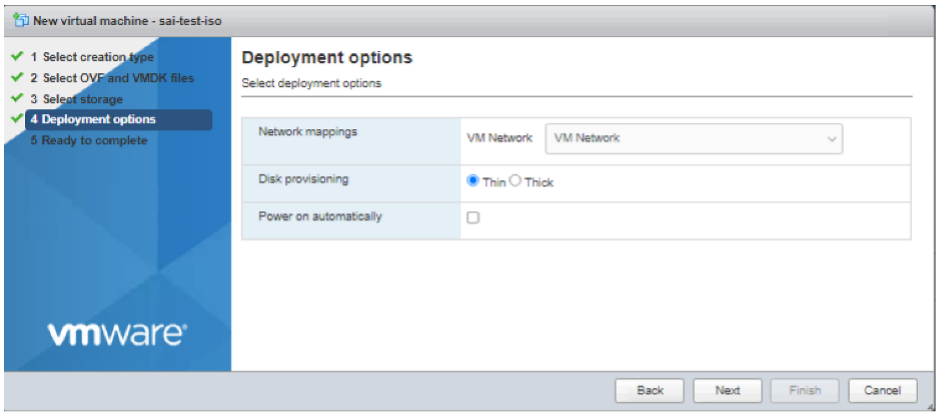
root@ubuntu:~/sai# ls preboot_userdata_155_193 userdata
root@ubuntu:~/sai# mkisofs -o preboot_userdata_155_193.iso ./
    preboot_userdata_155_193
```



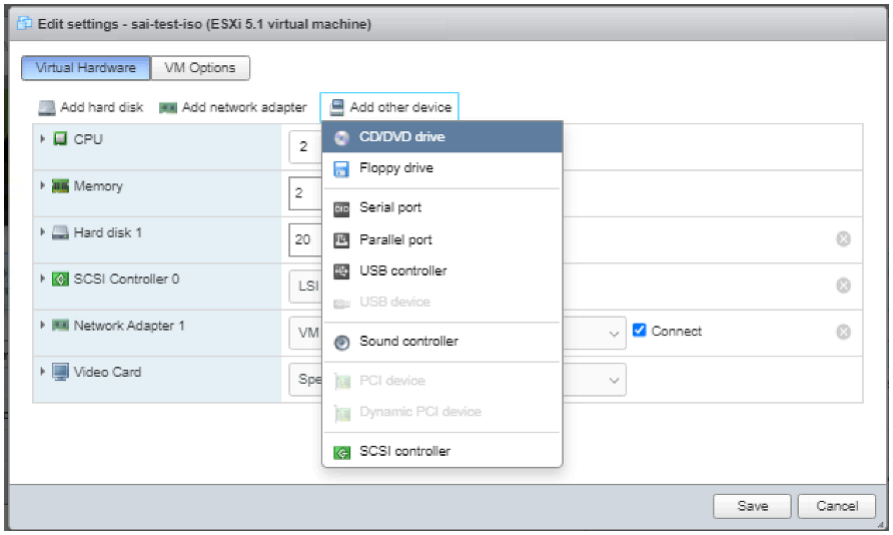
```
I: -input-charset not specified, using utf-8 (detected in locale
    settings)
Total translation table size: 0
Total rockridge attributes bytes: 0
Total directory bytes: 112
Path table size(bytes): 10
Max brk space used 0
176 extents written (0 MB)

<!--NeedCopy-->
```

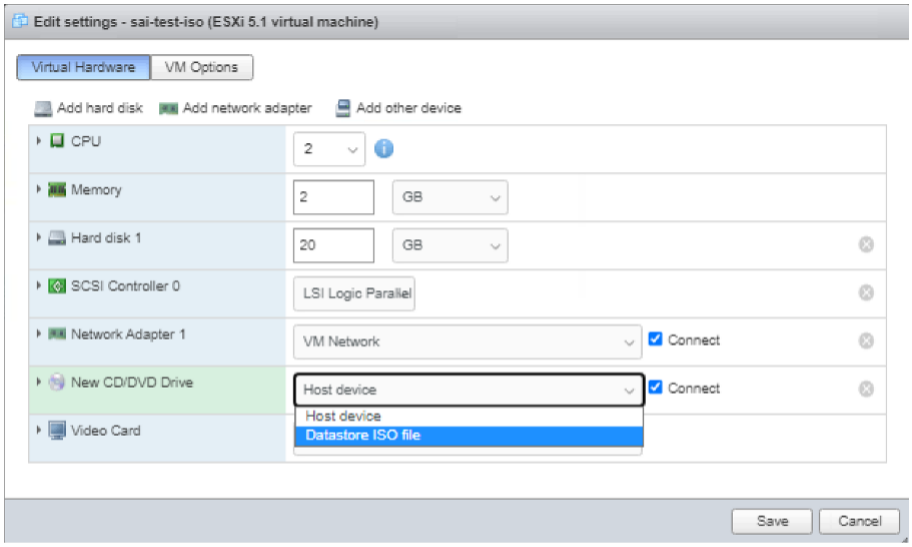
3. Aprovisione la instancia de Citrix ADC VPX mediante el proceso de implementación estándar para crear la VM. Pero no encienda la VM automáticamente.



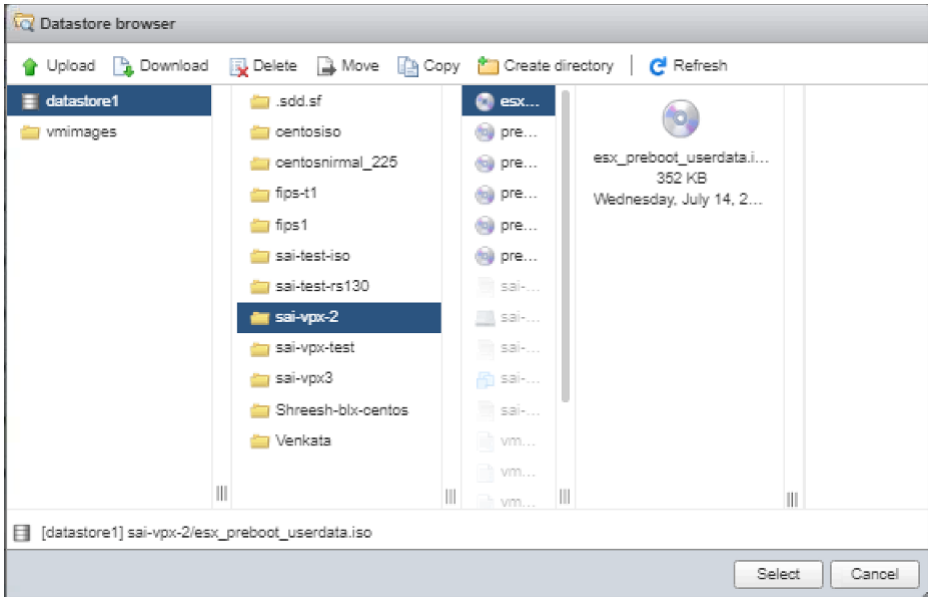
4. Una vez que la VM se haya creado correctamente, adjunte el archivo ISO como unidad de CD/DVD a la VM.



5. Vaya a **Nueva unidad de CD/DVD** y elija **Archivo ISO de Datastore** en el menú desplegable.



6. Seleccione un almacén de datos en vSphere Client.



7. Encienda la máquina virtual.

Proporcionar datos de usuario mediante la propiedad OVF

Siga estos pasos para proporcionar datos del usuario mediante la propiedad OVF.

1. Cree un archivo con contenido de datos del usuario.


```
root@ubuntu:~/sai/14jul2021# cat esx_userdata.xml
<NS-PRE-BOOT-CONFIG>
    <NS-CONFIG>
        add route 0.0.0.0 0.0.0.0 10.102.38.1
    </NS-CONFIG>

    <NS-BOOTSTRAP>
            <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
            <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>

        <MGMT-INTERFACE-CONFIG>
                <INTERFACE-NUM> eth0 </INTERFACE-NUM>
                <IP>    10.102.38.219 </IP>
                <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
        </MGMT-INTERFACE-CONFIG>
    </NS-BOOTSTRAP>
</NS-PRE-BOOT-CONFIG>
```

2. Codifique el contenido de los datos del usuario con codificación Base64. Puede realizar la codificación Base64 mediante los dos métodos siguientes:

   - En Linux, usa el siguiente comando:

   ```
   base64 <userdata-filename>  >   <outuput-file>
   <!--NeedCopy-->
   ```

   Ejemplo:

   ```
   base64 esx_userdata.xml  > esx_userdata_b64
   <!--NeedCopy-->
   ```

   ```
   root@ubuntu:~/sai/14jul2021# base64 esx_userdata.xml > esx_userdata_b64
   root@ubuntu:~/sai/14jul2021#
   root@ubuntu:~/sai/14jul2021# cat esx_userdata_b64
   PE5TLVBSRS1CT09ULUNPTkZJRz4KICAgIDxOUy1DT05GSUc+CglhZGQgcm91dGUgMC4wLjAuMCAw
   LjAuMC4wIDEwLjEwMi4zOC4xCiAgICA8L05TLUNPTkZJRz4KICAgICA8TlMtQk9PVFNUUkFQPgog
   ICAgICAgICAgICA8U0tJUC1ERUZBVUxULUJPT1RTVFJBUD5ZRVM8L1NLSVAtREVGQVVMVC1CT09U
   U1RSQVA+CiAgICAgICAgICAgIDxORVctQk9PVFNUUkFQLVNFUVVFTkNFPllFUzwvTkVXLUJPT1RT
   VFJBUC1TRVFVRU5DRT4KCiAgICAgICAgPE1HTVQtSU5URVJGQUNFLUNPTkZJRz4KICAgICAgICAg
   ICAgICAgIDxJTlRFUkZBQ0UtTlVNPiBldGgwIDwvSU5URVJGQUNFLU5VTT4KICAgICAgICAgICAg
   ICAgIDxJUD4gICAgMTAuMTAyLjM4LjIxOSA8L0lQPgogICAgICAgICAgICAgICAgPFNVQk5FVC1N
   QVNLPiAyNTUuMjU1LjI1NS4wIDwvU1VCTkVULU1BU0s+CiAgICAgICAgPC9NR01ULUlOVEVSRkFD
   RS1DT05GSUc+CiAgICA8L05TLUJPT1RTVFJBUD4KPC9OUy1QUkUtQk9PVC1DT05GSUc+Cg==
   ```

   - Utilice herramientas en línea para codificar el contenido de datos del usuario, por ejemplo, Base64 Encode and Decode.

3. Incluya una sección de **productos** en la plantilla de OVF de una instancia de Citrix ADC VPX en el hipervisor ESX.

   Sección de productos de muestra:


```
<ProductSection>

  <Info>Information about the installed software</Info>
  <Product>NSVPX-VSK Template</Product>
  <Vendor>Citrix</Vendor>
  <VendorUrl>www.citrix.com</VendorUrl>
  <Category> Preboot Userdata </Category>

  <Property ovf:key="guestinfo.userdata" ovf:type="string" ovf:
     userConfigurable="true" ovf:value="">

    <Label>Userdata</Label>
    <Description> Userdata for ESX VPX </Description>
  </Property>

</ProductSection>
<!--NeedCopy-->
```

4. Proporcionar los datos de usuario codificados en base64 como `ovf:value` para la propiedad `guestinfo.userdata` en la sección Producto.

```
<ProductSection>

  <Info>Information about the installed software</Info>
  <Product>NSVPX-VSK Template</Product>
  <Vendor>Citrix</Vendor>
  <VendorUrl>www.citrix.com</VendorUrl>
  <Category> Preboot Userdata </Category>
  <Property ovf:key="guestinfo.userdata" ovf:type="string" ovf:
     userConfigurable="true"
    ovf:value="PE5TLVBSRS1CT09ULUNPTkZJRz4KICAgIDxOUy1DT05GSUc+
       CglhZGQgcm91dGUgMC4wLjAuMCAw
    LjAuMC4wIDEwLjEwMi4zOC4xCiAgICA8L05TLUNPTkZJRz4KCiAgICA8TlMtQk9PVFNUUkFQ

    ICAgICAgICAgICA8U0tJUC1ERUZBVUxULUJPT1RTVFJBUD5ZRVM8L1NLSVAtREVGQVVMVC1C

    U1RSQVA+
       CiAgICAgICAgICAgIDxORVctQk9PVFNUUkFQLVNFUVVFTkNFPllFUzwvTkVXLUJPT1RT

    VFJBUC1TRVFVRU5DRT4KICAgICAgICAgPE1HTVQtSU5URVJGQUNFLUNPTkZJRz4KICAgICAg

    ICAgICAgICAgIDxJTlRFUkZBQ0UtTlVNPiBldGgwIDwvSU5URVJGQUNFLU5VTT4KICAgICAg
```



```
15      ICAgIDxJUD4gICAgMTAuMTAyLjM4LjIxOSA8L0lQPgogICAgICAgICAgICAgICAgPFNVQk5F
16      QVNLPiAyNTUuMjU1LjI1NS4wIDwvU1VCTkVULU1BU0s+
           CiAgICAgICAgPC9NR01ULULlOVEVSRkFD
17      RS1DT05GSUc+
           CiAgICA8L05TLUJPT1RTVFJBUD4KPC9OUy1QUkUtQk9PVC1DT05GSUc+Cg
           ==”>
18
19      <Label>Userdata</Label>
20      <Description> Userdata for ESX VPX </Description>
21    </Property>
22
23  </ProductSection>
24  <!--NeedCopy-->
```

5. Use la plantilla OVF modificada con la sección Product para la implementación de VM.

```
Please change the default NSROOT password.
Enter new password:
Please re-enter your password:
 Done
> sh ns ver
        NetScaler NS13.0: Build 83.9005.nc, Date: Jul 13 2021, 02:56:05   (64-bit)
 Done
> sh ns ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  S
tate
        ---------        --------------  ----             ----     ---      ----     -------  -
-----
1)      10.102.38.219    0               NetScaler IP     Active   Enabled  Enabled  NA       E
nabled
 Done
> sh route
        Network          Netmask          Gateway/OwnedIP  VLAN    State   Traffic Domain  Type
        -------          -------          ---------------  -----   -----   --------------  ----
1)      0.0.0.0          0.0.0.0          10.102.38.1      0       UP      0               STATI
C
2)      127.0.0.0        255.0.0.0        127.0.0.1        0       UP      0               PERMA
NENT
3)      10.102.38.0      255.255.255.0    10.102.38.219    0       UP      0               DIREC
T
 Done
```

Instalar una instancia de Citrix ADC VPX en la nube de VMware en AWS

August 20, 2021

VMware Cloud (VMC) en AWS le permite crear centros de datos definidos por software (SDDC) en la nube en AWS con el número deseado de hosts ESX. VMC en AWS admite implementaciones de Citrix ADC VPX. VMC proporciona una interfaz de usuario igual que vCenter en las instalaciones. Funciona idéntico a las implementaciones de Citrix ADC VPX basadas en ESX.

Requisitos previos

Antes de comenzar a instalar un dispositivo virtual, haga lo siguiente:

- Debe estar presente un SDDC de VMware con al menos un host.
- Descargue los archivos de configuración del dispositivo Citrix ADC VPX.
- Cree segmentos de red adecuados en VMware SDDC a los que se conectan las máquinas virtuales.
- Obtenga archivos de licencia VPX. Para obtener más información acerca de las licencias de instancia de Citrix ADC VPX, consulte la *Guía de licencias de Citrix ADC VPX* en http://support.citrix.com/article/ctx131110.

RequiVMware de hardware en la nube

En la tabla siguiente se enumeran los recursos informáticos virtuales que el SDDC de VMware debe proporcionar para cada dispositivo virtual VPX nCore.

Cuadro 1 Recursos informáticos virtuales mínimos necesarios para ejecutar una instancia de Citrix ADC VPX

Componente	Requisito
Memoria	2 GB
CPU virtual (vCPU)	2
Interfaces de red virtual	En VMware SDDC, puede instalar un máximo de 10 interfaces de red virtual si el hardware VPX se actualiza a la versión 7 o superior.
Espacio en disco	20 GB

> Nota
>
> Esto se suma a cualquier requisito de disco para el Hypervisor.

Para el uso en producción del dispositivo virtual VPX, debe reservarse la asignación de memoria completa.

Requisitos del sistema OVF Tool 1.0

OVF Tool es una aplicación cliente que puede ejecutarse en sistemas Windows y Linux. En la siguiente tabla se describen los requisitos mínimos del sistema.

Tabla 2. Requisitos mínimos del sistema para la instalación de herramientas OVF

Componente	Requisito
Sistema operativo	Para obtener información detallada sobre los requisitos de VMware, busque el archivo PDF "OVF Tool User Guide" en http://kb.vmware.com/.
CPU	750 MHz como mínimo, se recomienda 1 GHz o más rápido
RAM	1 GB mínimo, 2 GB recomendado
NIC	NIC de 100 Mbps o más rápido

Para obtener información acerca de la instalación de OVF, busque el archivo PDF "Guía del usuario de la herramienta OVF" en http://kb.vmware.com/.

Descarga de los archivos de configuración de Citrix ADC VPX

El paquete de instalación de instancias de Citrix ADC VPX para VMware ESX sigue el estándar de formato Open Virtual Machine (OVF). Puede descargar los archivos desde el sitio web de Citrix. Necesita una cuenta de Citrix para iniciar sesión. Si no tiene una cuenta de Citrix, acceda a la página de inicio en http://www.citrix.com. Haga clic en el **vínculo Nuevos usuarios** y siga las instrucciones para crear una nueva cuenta de Citrix.

Una vez iniciada la sesión, navegue por la siguiente ruta desde la página principal de Citrix:

Citrix.com > **Descargas > Citrix ADC > Dispositivos virtuales**.

Copie los siguientes archivos en una estación de trabajo en la misma red que el servidor ESX. Copie los tres archivos en la misma carpeta.

- NSVPX-ESX- <release number>- <build number>-disk1.vmdk (por ejemplo, NSVPX-ESX-13.0-79.64-disk1.vmdk)
- NSVPX-ESX- <release number>- <build number>.ovf (por ejemplo, NSVPX-ESX-13.0-79.64.ovf)
- NSVPX-ESX- <release number>- <build number>.mf (por ejemplo, NSVPX-ESX-13.0-79.64.mf)

Instalar una instancia de Citrix ADC VPX en la nube de VMware

Después de instalar y configurar VMware SDDC, puede usar el SDDC para instalar dispositivos virtuales en la nube de VMware. El número de dispositivos virtuales que puede instalar depende de la cantidad de memoria disponible en el SDDC.

Para instalar instancias de Citrix ADC VPX en la nube de VMware, siga estos pasos:

1. Abra VMware SDDC en su estación de trabajo.
2. En los cuadros de texto **Nombre de usuario** y **Contraseña**, escriba las credenciales de administrador y, a continuación, haga clic en Iniciar sesión.
3. En el menú **Archivo**, haga clic en **Implementar plantilla OVF**.
4. En el cuadro de diálogo **Implementar plantilla OVF**, en **Implementar desde archivo**, busque la ubicación en la que guardó los archivos de configuración de instancias de Citrix ADC VPX, seleccione el archivo.ovf y haga clic en **Siguiente**.

   > **Nota:** De forma predeterminada, la instancia de Citrix ADC VPX utiliza interfaces de red E1000. Para implementar ADC con la interfaz VMXNET3, modifique el OVF para utilizar la interfaz VMXNET3 en lugar de E1000.

5. Asigne las redes que se muestran en la plantilla OVF del dispositivo virtual a las redes configuradas en el SDDC de VMware. Haga clic en **Siguiente** para iniciar la instalación de un dispositivo virtual en VMware SDDC.
6. Ya está listo para iniciar la instancia de Citrix ADC VPX. En el panel de navegación, seleccione la instancia de Citrix ADC VPX que ha instalado y, en el menú contextual, seleccione **Encendido**. Haga clic en la ficha **Console** para emular un puerto de consola.
7. Si quiere instalar otro dispositivo virtual, repita desde el paso 6.
8. Especifique la dirección IP de administración del mismo segmento seleccionado para ser la red de administración. Se utiliza la misma subred para la puerta de enlace.
9. VMware SDDC requiere que las reglas de NAT y firewall se creen explícitamente para todas las direcciones IP privadas pertenecientes a segmentos de red.

Instalar una instancia de Citrix ADC VPX en el servidor Microsoft Hyper-V

August 20, 2021

Para instalar instancias de Citrix ADC VPX en Microsoft Windows Server, primero debe instalar Windows Server, con la función Hyper-V habilitada, en un equipo con los recursos del sistema adecuados. Cuando instale el rol Hyper-V, debe especificar las tarjetas de interfaz de red (NIC) en el servidor que Hyper-V usa para crear las redes virtuales. Puede reservar algunas tarjetas para el host. Utilice el Administrador de Hyper-V para realizar la instalación de la instancia de Citrix ADC VPX.

La instancia Citrix ADC VPX para Hyper-V se entrega en formato de disco duro virtual (VHD). Incluye la configuración predeterminada para elementos como CPU, interfaces de red y tamaño y formato del disco duro. Después de instalar la instancia Citrix ADC VPX, puede configurar los adaptadores de red

en el dispositivo virtual, agregar NIC virtuales y, a continuación, asignar la dirección IP de Citrix ADC, la máscara de subred y la Gateway, y completar la configuración básica del dispositivo virtual.

Después de la configuración inicial de la instancia VPX, si desea actualizar el dispositivo a la última versión de software, consulte Actualización de un dispositivo independiente Citrix ADC VPX

> **Nota**
>
> El protocolo de sistema intermedio a sistema intermedio (ISIS) no es compatible con el dispositivo virtual Citrix ADC VPX alojado en la plataforma HyperV-2012.

Requisitos previos para instalar la instancia de Citrix ADC VPX en servidores Microsoft

Antes de comenzar a instalar un dispositivo virtual, haga lo siguiente:

- Habilite el rol Hyper-V en servidores Windows. Para obtener más información, consulte http://technet.microsoft.com/en-us/library/ee344837(WS.10).aspx.
- Descargue los archivos de configuración del dispositivo virtual.
- Obtenga archivos de licencia de instancia de Citrix ADC VPX. Para obtener más información acerca de las licencias de instancia de Citrix ADC VPX, consulte la *Guía de licencias de Citrix ADC VPX* en http://support.citrix.com/article/ctx131110.

Requisitos de hardware de servidor de Microsoft

En la tabla siguiente se describen los requisitos mínimos del sistema para los servidores Microsoft.

Cuadro 1 Requisitos mínimos del sistema para servidores Microsoft

Componente	Requisito
CPU	Procesador de 64 bits de 1,4 GHz
RAM	8 GB
Espacio en disco	32 GB o superior

En la siguiente tabla se enumeran los recursos informáticos virtuales para cada instancia de Citrix ADC VPX.

Tabla 2. Recursos informáticos virtuales mínimos necesarios para ejecutar una instancia de Citrix ADC VPX

Componente	Requisito
RAM	4 GB

Componente	Requisito
CPU virtual	2
Espacio en disco	20 GB
Interfaces de red virtual	1

Descargue los archivos de configuración de Citrix ADC VPX

La instancia de Citrix ADC VPX para Hyper-V se entrega en formato de disco duro virtual (VHD). Puede descargar los archivos desde el sitio web de Citrix. Necesita una cuenta de Citrix para iniciar sesión. Si no tiene una cuenta de Citrix, acceda a la página de inicio en http://www.citrix.com, haga clic **en Iniciar sesión > Mi cuenta > Crear cuenta de Citrix**y siga las instrucciones para crear una cuenta Citrix.

Para descargar los archivos de configuración de instancias de Citrix ADC VPX, siga estos pasos:

1. Desde un explorador web, vaya a http://www.citrix.com/.
2. Inicie sesión con su nombre de usuario y contraseña.
3. Haga clic en **Descargas**.
4. En **el menú desplegable Seleccionar un producto**, seleccione **Citrix ADC (NetScaler ADC)**.
5. En **Citrix ADC Release X.X > Virtual Appliances**, haga clic en **Citrix ADC VPX Release X.X**
6. Descargue el archivo comprimido en su servidor.

Instalar la instancia de Citrix ADC VPX en servidores Microsoft

Después de habilitar la función Hyper-V en Microsoft Server y extraer los archivos del dispositivo virtual, puede utilizar el Administrador de Hyper-V para instalar la instancia de Citrix ADC VPX. Después de importar la máquina virtual, debe configurar las NIC virtuales asociándolas a las redes virtuales creadas por Hyper-V.

Puede configurar un máximo de ocho NIC virtuales. Incluso si la NIC física está DOWN, el dispositivo virtual asume que la NIC virtual está UP, ya que aún puede comunicarse con los demás dispositivos virtuales del mismo host (servidor).

> **Nota**
>
> No puede cambiar ninguna configuración mientras se está ejecutando el dispositivo virtual. Apague el dispositivo virtual y, a continuación, realice los cambios.

Para instalar una instancia de Citrix ADC VPX en Microsoft Server mediante el Administrador de Hyper-V:

1. Para iniciar el Administrador de Hyper-V, haga clic en **Inicio**, seleccione **Herramientas administrativas** y, a continuación, haga clic en **Administrador de Hyper-V**.
2. En el panel de navegación, en **Hyper-V Manage**r, seleccione el servidor en el que quiere instalar la instancia de Citrix ADC VPX.
3. En el menú **Acción**, haga clic **en Importar máquina virtual**e.
4. En el cuadro de diálogo **Importar máquina virtual**, en **Ubicación**, especifique la ruta de acceso de la carpeta que contiene los archivos de software de instancia de Citrix ADC VPX y, a continuación, seleccione **Copiar la máquina virtual (cree un nuevo ID único)**. Esta carpeta es la carpeta principal que contiene las carpetas Instantáneas, Discos duros virtuales y Máquinas virtuales.
5. Nota: Si ha recibido un archivo comprimido, asegúrese de extraer los archivos en una carpeta antes de especificar la ruta de acceso a la carpeta.
6. Haga clic en **Importar**.
7. Compruebe que el dispositivo virtual que ha importado aparece en **Máquinas virtuales**.
8. Para instalar otro dispositivo virtual, repita los pasos **2** a **6**.

> **Importante**
>
> Asegúrese de extraer los archivos en una carpeta diferente en el paso **4**.

Aprovisionamiento automático de una instancia Citrix ADC VPX en Hyper-V

El aprovisionamiento automático de la instancia Citrix ADC VPX es opcional. Si no se realiza el aprovisionamiento automático, el dispositivo virtual proporciona una opción para configurar la dirección IP, etc.

Para aprovisionar automáticamente la instancia Citrix ADC VPX en Hyper-V, siga estos pasos.

1. Cree una imagen ISO compatible con ISO9660 mediante el archivo xml como se muestra en el ejemplo. Asegúrese de que el nombre del archivo xml es **userdata**.

```
<?xml version=”1.0” encoding=”UTF-8” standalone=”no”?>

<Environment xmlns:oe=`”http://schemas.dmtf.org/ovf/environment/1`
    ”

xmlns:xsi=`”http://www.w3.org/2001/XMLSchema-instance`”

oe:id=””

xmlns=`”http://schemas.dmtf.org/ovf/environment/1`”>

<PlatformSection>
```



```
12
13 <Kind>HYPER-V</Kind>
14
15 <Version>2013.1</Version>
16
17 <Vendor>CISCO</Vendor>
18
19 <Locale>en</Locale>
20
21 </PlatformSection>
22
23 <PropertySection>
24
25 <Property oe:key="com.citrix.netscaler.ovf.version" oe:value="1.0"
      />
26
27 <Property oe:key="com.citrix.netscaler.platform" oe:value="NS1000V
      "/>
28
29 <Property oe:key="com.citrix.netscaler.orch_env" oe:value="cisco-
      orch-env"/>
30
31 <Property oe:key="com.citrix.netscaler.mgmt.ip" oe:value="
      10.102.100.122"/>
32
33 <Property oe:key="com.citrix.netscaler.mgmt.netmask" oe:value="
      255.255.255.128"/>
34
35 <Property oe:key="com.citrix.netscaler.mgmt.gateway" oe:value="
      10.102.100.67"/></PropertySection>
36
37 </Environment>
38 <!--NeedCopy-->
```

2. Copie la imagen ISO en el servidor hyper-v.
3. Seleccione el dispositivo virtual que ha importado y, a continuación, en el menú **Acción**, seleccione **Configuración**. También puede seleccionar el dispositivo virtual y, a continuación, hacer clic con el botón derecho y seleccionar **Configuración**. Aparecerá la ventana **Configuración** del dispositivo virtual seleccionado.
4. En la ventana **Configuración**, en la sección de hardware, haga clic en **Controlador IDE**.
5. En el panel de la ventana derecha, seleccione **Unidad de DVD** y haga clic en **Agregar**. La unidad de DVD se agrega en la sección **Controlador IDE** en el panel izquierdo de la ventana.

6. Seleccione la **unidad de DVD** agregada en el paso 5. En el panel derecho de la ventana, seleccione el **botón de opción Archivo de imagen** y haga clic en **Examinar** y seleccione la imagen ISO que copió en el servidor Hyper-V, en el paso 2.
7. Haga clic en **Aplicar**.

> **Nota**
>
> La instancia del dispositivo virtual aparece en la dirección IP predeterminada cuando:
>
> - La unidad de DVD está conectada y no se proporciona el archivo ISO.
> - El archivo ISO no incluye el archivo de datos de usuario.
> - El nombre o el formato del archivo de datos de usuario no es correcto.

Para configurar NIC virtuales en la instancia Citrix ADC VPX, siga estos pasos:

1. Seleccione el dispositivo virtual que ha importado y, a continuación, en el menú **Acción**, seleccione **Configuración**.
2. En el ****<virtual appliance name> cuadro de diálogo Configuración para, haga clic en ****Agregar hardware** en el panel izquierdo.
3. En el panel derecho, en la lista de dispositivos, seleccione **Adaptador de red**.
4. Haga clic en **Agregar**.
5. Compruebe que el **adaptador de red (no conectado)** aparece en el panel izquierdo.
6. Seleccione el adaptador de red en el panel izquierdo.
7. En el panel derecho, en el menú **Red**, seleccione la red virtual a la que conectar el adaptador.
8. Para seleccionar la red virtual para otros adaptadores de red que quiere utilizar, repita los pasos **6** y **7**.
9. Haga clic en **Aplicar** y, a continuación, haga clic en **Aceptar**.

Para configurar la instancia de Citrix ADC VPX:

1. Haga clic con el botón secundario en el dispositivo virtual que instaló anteriormente y, a continuación, seleccione **Iniciar**.
2. Acceda a la consola haciendo doble clic en el dispositivo virtual.
3. Escriba la dirección IP de Citrix ADC, la máscara de subred y la Gateway para su dispositivo virtual.

Ha completado la configuración básica de su dispositivo virtual. Escriba la dirección IP en un explorador web para acceder al dispositivo virtual.

> **Nota**
>
> También puede utilizar la plantilla de máquina virtual (VM) para aprovisionar la instancia de Citrix ADC VPX mediante SCVMM.
>
> Si utiliza la solución de agrupación de NIC Microsoft Hyper-V con instancias NetScaler VPX, consulte el artículo CTX224494 para obtener más información.

Instalar una instancia de Citrix ADC VPX en la plataforma Linux-KVM

August 20, 2021

Para configurar un Citrix ADC VPX para la plataforma Linux-KVM, puede utilizar la aplicación gráfica Virtual Machine Manager (Virtual Manager). Si prefiere la línea de comandos Linux-KVM, puede utilizar el `virsh` programa.

El sistema operativo Linux host debe instalarse en el hardware adecuado mediante herramientas de virtualización como el módulo KVM y QEMU. El número de máquinas virtuales (VM) que se pueden implementar en el Hypervisor depende del requisito de la aplicación y del hardware elegido.

Después de aprovisionar una instancia Citrix ADC VPX, puede agregar más interfaces.

Limitaciones y directrices de uso

Recomendaciones generales

Para evitar comportamientos impredecibles, aplique las siguientes recomendaciones:

- No cambie la MTU de la interfaz de VNet asociada a la VM VPX. Apague la VM VPX antes de modificar los parámetros de configuración, como los modos de interfaz o la CPU.
- No fuerce el apagado de la VM VPX. Es decir, no use el comando **Force off**.
- Cualquier configuración realizada en el host Linux puede o no ser persistente, en función de la configuración de distribución de Linux. Puede optar por hacer que estas configuraciones sean persistentes para garantizar un comportamiento coherente en todos los reinicios del sistema operativo Linux host.
- El paquete Citrix ADC debe ser único para cada instancia de Citrix ADC VPX aprovisionada.

Limitaciones

- No se admite la migración en vivo de una instancia VPX que se ejecuta en KVM.

Requisitos previos para instalar una instancia de Citrix ADC VPX en la plataforma Linux-KVM

August 20, 2021

Compruebe los requisitos mínimos del sistema para un servidor Linux-KVM que se ejecuta en una instancia Citrix ADC VPX.

Requisito de CPU:

- Procesadores x86 de 64 bits con la función de virtualización de hardware incluida en los procesadores Intel VT-X.

Para comprobar si la CPU es compatible con el host Linux, introduzca el siguiente comando en el símbolo del shell de Linux del host:

```
\*.egrep '^flags.\*(vmx|svm)' /proc/cpuinfo*
<!--NeedCopy-->
```

Si la configuración del **BIOS** de la extensión anterior está inhabilitada, debe habilitarla en el BIOS.

- Proporcione al menos 2 núcleos de CPU al host Linux.
- No hay ninguna recomendación específica para la velocidad del procesador, pero mayor es la velocidad, mejor será el rendimiento de la aplicación de VM.

Requisito de memoria (RAM):

Mínimo 4 GB para el kernel Linux host. Agregue más memoria según lo requieran las máquinas virtuales.

Requisito de disco duro:

Calcule el espacio para los requisitos del kernel y VM de host Linux. Una sola máquina virtual Citrix ADC VPX requiere 20 GB de espacio en disco.

Requisitos de software

El núcleo host utilizado debe ser un núcleo Linux de 64 bits, versión 2.6.20 o posterior, con todas las herramientas de virtualización. Citrix recomienda los núcleos más nuevos, como 3.6.11-4 y versiones posteriores.

Muchas distribuciones de Linux, como Red Hat, CentOS y Fedora, han probado versiones del núcleo y herramientas de virtualización asociadas.

Requisitos de hardware de VM invitada

Citrix ADC VPX admite el tipo de disco duro IDE y Virtio. El tipo de disco duro se ha configurado en el archivo XML, que forma parte del paquete Citrix ADC.

Requisitos de red

Citrix ADC VPX admite interfaces de red Virtio para-virtualizadas, SR-IOV y PCI Passthrough.

Para obtener más información acerca de las interfaces de red compatibles, consulte:

- Aprovisione la instancia de Citrix ADC VPX mediante Virtual Machine Manager
- Configurar una instancia de Citrix ADC VPX para utilizar interfaces de red SR-IOV
- Configurar una instancia de Citrix ADC VPX para utilizar interfaces de red de transferencia PCI

Interfaz y modos de origen

El tipo de dispositivo de origen puede ser Bridge o MacVtap. En MacVTap, son posibles cuatro modos: VEPA, Bridge, Privado y Pass-through. Compruebe los tipos de interfaces que puede utilizar y los tipos de tráfico admitidos, según lo siguiente:

Puente:

- Puente Linux.
- `Ebtables` y la `iptables` configuración del host Linux puede filtrar el tráfico en el puente si no elige la configuración correcta o inhabilita `IPtable` los servicios.

MacVtap (modo VEPA):

- Mejor rendimiento que un puente.
- Las interfaces del mismo dispositivo inferior se pueden compartir entre las VM.
- Comunicación entre VM mediante el mismo
- dispositivo inferior solo es posible si el conmutador ascendente o descendente admite el modo VEPA.

MacVTap (modo privado):

- Mejor rendimiento que un puente.
- Las interfaces del mismo dispositivo inferior se pueden compartir entre las VM.
- No es posible la comunicación entre VM mediante el mismo dispositivo inferior.

MacVTap (modo puente):

- Mejor en comparación con bridge.
- Las interfaces del mismo dispositivo inferior se pueden compartir entre las máquinas virtuales.
- Es posible la comunicación entre VM mediante el mismo dispositivo inferior, si el enlace inferior del dispositivo es UP.

MacVTap (modo de paso):

- Mejor en comparación con bridge.
- Las interfaces del mismo dispositivo inferior no se pueden compartir entre las máquinas virtuales.
- Solo una VM puede usar el dispositivo inferior.

> Nota: Para obtener el mejor rendimiento de la instancia VPX, asegúrese de que las `lro` capacidades `gro` y estén desactivadas en las interfaces de origen.

Propiedades de las interfaces de origen

Asegúrese de desactivar las capacidades genérico-recepve-offload (`gro`) y large-receive-offload (`lro`) de las interfaces de origen. Para desactivar las `lro` capacidades `gro` y, ejecute los siguientes comandos en el símbolo del shell de Linux del host.

```
ethtool -K eth6 gro off
ethool -K eth6 lro off
```

Ejemplo:

```
    [root@localhost ~]# ethtool -K eth6

                    Offload parameters for eth6:

                                        rx-checksumming: on

                                        tx-checksumming: on

                    scatter-gather: on

                    tcp-segmentation-offload: on

                    udp-fragmentation-offload: off

                    generic-segmentation-offload: on

                    generic-receive-offload: off

                    large-receive-offload: off

                    rx-vlan-offload: on

                    tx-vlan-offload: on

                    ntuple-filters: off

                    receive-hashing: on

    [root@localhost ~]#
<!--NeedCopy-->
```

Ejemplo:

Si el puente Linux host se utiliza como dispositivo de origen, como en el ejemplo siguiente, y `lro`

las capacidades deben desactivarse en las interfaces de VNet, que son las interfaces virtuales que conectan el host a las máquinas virtuales invitadas.

```
    [root@localhost ~]# brctl show eth6_br

    bridge name     bridge  id               STP enabled interfaces

    eth6_br         8000.00e0ed1861ae          no         eth6

                                                          vnet0

                                                          vnet2

    [root@localhost ~]#
<!--NeedCopy-->
```

En el ejemplo anterior, las dos interfaces virtuales se derivan de eth6_br y se representan como vnet0 y vnet2. Ejecute los siguientes comandos para desactivar `gro` y activar `lro` las capacidades en estas interfaces.

```
    ethtool -K vnet0 gro off
            ethtool -K vnet2 gro off
            ethtool -K vnet0 lro off
                    ethtool -K vnet2 lro off
<!--NeedCopy-->
```

Modo promiscuo

El modo promiscuo debe estar habilitado para que funcionen las siguientes funciones:

- Modo L2
- Procesamiento de tráfico de multidifusión
- Emisión
- Tráfico IPv6
- MAC virtual
- Redirección dinámica

Utilice el siguiente comando para habilitar el modo promiscuo.

```
[root@localhost ~]# ifconfig eth6 promisc
```



```
[root@localhost ~]# ifconfig eth6
eth6       Link encap:Ethernet  HWaddr 78:2b:cb:51:54:a3
           inet6 addr: fe80::7a2b:cbff:fe51:54a3/64 Scope:Link
           UP BROADCAST RUNNING PROMISC MULTICAST  MTU:9000  Metric:1
           RX packets:142961 errors:0 dropped:0 overruns:0 frame:0
           TX packets:2895843 errors:0 dropped:0 overruns:0 carrier:0
           collisions:0 txqueuelen:1000
           RX bytes:14330008 (14.3 MB)  TX bytes:1019416071 (1.0 GB)

[root@localhost ~]#
<!--NeedCopy-->
```

Módulo requerido

Para un mejor rendimiento de red, asegúrese de que el módulo vhost_net esté presente en el host Linux. Para comprobar la existencia del módulo vhost_net, ejecute el siguiente comando en el host Linux:

```
lsmod | grep "vhost_net"
<!--NeedCopy-->
```

Si vhost_net aún no se está ejecutando, introduzca el siguiente comando para ejecutarlo:

```
modprobe vhost_net
<!--NeedCopy-->
```

Aprovisione la instancia Citrix ADC VPX mediante OpenStack

August 20, 2021

Puede aprovisionar una instancia Citrix ADC VPX en un entorno OpenStack mediante el comando de **arranque Nova** (CLI de OpenStack) u Horizon (panel de OpenStack).

Aprovisionar una instancia VPX, opcionalmente implica el uso de datos de la unidad de configuración. La unidad de configuración es una unidad de configuración especial que se conecta a la instancia como un dispositivo de CD-ROM cuando se inicia. Esta unidad de configuración se puede utilizar para pasar la configuración de red, como la dirección IP de administración, la máscara de red, la Gateway predeterminada y para inyectar scripts de clientes.

En un dispositivo Citrix ADC, el mecanismo de autenticación predeterminado se basa en contraseña. Ahora, el mecanismo de autenticación de pares de claves SSH es compatible con instancias Citrix ADC VPX en el entorno OpenStack.

El par de claves (clave pública y clave privada) se genera antes de utilizar el mecanismo de criptografía de clave pública. Puede utilizar distintos mecanismos, como Horizon, Puttygen.exe para Windows y `ssh-keygen` para el entorno Linux, para generar el par de claves. Consulte la documentación en línea de los respectivos mecanismos para obtener más información sobre la generación de pares de claves.

Una vez disponible un par de claves, copie la clave privada en una ubicación segura a la que tienen acceso las personas autorizadas. En OpenStack, la clave pública se puede implementar en una instancia VPX mediante el comando de arranque Horizon o Nova. Cuando se aprovisiona una instancia VPX mediante OpenStack, primero detecta que la instancia se está iniciando en un entorno OpenStack leyendo una cadena de BIOS específica. Esta cadena es “OpenStack Foundation” y para las distribuciones de Red Hat Linux se almacena en /etc/nova/release. Se trata de un mecanismo estándar que está disponible en todas las implementaciones de OpenStack basadas en la plataforma de hipervisor KVM. La unidad debe tener una etiqueta OpenStack específica.

Si se detecta la unidad de configuración, la instancia intenta leer la configuración de red, los scripts personalizados y el par de claves SSH si se proporciona.

Archivo de datos de usuario

La instancia Citrix ADC VPX utiliza un archivo OVF personalizado, también conocido como archivo de datos de usuario, para inyectar la configuración de red, scripts personalizados. Este archivo se proporciona como parte de la unidad de configuración. A continuación se muestra un ejemplo de un archivo OVF personalizado.

```
```
<?xml version=”1.0” encoding=”UTF-8” standalone=”no”?>
<Environment xmlns:oe=”http://schemas.dmtf.org/ovf/environment/1”
xmlns:xsi=”http://www.w3.org/2001/XMLSchema-instance”
oe:id=””
xmlns=”http://schemas.dmtf.org/ovf/environment/1”
xmlns:cs=”http://schemas.citrix.com/openstack”>
<PlatformSection>
<Kind></Kind>
<Version>2016.1</Version>
<Vendor>VPX</Vendor>
<Locale>en</Locale>
</PlatformSection>
<PropertySection>
```

 
```

```
<Property oe:key="com.citrix.netscaler.ovf.version" oe:value="1.0"/>
<Property oe:key="com.citrix.netscaler.platform" oe:value="NSVPX"/>
<Property oe:key="com.citrix.netscaler.orch_env" oe:value="openstack-
   orch-env"/>
<Property oe:key="com.citrix.netscaler.mgmt.ip" oe:value="10.1.2.22"/>
<Property oe:key="com.citrix.netscaler.mgmt.netmask" oe:value="
   255.255.255.0"/>
<Property oe:key="com.citrix.netscaler.mgmt.gateway" oe:value="10.1.2.1
   "/>
</PropertySection>
 <cs:ScriptSection>
   <cs:Version>1.0</cs:Version>
     <ScriptSettingSection xmlns="http://schemas.citrix.com/openstack"
        xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
         <Scripts>
           <Script>
                 <Type>shell</Type>
                 <Parameter>X Y</Parameter>
                <Parameter>Z</Parameter>
                <BootScript>before</BootScript>
                  <Text>
                        #!/bin/bash
                        echo "Hi, how are you" $1 $2 >> /var/sample.txt
                  </Text>
           </Script>
           <Script>
                 <Type>python</Type>
                 <BootScript>after</BootScript>
                  <Text>
                       #!/bin/python
print("Hello");
                  </Text>
           </Script>
   <Script>
                <Type>perl</Type>
                <BootScript>before</BootScript>
                 <Text>
                      !/usr/bin/perl
my $name = "VPX";
print "Hello, World $name !\n" ;
                  </Text>
           </Script>
           <Script>
                <Type>nscli</Type>
                <BootScript>after</BootScript>
```



```
56                 <Text>
57                  add vlan 33
58  bind vlan 33 -ifnum 1/2
59                 </Text>
60              </Script>
61           </Scripts>
62       </ScriptSettingSection>
63   </cs:ScriptSection>
64 </Environment>
65 <!--NeedCopy--> ```
```

En el archivo OVF anterior a ”PropertySection” se utiliza para la configuración de redes de NetScaler, mientras que <cs:ScriptSection> se utiliza para adjunto todos los scripts. <Scripts></Scripts> las etiquetas se utilizan para agrupar todos los scripts juntos. Cada script se define entre etiquetas <Script> </Script>. Cada etiqueta de script tiene los siguientes campos/etiquetas:

a) <Type>: Especifica el valor para el tipo de script. Valores posibles: Shell/Perl/Python/NSLCI (para scripts de NetScaler CLI)

b) <Parameter>: Proporciona parámetros al script. Cada script puede tener varias etiquetas <Parameter>.

c) <BootScript>: Especifica el punto de ejecución del script. Valores posibles para esta etiqueta: antes/después. “before” especifica que el script se ejecuta antes de que aparezca PE. “after” especifica que el script se ejecutará después de que aparezca PE.

d) <Text>: Pega el contenido de un script.

> **Nota**
>
> Actualmente, la instancia VPX no se ocupa de la desinfección de scripts. Como administrador, debe comprobar la validez del script.
>
> No todas las secciones necesitan estar presentes. Utilice una “PropertySection” vacía para definir únicamente los scripts que se ejecutarán en el primer arranque o en vacío para definir únicamente la configuración de red.
>
> Una vez completadas las secciones requeridas del archivo OVF (archivo de datos de usuario), utilícelo para aprovisionar la instancia VPX.

Configuración de red

Como parte de la configuración de red, la instancia VPX dice lo siguiente:

- Dirección IP de administración
- Máscara de red

- Puerta de enlace predeterminada

Después de leer correctamente los parámetros, se rellenan en la configuración de NetScaler para permitir la administración remota de la instancia. Si los parámetros no se leen correctamente o la unidad de configuración no está disponible, la instancia pasa al comportamiento predeterminado, que es:

- La instancia intenta recuperar la información de la dirección IP de DHCP.
- Si DHCP falla o se agota el tiempo, la instancia presenta la configuración de red predeterminada (192.168.100.1/16).

Script del cliente

La instancia VPX permite ejecutar un script personalizado durante el aprovisionamiento inicial. El dispositivo admite comandos de tipo Shell, Perl, Python y Citrix ADC CLI comandos.

Autenticación de par de claves SSH

La instancia VPX copia la clave pública, disponible dentro de la unidad de configuración como parte de metadatos de instancia, en su archivo “authorized_keys”. Esto permite al usuario acceder a la instancia con clave privada.

> **Nota**
>
> Cuando se proporciona una clave SSH, las credenciales predeterminadas (nsroot/nsroot) ya no funcionan, si se necesita acceso basado en contraseña, inicie sesión con la clave privada SSH correspondiente y establezca manualmente una contraseña.

Antes de comenzar

Antes de aprovisionar una instancia VPX en el entorno OpenStack, extraiga el `.qcow2` archivo del archivo.tgz y compilar

Imagen de OpenStack de la imagen qcow2. Siga estos pasos:

1. Extraiga el `.qcow2` archivo del `.tqz` archivo escribiendo el siguiente comando

```
tar xvzf <TAR file>
tar xvzf <NSVPX-KVM-12.0-26.2_nc.tgz>
NSVPX-KVM.xml
NSVPX-KVM-12.0-26.2_nc.qcow2
```

2. Cree una imagen de OpenStack mediante el `.qcoz2` archivo extraído en el paso 1 escribiendo el siguiente comando.


```
openstack image create --container-format bare --property
    hw_disk_bus=ide --disk-format qcow2 --file <path to qcow2 file>
     --public <name of the OpenStack image>

glance image-create --name=”NS-VPX-12-0-26-2” --property
    hw_disk_bus=ide --ispublic=
true --container-format=bare --disk-format=qcow2< NSVPX-KVM
    -12.0-26.2_nc.qcow2
```

Ilustración 1: La siguiente ilustración proporciona un ejemplo de salida para el comando glance image-create.

```
+------------------+--------------------------------------------------------+
| Field            | Value                                                  |
+------------------+--------------------------------------------------------+
| checksum         | 154ade3fc7dca7d1706b1d03d7d97552                       |
| container_format | bare                                                   |
| created_at       | 2017-03-13T08:52:31Z                                   |
| disk_format      | qcow2                                                  |
| file             | /v2/images/322c1e0f-cce8-4b7b-b53e-bd8152c388ed/file   |
| id               | 322c1e0f-cce8-4b7b-b53e-bd8152c388ed                   |
| min_disk         | 0                                                      |
| min_ram          | 0                                                      |
| name             | VPX-KVM-12.0-26.2
| owner            | 58d17d81df5d4406afbb4fdab3a58d79                       |
| properties       | hw_disk_bus='ide'                                      |
| protected        | False                                                  |
| schema           | /v2/schemas/image                                      |
| size             | 784338944                                              |
| status           | active                                                 |
| updated_at       | 2017-03-13T08:52:43Z                                   |
| virtual_size     | None                                                   |
| visibility       | public                                                 |
+------------------+--------------------------------------------------------+
```

Aprovisionamiento de la instancia VPX

Puede aprovisionar una instancia VPX de dos maneras mediante una de las opciones:

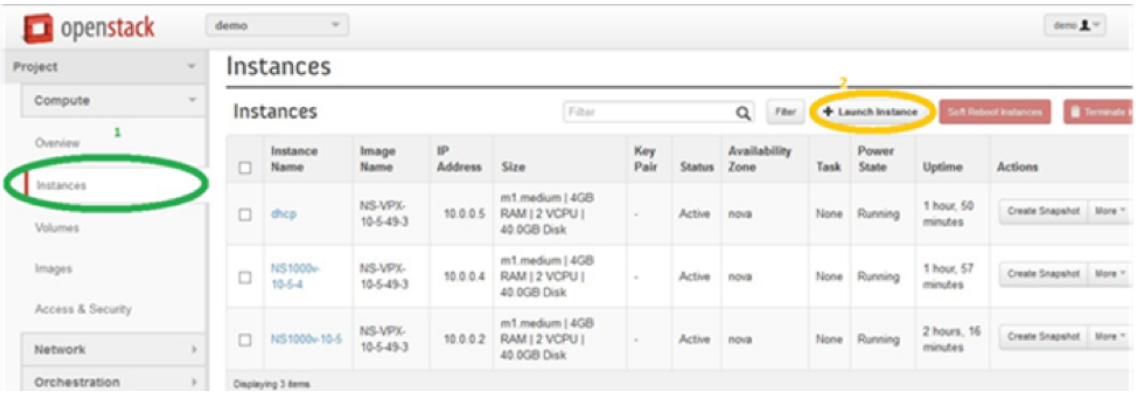
- Horizon (panel de control de OpenStack)
- Comando de arranque Nova (CLI de OpenStack)

Aprovisione una instancia VPX mediante el panel de control de OpenStack

Siga estos pasos para aprovisionar la instancia VPX mediante Horizon:

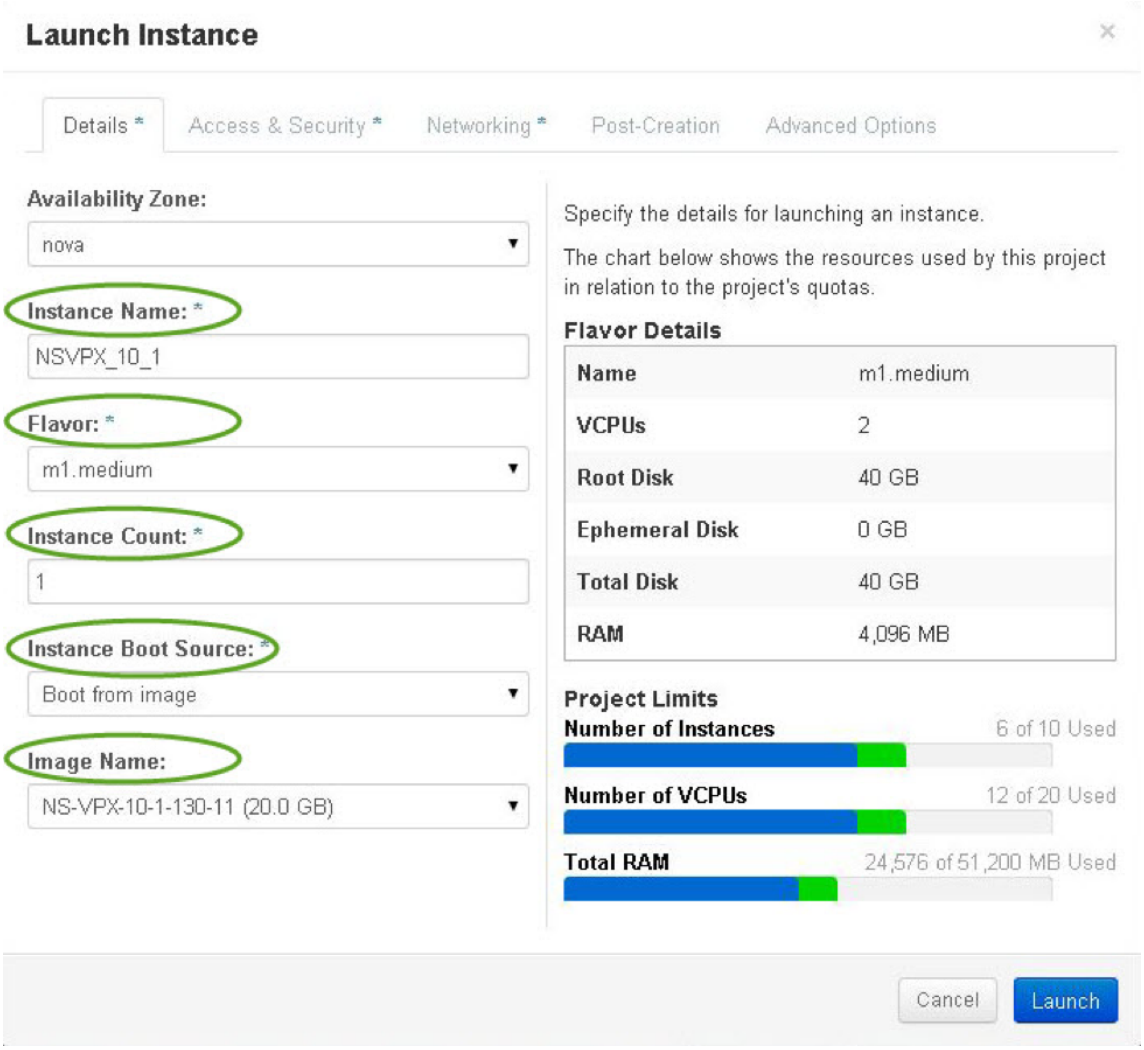
1. Inicie sesión en el panel de control de OpenStack.
2. En el panel Proyecto, situado a la izquierda del tablero de mandos, seleccione **Instancias**.

3. En el panel Instancias, haga clic en **Iniciar instancia** para abrir el Asistente de inicio de instancias.



4. En el asistente Iniciar instancia, rellene los detalles, como:

   a) Nombre de la instancia
   b) Sabor de instancia
   c) Recuento de instancias
   d) Origen de inicio de instancia
   e) Nombre de la imagen



5. Implemente un nuevo par de claves o un par de claves existente a través de Horizon siguiendo los pasos siguientes:

   a) Si no tiene un par de claves existente, cree la clave mediante cualquier mecanismo existente. Si ya tiene una clave, omita este paso.

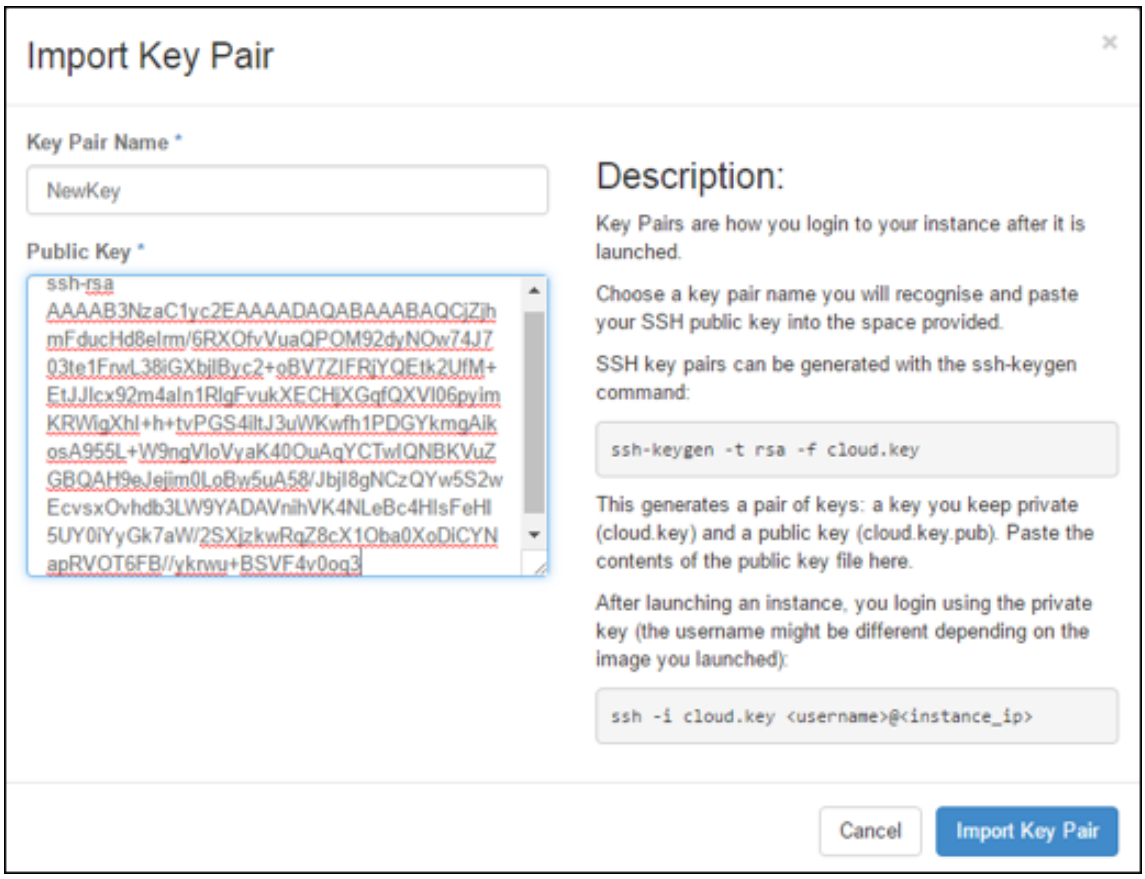
   b) Copiar el contenido de la clave pública.

   c) Vaya a **Horizon > Instancias > Crear nuevas instancias**.

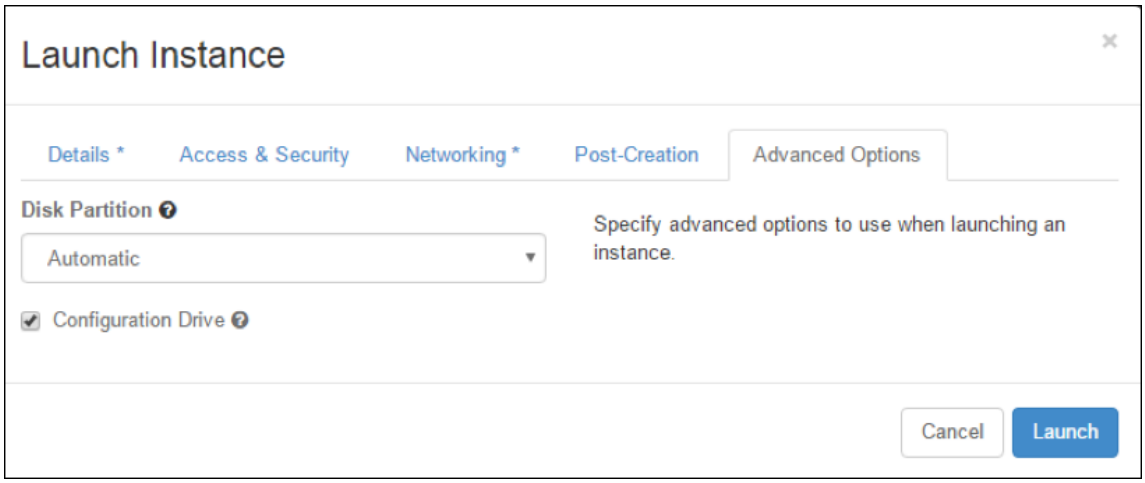
   d) Haga clic en **Acceso y seguridad**.

   e) Haga clic en el signo + situado junto al menú desplegable **Par de claves** y proporcione los valores de los parámetros mostrados.

   f) Pegar contenido de clave *pública en el cuadro Clave pública*, dar un nombre a la clave y hacer clic en **Importar par de claves**.



6. Haga clic en la ficha **Creación** de publicaciones del asistente. En Script de personalización, agregue el contenido del archivo de datos de usuario. El archivo de datos de usuario contiene la dirección IP, los detalles de la máscara de red y la puerta de enlace y los scripts de cliente de la instancia VPX.
7. Después de seleccionar o importar un par de claves, marque la opción config-drive y haga clic en **Iniciar**.



Aprovisione la instancia VPX mediante OpenStack CLI

Siga estos pasos para aprovisionar una instancia VPX mediante OpenStack CLI.

1. Para crear una imagen desde qcow2, escriba el siguiente comando:

   ```
   openstack image create --container-format bare --property hw_disk_bus=
   ide --diskformat qcow2 --file NSVPX-OpenStack.qcow2 --public VPX-ToT-
   Image
   ```

2. Para seleccionar una imagen para crear una instancia, escriba el siguiente comando:

   ```
   openstack image list | more
   ```

3. Para crear una instancia de un sabor determinado, escriba el siguiente comando para elegir un ID de sabor de una lista:

   ```
   openstack flavor list
   ```

4. Para conectar una NIC a una red determinada, escriba el siguiente comando para elegir un ID de red de una lista de redes:

   ```
   openstack network list
   ```

5. Para crear una instancia, escriba el siguiente comando:

```
1 openstack server create --flavor FLAVOR_ID --image IMAGE_ID --key-
     name KEY_NAME
2 --user-data USER_DATA_FILE_PATH --config-drive True --nic net-id=
     net-uuid
3 INSTANCE_NAME
4 openstack server create --image VPX-ToT-Image --flavor m1.medium
     --user-data
5 ovf.xml --config-drive True --nic net-id=2734911b-ee2b-48d0-a1b6-3
     efd44b761b9
6 VPX-ToT
```

Ilustración 2: La siguiente ilustración proporciona un resultado de ejemplo.


```
+--------------------------------------+--------------------------------------------------------------------------+
| Field                                | Value                                                                    |
+--------------------------------------+--------------------------------------------------------------------------+
| OS-DCF:diskConfig                    | MANUAL                                                                   |
| OS-EXT-AZ:availability_zone          |                                                                          |
| OS-EXT-SRV-ATTR:host                 | None                                                                     |
| OS-EXT-SRV-ATTR:hypervisor_hostname  | None                                                                     |
| OS-EXT-SRV-ATTR:instance_name        | instance-000001c2                                                        |
| OS-EXT-STS:power_state               | 0                                                                        |
| OS-EXT-STS:task_state                | scheduling                                                               |
| OS-EXT-STS:vm_state                  | building                                                                 |
| OS-SRV-USG:launched_at               | None                                                                     |
| OS-SRV-USG:terminated_at             | None                                                                     |
| accessIPv4                           |                                                                          |
| accessIPv6                           |                                                                          |
| addresses                            |                                                                          |
| adminPass                            | pFVvMtq7N8Z6                                                             |
| config_drive                         | True                                                                     |
| created                              | 2017-03-13T10:32:59Z                                                     |
| flavor                               | m1.medium (3)                                                            |
| hostId                               |                                                                          |
| id                                   | a1fe991e-3604-43a0-9dd6-59fa0f3749df                                     |
| image                                | VPX-ToT-Image (f0c2f9d1-08f2-4b2e-9943-2ee6bc2edbc7)                     |
| key_name                             | None                                                                     |
| name                                 |VPX-ToT                                                                   |
| os-extended-volumes:volumes_attached | []                                                                       |
| progress                             | 0                                                                        |
| project_id                           | 58d17d81df5d4406afbb4fdab3a58d79                                         |
| properties                           |                                                                          |
| security_groups                      | [{u'name': u'default'}]                                                  |
| status                               | BUILD                                                                    |
| updated                              | 2017-03-13T10:33:00Z                                                     |
| user_id                              | a6347b33916b4eb1b1f76360a9c8f935                                         |
+--------------------------------------+--------------------------------------------------------------------------+
```

Aprovisione la instancia de Citrix ADC VPX mediante Virtual Machine Manager

August 20, 2021

Virtual Machine Manager es una herramienta de escritorio para administrar invitados de VM. Le permite crear nuevos invitados de VM y varios tipos de almacenamiento, y administrar redes virtuales. Puede acceder a la consola gráfica de invitados de VM con el visor VNC integrado y ver estadísticas de rendimiento, ya sea local o remotamente.

Después de instalar la distribución Linux preferida, con la virtualización KVM habilitada, puede continuar con el Provisioning de máquinas virtuales.

Mientras utiliza Virtual Machine Manager para aprovisionar una instancia de Citrix ADC VPX, tiene dos opciones:

- Introduzca manualmente la dirección IP, la Gateway y la máscara de red
- Asignar automáticamente la dirección IP, la Gateway y la máscara de red (autoaprovisionamiento)

Puede utilizar dos tipos de imágenes para aprovisionar una instancia de Citrix ADC VPX:

- RAW
- QCOW2

Puede convertir una imagen RAW de Citrix ADC VPX en una imagen QCOW2 y aprovisionar la instancia de Citrix ADC VPX. Para convertir la imagen RAW en una imagen QCOW2, escriba el siguiente comando:

```
qemu-img convert -O qcow2 original-image.raw image-converted.qcow
```

Por ejemplo:

```
qemu-img convert -O qcow2 NSVPX-KVM-11.1-12.5_nc.raw NSVPX-KVM-11.1-12.5_nc
.qcow
```

Una implementación típica de Citrix ADC VPX en KVM incluye los siguientes pasos:

- Comprobación de los requisitos previos para el aprovisionamiento automático de una instancia Citrix ADC VPX
- Aprovisionamiento de la instancia Citrix ADC VPX mediante una imagen RAW
- Aprovisionamiento de la instancia Citrix ADC VPX mediante una imagen QCOW2
- Adición de interfaces adicionales a una instancia VPX mediante Virtual Machine Manager

Comprobar los requisitos previos para el aprovisionamiento automático de una instancia de Citrix ADC VPX

El aprovisionamiento automático es una función opcional, e implica el uso de datos de la unidad CDROM. Si esta función está habilitada, no es necesario introducir la dirección IP de administración, la máscara de red y la Gateway predeterminada de la instancia de Citrix ADC VPX durante la configuración inicial.

Debe completar las siguientes tareas antes de poder aprovisionar automáticamente una instancia VPX:

1. Cree un archivo XML de formato abierto de virtualización (OVF) personalizado o un archivo de datos de usuario.
2. Convierta el archivo OVF en una imagen ISO mediante una aplicación en línea (por ejemplo, PowerISO).
3. Monte la imagen ISO en el host KVM mediante cualquier herramienta basada en copia segura (SCP).

Archivo XML OVF de ejemplo:

Aquí hay un ejemplo del contenido de un archivo XML OVF, que puede usar como muestra para crear el archivo.

```
1 <?xml version=”1.0” encoding=”UTF-8” standalone=”no”?>
2
3 <Environment xmlns:oe=”`http://schemas.dmtf.org/ovf/environment/1”`
4
```



```
xmlns:xsi="`http://www.w3.org/2001/XMLSchema-instance"`

oe:id=""

xmlns="`http://schemas.dmtf.org/ovf/environment/1"`

xmlns:cs="`http://schemas.citrix.com/openstack">`

<PlatformSection>

<Kind></Kind>

<Version>2016.1</Version>

<Vendor>VPX</Vendor>

<Locale>en</Locale>

</PlatformSection>

<PropertySection>

<Property oe:key="com.citrix.netscaler.ovf.version" oe:value="1.0"/>

<Property oe:key="com.citrix.netscaler.platform" oe:value="NSVPX"/>

<Property oe:key="com.citrix.netscaler.orch_env" oe:value="KVM"/>

<Property oe:key="com.citrix.netscaler.mgmt.ip" oe:value="10.1.2.22"/>

<Property oe:key="com.citrix.netscaler.mgmt.netmask" oe:value="
   255.255.255.0"/>

<Property oe:key="com.citrix.netscaler.mgmt.gateway" oe:value="10.1.2.1
   "/>

</PropertySection>

</Environment>
<!--NeedCopy-->
```

En el archivo XML de OVF anterior, se utiliza “PropertySection” para la configuración de redes de NetScaler. Al crear el archivo, especifique valores para los parámetros que se resaltan al final del ejemplo:

- Dirección IP de administración
- Máscara de red
- Gateway

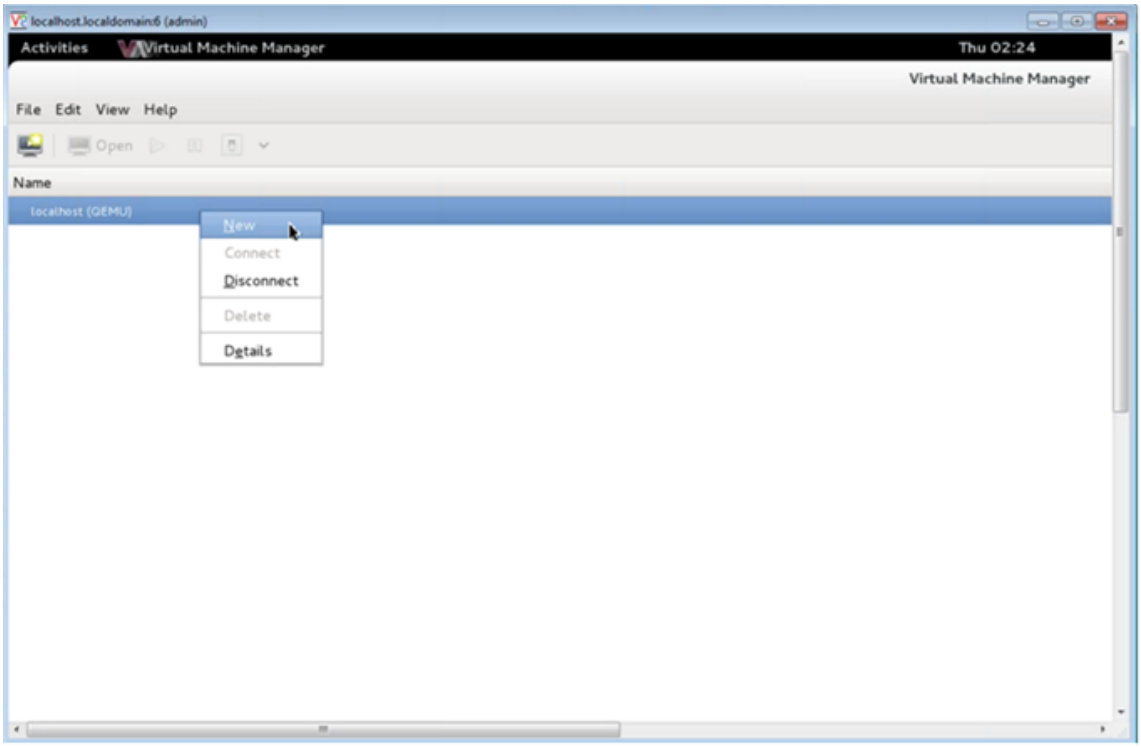
> **Importante**
>
> Si el archivo OVF no tiene el formato XML correcto, se asigna a la instancia VPX la configuración de red predeterminada, no a los valores especificados en el archivo.

Aprovisione la instancia de Citrix ADC VPX mediante una imagen RAW

Virtual Machine Manager permite aprovisionar una instancia de Citrix ADC VPX mediante una imagen RAW.

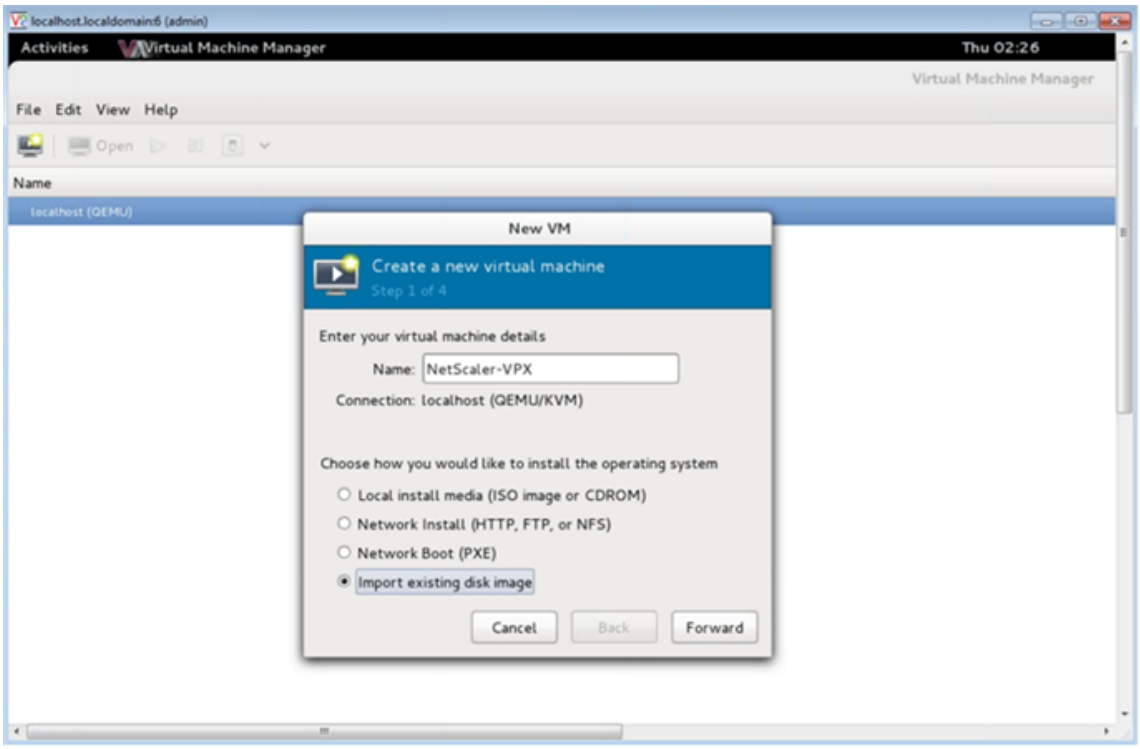
Para aprovisionar una instancia de Citrix ADC VPX mediante Virtual Machine Manager, siga estos pasos:

1. Abra Virtual Machine Manager (**Aplicación** > **Herramientas del sistema** > **Virtual Machine Manager**) e introduzca las credenciales de inicio de sesión en la ventana **Autenticar**.
2. Haga clic en el icono de  o haga clic con el botón derecho en **localhost (QEMU)** para crear una nueva instancia Citrix ADC VPX.

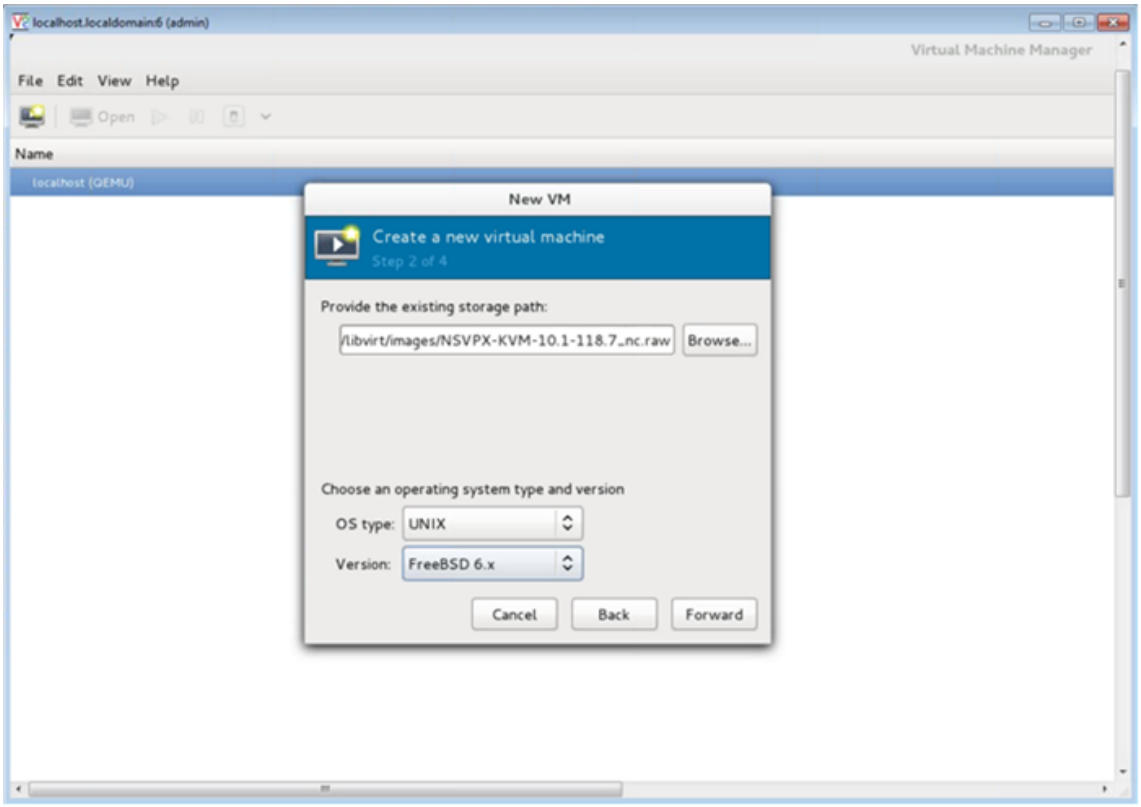


3. En el cuadro de texto **Nombre**, escriba un nombre para la nueva VM (por ejemplo, NetScaler-VPX).

4. En la ventana **Nueva máquina virtual**, en “Elija cómo quiere instalar el sistema operativo”, seleccione **Importar imagen de disco existente** y, a continuación, haga clic en **Reenviar**.

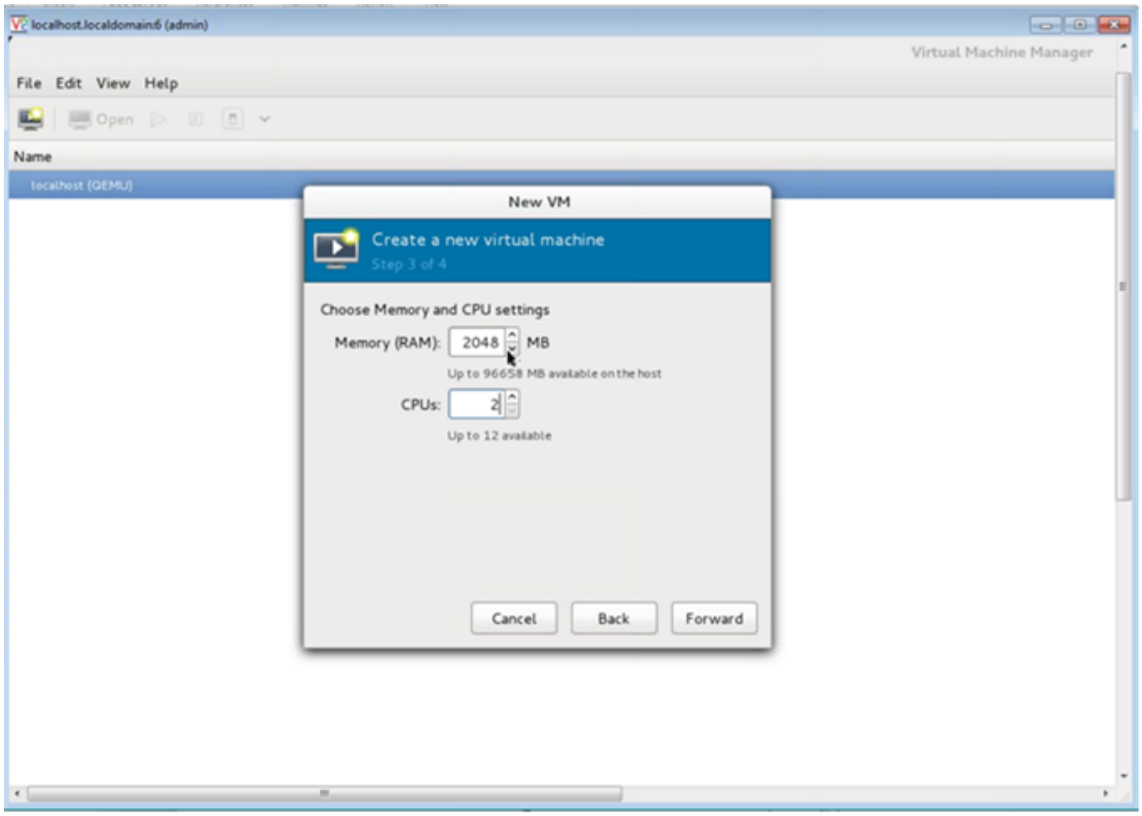


5. En el campo **Proporcionar la ruta de almacenamiento existente**, navegue por la ruta de acceso a la imagen. Elija el tipo de SO como UNIX y Versión como FreeBSD 6.x. A continuación, haga clic en **Reenviar**.

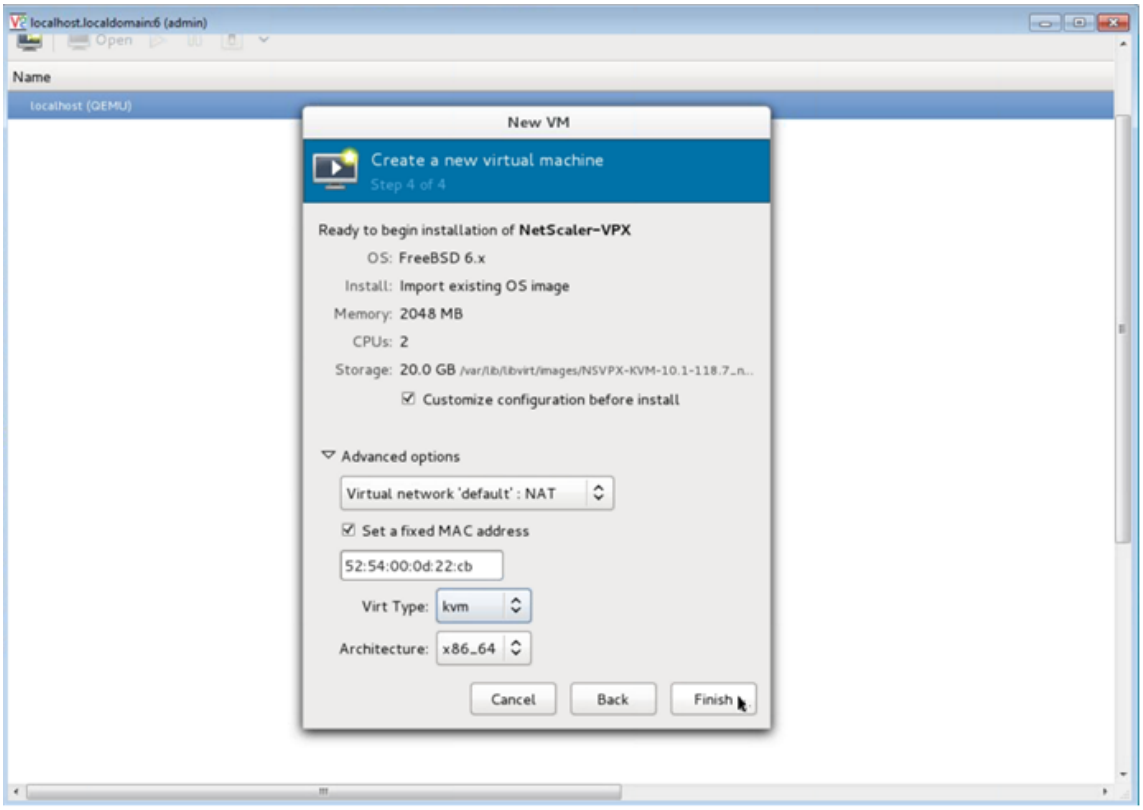


6. En **Elegir configuración de memoria y CPU**, seleccione la configuración siguiente y, a continuación, haga clic en **Reenviar** :

   - Memoria (RAM): 2048 MB
   - CPU— 2

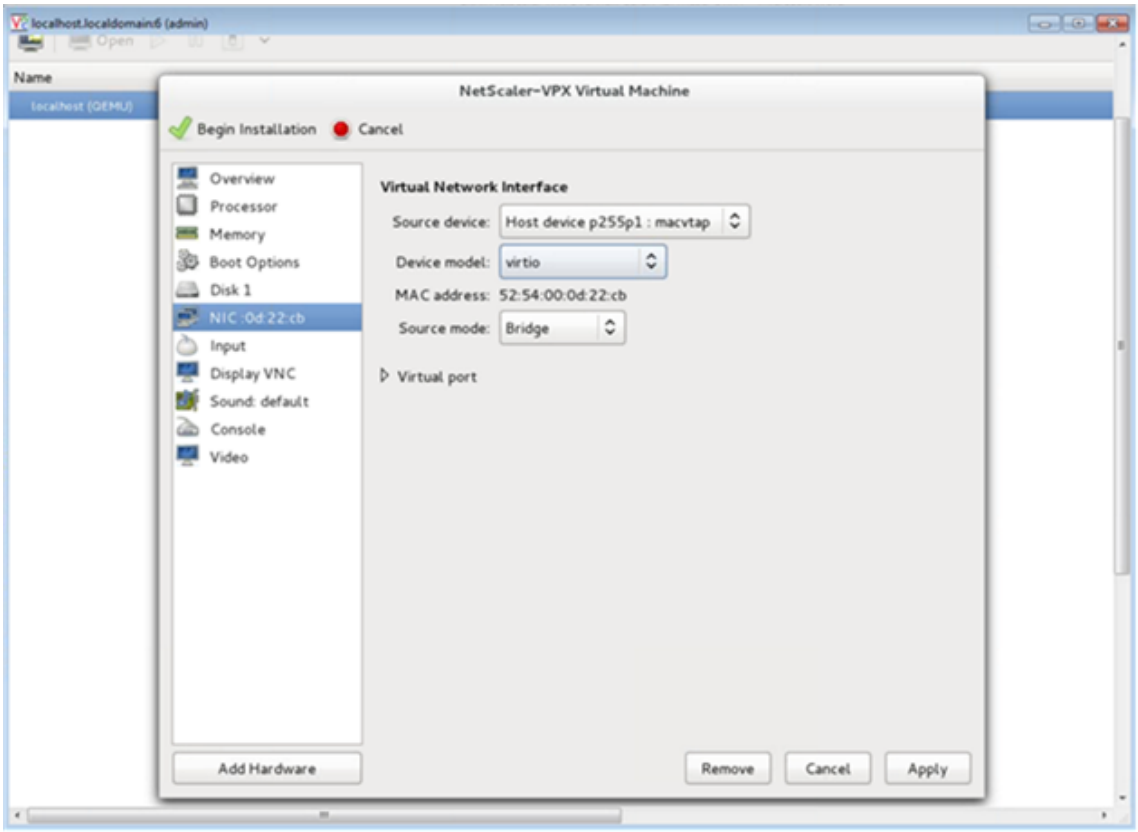


7. Active la casilla de verificación **Personalizar configuración antes de instalar**. Opcionalmente, en **Opciones avanzadas** puede personalizar la dirección MAC. Asegúrese de que el **tipo de Virt** seleccionado sea KVM y la arquitectura seleccionada es x86_64. Haga clic en **Finalizar**.



8. Seleccione una NIC y proporcione la siguiente configuración:

   - Dispositivo de origen `ethX macvtap` o Bridge
   - Modelo de dispositivo: `virtio`
   - Modo de origen: Puente



9. Haga clic en **Aplicar**.
10. Si quiere aprovisionar automáticamente la instancia VPX, consulte la sección **Habilitación de Auto-Provisioning mediante Adjuntar una unidad de CDROM** en este documento. De lo contrario, haga clic en **Iniciar instalación**. Después de aprovisionar Citrix ADC VPX en KVM, puede agregar más interfaces.

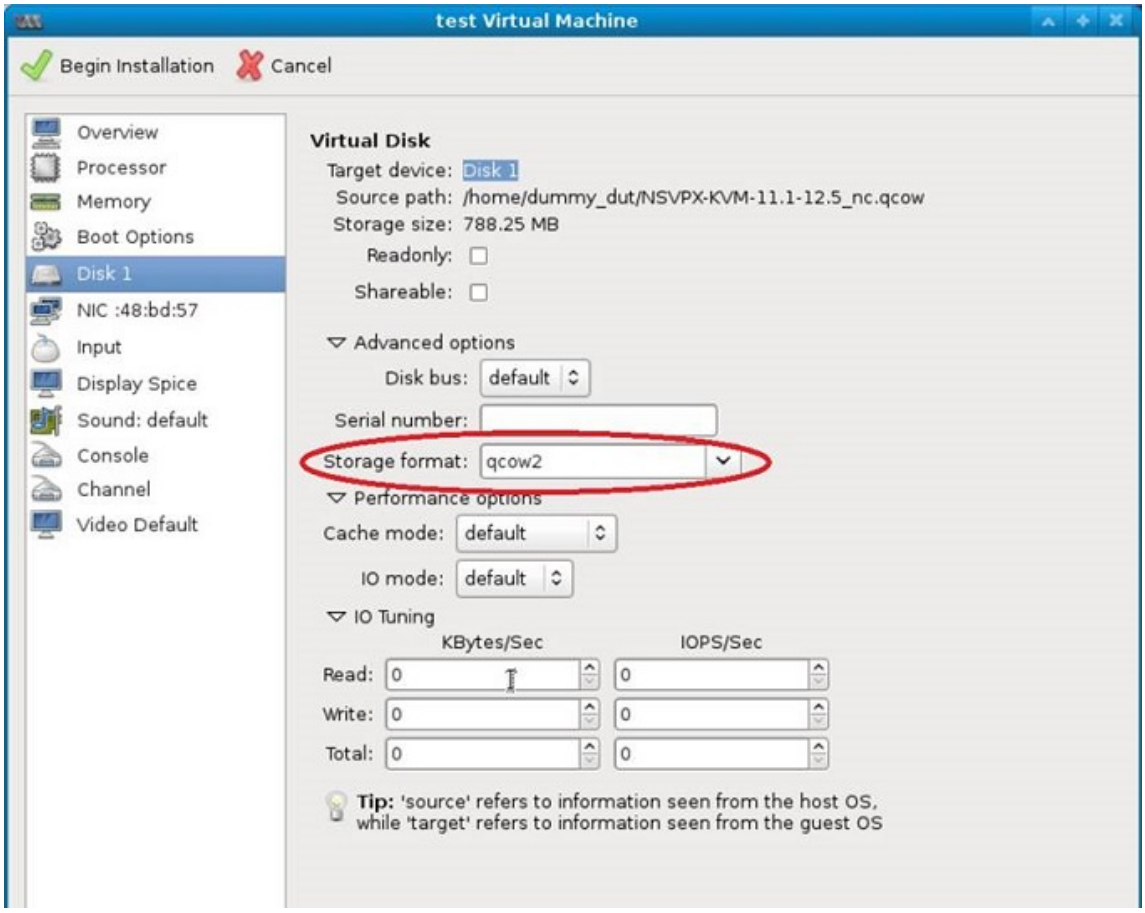
Aprovisione la instancia de Citrix ADC VPX mediante una imagen QCOW2

Con Virtual Machine Manager, puede aprovisionar la instancia de Citrix ADC VPX mediante una imagen QCOW2.

Para aprovisionar una instancia de Citrix ADC VPX mediante una imagen QCOW2, siga estos pasos:

1. Siga el **paso 1** al **paso 8** de Aprovisionamiento de la instancia Citrix ADC VPX mediante una imagen RAW.

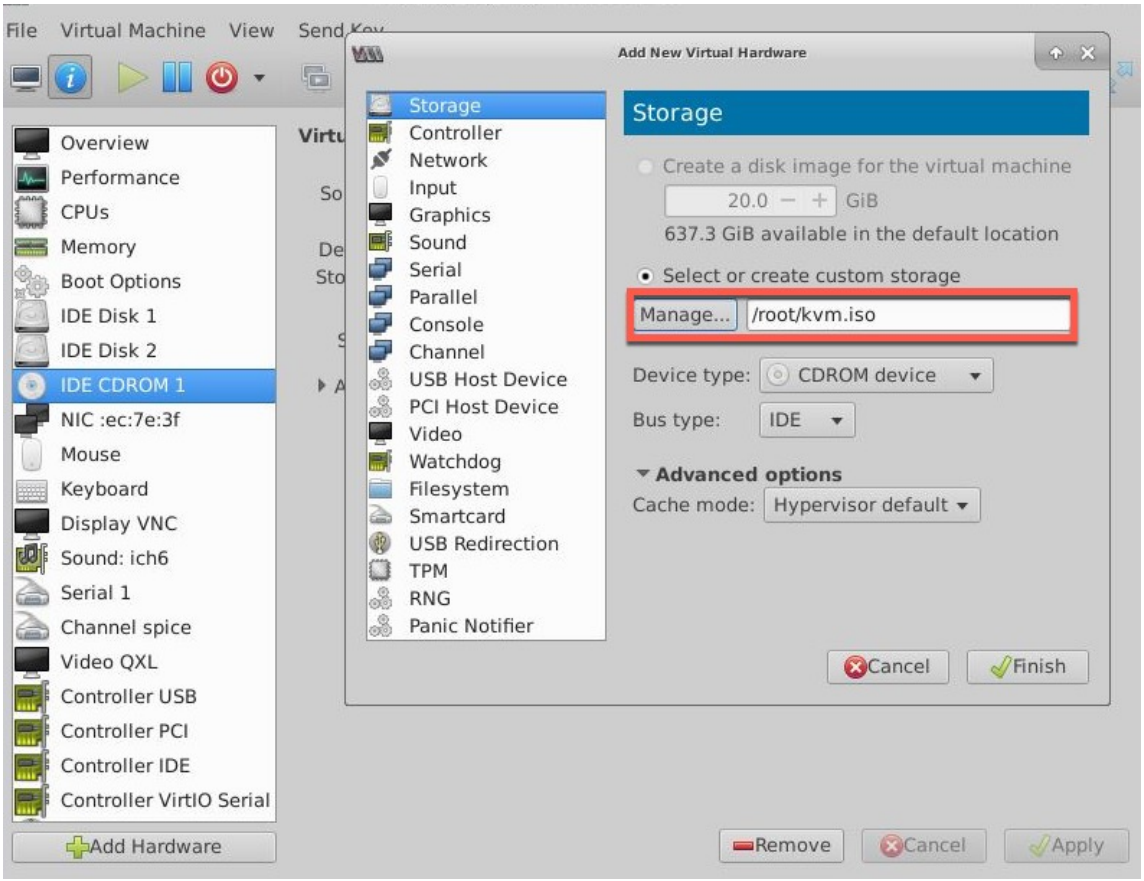
   Nota: Asegúrese de seleccionar la imagen **qcow2**en el **paso 5**.
2. Seleccione **Disco 1** y haga clic en **Opciones avanzadas**.
3. Seleccione **qcow2** en la lista desplegable Formato de almacenamiento.



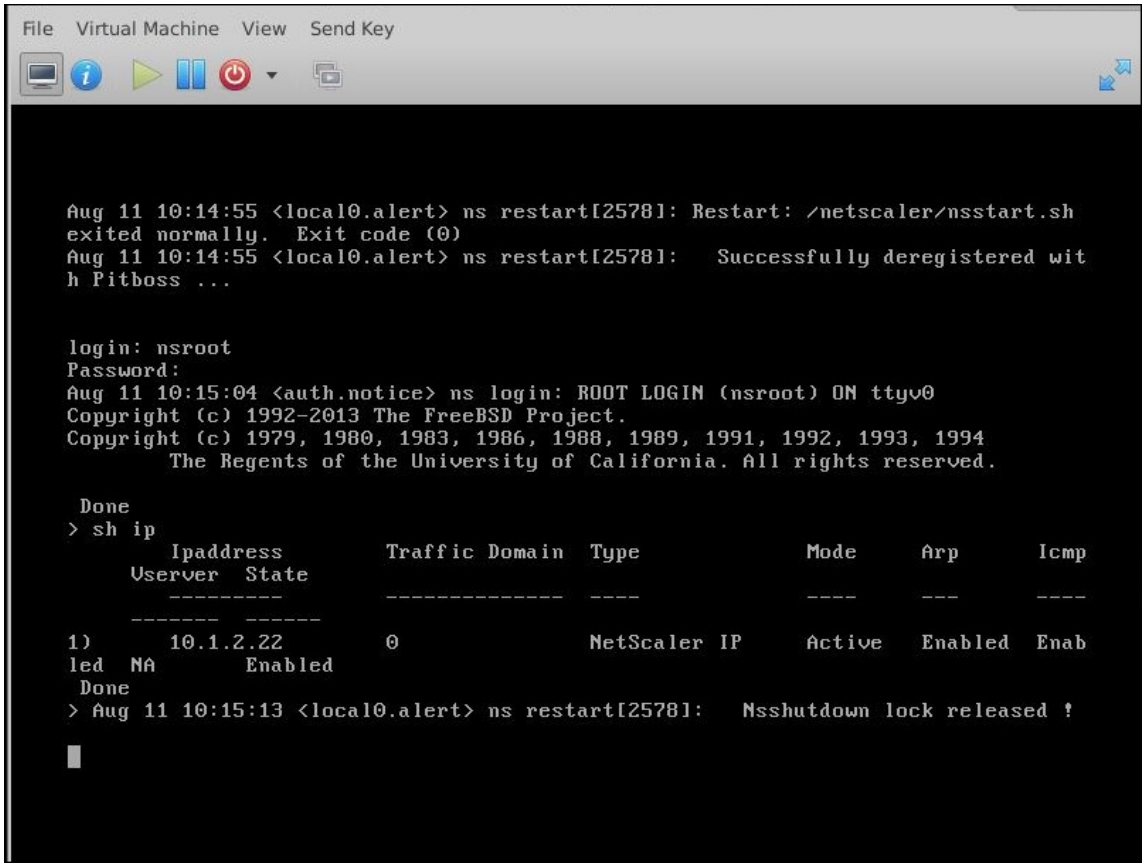
4. Haga clic en **Aplicar** y, a continuación, haga clic en **Iniciar instalación**. Después de aprovisionar Citrix ADC VPX en KVM, puede agregar más interfaces.

Habilitar el aprovisionamiento automático adjuntando una unidad de CDROM

1. Haga clic en Agregar **hardware > Almacenamiento > Tipo de dispositivo > Dispositivo CDROM**.
2. Haga clic en **Administrar** y seleccione el archivo ISO correcto que ha montado en la sección “Requisitos previos para el aprovisionamiento automático de una instancia Citrix ADC VPX” y haga clic en **Finalizar**. Se crea un nuevo CDROM en Recursos en la instancia de Citrix ADC VPX.



3. Encienda la instancia VPX y se aprovisiona automáticamente con la configuración de red proporcionada en el archivo OVF, como se muestra en la captura de pantalla de ejemplo.



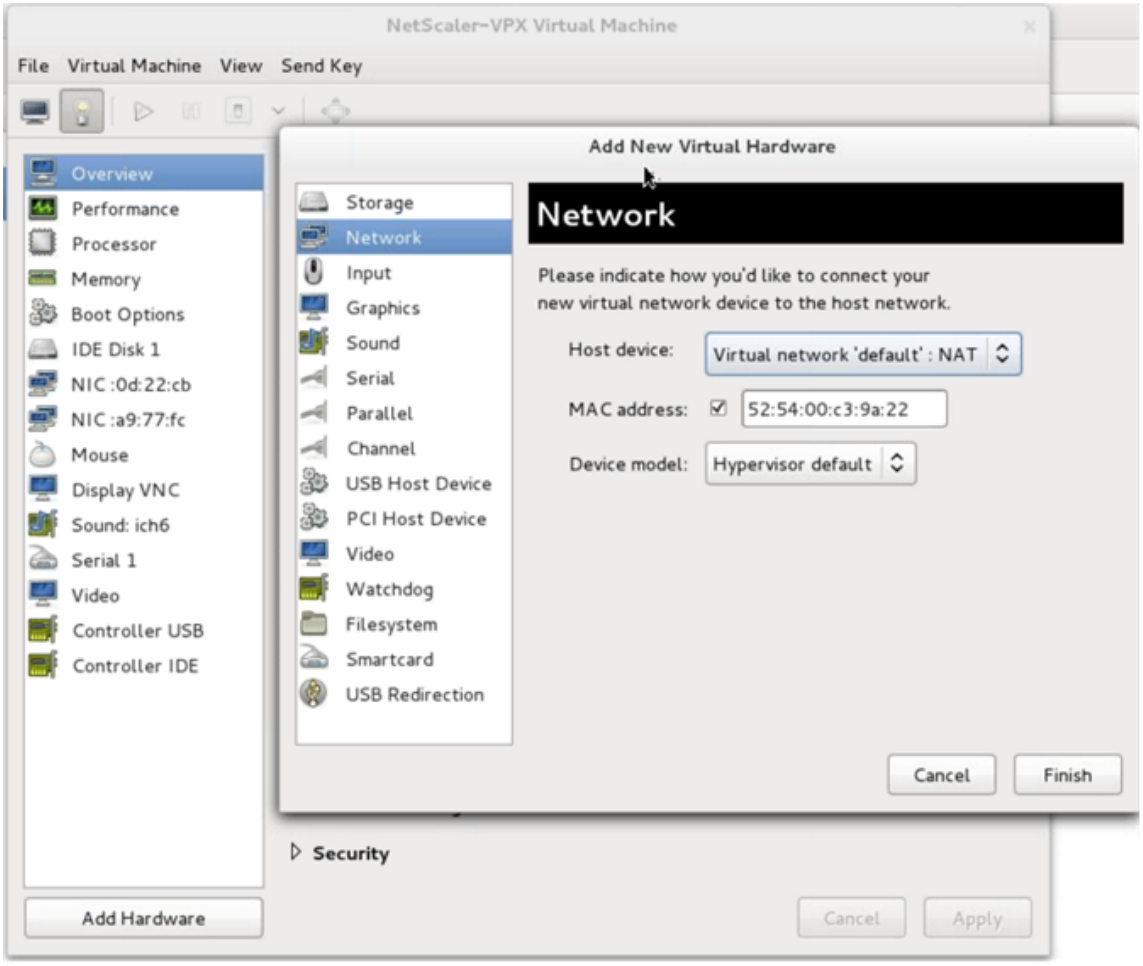
4. Si el aprovisionamiento automático falla, la instancia aparece con la dirección IP predeterminada (192.168.100.1). En ese caso, debe completar la configuración inicial manualmente. Para obtener más información, consulte Configurar el ADC por primera vez.

Agregar más interfaces a la instancia de Citrix ADC VPX mediante Virtual Machine Manager

Después de haber aprovisionado la instancia de NetScaler VPX en KVM, puede agregar interfaces adicionales.

Para añadir más interfaces, sigue estos pasos.

1. Apague la instancia de NetScaler VPX que se ejecuta en el KVM.
2. Haga clic con el botón derecho en la instancia de VPX y elija **Abrir** en el menú emergente.
3. Haga clic en el icono de  del encabezado para ver los detalles del hardware virtual.
4. Haga clic en **Agregar hardware**. En la **ventana Agregar nuevo hardware virtual**, seleccione **Red**en el menú de navegación.



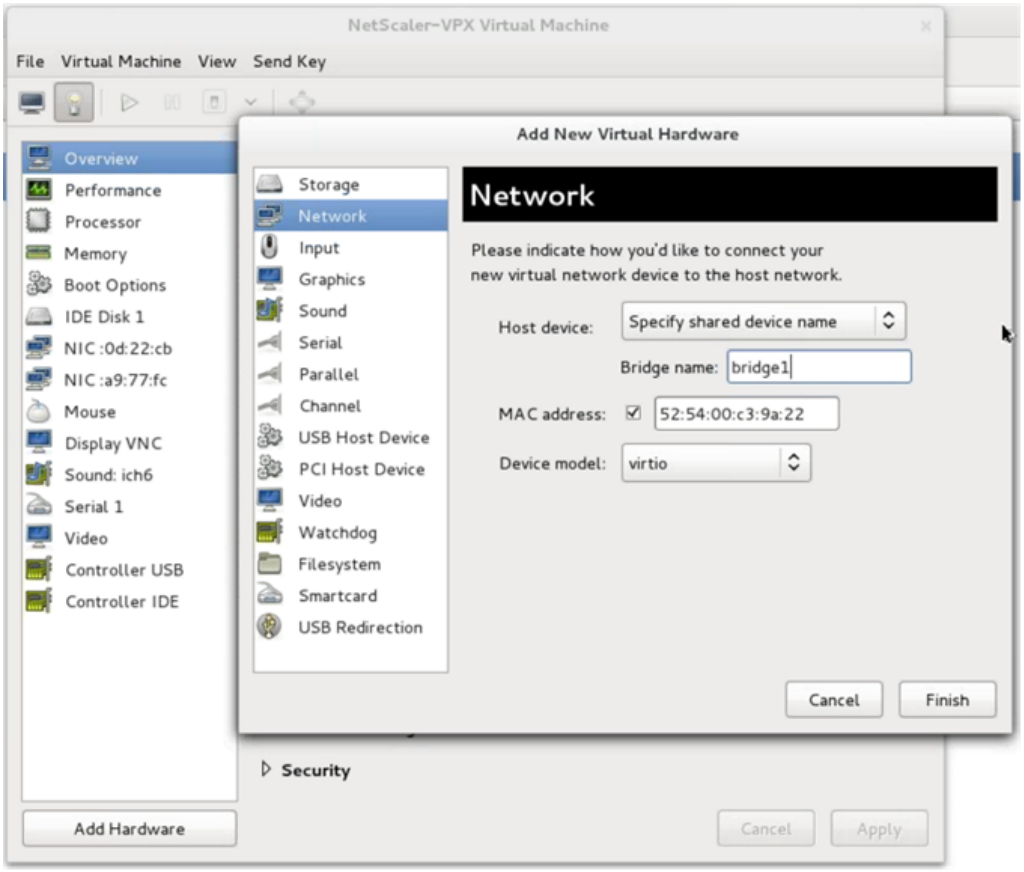
5. En el campo **Dispositivo de host**, seleccione el tipo de interfaz física. El tipo de dispositivo host puede ser Bridge o MacVtap. En el caso de MacVTap, cuatro modos posibles son VEPA, Bridge, Private y Pass-through.

    a) Para Bridge

        i. Dispositivo host: Seleccione la opción “Especificar nombre de dispositivo compartido”.

        ii. Proporcione el nombre del puente configurado en el host KVM.

            Nota: Asegúrese de haber configurado un puente Linux en el host KVM, enlazado la interfaz física al puente y poner el puente en el estado ACTIVO.



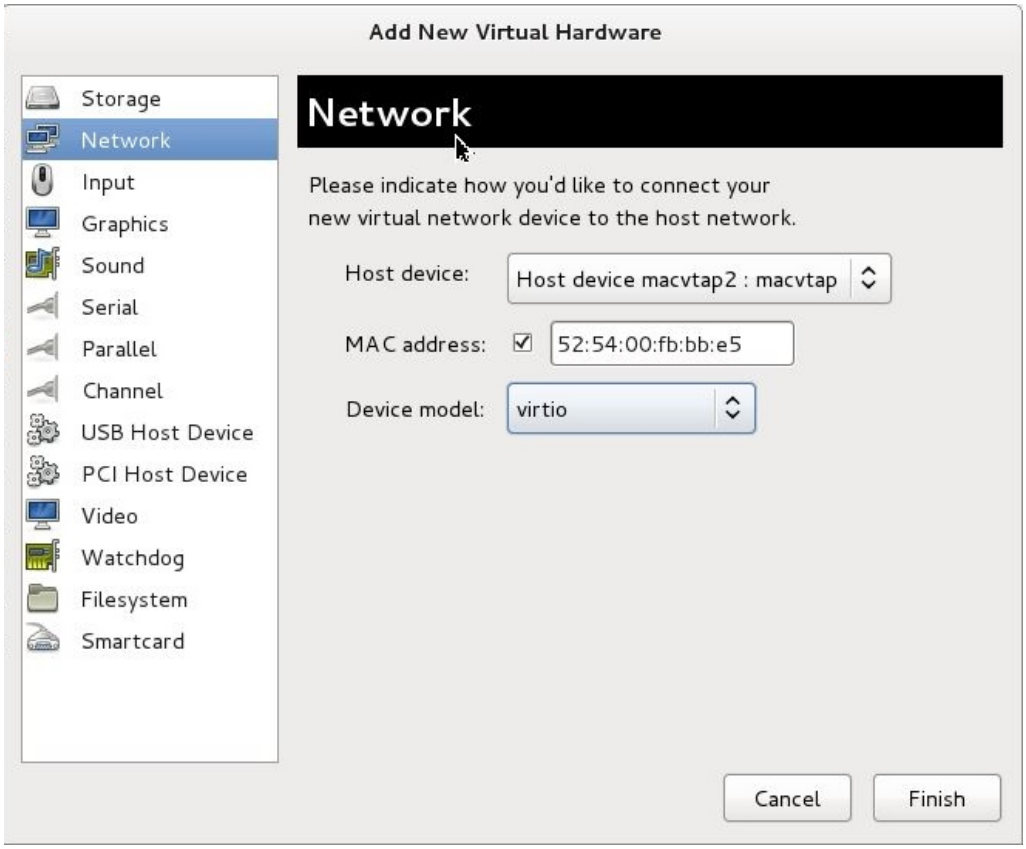
iii. Modelo de dispositivo:`virtio`.

iv. Haga clic en Finalizar.

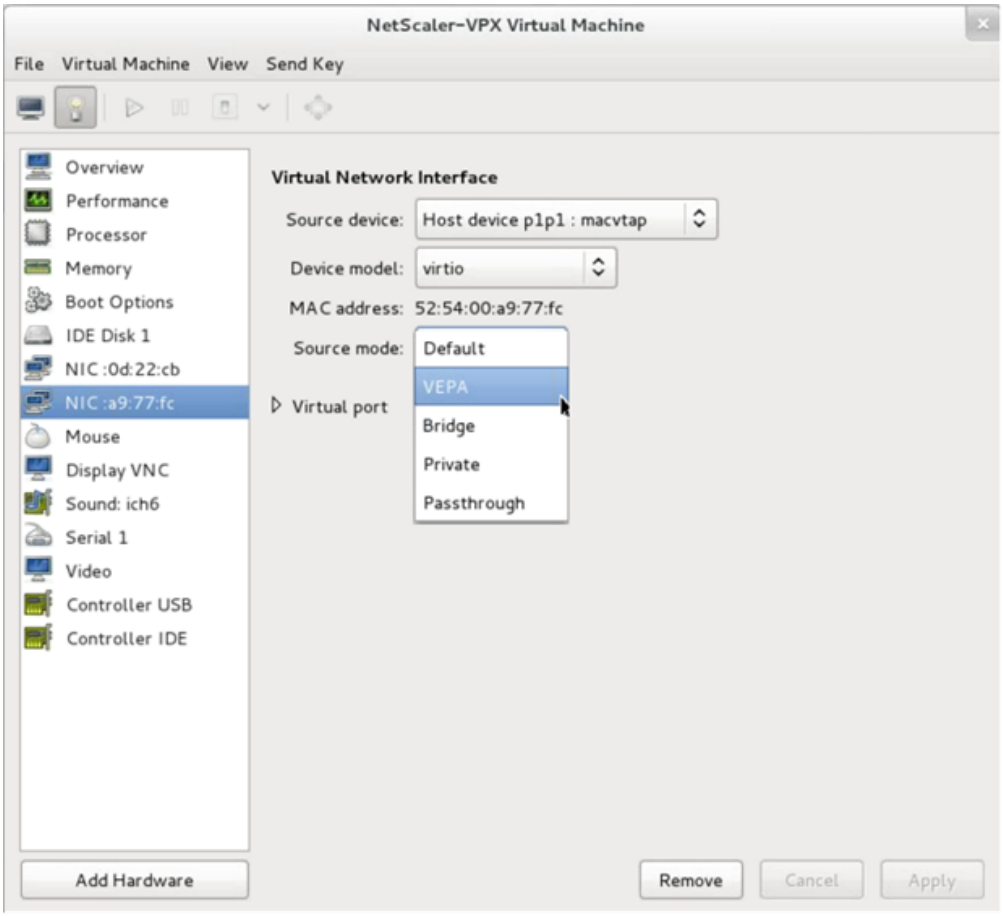
b) Para MacVtap

i. Dispositivo host: Seleccione la interfaz física en el menú.

ii. Modelo de dispositivo:`virtio`.



iii. Haga clic en Finalizar. Puede ver la NIC recién agregada en el panel de navegación.



iv. Seleccione la NIC recién agregada y seleccione el modo de origen para esta NIC. Los modos disponibles son VEPA, Bridge, Private y Passthrough. Para obtener más información sobre la interfaz y los modos, consulte Interfaz y modos de origen.

v. Haga clic en Aplicar.

6. Si quiere aprovisionar automáticamente la instancia VPX, consulte la sección “Agregar una unidad de configuración para habilitar el aprovisionamiento automático” en este documento. De lo contrario, encienda la instancia VPX para completar la configuración inicial manualmente.

> **Importante**
>
> No se admiten configuraciones de parámetros de interfaz como velocidad, dúplex y negociación automática.

Configurar una instancia de Citrix ADC VPX para utilizar interfaces de red SR-IOV

August 20, 2021

Puede configurar una instancia de Citrix ADC VPX que se ejecute en la plataforma Linux-KVM mediante virtualización de E/S raíz única (SR-IOV) con las siguientes NIC:

- Intel 82599 10G
- Intel X710 10G
- Intel XL710 40G
- Intel X722 10G

En esta sección se describe cómo:

- Configurar una instancia Citrix ADC VPX para utilizar la interfaz de red SR-IOV
- Configurar LA/LACP estático en la interfaz SR-IOV
- Configurar VLAN en la interfaz SR-IOV

Limitaciones

Tenga en cuenta las limitaciones al utilizar las NIC Intel 82599, X710, XL710 y X722. No se admiten las siguientes funciones.

Limitaciones para la NIC Intel 82599:

- Conmutación de modo L2.
- Partición de administrador (modo VLAN compartido).
- Alta disponibilidad (modo activo-activo).
- Marcos jumbo.
- IPv6: Solo puede configurar hasta 30 direcciones IPv6 únicas en una instancia VPX si tiene al menos una interfaz SR-IOV.
- No se admite la configuración de VLAN en Hypervisor para la interfaz VF de SRIOV a través del `ip link` comando.
- No se admiten configuraciones de parámetros de interfaz como velocidad, dúplex y negociaciones automáticas.

Limitaciones para las NIC Intel X710 10G, Intel XL710 40G e Intel X722 10G:

- Conmutación de modo L2.
- Partición de administrador (modo VLAN compartido).
- En un clúster, las tramas jumbo no se admiten cuando se utiliza la NIC XL710 como interfaz de datos.
- La lista de interfaces se reordena cuando las interfaces se desconectan y se vuelven a conectar.
- No se admiten configuraciones de parámetros de interfaz como velocidad, dúplex y negociaciones automáticas.
- El nombre de la interfaz es 40/X para las NIC Intel X710 10G, Intel XL710 40G e Intel X722 10G
- Se pueden admitir hasta 16 interfaces Intel XL710/X710/X722 SRIOV o PCI en una instancia VPX.

> **Nota:** Para que las NIC Intel X710 10G, Intel XL710 40G e Intel X722 10G sean compatibles con IPv6, debe habilitar el modo de confianza en las funciones virtuales (VF) escribiendo el siguiente comando en el host KVM:
>
> ```
> ## ip link set <PNIC> <VF> trust on
> ```
>
> Ejemplo:
>
> ```
> ## ip link set ens785f1 vf 0 trust on
> ```

Requisitos previos

Antes de configurar una instancia de Citrix ADC VPX para utilizar interfaces de red SR-IOV, complete las siguientes tareas de requisitos previos. Consulte la columna NIC para obtener información detallada sobre cómo completar las tareas correspondientes.

Tarea	NIC Intel 82599	NIC Intel X710, XL710 y X722
1. Agregue la NIC al host KVM.	-	-
2. Descargue e instale el controlador Intel más reciente.	Controlador IXGBE	Controlador I40E
3. Lista de bloques del controlador del host KVM.	Agregue la siguiente entrada en el archivo /etc/modprobe.d/blacklist.conf:`blacklist ixgbevf`. Utilice el controlador IXGBE versión 4.3.15 (recomendado).	Agregue la siguiente entrada en el archivo /etc/modprobe.d/blacklist.conf:`blacklist i40evf`. Utilice el controlador i40e versión 2.0.26 (recomendado).

Tarea	NIC Intel 82599	NIC Intel X710, XL710 y X722
4. Habilite las funciones virtuales (VF) SR-IOV en el host KVM. En ambos comandos de las dos columnas siguientes:`number_of_VFs` = el número de VF virtuales que quiere crear.`device_name` = el nombre de la interfaz.	Si está usando una versión anterior del kernel 3.8, agregue la siguiente entrada al archivo /etc/modprobe.d/ixgbe y reinicie el host KVM: `options ixgbe max_vfs =<number_of_VFs>`. Si está usando la versión 3.8 del kernel o posterior, cree VF mediante el siguiente comando:`echo <number_of_VFs> > /sys/class/net/<device_name>/device/sriov_numvfs`. Consulte el ejemplo de la imagen 1.	Si está usando la versión anterior del kernel 3.8, agregue la siguiente entrada al archivo /etc/modprobe.d/i40e.conf y reinicie el host KVM:`options i40e max_vfs=<number_of_VFs>`. Si está usando la versión 3.8 del kernel o posterior, cree VF mediante el siguiente comando:`echo<number_of_VFs> > /sys/class/net/<device_name>/device/sriov_numvfs`. Vea el ejemplo en la ilustración 2.
5. Haga que los VF sean persistentes agregando los comandos que utilizó para crear VF, al archivo rc.local.	Consulte el ejemplo en la imagen 3.	Consulte el ejemplo en la imagen 3.

> **Importante**
>
> Cuando cree los VF SR-IOV, asegúrese de que no asigna direcciones MAC a los VF.

Ilustración 1: Habilitar las VFs SR-IOV en el host KVM para la NIC Intel 82599 10G.

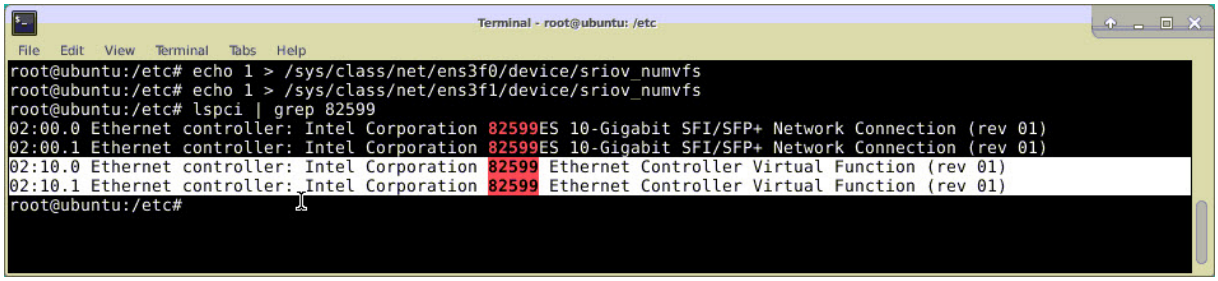


Ilustración 2: Habilitar VF SR-IOV en el host KVM para las NIC Intel X710 10G y XL710 40G.


```
root@ubuntu:~# lspci | grep 710
03:00.0 Ethernet controller: Intel Corporation Ethernet Controller X710 for 10GbE SFP+ (rev 01)
03:00.1 Ethernet controller: Intel Corporation Ethernet Controller X710 for 10GbE SFP+ (rev 01)
03:00.2 Ethernet controller: Intel Corporation Ethernet Controller X710 for 10GbE SFP+ (rev 01)
03:00.3 Ethernet controller: Intel Corporation Ethernet Controller X710 for 10GbE SFP+ (rev 01)
03:06.0 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 01)
03:06.1 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 01)
03:0a.0 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 01)
03:0a.1 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 01)
03:0a.2 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 01)
03:0a.3 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 01)
03:0e.0 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 01)
03:0e.1 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 01)
03:0e.2 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 01)
03:0e.3 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 01)
81:00.0 Ethernet controller: Intel Corporation Ethernet Controller XL710 for 40GbE QSFP+ (rev 01)
82:00.0 Ethernet controller: Intel Corporation Ethernet Controller XL710 for 40GbE QSFP+ (rev 02)
82:00.1 Ethernet controller: Intel Corporation Ethernet Controller XL710 for 40GbE QSFP+ (rev 02)
82:02.0 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 02)
82:02.1 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 02)
82:0a.0 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 02)
82:0a.1 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 02)
root@ubuntu:~#
```

Ilustración 3: Habilitar las VFs SR-IOV en el host KVM para la NIC Intel X722 10G.

```
root@ubuntu:~# lspci | grep  "37cd"
84:02.0 Ethernet controller: Intel Corporation Device 37cd (rev 04)
84:0a.0 Ethernet controller: Intel Corporation Device 37cd (rev 04)
```

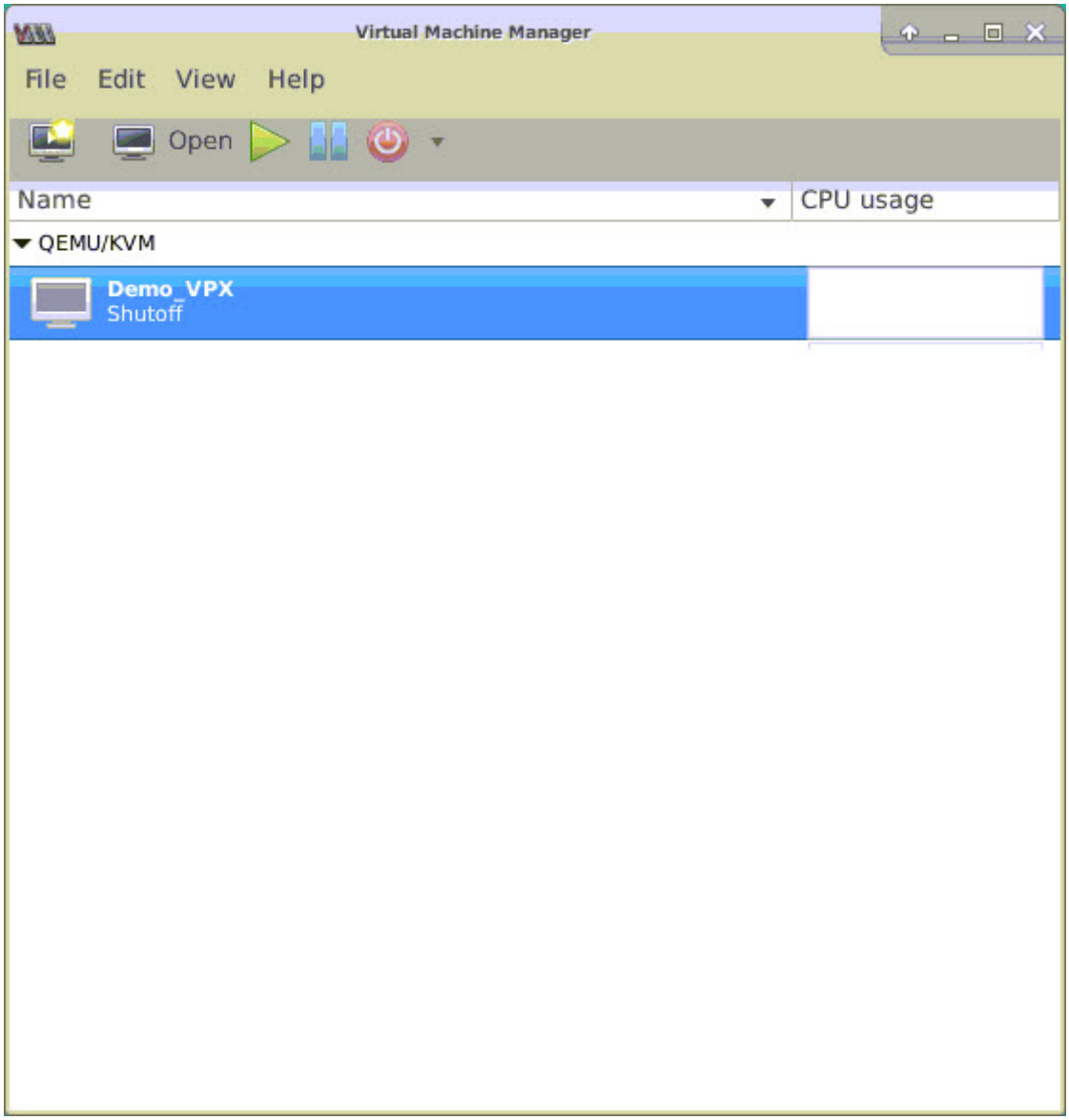
Ilustración 4: Hacer que los VF sean persistentes.

```
Terminal - root@ubuntu: /etc
File  Edit  View  Terminal  Tabs  Help
root@ubuntu:/etc# cat /etc/rc.local
#!/bin/sh -e
#
# rc.local
#
# This script is executed at the end of each multiuser runlevel.
# Make sure that the script will "exit 0" on success or any other
# value on error.
#
# In order to enable or disable this script just change the execution
# bits.
#
# By default this script does nothing.
echo 1 > /sys/class/net/ens3f0/device/sriov_numvfs
echo 1 > /sys/class/net/ens3f1/device/sriov_numvfs
exit 0
root@ubuntu:/etc#
```

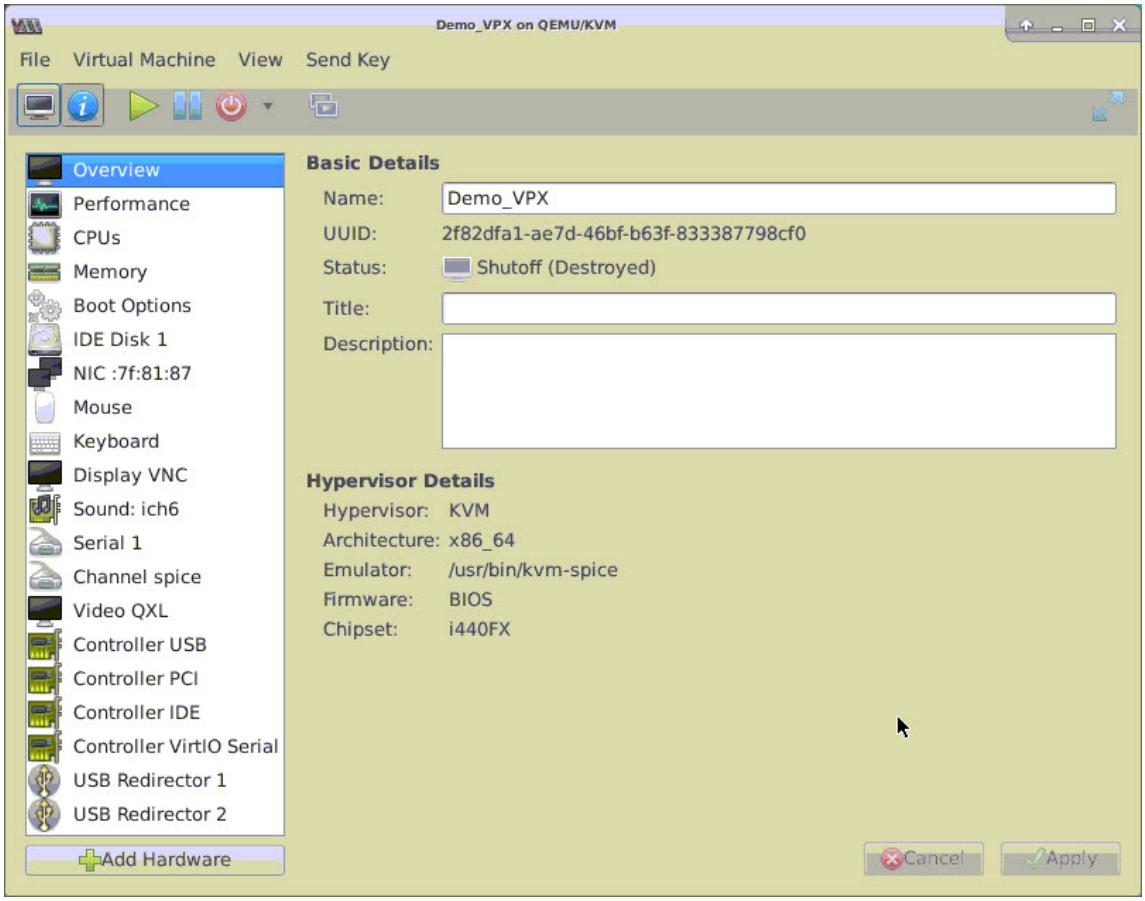
Configurar una instancia de Citrix ADC VPX para utilizar la interfaz de red SR-IOV

Para configurar la instancia Citrix ADC VPX para que use la interfaz de red SR-IOV mediante Virtual Machine Manager, siga estos pasos:

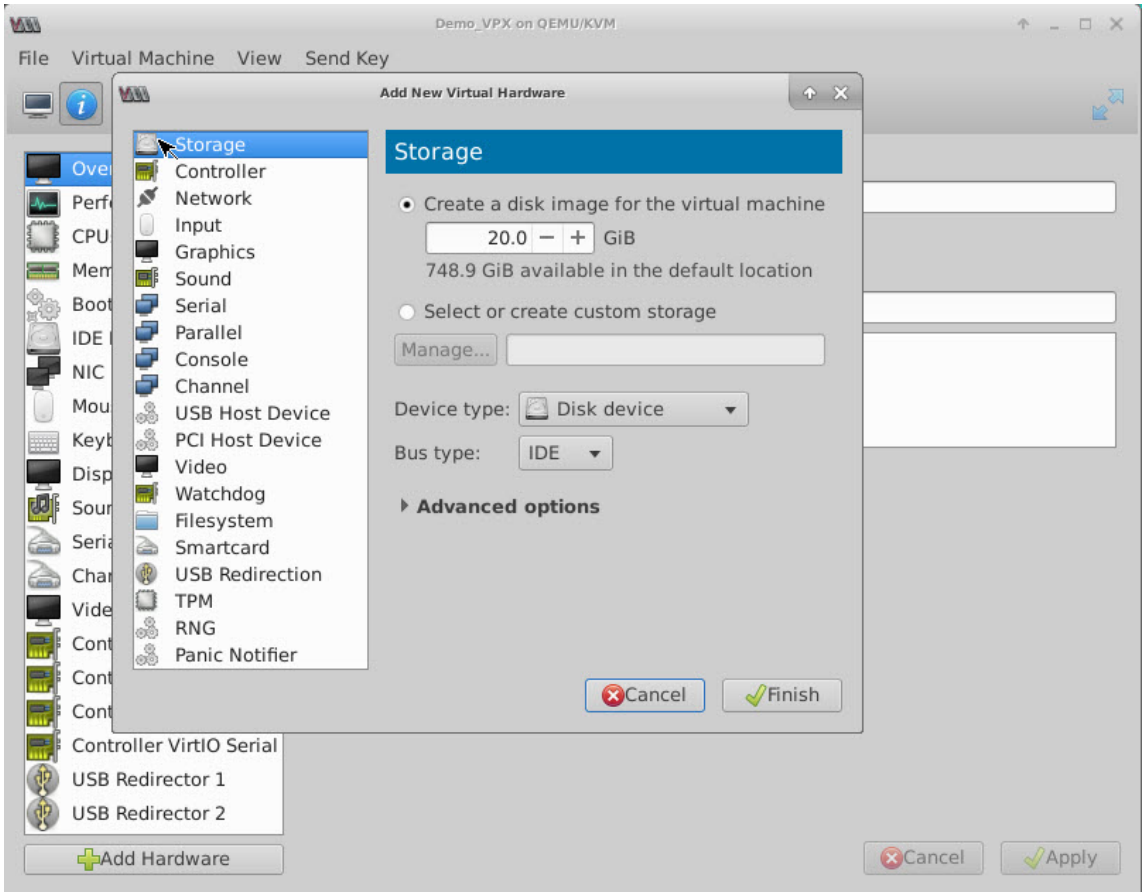
1. Apague la instancia de Citrix ADC VPX.
2. Seleccione la instancia de Citrix ADC VPX y, a continuación, seleccione Abrir.



3. En la <virtual machine on KVM>ventana, selecciona el icono **i** .



4. Seleccione **Agregar hardware**.



5. En el cuadro de diálogo **Agregar nuevo hardware virtual**, haga lo siguiente:

   a) Seleccione Dispositivo de host PCI.

   b) En la sección Dispositivo host, seleccione el VF que ha creado y haga clic en Finalizar.

Ilustración 4: VF para NIC Intel 82599 10G

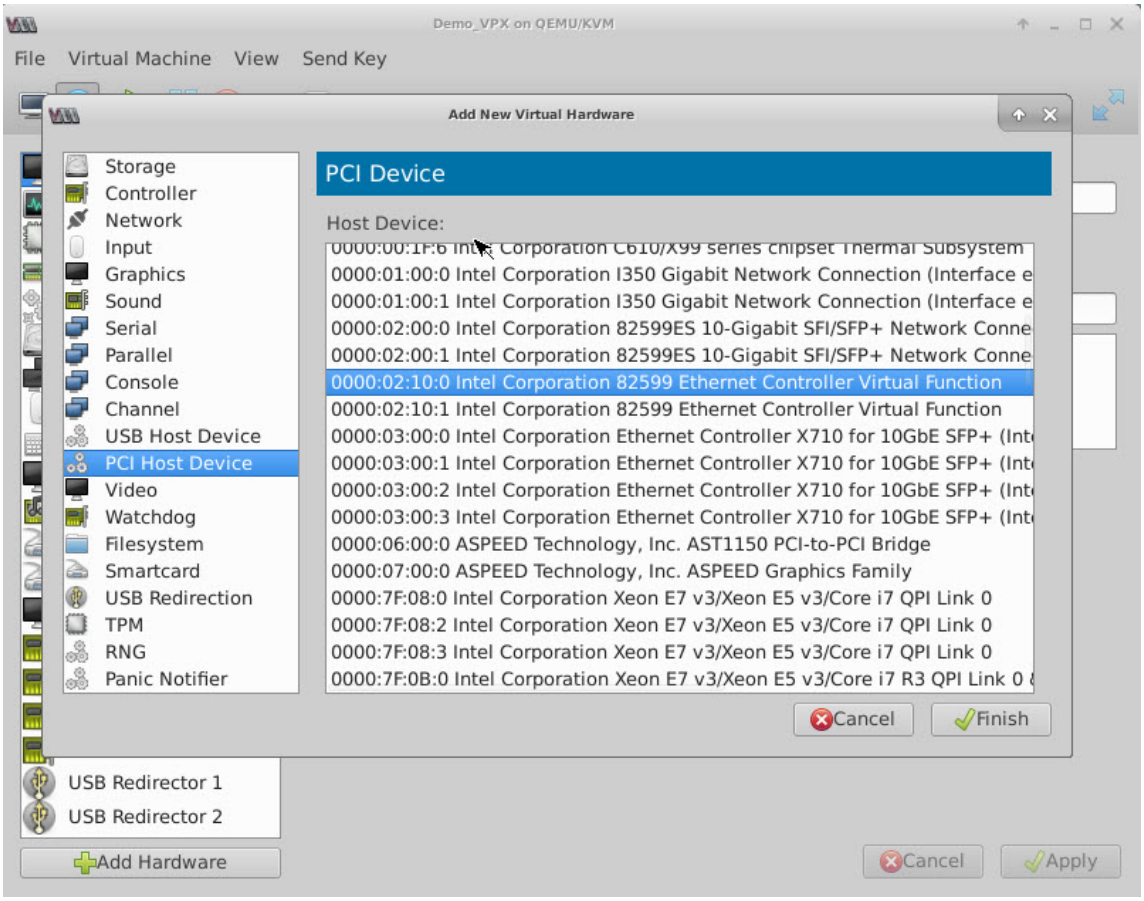


Ilustración 5: VF para la NIC Intel XL710 40G

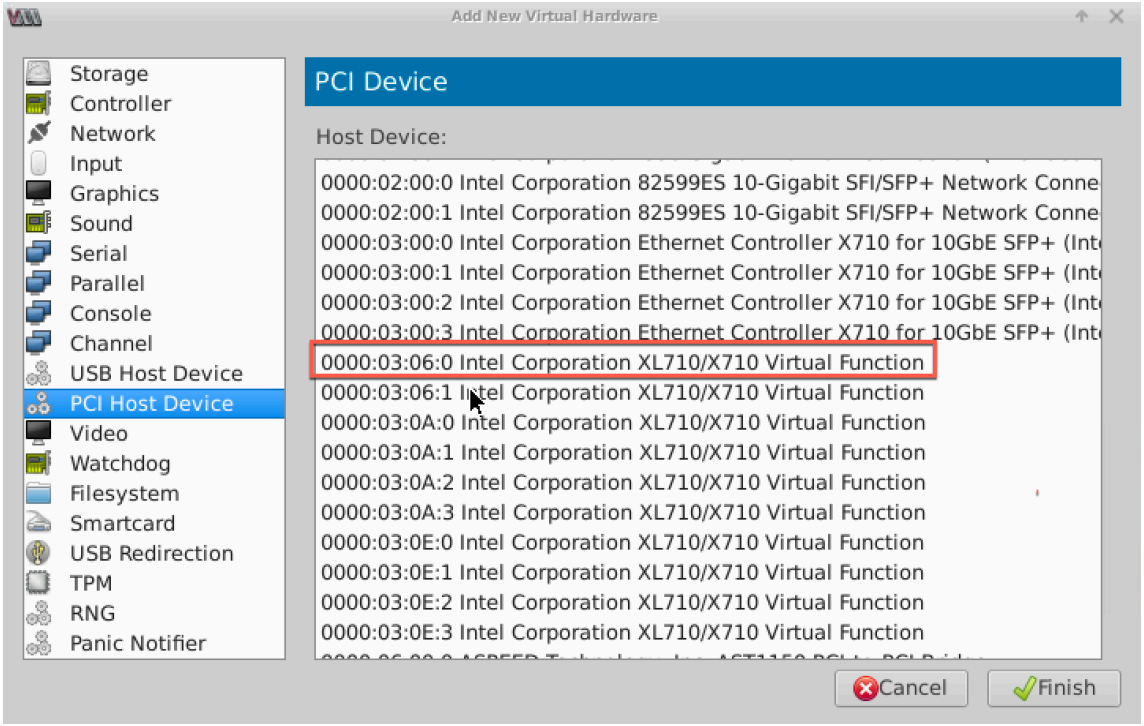
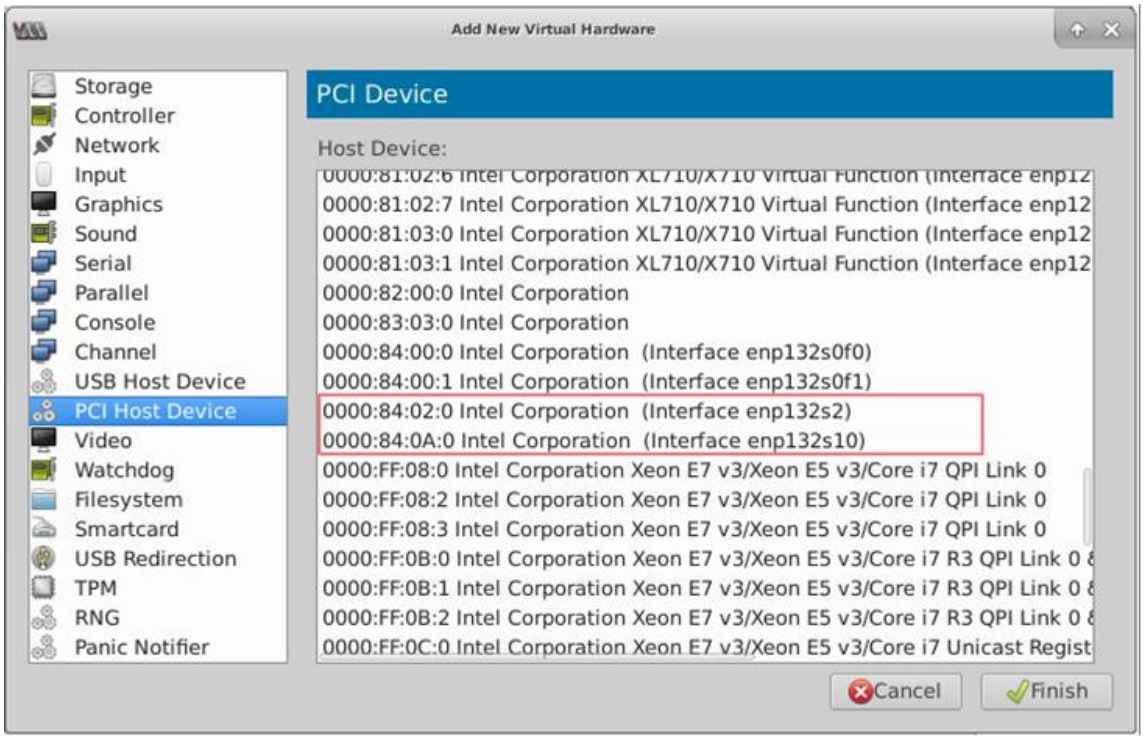


Ilustración 6: VF para la NIC Intel X722 10G



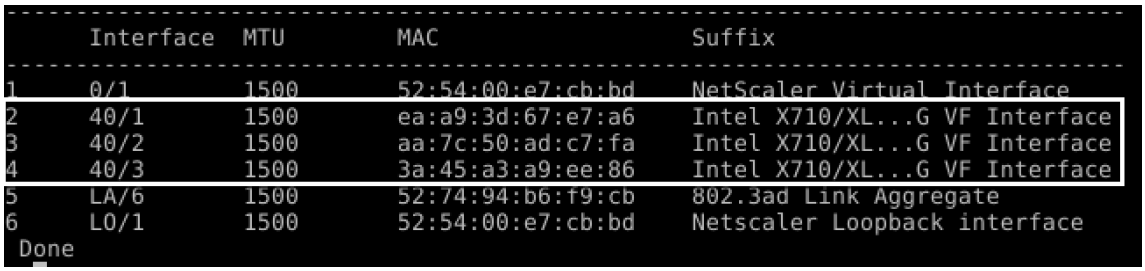
6. Repita los pasos 4 y 5 para agregar los VF que ha creado.
7. Encienda la instancia de Citrix ADC VPX.
8. Después de que se enciente la instancia de Citrix ADC VPX, utilice el siguiente comando para verificar la configuración:

```
show interface summary
<!--NeedCopy-->
```

El resultado muestra todas las interfaces que configuró.

Ilustración 6: Resumen de salida para la NIC Intel 82599.

Ilustración 7. Resumen de salida de las NIC Intel X710 y XL710.



Configurar LA/LACP estático en la interfaz SR-IOV

> **Importante**
>
> Cuando cree las VFs SR-IOV, asegúrese de no asignar direcciones MAC a las VFs.

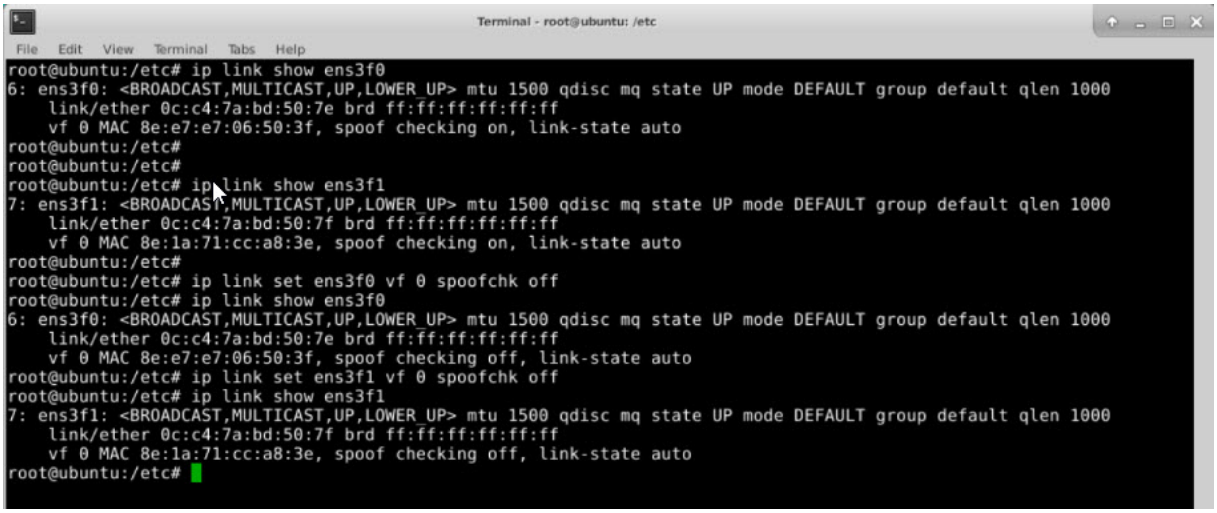
Para utilizar las VF SR-IOV en modo de agregación de enlaces, inhabilite la comprobación de suplantación de VF que haya creado. En el host KVM, utilice el siguiente comando para inhabilitar la comprobación de suplantación:

```
*ip link set \<interface\\_name\> vf \<VF\\_id\> spoofchk off*
```

Donde:

- INTERFACE_NAME: Es el nombre de la interfaz.
- vf_id: Es el id de la función virtual.

Ejemplo:



Después de inhabilitar la comprobación de suplantación para todos los VF que ha creado. Reinicie la instancia de Citrix ADC VPX y configure la agregación de enlaces. Para obtener instrucciones detalladas, consulte Configuración de la agregación de enlaces.

Configuración de VLAN en la interfaz SR-IOV

Puede configurar VLAN en las VFs SR-IOV. Para obtener instrucciones detalladas, consulte Configuración de una VLAN.

> **Importante**
>
> Asegúrese de que el host KVM no contenga la configuración de VLAN para la interfaz VF.

Configurar una instancia de Citrix ADC VPX para utilizar interfaces de red de transferencia PCI

August 20, 2021

Después de instalar y configurar una instancia de Citrix ADC VPX en la plataforma Linux-KVM, puede utilizar Virtual Machine Manager para configurar el dispositivo virtual para utilizar interfaces de red de paso PCI.

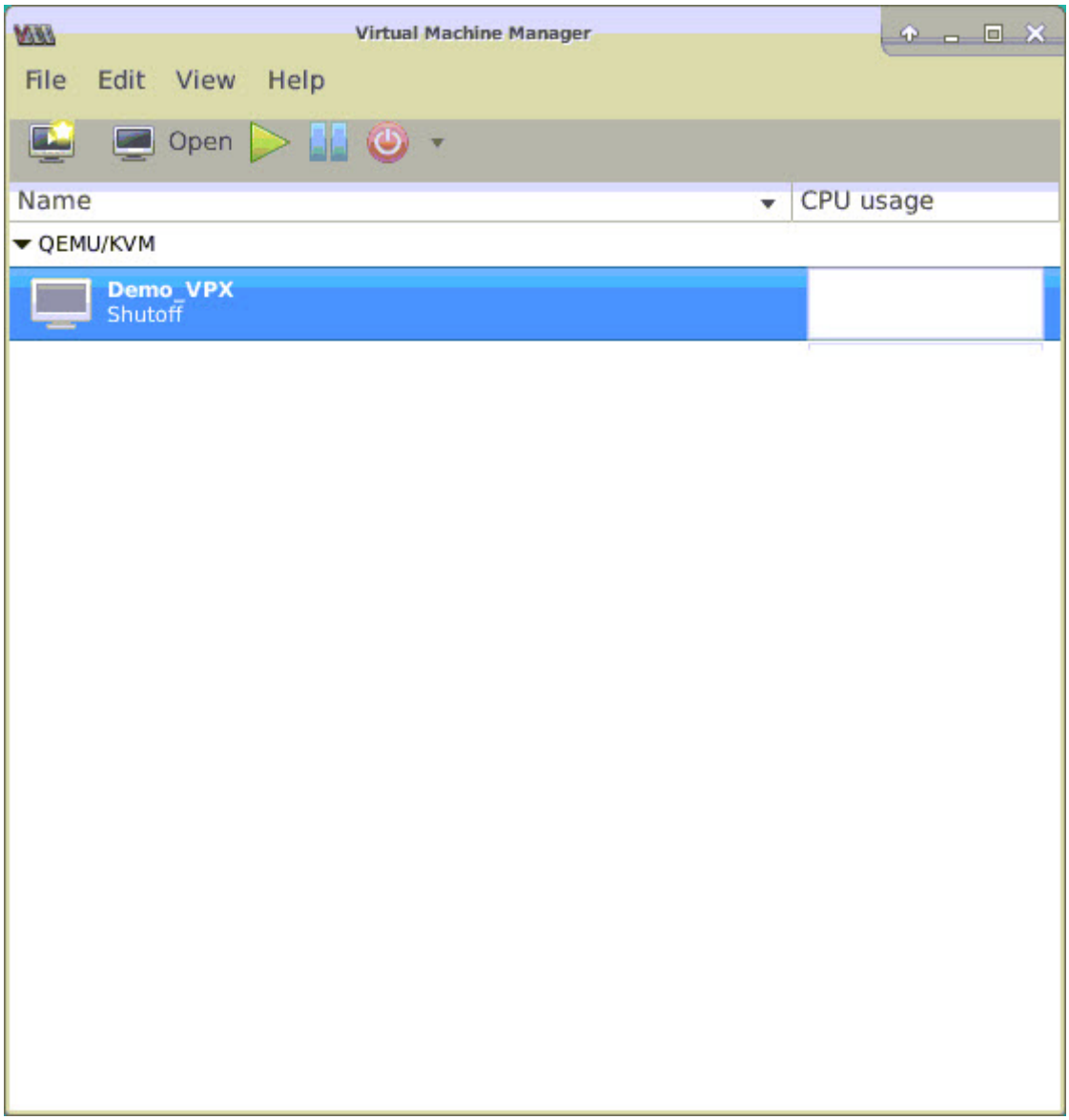
Requisitos previos

- La versión de firmware de la NIC (NIC) Intel XL710 en el host KVM es 5.04.
- El host KVM admite la unidad de administración de memoria de entrada/salida (IOMMU) e Intel VT-d, y están habilitados en el BIOS del host KVM. En el host KVM, para habilitar IOMMU, agregue la siguiente entrada al archivo **/boot/grub2/grub.cfg**: **intel_iommu=1**

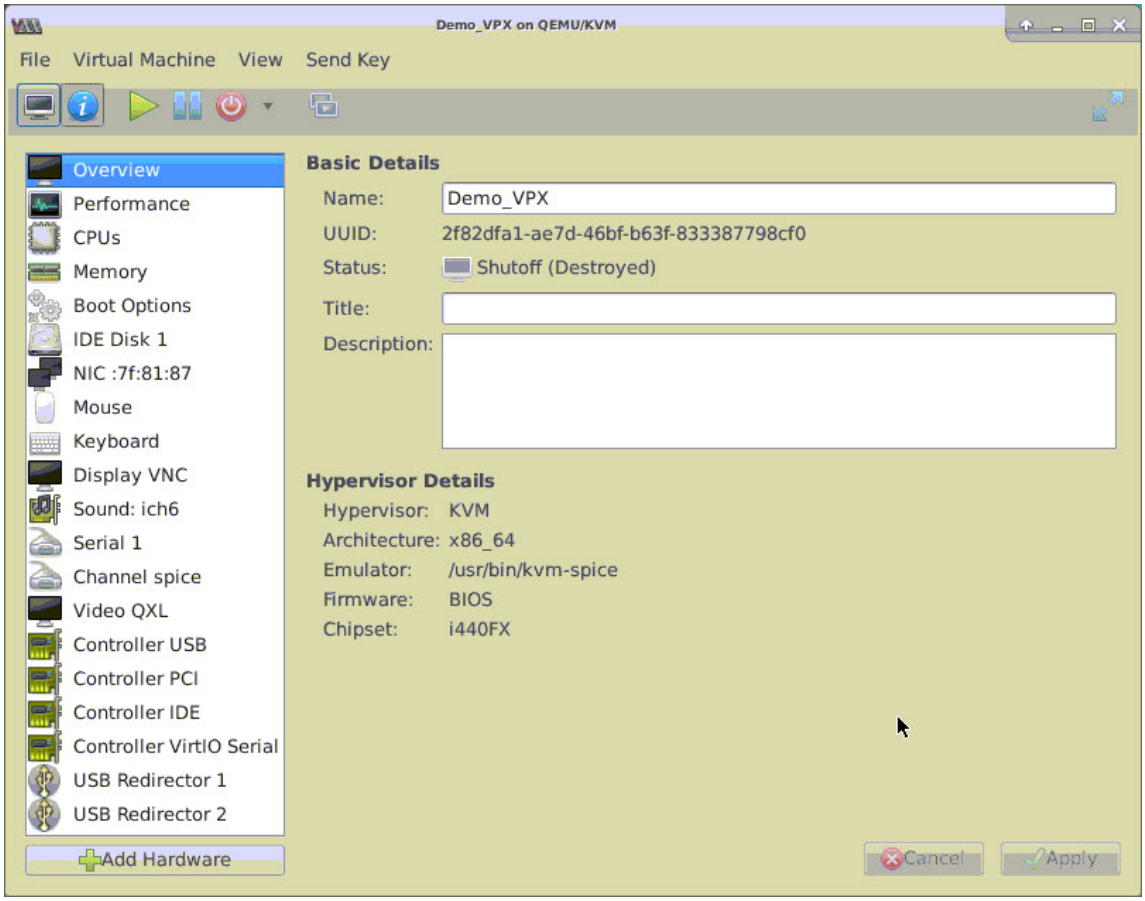
- Ejecute el siguiente comando y reinicie el host KVM: **Grub2-mkConfig —o /boot/grub2/grub.cfg**

Para configurar instancias de Citrix ADC VPX para que utilicen interfaces de red de transferencia PCI mediante Virtual Machine Manager:

1. Apague la instancia de Citrix ADC VPX.
2. Seleccione la instancia de Citrix ADC VPX y haga clic en **Abrir**.



3. En la ventana **virtual_machine en KVM**, haga clic en el icono **i** .

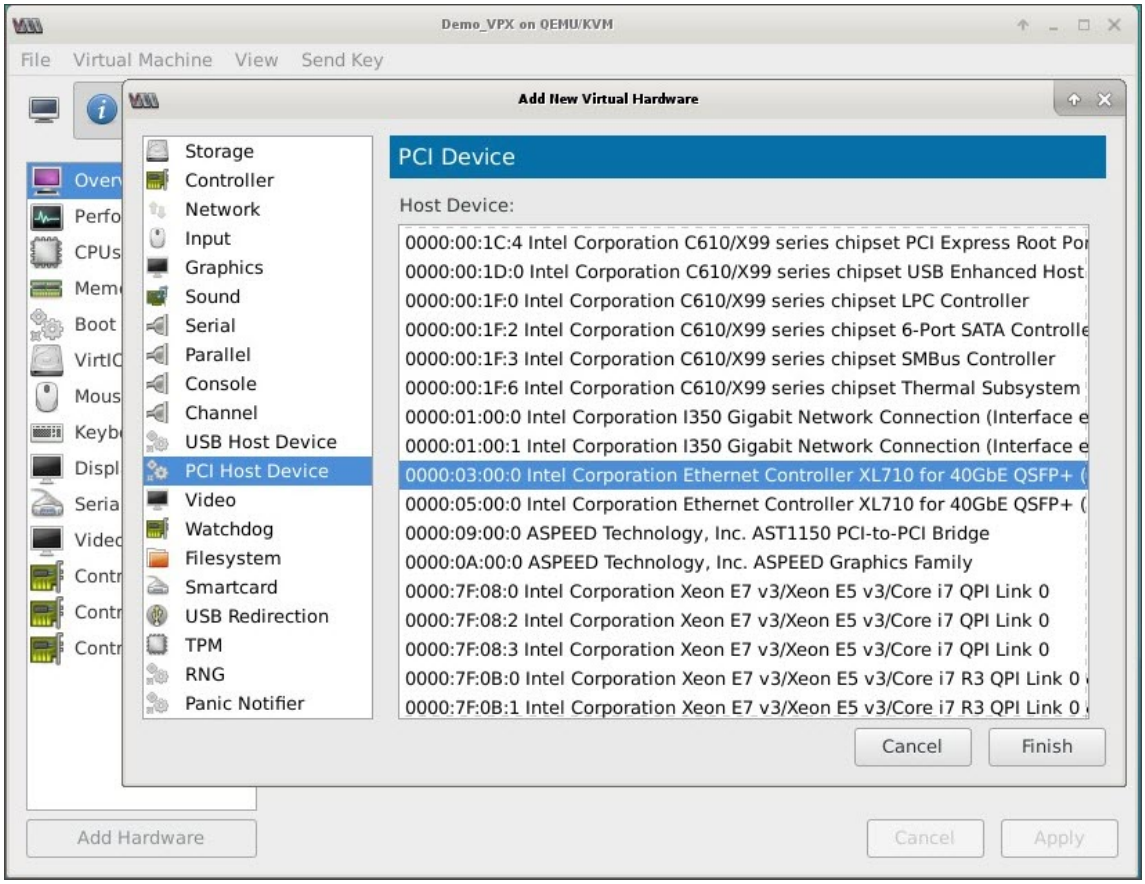


4. Haga clic en **Agregar hardware**.
5. En el cuadro de diálogo **Agregar nuevo hardware virtual**, haga lo siguiente:

   a. Seleccione **Dispositivo de host PCI**.

   b. En la sección **Dispositivo host**, seleccione la función física Intel XL710.

   c. Haga clic en **Finalizar**.

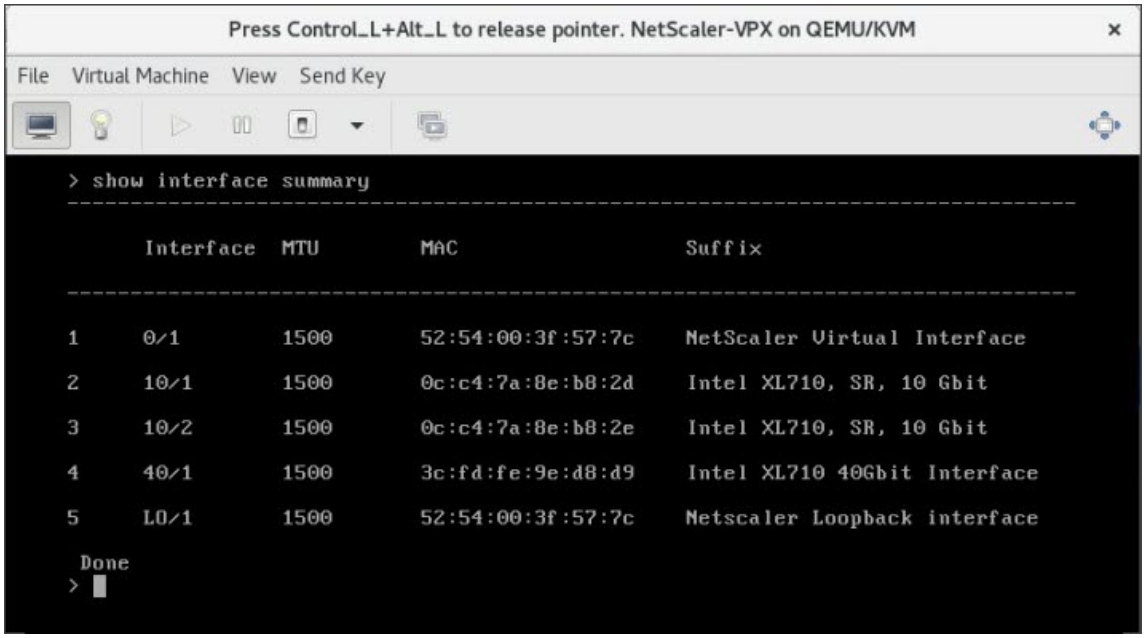


6. Repita los pasos **4** y **5** para agregar funciones físicas adicionales de Intel XL710.
7. Encienda la instancia de Citrix ADC VPX.
8. Una vez que se enciende la instancia de Citrix ADC VPX, puede utilizar el siguiente comando para verificar la configuración:

```
COMMAND

> show interface summary
```

El resultado debe mostrar todas las interfaces que ha configurado:



Aprovisionamiento de la instancia Citrix ADC VPX mediante el virsh programa

August 20, 2021

El `virsh` programa es una herramienta de línea de comandos para administrar invitados de VM. Su funcionalidad es similar a la de Virtual Machine Manager. Le permite cambiar el estado de un invitado de VM (iniciar, detener, pausar, etc.), configurar nuevos invitados y dispositivos y modificar las configuraciones existentes. El `virsh` programa también es útil para crear scripts de operaciones de administración de invitados de VM.

Para aprovisionar Citrix ADC VPX mediante el `virsh` programa, siga estos pasos:

1. Utilice el comando tar para desatar el paquete Citrix ADC VPX. El paquete NSVPX-KVM-*_NC.tgz contiene los siguientes componentes:
   - Archivo XML de dominio que especifica atributos VPX [NSVPX-KVM-*_NC.xml]
   - Comprobar la suma de la imagen de disco NS-VM [CheckSum.txt]
   - Imagen de disco NS-VM [NSVPX-KVM-*_NC.raw]

   Ejemplo:

```
tar -xvzf NSVPX-KVM-10.1-117_nc.tgz
NSVPX-KVM-10.1-117_nc.xml
NSVPX-KVM-10.1-117_nc.raw
```



```
4 checksum.txt
5 <!--NeedCopy-->
```

2. Copie el archivo XML Nsvpx-kvm-*_nc.xml en un archivo denominado <DomainName> -nsvpx-kvm-*_nc.xml. El <DomainName> es también el nombre de la máquina virtual. Ejemplo:

```
1 cp NSVPX-KVM-10.1-117_nc.xml NetScaler-VPX-NSVPX-KVM-10.1-117_nc.
     xml
2 <!--NeedCopy-->
```

3. Modifique el archivo <DomainName> -nsvpx-kvm-*_nc.xml para especificar los siguientes parámetros:

   - name: Especifique el nombre.
   - Mac: especifique la dirección MAC.
     Nota: El nombre de dominio y la dirección MAC tienen que ser únicos.
   - archivo fuente: especifique la ruta de origen absoluta de la imagen de disco. La ruta del archivo tiene que ser absoluta. Puede especificar la ruta del archivo de imagen RAW o de un archivo de imagen QCOW2.

     Si quiere especificar un archivo de imagen RAW, especifique la ruta de origen de la imagen de disco como se muestra en el ejemplo siguiente:

     Ejemplo:

```
1   <name>NetScaler-VPX</name>
2   <mac address='52:54:00:29:74:b3'/>
3   <source file='/root/NSVPX-KVM-10.1-117_nc.raw'/>
4   <!--NeedCopy-->
```

     Especifique la ruta de origen de imagen de disco QCOW2 absoluta y defina el tipo de controlador como **qcow2**, como se muestra en el ejemplo siguiente:

     Ejemplo:

```
1   <name>NetScaler-VPX</name>
2   <mac address='52:54:00:29:74:b3'/>
3   <driver name ='qemu' type='qcow2'/>
4   <source file='/root/NSVPX-KVM-10.1-117_nc.qcow'/>*
5   <!--NeedCopy-->
```


4. Modifique el archivo <DomainName>-NSVPX-KVM-*_nc.xml para configurar los detalles de la red:

   - source dev: Especifique la interfaz.
   - modo: Especifique el modo. La interfaz predeterminada es **Macvtap Bridge**.

   Ejemplo: Modo: puente MacVTap Establecer interfaz de destino como `ethx` y modo como puente Tipo de modelo como `virtio`

```
<interface type='direct'>
    <mac address='52:54:00:29:74:b3'/>
    <source dev='eth0' mode='bridge'/>
    <target dev='macvtap0'/>
    <model type='virtio'/>
    <alias name='net0'/>
    <address type='pci' domain='0x0000' bus='0x00' slot='0x03'
       function='0x0'/>
  </interface>
<!--NeedCopy-->
```

   Aquí, eth0 es la interfaz física conectada a la VM.

5. Defina los atributos de VM en el <DomainName>archivo -NSVPX-KVM-*_nc.xml mediante el siguiente comando: `virsh` define <DomainName>-NSVPX-KVM-*_nc.xml Ejemplo:

```
virsh define NS-VPX-NSVPX-KVM-10.1-117_nc.xml
<!--NeedCopy-->
```

6. Inicie la máquina virtual introduciendo el siguiente comando: `virsh` start [<DomainName>|<DomainUUID>] Ejemplo:

```
virsh start NetScaler-VPX
<!--NeedCopy-->
```

7. Conecte la máquina virtual invitada a través de la `virsh` consola [<DomainName><DomainUUID>| |<DomainID>] Ejemplo:

```
virsh console NetScaler-VPX
<!--NeedCopy-->
```


Agregar más interfaces a la instancia Citrix ADC VPX mediante el `virsh` programa

Después de haber aprovisionado Citrix ADC VPX en KVM, puede agregar interfaces adicionales.

Para añadir más interfaces, sigue estos pasos:

1. Apague la instancia de Citrix ADC VPX que se ejecuta en el KVM.
2. Modifique el archivo <DomainName>-NSVPX-KVM-*_nc.xml mediante el comando: `virsh` edit [<DomainName>|<DomainUUID>]
3. En el archivo <DomainName> -nsvpx-kvm-*_nc.xml, agregue los siguientes parámetros:

   a) **Para MacVtap**

   - Tipo de interfaz: Especifique el tipo de interfaz como 'direct'.
   - Dirección MAC: especifique la dirección MAC y asegúrese de que la dirección MAC sea única en todas las interfaces.
   - source dev: Especifique el nombre de la interfaz.
   - mode: especifique el modo. Los modos admitidos son: Bridge, VEPA, Privado y Pass-through
   - tipo de modelo: especifique el tipo de modelo como `virtio`

   Ejemplo:

   Modo: MacVTap PassThrough

   Establecer la interfaz de destino como
   `ethx`, Modo como
   puente y tipo de modelo como
   `virtio`

   ```
   <interface type='direct'>
         <mac address='52:54:00:29:74:b3'/>
         <source dev='eth1' mode='passthrough'/>
         <model type='virtio'/>
    </interface>
   <!--NeedCopy-->
   ```

   Aquí eth1 es la interfaz física conectada a la VM.

   b) **Para modo puente**

   Nota: Asegúrese de haber configurado un puente Linux en el host KVM, enlazado la interfaz física al puente y poner el puente en el estado ACTIVO.

   - Tipo de interfaz: Especifique el tipo de interfaz como "puente".

- Dirección MAC: especifique la dirección MAC y asegúrese de que la dirección MAC sea única en todas las interfaces.
- puente de origen: Especifique el nombre del puente.
- tipo de modelo: especifique el tipo de modelo como `virtio`

Ejemplo: modo Bridge

```
<interface type='bridge'>
      <mac address='52:54:00:2d:43:a4'/>
      <source bridge='br0'/>
      <model type='virtio'/>
 </interface>
<!--NeedCopy-->
```

Administrar las VM invitadas de Citrix ADC VPX

August 20, 2021

Puede utilizar Virtual Machine Manager y el `virsh` programa para realizar tareas de administración, como iniciar o detener un invitado de máquina virtual, configurar nuevos invitados y dispositivos, modificar configuraciones existentes y conectarse a la consola gráfica mediante Virtual Network Computing (VNC).

Administrar las VM invitadas VPX mediante Virtual Machine Manager

- Listar los invitados de VM

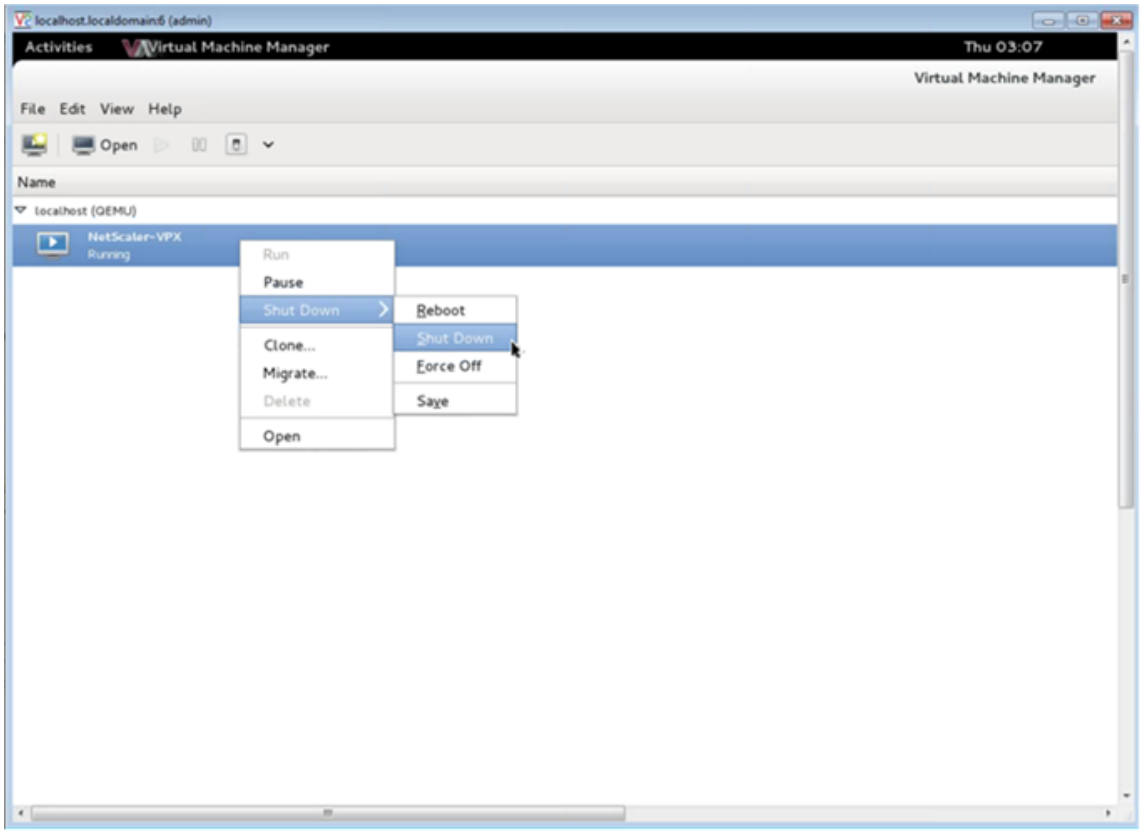
  La ventana principal de Virtual Machine Manager muestra una lista de todos los invitados de VM para cada servidor host de VM al que está conectado. Cada entrada de invitado de máquina virtual contiene el nombre de la máquina virtual, junto con su estado (En ejecución, pausa o apagado) que se muestra como en el icono.

- Abrir una consola gráfica

  Abrir una consola gráfica a un invitado de VM le permite interactuar con la máquina como lo haría con un host físico a través de una conexión VNC. Para abrir la consola gráfica en Virtual Machine Manager, haga clic con el botón derecho en la entrada de VM Guest y seleccione la opción Abrir en el menú emergente.

- Iniciar y cerrar un invitado

Puede iniciar o detener un invitado de VM desde Virtual Machine Manager. Para cambiar el estado de la VM, haga clic con el botón secundario en la entrada Invitado de VM y seleccione Ejecutar o una de las opciones de Apagar en el menú emergente.



- Reiniciar un invitado

  Puede reiniciar un invitado de VM desde Virtual Machine Manager. Para reiniciar la VM, haga clic con el botón secundario en la entrada Invitado de VM y, a continuación, seleccione Apagar > Reiniciar en el menú emergente.

- Eliminar un invitado

  Al eliminar un invitado de VM, se elimina su configuración XML de forma predeterminada. También puede eliminar los archivos de almacenamiento de un invitado. Al hacerlo, se borra completamente al invitado.

  1. En Virtual Machine Manager, haga clic con el botón secundario en la entrada VM Guest.
  2. Seleccione Eliminar en el menú emergente. Se abre una ventana de confirmación.
     Nota: La opción Eliminar solo está habilitada cuando el invitado de VM está apagado.
  3. Haga clic en Eliminar.
  4. Para borrar completamente el invitado, elimine el archivo.raw asociado activando la casilla de verificación Eliminar archivos de almacenamiento asociados.

Administrar las máquinas virtuales invitadas Citrix ADC VPX mediante el `virsh` programa

- Enumere los invitados de VM y sus estados actuales.

  Para utilizar `virsh` para mostrar información sobre los Huéspedes

  ```
  virsh list --all
  ```

  El resultado del comando muestra todos los dominios con sus estados. Ejemplo de salida:

  ```
  Id Name                 State
  ----------------------------------
    0 Domain-0            running
    1 Domain-1            paused
    2 Domain-2            inactive
    3 Domain-3            crashed
  <!--NeedCopy-->
  ```

- Abre una `virsh` consola.

  Conectar la VM invitada a través de la consola

  ```
  virsh console [<DomainID> | <DomainName> | <DomainUUID>]
  ```

  Ejemplo:

  ```
  virsh console NetScaler-VPX
  ```

- Empezar y cerrar a un invitado.

  Los invitados se pueden iniciar mediante DomainName o Domain-UUID.

  ```
  virsh start [<DomainName> | <DomainUUID>]
  ```

  Ejemplo:

  ```
  virsh start NetScaler-VPX
  ```

  Para cerrar un invitado:

  ```
  virsh shutdown [<DomainID> | <DomainName> | <DomainUUID>]
  ```

  Ejemplo:

  ```
  virsh shutdown NetScaler-VPX
  ```

- Reiniciar un invitado

  ```
  virsh reboot [<DomainID> | <DomainName> | <DomainUUID>]
  ```

  Ejemplo:


```
virsh reboot NetScaler-VPX
```

Eliminar un invitado

Para eliminar una máquina virtual invitada, debe apagar el invitado y anular la definición <DomainName>-NSVPX-KVM-*_nc.xml antes de ejecutar el comando delete.

```
virsh shutdown [<DomainID> | <DomainName> | <DomainUUID>]
virsh undefine [<DomainName> | <DomainUUID>]
<!--NeedCopy-->
```

Ejemplo:

```
virsh shutdown NetScaler-VPX
virsh undefine NetScaler-VPX
<!--NeedCopy-->
```

> Nota: El comando delete no elimina el archivo de imagen de disco que debe eliminarse manualmente.

Aprovisione la instancia Citrix ADC VPX con SR-IOV, en OpenStack

August 20, 2021

Puede implementar instancias de alto rendimiento de Citrix ADC VPX que utilicen tecnología de virtualización de E/S de raíz única (SR-IOV) en OpenStack.

Puede implementar una instancia de Citrix ADC VPX que utilice la tecnología SR-IOV, en OpenStack, en tres pasos:

- Habilite las funciones virtuales (VF) de SR-IOV en el host.
- Configure y haga que los VF estén disponibles para OpenStack.
- Aprovisione Citrix ADC VPX en OpenStack.

Requisitos previos

Asegúrese de que:

- Agregue la NIC (NIC) Intel 82599 al host.
- Descargue e instale el controlador IXGBE más reciente de Intel.

- Lista de bloques del controlador IXGBEVF del host. Agregue la siguiente entrada en el archivo /etc/modprobe.d/blacklist.conf: Lista de bloques `ixgbevf`

> **Nota**
>
> La versión del `ixgbe` controlador debe ser mínima 5.0.4.

Habilitar las VF SR-IOV en el host

Realice uno de los siguientes pasos para habilitar las VF SR-IOV:

- <number_of_VFs>Si está usando una versión del núcleo anterior a 3.8, agregue la siguiente entrada al archivo /etc/modprobe.d/ixgbe y reinicie el host: Options ixgbe max_vfs=
- Si está usando la versión 3.8 del kernel o posterior, cree VF mediante el siguiente comando:

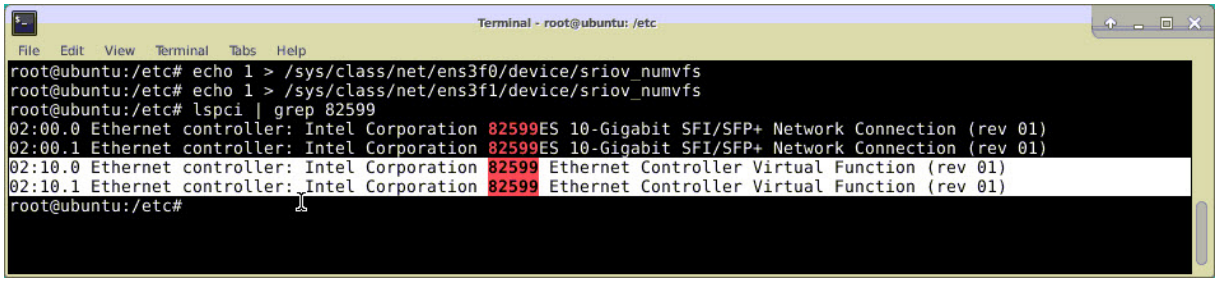
```
1     echo <number_of_VFs> > /sys/class/net/<device_name>/device/
         sriov_numvfs
2 <!--NeedCopy-->
```

Donde:

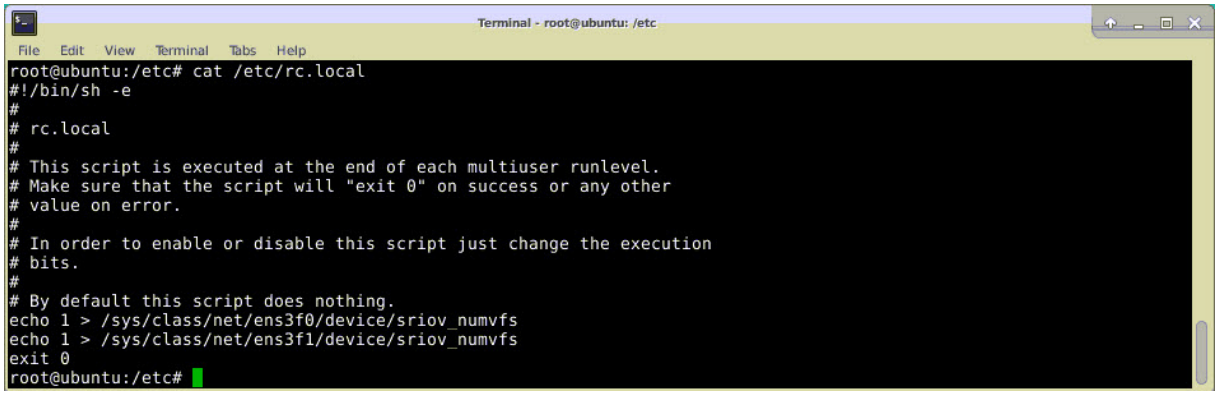
- número_de_vfs es el número de funciones virtuales que quiere crear.
- nombre_dispositivo es el nombre de la interfaz.

> **Importante**
>
> Mientras crea las VFs SR-IOV, asegúrese de no asignar direcciones MAC a las VFs.

Aquí hay un ejemplo de cuatro VF que se están creando.



Haga que los VF sean persistentes, agregue los comandos que utilizó para crear VF al archivo **rc.local**. A continuación se muestra un ejemplo que muestra el contenido del archivo rc.local.



Para obtener más información, consulte esta Guía de configuración de Intel SR-IOV.

Configurar y hacer que los VF estén disponibles para OpenStack

Siga los pasos que se indican en el siguiente enlace para configurar SR-IOV en OpenStack: https://wiki.openstack.org/wiki/SR-IOV-Passthrough-For-Networking.

Aprovisione la instancia Citrix ADC VPX en OpenStack

Puede aprovisionar una instancia Citrix ADC VPX en un entorno OpenStack mediante la CLI de OpenStack.

Aprovisionar una instancia VPX, opcionalmente implica el uso de datos de la unidad de configuración. La unidad de configuración es una unidad de configuración especial que se conecta a la instancia cuando se inicia. Esta unidad de configuración se puede utilizar para pasar información de configuración de red, como la dirección IP de administración, la máscara de red y la puerta de enlace predeterminada, etc. a la instancia antes de configurar la configuración de red de la instancia.

Cuando OpenStack aprovisiona una instancia VPX, primero detecta que la instancia se está iniciando en un entorno OpenStack, leyendo una cadena de BIOS específica (OpenStack Foundation) que indica OpenStack. Para distribuciones de Red Hat Linux, la cadena se almacena en /etc/nova/release. Este es un mecanismo estándar que está disponible en todas las implementaciones de OpenStack basadas en la plataforma de hipervisor KVM. La unidad debe tener una etiqueta OpenStack específica. Si se detecta la unidad de configuración, la instancia intenta leer la siguiente información del nombre de archivo especificado en el comando de `nova` arranque. En los procedimientos siguientes, el archivo se llama “userdata.txt”.

- Dirección IP de administración
- Máscara de red
- Puerta de enlace predeterminada

Una vez que los parámetros se leen correctamente, se rellenan en la pila NetScaler. Esto ayuda a administrar la instancia de forma remota. Si los parámetros no se leen correctamente o la unidad de

configuración no está disponible, la instancia pasa al comportamiento predeterminado, que es:

- La instancia intenta recuperar la información de la dirección IP de DHCP.
- Si DHCP falla o supera el tiempo de espera, la instancia aparece con la configuración de red predeterminada (192.168.100.1/16).

Aprovisione la instancia Citrix ADC VPX en OpenStack a través de CLI

Puede aprovisionar una instancia VPX en un entorno OpenStack mediante la CLI de OpenStack. Este es el resumen de los pasos para aprovisionar una instancia de Citrix ADC VPX en OpenStack:

1. Extracción del `.qcow2` archivo del archivo.tgz
2. Crear una imagen de OpenStack a partir de la imagen qcow2
3. Aprovisionamiento de una instancia VPX

Para aprovisionar una instancia VPX en un entorno OpenStack, siga estos pasos.

1. Extraiga el. `qcow2` del `.tqz` archivo escribiendo el comando:

```
tar xvzf <TAR file>
tar xvzf NSVPX-KVM-12.0-26.2_nc.tgz
NSVPX-KVM.xml
NSVPX-KVM-12.0-26.2_nc.qcow2
<!--NeedCopy-->
```

2. Cree una imagen de OpenStack mediante el `.qcoz2` archivo extraído en el paso 1 escribiendo el siguiente comando:

```
glance image-create --name="<name of the OpenStack image>" --
    property hw_disk_bus=ide --is-public=true --container-format=
    bare --disk-format=qcow2< <name of the qcow2 file>

glance image-create --name="NS-VPX-12-0-26-2" --property
    hw_disk_bus=ide --is-public= true --container-format=bare --
    disk-format=qcow2< NSVPX-KVM-12.0-26.2_nc.qcow2
<!--NeedCopy-->
```

La siguiente ilustración proporciona un ejemplo de salida para el comando glance image-create.

Property	Value
checksum	735dae4ea6e46e39ed3f0acfba02e755
container_format	bare
created_at	2017-02-16T10:03:29Z
disk_format	qcow2
hw_disk_bus	ide
id	aeaa13e9-b49b-411c-ab54-c61820a8e2f3
min_disk	0
min_ram	0
name	NSVPX-KVM-12.0-26.2
owner	06c41a73b32f4b48af55359fd7d3502c
protected	False
size	717946880
status	active
tags	[]
updated_at	2017-02-16T10:03:38Z
virtual_size	None
visibility	private

3. Después de crear una imagen de OpenStack, aprovisione la instancia Citrix ADC VPX.

```
nova boot --image NSVPX-KVM-12.0-26.2 --config-drive=true --
   userdata
./userdata.txt --flavor m1. medium --nic net-id=3b258725-eaae-
455e-a5de-371d6d1f349f --nic port-id=218ba819-9f55-4991-adb6-
02086a6bdee2 NSVPX-10
<!--NeedCopy-->
```

En el comando anterior, userdata.txt es el archivo que contiene detalles como dirección IP, máscara de red y puerta de enlace predeterminada para la instancia VPX. El archivo de datos de usuario es un archivo personalizable por el usuario. NSVPX-KVM-12.0-26.2 es el nombre del dispositivo virtual que desea aprovisionar. —NIC port-id=218ba819-9f55-4991-adb6-02086a6bdee2 es OpenStack VF.

En la siguiente ilustración se muestra un resultado de ejemplo del comando de nova arranque.

Property	Value
OS-DCF:diskConfig	MANUAL
OS-EXT-AZ:availability_zone	
OS-EXT-SRV-ATTR:host	-
OS-EXT-SRV-ATTR:hypervisor_hostname	-
OS-EXT-SRV-ATTR:instance_name	instance-0000003c
OS-EXT-STS:power_state	0
OS-EXT-STS:task_state	scheduling
OS-EXT-STS:vm_state	building
OS-SRV-USG:launched_at	-
OS-SRV-USG:terminated_at	-
accessIPv4	
accessIPv6	
adminPass	43EjPdM5shLz
config_drive	True
created	2017-02-20T11:53:37Z
flavor	m1.medium (3)
hostId	
id	6b9f6968-aab9-463c-b619-d58c73db3187
image	NSVPX-KVM-12.0-26.2 (a5478b8a-8435-48d1-b4a0-1494e2c8f8b1)
key_name	-
metadata	{}
name	NSVPX-10
os-extended-volumes:volumes_attached	[]
progress	0
security_groups	default
status	BUILD
tenant_id	06c41a73b32f4b48af55359fd7d3502c
updated	2017-02-20T11:53:38Z
user_id	418524f7101b4f0389ecbb36da9916b5

En la siguiente ilustración se muestra un ejemplo del archivo userdata.txt. Los valores de las<PropertySection></PropertySection> etiquetas son los valores configurables por el usuario y contienen información como dirección IP, máscara de red y puerta de enlace predeterminada.

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<Environment xmlns:oe="http://schemas.dmtf.org/ovf/environment/1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
oe:id=""
xmlns="http://schemas.dmtf.org/ovf/environment/1">
<PlatformSection>
<Kind>NOVA</Kind>
<Version>2013.1</Version>
<Vendor>Openstack</Vendor>
<Locale>en</Locale>
</PlatformSection>
<PropertySection>
<Property oe:key="com.citrix.netscaler.ovf.version" oe:value="1.0"
   />
<Property oe:key="com.citrix.netscaler.platform" oe:value="vpx"/>
citrix.com 4
<Property oe:key="com.citrix.netscaler.orch_env"
oe:value="openstack-orch-env"/>
```



```
<Property oe:key="com.citrix.netscaler.mgmt.ip"
oe:value="10.1.0.100"/>
<Property oe:key="com.citrix.netscaler.mgmt.netmask"
oe:value="255.255.0.0"/>
<Property oe:key="com.citrix.netscaler.mgmt.gateway"
oe:value="10.1.0.1"/>
</PropertySection>
</Environment>
<!--NeedCopy-->
```

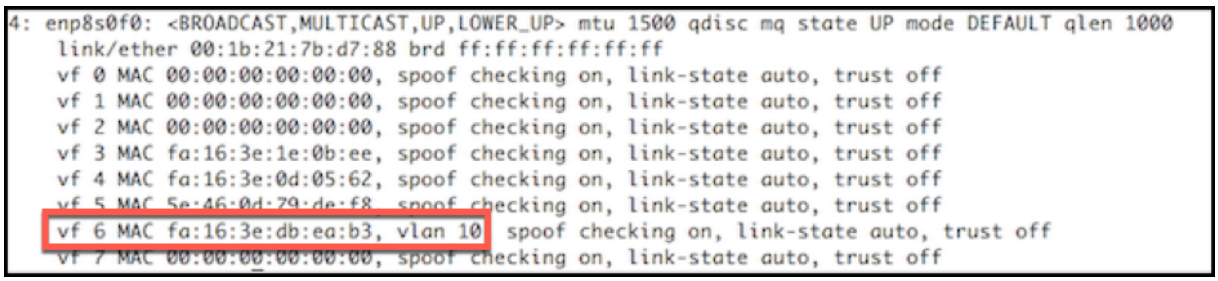
Configuraciones adicionales admitidas: Creación y eliminación de VLAN en VF SR-IOV del host

Escriba el siguiente comando para crear una VLAN en SR-IOV VF:

```
ip link show enp8s0f0 vf 6 vlan 10
```

En el comando anterior, "enp8s0f0" aparece el nombre de la función física.

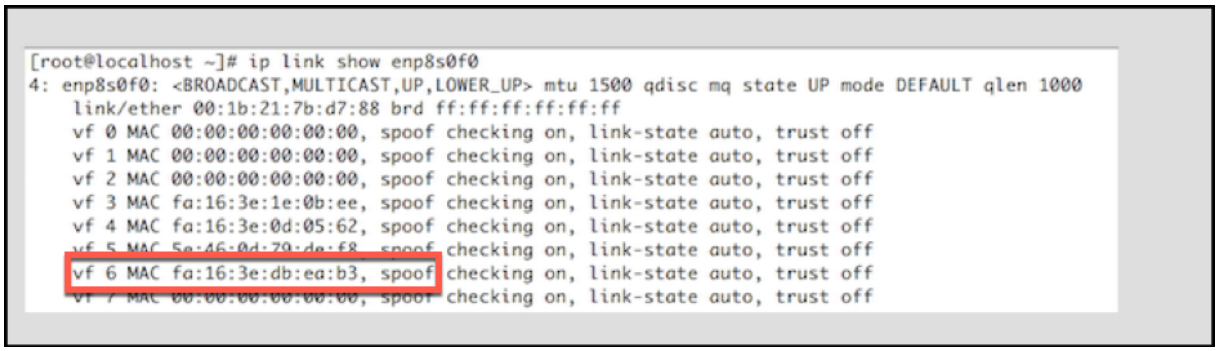
Ejemplo: VLAN 10, creada en vf 6



Escriba el siguiente comando para eliminar una VLAN en la VF SR-IOV:

```
ip link show enp8s0f0 vf 6 vlan 0
```

Ejemplo: VLAN 10, eliminada de vf 6



Estos pasos completan el procedimiento para implementar una instancia de Citrix ADC VPX que utiliza la tecnología SRIOV, en OpenStack.

Configurar una instancia de Citrix ADC VPX en KVM para utilizar interfaces de host basadas en OVS DPDK

August 20, 2021

Puede configurar una instancia de Citrix ADC VPX que se ejecute en KVM (Fedora y RHOS) para utilizar Open vSwitch (OVS) con el Kit de desarrollo de planos de datos (DPDK) para un mejor rendimiento de la red. En este documento se describe cómo configurar la instancia Citrix ADC VPX para que funcione en los `vhost-user` puertos expuestos por OVS-DPDK en el host KVM.

OVS es un conmutador virtual multicapa licenciado bajo la licencia Apache 2.0 de código abierto. DPDK es un conjunto de bibliotecas y controladores para un procesamiento rápido de paquetes.

Las siguientes versiones de Fedora, RHOS, OVS y DPDK están calificadas para configurar una instancia de Citrix ADC VPX:

Fedora	RHOS
Fedora 25	RHOS 7,4
OVS 2.7.0	OVS 2.6.1
DPDK 16.11.12	DPDK 16.11.12

Requisitos previos

Antes de instalar DPDK, asegúrese de que el host tiene páginas enormes de 1 GB.

Para obtener más información, consulte esta documentación de requisitos del sistema de DPDK. A continuación se presenta un resumen de los pasos necesarios para configurar una instancia de Citrix ADC VPX en KVM para utilizar interfaces de host basadas en DPDK de OVS:

- Instale DPDK.
- Construir e instalar OVS.
- Cree un puente OVS.
- Conecte una interfaz física al puente OVS.
- Conecte `vhost-user` puertos a la ruta de datos OVS.
- Aprovisione un KVM-VPX con `vhost-user` puertos basados en OVS-DPDK.

Instalar DPDK

Para instalar DPDK, siga las instrucciones que se dan en este documento Open vSwitch con DPDK .

Crear e instalar OVS

Descargue OVS desde la página de descargasde OVS. A continuación, cree e instale OVS mediante una ruta de datos DPDK. Siga las instrucciones que figuran en el documento Instalación de Open vSwitch .

Para obtener información más detallada, Guía de introducción de DPDK para Linux.

Creación de un puente OVS

Dependiendo de su necesidad, escriba el comando Fedora o RHOS para crear un puente OVS:

Comando de Fedora:

```
> $OVS_DIR/utilities/ovs-vsctl add-br ovs-br0 -- set bridge ovs-br0
   datapath_type=netdev
<!--NeedCopy-->
```

Comando RHOS:

```
ovs-vsctl add-br ovs-br0 -- set bridge ovs-br0 datapath_type=netdev
<!--NeedCopy-->
```

Conecte la interfaz física al puente OVS

Enlace los puertos a DPDK y luego conéctelos al puente OVS escribiendo los siguientes comandos de Fedora o RHOS:

Comando de Fedora:

```
> $OVS_DIR/utilities/ovs-vsctl add-port ovs-br0 dpdk0 -- set Interface
   dpdk0 type=dpdk  options:dpdk-devargs=0000:03:00.0

> $OVS_DIR/utilities/ovs-vsctl add-port ovs-br0 dpdk1 -- set Interface
   dpdk1 type=dpdk  options:dpdk-devargs=0000:03:00.1
<!--NeedCopy-->
```

Comando RHOS:


```
1 ovs-vsctl add-port ovs-br0 dpdk0 -- set Interface dpdk0 type=dpdk
     options:dpdk-devargs=0000:03:00.0
2
3
4 ovs-vsctl add-port ovs-br0 dpdk1 -- set Interface dpdk1 type=dpdk
     options:dpdk-devargs=0000:03:00.1
5 <!--NeedCopy-->
```

El `dpdk-devargs` mostrado como parte de las opciones especifica el PCI BDF de la NIC física respectiva.

Adjuntar `vhost-user` puertos a la ruta de datos OVS

Escriba los siguientes comandos de Fedora o RHOS para conectar `vhost-user` puertos a la ruta de datos OVS:

Comando de Fedora:

```
1 > $OVS_DIR/utilities/ovs-vsctl add-port ovs-br0 vhost-user1 -- set
     Interface vhost-user1 type=dpdkvhostuser -- set Interface vhost-
     user1  mtu_request=9000
2
3 > $OVS_DIR/utilities/ovs-vsctl add-port ovs-br0 vhost-user2 -- set
     Interface vhost-user2 type=dpdkvhostuser -- set Interface vhost-
     user2  mtu_request=9000
4
5 chmod g+w  /usr/local/var/run/openvswitch/vhost*
6 <!--NeedCopy-->
```

Comando RHOS:

```
1 ovs-vsctl add-port ovs-br0 vhost-user1 -- set Interface vhost-user1
     type=dpdkvhostuser -- set Interface vhost-user1  mtu_request=9000
2
3 ovs-vsctl add-port ovs-br0 vhost-user2 -- set Interface vhost-user2
     type=dpdkvhostuser -- set Interface vhost-user2  mtu_request=9000
4
5 chmod g+w /var/run/openvswitch/vhost*
6 <!--NeedCopy-->
```


Aprovisionamiento de un KVM-VPX con `vhost-user` puertos basados en OVS-DPDK

Puede aprovisionar una instancia VPX en KVM de Fedora con `vhost-user` puertos basados en OVS-DPDK solo desde la CLI mediante los siguientes comandos QEMU:
comando Fedora:

```
qemu-system-x86_64 -name KVM-VPX -cpu host -enable-kvm -m 4096M \

-object memory-backend-file,id=mem,size=4096M,mem-path=/dev/hugepages,
   share=on -numa node,memdev=mem \

-mem-prealloc -smp sockets=1,cores=2 -drive file=<absolute-path-to-disc
   -image-file>,if=none,id=drive-ide0-0-0,format=<disc-image-format> \

-device ide-drive,bus=ide.0,unit=0,drive=drive-ide0-0-0,id=ide0-0-0,
   bootindex=1 \

-netdev type=tap,id=hostnet0,script=no,downscript=no,vhost=on \

-device virtio-net-pci,netdev=hostnet0,id=net0,mac=52:54:00:3c:d1:ae,
   bus=pci.0,addr=0x3 \

-chardev socket,id=char0,path=</usr/local/var/run/openvswitch/vhost-
   user1> \

-netdev type=vhost-user,id=mynet1,chardev=char0,vhostforce -device
   virtio-net-pci,mac=00:00:00:00:00:01,netdev=mynet1,mrg_rxbuf=on \

-chardev socket,id=char1,path=</usr/local/var/run/openvswitch/vhost-
   user2> \

-netdev type=vhost-user,id=mynet2,chardev=char1,vhostforce -device
   virtio-net

pci,mac=00:00:00:00:00:02,netdev=mynet2,mrg_rxbuf=on \

--nographic
<!--NeedCopy-->
```

Para RHOS, utilice el siguiente archivo XML de ejemplo para aprovisionar la instancia Citrix ADC VPX, mediante `virsh`.


```
<domain type='kvm'>

  <name>dpdk-vpx1</name>

  <uuid>aedb844b-f6bc-48e6-a4c6-36577f2d68d6</uuid>

  <memory unit='KiB'>16777216</memory>

  <currentMemory unit='KiB'>16777216</currentMemory>

  <memoryBacking>

    <hugepages>

      <page size='1048576' unit='KiB'/>

    </hugepages>

  </memoryBacking>

  <vcpu placement='static'>6</vcpu>

  <cputune>

    <shares>4096</shares>

    <vcpupin vcpu='0' cpuset='0'/>

    <vcpupin vcpu='1' cpuset='2'/>

    <vcpupin vcpu='2' cpuset='4'/>

    <vcpupin vcpu='3' cpuset='6'/>

    <emulatorpin cpuset='0,2,4,6'/>

  </cputune>

  <numatune>

    <memory mode='strict' nodeset='0'/>

  </numatune>

  <resource>
```



```
46
47      <partition>/machine</partition>
48
49    </resource>
50
51    <os>
52
53      <type arch='x86_64' machine='pc-i440fx-rhel7.0.0'>hvm</type>
54
55      <boot dev='hd'/>
56
57    </os>
58
59    <features>
60
61      <acpi/>
62
63      <apic/>
64
65    </features>
66
67    <cpu mode='custom' match='minimum' check='full'>
68
69      <model fallback='allow'>Haswell-noTSX</model>
70
71      <vendor>Intel</vendor>
72
73      <topology sockets='1' cores='6' threads='1'/>
74
75      <feature policy='require' name='ss'/>
76
77      <feature policy='require' name='pcid'/>
78
79      <feature policy='require' name='hypervisor'/>
80
81      <feature policy='require' name='arat'/>
82
83  <domain type='kvm'>
84
85    <name>dpdk-vpx1</name>
86
87    <uuid>aedb844b-f6bc-48e6-a4c6-36577f2d68d6</uuid>
88
89    <memory unit='KiB'>16777216</memory>
90
```



```
<currentMemory unit='KiB'>16777216</currentMemory>

<memoryBacking>

  <hugepages>

    <page size='1048576' unit='KiB'/>

  </hugepages>

</memoryBacking>

<vcpu placement='static'>6</vcpu>

<cputune>

  <shares>4096</shares>

  <vcpupin vcpu='0' cpuset='0'/>

  <vcpupin vcpu='1' cpuset='2'/>

  <vcpupin vcpu='2' cpuset='4'/>

  <vcpupin vcpu='3' cpuset='6'/>

  <emulatorpin cpuset='0,2,4,6'/>

</cputune>

<numatune>

  <memory mode='strict' nodeset='0'/>

</numatune>

<resource>

  <partition>/machine</partition>

</resource>

<os>

  <type arch='x86_64' machine='pc-i440fx-rhel7.0.0'>hvm</type>
```



```
136
137       <boot dev='hd'/>
138
139     </os>
140
141     <features>
142
143       <acpi/>
144
145       <apic/>
146
147     </features>
148
149     <cpu mode='custom' match='minimum' check='full'>
150
151       <model fallback='allow'>Haswell-noTSX</model>
152
153       <vendor>Intel</vendor>
154
155       <topology sockets='1' cores='6' threads='1'/>
156
157       <feature policy='require' name='ss'/>
158
159       <feature policy='require' name='pcid'/>
160
161       <feature policy='require' name='hypervisor'/>
162
163       <feature policy='require' name='arat'/>
164
165       <feature policy='require' name='tsc_adjust'/>
166
167       <feature policy='require' name='xsaveopt'/>
168
169       <feature policy='require' name='pdpe1gb'/>
170
171       <numa>
172
173         <cell id='0' cpus='0-5' memory='16777216' unit='KiB' memAccess='
              shared'/>
174
175       </numa>
176
177     </cpu>
178
179     <clock offset='utc'/>
```



```
180
181   <on_poweroff>destroy</on_poweroff>
182
183   <on_reboot>restart</on_reboot>
184
185   <on_crash>destroy</on_crash>
186
187   <devices>
188
189     <emulator>/usr/libexec/qemu-kvm</emulator>
190
191     <disk type='file' device='disk'>
192
193       <driver name='qemu' type='qcow2' cache='none'/>
194
195       <source file='/home/NSVPX-KVM-12.0-52.18_nc.qcow2'/>
196
197       <target dev='vda' bus='virtio'/>
198
199       <address type='pci' domain='0x0000' bus='0x00' slot='0x07'
              function='0x0'/>
200
201     </disk>
202
203     <controller type='ide' index='0'>
204
205       <address type='pci' domain='0x0000' bus='0x00' slot='0x01'
              function='0x1'/>
206
207     </controller>
208
209     <controller type='usb' index='0' model='piix3-uhci'>
210
211       <address type='pci' domain='0x0000' bus='0x00' slot='0x01'
              function='0x2'/>
212
213     </controller>
214
215     <controller type='pci' index='0' model='pci-root'/>
216
217     <interface type='direct'>
218
219       <mac address='52:54:00:bb:ac:05'/>
220
221       <source dev='enp129s0f0' mode='bridge'/>
```



```
222
223         <model type='virtio'/>
224
225         <address type='pci' domain='0x0000' bus='0x00' slot='0x03'
               function='0x0'/>
226
227       </interface>
228
229       <interface type='vhostuser'>
230
231         <mac address='52:54:00:55:55:56'/>
232
233         <source type='unix' path='/var/run/openvswitch/vhost-user1' mode=
               'client'/>
234
235         <model type='virtio'/>
236
237         <address type='pci' domain='0x0000' bus='0x00' slot='0x04'
               function='0x0'/>
238
239       </interface>
240
241       <interface type='vhostuser'>
242
243         <mac address='52:54:00:2a:32:64'/>
244
245         <source type='unix' path='/var/run/openvswitch/vhost-user2' mode=
               'client'/>
246
247         <model type='virtio'/>
248
249         <address type='pci' domain='0x0000' bus='0x00' slot='0x05'
               function='0x0'/>
250
251       </interface>
252
253       <interface type='vhostuser'>
254
255         <mac address='52:54:00:2a:32:74'/>
256
257         <source type='unix' path='/var/run/openvswitch/vhost-user3' mode=
               'client'/>
258
259         <model type='virtio'/>
260
```



```
261         <address type='pci' domain='0x0000' bus='0x00' slot='0x06'
               function='0x0'/>
262
263       </interface>
264
265       <interface type='vhostuser'>
266
267         <mac address='52:54:00:2a:32:84'/>
268
269         <source type='unix' path='/var/run/openvswitch/vhost-user4' mode=
               'client'/>
270
271        <model type='virtio'/>
272
273         <address type='pci' domain='0x0000' bus='0x00' slot='0x09'
               function='0x0'/>
274
275       </interface>
276
277       <serial type='pty'>
278
279         <target port='0'/>
280
281       </serial>
282
283       <console type='pty'>
284
285         <target type='serial' port='0'/>
286
287       </console>
288
289       <input type='mouse' bus='ps2'/>
290
291       <input type='keyboard' bus='ps2'/>
292
293       <graphics type='vnc' port='-1' autoport='yes'>
294
295         <listen type='address'/>
296
297       </graphics>
298
299       <video>
300
301         <model type='cirrus' vram='16384' heads='1' primary='yes'/>
302
```



```
303         <address type='pci' domain='0x0000' bus='0x00' slot='0x02'
               function='0x0'/>
304
305       </video>
306
307       <memballoon model='virtio'>
308
309         <address type='pci' domain='0x0000' bus='0x00' slot='0x08'
               function='0x0'/>
310
311       </memballoon>
312
313     </devices>
314
315 </domain
316 <!--NeedCopy-->
```

Puntos a tener en cuenta

En el archivo XML, el hugepage tamaño debe ser de 1 GB, como se muestra en el archivo de ejemplo.

```
1 <memoryBacking>
2
3     <hugepages>
4
5       <page size='1048576' unit='KiB'/>
6
7     </hugepages>
8 <!--NeedCopy-->
```

Además, en el archivo de ejemplo vhost-user1 está el puerto de vhost usuario vinculado a ovs-br0.

```
1 <interface type='vhostuser'>
2
3       <mac address='52:54:00:55:55:56'/>
4
5       <source type='unix' path='/var/run/openvswitch/vhost-user1' mode=
           'client'/>
6
7       <model type='virtio'/>
8
```



```
9         <address type='pci' domain='0x0000' bus='0x00' slot='0x04'
              function='0x0'/>
10
11      </interface>
12  <!--NeedCopy-->
```

Para abrir la instancia Citrix ADC VPX, empiece a utilizar el `virsh` comando.

Aplique las configuraciones de Citrix ADC VPX en el primer arranque del dispositivo Citrix ADC en el hipervisor KVM

March 9, 2022

Puede aplicar las configuraciones de Citrix ADC VPX en el hipervisor KVM durante el primer arranque del dispositivo Citrix ADC. Por lo tanto, la configuración de un cliente en una instancia VPX se puede configurar en mucho menos tiempo.

Para obtener más información sobre los datos de usuario de prearranque y su formato, consulte Aplicar configuraciones de Citrix ADC VPX en el primer arranque del dispositivo Citrix ADC en la nube.

> Nota:
>
> Para arrancar utilizando los datos de usuario de prearranque en el hipervisor KVM, la configuración de puerta de enlace predeterminada debe pasarse en la sección <NS-CONFIG>. Para obtener más información sobre el contenido de la etiqueta <NS-CONFIG>, consulte esta sección <NS-CONFIG> de ejemplo.

<NS-CONFIG> Sección de muestra:

```
1  <NS-PRE-BOOT-CONFIG>
2
3      <NS-CONFIG>
4          add route 0.0.0.0 0.0.0.0  10.102.38.1
5      </NS-CONFIG>
6
7      <NS-BOOTSTRAP>
8              <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
9              <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>
10
11         <MGMT-INTERFACE-CONFIG>
12                 <INTERFACE-NUM> eth0 </INTERFACE-NUM>
13                 <IP> 10.102.38.216 </IP>
```



```
                <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
        </MGMT-INTERFACE-CONFIG>
    </NS-BOOTSTRAP>

</NS-PRE-BOOT-CONFIG>
<!--NeedCopy-->
```

Cómo proporcionar datos de usuario previos al arranque en el hipervisor KVM

Puede proporcionar datos de usuario de prearranque en el hipervisor KVM a través de un archivo ISO, que se adjunta mediante un dispositivo CDROM.

Proporcionar datos de usuario mediante un archivo ISO de CDROM

Puede usar Virtual Machine Manager (VMM) para inyectar datos de usuario en la máquina virtual (VM) como una imagen ISO mediante el dispositivo CDROM. KVM admite CD-ROM en VM Guest, ya sea accediendo directamente a una unidad física en el servidor host de VM o accediendo a imágenes ISO.

Los siguientes pasos le permiten proporcionar datos de usuario mediante el archivo ISO de CDROM:

1. Cree un archivo con un nombre de archivo `userdata` que contenga el contenido de datos de usuario antes del arranque.

   > Nota: El nombre del archivo debe usarse estrictamente como `userdata`.

2. Guarde el archivo `userdata` en una carpeta y cree una imagen ISO con la carpeta.

   Puede crear una imagen ISO con un archivo `userdata` mediante los dos métodos siguientes:

   - Usar cualquier herramienta de procesamiento de imágenes, como PowerISO.
   - Mediante comandos `mkisofs` en Linux.

   La siguiente configuración de ejemplo muestra cómo generar una imagen ISO con el comando `mkisofs` en Linux.

```
root@ubuntu:~/sai/19oct# ls -lh
total 4.0K
-rw-r--r-- 1 root root 1.1K Oct 19 16:25 userdata
root@ubuntu:~/sai/19oct#
root@ubuntu:~/sai/19oct# mkisofs -o kvm-userdata.iso userdata
I: -input-charset not specified, using utf-8 (detected in locale
    settings)
Total translation table size: 0
Total rockridge attributes bytes: 0
```



```
Total directory bytes: 0
Path table size(bytes): 10
Max brk space used 0
175 extents written (0 MB)
root@ubuntu:~/sai/19oct#
root@ubuntu:~/sai/19oct# ls -lh
total 356K
-rw-r--r-- 1 root root 350K Oct 19 16:25 kvm-userdata.iso
-rw-r--r-- 1 root root 1.1K Oct 19 16:25 userdata
<!--NeedCopy-->
```

3. Aprovisione la instancia de Citrix ADC VPX mediante el proceso de implementación estándar para crear la VM. Pero no encienda la VM automáticamente.
4. Agregue un dispositivo de CD-ROM con Virtual Machine Manager mediante los siguientes pasos:
   a) Haga doble clic en una entrada de VM Guest en Virtual Machine Manager para abrir su consola y cambiar a la vista Detalles con **Ver > Detalles**.
   b) Haga clic en **Agregar hardware > Almacenamiento > Tipo de dispositivo > Dispositivo CDROM**.
   c) Haga clic en **Administrar**, seleccione el archivo ISO correcto y haga clic en **Finalizar**. Se crea un nuevo CDROM en **Recursos** en la instancia de Citrix ADC VPX.
5. Encienda la máquina virtual.

Citrix ADC VPX en AWS

April 5, 2022

Puede lanzar una instancia de Citrix ADC VPX en Amazon Web Services (AWS). El dispositivo Citrix ADC VPX está disponible como Amazon Machine Image (AMI) en el mercado de AWS. Una instancia Citrix ADC VPX en AWS le permite utilizar las capacidades de computación en la nube de AWS y utilizar las funciones de equilibrio de carga y administración de tráfico de Citrix ADC para sus necesidades empresariales. La instancia VPX admite todas las funciones de administración del tráfico de un dispositivo Citrix ADC físico, y se puede implementar como instancias independientes o en pares de alta disponibilidad. Para obtener más información sobre las funciones de VPX, consulte la hoja de datos de VPX.

Introducción

Antes de empezar con la implementación de VPX, debe estar familiarizado con la siguiente información:

- Terminología de AWS

- Tabla de compatibilidad de AWS-VPX
- Limitaciones y directrices de uso
- Requisitos previos
- Cómo funciona una instancia de Citrix ADC VPX en AWS

Implementar una instancia de Citrix ADC VPX en AWS

En AWS, se admiten los siguientes tipos de implementación para las instancias VPX:

- Independiente
- Alta disponibilidad (activo-pasivo)
  - Alta disponibilidad dentro de la misma zona
  - Alta disponibilidad en diferentes zonas mediante Elastic IP
  - Alta disponibilidad en diferentes zonas mediante IP privada
- GSLB activo-activo
- Escalado automático (activo-activo) mediante ADM

Implementaciones híbridas

- Implementación de Citrix ADC en AWS Outpost
- Implementación de Citrix ADC en VMC en AWS

Licencias

Una instancia de Citrix ADC VPX en AWS requiere una licencia. Las siguientes opciones de licencia están disponibles para las instancias de Citrix ADC VPX que se ejecutan en AWS:

- Gratis (ilimitado)
- Cada hora
- Anual
- BYOL
- Prueba gratuita (todas las ofertas de suscripción a Citrix ADC VPX-AWS durante 21 días gratis en el mercado de AWS).

Automatización

- Citrix ADM: implementación inteligente
- Inicio rápido de AWS: Citrix ADC VPX para aplicaciones web en AWS
- CFT de GitHub: plantillas y scripts de Citrix ADC para la implementación de AWS
- GitHub Ansible: plantillas y scripts de Citrix ADC para la implementación de AWS

- GitHub Terraform: plantillas y scripts de Citrix ADC para la implementación de AWS
- Biblioteca de patrones de AWS (PL): Citrix ADC VPX

Entradas de blog

- Cómo Citrix ADC en AWS ayuda a los clientes a entregar aplicaciones de forma segura
- Entrega de aplicaciones en la nube híbrida con Citrix ADC y AWS
- Citrix es socio competente en redes de AWS
- Citrix ADC: siempre preparado para las nubes públicas
- Escale o amplíe fácilmente en nubes públicas a través de Citrix ADC
- Citrix amplía las opciones de implementación de ADC con AWS Outposts
- Uso de Citrix ADC con redirección de entrada de Amazon VPC
- Citrix ofrece opciones, rendimiento e implementación simplificada en AWS
- La seguridad de Citrix Web App Firewall, ahora en AWS Marketplace
- Cómo Aria Systems usa Citrix Web App Firewall en AWS

Vídeos

- Simplificación de las implementaciones de Citrix ADC en la nube pública a través de ADM
- Aprovisionamiento y configuración de Citrix ADC VPX en AWS mediante scripts de terraform listos para usar
- Implementación de Citrix ADC HA en AWS mediante la plantilla de CloudFormation
- Implemente Citrix ADC HA en las zonas de disponibilidad mediante AWS QuickStart
- Cómo implementar Citrix ADC en AWS
- Citrix ADC Autoscale mediante ADM
- Citrix ADC admite el escalado automático de servidores back-end en AWS o el grupo de AWS Autoscaling

Estudios de casos de clientes

- Solución tecnológica - Xenit AB
- Una mejor manera de hacer negocios con Citrix y la nube de AWS — Aria
- Descubra las ventajas de Citrix ADC y AWS
- Rain for Rent - Historia de cliente

Soluciones

- Implementar una plataforma de publicidad digital en AWS con Citrix ADC
- Mejorar el análisis de Clickstream en AWS con Citrix ADC

Asistencia

- Abrir un caso de asistencia
- Para obtener información sobre la oferta de suscripción de Citrix ADC, consulte Solución de problemas de una instancia VPX en AWS. Para presentar un caso de asistencia técnica, busque el número de cuenta de AWS y el código PIN de asistencia, y llame al servicio de asistencia de Citrix.
- Para la oferta con licencia del cliente de Citrix ADC o BYOL, asegúrese de tener el acuerdo de asistencia y mantenimiento válido. Si no tiene un acuerdo, póngase en contacto con su representante de Citrix.

Referencias adicionales

- Seminario web bajo demanda de AWS: Citrix ADC en AWS
- Guías de implementación de Citrix ADC VPX en AWS
- Creación de una Amazon Machine Image VPX (AMI) en SC2S/región secreta
- Citrix ADC en AWS
- Diseño de referencia validado de Citrix ADC y AWS
- Hoja de datos de Citrix ADC VPX
- Citrix ADC en AWS Marketplace
- Citrix ADC forma parte de las soluciones de socios de redes de AWS (balanceadores de carga)
- Citrix ADC para VMware cloud on AWS
- Preguntas frecuentes sobre AWS

Terminología de AWS

August 20, 2021

En esta sección se describe la lista de términos y frases de AWS de uso común. Para obtener más información, consulte Glosario de AWS.

Término	Definición
Imagen de máquina de Amazon (AMI)	Imagen de máquina, que proporciona la información necesaria para iniciar una instancia, que es un servidor virtual en la nube.
Elastic Block Store	Proporciona volúmenes de almacenamiento de bloques persistentes para su uso con instancias de Amazon EC2 en la nube de AWS.
Servicio de almacenamiento simple (S3)	Almacenamiento para Internet. Está diseñado para que la informática a escala web sea más fácil para los desarrolladores.
Elastic Compute Cloud (EC2)	Un servicio web que proporciona una capacidad informática segura y de tamaño variable en la nube. Está diseñado para que la informática en la nube a escala web sea más fácil para los desarrolladores.
Elastic Load Balancing (ELB)	Distribuye el tráfico de aplicaciones entrantes en varias instancias de EC2, en varias zonas de disponibilidad. Esto aumenta la tolerancia a fallos de sus aplicaciones.
Interfaz de red elástica (ENI)	Interfaz de red virtual que puede adjuntar a una instancia en una nube privada virtual (VPC).
Dirección IP elástica (EIP)	Dirección IPv4 pública y estática que ha asignado en Amazon EC2 o Amazon VPC y que, a continuación, se adjunta a una instancia. Las direcciones IP elásticas están asociadas a su cuenta, no a una instancia específica. Son elásticas porque puede asignarlos, conectarlos, separarlos y liberarlos fácilmente a medida que cambien tus necesidades.

Término	Definición
Tipo de instancia	Amazon EC2 ofrece una amplia selección de tipos de instancia optimizados para adaptarse a diferentes casos de uso. Los tipos de instancia comprenden diversas combinaciones de CPU, memoria, almacenamiento y capacidad de red, y le ofrecen la flexibilidad de elegir la combinación adecuada de recursos para sus aplicaciones.
Identity and Access Management (IAM)	Una identidad de AWS con directivas de permisos que determinan lo que la identidad puede y no puede hacer en AWS. Puede utilizar un rol de IAM para permitir que las aplicaciones que se ejecutan en una instancia de EC2 accedan de forma segura a los recursos de AWS. El rol de IAM es necesario para implementar instancias VPX en una configuración de alta disponibilidad.
Puerta de enlace de Internet	Conecta una red a Internet. Puede enrutar el tráfico de direcciones IP fuera de la VPC a la Gateway de Internet.
Par de llaves	Conjunto de credenciales de seguridad que utiliza para demostrar su identidad electrónicamente. Un par de claves consiste en una clave privada y una clave pública.
Tablas de redirecciones	Conjunto de reglas de redirección que controla el tráfico que sale de cualquier subred asociada a la tabla de redirecciones. Puede asociar varias subredes a una sola tabla de redirecciones, pero una subred solo puede asociarse a una tabla de redirecciones a la vez.
Grupos de seguridad	Conjunto con nombre asignado de conexiones de red entrantes permitidas para una instancia.

Término	Definición
Subredes	Segmento del intervalo de direcciones IP de una VPC al que se pueden conectar instancias EC2. Puede crear subredes para agrupar instancias de acuerdo con las necesidades operativas y de seguridad.
Nube privada virtual (VPC)	Un servicio web para Provisioning una sección aislada lógicamente de la nube de AWS donde puede lanzar recursos de AWS en una red virtual que defina.
Escalado automático	Servicio web para iniciar o finalizar instancias de Amazon EC2 automáticamente en función de directivas, programaciones y comprobaciones de estado definidas por el usuario.
CloudFormation	Un servicio para escribir o cambiar plantillas que crean y eliminan recursos relacionados de AWS juntos como una unidad.

Tabla de compatibilidad de VPX-AWS

December 2, 2021

En las siguientes tablas se enumeran el modelo VPX y las regiones, los tipos de instancias y los servicios de AWS admitidos.

Tabla 1: Modelos VPX compatibles en AWS

Modelo VPX compatible
Citrix ADC VPX Standard/Advanced/Premium Edition: 200 Mbps
Citrix ADC VPX Standard/Advanced/Premium Edition: 1000 Mbps
Citrix ADC VPX Standard/Advanced/Premium Edition: 3 Gbps
Citrix ADC VPX Standard/Advanced/Premium Edition: 5 Gbps
Citrix ADC VPX Standard/Advanced/Premium: 10 Mbps
Citrix ADC VPX Express: 20 Mbps

Modelo VPX compatible
Citrix ADC VPX: licencia del cliente
Citrix ADC (anteriormente NetScaler) VPX FIPS: licencia del cliente

Tabla: 2 regiones de AWS compatibles

Regiones de AWS admitidas
Región EE.UU. Oeste (Oregón)
Región EE.UU. Oeste (Norte de California)
Región EE.UU. Este (Ohio)
Región EE.UU. Este (Virginia del Norte)
Región de Asia Pacífico (Mumbai)
Región de Asia Pacífico (Seúl)
Región de Canadá (Central)
Región Asia-Pacífico (Singapur)
Región Asia-Pacífico (Sídney)
Región de Asia Pacífico (Tokio)
Región de Asia Pacífico (Hong Kong)
Región de Canadá (Central)
Región de China (Pekín)
Región de China (Ningxia)
Región de la UE (Frankfurt)
Región de la UE (Irlanda)
Región de la UE (Londres)
Región de la UE (París)
Región de la UE (Milán)
Región de América del Sur (São Paulo)
Región de AWS GovCloud (EE. UU.)
Región de AWS GovCloud (EE. UU. Oeste)
Región de alto secreto (C2S) de AWS

Regiones de AWS admitidas
Región de Oriente Medio (Bahréin)
África (Ciudad del Cabo)
C2S

Tabla 3: tipos de instancias de AWS compatibles

Tipos de instancia de AWS admitidos
t2.medium, t2.large, t2.x grande, t2.2x grande
m3.large, m3.x grande, m3,2x grande
c4.large, c4.large, c4,2x grande, c4,4 x grande, c4,8 x grande
m4.large, m4.large, m4,2x grande, m4,4 x grande, m4,10 x grande
m5.large, m5.x grande, m5,2 x grande, m5,4 x grande, m5,12 x grande, m5,24 x grande
c5.large, c5.x grande, c5,2 x grande, c5,4 x grande, c5,9 x grande, c5,18 x grande, c5,24 x grande
C5n.grande, C5n.x grande, C5n.2 x grande, C5n.4x grande, C5n.9x grande, C5n.18 x grande
D2.x grande, D2,2x grande, D2,4 x grande, D2,8 x grande
m5a.large, m5a.xlarge, m5a.2xlarge, m5a.8xlarge, m5a.12xlarge, m5a.16xlarge, m5a.24xlarge
t3a.medium, t3a.large, t3a.xlarge, t3a.2xlarge

Tabla 4: Servicios de AWS admitidos

Servicios de AWS compatibles
EC2: lanza instancias de ADC.
Lambda: invoca las API NITRO de Citrix ADC VPX durante el aprovisionamiento de instancias de Citrix ADC VPX desde CFT.
Redirección de entrada de VPC y VPC: VPC crea redes aisladas en las que se puede iniciar ADC. La redirección de entrada de VPC se utiliza en la solución de equilibrio de carga del firewall.
Route53: distribuye el tráfico entre todos los nodos VPX de ADC de la solución Citrix ADC Autoscale.
ELB: distribuye el tráfico en todos los nodos VPX de ADC de la solución Citrix ADC Autoscale.
Cloudwatch: supervisa el rendimiento y los parámetros del sistema para la instancia de Citrix ADC VPX.

Servicios de AWS compatibles
AWS Autoscaling: se utiliza para el escalado automático de servidores back-end.
Formación en la nube: las plantillas de CloudFormation se utilizan para implementar instancias de Citrix ADC VPX.
Servicio de cola simple (SQS): supervisa los eventos de escalado hacia arriba y hacia abajo en el escalado automático de back-end.
Servicio de notificación simple (SNS): supervisa los eventos de escalado hacia arriba y hacia abajo en el escalado automático de back-end.
Administración de identidades y accesos (IAM): proporciona acceso a los servicios y recursos de AWS.
AWS Outposts: aprovisiones de instancias de Citrix ADC VPX en AWS Outposts.

Citrix recomienda los siguientes tipos de instancias de AWS:

- Series M5 y C5n para ediciones de mercado o licencias de grupos basadas en ancho de banda.
- Serie C5n para licencias de grupos basados en vCPU.

Oferta de VPX en el mercado de AWS	Recomendación de instancia de AWS
VPX 10, VPX Express 20, VPX 200	M5.xLarge
VPX 1000, VPX 3G, VPX 5G	M5.2xLarge

Citrix recomienda los siguientes tipos de instancias de AWS en función del rendimiento.

VPX con licencias agrupadas (licencias de ancho de banda)	Recomendación de instancia de AWS
VPX 8 G	C5n.4xLarge
VPX 10 G, VPX 15 G, VPX 25 G	C5n.9xLarge

> Nota:
>
> La oferta VPX 25G no proporciona el rendimiento deseado de 25 G en AWS, pero puede ofrecer una tasa de transacciones SSL más alta.

Para lograr un rendimiento superior a 5G, haga lo siguiente:

- Elija **Citrix ADC VPX: oferta con licencia de cliente (BYOL)** en el mercado de AWS.

- Seleccione Licencias **agrupadas (licencias de ancho de banda)** en la GUI o la CLI de Citrix ADC.

Para determinar su instancia en función de diferentes métricas, como paquetes por segundo, tasa de transacciones SSL, comuníquese con su contacto de Citrix para obtener orientación. Para obtener información sobre licencias y tamaños de grupos basados en vCPU, contacte con Citrix Support.

Limitaciones y directrices de uso

August 20, 2021

Las siguientes limitaciones y directrices de uso se aplican al implementar una instancia de Citrix ADC VPX en AWS:

- Antes de comenzar, lea la sección terminología de AWS en Implementación de una instancia Citrix ADC VPX en AWS.
- La función de agrupación de clústeres no es compatible con VPX.
- Para que la configuración de alta disponibilidad funcione eficazmente, asocie un dispositivo NAT dedicado a la interfaz de administración o asocie EIP a NSIP. Para obtener más información sobre NAT, en la documentación de AWS, consulte Instancias NAT.
- El tráfico de datos y el tráfico de administración deben estar segregados con ENIs pertenecientes a diferentes subredes.
- Solo la dirección NSIP debe estar presente en el ENI de gestión.
- Si se utiliza una instancia de NAT para la seguridad en lugar de asignar un EIP al NSIP, se requieren cambios de redirección de nivel de VPC adecuados. Para obtener instrucciones sobre cómo realizar cambios de redirección a nivel de VPC, en la documentación de AWS, consulte Caso 2: VPC con subredes públicas y privadas.
- Una instancia VPX se puede mover de un tipo de instancia EC2 a otro (por ejemplo, de m3.large a m3.xlarge).
- Para las opciones de almacenamiento para VPX en AWS, Citrix recomienda EBS, porque es duradero y los datos están disponibles incluso después de separarlos de la instancia.
- No se admite la adición dinámica de ENIs a VPX. Reinicie la instancia VPX para aplicar la actualización. Citrix recomienda detener la instancia independiente o de alta disponibilidad, conectar la nueva ENI y reiniciar la instancia.
- Puede asignar varias direcciones IP a un ENI. El número máximo de direcciones IP por ENI viene determinado por el tipo de instancia EC2; consulte la sección “Direcciones IP por interfaz de red por tipo de instancia” en Interfaces de red elásticas. Debe asignar las direcciones IP en AWS antes de asignarlas a ENI. Para obtener más información, consulte Interfaces de red elásticas.

- Citrix recomienda evitar el uso de los comandos enable and disable interface en las interfaces Citrix ADC VPX.
- Los comandos `set ha node \<NODE\\_ID\> -haStatus STAYPRIMARY` y `set ha node \<NODE\\_ID\> -haStatus STAYSECONDARY` de Citrix ADC están inhabilitados de forma predeterminada.
- IPv6 no es compatible con VPX.
- Debido a las limitaciones de AWS, estas funciones no son compatibles:
  - ARP gratuito (GARP)
  - Modo L2
  - VLAN etiquetada
  - Redirección dinámica
  - MAC virtual
- Para que RNAT funcione, asegúrese de que la **comprobación de origen/destino** esté inhabilitada. Para obtener más información, consulte "Cambio de la comprobación de origen/destino" en Elastic Network Interfaces.
- En una implementación de Citrix ADC VPX en AWS, en algunas regiones de AWS, es posible que la infraestructura de AWS no pueda resolver llamadas a la API de AWS. Esto sucede si las llamadas a la API se emiten a través de una interfaz de no administración en la instancia de Citrix ADC VPX.
  Como solución alternativa, restrinja las llamadas a la API únicamente a la interfaz de administración. Para ello, cree una NSVLAN en la instancia VPX y vincule la interfaz de administración a la NSVLAN mediante el comando apropiado.
  Por ejemplo:
  ```
  set ns config -nsvlan <vlan id> -ifnum 1/1 -tagged NO
  save config
  ```
  Reinicie la instancia VPX en la solicitud. Para obtener más información sobre la configuración `nsvlan`, consulte Configuración de NSVLAN.
- En la consola de AWS, el uso de vCPU mostrado para una instancia VPX en la ficha **Supervisión** puede ser alto (hasta el 100 por ciento), incluso cuando el uso real sea mucho menor. Para ver el uso real de vCPU, vaya a **Ver todas las métricas de CloudWatch**. Para obtener más información, consulte Supervisar las instancias mediante Amazon CloudWatch.

Requisitos previos

July 15, 2022

Antes de intentar crear una instancia VPX en AWS, asegúrese de tener lo siguiente:

- **Una cuenta de AWS**: para lanzar una AMI de Citrix ADC VPX en una nube privada virtual (VPC) de AWS. Puede crear una cuenta de AWS de forma gratuita en www.aws.amazon.com.
- **Una cuenta de usuario de AWS Identity and Access Management (IAM)**: Para controlar de forma segura el acceso a los servicios y recursos de AWS para sus usuarios. Para obtener más información sobre cómo crear una cuenta de usuario de IAM, consulte Creación de usuarios de IAM (consola). Una función de IAM es obligatoria tanto para implementaciones independientes como para implementaciones de alta disponibilidad.

  La función de IAM asociada a su cuenta de AWS debe tener los siguientes permisos de IAM para varios casos.

  HA se empareja con direcciones IPv4 en la misma zona de AWS:

```
”ec2:DescribeInstances”,
”ec2:AssignPrivateIpAddresses”,
”iam:SimulatePrincipalPolicy”,
”iam:GetRole”
<!--NeedCopy-->
```

  Ha emparejado con direcciones IPv6 en la misma zona de AWS:

```
”ec2:DescribeInstances”,
”ec2:AssignIpv6Addresses”,
”ec2:UnassignIpv6Addresses”,
”iam:SimulatePrincipalPolicy”,
”iam:GetRole”
<!--NeedCopy-->
```

  HA se empareja con direcciones IPv4 e IPv6 en la misma zona de AWS:

```
”ec2:DescribeInstances”,
”ec2:AssignPrivateIpAddresses”,
”ec2:AssignIpv6Addresses”,
”ec2:UnassignIpv6Addresses”,
”iam:SimulatePrincipalPolicy”,
”iam:GetRole”
<!--NeedCopy-->
```

  La alta disponibilidad se empareja con direcciones IP elásticas en diferentes zonas de AWS:


```
"ec2:DescribeInstances",
"ec2:DescribeAddresses",
"ec2:AssociateAddress",
"ec2:DisassociateAddress",
"iam:SimulatePrincipalPolicy",
"iam:GetRole"
<!--NeedCopy-->
```

La alta disponibilidad se empareja con direcciones IP privadas en diferentes zonas de AWS:

```
"ec2:DescribeInstances",
"ec2:DescribeRouteTables",
"ec2:DeleteRoute",
"ec2:CreateRoute",
"ec2:ModifyNetworkInterfaceAttribute",
"iam:SimulatePrincipalPolicy",
"iam:GetRole"
<!--NeedCopy-->
```

HA se empareja con direcciones IP privadas e IP elásticas en diferentes zonas de AWS:

```
"ec2:DescribeInstances",
"ec2:DescribeAddresses",
"ec2:AssociateAddress",
"ec2:DisassociateAddress",
"ec2:DescribeRouteTables",
"ec2:DeleteRoute",
"ec2:CreateRoute",
"ec2:ModifyNetworkInterfaceAttribute",
"iam:SimulatePrincipalPolicy",
"iam:GetRole"
<!--NeedCopy-->
```

Escalado automático de backend de AWS:

```
"ec2:DescribeInstances",
"autoscaling:*",
"sns:CreateTopic",
"sns:DeleteTopic",
```



```
5   "sns:ListTopics",
6   "sns:Subscribe",
7   "sqs:CreateQueue",
8   "sqs:ListQueues",
9   "sqs:DeleteMessage",
10  "sqs:GetQueueAttributes",
11  "sqs:SetQueueAttributes",
12  "iam:SimulatePrincipalPolicy",
13  "iam:GetRole",
14  <!--NeedCopy-->
```

> Nota:
>
> - Si usa cualquier combinación de las funciones anteriores, use la combinación de permisos de IAM para cada una de las funciones.
> - Si usa la plantilla de Citrix CloudFormation, la función de IAM se crea automáticamente. La plantilla no permite seleccionar una función de IAM ya creada.
> - Cuando inicia sesión en la instancia VPX a través de la GUI, aparece un mensaje para configurar los privilegios necesarios para la función de IAM. Ignore la solicitud si ya configuró los privilegios.

- **CLI de AWS**: Para utilizar toda la funcionalidad proporcionada por AWS Management Console desde el programa de terminal. Para obtener más información, consulte la guía del usuario de la CLI de AWS. También necesita la CLI de AWS para cambiar el tipo de interfaz de red a SR-IOV.
- **Adaptador de red elástico (ENA)**: para el tipo de instancia habilitada para controladores ENA, por ejemplo, instancias M5, C5, la versión del firmware debe ser 13.0 y superior.

Cómo funciona una instancia de Citrix ADC VPX en AWS

August 20, 2021

La instancia de Citrix ADC VPX está disponible como AMI en el mercado de AWS y se puede lanzar como una instancia EC2 dentro de una VPC de AWS. La instancia de AMI de Citrix ADC VPX requiere un mínimo de 2 CPU virtuales y 2 GB de memoria. Una instancia EC2 lanzada dentro de una VPC de AWS también puede proporcionar las múltiples interfaces, varias direcciones IP por interfaz y direcciones IP públicas y privadas necesarias para la configuración VPX. Cada instancia VPX requiere al menos tres subredes IP:

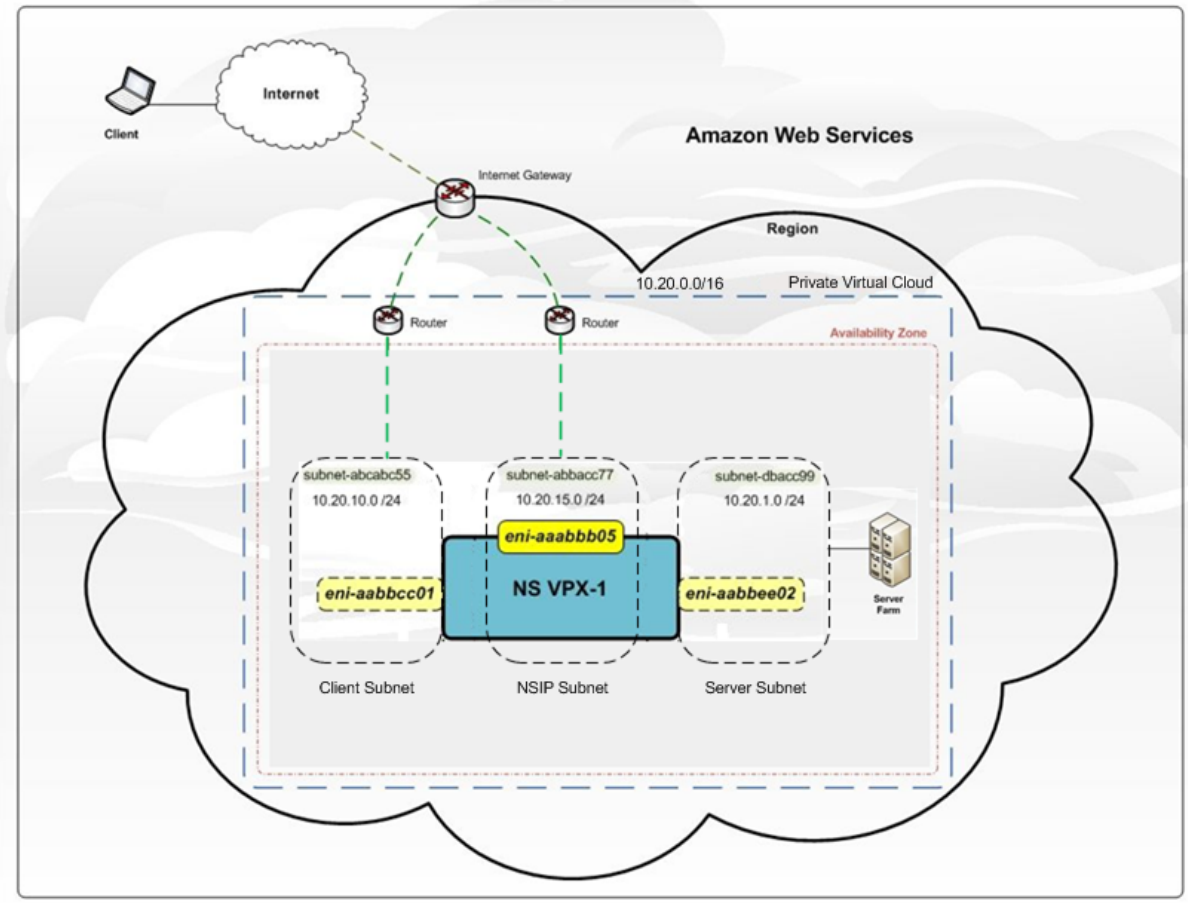
- Una subred de administración
- Una subred (VIP) orientada al cliente
- Una subred orientada al back-end (SNIP, MIP, etc.)

Citrix recomienda tres interfaces de red para una instancia VPX estándar en la instalación de AWS.

Actualmente, AWS hace que la funcionalidad multiIP esté disponible solo para instancias que se ejecutan dentro de una VPC de AWS. Una instancia VPX en una VPC se puede utilizar para equilibrar la carga de servidores que se ejecutan en instancias EC2. Una VPC de Amazon le permite crear y controlar un entorno de red virtual, incluido su propio intervalo de direcciones IP, subredes, tablas de rutas y puertas de enlace de red.

Nota: De forma predeterminada, puede crear hasta 5 instancias de VPC por región de AWS para cada cuenta de AWS. Puede solicitar mayores límites de VPC enviando el formulario de solicitud de Amazon http://aws.amazon.com/contact-us/vpc-request.

Ilustración 1. Una implementación de instancia de Citrix ADC VPX de ejemplo en la arquitectura de AWS



La ilustración 1 muestra una topología simple de una VPC de AWS con una implementación de Citrix ADC VPX. La VPC de AWS tiene:

1. Una única Gateway de Internet para enrutar el tráfico de entrada y salida de la VPC.
2. Conectividad de red entre la Gateway de Internet e Internet.
3. Tres subredes, una para administración, cliente y servidor cada una.

4. Conectividad de red entre la Gateway de Internet y las dos subredes (administración y cliente).
5. Una instancia independiente de Citrix ADC VPX implementada dentro de la VPC. La instancia VPX tiene tres ENIs, uno asociado a cada subred.

Implementar una instancia independiente de Citrix ADC VPX en AWS

August 20, 2021

Puede implementar una instancia independiente de Citrix ADC VPX en AWS mediante las siguientes opciones:

- Consola web de AWS
- Plantilla CloudFormation creada por Citrix
- AWS CLI

En este tema se describe el procedimiento para implementar una instancia de Citrix ADC VPX en AWS.

Antes de iniciar la implementación, lea los siguientes temas:

- Requisitos previos
- Directrices de limitación y uso

Implementar una instancia de Citrix ADC VPX en AWS mediante la consola web de AWS

Puede implementar una instancia de Citrix ADC VPX en AWS a través de la consola web de AWS. El proceso de implementación incluye los siguientes pasos:

1. Crear un par de claves
2. Crear una nube privada virtual (VPC)
3. Agregar más subredes
4. Crear grupos de seguridad y reglas de seguridad
5. Agregar tablas de redirecciones
6. Crear una Gateway a Internet
7. Crear una instancia de Citrix ADC VPX
8. Crear y conectar más interfaces de red
9. Adjuntar IP elásticas a la NIC de administración
10. Conectarse a la instancia VPX

Paso 1: Crear un par de claves.

Amazon EC2 utiliza un par de claves para cifrar y descifrar la información de inicio de sesión. Para iniciar sesión en la instancia, debe crear un par de claves, especificar el nombre del par de claves al iniciar la instancia y proporcionar la clave privada cuando se conecte a la instancia.

Cuando revise e inicie una instancia mediante el asistente AWS Launch Instance, se le pedirá que utilice un par de claves existente o cree un nuevo par de claves. Para obtener más información sobre cómo crear un par de claves, consulte Pares de claves de Amazon EC2.

Paso 2: Cree una VPC.

Una instancia de VPC de Citrix ADC se implementa dentro de una VPC de AWS. Una VPC le permite definir la red virtual dedicada a su cuenta de AWS. Para obtener más información sobre AWS VPC, consulte Introducción a Amazon VPC.

Al crear una VPC para su instancia de Citrix ADC VPX, tenga en cuenta los siguientes puntos.

- Utilice la opción VPC con una única subred pública únicamente para crear una VPC de AWS en una zona de disponibilidad de AWS.
- Citrix recomienda crear al menos **tres subredes**, de los siguientes tipos:
  - Una subred para el tráfico de administración. Coloque la IP de administración (NSIP) en esta subred. Por defecto, la interfaz de red elástica (ENI) eth0 se utiliza para la administración de IP.
  - Una o más subredes para el tráfico de acceso de cliente (de usuario a Citrix ADC VPX), a través de las cuales los clientes se conectan a una o más direcciones IP virtuales (VIP) asignadas a servidores virtuales de equilibrio de carga ADC de Citrix.
  - Una o más subredes para el tráfico de acceso al servidor (VPX a Servidor), a través del cual los servidores se conectan a direcciones IP de subred (SNIP) propiedad de VPX. Para obtener más información sobre el equilibrio de carga de Citrix ADC y los servidores virtuales, las direcciones IP virtuales (VIP) y las direcciones IP de subred (SNIP), consulte:
  - Todas las subredes deben estar en la misma zona de disponibilidad.

Paso 3: Agregar subredes.

Cuando utilizó el Asistente para VPC, solo se creó una subred. Dependiendo de sus necesidades, es posible que quiera crear más subredes. Para obtener más información sobre cómo crear más subredes, consulte Adición de una subred a la VPC.

Paso 4: Crear grupos de seguridad y reglas de seguridad.

Para controlar el tráfico entrante y saliente, cree grupos de seguridad y agregue reglas a los grupos. Para obtener más información sobre cómo crear grupos y agregar reglas, consulte Grupos de seguridad para la VPC.

Para las instancias de Citrix ADC VPX, el asistente EC2 proporciona grupos de seguridad predeterminados, generados por AWS Marketplace y basados en la configuración recomendada por Citrix. Sin embargo, puede crear más grupos de seguridad según sus requisitos.

> **Nota**
>
> Puertos 22, 80, 443 que se abrirá en el grupo Seguridad para acceso SSH, HTTP y HTTPS respec-

> tivamente.

Paso 5: Agregar tablas de redirecciones.

La tabla de redirecciones contiene un conjunto de reglas, denominadas redirecciones, que se utilizan para determinar adónde se dirige el tráfico de red. Cada subred de la VPC debe estar asociada a una tabla de redirecciones. Para obtener más información sobre cómo crear una tabla de redirección, consulte Tablas de redirección.

Paso 6: Crear una puerta de enlace a Internet.

Una puerta de enlace de Internet tiene dos propósitos: proporcionar un destino en las tablas de redirecciones de VPC para el tráfico redirigible a Internet y realizar la traducción de direcciones de red (NAT) para las instancias a las que se han asignado direcciones IPv4 públicas.

Crear una Gateway de Internet para el tráfico de Internet. Para obtener más información sobre cómo crear una puerta de enlace de Internet, consulte la sección Adjuntar una puerta de enlace de Internet.

Paso 7: Cree una instancia de Citrix ADC VPX mediante el servicio AWS EC2.

Para crear una instancia de Citrix ADC VPX mediante el servicio AWS EC2, siga los pasos siguientes.

1. En el panel de AWS, vaya a **Compute > EC2 > Launch Instance > AWS Marketplace**.

   Antes de hacer clic en **Launch Instance**, asegúrese de que su región es correcta comprobando la nota que aparece en **Launch Instance**.

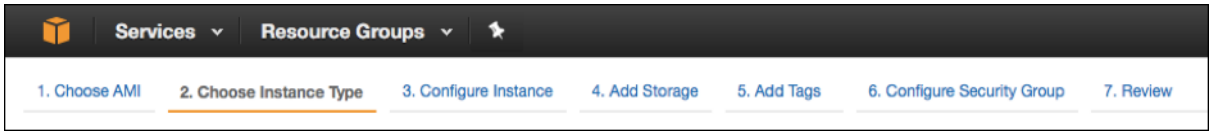
   

2. En la barra Buscar en AWS Marketplace, busque con la palabra clave Citrix ADC VPX.
3. Seleccione la versión que quiere implementar y, a continuación, haga clic en **Seleccionar**. Para la versión Citrix ADC VPX, tiene las siguientes opciones:
   - Una versión con licencia
   - Dispositivo Citrix ADC VPX Express (es un dispositivo virtual gratuito, disponible en Citrix ADC 12.0 56.20).
   - Trae su propio dispositivo

Se inicia el asistente Iniciar instancia. Siga el asistente para crear una instancia. El asistente le pide que:

- Elegir tipo de instancia
- Configurar instancia

- Agregar almacenamiento
- Agregar etiquetas
- Configurar grupo de seguridad
- Revisar



Paso 8: Cree y conecte más interfaces de red.

Cree dos interfaces de red más para VIP y SNIP. Para obtener más información sobre cómo crear más interfaces de red, consulte la sección Creación de una interfaz de red .

Después de crear las interfaces de red, debe adjuntarlas a la instancia VPX. Antes de conectar la interfaz, apague la instancia VPX, conecte la interfaz y encienda la instancia. Para obtener más información sobre cómo conectar interfaces de red, consulte la sección Adjuntar una interfaz de red al iniciar una instancia .

Paso 9: Asignar y asociar IP elásticas.

Si asigna una dirección IP pública a una instancia EC2, permanecerá asignada solo hasta que se detenga la instancia. Después de eso, la dirección se libera de nuevo al grupo. Al reiniciar la instancia, se asigna una nueva dirección IP pública.

Por el contrario, una dirección IP elástica (EIP) permanece asignada hasta que la dirección se desasocia de una instancia.

Asigne y asocie una IP elástica para la NIC de administración. Para obtener más información acerca de cómo asignar y asociar direcciones IP elásticas, consulte estos temas:

- Asignación de una dirección IP elástica
- Asociación de una dirección IP elástica con una instancia en ejecución

Estos pasos completan el procedimiento para crear una instancia de Citrix ADC VPX en AWS. La instancia puede tardar unos minutos en estar lista. Compruebe que su instancia ha superado las comprobaciones de estado. Puede ver esta información en la columna **Comprobaciones de estado** de la página Instancias.

Paso 10: Conéctese a la instancia VPX.

Después de crear la instancia VPX, se conecta la instancia mediante la interfaz gráfica de usuario y un cliente SSH.

- Interfaz gráfica (GUI)

Las siguientes son las credenciales de administrador predeterminadas para acceder a una instancia de Citrix ADC VPX

Nombre de usuario: `nsroot`

Contraseña: La contraseña predeterminada para la cuenta raíz ns se establece en el ID de instancia de AWS de la instancia de Citrix ADC VPX. En el primer inicio de sesión, se le pedirá que cambie la contraseña por razones de seguridad. Después de cambiar la contraseña, debe guardar la configuración. Si la configuración no se guarda y la instancia se reinicia, debe iniciar sesión con la contraseña predeterminada. Vuelva a cambiar la contraseña en el indicador.

- Cliente SSH

En la consola de administración de AWS, seleccione la instancia de Citrix ADC VPX y haga clic en **Conectar**. Siga las instrucciones que se indican en la página **Conectar a su instancia**.

Para obtener más información acerca de cómo implementar una instancia independiente de Citrix ADC VPX en AWS mediante la consola web de AWS, consulte:

- Caso: Instancia independiente
- Cómo configurar una instancia de Citrix NetScaler VPX en AWS mediante la plantilla de Citrix CloudFormation

Configurar una instancia de Citrix ADC VPX mediante la plantilla de Citrix CloudFormation

Puede utilizar la plantilla CloudFormation proporcionada por Citrix para automatizar el lanzamiento de instancias VPX. La plantilla proporciona funcionalidad para iniciar una única instancia de Citrix ADC VPX o crear un entorno de alta disponibilidad con un par de instancias de Citrix ADC VPX.

Puede iniciar la plantilla desde AWS Marketplace o GitHub.

La plantilla CloudFormation requiere un entorno de VPC existente y lanza una instancia VPX con tres interfaces de red elásticas (ENI). Antes de iniciar la plantilla de CloudFormation, asegúrese de completar los siguientes requisitos:

- Una nube privada virtual (VPC) de AWS
- Tres subredes dentro de la VPC: Una para administración, otra para tráfico de clientes y otra para servidores back-end
- Un par de claves EC2 para habilitar el acceso SSH a la instancia
- Un grupo de seguridad con puertos UDP 3003, TCP 3009—3010, HTTP, SSH abiertos

Consulte la sección “Implementar una instancia de Citrix ADC VPX en AWS mediante el uso de la consola web de AWS” o la documentación de AWS para obtener más información sobre cómo completar los requisitos previos.

Vea este vídeo para obtener información sobre cómo configurar e iniciar una instancia independiente Citrix ADC VPX mediante la plantilla Citrix CloudFormation disponible en AWS Marketplace.

Además, puede configurar e iniciar una instancia independiente de Citrix ADC VPX Express mediante la plantilla de Citrix CloudFormation disponible en GitHub:

https://github.com/citrix/citrix-adc-aws-cloudformation/tree/master/templates/standalone/

Una función de IAM no es obligatoria para una implementación independiente. Sin embargo, Citrix recomienda crear y adjuntar un rol de IAM con los privilegios necesarios a la instancia, para futuras necesidades. El rol de IAM garantiza que la instancia independiente se convierta fácilmente a un nodo de alta disponibilidad con SR-IOV, cuando sea necesario.

Para obtener más información sobre los privilegios necesarios, consulte Configuración de instancias Citrix ADC VPX para utilizar la interfaz de red SR-IOV.

> Nota
> Si implementa una instancia Citrix ADC VPX en AWS mediante la consola web de AWS, el servicio CloudWatch está habilitado de forma predeterminada. Si implementa una instancia de Citrix ADC VPX mediante la plantilla de Citrix CloudFormation, la opción predeterminada es "Sí". Si quiere inhabilitar el servicio CloudWatch, seleccione "No". Para obtener más información, consulte Supervisar las instancias mediante Amazon CloudWatch.

Configure una instancia de Citrix ADC VPX mediante la CLI de AWS

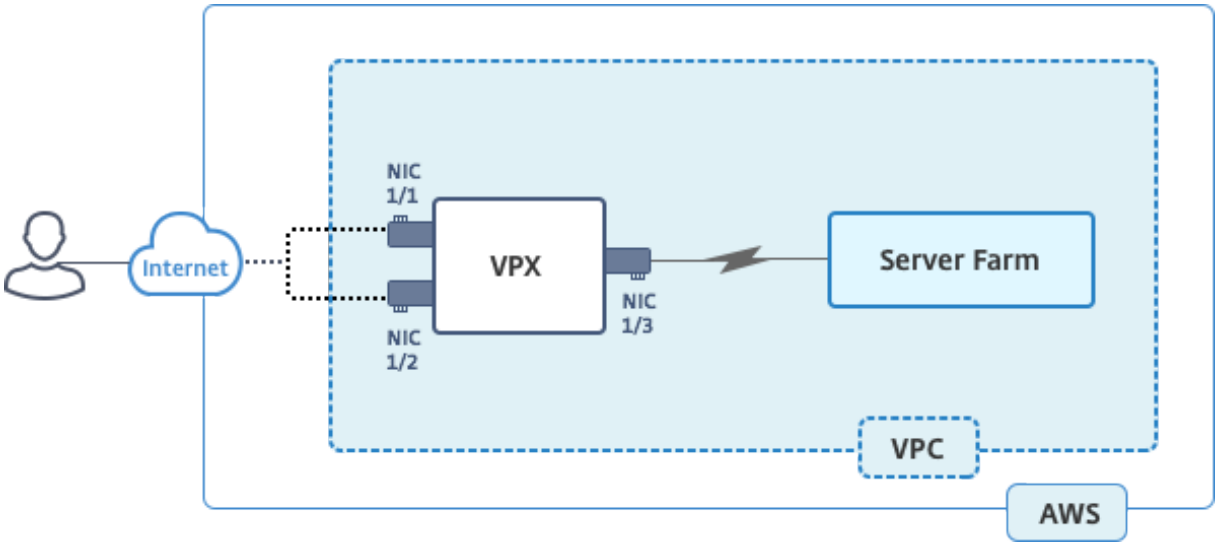
Puede utilizar la CLI de AWS para iniciar instancias. Para obtener más información, consulte la documentación de AWS Command Line Interface.

Caso: Instancia independiente

August 20, 2021

Este caso ilustra cómo implementar una instancia de EC2 independiente de Citrix ADC VPX en AWS mediante la GUI de AWS. Cree una instancia VPX independiente con tres NIC. La instancia, que se configura como servidor virtual de equilibrio de carga, se comunica con los servidores back-end (la comunidad de servidores). Para esta configuración, configure las rutas de comunicación necesarias entre la instancia y los servidores back-end, y entre la instancia y los hosts externos en Internet público.

Para obtener más información sobre el procedimiento para implementar una instancia VPX, consulte Implementación de una instancia independiente Citrix ADC VPX en AWS.

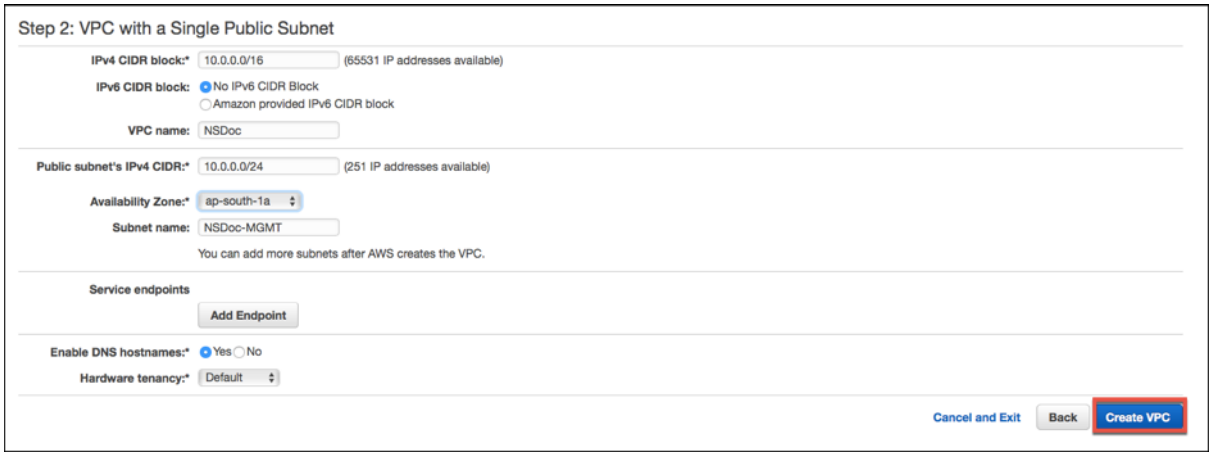


Cree tres NIC. Cada NIC se puede configurar con un par de direcciones IP (públicas y privadas). Las NIC cumplen los siguientes propósitos.

NIC	Propósito	Asociada con
eth0	Sirve tráfico de administración (NSIP)	Una dirección IP pública y una dirección IP privada
eth1	Sirve tráfico del lado del cliente (VIP)	Una dirección IP pública y una dirección IP privada
eth2	Se comunica con servidores back-end (SNIP)	Una dirección IP pública (la dirección IP privada no es obligatoria)

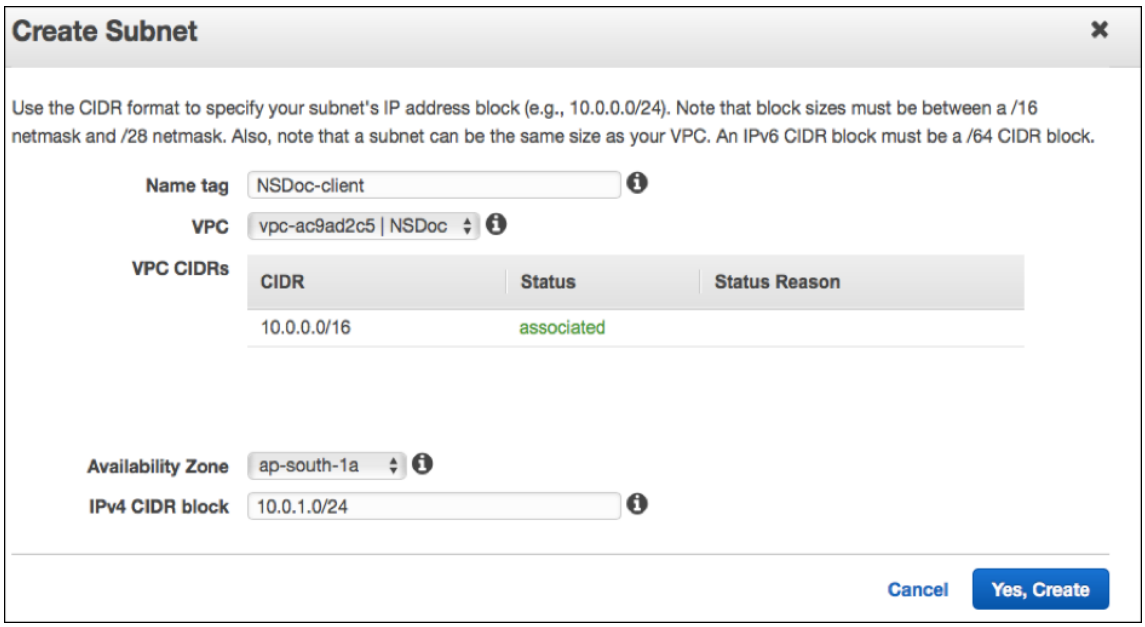
Paso 1: Cree una VPC.

1. Inicie sesión en la consola web de AWS y vaya a **Redes y entrega de contenido** > **VPC**. Haga clic en **Iniciar VPC Wizard**.
2. Seleccione **VPC con una única subred pública** y haga clic en **Seleccionar**.
3. Establezca el bloque CIDR IP en 10.0.0.0/16, para este caso.
4. Dé un nombre para la VPC.
5. Establezca la subred pública en 10.0.0.0/24. (Esta es la red de administración).
6. Seleccione una zona de disponibilidad.
7. Dé un nombre a la subred.
8. Haga clic en Crear **VPC**.

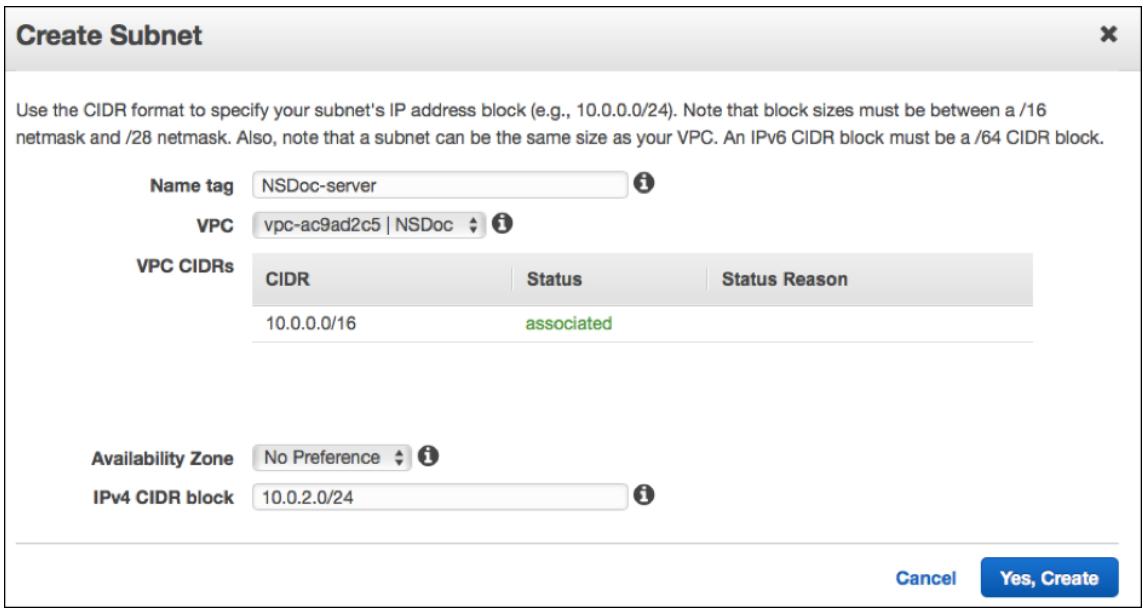


Paso 2: Crear subredes adicionales.

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Subredes y Crear subred después de introducir los siguientes detalles.
   - Etiqueta de nombre: Proporcione un nombre para la subred.
   - VPC: Elija la VPC para la que está creando la subred.
   - Zona de disponibilidad: Seleccione la zona de disponibilidad en la que creó la VPC en el paso 1.
   - Bloque CIDR IPv4: Especifique un bloque CIDR IPv4 para su subred. Para este caso, elija 10.0.1.0/24.

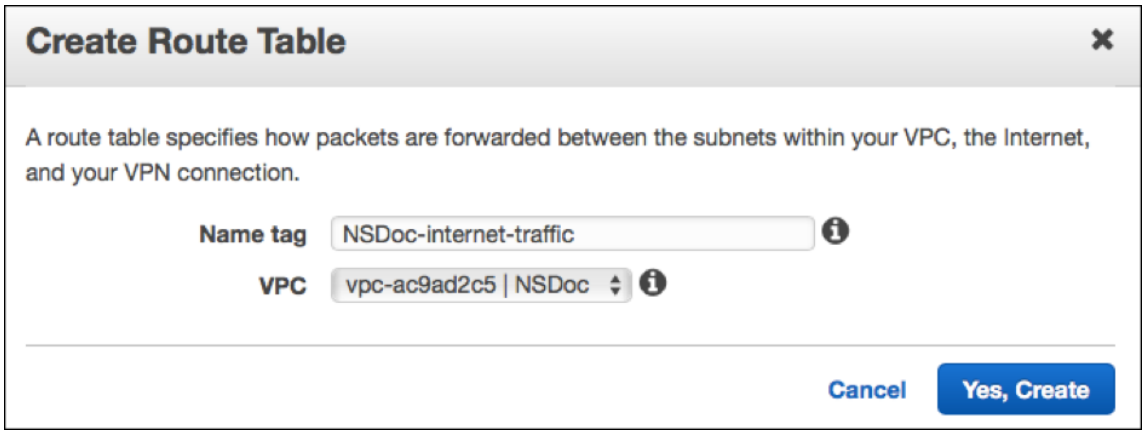


3. Repita los pasos para crear una subred más para los servidores back-end.



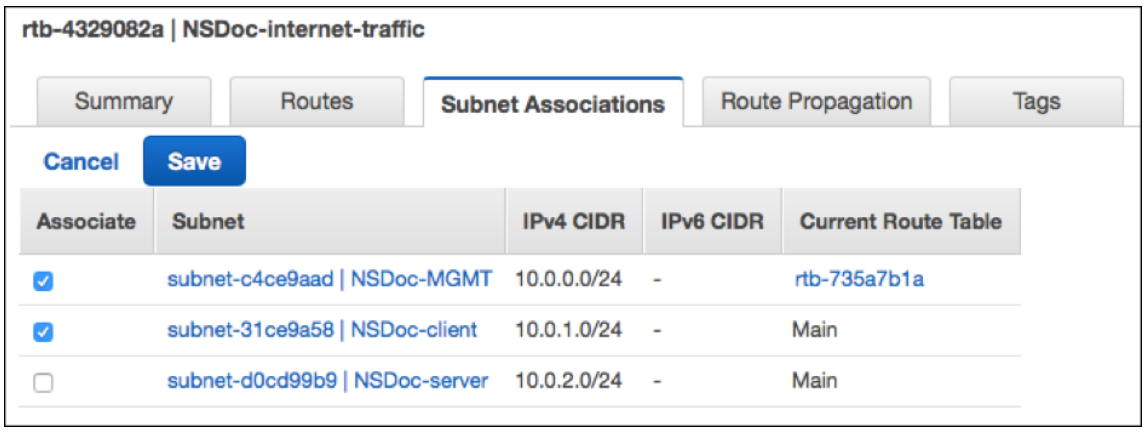
Paso 3: Crear una tabla de redirecciones.

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija **Tablas de redirecciones** > **Crear tabla de redirecciones.**
3. En la ventana Crear tabla de redirecciones, agregue un nombre y seleccione la VPC que creó en el paso 1.
4. Haga clic en **Yes, Create**.



   La tabla de redirección se asigna a todas las subredes que ha creado para esta VPC, de modo que la redirección del tráfico de una instancia de una subred pueda llegar a una instancia de otra subred.

5. Haga clic en Asociaciones de subred y, a continuación, haga clic en Modificar.
6. Haga clic en la subred de administración y cliente y haga clic en Guardar. Esto crea una tabla de redirecciones solo para el tráfico de Internet.



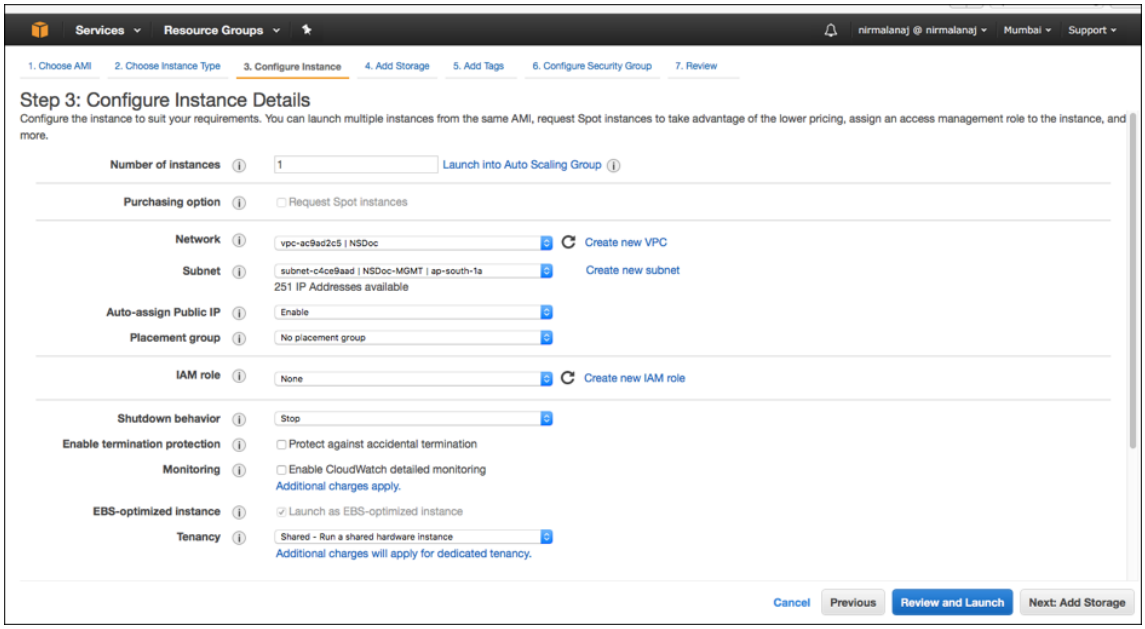
7. Haga clic en **Rutas > Modificar > Agregar otra ruta**.
8. En el campo Destino, agregue 0.0.0.0/0 y haga clic en el campo Destino para seleccionar igw-<xxxx> la puerta de enlace de Internet que el Asistente de VPC creó automáticamente.
9. Haga clic en Guardar.

10. Siga los pasos para crear una tabla de redirecciones para el tráfico del lado del servidor.

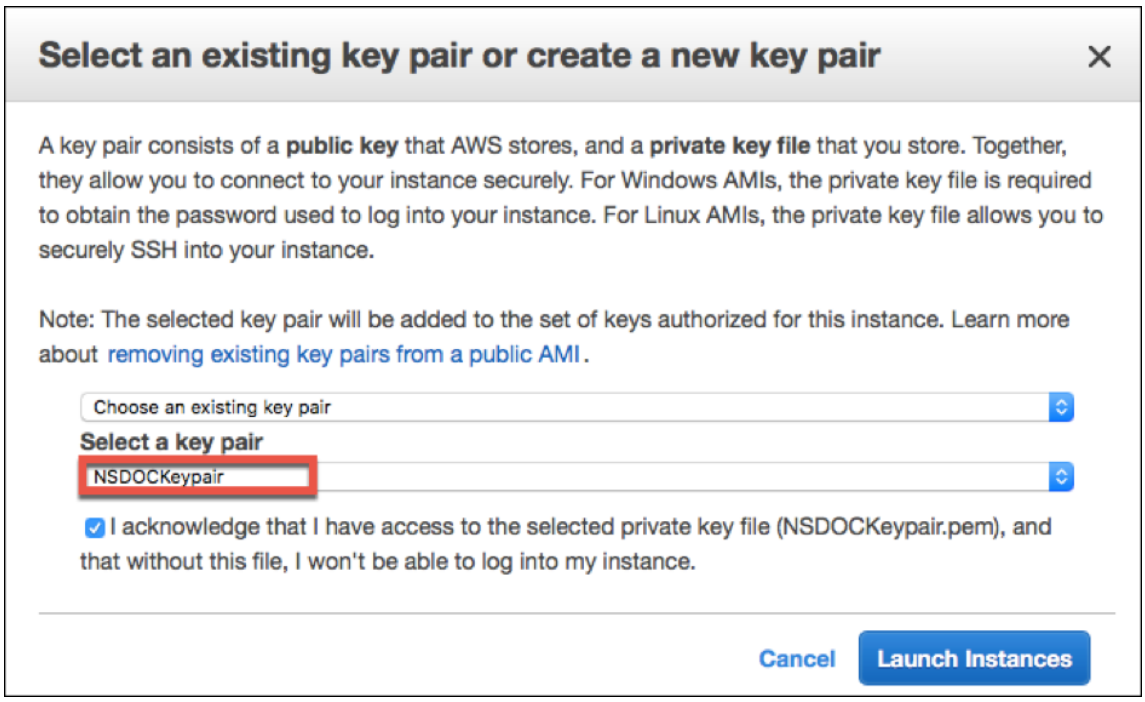
Paso 4: Cree una instancia de Citrix ADC VPX.

1. Inicie sesión en la consola de administración de AWS y haga clic en **EC2** en **Compute**.
2. Haga clic en AWS Marketplace. En la barra Buscar en AWS Marketplace, escriba Citrix ADC VPX y presione Entrar. Se muestran las ediciones disponibles de Citrix ADC VPX.
3. Haga clic en **Seleccionar** para elegir la edición Citrix ADC VPX que quiera. Se inicia el asistente de instancias de EC2.
4. En la página **Elegir tipo de instancia**, seleccione **m4. Xlarge** (recomendado) y haga clic en **Siguiente: Configurar detalles de instancia**.
5. En la página Configurar detalles de instancia, seleccione lo siguiente y, a continuación, haga clic en Siguiente: Agregar almacenamiento.

- Número de instancias: 1
- Red: La VPC que creó en el paso 1
- Subred: La subred de gestión
- Asignación automática de IP pública: Habilitar



6. En la página Agregar almacenamiento, seleccione la opción predeterminada y haga clic en Siguiente: Agregar etiquetas.
7. En la página Agregar etiquetas, agregue un nombre para la instancia y haga clic en Siguiente: Configurar grupo de seguridad.
8. En la página Configurar grupo de seguridad, seleccione la opción predeterminada (que genera AWS Marketplace y se basa en la configuración recomendada por Citrix Systems) y, a continuación, haga clic en **Revisar y lanzar > Iniciar**.
9. Se le pedirá que seleccione un par de claves existente o cree un par de claves nuevo. En la lista desplegable Seleccionar un par de claves, seleccione el par de claves creado como requisito previo (consulte la sección Requisitos previos).
10. Marque la casilla para confirmar el par de claves y haga clic en Iniciar instancias.



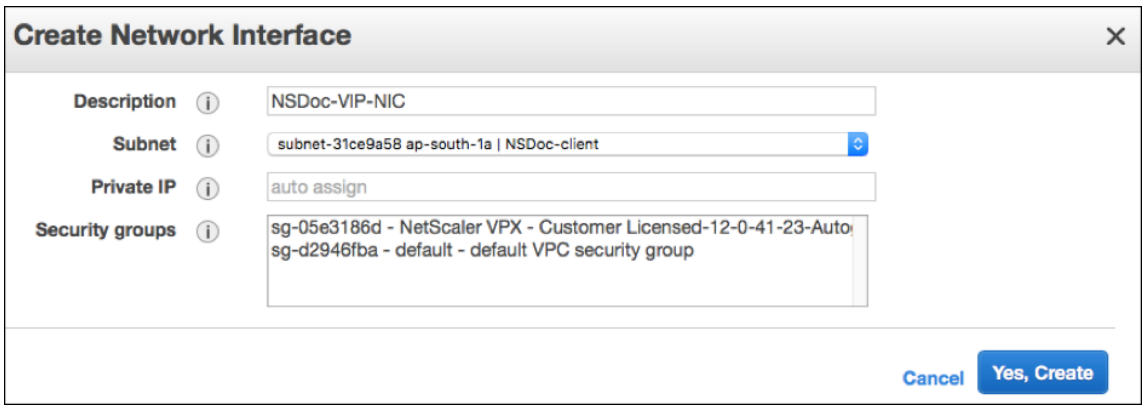
El Asistente de inicio de instancias muestra el estado de inicio y la instancia aparece en la lista de instancias cuando se inicia completamente.

En la instancia de comprobación, vaya a la consola de AWS, haga clic en EC2 > Ejecutando instancias. Seleccione la instancia y agregue un nombre. Asegúrese de que el estado de instancia se está ejecutando y de que las comprobaciones de estado se hayan completado.

Paso 5: Cree y conecte más interfaces de red.

Cuando creó la VPC, solo una interfaz de red asociada a ella. Ahora agregue dos interfaces de red más a la VPC, para VIP y SNIP.

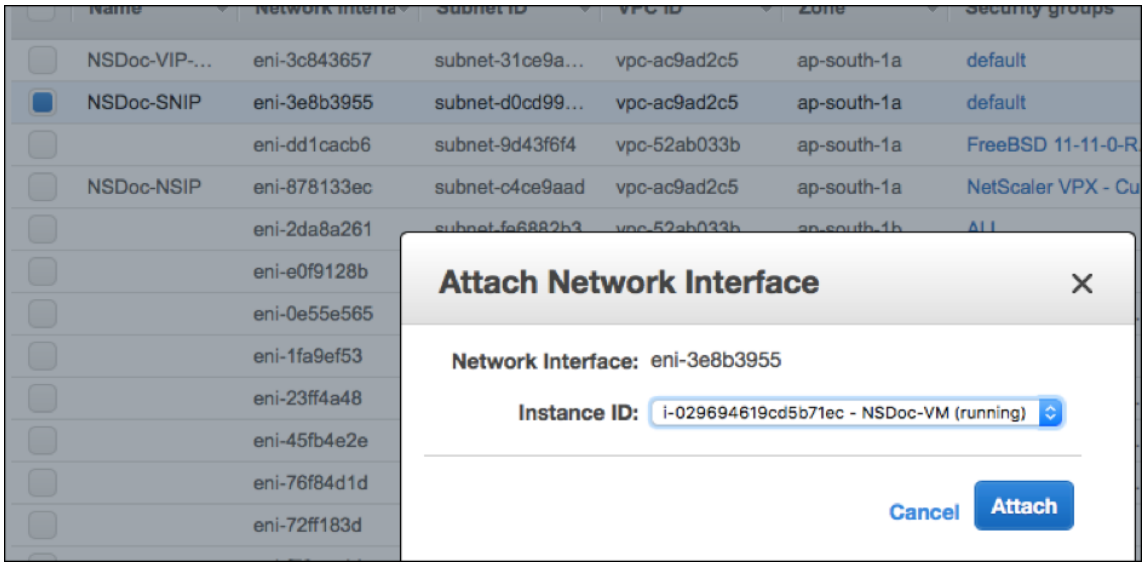
1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Interfaces de red.
3. Elija Crear interfaz de red.
4. En Descripción, escriba un nombre descriptivo.
5. En Subred, seleccione la subred que creó anteriormente para el VIP.
6. Para IP privada, deje la opción predeterminada.
7. En Grupos de seguridad, seleccione el grupo.
8. Haga clic en **Yes, Create**.



9. Después de crear la interfaz de red, agregue un nombre a la interfaz.
10. Repita los pasos para crear una interfaz de red para el tráfico del lado del servidor.

Conecte las interfaces de red:

1. En el panel de navegación, elija Interfaces de red.
2. Seleccione la interfaz de red y elija Adjuntar.
3. En el cuadro de diálogo Adjuntar interfaz de red, seleccione la instancia y elija Adjuntar.



Paso 6: Adjunte una IP elástica al NSIP.

1. Desde la consola de administración de AWS, vaya a **NETWORK & SECURITY > Elastic IPs**.
2. Compruebe si hay EIP gratuito disponible para adjuntar. Si no hay ninguno, haga clic en **Asignar nueva dirección**.
3. Seleccione la dirección IP recién asignada y elija **Acciones > Dirección asociada**.
4. Haga clic en el botón **de opción Interfaz de red**.
5. En la lista desplegable Interfaz de red, seleccione la NIC de administración.

6. En el menú desplegable **IP privada**, seleccione la dirección IP generada por AWS.
7. Active la casilla de verificación **Volver** a asociar.
8. Haga clic en **Asociar**.

Acceda a la instancia VPX:

Después de configurar una instancia de Citrix ADC VPX independiente con tres NIC, inicie sesión en la instancia VPX para completar la configuración del lado de Citrix ADC. Uso de las siguientes opciones:

- GUI: Escriba la IP pública de la NIC de administración en el explorador. Inicie sesión mediante `nsroot` como nombre de usuario y el ID de instancia (i-0c1ffe1d987817522) como contraseña.

> Nota
>
> En el primer inicio de sesión, se le pedirá que cambie la contraseña por razones de seguridad. Después de cambiar la contraseña, debe guardar la configuración. Si la configuración no se guarda y la instancia se reinicia, debe iniciar sesión con la contraseña predeterminada. Vuelva a cambiar la contraseña en el indicador y guarde la configuración.

- SSH: Abra un cliente SSH y escriba:

```
ssh -i \<location of your private key\> ns root@\<public DNS of the instance
\>
```

Para buscar el DNS público, haga clic en la instancia y haga clic en **Conectar**.

Información relacionada:

- Para configurar las direcciones IP propiedad de Citrix ADC (NSIP, VIP y SNIP), consulte Configuración de direcciones IP propiedad de Citrix ADC.
- Ha configurado una versión BYOL del dispositivo Citrix ADC VPX, para obtener más información, consulte la Guía de licencias de VPX en http://support.citrix.com/article/CTX122426

Descargar una licencia de Citrix ADC VPX

March 9, 2022

Después del lanzamiento de la instancia con licencia del cliente de Citrix ADC VPX desde el mercado de AWS, se requiere una licencia. Para obtener más información sobre las licencias VPX, consulte Descripción general de licencias.

Es necesario que:

1. Utilice el portal de licencias del sitio web de Citrix para generar una licencia válida.
2. Cargue la licencia en la instancia.

Si se trata de una instancia de mercado de **pago**, no es necesario instalar licencia. El conjunto de funciones y el rendimiento correctos se activan automáticamente.

Si utiliza una instancia de Citrix ADC VPX con un número de modelo superior a VPX 5000, es posible que el rendimiento de red no sea el mismo especificado en la licencia de la instancia. Sin embargo, otras funciones, como el rendimiento SSL y las transacciones SSL por segundo, podrían mejorar.

El ancho de banda de red de 5 Gbps se observa en el tipo de `c4.8xlarge` instancia.

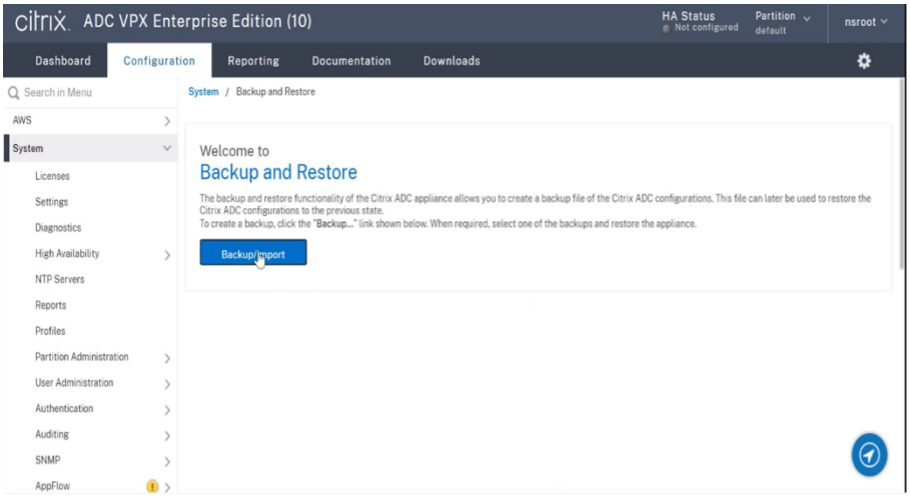
Cómo migrar la suscripción de AWS a BYOL

En esta sección se describe el procedimiento para migrar de la suscripción de AWS a Bring your own license (BYOL) y, por el contrario.

Siga los siguientes pasos para migrar una suscripción de AWS a BYOL:

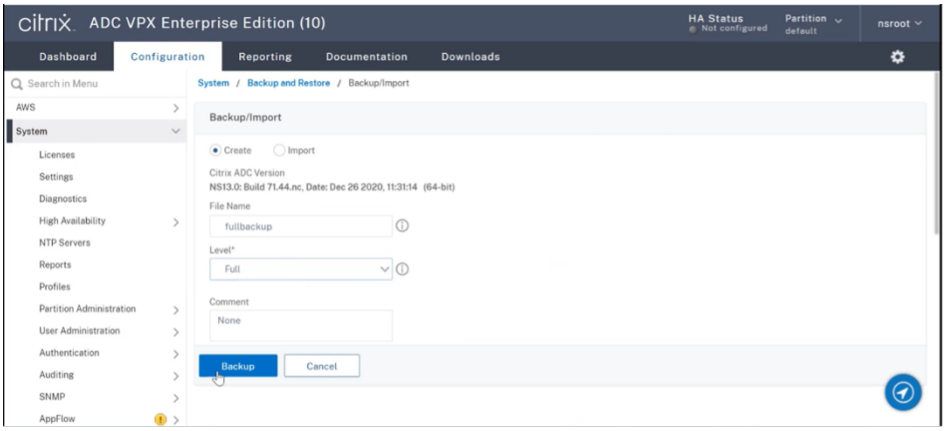
> Nota
>
> Los **pasos 2** y **3** se realizan en la instancia Citrix ADC VPX y todos los demás pasos se realizan en el portal de AWS.

1. Cree una instancia BYOL EC2 mediante Citrix ADC VPX: licencia del cliente en la misma zona de disponibilidad que la antigua instancia de EC2 que tiene el mismo grupo de seguridad, rol de IAM y subred. La nueva instancia EC2 debe tener solo una interfaz ENI.
2. Para hacer copias de seguridad de los datos de la antigua instancia de EC2 mediante la GUI de Citrix ADC, siga estos pasos.
    a) Vaya a **Sistema > Copia de seguridad y restauración**.
    b) En la página de **bienvenida**, haga clic **en Copia/Importar** para iniciar el proceso.

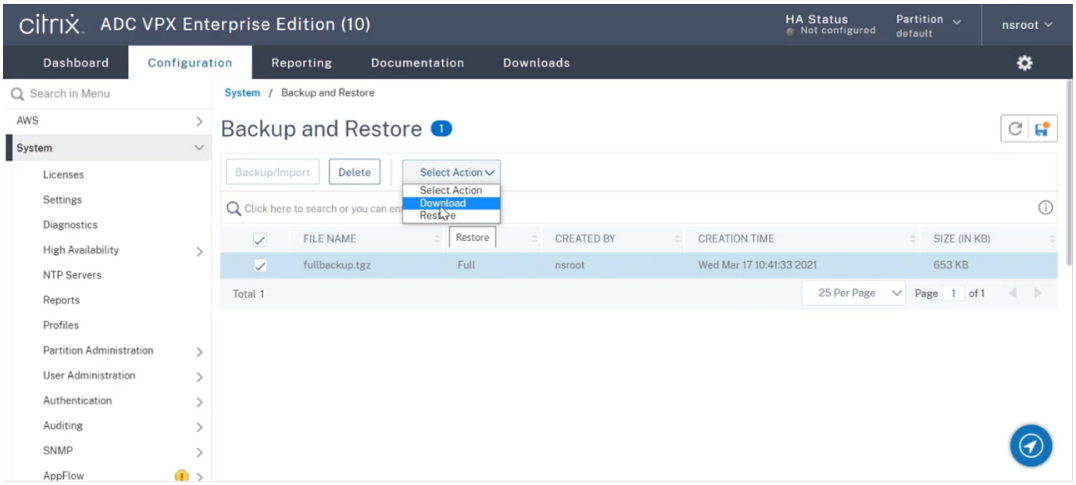


c) En la página **Copia/Importación**, rellene los siguientes detalles:

- **Nombre**: Nombre del archivo de copia de seguridad.
- **Nivel**: Seleccione el nivel de copia de seguridad como **Completo**.
- **Comentario**: Proporcione una breve descripción de la copia de seguridad.



d) Haga clic en **Copia de seguridad**. Una vez finalizada la copia de seguridad, puede seleccionar el archivo y descargarlo en el equipo local.

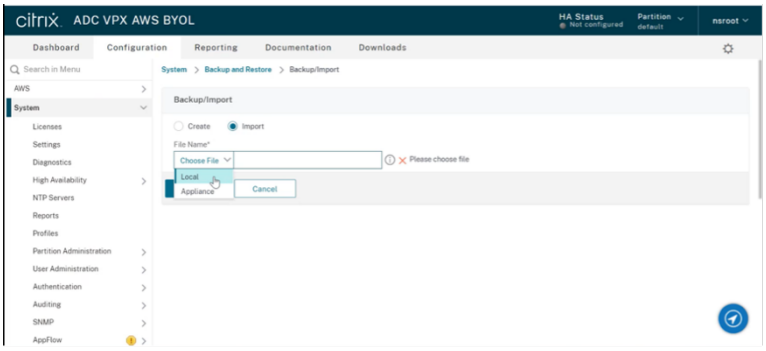


3. Para restaurar los datos de la nueva instancia de EC2 mediante la GUI de Citrix ADC, siga estos pasos:

   a) Vaya a **Sistema > Copia de seguridad y restauración**.

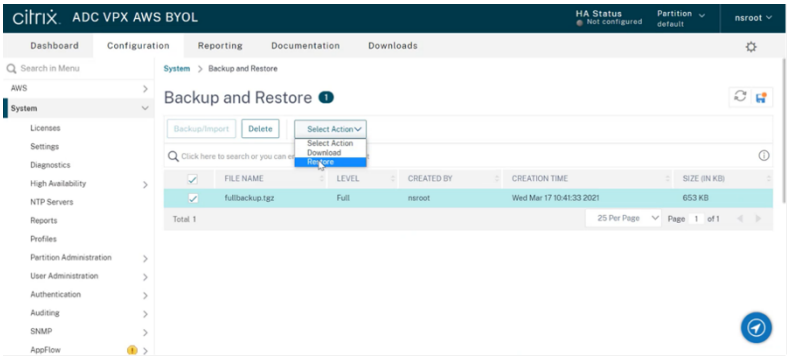
   b) Haga clic en **Copia de seguridad/importación** para iniciar el proceso.

   c) Seleccione la opción **Importar** y cargue el archivo de copia de seguridad.

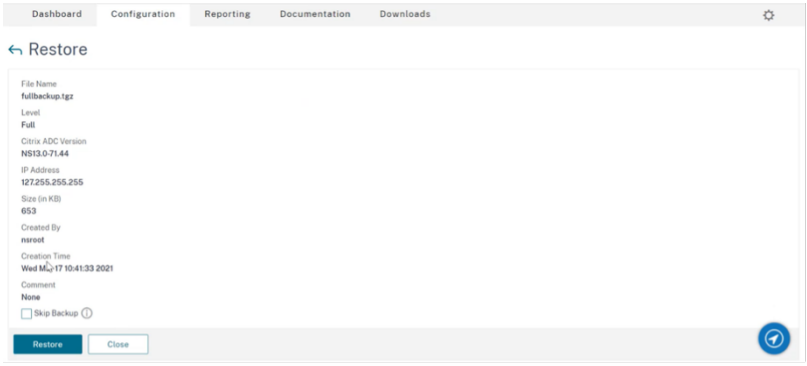


   d) Selecciona el archivo.

   e) En el menú desplegable **Seleccionar acción**, seleccione **Restaurar**.



   f) En la página **Restaurar**, verifique los detalles del archivo y haga clic en **Restaurar**.



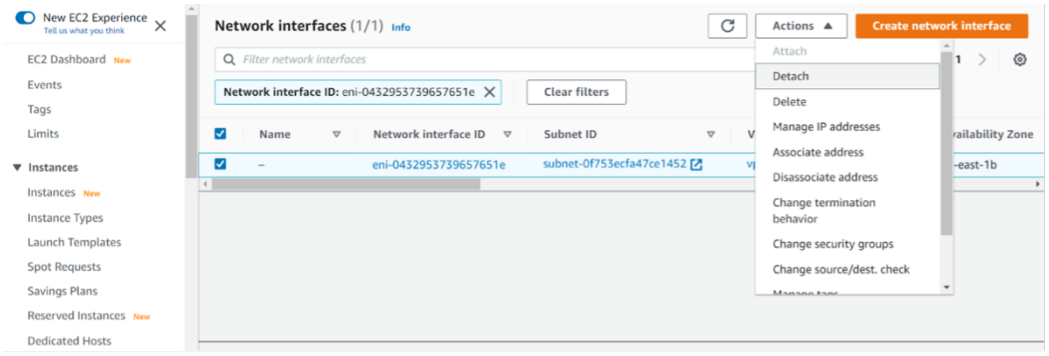
g) Después de la restauración, reinicie la instancia EC2.

4. Mueva todas las interfaces (excepto la interfaz de administración a la que está enlazada la dirección NSIP) de la antigua instancia EC2 a la nueva instancia EC2. Para mover una interfaz de red de una instancia EC2 a otra, sigue estos pasos:

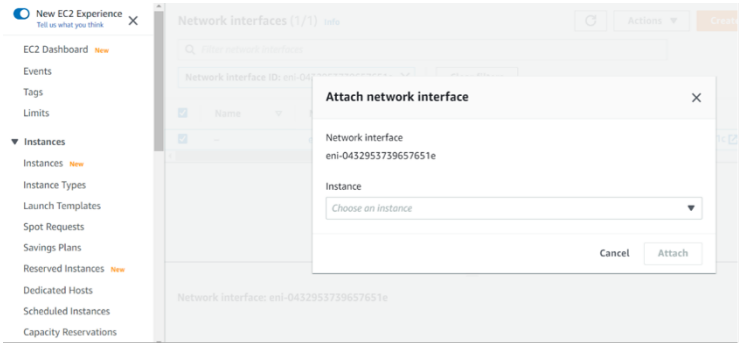
   a) En el **portal de AWS**, detenga las instancias EC2 antiguas y nuevas.

   b) Vaya a **Interfaces de red**y seleccione la interfaz de red conectada a la antigua instancia EC2.

   c) Desconecte la instancia de EC2 haciendo clic en **Acciones > Desconectar**.



   d) Adjunte la interfaz de red a la nueva instancia de EC2 haciendo clic en **Acciones > Adjuntar**. Introduzca el nombre de instancia EC2 al que debe asociarse la interfaz de red.



   e) Realice el **paso 1** al **paso 4** para todas las demás interfaces conectadas. Asegúrese de seguir la secuencia y mantener el orden de la interfaz. Es decir, primero desconecte la

interfaz 2 y conéctela, y luego desmonte la interfaz 3 y conéctela, etc.

5. No se puede separar la interfaz de administración de una instancia EC2 anterior. Por lo tanto, mueva todas las direcciones IP secundarias (si las hay) de la interfaz de administración (interfaz de red principal) de la antigua instancia EC2 a la nueva instancia EC2. Para mover una dirección IP de una interfaz a otra, sigue estos pasos:

   a) En el **portal de AWS**, asegúrese de que las instancias EC2 antiguas y nuevas estén en estado **Stop** .

   b) Vaya a **Interfaces de red**y seleccione la interfaz de red de administración asociada a la antigua instancia EC2.

   c) Haga clic en **Acciones > Administrar dirección IP**y anote todas las direcciones IP secundarias asignadas (si las hay).

   d) Desplácese hasta la interfaz de red de administración o la interfaz principal de la nueva instancia EC2.

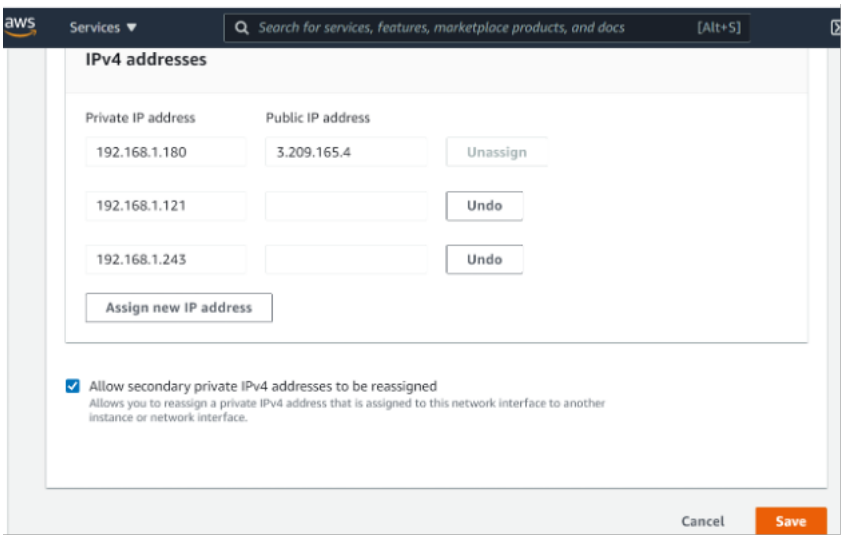
   e) Haga clic en **Acciones > Administrar direcciones IP**.

   f) En **Direcciones IPv4**, haga clic en **Asignar nueva dirección IP**.

   g) Introduzca las direcciones IP, que se indican en el **paso 3**.

   h) Active la casilla de verificación **Permitir que se reasignen direcciones IP privadas secundarias** .

   i) Haga clic en **Guardar**.



6. Inicie la nueva instancia de EC2 y verifique la configuración. Después de mover toda la configuración, puede eliminar o conservar la antigua instancia de EC2 según sus necesidades.

7. Si se adjunta alguna dirección EIP a la dirección NSIP de la instancia EC2 anterior, mueva la dirección NSIP de la instancia anterior a la nueva dirección NSIP de instancia.

8. Si quieres volver a la instancia anterior, sigue los mismos pasos en sentido contrario entre la instancia anterior y la nueva.
9. Después de pasar de la instancia de suscripción a la instancia BYOL, se requiere una licencia. Para instalar una licencia, siga estos pasos:
    - Utilice el portal de licencias del sitio web de Citrix para generar una licencia válida.
    - Cargue la licencia en la instancia. Para obtener más información, consulte VPX ADC: instalación de una nueva licencia.

> Nota
>
> Cuando mueve la instancia BYOL a la instancia de suscripción (instancia de mercado de pago), no es necesario instalar la licencia. El conjunto de funciones y el rendimiento correctos se activan automáticamente.

Limitaciones

La interfaz de administración no se puede mover a la nueva instancia EC2. Por lo tanto, Citrix recomienda configurar manualmente la interfaz de administración. Para obtener más información, consulte el **paso 5** del procedimiento anterior. Se crea una nueva instancia EC2 con la réplica exacta de la antigua instancia EC2, pero solo la dirección NSIP tiene una nueva dirección IP.

Servidores de equilibrio de carga en diferentes zonas de disponibilidad

August 20, 2021

Una instancia VPX se puede utilizar para equilibrar la carga de servidores que se ejecutan en la misma zona de disponibilidad, o en:

- Una zona de disponibilidad diferente (AZ) en la misma VPC de AWS
- Una región de AWS diferente
- AWS EC2 en una VPC

Para habilitar una instancia VPX para equilibrar la carga de los servidores que se ejecutan fuera de la VPC de AWS en la que se encuentra la instancia
VPX, configure la instancia para que utilice EIP para enrutar el tráfico a través de la Gateway de Internet, de la siguiente manera:

1. Configure un SNIP en la instancia de Citrix ADC VPX mediante la CLI de Citrix ADC o la GUI.
2. Habilite que el tráfico se enrute fuera de la AZ, creando una subred pública para el tráfico del lado del servidor.
3. Agregue una ruta de Gateway de Internet a la tabla de redirecciones mediante la consola GUI de AWS.

4. Asocie la tabla de redirección que ha actualizado a la subred del lado del servidor.
5. Asocie un EIP con la dirección IP privada del servidor asignada a una dirección SNIP de Citrix ADC.

Cómo funciona la alta disponibilidad en AWS

August 20, 2021

Puede configurar dos instancias de Citrix ADC VPX en AWS como un par activo-pasivo de alta disponibilidad (HA). Cuando configura una instancia como nodo principal y la otra como nodo secundario, el nodo principal acepta conexiones y administra servidores. El nodo secundario supervisa el principal. Si, por cualquier motivo, el nodo principal no puede aceptar conexiones, el nodo secundario se hace cargo.

En AWS, se admiten los siguientes tipos de implementación para las instancias VPX:

- Alta disponibilidad dentro de la misma zona
- Alta disponibilidad en diferentes zonas

> **Nota**
>
> Para que funcione una alta disponibilidad, asegúrese de que las instancias Citrix ADC VPX estén asociadas con roles de IAM y asignadas con la dirección IP elástica (EIP) al NSIP. No es necesario asignar un EIP en NSIP si el NSIP puede llegar a Internet a través de la instancia NAT.

Alta disponibilidad dentro de las mismas zonas

En una implementación de alta disponibilidad dentro de las mismas zonas, ambas instancias VPX deben tener configuraciones de red similares.

Siga estas dos reglas:

Artículo 1. Cualquier NIC de una instancia VPX debe estar en la misma subred que la NIC correspondiente de la otra VPX. Ambas instancias deben tener:

- Interfaz de administración en la misma subred (denominada subred de administración)
- Interfaz de cliente en la misma subred (denominada subred de cliente)
- Interfaz del servidor en la misma subred (denominada subred del servidor)

Artículo 2. La secuencia de NIC de administración, NIC cliente y NIC de servidor en ambas instancias debe ser la misma.
Por ejemplo, no se admite el siguiente caso.

Instancia VPX 1

NIC 0: Administración
NIC 1:
NIC 2 cliente: Servidor

Instancia VPX 2

NIC 0: Administración

NIC 1: Servidor

NIC 2: Cliente

En este caso, la NIC 1 de la instancia 1 está en la subred del cliente mientras que la NIC 1 de la instancia 2 está en la subred del servidor. Para que ha funcionado, la NIC 1 de ambas instancias debe estar en la subred cliente o en la subred del servidor.

A partir de 13.0 41.xx, se puede lograr una alta disponibilidad migrando direcciones IP privadas secundarias conectadas a las NIC (NIC del cliente y del servidor) del nodo HA primario al nodo HA secundario después de la conmutación por error. En esta implementación:

- Ambas instancias VPX tienen el mismo número de NIC y asignación de subred según la enumeración de NIC.
- Cada NIC VPX tiene una dirección IP privada adicional, excepto la primera NIC, que corresponde a la dirección IP de administración. La dirección IP privada adicional aparece como la dirección IP privada principal en la consola web de AWS. En nuestro documento, nos referimos a esta dirección IP adicional como la dirección IP ficticia).
- Las direcciones IP ficticias no deben configurarse en la instancia Citrix ADC como VIP y SNIP.
- Otras direcciones IP privadas secundarias deben crearse, según sea necesario, y configurarse como VIP y SNIP.
- En la conmutación por error, el nuevo nodo principal busca SNIP y VIP configurados y los mueve de las NIC asociadas al principal anterior a las NIC correspondientes en el nuevo primario.
- Las instancias Citrix ADC requieren permisos de IAM para que funcione HA. Agregue los siguientes privilegios de IAM a la directiva de IAM agregada a cada instancia.

```
"iam:GetRole"
"ec2:DescribeInstances"
"ec2:DescribeNetworkInterfaces"
"ec2:AssignPrivateIpAddresses"
```

> Nota: `unassignPrivateIpAddress` no es obligatorio.

Este método es más rápido que el método heredado. En el método anterior, HA depende de la migración de las interfaces de red elásticas de AWS del nodo principal al nodo secundario.

Para un método heredado, se requieren las siguientes directivas:


```
"iam:GetRole"
"ec2:DescribeInstances"
"ec2:DescribeAddresses"
"ec2:AssociateAddress"
"ec2:DisassociateAddress"
```

Para obtener más información, consulte Implementación de un par de alta disponibilidad en AWS.

Alta disponibilidad en diferentes zonas

Puede configurar dos instancias de Citrix ADC VPX en dos subredes diferentes o en dos zonas de disponibilidad de AWS diferentes, como un par activo-pasivo de alta disponibilidad en el modo Configuración de red independiente (INC). Tras la conmutación por error, el EIP (Elastic IP) del VIP de la instancia principal migra al secundario, que toma el relevo como el nuevo primario. En el proceso de conmutación por error, la API de AWS:

- Comprueba los servidores virtuales que se han `IPSets` adjuntado a ellos.
- Busca la dirección IP que tiene una IP pública asociada, de las dos direcciones IP en las que está escuchando el servidor virtual. Uno que está conectado directamente al servidor virtual y otro que está conectado a través del conjunto de IP.
- Vuelve a asociar la IP pública (EIP) a la IP privada que pertenece a la nueva VIP principal.

Para HA en diferentes zonas, se requieren las siguientes directivas:

```
"iam:GetRole"
"ec2:DescribeInstances"
"ec2:DescribeAddresses"
"ec2:AssociateAddress"
"ec2:DisassociateAddress"
```

Para obtener más información, consulte Alta disponibilidad en las zonas de disponibilidad de AWS.

Antes de iniciar la implementación

Antes de iniciar cualquier implementación de HA en AWS, lea el siguiente documento:

- Requisitos previos
- Limitaciones y directrices de uso
- Implementar una instancia de Citrix ADC VPX en AWS
- Alta disponibilidad

Implementar un par de alta disponibilidad de VPX en la misma zona de disponibilidad de AWS

July 15, 2022

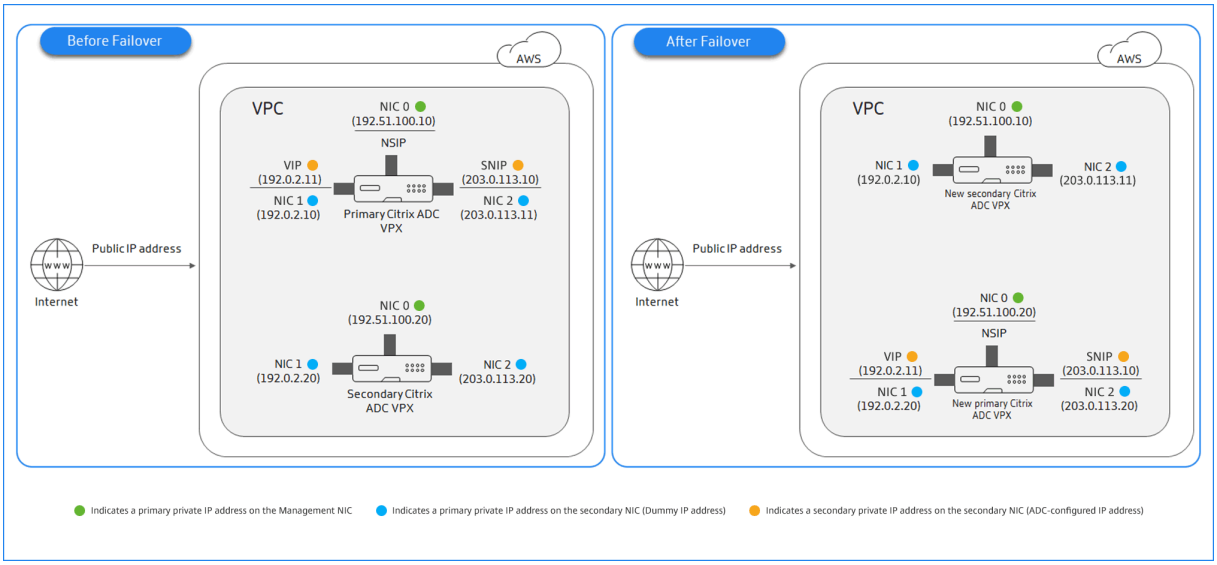
> **Nota:**
>
> A partir de la versión 13.1 compilación 27.x de Citrix ADC, el par VPX HA en la misma zona de disponibilidad de AWS admite direcciones IPv6.

Puede configurar dos instancias Citrix ADC VPX en AWS como un par de alta disponibilidad, en la misma zona de AWS, donde ambas instancias VPX están en la misma subred. La alta disponibilidad se logra migrando las direcciones IP privadas secundarias conectadas a las NIC (NIC del lado del cliente y del servidor) del nodo de alta disponibilidad principal al nodo de alta disponibilidad secundario después de la conmutación por error. También se migran todas las direcciones IP elásticas asociadas a las direcciones IP privadas secundarias.

El par de alta disponibilidad de Citrix ADC VPX admite direcciones IPv4 e IPv6 en la misma zona de disponibilidad de AWS.

En la siguiente ilustración se muestra un caso de conmutación por error de alta disponibilidad mediante la migración de direcciones IP privadas secundarias.

Ilustración 1. Un par de alta disponibilidad de Citrix ADC VPX en AWS, mediante la migración de IP privada



Antes de empezar el documento, lee los siguientes documentos:

- Requisitos previos
- Limitaciones y directrices de uso

- Implementar una instancia de Citrix ADC VPX en AWS
- Alta disponibilidad

Cómo implementar un par VPX HA en la misma zona

Este es el resumen de los pasos para implementar un par VPX HA en la misma zona:

1. Cree dos instancias VPX en AWS, cada una con tres NIC
2. Asignar una dirección IP privada secundaria de AWS a VIP y SNIP del nodo principal
3. Configurar VIP y SNIP en el nodo principal mediante direcciones IP privadas secundarias de AWS
4. Configurar alta disponibilidad en ambos nodos

Paso 1. Cree dos instancias VPX (nodos primario y secundario) mediante la misma VPC, cada una con tres NIC (Ethernet 0, Ethernet 1, Ethernet 2)

Siga los pasos que se indican en Implementación de una instancia Citrix ADC VPX en AWS mediante la consola web de AWS.

Paso 2. En el nodo principal, asigne direcciones IP privadas para Ethernet 1 (IP de cliente o VIP) y Ethernet 2 (IP de servidor back-end o SNIP)

La consola de AWS asigna automáticamente direcciones IP privadas principales a las NIC configuradas. Asigne más direcciones IP privadas a VIP y SNIP, conocidas como direcciones IP privadas secundarias.

Para asignar una dirección IP privada a una interfaz de red, siga estos pasos:

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija **Interfaces de red** y, a continuación, seleccione la interfaz de red conectada a la instancia.
3. Elija **Acciones > Administrar direcciones IP**.
4. Seleccione **Direcciones IPv4** o **Direcciones IPv6** según sus necesidades.
5. Para direcciones IPv4:
   a) Selecciona **Asignar nueva IP**.
   b) Introduce una dirección IPv4 específica que esté dentro del intervalo de subredes de la instancia o deja el campo en blanco para que Amazon seleccione una dirección IP para ti.
   c) (Opcional) Elija **Permitir reasignación** para permitir que se reasigne la dirección IP privada secundaria si ya está asignada a otra interfaz de red.
6. Para direcciones IPv6:
   a) Selecciona **Asignar nueva IP**.

b) Introduce una dirección IPv6 específica que esté dentro del rango de subredes de la instancia o deja el campo en blanco para que Amazon pueda seleccionar una dirección IP por ti.
c) (Opcional) Elija **Permitir reasignación** para permitir que se reasigne la dirección IP privada principal o secundaria si ya está asignada a otra interfaz de red.

7. Selecciona **Sí > Actualizar**.

En la **descripción de la instancia**, aparecen las direcciones IP privadas asignadas.

> **Nota:**
>
> En una implementación de par de alta disponibilidad IPv4, puede asignar solo las direcciones IPv4 secundarias en la interfaz y usarlas como direcciones VIP y SNIP. Sin embargo, en una implementación de par IPv6 HA, puede asignar la dirección IPv6 principal o la dirección IPv6 secundaria en la interfaz y utilizarlas como direcciones VIP y SNIP.

Paso 3. Configurar VIP y SNIP en el nodo principal, mediante direcciones IP privadas secundarias

Acceda al nodo principal mediante SSH. Abra un cliente ssh y escriba:

```
ssh -i <location of your private key> nsroot@<public DNS of the
   instance>
<!--NeedCopy-->
```

A continuación, configure VIP y SNIP.

Para VIP, escriba:

```
add ns ip <IPAddress> <netmask> -type <type>
<!--NeedCopy-->
```

Para SNIP, escriba:

```
add ns ip <IPAddress> <netmask> -type SNIP
<!--NeedCopy-->
```

Escriba `save config` para guardar.

Para ver las direcciones IP configuradas, escriba el siguiente comando:


```
show ns ip
<!--NeedCopy-->
```

Para obtener más información, consulte estos temas:

- Configurar y administrar direcciones IP virtuales (VIP)
- Configurar la dirección IP de NetScaler

Paso 4: configurar HA en ambas instancias

En el nodo principal, abra un cliente de Shell y escriba el siguiente comando:

```
add ha node <id> <private IP address of the management NIC of the
   secondary node>
<!--NeedCopy-->
```

En el nodo secundario, escriba el siguiente comando:

```
add ha node <id> < private IP address of the management NIC of the
   primary node >
<!--NeedCopy-->
```

Escriba `save config` para guardar la configuración.

Para ver los nodos de alta disponibilidad configurados, escriba `show ha node`.

Tras la conmutación por error, las direcciones IP privadas secundarias configuradas como VIP y SNIP en el nodo principal anterior se migran al nuevo nodo principal.

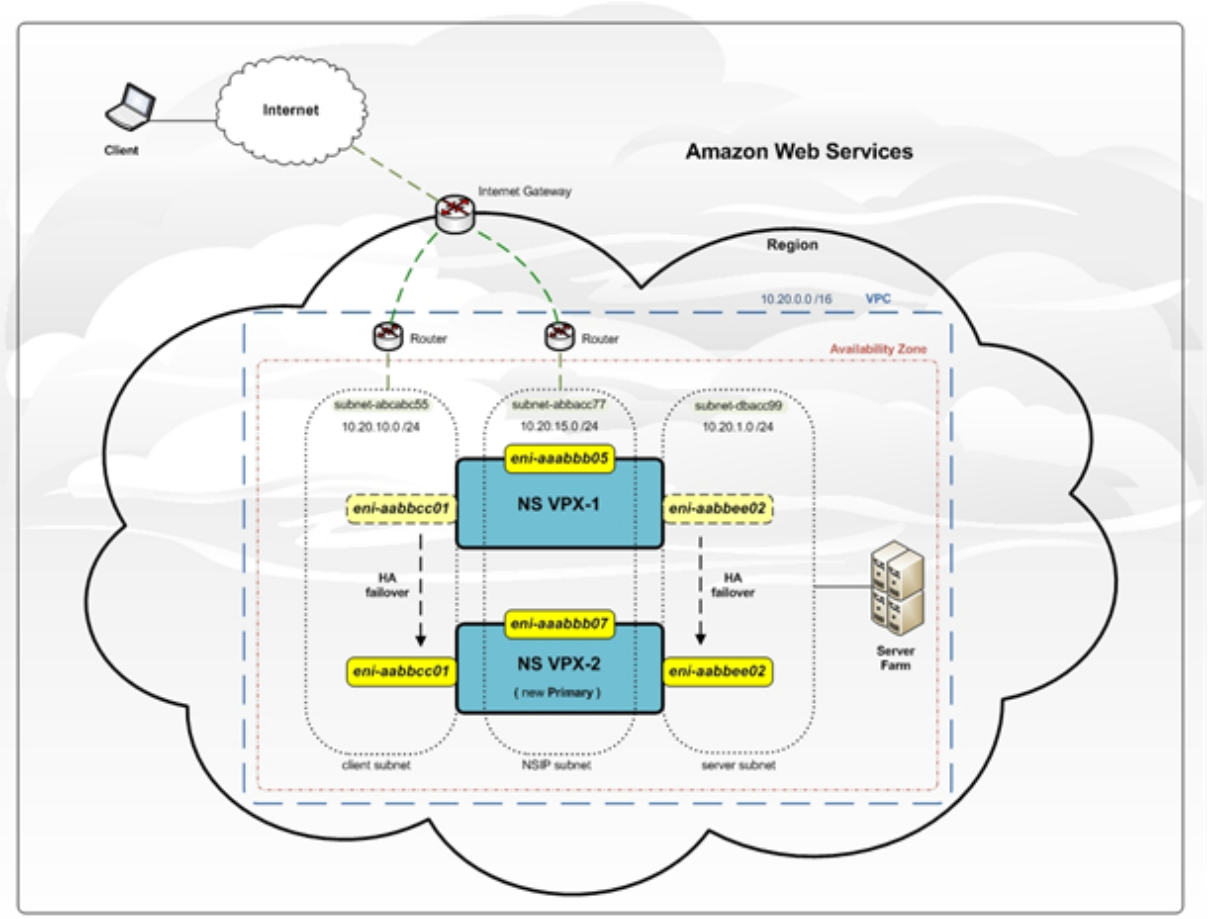
Para forzar una conmutación por error en un nodo, escriba `force HA`conmutación por error.

Método heredado para implementar un par de HA VPX

Antes de la versión 13.0 41.x, la alta disponibilidad dentro de la misma zona se lograba mediante la migración de la interfaz de red elástica (ENI) de AWS. Sin embargo, este método se retirará lentamente.

La siguiente ilustración muestra un ejemplo de la arquitectura de implementación de alta disponibilidad para instancias de Citrix ADC VPX en AWS.

Ilustración 1. Un par de Citrix ADC VPX HA en AWS, mediante migración ENI



Puede implementar dos instancias VPX en AWS como un par de HA mediante una de las siguientes opciones:

- Cree las instancias con la función de IAM manualmente mediante la AWS Management Console y, a continuación, configure la alta disponibilidad en ellas.
- O automatice la implementación de alta disponibilidad mediante la plantilla de Citrix CloudFormation.

La plantilla de CloudFormation reduce significativamente el número de pasos necesarios para crear un par de alta disponibilidad y crea automáticamente un rol de IAM. En esta sección se muestra cómo implementar un par Citrix ADC VPX HA (activo-pasivo) mediante la plantilla de Citrix CloudFormation.

Tenga en cuenta los siguientes puntos al implementar dos instancias de Citrix ADC VPX como un par de alta disponibilidad.

Puntos que tener en cuenta

- HA en AWS requiere que el nodo principal tenga al menos dos ENI (uno para la administración y el otro para el tráfico de datos) y que el nodo secundario tenga un ENI de administración. Sin em-

bargo, por motivos de seguridad, cree tres ENI en el nodo principal, porque esta configuración le permite segregar la red privada y pública (recomendado).

- El nodo secundario siempre tiene una interfaz ENI (para administración) y el nodo primario puede tener hasta cuatro ENI.
- Las direcciones NSIP de cada instancia VPX en un par de alta disponibilidad deben configurarse en el ENI predeterminado de la instancia.
- Amazon no permite ningún paquete de difusión/multidifusión en AWS. Como resultado, en una configuración de HA, los ENI del plano de datos se migran desde la instancia VPX principal a la secundaria cuando falla la instancia VPX principal.
- Como la ENI (de administración) predeterminada no se puede mover a otra instancia VPX, no utilice la ENI predeterminada para el tráfico de clientes y servidores (tráfico de plano de datos).
- El mensaje AWSCONFIG IOCTL NSAPI_HOTPLUG_INTF con éxito en la salida 0 del /var/log/ns.log indica que los dos ENI de datos se han adjuntado correctamente a la instancia secundaria (la nueva principal).
- La conmutación por error puede tardar hasta 20 segundos debido al mecanismo ENI de separación/conexión de AWS.
- Tras la conmutación por error, la instancia fallida siempre se reinicia.
- Los paquetes de latidos se reciben solo en la interfaz de administración.
- El archivo de configuración de las instancias VPX principales y secundarias se sincroniza, incluida la contraseña `nsroot`. La contraseña `nsroot` del nodo secundario se establece en la del nodo primario después de la sincronización de la configuración de HA.
- Para tener acceso a los servidores API de AWS, la instancia VPX debe tener asignada una dirección IP pública o la redirección debe configurarse correctamente a nivel de subred de VPC que apunte a la puerta de enlace de Internet de la VPC.
- Servidores de nombres y servidores DNS se configuran a nivel de VPC mediante las opciones DHCP.
- La plantilla de Citrix CloudFormation no crea una configuración de alta disponibilidad entre diferentes zonas de disponibilidad.
- La plantilla de Citrix CloudFormation no crea un modo INC.
- Los mensajes de depuración de AWS están disponibles en el archivo de registros, /var/log/ns.log, en la instancia VPX.

Implemente un par de alta disponibilidad mediante la plantilla Citrix CloudFormation

Antes de iniciar la plantilla de CloudFormation, asegúrese de cumplir los siguientes requisitos:

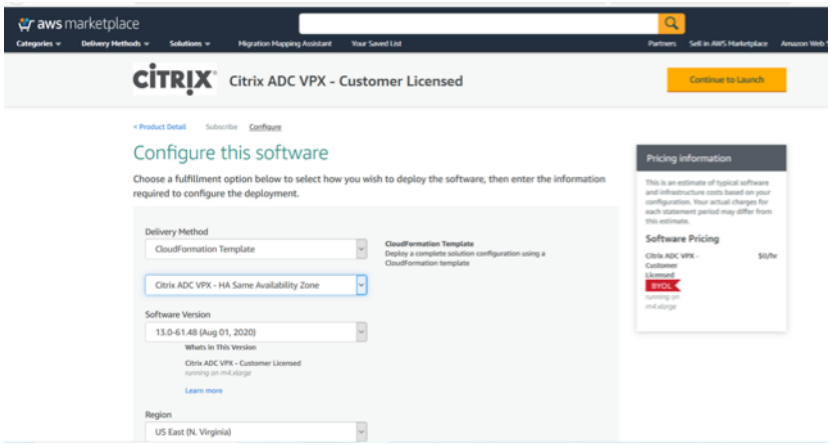
- UN VPC
- Tres subredes dentro de la VPC
- Un grupo de seguridad con puertos UDP 3003, TCP 3009—3010, HTTP y SSH abiertos
- Un par de llaves

- Crea una puerta de enlace a internet
- Modificar tablas de rutas para que las redes de clientes y de administración apunten a la puerta de enlace de Internet

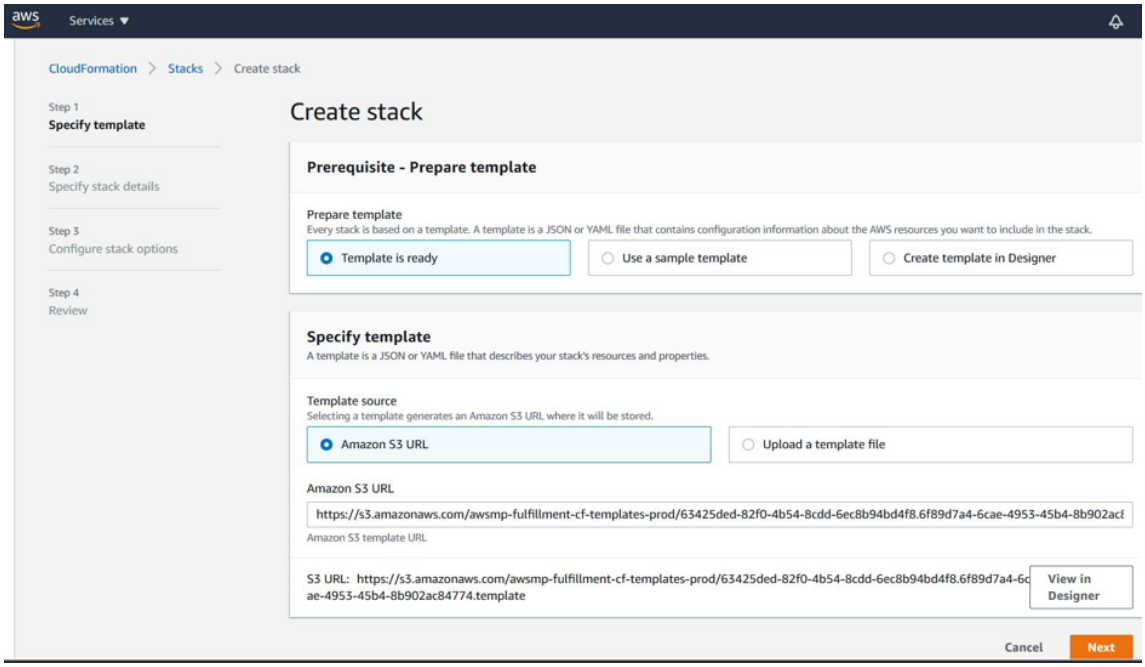
> **Nota**
>
> La plantilla de Citrix CloudFormation crea automáticamente un rol de IAM. Las funciones de IAM existentes no aparecen en la plantilla.

Para iniciar la plantilla de Citrix CloudFormation:

1. Inicie sesión en el mercado de AWS mediante sus credenciales de AWS.
2. En el campo de búsqueda, escriba **Citrix ADC VPX** para buscar la AMI de Citrix ADC y haga clic en **Ir**.
3. En la página de resultados de búsqueda, haga clic en la oferta de Citrix ADC VPX deseada.
4. Haga clic en la ficha **Precios** para ir a **Información de precios**.
5. Seleccione la región y la **opción de gestión logística** como **Citrix ADC VPX: licencia del cliente**.
6. Haga clic en **Continuar para suscribirse**.
7. Consulte los detalles en la página **Suscribirse** y haga clic en **Continuar con la configuración**.
8. Seleccione **Método de entrega** como **plantilla de CloudFormation**.
9. Seleccione la plantilla de CloudFormation requerida.
10. Seleccione **Versión de software** y **región**y haga clic en **Continuar para iniciar**.



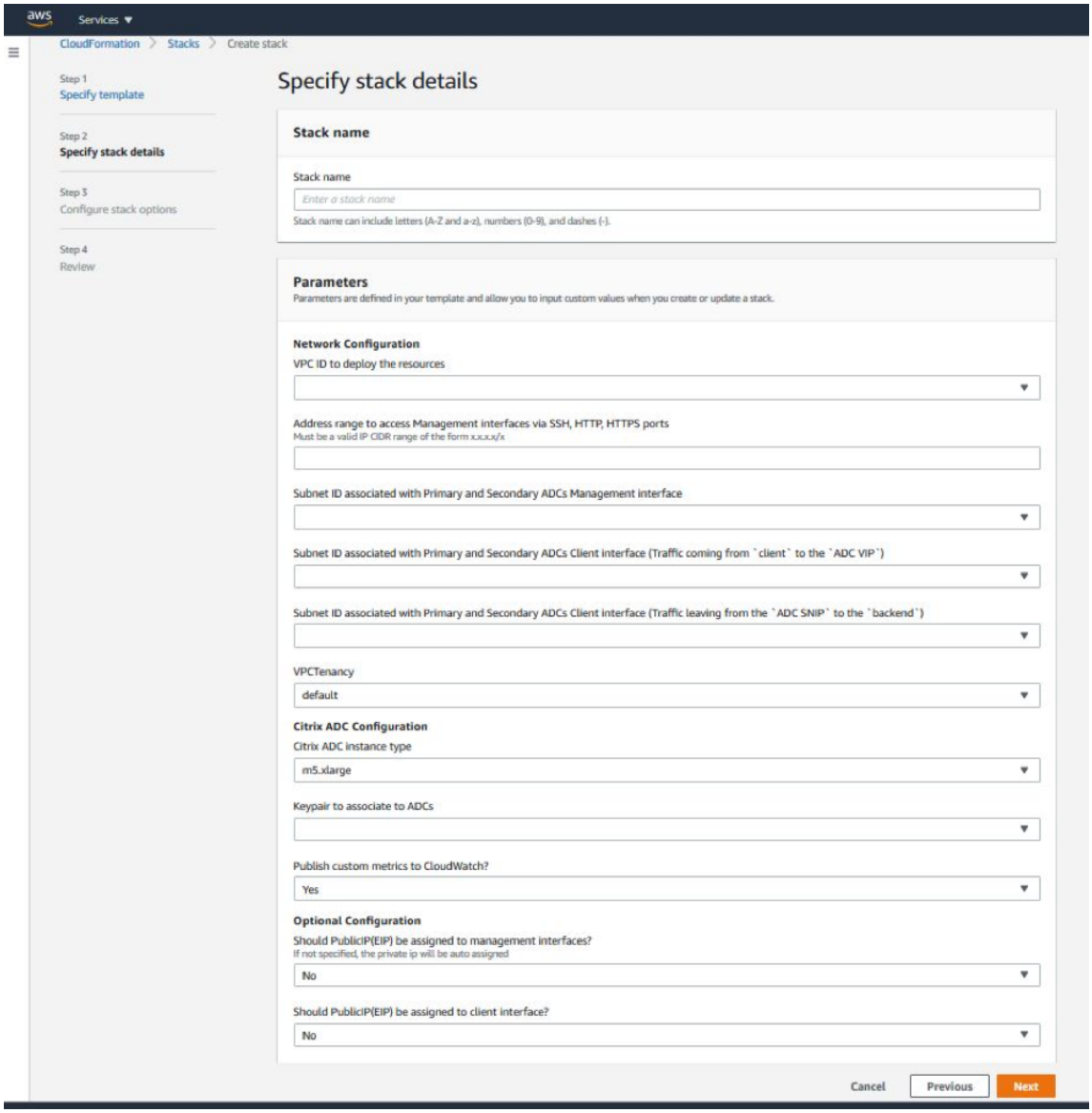
11. En **Elegir acción**, seleccione **Launch CloudFormation** y haga clic en **Launch**. Aparece la página **Crear pila**.
12. Haga clic en **Siguiente**.



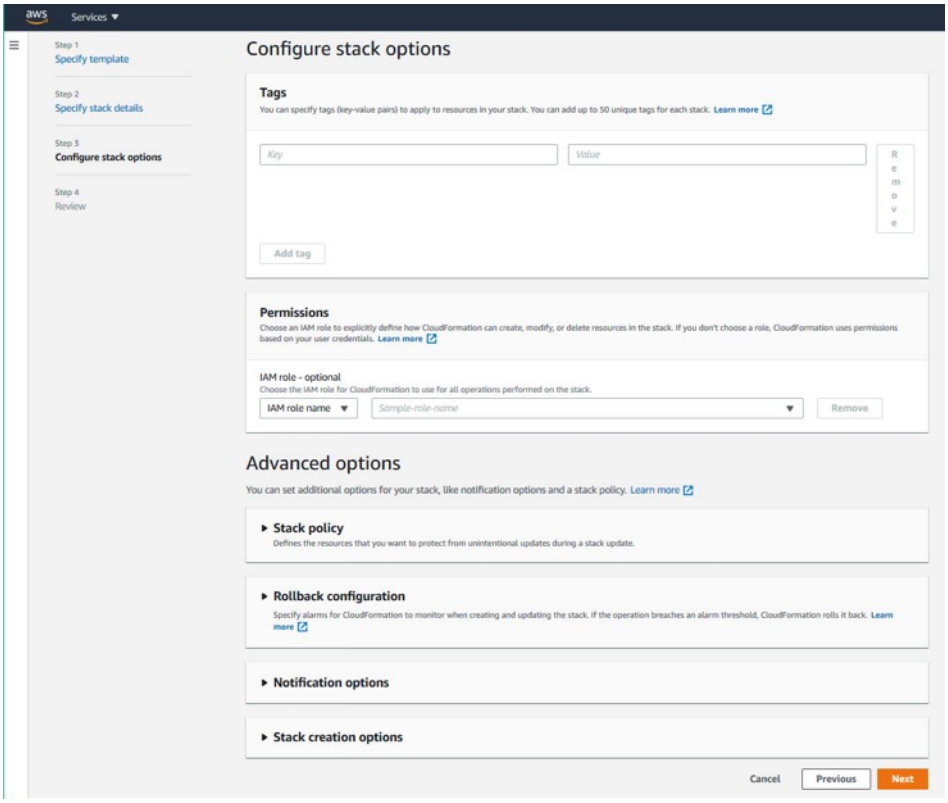
13. Aparece la página **Especificar detalles de pila**. Introduzca los siguientes detalles.

    - Escriba un **nombre de pila**. El nombre debe tener 25 caracteres.
    - En **Configuración de red**, lleve a cabo lo siguiente:
        - Seleccione **Subred de administración**, **Subred de cliente** y **Subred de servidor**. Asegúrese de seleccionar las subredes correctas que creó en la VPC que seleccionó bajo ID de VPC.
        - Agregue **IP de administración primaria**, **IP de administración secundaria**, **IP de cliente**e **IP de servidor**. Las direcciones IP deben pertenecer a las mismas subredes de las respectivas subredes. Alternativamente, puede dejar que la plantilla asigne las direcciones IP automáticamente.
        - Seleccione el **valor predeterminado** para **VPCTenancy**.
    - En **Configuración de Citrix ADC**, lleve a cabo lo siguiente:
        - Seleccione **m5.xlarge** para **Tipo de instancia**.
        - Seleccione el par de claves que ya ha creado en el menú de **Par de claves**.
        - De forma predeterminada, ¿ **Publicar métricas personalizadas en CloudWatch?** está configurada en **Sí**. Si quiere inhabilitar esta opción, seleccione **No**.

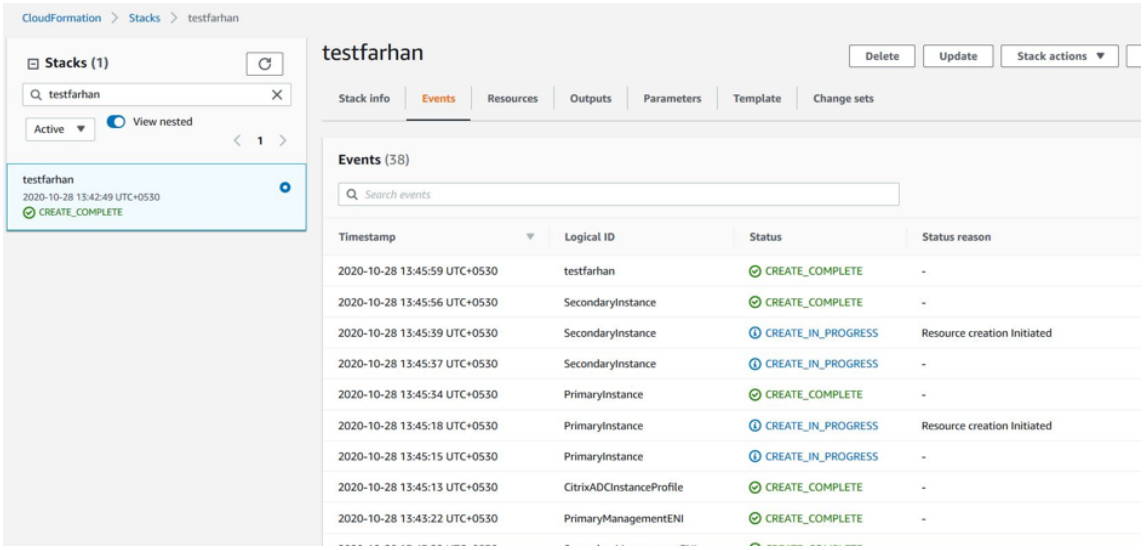
          Para obtener más información sobre las métricas de CloudWatch, consulte Supervisar las instancias mediante Amazon CloudWatch.
    - En **Configuración opcional**, haga lo siguiente:
        - De forma predeterminada, **¿Debería asignarse publicIP(EIP) a las interfaces de administración?** está establecida en **No**.
        - De forma predeterminada, **¿Debería asignarse publicIP(EIP) a la interfaz del cliente?** está establecida en **No**.



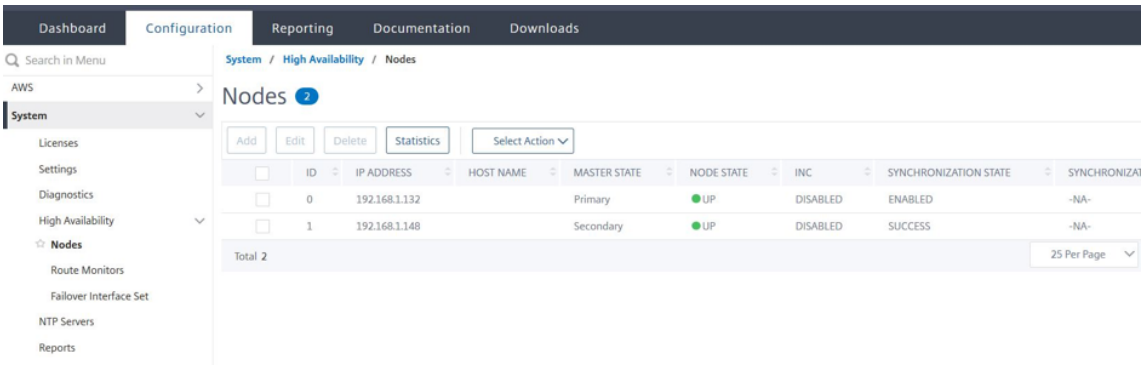
14. Haga clic en **Siguiente**.
15. Aparece la página **Configurar opciones de pila**. Esta página es opcional.



16. Haga clic en **Siguiente**.
17. Aparecerá la página **Opciones**. (Esta es una página opcional). Haga clic en **Siguiente**.
18. Aparecerá la página **Revisar**. Dedique un momento a revisar la configuración y realizar cambios, si es necesario.
19. Seleccione la opción **Acepto que AWS CloudFormation podría crear recursos de IAM.** casilla de verificación y, a continuación, haga clic en **Crear pila**.
20. Aparece el estado **CREATE-IN-PROGRESS**. Espere hasta que el estado sea **CREATE-COMPLETE**. Si el estado no cambia a **COMPLETADO**, compruebe la ficha **Eventos** por el motivo de un error y vuelva a crear la instancia con las configuraciones adecuadas.



21. Después de crear un recurso de IAM, vaya a **EC2 Management Console > Instancias**. Encontrará dos instancias VPX creadas con el rol de IAM. Los nodos principal y secundario se crean cada uno con tres direcciones IP privadas y tres interfaces de red.
22. Inicie sesión en el nodo principal con el nombre de usuario `nsroot` y el ID de instancia como contraseña. Desde la GUI, vaya a **Sistema > Alta disponibilidad > Nodos**. Citrix ADC VPX ya está configurado en par HA mediante la plantilla CloudFormation.
23. Aparece el par Citrix ADC VPX HA.



Supervisar las instancias con Amazon CloudWatch

Puede utilizar el servicio Amazon CloudWatch para supervisar un conjunto de métricas de Citrix ADC VPX, como la utilización de la CPU y la memoria, y el rendimiento. CloudWatch supervisa los recursos y las aplicaciones que se ejecutan en AWS, en tiempo real. Puede acceder al panel de Amazon CloudWatch mediante la consola de administración de AWS. Para obtener más información, consulte Amazon CloudWatch.

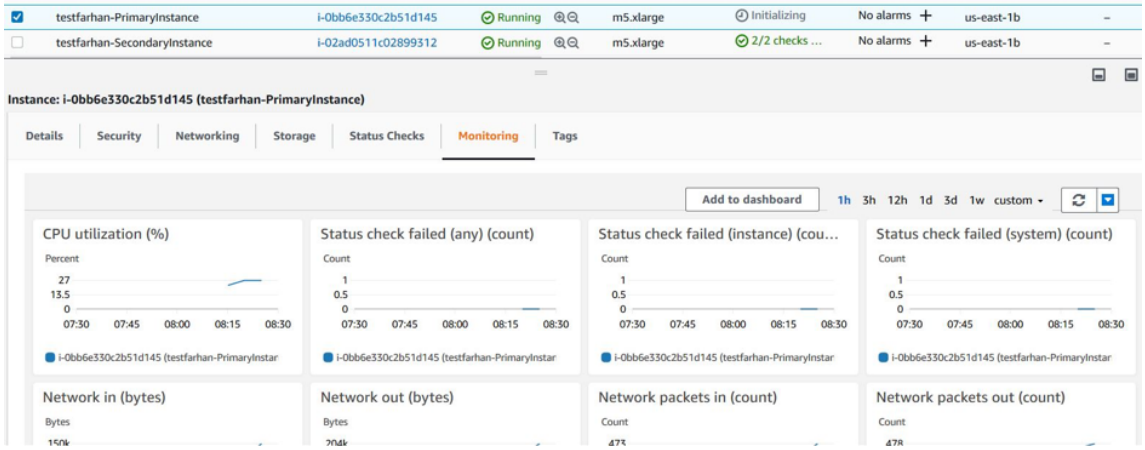
Puntos que tener en cuenta

- Si implementa una instancia de Citrix ADC VPX en AWS mediante la consola web de AWS, el servicio CloudWatch está habilitado de forma predeterminada.
- Si implementa una instancia de Citrix ADC VPX mediante la plantilla de Citrix CloudFormation, la opción predeterminada es “Sí. “ Si quiere inhabilitar el servicio CloudWatch, seleccione “No. “
- Las métricas están disponibles para la CPU (administración y uso de la CPU de paquetes), la memoria y el rendimiento (entrante y saliente).

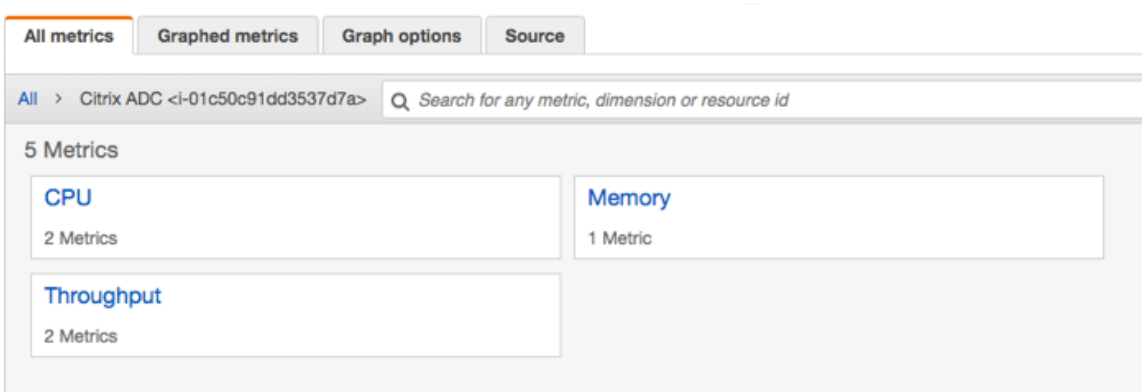
Cómo ver las métricas de CloudWatch

Para ver las métricas de CloudWatch de su instancia, siga estos pasos:

1. Inicie sesión en la **consola de administración de AWS > EC2 > Instancias**.
2. Seleccione la instancia.
3. Haga clic en **Supervisión**.
4. Haga clic en **Ver todas las métricas de CloudWatch**.

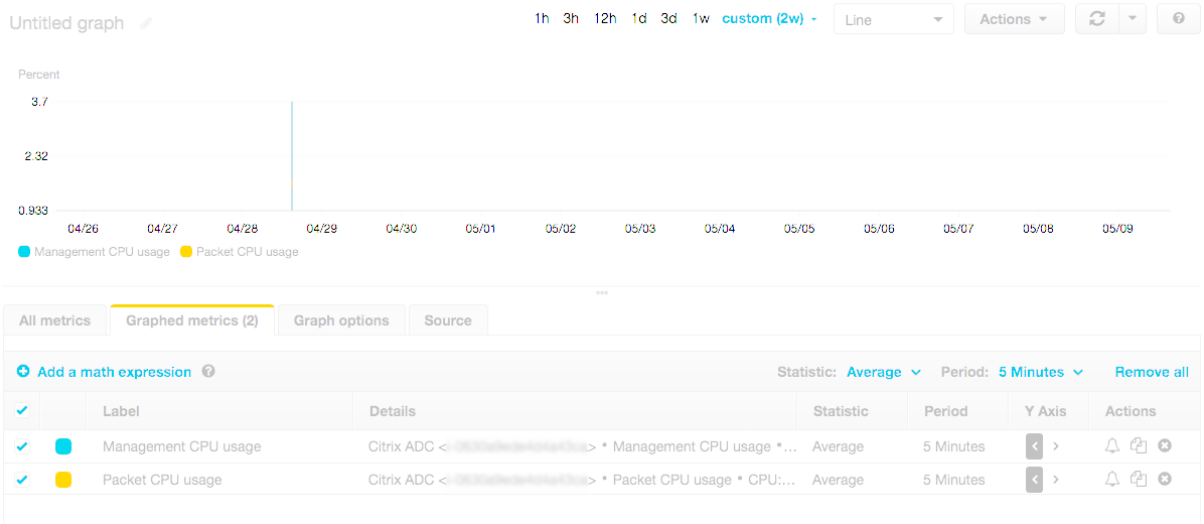


5. En Todas las métricas, haga clic en su ID de instancia.



6. Haga clic en las métricas que quiera ver y establezca la duración (en minutos, horas, días, semanas, meses).
7. Haga clic en **Métricas gráficas** para ver las estadísticas de uso. Use las **opciones de Gráfica** para personalizar su gráfica.

Ilustración. Métricas gráficas para el uso de la CPU



Configuración de SR-IOV en una configuración de alta disponibilidad

La compatibilidad con interfaces SR-IOV en una configuración de alta disponibilidad está disponible desde Citrix ADC versión 12.0 57.19 en adelante. Para obtener más información sobre cómo configurar SR-IOV, consulte Configuración de instancias Citrix ADC VPX para utilizar la interfaz de red SR-IOV.

Recursos conexos

Cómo funciona la alta disponibilidad en AWS

Alta disponibilidad en diferentes zonas de disponibilidad de AWS

March 9, 2022

Puede configurar dos instancias de Citrix ADC VPX en dos subredes diferentes o en dos zonas de disponibilidad de AWS diferentes, como un par activo-pasivo de alta disponibilidad en modo de configuración de red independiente (INC). Si, por cualquier motivo, el nodo principal no puede aceptar conexiones, el nodo secundario se hace cargo.

Para obtener más información sobre la alta disponibilidad, consulte Alta disponibilidad. Para obtener más información sobre INC, consulte Configuración de nodos de alta disponibilidad en distintas subredes.

Puntos que tener en cuenta

- Lea los siguientes documentos antes de comenzar la implementación:
  - Terminología de AWS
  - Requisitos previos
  - Limitaciones y directrices de uso
- El par de alta disponibilidad VPX puede residir en la misma zona de disponibilidad en una subred diferente o en dos zonas de disponibilidad de AWS diferentes.
- Citrix recomienda usar diferentes subredes para la administración (NSIP), el tráfico de clientes (VIP) y el servidor back-end (SNIP).
- La alta disponibilidad debe establecerse en el modo Configuración de red independiente (INC) para que funcione una conmutación por error.
- Las dos instancias deben tener el puerto 3003 abierto para el tráfico UDP, ya que se usa para los latidos.
- Las subredes de administración de ambos nodos deben tener acceso a Internet o al servidor API de AWS a través de NAT interna para que las demás API funcionen.
- El rol de IAM debe tener permiso E2 para la migración de IP pública o IP elástica (EIP) y permisos de tabla de ruta EC2 para la migración de IP privada.

Puede implementar alta disponibilidad en las zonas de disponibilidad de AWS de las siguientes formas:

- Uso de direcciones IP elásticas
- Uso de direcciones IP privadas

Referencias adicionales

Para obtener más información sobre Citrix Application Delivery Management (ADM) para AWS, consulte Instalar el agente Citrix ADM en AWS.

Implementación de un par de alta disponibilidad VPX con direcciones IP elásticas en distintas zonas de AWS

January 31, 2022

Puede configurar dos instancias de Citrix ADC VPX en dos subredes diferentes o en dos zonas de disponibilidad de AWS diferentes mediante direcciones IP elásticas (EIP) en el modo INC.

Para obtener más información sobre la alta disponibilidad, consulte Alta disponibilidad. Para obtener más información sobre INC, consulte Configuración de nodos de alta disponibilidad en distintas subredes.

Cómo funciona la HA con direcciones EIP en diferentes zonas de AWS

Tras la conmutación por error, el EIP del VIP de la instancia principal migra a la secundaria, que se convierte en la nueva instancia principal. En el proceso de conmutación por error, la API de AWS:

1. Comprueba los servidores virtuales que tienen `IPSets` adjuntado a ellos.
2. Busca la dirección IP que tiene una IP pública asociada, de las dos direcciones IP en las que está escuchando el servidor virtual. Uno que se conecta directamente al servidor virtual y el que se conecta a través del conjunto de IP.
3. Reasocia la IP pública (EIP) a la IP privada que pertenece al nuevo VIP principal.

> **Nota**
>
> Para proteger su red de ataques como la denegación de servicio (DoS), al utilizar una EIP, puede crear grupos de seguridad en AWS para restringir el acceso a la IP. Para obtener una alta disponibilidad, puede cambiar de EIP a una solución de movimiento IP privada según sus implementaciones.

Cómo implementar un par de alta disponibilidad VPX con direcciones IP elásticas en diferentes zonas de AWS

A continuación se presenta un resumen de los pasos para implementar un par VPX en dos subredes diferentes o en dos zonas de disponibilidad de AWS diferentes.

1. Cree una nube privada virtual de Amazon.
2. Implemente dos instancias VPX en dos zonas de disponibilidad diferentes o en la misma zona pero en subredes diferentes.
3. Configurar alta disponibilidad
    a) Configure la alta disponibilidad en modo INC en ambas instancias.
    b) Agregue un conjunto de IP en ambas instancias.
    c) Enlazar el conjunto de IP en ambas instancias al VIP.
    d) Agrega un servidor virtual en la instancia principal.

Para los pasos 1 y 2, utilice la consola de AWS. Para los pasos 3, use la GUI de Citrix ADC VPX o la CLI.

Paso 1. Cree una nube privada virtual (VPC) de Amazon.

Paso 2. Implemente dos instancias VPX en dos zonas de disponibilidad diferentes o en la misma zona pero en subredes diferentes. Adjunte un EIP al VIP de la VPX principal.

Para obtener más información sobre cómo crear una VPC e implementar una instancia VPX en AWS, consulte Implementación de una instancia independiente Citrix ADC VPX en AWS and Scenario: instancia independiente

Paso 3. Configure la alta disponibilidad. Puede utilizar la CLI o la GUI de Citrix ADC VPX para configurar la alta disponibilidad.

Configurar la alta disponibilidad mediante la CLI

1. Configure la alta disponibilidad en modo INC en ambas instancias.

   En el nodo principal:

   ```
   add ha node 1 <sec_ip> -inc ENABLED
   ```

   En el nodo secundario:

   ```
   add ha node 1 <prim_ip> -inc ENABLED
   ```

   <sec_ip> hace referencia a la dirección IP privada de la NIC de administración del nodo secundario

   <prim_ip> hace referencia a la dirección IP privada de la NIC de administración del nodo principal

2. Agregue el conjunto de IP en ambas instancias.

   Escriba el siguiente comando en ambas instancias.

   ```
   add ipset <ipsetname>
   ```

3. Enlaza el conjunto de IP al conjunto VIP en ambas instancias.

   Escriba el siguiente comando en ambas instancias:

   ```
   add ns ip <secondary vip> <subnet> -type VIP
   ```

   ```
   bind ipset <ipsetname> <secondary VIP>
   ```

   > **Nota**
   >
   > Puede vincular el conjunto de IP a la VIP principal o a la VIP secundaria. Sin embargo, si vincula el conjunto de IP a la VIP principal, use la VIP secundaria para agregarla al servidor virtual y viceversa.

4. Agregue un servidor virtual en la instancia principal.

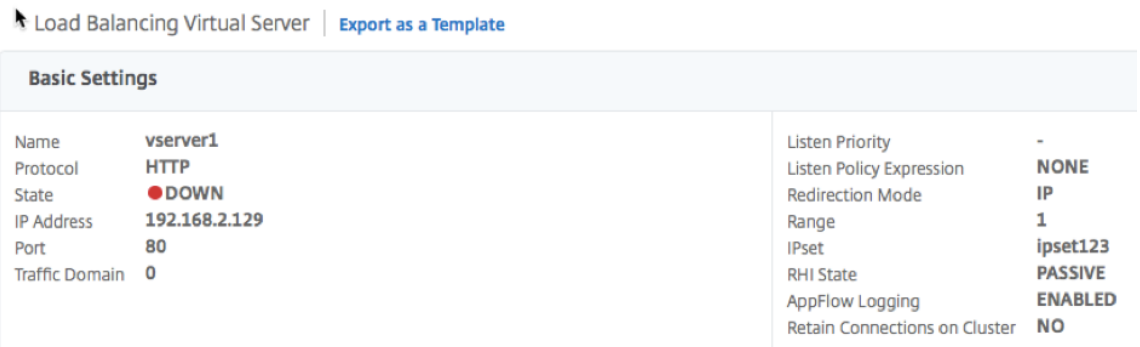
   Escriba el siguiente comando:


```
add <server_type> vserver <vserver_name> <protocol> <primary_vip> <port
> -ipset \<ipset_name>
```

Configure la alta disponibilidad mediante la interfaz gráfica de usuario

1. Configurar la alta disponibilidad en modo INC en ambas instancias
2. Inicie sesión en el nodo principal con el nombre de usuario `nsroot` y el ID de instancia como contraseña.
3. Desde la GUI, vaya a **Configuración** > **Sistema** > **Alta disponibilidad**. Haga clic en **Agregar**.
4. En el campo **Dirección IP de nodo remoto**, agregue la dirección IP privada de la NIC de administración del nodo secundario.
5. Seleccione **Activar el modo NIC (Configuración de red independiente)** en el nodo propio.
6. En **Credencial de inicio de sesión del sistema remoto**, agregue el nombre de usuario y la contraseña del nodo secundario y haga clic en **Crear**.
7. Repita los pasos en el nodo secundario.
8. Agregue el conjunto de IP y el conjunto de IP de enlace al conjunto VIP en ambas instancias.
9. Desde la GUI, vaya a **Sistema** > **Red** > **IP** > **Agregar**.
10. Agregue los valores requeridos para Dirección IP, máscara de red, Tipo de IP (IP virtual) y haga clic en **Crear**.
11. Vaya a **Sistema** > **Red** > **Conjuntos de IP** > **Agregar**. Agregue un nombre de conjunto de IP y haga clic en **Insertar**.
12. En la página IPv4s, seleccione la IP virtual y haga clic en **Insertar**. Haga clic en **Crear** para crear el conjunto de IP.
13. Agregar un servidor virtual en la instancia principal

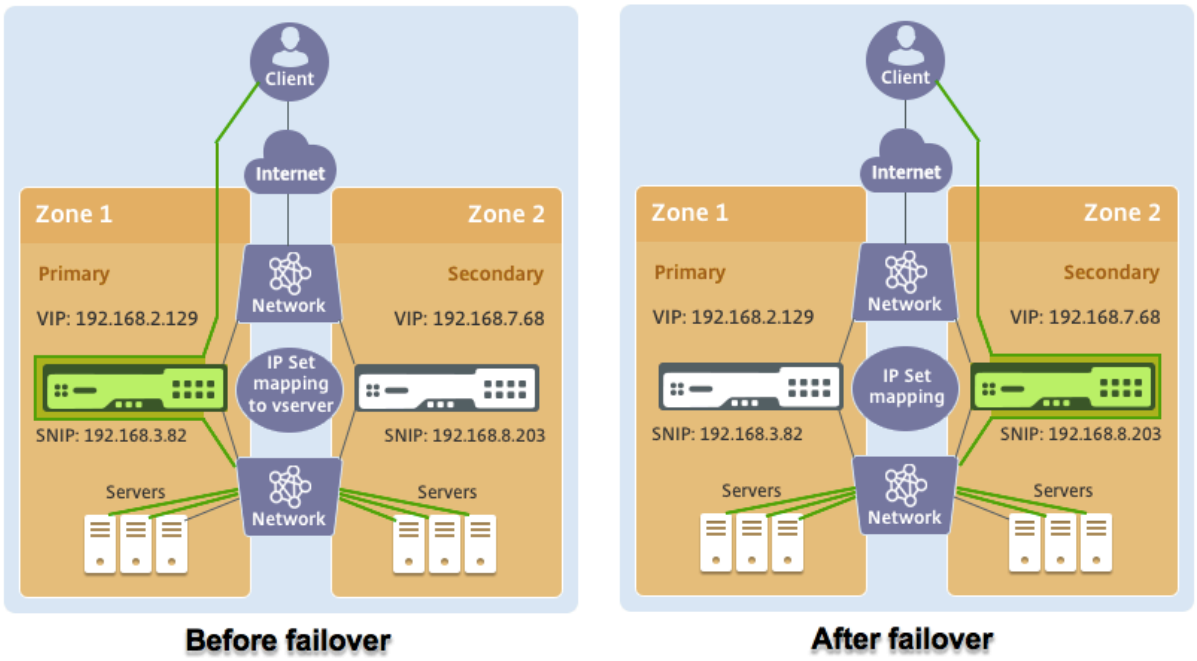
    En la GUI, vaya a **Configuración** > **Administración del tráfico** > **Servidores virtuales** > **Agregar**.



Caso

En este caso, se crea una única VPC. En esa VPC, se crean dos instancias VPX en dos zonas de disponibilidad. Cada instancia tiene tres subredes: una para administración, otra para el cliente y otra para el servidor back-end. Se adjunta una EIP al VIP del nodo principal.

Diagrama: Este diagrama ilustra la configuración de alta disponibilidad de Citrix ADC VPX en modo INC, en AWS



En este caso, utilice la CLI para configurar la alta disponibilidad.

1. Configure la alta disponibilidad en modo INC en ambas instancias.

   Escriba los siguientes comandos en los nodos primario y secundario.

   En primaria:

   ```
   add ha node 1 192.168.6.82 -inc enabled
   ```

   En este caso, 192.168.6.82 se refiere a la dirección IP privada de la NIC de administración del nodo secundario.

   En secundaria:

   ```
   add ha node 1 192.168.1.108 -inc enabled
   ```

   En este caso, 192.168.1.108 se refiere a la dirección IP privada de la NIC de administración del nodo principal.

2. Agregue un conjunto de IP y enlace el conjunto de IP a la VIP en ambas instancias

   En primaria:


```
add ipset ipset123
add ns ip 192.168.7.68 255.255.255.0 -type VIP
bindipset ipset123 192.168.7.68
```

En secundaria:

```
add ipset ipset123
add ns ip 192.168.7.68 255.255.255.0 -type VIP
bind ipset ipset123 192.168.7.68
```

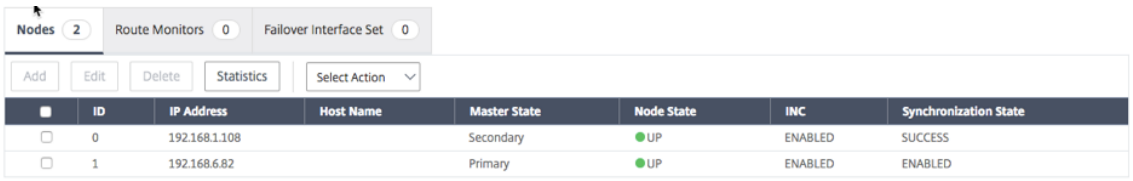
3. Agregue un servidor virtual en la instancia principal.

   El siguiente comando:

   ```
   add lbvserver vserver1 http 192.168.2.129 80 -ipset ipset123
   ```

4. Guarde la configuración.

5. Después de una conmutación por error forzada, el secundario se convierte en el nuevo primario.



Implementar un par de alta disponibilidad VPX con direcciones IP privadas en distintas zonas de AWS

February 19, 2022

Puede configurar dos instancias de Citrix ADC VPX en dos subredes diferentes o en dos zonas de disponibilidad de AWS diferentes mediante direcciones IP privadas en el modo INC. Esta solución se puede integrar fácilmente con el par de alta disponibilidad VPX multizona existente con direcciones IP elásticas. Por lo tanto, puede utilizar ambas soluciones juntas.

Para obtener más información sobre la alta disponibilidad, consulte Alta disponibilidad. Para obtener más información sobre INC, consulte Configuración de nodos de alta disponibilidad en distintas subredes.

> Nota:
>
> Esta implementación se admite desde Citrix ADC versión 13.0 compilación 67.39 en adelante. Esta implementación es compatible con AWS Transit Gateway.

Emparejamiento de alta disponibilidad con direcciones IP privadas mediante una VPC no compartida de AWS

Requisitos previos

Asegúrese de que el rol de IAM asociado a su cuenta de AWS tenga los siguientes permisos de IAM:

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeAddresses",
                "ec2:AssociateAddress",
                "ec2:DisassociateAddress",
                "ec2:DescribeRouteTables",
                "ec2:DeleteRoute",
                "ec2:CreateRoute",
                "ec2:ModifyNetworkInterfaceAttribute",
                "iam:SimulatePrincipalPolicy",
                "iam:GetRole"
            ],
            "Resource": "*",
            "Effect": "Allow"
         }

    ]
 }


<!--NeedCopy-->
```


Implemente un par de alta disponibilidad de VPX con direcciones IP privadas mediante una VPC no compartida de AWS

A continuación se presenta un resumen de los pasos para implementar un par VPX en dos subredes diferentes o en dos zonas de disponibilidad de AWS distintas mediante direcciones IP privadas.

1. Cree una nube privada virtual de Amazon.
2. Implementa dos instancias VPX en dos zonas de disponibilidad diferentes.
3. Configurar alta disponibilidad
    a) Configure la alta disponibilidad en modo INC en ambas instancias.
    b) Agregue las tablas de redirección respectivas en la VPC que apunta a la interfaz del cliente.
    c) Agrega un servidor virtual en la instancia principal.

Para los pasos 1, 2 y 3b, use la consola de AWS. Para los pasos 3a y 3c, use la GUI de Citrix ADC VPX o la CLI.

Paso 1. Cree una nube privada virtual (VPC) de Amazon.

Paso 2. Implemente dos instancias VPX en dos zonas de disponibilidad diferentes con el mismo número de ENI (interfaz de red).

Para obtener más información sobre cómo crear una VPC e implementar una instancia VPX en AWS, consulte Implementación de una instancia independiente Citrix ADC VPX en AWS and Scenario: instancia independiente

Paso 3. Configure las direcciones VIP de ADC eligiendo una subred que no se superponga con las subredes de Amazon VPC. Si su VPC es 192.168.0.0/16, para configurar las direcciones VIP de ADC, puede elegir cualquier subred de estos intervalos de direcciones IP:

- 0.0.0.0 - 192.167.0.0
- 192.169.0.0 - 254.255.255.0

En este ejemplo, la subred 10.10.10.0/24 elegida y se crearon VIP en esta subred. Puede elegir cualquier subred que no sea la subred VPC (192.168.0.0/16).

Paso 4. Agregue una ruta que apunte a la interfaz de cliente (VIP) del nodo principal desde la tabla de rutas de la VPC.

En la CLI de AWS, escriba el siguiente comando:

```
aws ec2 create-route --route-table-id rtb-2272532 --destination-cidr-
    block 10.10.10.0/24 --gateway-id <eni-client-primary>
<!--NeedCopy-->
```

Desde la GUI de AWS, lleve a cabo los siguientes pasos para agregar una ruta:

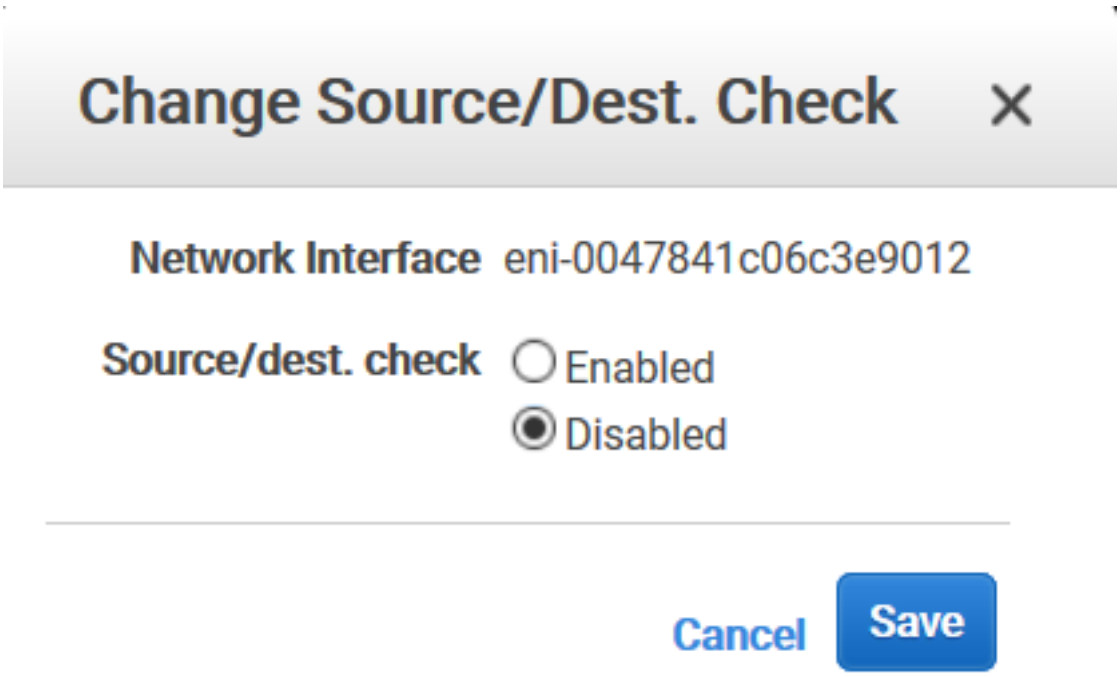
1. Abra la consola de Amazon EC2.

2. En el panel de navegación, elija **Tablas de redirección**y seleccione la tabla de redirección.
3. Seleccione **Acciones**y haga clic en **Modificar rutas**.
4. Para agregar una ruta, elige **Agregar ruta**. En **Destino**, introduzca el bloque CIDR de destino, una única dirección IP o el ID de una lista de prefijos. Para ID de puerta de enlace, seleccione el ENI de una interfaz de cliente del nodo principal.

> Nota
>
> Debe inhabilitar la **comprobación de origen/destino** en el ENI del cliente de la instancia principal.

Para inhabilitar la comprobación de origen/destino de una interfaz de red mediante la consola, realice los siguientes pasos:

1. Abra la consola de Amazon EC2.
2. En el panel de navegación, elija **Interfaces de red**.
3. Seleccione la interfaz de red de una interfaz de cliente principal, elija **Acciones**y haga clic en **Cambiar fuente/destino. Comprobar**.
4. En el cuadro de diálogo, seleccione **Inhabilitado**y haga clic en **Guardar**.



Paso 5. Configure la alta disponibilidad. Puede utilizar la CLI o la GUI de Citrix ADC VPX para configurar la alta disponibilidad.

Configurar la alta disponibilidad mediante la CLI

1. Configure la alta disponibilidad en modo INC en ambas instancias.

   En el nodo principal:

   ```
   1 add ha node 1 <sec_ip> -inc ENABLED
   2 <!--NeedCopy-->
   ```

   En el nodo secundario:

   ```
   1 add ha node 1 <prim_ip> -inc ENABLED
   2 <!--NeedCopy-->
   ```

   <sec_ip>hace referencia a la dirección IP privada de la NIC de administración del nodo secundario.

   <prim_ip>hace referencia a la dirección IP privada de la NIC de administración del nodo principal.

2. Agregue un servidor virtual en la instancia principal. Debe agregarlo desde la subred elegida, por ejemplo, 10.10.10.0/24.

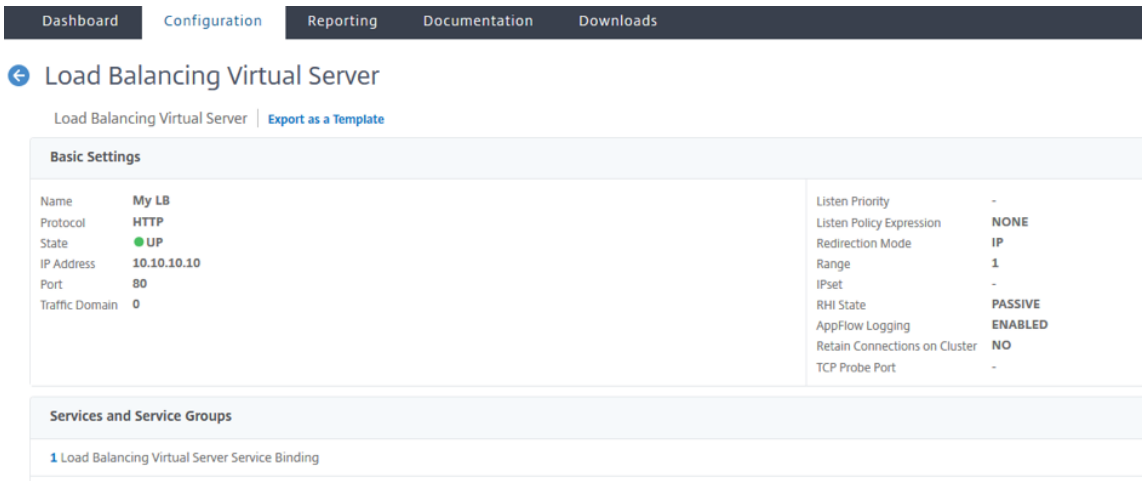
   Escriba el siguiente comando:

```
1 add \<server\_type\> vserver \<vserver\_name\> \<protocol\> \<
     primary\_vip\> \<port\>
2 <!--NeedCopy-->
```

Configure la alta disponibilidad mediante la interfaz gráfica de usuario

1. Configurar la alta disponibilidad en modo INC en ambas instancias
2. Inicie sesión en el nodo principal con el nombre de usuario `nsroot` y el ID de instancia como contraseña.
3. Vaya a **Configuración** > **Sistema** > **Alta disponibilidad**y haga clic en **Agregar**.
4. En el campo **Dirección IP de nodo remoto**, agregue la dirección IP privada de la NIC de administración del nodo secundario.
5. Seleccione **Activar el modo NIC (Configuración de red independiente)** en el nodo propio.
6. En **Credencial de inicio de sesión del sistema remoto**, agregue el nombre de usuario y la contraseña del nodo secundario y haga clic en **Crear**.
7. Repita los pasos en el nodo secundario.
8. Agregar un servidor virtual en la instancia principal

   Vaya a **Configuración** > **Administración del tráfico** > **Servidores virtuales** > **Agregar**.



Implemente un par de alta disponibilidad de VPX con direcciones IP privadas mediante la VPC compartida de AWS

En un modelo de VPC compartida de AWS, la cuenta propietaria de la VPC (propietario) comparte una o más subredes con otras cuentas (participantes). Por lo tanto, tiene una cuenta de propietario de VPC y una cuenta de participante. Después de compartir una subred, los participantes pueden ver, crear, modificar y eliminar sus recursos de aplicación en las subredes compartidas con ellos. Los participantes no pueden ver, modificar ni eliminar recursos que pertenezcan a otros participantes o al propietario de la VPC.

Para obtener información sobre la VPC compartida de AWS, consulte la documentación de AWS.

> Nota:
>
> Los pasos de configuración para implementar un par de alta disponibilidad de VPX con direcciones IP privadas mediante una VPC compartida de AWS son los mismos que los de Implementar un par de alta disponibilidad de VPX con direcciones IP privadas mediante una VPC no compartida de AWS, con la siguiente excepción:
>
> - Las tablas de rutas de la VPC que apuntan a la interfaz del cliente deben agregarse desde la *cuenta del propietario de la VPC*.

Requisitos previos

- Asegúrese de que la función de IAM asociada a la instancia de ADC VPX en la cuenta de participante de AWS tenga los siguientes permisos de IAM:

```
”Version”: ”2012-10-17”,
    ”Statement”: [
        {

            ”Sid”: ”VisualEditor0”,
            ”Effect”: ”Allow”,
            ”Action”: [
                ”ec2:DisassociateAddress”,
                ”iam:GetRole”,
                ”iam:SimulatePrincipalPolicy”,
                ”ec2:DescribeInstances”,
                ”ec2:DescribeAddresses”,
                ”ec2:ModifyNetworkInterfaceAttribute”,
                 “ec2:AssociateAddress” ,
                ”sts:AssumeRole”
        ],
            ”Resource”: ”*”
```



```
18            }
19
20        ]
21     }
22
23  <!--NeedCopy-->
```

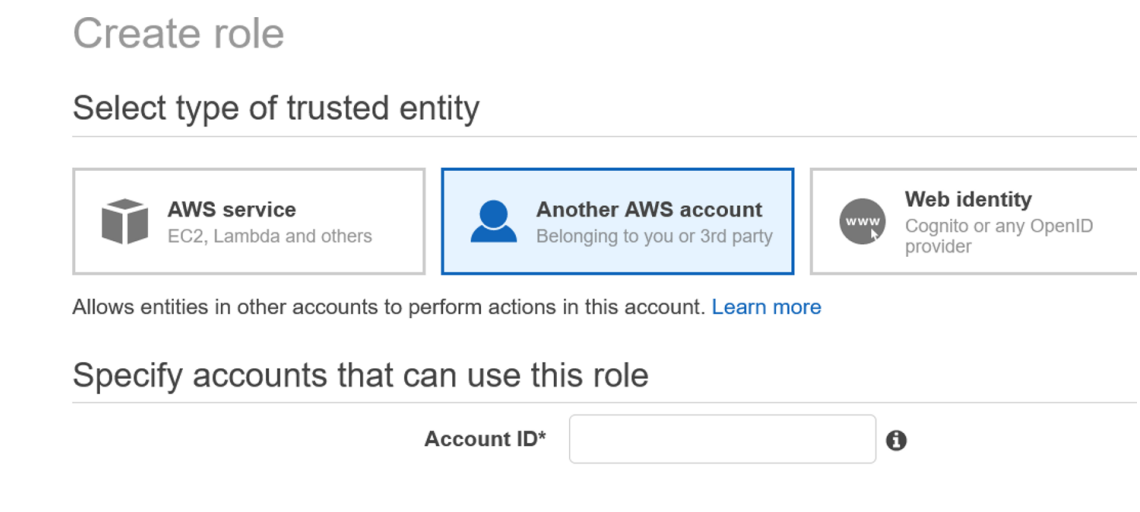
> Nota:
>
> **AssumeRole** permite a la instancia de Citrix ADC VPX asumir la función de IAM multicuenta, que crea la cuenta del propietario de la VPC.

- Asegúrese de que la cuenta del propietario de la VPC proporcione los siguientes permisos de IAM a la cuenta del participante mediante la función de IAM multicuenta:

```
1  {
2
3      ”Version”: ”2012-10-17”,
4      ”Statement”: [
5          {
6
7              ”Sid”: ”VisualEditor0”,
8              ”Effect”: ”Allow”,
9              ”Action”: [
10                 ”ec2:CreateRoute”,
11                 ”ec2:DeleteRoute”,
12                 ”ec2:DescribeRouteTables”
13             ],
14             ”Resource”: ”*”
15         }
16
17     ]
18  }
19
20 <!--NeedCopy-->
```

Crear función de IAM multicuenta

1. Inicie sesión en la consola web de AWS.
2. En la ficha **IAM**, vaya a **Roles** y, a continuación, elija **Create Role**.
3. Elija **otra cuenta de AWS**.



4. Introduzca el número de identificación de cuenta de 12 dígitos de la cuenta de participante a la que quiere conceder acceso de administrador.

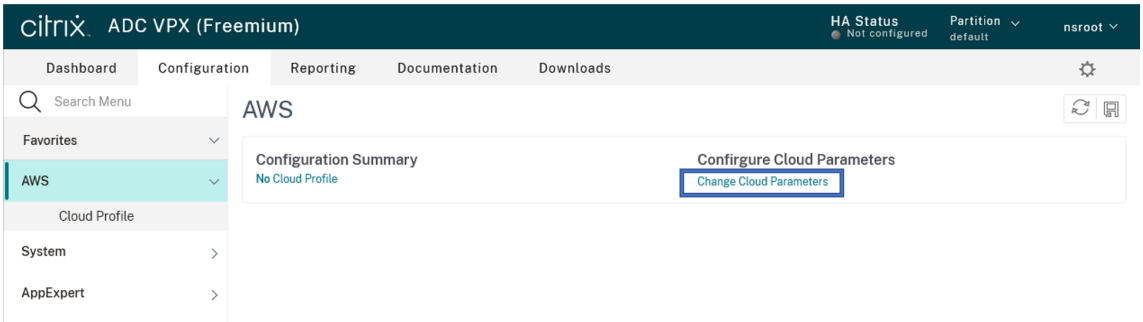
Establecer la función de IAM multicuenta mediante la CLI de Citrix ADC

El siguiente comando permite que la instancia de ADC VPX asuma la función de IAM multicuenta que existe en la cuenta del propietario de la VPC.

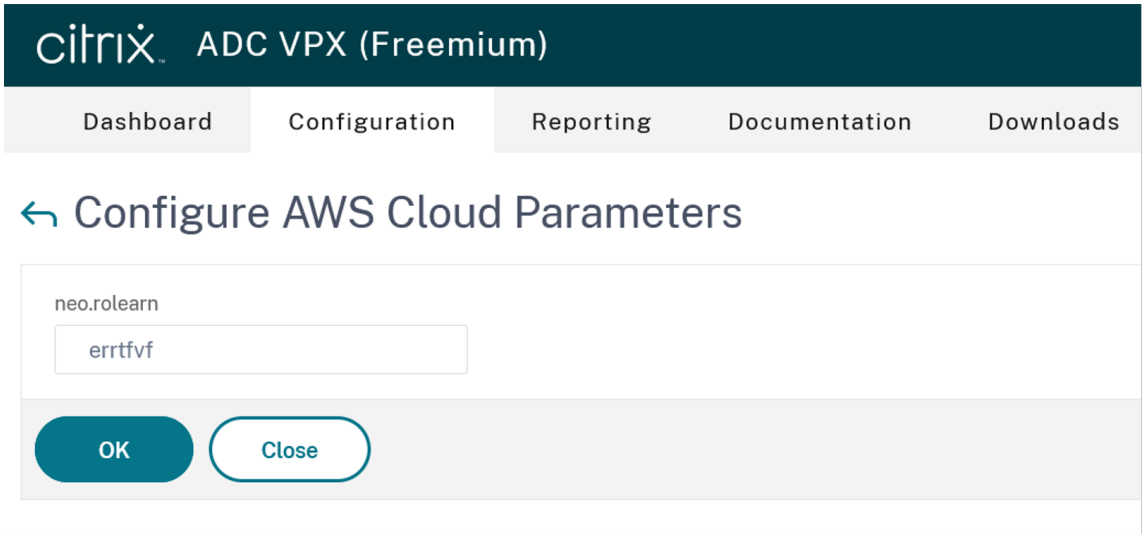
```
set cloud awsParam -roleARN <string>
<!--NeedCopy-->
```

Establecer la función de IAM multicuenta mediante la GUI de Citrix ADC

1. Inicie sesión en el dispositivo Citrix ADC y vaya a **Configuración > AWS > Cambiar parámetros de la nube**.



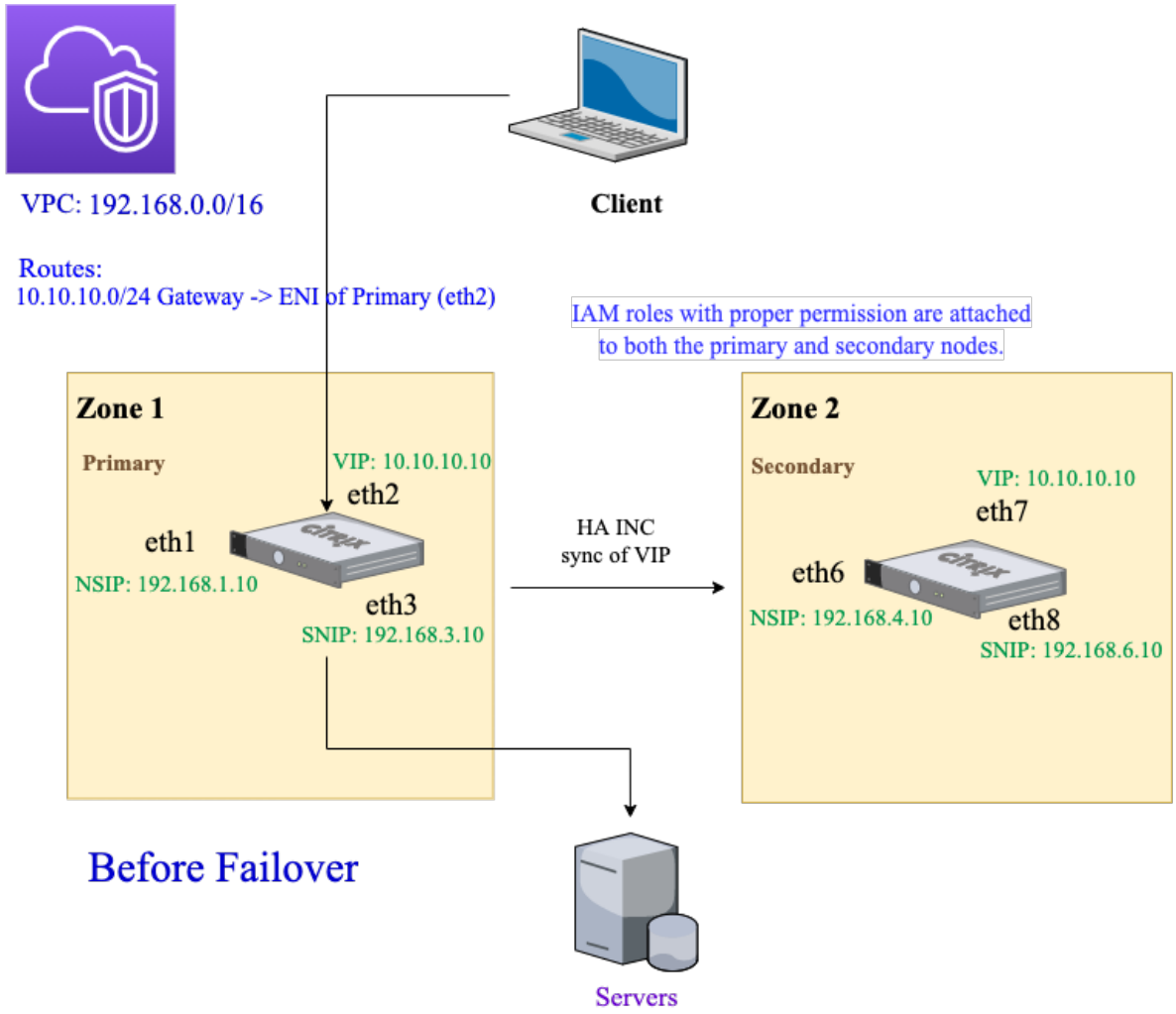
2. En la página **Configure AWS Cloud Parameters**, introduzca un valor para el campo **RoleARN** .

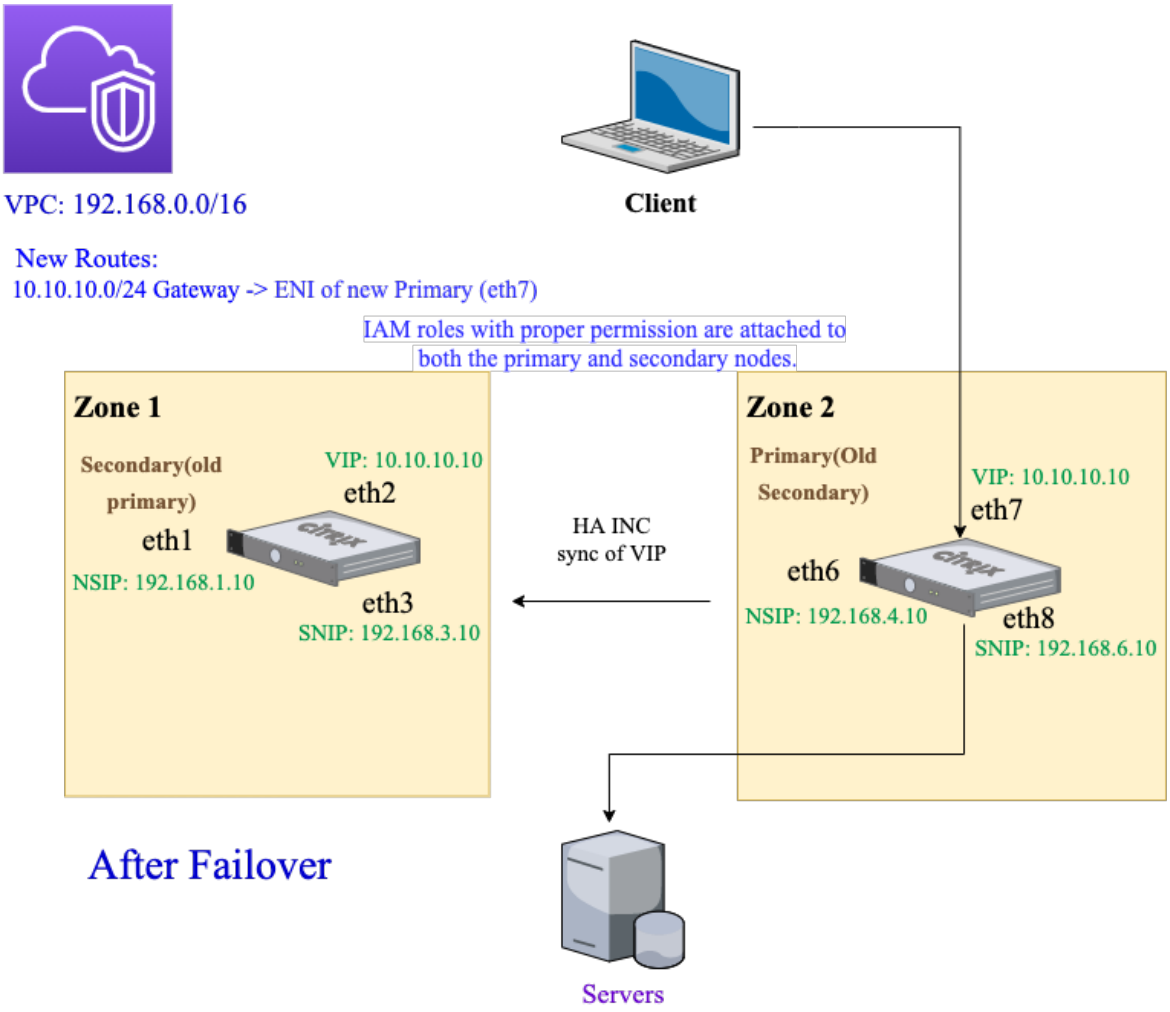


Caso

En este caso, se crea una única VPC. En esa VPC, se crean dos instancias VPX en dos zonas de disponibilidad. Cada instancia tiene tres subredes: una para administración, otra para el cliente y otra para el servidor back-end.

Los diagramas siguientes ilustran la configuración de alta disponibilidad de Citrix ADC VPX en modo INC, en AWS. La subred personalizada 10.10.10.10, que no forma parte de la VPC, se utiliza como VIP. Por lo tanto, la subred 10.10.10.10 se puede utilizar en todas las zonas de disponibilidad.





En este caso, utilice la CLI para configurar la alta disponibilidad.

1. Configure la alta disponibilidad en modo INC en ambas instancias.

   Escriba los siguientes comandos en los nodos primario y secundario.

   En el nodo principal:

```
1 add ha node 1 192.168.4.10 -inc enabled
2 <!--NeedCopy-->
```

   En este caso, 192.168.4.10 se refiere a la dirección IP privada de la NIC de administración del nodo secundario.

   En el nodo secundario:

```
1 add ha node 1 192.168.1.10 -inc enabled
```



```
<!--NeedCopy-->
```

En este caso, 192.168.1.10 se refiere a la dirección IP privada de la NIC de administración del nodo principal.

2. Agregue un servidor virtual en la instancia principal.

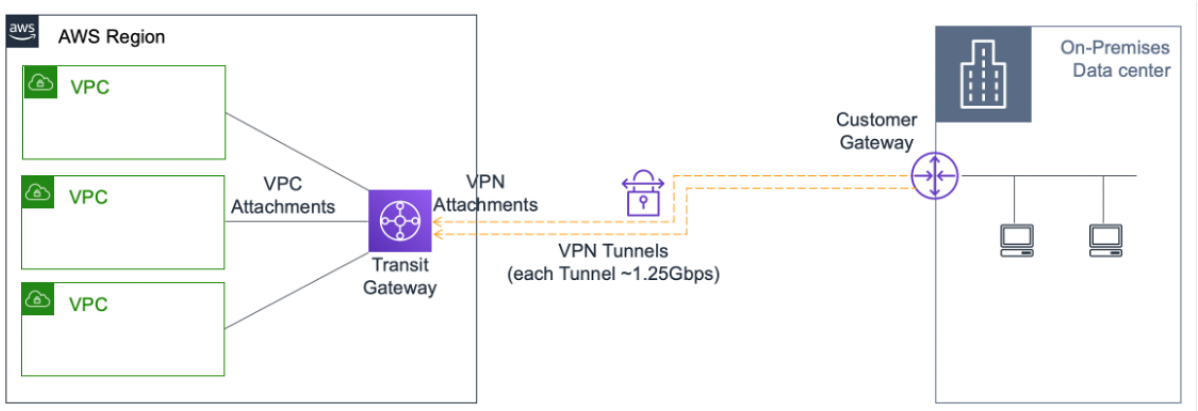
   Escriba el siguiente comando:

```
add lbvserver vserver1 http 10.10.10.10 80
<!--NeedCopy-->
```

3. Guarde la configuración.
4. Tras una conmutación por error forzada:
   - La instancia secundaria se convierte en la nueva instancia principal.
   - La ruta de la VPC que apunta al ENI principal migra al ENI del cliente secundario.
   - El tráfico del cliente se reanuda en la nueva instancia principal.

Configuración de AWS Transit Gateway para solución IP privada de alta disponibilidad

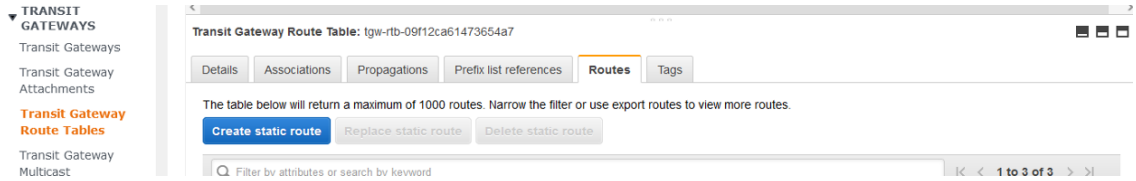
Necesita AWS Transit Gateway para que la subred VIP privada se pueda redirigir dentro de la red interna, en las VPC de AWS, regiones y redes locales. La VPC debe conectarse a AWS Transit Gateway. Se crea una ruta estática para la subred VIP o el grupo de IP dentro de la tabla de rutas de AWS Transit Gateway y se dirige hacia la VPC.



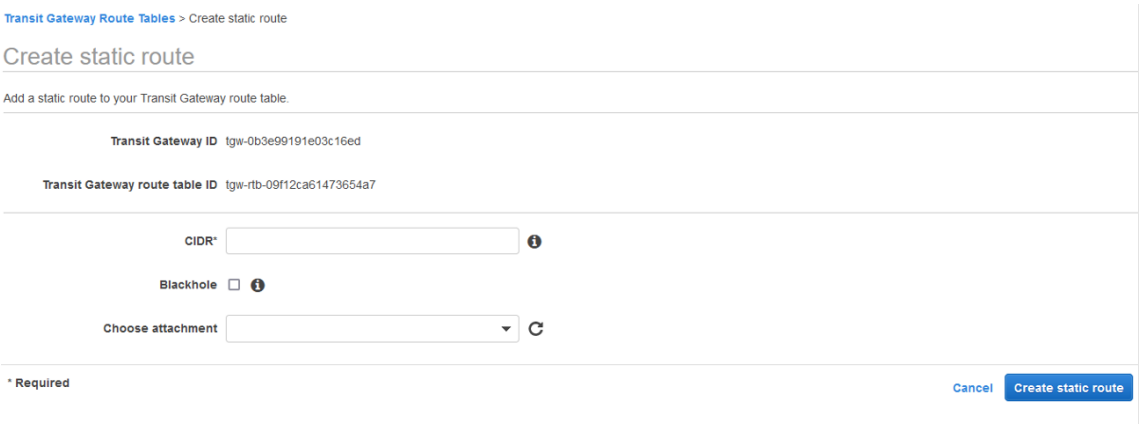
Para configurar AWS Transit Gateway, siga estos pasos:

1. Abra la consola de Amazon VPC.
2. En el panel de navegación, elija **Tablas de rutas de Transit Gateway**.

3. Seleccione la ficha **Rutas** y haga clic en **Crear ruta estática**.



4. Cree una ruta estática en la que CIDR apunte a su subred VIPS privada y puntos de adjunto a la VPC que tenga ADC VPX.



5. Haga clic en **Crear ruta estática**y selecciona **Cerrar**.

Implementar una instancia de Citrix ADC VPX en AWS Outposts

August 20, 2021

AWS Outposts es un grupo de capacidad informática y almacenamiento de AWS implementado en su sitio. Outposts proporciona infraestructura y servicios de AWS en su ubicación local. AWS opera, supervisa y administra esta capacidad como parte de una región de AWS. Puede utilizar las mismas instancias de Citrix ADC VPX, API de AWS, herramientas e infraestructura en las instalaciones locales y en la nube de AWS para una experiencia híbrida coherente.

Puede crear subredes en sus puestos avanzados y especificarlas al crear recursos de AWS, como instancias de EC2, volúmenes de EBS, clústeres de ECS e instancias de RDS. Las instancias de las subredes Outposts se comunican con otras instancias de la región de AWS mediante direcciones IP privadas, todas dentro de la misma Amazon Virtual Private Cloud (VPC).

Para obtener más información, consulte la guía del usuario de AWS Outposts.

Cómo funciona AWS Outposts

AWS Outposts está diseñado para funcionar con una conexión constante y coherente entre sus puestos avanzados y una región de AWS. Para lograr esta conexión con la región y con las cargas de trabajo locales en el entorno local, debe conectar la avanzada a la red local. La red local debe proporcionar acceso WAN a la región y a Internet. Internet también debe proporcionar acceso LAN o WAN a la red local donde residen las aplicaciones o cargas de trabajo locales.

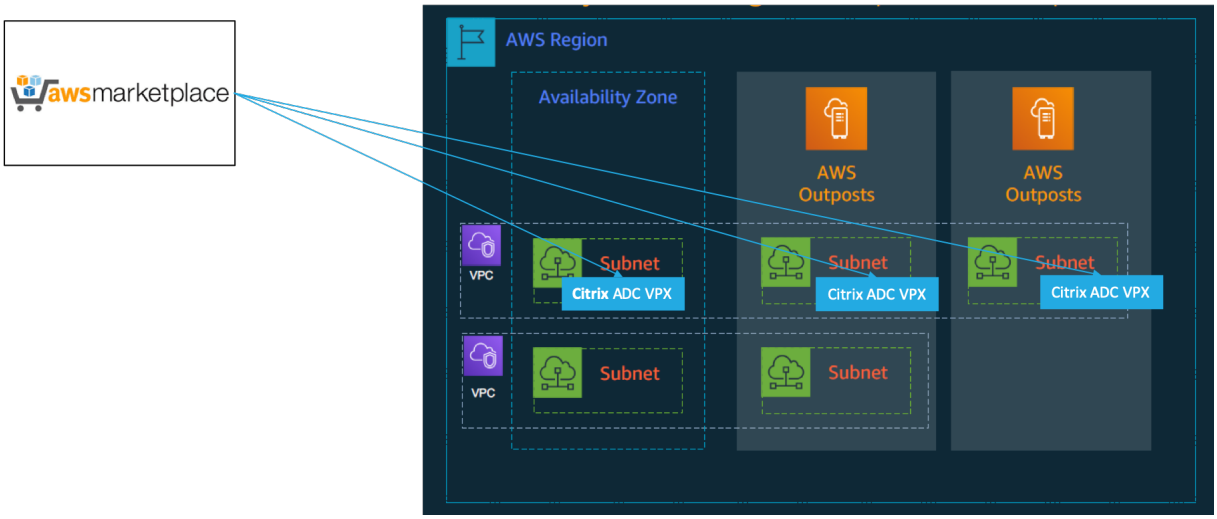
Requisito previo

- Debe instalar AWS Outposts en su sitio.
- La capacidad de procesamiento y almacenamiento de AWS Outpost debe estar disponible para su uso.

Para obtener más información sobre cómo realizar un pedido de AWS Outposts, consulte la siguiente documentación de AWS:
https://aws.amazon.com/blogs/aws/aws-outposts-now-available-order-your-racks-today/

Implementar una instancia de Citrix ADC VPX en AWS Outposts mediante la consola web de AWS

En la siguiente ilustración se muestra una implementación sencilla de instancias de Citrix ADC VPX en Outposts. La AMI de Citrix ADC presente en AWS Marketplace también se implementa en Outposts.



Inicie sesión en la consola web de AWS y complete los siguientes pasos para implementar instancias de ADC VPX EC2 en sus AWS Outposts.

1. Cree un par de claves.
2. Cree una nube privada virtual (VPC).
3. Agregue más subredes.

4. Crear grupos de seguridad y reglas de seguridad.
5. Agregar tablas de redirecciones.
6. Cree una Gateway a Internet.
7. Cree una instancia de ADC VPX mediante el servicio AWS EC2.
   En el panel de AWS, vaya a **Compute > EC2 > Launch Instance > AWS Marketplace**.
8. Cree y conecte más interfaces de red.
9. Conecte IP elásticas a la NIC de administración.
10. Conéctese a la instancia de VPX.

Para obtener instrucciones detalladas sobre cada uno de los pasos, consulte Implementación de una instancia Citrix ADC VPX en AWS mediante la consola web de AWS.

Para obtener una alta disponibilidad dentro de la misma implementación de zona de disponibilidad, consulte Implementación de un par de alta disponibilidad en AWS.

Proteja AWS API Gateway mediante el firewall de aplicaciones web de Citrix

April 21, 2022

Puede implementar un dispositivo Citrix ADC en frente de su AWS API Gateway y proteger la puerta de enlace de API de amenazas externas. Citrix Web Application Firewall (WAF) puede defender su API contra las 10 amenazas principales y los ataques zero-day de OWASP. Citrix WAF utiliza una base de código única en todos los factores de forma de ADC. Por lo tanto, puede aplicar y aplicar directivas de seguridad de manera consistente en cualquier entorno. Citrix WAF es fácil de implementar y está disponible como una licencia única. Citrix WAF le proporciona las siguientes funciones:

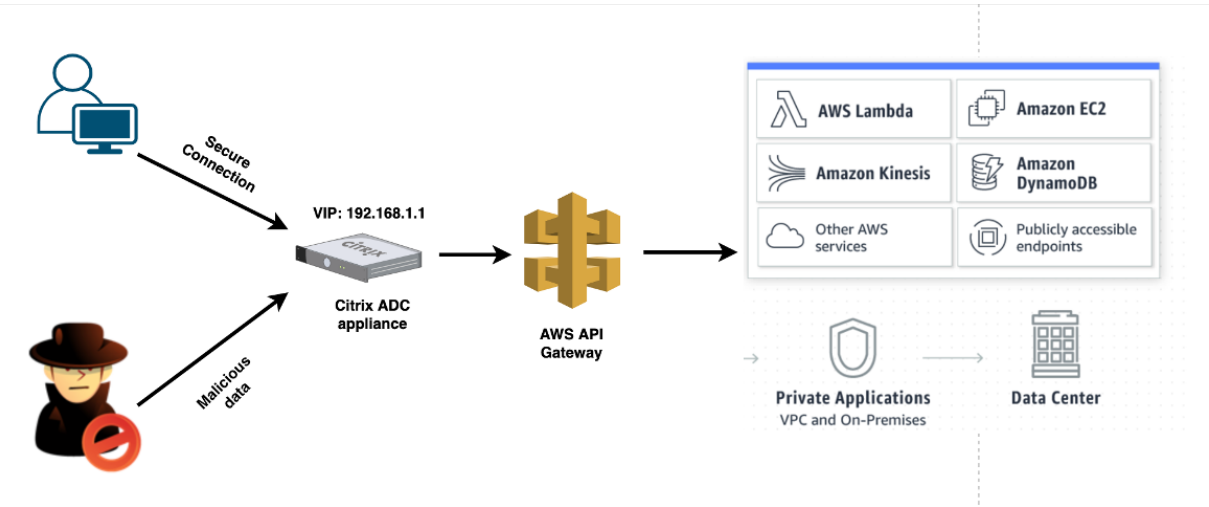
- Configuración simplificada
- Gestión de bots
- Visibilidad integral
- Recopilar datos de varias fuentes y mostrar los datos en una pantalla unificada

Además de la protección de puerta de enlace de API, también puede usar las demás funciones de Citrix ADC. Para obtener más información, consulte la documentación de Citrix ADC. Además de evitar las conmutaciones por error del centro de datos y minimizar el tiempo de apagado, puede colocar ADC en alta disponibilidad dentro o entre las zonas de disponibilidad. También puede usar o configurar la agrupación en clústeres con la función Autoscale.

Anteriormente, AWS API Gateway no admitía las protecciones necesarias para proteger las aplicaciones detrás de él. Sin las protecciones de firewall de aplicaciones web (WAF), las API eran propensas a las amenazas de seguridad.

Implementar el dispositivo Citrix ADC frente a la puerta de enlace de API de AWS

En el siguiente ejemplo, se implementa un dispositivo Citrix ADC frente a la puerta de enlace de la API de AWS.



Supongamos que hay una solicitud de API genuina para el servicio de AWS Lambda. Esta solicitud puede ser para cualquiera de los servicios de API, como se menciona en la documentación de Amazon API Gateway. Como se muestra en el diagrama anterior, el flujo de tráfico es el siguiente:

1. El cliente envía una solicitud a la función AWS Lambda (XYZ). Esta solicitud de cliente se envía al servidor virtual Citrix ADC (192.168.1.1).
2. El servidor virtual inspecciona el paquete y comprueba si hay contenido malicioso.
3. El dispositivo Citrix ADC desencadena una directiva de reescritura para cambiar el nombre de host y la URL en una solicitud de cliente. Por ejemplo, quiere cambiar `https://restapi.citrix.com/default/LamdaFunctionXYZ` a `https://citrix.execute-api.<region>.amazonaws.com/default/LambdaFunctionXYZ`.
4. El dispositivo Citrix ADC reenvía esta solicitud a la puerta de enlace de la API de AWS.
5. AWS API Gateway envía la solicitud al servicio de Lambda y llama a la función de Lambda “XYZ”.
6. Al mismo tiempo, si un atacante envía una solicitud de API con contenido malicioso, la solicitud maliciosa llega al dispositivo Citrix ADC.
7. El dispositivo Citrix ADC inspecciona los paquetes y los descarta en función de la acción configurada.

Configurar el dispositivo Citrix ADC con WAF habilitado

Para habilitar WAF en un dispositivo Citrix ADC, lleve a cabo los siguientes pasos:

1. Agregue un servidor virtual de conmutación de contenido o equilibrio de carga. Supongamos que la dirección IP del servidor virtual es 192.168.1.1, que se resuelve en un nombre de dominio (restapi.citrix.com).

2. Habilite la directiva WAF en el servidor virtual Citrix ADC. Para obtener más información, consulte Configuración de Web App Firewall.
3. Habilite la directiva de reescritura para cambiar el nombre de dominio. Supongamos que quiere cambiar la solicitud entrante a un equilibrador de carga en el nombre de dominio "restapi.citrix.com" para que se vuelva a escribir en la puerta de enlace de la API de AWS de back-end en "citrix.execute-api".<region>.amazonaws".
4. Habilite el modo L3 en el dispositivo Citrix ADC para que actúe como proxy. Utilice el siguiente comando:

```
1 enable ns mode L3
2 <!--NeedCopy-->
```

En el paso 3 del ejemplo anterior, supongamos que el administrador del sitio web quiere que el dispositivo Citrix ADC reemplace el nombre de dominio "restapi.citrix.com" por "citrix.execute-api.<region>.amazonaws.com" y la URL con "Default/Lambda/xyz".

El siguiente procedimiento describe cómo cambiar el nombre de host y la URL en una solicitud de cliente mediante la función de reescritura:

1. Inicie sesión en el dispositivo Citrix ADC mediante SSH.
2. Agregue acciones de reescritura.

```
1 add rewrite action rewrite_host_hdr_act replace "HTTP.REQ.HEADER("
     Host")" ""citrix.execute-api.<region>.amazonaws.com""
2
3 add rewrite action rewrite_url_act replace HTTP.REQ.URL.
     PATH_AND_QUERY ""/default/lambda/XYZ""
4 <!--NeedCopy-->
```

3. Agregue directivas de reescritura para las acciones de reescritura.

```
1 add rewrite policy rewrite_host_hdr_pol "HTTP.REQ.HEADER("Host").
     CONTAINS("restapi.citrix.com") "rewrite_host_hdr_act
2
3 add rewrite policy rewrite_url_pol "HTTP.REQ.HEADER("Host").
     CONTAINS("restapi.citrix.com") "rewrite_url_act
4 <!--NeedCopy-->
```


4. Enlazar las directivas de reescritura a un servidor virtual.

```
bind lb vserver LB_API_Gateway -policyName rewrite_host_hdr_pol -
    priority 10 -gotoPriorityExpression 20 -type REQUEST

bind lb vserver LB_API_Gateway -policyName rewrite_url_pol -
    priority 20 -gotoPriorityExpression END -type REQUEST
<!--NeedCopy-->
```

Para obtener más información, consulte Configurar la reescritura para cambiar el nombre de host y la URL en la solicitud del cliente en el dispositivo Citrix ADC.

Características y capacidades de Citrix ADC

El dispositivo Citrix ADC, además de proteger la implementación, también puede mejorar la solicitud en función de los requisitos del usuario. El dispositivo Citrix ADC proporciona las siguientes funciones clave.

- **Equilibrar la puerta de enlace de API:** Si tiene más de una puerta de enlace de API, puede equilibrar la carga de varias puertas de enlace de API mediante el dispositivo Citrix ADC y definir el comportamiento de la solicitud de API.
  - Hay diferentes métodos de equilibrio de carga disponibles. Por ejemplo, el método de conexión mínima evita la sobrecarga del límite de API Gateway, el método de carga personalizada mantiene una carga específica en una puerta de enlace de API en particular, etc. Para obtener más información, consulte Algoritmos de equilibrio de carga
  - La descarga SSL se configura sin interrumpir el tráfico.
  - El modo Usar IP de origen (USIP) está habilitado para conservar la dirección IP del cliente.
  - Configuración SSL definida por el usuario: puede tener su propio servidor virtual SSL con sus propios certificados y algoritmos firmados.
  - Servidor virtual de respaldo: si no se puede acceder a la puerta de enlace de la API, puede enviar la solicitud a un servidor virtual de respaldo para realizar acciones adicionales.
  - Hay disponibles muchas otras funciones de equilibrio de carga. Para obtener más información, consulte Equilibrio de carga del tráfico en un dispositivo Citrix ADC.
- **Autenticación, autorización y auditoría:** puede definir sus propios métodos de autenticación, como LDAP, SAML, RADIUS, y autorizar y auditar las solicitudes de API.
- **Respondedor:** puede redirigir las solicitudes de API a otra puerta de enlace de API durante el tiempo de cierre.

- **Limitación de velocidad:** puede configurar la función de limitación de velocidad para evitar la sobrecarga de una puerta de enlace de API.
- **Mejor disponibilidad:** puede configurar un dispositivo Citrix ADC en una configuración de alta disponibilidad o en una configuración de clúster para brindar una mejor disponibilidad a sus tráficos de API de AWS.
- **API REST:** admite la API REST, que se puede utilizar para automatizar el trabajo en entornos de producción en la nube.
- **Supervisar datos:** supervisa y registra los datos como referencia.

El dispositivo Citrix ADC proporciona muchas más funciones, que se pueden integrar con la puerta de enlace de la API de AWS. Para obtener más información, consulte la documentación de Citrix ADC.

Agregar el servicio de autoescalado de AWS de back-end

August 20, 2021

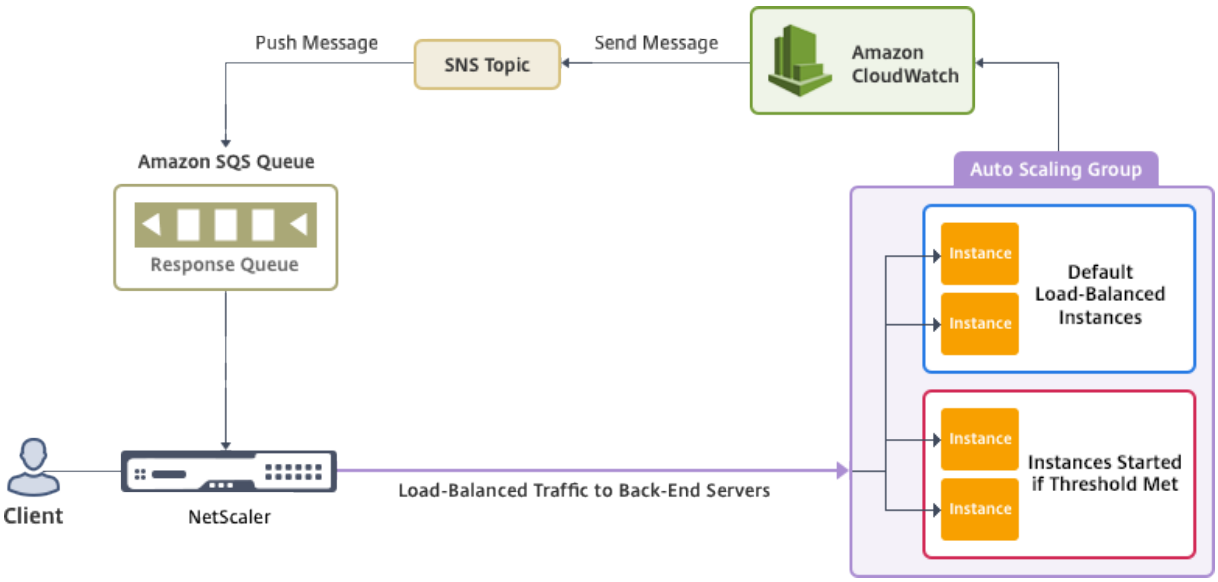
El alojamiento eficiente de aplicaciones en una nube implica una gestión fácil y rentable de los recursos en función de la demanda de la aplicación. Para satisfacer la creciente demanda, debe escalar los recursos de red hacia arriba. Independientemente de que la demanda disminuya, debe reducir la escala para evitar el coste innecesario de los recursos inactivos. Para minimizar el coste de ejecutar la aplicación implementando solo tantas instancias como sean necesarias durante un tiempo dado, debe supervisar constantemente el tráfico, la memoria y el uso de la CPU, etc. Sin embargo, supervisar el tráfico manualmente es engorroso. Para que el entorno de aplicaciones se amplíe o disminuya dinámicamente, debe automatizar los procesos de supervisión del tráfico y de ampliación de los recursos siempre que sea necesario.

Integrada con el servicio AWS Auto Scaling, la instancia Citrix ADC VPX ofrece las siguientes ventajas:

- **Equilibrio de carga y administración**: Configura automáticamente los servidores para escalarlos y reducirlos, en función de la demanda. La instancia VPX automática detecta grupos de Autoscale en la subred back-end y permite al usuario seleccionar los grupos Autoscale para equilibrar la carga. Todo esto se hace configurando automáticamente las direcciones IP virtuales y de subred en la instancia VPX.
- **Alta disponibilidad**: Detecta grupos de escala automática que abarcan varias zonas de disponibilidad y servidores de equilibrio de carga.
- **Mejor disponibilidad de red**: La instancia VPX admite:
  - Servidores back-end en diferentes VPC, mediante el uso de pares de VPC
  - Servidores back-end en los mismos grupos de ubicación
  - Servidores back-end en diferentes zonas de disponibilidad

- **Terminación de conexión graciosa**: Elimina los servidores de escala automática correctamente, lo que evita la pérdida de conexiones de cliente cuando se produce una actividad de escala reducida, mediante la función Graceful Timeout.

Diagrama: Servicio de autoescalado de AWS con una instancia de Citrix ADC VPX



Este diagrama muestra cómo el servicio AWS Autoscaling es compatible con una instancia de Citrix ADC VPX (servidor virtual de equilibrio de carga). Para obtener más información, consulte los siguientes temas de AWS.

- Grupos de escalado automático
- CloudWatch
- Servicio de notificación simple (SNS)
- Servicio de cola simple (Amazon SQS)

Antes de comenzar

Antes de empezar a utilizar el escalado automático con su instancia de Citrix ADC VPX, debe realizar las siguientes tareas.

1. Lea los siguientes temas:
   - Requisitos previos
   - Directrices de limitación y uso
2. Cree una instancia de Citrix ADC VPX en AWS según sus requisitos.
   - Para obtener más información sobre cómo crear una instancia independiente Citrix ADC VPX, consulte Implementación de una instancia independiente Citrix ADC VPX en AWS and Scenario: instancia independiente

- Para obtener más información sobre cómo implementar instancias VPX en modo HA, consulte Implementación de un par de alta disponibilidad en AWS.

> **Nota**
>
> Citrix recomienda la plantilla CloudFormation para crear instancias de Citrix ADC VPX en AWS.
>
> Citrix recomienda crear tres interfaces: Una para administración (NSIP), otra para servidor virtual LB (VIP) orientado al cliente y otra para IP de subred (NSIP).

3. Cree un grupo de autoescala de AWS. Si no tiene una configuración de Autoscaling existente, debe:

   a) Crear una configuración de inicio

   b) Crear un grupo de autoescala

   c) Verificar el grupo de autoescalado

   Para obtener más información, consulte http://docs.aws.amazon.com/autoscaling/latest/userguide/GettingStartedTutorial.html.

4. En el grupo Autoscale de AWS, debe especificar al menos una directiva de reducción de escala. La instancia de Citrix ADC VPX solo admite la directiva de escalado Step. La directiva de escala simple y la directiva de escala de seguimiento de destino no son compatibles con el grupo de escala automática.

Agregar el servicio AWS Autoscaling a una instancia de Citrix ADC VPX

Puede agregar el servicio Autoscaling a una instancia VPX con un solo clic mediante la GUI. Complete estos pasos para agregar el servicio Autoscaling a la instancia de VPX:

1. Inicie sesión en la instancia de VPX mediante sus credenciales para `nsroot`.
2. Cuando inicia sesión en la instancia de Citrix ADC VPX por primera vez, verá la página de perfil de nube predeterminada. Seleccione el grupo AWS Autoscaling en el menú desplegable y haga clic en **Crear** para crear un perfil de nube. Haga clic en **Omitir** si quiere crear el perfil de nube más adelante.

   Puntos a tener en cuenta al crear un perfil de nube: De forma predeterminada, la plantilla de CloudFormation crea y adjunta el siguiente rol de IAM.

```
1 {
2
3
4     "Version": "2012-10-17",
```



```
5
6     "Statement": [
7
8      {
9
10
11            "Action": [
12
13                "ec2:DescribeInstances",
14
15                "ec2:DescribeNetworkInterfaces",
16
17                "ec2:DetachNetworkInterface",
18
19                "ec2:AttachNetworkInterface",
20
21                "ec2:StartInstances",
22
23                "ec2:StopInstances",
24
25                "ec2:RebootInstances",
26
27                "autoscaling:*",
28
29                "sns:*",
30
31                "sqs:*"
32
33                "iam: SimulatePrincipalPolicy"
34
35                "iam: GetRole"
36
37            ],
38
39            "Resource": "*",
40
41            "Effect": "Allow"
42
43          }
44
45
46     ]
47
48  }
49
```

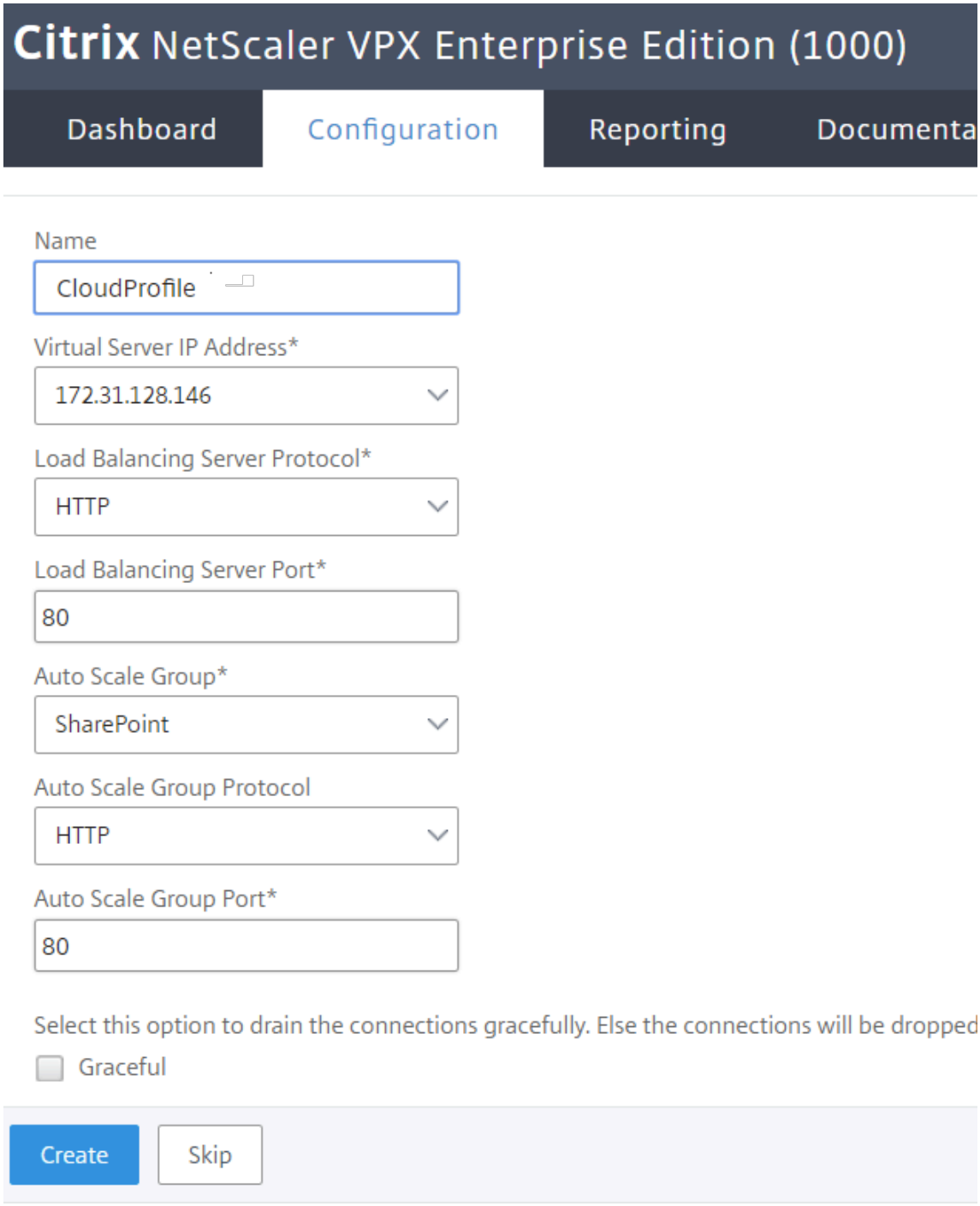


```
<!--NeedCopy-->
```

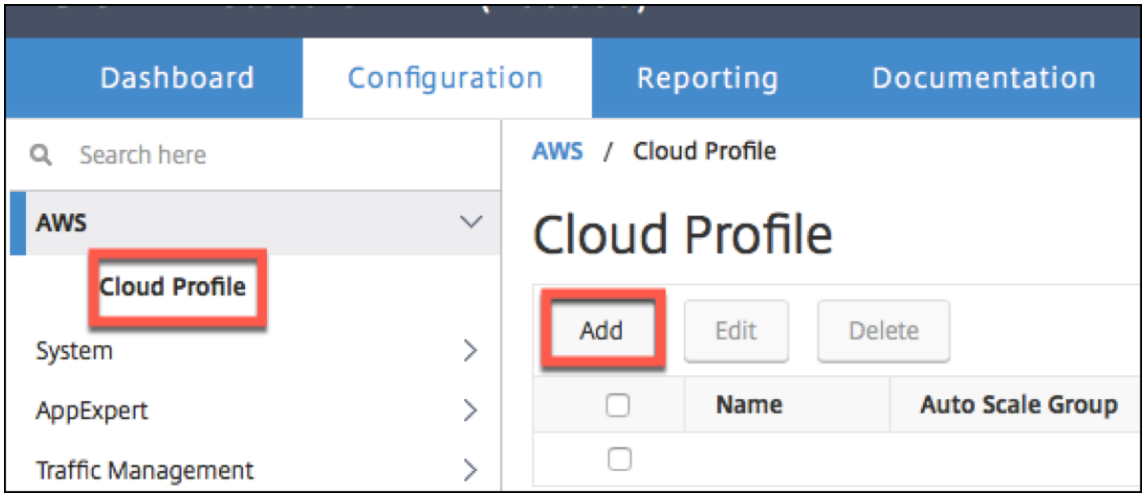
Asegúrese de que el rol de IAM de una instancia tenga los permisos adecuados.

- La dirección IP del servidor virtual se rellena automáticamente desde la dirección IP libre disponible para la instancia VPX. https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/MultipleIP.html#ManageMultipleIP
- El grupo Autoscale se rellena previamente desde el grupo Autoscale configurado en su cuenta de AWS. http://docs.aws.amazon.com/autoscaling/latest/userguide/AutoScalingGroup.html.
- Al seleccionar el protocolo y el puerto del grupo de escalado automático, asegúrese de que los servidores escuchen esos protocolos y puertos y vincule el monitor correcto en el grupo de servicios. De forma predeterminada, se utiliza el monitor TCP.
- Para el tipo de protocolo SSL Autoscaling, después de crear el perfil de nube, el servidor virtual de equilibrio de carga o el grupo de servicios está inactivo debido a que falta un certificado. Puede enlazar el certificado al servidor virtual o grupo de servicios manualmente.
- Seleccione la opción Tiempo de espera de gracia para quitar los servidores de escala automática correctamente. Si esta opción no está seleccionada, el servidor es el grupo Autoscale se quita inmediatamente después de que la carga baja, lo que podría causar una interrupción del servicio para los clientes conectados existentes. Seleccionar Graceful y dar un tiempo de espera significa en caso de reducción de escala. La instancia VPX no quita el servidor inmediatamente, pero marca uno de los servidores para su eliminación correcta. Durante este período, la instancia no permite nuevas conexiones a este servidor. La conexión existente se sirve hasta que se produce el tiempo de espera y, tras un tiempo de espera, la instancia VPX elimina el servidor.

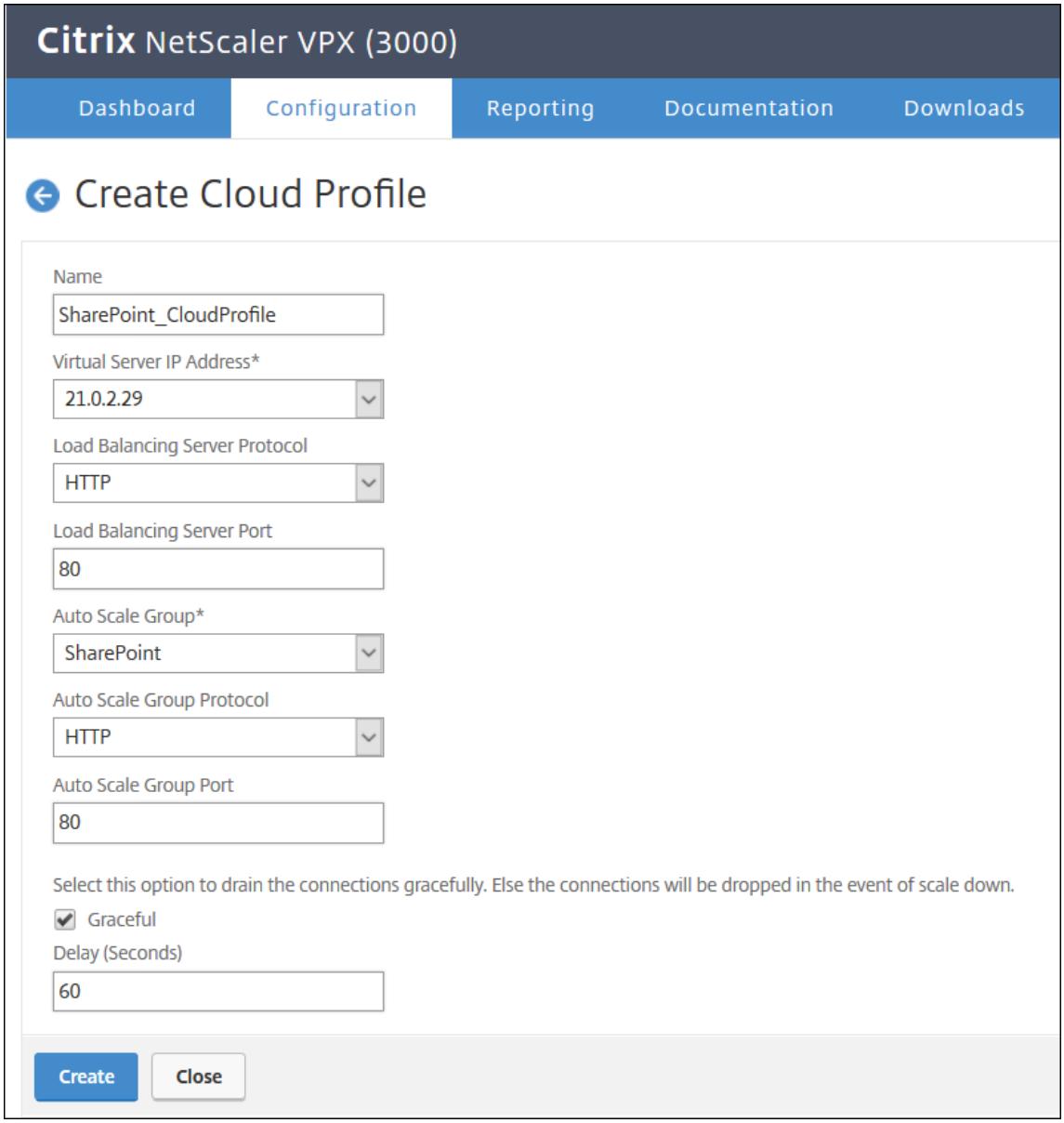
Ilustración: página Perfil de nube predeterminado



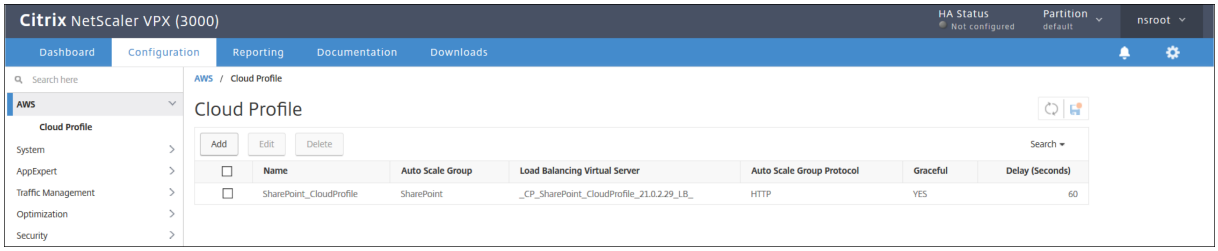
3. Después del primer inicio de sesión si quiere crear un perfil de nube, en la GUI vaya a **Sistema > AWS > Perfil de nube** y haga clic en **Agregar**.



Aparecerá la página **de configuración Crear perfil de nube**.



Cloud Profile crea un servidor virtual de equilibrio de carga de Citrix ADC y un grupo de servicios con miembros como servidores del grupo Autoscaling. Los servidores back-end deben ser accesibles a través del SNIP configurado en la instancia VPX.



> **Nota**
>
> Para ver información relacionada con AutoScale en la consola de AWS, vaya a **EC2** > **Panel de control** > **Auto Scaling** > **Auto Scaling Group**.

Configurar una instancia de Citrix ADC VPX para utilizar la interfaz de red SR-IOV

August 20, 2021

> **Nota**
>
> La compatibilidad con interfaces SR-IOV en una configuración de alta disponibilidad está disponible desde Citrix ADC versión 12.0 57.19 en adelante.

Después de crear una instancia Citrix ADC VPX en AWS, puede configurar el dispositivo virtual para que use interfaces de red SR-IOV mediante la CLI de AWS.

En todos los modelos de Citrix ADC VPX, excepto Citrix ADC VPX AWS Marketplace Editions de 3G y 5G, SR-IOV no está habilitado en la configuración predeterminada de una interfaz de red.

Antes de iniciar la configuración, lea los siguientes temas:

- Requisitos previos
- Instrucciones de uso y limitaciones

Esta sección incluye los siguientes temas:

- Cambiar el tipo de interfaz a SR-IOV
- Configurar SR-IOV en una configuración de alta disponibilidad

Cambiar el tipo de interfaz a SR-IOV

Puede ejecutar el comando show interface summary para comprobar la configuración predeterminada de una interfaz de red.

Ejemplo 1: La siguiente captura de pantalla de CLI muestra la configuración de una interfaz de red en la que SR-IOV está habilitado de forma predeterminada en Citrix ADC VPX AWS Marketplace Editions of 3G y 5G.

```
> show interface summary
-------------------------------------------------------------------------------
     Interface  MTU       MAC                Suffix
-------------------------------------------------------------------------------
1      1/1      1500      0a:1e:2e:17:a2:37  Intel 82599 10G VF Interface
2      LO/1     1500      0a:1e:2e:17:a2:37  Netscaler Loopback interface
 Done
```


Ejemplo 2: La siguiente captura de pantalla CLI muestra la configuración predeterminada de una interfaz de red donde SR-IOV no está habilitado.

```
 Done
> sh int s
-------------------------------------------------------------------------------
      Interface  MTU        MAC                Suffix
-------------------------------------------------------------------------------
1     1/1        1500       12:fc:04:c5:d0:12  NetScaler Virtual Interface
2     LO/1       1500       12:fc:04:c5:d0:12  Netscaler Loopback interface
 Done
>
```

Para obtener más información sobre cómo cambiar el tipo de interfaz a SR-IOV, consulte http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/sriov-networking.html

Para cambiar el tipo de interfaz a SR-IOV

1. Apague la instancia de Citrix ADC VPX que se ejecuta en AWS.
2. Para habilitar SR-IOV en la interfaz de red, escriba el siguiente comando en la CLI de AWS.

   ```
   $ aws ec2 modify-instance-attribute --instance-id \<instance\\_id\> --sriov-net-support simple
   ```

3. Para comprobar si SR-IOV se ha habilitado, escriba el siguiente comando en la CLI de AWS.

   ```
   $ aws ec2 describe-instance-attribute --instance-id \<instance\\_id\> --attribute sriovNetSupport
   ```

   Ejemplo 3: El tipo de interfaz de red cambió a SR-IOV mediante la CLI de AWS.

   ```
   aws ec2 modify-instance-attribute --instance-id i-008c1230aaf303bee --sriov-net-support simple
   aws ec2 describe-instance-attribute --instance-id   i-008c1230aaf303bee  --attribute sriovNetSupport
   {
       "InstanceId": "i-008c1230aaf303bee",
       "SriovNetSupport": {
           "Value": "simple"
       }
   }
   ```

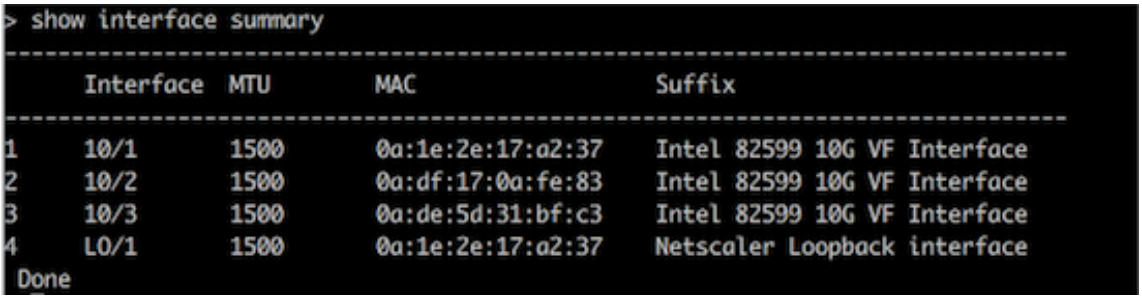
   Si SR-IOV no está habilitado, el valor para SriovnetSupport está ausente.

   Ejemplo 4: En el ejemplo siguiente, el soporte para SR-IOV no está habilitado.

   ```
   {
       "InstanceId": "i-0c3e84cfa65b04cc8",
       "SriovNetSupport": {}
   }
   ```


4. Encienda la instancia VPX. Para ver el estado modificado de la interfaz de red, escriba “show interface summary” en la CLI.

   Ejemplo 5: La siguiente captura de pantalla muestra las interfaces de red con SR-IOV habilitado. Las interfaces 10/1, 10/2, 10/3 están habilitadas para SR-IOV.



Estos pasos completan el procedimiento para configurar las instancias VPX para utilizar interfaces de red SR-IOV.

Configurar SR-IOV en una configuración de alta disponibilidad

La alta disponibilidad es compatible con las interfaces SR-IOV de Citrix ADC versión 12.0 compilación 57.19 en adelante.

Si la configuración de alta disponibilidad se implementó manualmente o mediante la plantilla de Citrix CloudFormation para Citrix ADC versión 12.0 56.20 y versiones posteriores, la función de IAM asociada a la configuración de alta disponibilidad debe tener los siguientes privilegios:

- ec2:DescribeInstances
- ec2:DescribeNetworkInterfaces
- ec2:DetachNetworkInterface
- ec2:AttachNetworkInterface
- ec2:StartInstances
- ec2:StopInstances
- ec2:RebootInstances
- autoscaling:*
- sns:*
- sqs: *
- IAM: Simular directiva principal
- Soy: obtener rol

De forma predeterminada, la plantilla de Citrix CloudFormation para Citrix ADC versión 12.0 57.19 agrega automáticamente los privilegios necesarios a la función de IAM.

> **Nota**
>
> Una configuración de alta disponibilidad con interfaces SR-IOV tarda alrededor de 100 segundos de tiempo de inactividad.

Recursos relacionados:

Para obtener más información sobre los roles de IAM, consulte la documentación de AWS.

Configurar una instancia de Citrix ADC VPX para utilizar redes mejoradas con AWS ENA

August 20, 2021

Después de crear una instancia Citrix ADC VPX en AWS, puede configurar el dispositivo virtual para utilizar redes mejoradas con AWS Elastic Network Adapter (ENA)mediante AWS CLI.

Junto con AWS ENA, las redes mejoradas proporcionan mayor ancho de banda, mayor rendimiento de paquete por segundo (PPS) y latencia entre instancias cada vez menor.

Antes de iniciar la configuración, lea los siguientes temas:

- Requisitos previos
- Instrucciones de uso y limitaciones

Se admiten las siguientes configuraciones de alta disponibilidad para instancias habilitadas para ENA:

- Las direcciones IP privadas se pueden mover dentro de la misma zona de disponibilidad.
- Las direcciones IP elásticas se pueden mover a través de las zonas de disponibilidad.

Actualizar una instancia de Citrix ADC VPX en AWS

August 20, 2021

Puede actualizar el tipo de instancia de EC2, el rendimiento, la edición de software y el software del sistema de un dispositivo Citrix ADC VPX que se ejecuta en AWS. Para ciertos tipos de actualizaciones, Citrix recomienda utilizar el método Configuración de alta disponibilidad para minimizar el tiempo de inactividad.

> Nota:
>
> - La versión 10.1.e-124.1308.e o posterior del software Citrix ADC VPX AMI (incluidas las licencias de utilidad y las licencias de cliente) no admite las familias de instancias M1 y M2.

> - Debido a los cambios en la compatibilidad con instancias VPX, no se admite la reducción de 10.1.e-124 o una versión posterior a 10.1.123.x o una versión anterior.
> - La mayoría de las actualizaciones no requieren el inicio de una nueva AMI, y la actualización se puede realizar en la instancia actual de AMI de Citrix ADC. Si quiere actualizar a una nueva instancia de AMI de Citrix ADC, utilice el método de configuración de alta disponibilidad.

Cambiar el tipo de instancia EC2 de una instancia de Citrix ADC VPX en AWS

Si las instancias de Citrix ADC VPX están ejecutando la versión 10.1.e-124.1308.e o posterior, puede cambiar el tipo de instancia EC2 desde la consola de AWS de la siguiente manera:

1. Detenga la instancia VPX.
2. Cambie el tipo de instancia de EC2 desde la consola de AWS.
3. Inicie la instancia.

También puede utilizar el procedimiento anterior para cambiar el tipo de instancia EC2 para una versión anterior a 10.1.e-124.1308.e, a menos que quiera cambiar el tipo de instancia a M3. En ese caso, debe seguir primero el procedimiento de actualización estándar de Citrix ADC, en, para actualizar el software Citrix ADC a 10.1.e-124 o a una versión posterior y, a continuación, seguir los pasos anteriores.

Actualice el rendimiento o la edición de software de una instancia de Citrix ADC VPX en AWS

Para actualizar la edición de software (por ejemplo, para actualizar de la edición estándar a la Premium) o el rendimiento (por ejemplo, para actualizar de 200 Mbps a 1000 mbps), el método depende de la licencia de la instancia.

Uso de una licencia de cliente (Bring-Your-Own-License)

Si utiliza una licencia de cliente, puede comprar y descargar la nueva licencia desde el sitio web de Citrix y, a continuación, instalar la licencia en la instancia de VPX. Para obtener más información acerca de cómo descargar e instalar una licencia desde el sitio web de Citrix, consulte la Guía de licencias de VPX.

Uso de una licencia de utilidad (licencia de utilidad con tarifa horaria)

AWS no admite actualizaciones directas para instancias basadas en tarifas. Para actualizar la edición de software o el rendimiento de una instancia de Citrix ADC VPX basada en tarifas, inicie una nueva AMI con la licencia y la capacidad deseadas y migre la configuración de instancia anterior a la nueva instancia. Esto se puede lograr mediante una configuración de alta disponibilidad de Citrix ADC como se describe en Actualizar a una nueva instancia de la AMI de Citrix ADC mediante una subsección de configuración de alta disponibilidad de Citrix ADC de esta página.

Actualizar el software del sistema de una instancia de Citrix ADC VPX en AWS

Si necesita actualizar una instancia VPX que ejecuta 10.1.e-124.1308.e o una versión posterior, siga el procedimiento de actualización estándar de Citrix ADC en Actualizar y bajar de categoría un dispositivo Citrix ADC.

Si necesita actualizar una instancia VPX que ejecute una versión anterior a 10.1.e-124.1308.e a 10.1.e-124.1308.e o una versión posterior, actualice primero el software del sistema y, a continuación, cambie el tipo de instancia a M3 de la siguiente manera:

1. Detenga la instancia VPX.
2. Cambie el tipo de instancia de EC2 desde la consola de AWS.
3. Inicie la instancia.

Actualizar a una nueva instancia de AMI de Citrix ADC mediante una configuración de alta disponibilidad de Citrix ADC

Para utilizar el método de alta disponibilidad para actualizar a una nueva instancia de AMI de Citrix ADC, realice las siguientes tareas:

- Cree una nueva instancia con el tipo de instancia EC2, la edición de software, el rendimiento o la versión de software deseados desde el mercado de AWS.
- Configure la alta disponibilidad entre la instancia antigua (que se va a actualizar) y la nueva. Una vez configurada la alta disponibilidad entre la instancia anterior y la nueva, la configuración de la instancia anterior se sincroniza con la nueva instancia.
- Forzar una conmutación por error de alta disponibilidad de la instancia anterior a la nueva instancia. Como resultado, la nueva instancia se convierte en primaria y comienza a recibir tráfico.
- Detenga y vuelva a configurar o eliminar la instancia anterior de AWS.

Requisitos previos y puntos a considerar

- Asegúrese de comprender cómo funciona la alta disponibilidad entre dos instancias de Citrix ADC VPX en AWS. Para obtener más información sobre la configuración de alta disponibilidad entre dos instancias Citrix ADC VPX en AWS, consulte Implementación de un par de alta disponibilidad en AWS.
- Debe crear la nueva instancia en la misma zona de disponibilidad que la instancia anterior, teniendo exactamente el mismo grupo de seguridad y subred.
- La configuración de alta disponibilidad requiere claves de acceso y secretas asociadas a la cuenta de AWS Identity and Access Management (IAM) del usuario para ambas instancias. Si no se utiliza la información de clave correcta al crear instancias VPX, se produce un error en la configuración de HA. Para obtener más información sobre cómo crear una cuenta de IAM para una instancia VPX, consulte Requisitos previos.

- Debe utilizar la consola EC2 para crear la nueva instancia. No puede utilizar el inicio de AWS 1-Clic, ya que no acepta las claves de acceso y secretas como entrada.
- La nueva instancia debe tener solo una interfaz ENI.

Para actualizar una instancia de Citrix ADC VPX mediante una configuración de alta disponibilidad, siga estos pasos:

1. Configure la alta disponibilidad entre la instancia anterior y la nueva. Para configurar la alta disponibilidad entre dos instancias Citrix ADC VPX, en el símbolo del sistema de cada instancia, escriba:

   - `add ha node <nodeID> <IPaddress of the node to be added>`
   - `save config`

   Ejemplo:

   En el símbolo del sistema de la instancia anterior, escriba:

   ```
   1 add ha node 30 192.0.2.30
   2 Done
   3 <!--NeedCopy-->
   ```

   En el símbolo del sistema de la nueva instancia, escriba:

   ```
   1 add ha node 10 192.0.2.10
   2 Done
   3 <!--NeedCopy-->
   ```

   Tenga en cuenta lo siguiente:

   - En la configuración de HA, la instancia anterior es el nodo principal y la nueva instancia es el nodo secundario.
   - La dirección IP de NSIP no se copia de la instancia anterior a la nueva instancia. Por lo tanto, después de la actualización, la nueva instancia tiene una dirección IP de administración diferente de la anterior.
   - La contraseña de `nsroot` cuenta de la nueva instancia se establece en la de la instancia anterior tras la sincronización de alta disponibilidad.

   Para obtener más información sobre la configuración de alta disponibilidad entre dos instancias Citrix ADC VPX en AWS, consulte Implementación de un par de alta disponibilidad en AWS.

2. Forzar una conmutación por error de alta disponibilidad. Para forzar una conmutación por error en una configuración de alta disponibilidad, en el símbolo del sistema de cualquiera de las instancias, escriba:


```
force HA failover
<!--NeedCopy-->
```

Como resultado de forzar una conmutación por error, los ENI de la instancia anterior se migran a la nueva instancia y el tráfico fluye a través de la nueva instancia (el nuevo nodo principal). La instancia anterior (el nuevo nodo secundario) se reinicia.

Si aparece el siguiente mensaje de advertencia, escriba N para anular la operación:

```
[WARNING]:Force Failover may cause configuration loss, peer health
    not optimum. Reason(s):
HA version mismatch
HA heartbeats not seen on some interfaces
Please confirm whether you want force-failover (Y/N)?
<!--NeedCopy-->
```

El mensaje de advertencia aparece porque el software del sistema de las dos instancias VPX no es compatible con HA. Como resultado, la configuración de la instancia anterior no se puede sincronizar automáticamente con la nueva instancia durante una conmutación por error forzada.

A continuación se presenta la solución alternativa para este problema:

a) En el símbolo del shell de Citrix ADC de la instancia anterior, escriba el siguiente comando para crear una copia de seguridad del archivo de configuración (ns.conf):

   ```
   copy /nsconfig/ns.conf to /nsconfig/ns.conf.bkp
   ```

b) Elimine la siguiente línea del archivo de configuración de copia de seguridad (ns.conf.bkp):

   - `set ns config -IPAddress <IP> -netmask <MASK>`

   Por ejemplo: `set ns config -IPAddress 192.0.2.10 -netmask 255.255.255.0`

c) Copie el archivo de configuración de copia de seguridad de la antigua instancia (ns.conf.bkp) en el directorio /nsconfig de la nueva instancia.

d) En el símbolo del shell de Citrix ADC de la nueva instancia, escriba el siguiente comando para cargar el archivo de configuración de la instancia anterior (ns.conf.bkp) en la nueva instancia:

   - `batch -f /nsconfig/ns.conf.bkp`

e) Guarde la configuración en la nueva instancia.

   - `save conifg`

f) En el símbolo del sistema de cualquiera de los nodos, escriba el comando siguiente para forzar una conmutación por error y, a continuación, escriba Y para el mensaje de advertencia para confirmar la operación de conmutación por error de fuerza:

- `force ha failover`

Ejemplo:

```
        > force ha failover

WARNING]:Force Failover may cause configuration loss, peer health
    not optimum.
        Reason(s):
        HA version mismatch
        HA heartbeats not seen on some interfaces
        Please confirm whether you want force-failover (Y/N)? Y
<!--NeedCopy-->
```

3. Elimine la configuración de HA, de modo que las dos instancias ya no estén en una configuración de HA. Primero elimine la configuración de HA del nodo secundario y, a continuación, elimine la configuración de HA del nodo primario.

   Para quitar una configuración de alta disponibilidad entre dos instancias de Citrix ADC VPX, en el símbolo del sistema de cada instancia, escriba:

```
    > remove ha node <nodeID>
    >  save config
<!--NeedCopy-->
```

   Para obtener más información sobre la configuración de alta disponibilidad entre dos instancias VPX en AWS, consulte Implementar un par de alta disponibilidad en AWS.

   Ejemplo:

En el símbolo del sistema de la instancia anterior (nuevo nodo secundario), escriba:

```
        > remove ha node 30
          Done
        > save config
          Done
<!--NeedCopy-->
```


En el símbolo del sistema de la nueva instancia (nuevo nodo principal), escriba:

```
1          > remove ha node 10
2            Done
3          > save config
4            Done
5  <!--NeedCopy-->
```

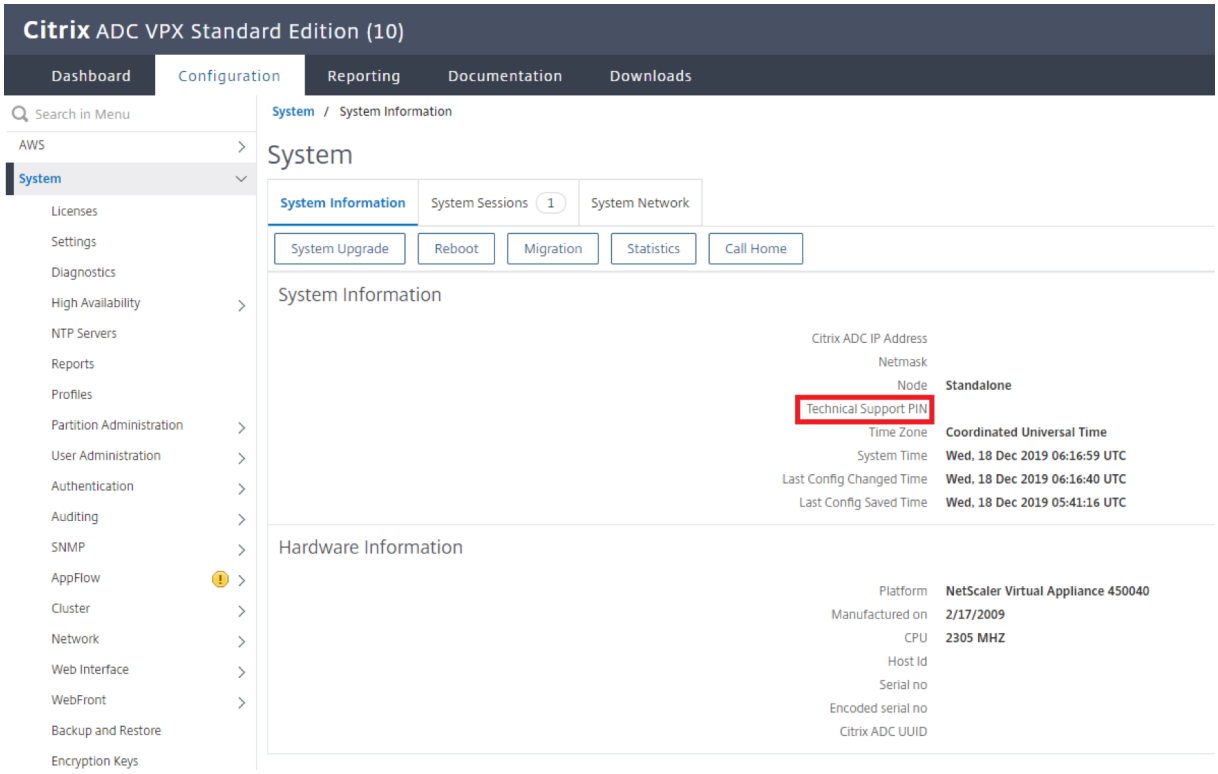
Solucionar problemas de una instancia VPX en AWS

August 20, 2021

Amazon no proporciona acceso de consola a una instancia de Citrix ADC VPX. Para solucionar problemas, debe utilizar la interfaz gráfica de usuario de AWS para ver el registro de actividades. Solo puede depurar si la red está conectada. Para ver el registro del sistema de una instancia, haga clic con el botón derecho en la instancia y seleccione Registro del sistema.

Citrix ofrece compatibilidad con las instancias de Citrix ADC VPX con licencia de AWS Marketplace (licencia de utilidad con tarifa horaria) en AWS. Para presentar un caso de soporte técnico, busque el número de cuenta de AWS y el código PIN de soporte, y llame al servicio de asistencia de Citrix. También se le pedirá su nombre y su dirección de correo electrónico. Para encontrar el PIN de soporte, inicie sesión en la GUI de VPX y vaya a la página Sistema.

Aquí hay un ejemplo de una página del sistema que muestra el PIN de soporte.



Preguntas frecuentes sobre AWS

February 19, 2022

- **¿ Admite una instancia de Citrix ADC VPX los volúmenes cifrados en AWS?**

  El cifrado y el descifrado ocurren a nivel del Hypervisor y, por lo tanto, funcionan perfectamente con cualquier instancia. Para obtener más información acerca de los volúmenes cifrados, consulte el siguiente documento de AWS:

  https://docs.aws.amazon.com/kms/latest/developerguide/services-ebs.html

- **¿ Cuál es la mejor manera de aprovisionar una instancia de Citrix ADC VPX en AWS?**

  Puede aprovisionar una instancia de Citrix ADC VPX en AWS de cualquiera de las siguientes maneras:

  - Plantilla de AWS CloudFormation (CFT) en el mercado de AWS
  - Citrix ADM
  - Inicio rápido de AWS
  - Citrix AWS CFT en GitHub
  - Scripts de Citrix Terraform en GitHub
  - Libros de jugadas de Citrix Ansible en GitHub

- flujo de trabajo de lanzamiento de AWS EC2

Puede elegir cualquiera de las opciones enumeradas en función de la herramienta de automatización que utilice.

Para obtener más información sobre las opciones, consulte Citrix ADC VPX en AWS.

- **¿ Cómo actualizar la instancia de Citrix ADC VPX en AWS?**

  Para actualizar la instancia Citrix ADC VPX en AWS, puede actualizar el software del sistema o actualizar a una nueva Amazon Machine Image (AMI) de Citrix ADC VPX mediante el procedimiento de Actualización de una instancia Citrix ADC VPX en AWS.

  La forma recomendada de actualizar una instancia Citrix ADC VPX es utilizar el servicio ADM siguiendo el procedimiento de Utilizar trabajos para actualizar instancias de Citrix ADC.

- **¿ Cuál es el tiempo de conmutación por error de alta disponibilidad para Citrix ADC VPX en AWS?**

  - La conmutación por error de alta disponibilidad de Citrix ADC VPX dentro de la zona de disponibilidad de AWS tarda aproximadamente 3 segundos.
  - La conmutación por error de alta disponibilidad de Citrix ADC VPX en las zonas de disponibilidad de AWS tarda unos 5 segundos.

- **¿ Qué nivel de soporte se proporciona a los clientes de suscripción de Citrix ADC VPX Marketplace que proporcionan el PIN de soporte técnico?**

  De forma predeterminada, el servicio “Seleccionar software” se proporciona a los clientes que proporcionan el PIN de soporte técnico.

- **En Alta disponibilidad en diferentes zonas mediante la implementación de IP elástica, ¿necesitamos crear varios conjuntos de IPsets para cada aplicación?**

  Sí. Si hay varias aplicaciones con varios VIP asignados a varios EIP, se requieren varios IPsets. Por lo tanto, durante la conmutación por error de alta disponibilidad, todas las asignaciones VIP principales de los EIP se cambian a VIP secundarias (nuevas primarias).

- **¿Por qué está habilitado el modo INC en alta disponibilidad en diferentes implementaciones de zonas?**

  Los pares de alta disponibilidad en todas las zonas de disponibilidad se encuentran en redes diferentes. Para la sincronización de alta disponibilidad, la configuración de red no debe sincronizarse. Esto se logra habilitando el modo INC en el par HA.

- **¿Puede el nodo de alta disponibilidad de una zona de disponibilidad comunicarse con los servidores back-end de otra zona de disponibilidad, siempre que esas zonas de disponibilidad estén en la misma VPC?**

Sí, se puede acceder a subredes de diferentes zonas de disponibilidad de la misma VPC agregando una ruta adicional que apunta a la subred del servidor backend mediante SNIP. Por ejemplo, si la subred SNIP de ADC en AZ1 es 192.168.3.0/24 y la subred del servidor backend de AZ2 es 192.168.6.0/24, se debe agregar una ruta en el dispositivo Citrix ADC presente en AZ1 como 192.168.6.0 255.255.255.0 192.168.3.1.

- **¿ La alta disponibilidad en distintas zonas mediante IP elástica y alta disponibilidad en distintas zonas mediante implementaciones de IP privada pueden funcionar conjuntamente?**

  Sí, ambas configuraciones se pueden aplicar en el mismo par HA.

- **En Alta disponibilidad en distintas zonas mediante la implementación de IP privada, si hay varias subredes con varias tablas de redirección en una VPC, ¿cómo sabe un nodo secundario del par HA de comprobar la tabla de rutas durante la conmutación por error de alta disponibilidad?**

  El nodo secundario conoce las NIC principales y busca en todas las tablas de redirección de una VPC.

- **¿Cuál es el tamaño de la `/var` partición cuando se utiliza la imagen predeterminada para VPX en AWS? ¿Cómo aumentar el espacio en disco?**

  El tamaño del disco raíz está limitado a 20 GB para mantener la imagen del disco pequeña.

  Si desea aumentar el espacio del directorio `/var/core/` o el `/var/crash/` directorio, conecte un disco adicional. Para aumentar el `/var` tamaño, actualmente, debe adjuntar un disco adicional y crear un enlace simbólico al `/var`, después de copiar el contenido crítico en el nuevo disco.

- **¿Cuántos motores de paquetes están activados y asignados a vCPU?**

  Los motores de paquetes (PE) están limitados por el número de vCPU con licencia. Los daemons de Citrix ADC no están anclados a ninguna vCPU concreta y pueden ejecutarse en cualquiera de las vCPU que no sean PE. Según AWS, la C5.9xLarge es una instancia de 36 VCPU con 72 GB de memoria. Con las licencias agrupadas, la instancia Citrix ADC VPX se implementa con el número máximo de PE. En este caso, 19 PE se ejecutan en los núcleos del 1 al 19. Sin embargo, los procesos de administración de ADC se ejecutan desde las CPU 20-31.

- **¿Cómo decidir la instancia de AWS correcta para ADC?**

  1. Comprenda su caso de uso y requisitos, como el rendimiento, el PPS, los requisitos SSL y el tamaño medio de los paquetes.
  2. Elija la oferta y las licencias de ADC correctas que cumplan sus requisitos, como las ofertas de ancho de banda VPX o las licencias basadas en vCPU.
  3. En función de la oferta elegida, decida la instancia de AWS.

  Ejemplo:

Una licencia de 5 Gbps permite 5 motores de paquetes de datos. Por lo tanto, el requisito de vCPU es 6 (5+1 para administración). Sin embargo, la instancia de 6 vCPU no está disponible. Por lo tanto, una CPU virtual de 8 es lo suficientemente buena para alcanzar ese rendimiento siempre que elija una red que admita un ancho de banda de 5 Gbps. Por ejemplo, debe elegir m5.2xlarge para una licencia de ancho de banda de 5 Gbps para permitir la asignación máxima de PE para una licencia de 5 Gbps. Pero si utiliza una licencia de vCPU que no está limitada por el rendimiento, es posible que obtenga un rendimiento de 5 Gbps mediante la propia instancia m5.xlarge.

Instance Size	vCPU	Memory (GiB)	Instance Storage (GiB)	Network Bandwidth (Gbps)	EBS Bandwidth (Mbps)
m5.large	2	8	EBS-Only	Up to 10	Up to 4,750
m5.xlarge	4	16	EBS-Only	Up to 10	Up to 4,750
m5.2xlarge	8	32	EBS-Only	Up to 10	Up to 4,750
m5.4xlarge	16	64	EBS-Only	Up to 10	4,750

- **¿Es obligatoria la implementación de tres NIC y tres subredes para ADC en AWS**?

  `Three NICs-three subnets` es la implementación recomendada, donde cada una para la administración, el cliente y la red de servidores. Esta implementación proporciona un mejor aislamiento del tráfico y un rendimiento VPX. Dos NIC, dos subredes y una subred NIC uno son las otras opciones disponibles. Citrix no recomienda que varias NIC compartan una subred en AWS, como dos NIC, una implementación de subred. Porque podría provocar problemas de red, como la redirección asimétrico. Para obtener más información, consulte Prácticas recomendadas para configurar interfaces de red en AWS.

Implementar una instancia de Citrix ADC VPX en Microsoft Azure

June 2, 2022

Al implementar una instancia de Citrix ADC VPX en Microsoft Azure Resource Manager (ARM), puede usar los dos conjuntos de funciones siguientes para satisfacer las necesidades de su empresa:

- Capacidades de cloud computing de Azure
- Funciones de equilibrio de carga y administración del tráfico de Citrix ADC

Puede implementar instancias Citrix ADC VPX en ARM como instancias independientes o como pares de alta disponibilidad en modos activo-en espera.

Puede implementar una instancia Citrix ADC VPX en Microsoft Azure de dos formas:

- A través de Azure Marketplace. El dispositivo virtual Citrix ADC VPX está disponible como imagen en Microsoft Azure Marketplace.
- Usar la plantilla json de Azure Resource Manager (ARM) de Citrix ADC disponible en GitHub. Para obtener más información, consulte el repositorio de GitHub para las plantillas de soluciones Citrix ADC.

La pila de Microsoft Azure es una plataforma integrada de hardware y software que ofrece los servicios de nube pública de Microsoft Azure en un centro de datos local para que las organizaciones puedan construir nubes híbridas. Ahora puede implementar las instancias de Citrix ADC VPX en la pila de Microsoft Azure.

Requisito previo

Necesita conocimientos previos antes de implementar una instancia de Citrix VPX en Azure.

- Familiaridad con la terminología de Azure y los detalles de red. Para obtener información, consulte Terminología de Azure.
- Conocimiento de un dispositivo Citrix ADC. Para obtener información detallada sobre el dispositivo Citrix ADC, consulte Citrix ADC.
- Conocimiento de las redes Citrix ADC. Consulte el tema Redes.

Cómo funciona una instancia de Citrix ADC VPX en Azure

En una implementación local, una instancia de Citrix ADC VPX requiere al menos tres direcciones IP:

- Dirección IP de administración, denominada dirección NSIP
- Dirección IP de subred (SNIP) para comunicarse con el conjunto de servidores
- Dirección IP del servidor virtual (VIP) para aceptar solicitudes de clientes

Para obtener más información, consulte Arquitectura de red para instancias Citrix ADC VPX en Microsoft Azure.

> **Nota**
>
> Los dispositivos virtuales VPX se pueden implementar en cualquier tipo de instancia que tenga dos o más núcleos Intel VT-X y más de 2 GB de memoria. Para obtener más información sobre los requisitos del sistema, consulte la hoja de datos de Citrix ADC VPX. Actualmente, la instancia Citrix ADC VPX admite solo los procesadores Intel.

En una implementación de Azure, puede aprovisionar una instancia de Citrix ADC VPX en Azure de tres maneras:

- Arquitectura multi-IP multi-NIC
- Arquitectura multi-IP de NIC única

- IP única NIC única

Según sus necesidades, puede utilizar cualquiera de estos tipos de arquitectura compatibles.

Arquitectura multi-IP multi-NIC

En este tipo de implementación, puede tener más de una interfaz de red (NIC) conectada a una instancia VPX. Cualquier NIC puede tener una o más configuraciones IP: direcciones IP públicas y privadas estáticas o dinámicas asignadas.

Para obtener más información, consulte los siguientes casos de uso:

- Configurar una configuración de alta disponibilidad con varias direcciones IP y NIC
- Configurar una configuración de alta disponibilidad con varias direcciones IP y NIC mediante comandos de PowerShell

> Nota
>
> Para evitar movimientos MAC y silenciar la interfaz en entornos Azure, Citrix recomienda crear una VLAN por interfaz de datos (sin etiqueta) de la instancia VPX de ADC y vincular la IP principal de la NIC en Azure. Para obtener más información, consulte el artículo CTX224626.

Arquitectura multi-IP de NIC única

En este tipo de implementación, una interfaz de red (NIC) asociada a varias configuraciones IP: direcciones IP públicas y privadas estáticas o dinámicas asignadas.
Para obtener más información, consulte los siguientes casos de uso:

- Configuración de varias direcciones IP para una instancia independiente Citrix ADC VPX
- Configurar varias direcciones IP para una instancia independiente de Citrix ADC VPX mediante comandos de PowerShell

IP única NIC única

En este tipo de implementación, una interfaz de red (NIC) asociada a una única dirección IP, que se utiliza para realizar las funciones de NSIP, SNIP y VIP.

Para obtener más información, consulte el siguiente caso de uso:

- Configurar una instancia independiente de Citrix ADC VPX

> **Nota**
>
> El modo IP única solo está disponible en implementaciones de Azure. Este modo no está

> disponible para una instancia de Citrix ADC VPX en sus instalaciones, en AWS ni en ningún otro tipo de implementación.

Licencias de Citrix ADC VPX

Una instancia de Citrix ADC VPX en Azure requiere una licencia. Las siguientes opciones de licencia están disponibles para las instancias Citrix ADC VPX que se ejecutan en Azure.

- **Licencias basadas en suscripción**: los dispositivos Citrix ADC VPX están disponibles como instancias de pago en Azure Marketplace. Las licencias basadas en suscripciones son una opción de pago por uso. A los usuarios se les cobra cada hora. Los siguientes modelos y tipos de licencia VPX están disponibles en Azure Marketplace.

Modelo VPX	Tipo de licencia	Instancia recomendada
VPX10	Estándar, Avanzado, Premium	Standard_D2s_v4
VPX200	Estándar, Avanzado, Premium	Standard_D2s_v4
VPX1000*	Estándar, Avanzado, Premium	Standard_D4s_v4
VPX3000*	Estándar, Avanzado, Premium	Standard_D4s_v4
VPX5000*	Estándar, Avanzado, Premium	Standard_D8s_v4

> *: De los modelos VPX 1000 a VPX 5000, debe habilitar las redes aceleradas en las instancias Citrix ADC VPX para obtener el rendimiento deseado. Para obtener más información sobre la configuración de redes aceleradas, consulte Configurar una instancia de Citrix ADC VPX para usar redes aceleradas de Azure.

  Citrix proporciona asistencia técnica para instancias de licencia basadas en suscripciones. Para presentar un caso de asistencia, consulte Asistencia para Citrix ADC en Azure: licencia de suscripción con precio por hora.

- **Traiga su propia licencia (BYOL)**: Si trae su propia licencia (BYOL), consulte la Guía de licencias de VPX en http://support.citrix.com/article/CTX122426. Es necesario que:
  - Utilice el portal de licencias del sitio web de Citrix para generar una licencia válida.
  - Cargue la licencia en la instancia.

Modelo VPX	Tipo de licencia	Instancia recomendada
VPX10	Estándar, Avanzado, Premium	Standard_D2s_v4
VPX200	Estándar, Avanzado, Premium	Standard_D2s_v4
VPX1000*	Estándar, Avanzado, Premium	Standard_D4s_v4

Modelo VPX	Tipo de licencia	Instancia recomendada
VPX3000*	Estándar, Avanzado, Premium	Standard_D4s_v4
VPX5000*	Estándar, Avanzado, Premium	Standard_D8s_v4
VPX8000*	Estándar, Avanzado, Premium	Standard_D8s_v4
VPX10000*	Estándar, Avanzado, Premium	Standard_D16s_v4

> *: De los modelos VPX 1000 a VPX 10000, debe habilitar las redes aceleradas en las instancias Citrix ADC VPX para obtener el rendimiento deseado. Para obtener más información sobre la configuración de redes aceleradas, consulte Configurar una instancia de Citrix ADC VPX para usar redes aceleradas de Azure.

- Licencias de**Check-in/Check-out de Citrix ADC VPX: Para obtener más información, consulte Licencias**de Check-in/Check-out de Citrix ADC VPX.

> **Nota**
>
> En un entorno de pila de Azure, **BYOL** es la única opción de licencia disponible.

A partir de NetScaler versión 12.0 56.20, VPX Express para implementaciones locales y en la nube no requiere un archivo de licencia. Para obtener más información sobre Citrix ADC VPX Express, consulte la sección “Licencia de Citrix ADC VPX Express” de la descripción general de licencias de Citrix ADC.

> **Nota**
>
> Independientemente de la licencia por hora basada en suscripción adquirida en Azure Marketplace, en casos excepcionales, la instancia de Citrix ADC VPX implementada en Azure podría tener una licencia predeterminada de Citrix ADC. Esto ocurre debido a problemas con Azure Instance Metadata Service (IMDS).
>
> Realice un reinicio en caliente antes de realizar cualquier cambio de configuración en la instancia de Citrix ADC VPX, para habilitar la licencia de Citrix ADC VPX correcta.

Compatibilidad con IPv6 para la instancia de Citrix ADC VPX en Azure

A partir de la versión 13.1-21.x, la instancia independiente de Citrix ADC VPX admite direcciones IPv6 en Azure. Puede configurar las direcciones IPv6 como direcciones VIP y SNIP en la instancia independiente de Citrix ADC VPX en la nube de Azure.

Para obtener información sobre cómo habilitar IPv6 en Azure, consulte la siguiente documentación de Azure:

- ¿Qué es IPv6 para la red virtual de Azure?

- Agregar IPv6 a una aplicación IPv4 en la red virtual de Azure: CLI de Azure
- Tipos de direcciones

Para obtener información sobre cómo el dispositivo Citrix ADC admite IPv6, consulte Protocolo de Internet versión 6.

Limitaciones:

- Las implementaciones de IPv6 en Citrix ADC actualmente no admiten el escalado automático de backend de Azure.
- La implementación de alta disponibilidad de Citrix ADC VPX no admite IPv6.

Limitaciones

La ejecución de la solución de equilibrio de carga de Citrix ADC VPX en ARM impone las siguientes limitaciones:

- La arquitectura de Azure no admite las siguientes funciones de Citrix ADC:
  - ARP gratuito (GARP)
  - Modo L2
  - VLAN etiquetada
  - Redirección dinámica
  - MAC virtual
  - USIP
  - Marcos Jumbo
  - Agrupar en clústeres

  > Nota
  >
  > Con la función de escalabilidad automática de Citrix Application Delivery Management (ADM) (implementación en la nube), las instancias de ADC admiten la agrupación en clústeres en todas las licencias. Para obtener información, consulte Escalado automático de Citrix ADC VPX en Microsoft Azure mediante Citrix ADM.

- Si espera que tenga que apagar y desasignar temporalmente la máquina virtual Citrix ADC VPX en cualquier momento, asigne una dirección IP interna estática al crear la máquina virtual. Si no asigna una dirección IP interna estática, Azure podría asignar a la máquina virtual una dirección IP diferente cada vez que se reinicie, y es posible que no se pueda acceder a la máquina virtual.
- En una implementación de Azure, solo se admiten los siguientes modelos de Citrix ADC VPX: VPX 10, VPX 200, VPX 1000 y VPX 3000. Para obtener información, consulte la hoja de datos de Citrix ADC VPX.

  Si utiliza una instancia de Citrix ADC VPX con un número de modelo superior a VPX 3000, es posible que el rendimiento de red no sea el mismo especificado en la licencia de la instancia.

Sin embargo, otras funciones, como el rendimiento de SSL y las transacciones SSL por segundo, podrían mejorar.

- El "ID de implementación" generado por Azure durante el Provisioning de máquinas virtuales no es visible para el usuario en ARM. No puede usar el ID de implementación para implementar el dispositivo Citrix ADC VPX en ARM.
- La instancia de Citrix ADC VPX admite un rendimiento de 20 MB/s y funciones de edición estándar cuando se inicializa.
- Las instancias Citrix ADC VPX en Azure con redes aceleradas habilitadas proporcionan un mejor rendimiento. Las instancias de Citrix ADC VPX admiten redes aceleradas de Azure a partir de la versión 13.0 compilación 76.x. Para habilitar la red acelerada en ADC VPX, Citrix recomienda utilizar un tipo de instancia de Azure que admita redes aceleradas.
- Para una implementación de XenApp y XenDesktop, un servidor virtual VPN en una instancia VPX se puede configurar en los siguientes modos:
  - Modo básico, donde el parámetro del servidor virtual `ICAOnly` VPN se establece en ACTIVADO. El modo Básico funciona completamente en una instancia de Citrix ADC VPX sin licencia.
  - Modo SmartAccess, donde el parámetro del servidor virtual `ICAOnly` VPN se establece en DESACTIVADO. El modo SmartAccess solo funciona para cinco usuarios de sesión de Citrix ADC AAA en una instancia de Citrix ADC VPX sin licencia.

> **Nota**
>
> Para configurar la función SmartControl, debe aplicar una licencia Premium a la instancia de Citrix ADC VPX.

Terminología de Azure

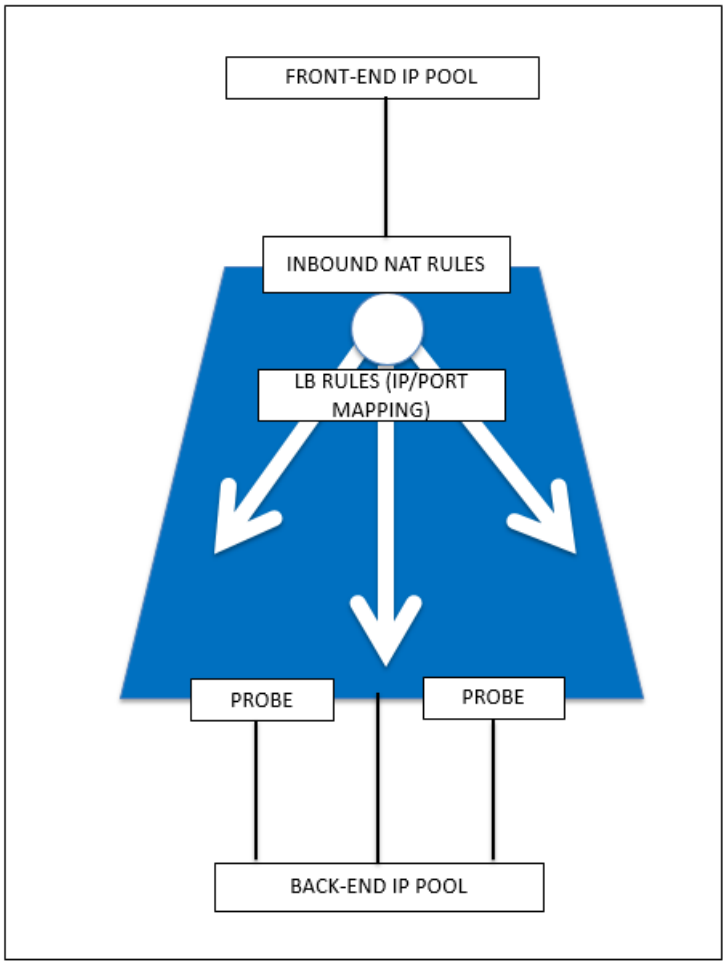
August 20, 2021

A continuación se enumeran algunos de los términos de Azure que se utilizan en la documentación de Citrix ADC VPX Azure.

1. Equilibrador de carga de Azure: El equilibrador de carga de Azure es un recurso que distribuye el tráfico entrante entre los equipos de una red. El tráfico se distribuye entre máquinas virtuales definidas en un conjunto de equilibradores de carga. Un equilibrador de carga puede ser externo o orientado a Internet, o puede ser interno.
2. Azure Resource Manager (ARM): ARM es el nuevo marco de administración para los servicios de Azure. Azure Load Balancer se administra mediante API y herramientas basadas en ARM.

3. Grupo de direcciones de back-end: son direcciones IP asociadas a la NIC de máquina virtual (NIC) a la que se distribuirá la carga.
4. BLOB: Objeto binario grande: Cualquier objeto binario como un archivo o una imagen que se puede almacenar en el almacenamiento de Azure.
5. Configuración de IP de front-end: Un equilibrador de carga de Azure puede incluir una o más direcciones IP de front-end, también conocidas como IP virtuales (VIP). Estas direcciones IP sirven como entrada para el tráfico.
6. IP pública de nivel de instancia (ILPIP): Un ILPIP es una dirección IP pública que puede asignar directamente a su máquina virtual o instancia de rol, en lugar de al servicio en la nube en el que reside la máquina virtual o la instancia de rol. Esto no ocupa el lugar del VIP (IP virtual) que se asigna a su servicio en la nube. Más bien, es una dirección IP adicional que puede usar para conectarse directamente a su máquina virtual o instancia de rol.

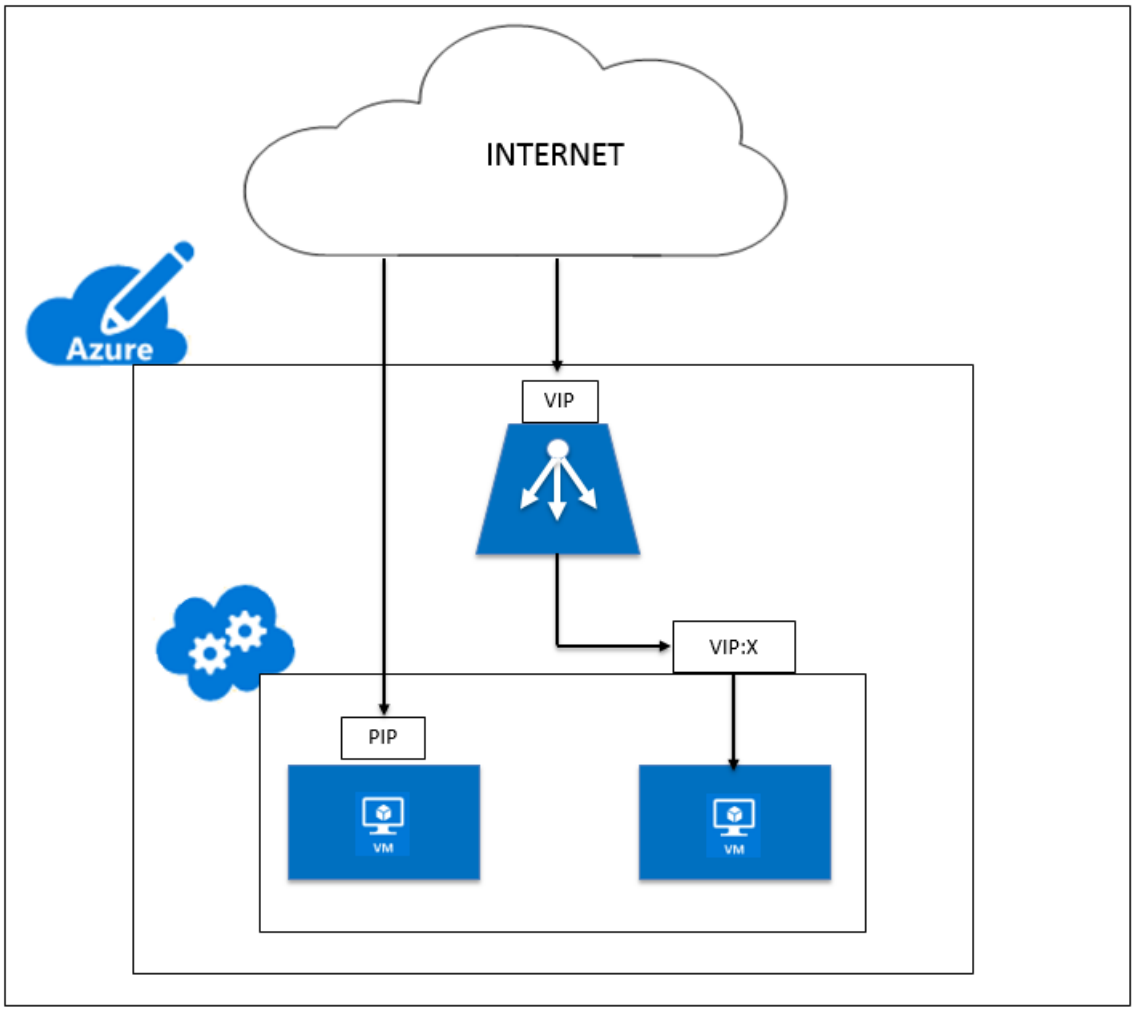
   Nota: En el pasado, un ILPIP se denominaba PIP, que significa IP pública.
7. Reglas NAT entrantes: Contiene reglas que asignan un puerto público en el equilibrador de carga a un puerto para una máquina virtual específica en el grupo de direcciones back-end.
8. IP-config: Se puede definir como un par de direcciones IP (IP pública e IP privada) asociado a una NIC individual. En una configuración IP, la dirección IP pública puede ser NULL. Cada NIC puede tener varias IP-config asociadas, que pueden ser de hasta 255.
9. Reglas de equilibrio de carga: Propiedad de regla que asigna una combinación de puertos y IP de front-end dada a un conjunto de direcciones IP de back-end y combinación de puertos. Con una sola definición de un recurso de equilibrador de carga, puede definir varias reglas de equilibrio de carga, cada regla refleja una combinación de una IP de front-end y una IP de puerto y de back-end y un puerto asociado con máquinas virtuales.



10. Grupo de seguridad de red: contiene una lista de reglas de lista de control de acceso (ACL) que permiten o deniegan el tráfico de red a las instancias de máquina virtual en una red virtual. Los NSG se pueden asociar con subredes o instancias individuales de máquinas virtuales dentro de esa subred. Cuando un grupo de seguridad de red está asociado a una subred, las reglas de ACL se aplican a todas las instancias de máquina virtual de esa subred. Además, el tráfico a una máquina virtual individual se puede restringir aún más asociando un grupo de seguridad de red directamente a esa máquina virtual.
11. Direcciones IP privadas: Se utilizan para la comunicación dentro de una red virtual de Azure y la red local cuando utiliza una Gateway VPN para extender la red a Azure. Las direcciones IP privadas permiten que los recursos de Azure se comuniquen con otros recursos de una red virtual o local a través de una Gateway VPN o un circuito ExpressRoute, sin utilizar una dirección IP accesible a Internet. En el modelo de implementación de Azure Resource Manager, se asocia una dirección IP privada con los siguientes tipos de recursos de Azure: Máquinas virtuales, equilibradores de carga internos (ILB) y puertas de enlace de aplicaciones.
12. Sondeos: Contiene sondeos de estado utilizados para comprobar la disponibilidad de instancias de máquinas virtuales en el grupo de direcciones back-end. Si una máquina virtual en par-

ticular no responde a los sondeos de estado durante algún tiempo, entonces se saca del servicio de tráfico. Los sondeos permiten realizar un seguimiento del estado de las instancias virtuales. Si falla un sondeo de estado, la instancia virtual se quitará automáticamente de rotación.

13. Direcciones IP públicas (PIP): PIP se utiliza para la comunicación con Internet, incluidos los servicios públicos de Azure y se asocia con máquinas virtuales, equilibradores de carga orientados a Internet, puertas de enlace VPN y puertas de enlace de aplicaciones.
14. Región: área dentro de una geografía que no cruza las fronteras nacionales y que contiene uno o varios centros de datos. Los precios, los servicios regionales y los tipos de oferta están expuestos a nivel regional. Una región suele estar emparejada con otra región, que puede estar hasta varios cientos de millas de distancia, para formar un par regional. Los pares regionales se pueden utilizar como mecanismo para la recuperación ante desastres y casos de alta disponibilidad. También se conoce generalmente como ubicación.
15. Grupo de recursos: Un contenedor en el Administrador de recursos contiene recursos relacionados para una aplicación. El grupo de recursos puede incluir todos los recursos de una aplicación, o solo aquellos recursos que se agrupan lógicamente
16. Cuenta de almacenamiento: Una cuenta de almacenamiento de Azure le da acceso a los servicios de blob, colas, tablas y archivos de Azure en Almacenamiento de Azure. La cuenta de almacenamiento proporciona el espacio de nombres único para los objetos de datos de almacenamiento de Azure.
17. Máquina virtual: Implementación de software de un equipo físico que ejecuta un sistema operativo. Varias máquinas virtuales pueden ejecutarse simultáneamente en el mismo hardware. En Azure, las máquinas virtuales están disponibles en una variedad de tamaños.
18. Red virtual: Una red virtual de Azure es una representación de su propia red en la nube. Es un aislamiento lógico de la nube de Azure dedicada a su suscripción. Puede controlar completamente los bloques de direcciones IP, la configuración de DNS, las directivas de seguridad y las tablas de redirecciones dentro de esta red. También puede segmentar aún más su vNet en subredes e iniciar máquinas virtuales de Azure IaaS y servicios en la nube (instancias de rol PaaS). Además, puede conectar la red virtual a la red local mediante una de las opciones de conectividad disponibles en Azure. En esencia, puede expandir su red a Azure, con un control completo de los bloques de direcciones IP con el beneficio de Azure a escala empresarial.



Arquitectura de red para instancias de Citrix ADC VPX en Microsoft Azure

August 20, 2021

En Azure Resource Manager (ARM), una máquina virtual (VM) Citrix ADC VPX reside en una red virtual. Se puede crear una única interfaz de red en una subred dada de la Red Virtual y se puede conectar a la instancia VPX. Puede filtrar el tráfico de red hacia y desde una instancia VPX en una red virtual de Azure con un grupo de seguridad de red. Un grupo de seguridad de red contiene reglas de seguridad que permiten o deniegan el tráfico de red entrante o saliente desde una instancia VPX. Para obtener más información, consulte Grupos de seguridad.

El grupo de seguridad de red filtra las solicitudes a la instancia de Citrix ADC VPX y la instancia VPX las envía a los servidores. La respuesta de un servidor sigue la misma ruta en sentido inverso. El grupo de seguridad de red se puede configurar para filtrar una sola VM VPX o, con subredes y redes virtuales,

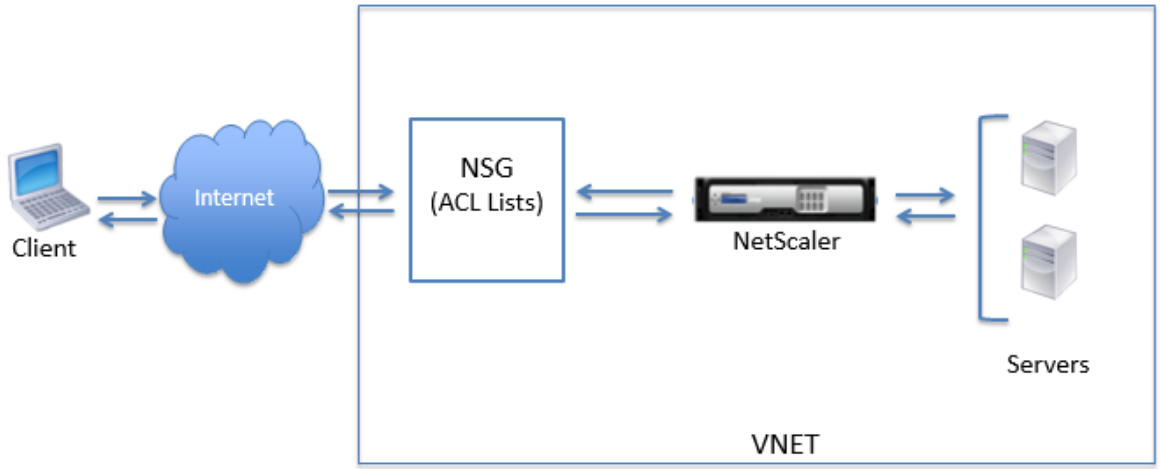
puede filtrar el tráfico en la implementación de varias instancias VPX.

La NIC contiene detalles de configuración de red como la red virtual, las subredes, la dirección IP interna y la dirección IP pública.

Mientras esté en ARM, es bueno conocer las siguientes direcciones IP que se utilizan para acceder a las VM implementadas con una sola NIC y una sola dirección IP:

- La dirección IP pública (PIP) es la dirección IP orientada a Internet configurada directamente en la NIC virtual de la máquina virtual de NetScaler. Esto le permite acceder directamente a una máquina virtual desde la red externa.
- La dirección IP de Citrix ADC (también conocida como NSIP) es la dirección IP interna configurada en la máquina virtual. No es enrutable.
- La dirección IP virtual (VIP) se configura mediante el NSIP y un número de puerto. Los clientes acceden a los servicios de NetScaler a través de la dirección PIP, y cuando la solicitud llega a la NIC de la máquina virtual NetScaler VPX o el equilibrador de carga de Azure, el VIP se traduce a IP interna (NSIP) y número de puerto interno.
- La dirección IP interna es la dirección IP interna privada de la máquina virtual del grupo de espacio de direcciones de la red virtual. No se puede acceder a esta dirección IP desde la red externa. Esta dirección IP es dinámica de forma predeterminada, a menos que la establezca en estática. El tráfico de Internet se enruta a esta dirección de acuerdo con las reglas creadas en el grupo de seguridad de red. El grupo de seguridad de red se integra con la NIC para enviar selectivamente el tipo de tráfico correcto al puerto correcto de la NIC, lo que depende de los servicios configurados en la máquina virtual.

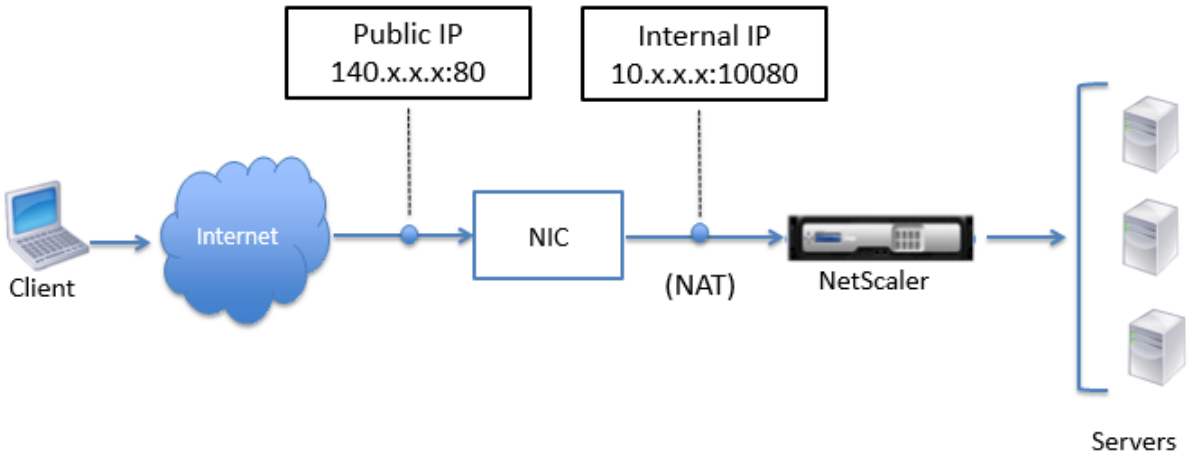
La siguiente ilustración muestra cómo fluye el tráfico de un cliente a un servidor a través de una instancia de NetScaler VPX aprovisionada en ARM.



Flujo de tráfico a través de la traducción de direcciones de red

También puede solicitar una dirección IP pública (PIP) para su instancia de Citrix ADC VPX (nivel de instancia). Si utiliza este PIP directo en el nivel de VM, no necesita definir reglas de entrada y salida para interceptar el tráfico de red. La solicitud entrante de Internet se recibe directamente en la máquina virtual. Azure realiza la traducción de direcciones de red (NAT) y reenvía el tráfico a la dirección IP interna de la instancia VPX.

La siguiente ilustración muestra cómo Azure realiza la traducción de direcciones de red para asignar la dirección IP interna de NetScaler.



En este ejemplo, la IP pública asignada al grupo de seguridad de red es 140.x.x.x y la dirección IP interna es 10.x.x.x. Cuando se definen las reglas de entrada y salida, el puerto HTTP público 80 se define como el puerto en el que se reciben las solicitudes del cliente, y el puerto privado correspondiente, 10080, se define como el puerto en el que escucha la instancia de Citrix ADC VPX. La solicitud del cliente se recibe en la dirección IP pública (140.x.x.x). Azure realiza la traducción de direcciones de red para asignar el PIP a la dirección IP interna 10.x.x.x en el puerto 10080 y reenvía la solicitud del cliente.

> **Nota**
>
> Las máquinas virtuales Citrix ADC VPX con alta disponibilidad están controladas por equilibradores de carga externos o internos que tienen reglas de entrada definidas para controlar el tráfico de equilibrio de carga. El tráfico externo es interceptado primero por estos equilibradores de carga y el tráfico se desvía de acuerdo con las reglas de equilibrio de carga configuradas, que tienen grupos back-end, reglas NAT y sondeos de estado definidos en los equilibradores de carga.

Directrices de uso de puertos

Puede configurar más reglas entrantes y salientes en un grupo de seguridad de red mientras crea la instancia Citrix ADC VPX o después de aprovisionar la máquina virtual. Cada regla de entrada y salida está asociada con un puerto público y un puerto privado.

Antes de configurar las reglas de grupo de seguridad de red, tenga en cuenta las siguientes pautas relativas a los números de puerto que puede utilizar:

1. La instancia de Citrix ADC VPX reserva los siguientes puertos. No se pueden definir como puertos privados cuando se utiliza la dirección IP pública para las solicitudes de Internet.

   Puertos 21, 22, 80, 443, 8080, 67, 161, 179, 500, 520, 3003, 3008, 3009, 3010, 3011, 4001, 5061, 9000, 7000.

   Sin embargo, si desea que los servicios orientados a Internet, como el VIP, utilicen un puerto estándar (por ejemplo, el puerto 443), debe crear una asignación de puertos mediante el grupo de seguridad de red. A continuación, el puerto estándar se asigna a un puerto diferente configurado en NetScaler para este servicio VIP.

   Por ejemplo, un servicio VIP podría estar ejecutándose en el puerto 8443 en la instancia VPX, pero asignarse al puerto público 443. Por lo tanto, cuando el usuario accede al puerto 443 a través de la IP pública, la solicitud se dirige al puerto privado 8443.
2. La dirección IP pública no admite protocolos en los que la asignación de puertos se abre dinámicamente, como FTP pasivo o ALG.
3. La alta disponibilidad no funciona para el tráfico que utiliza una dirección IP pública (PIP) asociada a una instancia VPX, en lugar de un PIP configurado en el equilibrador de carga de Azure.

> **Nota**
>
> En Azure Resource Manager, una instancia de Citrix ADC VPX está asociada a dos direcciones IP: Una dirección IP pública (PIP) y una dirección IP interna. Mientras el tráfico externo se conecta al PIP, la dirección IP interna o el NSIP no se puede enrutar. Para configurar VIP en VPX, utilice la dirección IP interna y cualquiera de los puertos libres disponibles. No utilice el PIP para configurar VIP.

Configurar una instancia independiente de Citrix ADC VPX

August 20, 2021

Puede aprovisionar una única instancia de Citrix ADC VPX en el portal de Azure Resource Manager (ARM) en modo independiente mediante la creación de la máquina virtual y la configuración de otros recursos.

Antes de comenzar

Asegúrese de que dispone de lo siguiente:

- Una cuenta de usuario de Microsoft Azure
- Acceso a Microsoft Azure Resource Manager
- SDK de Microsoft Azure
- Microsoft Azure PowerShell

En la página Microsoft Azure Portal, inicie sesión en el portal de Azure Resource Manager proporcionando su nombre de usuario y contraseña.

> **Nota**
>
> En el portal ARM, al hacer clic en una opción de un panel, se abre un nuevo panel a la derecha. Desplácese de un panel a otro para configurar el dispositivo.

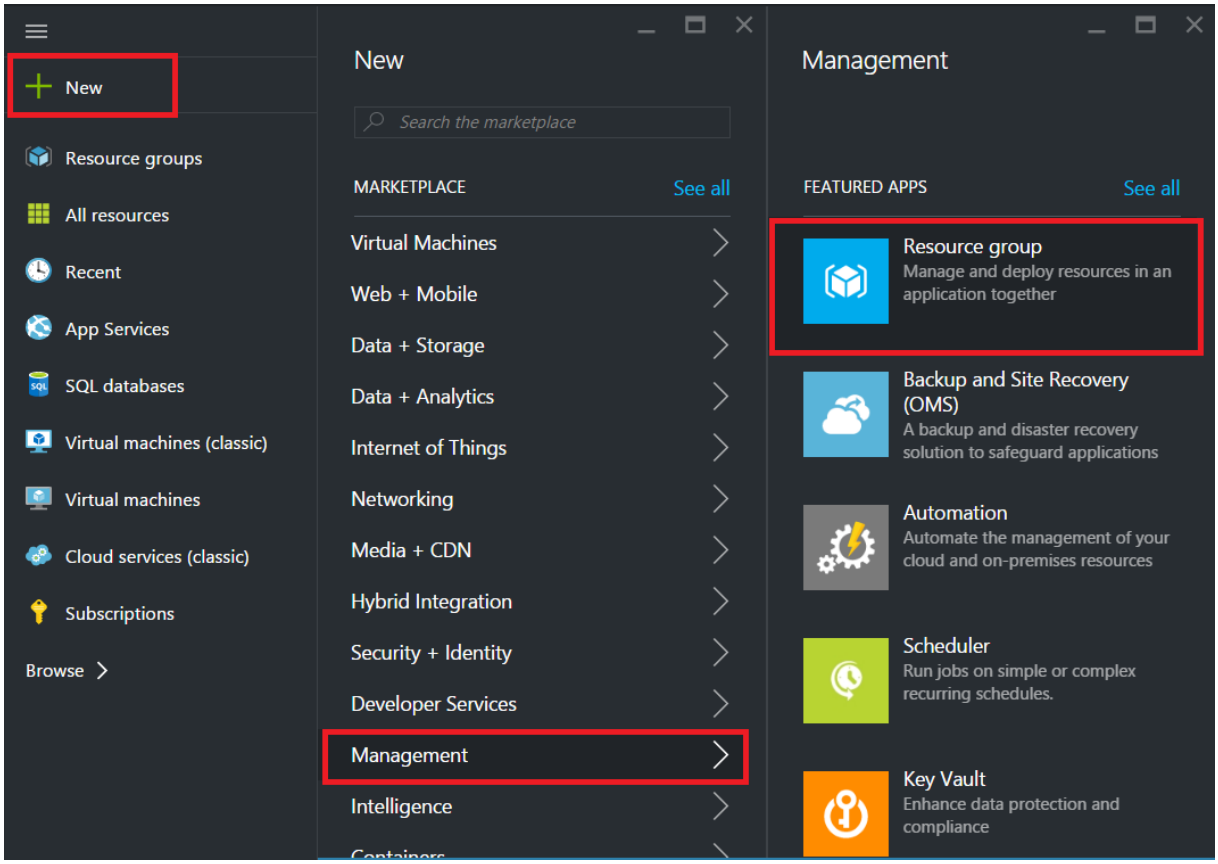
Resumen de los pasos de configuración

1. Configurar un grupo de recursos
2. Configurar un grupo de seguridad de red
3. Configurar la red virtual y sus subredes
4. Configurar una cuenta de almacenamiento
5. Configurar un conjunto de disponibilidad
6. Configure una instancia de Citrix ADC VPX.

Configurar un grupo de recursos

Cree un nuevo grupo de recursos que sea un contenedor para todos los recursos. Utilice el grupo de recursos para implementar, administrar y supervisar los recursos como grupo.

1. Haga clic en **Nuevo** > **Gestión** > **Grupo de recursos**.
2. En el panel **Grupo de recursos**, introduzca los siguientes detalles:
    - Nombre del grupo de recursos
    - Ubicación del grupo de recursos
3. Haga clic en **Crear**.

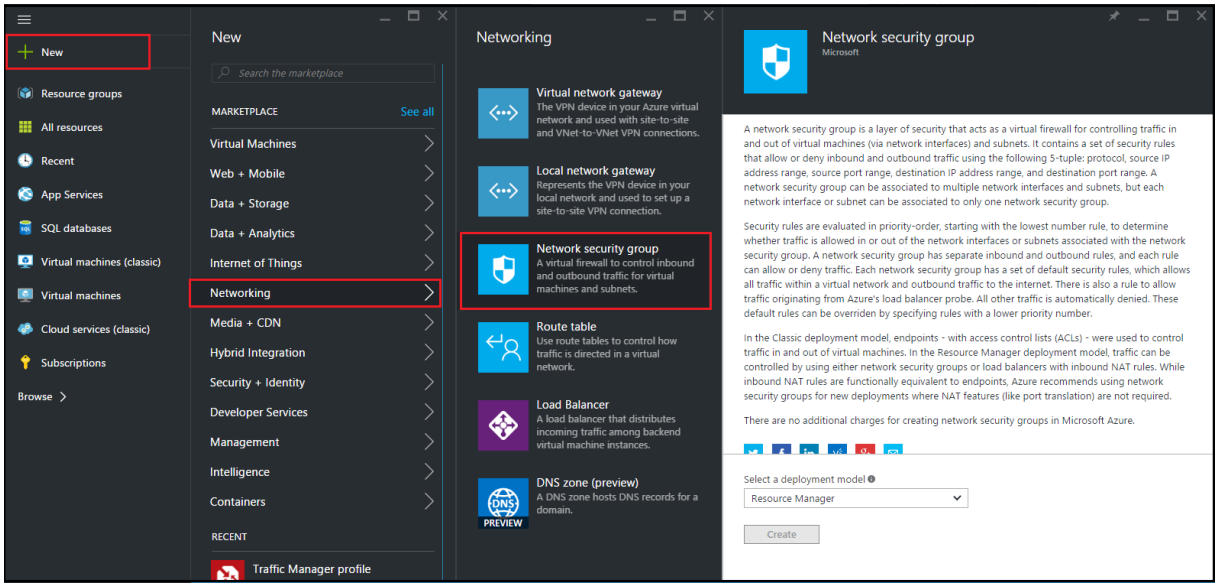


Configurar un grupo de seguridad de red

Cree un grupo de seguridad de red para asignar reglas entrantes y salientes para controlar el tráfico entrante y saliente dentro de la red virtual. El grupo de seguridad de red le permite definir reglas de seguridad para una única máquina virtual y también definir reglas de seguridad para una subred de red virtual.

1. Haga clic en **Nuevo** > **Redes** > **Grupo de seguridad de red**.
2. En el panel **Crear grupo de seguridad de red**, escriba los siguientes detalles y, a continuación, haga clic en **Crear**.
   - Nombre: Escriba un nombre para el grupo de seguridad
   - Grupo de recursos: Seleccione el grupo de recursos de la lista desplegable

> **Nota**
>
> Asegúrese de que ha seleccionado la ubicación correcta. La lista de recursos que aparecen en la lista desplegable es diferente para diferentes ubicaciones.

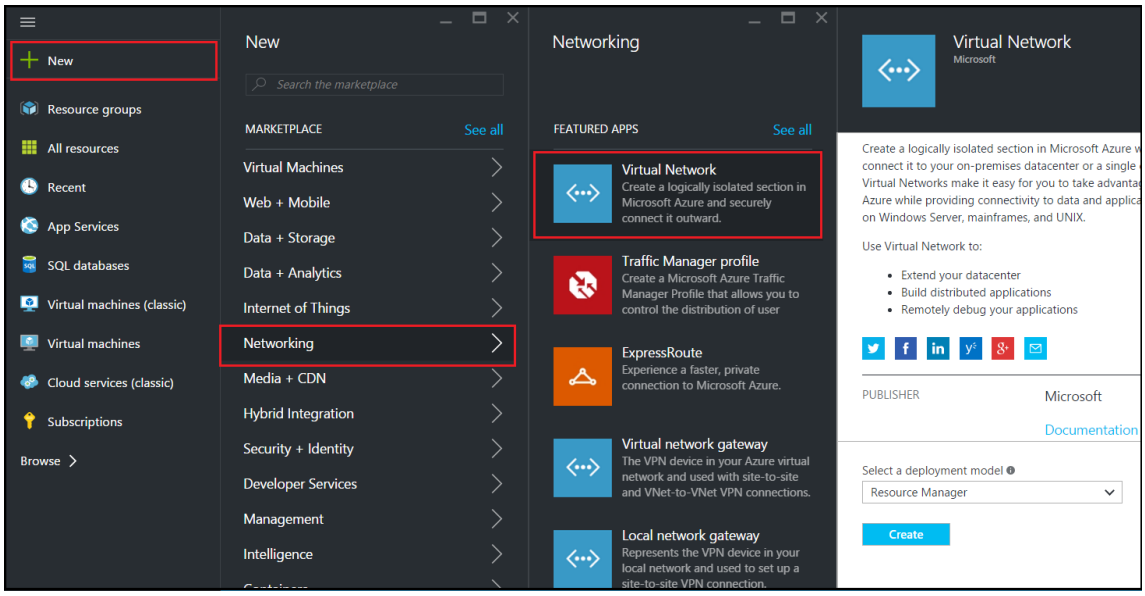


Configurar una red virtual y subredes

Las redes virtuales en ARM proporcionan una capa de seguridad y aislamiento a sus servicios. Las máquinas virtuales y los servicios que forman parte de la misma red virtual pueden tener acceso entre sí.

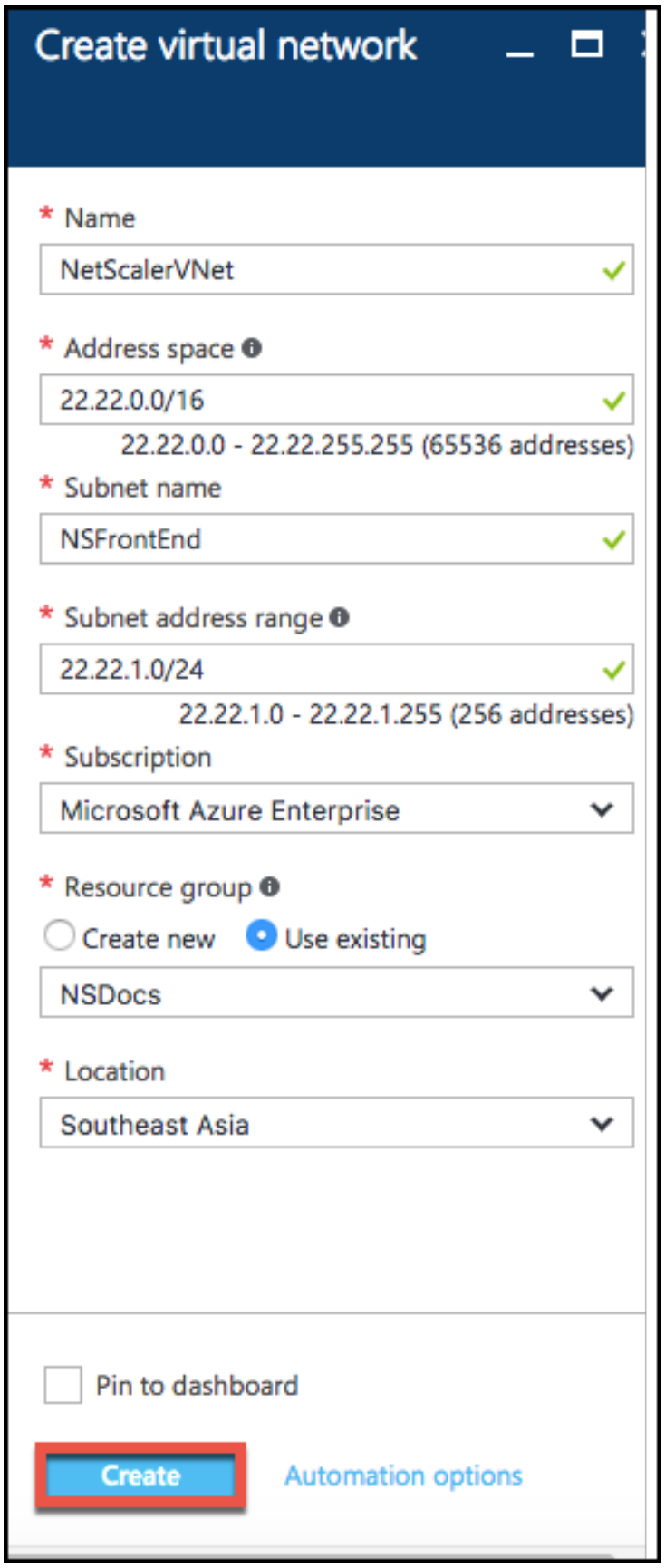
Para estos pasos para crear una red virtual y subredes.

1. Haga clic en **Nuevo** > **Redes** > **Red virtual**.
2. En el panel **Red virtual**, asegúrese de que el modo de implementación es **Administrador de recursos** y haga clic en **Crear**.



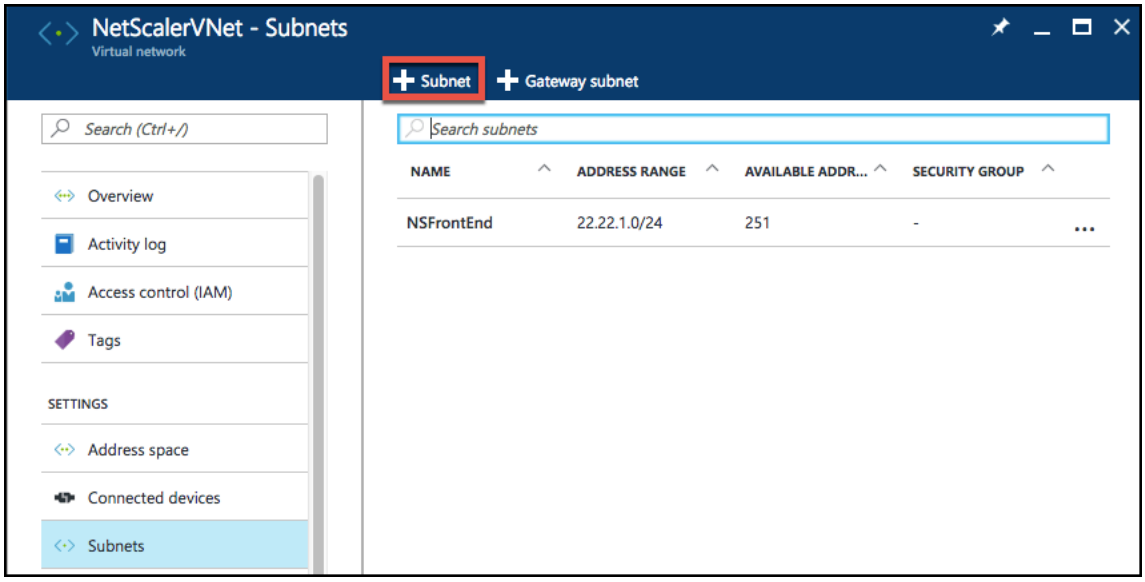
3. En el panel **Crear red virtual**, escriba los siguientes valores y, a continuación, haga clic en **Crear**.

- Nombre de la red virtual
- Espacio de direcciones: Escriba el bloque de direcciones IP reservado para la red virtual
- Subred: Escriba el nombre de la primera subred (creará la segunda subred más adelante en este paso)
- Intervalo de direcciones de subred: Escriba el bloque de direcciones IP reservadas de la subred
- Grupo de recursos: Seleccione el grupo de recursos creado anteriormente en la lista desplegable

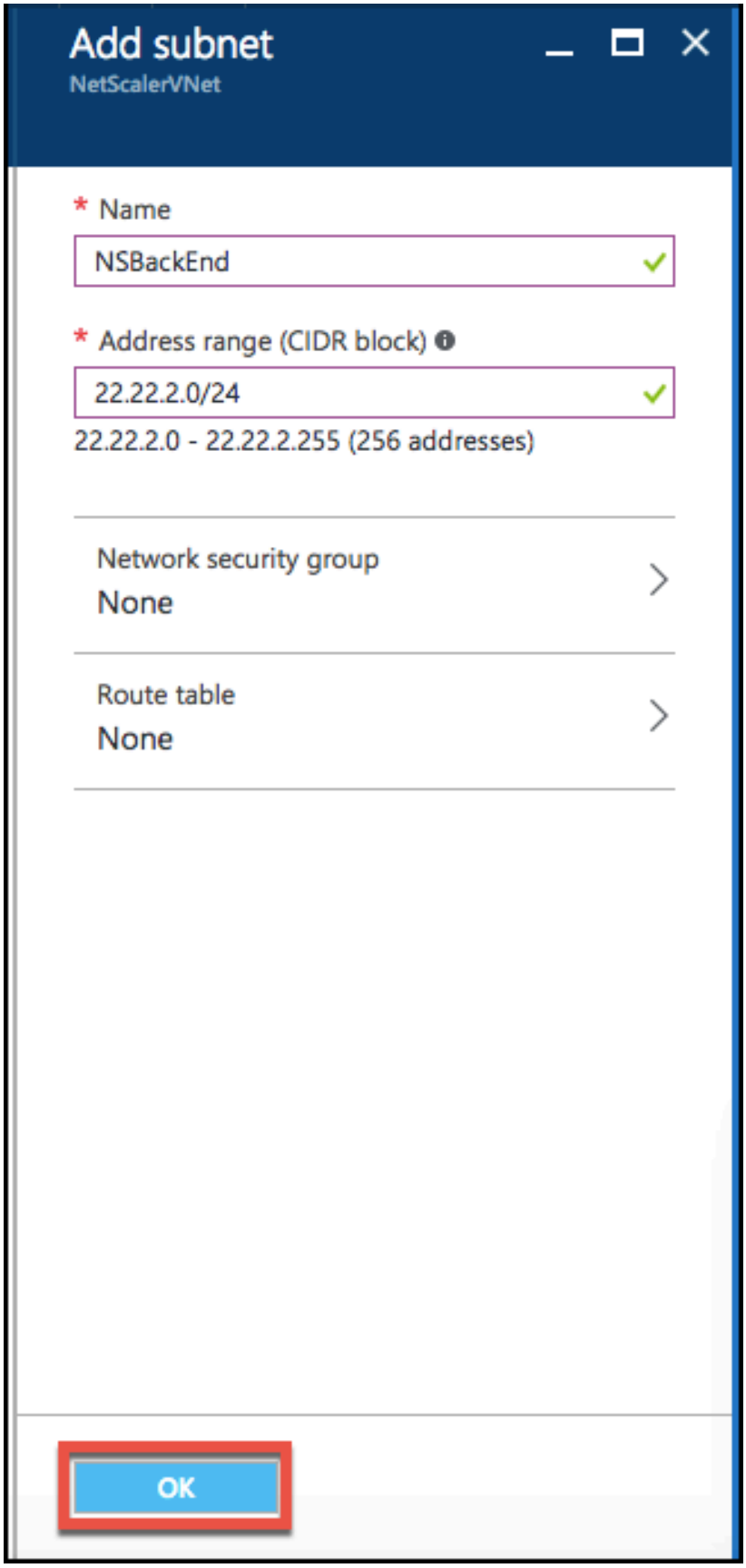


Configurar la segunda subred

1. Seleccione la red virtual recién creada en el panel **Todos los recursos** y, en el panel **Configuración**, haga clic en **Subredes**.



2. Haga clic en **+Subred** y cree la segunda subred introduciendo los siguientes detalles.
   - Nombre de la segunda subred
   - Intervalo de direcciones: Escriba el bloque de direcciones IP reservado de la segunda subred
   - Grupo de seguridad de red: seleccione el grupo de seguridad de red de la lista desplegable
3. Haga clic en **Crear**.

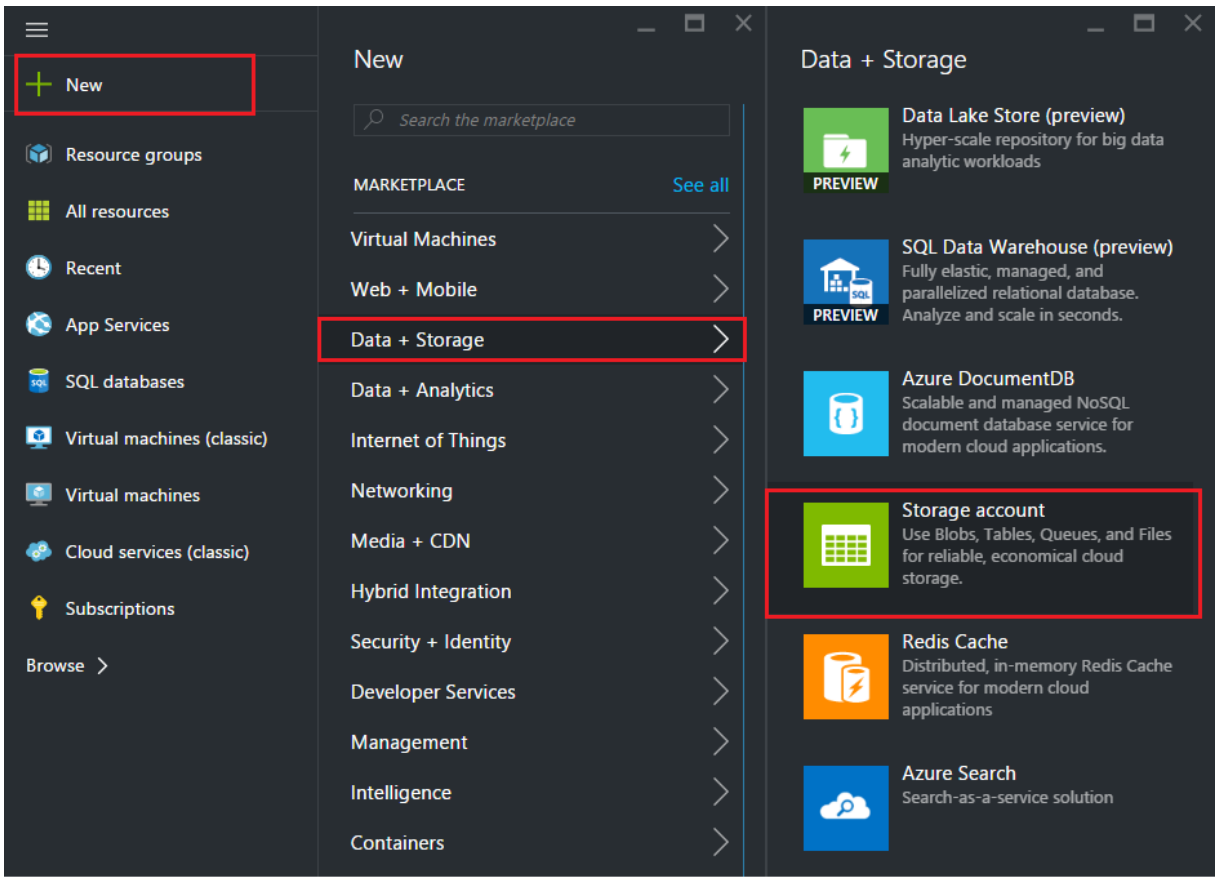


Configurar una cuenta de almacenamiento

El almacenamiento de infraestructura ARM IaaS incluye todos los servicios en los que podemos almacenar datos en forma de blobs, tablas, colas y archivos. También puede crear aplicaciones mediante estas formas de datos de almacenamiento en ARM.

Cree una cuenta de almacenamiento para almacenar todos sus datos.

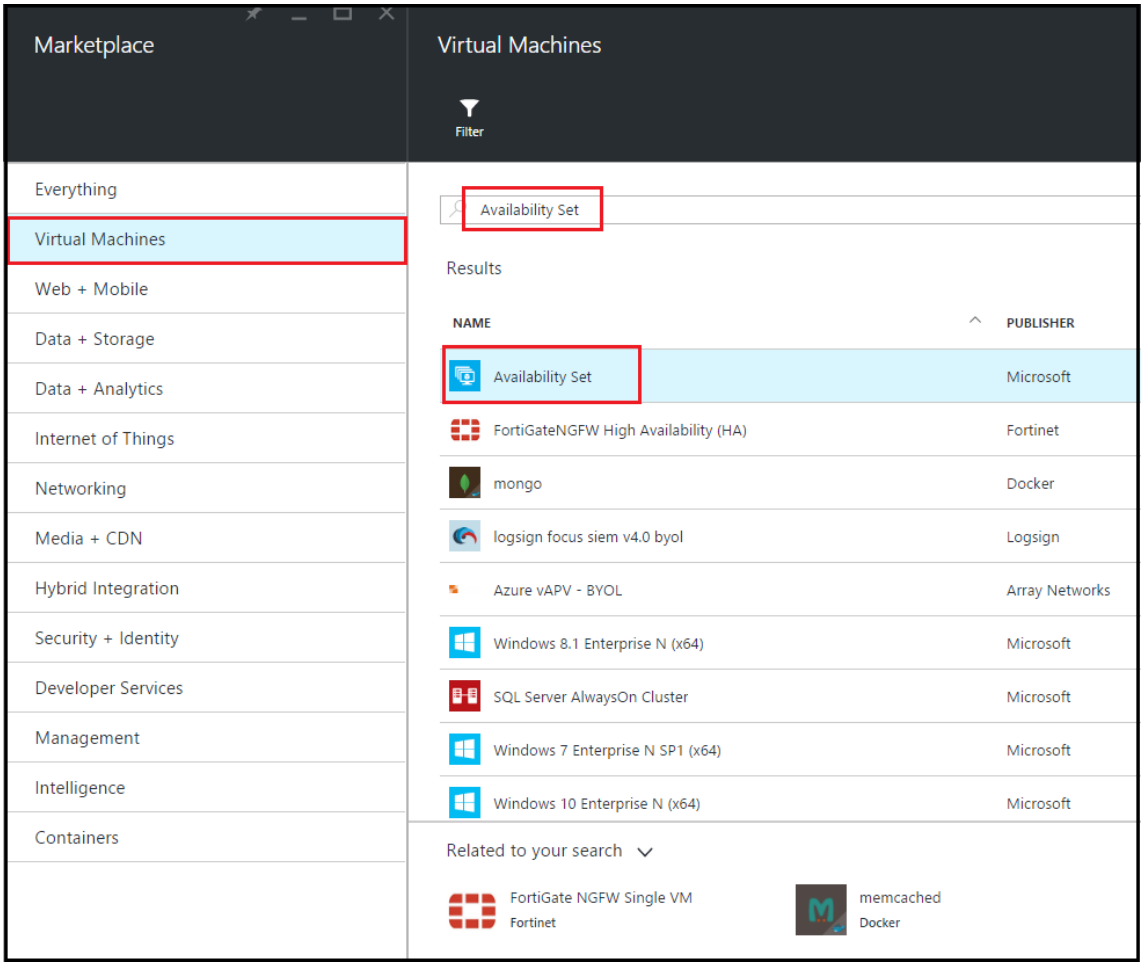
1. Haga clic en **+Nuevo** > **Datos + Almacenamiento** > **Cuenta de almacenamiento**.
2. En el panel **Crear cuenta de almacenamiento**, introduzca los siguientes detalles:
    - Nombre de la cuenta
    - Modo de implementación: Asegúrese de seleccionar **Administrador de recursos**
    - Tipo de cuenta: Seleccione **Propósito general** en la lista desplegable
    - Replicación: Seleccione **Almacenamiento redundante localmente** en la lista desplegable
    - Grupo de recursos: Seleccione el grupo de recursos recién creado en la lista desplegable
3. Haga clic en **Crear**.



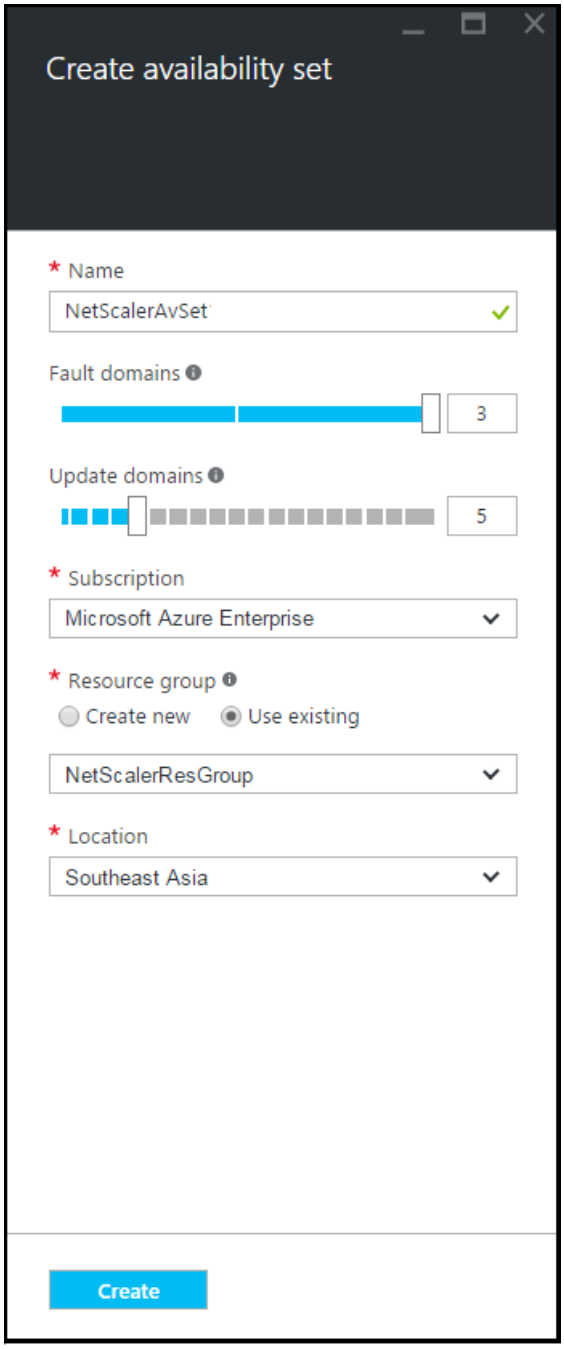
Configurar un conjunto de disponibilidad

Un conjunto de disponibilidad garantiza que al menos una máquina virtual se mantiene en funcionamiento en caso de mantenimiento planificado o no planificado. Dos o más máquinas virtuales bajo el mismo “conjunto de disponibilidad” se colocan en diferentes dominios de fallas para lograr servicios redundantes.

1. Haga clic en **+Nuevo**.
2. Haga clic en **Ver todo** en el panel MARKETPLACE y haga clic en **Máquinas virtuales**.
3. Busque el conjunto de disponibilidad y, a continuación, seleccione Entidad de **conjunto de disponibilidad** en la lista que se muestra.



4. Haga clic en **Crear y,** en el panel **Crear conjunto de disponibilidad**, introduzca los siguientes detalles:
   - Nombre del conjunto
   - Grupo de recursos: Seleccione el grupo de recursos recién creado en la lista desplegable
5. Haga clic en **Crear**.



Configurar una instancia de Citrix ADC VPX

Cree una instancia de Citrix ADC VPX en la red virtual. Obtenga la imagen de Citrix ADC VPX desde Azure Marketplace y, a continuación, use el portal de Azure Resource Manager para crear una instancia de Citrix ADC VPX.

Antes de comenzar a crear la instancia de Citrix ADC VPX, asegúrese de haber creado una red virtual con las subredes necesarias en las que reside la instancia. Puede crear redes virtuales durante el Provi-

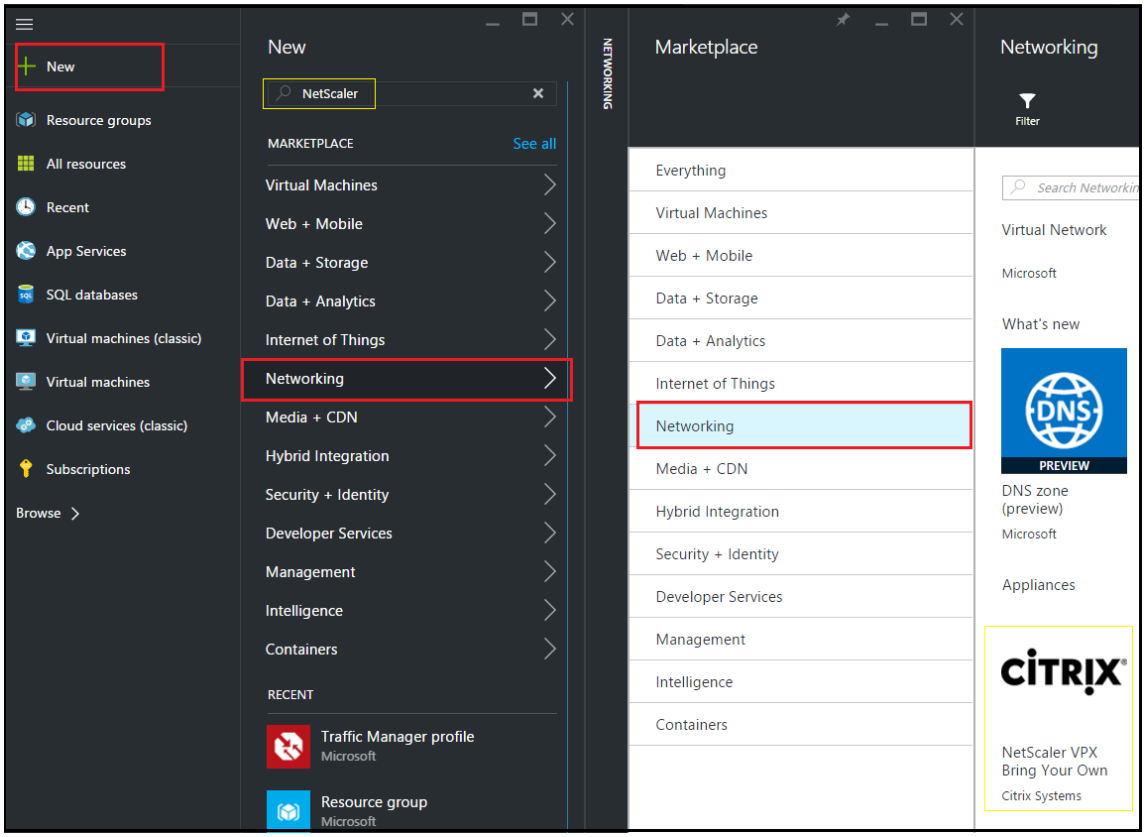
sioning de VM, pero sin la flexibilidad necesaria para crear subredes diferentes. Para obtener información sobre la creación de redes virtuales, consulte http://azure.microsoft.com/en-us/documentation/articles/create-virtual-network/.

Opcionalmente, configure el servidor DNS y la conectividad VPN que permita a una máquina virtual acceder a los recursos de Internet.

> **Nota**
>
> Citrix recomienda crear grupos de recursos, grupos de seguridad de red, redes virtuales y otras entidades antes de aprovisionar Citrix ADC VPX VM, de modo que la información de red esté disponible durante el Provisioning.

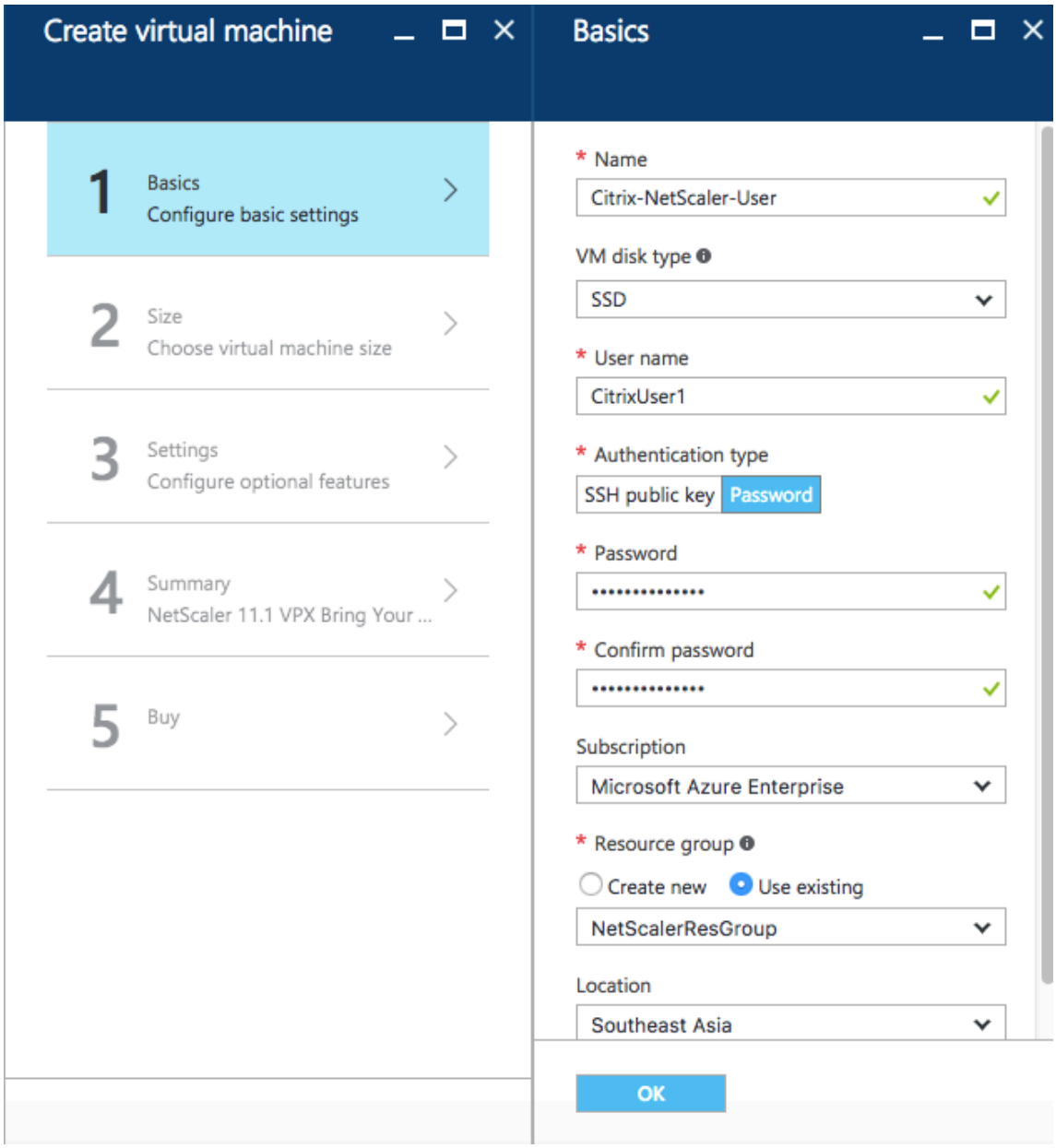
1. Haga clic en **+Nuevo** > **Redes**.
2. Haga clic en **Ver todo** y, en el panel Redes, haga clic en **Citrix ADC 13.0**.
3. Seleccione **Citrix ADC 13.0 VPX Bring Your Own License** en la lista de planes de software.

   Como forma rápida de encontrar cualquier entidad en el portal ARM, también puede escribir el nombre de la entidad en el cuadro de búsqueda de Azure Marketplace y presionar <Enter>. Escriba NetScaler en el cuadro de búsqueda para buscar las imágenes de Citrix NetScaler.



> **Nota**
>
> Asegúrese de seleccionar la imagen más reciente. Es posible que la imagen de Citrix NetScaler tenga el número de versión en el nombre.

4. En la página **Citrix ADC VPX Bring Your Own License**, en la lista desplegable, seleccione **Resource Manager** y haga clic en **Crear**.



5. En el panel **Crear máquina virtual**, especifique los valores necesarios en cada sección para crear una máquina virtual. Haga clic en **Aceptar** en cada sección para guardar la configuración.

Básico:

- Nombre: Especifique un nombre para la instancia de Citrix ADC VPX

- Tipo de disco VM: Seleccione SSD (valor predeterminado) o HDD en el menú desplegable
- Nombre de usuario y contraseña: Especifique un nombre de usuario y una contraseña para acceder a los recursos del grupo de recursos que ha creado
- Tipo de autenticación: Seleccione Clave pública SSH o Contraseña
- Grupo de recursos: Seleccione el grupo de recursos que ha creado en la lista desplegable

Puede crear un grupo de recursos aquí, pero Citrix recomienda crear un grupo de recursos a partir de grupos de recursos en Azure Resource Manager y, a continuación, seleccionar el grupo en la lista desplegable.

> **Nota**
>
> En un entorno de pila de Azure, además de los parámetros básicos, especifique los siguientes parámetros:
>
> - Dominio de pila de Azure
> - Arrendatario de pila de Azure (opcional)
> - Cliente de Azure (opcional)
> - Secreto de cliente de Azure (opcional)

Tamaño:

Según el tipo de disco de VM, SDD o HDD, que haya seleccionado en Configuración básica, se mostrarán los tamaños de disco.

- Seleccione un tamaño de disco según sus requisitos y haga clic en **Seleccionar**.

Configuración:

- Seleccione el tipo de disco predeterminado (Estándar)
- Cuenta de almacenamiento: Seleccione la cuenta de almacenamiento
- Red virtual: Seleccione la red virtual
- Subred: Establecer la dirección de subred
- Dirección IP pública: Seleccione el tipo de asignación de dirección IP
- Grupo de seguridad de red: Seleccione el grupo de seguridad que ha creado. Asegúrese de que las reglas de entrada y salida están configuradas en el grupo de seguridad.
- Conjunto de disponibilidad: Seleccione el conjunto de disponibilidad en el cuadro de menú desplegable

Resumen:

Los valores de configuración se validan y la página Resumen muestra el resultado de la validación. Si se produce un error en la validación, la página Resumen muestra el motivo del error. Vuelva a la sección en particular y realice los cambios necesarios. Si se pasa la validación, haga clic en **Aceptar**.

Comprar:

Revise los detalles de la oferta y los términos legales en la página Compra y haga clic en **Comprar**.

Para una implementación de alta disponibilidad, cree dos instancias independientes de Citrix ADC VPX en el mismo conjunto de disponibilidad y en el mismo grupo de recursos para implementarlas en configuración activa en espera.

Configurar varias direcciones IP para una instancia independiente de Citrix ADC VPX

August 20, 2021

En esta sección se explica cómo configurar una instancia independiente de Citrix ADC VPX con varias direcciones IP, en Azure Resource Manager (ARM). La instancia VPX puede tener una o más NIC conectadas a ella, y cada NIC puede tener asignada una o más direcciones IP públicas y privadas estáticas o dinámicas. Puede asignar varias direcciones IP como NSIP, VIP, SNIP, etc.

Para obtener más información, consulte la documentación de Azure Asignar varias direcciones IP a máquinas virtuales mediante el portal de Azure.

Si desea utilizar comandos de PowerShell, consulte Configuración de varias direcciones IP para una instancia Citrix ADC VPX en modo independiente mediante comandos de PowerShell.

Caso de uso

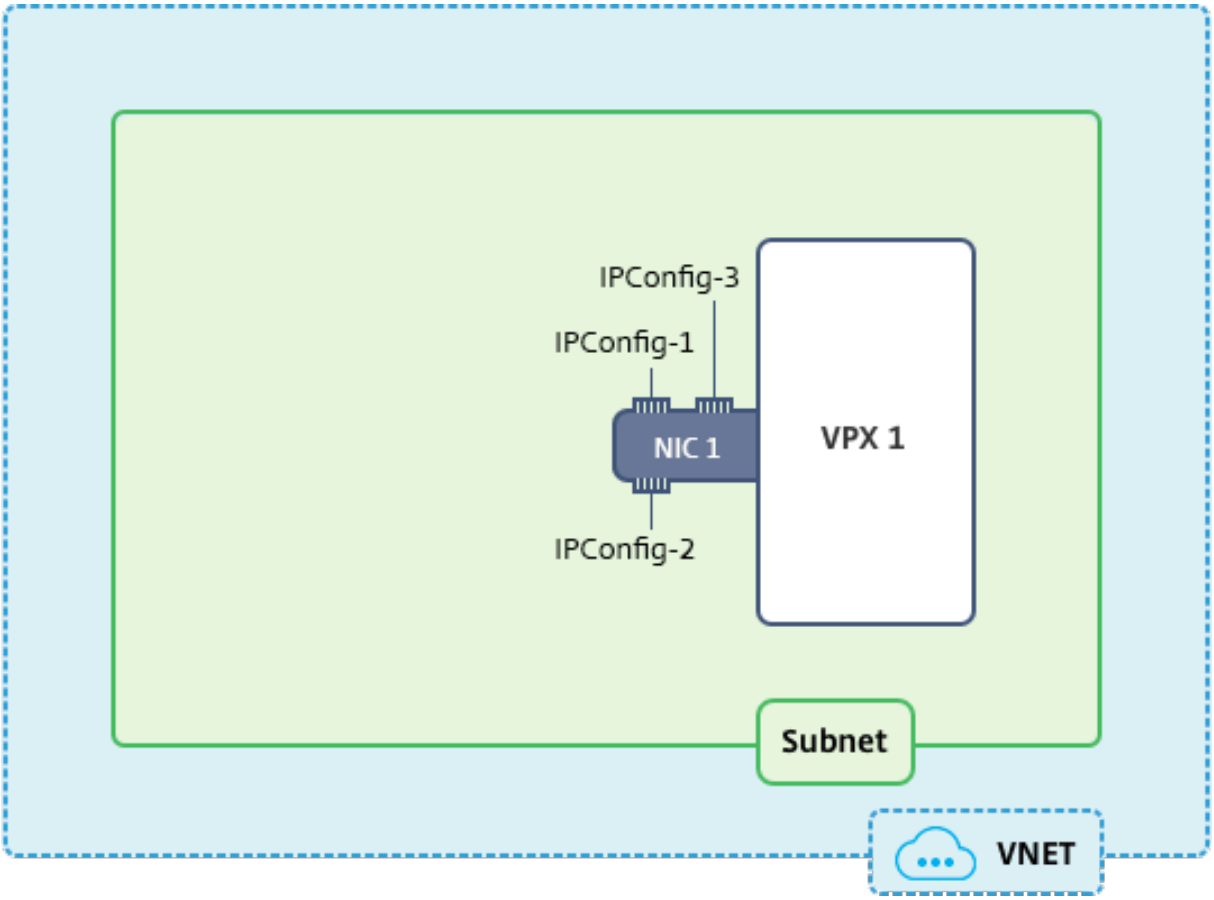
En este caso, un dispositivo Citrix ADC VPX independiente se configura con una única NIC conectada a una red virtual (VNET). La NIC está asociada a tres configuraciones IP (ipconfig), cada servidor tiene un propósito diferente, como se muestra en la tabla.

Configuración IP	Asociada con	Propósito
ipconfig1	Dirección IP pública estática; dirección IP privada estática	Sirve tráfico de administración
ipconfig2	Dirección IP pública estática; dirección privada estática	Sirve tráfico del lado del cliente
ipconfig3	Dirección IP privada estática	Se comunica con servidores back-end

> **Nota**
>
> `IPConfig-3` no está asociada a ninguna dirección IP pública.

Diagrama: Topología

Aquí está la representación visual del caso de uso.



> **Nota**
>
> En una implementación Multi-NIC, Multi-IP Azure Citrix ADC VPX, la IP privada asociada a la principal (primera) `IPConfig` de la NIC principal (primera) se agrega automáticamente como NSIP de administración del dispositivo. Las restantes direcciones IP privadas asociadas `IPConfigs` deben agregarse a la instancia VPX como VIP o SNIP mediante el `add ns ip` comando, de acuerdo con sus requisitos.

Antes de comenzar

Antes de comenzar, cree una instancia VPX siguiendo los pasos que se indican en este enlace:

Configurar una instancia independiente de Citrix ADC VPX

Para este caso de uso, se crea la instancia VPX NSDOC0330VM.

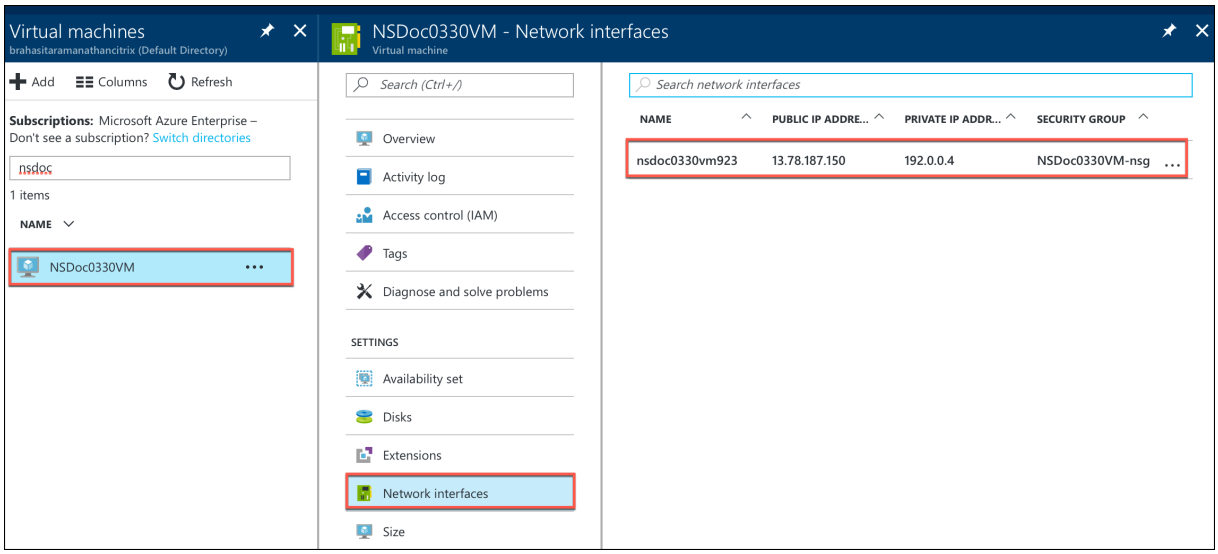
Procedimiento para configurar varias direcciones IP para una instancia de Citrix ADC VPX en modo independiente.

Para configurar varias direcciones IP para un dispositivo Citrix ADC VPX en modo independiente:

1. Agregar direcciones IP a la VM
2. Configurar direcciones IP propiedad de Citrix ADC

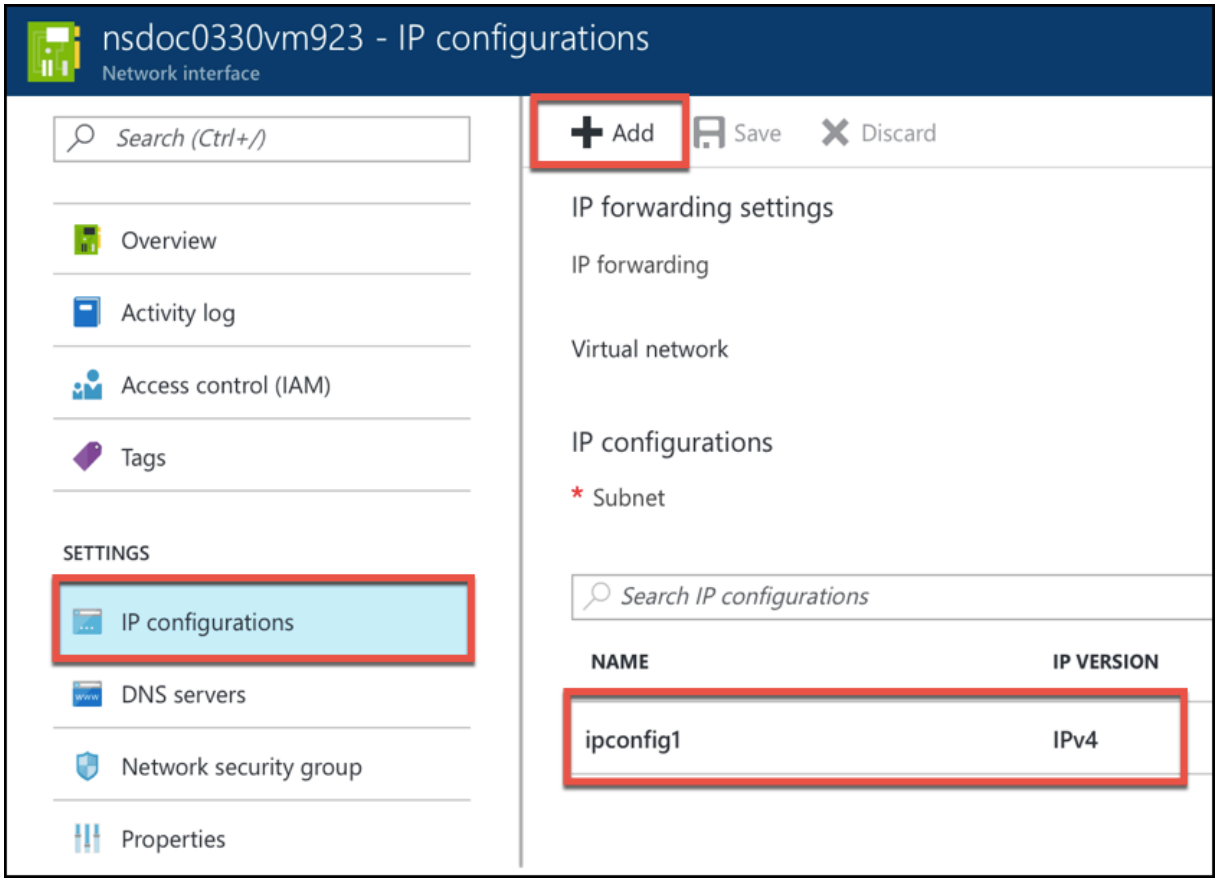
Paso 1: Agregar direcciones IP a la VM

1. En el portal, haga clic en **Más servicios > escriba máquinas virtuales** en el cuadro de filtro y, a continuación, haga clic en **Máquinas virtuales**.
2. En el blade **Máquinas virtuales**, haga clic en la máquina virtual a la que quiere agregar direcciones IP. Haga clic en **Interfaces de red** en el blade de máquina virtual que aparece y, a continuación, seleccione la interfaz de red.



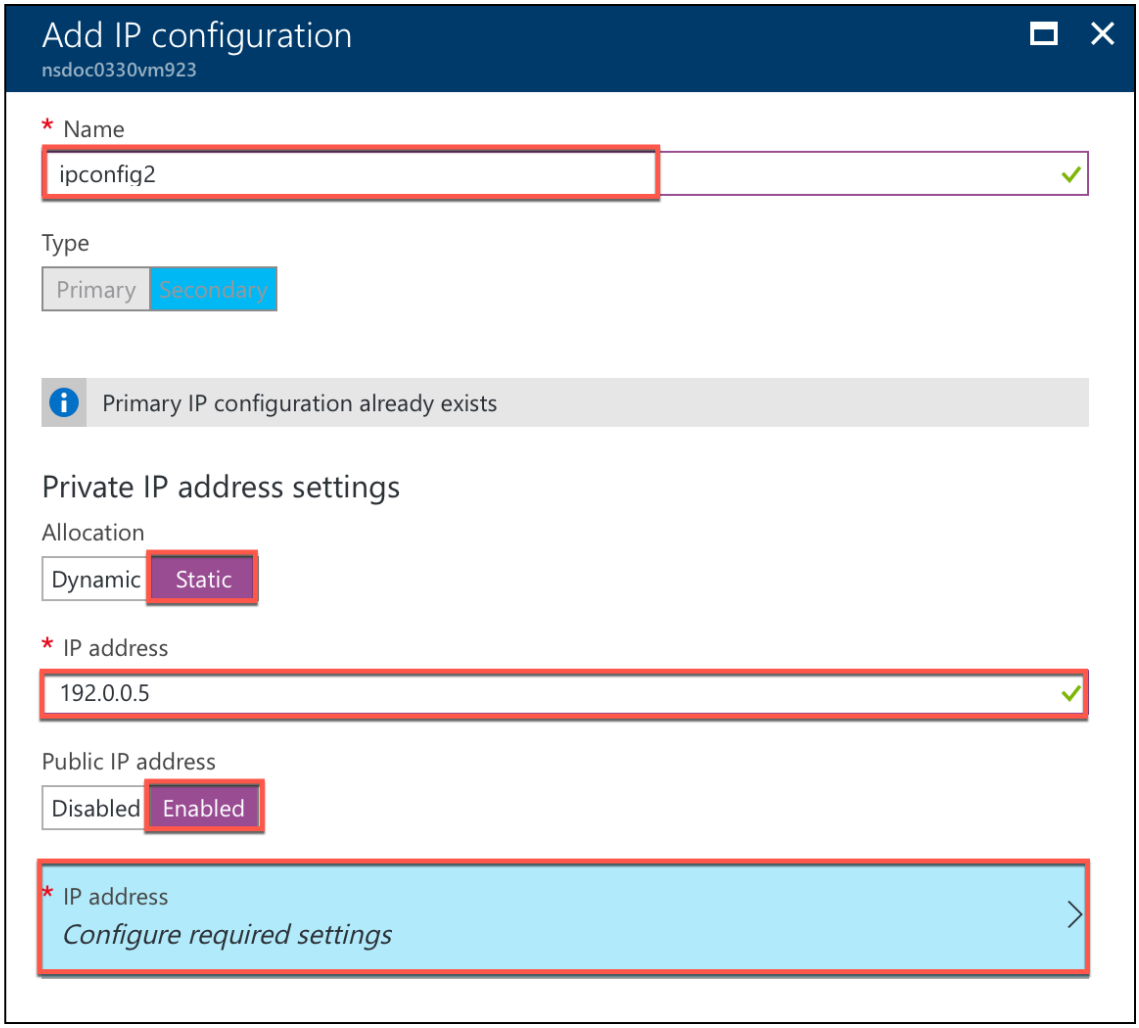
En el blade que aparece para la NIC seleccionada, haga clic en **Configuraciones IP**. Se muestra la configuración IP existente que se asignó al crear la VM, **ipconfig1**. Para este caso de uso, asegúrese de que las direcciones IP asociadas con ipconfig1 sean estáticas. A continuación, cree dos configuraciones IP más: Ipconfig2 (VIP) e ipconfig3 (SNIP).

Para crear más `ipconfigs`, crea **Agregar**.



En la ventana **Agregar configuración de IP**, introduzca un **nombre**, especifique el método de asignación como **estático**, introduzca una dirección IP (192.0.0.5 para este caso de uso) y habilite la **dirección IP pública**.

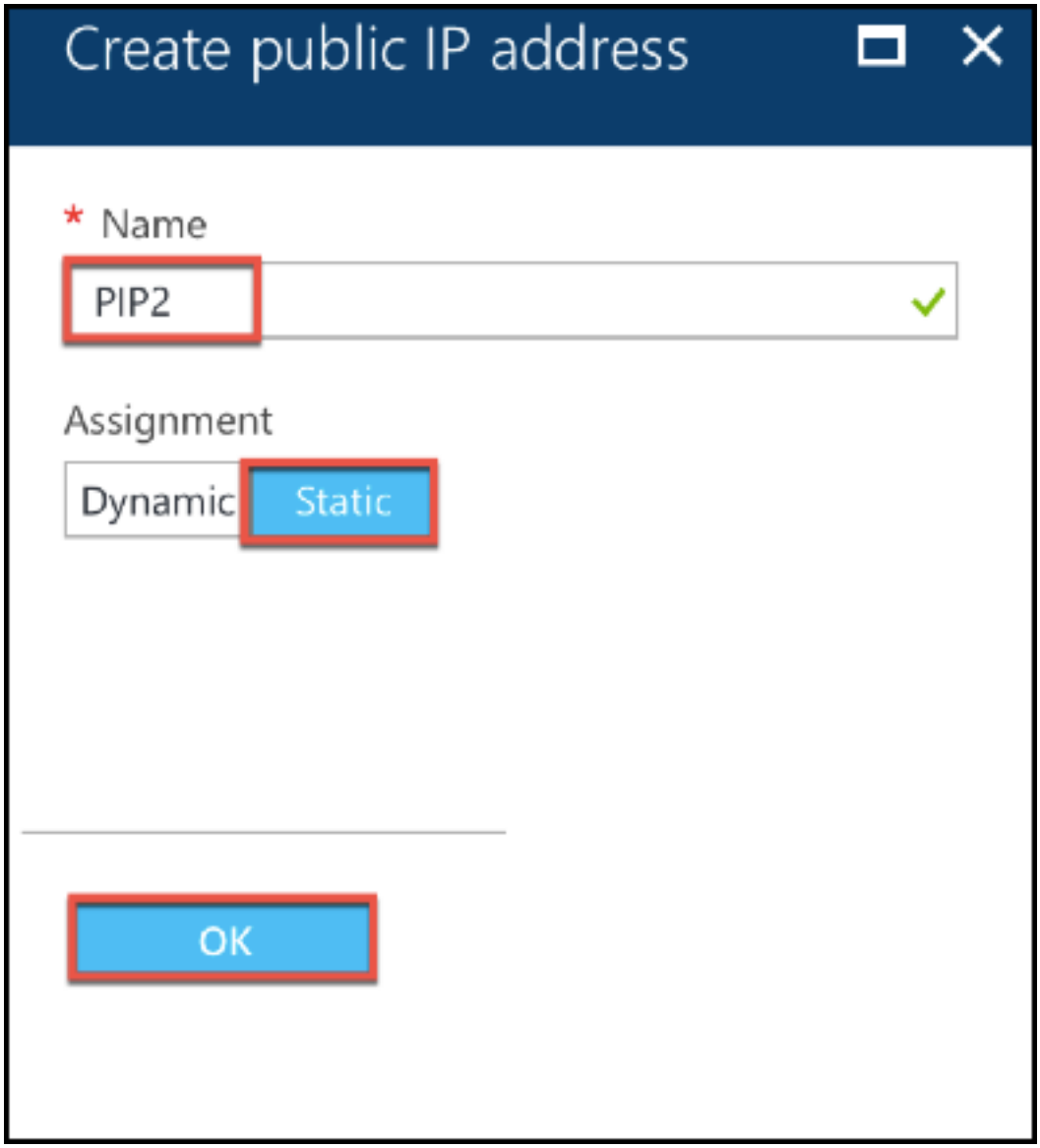
> **Nota**
>
> Antes de agregar una dirección IP privada estática, compruebe la disponibilidad de la dirección IP y asegúrese de que la dirección IP pertenece a la misma subred a la que está conectada la NIC.



A continuación, haga clic en **Configurar los ajustes necesarios** para crear una dirección IP pública estática para ipconfig2.

De forma predeterminada, las direcciones IP públicas son dinámicas. Para asegurarse de que la máquina virtual siempre utiliza la misma dirección IP pública, cree una IP pública estática.

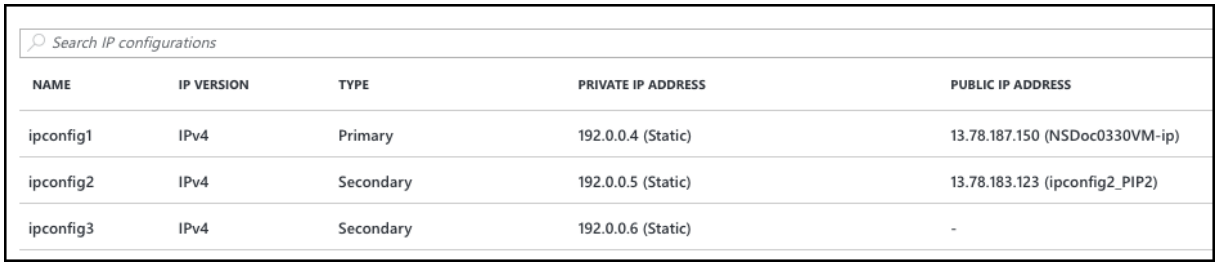
En el blade Crear dirección IP pública, agregue un nombre y, en Asignación, haga clic en **Estático**. Y, a continuación, haga clic en **Aceptar**.



Nota

Incluso cuando establezca el método de asignación en estático, no puede especificar la dirección IP real asignada al recurso IP público. En su lugar, se asigna desde un grupo de direcciones IP disponibles en la ubicación de Azure en la que se crea el recurso.

Siga los pasos para agregar una configuración IP más para ipconfig3. La IP pública no es obligatoria.



Paso 2: Configurar direcciones IP propiedad de Citrix ADC

Configure las direcciones IP propiedad de Citrix ADC mediante la GUI o el comando `add ns ip`. Para obtener más información, consulte Configuración de direcciones IP propiedad de Citrix ADC.

Configurar una configuración de alta disponibilidad con varias direcciones IP y NIC

August 20, 2021

En una implementación de Microsoft Azure, se logra una configuración de alta disponibilidad de dos instancias de Citrix ADC VPX mediante Azure Load Balancer (ALB). Esto se consigue configurando un sondeo de estado en ALB, que monitorea cada instancia VPX enviando un sondeo de estado cada 5 segundos a instancias primarias y secundarias.

En esta configuración, solo el nodo principal responde a los sondeos de estado y el secundario no. Una vez que el primario envía la respuesta al sondeo de estado, el ALB comienza a enviar el tráfico de datos a la instancia. Si la instancia principal pierde dos sondeos de mantenimiento consecutivos, ALB no redirige el tráfico a esa instancia. En caso de conmutación por error, el nuevo primario comienza a responder a los sondeos de mantenimiento y el ALB redirige el tráfico hacia él. El tiempo de conmutación por error de alta disponibilidad VPX estándar es de tres segundos. El tiempo total de conmutación por error que puede tardar en cambiar el tráfico puede ser de un máximo de 13 segundos.

Puede implementar un par de instancias de Citrix ADC VPX con varias NIC en una configuración de alta disponibilidad (HA) activo-pasiva en Azure. Cada NIC puede contener varias direcciones IP.

Las siguientes opciones están disponibles para una implementación de alta disponibilidad de varias NIC:

- Alta disponibilidad con el conjunto de disponibilidad de Azure
- Alta disponibilidad mediante zonas de disponibilidad de Azure

Para obtener más información sobre Azure Availability Set y zonas de disponibilidad, consulte la documentación de Azure Administrar la disponibilidad de máquinas virtuales Linux.

Alta disponibilidad mediante el conjunto de disponibilidad

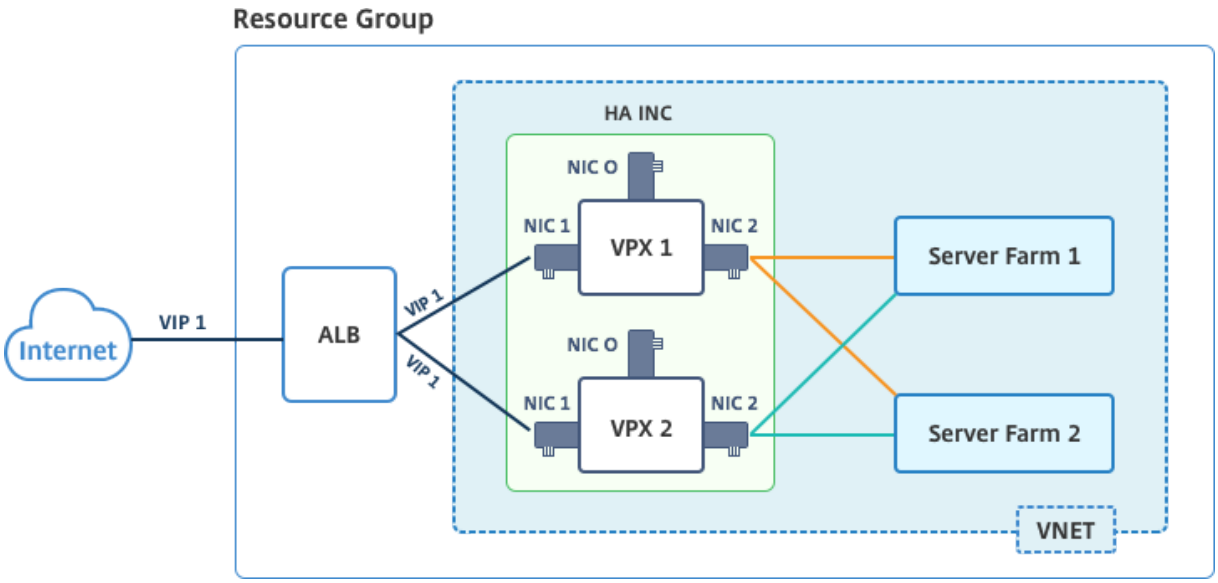
Una configuración de alta disponibilidad que utilice un conjunto de disponibilidad debe cumplir los siguientes requisitos:

- Configuración de red independiente de HA (INC)
- El equilibrador de carga de Azure (ALB) en modo de devolución directa del servidor (DSR)

Todo el tráfico pasa por el nodo principal. El nodo secundario permanece en modo de espera hasta que falla el nodo principal.

> **Nota**
>
> Para que funcione una implementación de alta disponibilidad de Citrix VPX en la nube de Azure, necesita una IP pública flotante (PIP) que se pueda mover entre los dos nodos VPX. Azure Load Balancer (ALB) proporciona ese PIP flotante, que se mueve automáticamente al segundo nodo en caso de una conmutación por error.

Diagrama: Ejemplo de una arquitectura de implementación de alta disponibilidad, con el conjunto de disponibilidad de Azure



En una implementación activo-pasiva, las direcciones IP públicas (PIP) front-end de ALB se añaden como direcciones VIP en cada nodo VPX. En la configuración HA-INC, las direcciones VIP son flotantes y las direcciones SNIP son específicas de la instancia.

Puede implementar un par VPX en modo de alta disponibilidad activo-pasivo de dos maneras mediante:

- **Plantilla de alta disponibilidad estándar de Citrix ADC VPX**: Utilice esta opción para configurar un par de alta disponibilidad con la opción predeterminada de tres subredes y seis NIC.
- **Comandos de Windows PowerShell**: Utilice esta opción para configurar un par de HA de acuerdo con los requisitos de la subred y NIC.

En este tema se describe cómo implementar un par VPX en la configuración de HA activo-pasiva mediante la plantilla de Citrix. Si desea utilizar comandos de PowerShell, consulte Configuración de una configuración de alta disponibilidad con varias direcciones IP y NIC mediante comandos de PowerShell.

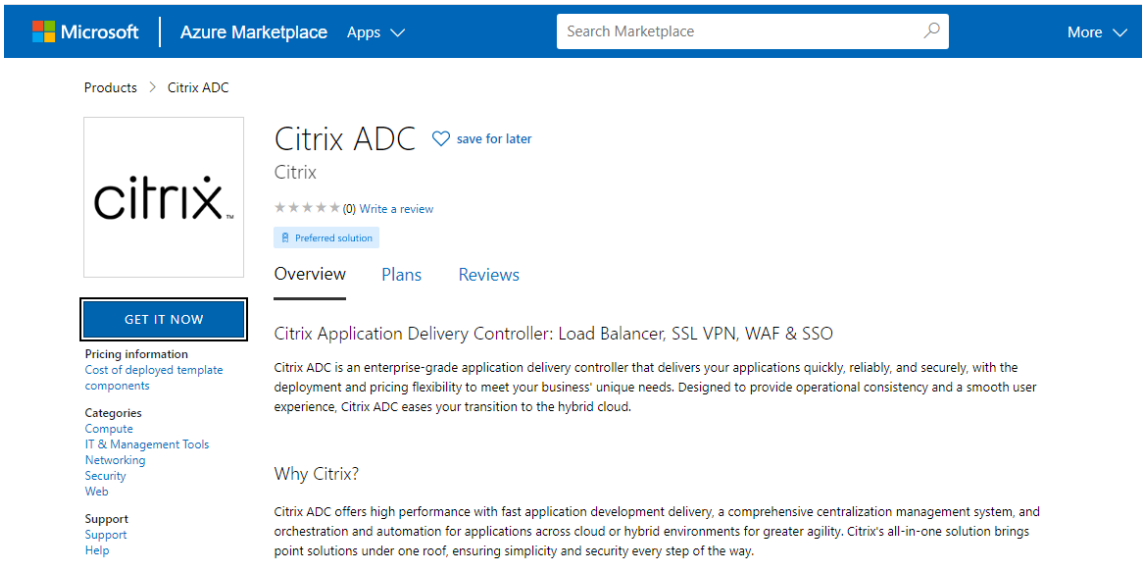
Configurar nodos HA-INC mediante la plantilla de alta disponibilidad de Citrix

Puede implementar de forma rápida y eficiente un par de instancias VPX en modo HA-INC mediante la plantilla estándar. La plantilla crea dos nodos, con tres subredes y seis NIC. Las subredes son para la administración, el cliente y el tráfico del lado del servidor, y cada subred tiene dos NIC para ambas instancias VPX.

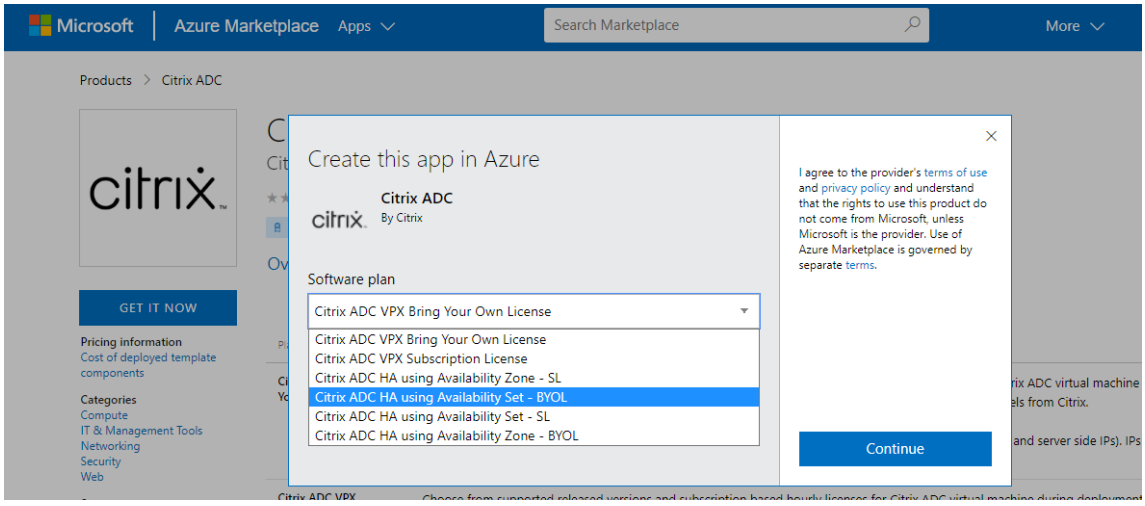
Puede obtener la plantilla Citrix ADC HA Pair en Azure Marketplace.

Complete los siguientes pasos para lanzar la plantilla e implementar un par VPX de alta disponibilidad mediante conjuntos de disponibilidad de Azure.

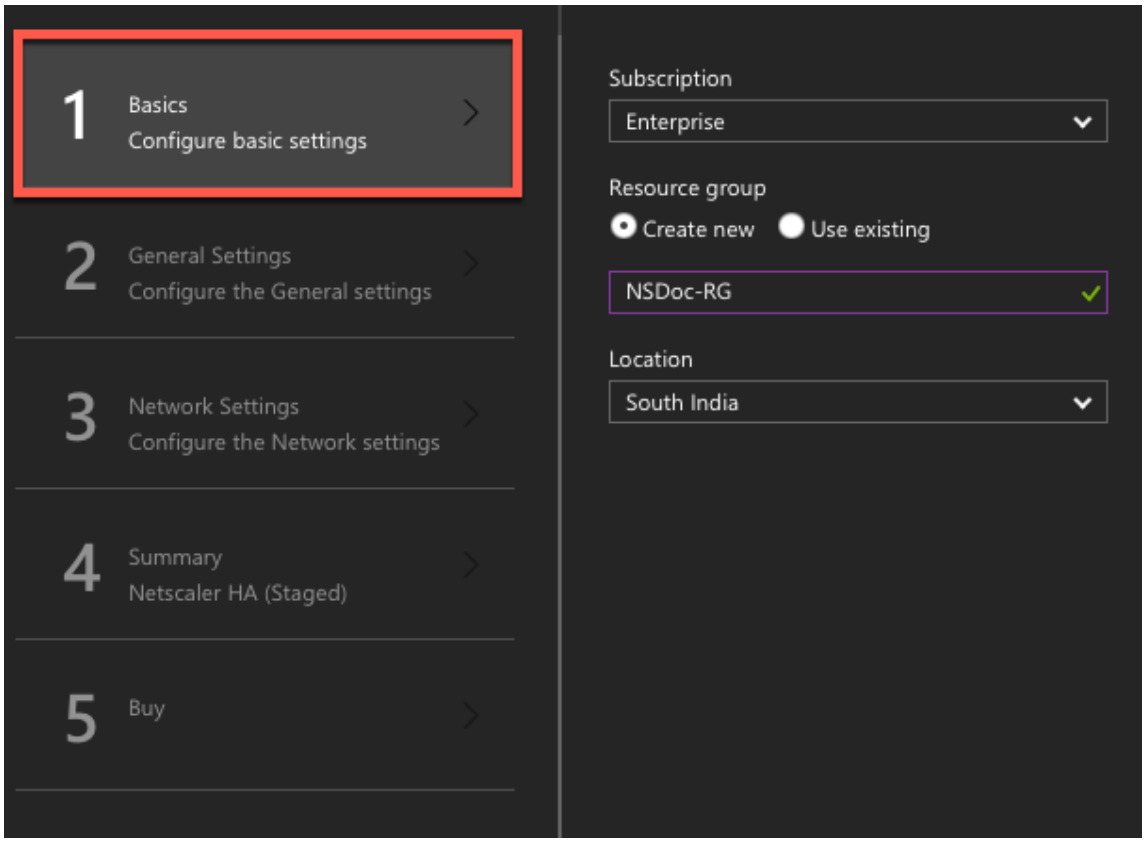
1. En Azure Marketplace, busque **Citrix ADC**.



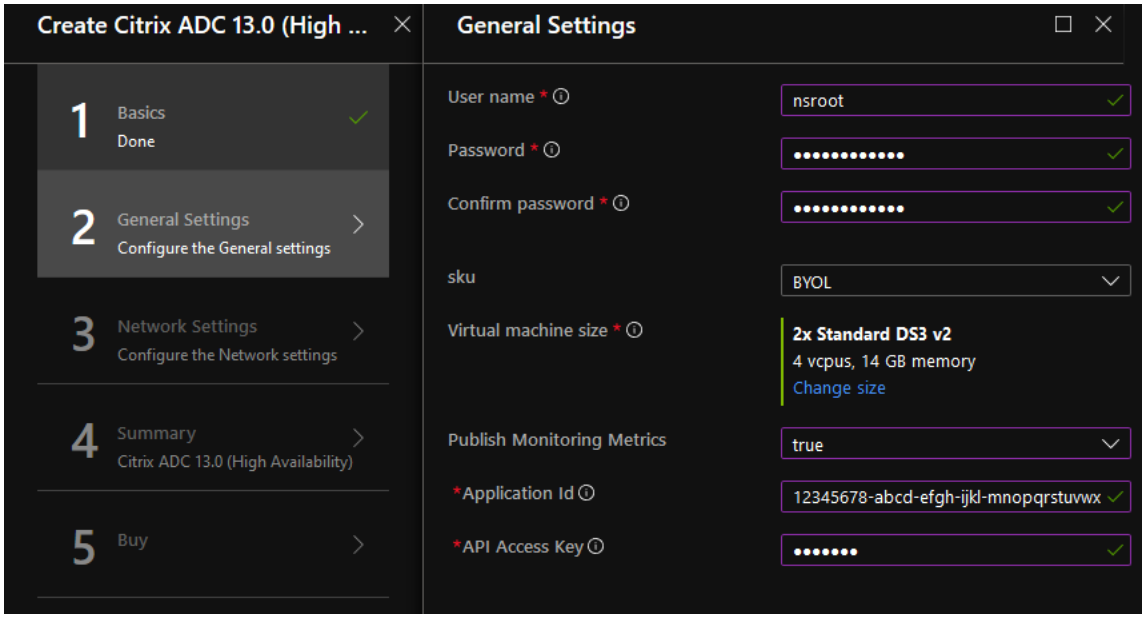
2. Haga clic en **OBTENER AHORA**.
3. Seleccione la implementación de alta disponibilidad requerida junto con la licencia y haga clic en **Continuar**.



4. Aparecerá la página **Básicos**. Cree un grupo de recursos y seleccione **Aceptar**.



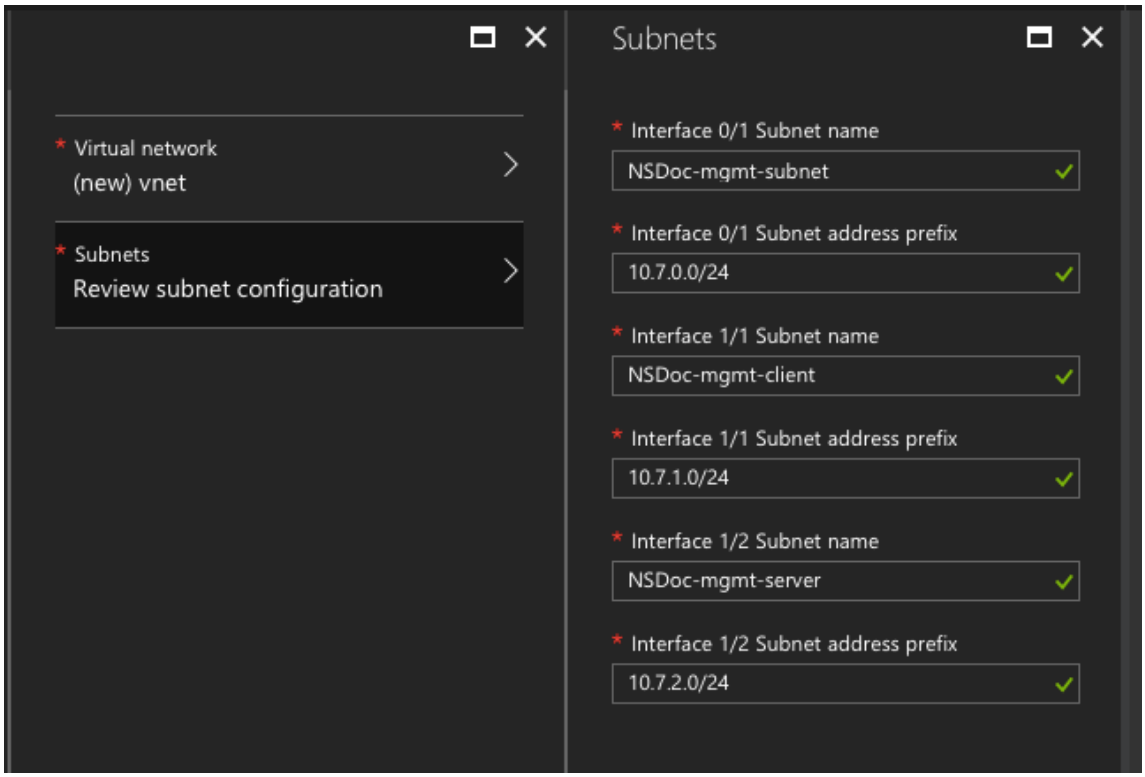
5. Aparecerá la página **Configuración general**. Escriba los detalles y seleccione **Aceptar**.



> Nota:
>
> De forma predeterminada, la opción **Métricas de supervisión de publicación** está estable-

> cida en **false**. Si quiere habilitar esta opción, seleccione **true**.
> Cree una aplicación de Azure Active Directory (ADD) y una entidad de servicio que pueda tener acceso a los recursos. Asigne el rol colaborador a la aplicación AAD recién creada. Para obtener más información, consulte Uso del portal para crear una aplicación y un principal de servicio de Azure Active Directory que pueda acceder a los recursos.

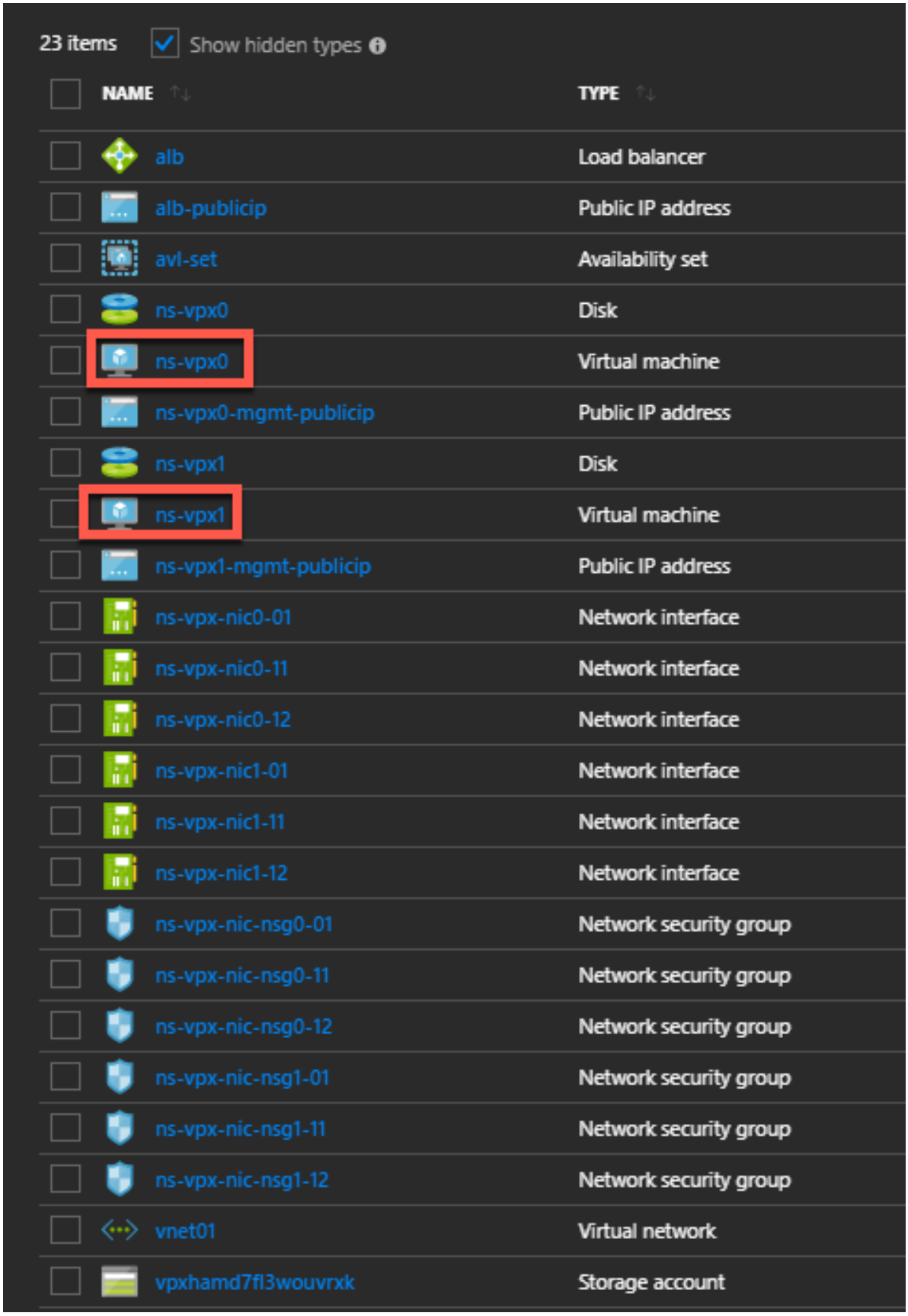
6. Aparecerá la página **Configuración de red**. Compruebe las configuraciones de VNet y subred, modifique la configuración requerida y seleccione **Aceptar**.



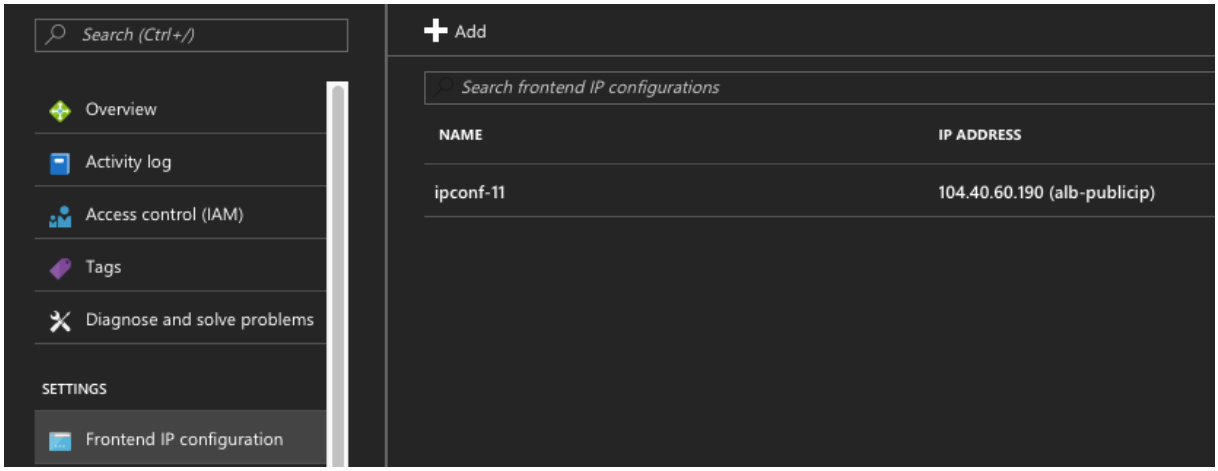
7. Aparecerá la página **Resumen**. Revise la configuración y modifique en consecuencia. Seleccione **Aceptar** para confirmar.
8. Aparecerá la página **Comprar**. Seleccione **Comprar** para completar la implementación.

El grupo de recursos de Azure puede tardar un momento en crearse con las configuraciones requeridas. Una vez finalizado, seleccione el **grupo de recursos** en el portal de Azure para ver los detalles de configuración, como reglas de LB, grupos de back-end, sondeos de estado. El par de alta disponibilidad aparece como ns-vpx0 y ns-vpx1.

Si se requieren más modificaciones para la configuración de HA, como la creación de más reglas de seguridad y puertos, puede hacerlo desde el portal de Azure.



A continuación, debe configurar el servidor virtual de equilibrio de carga con la **dirección IP pública (PIP) del Frontend de ALB**, en el nodo principal. Para buscar el PIP de ALB, seleccione ALB > **Configuración IP de frontend**.



Consulte la sección **Recursos** para obtener más información acerca de cómo configurar el servidor virtual de equilibrio de carga.

Recursos:

Los siguientes vínculos proporcionan información adicional relacionada con la implementación de HA y la configuración del servidor virtual:

- Configuración de nodos de alta disponibilidad en diferentes subredes
- Configurar el equilibrio de carga básico

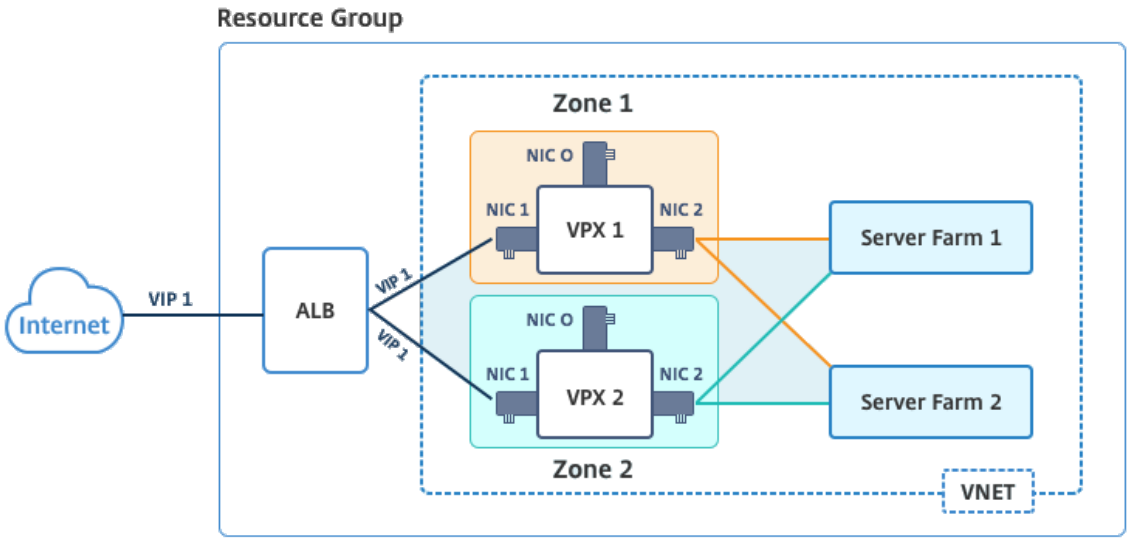
Recursos relacionados:

- Configurar una configuración de alta disponibilidad con varias direcciones IP y NIC mediante comandos de PowerShell
- Configuración de GSLB en la implementación de HA activa en espera en Azure

Alta disponibilidad mediante zonas de disponibilidad

Las zonas de disponibilidad de Azure son ubicaciones aisladas por errores dentro de una región de Azure, que proporcionan alimentación redundante, refrigeración y redes y aumentan la resiliencia. Solo las regiones específicas de Azure admiten zonas de disponibilidad. Para obtener más información, consulte la documentación de Azure [Qué son las zonas de disponibilidad en Azure.

Diagrama: Ejemplo de una arquitectura de implementación de alta disponibilidad, con zonas de disponibilidad de Azure



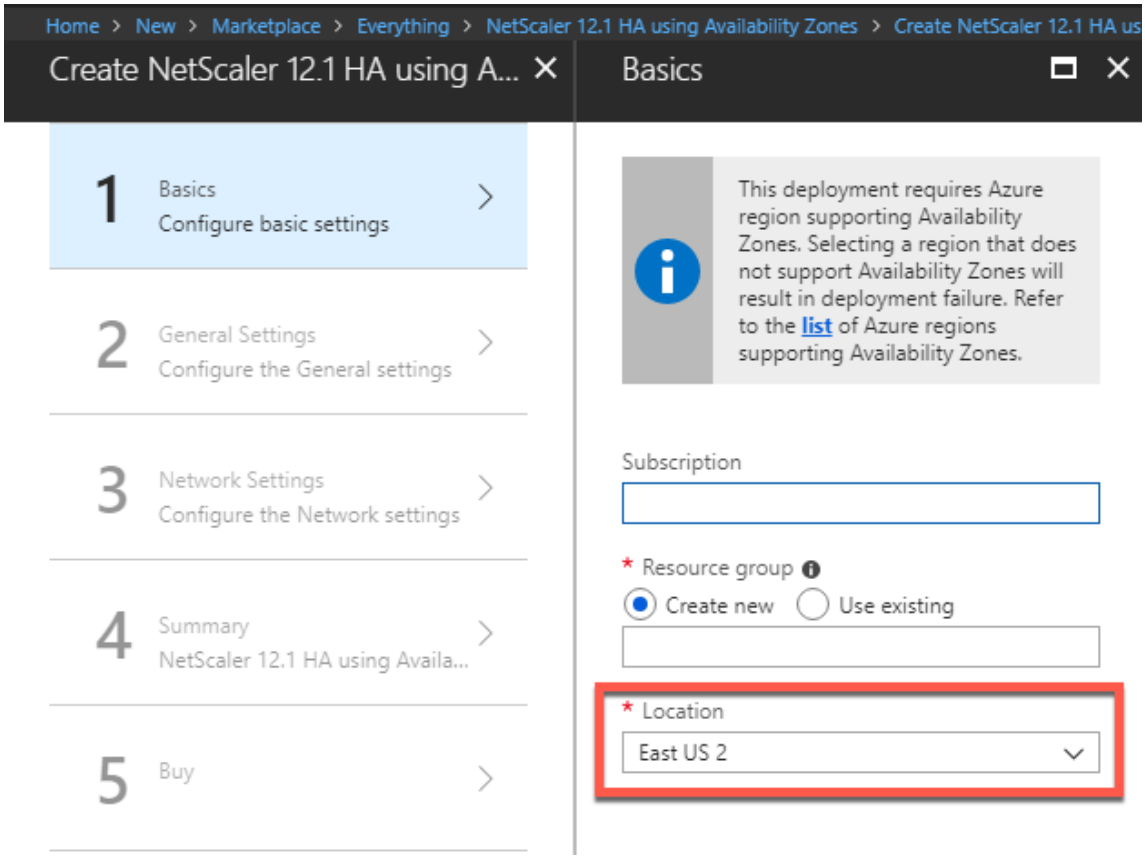
Puede implementar un par VPX en modo de alta disponibilidad mediante la plantilla denominada "NetScaler 13.0 HA mediante las zonas de disponibilidad", disponible en Azure Marketplace.

Complete los siguientes pasos para iniciar la plantilla e implementar un par VPX de alta disponibilidad mediante las zonas de disponibilidad de Azure.

1. En Azure Marketplace, seleccione e inicie la plantilla de solución Citrix.

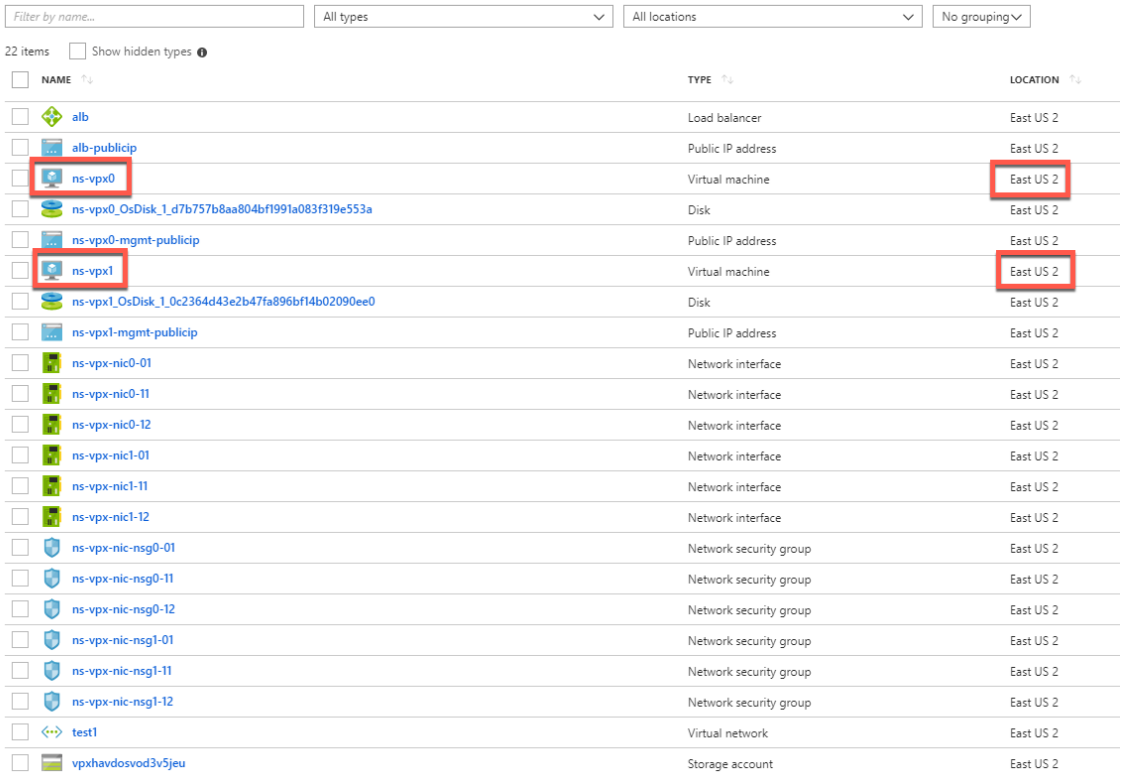
2. Asegúrese de que el tipo de implementación sea Administrador de recursos y seleccione **Crear**.
3. Aparecerá la página **Básicos**. Introduzca los detalles y haga clic en **Aceptar**.

> Nota: Asegúrese de seleccionar una región de Azure que admita zonas de disponibilidad. Para obtener más información sobre las regiones que admiten zonas de disponibilidad, consulte la documentación de Azure ¿Qué son las zonas de disponibilidad de Azure?



4. Aparecerá la página **Configuración general**. Escriba los detalles y seleccione **Aceptar**.
5. Aparecerá la página **Configuración de red**. Compruebe las configuraciones de VNet y subred, modifique la configuración requerida y seleccione **Aceptar**.
6. Aparecerá la página **Resumen**. Revise la configuración y modifique en consecuencia. Seleccione **Aceptar** para confirmar.
7. Aparecerá la página **Comprar**. Seleccione **Comprar** para completar la implementación.

   El grupo de recursos de Azure puede tardar un momento en crearse con las configuraciones requeridas. Después de finalizar, seleccione el **grupo de recursos** para ver los detalles de configuración, como reglas LB, grupos de back-end, sondeos de estado, etc., en el portal de Azure. El par de alta disponibilidad aparece como ns-vpx0 y ns-vpx1. Además, puede ver la ubicación en la columna **Ubicación**.



NAME	TYPE	LOCATION
alb	Load balancer	East US 2
alb-publicip	Public IP address	East US 2
ns-vpx0	Virtual machine	East US 2
ns-vpx0_OsDisk_1_d7b757b8aa804bf1991a083f319e553a	Disk	East US 2
ns-vpx0-mgmt-publicip	Public IP address	East US 2
ns-vpx1	Virtual machine	East US 2
ns-vpx1_OsDisk_1_0c2364d43e2b47fa896bf14b02090ee0	Disk	East US 2
ns-vpx1-mgmt-publicip	Public IP address	East US 2
ns-vpx-nic0-01	Network interface	East US 2
ns-vpx-nic0-11	Network interface	East US 2
ns-vpx-nic0-12	Network interface	East US 2
ns-vpx-nic1-01	Network interface	East US 2
ns-vpx-nic1-11	Network interface	East US 2
ns-vpx-nic1-12	Network interface	East US 2
ns-vpx-nic-nsg0-01	Network security group	East US 2
ns-vpx-nic-nsg0-11	Network security group	East US 2
ns-vpx-nic-nsg0-12	Network security group	East US 2
ns-vpx-nic-nsg1-01	Network security group	East US 2
ns-vpx-nic-nsg1-11	Network security group	East US 2
ns-vpx-nic-nsg1-12	Network security group	East US 2
test1	Virtual network	East US 2
vpxhavdosvod3v5jeu	Storage account	East US 2

Si se requieren más modificaciones para la configuración de HA, como la creación de más reglas de seguridad y puertos, puede hacerlo desde el portal de Azure.

Supervisar las instancias mediante métricas en el monitor de Azure

Puede utilizar métricas en la plataforma de datos de monitor de Azure para supervisar un conjunto de recursos Citrix ADC VPX, como CPU, utilización de memoria y rendimiento. El servicio de métricas supervisa los recursos de Citrix ADC VPX que se ejecutan en Azure, en tiempo real. Puede utilizar el **Explorador de métricas** para acceder a los datos recopilados. Para obtener más información, consulte Descripción general de las métricas de Azure Monitor.

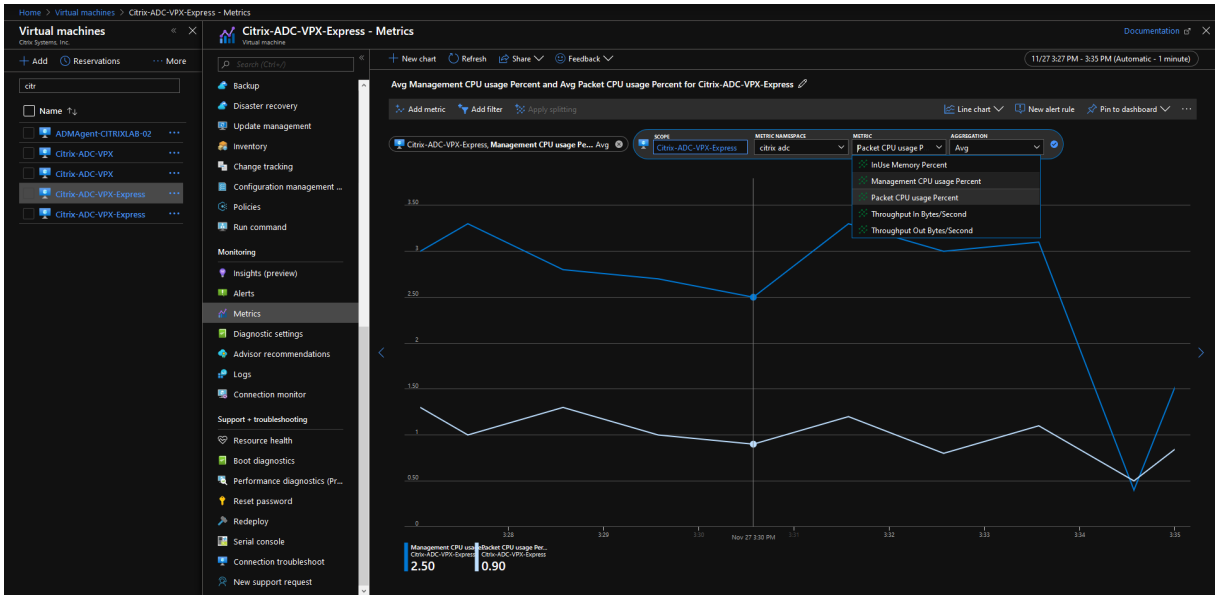
Puntos a tener en cuenta

- Si implementa una instancia de Citrix ADC VPX en Azure mediante la oferta de Azure Marketplace, el servicio Métricas está inhabilitado de forma predeterminada.
- El servicio Métricas no es compatible con la CLI de Azure.
- Las métricas están disponibles para CPU (administración y uso de CPU de paquetes), memoria y rendimiento (entrante y saliente).

Cómo ver métricas en el monitor de Azure

Para ver las métricas en el monitor de Azure de la instancia, lleve a cabo estos pasos:

1. Inicie sesión en **Azure Portal > Máquinas virtuales**.
2. Seleccione la máquina virtual que es el nodo principal.
3. En la sección **Supervisión**, haga clic en **Métricas**.
4. En el menú desplegable Espacio de **nombres métrico**, haga clic en **Citrix ADC**.
5. En el menú desplegable **Todas las métricas** del menú desplegable **Métricas**, haga clic en las métricas que quiera ver.
6. Haga clic en **Agregar métrica** para ver otra métrica en el mismo gráfico. Utilice las opciones Gráfico para personalizar el gráfico.



Configurar una configuración de alta disponibilidad con varias direcciones IP y NIC mediante comandos de PowerShell

August 20, 2021

Puede implementar un par de instancias de Citrix ADC VPX con varias NIC en una configuración de alta disponibilidad (HA) activo-pasiva en Azure. Cada NIC puede contener varias direcciones IP.

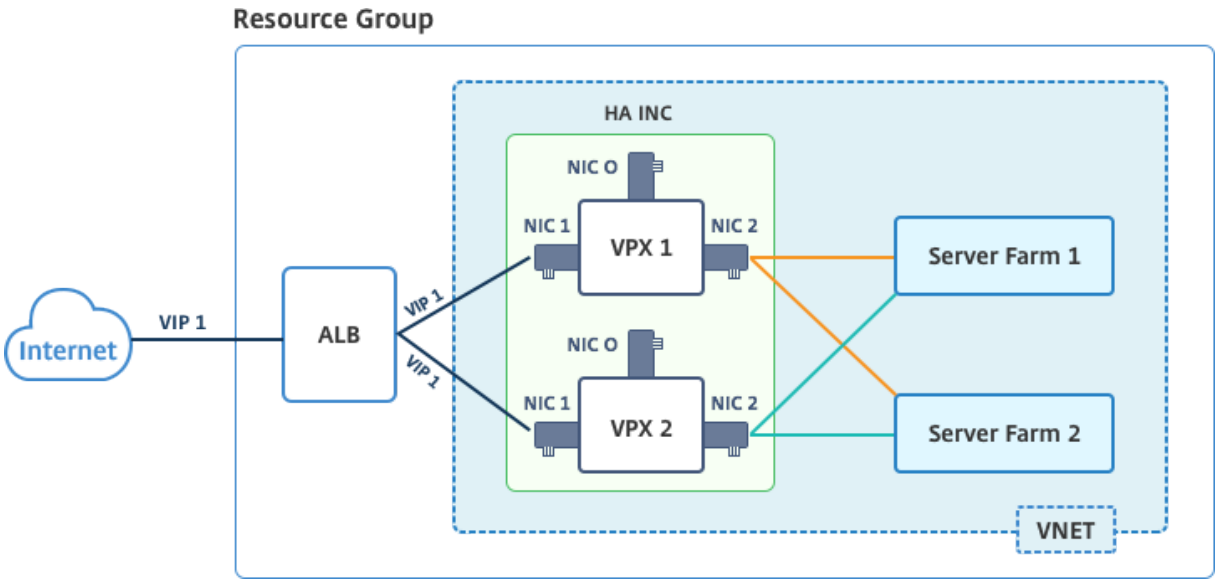
Una implementación activo-pasiva requiere:

- Configuración de red independiente de HA (INC)
- El equilibrador de carga de Azure (ALB) en modo de devolución directa del servidor (DSR)

Todo el tráfico pasa por el nodo principal. El nodo secundario permanece en modo de espera hasta que falla el nodo principal.

> **Nota**
>
> Para que funcione una implementación de alta disponibilidad de Citrix ADC VPX en una nube de Azure, necesita una IP pública flotante (PIP) que se pueda mover entre los dos nodos de alta disponibilidad. Azure Load Balancer (ALB) proporciona ese PIP flotante, que se mueve automáticamente al segundo nodo en caso de una conmutación por error.

Diagrama: Ejemplo de una arquitectura de implementación activo-pasiva



En una implementación activo-pasiva, las direcciones IP públicas flotantes (PIP) ALB se agregan como direcciones VIP en cada nodo VPX. En la configuración HA-INC, las direcciones VIP son flotantes y las direcciones SNIP son específicas de la instancia.

ALB supervisa cada instancia VPX enviando una sonda de estado cada 5 segundos y redirige el tráfico a esa instancia solo que envía la respuesta de los sondeos de estado en intervalos regulares. Por lo tanto, en una configuración de HA, el nodo primario responde a sondeos de estado y secundario no. Si las instancias principales pierden dos sondeos de estado consecutivos, ALB no redirige el tráfico a esa instancia. En caso de conmutación por error, el nuevo primario comienza a responder a los sondeos de mantenimiento y el ALB redirige el tráfico hacia él. El tiempo de conmutación por error de alta disponibilidad VPX estándar es de tres segundos. El tiempo total de conmutación por error que puede tardar en el cambio de tráfico puede ser de 13 segundos como máximo.

Puede implementar un par VPX en la configuración de HA activa-pasiva de dos maneras mediante:

- **Plantilla de alta disponibilidad estándar de Citrix ADC VPX**: Utilice esta opción para configurar un par de alta disponibilidad con la opción predeterminada de tres subredes y seis NIC.
- **Comandos de Windows PowerShell**: Utilice esta opción para configurar un par de HA de acuerdo con los requisitos de la subred y NIC.

En este tema se describe cómo implementar un par VPX en la instalación de HA activo-pasiva me-

diante comandos de PowerShell. Si desea utilizar la plantilla Citrix ADC VPX Standard HA, consulte Configuración de una configuración de alta disponibilidad con varias direcciones IP y NIC.

Configuración de nodos HA-INC mediante comandos de PowerShell

Caso: Implementación de PowerShell de HA-INC

En este caso, se implementa un par de Citrix ADC VPX mediante la topología indicada en la tabla. Cada instancia VPX contiene tres NIC, cada NIC se implementa en una subred diferente. A cada NIC se le asigna una configuración IP.

ALB	VPX1	VPX2
ALB está asociado con IP pública 3 (pip3)	La IP de administración se configura con IPConfig1, que incluye una IP pública (pip1) y una IP privada (12.5.2.24); nic1; Mgmtsubnet=12.5.2.0/24	La IP de administración se configura con IPConfig5, que incluye una IP pública (pip3) y una IP privada (12.5.2.26); nic4; Mgmtsubnet=12.5.2.0/24
Las reglas LB y el puerto configurados son HTTP (80), SSL (443), sonda de estado (9000)	La IP del lado del cliente está configurada con IPConfig3, que incluye una IP privada (12.5.1.27); nic2; FrontenDSubet=12.5.1.0/24	La IP del lado del cliente está configurada con IPConfig7, que incluye una IP privada (12.5.1.28); nic5; FrontenDSubet=12.5.1.0/24
-	La IP del lado del servidor está configurada con IPConfig4, que incluye una IP privada (12.5.3.24); nic3; backendSubnet=12.5.3.0/24	La IP del lado del servidor está configurada con IPConfig8, que incluye una IP privada (12.5.3.28); nic6; backendSubnet=12.5.3.0/24
-	Las reglas y puertos para NSG son SSH (22), HTTP (80), HTTPS (443)	-

Configuración de parámetros

En este caso se utilizan los parámetros siguientes.

$locName= “South east Asia”

$rgName = “MulitIP-MultiNIC-RG”

$nicName1= “VM1-NIC1”

$nicName2 = “VM1-NIC2”

$nicName3= “VM1-NIC3”

$nicName4 = “VM2-NIC1”

$nicName5= “VM2-NIC2”

$nicName6 = “VM2-NIC3”

$vNetName = “Azure-MultiIP-ALB-vnet”

$vNetAddressRange= “12.5.0.0/16”

$frontEndSubnetName= “frontEndSubnet”

$frontEndSubnetRange= “12.5.1.0/24”

$mgmtSubnetName= “mgmtSubnet”

$mgmtSubnetRange= “12.5.2.0/24”

$backEndSubnetName = “backEndSubnet”

$backEndSubnetRange = “12.5.3.0/24”

$prmStorageAccountName = “multiipmultinicbstorage”

$avSetName = “multiple-avSet”

$vmSize= “Standard_DS4_V2”

$editor = “Citrix”

$offer = “netscalervpx-120”

$sku = “netscalerbyol”

$version=”latest”

$pubIPName1=”VPX1MGMT”

$pubIPName2=”VPX2MGMT”

$pubIPName3=”ALBPIP”

$domName1=”vpx1dns”

$domName2=”vpx2dns”

$domName3=”vpxalbdns”

$vmNamePrefix=”VPXMultiIPALB”

$osDiskSuffix1=”osmultiipalbdiskdb1”

$osDiskSuffix2=”osmultiipalbdiskdb2”

$lbName= “MultiIPALB”

$frontEndConfigName1= “FrontEndIP”

$backendPoolName1= “BackendPoolHttp”

$lbRuleName1= “LBRuleHttp”

$healthProbeName= “HealthProbe”

$nsgName=”NSG-MultiIP-ALB”

$rule1Name=”Inbound-HTTP”

$rule2Name=”Inbound-HTTPS”

$rule3Name=”Inbound-SSH”

Para completar la implementación, complete los pasos siguientes mediante comandos de PowerShell:

1. Crear un grupo de recursos, una cuenta de almacenamiento y un conjunto de disponibilidad
2. Crear un grupo de seguridad de red y agregar reglas
3. Crear una red virtual y tres subredes
4. Crear direcciones IP públicas
5. Crear configuraciones IP para VPX1
6. Crear configuraciones IP para VPX2
7. Crear NIC para VPX1
8. Crear NIC para VPX2
9. Crear VPX1
10. Crear VPX2
11. Crear ALB

Cree un grupo de recursos, una cuenta de almacenamiento y un conjunto de disponibilidad.

```
New-AzureRmResourceGroup -Name $rgName -Location $locName


$prmStorageAccount=New-AzureRMStorageAccount -Name
    $prmStorageAccountName -ResourceGroupName $rgName -Type Standard_LRS
     -Location $locName


$avSet=New-AzureRMAvailabilitySet -Name $avSetName -ResourceGroupName
    $rgName -Location $locName
```

Cree un grupo de seguridad de red y agregue reglas.


```
$rule1 = New-AzureRmNetworkSecurityRuleConfig -Name $rule1Name -
    Description ”Allow HTTP” -Access Allow -Protocol Tcp -Direction
    Inbound -Priority 101


-SourceAddressPrefix Internet -SourcePortRange * -
    DestinationAddressPrefix * -DestinationPortRange 80


$rule2 = New-AzureRmNetworkSecurityRuleConfig -Name $rule2Name -
    Description ”Allow HTTPS” -Access Allow -Protocol Tcp -Direction
    Inbound -Priority 110


-SourceAddressPrefix Internet -SourcePortRange * -
    DestinationAddressPrefix * -DestinationPortRange 443


$rule3 = New-AzureRmNetworkSecurityRuleConfig -Name $rule3Name -
    Description ”Allow SSH” -Access Allow -Protocol Tcp -Direction
    Inbound -Priority 120


-SourceAddressPrefix Internet -SourcePortRange * -
    DestinationAddressPrefix * -DestinationPortRange 22


$nsg = New-AzureRmNetworkSecurityGroup -ResourceGroupName $rgName -
    Location $locName -Name $nsgName -SecurityRules $rule1,$rule2,$rule3
```

Cree una red virtual y tres subredes.

```
$frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
    $frontEndSubnetName -AddressPrefix $frontEndSubnetRange (this
    parameter value should be as per your requirement)


$mgmtSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name $mgmtSubnetName
     -AddressPrefix $mgmtSubnetRange


$backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
```



```
    $backEndSubnetName -AddressPrefix $backEndSubnetRange
8
9
10 $vnet =New-AzureRmVirtualNetwork -Name $vNetName -ResourceGroupName
    $rgName -Location $locName -AddressPrefix $vNetAddressRange -Subnet
    $frontendSubnet,$backendSubnet, $mgmtSubnet
11
12
13 $subnetName =”frontEndSubnet”
14
15
16 $subnet1=$vnet.Subnets|?{
17  $_.Name -eq $subnetName }
18
19
20
21 $subnetName=”backEndSubnet”
22
23
24 $subnet2=$vnet.Subnets|?{
25  $_.Name -eq $subnetName }
26
27
28
29 $subnetName=”mgmtSubnet”
30
31
32 $subnet3=$vnet.Subnets|?{
33  $_.Name -eq $subnetName }
```

Crear direcciones IP públicas.

```
1 $pip1=New-AzureRmPublicIpAddress -Name $pubIPName1 -ResourceGroupName
    $rgName -DomainNameLabel $domName1 -Location $locName -
    AllocationMethod Dynamic
2
3 $pip2=New-AzureRmPublicIpAddress -Name $pubIPName2 -ResourceGroupName
    $rgName -DomainNameLabel $domName2 -Location $locName -
    AllocationMethod Dynamic
4
5 $pip3=New-AzureRmPublicIpAddress -Name $pubIPName3 -ResourceGroupName
    $rgName -DomainNameLabel $domName3 -Location $locName -
    AllocationMethod Dynamic
```


Cree configuraciones IP para VPX1.

```
$IpConfigName1 = ”IPConfig1”


$IPAddress = ”12.5.2.24”


$IPConfig1=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName1 -
    Subnet $subnet3 -PrivateIpAddress $IPAddress -PublicIpAddress $pip1
    -Primary


$IPConfigName3=”IPConfig-3”


$IPAddress=”12.5.1.27”


$IPConfig3=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName3 -
    Subnet $subnet1 -PrivateIpAddress $IPAddress -Primary


$IPConfigName4 = ”IPConfig-4”


$IPAddress = ”12.5.3.24”


$IPConfig4 = New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName4 -
    Subnet $subnet2 -PrivateIpAddress $IPAddress -Primary
```

Cree configuraciones IP para VPX2.

```
$IpConfigName5 = ”IPConfig5”


$IPAddress=”12.5.2.26”


$IPConfig5=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName5 -
    Subnet $subnet3 -PrivateIpAddress $IPAddress -PublicIpAddress $pip2
```



```
    -Primary
8
9
10 $IPConfigName7=”IPConfig-7”
11
12
13 $IPAddress=”12.5.1.28”
14
15
16 $IPConfig7=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName7 -
    Subnet $subnet1 -PrivateIpAddress $IPAddress -Primary
17
18
19 $IPConfigName8=”IPConfig-8”
20
21
22 $IPAddress=”12.5.3.28”
23
24
25 $IPConfig8=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName8 -
    Subnet $subnet2 -PrivateIpAddress $IPAddress -Primary
```

Crear NIC para VPX1.

```
1 $nic1=New-AzureRmNetworkInterface -Name $nicName1 -ResourceGroupName
    $rgName -Location $locName -IpConfiguration $IpConfig1 -
    NetworkSecurityGroupId $nsg.Id
2
3
4 $nic2=New-AzureRmNetworkInterface -Name $nicName2 -ResourceGroupName
    $rgName -Location $locName -IpConfiguration $IpConfig3 -
    NetworkSecurityGroupId $nsg.Id
5
6
7 $nic3=New-AzureRmNetworkInterface -Name $nicName3 -ResourceGroupName
    $rgName -Location $locName -IpConfiguration $IpConfig4 -
    NetworkSecurityGroupId $nsg.Id
```

Crear NIC para VPX2.

```
1 $nic4=New-AzureRmNetworkInterface -Name $nicName4 -ResourceGroupName
    $rgName -Location $locName -IpConfiguration $IpConfig5 -
```



```
    NetworkSecurityGroupId $nsg.Id
2
3
4 $nic5=New-AzureRmNetworkInterface -Name $nicName5 -ResourceGroupName
    $rgName -Location $locName -IpConfiguration $IpConfig7 -
    NetworkSecurityGroupId $nsg.Id
5
6
7 $nic6=New-AzureRmNetworkInterface -Name $nicName6 -ResourceGroupName
    $rgName -Location $locName -IpConfiguration $IpConfig8 -
    NetworkSecurityGroupId $nsg.Id
```

Crear VPX1.

Este paso incluye los siguientes pasos secundarios:

- Crear objeto de configuración de VM
- Establecer credenciales, SO e imagen
- Agregar NIC
- Especificar el disco del sistema operativo y crear VM

```
1  $suffixNumber = 1
2
3  $vmName=$vmNamePrefix + $suffixNumber
4
5  $vmConfig=New-AzureRMVMConfig -VMName $vmName -VMSize $vmSize -
     AvailabilitySetId $avSet.Id
6
7  $cred=Get-Credential -Message "Type the name and password for VPX
       login."
8
9  $vmConfig=Set-AzureRMVMOperatingSystem -VM $vmConfig -Linux -
     ComputerName $vmName -Credential $cred
10
11 $vmConfig=Set-AzureRMVMSourceImage -VM $vmConfig -PublisherName
     $publisher -Offer $offer -Skus $sku -Version $version
12
13 $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic1.
     Id -Primary
14
15 $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic2.
     Id
16
```



```
$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic3.Id

$osDiskName=$vmName + "-" + $osDiskSuffix1

$osVhdUri=$prmStorageAccount.PrimaryEndpoints.Blob.ToString() + "vhds/" + $osDiskName + ".vhd"

$vmConfig=Set-AzureRMVMOSDisk -VM $vmConfig -Name $osDiskName -VhdUri $osVhdUri -CreateOption fromImage

Set-AzureRmVMPlan -VM $vmConfig -Publisher $publisher -Product $offer -Name $sku

New-AzureRMVM -VM $vmConfig -ResourceGroupName $rgName -Location $locName
```

Crear VPX2.

```
```
$suffixNumber=2

$vmName=$vmNamePrefix + $suffixNumber

$vmConfig=New-AzureRMVMConfig -VMName $vmName -VMSize $vmSize -AvailabilitySetId $avSet.Id

$cred=Get-Credential -Message "Type the name and password for VPX login."

$vmConfig=Set-AzureRMVMOperatingSystem -VM $vmConfig -Linux -ComputerName $vmName -Credential $cred

$vmConfig=Set-AzureRMVMSourceImage -VM $vmConfig -PublisherName $publisher -Offer $offer -Skus $sku -Version $version

$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic4.Id -
```

 
```

```
    Primary
21
22
23 $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic5.Id
24
25
26 $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic6.Id
27
28
29 $osDiskName=$vmName + "-" + $osDiskSuffix2
30
31
32 $osVhdUri=$prmStorageAccount.PrimaryEndpoints.Blob.ToString() + "vhds/"
     + $osDiskName + ".vhd"
33
34
35 $vmConfig=Set-AzureRMVMOSDisk -VM $vmConfig -Name $osDiskName -VhdUri
    $osVhdUri -CreateOption fromImage
36
37
38 Set-AzureRmVMPlan -VM $vmConfig -Publisher $publisher -Product $offer -
    Name $sku
39
40
41 New-AzureRMVM -VM $vmConfig -ResourceGroupName $rgName -Location
    $locName
42 <!--NeedCopy--> ```
```

Para ver las direcciones IP privadas y públicas asignadas a las NIC, escriba los siguientes comandos:

```
1 ```
2 $nic1.IPConfig
3
4
5 $nic2.IPConfig
6
7
8 $nic3.IPConfig
9
10
11 $nic4.IPConfig
12
13
```



```
$nic5.IPConfig


$nic6.IPConfig
<!--NeedCopy--> ```
```

Crear equilibrio de carga de Azure (ALB).

Este paso incluye los siguientes pasos secundarios:

- Crear configuración IP front-end
- Crear sondeo de estado
- Crear grupo de direcciones de backend
- Crear reglas de equilibrio de carga (HTTP y SSL)
- Crear ALB con configuración IP front-end, grupo de direcciones backend y regla LB
- Asociar configuración de IP con grupos de back-end

```
$frontEndIP1=New-AzureRmLoadBalancerFrontendIpConfig -Name $frontEndConfigName1
 -PublicIpAddress $pip3

$healthProbe=New-AzureRmLoadBalancerProbeConfig -Name $healthProbeName
-Protocol Tcp -Port 9000 -IntervalInSeconds 5 -ProbeCount 2

$beAddressPool1=New-AzureRmLoadBalancerBackendAddressPoolConfig -Name
$backendPoolName1

$lbRule1=New-AzureRmLoadBalancerRuleConfig -Name $lbRuleName1 -FrontendIpConfigur
 $frontEndIP1 -BackendAddressPool $beAddressPool1 -Probe $healthProbe -
Protocol Tcp -FrontendPort 80 -BackendPort 80 -EnableFloatingIP

$lb=New-AzureRmLoadBalancer -ResourceGroupName $rgName -Name $lbName -
Location $locName -FrontendIpConfiguration $frontEndIP1 -LoadBalancingRule
 $lbRule1 -BackendAddressPool $beAddressPool1 -Probe $healthProbe

$nic2.IpConfigurations[0].LoadBalancerBackendAddressPools.Add($lb.
BackendAddressPools[0])

$nic5.IpConfigurations[0].LoadBalancerBackendAddressPools.Add($lb.
BackendAddressPools[0])

$lb=$lb |Set-AzureRmLoadBalancer

$nic2=$nic2 | Set-AzureRmNetworkInterface

$nic5=$nic5 | Set-AzureRmNetworkInterface
```


Después de implementar correctamente el par Citrix ADC VPX, inicie sesión en cada instancia VPX para configurar HA-INC y las direcciones SNIP y VIP.

1. Escriba el siguiente comando para agregar nodos HA.

   ```
   add ha node 1 PeerNodeNSIP -inc Enabled
   ```

2. Agregar direcciones IP privadas de NIC del lado del cliente como SNIP para VPX1 (NIC2) y VPX2 (NIC5)

   ```
   add nsip privateIPofNIC2 255.255.255.0 -type SNIP
   add nsip privateIPofNIC5 255.255.255.0 -type SNIP
   ```

3. Agregue un servidor virtual de equilibrio de carga en el nodo principal con la dirección IP front-end (IP pública) de ALB.

   ```
   add lb virtual server v1 HTTP FrontEndIPofALB 80
   ```

Recursos relacionados:

Configuración de GSLB en la implementación de HA activa en espera en Azure

Implemente un par de alta disponibilidad de Citrix ADC en Azure con ALB en el modo flotante de IP inhabilitada

June 2, 2022

Puede implementar un par de instancias de Citrix ADC VPX con varias NIC en una configuración de alta disponibilidad (HA) activo-pasiva en Azure. Cada NIC puede contener muchas direcciones IP.

Una implementación activa-pasiva requiere:

- Configuración de red independiente de HA (INC)
- Azure Load Balancer (ALB) con:
  - Modo habilitado para IP flotante o modo Direct Server Return (DSR)
  - Modo de IP flotante inhabilitado

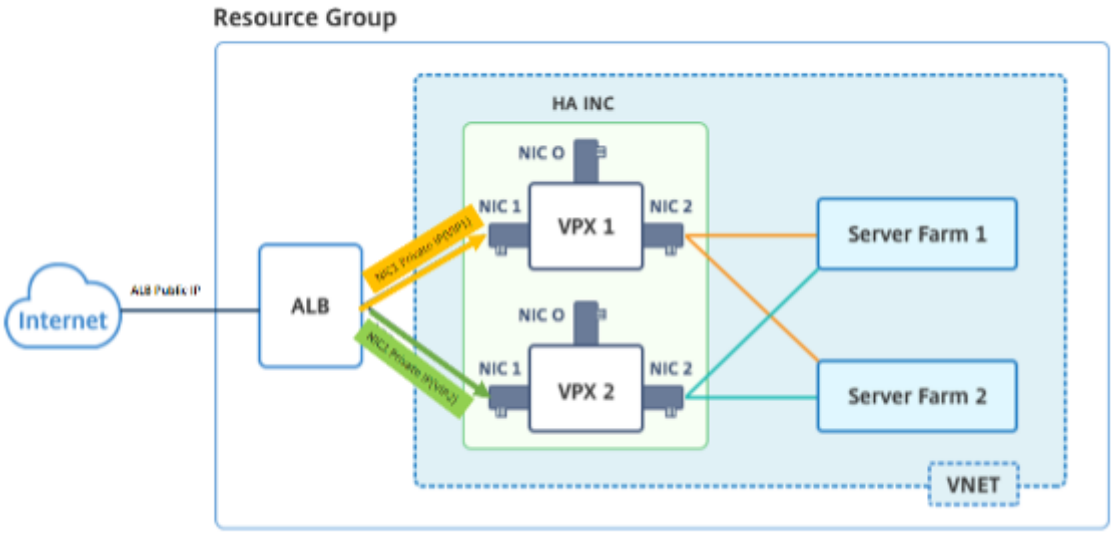
Para obtener más información sobre las opciones de IP flotante de ALB, consulte la documentación de Azure.

Si desea implementar un par VPX en una configuración de alta disponibilidad activa-pasiva en Azure con IP flotante de ALB habilitada, consulte Configurar una configuración de alta disponibilidad con varias direcciones IP y NIC mediante comandos de PowerShell.

Arquitectura de implementación de alta disponibilidad con ALB en modo flotante con IP inhabilitada

En una implementación activa-pasiva, las direcciones IP privadas de la interfaz de cliente de cada instancia se agregan como direcciones VIP en cada instancia VPX. Configure en el modo HA-INC con las direcciones VIP que se comparten mediante IPset y las direcciones SNIP son específicas de la instancia. Todo el tráfico pasa por la instancia principal. La instancia secundaria está en modo de espera hasta que se produce un error en la instancia principal.

Diagrama: Ejemplo de una arquitectura de implementación activo-pasiva



Requisitos previos

Debe estar familiarizado con la siguiente información antes de implementar una instancia de Citrix ADC VPX en Azure.

- Terminología y detalles de red de Azure. Para obtener más información, consulte Terminología de Azure.
- Funcionamiento de un dispositivo Citrix ADC. Para obtener más información, consulte la documentación de Citrix ADC.
- Redes Citrix ADC. Para obtener más información, consulte ADC Networking.
- Configuración de reglas de equilibrio de carga y equilibrador de carga de Azure. Para obtener más información, consulte la documentación de Azure ALB.

Cómo implementar un par de alta disponibilidad de VPX en Azure con la IP flotante de ALB inhabilitada

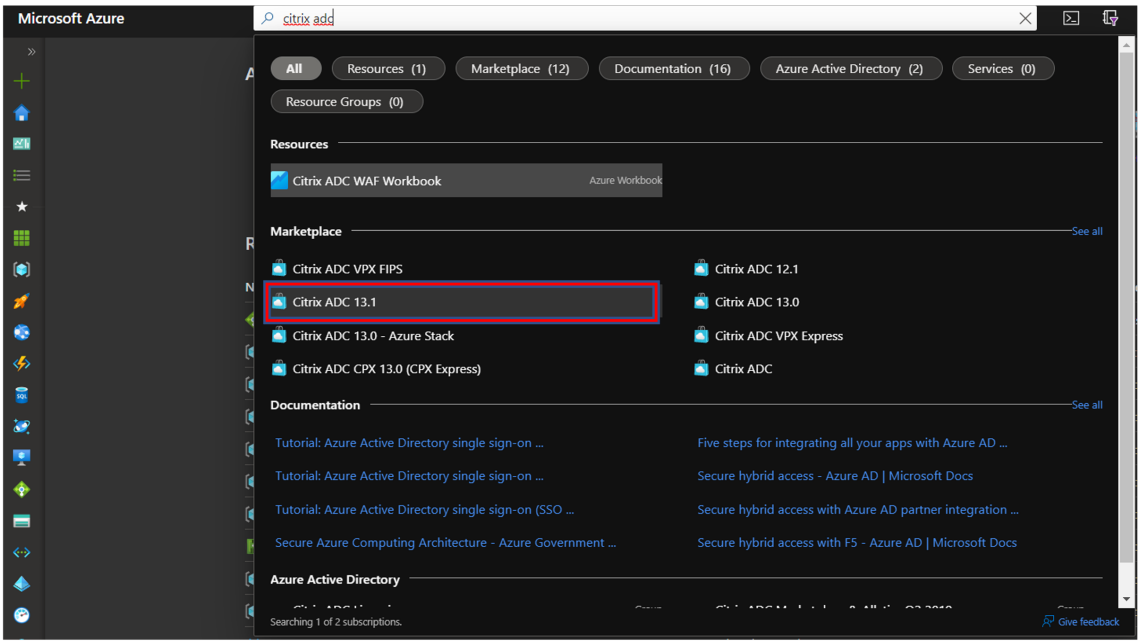
Este es un resumen de los pasos de implementación de HA y ALB:

1. Implemente dos instancias VPX (instancias principal y secundaria) en Azure.
2. Agregue NIC de cliente y servidor en ambas instancias.
3. Implemente una ALB con regla de equilibrio de carga cuyo modo de IP flotante esté inhabilitado.
4. Configure la configuración de HA en ambas instancias mediante la GUI de Citrix ADC.

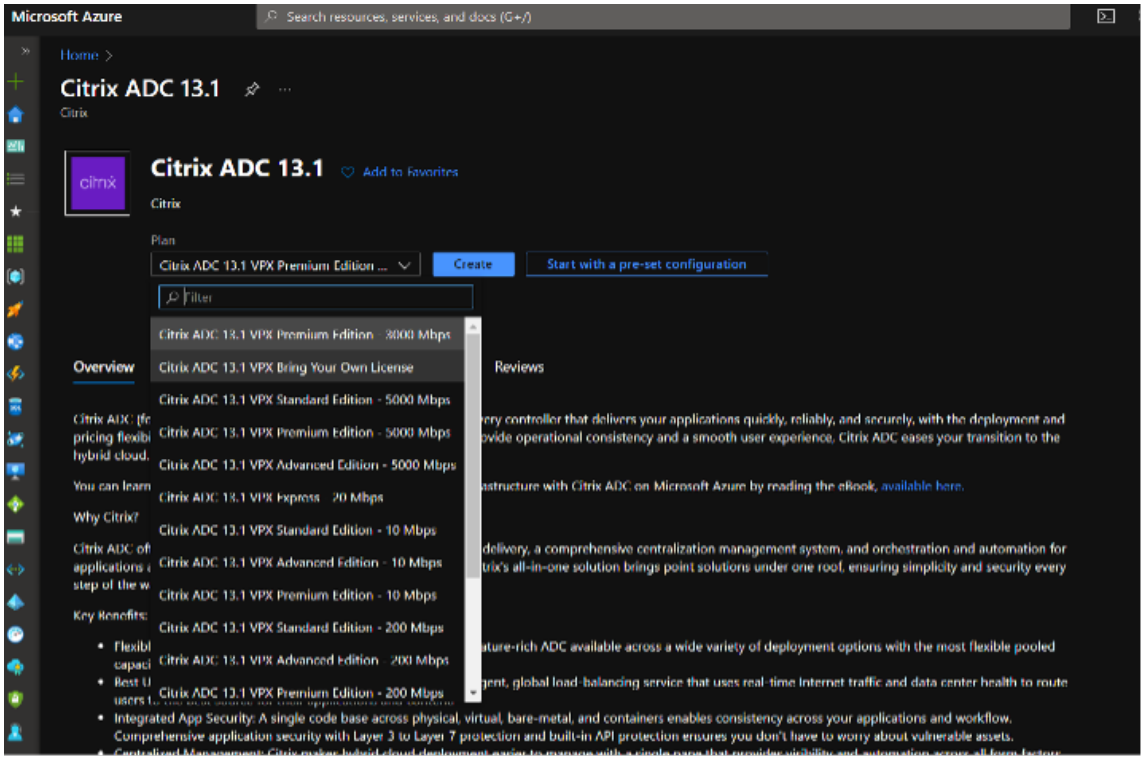
Paso 1. Implemente dos instancias VPX en Azure.

Cree dos instancias VPX siguiendo estos pasos:

1. Seleccione la versión de Citrix ADC en Azure Marketplace (en este ejemplo, se utiliza la versión 13.1 de Citrix ADC).

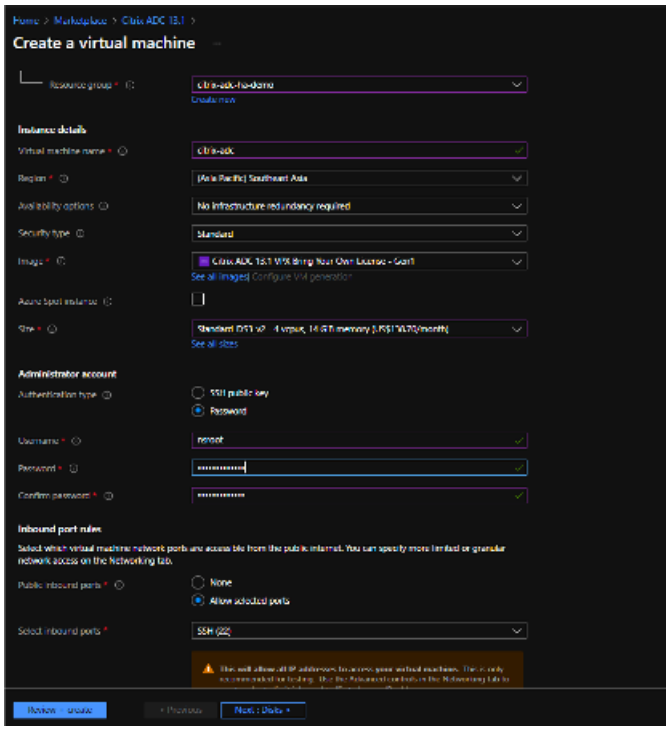


2. Seleccione el modo de licencia de ADC requerido y haga clic en **Crear**.



Se abre la página **Crear una máquina virtual** .

3. Complete los detalles necesarios en cada ficha para una implementación correcta.

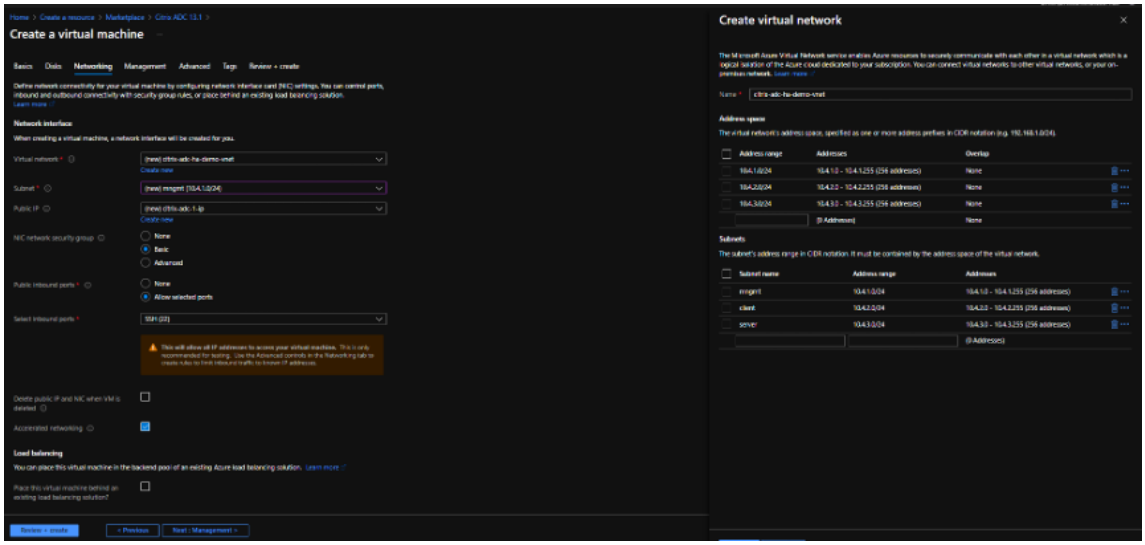


4. En la ficha **Redes**, cree una nueva red virtual con 3 subredes, una para cada una: NIC de administración, cliente y servidor. De lo contrario, también puede utilizar una red virtual existente. La

NIC de administración se crea durante la implementación de la VM. Las NIC de cliente y servidor se crean y se conectan después de crear la máquina virtual. Para el grupo de seguridad de red de NIC, puede realizar una de las siguientes acciones:

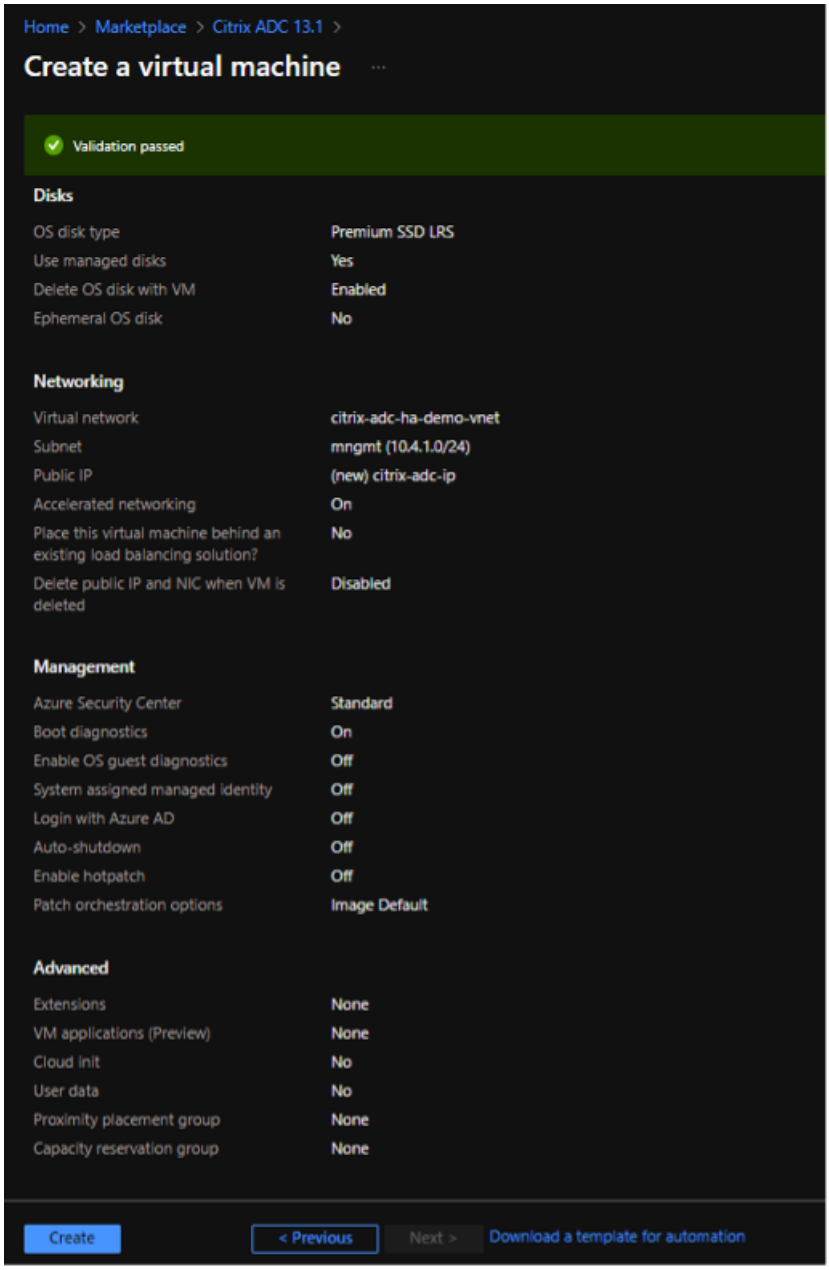
- Seleccione **Avanzado** y utilice un grupo de seguridad de red existente que se adapte a sus requisitos.
- Seleccione **Basic** y seleccione los puertos necesarios.

> **Nota:**
>
> También puede cambiar la configuración del grupo de seguridad de red después de que se complete la implementación de la VM.

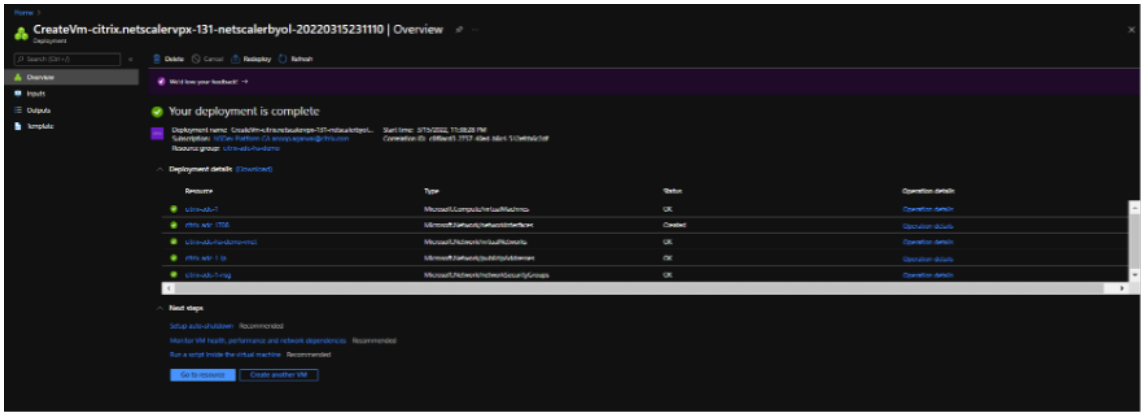


5. Haga clic en Siguiente: **Revisar + crear**.

   Una vez que la validación se haya realizado correctamente, revise la configuración básica, las configuraciones de VM, la red y la configuración adicional y haga clic en **Crear**.



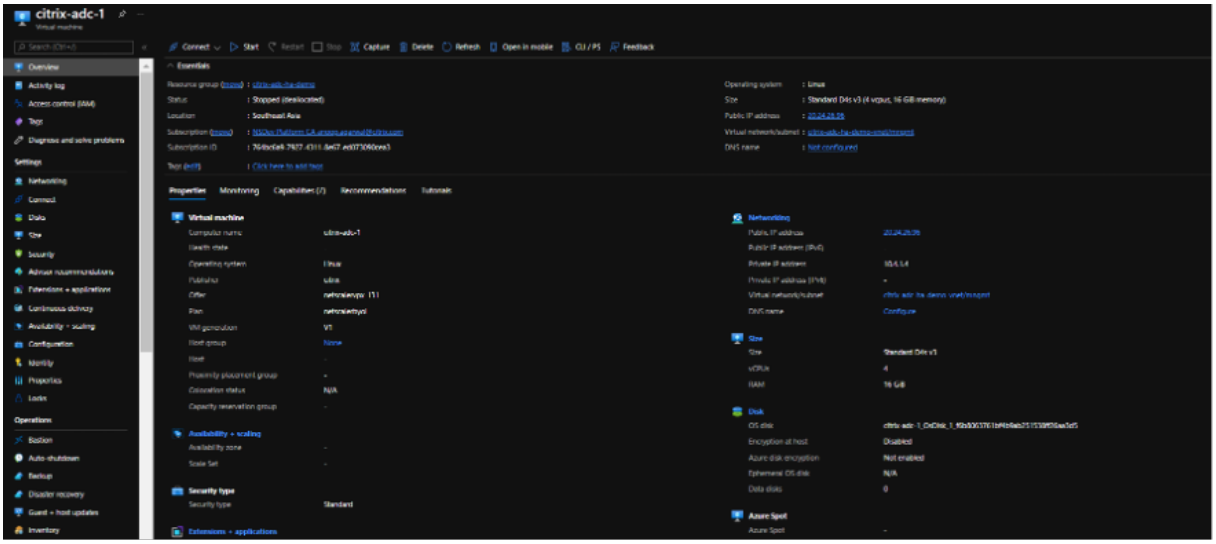
6. Una vez finalizada la implementación, haga clic en **Ir al recurso** para ver los detalles de la configuración.



Del mismo modo, implemente una segunda instancia de Citrix ADC VPX.

Paso 2. Agregue NIC de cliente y servidor en ambas instancias.

> **Nota:**
>
> Para conectar más NIC, primero debe detener la VM. En el portal de Azure, seleccione la VM que quiere detener. En la ficha **Descripción general**, haga clic en **Detener**. Espere a que el estado aparezca como **Detenido**.

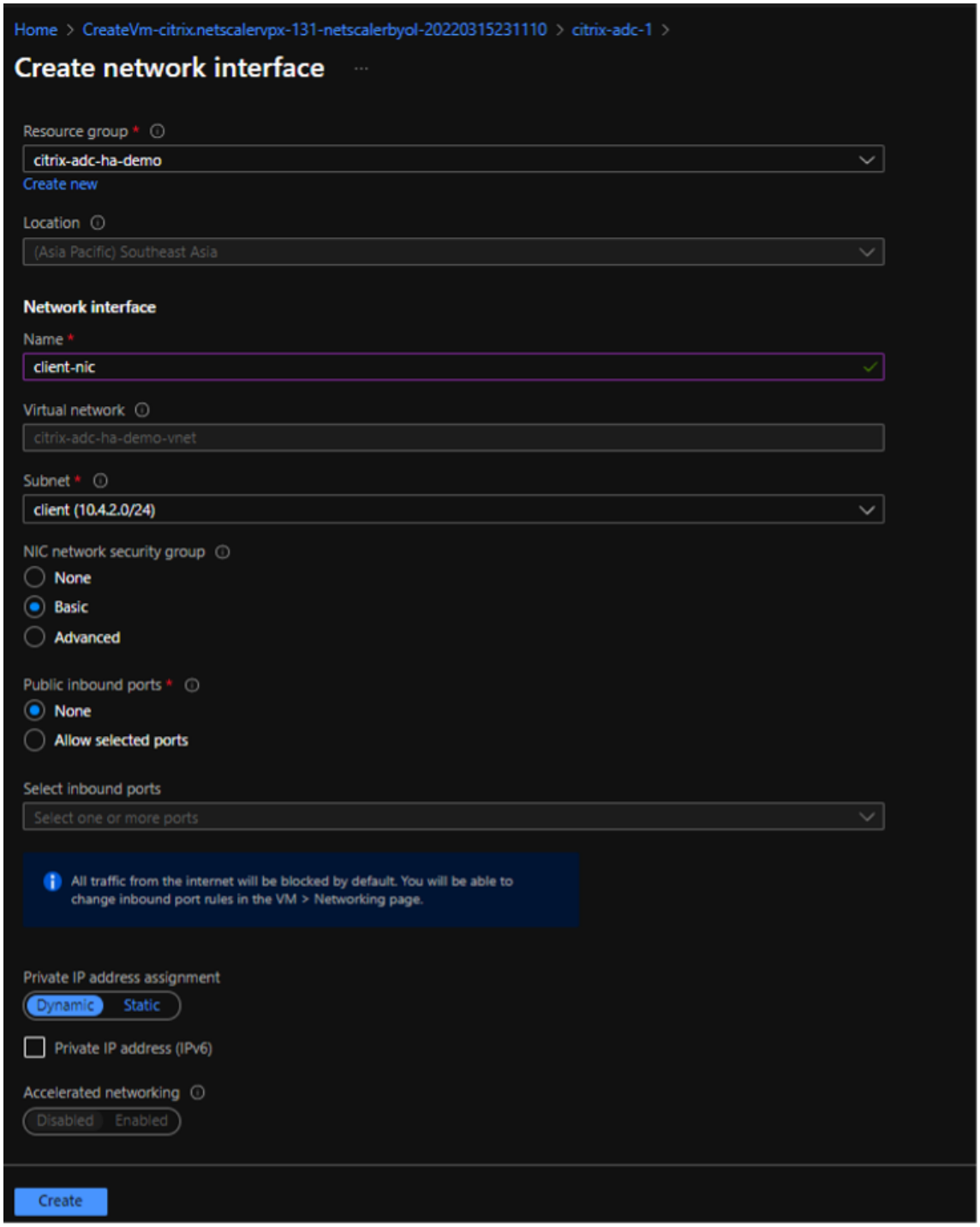


Para agregar una NIC de cliente en la instancia principal, sigue estos pasos:

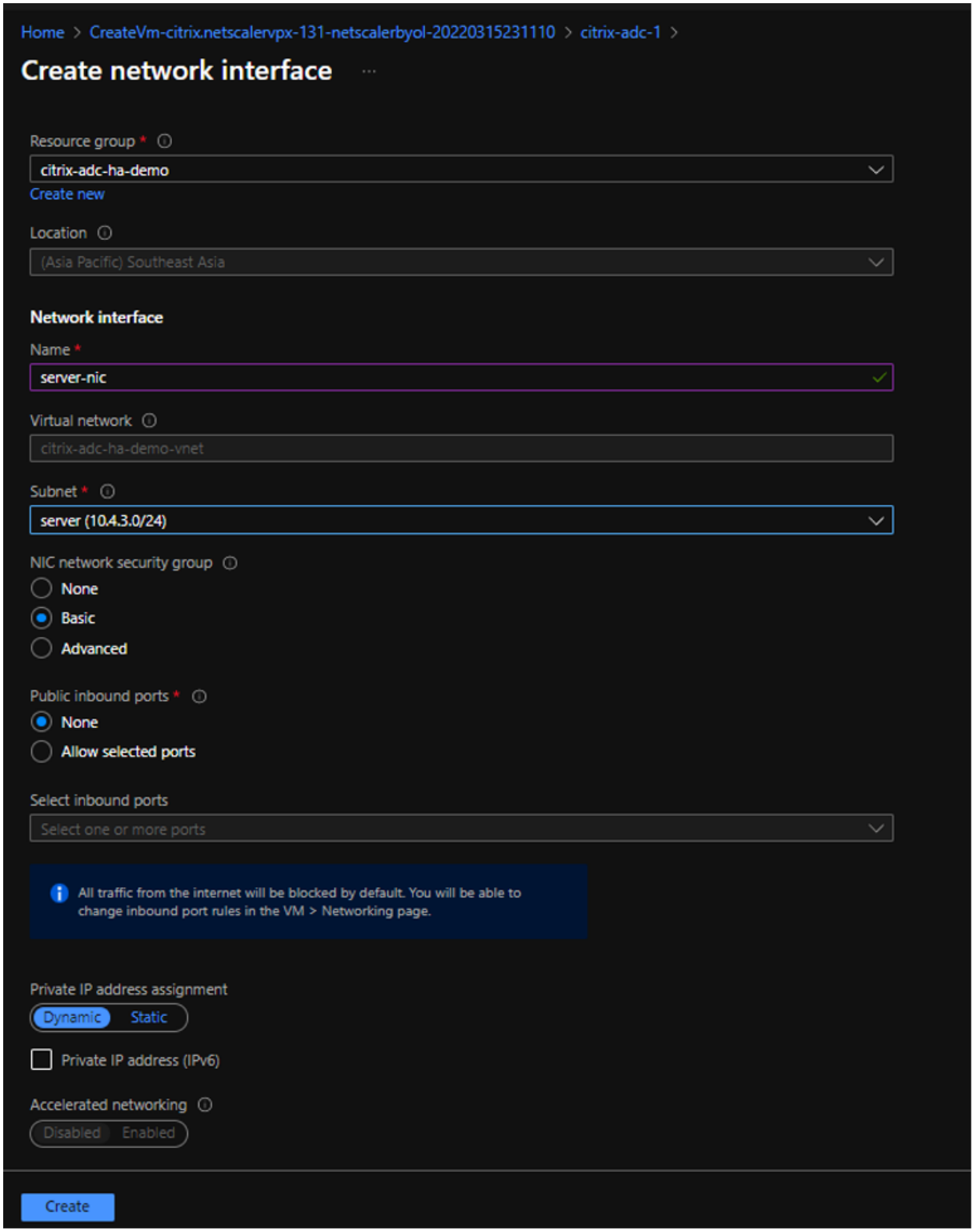
1. Vaya a **Redes > Adjuntar interfaz de red**.

   Puede seleccionar una NIC existente o crear y conectar una nueva interfaz.

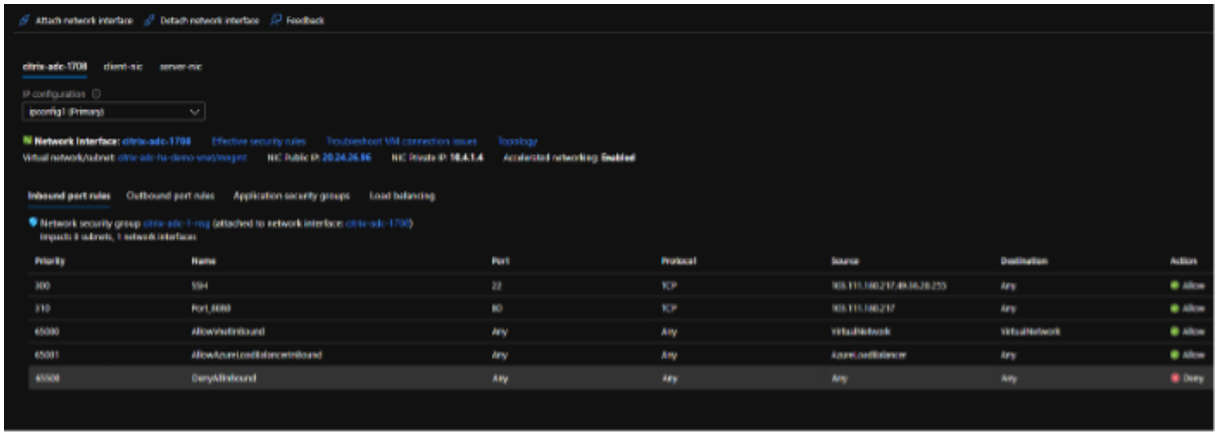
2. Para el grupo de seguridad de red de NIC, puede usar un grupo de seguridad de red existente seleccionando **Avanzado** o crear uno seleccionando **Básico**.



Para agregar una NIC de servidor, siga los mismos pasos que para agregar una NIC de cliente.



La instancia de Citrix ADC VPX tiene las tres NIC (NIC de administración, NIC de cliente y NIC de servidor) conectadas.

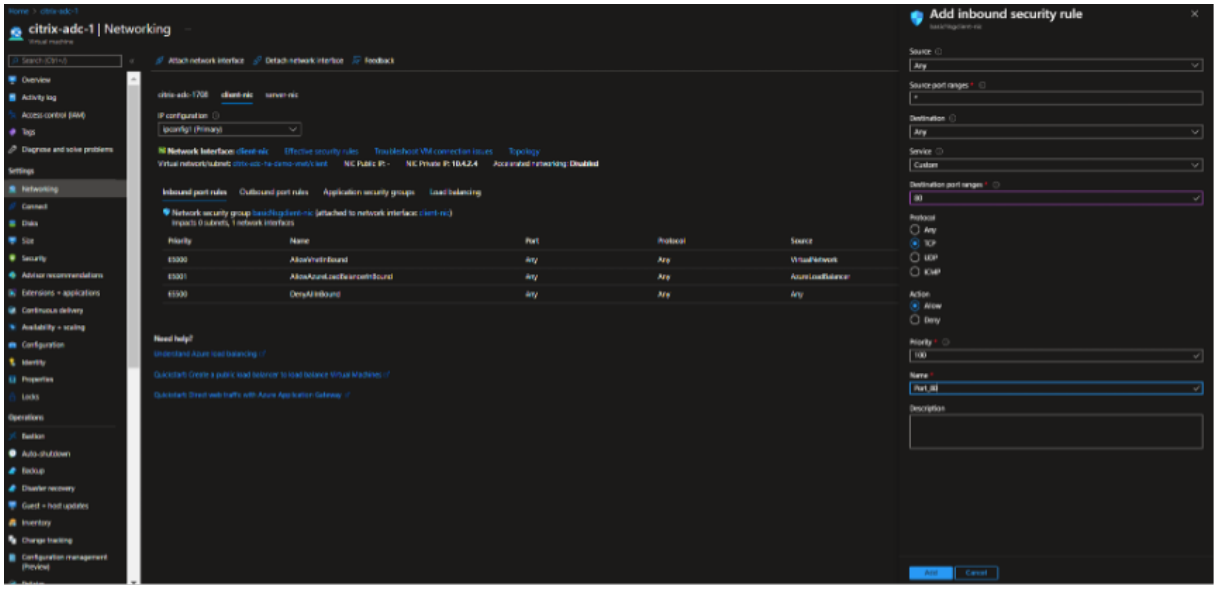


Repita los pasos anteriores para agregar NIC en la instancia secundaria.

Después de crear y conectar las NIC en ambas instancias, reinicie ambas instancias en **Descripción general > Iniciar**.

> **Nota:**
>
> Debe permitir el tráfico a través del puerto en la regla de entrada de la NIC del cliente, que se utilizará más adelante para crear un servidor virtual de equilibrio de carga al configurar la instancia de Citrix ADC VPX.

En el siguiente ejemplo, se agrega un puerto HTTP 80 a la regla de seguridad de entrada.



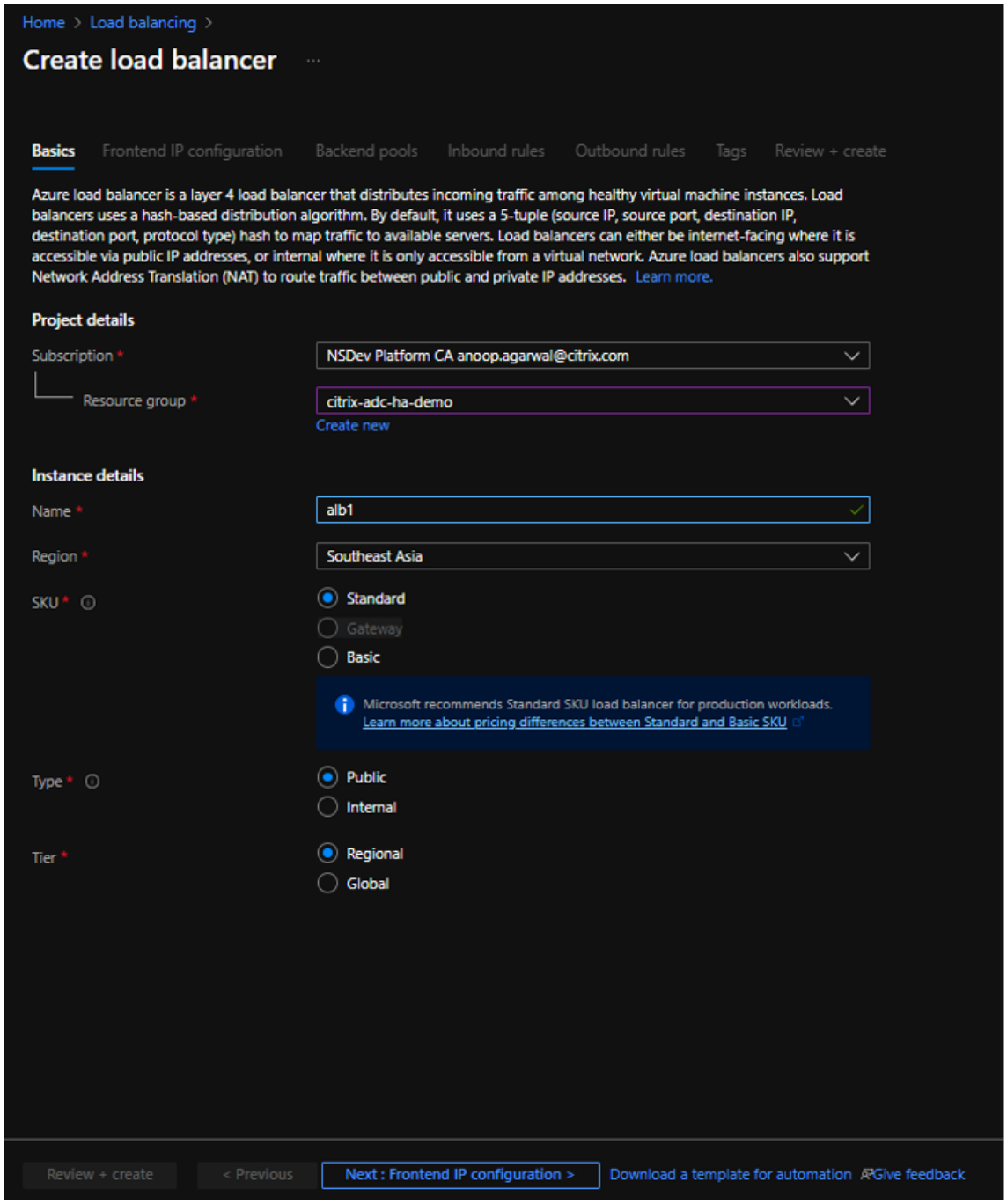
Paso 3. Implemente una ALB con regla de equilibrio de carga cuyo modo de IP flotante esté inhabilitado.

Para iniciar la configuración de ALB, siga estos pasos:

1. Vaya a la página **Equilibradores de carga** y haga clic en **Crear**.

2. En la página **Crear equilibrador de cargas**, proporcione los detalles necesarios.

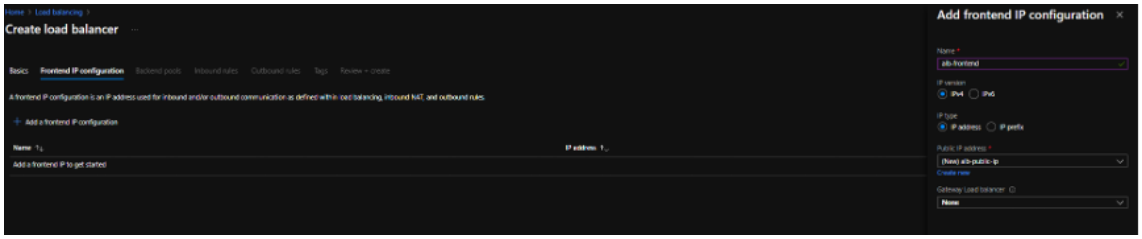
   En el siguiente ejemplo, implementamos un equilibrador de carga público regional de SKU estándar.



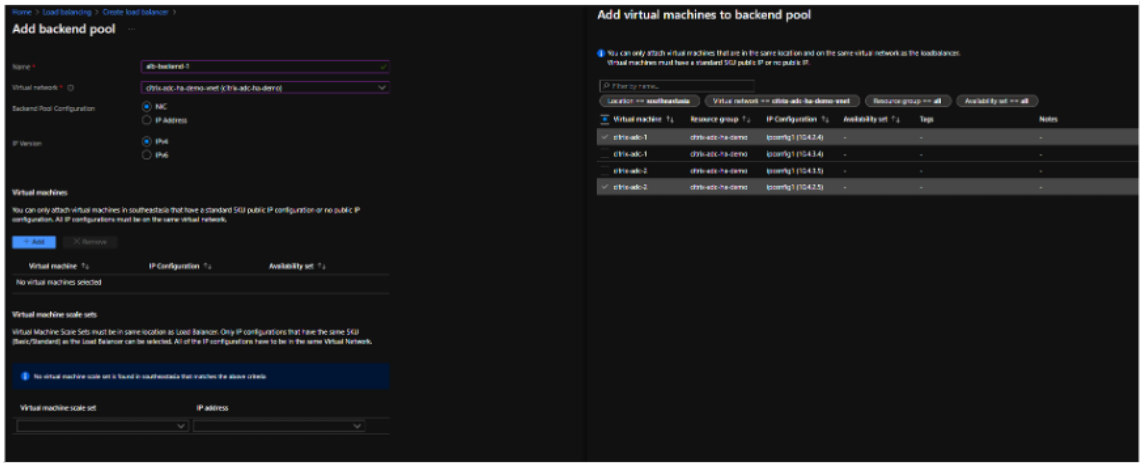
> **Nota:**
>
> Todas las IP públicas conectadas a las máquinas virtuales de Citrix ADC deben tener la misma SKU que la de ALB. Para obtener más información sobre las SKU de ALB, consulte

> la documentación de las SKU de Azure Load Balancer.

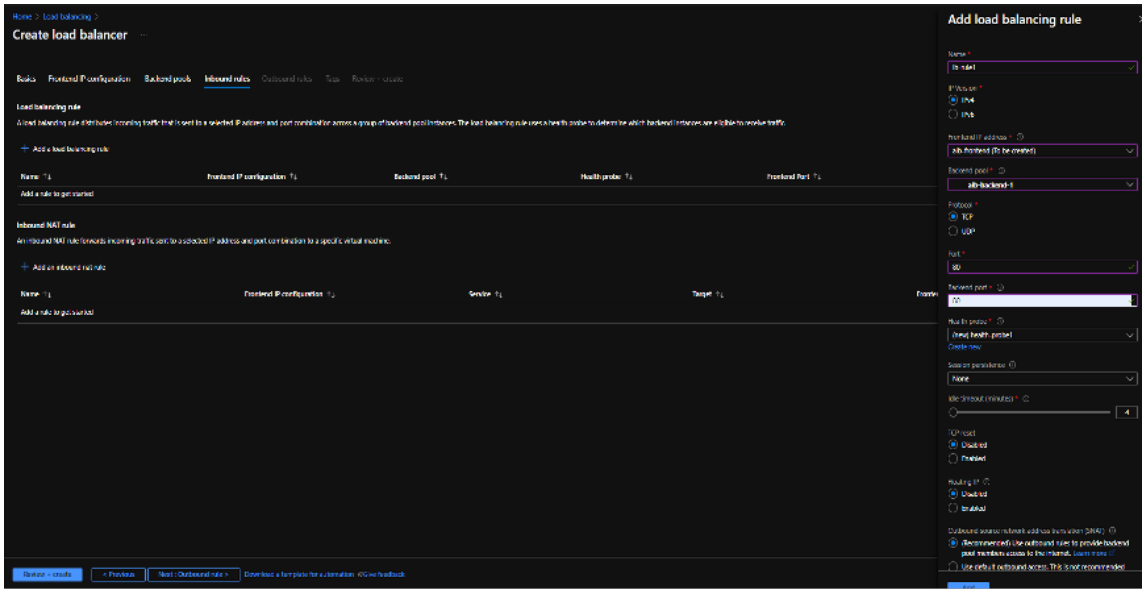
3. En la ficha **Configuración de IP de frontend**, cree una dirección IP o utilice una dirección IP existente.



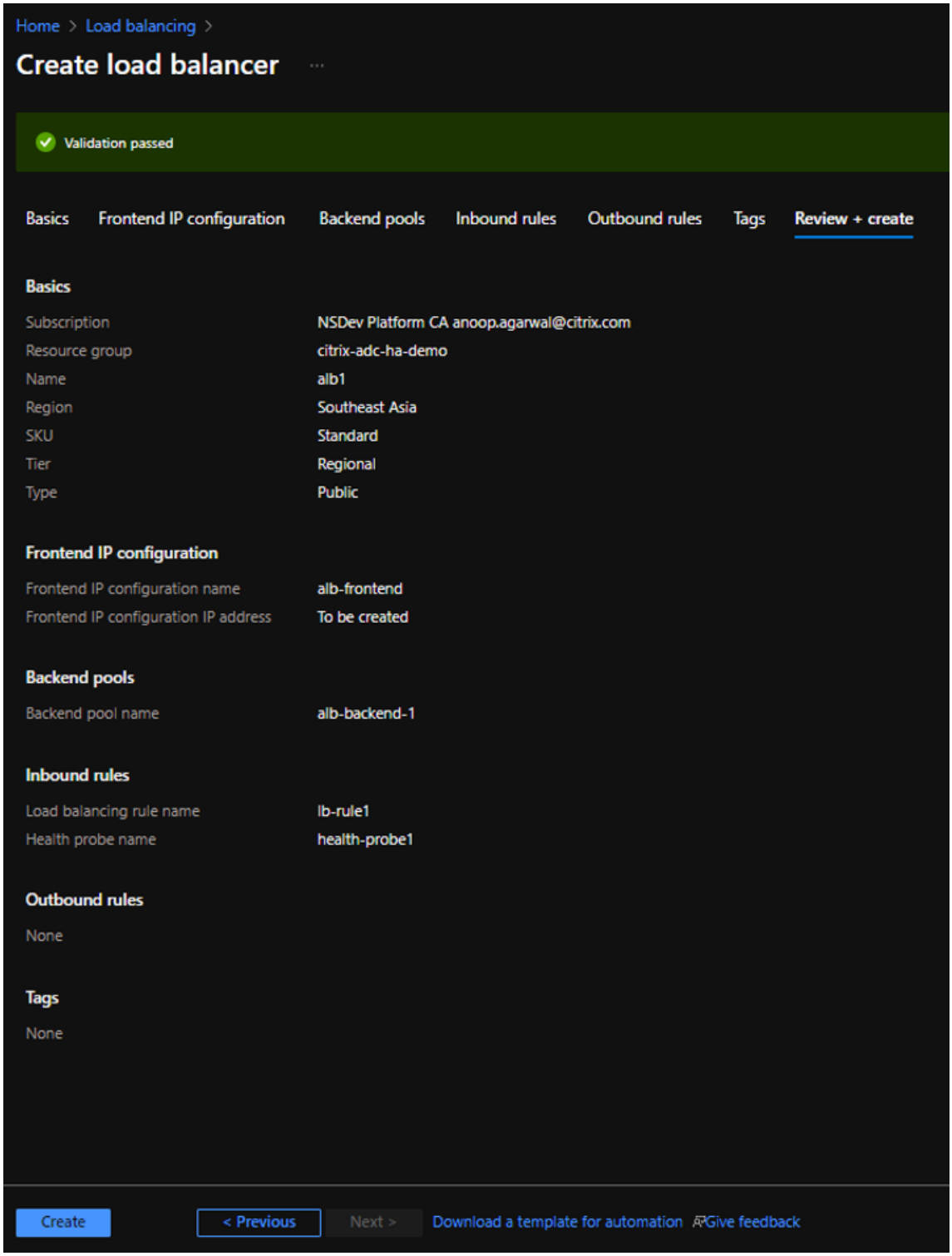
4. En la ficha **Grupos de backend**, seleccione Configuración de grupos de backend basada en NIC y agregue las NIC de cliente de ambas máquinas virtuales de Citrix ADC.



5. En la ficha **Reglas de entrada**, haga clic en **Agregar una regla de equilibrio de carga** y proporcione la dirección IP de frontend y el grupo de backend creados en los pasos anteriores. Seleccione el protocolo y el puerto según sus necesidades. Cree o utilice una sonda de estado existente. La opción IP flotante debe estar configurada como **Desactivada**.



6. Haga clic en **Revisar + Crear**. Una vez superada la validación, haga clic en **Crear**.



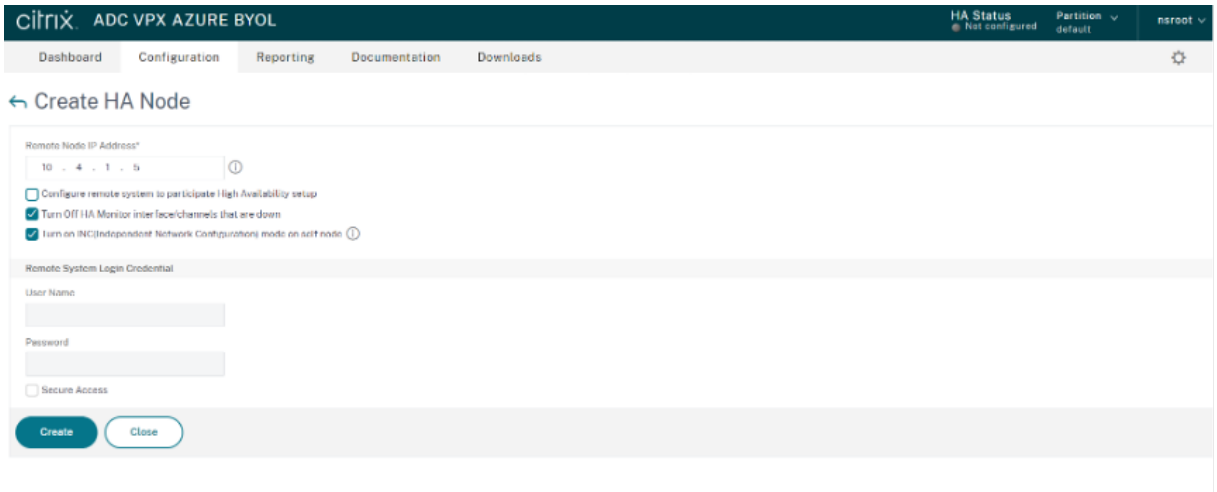
Paso 4. Configure los parámetros de alta disponibilidad en ambas instancias de Citrix ADC VPX mediante la GUI de Citrix ADC.

Después de crear las instancias de Citrix ADC VPX en Azure, puede configurar HA mediante la GUI de Citrix ADC.

Paso 1. Configure la alta disponibilidad en modo INC en ambas instancias.

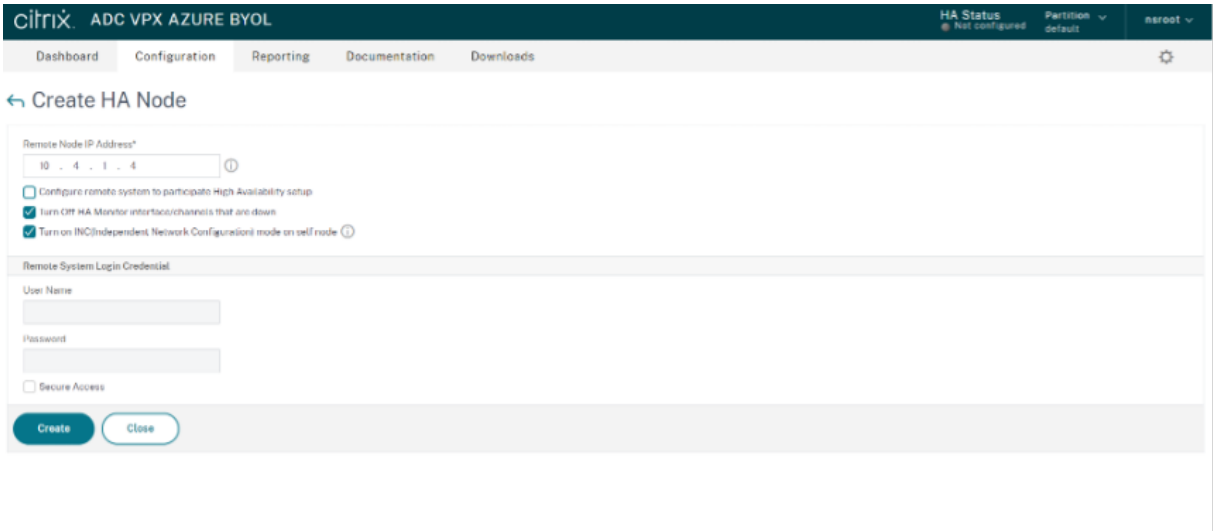
En la instancia principal, realice los siguientes pasos:

1. Inicie sesión en la instancia con el nombre de usuario `nsroot` y la contraseña proporcionados al implementar la instancia.
2. Vaya a **Configuración > Sistema > Alta disponibilidad > Nodos** y haga clic en **Agregar**.
3. En el campo **Dirección IP del nodo remoto**, introduzca la dirección IP privada de la NIC de administración de la instancia secundaria, por ejemplo: 10.4.1.5.
4. Marque la casilla **Activar el modo INC (Configuración de red independiente) en el autonodo**.
5. Haga clic en **Crear**.



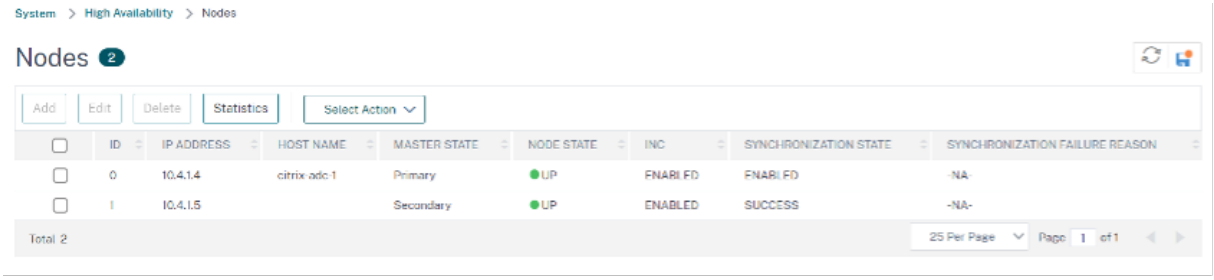
En la instancia secundaria, realice los siguientes pasos:

1. Inicie sesión en la instancia con el nombre de usuario `nsroot` y la contraseña proporcionados al implementar la instancia.
2. Vaya a **Configuración > Sistema > Alta disponibilidad > Nodos** y haga clic en **Agregar**.
3. En el campo **Dirección IP del nodo remoto**, introduzca la dirección IP privada de la NIC de administración de la instancia principal, por ejemplo: 10.4.1.4.
4. Marque la casilla **Activar el modo INC (Configuración de red independiente) en el autonodo**.
5. Haga clic en **Crear**.



Antes de continuar, asegúrese de que el **estado de sincronización** de la instancia secundaria aparezca como **SUCCESS** en la página **Nodos** .

> **Nota:**
>
> Ahora, la instancia secundaria tiene las mismas credenciales de inicio de sesión que la instancia principal.



Paso 2. Agregue la dirección IP virtual y la dirección IP de subred en ambas instancias.

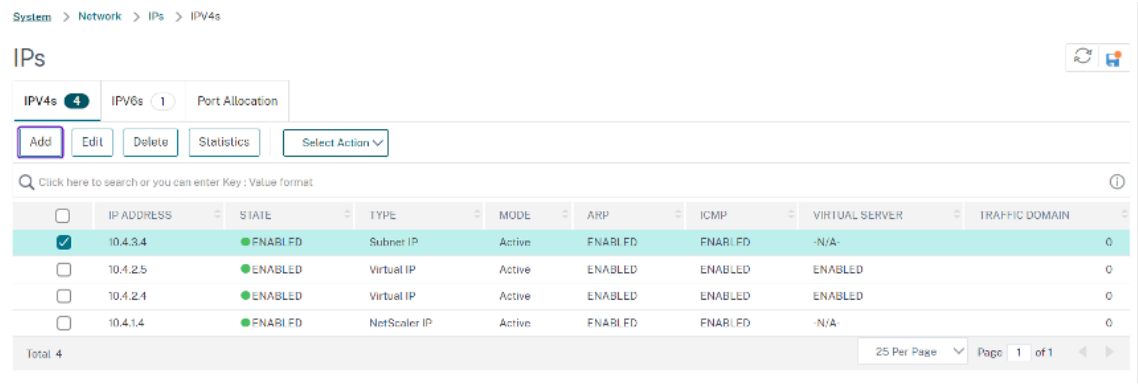
En la instancia principal, lleve a cabo los siguientes pasos:

1. Vaya a **Sistema > Red > IPs > IPv4s** y haga clic en **Agregar**.
2. Agregue una dirección VIP principal siguiendo estos pasos:
   a) Introduzca la dirección IP privada de la NIC cliente de la instancia principal y la máscara de red configuradas para la subred del cliente en la instancia de VM.
   b) En el campo **Tipo de IP**, seleccione **IP virtual** en el menú desplegable.
   c) Haga clic en **Crear**.
3. Agregue una dirección SNIP principal siguiendo estos pasos:
   a) Introduzca la dirección IP interna de la NIC del servidor de la instancia principal y la máscara de red configurada para la subred del servidor en la instancia principal.

b) En el campo **Tipo de IP**, seleccione **IP de subred** en el menú desplegable.
c) Haga clic en **Crear**.

4. Agregue una dirección VIP secundaria siguiendo estos pasos:

a) Introduzca la dirección IP interna de la NIC cliente de la instancia secundaria y la máscara de red configurada para la subred del cliente en la instancia de VM.
b) En el campo **Tipo de IP**, seleccione **IP virtual** en el menú desplegable.
c) Haga clic en **Crear**.



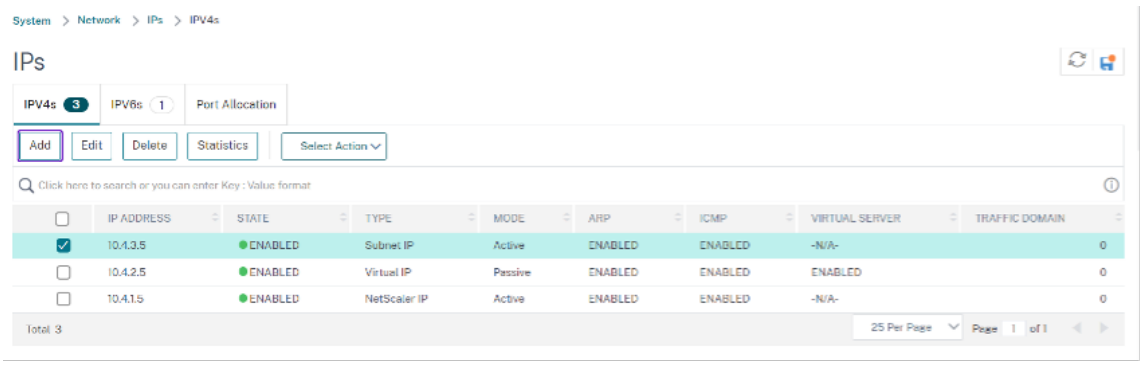
En la instancia secundaria, lleve a cabo los siguientes pasos:

1. Vaya a **Sistema > Red > IPs > IPv4s** y haga clic en **Agregar**.
2. Agregue una dirección VIP secundaria siguiendo estos pasos:

a) Introduzca la dirección IP interna de la NIC cliente de la instancia secundaria y la máscara de red configurada para la subred del cliente en la instancia de VM.
b) En el campo **Tipo de IP**, seleccione **IP virtual** en el menú desplegable.

3. Agregue una dirección SNIP secundaria siguiendo estos pasos:

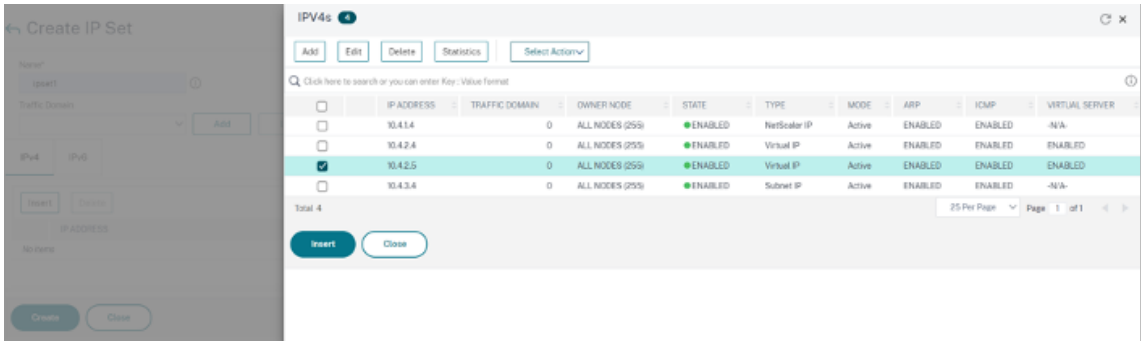
a) Introduzca la dirección IP interna de la NIC del servidor de la instancia secundaria y la máscara de red configurada para la subred del servidor en la instancia secundaria.
b) En el campo **Tipo de IP**, seleccione **IP de subred** en el menú desplegable.
c) Haga clic en **Crear**.



Paso 3. Agregue un conjunto de IP y vincule el conjunto de IP al VIP secundario en ambas instancias.

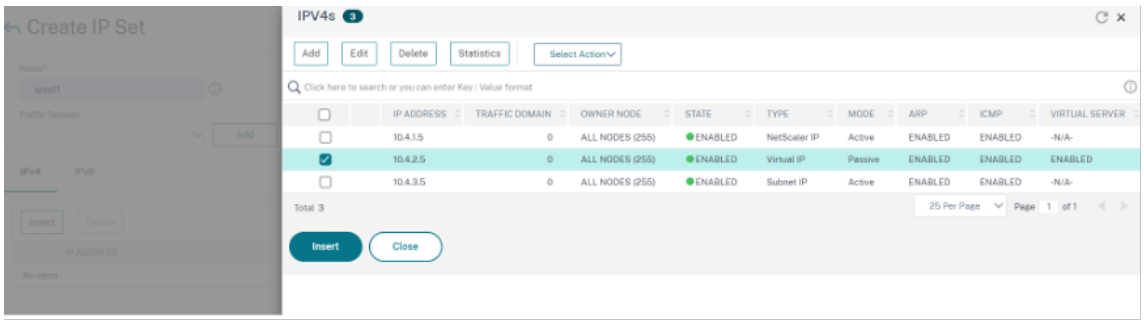
En la instancia principal, realice los siguientes pasos:

1. Vaya a **Sistema > Red > Conjuntos de IP > Agregar**.
2. Agregue un nombre de conjunto de IP y haga clic en **Insertar**.
3. En la página **IPv4**, seleccione la IP virtual (VIP secundaria) y haga clic en **Insertar**.
4. Haga clic en **Crear** para crear el conjunto de IP.



En la instancia secundaria, realice los siguientes pasos:

1. Vaya a **Sistema > Red > Conjuntos de IP > Agregar**.
2. Agregue un nombre de conjunto de IP y haga clic en **Insertar**.
3. En la página **IPv4**, seleccione la IP virtual (VIP secundaria) y haga clic en **Insertar**.
4. Haga clic en **Crear** para crear el conjunto de IP.

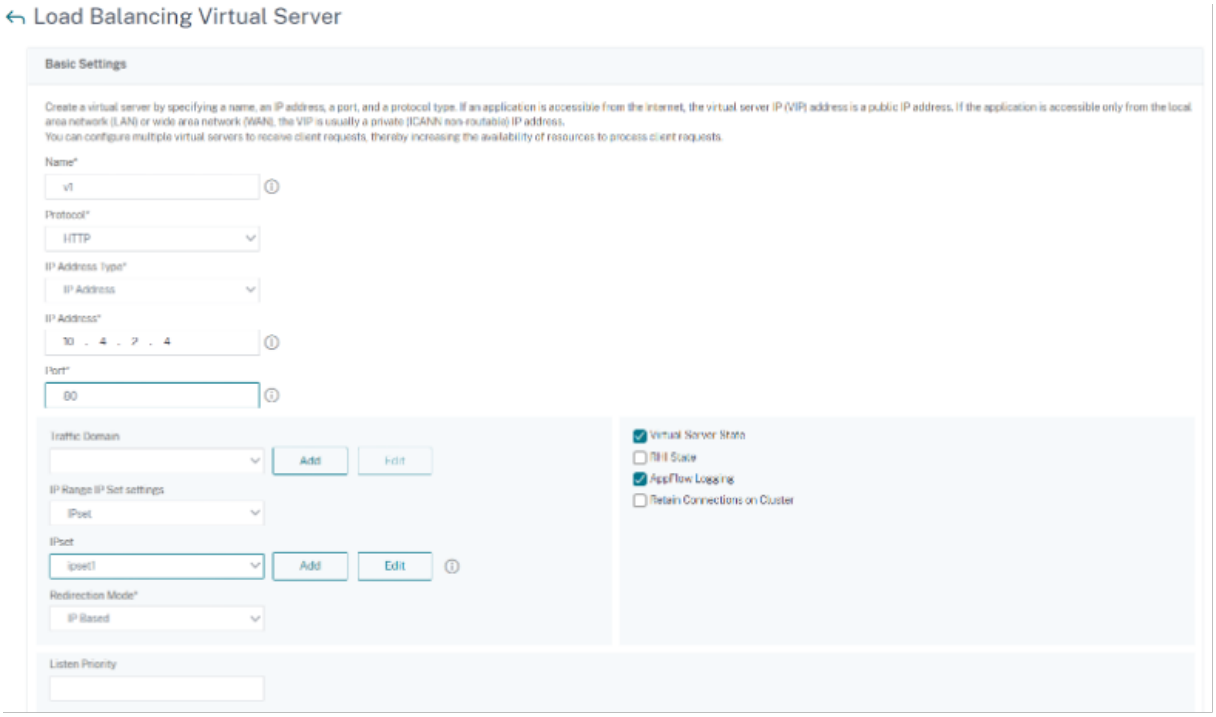


> **Nota:**
>
> El nombre del conjunto de IP debe ser el mismo en las instancias principal y secundaria.

Paso 4. Agregue un servidor virtual de equilibrio de carga en la instancia principal.

1. Vaya a **Configuración > Administración del tráfico > Equilibrio de carga > Servidores virtuales > Agregar**.
2. Agregue los valores necesarios para Nombre, Protocolo, Tipo de dirección IP (dirección IP), dirección IP (VIP principal) y Puerto.

3. Haga clic en **Más**. Vaya a **Configuración del conjunto de IP de rango IP**, seleccione **IPset** en el menú desplegable y proporcione el IPset creado en el **paso 3**.
4. Haga clic en **Aceptar** para crear el servidor virtual de equilibrio de carga.

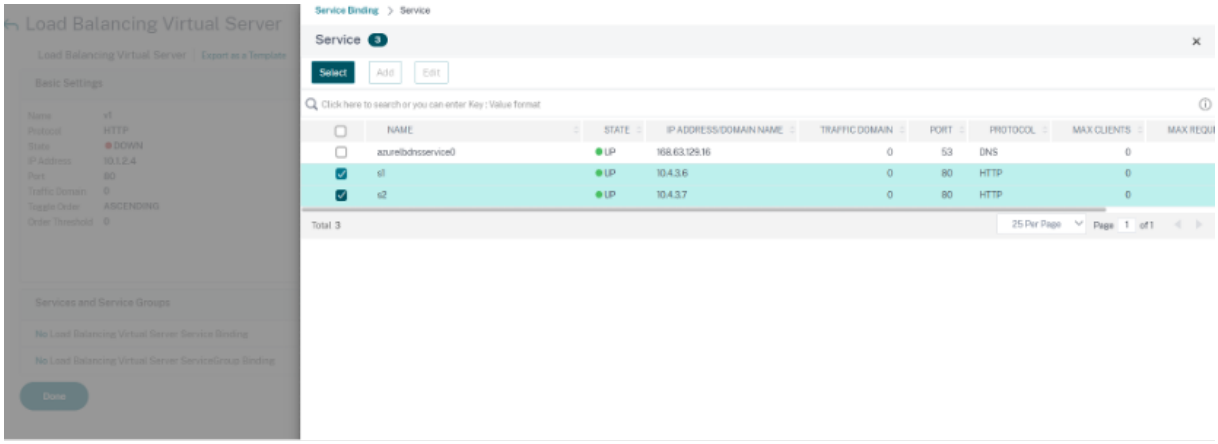


Paso 5. Agregue un servicio o grupo de servicios en la instancia principal.

1. Vaya a **Configuración > Administración del tráfico > Equilibrio de carga > Servicios > Agregar**.
2. Agregue los valores necesarios para Nombre de servicio, Dirección IP, Protocolo y Puerto, y haga clic en **Aceptar**.

Paso 6. Enlazar el servicio o el grupo de servicios al servidor virtual de equilibrio de carga de la instancia principal.

1. Vaya a **Configuración > Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. Seleccione el servidor virtual de equilibrio de carga configurado en el **paso 4**y haga clic en **Modificar**.
3. En la ficha **Grupos de servicios y servicios**, haga clic en **Enlace de servicio de servidor virtual sin equilibrio de carga**.
4. Seleccione el servicio configurado en el **paso 5**y haga clic en **Enlazar**.



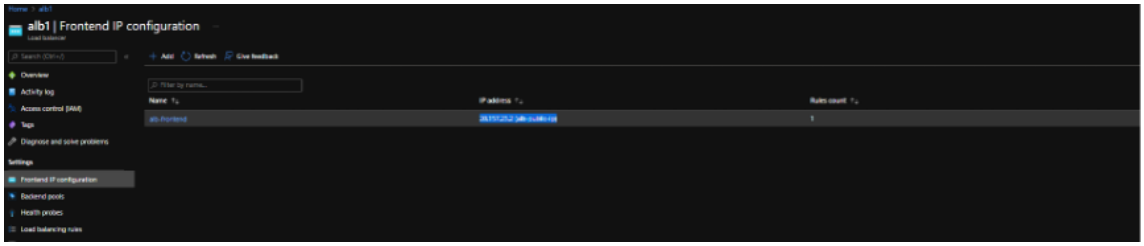
Paso 7. Guarde la configuración.

De lo contrario, toda la configuración se pierde tras un reinicio o si se produce un reinicio instantáneo.

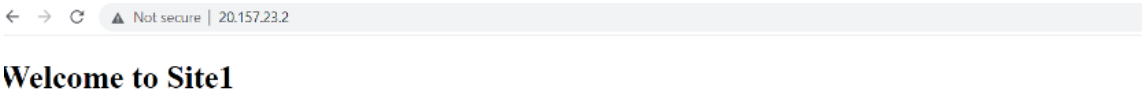
Paso 8. Verifique la configuración.

Asegúrese de que se pueda acceder a la dirección IP del frontend de ALB después de una conmutación por error.

1. Copie la dirección IP del frontend de ALB.



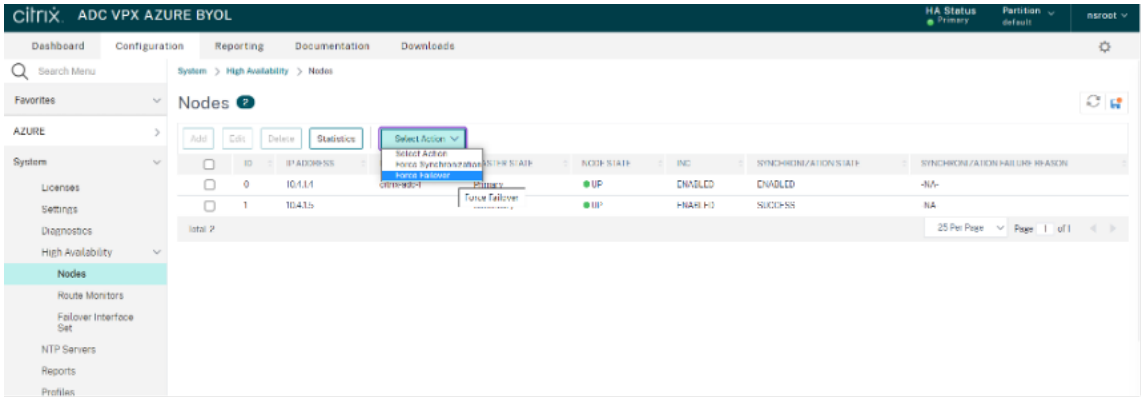
2. Pegue la dirección IP en el explorador y asegúrese de que los servidores back-end estén accesibles.



Welcome to Site1

3. En la instancia principal, realice la conmutación por error:

   En la GUI de Citrix ADC, vaya a **Configuración > Sistema > Alta disponibilidad > Acción > Forzar conmutación por error**.



4. Asegúrese de que los servidores back-end estén accesibles después de la conmutación por error a través de la IP de frontend de ALB utilizada anteriormente.

Configurar una instancia de Citrix ADC VPX para usar redes aceleradas de Azure

August 20, 2021

Las redes aceleradas permiten la tarjeta NIC de función virtual (VF) de virtualización de E/S de raíz única (SR-IOV) en una máquina virtual, lo que mejora el rendimiento de la red. Puede utilizar esta función con cargas de trabajo pesadas que necesitan enviar o recibir datos a un mayor rendimiento con streaming fiable y una menor utilización de la CPU.
Cuando una NIC está habilitada con redes aceleradas, Azure agrupa la interfaz parvirtualizada (PV) existente de la NIC con una interfaz VF SR-IOV. El soporte de la interfaz VF SR-IOV permite y mejora el rendimiento de la instancia Citrix ADC VPX.

Las redes aceleradas ofrecen las siguientes ventajas:

- Latencia inferior
- Mayor rendimiento de paquetes por segundo (pps)
- Rendimiento mejorado
- Fitter reducido
- Disminución del uso de CPU

> Nota
>
> Las redes aceleradas de Azure se admiten en instancias Citrix ADC VPX a partir de la versión 13.0 compilación 76.29 en adelante.

Requisitos previos

- Asegúrese de que el tamaño de su máquina virtual cumple los requisitos de la red acelerada de Azure.
- Detenga las máquinas virtuales (individuales o en un conjunto de disponibilidad) antes de habilitar la red acelerada en cualquier NIC.

Limitaciones

Las redes aceleradas solo se pueden habilitar en algunos tipos de instancias. Para obtener más información, consulte Tipos de instancias compatibles.

NIC compatibles para redes aceleradas

Azure proporciona NIC Mellanox ConnectX3 y ConnectX4 en modo SR-IOV para redes aceleradas.

Cuando se habilita la red acelerada en una interfaz Citrix ADC VPX, Azure agrupa la interfaz ConnectX3 o ConnectX4 con la interfaz fotovoltaica existente de un dispositivo Citrix ADC VPX.

Para obtener más información sobre cómo habilitar redes aceleradas antes de conectar una interfaz a una máquina virtual, consulte Creación de una interfaz de red con redes aceleradas.

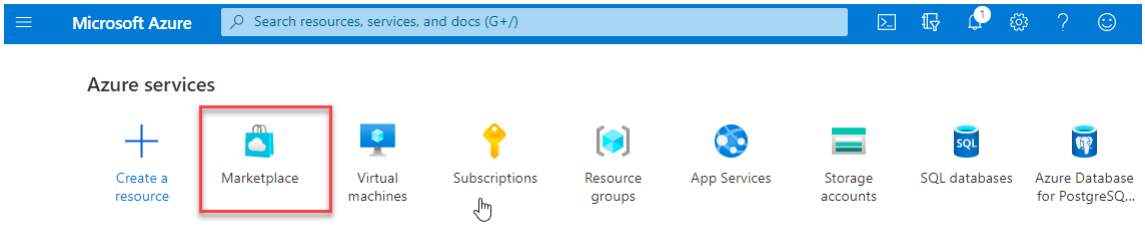
Para obtener más información sobre cómo habilitar redes aceleradas en una interfaz existente de una máquina virtual, consulte Habilitar interfaces existentes en una máquina virtual.

Cómo habilitar la red acelerada en la instancia Citrix ADC VPX mediante la consola de Azure

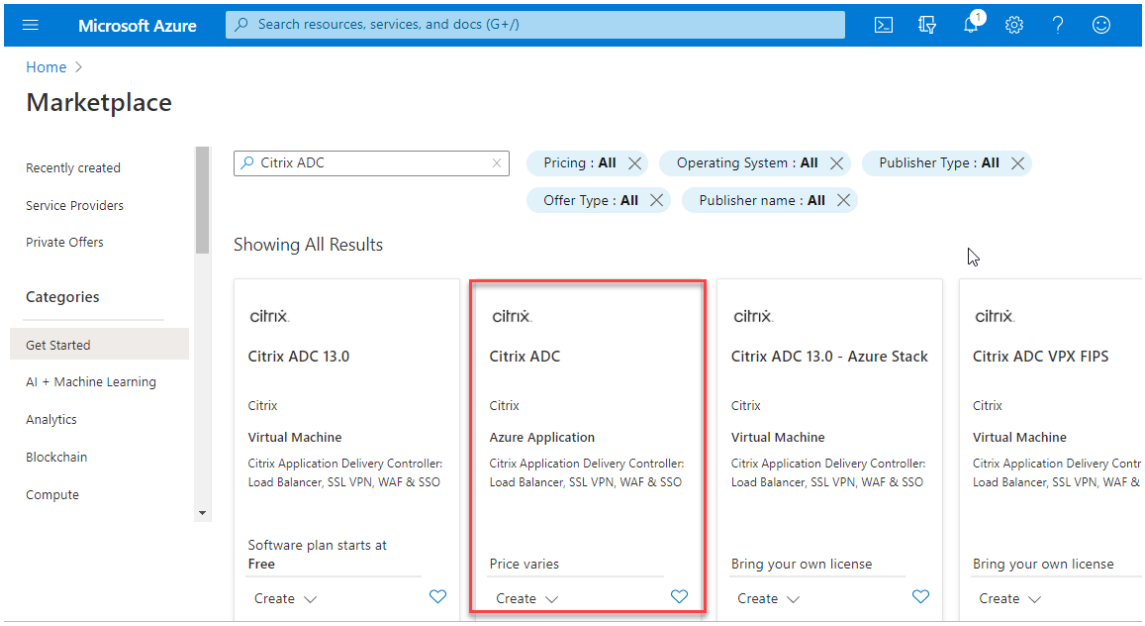
Puede habilitar la red acelerada en una interfaz específica mediante la consola de Azure o Azure PowerShell.

Siga los siguientes pasos para habilitar redes aceleradas mediante conjuntos de disponibilidad o zonas de disponibilidad de Azure.

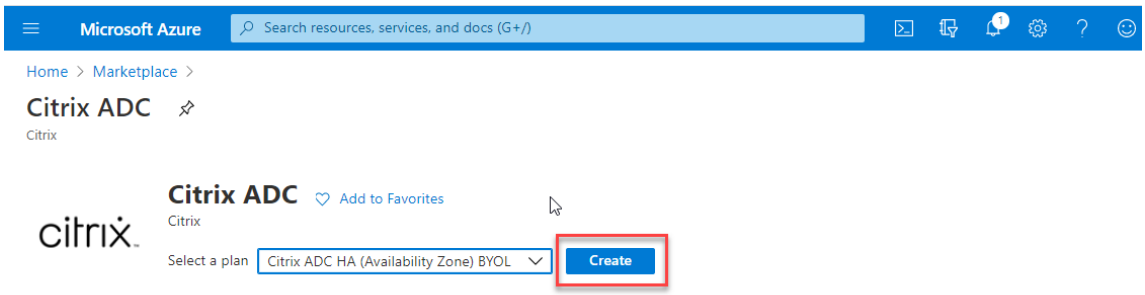
1. Inicie sesión en el portal de Azurey vaya a **Azure Marketplace**.



2. En **Azure Marketplace**, busque **Citrix ADC**.

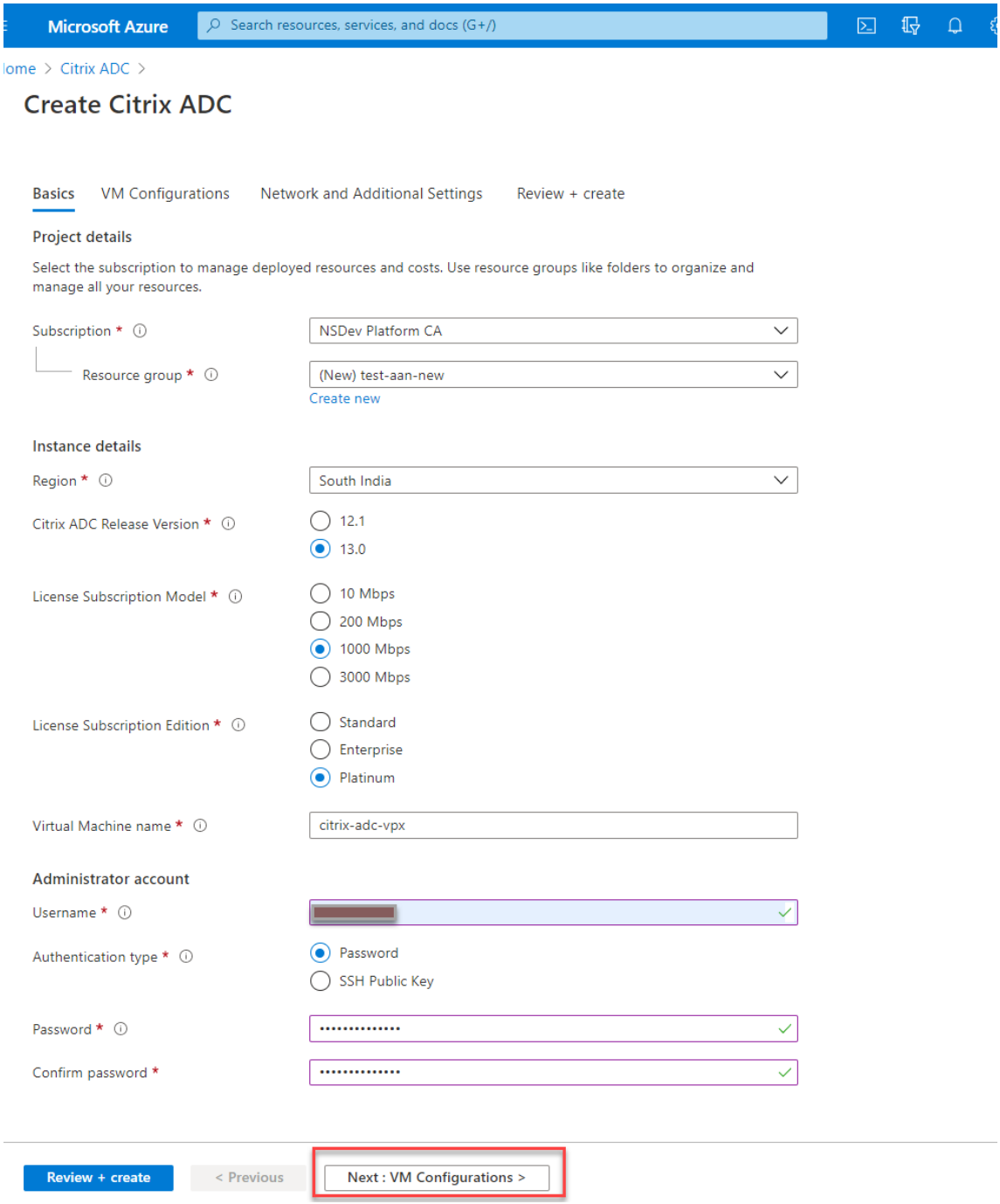


3. Seleccione un plan Citrix ADC que no sea FIPS junto con la licencia y haga clic en **Crear**.



Aparece la página **Crear Citrix ADC** .

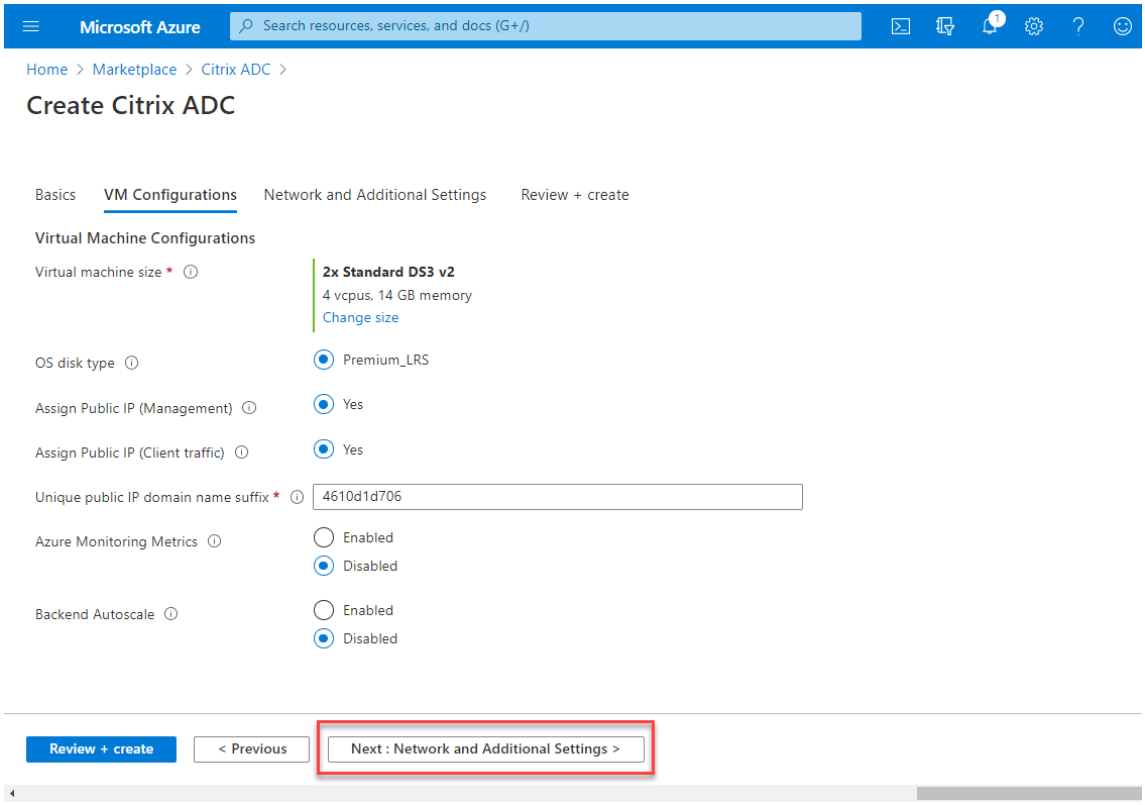
4. En la ficha **Conceptos básicos**, cree un grupo de recursos. En la ficha **Parámetros**, introduce los detalles de la región, el nombre de usuario del administrador, la contraseña de administrador, el tipo de licencia (SKU de máquina virtual) y otros campos.



5. Haga clic en **Siguiente: Configuraciones de VM**.

   En la página **Configuraciones de VM**, realice lo siguiente:

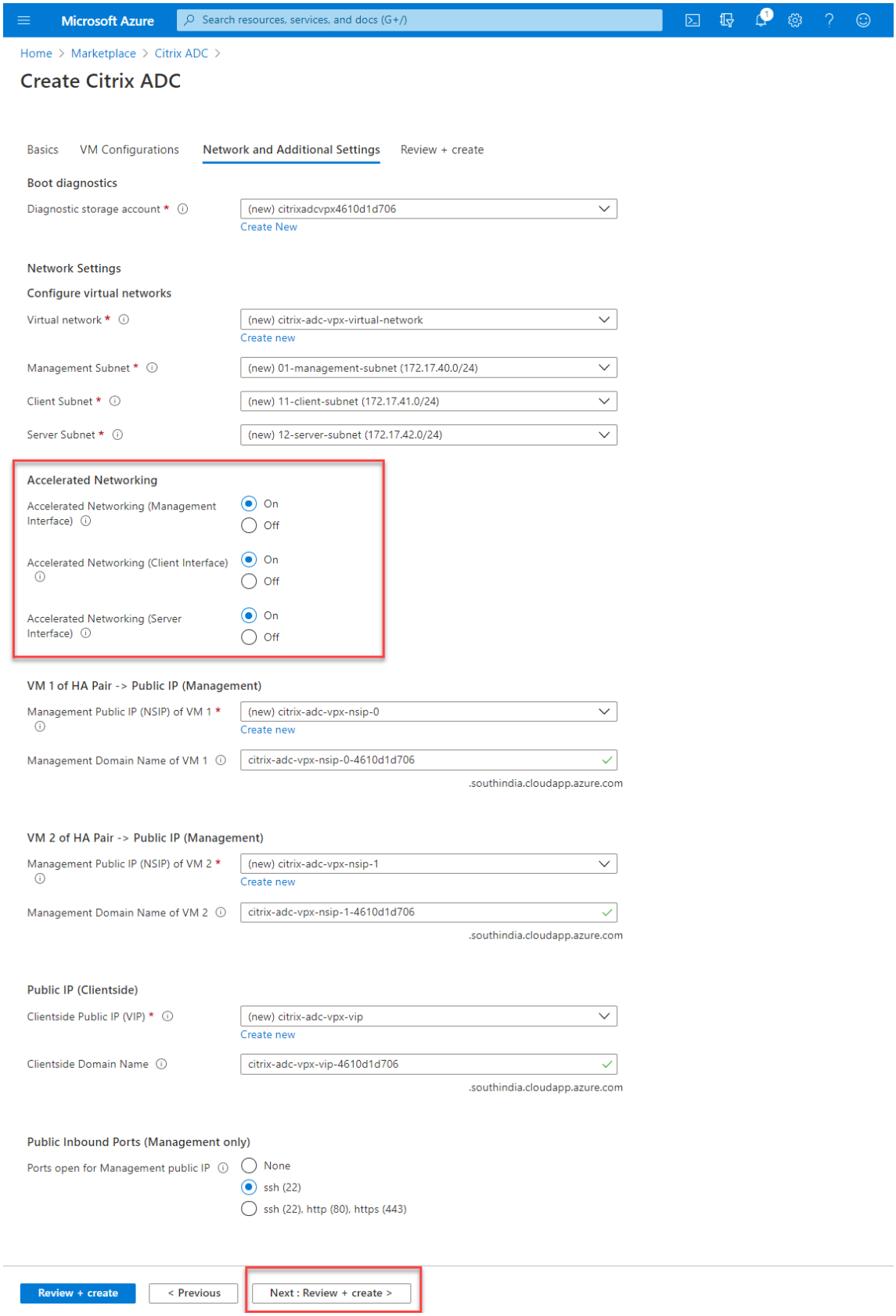
   a) Configure el sufijo de nombre de dominio IP público.
   b) Habilitar o inhabilitar las **métricas de Azure Monitoring**.
   c) Habilitar o inhabilitar la **escalabilidad automática de backend**.



6. Haga clic en **Siguiente: Red y configuración adicional**.

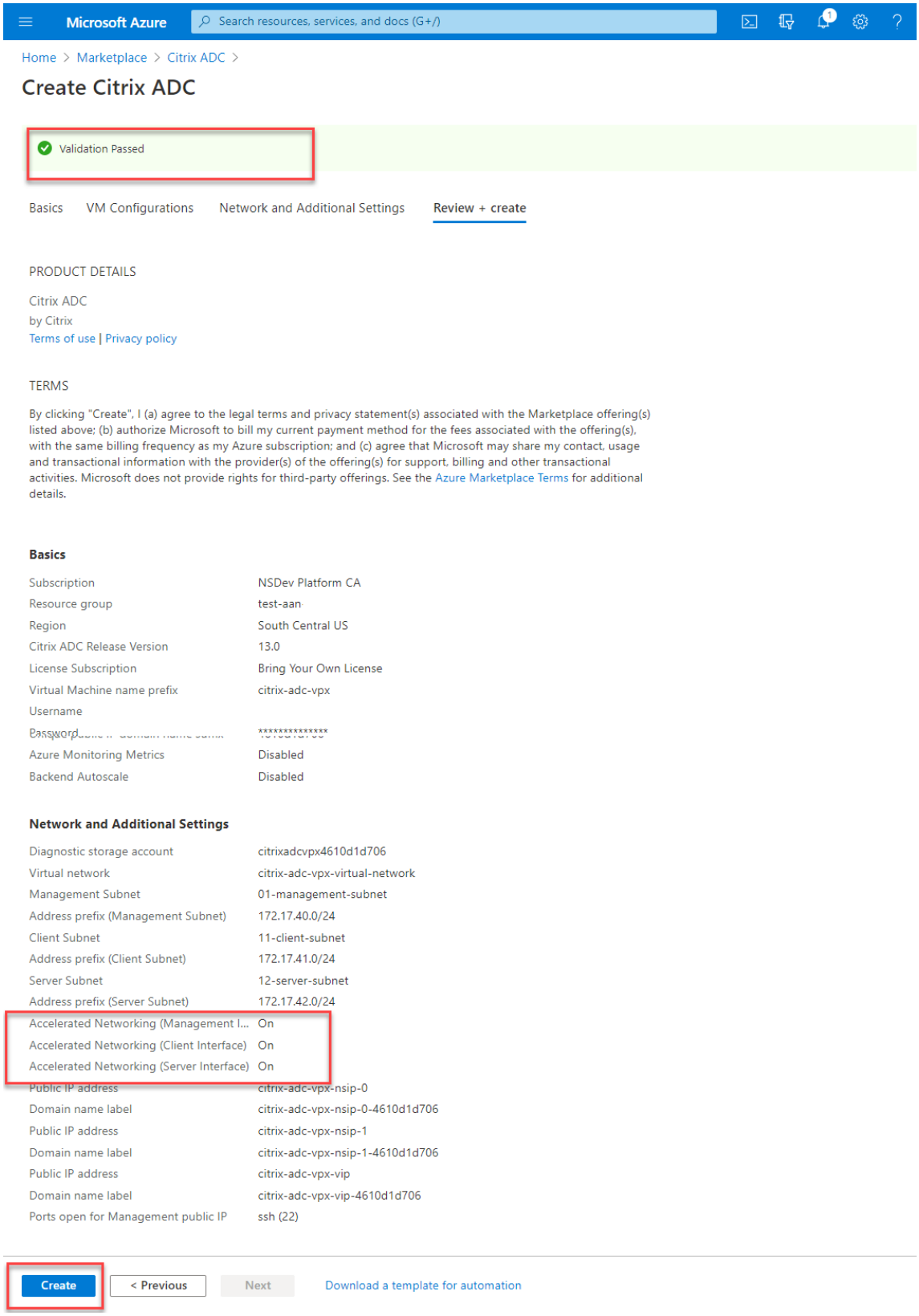
   En la página **Red y Configuración adicional**, cree una cuenta de diagnóstico de arranque y configure los ajustes de red.

   En la sección **Redes aceleradas**, tiene la opción de habilitar o inhabilitar la red acelerada por separado para la interfaz de administración, la interfaz del cliente y la interfaz del servidor.



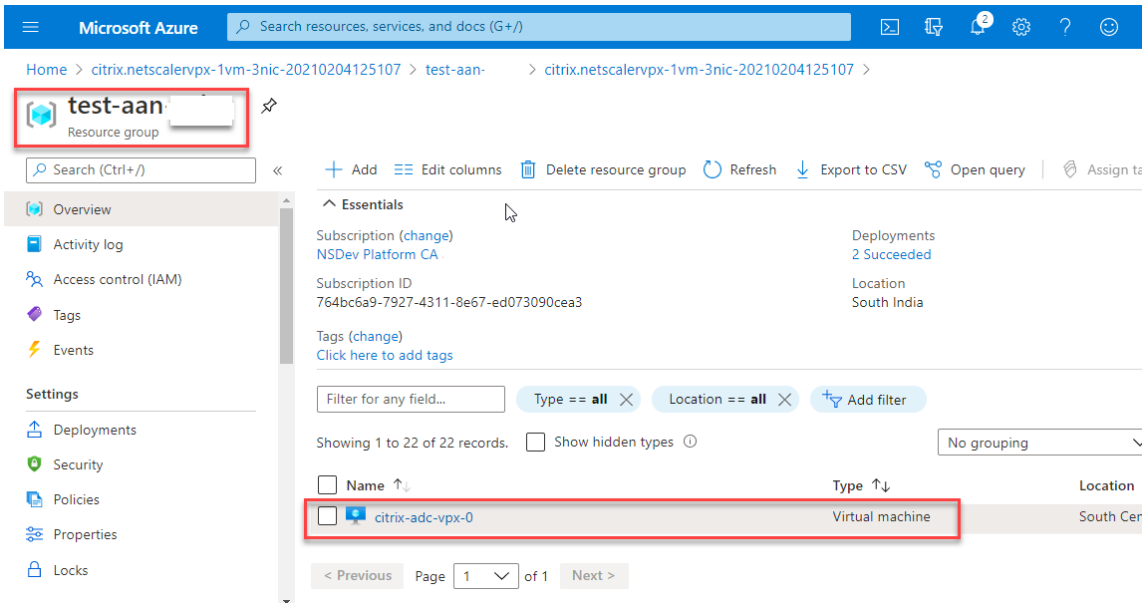
7. Haga clic en **Siguiente: Revisar + crear**.

   Una vez que la validación se haya realizado correctamente, revise la configuración básica, las configuraciones de VM, la red y la configuración adicional y haga clic en **Crear**. El grupo de recursos de Azure puede tardar algún tiempo en crearse con las configuraciones necesarias.

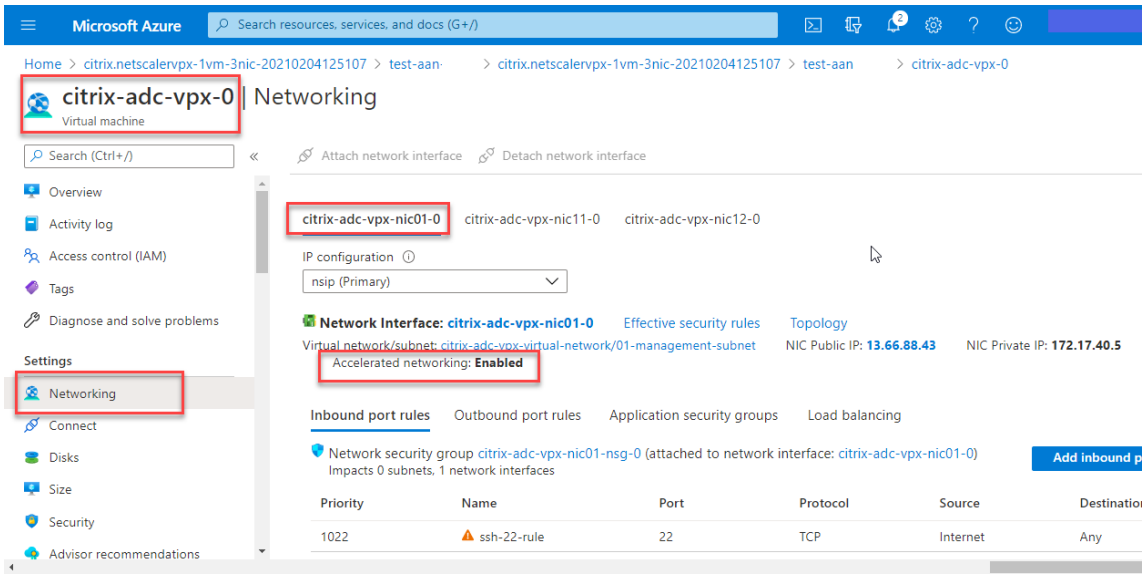


8. Una vez finalizada la implementación, seleccione el **grupo de recursos** para ver los detalles de

configuración.



9. Para verificar las configuraciones de redes aceleradas, seleccione **Máquina virtual > Redes**. El estado Redes aceleradas se muestra como **Habilitado o**Inhabilitado** para cada NIC.



Habilitar redes aceleradas mediante Azure PowerShell

Si necesita habilitar la red acelerada después de la creación de la máquina virtual, puede hacerlo mediante Azure PowerShell.

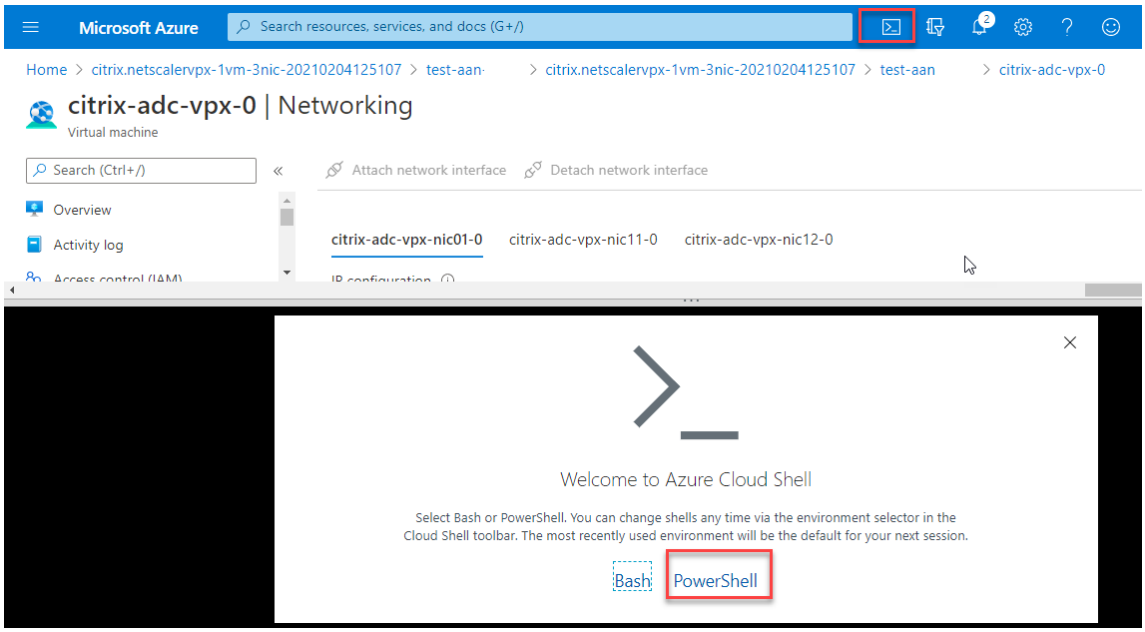
> Nota:
>
> Asegúrese de detener la máquina virtual antes de habilitar la red acelerada mediante Azure Pow-

> erShell.

Lleve a cabo los siguientes pasos para habilitar la red acelerada mediante Azure PowerShell.

1. Vaya al **portal de Azure**y haga clic en el icono de **PowerShell** en la esquina superior derecha.

   > Nota:
   >
   > Si se encuentra en modo Bash, cambie al modo PowerShell.



2. En el símbolo del sistema, ejecute el siguiente comando:

```
az network nic update --name <nic-name> --accelerated-networking [true | false] --resource-group <resourcegroup-name>
<!--NeedCopy-->
```

El parámetro de red acelerada acepta uno de los siguientes valores:

- **True:** habilita la red acelerada en la NIC especificada.
- **False:** inhabilita la red acelerada en la NIC especificada.

Para habilitar redes aceleradas en una NIC específica:

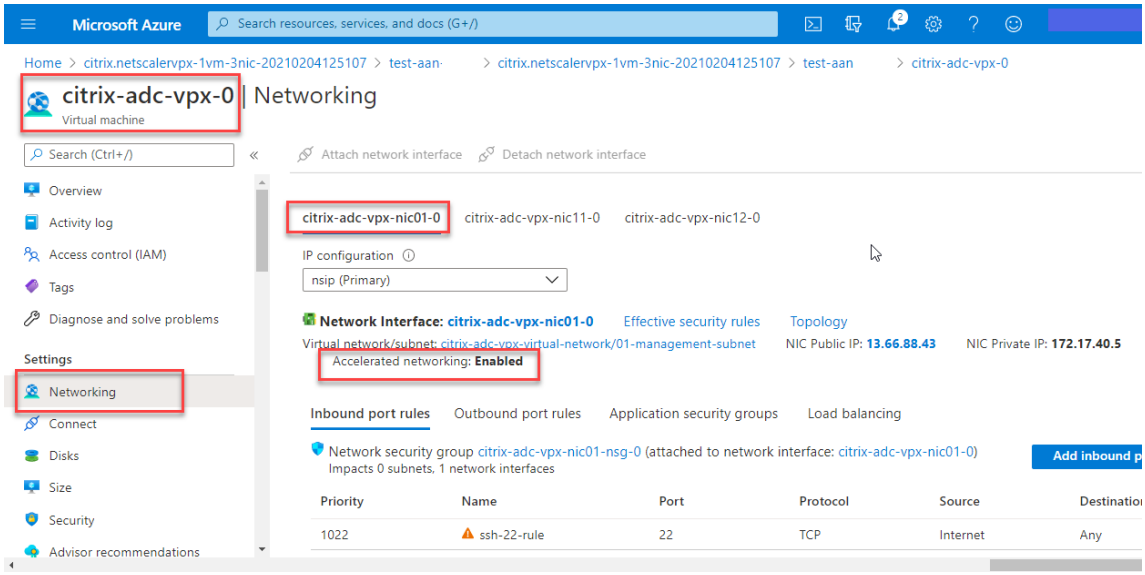
```
az network nic update --name citrix-adc-vpx-nic01-0 --accelerated-networking true --resource-group rsgp1-aan
<!--NeedCopy-->
```

Para inhabilitar la red acelerada en una NIC específica:

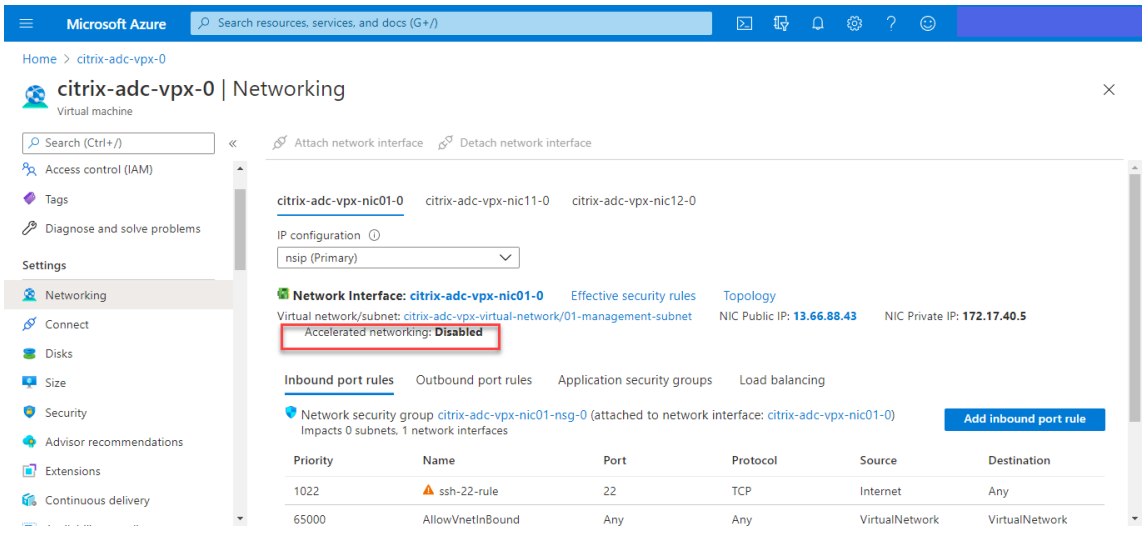

```
az network nic update --name citrix-adc-vpx-nic01-0 --accelerated-networking false --resource-group rsgp1-aan
<!--NeedCopy-->
```

3. Para verificar el estado de las redes aceleradas una vez finalizada la implementación, vaya a **VM > Redes**.

   En el siguiente ejemplo, puede ver que la red acelerada está **habilitada**.



   En el siguiente ejemplo, puede ver que la red acelerada está **inhabilitada**.



Para verificar la aceleración de la red en una interfaz mediante FreeBSD Shell de Citrix ADC

Puede iniciar sesión en el shell de FreeBSD de Citrix ADC y ejecutar los siguientes comandos para verificar el estado de la red acelerada.

Ejemplo de NIC ConnectX3:

En el ejemplo siguiente se muestra el resultado del comando "ifconfig" de la NIC Mellanox ConnectX3. El "50/n" indica las interfaces VF de las NIC Mellanox ConnectX3. 0/1 y 1/1 indican las interfaces fotovoltaicas de la instancia VPX de Citrix ADC VPX. Puede observar que tanto la interfaz fotovoltaica (1/1) como la interfaz VF CX3 (50/1) tienen las mismas direcciones MAC (00:22:48:1 c: 99:3 e). Esto indica que las dos interfaces están agrupadas juntas.


```
root@nvr-us-cx3# ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 1500
        options=3<RXCSUM,TXCSUM>
        inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        nd6 options=3<PERFORMNUD,ACCEPT_RTADV>
0/1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=80019<RXCSUM,VLAN_MTU,VLAN_HWTAGGING,LINKSTATE>
        ether 00:0d:3a:98:71:be
        inet 172.16.27.11 netmask 0xffffff00 broadcast 172.16.27.255
        inet6 fe80::20d:3aff:fe98:71be%0/1 prefixlen 64 autoconf scopeid 0x2
        nd6 options=3<PERFORMNUD,ACCEPT_RTADV>
        media: Ethernet autoselect (10Gbase-T <full-duplex>)
        status: active
1/1: flags=8802<BROADCAST,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=80019<RXCSUM,VLAN_MTU,VLAN_HWTAGGING,LINKSTATE>
        ether 00:22:48:1c:99:3e
        media: Ethernet autoselect (10Gbase-T <full-duplex>)
        status: active
50/1: flags=8842<BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500

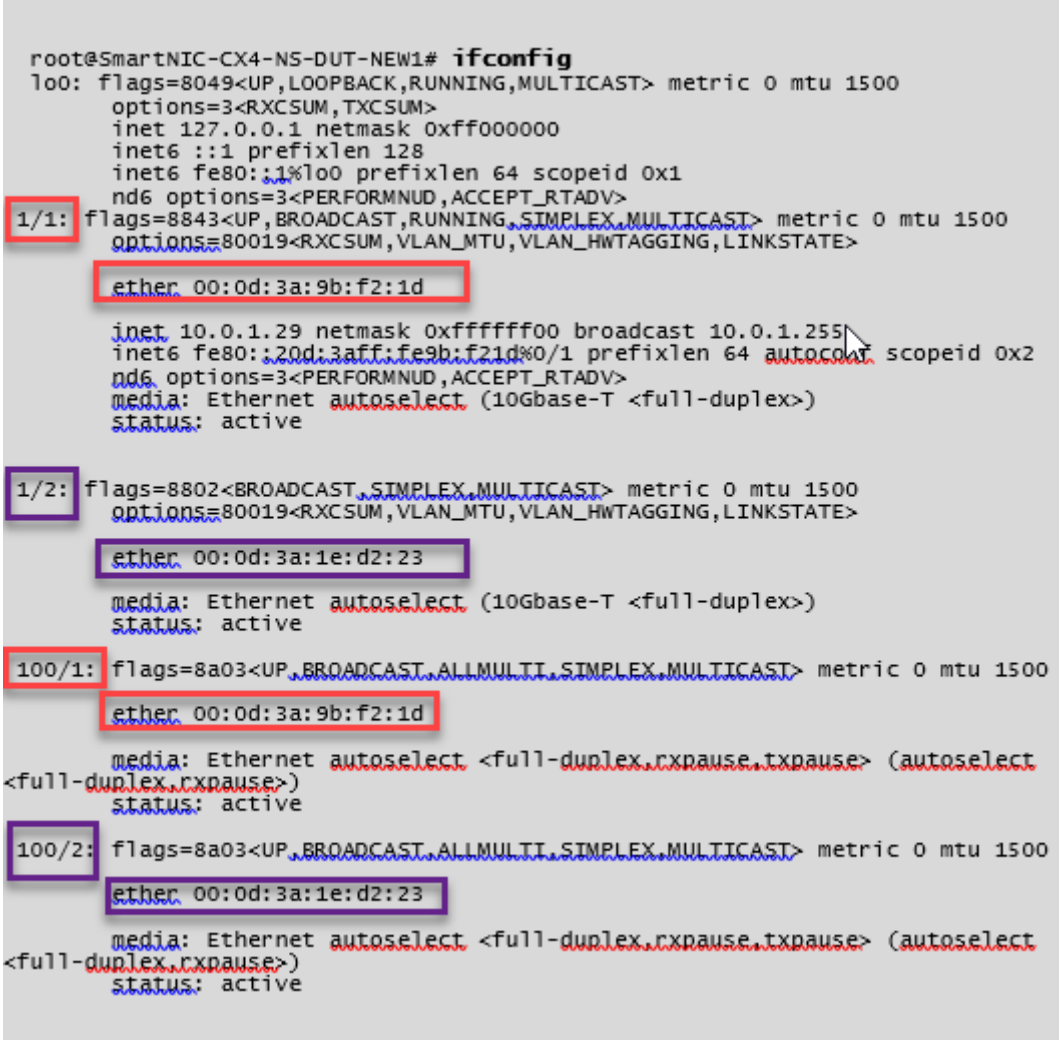
options=900b8<VLAN_MTU,VLAN_HWTAGGING,JUMBO_MTU,VLAN_HWCSUM,VLAN_HWFILTER,LINKSTATE>
        ether 00:22:48:1c:99:3e
        media: Ethernet autoselect (<unknown subtype>)
        status: active
```

Ejemplo de NIC ConnectX4:

En el ejemplo siguiente se muestra el resultado del comando “ifconfig” de la NIC Mellanox ConnectX4. El “100/n” indica las interfaces VF de las NIC Mellanox ConnectX4. 0/1, 1/1 y 1/2 indican las interfaces PV de la instancia Citrix ADC VPX.

Puede observar que tanto la interfaz fotovoltaica (1/1) como la interfaz CX4 VF (100/1) tienen las mismas direcciones MAC (00:0 d:3a:9b:f 2:1 d). Esto indica que las dos interfaces están agrupadas juntas. Del mismo modo, la interfaz fotovoltaica (1/2) y la interfaz CX4 VF (100/2) tienen las mismas direc-

ciones MAC (00:0 d:3a:1e:d 2:23).



Para verificar redes aceleradas en una interfaz mediante la CLI de ADC

Ejemplo de NIC ConnectX3:

El siguiente resultado del comando show interface indica que la interfaz PV 1/1 está incluida con la función virtual 50/1, que es una NIC VF SR-IOV. Las direcciones MAC de las NIC 1/1 y 50/1 son las mismas. Una vez habilitada la red acelerada, los datos de la interfaz 1/1 se envían a través de la ruta de datos de la interfaz 50/1, que es una interfaz ConnectX3. Puede ver que la salida “show interface” de la interfaz fotovoltaica (1/1) apunta al VF (50/1). Del mismo modo, la salida “show interface” de la interfaz VF (50/1) apunta a la interfaz fotovoltaica (1/1).


```
> show interface 1/1

        Interface 1/1 (NetScaler Virtual Interface, SmartNIC, VF 50/1 Datapath 50/1) #1
        flags=0xe060 <ENABLED, UP, UP, HEARTBEAT, 802.1q>
        MTU=1500, native vlan=1, MAC=00:22:48:1c:99:3e, uptime 0h00m07s
        LLDP Mode: NONE,                LR Priority: 1024

        RX: Pkts(0) Bytes(0) Errs(0) Drops(0) Stalls(0)
        TX: Pkts(0) Bytes(0) Errs(0) Drops(0) Stalls(0)
        NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)
        Bandwidth thresholds are not set.

Done

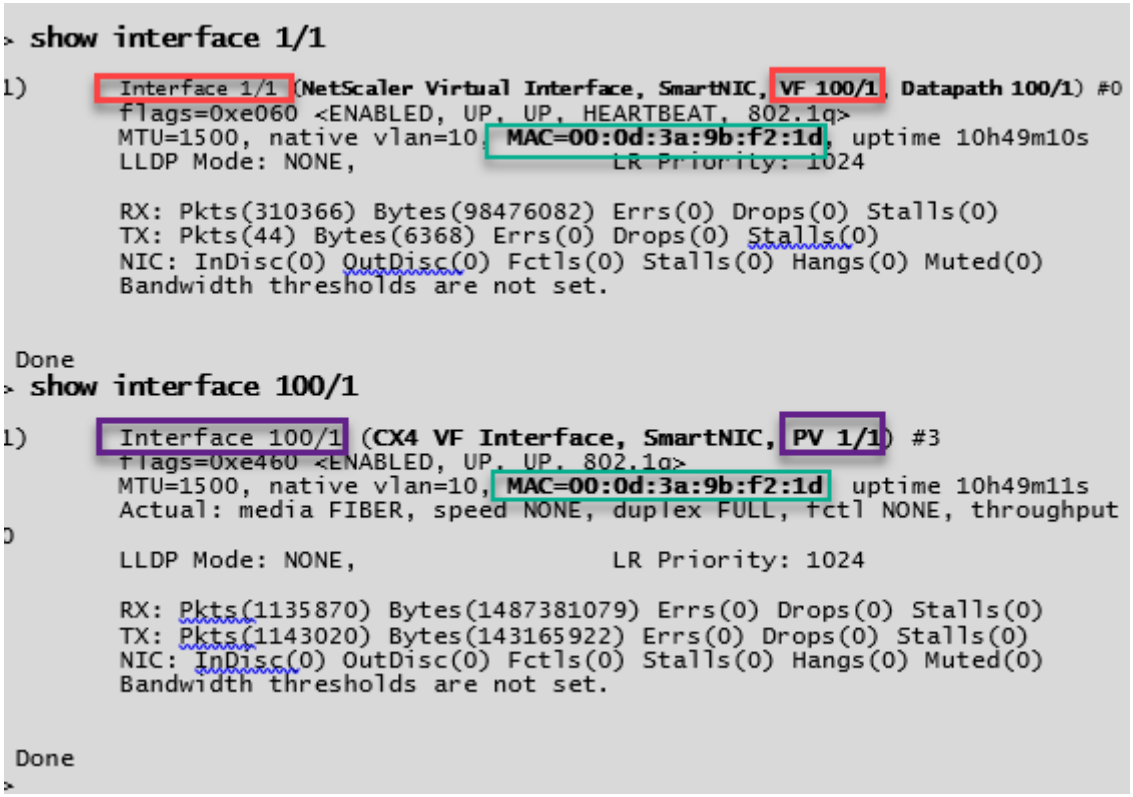
> show interface 50/1

      Interface 50/1 (CX3 VF Interface, SmartNIC, PV 1/1) #2
        flags=0xe460 <ENABLED, UP, UP, 802.1q>
        MTU=1500, native vlan=1, MAC=00:22:48:1c:99:3e, uptime 0h00m08s
        Actual: media NONE, speed 50000, duplex FULL, fctl NONE, throughput 50000
        LLDP Mode: NONE,                LR Priority: 1024

        RX: Pkts(0) Bytes(0) Errs(0) Drops(0) Stalls(0)
        TX: Pkts(0) Bytes(0) Errs(0) Drops(0) Stalls(0)
        NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)
        Bandwidth thresholds are not set.
```

Ejemplo de NIC ConnectX4:

El siguiente resultado del comando show interface indica que la interfaz PV 1/1 está incluida con la función virtual 100/1, que es una NIC VF SR-IOV. Las direcciones MAC de las NIC 1/1 y 100/1 son las mismas. Una vez habilitada la red acelerada, los datos de la interfaz 1/1 se envían a través de la ruta de datos de la interfaz 100/1, que es una interfaz ConnectX4. Puede ver que la salida “show interface” de la interfaz fotovoltaica (1/1) apunta al VF (100/1). Del mismo modo, la salida “show interface” de la interfaz VF (100/1) apunta a la interfaz fotovoltaica (1/1).



Puntos a tener en cuenta en Citrix ADC

- La interfaz fotovoltaica se considera la interfaz principal o principal para todas las operaciones necesarias. Las configuraciones deben realizarse únicamente en interfaces fotovoltaicas.
- Todas las operaciones de “set” en una interfaz VF están bloqueadas excepto las siguientes:
  - habilitar interfaz
  - inhabilitar interfaz
  - interfaz de reinicio
  - estadísticas claras

  > Nota:
  >
  > Citrix recomienda que no realice ninguna operación en la interfaz VF.

- Puede verificar la vinculación de la interfaz fotovoltaica con la interfaz VF mediante el `show interface` comando.

Configurar una VLAN en una interfaz fotovoltaica

Cuando una interfaz fotovoltaica está enlazada a una VLAN, la interfaz VF acelerada asociada también se enlaza a la misma VLAN que la interfaz fotovoltaica. En este ejemplo, la interfaz fotovoltaica (1/1)

está enlazada a VLAN (20). La interfaz VF (100/1) que se incluye con la interfaz fotovoltaica (1/1) también está enlazada a la VLAN 20.

Ejemplo:

1. Cree una VLAN.

```
add vlan 20
<!--NeedCopy-->
```

2. Enlazar una VLAN a la interfaz PV.

```
bind vlan 20  - ifnum 1/1

show vlan

1)  VLAN ID: 1
    Link-local IPv6 addr: fe80::20d:3aff:fe9b:f21d/64
    Interfaces : LO/1

2)  VLAN ID: 10     VLAN Alias Name:
    Interfaces : 0/1 100/1
    IPs : 10.0.1.29  Mask: 255.255.255.0

3)  VLAN ID: 20     VLAN Alias Name:
    Interfaces :  1/1 100/2

<!--NeedCopy-->
```

> Nota
>
> No se permite la operación de enlace de VLAN en una interfaz VF acelerada.

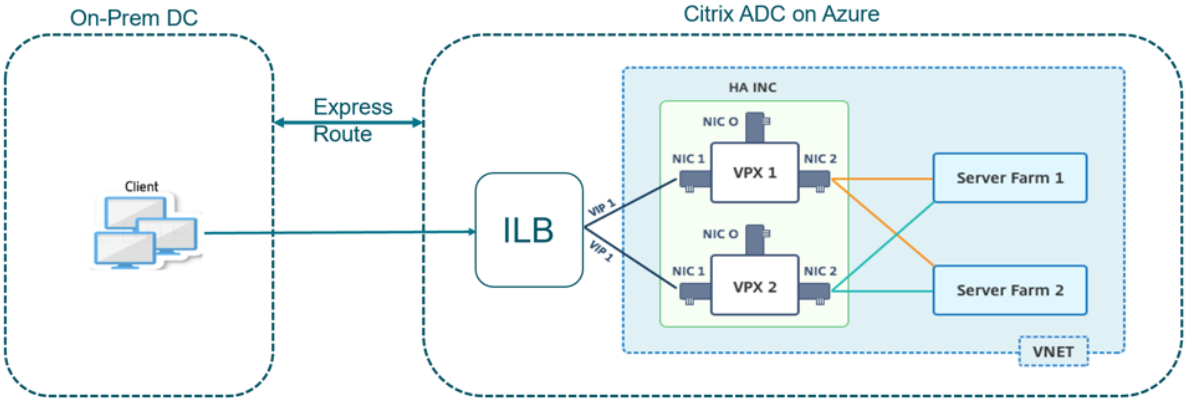
```
bind vlan 1 -ifnum 100/1
ERROR: Operation not permitted
<!--NeedCopy-->
```


Configurar nodos HA-INC mediante la plantilla de alta disponibilidad de Citrix con Azure ILB

January 21, 2022

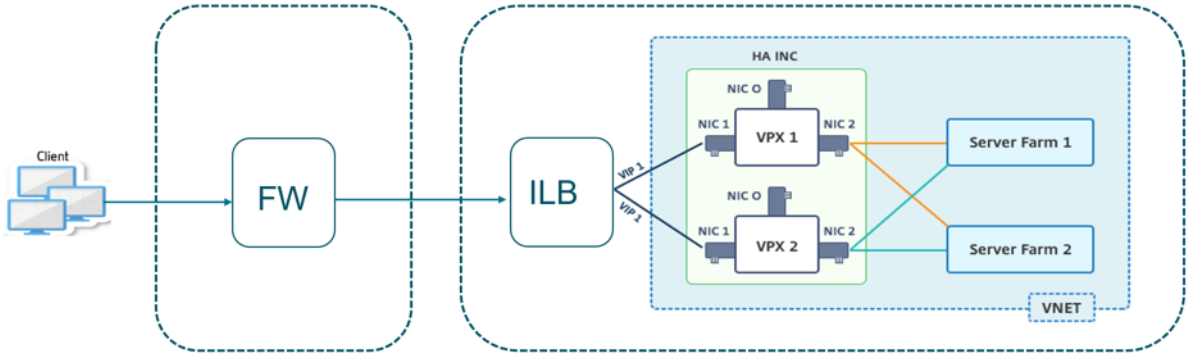
Puede implementar de forma rápida y eficiente un par de instancias VPX en modo HA-INC mediante la plantilla estándar para aplicaciones de intranet. El equilibrador de carga interna (ILB) de Azure utiliza una dirección IP interna o privada para el front-end, como se muestra en la Ilustración 1. La plantilla crea dos nodos, con tres subredes y seis NIC. Las subredes son para el tráfico de administración, del cliente y del lado del servidor, y cada subred pertenece a una NIC diferente en cada dispositivo.

Ilustración 1: Par de Citrix ADC HA para clientes de una red interna



También puede utilizar esta implementación cuando el par de Citrix ADC HA está detrás de un firewall, como se muestra en la Ilustración 2. La dirección IP pública pertenece al firewall y es NAT a la dirección IP del front-end del ILB.

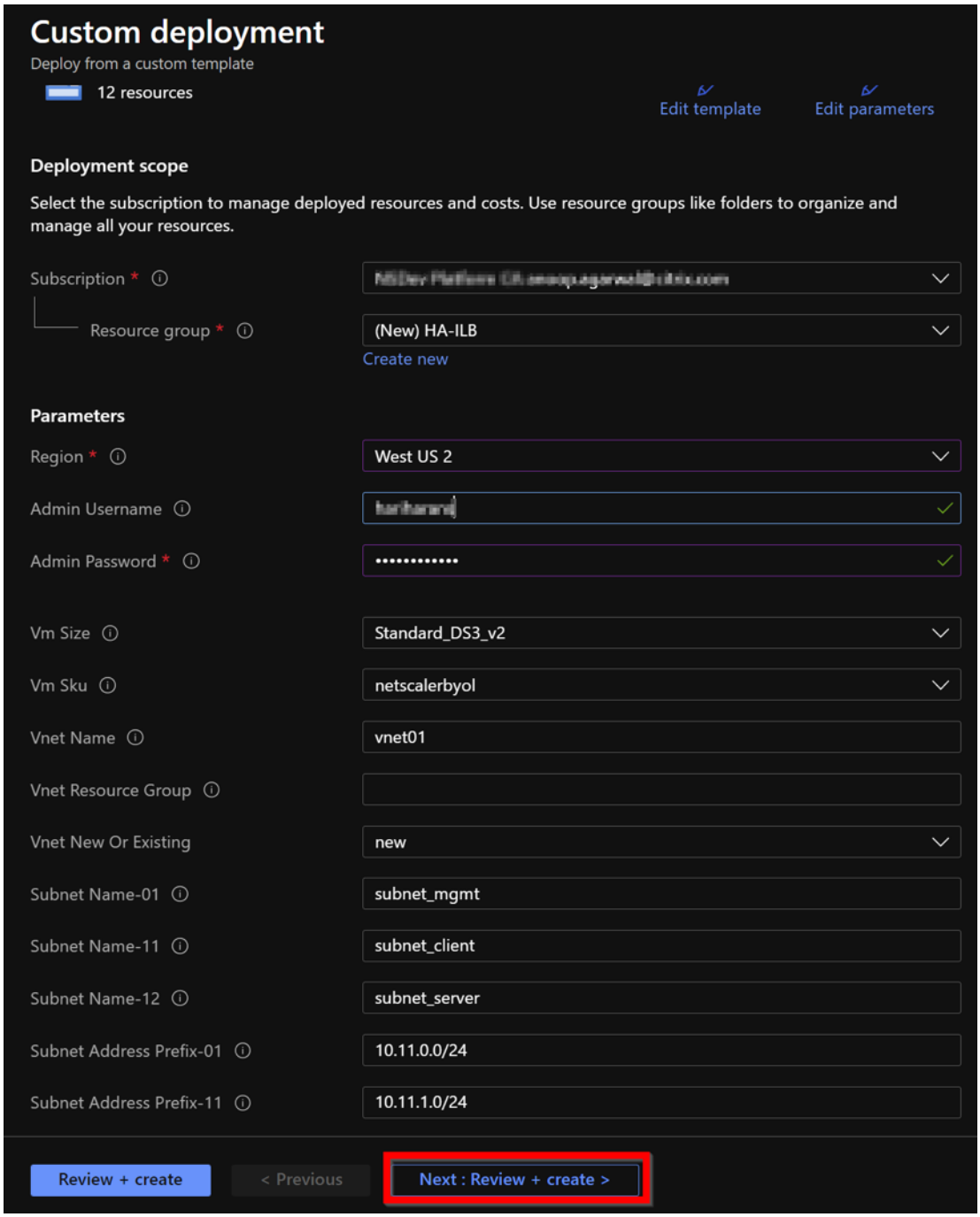
Ilustración 2: Citrix ADC HA emparejar con firewall con dirección IP pública



Puede obtener la plantilla de par de alta disponibilidad de Citrix ADC para aplicaciones de intranet en el portal de Azure

Complete los pasos siguientes para iniciar la plantilla e implementar un par VPX de alta disponibilidad mediante los conjuntos de disponibilidad de Azure.

1. En el portal de Azure, vaya a la página **Implementación personalizada**.
2. Aparecerá la página **Básicos**. Cree un grupo de recursos. En la ficha **Parámetros**, introduzca los detalles de la región, el nombre de usuario de administrador, la contraseña de administrador, el tipo de licencia (`VM sku`) y otros campos.

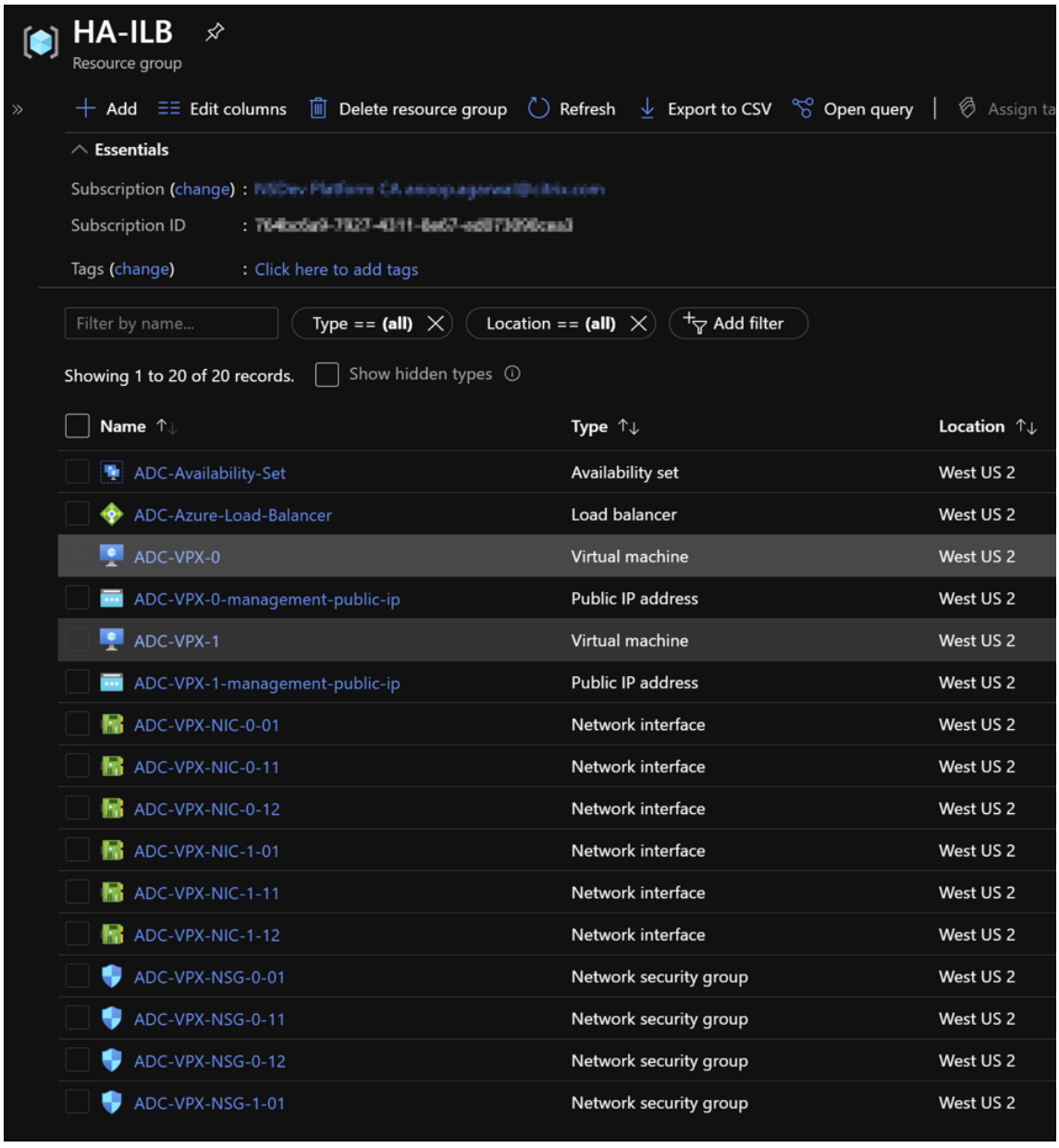


3. Haga clic en **Siguiente: Revisar y crear >**.

Es posible que el Azure Resource Group demore un momento en crearse con las configuraciones requeridas. Una vez finalizado, seleccione el grupo de recursos en el portal de Azure para ver los detalles de configuración, como reglas de LB, grupos de back-end, sondeos de estado. El par de alta disponibilidad aparece como ADC-VPX-0 y ADC-VPX-1.

Si se requieren más modificaciones para la configuración de HA, como la creación de más reglas de seguridad y puertos, puede hacerlo desde el portal de Azure.

Una vez completada la configuración requerida, se crean los siguientes recursos.

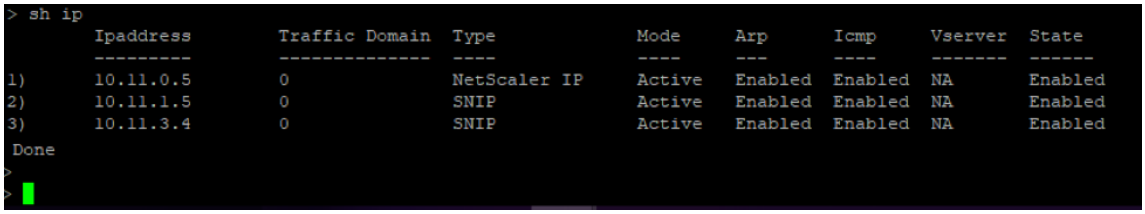


4. Inicie sesión en los nodos **ADC-VPX-0** y **ADC-VPX-1** para validar la siguiente configuración:
   - Las direcciones NSIP de ambos nodos deben estar en la subred de administración.

- En los nodos principal (ADC-VPX-0) y secundario (ADC-VPX-1), debe ver dos direcciones SNIP. Un SNIP (subred cliente) se usa para responder a las sondas de ILB y el otro SNIP (subred del servidor) se usa para la comunicación del servidor back-end.

> Nota
>
> En el modo HA-INC, la dirección de SNIP de las máquinas virtuales ADC-VPX-0 y ADC-VPX-1 son diferentes mientras se encuentran en la misma subred, a diferencia de la implementación clásica de ADC de alta disponibilidad local donde ambas son iguales.
> Para admitir implementaciones cuando el SNIP del par VPX se encuentra en subredes diferentes o cuando el VIP no esté en la misma subred que un SNIP, debe habilitar el reenvío basado en Mac (MBF) o agregar una ruta de host estática para cada VIP a cada nodo VPX.

En el nodo principal (ADC-VPX-0)



```
> sh ip
        Ipaddress        Traffic Domain  Type            Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----            ----     ---      ----     -------  ------
1)      10.11.0.5        0               NetScaler IP    Active   Enabled  Enabled  NA       Enabled
2)      10.11.1.5        0               SNIP            Active   Enabled  Enabled  NA       Enabled
3)      10.11.3.4        0               SNIP            Active   Enabled  Enabled  NA       Enabled
 Done
>
>
```



```
> sh ha node
1)      Node ID:      0
        IP:       10.11.0.5 (ADC-VPX-0)
        Node State: UP
        Master State: Primary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: ENABLED
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
        Sync Status Strict Mode: DISABLED
        Hello Interval: 200 msecs
        Dead Interval: 3 secs
        Node in this Master State for: 0:0:20:26 (days:hrs:min:sec)
2)      Node ID:      1
        IP:       10.11.0.4
        Node State: UP
        Master State: Secondary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: SUCCESS
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
 Done
>
```

En el nodo secundario (ADC-VPX-1)

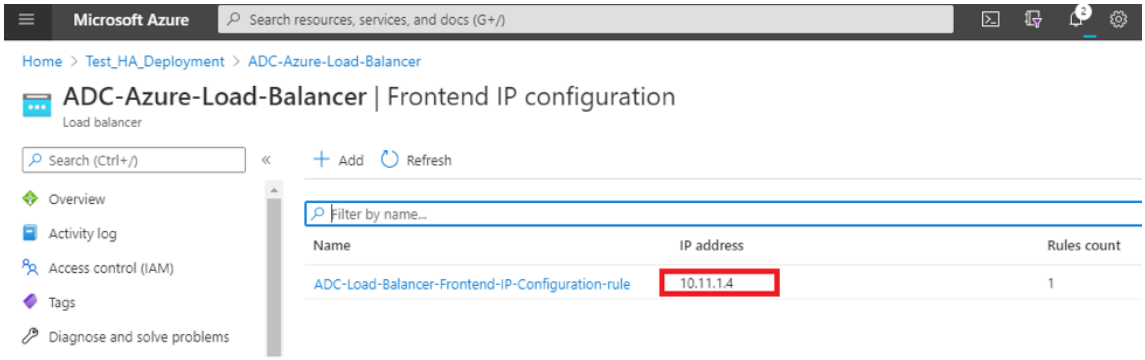
```
> sh ip
       Ipaddress        Traffic Domain  Type            Mode     Arp      Icmp     Vserver  State
       ---------        --------------  ----            ----     ---      ----     -------  ------
1)     10.11.0.4        0               NetScaler IP    Active   Enabled  Enabled  NA       Enabled
2)     10.11.1.6        0               SNIP            Active   Enabled  Enabled  NA       Enabled
3)     10.11.3.5        0               SNIP            Active   Enabled  Enabled  NA       Enabled
 Done
>
>
```



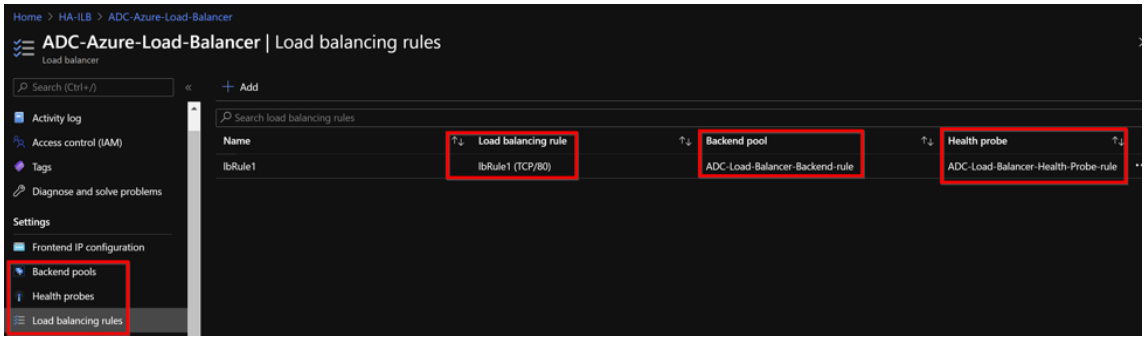
```
> sh ha node
1)      Node ID:      0
        IP:       10.11.0.4 (ADC-VPX-1)
        Node State: UP
        Master State: Secondary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: SUCCESS
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
        Sync Status Strict Mode: DISABLED
        Hello Interval: 200 msecs
        Dead Interval: 3 secs
        Node in this Master State for: 0:0:24:18 (days:hrs:min:sec)
2)      Node ID:      1
        IP:       10.11.0.5
        Node State: UP
        Master State: Primary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: ENABLED
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
 Done
>
```

5. Después de que los nodos principal y secundario estén ACTIVADOS y el estado de sincronización sea **SUCCESS**, debe configurar el servidor virtual de equilibrio de carga o el servidor virtual de puerta de enlace en el nodo principal (ADC-VPX-0) con la dirección IP flotante privada (FIP) del equilibrador de carga ADC Azure. Para obtener más información, consulte la sección Configuración de ejemplo.

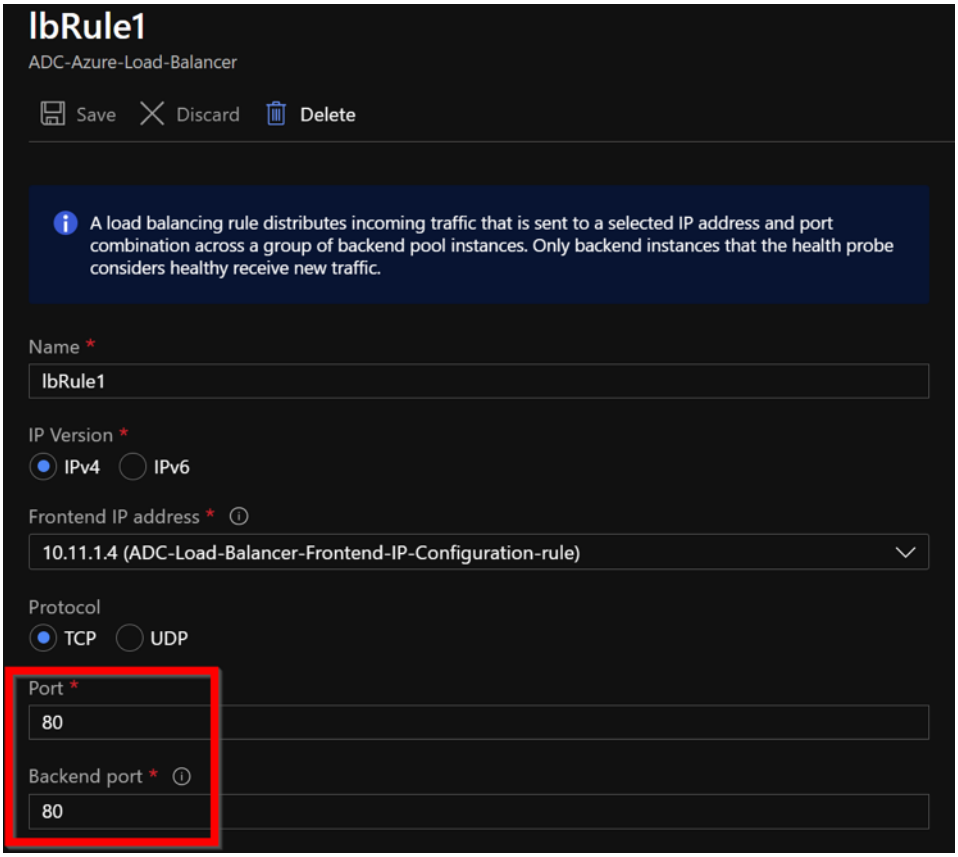
6. Para buscar la dirección IP privada del equilibrador de carga de ADC Azure, vaya a **Azure Portal > Equilibrador de carga de Azure ADC > Configuración de IP de frontend**.



7. En la página de configuración de **Azure Load Balancer**, la implementación de la plantilla ARM ayuda a crear la regla de LB, grupos de back-end y sondeos de estado.

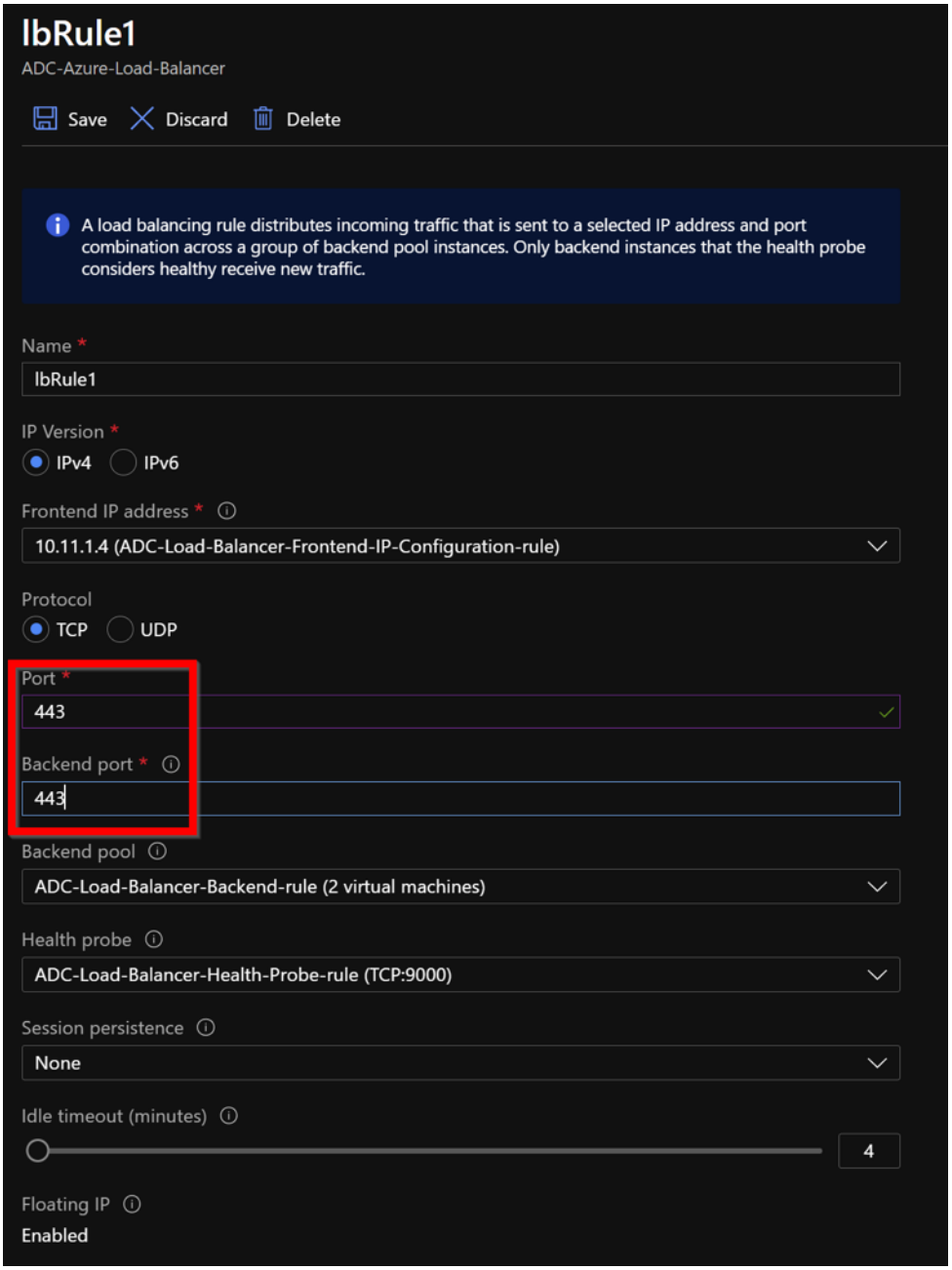


   - La regla LB (LBrule1) usa el puerto 80, de forma predeterminada.



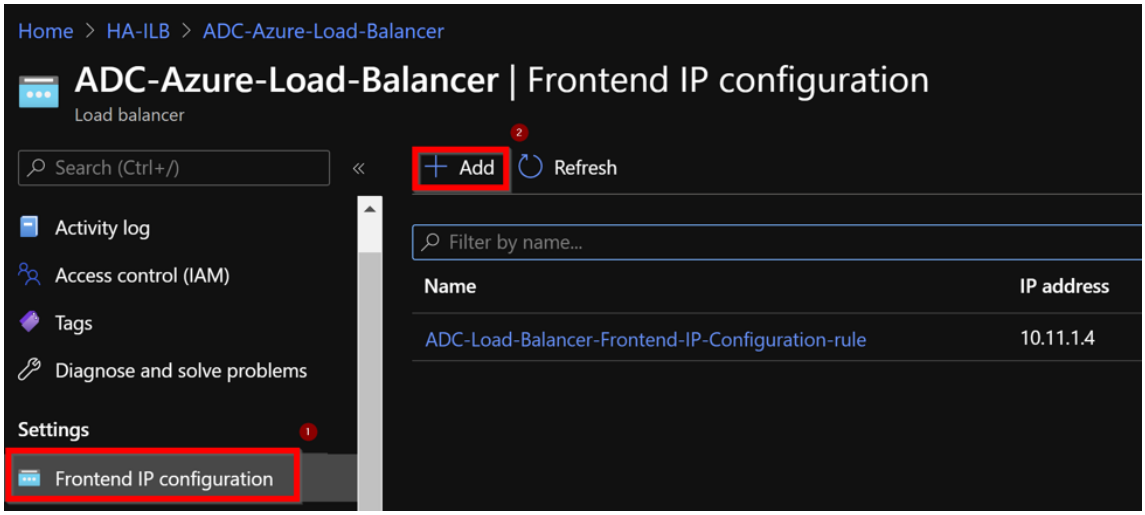
- Modifique la regla para usar el puerto 443 y guarde los cambios.

> Nota
>
> Para mejorar la seguridad, Citrix recomienda utilizar el puerto SSL 443 para el servidor virtual LB o el servidor virtual Gateway.

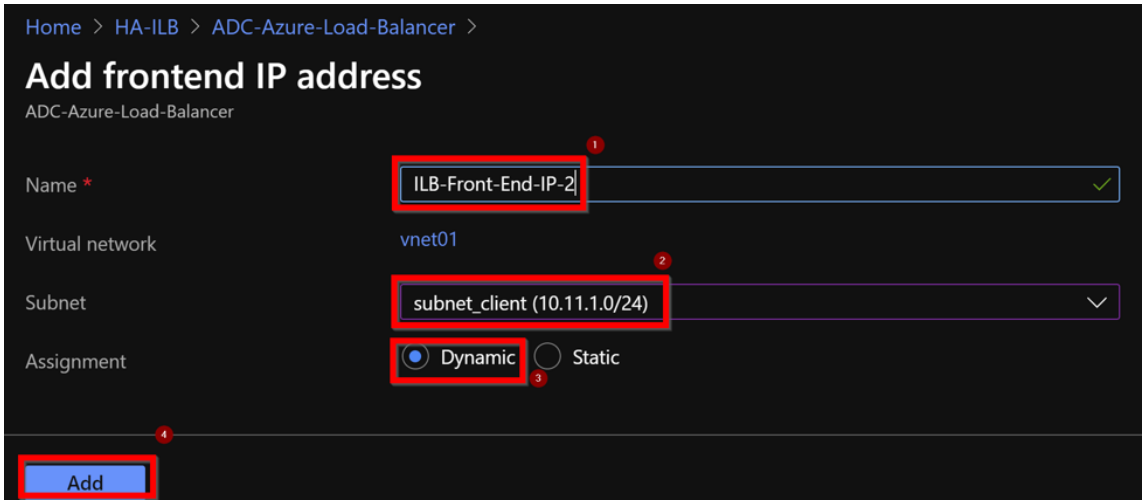


Para agregar más direcciones VIP en el ADC, lleve a cabo los siguientes pasos:

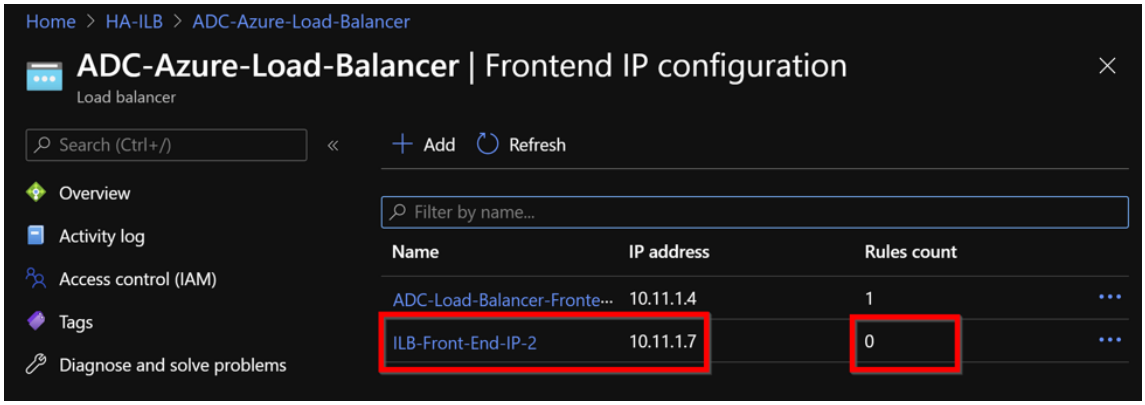
1. Vaya a **Azure Load Balancer > Configuración de IP de frontend** y haga clic en **Agregar** para crear una nueva dirección IP del equilibrador de carga interno.



2. En la página **Agregar dirección IP frontend**, introduce un nombre, elige la subred del cliente, asigna una dirección IP dinámica o estática y haga clic en **Agregar**.

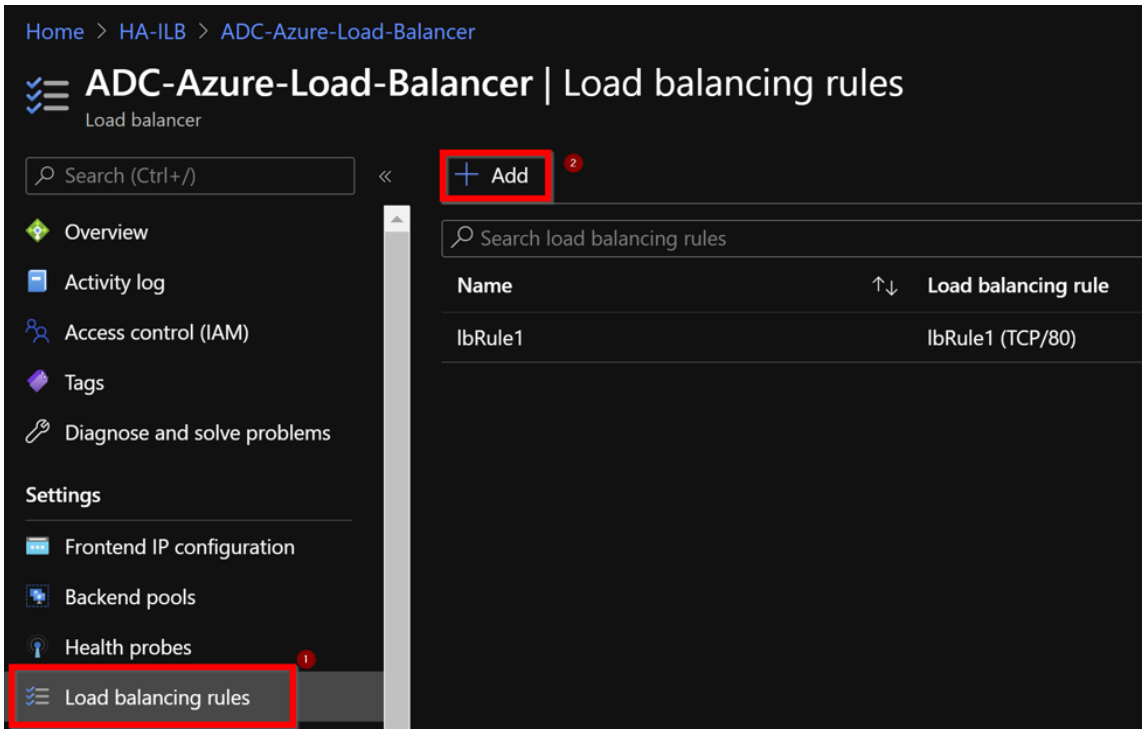


3. La dirección IP de front-end se crea pero no se asocia una regla de LB. Crea una nueva regla de equilibrio de carga y asocia a la dirección IP del front-end.

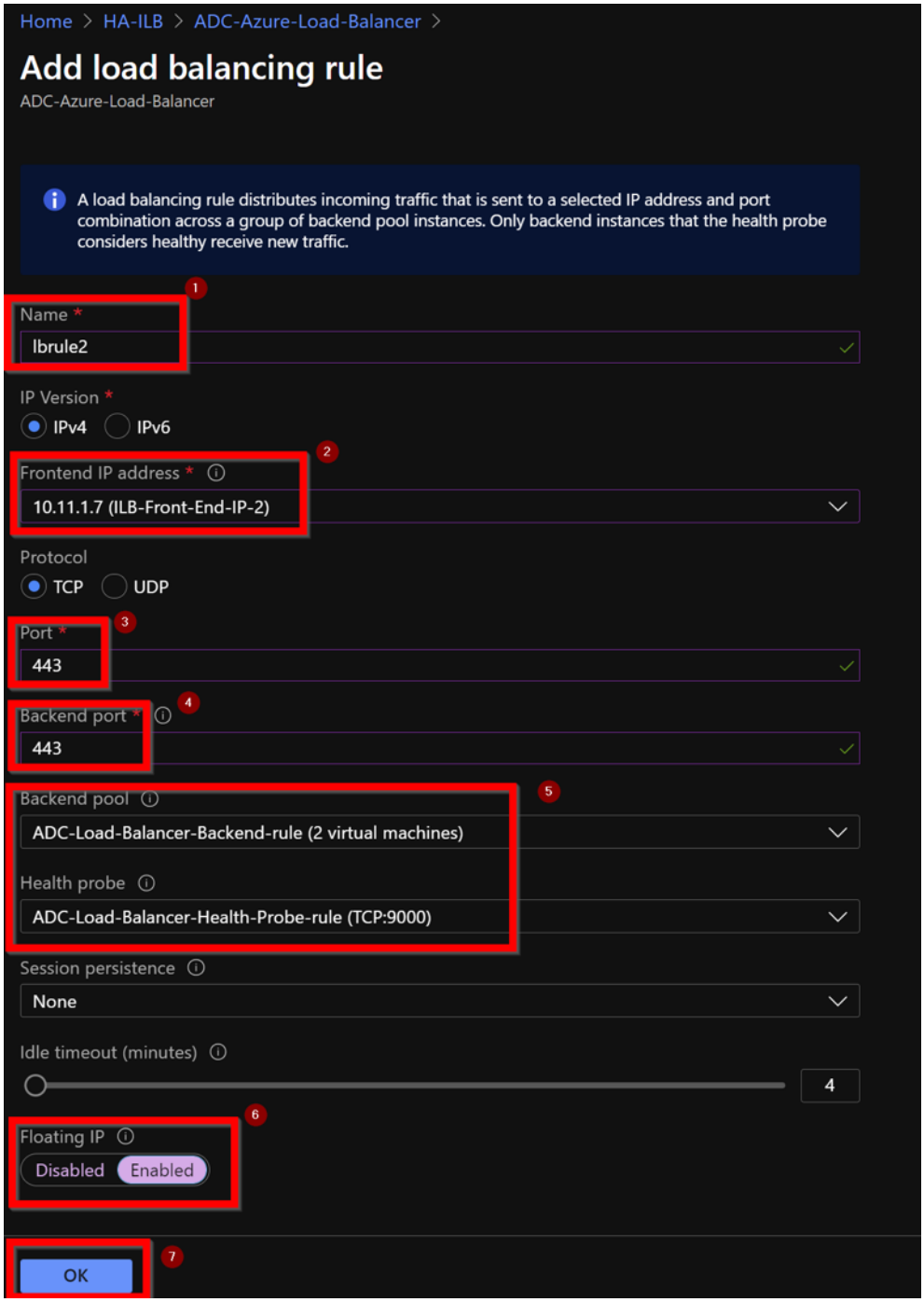


4. En la página **Azure Load Balancer**, seleccione **Reglas de equilibrio de carga** y, a continuación,

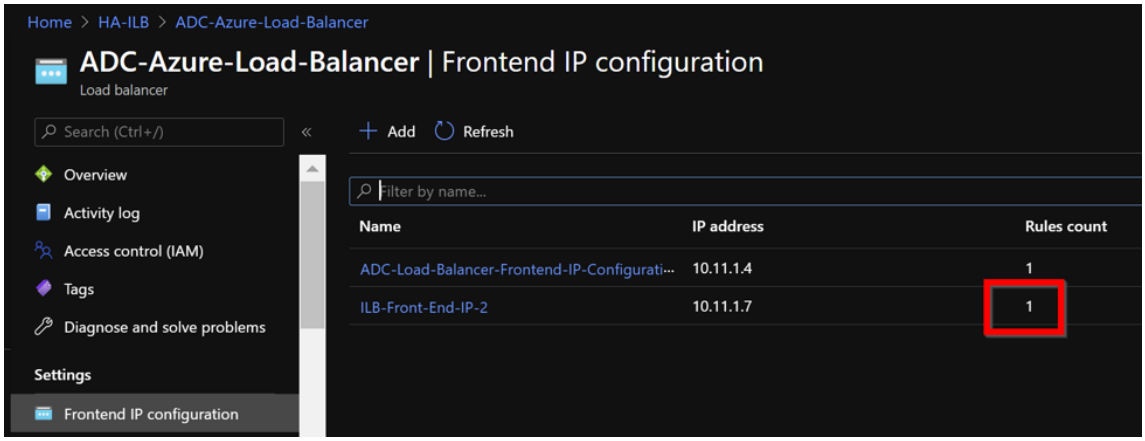
haga clic en **Agregar**.



5. Cree una nueva regla de LB eligiendo la nueva dirección IP de front-end y el puerto. El campo**IP flotante** debe establecerse en **Habilitado**.



6. Ahora la **configuración de IP frontend** muestra la regla LB que se aplica.



Configuración de ejemplo

Para configurar un servidor virtual VPN de puerta de enlace y un servidor virtual de equilibrio de carga, ejecute los siguientes comandos en el nodo principal (ADC-VPX-0). La configuración se sincroniza automáticamente con el nodo secundario (ADC-VPX-1).

Configuración de ejemplo de gateway

```
enable feature aaa LB SSL SSLVPN
enable ns mode MBF
add vpn vserver vpn_ssl SSL 10.11.1.4 443
add ssl certKey ckp -cert wild-cgwsanity.cer -key wild-cgwsanity.key
bind ssl vserver vpn_ssl -certkeyName ckp
<!--NeedCopy-->
```

Configuración de muestra de equilibrio de carga

```
enable feature LB SSL
enable ns mode MBF
add lb vserver lb_vs1 SSL 10.11.1.7 443
bind ssl vserver lb_vs1 -certkeyName ckp
<!--NeedCopy-->
```

Ahora puede acceder al servidor virtual de equilibrio de carga o VPN mediante el nombre de dominio completo (FQDN) asociado a la dirección IP interna del ILB.

Consulte la sección **Recursos** para obtener más información sobre cómo configurar el servidor virtual de equilibrio de carga.

Recursos:

Los siguientes enlaces proporcionan información adicional relacionada con la implementación de alta disponibilidad y la configuración del servidor virtual:

- Configuración de nodos de alta disponibilidad en diferentes subredes
- Configurar el equilibrio de carga básico

Recursos relacionados:

- Configurar una configuración de alta disponibilidad con varias direcciones IP y NIC mediante comandos de PowerShell
- Configuración de GSLB en la implementación de HA activa en espera en Azure

Configurar nodos HA-INC mediante la plantilla de alta disponibilidad de Citrix para aplicaciones con conexión a Internet

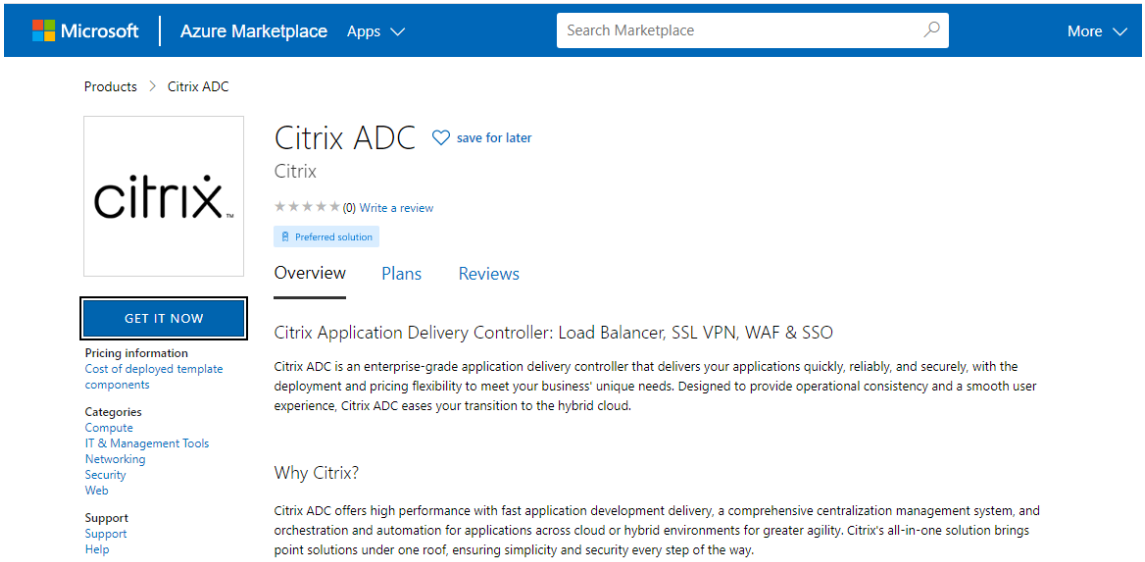
December 2, 2021

Puede implementar de forma rápida y eficiente un par de instancias VPX en modo HA-INC mediante la plantilla estándar para aplicaciones orientadas a Internet. El equilibrador de carga de Azure (ALB) utiliza una dirección IP pública para el front-end. La plantilla crea dos nodos, con tres subredes y seis NIC. Las subredes son para tráfico de administración, cliente y servidor. Cada subred tiene dos NIC para ambas instancias VPX.

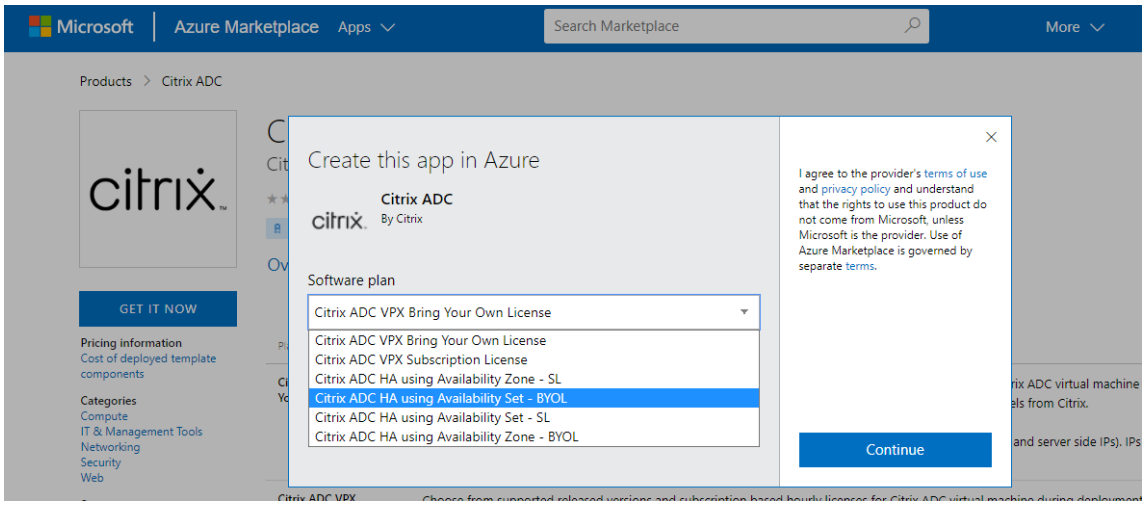
Puede obtener la plantilla de par Citrix ADC HA para aplicaciones orientadas a Internet en Azure Marketplace.

Complete los pasos siguientes para iniciar la plantilla e implementar un par VPX de alta disponibilidad mediante conjuntos de disponibilidad de Azure o zona de disponibilidad.

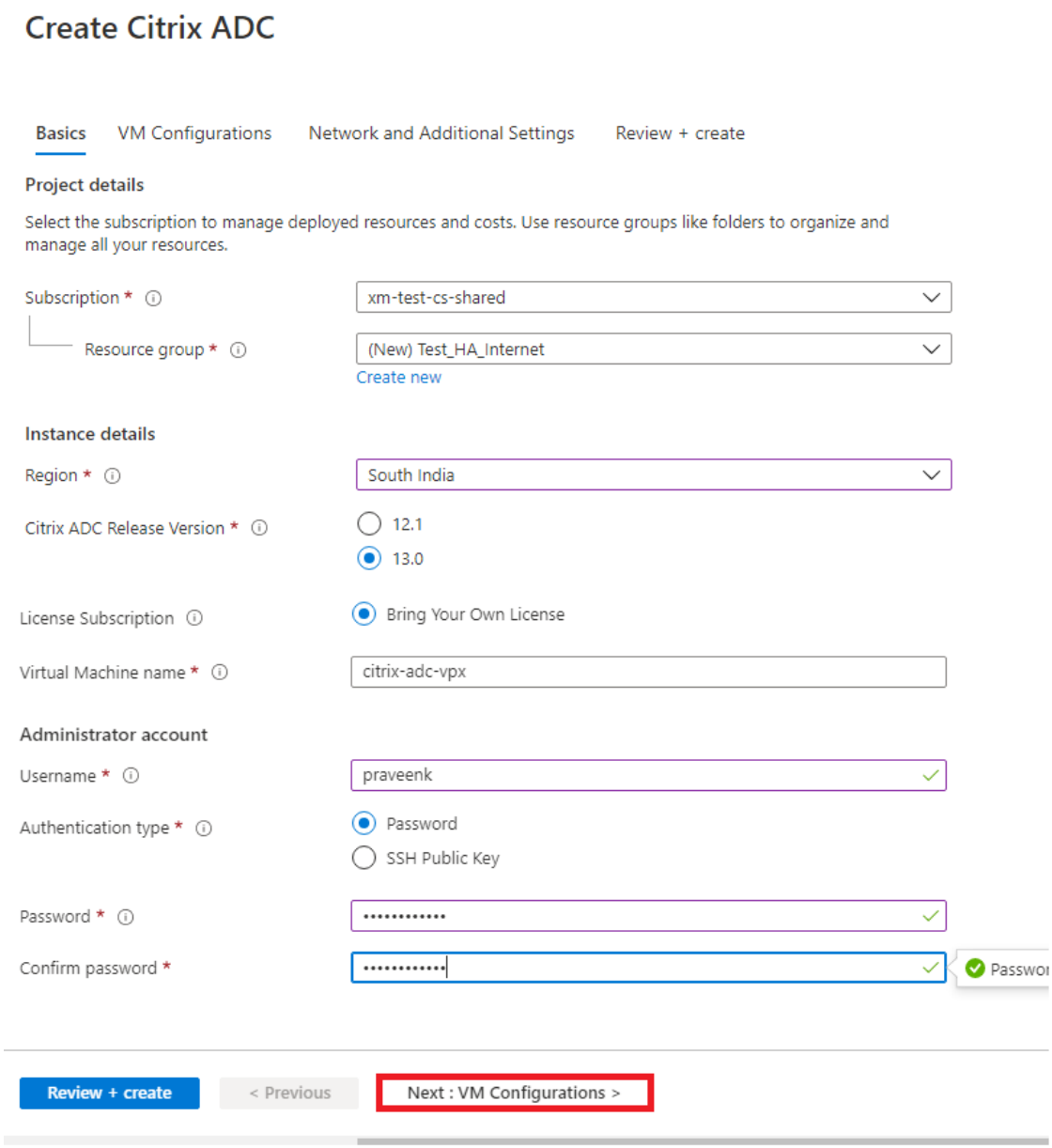
1. En Azure Marketplace, busque en **Citrix ADC**.
2. Haga clic en **OBTENER AHORA**.



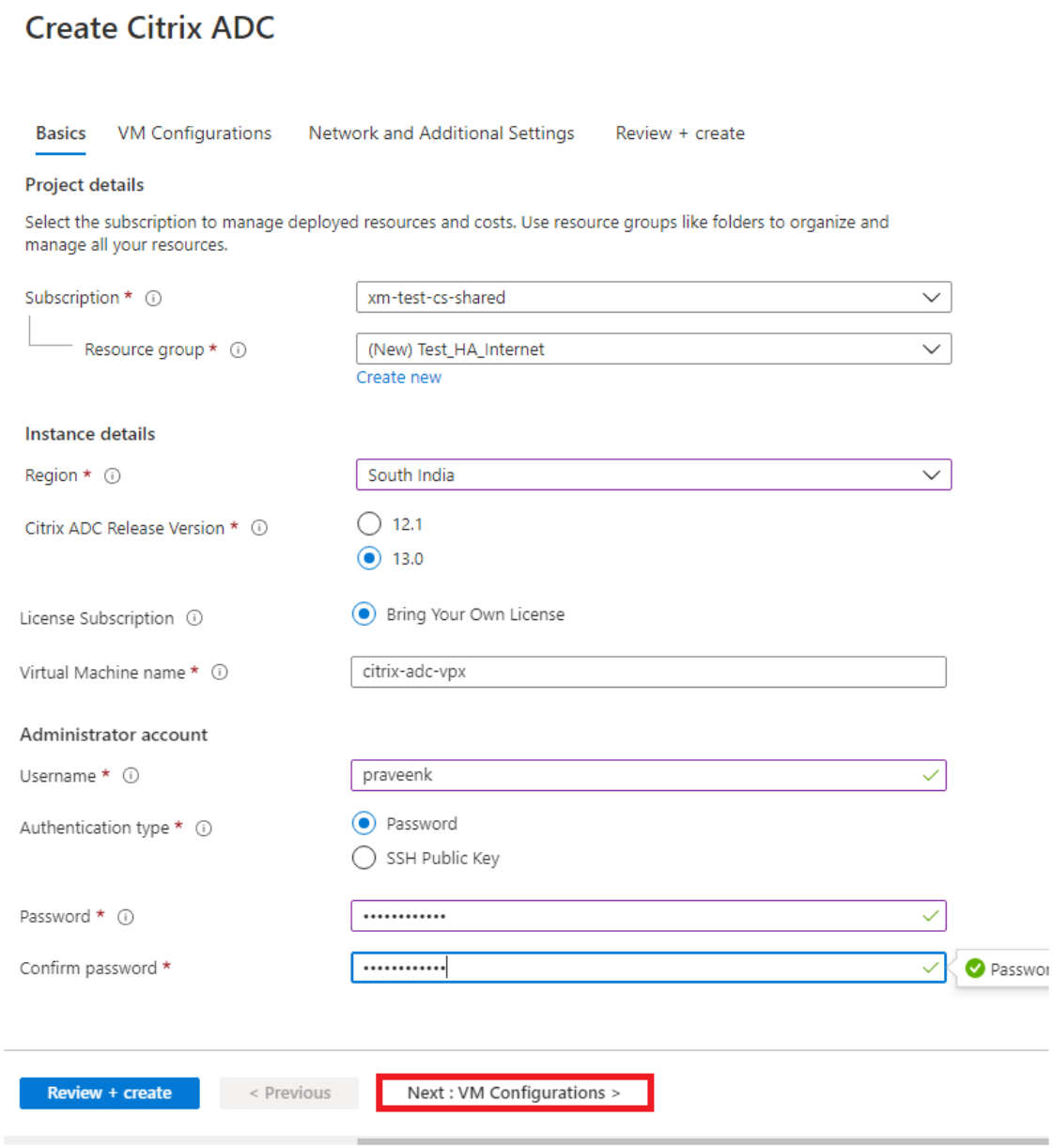
3. Seleccione la implementación de alta disponibilidad requerida junto con la licencia y haga clic en **Continuar**.



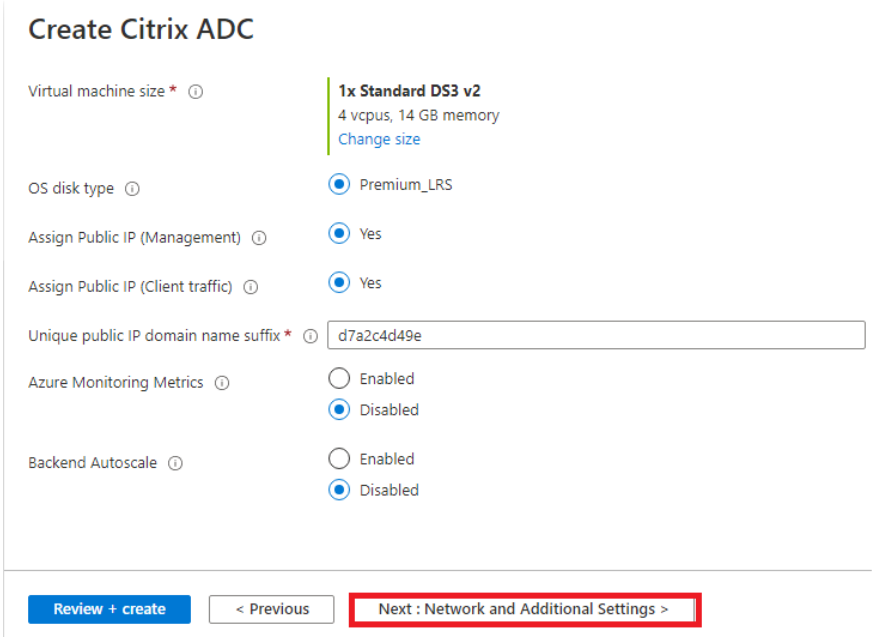
4. Aparecerá la página **Básicos**. Cree un grupo de recursos. En la ficha **Parámetros**, introduce los detalles de la región, el nombre de usuario del administrador, la contraseña de administrador, el tipo de licencia (SKU de máquina virtual) y otros campos.



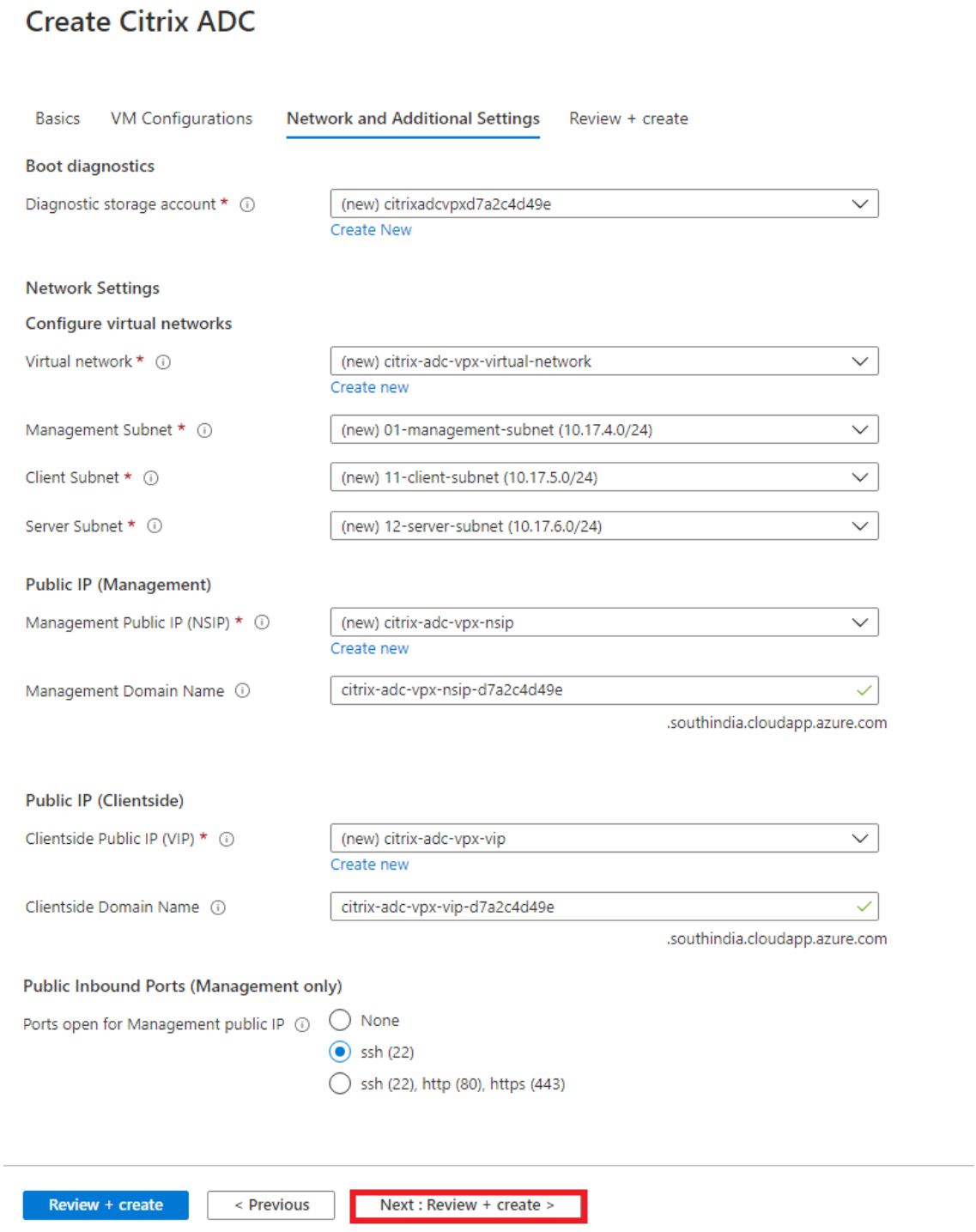
5. Haga clic en **Siguiente: Configuraciones de VM**.



6. En la página **Configuraciones de VM**, realice lo siguiente:
   - Configurar sufijo de nombre de dominio IP público
   - Habilitar o inhabilitar las **métricas de supervisión de Azure**
   - Habilitar o inhabilitar la **escala automática de back-end**
7. Haga clic en **Siguiente: Configuración de red y adicional**



8. En la página **Configuración de red y adicionales**, cree una cuenta de diagnóstico de arranque y configure la configuración de red.

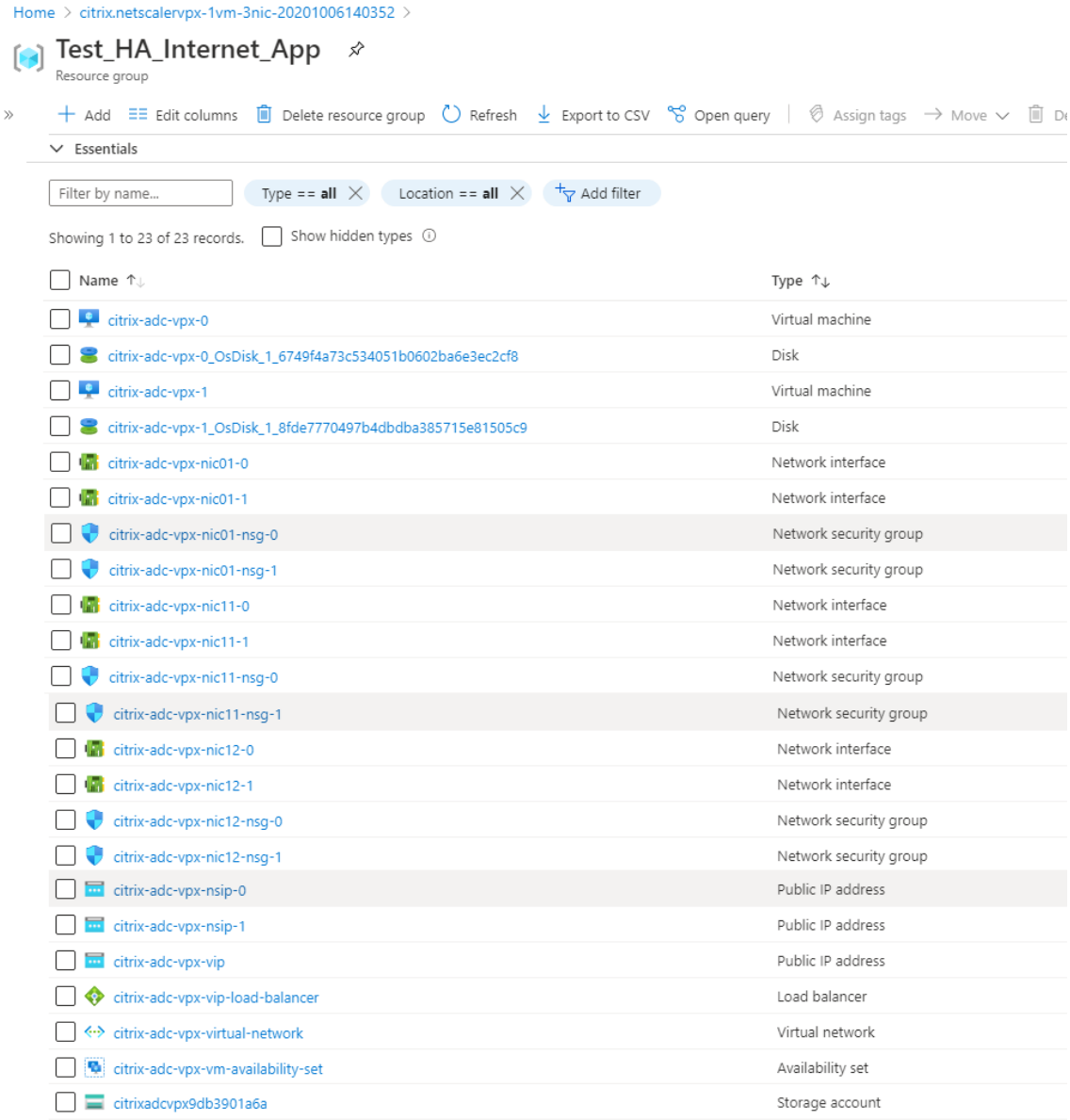


9. Haga clic en **Siguiente: Revisar + crear**.
10. Revise la configuración básica, la configuración de la máquina virtual, la red y la configuración adicional, y haga clic en **Crear**.

El grupo de recursos de Azure puede tardar un momento en crearse con las configuraciones requeridas. Una vez finalizado, seleccione el grupo de recursos en Azure Portal para ver los detalles de configuración, como reglas LB, grupos de back-end y sondeos de estado. El par de alta disponibilidad aparece como **citrix-adc-vpx-0** y **citrix-adc-vpx-1**.

Si se requieren más modificaciones para la configuración de HA, como la creación de más reglas de seguridad y puertos, puede hacerlo desde el portal de Azure.

Una vez completada la configuración requerida, se crean los siguientes recursos.



11. Debe iniciar sesión en los nodos **citrix-adc-vpx-0** y **citrix-adc-vpx-1** para validar la siguiente configuración:

    - Las direcciones NSIP de ambos nodos deben estar en la subred de administración.

- En los nodos primario (citrix-adc-vpx-0) y secundario (citrix-adc-vpx-1), debe ver dos direcciones SNIP. Un SNIP (subred de cliente) se utiliza para responder a los sondeos ALB y el otro SNIP (subred del servidor) se utiliza para la comunicación con el servidor back-end.

> Nota
>
> En el modo HA-INC, las direcciones SNIP de las máquinas virtuales citrix-adc-vpx-0 y citrix-adc-vpx-1 son diferentes, a diferencia de la implementación clásica de alta disponibilidad de ADC local donde ambas son iguales.

En el nodo principal (citrix-adc-vpx-0)

```
> sh ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----             ----     ---      ----     -------  ------
1)      10.18.0.4        0               NetScaler IP     Active   Enabled  Enabled  NA       Enabled
2)      10.18.1.5        0               SNIP             Active   Enabled  Enabled  NA       Enabled
3)      10.18.2.4        0               SNIP             Active   Enabled  Enabled  NA       Enabled
 Done
```

```
> sh ha node
1)      Node ID:      0
        IP:       10.18.0.4 (ns-vpx0)
        Node State: UP
        Master State: Primary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: ENABLED
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
        Sync Status Strict Mode: DISABLED
        Hello Interval: 200 msecs
        Dead Interval: 3 secs
        Node in this Master State for: 0:3:34:21 (days:hrs:min:sec)
2)      Node ID:      1
        IP:       10.18.0.5
        Node State: UP
        Master State: Secondary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: SUCCESS
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
 Done
```

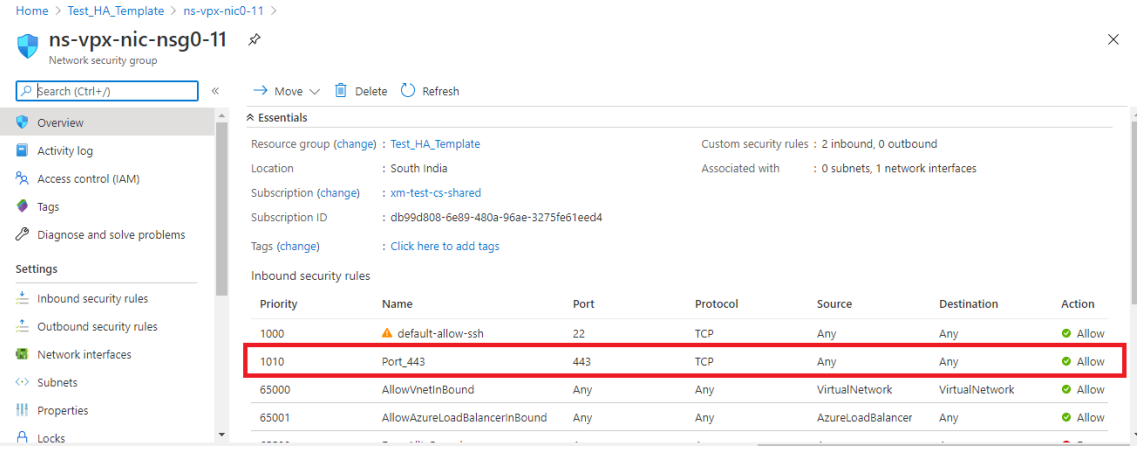
En el nodo secundario (citrix-adc-vpx-1)

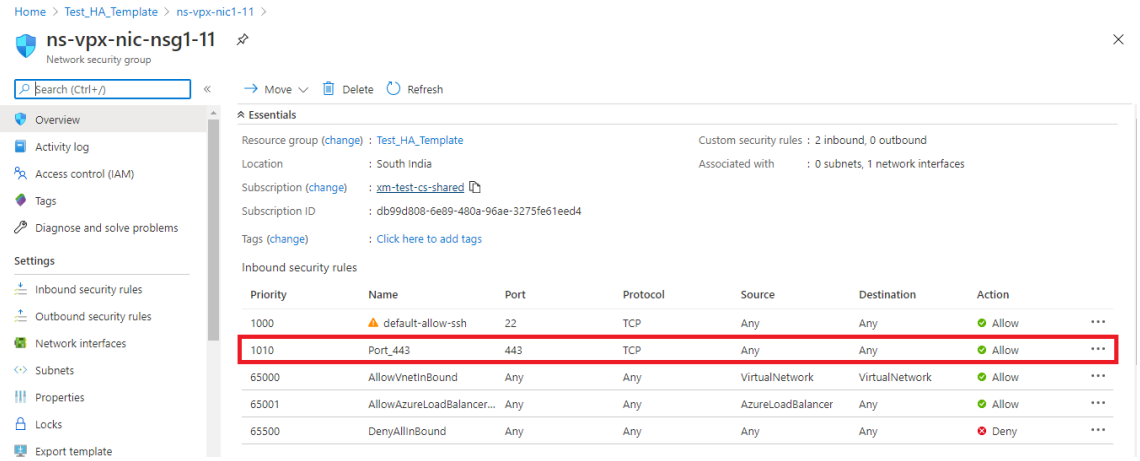

```
> show ip
        Ipaddress        Traffic Domain  Type            Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----            ----     ---      ----     -------  ------
1)      10.18.0.5        0               NetScaler IP    Active   Enabled  Enabled  NA       Enabled
2)      10.18.1.4        0               SNIP            Active   Enabled  Enabled  NA       Enabled
3)      10.18.2.5        0               SNIP            Active   Enabled  Enabled  NA       Enabled
 Done
>
```

```
> sh ha node
1)      Node ID:      0
        IP:       10.18.0.5 (ns-vpx1)
        Node State: UP
        Master State: Secondary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: SUCCESS
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
        Sync Status Strict Mode: DISABLED
        Hello Interval: 200 msecs
        Dead Interval: 3 secs
        Node in this Master State for: 0:3:23:51 (days:hrs:min:sec)
2)      Node ID:      1
        IP:       10.18.0.4
        Node State: UP
        Master State: Primary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: ENABLED
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
 Done
>
```

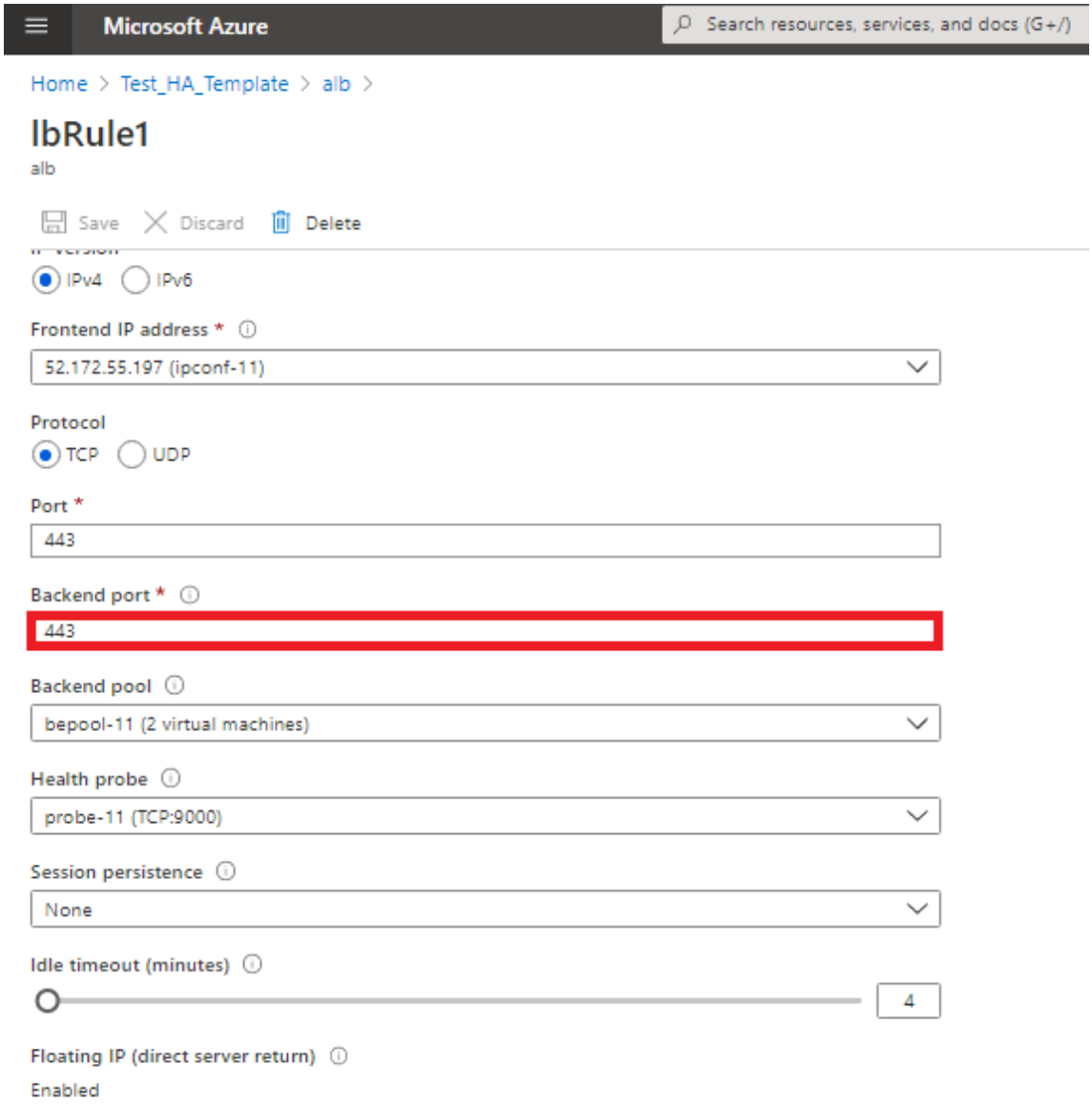
12. Después de que los nodos primario y secundario estén UP y el estado de sincronización es **SUCCESS**, debe configurar el servidor virtual de equilibrio de carga o el servidor virtual de puerta de enlace en el nodo principal (citrix-adc-vpx-0) con la dirección IP pública del servidor virtual ALB. Para obtener más información, consulte la sección Configuración de ejemplo .
13. Para buscar la dirección IP pública del servidor virtual ALB, vaya a **Azure Portal > Azure Load Balancer > Configuración de IP de frontend**.

14. Agregue la regla de seguridad entrante para el puerto 443 del servidor virtual en el grupo de seguridad de red de ambas interfaces de cliente.

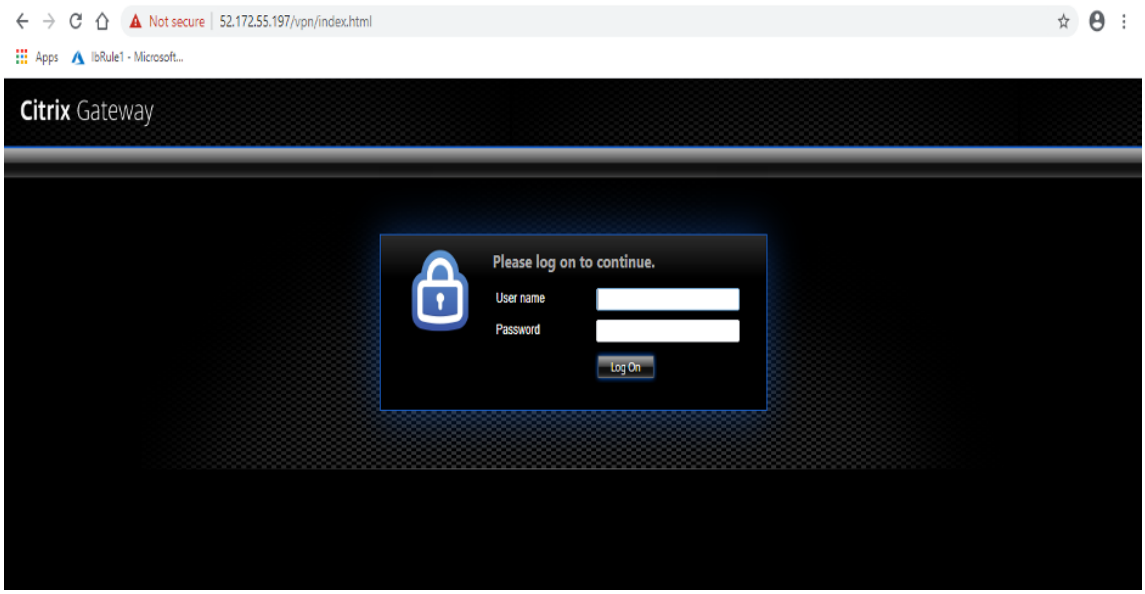




15. Configure el puerto ALB al que quiere acceder y cree una regla de seguridad entrante para el puerto especificado. El puerto Backend es el puerto del servidor virtual de equilibrio de carga o el puerto del servidor virtual VPN.



16. Ahora, puede acceder al servidor virtual de equilibrio de carga o al servidor virtual VPN mediante el FQDN asociado con la dirección IP pública ALB.



Configuración de ejemplo

Para configurar un servidor virtual VPN de puerta de enlace y un servidor virtual de equilibrio de carga, ejecute los siguientes comandos en el nodo principal (ADC-VPX-0). La configuración se sincroniza automáticamente con el nodo secundario (ADC-VPX-1).

Configuración de ejemplo de gateway

```
enable feature aaa LB SSL SSLVPN
add ip 52.172.55.197 255.255.255.0 -type VIP
add vpn vserver vpn_ssl SSL 52.172.55.197 443
add ssl certKey ckp -cert cgwsanity.cer -key cgwsanity.key
bind ssl vserver vpn_ssl -certkeyName ckp
<!--NeedCopy-->
```

Configuración de muestra de equilibrio de carga

```
enable feature LB SSL
enable ns mode MBF
add lb vserver lb_vs1 SSL 52.172.55.197 443
bind ssl vserver lb_vs1 -certkeyName ckp
<!--NeedCopy-->
```

Ahora puede acceder al servidor virtual de equilibrio de carga o VPN mediante el nombre de dominio completo (FQDN) asociado a la dirección IP interna de ILB.

Consulte la sección **Recursos** para obtener más información acerca de cómo configurar el servidor virtual de equilibrio de carga.

Recursos:

Los siguientes vínculos proporcionan información adicional relacionada con la implementación de HA y la configuración del servidor virtual:

- Crear servidores virtuales
- Configurar el equilibrio de carga básico

Configurar una configuración de alta disponibilidad con balanceadores de carga externos e internos de Azure simultáneamente

August 20, 2021

El par de alta disponibilidad de Azure admite equilibradores de carga externos e internos simultáneamente.

Dispone de las dos opciones siguientes para configurar un par de alta disponibilidad mediante equilibradores de carga externos e internos de Azure:

- Uso de dos servidores virtuales LB en el dispositivo Citrix ADC.
- Uso de un servidor virtual LB y un conjunto de IP. El único servidor virtual LB envía tráfico a varias IP, definidas por IPset.

Lleve a cabo los siguientes pasos para configurar un par de alta disponibilidad en Azure mediante los equilibradores de carga externos e internos simultáneamente:

Para los pasos 1 y 2, utilice el portal de Azure. Para los pasos 3 y 4, utilice la GUI de Citrix ADC VPX o la CLI.

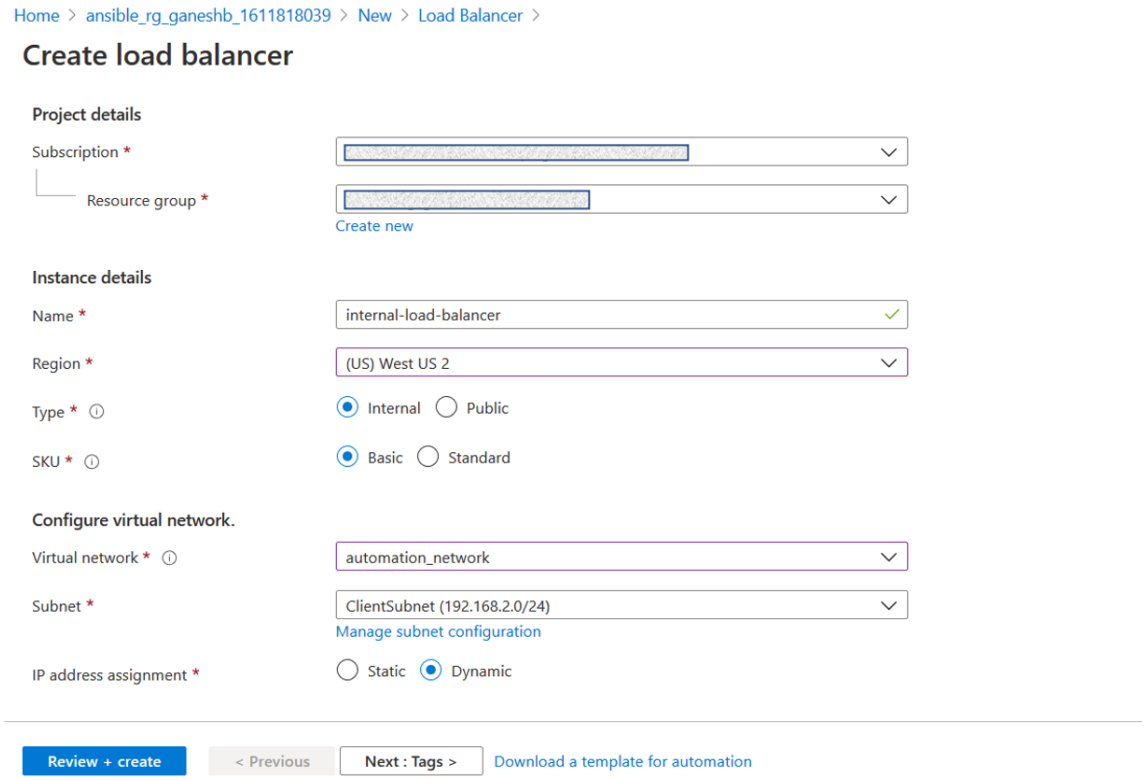
Paso 1. Configure un balanceador de carga de Azure, ya sea un balanceador de carga externo o un balanceador de carga interno.

Para obtener más información sobre la configuración de alta disponibilidad con balanceadores de carga externos de Azure, consulte Configurar una configuración de alta disponibilidad con varias direcciones IP y NIC.

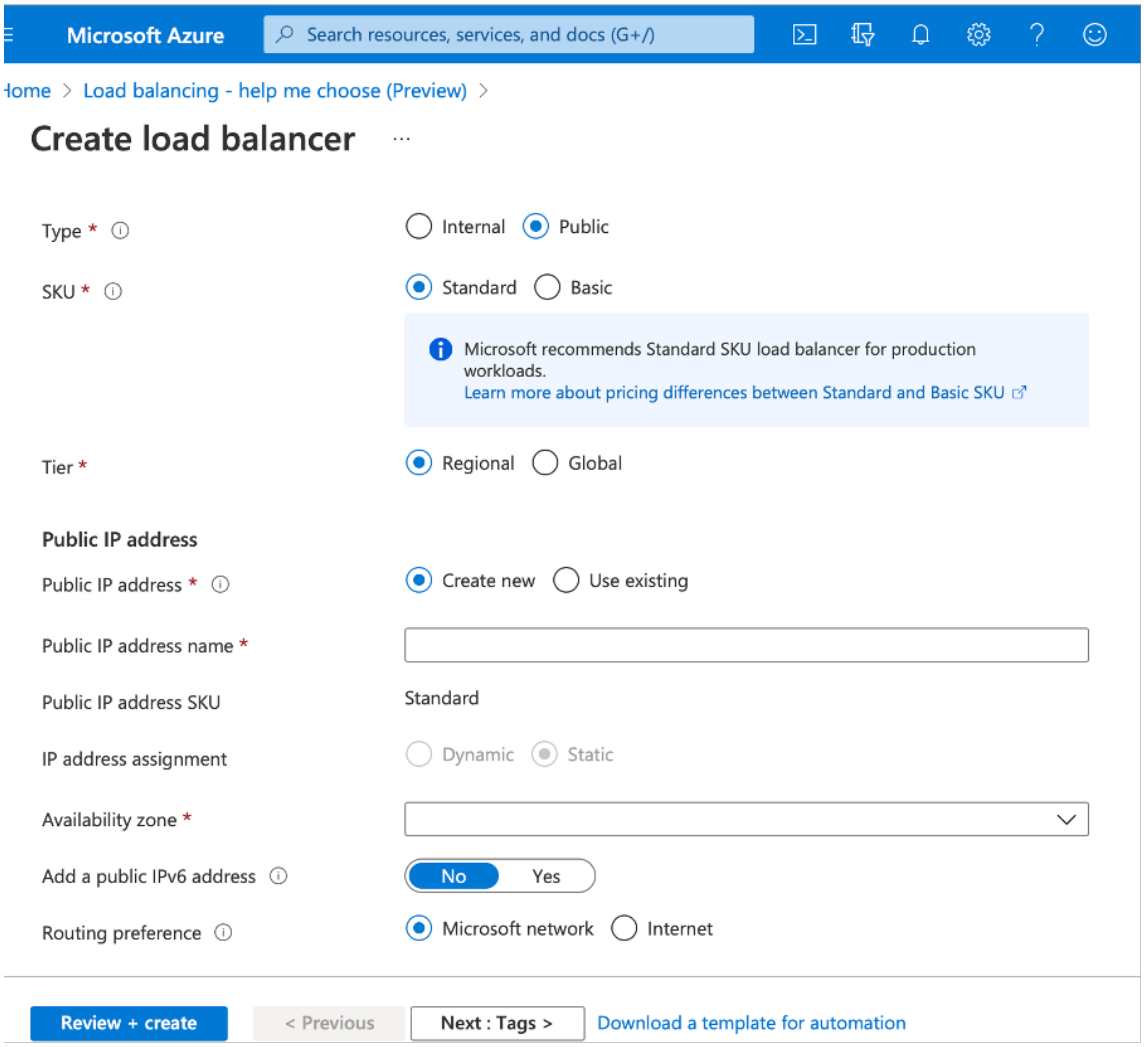
Para obtener más información sobre la configuración de alta disponibilidad con balanceadores de carga internos de Azure, consulte Configurar nodos HA-INC mediante la plantilla de alta disponibilidad de Citrix con Azure ILB.

Paso 2. Cree un equilibrador de carga adicional (ILB) en su grupo de recursos. En el paso 1, si ha creado un equilibrador de carga externo, ahora creará un equilibrador de carga interno y, por el contrario.

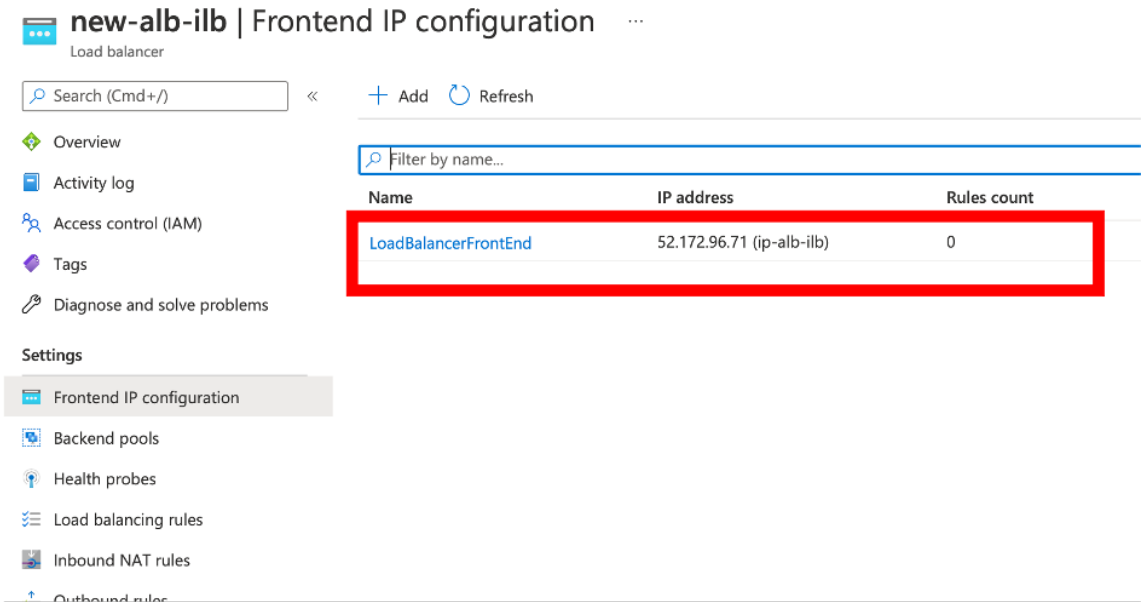
- Para crear un equilibrador de carga interno, elija el tipo de equilibrador de carga como **Interno**. Para el campo **Subred**, debe elegir la subred cliente Citrix ADC. Puede elegir proporcionar una dirección IP estática en esa subred, siempre que no haya conflictos. De lo contrario, elija la dirección IP dinámica.



- Para crear un balanceador de cargas externo, elija el tipo de equilibrador de carga como **Público** y cree aquí la dirección IP pública.



1. Después de crear Azure Load Balancer, vaya a **Configuración IP frontend** y anote la dirección IP que se muestra aquí. Debe utilizar esta dirección IP al crear el servidor virtual de equilibrio de carga de ADC como en el paso 3.



2. En la página de **configuración de Azure Load Balancer**, la implementación de plantillas ARM ayuda a crear la regla LB, los grupos de back-end y los sondeos de estado.
3. Agregue las NIC cliente de par de alta disponibilidad al grupo de back-end de la ILB.
4. Creación de un sondeo de estado (TCP, puerto 9000)
5. Cree dos reglas de equilibrio de carga:
    - Una regla LB para el tráfico HTTP (caso de uso de aplicaciones web) en el puerto 80. La regla también debe utilizar el puerto de back-end 80. Seleccione el grupo de back-end creado y el sondeo de estado. La IP flotante debe estar habilitada.
    - Otra regla LB para el tráfico HTTPS o CVAD en el puerto 443. El proceso es el mismo que el tráfico HTTP.

Paso 3. En el nodo principal del dispositivo Citrix ADC, cree un servidor virtual de equilibrio de carga para ILB.

1. Agregue un servidor virtual de equilibrio de carga.

```
add lb vserver <name> <serviceType> [<ILB Frontend IP address>] [<
    port>]
<!--NeedCopy-->
```

Ejemplo:

```
add lb vserver vserver_name HTTP 52.172.96.71 80
```



```
<!--NeedCopy-->
```

> Nota:
>
> Utilice la dirección IP frontend del equilibrador de carga, que está asociada con el equilibrador de carga adicional que crea en el paso 2.

2. Enlazar un servicio a un servidor virtual de equilibrio de carga.

```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Ejemplo:

```
bind lb vserver Vserver-LB-1 Service-HTTP-1
<!--NeedCopy-->
```

Para obtener más información, consulte Configuración del equilibrio de carga básico.

Paso 4: Como alternativa al paso 3, puede crear un servidor virtual de equilibrio de carga para ILB mediante IPsets.

1. Agregue una dirección IP del tipo IP del servidor virtual (VIP).

```
add nsip <ILB Frontend IP address> -type <type>
<!--NeedCopy-->
```

Ejemplo:

```
add nsip 52.172.96.71 -type vip
<!--NeedCopy-->
```

2. Agregue un IPset en los nodos primario y secundario.

```
add ipset <name>
<!--NeedCopy-->
```

Ejemplo:


```
add ipset ipset1
<!--NeedCopy-->
```

3. Enlazar direcciones IP al conjunto de IP.

```
bind ipset <name> <ILB Frontend IP address>
<!--NeedCopy-->
```

Ejemplo:

```
bind ipset ipset1 52.172.96.71
<!--NeedCopy-->
```

4. Configure el servidor virtual LB existente para que use el IPSet.

```
set lb vserver <vserver name> -ipset <ipset name>
<!--NeedCopy-->
```

Ejemplo:

```
set lb vserver vserver_name -ipset ipset1
<!--NeedCopy-->
```

Para obtener más información, consulte Configuración de un servidor virtual multi-IP.

Instalación de una instancia Citrix ADC VPX en Azure VMware Solution

July 15, 2022

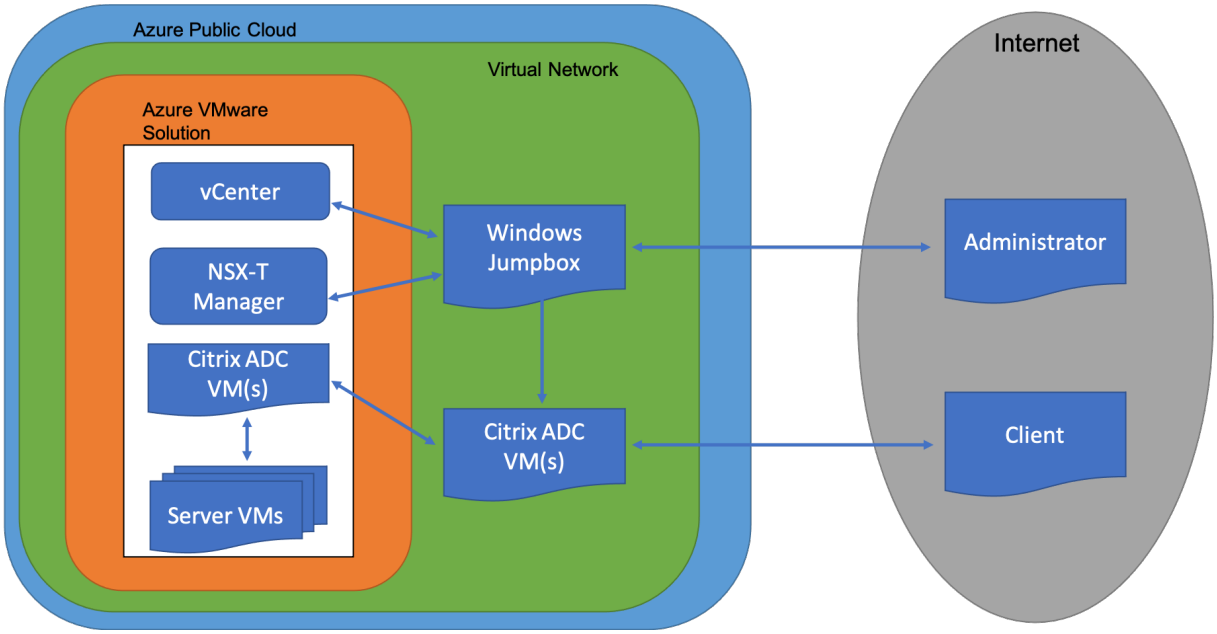
Azure VMware Solution (AVS) le proporciona nubes privadas que contienen clústeres de vSphere, creados a partir de una infraestructura exclusiva de Azure exclusiva. La implementación inicial mínima es de tres hosts, pero se pueden agregar hosts adicionales uno a uno, hasta un máximo de 16 hosts por clúster. Todas las nubes privadas aprovisionadas tienen vCenter Server, vSAN, vSphere y NSX-T.

VMware Cloud (VMC) en Azure le permite crear centros de datos definidos por software en la nube (SDDC) en Azure con el número de hosts ESX que desea. La VMC en Azure admite implementaciones

Citrix ADC VPX. VMC proporciona una interfaz de usuario igual que vCenter en las instalaciones. Funciona de forma similar a las implementaciones Citrix ADC VPX basadas en ESX.

En el siguiente diagrama se muestra la solución Azure VMware en la nube pública de Azure a la que un administrador o un cliente pueden acceder a través de Internet. Un administrador puede crear, administrar y configurar máquinas virtuales de servidor o de carga de trabajo mediante la solución Azure VMware. El administrador puede acceder a vCenter basado en web y NSX-T Manager de AVS desde un Windows Jumpbox. Puede crear instancias Citrix ADC VPX (par independientes o de alta disponibilidad) y las máquinas virtuales de servidor dentro de Azure VMware Solution mediante vCenter y administrar la red correspondiente mediante NSX-T manager. La instancia Citrix ADC VPX en AVS funciona de forma similar al clúster de hosts de VMware local. AVS se administra desde un Windows Jumpbox creado en la misma red virtual.

Un cliente solo puede acceder al servicio AVS si se conecta al VIP de ADC. Otra instancia Citrix ADC VPX fuera de Azure VMware Solution pero en la misma red virtual de Azure ayuda a agregar la VIP de la instancia Citrix ADC VPX dentro de Azure VMware Solution como servicio. Según el requisito, puede configurar la instancia Citrix ADC VPX para proporcionar servicio a través de Internet.



Requisitos previos

Antes de comenzar a instalar un dispositivo virtual, haga lo siguiente:

- Para obtener más información sobre la solución Azure VMware y sus requisitos previos, consulte la documentación de Azure VMware Solution.
- Para obtener más información sobre la implementación de la solución Azure VMware, consulte Implementación de una nube privada de Azure VMware Solution.

- Para obtener más información sobre la creación de una máquina virtual Windows Jump box para acceder y administrar Azure VMware Solution, consulte Acceso a una nube privada de Azure VMware Solution
- En la máquina virtual de Windows Jump box, descargue los archivos de configuración del dispositivo Citrix ADC VPX.
- Cree segmentos de red NSX-T apropiados en el SDDC de VMware al que se conectan las máquinas virtuales. Para obtener más información, consulte Agregar un segmento de red en Azure VMware Solution
- Obtenga archivos de licencia VPX.
- Las máquinas virtuales (VM) creadas o migradas a la nube privada de Azure VMware Solution deben estar conectadas a un segmento de red.

RequiVMware de hardware en la nube

En la tabla siguiente se enumeran los recursos informáticos virtuales que el SDDC de VMware debe proporcionar para cada dispositivo virtual VPX nCore.

Cuadro 1 Recursos informáticos virtuales mínimos necesarios para ejecutar una instancia de Citrix ADC VPX

Componente	Requisito
Memoria	2 GB
CPU virtual (vCPU)	2
Interfaces de red virtual	En VMware SDDC, puede instalar un máximo de 10 interfaces de red virtual si el hardware VPX se actualiza a la versión 7 o superior.
Espacio en disco	20 GB

> Nota
>
> Esto se suma a cualquier requisito de disco para el Hypervisor.

Para el uso en producción del dispositivo virtual VPX, debe reservarse la asignación de memoria completa.

Requisitos del sistema OVF Tool 1.0

OVF Tool es una aplicación cliente que puede ejecutarse en sistemas Windows y Linux. En la tabla siguiente se describen los requisitos del sistema para instalar la herramienta OVF.

Tabla 2. Requisitos del sistema para instalar herramientas OVF

Componente	Requisito
Sistema operativo	Para obtener información detallada sobre los requisitos de VMware, busque el archivo PDF "OVF Tool User Guide" en http://kb.vmware.com/.
CPU	750 MHz como mínimo, se recomienda 1 GHz o más rápido
RAM	1 GB mínimo, 2 GB recomendado
NIC	NIC de 100 Mbps o más rápido

Para obtener información acerca de la instalación de OVF, busque el archivo PDF "Guía del usuario de la herramienta OVF" en http://kb.vmware.com/.

Descarga de los archivos de configuración de Citrix ADC VPX

El paquete de instalación de instancias de Citrix ADC VPX para VMware ESX sigue el estándar de formato Open Virtual Machine (OVF). Puede descargar los archivos desde el sitio web de Citrix. Necesita una cuenta de Citrix para iniciar sesión. Si no tiene una cuenta de Citrix, acceda a la página de inicio en http://www.citrix.com. Haga clic en el **vínculo Nuevos usuarios** y siga las instrucciones para crear una nueva cuenta de Citrix.

Una vez iniciada la sesión, navegue por la siguiente ruta desde la página principal de Citrix:

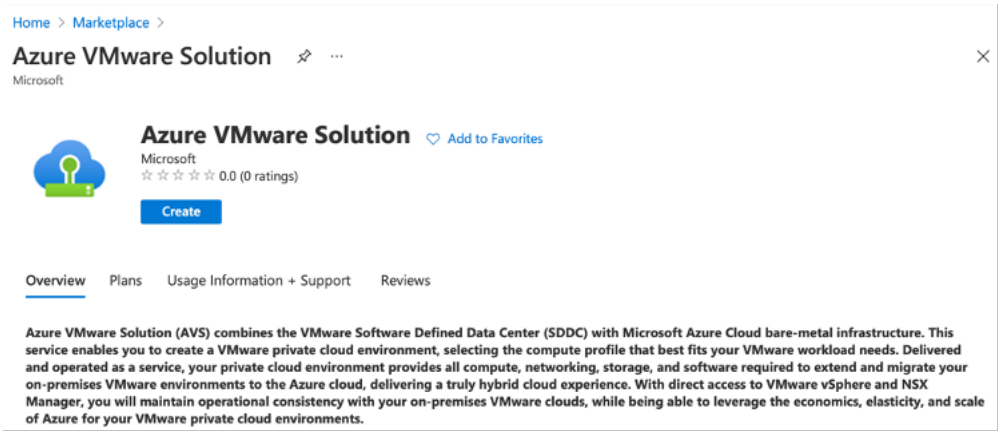
Citrix.com > **Descargas > Citrix ADC > Dispositivos virtuales**.

Copie los siguientes archivos en una estación de trabajo en la misma red que el servidor ESX. Copie los tres archivos en la misma carpeta.

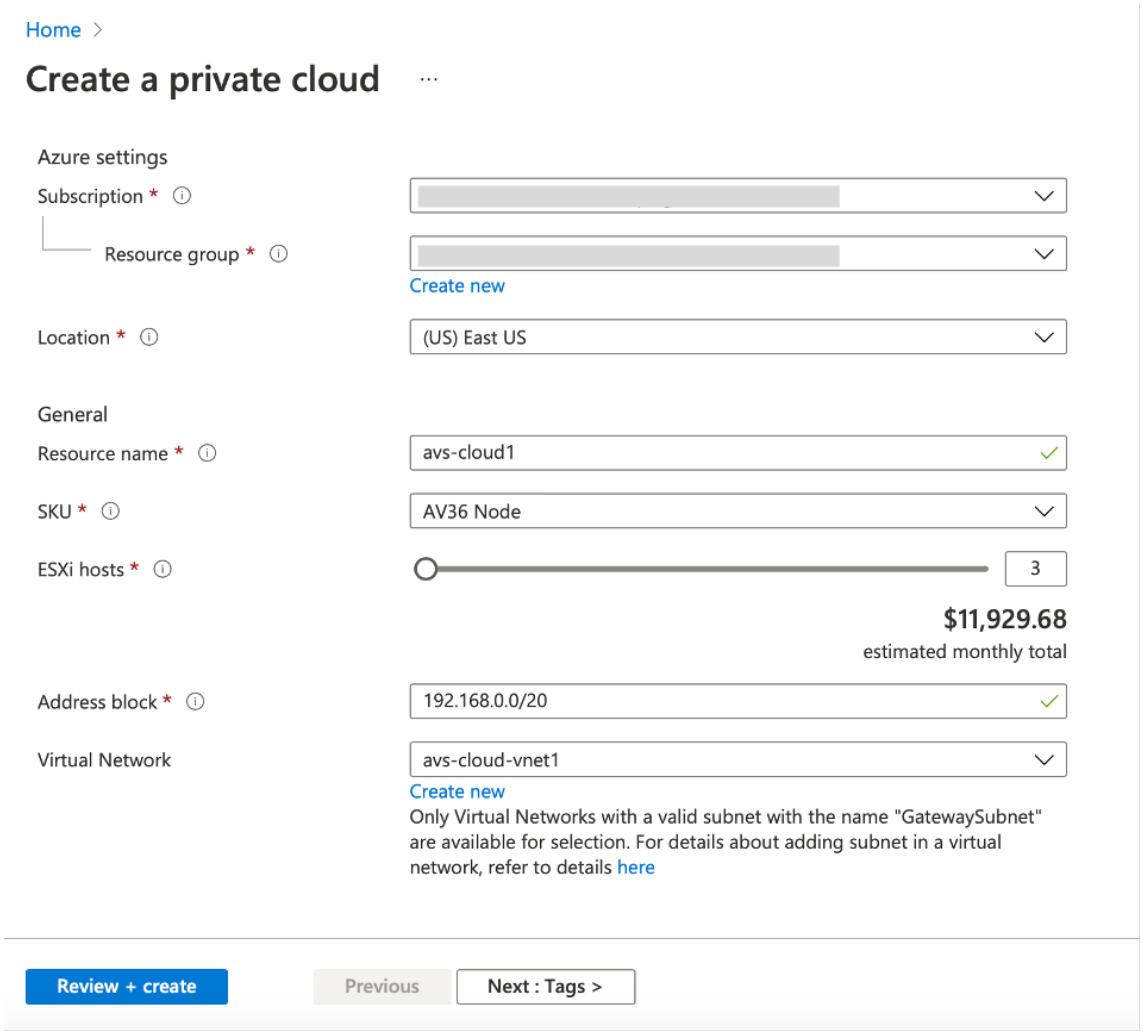
- NSVPX-ESX- <release number>- <build number>-disk1.vmdk (por ejemplo, NSVPX-ESX-13.0-79.64-disk1.vmdk)
- NSVPX-ESX- <release number>- <build number>.ovf (por ejemplo, NSVPX-ESX-13.0-79.64.ovf)
- NSVPX-ESX- <release number>- <build number>.mf (por ejemplo, NSVPX-ESX-13.0-79.64.mf)

Implementación de la solución Azure VMware

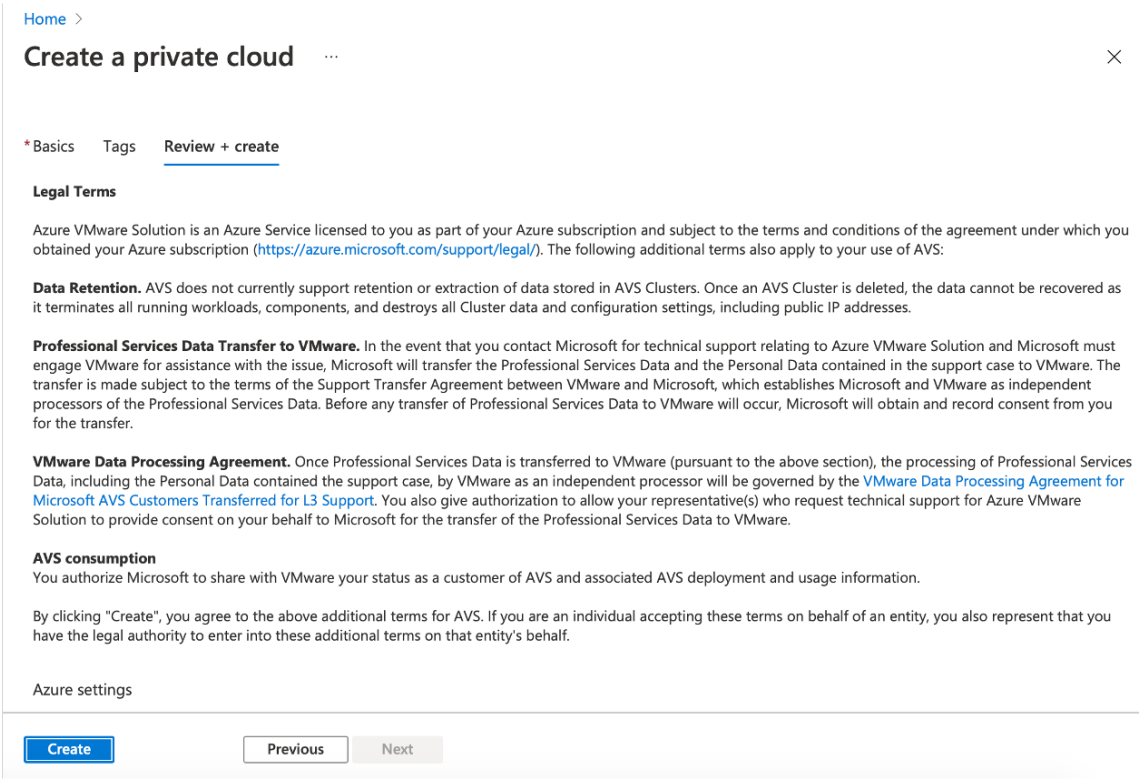
1. Inicie sesión en su portal de Microsoft Azurey vaya a **Azure Marketplace**.
2. En **Azure Marketplace**, busque **Azure VMware Solution** y haga clic en **Crear**.



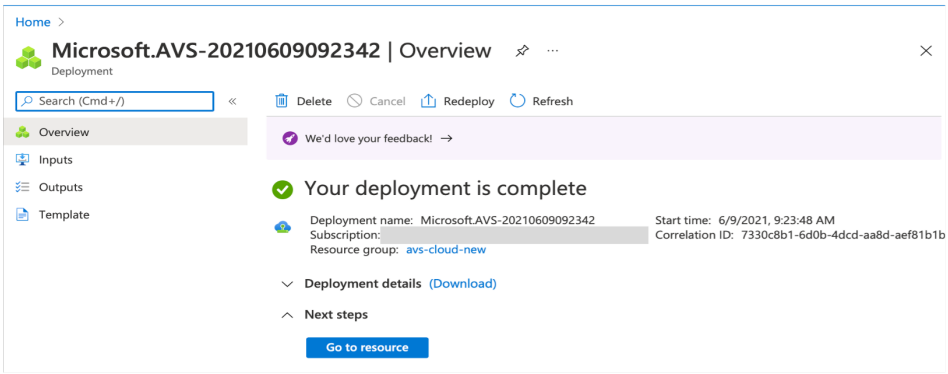
3. En la página **Crear una nube privada**, introduzca los siguientes detalles:
    - Seleccione un mínimo de 3 hosts ESXi para crear el clúster predeterminado de su nube privada.
    - Para el campo **Bloque de direcciones**, utilice el espacio de direcciones **/22** .
    - Para la **red virtual**, asegúrese de que el rango CIDR no se superponga con ninguna de sus subredes locales u otras subredes de Azure (redes virtuales) o con la subred de puerta de enlace.
    - La subred de puerta de enlace se utiliza para enrutar expresamente la conexión con la nube privada.



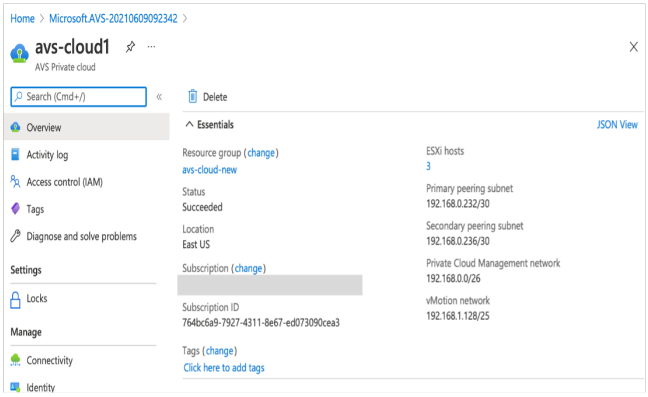
4. Haga clic en **Revisar + Crear**.
5. Revise la configuración. Si debe cambiar la configuración, haga clic en **Anterior**.



6. Haga clic en **Crear**. Comienza el proceso de aprovisionamiento de nube privada. La nube privada puede tardar hasta dos horas en aprovisionarse.



7. Haga clic en **Ir al recurso**para verificar la nube privada creada.



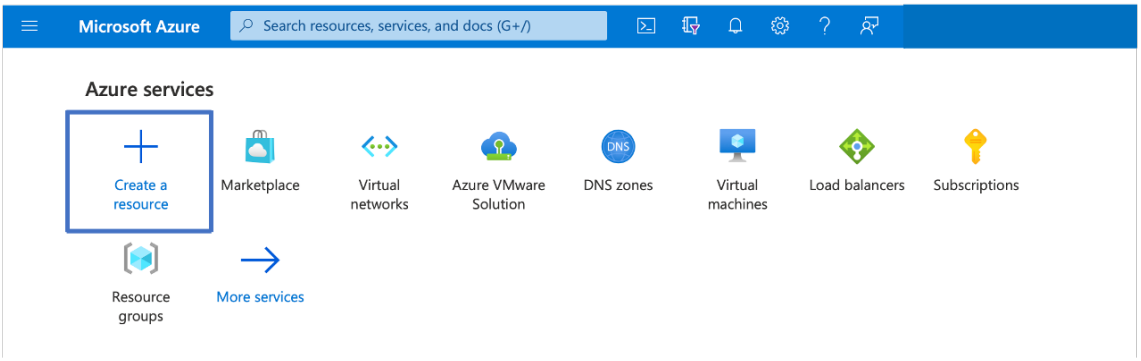
> Nota
>
> Para acceder a este recurso, necesita una máquina virtual en Windows que actúe como Jump box.

Conectarse a una máquina virtual de Azure que ejecuta Windows

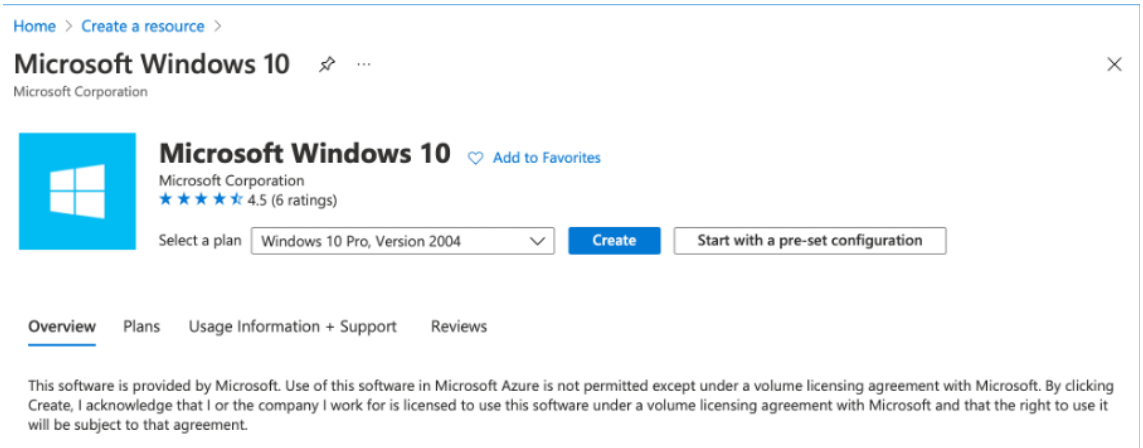
En este procedimiento se muestra cómo utilizar el portal de Azure para implementar una máquina virtual (VM) en Azure que ejecuta Windows Server 2019. Para ver la máquina virtual en acción, a continuación, RDP en la máquina virtual e instala el servidor web de IIS.

Para acceder a la nube privada que ha creado, debe crear un cuadro de Windows Jump dentro de la misma red virtual.

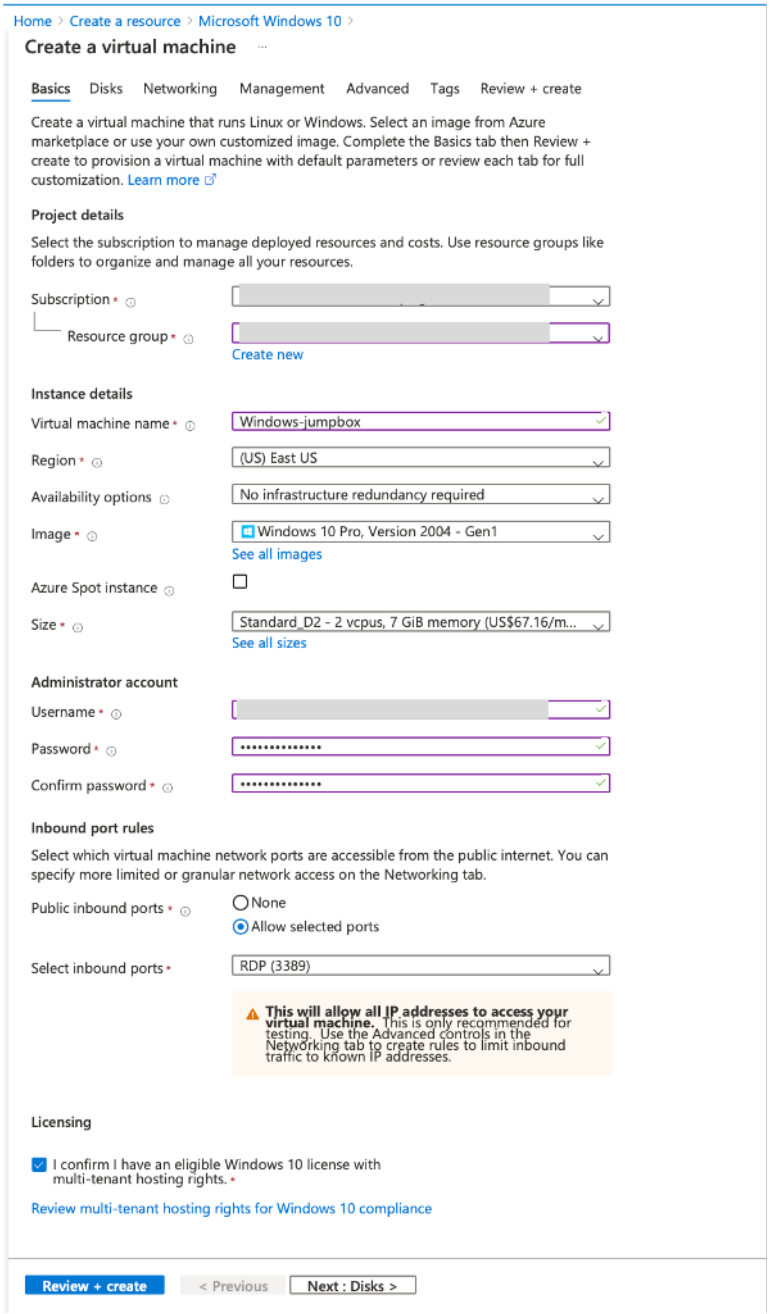
1. Vaya al **portal de Azure**y haga clic en **Crear un recurso**.



2. Busque **Microsoft Windows 10**y haga clic en **Crear**.



3. Cree una máquina virtual (VM) que ejecute Windows Server 2019. Aparece la página **Crear una máquina virtual**. Introduzca todos los detalles en la ficha **Conceptos básicos** y active la casilla de verificación **Licencias**. Deje los valores predeterminados restantes y, a continuación, seleccione el botón **Revisar + crear** en la parte inferior de la página.



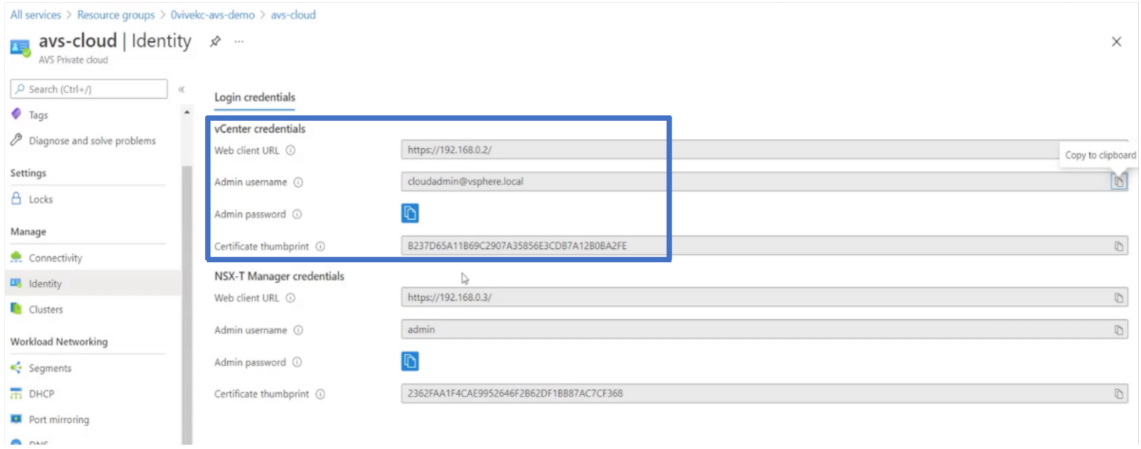
4. Una vez ejecutada la validación, seleccione el botón **Crear** en la parte inferior de la página.
5. Una vez finalizada la implementación, seleccione **Ir al recurso**.
6. Vaya a la máquina virtual de Windows que ha creado. Utilice la dirección IP pública de la máquina virtual de Windows y conéctese mediante RDP.

   Utilice el botón **Conectar** del portal de Azure para iniciar una sesión de Escritorio remoto (RDP) desde un escritorio Windows. Primero se conecta a la máquina virtual y, a continuación, inicia sesión.

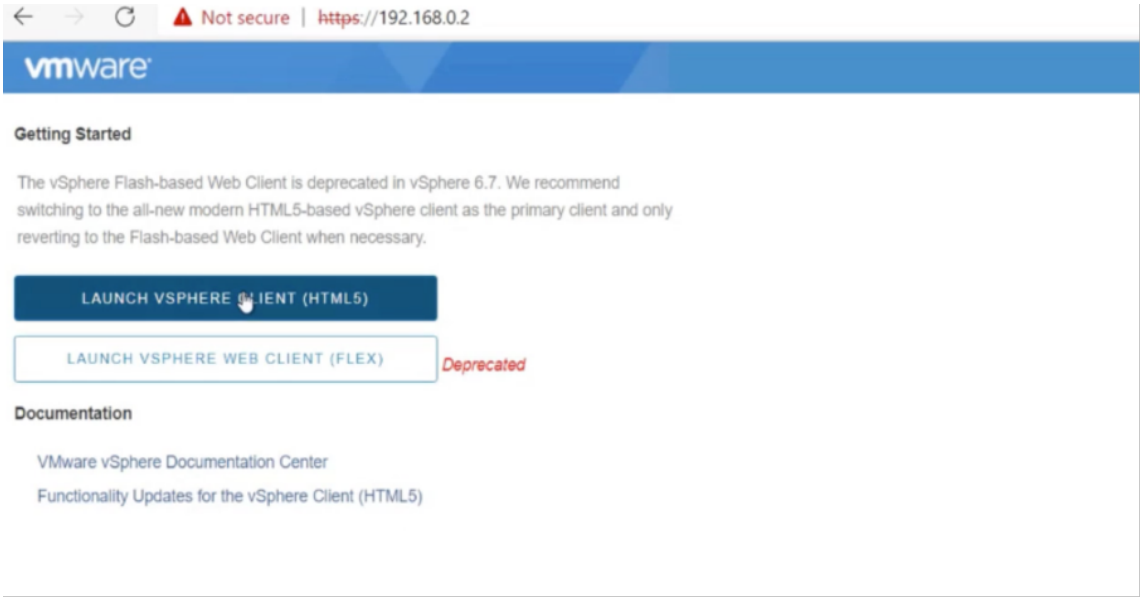
Para conectarse a una máquina virtual Windows desde una Mac, debe instalar un cliente RDP para Mac, como Microsoft Remote Desktop. Para obtener más información, consulte Cómo conectarse e iniciar sesión en una máquina virtual de Azure que ejecuta Windows.

Acceda a su portal vCenter de nube privada

1. En la nube privada de Azure VMware Solution, en **Administrar**, seleccione **Identidad**. Anote las credenciales de vCenter.

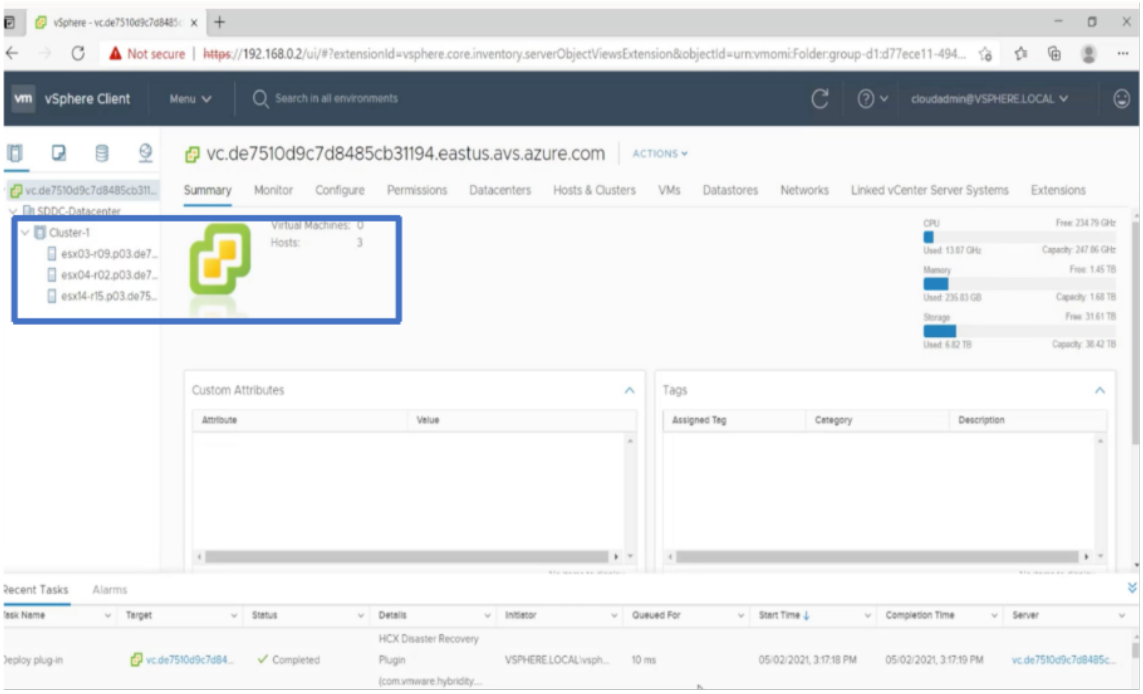


2. Inicie el cliente de vSphere escribiendo la URL del cliente web de vCenter.



3. Inicie sesión en VMware vSphere mediante las credenciales de vCenter de la nube privada de Azure VMware Solution.

4. En el cliente de vSphere, puede verificar los hosts ESXi que ha creado en el portal de Azure.



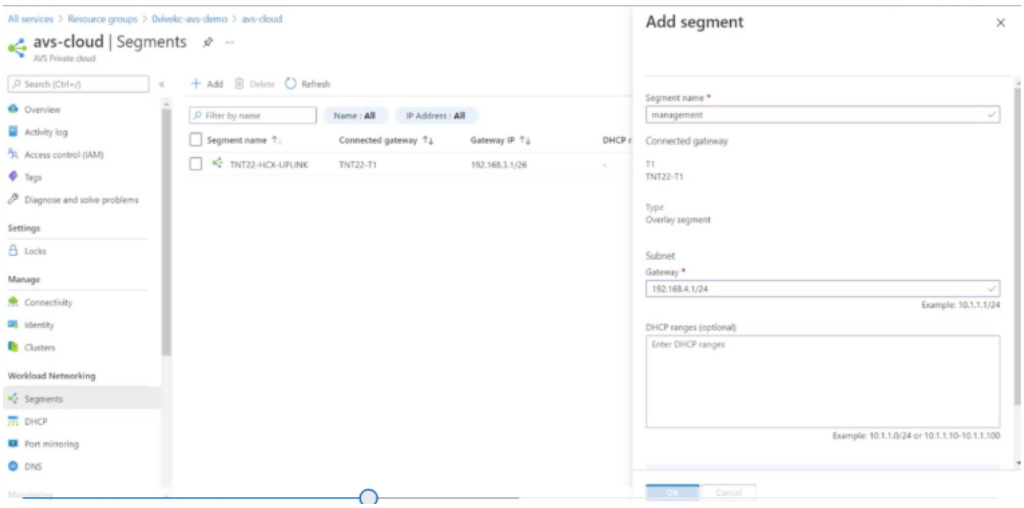
Para obtener más información, consulte Acceso al portal de vCenter de Private Cloud.

Creación de un segmento NSX-T en el portal de Azure

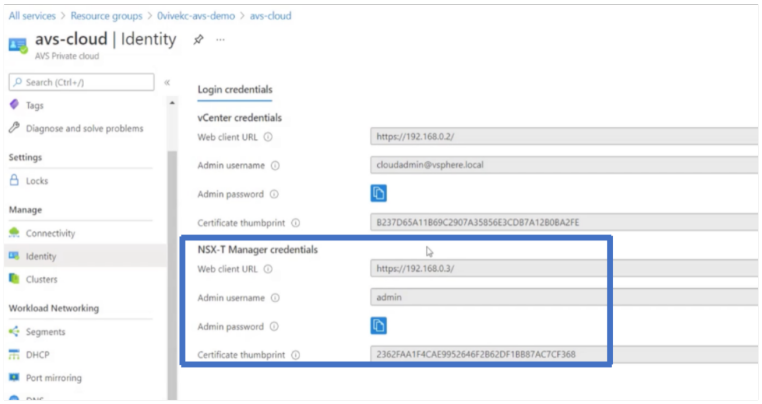
Puede crear y configurar un segmento de NSX-T desde la consola de Azure VMware Solution en el portal de Azure. Estos segmentos están conectados a la puerta de enlace predeterminada de nivel 1 y las cargas de trabajo de estos segmentos obtienen conectividad Este-Oeste y Norte-Sur. Una vez

creado el segmento, se muestra en NSX-T Manager y vCenter.

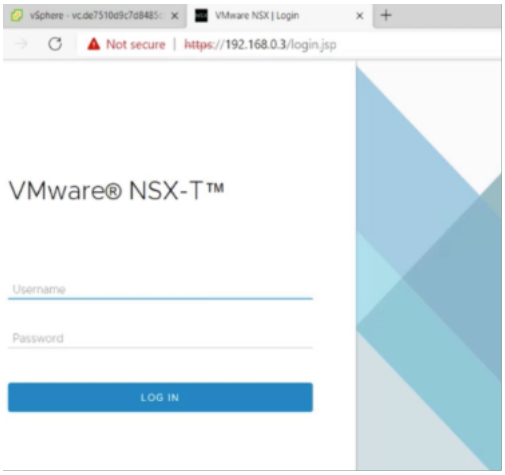
1. En la nube privada de Azure VMware Solution, en **Redes de carga de trabajo**, seleccione **Segmentos > Agregar**. Proporcione los detalles del nuevo segmento lógico y seleccione **Aceptar**. Puede crear tres segmentos independientes para las interfaces de cliente, administración y servidor.



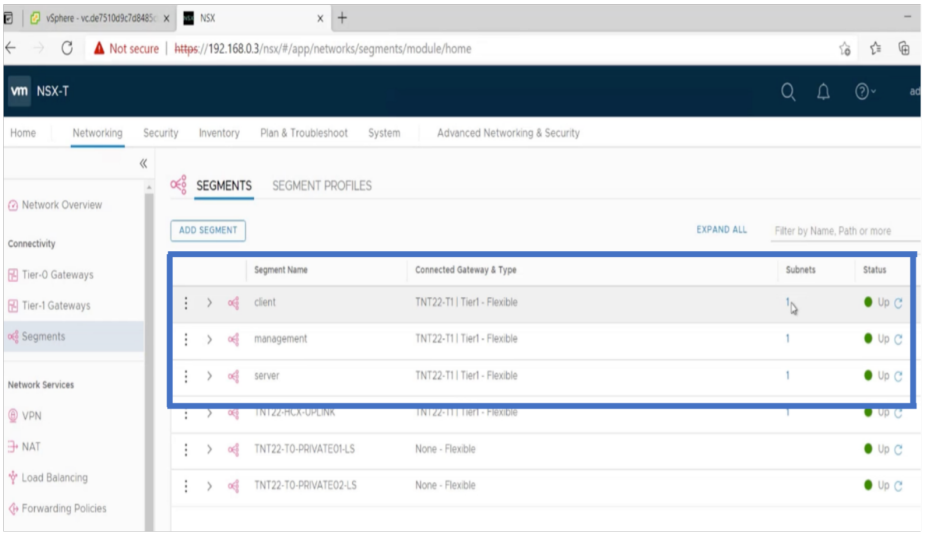
2. En la nube privada de Azure VMware Solution, en **Administrar**, seleccione **Identidad**. Anote las credenciales de NSX-T Manager.



3. Inicie VMware NSX-T Manager escribiendo la URL del cliente web de NSX-T.



4. En el gestor de NSX-T, en **Redes > Segmentos**, puede ver todos los segmentos que ha creado. También puede verificar las subredes.



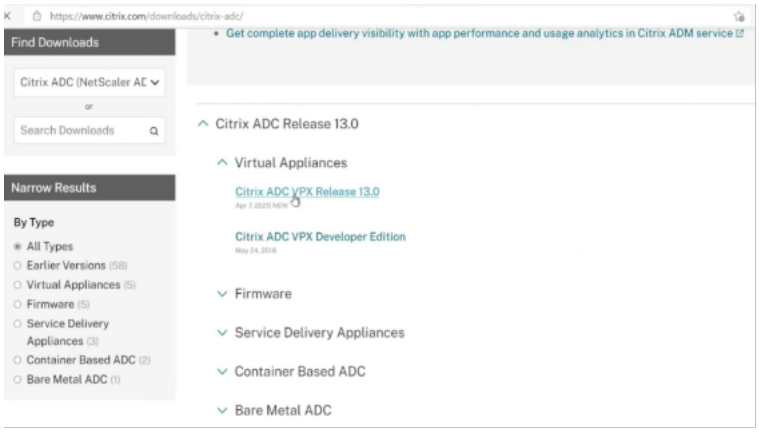
Para obtener más información, consulte Creación de un segmento de NSX-T en el portal de Azure.

Instalar una instancia de Citrix ADC VPX en la nube de VMware

Después de instalar y configurar el centro de datos definido por software (SDDC) de VMware, puede utilizar el SDDC para instalar dispositivos virtuales en la nube de VMware. El número de dispositivos virtuales que puede instalar depende de la cantidad de memoria disponible en el SDDC.

Para instalar instancias Citrix ADC VPX en la nube de VMware, lleve a cabo estos pasos en Windows Jumpbox VM:

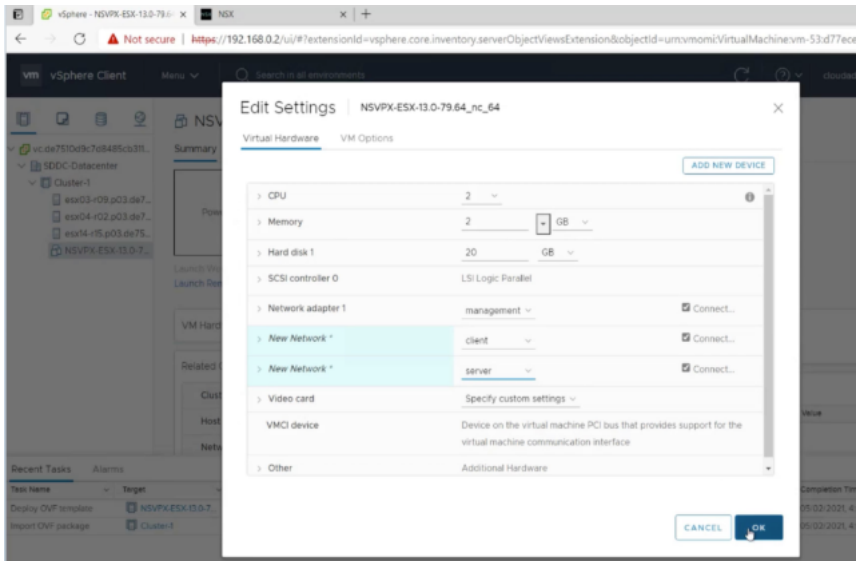
1. Descargue los archivos de configuración de instancias Citrix ADC VPX para el host ESXi del sitio de Citrix Downloads.



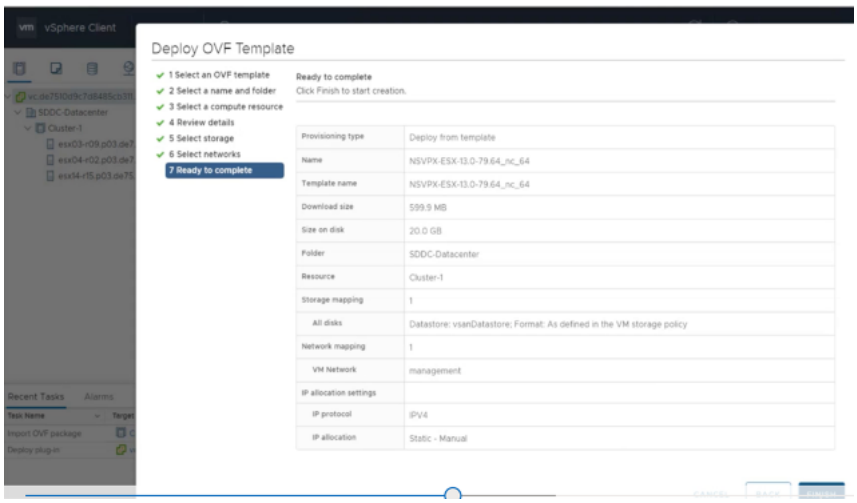
2. Abra VMware SDDC en Windows Jumpbox.
3. En los campos **Nombre de usuario** y **Contraseña**, escriba las credenciales de administrador y, a continuación, haga clic en **Iniciar sesión**.
4. En el menú **Archivo**, haga clic en **Implementar plantilla OVF**.
5. En el cuadro de diálogo **Implementar plantilla OVF**, en el campo **Implementar desde archivo**, vaya a la ubicación en la que guardó los archivos de configuración de instancias Citrix ADC VPX, seleccione el archivo.ovf y haga clic en **Siguiente**.

   > NOTA
   >
   > De forma predeterminada, la instancia de Citrix ADC VPX utiliza interfaces de red E1000. Para implementar ADC con la interfaz VMXNET3, modifique el OVF para utilizar la interfaz VMXNET3 en lugar de E1000. La disponibilidad de la interfaz VMXNET3 está limitada por la infraestructura de Azure y es posible que no esté disponible en Azure VMware Solution.

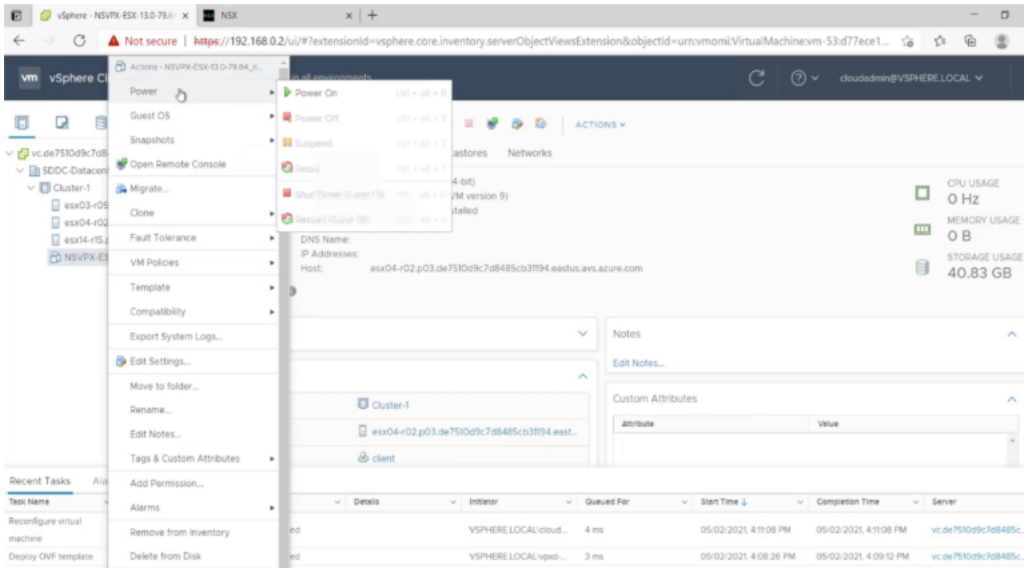
6. Asigne las redes que se muestran en la plantilla OVF del dispositivo virtual a las redes configuradas en el SDDC de VMware. Haga clic en **Aceptar**.



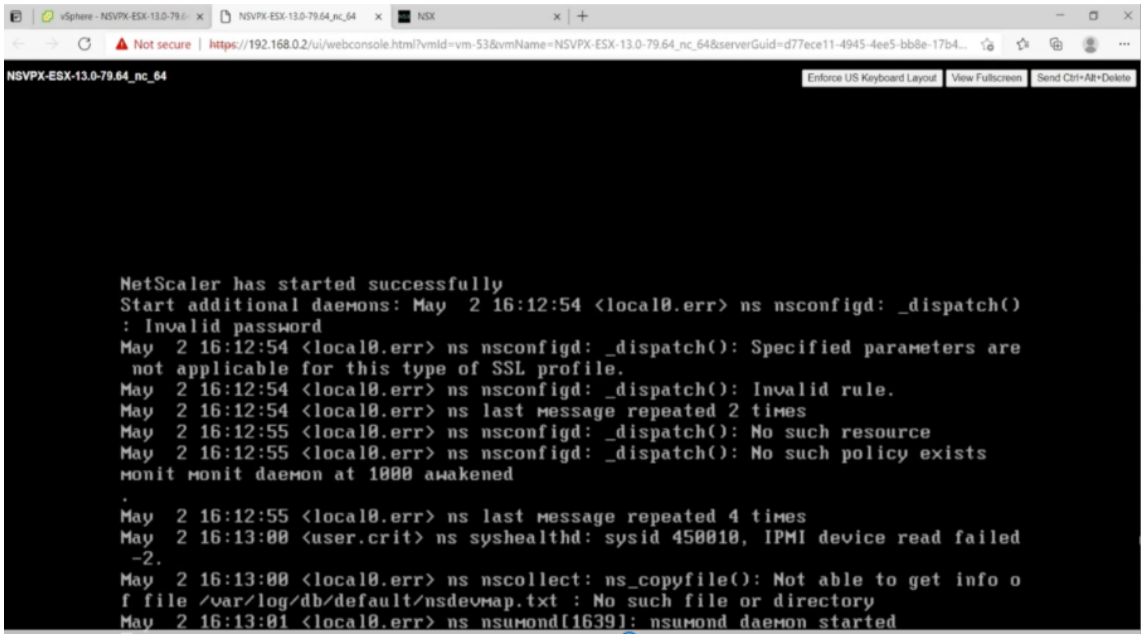
7. Haga clic en **Finalizar** para iniciar la instalación de un dispositivo virtual en VMware SDDC.



8. Ya está listo para iniciar la instancia de Citrix ADC VPX. En el panel de navegación, seleccione la instancia de Citrix ADC VPX que ha instalado y, en el menú contextual, seleccione **Encendido**. Haga clic en la ficha **Console** para emular un puerto de consola.



9. Ahora está conectado a la máquina virtual Citrix ADC desde el cliente de vSphere.



10. Para acceder al dispositivo Citrix ADC mediante las claves SSH, escriba el siguiente comando en la CLI:

```
ssh nsroot@<management IP address>
<!--NeedCopy-->
```

Ejemplo:

```
ssh nsroot@192.168.4.5
<!--NeedCopy-->
```

11. Puede verificar la configuración de ADC mediante el `show ns ip` comando.

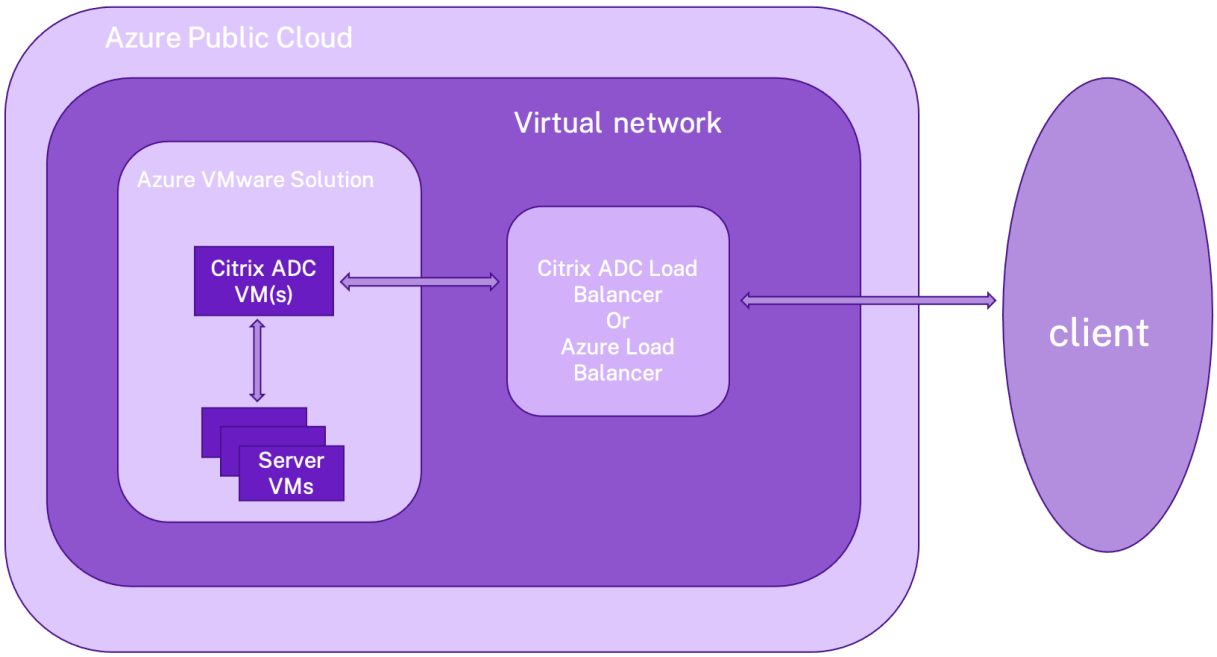
    ! [Verificar mediante `show nsip` el comando] (/en-us/citrix-adc/media/avs-show-nsip.png)

Configurar una instancia independiente de Citrix ADC VPX en la solución Azure VMware

February 19, 2022

Puede configurar una instancia independiente de Citrix ADC VPX en la solución Azure VMware (AVS) para aplicaciones orientadas a Internet.

El siguiente diagrama muestra la instancia independiente de Citrix ADC VPX en Azure VMware Solution. Un cliente puede acceder al servicio AVS conectándose a la dirección IP virtual (VIP) de Citrix ADC dentro del AVS. Puede lograrlo aprovisionando un equilibrador de carga Citrix ADC o la instancia del equilibrador de carga de Azure fuera de AVS pero en la misma red virtual de Azure. Configure el equilibrador de carga para acceder a la VIP de la instancia de Citrix ADC VPX dentro del servicio AVS.



Requisitos previos

Antes de comenzar a instalar un dispositivo virtual, lea los siguientes requisitos previos de Azure:

- Para obtener más información sobre la solución Azure VMware y sus requisitos previos, consulte la documentación de Azure VMware Solution.
- Para obtener más información sobre la implementación de la solución Azure VMware, consulte Implementación de una nube privada de Azure VMware Solution.
- Para obtener más información sobre la creación de una máquina virtual de Windows Jump Box para acceder y administrar la solución Azure VMware, consulte Acceder a una nube privada de Azure VMware Solution.
- En la máquina virtual de Windows Jump box, descargue los archivos de configuración del dispositivo Citrix ADC VPX.
- Cree segmentos de red NSX-T apropiados en el SDDC de VMware al que se conectan las máquinas virtuales. Para obtener más información, consulte Agregar un segmento de red en Azure VMware Solution
- Para obtener más información sobre cómo instalar una instancia de Citrix ADC VPX en la nube de VMware, consulte Instalar una instancia de Citrix ADC VPX en la nube de VMware.

Configurar una instancia independiente de Citrix ADC VPX en AVS mediante el equilibrador de carga Citrix ADC

Siga estos pasos para configurar la instancia independiente de Citrix ADC VPX en AVS para aplicaciones orientadas a Internet mediante el equilibrador de carga Citrix ADC.

1. Implemente una instancia de Citrix ADC VPX en la nube de Azure. Para obtener más información, consulte Configurar una instancia independiente de Citrix ADC VPX.

   > Nota:
   >
   > Asegúrese de que se implemente en la misma red virtual que Azure VMware Cloud.

2. Configure la instancia de Citrix ADC VPX para acceder a la dirección VIP de Citrix ADC VPX implementada en AVS.

   a) Agregue un servidor virtual de equilibrio de carga.

   ```
   add lb vserver <name> <serviceType> [<vip>] [<port>]
   <!--NeedCopy-->
   ```

   Ejemplo:

   ```
   add lb vserver lb1 HTTPS 172.31.0.6 443
   <!--NeedCopy-->
   ```

   b) Agregue un servicio que se conecte al VIP de Citrix ADC VPX implementado en AVS.

   ```
   add service <name> <ip> <serviceType> <port>
   <!--NeedCopy-->
   ```

   Ejemplo:

   ```
   add service webserver1 192.168.4.10 HTTP 80
   <!--NeedCopy-->
   ```

   c) Enlazar un servicio al servidor virtual de equilibrio de carga.

   ```
   bind lb vserver <name> <serviceName>
   <!--NeedCopy-->
   ```


Ejemplo:

```
bind lb vserver lb1 webserver1
<!--NeedCopy-->
```

Configurar la instancia independiente de Citrix ADC VPX en AVS mediante el equilibrador de carga de Azure

Siga estos pasos para configurar la instancia independiente de Citrix ADC VPX en AVS para aplicaciones orientadas a Internet mediante el equilibrador de carga de Azure.

1. Configure una instancia de Azure Load Balancer en la nube de Azure. Para obtener más información, consulte la documentación de Azure sobre la creación de equilibradores de carga.
2. Agregue la dirección VIP de la instancia de Citrix ADC VPX que se implementa en AVS al grupo back-end.

   El siguiente comando de Azure agrega una dirección IP de back-end al grupo de direcciones de back-end de equilibrio de carga.

```
az network lb address-pool address add
                                    --resource-group <Azure VMC
                                       Resource Group>
                                    --lb-name <LB Name>
                                    --pool-name <Backend pool name
                                       >
                                    --vnet <Azure VMC Vnet>
                                    --name <IP Address name>
                                    --ip-address <VIP of ADC in
                                       VMC>
<!--NeedCopy-->
```

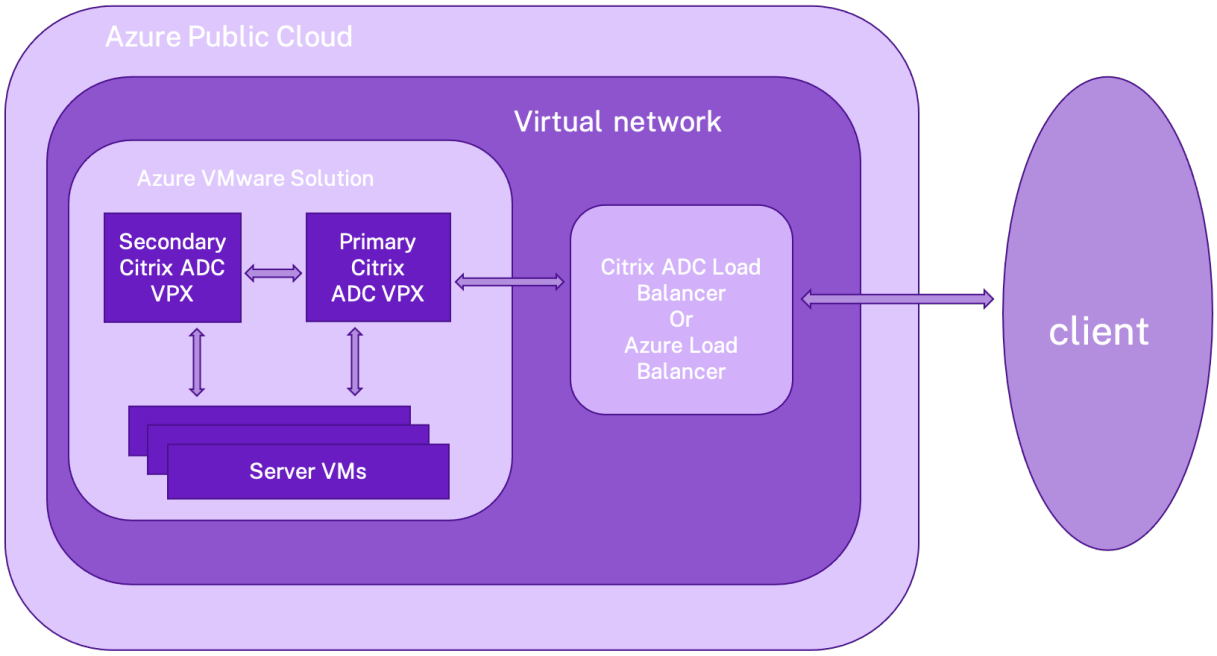
> Nota:
>
> Asegúrese de que el equilibrador de carga de Azure se implemente en la misma red virtual que la nube de Azure VMware.

Configurar una instalación de alta disponibilidad de Citrix ADC VPX en la solución Azure VMware

February 19, 2022

Puede configurar una configuración de alta disponibilidad de Citrix ADC VPX en la solución Azure VMware (AVS) para aplicaciones orientadas a Internet.

El siguiente diagrama muestra el par de alta disponibilidad de Citrix ADC VPX en AVS. Un cliente puede acceder al servicio AVS conectándose al VIP del nodo ADC principal dentro del AVS. Puede lograrlo aprovisionando un equilibrador de carga Citrix ADC o la instancia del equilibrador de carga de Azure fuera de AVS pero en la misma red virtual de Azure. Configure el equilibrador de carga para acceder al VIP del nodo ADC principal dentro del servicio AVS.



Requisitos previos

Antes de comenzar a instalar un dispositivo virtual, lea los siguientes requisitos previos de Azure:

- Para obtener más información sobre la solución Azure VMware y sus requisitos previos, consulte la documentación de Azure VMware Solution.
- Para obtener más información sobre la implementación de la solución Azure VMware, consulte Implementación de una nube privada de Azure VMware Solution.
- Para obtener más información sobre la creación de una máquina virtual de Windows Jump Box para acceder y administrar la solución Azure VMware, consulte Acceder a una nube privada de Azure VMware Solution.

- En la máquina virtual de Windows Jump box, descargue los archivos de configuración del dispositivo Citrix ADC VPX.
- Cree segmentos de red NSX-T apropiados en el SDDC de VMware al que se conectan las máquinas virtuales. Para obtener más información, consulte Agregar un segmento de red en Azure VMware Solution.

Pasos de configuración

Siga estos pasos para configurar la configuración de alta disponibilidad de Citrix ADC VPX en AVS para aplicaciones orientadas a Internet.

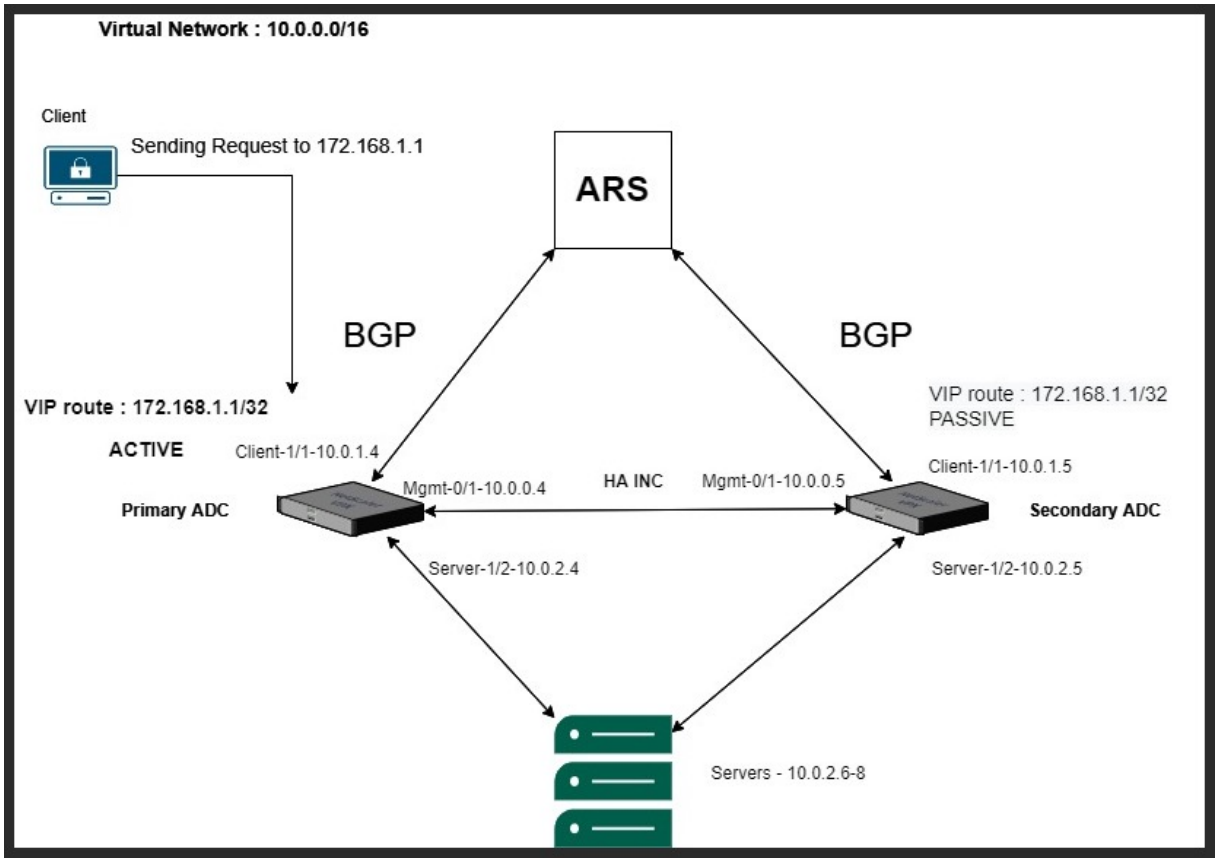
1. Cree dos instancias de Citrix ADC VPX en la nube de VMware. Para obtener más información, consulte Instalar una instancia de Citrix ADC VPX en la nube de VMware.
2. Configure la configuración de Citrix ADC HA. Para obtener más información, consulte Configuración de alta disponibilidad.
3. Configure la configuración de Citrix ADC HA para que sea accesible para las aplicaciones orientadas a Internet.
    - Para configurar la instancia de Citrix ADC VPX mediante el equilibrador de carga de Citrix ADC, consulte Configurar una instancia independiente de Citrix ADC VPX en AVS mediante el equilibrador de carga de Citrix ADC.
    - Para configurar la instancia de Citrix ADC VPX con el equilibrador de carga de Azure, consulte Configurar la instancia independiente de Citrix ADC VPX en AVS con el equilibrador de carga de Azure.

Configurar el servidor de rutas de Azure con un par de alta disponibilidad de Citrix ADC VPX

July 27, 2022

Puede configurar el servidor de rutas de Azure con la instancia Citrix ADC VPX para intercambiar las rutas VIP configuradas con la red virtual mediante el protocolo BGP. El Citrix ADC se puede implementar de forma independiente o en modo HA-INC y, a continuación, se puede configurar con BGP. Esta implementación no requiere un equilibrador de carga (ALB) de Azure delante del par de alta disponibilidad de ADC.

El siguiente diagrama muestra cómo se integra una topología de alta disponibilidad de VPX con el servidor de rutas de Azure. Cada una de las instancias de ADC tiene 3 interfaces: una para la administración, otra para el tráfico del cliente y otra para el tráfico del servidor.



El diagrama de topología utiliza las siguientes direcciones IP.

Ejemplo de configuración de IP para la instancia de ADC principal:

```
NSIP: 10.0.0.4/24
SNIP on 1/1: 10.0.1.4/24
SNIP on 1/2: 10.0.2.4/24
VIP: 172.168.1.1/32
<!--NeedCopy-->
```

Ejemplo de configuración de IP para la instancia de ADC secundaria:

```
NSIP: 10.0.0.5/24
SNIP on 1/1: 10.0.1.5/24
SNIP on 1/2: 10.0.2.5/24
VIP: 172.168.1.1/32
<!--NeedCopy-->
```


Requisitos previos

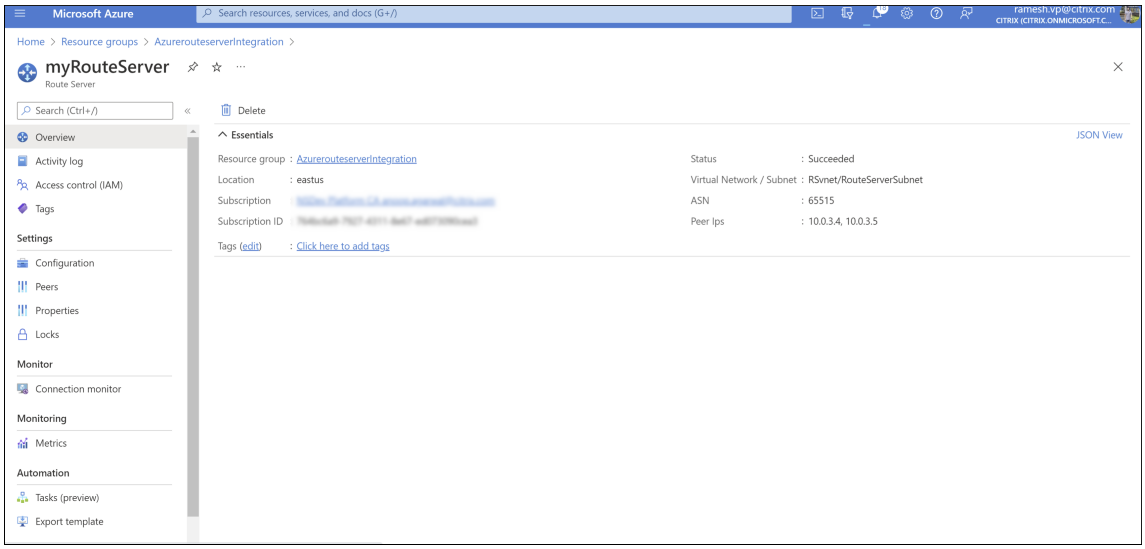
Debe estar familiarizado con la siguiente información antes de implementar una instancia de Citrix ADC VPX en Azure.

- Terminología y detalles de red de Azure. Para obtener más información, consulte Terminología de Azure.
- Descripción general del servidor de rutas de Azure. Para obtener más información, consulte What is Azure Route Server?.
- Funcionamiento de un dispositivo Citrix ADC. Para obtener más información, consulte la documentación de Citrix ADC.
- Redes Citrix ADC. Para obtener más información, consulte ADC Networking.

Cómo configurar un servidor de rutas de Azure con un par de alta disponibilidad de Citrix ADC VPX

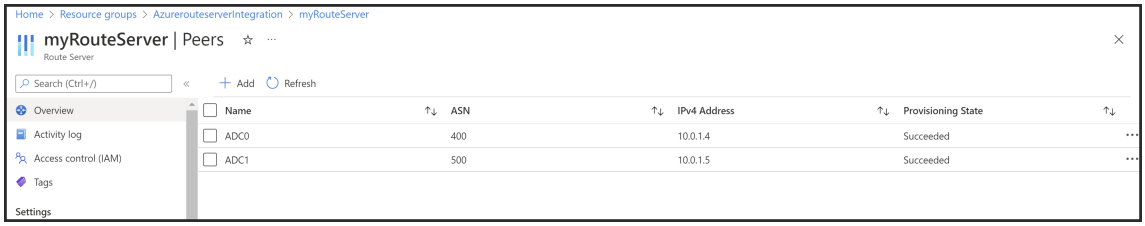
1. Cree un servidor de rutas en el portal de Azure. Para obtener más información, consulte Crear y configurar un servidor de rutas mediante el portal de Azure.

   En el siguiente ejemplo, la subred 10.0.3.0/24 se usa para implementar el servidor Azure. Una vez creado el servidor de rutas, obtenga las direcciones IP del servidor de rutas, por ejemplo: 10.0.3.4, 10.0.3.5.



2. Configure el emparejamiento con el dispositivo virtual de red (NVA) en el portal de Azure. Agregue su instancia Citrix ADC VPX como NVA. Para obtener más información, consulte Configurar el emparejamiento con NVA.

   En el siguiente ejemplo, se utilizan el SNIP de ADC en las interfaces 1/1: 10.0.1.4 y 10.0.1.5, y el ASN: 400 y 500, mientras se agrega el par.



3. Agregue dos instancias Citrix ADC VPX para la configuración de alta disponibilidad.

   Siga estos pasos:

   a) Implemente dos instancias VPX (instancias principal y secundaria) en Azure.
   b) Agregue NIC de cliente y servidor en ambas instancias.
   c) Configure la configuración de HA en ambas instancias mediante la GUI de Citrix ADC.

4. Configure la redirección dinámica en la instancia de ADC principal.

   Configuración de ejemplo:

```
enable ns mode L3 MBF USNIP SRADV DRADV  PMTUD
enable ns feature LB BGP
add ns ip 10.0.1.4 255.255.255.0 -vServer DISABLED -dynamicRouting
    ENABLED
VTYSH
configure terminal
router BGP 400
timers bgp 1 3
neighbor 10.0.3.4 remote-as 65515
neighbor 10.0.3.4 advertisement-interval 3
neighbor 10.0.3.4 fall-over  bfd
neighbor 10.0.3.5 remote-as 65515
neighbor 10.0.3.5 advertisement-interval 3
neighbor 10.0.3.5 fall-over  bfd
address-family ipv4
redistribute kernel
redistribute static
<!--NeedCopy-->
```

5. Configure la redirección dinámica en la instancia de ADC secundaria.

   Configuración de ejemplo:

```
enable ns mode L3 MBF USNIP SRADV DRADV  PMTUD
enable ns feature LB BGP
```



```
3 add ns ip 10.0.1.5 255.255.255.0 -vServer DISABLED -dynamicRouting
      ENABLED
4 VTYSH
5 configure terminal
6 router BGP 500
7 timers bgp 1 3
8 neighbor 10.0.3.4 remote-as 65515
9 neighbor 10.0.3.4 advertisement-interval 3
10 neighbor 10.0.3.4 fall-over  bfd
11 neighbor 10.0.3.5 remote-as 65515
12 neighbor 10.0.3.5 advertisement-interval 3
13 neighbor 10.0.3.5 fall-over  bfd
14 address-family ipv4
15 redistribute kernel
16 redistribute static
17 <!--NeedCopy-->
```

6. Verifique los pares de BGP establecidos mediante los comandos BGP en la interfaz de shell de VTY. Para obtener más información, consulte Verificación de la configuración de BGP.

```
1 show ip bgp neighbors
2 <!--NeedCopy-->
```

7. Configure el servidor virtual LB en la instancia de ADC principal.

   Configuración de ejemplo:

```
1 add ns ip 172.16.1.1 255.255.255.255 -type VIP -hostRoute ENABLED
2 add lbvserver v1 HTTP 172.16.1.1 80
3 add service s1 10.0.2.6 HTTP 80
4 bind lbvserver v1 s1
5 enable ns feature lb
6 <!--NeedCopy-->
```

   Un cliente en la misma red virtual que la instancia Citrix ADC VPX ahora puede acceder al servidor virtual LB. En este caso, la instancia VPX de ADC anuncia la ruta VIP al servidor de rutas de Azure.

Agregar configuración de escalabilidad automática de Azure

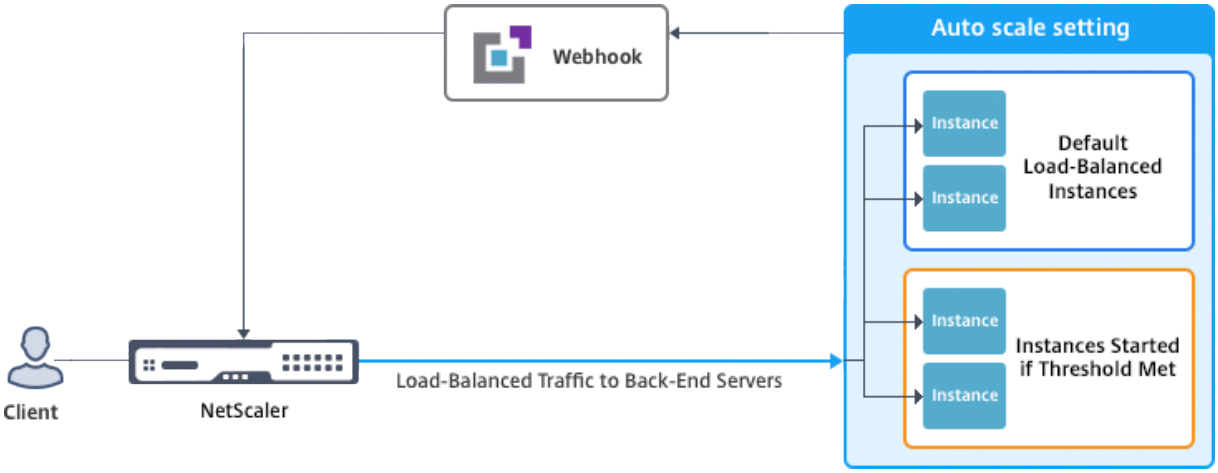
June 22, 2022

El alojamiento eficiente de aplicaciones en una nube implica una gestión fácil y rentable de los recursos en función de la demanda de la aplicación. Para satisfacer la creciente demanda, debe ampliar los recursos de la red. Ya sea que la demanda disminuya, debe reducir la escala para evitar el coste innecesario de los recursos inactivos. Para minimizar el coste de ejecutar la aplicación, debe supervisar constantemente el tráfico, la memoria y el uso de la CPU, y así sucesivamente. Sin embargo, la supervisión manual del tráfico es engorrosa. Para que el entorno de aplicaciones se amplíe o disminuya dinámicamente, debe automatizar los procesos de supervisión del tráfico y de ampliación de los recursos siempre que sea necesario.

Puede utilizar Autoscale con conjuntos de básculas de máquinas virtuales (VMSS) de Azure para la implementación de alta disponibilidad y autónoma de VPX Multi-IP en Azure.

Integrada con la función Azure VMSS y Autoscale, la instancia de Citrix ADC VPX ofrece las siguientes ventajas:

- Equilibrio de carga y administración: Configura automáticamente los servidores para escalarlos y reducirlos, en función de la demanda. La instancia de Citrix ADC VPX detecta automáticamente la configuración de escalabilidad automática de VMSS en la misma red virtual en la que se implementa la instancia VPX o las redes virtuales interconectadas que están en la misma suscripción de Azure. Puede seleccionar la configuración de escalabilidad automática de VMSS para equilibrar la carga. Esto se hace mediante la configuración automática de la dirección IP virtual y la dirección IP de subred de Citrix ADC en la instancia VPX.
- Alta disponibilidad: Detecta grupos de escalabilidad automática y servidores de equilibrio de carga.
- Mejor disponibilidad de red: La instancia VPX admite servidores back-end en diferentes redes virtuales (VNEs).



Para obtener más información, consulte el siguiente tema de Azure

- Documentación de conjuntos de escalas de máquinas virtuales
- Descripción general de la escalabilidad automática en máquinas virtuales Microsoft Azure, servicios en la nube y aplicaciones web

Antes de comenzar

1. Lea las pautas de uso relacionadas con Azure. Para obtener más información, consulte Implementación de una instancia Citrix ADC VPX en Microsoft Azure.
2. Cree una o más instancias de Citrix ADC VPX con tres interfaces de red en Azure según sus requisitos (implementación independiente o de alta disponibilidad).
3. Abra el puerto TCP 9001 en el grupo de seguridad de red de la interfaz 0/1 de la instancia VPX. La instancia VPX usa este puerto para recibir la notificación de escalamiento horizontal y vertical.
4. Cree un VMSS de Azure en la misma red virtual en la que se implementa la instancia de Citrix ADC VPX. Si la instancia de VMSS y Citrix ADC VPX se implementa en diferentes redes virtuales de Azure, se deben cumplir las siguientes condiciones:

   - Ambas redes virtuales deben estar en la misma suscripción a Azure.
   - Las dos redes virtuales deben estar conectadas mediante la función de emparejamiento de redes virtuales de Azure.

   Si no tiene una configuración de VMSS existente, realice las siguientes tareas:

   a) Crear un VMSS

   b) Habilitar escalado automático en VMSS

   c) Crear directivas de escalado y escalado horizontal en la configuración de Escala automática de VMSS

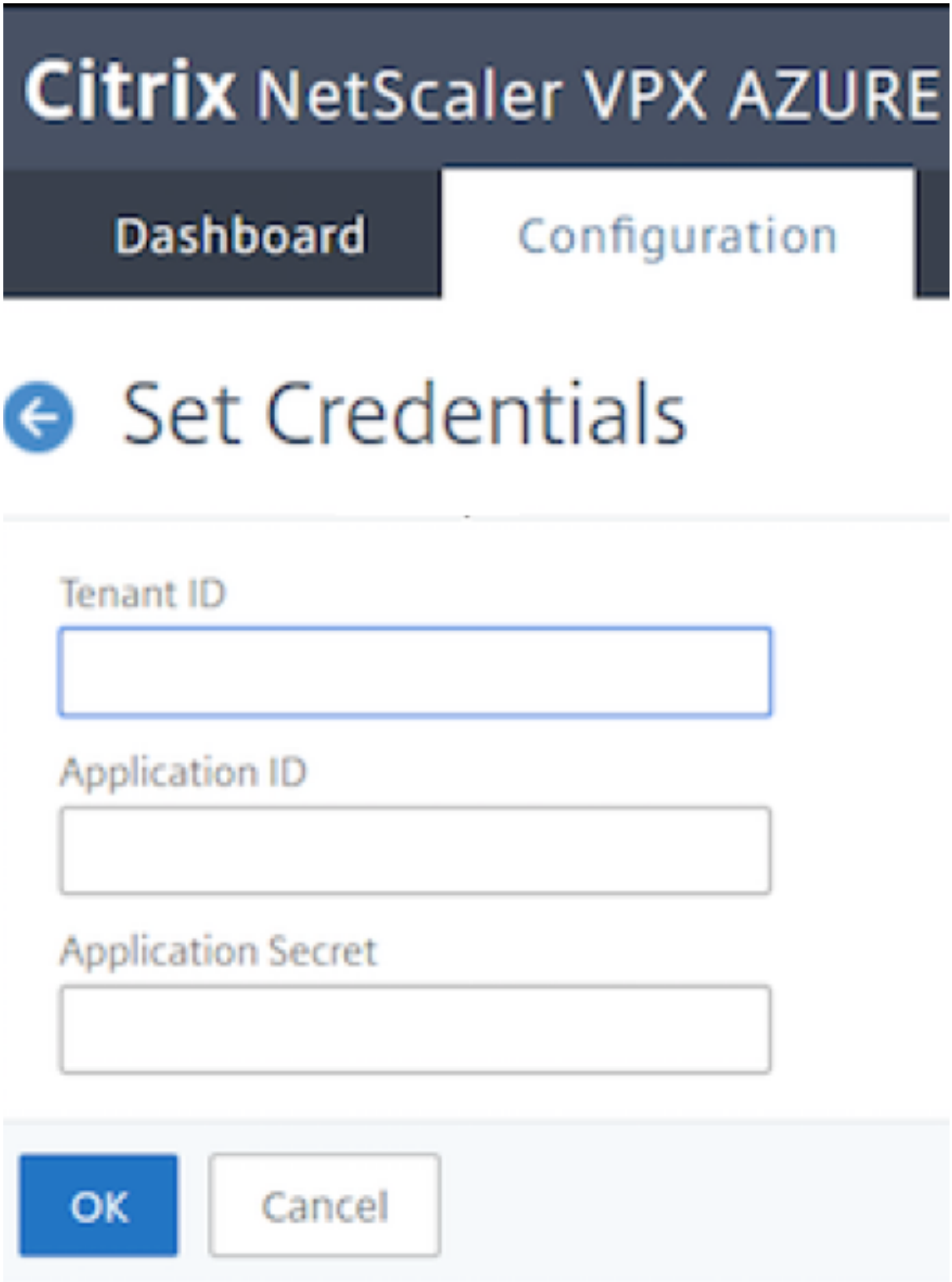
   Para obtener más información, consulte Descripción general de la escalabilidad automática con conjuntos de básculas de máquinas virtuales de Azure.
5. Cree una aplicación de Azure Active Directory (ADD) y una entidad de servicio que pueda tener acceso a los recursos. Asigne el rol colaborador a la aplicación AAD recién creada. Para obtener más información, consulte Uso del portal para crear una aplicación y un principal de servicio de Azure Active Directory que pueda acceder a los recursos.

Agregar VMSS a una instancia de Citrix ADC VPX

Puede agregar la configuración Escala automática a una instancia VPX con un solo clic mediante la GUI. Siga estos pasos para agregar la configuración Escala automática a la instancia VPX:

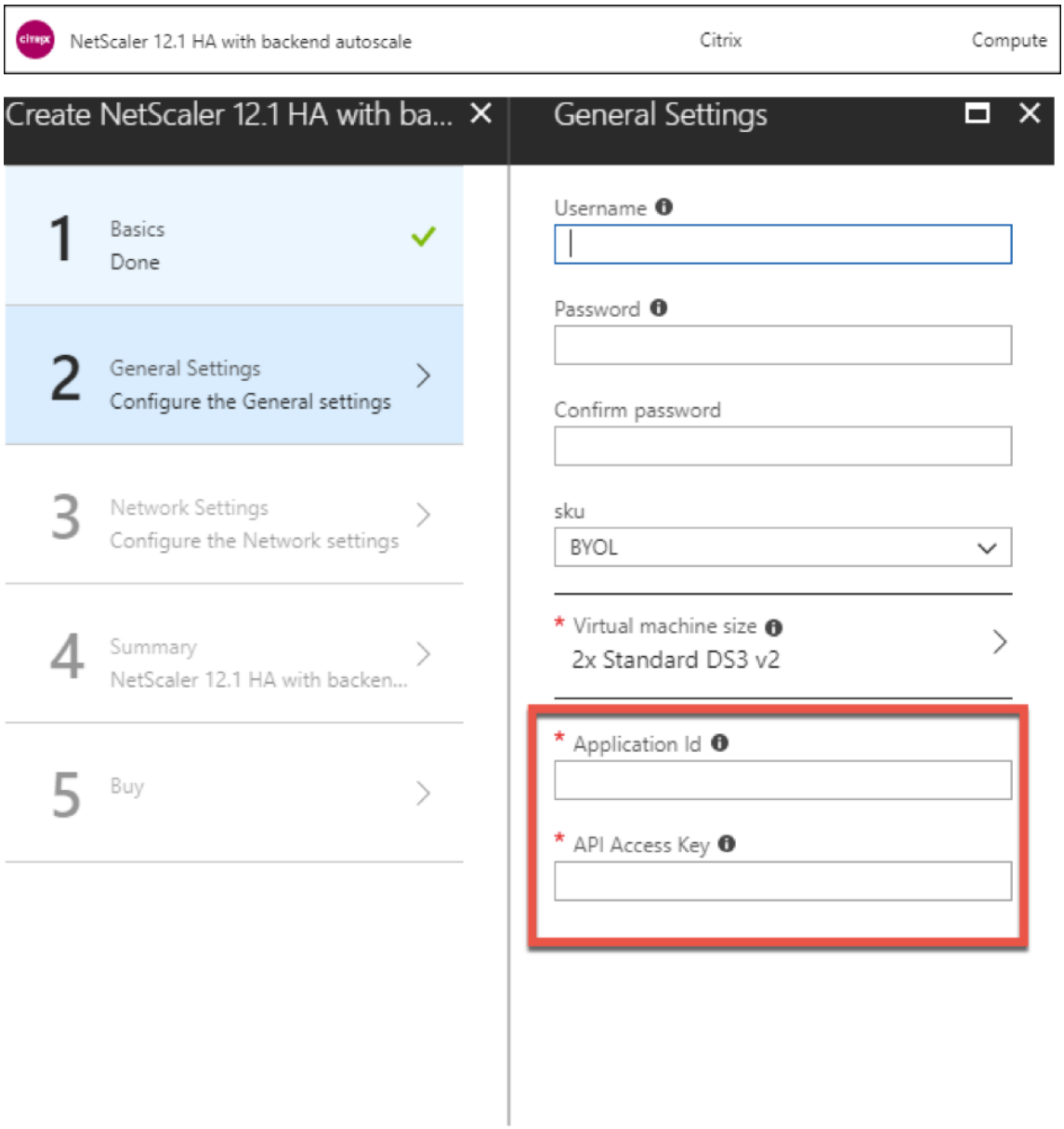
1. Inicie sesión en la instancia de VPX.

2. Cuando inicie sesión en la instancia de Citrix ADC VPX por primera vez, verá la página Establecer credenciales. Agregue las credenciales de Azure necesarias para que funcione la función de escalado automático.



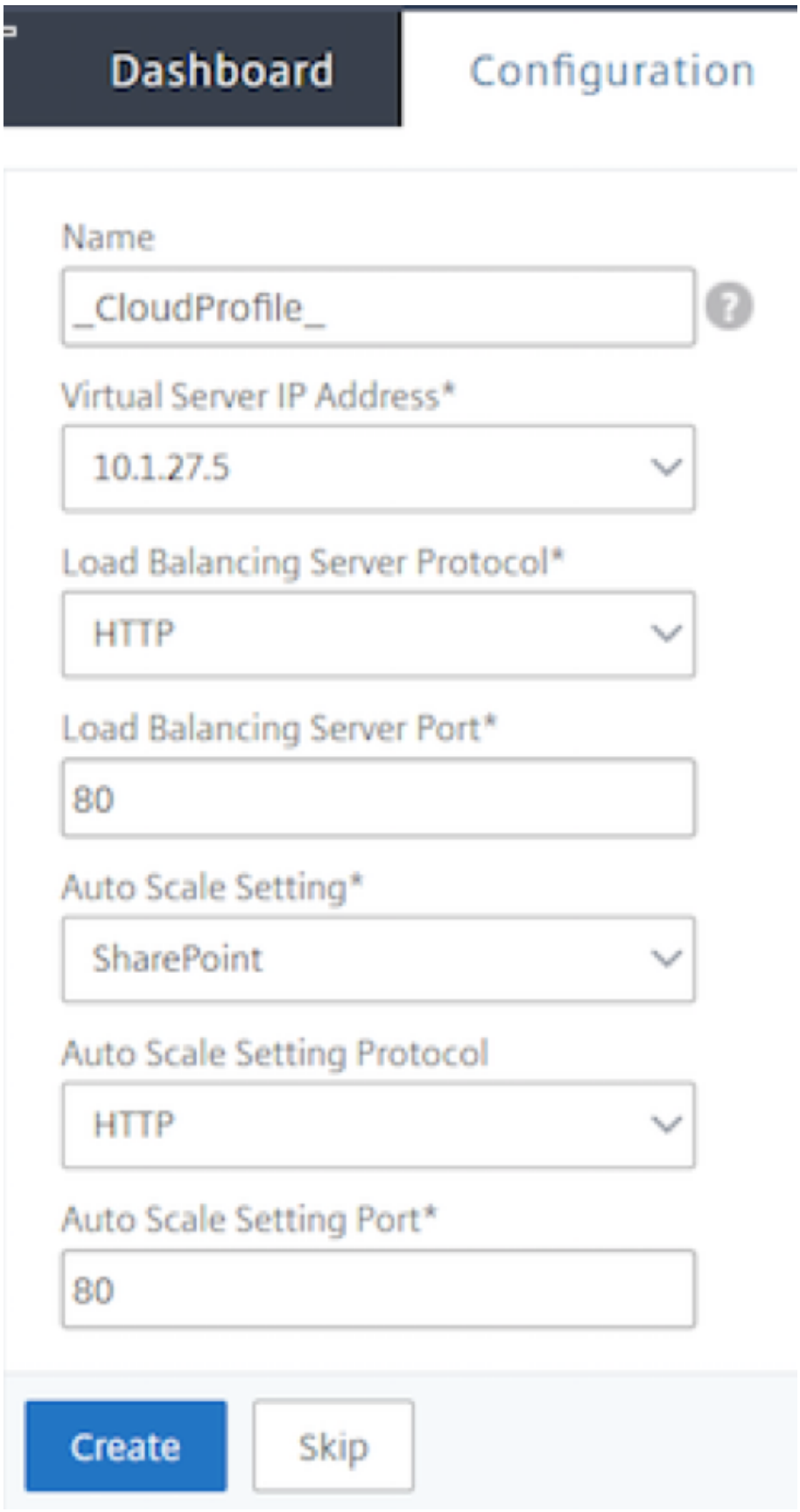
La página Establecer credenciales aparece solo cuando el ID de aplicación y la clave de acceso a la API no están configurados o el ID de aplicación y las claves de acceso de API correctas (igual que el secreto de la aplicación) no están configurados en el portal de Azure.

Cuando implementa la oferta “NetScaler 12.1 HA con escalado automático de backend” desde Azure Marketplace, el portal de Azure solicita las credenciales principales del servicio de Azure (ID de aplicación y clave de acceso de API).



Para obtener información sobre cómo crear un ID de aplicación, consulte Agregar una aplicación y crear una clave de acceso o un secreto de aplicación, consulte Configurar una aplicación cliente para acceder a las API web.

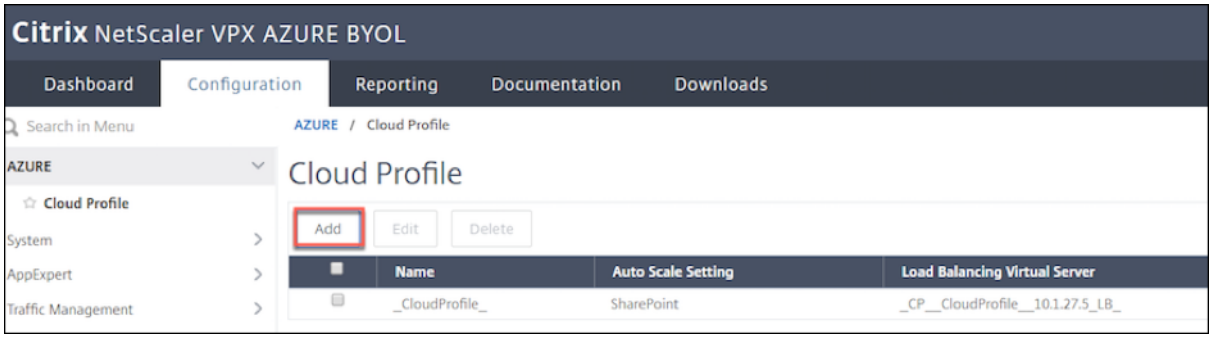
3. En la página de perfil de nube predeterminada, introduzca los detalles, como se muestra en el siguiente ejemplo, y haga clic en Crear.



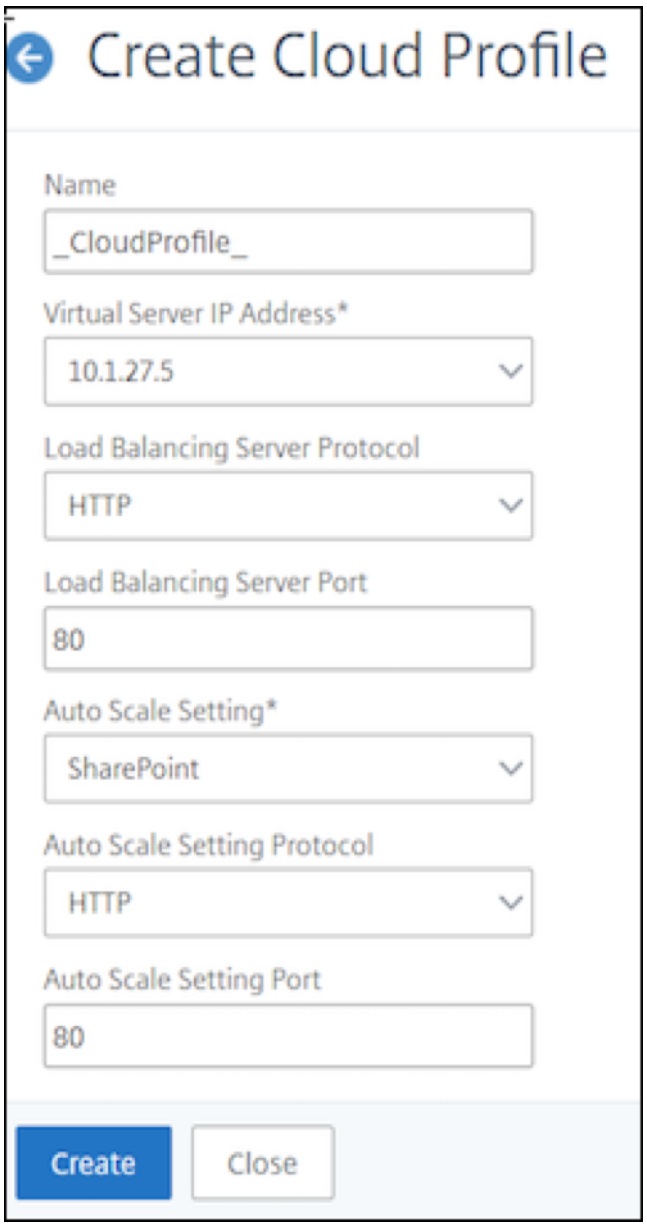
Puntos a tener en cuenta al crear un perfil de nube

- La dirección IP del servidor virtual se rellena automáticamente desde la dirección IP libre disponible para la instancia VPX. Para obtener más información, consulte Asignación de varias direcciones IP a máquinas virtuales mediante el portal de Azure.
- La configuración de escalabilidad automática se rellena previamente desde la instancia de VMSS que está conectada a la instancia de Citrix ADC VPX en la misma red virtual o en redes virtuales interconectadas. Para obtener más información, consulte Descripción general de la escalabilidad automática con conjuntos de básculas de máquinas virtuales de Azure.
- Al seleccionar el protocolo y el puerto del grupo de Auto Scaling, asegúrese de que los servidores escuchen en los protocolos y puertos, y de que vincule el monitor correcto en el grupo de servicios. De forma predeterminada, se utiliza el monitor TCP.
- Para el protocolo SSL de tipo Auto Scaling, después de crear el perfil de nube, el servidor virtual de equilibrio de carga o el grupo de servicios no funcionan porque falta un certificado. Puede enlazar el certificado al servidor virtual o grupo de servicios manualmente.

Después del primer inicio de sesión, si desea crear un perfil de nube, en la GUI vaya a **Sistema > Azure > Perfil de nube** y haga clic en **Agregar**.



Aparecerá la página de configuración Crear perfil de nube.



Cloud Profile crea un servidor virtual de equilibrio de carga de Citrix ADC y un grupo de servicios con miembros (servidores) como servidores del grupo de Auto Scaling. Los servidores back-end deben ser accesibles a través del SNIP configurado en la instancia VPX.

Para ver la información relacionada con la escalabilidad automática en el portal de Azure, vaya a **Todos los servicios > Conjunto de escalas de máquinas virtuales > Seleccionar conjunto de escalas de máquinas virtuales > Escalado**.

Etiquetas de Azure para la implementación de Citrix ADC VPX

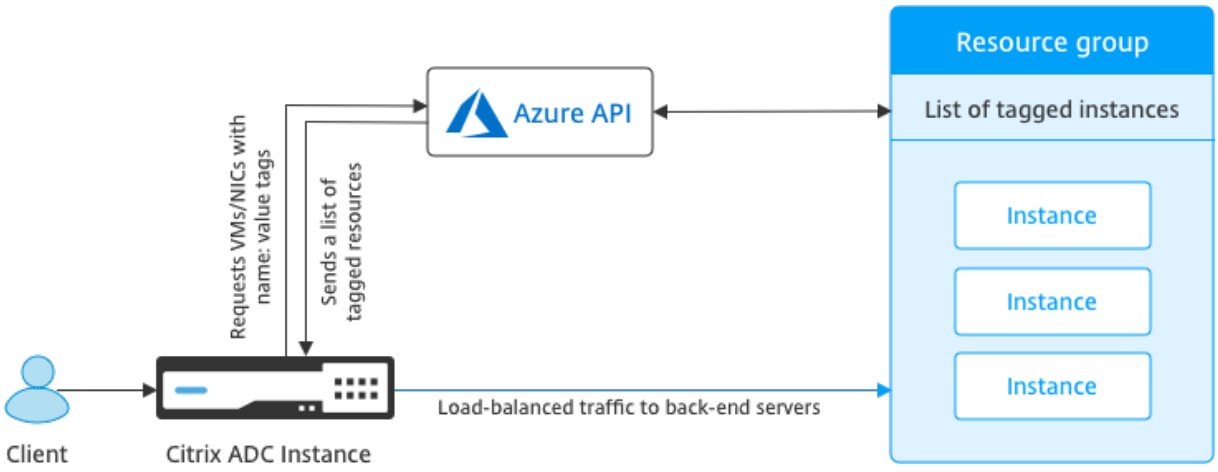
August 20, 2021

En el portal en la nube de Azure, puede etiquetar recursos con un nombre: par de valores (como Dept: Finance) para categorizar y ver los recursos de todos los grupos de recursos y, dentro del portal, entre suscripciones. El etiquetado es útil cuando necesita organizar los recursos para la facturación, la administración o la automatización.

Cómo funciona la etiqueta de Azure para la implementación de VPX

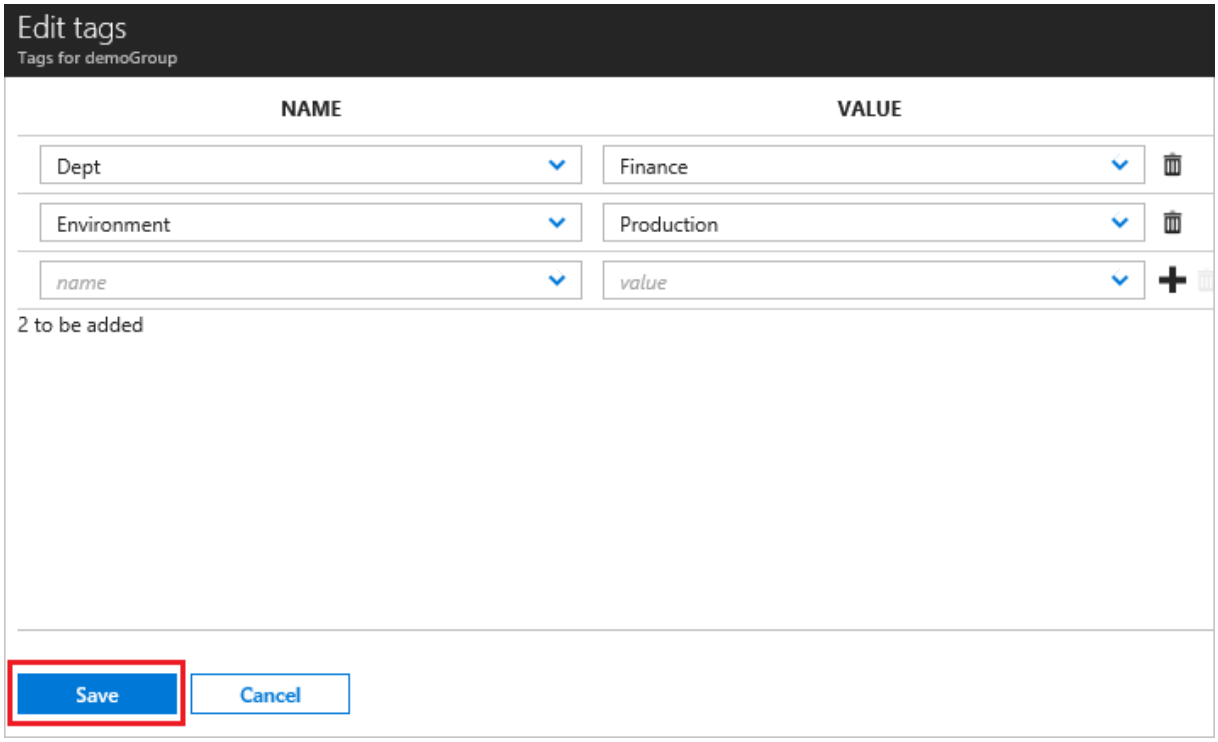
Para instancias independientes y de alta disponibilidad de Citrix ADC VPX implementadas en Azure Cloud, ahora puede crear grupos de servicios de equilibrio de carga asociados con una etiqueta de Azure. La instancia VPX supervisa constantemente las máquinas virtuales de Azure (servidores back-end) y las interfaces de red (NIC), o ambas, con la etiqueta respectiva y actualiza el grupo de servicios en consecuencia.

La instancia VPX crea el grupo de servicios que equilibra la carga de los servidores back-end mediante etiquetas. La instancia consulta la API de Azure para todos los recursos que están etiquetados con un nombre de etiqueta y un valor de etiqueta concretos. Dependiendo del período de sondeo asignado (de forma predeterminada 60 segundos), la instancia VPX sondea periódicamente la API de Azure y recupera los recursos disponibles con el nombre de etiqueta y los valores de etiqueta asignados en la GUI de VPX. Cada vez que se agrega o elimina una máquina virtual o NIC con la etiqueta adecuada, el ADC detecta el cambio respectivo y agrega o elimina automáticamente la dirección IP de la máquina virtual o de la NIC del grupo de servicios.



Antes de comenzar

Antes de crear grupos de servicios de equilibrio de carga de Citrix ADC, agregue una etiqueta a los servidores de Azure. Puede asignar la etiqueta a la máquina virtual o a la NIC.



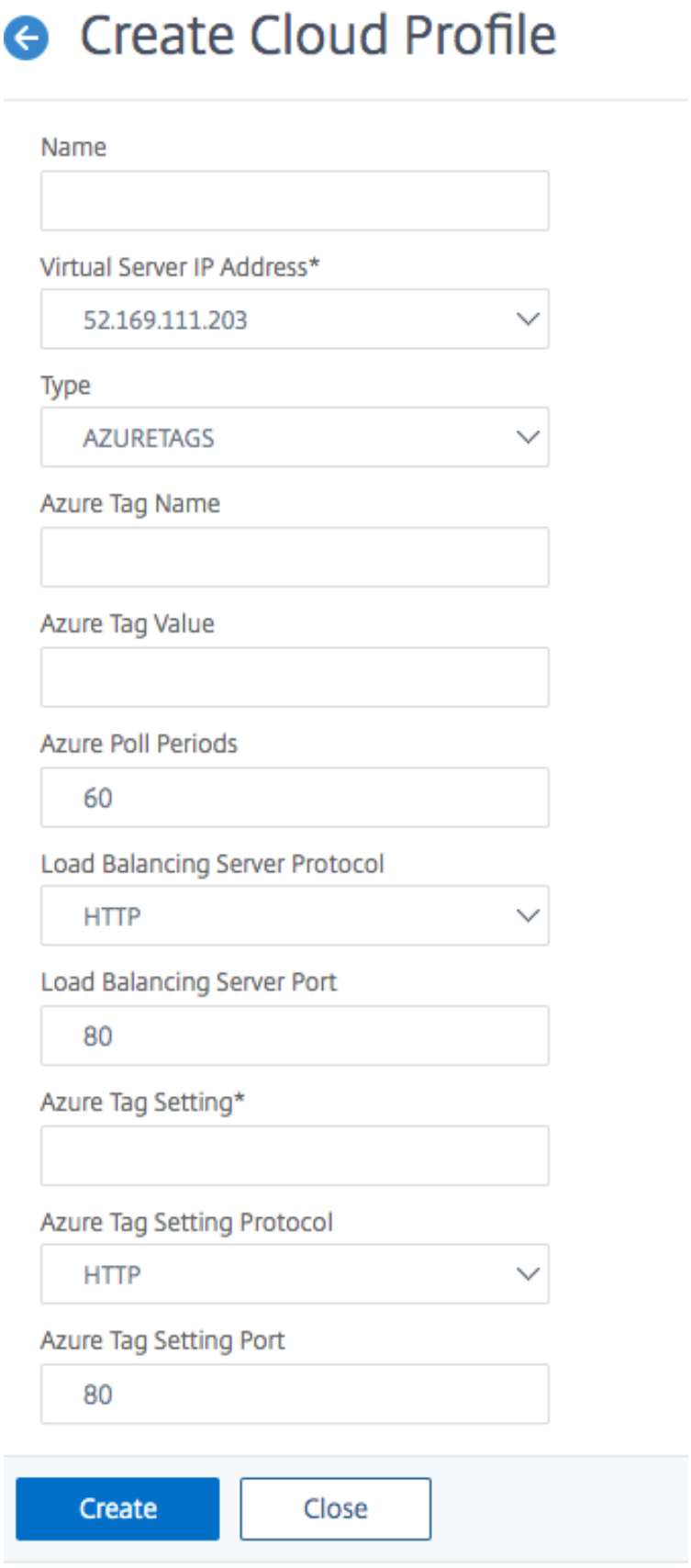
Para obtener más información sobre cómo agregar etiquetas de Azure, consulte el documento de Microsoft Utilizar etiquetas para organizar los recursos de Azure.

> Nota Los comandos de la CLI de
> ADC para agregar la configuración de etiquetas de Azure admiten nombres de etiquetas y valores de etiquetas que comienzan solo con números o alfabetos y no con otros caracteres de teclado.

Cómo agregar la configuración de etiquetas de Azure mediante la GUI de VPX

Puede agregar el perfil de nube de etiquetas de Azure a una instancia VPX mediante la GUI de VPX para que la instancia pueda equilibrar la carga de los servidores back-end mediante la etiqueta especificada. Siga estos pasos:

1. Desde la GUI de VPX, vaya a **Configuración > Azure > Perfil de nube**.
2. Haga clic en Agregar para crear un perfil de nube. Se abrirá la ventana de perfil de nube.



1. Introduzca valores para los siguientes campos:
   - Nombre: Agrega un nombre para su perfil
   - Dirección IP del servidor virtual: La dirección IP del servidor virtual se rellena automáticamente desde la dirección IP libre disponible para la instancia VPX. Para obtener más información, consulte Asignación de varias direcciones IP a máquinas virtuales mediante el portal de Azure.
   - Tipo: En el menú, seleccione AZURETAGS.
   - Nombre de etiqueta de Azure: Introduzca el nombre que ha asignado a las máquinas virtuales o NIC en el portal de Azure.
   - Valor de etiqueta de Azure: Especifique el valor que ha asignado a las máquinas virtuales o NIC en Azure Portal.
   - Períodos de encuesta de Azure: De forma predeterminada, el período de encuesta es de 60 segundos, que es el valor mínimo. Puede cambiarlo de acuerdo a su requerimiento.
   - Protocolo de servidor de equilibrio de carga: Seleccione el protocolo en el que escucha el equilibrador de carga.
   - Puerto del servidor de equilibrio de carga: Seleccione el puerto en el que escucha el equilibrador de carga.
   - Configuración de etiqueta de Azure: Nombre del grupo de servicios que se creará para este perfil de nube.
   - Protocolo de configuración de etiquetas de Azure: Seleccione el protocolo en el que escuchan los servidores back-end.
   - Puerto de configuración de etiquetas de Azure: Seleccione el puerto en el que escuchan los servidores back-end.
2. Haga clic en **Crear**.

Se crean un servidor virtual de equilibrador de carga y un grupo de servicios para las máquinas virtuales o NIC etiquetadas. Para ver el servidor virtual del equilibrador de carga, desde la GUI de VPX, vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.

Cómo agregar la configuración de etiquetas de Azure mediante VPX CLI

Escriba el siguiente comando en Citrix ADC CLI para crear un perfil de nube para etiquetas de Azure.

```
1 add cloud profile `<profile name>` -type azuretags -vServerName `<
    vserver name>` -serviceType HTTP -IPAddress `<vserver IP address>` -
    port 80 -serviceGroupName `<service group name>` -
    boundServiceGroupSvcType HTTP -vsvrbindsvcport 80 -azureTagName `<
    Azure tag specified on Azure portal>` -azureTagValue `<Azure value
    specified on the Azure portal>` -azurePollPeriod 60
2
```



```
<!--NeedCopy-->
```

> Importante
> Debe guardar todas las configuraciones; de lo contrario, las configuraciones se perderán después de reiniciar la instancia. Escriba `save config`.

Ejemplo 1: Aquí hay un comando de ejemplo para un perfil de nube para el tráfico HTTP de todas las VMS/NIC de Azure etiquetadas con el par "MyTagName/MyTagValue":

```
add cloud profile MyTagCloudProfile -type azuretags -vServerName
    MyTagVServer -serviceType HTTP -IPAddress 40.115.116.57 -port 80 -
    serviceGroupName MyTagsServiceGroup -boundServiceGroupSvcType HTTP -
    vsvrbindsvcport 80 -azureTagName myTagName -azureTagValue myTagValue
     -azurePollPeriod 60
Done
<!--NeedCopy-->
```

Para mostrar el perfil de nube, escriba `show cloudprofile`.

Ejemplo 2: El siguiente comando CLI imprime información sobre el perfil de nube recién agregado en el ejemplo 1.

```
show cloudprofile
1)    Name:  MyTagCloudProfile Type:  azuretags         VServerName:
    MyTagVServer ServiceType:  HTTP       IPAddress:  52.178.209.133
    Port:  80               ServiceGroupName:  MyTagsServiceGroup
    BoundServiceGroupSvcType:  HTTP
       Vsvrbindsvcport:  80     AzureTagName:  myTagName AzureTagValue:
           myTagValue AzurePollPeriod:  60     GraceFul:  NO
          Delay:  60
<!--NeedCopy-->
```

Para eliminar un perfil de nube, escriba rm cloud profile <`cloud profile name`>

Ejemplo 3: el siguiente comando quita el perfil de nube creado en el ejemplo 1.

```
> rm cloudprofile MyTagCloudProfile
  Done
<!--NeedCopy-->
```


Solucionar problemas

Problema: En casos muy raros, es posible que el comando de la CLI “rm cloud profile” no elimine el grupo de servicios y los servidores asociados con el perfil de nube eliminado. Esto sucede cuando el comando se emite segundos antes de que transcurra el período de sondeo del perfil de nube que se está eliminando.

Solución: Elimine manualmente los grupos de servicios restantes introduciendo el siguiente comando CLI para cada uno de los grupos de servicios restantes:

```
#> rm servicegroup <serviceGroupName>

<!--NeedCopy-->
```

Elimine también cada uno de los servidores restantes introduciendo el siguiente comando CLI para cada uno de los servidores restantes:

```
#> rm server <name>
<!--NeedCopy-->
```

Problema: Si agrega una configuración de etiqueta de Azure a una instancia VPX mediante la CLI, el proceso rain_tags continúa ejecutándose en un nodo de par HA tras un reinicio en caliente.

Solución: Termine manualmente el proceso en el nodo secundario después de un reinicio en caliente. Desde la CLI del nodo de alta disponibilidad secundario, salga al símbolo del shell:

```
#> shell

<!--NeedCopy-->
```

Utilice el siguiente comando para eliminar el proceso rain_tags:

```
# PID=`ps -aux | grep rain_tags | awk '{
 print $2 }
 '`; kill -9 $PID

<!--NeedCopy-->
```

Problema: Es posible que la instancia VPX no pueda acceder a los servidores back-end y que la instancia VPX los informe como DOWN, a pesar de estar en buen estado.

Solución: Asegúrese de que la instancia VPX puede alcanzar la dirección IP etiquetada correspondiente al servidor back-end. Para una NIC etiquetada, ésta es la dirección IP de la NIC; mientras que para una VM etiquetada, ésta es la dirección IP principal de la VM. Si la VM/NIC reside en otra Azure VNet diferente, asegúrese de que el peering de VNet esté habilitado.

Configurar GSLB en instancias de Citrix ADC VPX

August 20, 2021

Los dispositivos Citrix ADC configurados para el equilibrio de carga global del servidor (GSLB) proporcionan recuperación ante desastres y disponibilidad continua de las aplicaciones al protegerse contra los puntos de falla en una WAN. GSLB puede equilibrar la carga entre los centros de datos dirigiendo las solicitudes de los clientes al centro de datos más cercano o de mejor rendimiento, o a centros de datos sobrevivientes si se produce una interrupción.

En esta sección se describe cómo habilitar GSLB en instancias VPX en dos sitios en un entorno de Microsoft Azure, mediante comandos de Windows PowerShell.

> **Nota**
>
> Para obtener más información sobre GSLB, consulte Equilibrio de carga global del servidor.

Puede configurar GSLB en una instancia Citrix ADC VPX en Azure, en dos pasos:

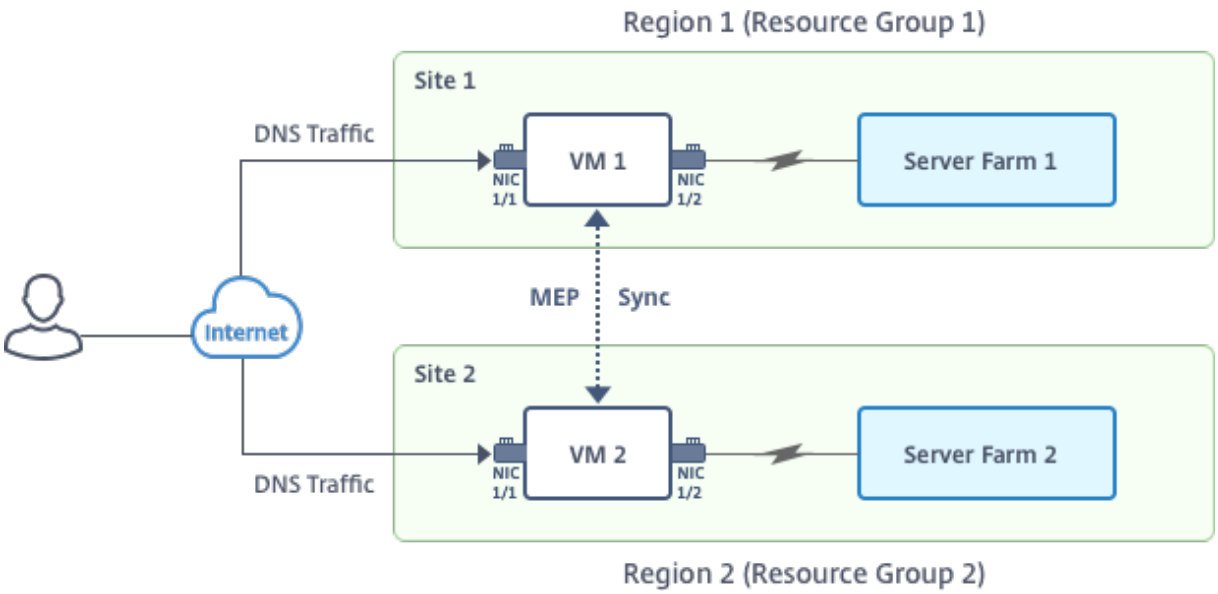
1. Cree una instancia VPX con varias NIC y varias direcciones IP en cada sitio.
2. Habilite GSLB en las instancias VPX.

> **Nota**
>
> Para obtener más información sobre la configuración de varias NIC y direcciones IP, consulte: Configurar varias direcciones IP para una instancia Citrix ADC VPX en modo independiente mediante comandos de PowerShell.

Caso

Este caso incluye dos sitios: Sitio 1 y Sitio 2. Cada sitio tiene una máquina virtual (VM1 y VM2) configurada con varias NIC, varias direcciones IP y GSLB.

Ilustración. Configuración de GSLB implementada en dos sitios: Sitio 1 y Sitio 2.



En este caso, cada VM tiene tres NIC: NIC 0/1, 1/1 y 1/2. Cada NIC puede tener varias direcciones IP privadas y públicas. Las NIC se configuran para los siguientes fines.

- NIC 0/1: Para servir el tráfico de administración
- NIC 1/1: Para servir el tráfico del lado del cliente
- NIC 1/2: Para comunicarse con servidores back-end

Para obtener información sobre las direcciones IP configuradas en cada NIC en este caso, consulte la sección Detalles de configuración IP .

Parámetros

A continuación se presentan parámetros de ejemplo de configuración para este caso en este documento. Puede usar diferentes configuraciones si lo quiere.

```
$location="West Central US"

$vnetName="NSVPX-vnet"

$RGName="multiIP-RG"

$prmStorageAccountName="multiipstorageaccnt"

$avSetName="MultiIP-avset"

$vmSize="Standard_DS3_V2"
<!--NeedCopy-->
```


Nota: El requisito mínimo para una instancia VPX es 2 vCPU y 2 GB de RAM.

```
$publisher="citrix"

$offer="netscalervpx111"

$sku="netscalerbyol"

$version="latest"

$vmNamePrefix="MultiIPVPX"

$nicNamePrefix="MultiipVPX"

$osDiskSuffix="osdiskdb"

$numberOfVMs=1

$ipAddressPrefix="10.0.0."

$ipAddressPrefix1="10.0.1."

$ipAddressPrefix2="10.0.2."

$pubIPName1="MultiIP-pip1"

$pubIPName2="MultiIP-pip2"

$IpConfigName1="IPConfig1"

$IPConfigName2="IPConfig-2"

$IPConfigName3="IPConfig-3"

$IPConfigName4="IPConfig-4"

$frontendSubnetName="default"

$backendSubnetName1="subnet_1"

$backendSubnetName2="subnet_2"

$suffixNumber=10
```



```
<!--NeedCopy-->
```

Crear una VM

Siga los pasos del 1 al 10 para crear VM1 con varias NIC y varias direcciones IP, mediante comandos de PowerShell:

1. Crear grupo de recursos
2. Crear cuenta de almacenamiento
3. Crear conjunto de disponibilidad
4. Crear red virtual
5. Crear dirección IP pública
6. Crear NIC
7. Crear objeto de configuración de VM
8. Obtener credenciales y establecer propiedades del sistema operativo para la VM
9. Agregar NIC
10. Especificar el disco del sistema operativo y crear VM

Después de completar todos los pasos y comandos para crear VM1, repita estos pasos para crear VM2 con parámetros específicos.

Crear grupo de recursos

```
New-AzureRMResourceGroup -Name $RGName -Location $location
<!--NeedCopy-->
```

Crear cuenta de almacenamiento

```
$prmStorageAccount=New-AzureRMStorageAccount -Name
    $prmStorageAccountName -ResourceGroupName $RGName -Type Standard_LRS
     -Location $location
<!--NeedCopy-->
```


Crear conjunto de disponibilidad

```
$avSet=New-AzureRMAvailabilitySet -Name $avSetName -ResourceGroupName
    $RGName -Location $location
<!--NeedCopy-->
```

Crear red virtual

1. Agregue subredes.

```
$subnet1=New-AzureRmVirtualNetworkSubnetConfig -Name
    $frontendSubnetName -AddressPrefix ”10.0.0.0/24”
$subnet2=New-AzureRmVirtualNetworkSubnetConfig -Name
    $backendSubnetName1 -AddressPrefix ”10.0.1.0/24”
$subnet3=New-AzureRmVirtualNetworkSubnetConfig -Name
    $backendSubnetName2 -AddressPrefix ”10.0.2.0/24”
<!--NeedCopy-->
```

2. Agregar objeto de red virtual.

```
$vnet=New-AzureRmVirtualNetwork -Name $vnetName -ResourceGroupName
     $RGName -Location $location -AddressPrefix 10.0.0.0/16 -Subnet
     $subnet1, $subnet2, $subnet3
<!--NeedCopy-->
```

3. Recuperar subredes.

```
$frontendSubnet=$vnet.Subnets|?{
 $\_.Name -eq $frontendSubnetName }

$backendSubnet1=$vnet.Subnets|?{
 $\_.Name -eq $backendSubnetName1 }

$backendSubnet2=$vnet.Subnets|?{
 $_.Name -eq $backendSubnetName2 }

<!--NeedCopy-->
```


Crear dirección IP pública

```
$pip1=New-AzureRmPublicIpAddress -Name $pubIPName1 -ResourceGroupName
    $RGName -Location $location -AllocationMethod Dynamic
$pip2=New-AzureRmPublicIpAddress -Name $pubIPName2 -ResourceGroupName
    $RGName -Location $location -AllocationMethod Dynamic
<!--NeedCopy-->
```

Crear NIC

Crear NIC 0/1

```
$nic1Name=$nicNamePrefix + $suffixNumber + "-Mgmnt"
$ipAddress1=$ipAddressPrefix + $suffixNumber
$IPConfig1=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName1 -
    SubnetId $frontendSubnet.Id -PublicIpAddress $pip1 -PrivateIpAddress
     $ipAddress1 -Primary
$nic1=New-AzureRMNetworkInterface -Name $nic1Name -ResourceGroupName
    $RGName -Location $location -IpConfiguration $IpConfig1
<!--NeedCopy-->
```

Crear NIC 1/1

```
$nic2Name $nicNamePrefix + $suffixNumber + "-frontend"
$ipAddress2=$ipAddressPrefix1 + ($suffixNumber)
$ipAddress3=$ipAddressPrefix1 + ($suffixNumber + 1)
$IPConfig2=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName2 -
    PublicIpAddress $pip2 -SubnetId $backendSubnet1.Id  -
    PrivateIpAddress $ipAddress2  -Primary
$IPConfig3=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName3 -
    SubnetId $backendSubnet1.Id  -PrivateIpAddress $ipAddress3
nic2=New-AzureRMNetworkInterface -Name $nic2Name -ResourceGroupName
    $RGName -Location $location -IpConfiguration $IpConfig2, $IpConfig3
<!--NeedCopy-->
```

Crear NIC 1/2

```
$nic3Name=$nicNamePrefix + $suffixNumber + "-backend"
$ipAddress4=$ipAddressPrefix2 + ($suffixNumber)
```



```
3 $IPConfig4=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName4 -
    SubnetId $backendSubnet2.Id -PrivateIpAddress $ipAddress4 -Primary
4 $nic3=New-AzureRMNetworkInterface -Name $nic3Name -ResourceGroupName
    $RGName -Location $location -IpConfiguration $IpConfig4
5 <!--NeedCopy-->
```

Crear objeto de configuración de VM

```
1 $vmName=$vmNamePrefix
2 $vmConfig=New-AzureRMVMConfig -VMName $vmName -VMSize $vmSize -
    AvailabilitySetId $avSet.Id
3 <!--NeedCopy-->
```

Obtener credenciales y establecer propiedades del sistema operativo

```
1 $cred=Get-Credential -Message "Type the name and password for VPX login
    ."
2 $vmConfig=Set-AzureRMVMOperatingSystem -VM $vmConfig -Linux -
    ComputerName $vmName -Credential $cred
3 $vmConfig=Set-AzureRMVMSourceImage -VM $vmConfig -PublisherName
    $publisher -Offer $offer -Skus $sku -Version $version
4 <!--NeedCopy-->
```

Agregar NIC

```
1 $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic1.Id -
    Primary
2 $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic2.Id
3 $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic3.Id
4 <!--NeedCopy-->
```

Especificar el disco del sistema operativo y crear VM

```
1 $osDiskName=$vmName + "-" + $osDiskSuffix
2 $osVhdUri=$prmStorageAccount.PrimaryEndpoints.Blob.ToString() + "vhds/"
     +$osDiskName + ".vhd"
3 $vmConfig=Set-AzureRMVMOSDisk -VM $vmConfig -Name $osDiskName -VhdUri
    $osVhdUri -CreateOption fromImage
```



```
4 Set-AzureRmVMPlan -VM $vmConfig -Publisher $publisher -Product $offer -
    Name $sku
5 New-AzureRMVM -VM $vmConfig -ResourceGroupName $RGName -Location
    $location
6 <!--NeedCopy-->
```

> **Nota**
>
> Repita los pasos 1 a 10 enumerados en “Crear máquinas virtuales multiNIC mediante comandos de PowerShell” para crear VM2 con parámetros específicos de VM2.

Detalles de configuración IP

Se utilizan las siguientes direcciones IP.

Tabla 1. Direcciones IP utilizadas en VM1

NIC	IP privada	IP pública (PIP)	Descripción
0/1	10.0.0.10	PIP1	Configurado como NSIP (IP de administración)
1/1	10.0.1.10	PIP2	Configurado como IP del sitio SNIP/GSLB
-	10.0.1.11	-	Configurado como IP del servidor LB. La IP pública no es obligatoria
1/2	10.0.2.10	-	Configurado como SNIP para enviar sondeos de monitor a servicios; IP pública no es obligatoria

Tabla 2. Direcciones IP utilizadas en VM2

NIC	IP interna	IP pública (PIP)	Descripción
0/1	20.0.0.10	PIP4	Configurado como NSIP (IP de administración)

NIC	IP interna	IP pública (PIP)	Descripción
1/1	20.0.1.10	PIP5	Configurado como IP del sitio SNIP/GSLB
-	20.0.1.11	-	Configurado como IP del servidor LB. La IP pública no es obligatoria
1/2	20.0.2.10	-	Configurado como SNIP para enviar sondeos de monitor a servicios; IP pública no es obligatoria

A continuación se muestran configuraciones de ejemplo para este caso, que muestran las direcciones IP y las configuraciones LB iniciales creadas a través de la CLI de Citrix ADC VPX para VM1 y VM2.

He aquí un ejemplo de configuración en VM1.

```
1 add ns ip 10.0.1.10 255.255.255.0 -mgmtAccess ENABLED
2 Add nsip 10.0.2.10 255.255.255.0
3 add service svc1 10.0.1.10 ADNS 53
4 add lb vserver v1 HTTP 10.0.1.11 80
5 add service s1 10.0.2.120 http 80
6 Add service s2 10.0.2.121 http 80
7 Bind lb vs v1 s[1-2]
8 <!--NeedCopy-->
```

He aquí un ejemplo de configuración en VM2.

```
1 add ns ip 20.0.1.10 255.255.255.0  -mgmtAccess ENABLED
2 Add nsip 20.0.2.10 255.255.255.0
3 add service svc1 20.0.1.10 ADNS 53
4 add lb vserver v1 HTTP 20.0.1.11 80
5 Add service s1 20.0.2.90 http 80
6 Add service s2 20.0.2.91 http 80
7 Bind lb vs v1 s[1-2]
8 <!--NeedCopy-->
```


Configurar sitios GSLB y otros parámetros

Realice las tareas descritas en el tema siguiente para configurar los dos sitios GSLB y otras opciones necesarias:

Equilibrio de carga global del servidor

Para obtener más información, consulte este artículo de asistencia técnica: https://support.citrix.com/article/CTX110348

He aquí un ejemplo de configuración GSLB en VM1 y VM2.

```
enable ns feature LB GSLB
add gslb site site1 10.0.1.10 -publicIP PIP2
add gslb site site2 20.0.1.10 -publicIP PIP5
add gslb service site1_gslb_http_svc1 10.0.1.11 HTTP 80 -publicIP PIP3
    -publicPort 80 -siteName site1
add gslb service site2_gslb_http_svc1 20.0.1.11 HTTP 80 -publicIP PIP6
    -publicPort 80 -siteName site2
add gslb vserver gslb_http_vip1 HTTP
bind gslb vserver gslb_http_vip1 -serviceName site2_gslb_http_svc1
bind gslb vserver gslb_http_vip1 -serviceName site1_gslb_http_svc1
bind gslb vserver gslb_http_vip1 -domainName www.gslbindia.com -TTL 5
<!--NeedCopy-->
```

Ha configurado GSLB en instancias Citrix ADC VPX que se ejecutan en Azure.

Para obtener información adicional acerca de cómo configurar GSLB en instancias de Citrix ADC VPX, haga clic en la imagen siguiente para ver el vídeo acerca de la configuración de Citrix ADC GSLB en Microsoft Azure.

Vídeo 

Configurar GSLB en una configuración de alta disponibilidad activa-en espera

June 22, 2022

Puede configurar el equilibrio de carga del servidor global (GSLB) en la implementación de HA activa-en espera en Azure en tres pasos:

1. Cree un par VPX HA en cada sitio GSLB. Consulte Configurar una configuración de alta disponibilidad con varias direcciones IP y NIC para obtener información sobre cómo crear un par de alta disponibilidad.
2. Configure Azure Load Balancer (ALB) con la dirección IP de front-end y las reglas para permitir el tráfico GSLB y DNS.

   Este paso incluye los siguientes pasos secundarios. Consulte el caso de esta sección para ver los comandos de PowerShell que se utilizan para completar estos pasos secundarios.

   a. Cree un front-end `IPconfig` para el sitio GSLB.

   b. Cree un grupo de direcciones back-end con la dirección IP de la NIC 1/1 de los nodos en HA.

   c. Cree reglas de equilibrio de carga para lo siguiente:

   ```
   TCP/3009 - gslb communication
   TCP/3008 - gslb communication
   UDP/53 - DNS communication
   ```

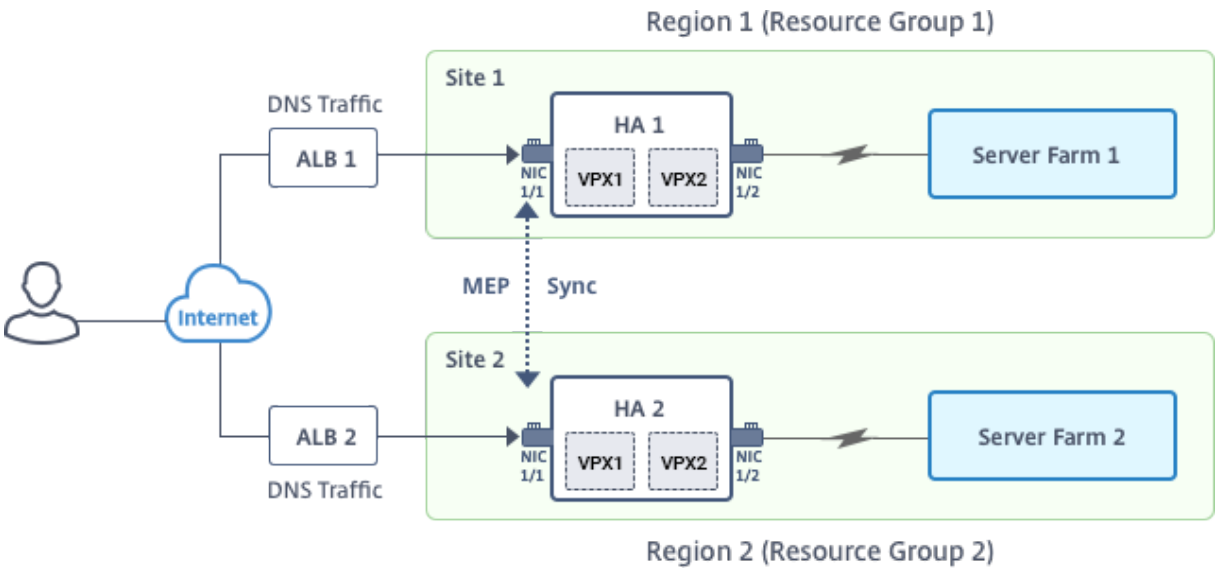
   d. Asocie el grupo de direcciones back-end con las reglas LB creadas en el paso c.

   e. Actualice el grupo de seguridad de red de la NIC 1/1 de los nodos en ambos pares HA para permitir el tráfico de los puertos TCP 3008, TCP 3009 y UDP 53.
3. Habilite GSLB en cada par HA.

Caso

Este caso incluye dos sitios: el sitio 1 y el sitio 2. Cada sitio tiene un par de HA (HA1 y HA2) configurado con varias NIC, varias direcciones IP y GSLB.

Ilustración: GLSB en la implementación de alta disponibilidad de activos en Azure



En este caso, cada VM tiene tres NIC: NIC 0/1, 1/1 y 1/2. Las NIC se configuran para los siguientes fines.

NIC 0/1: para dar servicio al tráfico de administración

NIC 1/1: para atender el tráfico del lado del cliente

NIC 1/2: Para comunicarse con servidores back-end

Configuración de parámetros

A continuación se presentan ejemplos de configuración de parámetros para ALB. Puede usar diferentes configuraciones si lo quiere.

```
$locName="South east Asia"

$rgName="MulitIP-MultiNIC-RG"

$pubIPName4="PIPFORGSLB1"

$domName4="vpxgslbdns"

$lbName="MultiIPALB"

$frontEndConfigName2="FrontEndIP2"

$backendPoolName1="BackendPoolHttp"

$lbRuleName2="LBRuleGSLB1"

```



```
$lbRuleName3=”LBRuleGSLB2”

$lbRuleName4=”LBRuleDNS”

$healthProbeName=”HealthProbe”
```

Configurar ALB con la dirección IP del front-end y las reglas para permitir el tráfico GSLB y DNS

Paso 1. **Crear una IP pública para la IP del sitio GSLB**

```
$pip4=New-AzureRmPublicIpAddress -Name $pubIPName4 -ResourceGroupName
    $rgName -DomainNameLabel $domName4 -Location $locName -
    AllocationMethod Dynamic


Get-AzureRmLoadBalancer -Name $lbName -ResourceGroupName $rgName | Add-
    AzureRmLoadBalancerFrontendIpConfig -Name $frontEndConfigName2 -
    PublicIpAddress $pip4 | Set-AzureRmLoadBalancer
```

Paso 2. **Cree reglas LB y actualice el ALB existente**.

```
$alb = get-AzureRmLoadBalancer -Name $lbName -ResourceGroupName $rgName


$frontendipconfig2=Get-AzureRmLoadBalancerFrontendIpConfig -
    LoadBalancer $alb -Name $frontEndConfigName2


$backendPool=Get-AzureRmLoadBalancerBackendAddressPoolConfig -
    LoadBalancer $alb -Name $backendPoolName1


$healthprobe=Get-AzureRmLoadBalancerProbeConfig -LoadBalancer $alb -
    Name $healthProbeName


$alb | Add-AzureRmLoadBalancerRuleConfig -Name $lbRuleName2 -
    BackendAddressPool $backendPool -FrontendIPConfiguration
    $frontendipconfig2 -Protocol ”Tcp” -FrontendPort 3009 -BackendPort
```



```
    3009 -Probe $healthprobe -EnableFloatingIP  | Set-
    AzureRmLoadBalancer
14
15
16 $alb | Add-AzureRmLoadBalancerRuleConfig -Name $lbRuleName3 -
    BackendAddressPool $backendPool -FrontendIPConfiguration
    $frontendipconfig2 -Protocol "Tcp" -FrontendPort 3008 -BackendPort
    3008 -Probe $healthprobe -EnableFloatingIP  | Set-
    AzureRmLoadBalancer
17
18
19 $alb | Add-AzureRmLoadBalancerRuleConfig -Name $lbRuleName4 -
    BackendAddressPool $backendPool -FrontendIPConfiguration
    $frontendipconfig2 -Protocol "Udp" -FrontendPort 53 -BackendPort 53
    -Probe $healthprobe -EnableFloatingIP  | Set-AzureRmLoadBalancer
```

Habilitar GSLB en cada par de alta disponibilidad

Ahora tiene dos direcciones IP de front-end para cada ALB: ALB 1 y ALB 2. Una dirección IP es para el servidor virtual de LB y la otra para la IP del sitio GSLB.

HA 1 tiene las siguientes direcciones IP de front-end:

- FrontendipOfAlb1 (para el servidor virtual LB)
- PIPFORGSLB1 (IP de GSLB)

HA 2 tiene las siguientes direcciones IP de front-end:

- FrontendipOfAlb2 (para el servidor virtual LB)
- PIPFORGSLB2 (IP de GSLB)

Los siguientes comandos se utilizan para este caso.

```
1 enable ns feature LB GSLB
2
3 add service dnssvc PIPFORGSLB1 ADNS 53
4
5 add gslb site site1 PIPFORGSLB1 -publicIP PIPFORGSLB1
6
7 add gslb site site2 PIPFORGSLB2 -publicIP PIPFORGSLB2
8
9 add gslb service site1_gslb_http_svc1 FrontEndIPofALB1 HTTP 80 -
    publicIP FrontEndIPofALB1 -publicPort 80 -siteName site1
10
```



```
add gslb service site2_gslb_http_svc1 FrontEndIPofALB2 HTTP 80 -
   publicIP FrontEndIPofALB2 -publicPort 80 -siteName site2

add gslb vserver gslb_http_vip1 HTTP

bind gslb vserver gslb_http_vip1 -serviceName site2_gslb_http_svc1

bind gslb vserver gslb_http_vip1 -serviceName site1_gslb_http_svc1

bind gslb vserver gslb_http_vip1 -domainName www.gslbindia.com -TTL 5
```

Recursos relacionados:

Configurar GSLB en instancias de Citrix ADC VPX

Global Server Load Balancing

Configurar IP de intranet de grupos de direcciones para un dispositivo Citrix Gateway

January 31, 2022

En algunas situaciones, los usuarios que se conectan con Citrix Gateway Plug-in necesitan una dirección IP única para un dispositivo Citrix ADC Gateway. Al habilitar grupos de direcciones (también conocidos como agrupación de IP) para un grupo, el dispositivo Citrix Gateway puede asignar un alias de dirección IP único a cada usuario. Los grupos de direcciones se configuran mediante direcciones IP de intranet (IIP).

Puede configurar grupos de direcciones en un dispositivo Citrix Gateway implementado en Azure siguiendo este procedimiento de dos pasos:

- Registro de las direcciones IP privadas que se utilizan en el grupo de direcciones, en Azure
- Configuración de grupos de direcciones en el dispositivo Citrix Gateway

Registre una dirección IP privada en el portal de Azure

En Azure, puede implementar una instancia de Citrix ADC VPX con varias direcciones IP. Puede agregar direcciones IP a una instancia VPX de dos maneras:

a. Durante el Provisioning de una instancia VPX

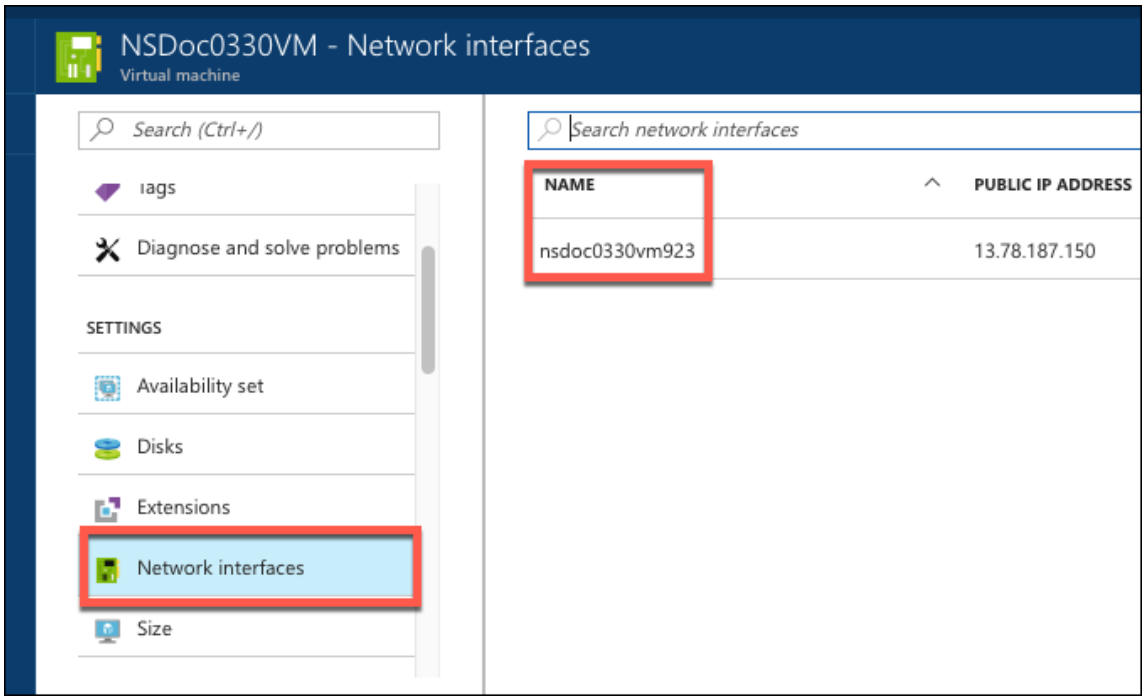
Para obtener más información sobre cómo agregar varias direcciones IP mientras se aprovisiona una instancia VPX, consulte Configurar varias direcciones IP para una instancia independiente de Citrix

ADC. Para agregar direcciones IP mediante comandos de PowerShell durante el aprovisionamiento de una instancia VPX, consulte Configurar varias direcciones IP para una instancia Citrix ADC VPX en modo independiente mediante comandos de PowerShell.

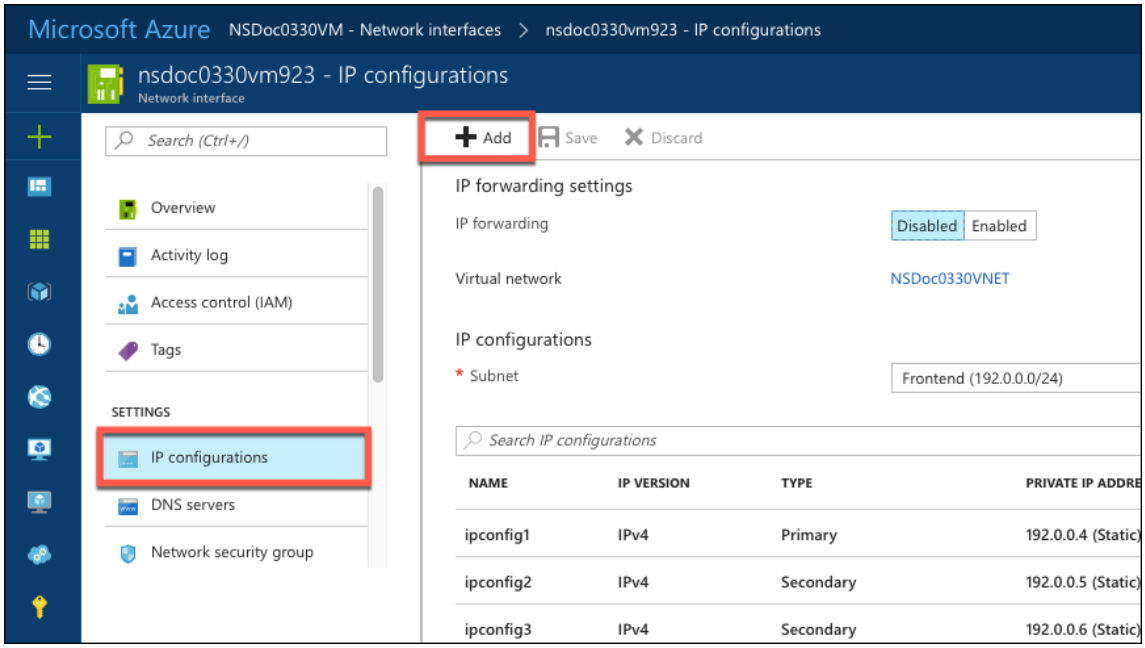
b. Después de Provisioning una instancia VPX

Después de aprovisionar una instancia VPX, siga estos pasos para registrar una dirección IP privada en el portal de Azure, que configura como grupo de direcciones en el dispositivo Citrix Gateway.

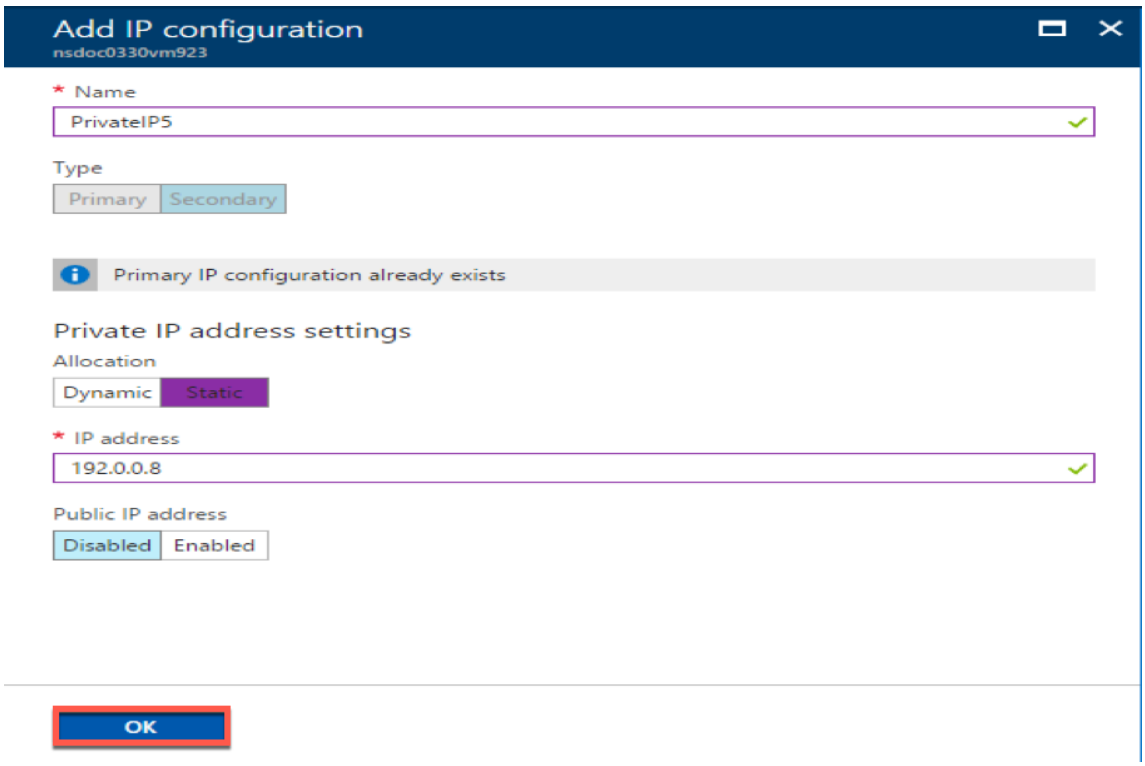
1. En Azure Resource Manager (ARM), vaya a la instancia de Citrix ADC VPX ya creada > **Interfaces de red**. Elija la interfaz de red que está enlazada a una subred a la que pertenece el IIP que quiere registrar.



2. Haga clic en **Configuraciones IP** y, a continuación, haga clic en **Agregar**.



3. Proporcione los detalles necesarios como se muestra en el ejemplo siguiente y haga clic en **Aceptar**.



Configurar grupos de direcciones en el dispositivo Citrix Gateway

Para obtener más información sobre cómo configurar grupos de direcciones en Citrix Gateway, consulte esta sección Configuración de grupos de direcciones.

Limitación: No se puede vincular un rango de direcciones IP a los usuarios. Todas las direcciones IP que se utilizan en un grupo de direcciones deben estar registradas.

Configurar varias direcciones IP para una instancia independiente Citrix ADC VPX mediante comandos de PowerShell

September 8, 2021

En un entorno Azure, se puede implementar un dispositivo virtual Citrix ADC VPX con varias NIC. Cada NIC puede tener varias direcciones IP. En esta sección se describe cómo implementar una instancia Citrix ADC VPX con una única NIC y varias direcciones IP mediante comandos de PowerShell. Puede utilizar el mismo script para la implementación de varias NIC y varias IP.

> **Nota**
>
> En este documento, IP-Config hace referencia a un par de direcciones IP, IP pública e IP privada, asociadas a una NIC individual. Para obtener más información, consulte la sección Terminología de Azure .

Caso de uso

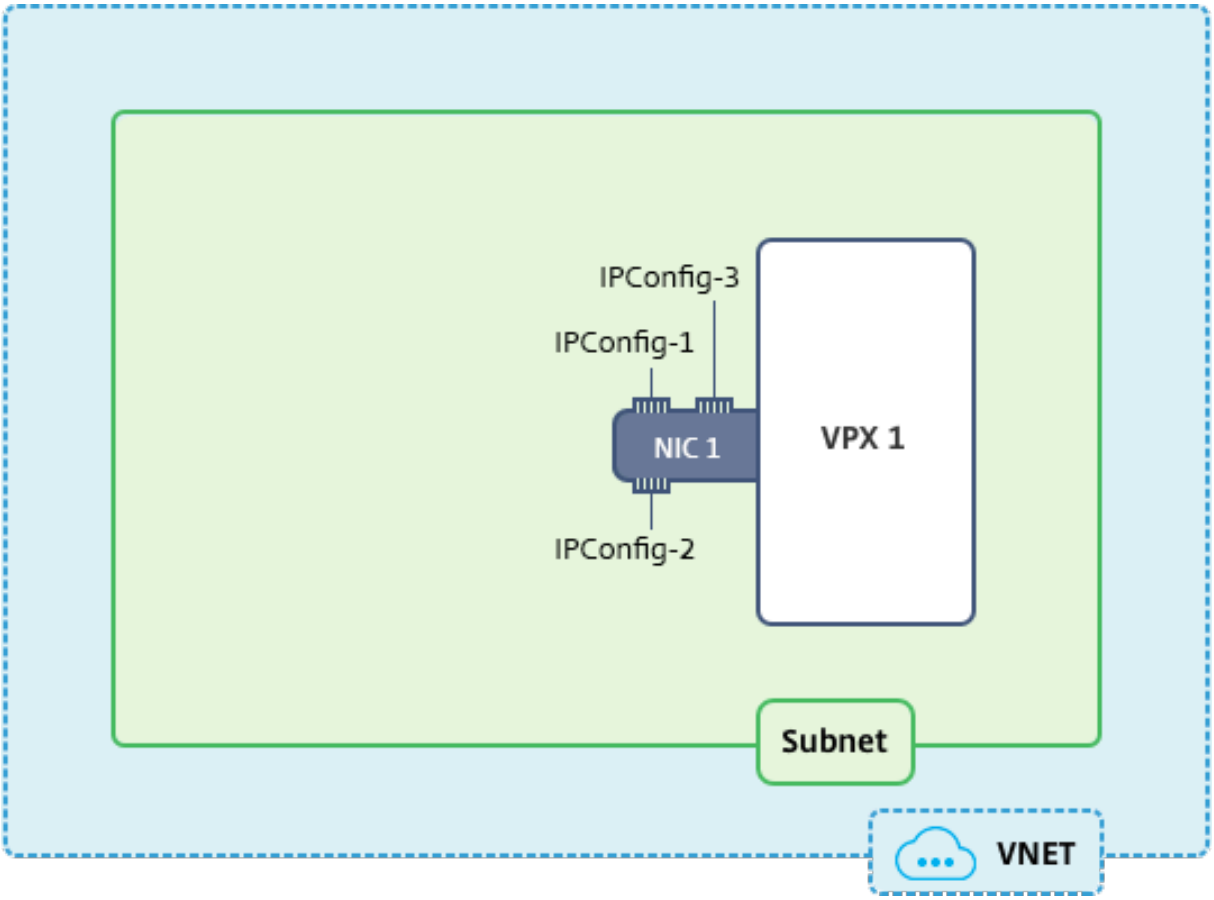
En este caso de uso, se conecta una única NIC a una red virtual (VNET). La NIC está asociada con tres configuraciones IP, como se muestra en la siguiente tabla.

Configuración IP	Asociada con
IPConfig-1	Dirección IP pública estática; dirección IP privada estática
IPConfig-2	Dirección IP pública estática; dirección privada estática
IPConfig-3	Dirección IP privada estática

> **Nota**
>
> IPConfig-3 no está asociado a ninguna dirección IP pública.

Diagrama: Topología

Aquí está la representación visual del caso de uso.



> **Nota**
>
> En una implementación Multi-NIC, Multi-IP Azure Citrix ADC VPX, la dirección IP privada asociada a la principal (primera) `IPConfig` de la NIC principal (primera) se agrega automáticamente como dirección NSIP de administración del dispositivo. El resto de direcciones IP privadas asociadas a la instancia VPX `IPConfigs` deben agregarse como VIP o SNIP mediante el `add ns ip` comando, según lo determinado por sus requisitos.

A continuación se muestra el resumen de los pasos necesarios para configurar varias direcciones IP para un dispositivo virtual Citrix ADC VPX en modo autónomo:

1. Crear grupo de recursos
2. Crear cuenta de almacenamiento
3. Crear conjunto de disponibilidad
4. Crear grupo de servicios de red
5. Crear red virtual
6. Crear dirección IP pública
7. Asignar configuración IP

8. Crear NIC
9. Crear instancia Citrix ADC VPX
10. Comprobar configuraciones de NIC
11. Comprobar las configuraciones del lado VPX

Script

Parámetros

A continuación se presentan parámetros de ejemplo de configuración para el caso de uso en este documento. Puede usar diferentes configuraciones si lo quiere.

$locName=”westcentralus”

$rgName=”Azure-MultiIP»

$nicName1=”VM1-NIC1”

$vnetName=”Azure-MultiIP-VNET»

$vNetAddressRange=”11.6.0.0/16”

$frontendSubnetName=”FrontendSubnet»

$frontEndSubnetRange=”11.6.1.0/24”

$prmStorageAccountName=”Almacenamiento MultiIP»

$avSetName=”multiip-avSet”

$VMsize=”standard_DS4_V2” (Este parámetro crea una máquina virtual con hasta cuatro NIC).

Nota: El requisito mínimo para una instancia VPX es 2 vCPU y 2 GB de RAM.

$editor = “Citrix”

$offer=”netscalervpx110-6531” (puede usar ofertas diferentes)

$sku=”netscalerbyol» (Según tu oferta, el SKU puede ser diferente).

$version=”latest»

$pubIPName1=”PIP1”

$pubIPName2=”PIP2”

$domName1=”multiipvpx1”

$domName2=”multiipvpx2”

$VMnamePrefix=”VPXMultiIP»

$osDiskSuffix=”osmultiipalbdiskdb1”

Información relacionada con Network Security Group (NSG):

$NSGname=”NSG-MultiIP»

$rule1Name=”Inbound-HTTP”

$rule2Name=”Inbound-HTTPS”

$rule3Name=”Inbound-SSH”

$IpConfigName1=”IPConfig1”

$IPConfigName2=”IPConfig-2”

$IPConfigName3=”IPConfig-3”

1. Crear grupo de recursos

```
New-AzureRmResourceGroup -Name $rgName -Location $locName
```

2. Crear cuenta de almacenamiento

```
$prmStorageAccount = New-AzureRMStorageAccount -Name $prmStorageAccountName
 -ResourceGroupName $rgName -Type Standard_LRS -Location $locName
```

3. Crear conjunto de disponibilidad

```
$avSet = New-AzureRMAvailabilitySet -Name $avSetName -ResourceGroupName
$rgName -Location $locName
```

4. Crear grupo de seguridad de red

1. Agregar reglas. Debe agregar una regla al grupo de seguridad de red para cualquier puerto que sirva el tráfico.

   ```
   $rule1=New-AzureRmNetworkSecurityRuleConfig -Name $rule1Name -Description
    ”Allow HTTP”-Access Allow -Protocol Tcp -Direction Inbound -Priority
   101 -SourceAddressPrefix Internet -SourcePortRange * -DestinationAddressPrefix
    * -DestinationPortRange 80
   $rule2=New-AzureRmNetworkSecurityRuleConfig -Name $rule2Name -Description
    ”Allow HTTPS”-Access Allow -Protocol Tcp -Direction Inbound -Priority
   110 -SourceAddressPrefix Internet -SourcePortRange * -DestinationAddressPrefix
    * -DestinationPortRange 443
   ```



```
$rule3=New-AzureRmNetworkSecurityRuleConfig -Name $rule3Name -Description
 "Allow SSH"-Access Allow -Protocol Tcp -Direction Inbound -Priority
120 -SourceAddressPrefix Internet -SourcePortRange * -DestinationAddressPrefix
 * -DestinationPortRange 22
```

2. Cree un objeto de grupo de seguridad de red.

```
$nsg=New-AzureRmNetworkSecurityGroup -ResourceGroupName $rgName -
Location $locName -Name $nsgName -SecurityRules $rule1,$rule2,$rule3
```

5. Crear red virtual

1. Añada subredes.

```
$frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name $frontEndSubnetName
 -AddressPrefix $frontEndSubnetRange
```

2. Agregue un objeto de red virtual.

```
$vnet=New-AzureRmVirtualNetwork -Name $vNetName -ResourceGroupName
$rgName -Location $locName -AddressPrefix $vNetAddressRange -Subnet
$frontendSubnet
```

3. Recuperar subredes.

```
$subnetName="frontEndSubnet"
$subnet1=$vnet.Subnets|?{ $_.Name -eq $subnetName }
```

6. Crear dirección IP pública

```
$pip1=New-AzureRmPublicIpAddress -Name $pubIPName1 -ResourceGroupName
$rgName -DomainNameLabel $domName1 -Location $locName -AllocationMethod
Static
$pip2=New-AzureRmPublicIpAddress -Name $pubIPName2 -ResourceGroupName
$rgName -DomainNameLabel $domName2 -Location $locName -AllocationMethod
Static
```

> **Nota**
>
> Compruebe la disponibilidad de los nombres de dominio antes de utilizarlos.
>
> El método de asignación de direcciones IP puede ser dinámico o estático.

7. Asignar configuración IP

En este caso de uso, tenga en cuenta los siguientes puntos antes de asignar direcciones IP:

- IPConfig-1 pertenece a la subred1 de VPX1.
- IPConfig-2 pertenece a la subred 1 de VPX1.
- IPConfig-3 pertenece a la subred 1 de VPX1.

> **Nota**
>
> Cuando asigna varias configuraciones IP a una NIC, se debe asignar una configuración como principal.

```
$IPAddress1="11.6.1.27"
$IPConfig1=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName1 -Subnet $subnet1 -PrivateIpAddress $IPAddress1 -PublicIpAddress $pip1 -Primary
$IPAddress2="11.6.1.28"
$IPConfig2=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName2 -Subnet $subnet1 -PrivateIpAddress $IPAddress2 -PublicIpAddress $pip2
$IPAddress3="11.6.1.29"
$IPConfig3=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName3 -Subnet $subnet1 -PrivateIpAddress $IPAddress3 -Primary
```

Utilice una dirección IP válida que cumpla los requisitos de la subred y compruebe su disponibilidad.

8. Crear NIC

```
$nic1=New-AzureRmNetworkInterface -Name $nicName1 -ResourceGroupName $rgName -Location $locName -IpConfiguration $IpConfig1,$IpConfig2,$IPConfig3 -NetworkSecurityGroupId $nsg.Id
```

9. Crear instancia Citrix ADC VPX

1. Inicializar variables.

   ```
   $suffixNumber = 1
   $vmName = $vmNamePrefix + $suffixNumber
   ```

2. Cree un objeto de configuración de máquina virtual.

   ```
   $vmConfig=New-AzureRMVMConfig -VMName $vmName -VMSize $vmSize -AvailabilitySetId $avSet.Id
   ```

3. Establezca credenciales, SO e imagen.

   ```
   $cred=Get-Credential -Message "Type the name and password for VPX login."
   ```



```
$vmConfig=Set-AzureRMVMOperatingSystem -VM $vmConfig -Linux -ComputerName
 $vmName -Credential $cred
$vmConfig=Set-AzureRMVMSourceImage -VM $vmConfig -PublisherName $publisher
 -Offer $offer -Skus $sku -Version $version
```

4. Agregue NIC.

```
$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic1.Id -
Primary
```

> **Nota**
>
> En una implementación VPX multi-NIC, una NIC debe ser principal. Por lo tanto, debe añadirse "-Primary" al agregar esa NIC a la instancia VPX.

5. Especifique el disco del sistema operativo y cree VM.

```
$osDiskName=$vmName + "-"+ $osDiskSuffix1
$osVhdUri=$prmStorageAccount.PrimaryEndpoints.Blob.ToString()+ "vhds/"+
 $osDiskName + ".vhd"
$vmConfig=Set-AzureRMVMOSDisk -VM $vmConfig -Name $osDiskName -VhdUri
$osVhdUri -CreateOption fromImage
Set-AzureRmVMPlan -VM $vmConfig -Publisher $publisher -Product $offer -
Name $sku
New-AzureRMVM -VM $vmConfig -ResourceGroupName $rgName -Location
$locName
```

10. Comprobar configuraciones de NIC

Una vez iniciada la instancia VPX, puede comprobar las direcciones IP asignadas a `IPConfigs` la NIC VPX mediante el siguiente comando.

```
$nic.IPConfig
```

11. Comprobar las configuraciones del lado VPX

Cuando se inicia la instancia Citrix ADC VPX, se agrega una dirección IP privada asociada al principal `IPconfig` de la NIC principal como dirección NSIP. Las direcciones IP privadas restantes deben agregarse como direcciones VIP o SNIP, según lo determinado por sus requisitos. Utilice el siguiente comando.

```
add nsip <Private IPAddress><netmask> -type VIP/SNIP
```

Ahora ha configurado varias direcciones IP para una instancia de Citrix ADC VPX en modo independiente.

Scripts de PowerShell adicionales para la implementación de Azure

August 20, 2021

Esta sección proporciona los cmdlets de PowerShell con los que puede realizar las siguientes configuraciones en Azure PowerShell:

- Aprovisionar una instancia independiente de Citrix ADC VPX
- Aprovisione un par Citrix ADC VPX en una configuración de alta disponibilidad con un equilibrador de carga externo de Azure
- Aprovisione un par Citrix ADC VPX en una configuración de alta disponibilidad con el equilibrador de carga interno de Azure

Consulte también los temas siguientes para las configuraciones que puede realizar mediante comandos de PowerShell:

- Configurar una configuración de alta disponibilidad con varias direcciones IP y NIC mediante comandos de PowerShell
- Configurar GSLB en instancias de Citrix ADC VPX
- Configurar GSLB en una configuración de alta disponibilidad activa en espera de NetScaler
- Configurar varias direcciones IP para una instancia de Citrix ADC VPX en modo independiente mediante comandos de PowerShell
- Configurar varios VIP de Azure para una instancia VPX independiente

Aprovisionar una instancia independiente de Citrix ADC VPX

1. **Crear un grupo de recursos**

   El grupo de recursos puede incluir todos los recursos de la solución o solo los recursos que desee administrar como grupo. La ubicación especificada aquí es la ubicación predeterminada de los recursos de ese grupo de recursos. Asegúrese de que todos los comandos para crear un equilibrador de carga utilizan el mismo grupo de recursos.

   ```
   $rgName=”<resource group name>”
   $locName=”<location name, such as West US>
   New-AzureRmResourceGroup -Name $rgName -Location $locName
   ```

   Por ejemplo:

   ```
   $rgName = ”ARM-VPX”
   $locName = ”West US”
   New-AzureRmResourceGroup -Name $rgName -Location $locName
   <!--NeedCopy-->
   ```


2. **Crear una cuenta de almacenamiento**

   Elija un nombre único para su cuenta de almacenamiento que contenga solo letras y números minúsculas.

   ```
   $saName="<storage account name>"
   $saType="<storage account type>", especifique uno: Standard_LRS, Standard_GRS, Standard_RAGRS o Premium_LRS
   New-AzureRmStorageAccount -Name $saName -ResourceGroupName $rgName -Type $saType -Location $locName
   ```

   Por ejemplo:

   ```
   1 $saName="vpxstorage"
   2 $saType="Standard_LRS"
   3 New-AzureRmStorageAccount -Name $saName -ResourceGroupName $rgName
         -Type $saType -Location $locName
   4 <!--NeedCopy-->
   ```

3. **Crear un conjunto de disponibilidad**

   El conjunto de disponibilidad ayuda a mantener las máquinas virtuales disponibles durante el tiempo de inactividad, como durante el mantenimiento. Un equilibrador de carga configurado con un conjunto de disponibilidad garantiza que la aplicación esté siempre disponible.

   ```
   $avName="<availability set name>"
   ```

   ```
   New-AzureRmAvailabilitySet -Name $avName -ResourceGroupName $rgName -Location $locName
   ```

4. **Crear una red virtual**

   Agregue una nueva red virtual con al menos una subred, si la subred no se creó previamente.

   ```
   $FrontendAddressPrefix="10.0.1.0/24"
   $BackendAddressPrefix="10.0.2.0/24"
   $vnetAddressPrefix="10.0.0.0/16"
   $frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name frontendSubnet
    -AddressPrefix $FrontendAddressPrefix
   $backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name backendSubnet
    -AddressPrefix $BackendAddressPrefix
   New-AzureRmVirtualNetwork -Name TestNet -ResourceGroupName $rgName -Location $locName -AddressPrefix $vnetAddressPrefix -Subnet $frontendSubnet
   ,$backendSubnet
   ```

   Por ejemplo:


```
$frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
    frontendSubnet -AddressPrefix $FrontendAddressPrefix

$backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
    backendSubnet -AddressPrefix $BackendAddressPrefix

New-AzureRmVirtualNetwork -Name TestNet -ResourceGroupName $rgName
     -Location $locName -AddressPrefix $vnetAddressPrefix -Subnet
    $frontendSubnet,$backendSubnet
<!--NeedCopy-->
```

5. **Crear una NIC**

   Cree una NIC y asocie la NIC con la instancia de Citrix ADC VPX. La subred front-end creada en el procedimiento anterior se indexa en 0 y la subred back-end se indexa en 1. Ahora cree NIC de una de las tres maneras siguientes:

   a) *NIC con dirección IP pública*

   ```
   $nicName="<name of the NIC of the VM>"

   $pip = New-AzureRmPublicIpAddress -Name $nicName -ResourceGroupName
   $rgName -Location $locName -AllocationMethod Dynamic

   $nic = New-AzureRmNetworkInterface -Name $nicName -ResourceGroupName
   $rgName -Location $locName -SubnetId $vnet.Subnets[$subnetIndex].Id -
   PublicIpAddressId $pip.Id
   ```

   b) *NIC con IP pública y etiqueta DNS*

   ```
   $nicName="<name of the NIC of the VM>"

   $domName="<domain name label>"

   $pip = New-AzureRmPublicIpAddress -Name $nicName -ResourceGroupName
   $rgName -DomainNameLabel $domName -Location $locName -AllocationMethod
   Dynamic
   ```

   Antes de asignar $DOMName, compruebe que está disponible o no mediante el comando:

   ```
   Test-AzureRmDnsAvailability -DomainQualifiedName $domName -Location
   $locName

   $nic = New-AzureRmNetworkInterface -Name $nicName -ResourceGroupName
   $rgName -Location $locName -SubnetId $vnet.Subnets[$subnetIndex].Id -
   PublicIpAddressId $pip.Id
   ```

   Por ejemplo:


```
$nicName="frontendNIC"

$domName="vpxazure"

$pip = New-AzureRmPublicIpAddress -Name $nicName -
    ResourceGroupName $rgName -DomainNameLabel $domName -Location
    $locName -AllocationMethod Dynamic

$nic = New-AzureRmNetworkInterface -Name $nicName -
    ResourceGroupName $rgName -Location $locName -SubnetId $vnet.
    Subnets[0].Id -PublicIpAddressId $pip.Id
<!--NeedCopy-->
```

c) *NIC con dirección pública dinámica y dirección IP privada estática*

Asegúrese de que la dirección IP privada (estática) que agregue a la máquina virtual debe ser el mismo rango que la de la subred especificada.

```
$nicName="<name of the NIC of the VM>"

$staticIP="<available static IP address on the subnet>"

$pip = New-AzureRmPublicIpAddress -Name $nicName -ResourceGroupName
$rgName -Location $locName -AllocationMethod Dynamic

$nic = New-AzureRmNetworkInterface -Name $nicName -ResourceGroupName
$rgName -Location $locName -SubnetId $vnet.Subnets[$subnetIndex].Id -
PublicIpAddressId $pip.Id -PrivateIpAddress $staticIP
```

6. **Crear un objeto virtual**

```
$vmName="<VM name>"

$vmSize="<VM size string>"

$avSet=Get-AzureRmAvailabilitySet -Name $avName -ResourceGroupName
$rgName

$vm=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -AvailabilitySetId
 $avset.Id
```

7. **Obtener la imagen de Citrix ADC VPX**

```
$pubName="<Image publisher name>"

$offerName="<Image offer name>"

$skuName="<Image SKU name>"
```



```
$cred=Get-Credential -Message "Type the name and password of the local administrator account."
```

Proporcione sus credenciales que se utilizan para iniciar sesión en VPX

```
$vm=Set-AzureRmVMOperatingSystem -VM $vm -Linux -ComputerName $vmName -Credential $cred -Verbose

$vm=Set-AzureRmVMSourceImage -VM $vm -PublisherName $pubName -Offer $offerName -Skus $skuName -Version "latest"

$vm=Add-AzureRmVMNetworkInterface -VM $vm -Id $nic.Id
```

Por ejemplo:

```
$pubName="citrix"
```

El siguiente comando se utiliza para mostrar todas las ofertas de Citrix:

```
Get-AzureRMVMImageOffer -Location $locName -Publisher $pubName |
    Select Offer

$offerName="netscalervpx110-6531"
<!--NeedCopy-->
```

El siguiente comando se utiliza para conocer el SKU ofrecido por el editor para un nombre de oferta específico:

```
Get-AzureRMVMImageSku -Location $locName -Publisher $pubName -Offer $offerName | Select Skus
```

8. **Crear una máquina virtual**

```
$diskName="<name identifier for the disk in Azure storage, such as OSDisk>"
```

Por ejemplo:

```
$diskName="dynamic"

$pubName="citrix"

$offerName="netscalervpx110-6531"

$skuName="netscalerbyol"

```



```
$storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName -
    Name $saName

$osDiskUri=$storageAcc.PrimaryEndpoints.Blob.ToString() + "vhds/"
    + $diskName  + ".vhd"

$vm=Set-AzureRmVMOSDisk -VM $vm -Name $diskName -VhdUri $osDiskUri
     -CreateOption fromImage
<!--NeedCopy-->
```

Al crear VM a partir de imágenes presentes en el mercado, utilice el siguiente comando para especificar el plan de VM:

```
Set-AzureRmVMPlan -VM $vm -Publisher $pubName -Product $offerName -Name
 $skuName

New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM $vm
```

Aprovisione un par Citrix ADC VPX en una configuración de alta disponibilidad con un equilibrador de carga externo de Azure

Inicie sesión en AzurermAccount con sus credenciales de usuario de Azure.

1. **Crear un grupo de recursos**

   La ubicación especificada aquí es la ubicación predeterminada de los recursos de ese grupo de recursos. Asegúrese de que todos los comandos utilizados para crear un equilibrador de carga utilizan el mismo grupo de recursos.

   ```
   $rgName="<resource group name>"

   $locName="<location name, such as West US>"

   New-AzureRmResourceGroup -Name $rgName -Location $locName
   ```

   Por ejemplo:

   ```
   $rgName = "ARM-LB-NS"

   $locName = "West US"

   New-AzureRmResourceGroup -Name $rgName -Location $locName
   <!--NeedCopy-->
   ```

2. **Crear una cuenta de almacenamiento**

Elija un nombre único para su cuenta de almacenamiento que contenga solo letras y números minúsculas.

`$saName="<storage account name>"`

`$saType="<storage account type>"`, especifique uno: `Standard_LRS`, `Standard_GRS`, `Standard_RAGRS` o `Premium_LRS`

```
New-AzureRmStorageAccount -Name $saName -ResourceGroupName $rgName -
Type $saType -Location $locName
```

Por ejemplo:

```
$saName="vpxstorage"

$saType="Standard_LRS"

New-AzureRmStorageAccount -Name $saName -ResourceGroupName $rgName
    -Type $saType -Location $locName
<!--NeedCopy-->
```

3. **Crear un conjunto de disponibilidad**

   Un equilibrador de carga configurado con un conjunto de disponibilidad garantiza que la aplicación esté siempre disponible.

   `$avName="<availability set name>"`

   ```
   New-AzureRmAvailabilitySet -Name $avName -ResourceGroupName $rgName -
   Location $locName
   ```

4. **Crear una red virtual**

   Agregue una nueva red virtual con al menos una subred, si la subred no se creó previamente.

```
$vnetName = "LBVnet"

$FrontendAddressPrefix="10.0.1.0/24"

$BackendAddressPrefix="10.0.2.0/24"

$vnetAddressPrefix="10.0.0.0/16"

$frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
   frontendSubnet -AddressPrefix $FrontendAddressPrefix

```



```
$backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
    backendSubnet -AddressPrefix $BackendAddressPrefix

$vnet=New-AzureRmVirtualNetwork -Name $vnetName -ResourceGroupName
     $rgName -Location $locName -AddressPrefix $vnetAddressPrefix -
    Subnet $frontendSubnet,$backendSubnet
<!--NeedCopy-->
```

Nota: Seleccione el valor del parámetro AddressPrefix según su requisito.

Asigne subred front-end y back-end a la red virtual que creó anteriormente en este paso.

Si la subred front-end es el primer elemento de la matriz VNet, SubnetID debe ser $vnet.subnets [0] .Id.

Si la subred front-end es el segundo elemento de la matriz, el ID de subred debe ser $vnet.subnets [1] .Id, etc.

5. **Configurar la dirección IP de front-end y crear un grupo de direcciones back-end**

   Configure una dirección IP front-end para el tráfico de red del equilibrador de carga entrante y cree un grupo de direcciones back-end para recibir el tráfico balanceado de carga.

```
$pubName="PublicIp1"

$publicIP1 = New-AzureRmPublicIpAddress -Name $pubName -
    ResourceGroupName $rgName -Location $locName -AllocationMethod
    Static -DomainNameLabel nsvpx
<!--NeedCopy-->
```

Nota: Compruebe la disponibilidad del valor de DomainNameLabel.

```
$FIPName = "ELBFIP"

$frontendIP1 = New-AzureRmLoadBalancerFrontendIpConfig -Name
    $FIPName -PublicIpAddress $publicIP1

$BEPool = "LB-backend-Pool"

$beaddresspool1= New-AzureRmLoadBalancerBackendAddressPoolConfig -
    Name $BEPool
<!--NeedCopy-->
```


6. **Crear un sondeo de estado**

   Cree un sondeo de estado TCP con el puerto 9000 y el intervalo de 5 segundos.

```
$healthProbe = New-AzureRmLoadBalancerProbeConfig -Name
    HealthProbe -Protocol Tcp -Port 9000 -IntervalInSeconds 5 -
    ProbeCount 2
<!--NeedCopy-->
```

7. **Crear una regla de equilibrio de carga**

   Cree una regla LB para cada servicio que esté equilibrando la carga.

   Por ejemplo:

   Puede utilizar el siguiente ejemplo para equilibrar la carga del servicio HTTP.

```
$lbrule1 = New-AzureRmLoadBalancerRuleConfig -Name "HTTP-LB" -
    FrontendIpConfiguration $frontendIP1 -BackendAddressPool
    $beAddressPool1 -Probe $healthProbe -Protocol Tcp -FrontendPort
     80 -BackendPort 80
<!--NeedCopy-->
```

8. **Crear reglas NAT entrantes**

   Cree reglas NAT para los servicios que no esté equilibrando la carga.

   Por ejemplo, al crear un acceso SSH a una instancia de Citrix ADC VPX.

   Nota: El triplete Protocol-frontendport-backendport no debe ser el mismo para dos reglas NAT.

```
$inboundNATRule1= New-AzureRmLoadBalancerInboundNatRuleConfig -
    Name SSH1     -FrontendIpConfiguration $frontendIP1 -Protocol
    TCP -FrontendPort 22 -BackendPort 22

$inboundNATRule2= New-AzureRmLoadBalancerInboundNatRuleConfig -
    Name SSH2 -FrontendIpConfiguration $frontendIP1 -Protocol TCP -
    FrontendPort 10022 -BackendPort 22
<!--NeedCopy-->
```

9. **Crear una entidad de equilibrador de carga**

   Cree el equilibrador de carga agregando todos los objetos (reglas NAT, reglas de equilibrador de carga, configuraciones de sondeo) juntos.


```
$lbName="ELB"

$NRPLB = New-AzureRmLoadBalancer -ResourceGroupName $rgName -Name
    $lbName -Location $locName -InboundNatRule $inboundNATRule1,
    $inboundNATRule2 -FrontendIpConfiguration $frontendIP1 -
    LoadBalancingRule $lbrule1 -BackendAddressPool $beAddressPool1
    -Probe $healthProbe
<!--NeedCopy-->
```

10. **Crear una NIC**

    Cree dos NIC y asocie cada NIC con cada instancia VPX

    a) NIC1 con VPX1

    Por ejemplo:

```
$nicName="NIC1"

$lbName="ELB"

$bePoolIndex=0

* Rule indexes starts from 0.

$natRuleIndex=0

$subnetIndex=0

* Frontend subnet index

$lb=Get-AzureRmLoadBalancer -Name $lbName -ResourceGroupName
    $rgName

$nic1=New-AzureRmNetworkInterface -Name $nicName -
    ResourceGroupName $rgName -Location $locName -Subnet $vnet.
    Subnets[$subnetIndex] -LoadBalancerBackendAddressPool $lb.
    BackendAddressPools[$bePoolIndex] -LoadBalancerInboundNatRule
    $lb.InboundNatRules[$natRuleIndex]
<!--NeedCopy-->
```

    b) NIC2 con VPX2

    Por ejemplo:


```
$nicName=”NIC2”

$lbName=”ELB”

$bePoolIndex=0

$natRuleIndex=1

* Second Inbound NAT (SSH) rule we need to use

`$subnetIndex=0

* Frontend subnet index

$lb=Get-AzureRmLoadBalancer -Name $lbName -ResourceGroupName
    $rgName

$nic2=New-AzureRmNetworkInterface -Name $nicName -
    ResourceGroupName $rgName -Location $locName -Subnet $vnet.
    Subnets[$subnetIndex] -LoadBalancerBackendAddressPool $lb.
    BackendAddressPools[$bePoolIndex] -LoadBalancerInboundNatRule
    $lb.InboundNatRules[$natRuleIndex]
<!--NeedCopy-->
```

11. **Crear instancias Citrix ADC VPX**

    Cree dos instancias de Citrix ADC VPX como parte del mismo grupo de recursos y conjunto de disponibilidad, y adjuntarlo al equilibrador de carga externo.

    a) Instancia 1 de Citrix ADC VPX

    Por ejemplo:

```
$vmName=”VPX1”

$vmSize=”Standard_A3”

$pubName=”citrix”

$offerName=”netscalervpx110-6531”

$skuName=”netscalerbyol”

```



```
$avSet=Get-AzureRmAvailabilitySet -Name $avName -ResourceGroupName
    $rgName

$vm1=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -
    AvailabilitySetId $avset.Id

$cred=Get-Credential -Message "Type Credentials which will be used
    to login to VPX instance"

$vm1=Set-AzureRmVMOperatingSystem -VM $vm1 -Linux -ComputerName
    $vmName -Credential $cred -Verbose

$vm1=Set-AzureRmVMSourceImage -VM $vm1 -PublisherName $pubName -
    Offer $offerName -Skus $skuName -Version "latest"

$vm1=Add-AzureRmVMNetworkInterface -VM $vm1 -Id $nic1.Id

$diskName="dynamic"

$storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName -
    Name $saName

$osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + "vhds1/
    " + $diskName  + ".vhd"

$vm1=Set-AzureRmVMOSDisk -VM $vm1 -Name $diskName -VhdUri
    $osDiskUri1 -CreateOption fromImage

Set-AzureRmVMPlan -VM $vm1 -Publisher $pubName -Product $offerName
    -Name $skuName

New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM
    $vm1
<!--NeedCopy-->
```

b) Instancia 2 de Citrix ADC VPX

Por ejemplo:

```
$vmName="VPX2"

$vmSize="Standard_A3"

$avSet=Get-AzureRmAvailabilitySet -Name $avName -ResourceGroupName
```



```
    $rgName
6
7  $vm2=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -
       AvailabilitySetId $avset.Id
8
9  $cred=Get-Credential -Message " Type Credentials which will be
       used to login to VPX instance "
10
11 $vm2=Set-AzureRmVMOperatingSystem -VM $vm2 -Linux -ComputerName
       $vmName -Credential $cred -Verbose
12
13 $vm2=Set-AzureRmVMSourceImage -VM $vm2 -PublisherName $pubName -
       Offer $offerName -Skus $skuName -Version "latest"
14
15 $vm2=Add-AzureRmVMNetworkInterface -VM $vm2 -Id $nic2.Id
16
17 $diskName="dynamic"
18
19 $storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName -
       Name $saName
20
21 $osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + "vhds2/
       " + $diskName  + ".vhd"
22
23 $vm2=Set-AzureRmVMOSDisk -VM $vm2 -Name $diskName -VhdUri
       $osDiskUri1 -CreateOption fromImage
24
25 Set-AzureRmVMPlan -VM $vm2 -Publisher $pubName -Product $offerName
     -Name $skuName
26
27 New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM
       $vm2
28 <!--NeedCopy-->
```

12. **Configurar las máquinas virtuales**

    Cuando se inician las dos instancias de Citrix ADC VPX, conéctese a ambas instancias de Citrix ADC VPX mediante el protocolo SSH para configurar las máquinas virtuales.

    a) Activo-Activo: Ejecute el mismo conjunto de comandos de configuración en la línea de comandos de ambas instancias de Citrix ADC VPX.

    b) Active-Passive: Ejecute este comando en la línea de comandos de ambas instancias de Citrix ADC VPX.

    ```
    add ha node ##nodeID <nsip of other Citrix ADC VPX>
    ```


En el modo Activo-Pasivo, ejecute comandos de configuración solo en el nodo principal.

Aprovisione un par Citrix ADC VPX en una configuración de alta disponibilidad con el equilibrador de carga interno de Azure

Inicie sesión en AzurermAccount con sus credenciales de usuario de Azure.

1. **Crear un grupo de recursos**

   La ubicación especificada aquí es la ubicación predeterminada de los recursos de ese grupo de recursos. Asegúrese de que todos los comandos para crear un equilibrador de carga utilizan el mismo grupo de recursos.

   `$rgName=”\<resource group name\>”`

   `$locName=”\<location name, such as West US\>”`

   `New-AzureRmResourceGroup -Name $rgName -Location $locName`

   Por ejemplo:

   ```
   $rgName = ”ARM-LB-NS”

   $locName = ”West US”

   New-AzureRmResourceGroup -Name $rgName -Location $locName
   <!--NeedCopy-->
   ```

2. **Crear una cuenta de almacenamiento**

   Elija un nombre único para su cuenta de almacenamiento que contenga solo letras y números minúsculas.

   `$saName=”<storage account name>”`

   `$saType=”<storage account type>”`, especifique uno: `Standard_LRS`, `Standard_GRS`, `Standard_RAGRS` o `Premium_LRS`

   `New-AzureRmStorageAccount -Name $saName -ResourceGroupName $rgName -Type $saType -Location $locName`

   Por ejemplo:

   ```
   $saName=”vpxstorage”

   $saType=”Standard_LRS”
   ```



```
4
5 New-AzureRmStorageAccount -Name $saName -ResourceGroupName $rgName
      -Type $saType -Location $locName
6 <!--NeedCopy-->
```

3. **Crear un conjunto de disponibilidad**

   Un equilibrador de carga configurado con un conjunto de disponibilidad garantiza que la aplicación esté siempre disponible.

   ```
   $avName="<availability set name>"
   ```

   ```
   New-AzureRmAvailabilitySet -Name $avName -ResourceGroupName $rgName -
   Location $locName
   ```

4. **Crear una red virtual**

   Agregue una nueva red virtual con al menos una subred, si la subred no se creó previamente.

```
1 $vnetName = "LBVnet"
2
3 $vnetAddressPrefix="10.0.0.0/16"
4
5 $FrontendAddressPrefix="10.0.1.0/24"
6
7 $BackendAddressPrefix="10.0.2.0/24"
8
9 $vnet=New-AzureRmVirtualNetwork -Name $vnetName -ResourceGroupName
     $rgName -Location $locName -AddressPrefix $vnetAddressPrefix -
    Subnet $frontendSubnet,$backendSubnet`
10
11 $frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
    frontendSubnet -AddressPrefix $FrontendAddressPrefix
12
13 $backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
    backendSubnet -AddressPrefix $BackendAddressPrefix
14 <!--NeedCopy-->
```

   Nota: Seleccione el valor del parámetro AddressPrefix según su requisito.

   Asigne subred front-end y back-end a la red virtual que creó anteriormente en este paso.

   Si la subred front-end es el primer elemento de la matriz VNet, SubnetID debe ser $vnet.subnets [0] .Id.

   Si la subred front-end es el segundo elemento de la matriz, el ID de subred debe ser $vnet.subnets [1] .Id, etc.

5. **Crear un grupo de direcciones back-end**

   ```
   $beaddresspool= New-AzureRmLoadBalancerBackendAddressPoolConfig -Name ”
   LB-backend”
   ```

6. **Crear reglas NAT**

   Cree reglas NAT para los servicios que no esté equilibrando la carga.

   ```
   $inboundNATRule1= New-AzureRmLoadBalancerInboundNatRuleConfig -
       Name ”Inboundnatrule1” -FrontendIpConfiguration $frontendIP -
       Protocol TCP -FrontendPort 3441 -BackendPort 3389

   $inboundNATRule2= New-AzureRmLoadBalancerInboundNatRuleConfig -
       Name ”RDP2” -FrontendIpConfiguration $frontendIP -Protocol TCP
       -FrontendPort 3442 -BackendPort 3389
   <!--NeedCopy-->
   ```

   Utilice puertos front-end y back-end según sus necesidades.

7. **Crear un sondeo de estado**

   Cree un sondeo de estado TCP con el puerto 9000 y el intervalo de 5 segundos.

   ```
   $healthProbe = New-AzureRmLoadBalancerProbeConfig -Name ”
       HealthProbe”  ” -Protocol tcp -Port 9000 -IntervalInSeconds 5 -
       ProbeCount 2
   <!--NeedCopy-->
   ```

8. **Crear una regla de equilibrio de carga**

   Cree una regla LB para cada servicio que esté equilibrando la carga.

   Por ejemplo:

   Puede utilizar el siguiente ejemplo para equilibrar la carga del servicio HTTP.

   ```
   $lbrule = New-AzureRmLoadBalancerRuleConfig -Name ”lbrule1” -
       FrontendIpConfiguration $frontendIP -BackendAddressPool
       $beAddressPool -Probe $healthProbe -Protocol Tcp -FrontendPort
       80 -BackendPort 80
   <!--NeedCopy-->
   ```

   Utilice puertos front-end y back-end según sus necesidades.

9. **Crear una entidad de equilibrador de carga**

   Cree el equilibrador de carga agregando todos los objetos (reglas NAT, reglas de equilibrador de carga, configuraciones de sondeo) juntos.

```
$NRPLB = New-AzureRmLoadBalancer -ResourceGroupName $rgname -Name
    ”InternalLB” -Location $locName -FrontendIpConfiguration
    $frontendIP -InboundNatRule $inboundNATRule1,$inboundNatRule2 -
    LoadBalancingRule $lbrule -BackendAddressPool $beAddressPool -
    Probe $healthProbe
<!--NeedCopy-->
```

10. **Crear una NIC**

    Cree dos NIC y asocie cada NIC con cada instancia de Citrix ADC VPX

```
$backendnic1= New-AzureRmNetworkInterface -ResourceGroupName
    $rgName -Name lb-nic1-be -Location $locName -PrivateIpAddress
    10.0.2.6 -Subnet $backendSubnet -LoadBalancerBackendAddressPool
     $nrplb.BackendAddressPools[0] -LoadBalancerInboundNatRule
    $nrplb.InboundNatRules[0]
<!--NeedCopy-->
```

    Esta NIC es para Citrix ADC VPX 1. La IP privada debe estar en la misma subred que la de la subred agregada.

```
$backendnic2= New-AzureRmNetworkInterface -ResourceGroupName
    $rgName -Name lb-nic2-be -Location $locName -PrivateIpAddress
    10.0.2.7 -Subnet $backendSubnet -LoadBalancerBackendAddressPool
     $nrplb.BackendAddressPools[0] -LoadBalancerInboundNatRule
    $nrplb.InboundNatRules[1].
<!--NeedCopy-->
```

    Esta NIC es para Citrix ADC VPX 2.El parámetro `Private IPAddress` puede tener cualquier IP privada según sus requisitos.

11. **Crear instancias Citrix ADC VPX**

    Cree dos instancias VPX que forman parte del mismo grupo de recursos y conjunto de disponibilidad, y conéctela al equilibrador de carga interno.

    a) Instancia 1 de Citrix ADC VPX

Por ejemplo:

```
$vmName="VPX1"

$vmSize="Standard_A3"

$avSet=Get-AzureRmAvailabilitySet -Name $avName -ResourceGroupName
    $rgName

$vm1=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -
   AvailabilitySetId $avset.Id

$cred=Get-Credential -Message "Type Credentials which will be used
    to login to VPX instance"

$vm1=Set-AzureRmVMOperatingSystem -VM $vm1 -Linux -ComputerName
   $vmName -Credential $cred -Verbose

$vm1=Set-AzureRmVMSourceImage -VM $vm1 -PublisherName $pubName -
   Offer $offerName -Skus $skuName -Version "latest"

$vm1=Add-AzureRmVMNetworkInterface -VM $vm1 -Id $backendnic1.Id

$diskName="dynamic"

$storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName -
   Name $saName

$osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + "vhds1/
   " + $diskName  + ".vhd"

$vm1=Set-AzureRmVMOSDisk -VM $vm1 -Name $diskName -VhdUri
   $osDiskUri1 -CreateOption fromImage

Set-AzureRmVMPlan -VM $vm1 -Publisher $pubName -Product $offerName
    -Name $skuName

New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM
   $vm1
<!--NeedCopy-->
```

b) Instancia 2 de Citrix ADC VPX

Por ejemplo:


```
$vmName=”VPX2”

$vmSize=”Standard_A3”

$avSet=Get-AzureRmAvailabilitySet -Name $avName -ResourceGroupName
    $rgName

$vm2=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -
    AvailabilitySetId $avset.Id

$cred=Get-Credential -Message ” Type Credentials which will be
    used to login to VPX instance ”

$vm2=Set-AzureRmVMOperatingSystem -VM $vm2 -Linux -ComputerName
    $vmName -Credential $cred -Verbose

$vm2=Set-AzureRmVMSourceImage -VM $vm2 -PublisherName $pubName -
    Offer $offerName -Skus $skuName -Version ”latest”

$vm2=Add-AzureRmVMNetworkInterface -VM $vm2 -Id $backendnic2.Id

$diskName=”dynamic”

$storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName -
    Name $saName

$osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + ”vhds2/
    ” + $diskName  + ”.vhd”

$vm2=Set-AzureRmVMOSDisk -VM $vm2 -Name $diskName -VhdUri
    $osDiskUri1 -CreateOption fromImage

Set-AzureRmVMPlan -VM $vm2 -Publisher $pubName -Product $offerName
    -Name $skuName

New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM
    $vm2
<!--NeedCopy-->
```

12. **Configurar las máquinas virtuales**

    Cuando se inician las dos instancias de Citrix ADC VPX, conéctese a ambas instancias de Citrix ADC VPX mediante el protocolo SSH para configurar las máquinas virtuales.

a) Activo-Activo: Ejecute el mismo conjunto de comandos de configuración en la línea de comandos de ambas instancias de Citrix ADC VPX.

b) Active-Passive: Ejecute este comando en la línea de comandos de ambas instancias de Citrix ADC VPX.

```
add ha node ##nodeID <nsip of other Citrix ADC VPX>
```

En el modo Activo-Pasivo, ejecute comandos de configuración solo en el nodo principal.

Preguntas frecuentes de Azure

August 20, 2021

- **¿ El procedimiento de actualización de la instancia de Citrix ADC VPX instalada desde Azure Marketplace es diferente del procedimiento de actualización local?**

  No. Puede actualizar la instancia de Citrix ADC VPX en la nube de Microsoft Azure a Citrix ADC VPX versión 11.1 o posterior, mediante procedimientos de actualización estándar de Citrix ADC VPX. Puede actualizar mediante procedimientos GUI o CLI. Para cualquier instalación nueva, use la imagen Citrix ADC VPX para la nube de Microsoft Azure.

  Para descargar las compilaciones de actualización de Citrix ADC VPX, vaya a **Descargas de Citrix** > **Firmware de Citrix ADC**.

- **¿Cómo corregir los movimientos MAC y los silenciamientos de la interfaz observados en instancias Citrix ADC VPX alojadas en Azure?**

  En el entorno Multi-NIC de Azure, de forma predeterminada, todas las interfaces de datos pueden mostrar movimientos MAC y silenciamientos de la interfaz. Para evitar movimientos MAC y silenciar la interfaz en entornos Azure, Citrix recomienda crear una VLAN por interfaz de datos (sin etiqueta) de la instancia VPX de ADC y vincular la IP principal de la NIC en Azure.

  Para obtener más información, consulte el artículo CTX224626 .

Implementar una instancia de Citrix ADC VPX en Google Cloud Platform

January 31, 2022

Puede implementar una instancia Citrix ADC VPX en Google Cloud Platform (GCP). Una instancia VPX en GCP le permite aprovechar las capacidades de computación en nube de GCP y utilizar las funciones de equilibrio de carga y administración de tráfico de Citrix para sus necesidades empresariales. Puede

implementar instancias VPX en GCP como instancias independientes. Se admiten configuraciones de NIC única y NIC múltiple.

Funcionalidades admitidas

Todas las funciones Premium, Advanced y Standard son compatibles con el GCP en función del tipo de licencia/versión utilizado.

Limitación

- No se admite IPv6.

Requisitos de hardware

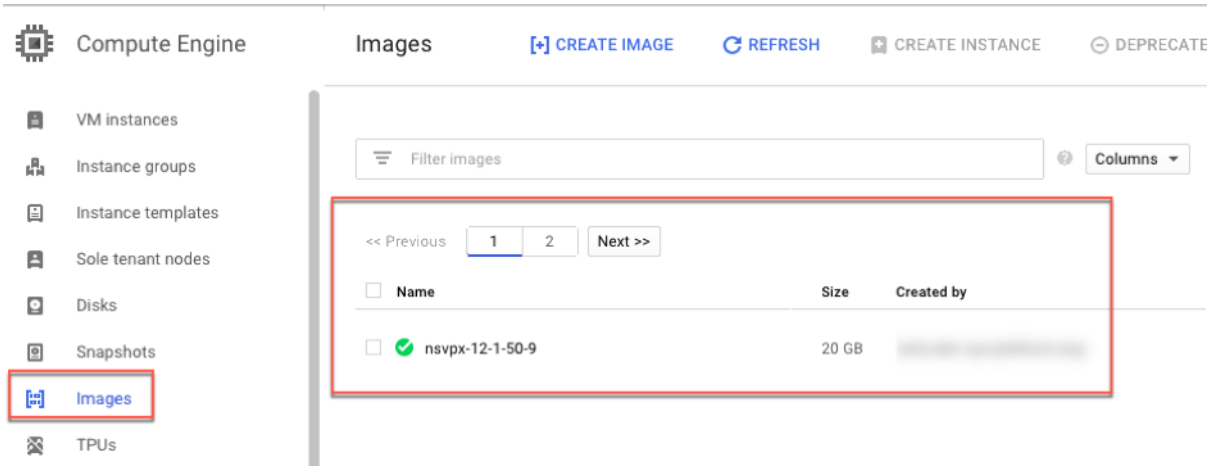
La instancia VPX en GCP debe tener un mínimo de 2 vCPU y 4 GB de RAM.

Requisitos previos

1. Instale la utilidad "gcloud" en su dispositivo. Puede encontrar la utilidad en este enlace: https://cloud.google.com/sdk/install
2. Descargue la imagen NSVPX-GCP del sitio de descargas de Citrix.
3. Sube el archivo (por ejemplo, NSVPX-GCP-12.1-50.9_NC_64.tar.gz) en un depósito de almacenamiento en Google siguiendo los pasos que se indican en https://cloud.google.com/storage/docs/uploading-objects.
4. Ejecuta el siguiente comando en la utilidad gcloud para crear una imagen.

```
1 gcloud compute images create <IMAGE_NAME> --source-uri=gs://<
    STORAGE_BUCKET_NAME>/<FILE_NAME>.tar.gz --guest-os-features=
    MULTI_IP_SUBNET
2 <!--NeedCopy-->
```

Puede que la imagen demore un momento en crearse. Después de crear la imagen, aparece en **Compute > ComputeEngine** en la consola de GCP.



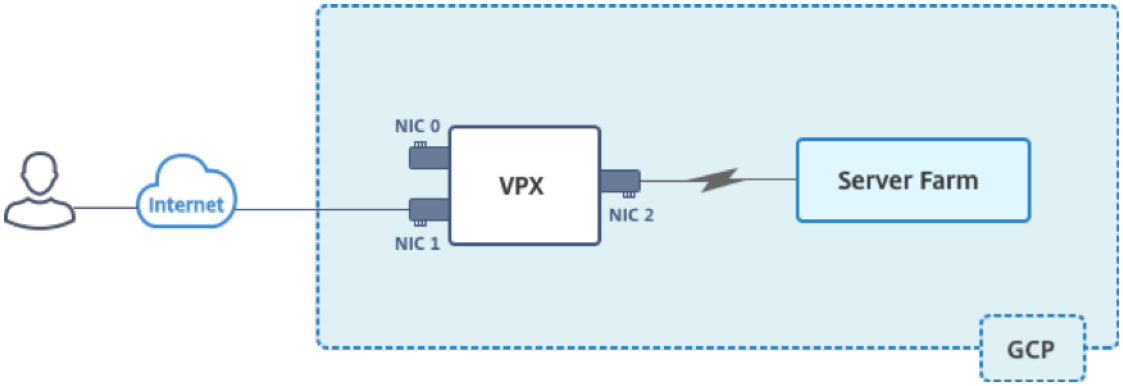
Puntos a tener en cuenta

Tenga en cuenta los siguientes puntos específicos de GCP antes de comenzar la implementación.

- Después de crear la instancia, no podrás agregar ni eliminar ninguna interfaz de red.
- Para una implementación de varias NIC, cree redes de VPC separadas para cada NIC. Una NIC solo se puede asociar a una red.
- Para una instancia de NIC única, la consola de GCP crea una red de forma predeterminada.
- Se requieren un mínimo de 4 vCPU para una instancia con más de dos interfaces de red.
- Si se requiere el reenvío de IP, debe habilitar el reenvío de IP al crear la instancia y configurar la NIC.

Caso: Implementar una instancia VPX independiente con varias NIC y varias IP

Este caso ilustra cómo implementar una instancia independiente de Citrix VPX en GCP. En este caso, se crea una instancia VPX independiente con muchas NIC. La instancia se comunica con los servidores back-end (la comunidad de servidores).



Cree tres NIC para cumplir los siguientes propósitos.

NIC	Propósito	Asociado a la red de VPC
NIC 0	Sirve el tráfico de administración (IP de Citrix ADC)	Red de gestión
NIC 1	Sirve tráfico del lado del cliente (VIP)	Red de clientes
NIC 2	Se comunica con servidores back-end (SNIP)	Red de servidores back-end

Configure las rutas de comunicación requeridas entre las siguientes:

- La instancia VPX y los servidores back-end.
- La instancia VPX y los hosts externos en la Internet pública.

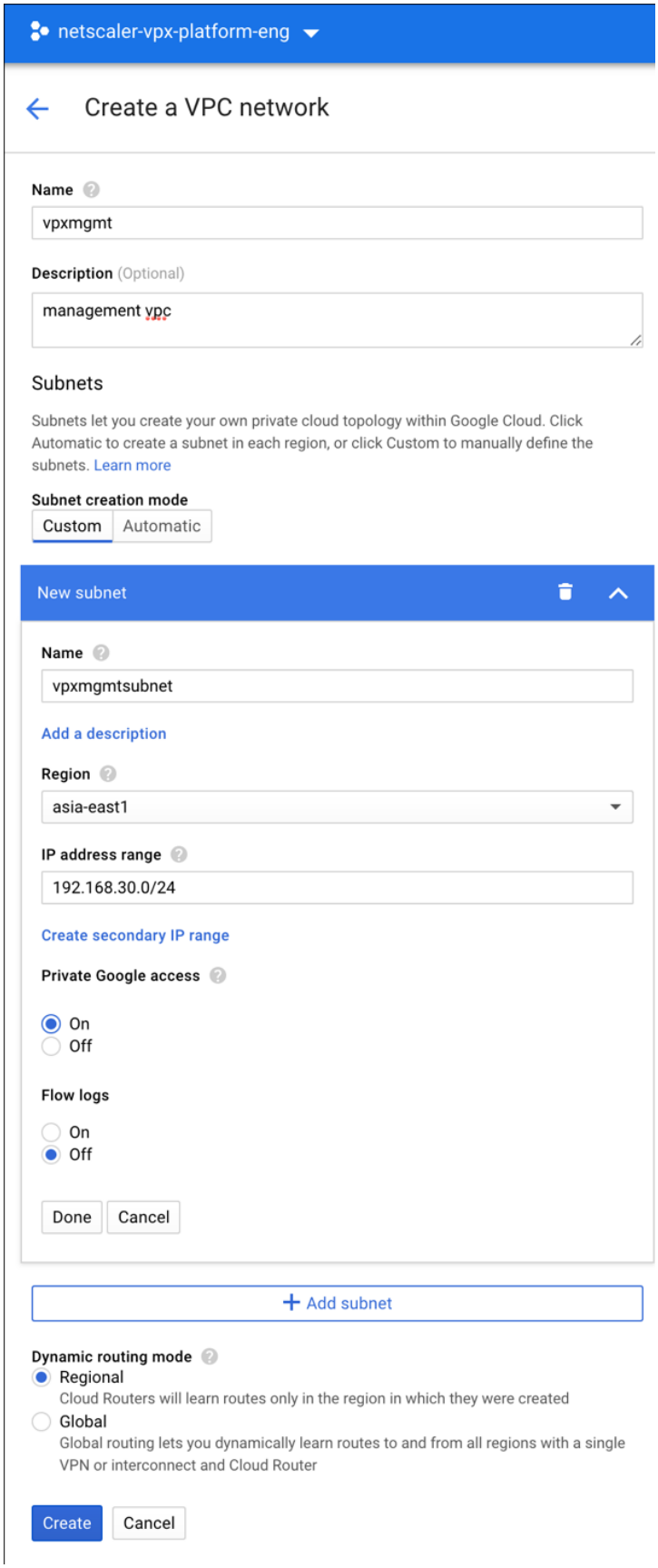
Resumen de los pasos de implementación

1. Cree tres redes de VPC para tres NIC diferentes.
2. Crear reglas de firewall para los puertos 22, 80 y 443
3. Crear una instancia con tres NIC

Nota: Crea una instancia en la misma región en la que creaste las redes de VPC.

Paso 1. Cree redes de VPC.

Cree tres redes de VPC asociadas con la NIC de administración, la NIC de cliente y la NIC de servidor. Para crear una red de VPC, inicie sesión en la **consola de Google > Redes > Red de VPC > Crear red de VPC**. Complete los campos obligatorios, como se muestra en la captura de pantalla, y haga clic en **Crear**.

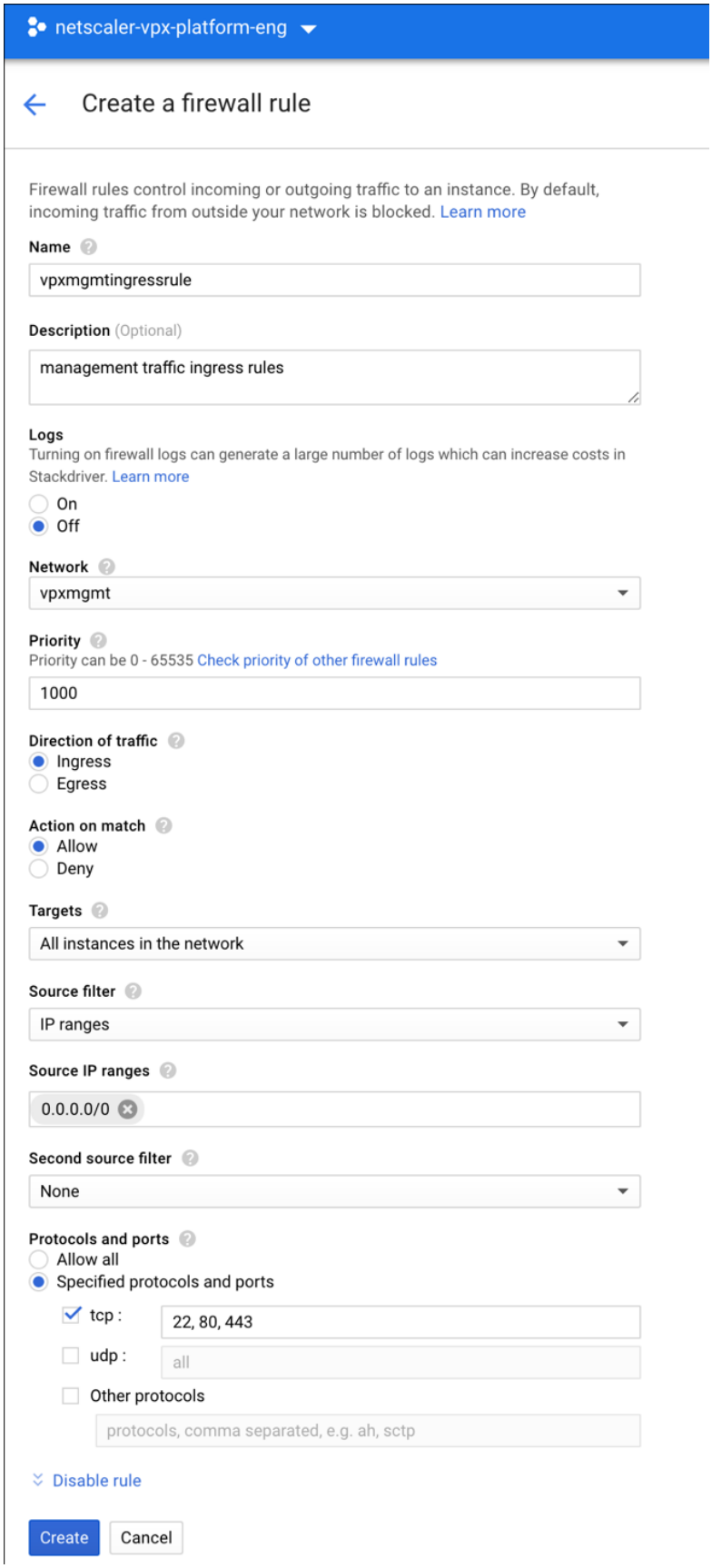


Del mismo modo, cree redes de VPC para NIC del lado del cliente y del servidor.

Nota: Las tres redes de VPC deben estar en la misma región, que es asia-east1 en este caso.

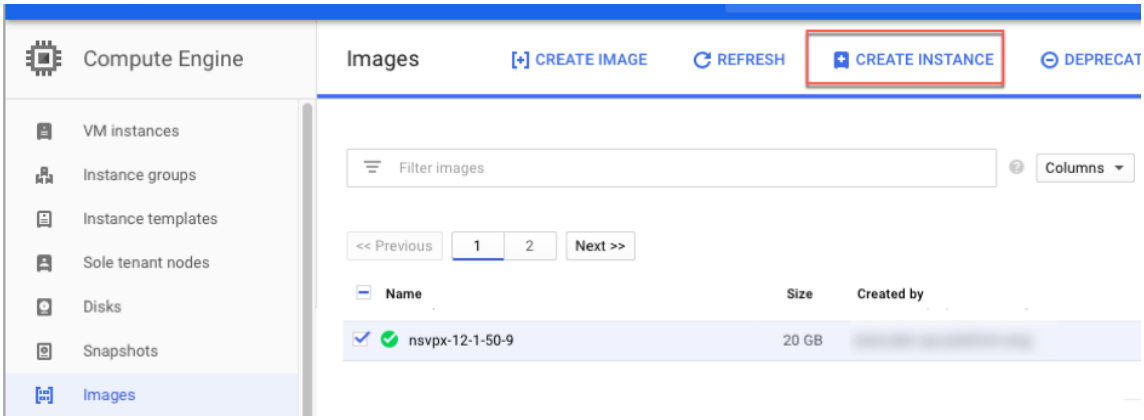
Paso 2. Cree reglas de firewall para los puertos 22, 80 y 443.

Cree reglas para SSH (puerto 22), HTTP (puerto 80) y HTTPS (puerto 443) para cada red VPC. Para obtener más información acerca de las reglas del firewall, consulte Descripción general de las reglas



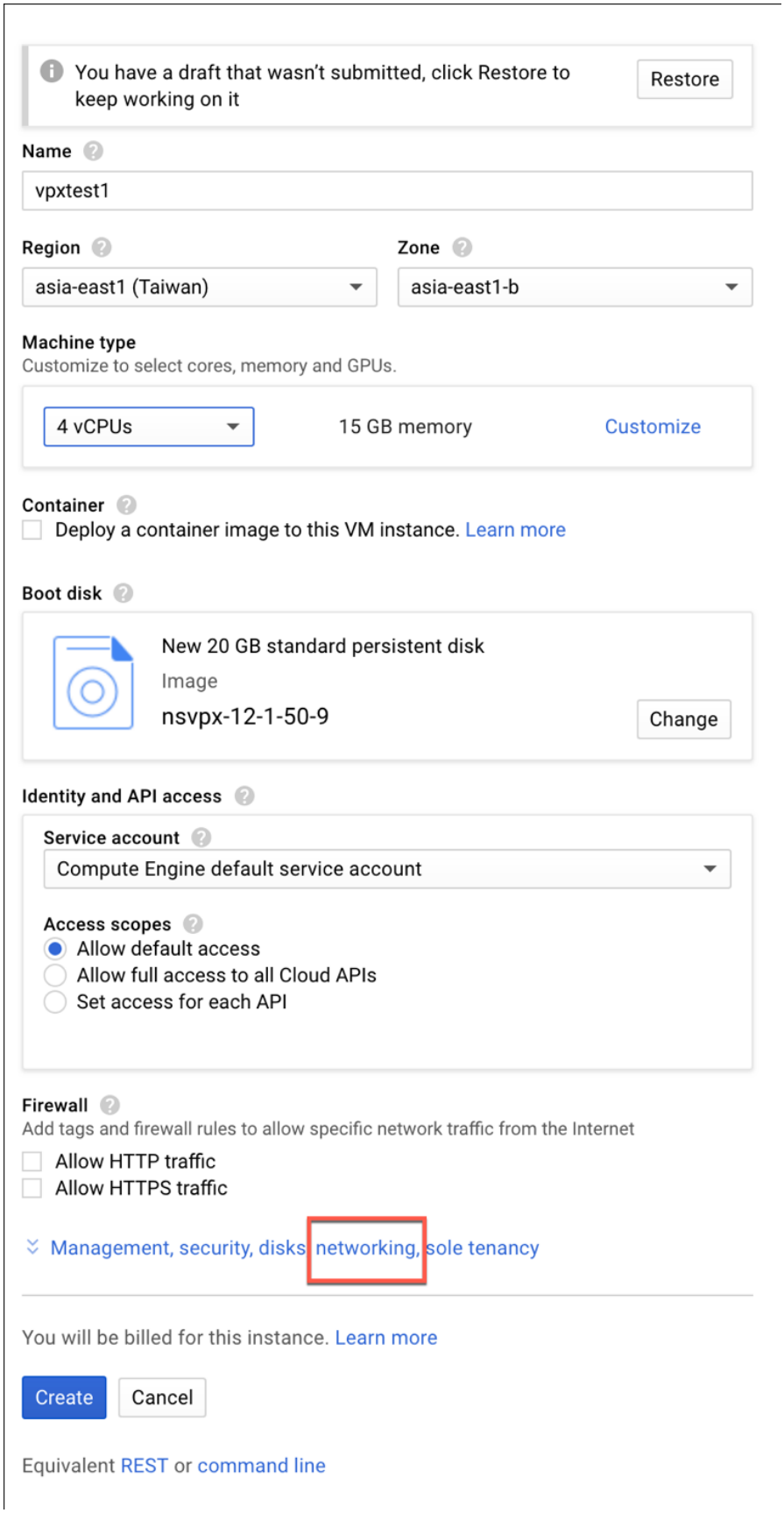
Paso 3. Crea la instancia VPX.

1. Inicie sesión en la consola de GCP.
2. En **Compute**, coloque el cursor sobre Compute Engine y seleccione **Imágenes**.
3. Seleccione la imagen y haga clic en **Crear instancia**.

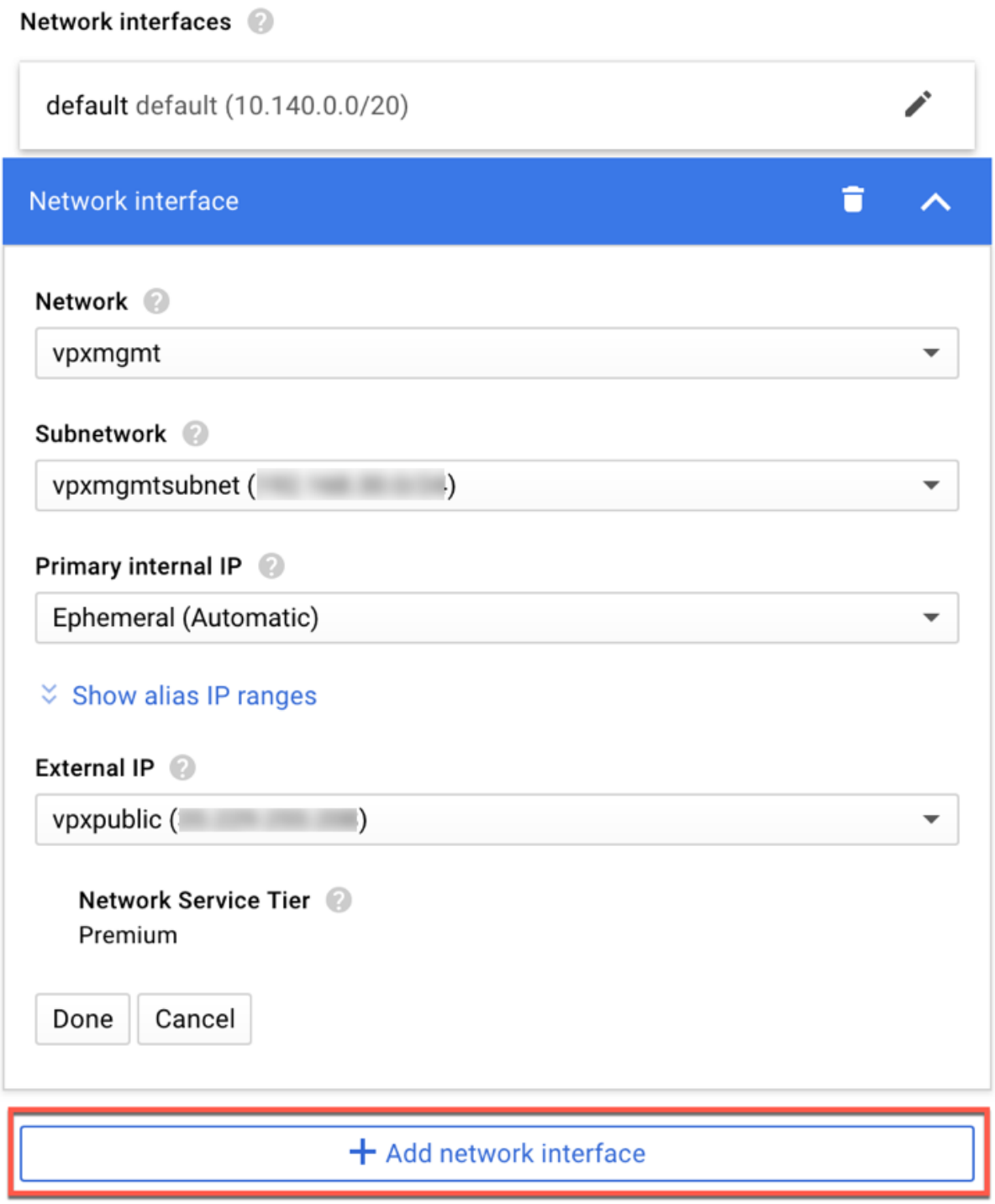


4. Seleccione una instancia con 4 vCPU para admitir varias NIC.
5. Haga clic en la opción de red en Administración, seguridad, discos, redes, arrendamiento único para agregar las NIC adicionales.

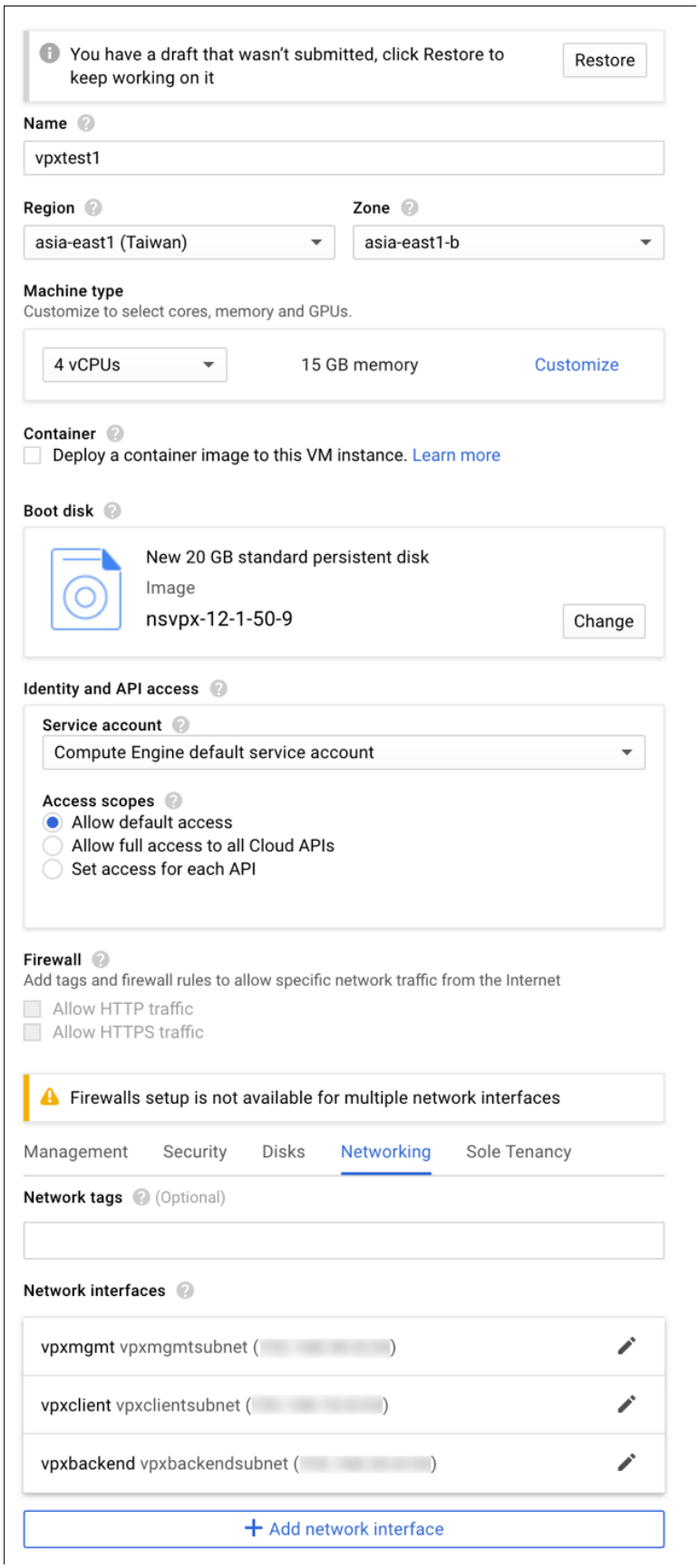
   Nota: La imagen de contenedor no se admite en instancias VPX en GCP.



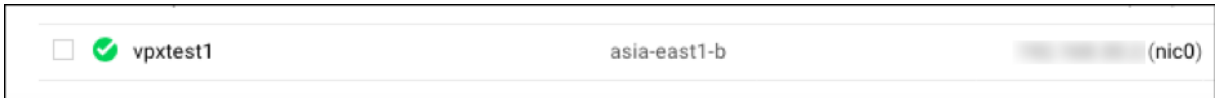
6. En **Interfaces de red**, haga clic en el icono de edición para modificar la NIC predeterminada. Esta NIC es la NIC de administración.
7. En la ventana **Interfaces de red**, en **Red**, seleccione la red de VPC que creó para la NIC de administración.
8. Para la NIC de administración, cree una dirección IP externa estática. En la lista IP externa, haga clic en **Crear dirección IP**.
9. En la ventana **Reservar una nueva dirección IP estática**, agrega un nombre y una descripción y haga clic en **Reservar**.
10. Haga clic en **Agregar interfaz de red** para crear NIC para el tráfico del lado del cliente y del servidor.



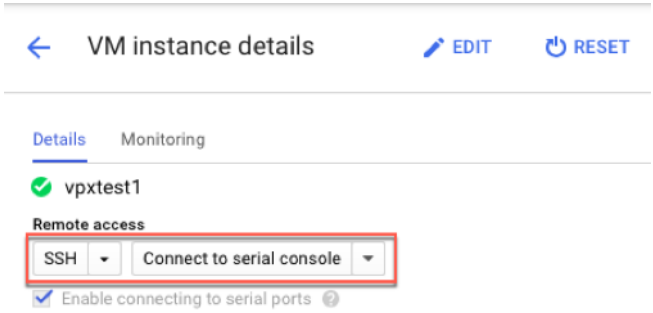
Una vez que hayas creado todas las NIC., haga clic en **Crear** para crear la instancia VPX.



La instancia aparece en **instancias de VM**.

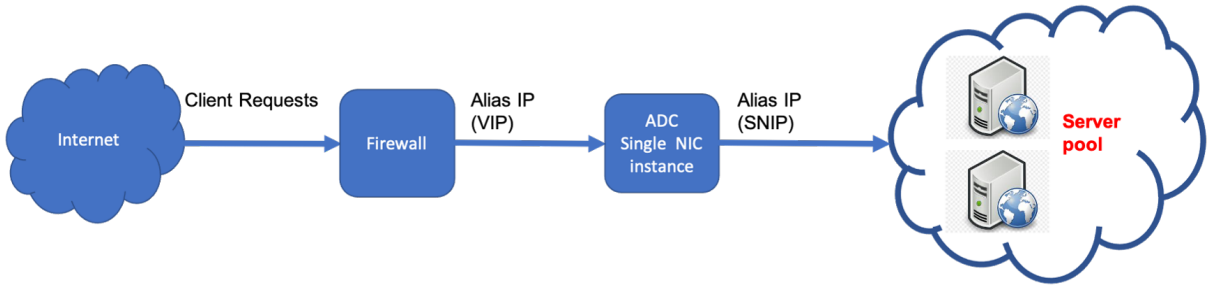


Usa el SSH de GCP o la consola serie para configurar y administrar la instancia VPX.



Caso: Implementar una instancia VPX independiente de NIC única

Este caso ilustra cómo implementar una instancia independiente de Citrix VPX con una única NIC en GCP. Las direcciones IP de alias se utilizan para lograr esta implementación.



Cree una única NIC (NIC0) para cumplir con los siguientes propósitos:

- Maneje el tráfico de administración (Citrix ADC IP) en la red de administración.
- Manejar el tráfico del lado del cliente (VIP) en la red del cliente.
- Comuníquese con los servidores back-end (SNIP) en la red de servidores back-end.

Configure las rutas de comunicación requeridas entre las siguientes:

- Servidores de instancias y back-end.
- Instancia y los hosts externos en la Internet pública.

Resumen de los pasos de implementación

1. Cree una red de VPC para NIC0.
2. Cree reglas de firewall para los puertos 22, 80 y 443.

3. Crea una instancia con una única NIC.
4. Agregue direcciones IP de alias a VPX.
5. Agrega VIP y SNIP en VPX.
6. Agregue un servidor virtual de equilibrio de carga.
7. Agrega un servicio o un grupo de servicios en la instancia.
8. Enlace el servicio o el grupo de servicios al servidor virtual de equilibrio de carga en la instancia.

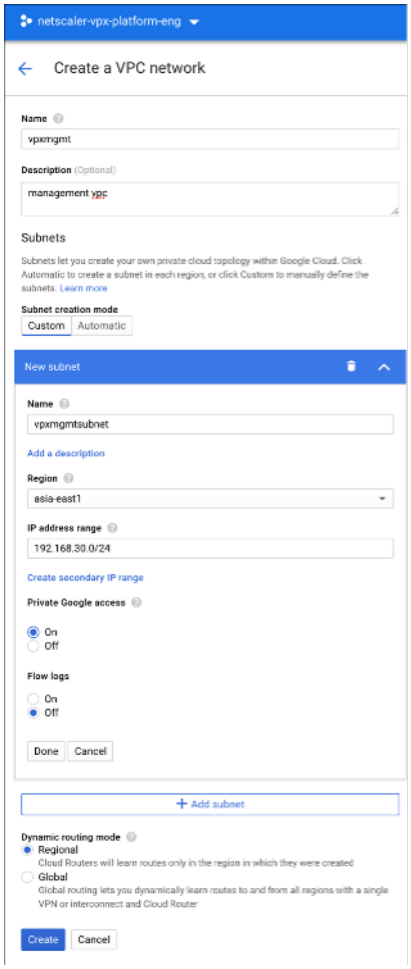
> **Nota**:
>
> Crea una instancia en la misma región en la que creaste las redes de VPC.

Paso 1. Cree una red de VPC.

Cree una red de VPC para asociarla a NIC0.

Para crear una red de VPC, siga estos pasos:

1. Inicie sesión en la **consola de GCP > Redes > Red de VPC > Crear red de VPC**
2. Complete los campos obligatorios y haga clic en **Crear**.



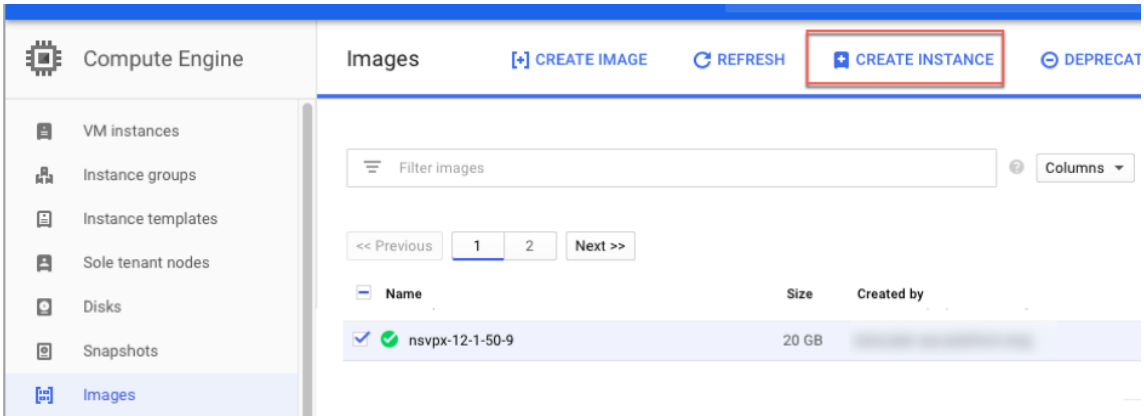
Paso 2. Cree reglas de firewall para los puertos 22, 80 y 443.

Cree reglas para SSH (puerto 22), HTTP (puerto 80) y HTTPS (puerto 443) para la red de VPC. Para obtener más información acerca de las reglas del firewall, consulte Descripción general de las reglas

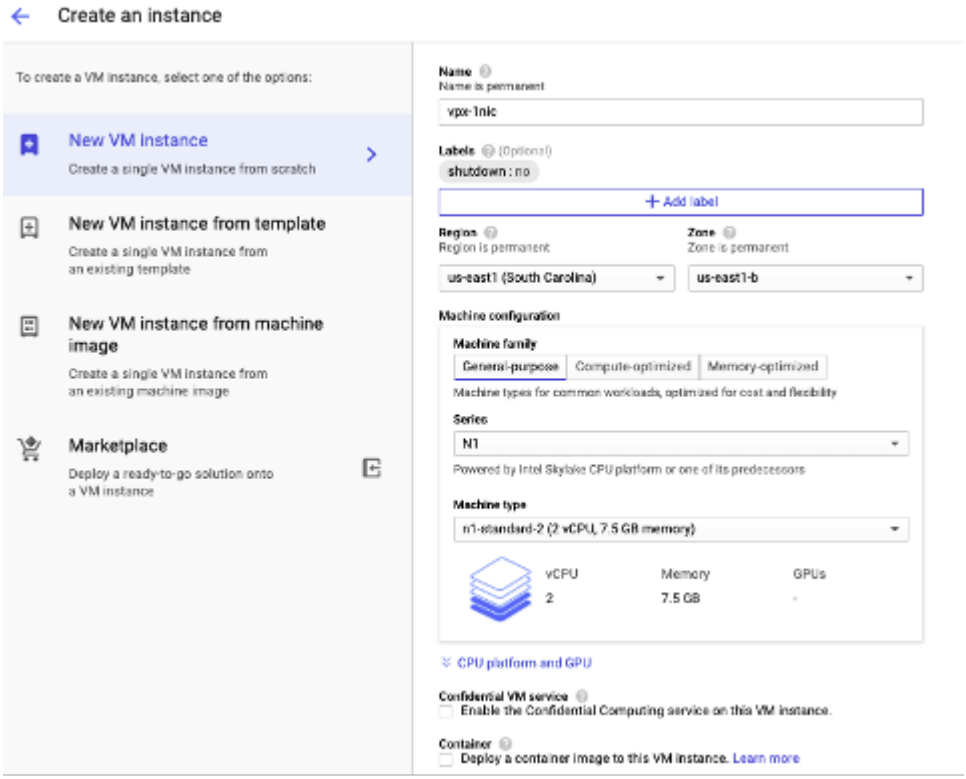
Paso 3. Cree una instancia con una NIC única.

Para crear una instancia con una sola NIC, siga estos pasos:

1. Inicie sesión en la **consola de GCP**.
2. En **Compute**, coloque el cursor sobre **Compute Engine** y seleccione **Imágenes**.
3. Seleccione la imagen y haga clic en **Crear instancia**.



4. Seleccione un tipo de instancia con dos vCPU (requisito mínimo para ADC).



5. Haga clic en la ficha **Redes** en la ventana **Administración, seguridad, discos, redes**.
6. En **Interfaces de red**, haga clic en el icono **Modificar** para modificar la NIC predeterminada.
7. En la ventana **Interfaces** de **red, en Red**, seleccione la red de VPC que creó.
8. Puede crear una dirección IP externa estática. En **Direcciones IP externas**, haga clic en **Crear dirección IP**.
9. En la ventana **Reservar una dirección estática**, agrega un nombre y una descripción y haga clic en **Reservar**.
10. Haga clic en **Crear** para crear la instancia VPX.

La nueva instancia aparece en instancias de VM.

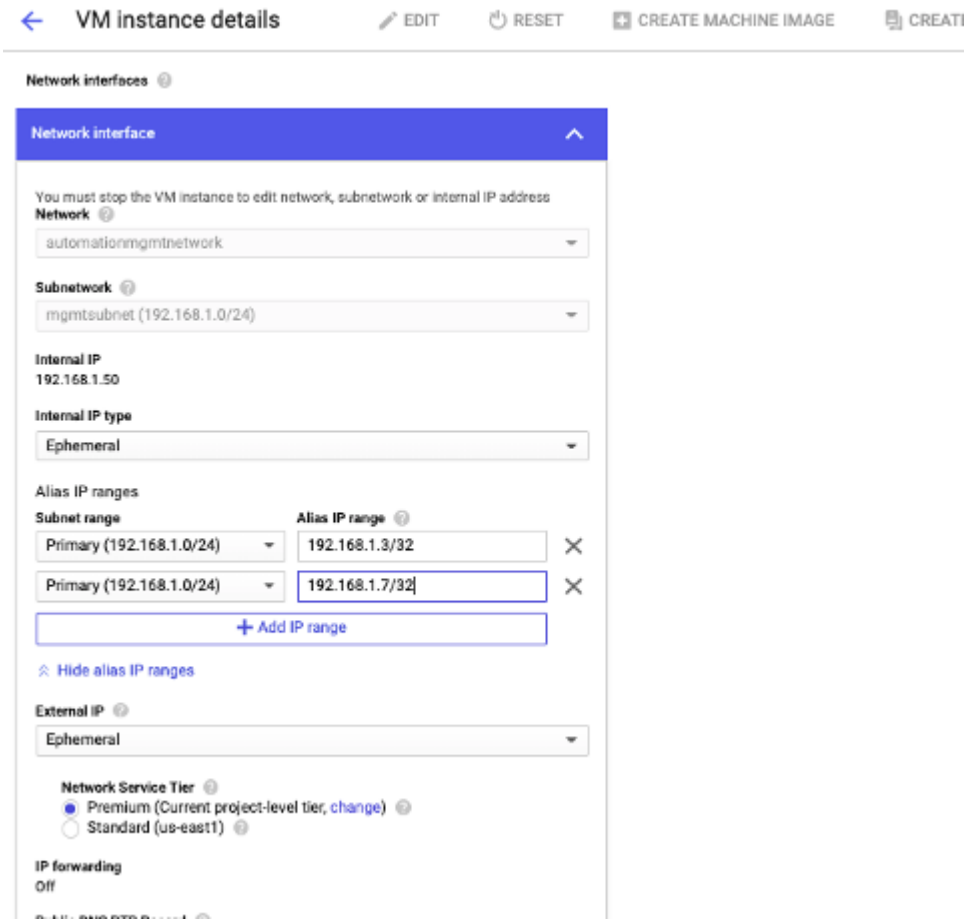
Paso 4. Agrega direcciones IP alias a la instancia VPX.

Asigne dos direcciones IP alias a la instancia VPX para usarlas como direcciones VIP y SNIP.

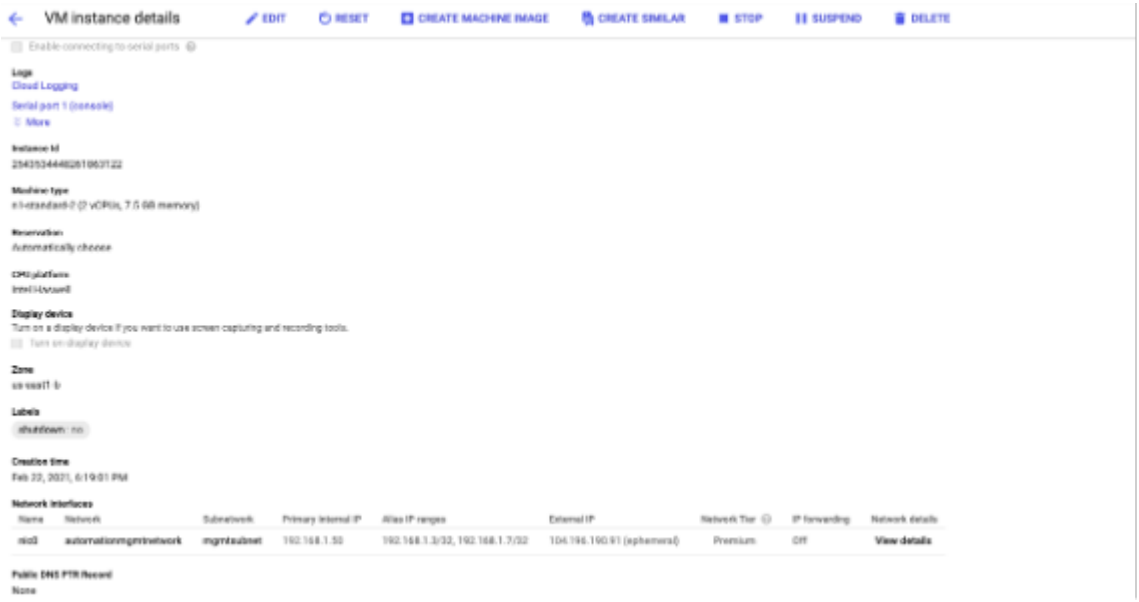
> **Nota:**
>
> No utilices la dirección IP interna principal de la instancia VPX para configurar el VIP o el SNIP.

Para crear una dirección IP de alias, lleve a cabo estos pasos:

1. Vaya a la instancia de VM y haga clic en **Modificar**.
2. En la ventana **Interfaz de red**, modifique la interfaz NIC0.
3. En el campo **Intervalo de IP de alias**, introduzca las direcciones IP de alias.



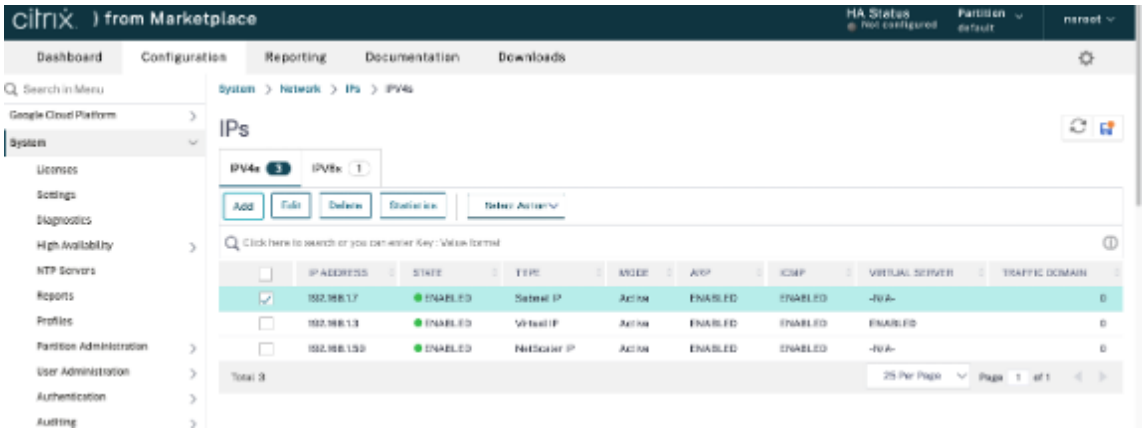
4. Haga clic en **Listo**y, a continuación, en **Guardar**.
5. Compruebe las direcciones IP de alias en la página de **detalles de la instancia de VM**.



Paso 5. Agrega VIP y SNIP en la instancia VPX.

En la instancia VPX, agregue la dirección IP del alias del cliente y la dirección IP del alias del servidor.

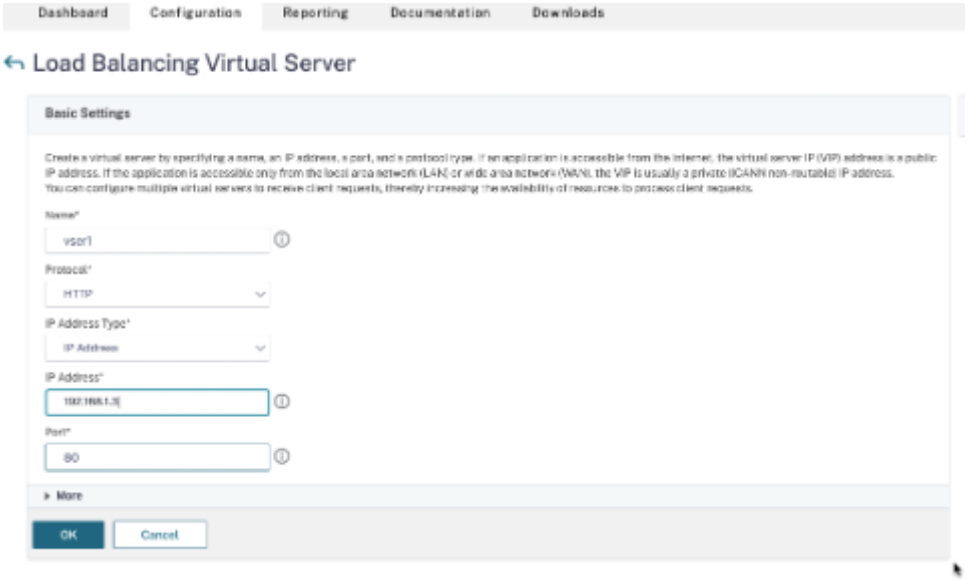
1. En la GUI de Citrix ADC, vaya a **Sistema > Red > IP > IPv4**y haga clic en **Agregar**.



2. Para crear una dirección IP (VIP) de alias de cliente:
   - Introduzca la dirección IP de alias de cliente y la máscara de red configuradas para la sub-red de VPC en la instancia de VM.
   - En el campo **Tipo de IP**, seleccione **IP virtual** en el menú desplegable.
   - Haga clic en **Crear**.
3. Para crear una dirección IP de alias de servidor (SNIP):
   - Introduzca la dirección IP de alias del servidor y la máscara de red configuradas para la subred de VPC en la instancia de VM.
   - En el campo **Tipo de IP**, seleccione **IP de subred** en el menú desplegable.
   - Haga clic en **Crear**.

Paso 6. Agregue un servidor virtual de equilibrio de carga.

1. En la GUI de Citrix ADC, vaya a **Configuración > Administración del tráfico > Equilibrio de carga > Servidores virtuales**y haga clic en **Agregar**.
2. Agregue los valores requeridos para Nombre, Protocolo, Tipo de dirección IP (dirección IP), Dirección IP (IP de alias de cliente) y Puerto.
3. Haga clic en **Aceptar** para crear el servidor virtual de equilibrio de carga.



Paso 7. Agrega un servicio o un grupo de servicios en la instancia VPX.

1. En la GUI de Citrix ADC, vaya a **Configuración > Administración del tráfico > Equilibrio de carga > Servicios**y haga clic en **Agregar**.
2. Agregue los valores requeridos para Nombre de servicio, Dirección IP, Protocolo y Puerto y haga clic en **Aceptar**.

Paso 8. Enlace el grupo de servicios/servicios al servidor virtual de equilibrio de carga en la instancia.

1. En la GUI, vaya a **Configuración > Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. Seleccione el servidor virtual de equilibrio de carga configurado en el **paso 6**y haga clic en **Modificar**.
3. En la ventana **Grupos de servicios y servicios**, haga clic en **Enlace de servicio de servidor virtual sin equilibrio de carga**.
4. Seleccione el servicio configurado en el **paso 7**y haga clic en **Vincular**.

Puntos a tener en cuenta después de implementar la instancia VPX en GCP

- Inicie sesión en el VPX con el nombre de usuario `nsroot` y el ID de instancia como contraseña. Cuando se le solicite, cambie la contraseña y guarde la configuración.
- Para recopilar un paquete de asistencia técnica, ejecute el comando `shell /netscaler/showtech_cloud.pl` en lugar del habitual `show techsupport`.
- Después de eliminar una VM de Citrix ADC de la consola de GCP, elimine también la instancia de destino interna de Citrix ADC asociada. Para hacerlo, vaya a la CLI de gcloud y escriba el siguiente comando:

```
1  gcloud compute -q  target-instances delete <instance-name>-
      adcinternal --zone <zone>
2  <!--NeedCopy-->
```

> Nota: `<instance-name>-adcinternal` es el nombre de la instancia de destino que se debe eliminar.

Licencias de Citrix ADC VPX

Una instancia de Citrix ADC VPX en GCP requiere una licencia. Las siguientes opciones de licencia están disponibles para instancias de Citrix ADC VPX que se ejecutan en GCP.

- **Licencias basadas en suscripción**: los dispositivos Citrix ADC VPX están disponibles como instancias de pago en el mercado de GCP. Las licencias basadas en suscripciones son una opción de pago por uso. A los usuarios se les cobra cada hora. Los siguientes modelos VPX y ediciones de licencias están disponibles en el mercado de GCP.

  |Modelo VPX|Ediciones de licencias|
  |—|—|
  |VPX10| Estándar, Avanzado, Premium|
  | |

- **Traiga su propia licencia (BYOL)**: Si trae su propia licencia (BYOL), consulte la Guía de licencias de VPX en http://support.citrix.com/article/CTX122426. Es necesario que:
  - Utilice el portal de licencias del sitio web de Citrix para generar una licencia válida.
  - Cargue la licencia en la instancia.
- Licencias de**Check-in/Check-out de Citrix ADC VPX: Para obtener más información, consulte Licencias**de Check-in/Check-out de Citrix ADC VPX.

VPX Express para implementaciones locales y en la nube no requiere un archivo de licencia. Para obtener más información sobre Citrix ADC VPX Express, consulte la sección “Licencia de Citrix ADC

VPX Express" de la descripción general de licencias de Citrix ADC.

Plantillas de GDM para implementar una instancia de Citrix ADC VPX

Puede utilizar una plantilla de Citrix ADC VPX Google Deployment Manager (GDM) para implementar una instancia VPX en GCP. Para obtener más información, consulte Plantillas GDM de Citrix ADC.

Imágenes del mercado de Citrix ADC

Puede utilizar las imágenes de las plantillas de GDM para que aparezca el dispositivo Citrix ADC.

En la siguiente tabla se enumeran las imágenes que están disponibles en el sitio web de GCP.

Versión	Nombre de imagen	Ubicación de la imagen
13.0	citrix-adc-vpx-10-enterprise-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-10-enterprise-13-0-83-29
13.0	citrix-adc-vpx-10-platinum-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-10-platinum-13-0-83-29
13.0	citrix-adc-vpx-10-standard-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-10-standard-13-0-83-29
13.0	citrix-adc-vpx-200-enterprise-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-200-enterprise-13-0-83-29
13.0	citrix-adc-vpx-200-platinum-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-200-platinum-13-0-83-29
13.0	citrix-adc-vpx-200-standard-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-200-standard-13-0-83-29

Versión	Nombre de imagen	Ubicación de la imagen
13.0	citrix-adc-vpx-1000-advanced-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-1000-advanced-13-0-83-29
13.0	citrix-adc-vpx-1000-premium-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-1000-premium-13-0-83-29
13.0	citrix-adc-vpx-1000-standard-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-1000-standard-13-0-83-29
13.0	citrix-adc-vpx-3000-enterprise-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-3000-enterprise-13-0-83-29
13.0	citrix-adc-vpx-3000-platinum-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-3000-platinum-13-0-83-29
13.0	citrix-adc-vpx-3000-standard-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-3000-standard-13-0-83-29
13.0	citrix-adc-vpx-5000-enterprise-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-5000-enterprise-13-0-83-29
13.0	citrix-adc-vpx-5000-platinum-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-5000-platinum-13-0-83-29
13.0	citrix-adc-vpx-5000-standard-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-5000-standard-13-0-83-29

Versión	Nombre de imagen	Ubicación de la imagen
13.0	citrix-adc-vpx-byol-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-byol-13-0-83-29
13.0	citrix-adc-vpx-express-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-express-13-0-83-29
13.0	citrix-adc-vpx-waf-1000-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-waf-1000-13-0-83-29
13.1	citrix-adc-vpx-10-enterprise-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-10-enterprise-13-1-9-60
13.1	citrix-adc-vpx-10-platinum-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-10-platinum-13-1-9-60
13.1	citrix-adc-vpx-10-standard-13-1-9-60	projects/citrix-master-project/global/imagescitrix-adc-vpx-10-standard-13-1-9-60
13.1	citrix-adc-vpx-200-enterprise-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-200-enterprise-13-1-9-60
13.1	citrix-adc-vpx-200-platinum-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-200-platinum-13-1-9-60
13.1	citrix-adc-vpx-200-standard-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-200-standard-13-1-9-60

Versión	Nombre de imagen	Ubicación de la imagen
13.1	citrix-adc-vpx-1000-advanced-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-1000-advanced-13-1-9-60
13.1	citrix-adc-vpx-1000-premium-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-1000-premium-13-1-9-60
13.1	citrix-adc-vpx-1000-standard-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-1000-standard-13-1-9-60
13.1	citrix-adc-vpx-3000-enterprise-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-3000-enterprise-13-1-9-60
13.1	citrix-adc-vpx-3000-platinum-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-3000-platinum-13-1-9-60
13.1	citrix-adc-vpx-3000-standard-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-3000-standard-13-1-9-60
13.1	citrix-adc-vpx-5000-enterprise-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-5000-enterprise-13-1-9-60
13.1	citrix-adc-vpx-5000-platinum-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-5000-platinum-13-1-9-60
13.1	citrix-adc-vpx-5000-standard-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-5000-standard-13-1-9-60

Versión	Nombre de imagen	Ubicación de la imagen
13.1	citrix-adc-vpx-byol-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-byol-13-1-9-60
13.1	citrix-adc-vpx-express-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-express-13-1-9-60
13.1	citrix-adc-vpx-waf-1000-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-waf-1000-13-1-9-60

Recursos

- Creación de instancias con múltiples interfaces de red
- Creación e inicio de una instancia de VM

Información relacionada

- Implementar un par de VPX de alta disponibilidad en Google Cloud Platform

Implementar un par de alta disponibilidad VPX en Google Cloud Platform

August 20, 2021

Puede configurar dos instancias de Citrix ADC VPX en Google Cloud Platform (GCP) como un par activo-pasivo de alta disponibilidad (HA). Cuando configura una instancia como nodo principal y la otra como nodo secundario, el nodo principal acepta conexiones y administra servidores. El nodo secundario supervisa el principal. Si, por cualquier motivo, el nodo principal no puede aceptar conexiones, el nodo secundario se hace cargo.

Para obtener más información sobre HA, consulte Alta disponibilidad.

Los nodos deben estar en la misma región; sin embargo, pueden estar en la misma zona o en zonas diferentes. Para obtener más información, consulte Regiones y zonas.

Cada instancia VPX requiere al menos tres subredes IP (redes de Google VPC):

- Una subred de administración

- Una subred (VIP) orientada al cliente
- Una subred orientada al back-end (SNIP, MIP, etc.)

Citrix recomienda tres interfaces de red para una instancia VPX estándar.

Puede implementar un par de alta disponibilidad VPX en los siguientes métodos:

- Uso de la dirección IP estática externa
- Uso de la dirección IP privada

Plantillas de GDM para implementar un par de alta disponibilidad VPX en GCP

Puede utilizar una plantilla de Citrix ADC Google Deployment Manager (GDM) para implementar un par de alta disponibilidad VPX en GCP. Para obtener más información, consulte Plantillas GDM de Citrix ADC.

Compatibilidad con reglas de reenvío para el par de alta disponibilidad VPX en GCP

Puede implementar un par de alta disponibilidad VPX en el GCP mediante reglas de reenvío.

Para obtener más información sobre las reglas de reenvío, consulte Descripción general de las reglas de reenvío.

Requisitos previos

- Las reglas de reenvío deben estar en la misma región que las instancias VPX.
- Las instancias de destino deben estar en la misma zona que la instancia VPX.
- El número de instancias de destino para nodos primario y secundario debe coincidir.

Ejemplo:

Tiene un par de alta disponibilidad en la `us-east1` región con VPX principal en la `us-east1-b` zona y VPX secundaria en la `us-east1-c` zona. Se configura una regla de reenvío para la VPX principal con la instancia de destino en la `us-east1-b` zona. Configure una instancia de destino para VPX secundaria en la `us-east1-c` zona para actualizar la regla de reenvío en caso de conmutación por error.

Limitaciones

Solo las reglas de reenvío configuradas con instancias de destino en el back-end se admiten en la implementación de alta disponibilidad de VPX.

Implementar un par de alta disponibilidad VPX con dirección IP estática externa en Google Cloud Platform

October 5, 2021

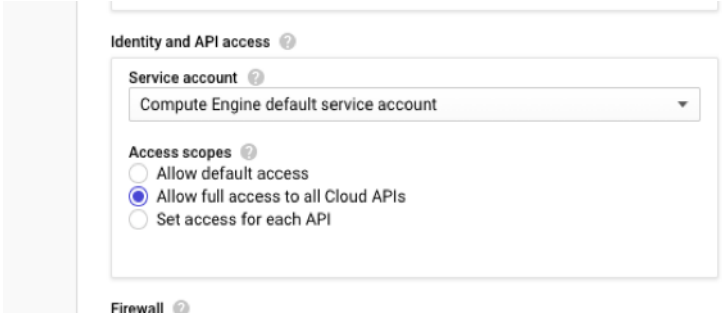
Puede implementar un par de alta disponibilidad VPX en GCP mediante una dirección IP estática externa. La dirección IP del cliente del nodo principal debe estar enlazada a una dirección IP estática externa. En caso de conmutación por error, la dirección IP estática externa se mueve al nodo secundario para que se reanude el tráfico.

Una dirección IP externa estática es una dirección IP externa que está reservada para su proyecto hasta que decidas publicarla. Si utiliza una dirección IP para acceder a un servicio, puede reservar esa dirección IP para que solo su proyecto pueda utilizarla. Para obtener más información, consulte Reserva de una dirección IP externa estática.

Para obtener más información sobre HA, consulte Alta disponibilidad.

Antes de comenzar

- Lea las limitaciones, requisitos de hardware y puntos a tener en cuenta que se mencionan en Implementar una instancia Citrix ADC VPX en Google Cloud Platform. Esta información se aplica también a implementaciones de alta disponibilidad.
- Habilite **Cloud Resource Manager API** para su proyecto GCP.
- Permite el acceso completo a todas las API de Cloud mientras creas las instancias.



- Asegúrese de que el rol de IAM asociado a su cuenta de servicio de GCP tenga los siguientes permisos de IAM:

```
REQUIRED_INSTANCE_IAM_PERMS = [

"compute.addresses.use",
"compute.forwardingRules.list",
"compute.forwardingRules.setTarget",
```



```
6   "compute.instances.setMetadata"
7   "compute.instances.addAccessConfig",
8   "compute.instances.deleteAccessConfig",
9   "compute.instances.get",
10  "Compute.instances.list",
11  "compute.networks.useExternalIp",
12  "compute.subnetworks.useExternalIp",
13  "compute.targetInstances.list",
14  "compute.targetInstances.use",
15  "compute.targetInstances.create",
16  "compute.zones.list",
17  "compute.zoneOperations.get",
18  ]
19  <!--NeedCopy-->
```

- Si has configurado direcciones IP de alias en una interfaz distinta de la interfaz de administración, asegúrate de que su cuenta de servicio de GCP tenga los siguientes permisos de IAM adicionales:

```
1   "compute.instances.updateNetworkInterface"
2   <!--NeedCopy-->
```

- Si ha configurado reglas de reenvío de GCP en el nodo principal, lea las limitaciones y requisitos mencionados en Compatibilidad con reglas de reenvío para el par de alta disponibilidad VPX en GCP para actualizarlas a nuevo primario en caso de conmutación por error.

Cómo implementar un par VPX HA en Google Cloud Platform

Este es un resumen de los pasos de implementación de alta disponibilidad:

1. Cree redes de VPC en la misma región. Por ejemplo, Asia-este.
2. Crea dos instancias VPX (nodos primario y secundario) en la misma región. Pueden estar en la misma zona o en zonas diferentes. Por ejemplo, Asia east-1a y Asia East-IB.
3. Configure la configuración de HA en ambas instancias mediante los comandos de Citrix ADC GUI o ADC CLI.

Paso 1. Creación de redes de VPC

Cree redes de VPC en función de sus requisitos. Citrix recomienda crear tres redes de VPC para asociarse con NIC de administración, NIC cliente y NIC de servidor.

Para crear una red VPC, lleve a cabo estos pasos:

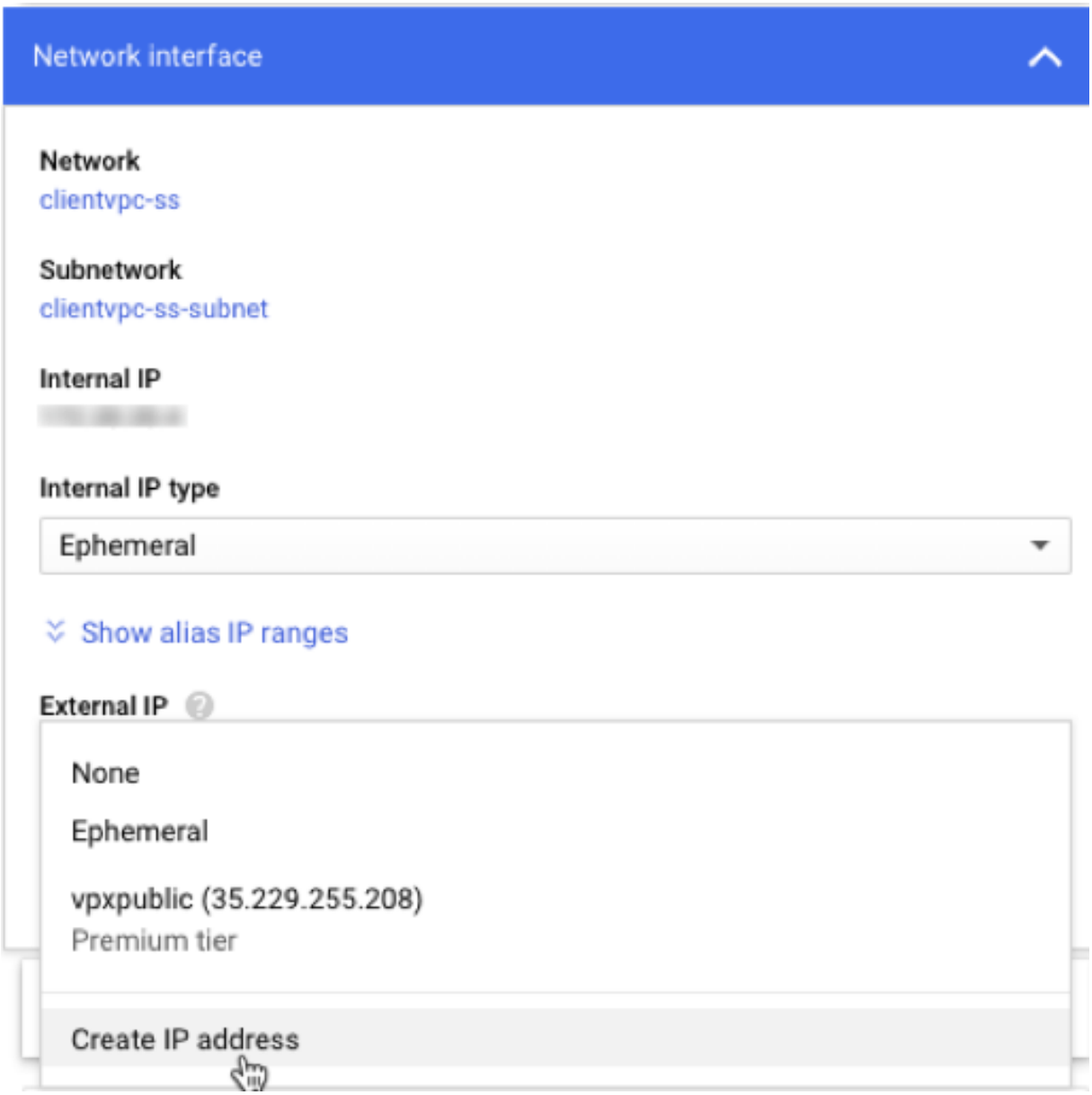
1. Inicie sesión en la **consola de Google > Redes > Red de VPC > Crear red de VPC**.
2. Complete los campos obligatorios y haga clic en **Crear**.

Para obtener más información, consulte la sección **Crear redes de VPC** en Implementación de una instancia Citrix ADC VPX en Google Cloud Platform.

Paso 2. Crear dos instancias VPX

Cree dos instancias VPX siguiendo los pasos indicados en Caso: implementar una instancia VPX independiente multi-NIC y Multi-IP.

> **Importante**
>
> Asigne una dirección IP externa estática a la dirección IP del cliente (VIP) del nodo principal. Puede utilizar una dirección IP reservada existente o crear una nueva. Para crear una dirección IP externa estática, vaya a **Interfaz de red > IP externa**y haga clic en **Crear dirección IP**.



Después de la conmutación por error, cuando el principal antiguo se convierte en el nuevo secundario, la dirección IP externa estática se mueve desde el primario antiguo y se adjunta al nuevo primario. Para obtener más información, consulta el documento de Google Cloud Reservar una dirección IP externa estática.

Después de configurar las instancias VPX, puede configurar las direcciones VIP y SNIP. Para obtener más información, consulte Configuración de direcciones IP propiedad de Citrix ADC.

Paso 3. Configurar alta disponibilidad

Después de crear las instancias en Google Cloud Platform, puede configurar HA mediante la GUI de Citrix ADC para CLI.

Configurar HA mediante la interfaz gráfica de usuario

Paso 1. Configure la alta disponibilidad en modo INC en ambas instancias.

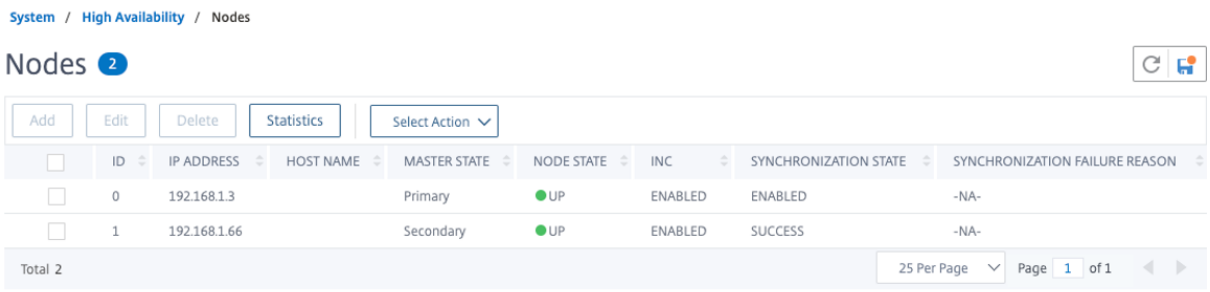
En el **nodo principal**, lleve a cabo los siguientes pasos:

1. Inicie sesión en la instancia con el nombre de usuario `nsroot` y el identificador de instancia del nodo desde la consola de GCP como contraseña.
2. Vaya a **Configuración > Sistema > Alta disponibilidad > Nodos** y haga clic en **Agregar**.
3. En el campo **Dirección IP del nodo remoto**, introduzca la dirección IP privada de la NIC de administración del nodo secundario.
4. Active la casilla **Activar el modo INC (Configuración de red independiente) en el autonodo** .
5. Haga clic en **Crear**.

En el **nodo secundario**, lleve a cabo los siguientes pasos:

1. Inicie sesión en la instancia con el nombre de usuario `nsroot` y el identificador de instancia del nodo desde la consola de GCP como contraseña.
2. Vaya a **Configuración > Sistema > Alta disponibilidad > Nodos** y haga clic en **Agregar**.
3. En el campo **Dirección IP de nodo remoto**, introduzca la dirección IP privada de la NIC de administración del nodo principal.
4. Active la casilla **Activar el modo INC (Configuración de red independiente) en el autonodo** .
5. Haga clic en **Crear**.

Antes de continuar, asegúrese de que el estado Sincronización del nodo secundario se muestre como **CORRECTO** en la página **Nodos** .



> **Nota**
>
> Ahora, el nodo secundario tiene las mismas credenciales de inicio de sesión que el nodo principal.

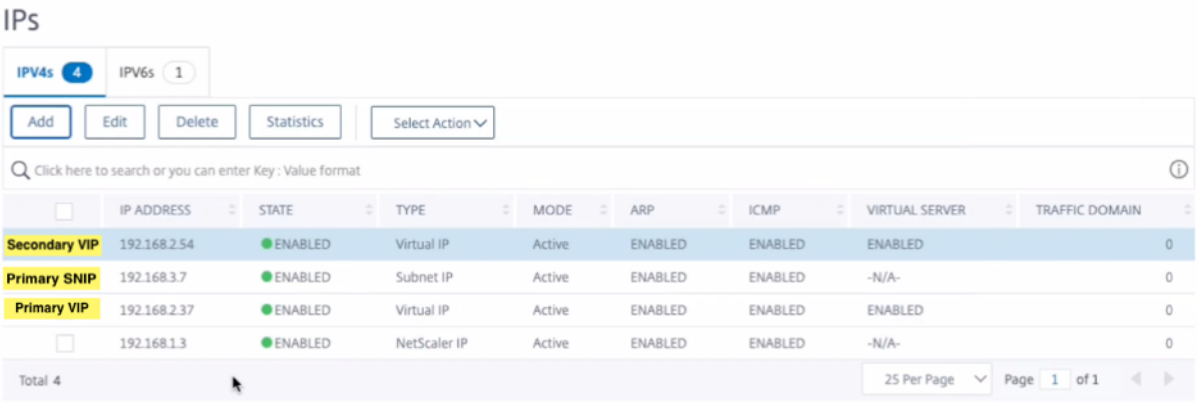
Paso 2. Agregue la dirección IP virtual y la dirección IP de subred en ambos nodos.

En el **nodo principal**, lleve a cabo los siguientes pasos:

1. Vaya a **Sistema > Red > IPs > IPv4s** y haga clic en **Agregar**.
2. Agregue una dirección VIP principal siguiendo estos pasos:

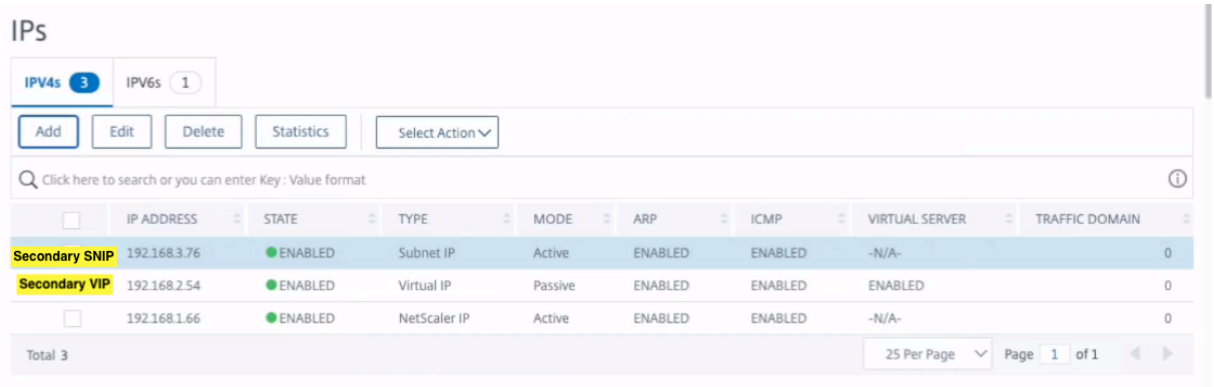
a) Introduzca la dirección IP interna de la interfaz orientada al cliente de la instancia principal y la máscara de red configurada para la subred cliente en la instancia de VM.
b) En el campo **Tipo de IP**, seleccione **IP virtual** en el menú desplegable.
c) Haga clic en **Crear**.

3. Agregue una dirección SNIP principal siguiendo estos pasos:
   a) Introduzca la dirección IP interna de la interfaz orientada al servidor de la instancia principal y la máscara de red configurada para la subred del servidor en la instancia principal.
   b) En el campo **Tipo de IP**, seleccione **IP de subred** en el menú desplegable.
   c) Haga clic en **Crear**.
4. Agregue una dirección VIP secundaria siguiendo estos pasos:
   a) Introduzca la dirección IP interna de la interfaz orientada al cliente de la instancia secundaria y la máscara de red configurada para la subred cliente en la instancia de VM.
   b) En el campo **Tipo de IP**, seleccione **IP virtual** en el menú desplegable.
   c) Haga clic en **Crear**.



En el **nodo secundario**, lleve a cabo los siguientes pasos:

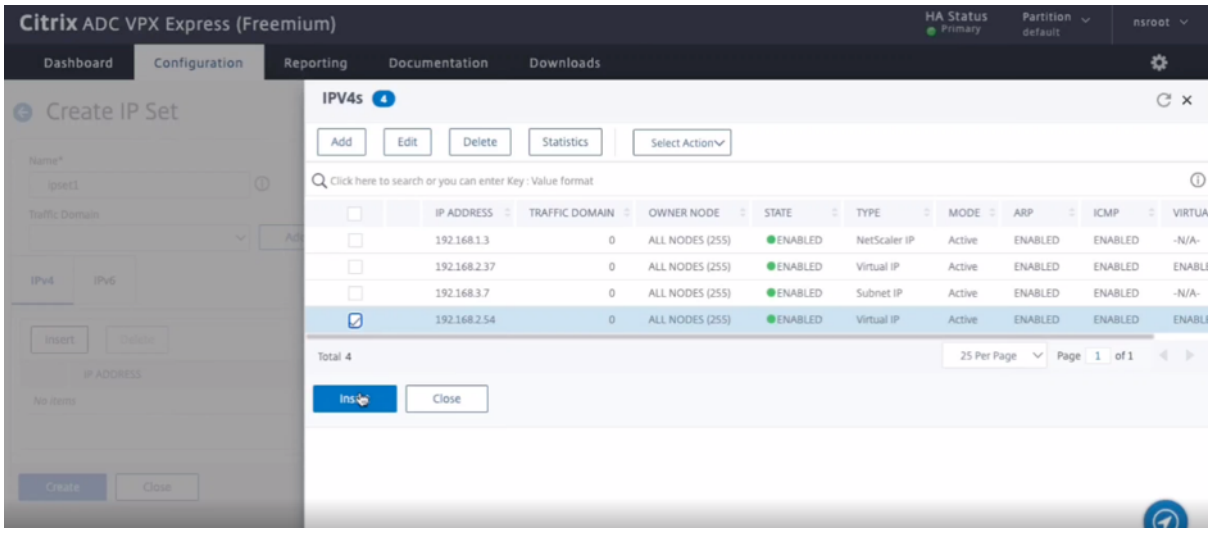
1. Vaya a **Sistema > Red > IPs > IPv4s** y haga clic en **Agregar**.
2. Agregue una dirección VIP secundaria siguiendo estos pasos:
   a) Introduzca la dirección IP interna de la interfaz orientada al cliente de la instancia secundaria y la máscara de red configurada para la subred cliente en la instancia de VM.
   b) En el campo **Tipo de IP**, seleccione **IP virtual** en el menú desplegable.
3. Agregue una dirección SNIP secundaria siguiendo estos pasos:
   a) Introduzca la dirección IP interna de la interfaz orientada al servidor de la instancia secundaria y la máscara de red configurada para la subred del servidor en la instancia secundaria.
   b) En el campo **Tipo de IP**, seleccione **IP de subred** en el menú desplegable.
   c) Haga clic en **Crear**.



Paso 3. Agregue un conjunto de IP y vincule el conjunto de IP al VIP secundario en ambas instancias.

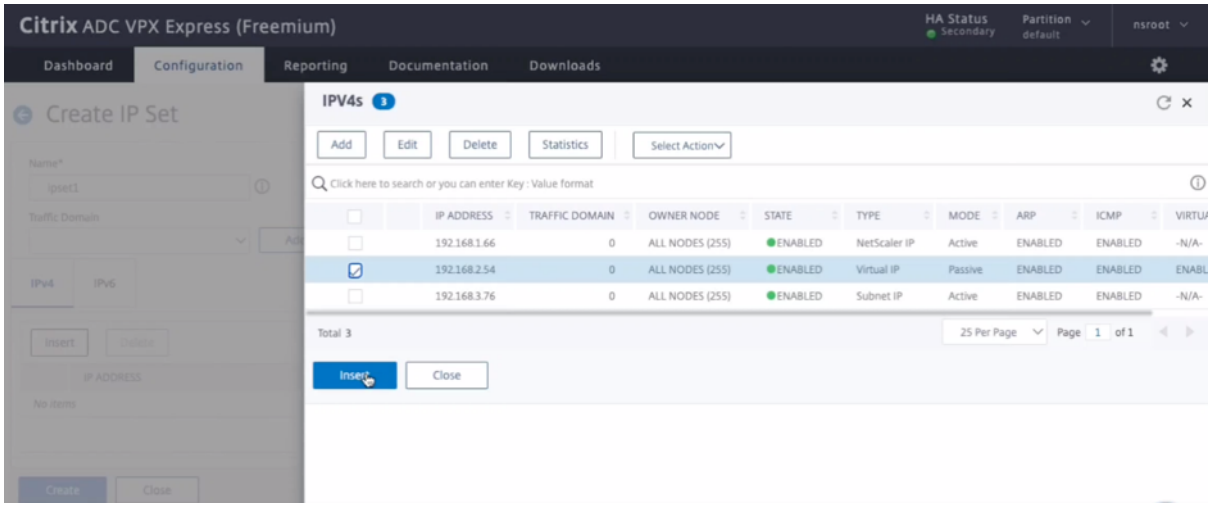
En el **nodo principal**, lleve a cabo los siguientes pasos:

1. Vaya a **Sistema > Red > Conjuntos de IP > Agregar**.
2. Agregue un nombre de conjunto de IP y haga clic en **Insertar**.
3. En la página **IPv4**, seleccione la IP virtual (VIP secundaria) y haga clic en **Insertar**.
4. Haga clic en **Crear** para crear el conjunto de IP.



En el **nodo secundario**, lleve a cabo los siguientes pasos:

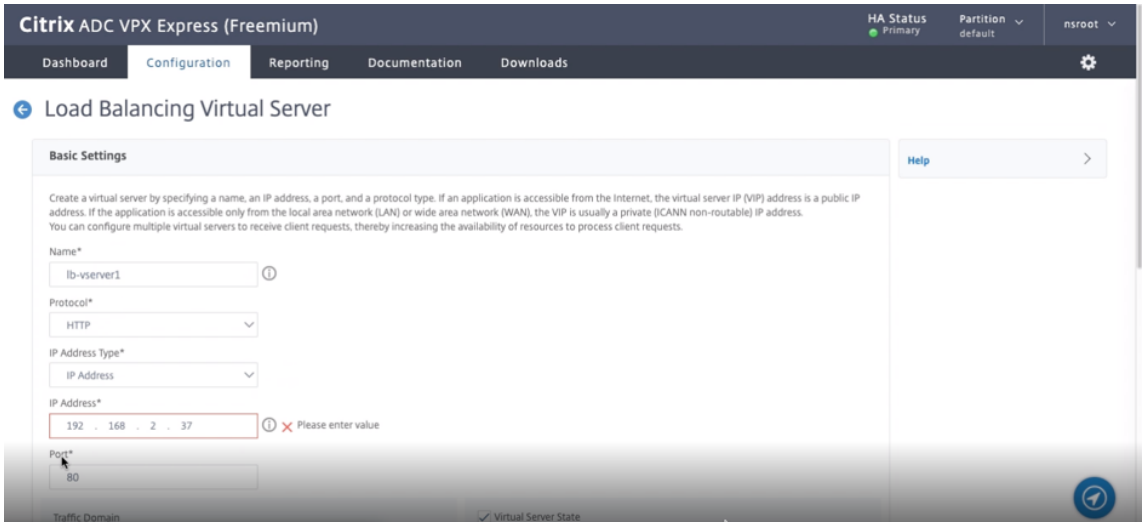
1. Vaya a **Sistema > Red > Conjuntos de IP > Agregar**.
2. Agregue un nombre de conjunto de IP y haga clic en **Insertar**.
3. En la página **IPv4**, seleccione la IP virtual (VIP secundaria) y haga clic en **Insertar**.
4. Haga clic en **Crear** para crear el conjunto de IP.



> **Nota**
>
> El nombre del conjunto de IP debe ser el mismo en ambas instancias.

Paso 4. Agregue un servidor virtual de equilibrio de carga en la instancia principal.

1. Vaya a **Configuración > Administración del tráfico > Equilibrio de carga > Servidores virtuales > Agregar**.
2. Agregue los valores necesarios para Nombre, Protocolo, Tipo de dirección IP (dirección IP), dirección IP (VIP principal) y Puerto.



3. Haga clic en **Más**. Vaya a **Configuración del conjunto de IP de rango IP**, seleccione **IPSet** en el menú desplegable y proporcione el IPset creado en el **paso 3**.
4. Haga clic en **Aceptar** para crear el servidor virtual de equilibrio de carga.

Paso 5. Agregue un servicio o grupo de servicios en el nodo principal.

1. Vaya a **Configuración > Administración del tráfico > Equilibrio de carga > Servicios > Agre-**

gar.

2. Agregue los valores necesarios para Nombre de servicio, Dirección IP, Protocolo y Puerto, y haga clic en **Aceptar**.

Paso 6. Vincule el servicio o grupo de servicios al servidor virtual de equilibrio de carga del nodo principal.

1. Vaya a **Configuración > Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. Seleccione el servidor virtual de equilibrio de carga configurado en el **paso 4**y haga clic en **Modificar**.
3. En la ficha **Grupos de servicios y servicios**, haga clic en **Enlace de servicio de servidor virtual sin equilibrio de carga**.
4. Seleccione el servicio configurado en el **paso 5**y haga clic en **Enlazar**.

Guarde la configuración. Después de una conmutación por error forzada, el secundario se convierte en el nuevo primario. La IP estática externa del antiguo VIP principal se traslada al nuevo VIP secundario.

Configurar la alta disponibilidad mediante CLI

Paso 1. Configure la alta disponibilidad en modo INC en ambas instancias.

En el nodo principal, escriba el siguiente comando.

```
add ha node 1 <sec_ip> -inc ENABLED
<!--NeedCopy-->
```

En el nodo secundario, escriba el siguiente comando.

```
add ha node 1 <prim_ip> -inc ENABLED
<!--NeedCopy-->
```

`sec_ip` hace referencia a la dirección IP interna de la NIC de administración del nodo secundario.

`prim_ip` hace referencia a la dirección IP interna de la NIC de administración del nodo principal.

Paso 2. Agregue IP virtuales y de subred en ambos nodos.

En el nodo principal, escriba el siguiente comando.


```
add ns ip <primary_vip> <subnet> -type VIP

add ns ip <secondary_vip> <subnet> -type VIP

add ns ip <primary_snip> <subnet> -type SNIP
<!--NeedCopy-->
```

primary_vip hace referencia a la dirección IP interna de la interfaz orientada al cliente de la instancia principal.

secondary_vip hace referencia a la dirección IP interna de la interfaz orientada al cliente de la instancia secundaria.

primary_snip hace referencia a la dirección IP interna de la interfaz orientada al servidor de la instancia principal.

En el nodo secundario, escriba el siguiente comando.

```
add ns ip <secondary_vip> <subnet> -type VIP

add ns ip <secondary_snip> <subnet> -type SNIP
<!--NeedCopy-->
```

secondary_vip hace referencia a la dirección IP interna de la interfaz orientada al cliente de la instancia secundaria.

secondary_snip hace referencia a la dirección IP interna de la interfaz orientada al servidor de la instancia secundaria.

Paso 3. Agregue un conjunto de IP y vincule el conjunto de IP a VIP secundario en ambas instancias.

En el nodo principal, escriba el siguiente comando:

```
add ipset <ipsetname>
bind ipset <ipsetname> <secondary VIP>
<!--NeedCopy-->
```

En el nodo secundario, escriba el siguiente comando:

```
add ipset <ipsetname>
bind ipset <ipsetname> <secondary VIP>
<!--NeedCopy-->
```


> **Nota**
>
> El nombre del conjunto de IP debe ser el mismo en ambas instancias.

Paso 4. Agregue un servidor virtual en la instancia principal.

Escriba el siguiente comando:

```
add <server_type> vserver <vserver_name> <protocol> <primary_vip> <port
    > -ipset <ipset_name>
<!--NeedCopy-->
```

Paso 5. Agregue un servicio o grupo de servicios en la instancia principal.

Escriba el siguiente comando:

```
add service <service_name> <service_ip_address> <protocol> <port>
<!--NeedCopy-->
```

Paso 6. Vincule el grupo de servicio/servicio al servidor virtual de equilibrio de carga de la instancia principal.

Escriba el siguiente comando:

```
bind <server_type> vserver <vserver_name> <service_name>
<!--NeedCopy-->
```

> *Nota*:
>
> Para guardar la configuración, escriba el comando `save config`. De lo contrario, las configuraciones se pierden después de reiniciar las instancias.

Paso 7. Verifique la configuración.

Asegúrese de que la dirección IP externa asociada a la NIC cliente principal se traslada a la secundaria en caso de failover.

1. Realice una solicitud cURL a la dirección IP externa y asegúrese de que se pueda acceder a ella.
2. En la instancia principal, realice la conmutación por error:

   Desde GUI, vaya a **Configuración > Sistema > Alta disponibilidad > Acción > Forzar conmutación por error**.

   En CLI, escriba el siguiente comando:


```
force ha failover -f
<!--NeedCopy-->
```

En la consola de GCP, vaya a la instancia secundaria. La dirección IP externa debe haberse trasladado a la NIC cliente o secundaria tras la conmutación por error.

3. Emita una solicitud cURL a la IP externa y asegúrese de que se pueda volver a acceder a ella.

Implementar un par VPX de alta disponibilidad con una dirección IP privada en Google Cloud Platform

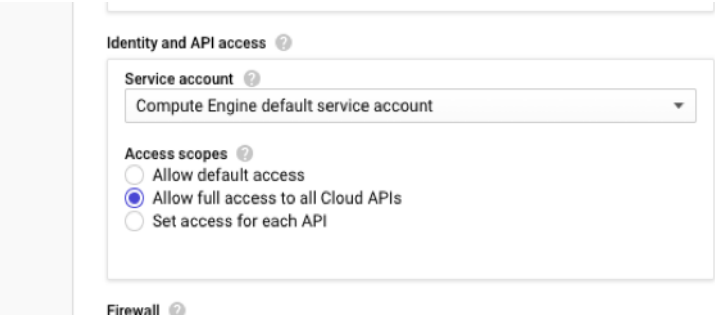
March 9, 2022

Puede implementar un par de alta disponibilidad VPX en GCP mediante una dirección IP privada. La IP del cliente (VIP) debe configurarse como dirección IP de alias en el nodo principal. Tras la conmutación por error, la dirección IP del cliente se mueve al nodo secundario para que el tráfico se reanude.

Para obtener más información sobre la alta disponibilidad, consulte Alta disponibilidad.

Antes de comenzar

- Lea las limitaciones, requisitos de hardware y puntos a tener en cuenta que se mencionan en Implementar una instancia Citrix ADC VPX en Google Cloud Platform. Esta información se aplica también a las implementaciones de alta disponibilidad.
- Habilite **Cloud Resource Manager API** para su proyecto GCP.
- Permite el acceso completo a todas las API de Cloud mientras creas las instancias.



- Asegúrese de que su cuenta de servicio de GCP tenga los siguientes permisos de IAM:

```
REQUIRED_INSTANCE_IAM_PERMS = [
```

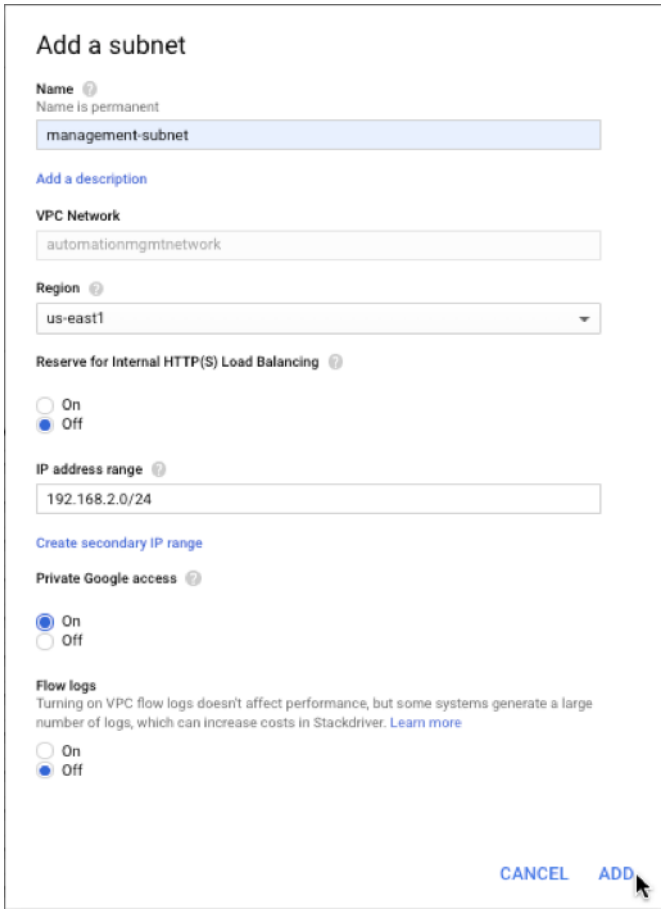


```
2  "compute.forwardingRules.list",
3  "compute.forwardingRules.setTarget",
4  "compute.instances.setMetadata",
5  "compute.instances.get",
6  "compute.instances.list",
7  "compute.instances.updateNetworkInterface",
8  "compute.targetInstances.list",
9  "compute.targetInstances.use",
10 "compute.targetInstances.create",
11 "compute.zones.list",
12 "compute.zoneOperations.get",
13 ]
14 <!--NeedCopy-->
```

- Si ha configurado direcciones IP externas en una interfaz distinta de la interfaz de administración, asegúrese de que su cuenta de servicio de GCP tenga los siguientes permisos de IAM adicionales:

```
1  REQUIRED_INSTANCE_IAM_PERMS = [
2  "compute.addresses.use"
3  "compute.instances.addAccessConfig",
4  "compute.instances.deleteAccessConfig",
5  "compute.networks.useExternalIp",
6  "compute.subnetworks.useExternalIp",
7  ]
8  <!--NeedCopy-->
```

- Si sus máquinas virtuales no tienen acceso a Internet, debe habilitar **Private Google Access** en la subred de administración.



- Si ha configurado reglas de reenvío de GCP en el nodo principal, lea las limitaciones y requisitos mencionados en Compatibilidad con reglas de reenvío para el par de alta disponibilidad VPX en GCP para actualizarlas a nuevo primario en caso de conmutación por error.

Cómo implementar un par de alta disponibilidad VPX en Google Cloud Platform

A continuación se presenta un resumen de los pasos de implementación de alta disponibilidad:

1. Cree redes de VPC en la misma región. Por ejemplo, Asia-este.
2. Crea dos instancias VPX (nodos primario y secundario) en la misma región. Pueden estar en la misma zona o en zonas diferentes. Por ejemplo, Asia east-1a y Asia East-IB.
3. Configure los ajustes de alta disponibilidad en ambas instancias mediante los comandos de la GUI de Citrix ADC o de la CLI de ADC.

Paso 1. Creación de redes de VPC

Cree redes de VPC en función de sus requisitos. Citrix recomienda crear tres redes de VPC para asociarse con NIC de administración, NIC cliente y NIC de servidor.

Para crear una red VPC, lleve a cabo estos pasos:

1. Inicie sesión en la **consola de Google > Redes > Red de VPC > Crear red de VPC**.
2. Complete los campos obligatorios y haga clic en **Crear**.

Para obtener más información, consulte la sección **Crear redes de VPC** en Implementación de una instancia Citrix ADC VPX en Google Cloud Platform.

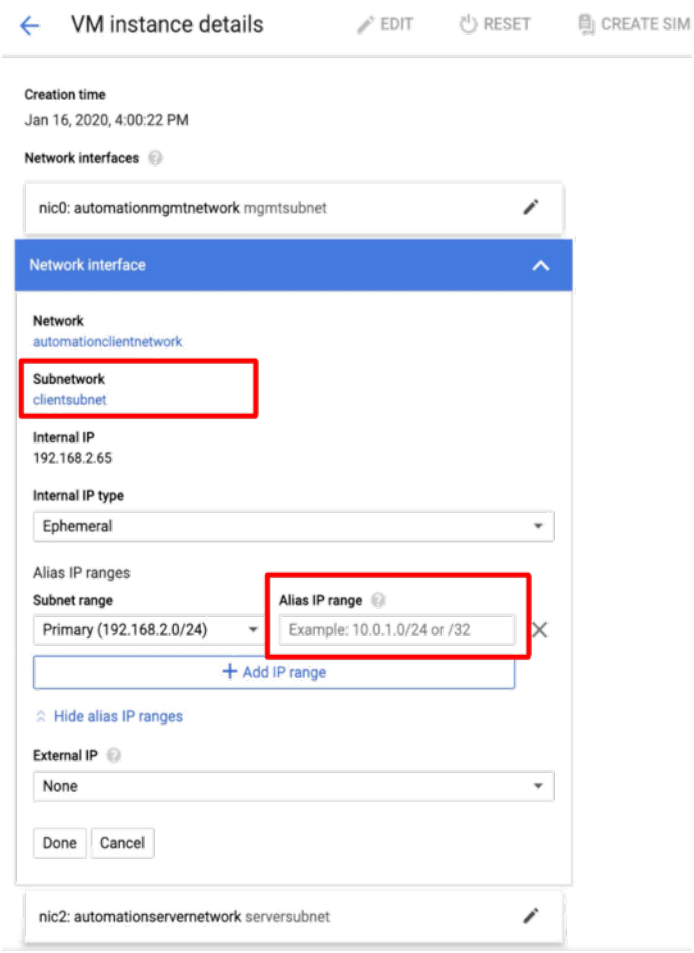
Paso 2. Crear dos instancias VPX

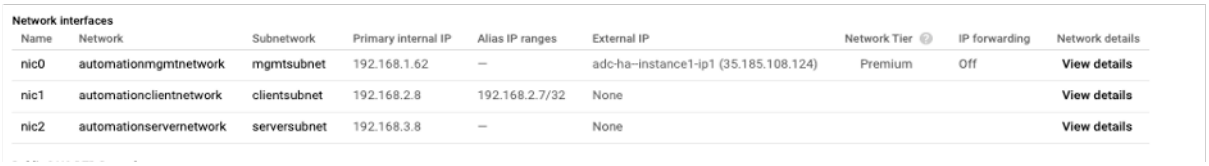
Cree dos instancias VPX siguiendo los pasos indicados en Caso: implementar una instancia VPX independiente multi-NIC y Multi-IP.

> **Importante:**
>
> Asigne una dirección IP de alias de cliente al nodo principal. No utilice la dirección IP interna de la instancia VPX para configurar el VIP.

Para crear una dirección IP de alias de cliente, realice estos pasos:

1. Vaya a la instancia de VM y haga clic en **Modificar**.
2. En la ventana **Interfaz de red**, modifique la interfaz del cliente.
3. En el campo **Intervalo de IP de alias**, introduzca la dirección IP del alias del cliente.





Network interfaces

Name	Network	Subnetwork	Primary internal IP	Alias IP ranges	External IP	Network Tier	IP forwarding	Network details
nic0	automationmgmtnetwork	mgmtsubnet	192.168.1.62	–	adc-ha--instance1-ip1 (35.185.108.124)	Premium	Off	View details
nic1	automationclientnetwork	clientsubnet	192.168.2.8	192.168.2.7/32	None			View details
nic2	automationservernetwork	serversubnet	192.168.3.8	–	None			View details

Después de la conmutación por error, cuando el primario anterior se convierte en el nuevo secundario, las direcciones IP de alias se mueven del principal anterior y se adjuntan al nuevo primario.

Después de configurar las instancias VPX, puede configurar las direcciones IP virtual (VIP) y de subred (SNIP). Para obtener más información, consulte Configuración de direcciones IP propiedad de Citrix ADC.

Paso 3. Configurar alta disponibilidad

Después de crear las instancias en Google Cloud Platform, puede configurar la alta disponibilidad mediante la GUI o CLI de Citrix ADC.

Configure la alta disponibilidad mediante la interfaz gráfica de usuario

Paso 1. Configure la alta disponibilidad en el modo Enabled INC en ambos nodos.

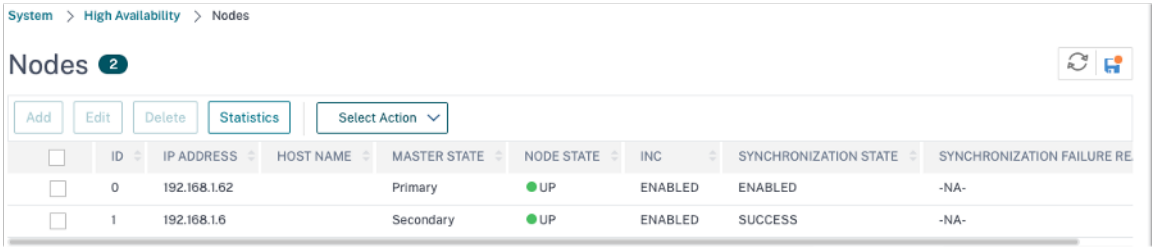
En el **nodo principal**, lleve a cabo los siguientes pasos:

1. Inicie sesión en la instancia con el nombre de usuario `nsroot` y el identificador de instancia del nodo desde la consola de GCP como contraseña.
2. Vaya a **Configuración > Sistema > Alta disponibilidad > Nodos** y haga clic en **Agregar**.
3. En el campo **Dirección IP del nodo remoto**, introduzca la dirección IP privada de la NIC de administración del nodo secundario.
4. Marque la casilla **Activar el modo INC (Configuración de red independiente) en el autonodo**.
5. Haga clic en **Create**.

En el **nodo secundario**, lleve a cabo los siguientes pasos:

1. Inicie sesión en la instancia con el nombre de usuario `nsroot` y el identificador de instancia del nodo desde la consola de GCP como contraseña.
2. Vaya a **Configuración > Sistema > Alta disponibilidad > Nodos** y haga clic en **Agregar**.
3. En el campo **Dirección IP de nodo remoto**, introduzca la dirección IP privada de la NIC de administración del nodo principal.
4. Marque la casilla **Activar el modo INC (Configuración de red independiente) en el autonodo**.
5. Haga clic en **Create**.

Antes de continuar, asegúrese de que el estado Sincronización del nodo secundario se muestre como **CORRECTO** en la página **Nodos**.



> **Nota**
>
> Ahora, el nodo secundario tiene las mismas credenciales de inicio de sesión que el nodo principal.

Paso 2. Agregue la dirección IP virtual y la dirección IP de subred en ambos nodos.

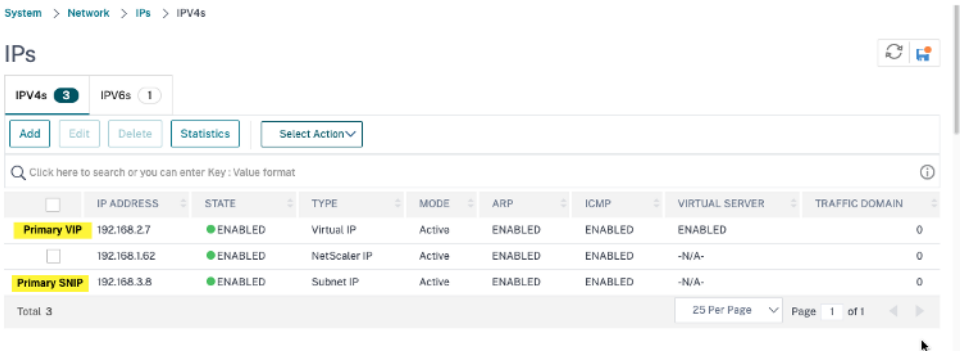
En el nodo principal, lleve a cabo los siguientes pasos:

1. Vaya a **Sistema > Red > IPs > IPv4s** y haga clic en **Agregar**.
2. Para crear una dirección IP (VIP) de alias de cliente:
   a) Introduzca la dirección IP del alias y la máscara de red configuradas para la subred del cliente en la instancia de VM.

b) En el campo **Tipo de IP**, seleccione **IP virtual** en el menú desplegable.
c) Haga clic en **Create**.

3. Para crear una dirección IP del servidor (SNIP):

a) Introduzca la dirección IP interna de la interfaz orientada al servidor de la instancia principal y la máscara de red configurada para la subred del servidor.
b) En el campo **Tipo de IP**, seleccione **IP de subred** en el menú desplegable.
c) Haga clic en **Create**.



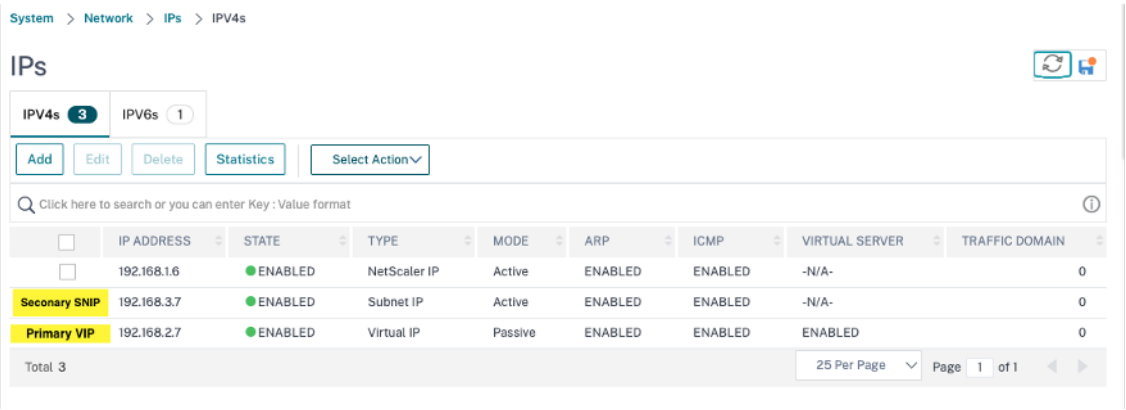
En el nodo secundario, lleve a cabo los siguientes pasos:

1. Vaya a **Sistema > Red > IPs > IPv4s** y haga clic en **Agregar**.
2. Para crear una dirección IP (VIP) de alias de cliente:

a) Introduzca la dirección IP de alias y la máscara de red configuradas para la subred cliente en la instancia principal de VM.
b) En el campo **Tipo de IP**, seleccione **IP de subred** en el menú desplegable.
c) Haga clic en **Create**.

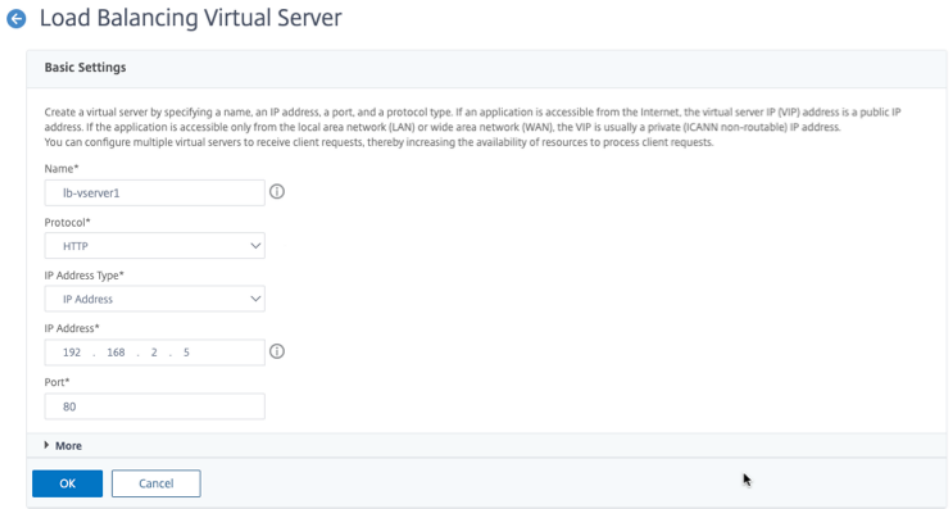
3. Para crear una dirección IP del servidor (SNIP):

a) Introduzca la dirección IP interna de la interfaz orientada al servidor de la instancia secundaria y la máscara de red configurada para la subred del servidor.
b) En el campo **Tipo de IP**, seleccione **IP de subred** en el menú desplegable.
c) Haga clic en **Create**.



Paso 3. Agregue un servidor virtual de equilibrio de carga en el nodo principal.

1. Vaya a **Configuración > Administración del tráfico > Equilibrio de carga > Servidores virtuales > Agregar**.
2. Agregue los valores necesarios para Nombre, Protocolo, Tipo de dirección IP (dirección IP), Dirección IP (dirección IP del alias del cliente principal) y Puerto, y haga clic en **Aceptar**.



Paso 4. Agregue un servicio o grupo de servicios en el nodo principal.

1. Vaya a **Configuración > Administración del tráfico > Equilibrio de carga > Servicios > Agregar**.
2. Agregue los valores necesarios para Nombre de servicio, Dirección IP, Protocolo y Puerto, y haga clic en **Aceptar**.

Paso 5. Vincule el servicio o grupo de servicios al servidor virtual de equilibrio de carga del nodo principal.

1. Vaya a **Configuración > Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. Seleccione el servidor virtual de equilibrio de carga configurado en el **paso 3**y haga clic en **Modificar**.
3. En la ficha **Grupos de servicios y servicios**, haga clic en **Enlace de servicio de servidor virtual sin equilibrio de carga**.
4. Seleccione el servicio configurado en el **paso 4**y haga clic en **Enlazar**.

Paso 5. Guarde la configuración.

Después de una conmutación por error forzada, el secundario se convierte en el nuevo primario. La IP del alias de cliente (VIP) y la IP del alias del servidor (SNIP) de la antigua primaria se trasladan al nuevo principal.

Configurar la alta disponibilidad mediante la CLI

Paso 1. Configure la alta disponibilidad en modo **habilitado para INC** en ambas instancias mediante la CLI de Citrix ADC.

En el nodo principal, escriba el siguiente comando.

```
add ha node 1 <sec_ip> -inc ENABLED
<!--NeedCopy-->
```

En el nodo secundario, escriba el siguiente comando.

```
add ha node 1 <prim_ip> -inc ENABLED
<!--NeedCopy-->
```

`sec_ip` hace referencia a la dirección IP interna de la NIC de administración del nodo secundario.

`prim_ip` hace referencia a la dirección IP interna de la NIC de administración del nodo principal.

Paso 2. Agrega VIP y SNIP en ambos nodos.

Escriba los siguientes comandos en el nodo principal:

```
add ns ip <primary_client_alias_ip> <subnet> -type VIP

<!--NeedCopy-->
```

> **Nota:**
>
> Introduzca la dirección IP del alias y la máscara de red configuradas para la subred del cliente en la instancia de VM.

```
add ns ip <primary_snip> <subnet> -type SNIP
<!--NeedCopy-->
```

`primary_snip` hace referencia a la dirección IP interna de la interfaz orientada al servidor de la instancia principal.

Escriba los siguientes comandos en el nodo secundario:


```
add ns ip <primary_client_alias_ip> <subnet> -type VIP
<!--NeedCopy-->
```

> Nota
>
> Introduzca la dirección IP de alias y la máscara de red configuradas para la subred cliente en la instancia principal de VM.

```
add ns ip <secondary_snip> <subnet> -type SNIP
<!--NeedCopy-->
```

`secondary_snip` hace referencia a la dirección IP interna de la interfaz orientada al servidor de la instancia secundaria.

> **Nota:**
>
> Introduzca la dirección IP y la máscara de red configuradas para la subred del servidor en la instancia de VM.

Paso 3. Agregue un servidor virtual en el nodo principal.

Escriba el siguiente comando:

```
add <server_type> vserver <vserver_name> <protocol> <
   primary_client_alias_ip> <port>
<!--NeedCopy-->
```

Paso 4. Agregue un servicio o grupo de servicios en el nodo principal.

Escriba el siguiente comando:

```
add service <service_name> <service_ip_address> <protocol> <port>
<!--NeedCopy-->
```

Paso 5. Vincule el servicio o grupo de servicios al servidor virtual de equilibrio de carga del nodo principal.

Escriba el siguiente comando:

```
bind <server_type> vserver <vserver_name> <service_name>
<!--NeedCopy-->
```


> **Nota:**
>
> Para guardar la configuración, escriba el comando `save config`. De lo contrario, las configuraciones se pierden después de reiniciar las instancias.

Agregar servicio de escalado automático GCP back-end

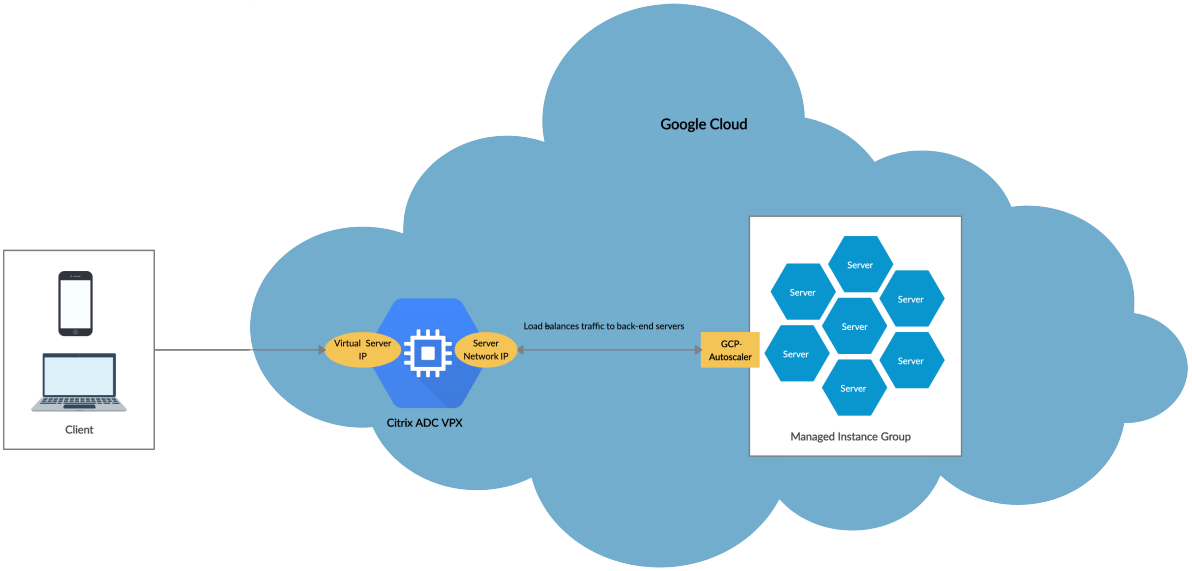
August 20, 2021

El alojamiento eficiente de las aplicaciones en una nube requiere una gestión fácil y rentable de los recursos, en función de la demanda de las aplicaciones. Para satisfacer la creciente demanda, debe escalar los recursos de red hacia arriba. Cuando la demanda disminuye, es necesario reducir la escala para evitar el coste innecesario de los recursos infrautilizados. Para minimizar el coste de ejecutar la aplicación, debe supervisar constantemente el tráfico, la memoria y el uso de la CPU, y así sucesivamente. Sin embargo, supervisar el tráfico manualmente es engorroso. Para que el entorno de aplicaciones se amplíe o disminuya dinámicamente, debe automatizar los procesos de supervisión del tráfico y de ampliación de los recursos siempre que sea necesario.

Integrada con el servicio GCP Autoscaling, la instancia de Citrix ADC VPX ofrece las siguientes ventajas:

- **Equilibrio de carga y administración**: Configura automáticamente los servidores para escalarlos y reducirlos, en función de la demanda. La instancia de VPX detecta automáticamente los grupos de instancias administradas en la subred back-end y permite seleccionar los grupos de instancias administradas para equilibrar la carga. Las direcciones IP virtuales y de subred se configuran automáticamente en la instancia de VPX.
- **Alta disponibilidad**: Detecta grupos de instancias administradas que abarcan varias zonas y servidores de equilibrio de carga.
- **Mejor disponibilidad de red**: La instancia VPX admite:
  - Servidores back-end en los mismos grupos de ubicación
  - Servidores back-end en diferentes zonas

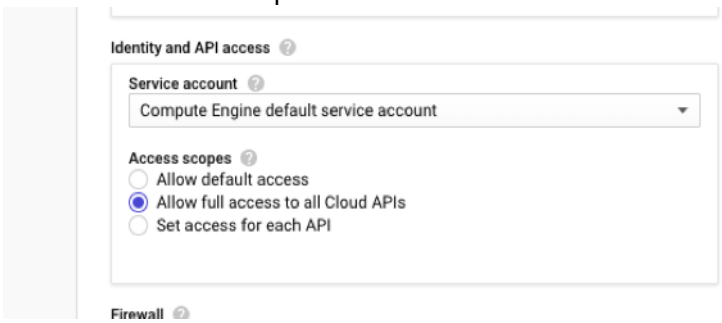
Este diagrama ilustra cómo funciona el servicio GCP Autoscaling en una instancia de Citrix ADC VPX que actúa como servidor virtual de equilibrio de carga.



Antes de comenzar

Antes de empezar a utilizar el escalado automático con su instancia de Citrix ADC VPX, debe realizar las siguientes tareas.

- Cree una instancia de Citrix ADC VPX en GCP según sus necesidades.
  - Para obtener más información sobre cómo crear una instancia VPX de Citrix ADC, consulte Implementación de una instancia Citrix ADC VPX en Google Cloud Platform.
  - Para obtener más información sobre cómo implementar instancias VPX en modo HA, consulta Implementar un par de alta disponibilidad VPX en Google Cloud Platform.
- Habilite **Cloud Resource Manager API** para su proyecto GCP.
- Permite el acceso completo a todas las API de Cloud mientras creas las instancias.



- Asegúrese de que su cuenta de servicio GCP tenga los siguientes permisos de IAM:

```
REQUIRED_INSTANCE_IAM_PERMS = [

```



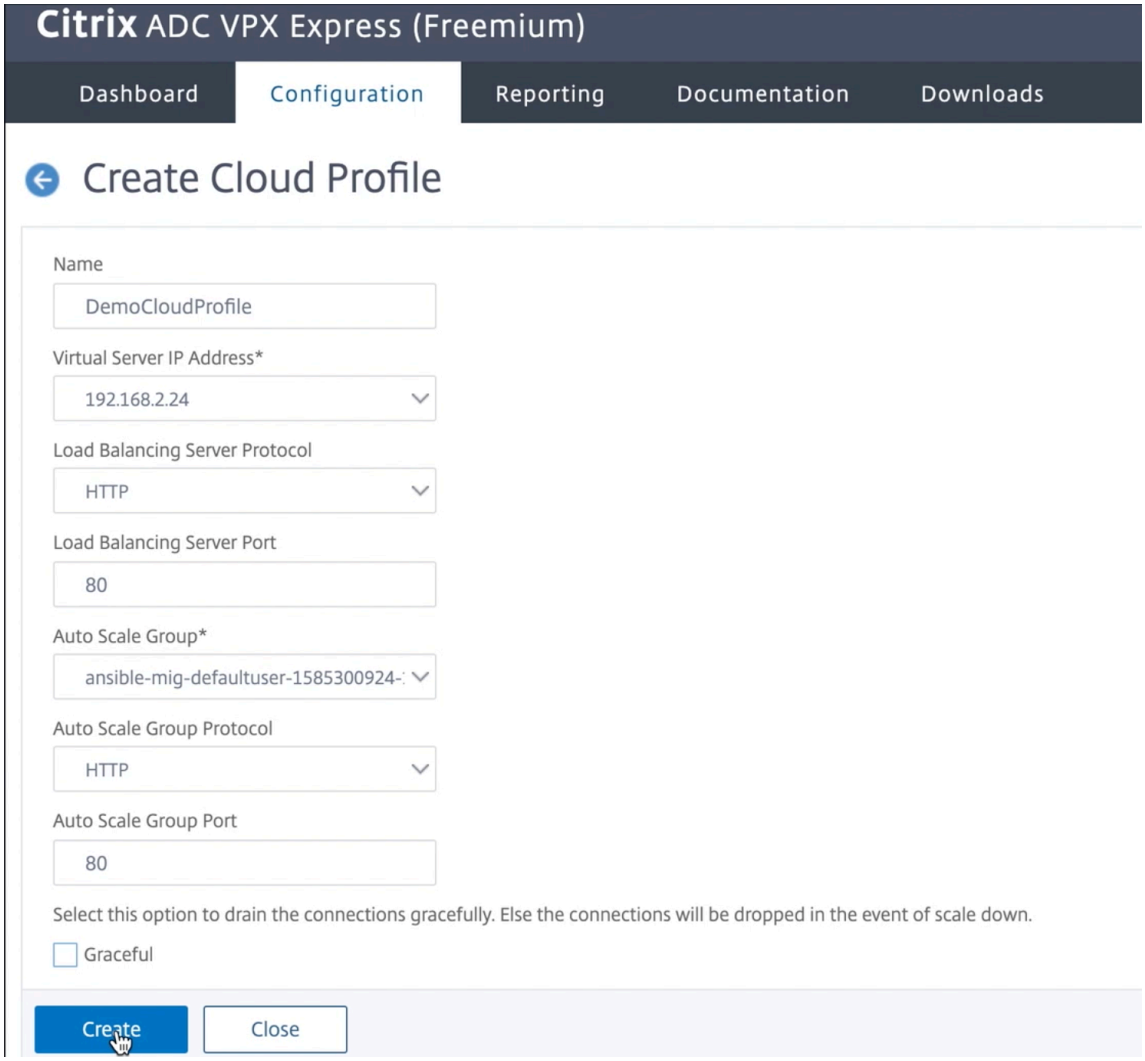
```
3   "compute.instances.get",
4   "compute.zones.list",
5   "compute.instanceGroupManagers.list",
6   "compute.instanceGroupManagers.get"
7   ]
8   <!--NeedCopy-->
```

- Para configurar el escalado automático, asegúrese de que esté configurado lo siguiente:
  - Plantilla instancia
  - Grupo de instancias administradas
  - Directiva de escalado automático

Agregar el servicio GCP Autoscaling a una instancia de Citrix ADC VPX

Puede agregar el servicio Autoscaling a una instancia VPX con un solo clic mediante la GUI. Complete estos pasos para agregar el servicio Autoscaling a la instancia de VPX:

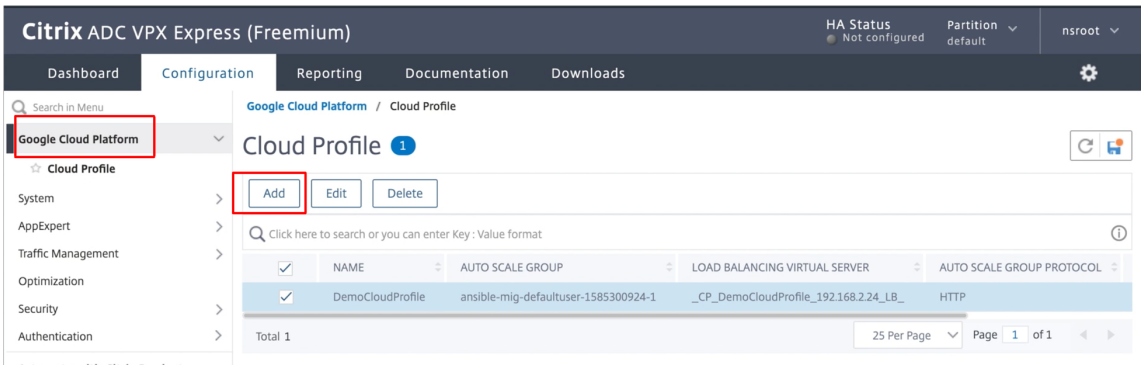
1. Inicie sesión en la instancia de VPX mediante sus credenciales para `nsroot`.
2. Cuando inicia sesión en la instancia de Citrix ADC VPX por primera vez, verá la página de perfil de nube predeterminada. Seleccione el grupo de instancias administradas de GCP en el menú desplegable y haga clic en **Crear** para crear un perfil de nube.



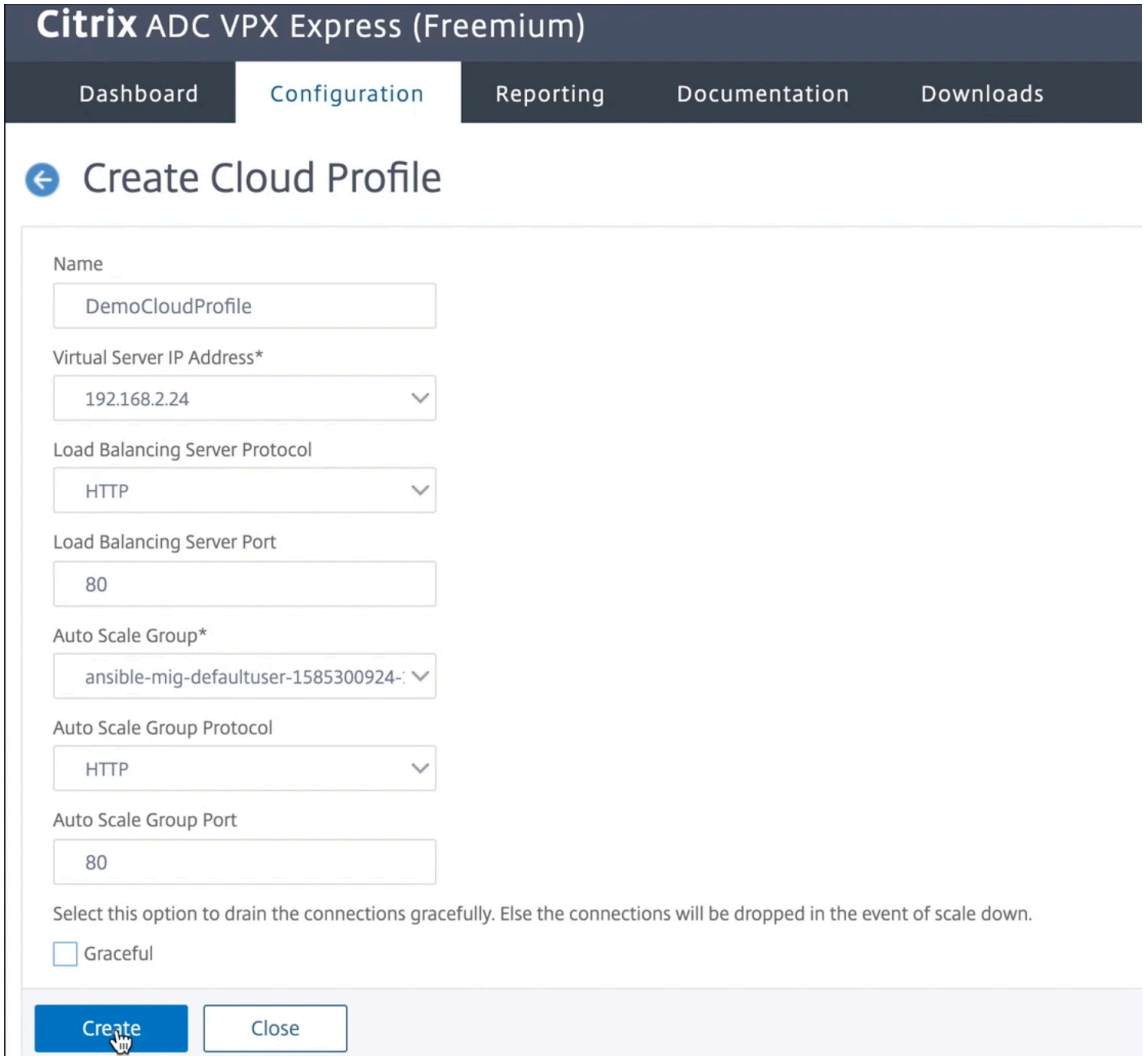
- El campo **Dirección IP del servidor virtual** se rellena automáticamente a partir de todas las direcciones IP asociadas a las instancias.
- El **grupo de escalabilidad automática** se rellena previamente desde el grupo de instancias administrado configurado en su cuenta de GCP.
- Al seleccionar el **Protocolo de grupo de escala automática** y el **puerto de grupo de escala automática**, asegúrese de que los servidores escuchan en el protocolo y los puertos configurados. Enlazar el monitor correcto en el grupo de servicios. De forma predeterminada, se utiliza el monitor TCP.
- Desactive la casilla **Graceful** porque no es compatible.

> Nota:
>
> Para el tipo de protocolo SSL Autoscaling, después de crear el perfil de nube, el servidor virtual de equilibrio de carga o el grupo de servicios está inactivo debido a que falta un certificado. Puede enlazar el certificado al servidor virtual o grupo de servicios manualmente.

3. Después del inicio de sesión por primera vez si quieres crear Cloud Profile, en la GUI ve a **Sistema > Google Cloud Platform > Cloud Profile** y haga clic en **Agregar**.

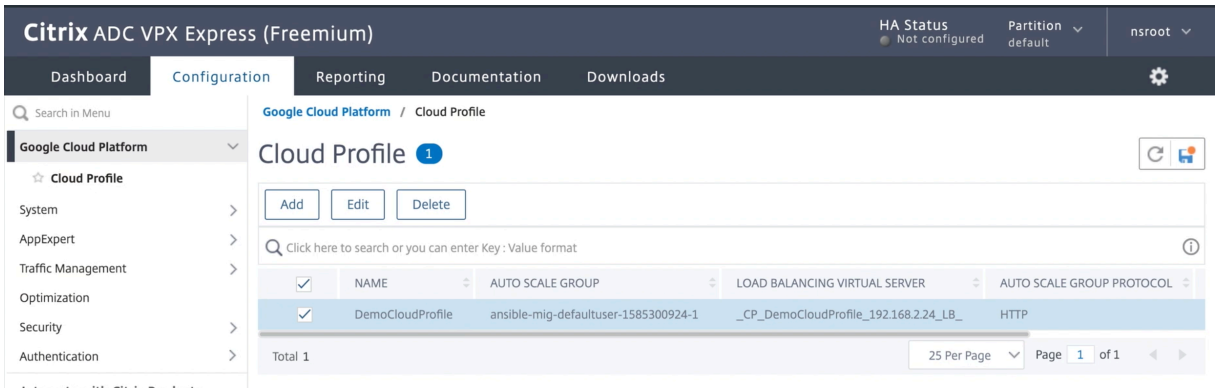


Aparecerá la página **de configuración Crear perfil de nube**.



Cloud Profile crea un servidor virtual de equilibrio de carga de Citrix ADC y un grupo de servicios con miembros como servidores del grupo de instancias administradas. Los servidores back-end

deben ser accesibles a través del SNIP configurado en la instancia VPX.



Compatibilidad con escalado VIP para la instancia Citrix ADC VPX en GCP

October 5, 2021

Un dispositivo Citrix ADC reside entre los clientes y los servidores, de modo que las solicitudes de los clientes y las respuestas del servidor pasan por él. En una instalación típica, los servidores virtuales configurados en el dispositivo proporcionan puntos de conexión que los clientes utilizan para acceder a las aplicaciones que hay detrás del dispositivo. El número de direcciones IP virtuales públicas (VIP) necesarias para una implementación varía según el caso.

La arquitectura de GCP restringe que cada interfaz de la instancia se conecte a una VPC diferente. Una VPC en GCP es un conjunto de subredes y cada subred puede extenderse por zonas de una región. Además, GCP impone la siguiente limitación:

- Hay una asignación 1:1 del número de direcciones IP públicas al número de NIC. Solo se puede asignar una dirección IP pública a una NIC.
- Se pueden conectar un máximo de 8 NIC en un tipo de instancia de mayor capacidad.

Por ejemplo, una instancia n1-standard 2 solo puede tener 2 NIC, y las VIP públicas que se pueden agregar están limitadas a 2. Para obtener más información, consulte Cuotas de recursos de VPC.

Para lograr escalas más altas de direcciones IP virtuales públicas en una instancia de Citrix ADC VPX, puede configurar las direcciones VIP como parte de los metadatos de la instancia. La instancia VPX de ADC utiliza internamente reglas de reenvío proporcionadas por el GCP para lograr el escalado VIP. La instancia VPX de ADC también proporciona alta disponibilidad para los VIP configurados.
Después de configurar las direcciones VIP como parte de los metadatos, puede configurar un servidor virtual LB mediante la misma IP que se utiliza para crear las reglas de reenvío. Por lo tanto, podemos usar reglas de reenvío para mitigar las limitaciones que tenemos la escala w.r.t en el uso de direcciones VIP públicas en una instancia ADC VPX en GCP.

Para obtener más información sobre las reglas de reenvío, consulte Descripción general de las reglas de reenvío.

Para obtener más información sobre HA, consulte Alta disponibilidad.

Puntos a tener en cuenta

- Google cobra un coste adicional por cada regla de reenvío de IP virtual. El coste real depende del número de entradas creadas. El coste asociado se encuentra en los documentos de precios de Google.
- Las reglas de reenvío solo se aplican a los VIP públicos. Puede utilizar direcciones IP de alias cuando la implementación necesite direcciones IP privadas como VIP.
- Puede crear reglas de reenvío solo para los protocolos, que necesitan el servidor virtual LB. Los VIP se pueden crear, actualizar o eliminar sobre la marcha. También puede agregar un nuevo servidor virtual de equilibrio de carga con la misma dirección VIP pero con un protocolo diferente.

Antes de comenzar

- La instancia Citrix ADC VPX debe implementarse en GCP.
- La dirección IP externa debe estar reservada. Para obtener más información, consulte Reserva de una dirección IP externa estática.
- Asegúrese de que su cuenta de servicio de GCP tenga los siguientes permisos de IAM:

```
REQUIRED_IAM_PERMS = [
”compute.addresses.list”,
”compute.addresses.get”,
”compute.addresses.use”,
”compute.forwardingRules.create”,
”compute.forwardingRules.delete”,
”compute.forwardingRules.get”,
”compute.forwardingRules.list”,
”compute.instances.use”,
”compute.subnetworks.use”,
”compute.targetInstances.create”
”compute.targetInstances.get”
”compute.targetInstances.use”,
]

<!--NeedCopy-->
```


- Habilite **Cloud Resource Manager API** para su proyecto GCP.
- Si utilizas el escalado VIP en una instancia VPX independiente, asegúrate de que su cuenta de servicio de GCP tenga los siguientes permisos de IAM:

```
REQUIRED_IAM_PERMS = [
”compute.addresses.list”,
”compute.addresses.get”,
”compute.addresses.use”,
”compute.forwardingRules.create”,
”compute.forwardingRules.delete”,
”compute.forwardingRules.get”,
”compute.forwardingRules.list”,
”compute.instances.use”,
”compute.subnetworks.use”,
”compute.targetInstances.create”,
”compute.targetInstances.list”,
”compute.targetInstances.use”,
]
<!--NeedCopy-->
```

- Si utilizas el escalado VIP en un modo de alta disponibilidad, asegúrate de que su cuenta de servicio de GCP tenga los siguientes permisos de IAM:

```
REQUIRED_IAM_PERMS = [
”compute.addresses.get”,
”compute.addresses.list”,
”compute.addresses.use”,
”compute.forwardingRules.create”,
”compute.forwardingRules.delete”,
”compute.forwardingRules.get”,
”compute.forwardingRules.list”,
”compute.forwardingRules.setTarget”,
”compute.instances.use”,
”compute.instances.get”,
”compute.instances.list”,
”compute.instances.setMetadata”,
”compute.subnetworks.use”,
”compute.targetInstances.create”,
”compute.targetInstances.list”,
”compute.targetInstances.use”,
”compute.zones.list”,
```



```
19   ]
20   <!--NeedCopy-->
```

> Nota:
>
> En un modo de alta disponibilidad, si su cuenta de servicio no tiene funciones de propietario o editor, debe agregar la **función Usuario de cuenta de servicio** a su cuenta de servicio.

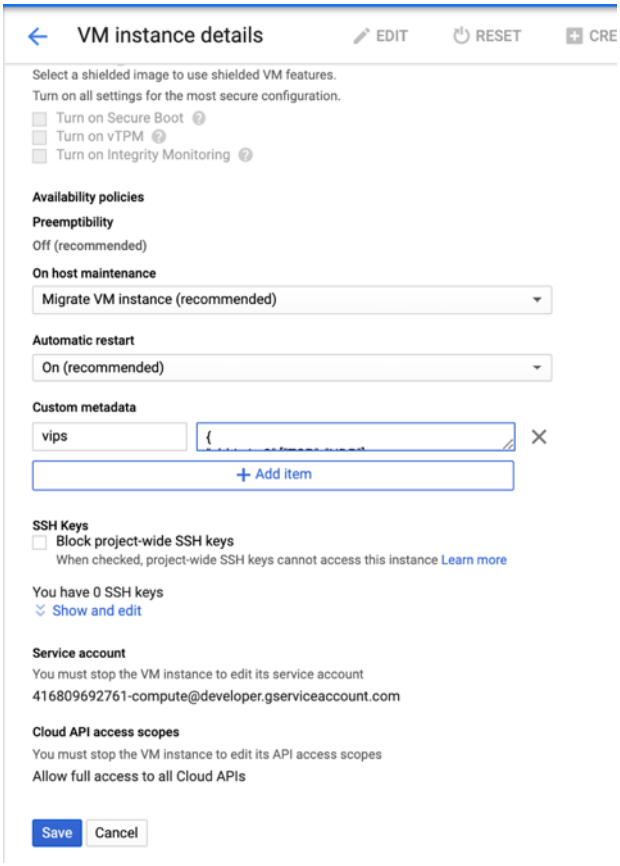
Configurar direcciones IP externas para escalado de VIP en la instancia de Citrix ADC VPX

1. En Google Cloud Console, vaya a la página **Instancias de VM** .
2. Crea una nueva instancia de VM o usa una instancia existente.
3. Haga clic en el nombre de la instancia. En la página de **detalles de la instancia de VM**, haga clic en **Modificar**.
4. Actualice los **metadatos personalizados** introduciendo lo siguiente:
   - Clave = vips
   - Valor = Proporcionar un valor en el siguiente formato JSON:

     {
     “Nombre de la IP reservada externa”: [lista de protocolos],
     }

   GCP admite los siguientes protocolos:

   - AH
   - ESP
   - ICMP
   - SCT
   - TCP
   - UDP



Para obtener más información, consulte Metadatos personalizados.

Ejemplo de metadatos personalizados:

{
“external-ip1-name”:[“TCP”, “UDP”],
“external-ip2-name”:[“ICMP”, “AH”]
}

En este ejemplo, la instancia VPX de ADC crea internamente una regla de reenvío para cada par IP y protocolo. Las entradas de metadatos se asignan a las reglas de reenvío. Este ejemplo le ayuda a comprender cuántas reglas de reenvío se crean para una entrada de metadatos.

Se crean cuatro reglas de reenvío de la siguiente manera:

a) external-ip1-name y TCP
b) external-ip1-name y UDP
c) external-ip2-name e ICMP
d) external-ip2-name y AH

> Nota:
>
> En el modo HA, debes agregar metadatos personalizados solo en la instancia principal. En

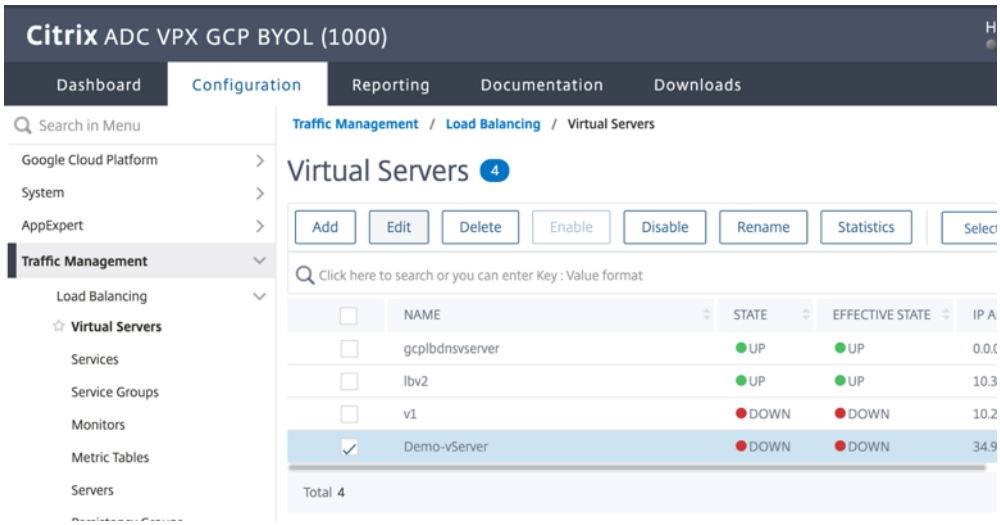
> caso de conmutación por error, los metadatos personalizados se sincronizan con el nuevo principal.

5. Haga clic en **Guardar**.

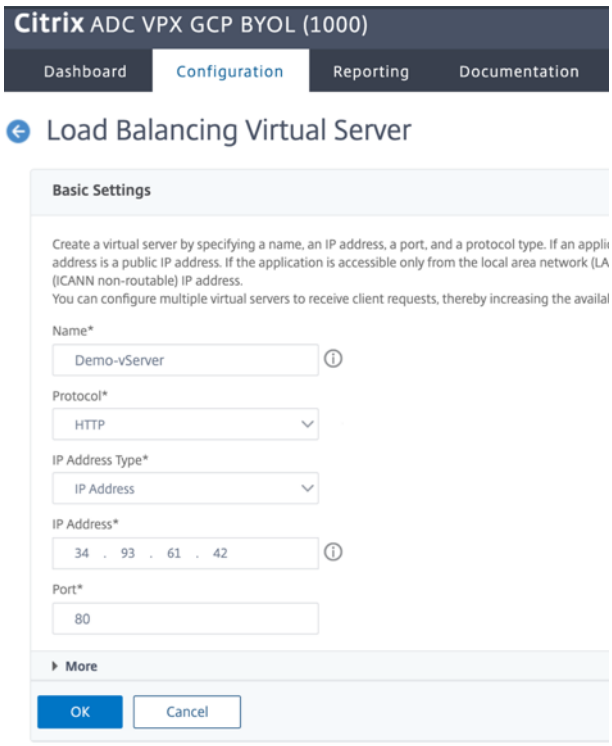
Configuración de un servidor virtual de equilibrio de carga con dirección IP externa en una instancia de Citrix ADC VPX

Paso 1. Agregue un servidor virtual de equilibrio de carga.

1. Vaya a **Configuración > Administración del tráfico > Equilibrio de carga > Servidores virtuales > Agregar**.

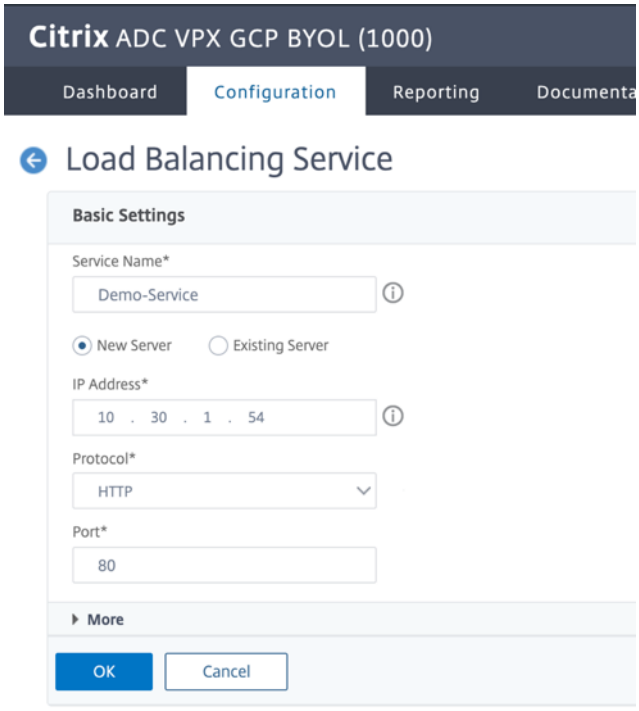


2. Agregue los valores necesarios para Nombre, Protocolo, Tipo de dirección IP (dirección IP), Dirección IP (dirección IP externa de la regla de reenvío que se agrega como VIP en ADC) y Puerto y haga clic en **Aceptar**.



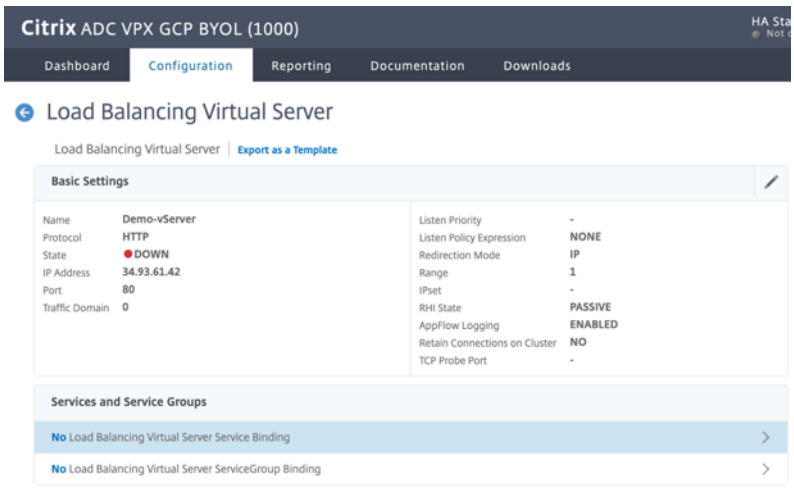
Paso 2. Agregue un servicio o grupo de servicios.

1. Vaya a **Configuración > Administración del tráfico > Equilibrio de carga > Servicios > Agregar**.
2. Agregue los valores necesarios para Nombre de servicio, Dirección IP, Protocolo y Puerto, y haga clic en **Aceptar**.

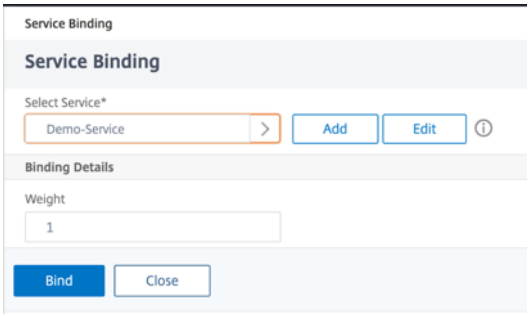


Paso 3. Enlazar el servicio o el grupo de servicios al servidor virtual de equilibrio de carga.

1. Vaya a **Configuración > Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. Seleccione el servidor virtual de equilibrio de carga configurado en el **paso 1**y haga clic en **Modificar**.
3. En la página **Grupos de servicios y servicios**, haga clic en **Sin enlace de servicio de servidor virtual de equilibrio de carga**.



4. Seleccione el servicio configurado en el **paso 3**y haga clic en **Enlazar**.



5. Guarde la configuración.

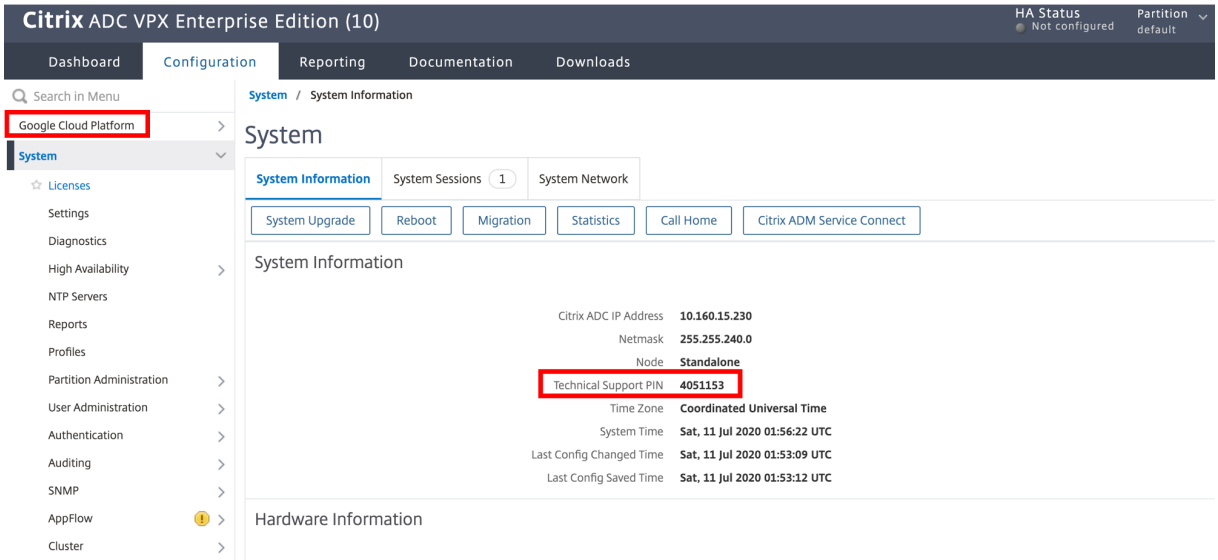
Solucionar problemas de una instancia de VPX en GCP

August 20, 2021

Google Cloud Platform (GCP) proporciona acceso de consola a una instancia de Citrix ADC VPX. Solo puede depurar si la red está conectada. Para ver el registro del sistema de una instancia, acceda a la consola y compruebe **los archivos del registro del sistema**.

Citrix admite instancias de Citrix ADC VPX basadas en tarifas (licencia de utilidad con tarifa por hora) en GCP. Para presentar un caso de soporte técnico, busque el número de cuenta de GCP y el código PIN de soporte técnico, y llame al servicio de soporte técnico de Citrix. Se le pedirá que proporcione su nombre y dirección de correo electrónico. Para encontrar el PIN de soporte, inicie sesión en la GUI de VPX y vaya a la página **Sistema**.

Aquí hay un ejemplo de una página del sistema que muestra el PIN de soporte.



tramas jumbo en instancias Citrix ADC VPX

August 20, 2021

Los dispositivos Citrix ADC VPX admiten la recepción y transmisión de tramas jumbo que contienen hasta 9216 bytes de datos IP. Las tramas gigantes pueden transferir archivos grandes de forma más eficiente de lo que es posible con el tamaño MTU IP estándar de 1500 bytes.

Un dispositivo Citrix ADC puede utilizar tramas jumbo en los siguientes casos de implementación:

- Jumbo a Jumbo. El dispositivo recibe datos como tramas jumbo y los envía como tramas jumbo.
- No Jumbo a Jumbo. El dispositivo recibe datos como tramas normales y los envía como tramas jumbo.
- Jumbo a No Jumbo. El dispositivo recibe datos como tramas gigantes y los envía como tramas normales.

Para obtener más información, consulteConfiguración del soporte de tramas jumbo en un dispositivo Citrix ADC.

La compatibilidad con tramas gigantes está disponible en los dispositivos Citrix ADC VPX que se ejecutan en las siguientes plataformas de virtualización:

- VMware ESX
- Plataforma Linux-KVM
- Citrix XenServer
- Amazon Web Services (AWS)

Las tramas jumbo en los dispositivos VPX funcionan de forma similar a las tramas jumbo en los dispositivos MPX. Para obtener más información sobre las tramas Jumbo y sus casos de uso, consulte Configuración de tramas Jumbo en dispositivos MPX. Los casos de uso de tramas jumbo en dispositivos MPX también se aplican a los dispositivos VPX.

Configurar tramas jumbo para una instancia VPX que se ejecuta en VMware ESX

Realice las siguientes tareas para configurar tramas gigantes en un dispositivo Citrix ADC VPX que se ejecuta en el servidor VMware ESX:

1. Establezca la MTU de la interfaz o canal del dispositivo VPX en un valor del rango 1501-9000. Utilice la CLI o GUI para establecer el tamaño de MTU. Los dispositivos Citrix ADC VPX que se ejecutan en VMware ESX admiten la recepción y transmisión de tramas gigantes que contienen hasta 9000 bytes de datos IP.
2. Establezca el mismo tamaño de MTU en las interfaces físicas correspondientes del servidor VMware ESX mediante sus aplicaciones de administración. Para obtener más información so-

bre cómo configurar el tamaño de la MTU en las interfaces físicas de VMware ESX, consulte http://vmware.com/.

Configurar tramas jumbo para una instancia VPX que se ejecuta en el servidor Linux-KVM

Realice las siguientes tareas para configurar tramas jumbo en un dispositivo Citrix ADC VPX que se ejecuta en un servidor Linux-KVM:

1. Establezca la MTU de la interfaz o canal del dispositivo VPX en un valor del rango 1501-9216. Utilice Citrix ADC VPX CLI o GUI para establecer el tamaño de MTU.
2. Establezca el mismo tamaño de MTU en las interfaces físicas correspondientes de un servidor Linux-KVM mediante sus aplicaciones de administración. Para obtener más información sobre cómo configurar el tamaño de MTU en las interfaces físicas de Linux-KVM, consulte http://www.linux-kvm.org/.

Configurar tramas jumbo para una instancia VPX que se ejecuta en Citrix XenServer

Realice las siguientes tareas para configurar tramas jumbo en un dispositivo Citrix ADC VPX que se ejecuta en Citrix XenServer:

1. Conéctese a XenServer mediante XenCenter.
2. Apague todas las instancias VPX que utilizan las redes para las que se debe cambiar la MTU.
3. En la ficha **Redes**, seleccione la red: Red 0/1/2.
4. Seleccione **Propiedades** y modifique MTU.

Después de configurar las tramas gigantes en XenServer, puede configurar las tramas gigantes en el dispositivo ADC. Para obtener más información, consulteConfiguración del soporte de tramas jumbo en un dispositivo Citrix ADC.

Configurar tramas jumbo para una instancia VPX que se ejecuta en AWS

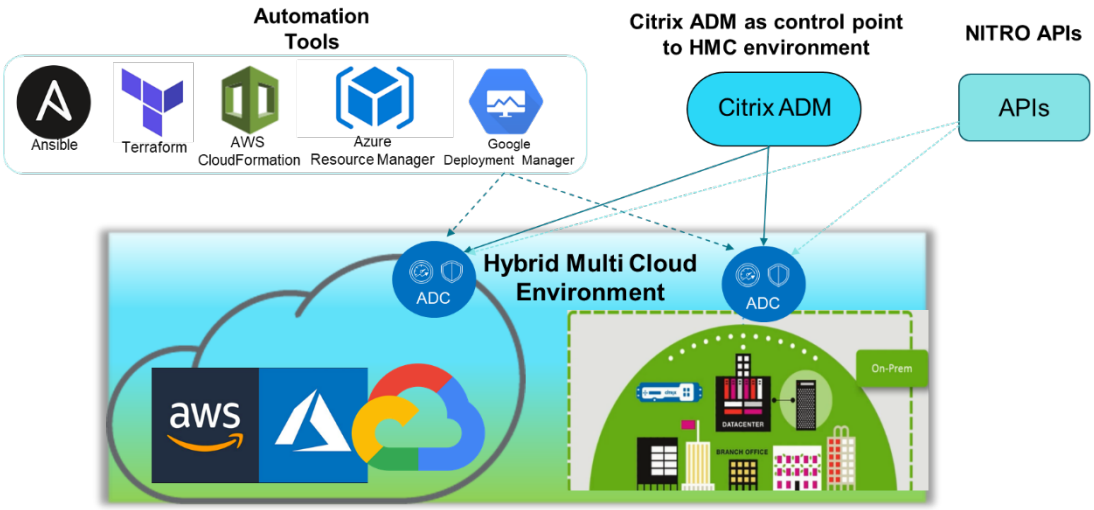
La configuración de nivel de host no es necesaria para VPX en Azure. Para configurar Jumbo Frames en VPX, siga los pasos que se indican en Configuración del soporte de tramas jumbo en un dispositivo Citrix ADC.

Automatizar la implementación y las configuraciones de Citrix ADC

March 9, 2022

Citrix ADC proporciona varias herramientas para automatizar las implementaciones y configuraciones de ADC. Este documento proporciona un breve resumen de varias herramientas de automatización y referencias a varios recursos de automatización que puede utilizar para administrar las configuraciones de ADC.

La siguiente ilustración proporciona una descripción general de la automatización de Citrix ADC en un entorno híbrido de múltiples nubes (HMC).



Automatice Citrix ADC con Citrix ADM

Citrix ADM actúa como un punto de control de automatización para su infraestructura ADC distribuida. Citrix ADM proporciona un conjunto completo de capacidades de automatización, desde el aprovisionamiento de dispositivos ADC hasta su actualización. Las siguientes son las principales funciones de automatización de ADM:

- Aprovisionamiento de instancias de Citrix ADC VPX en AWS
- Aprovisionamiento de instancias de Citrix ADC VPX en Azure
- StyleBooks
- Trabajos de configuración
- Auditoría de configuración
- Actualizaciones de ADC
- Administración de certificados SSL
- Integraciones - GitHub, ServiceNow, Integraciones de notificaciones de eventos

blogs y vídeos de Citrix ADM sobre automatización

- Migraciones de aplicaciones mediante StyleBooks
- Integre configuraciones de ADC con CI/CD mediante ADM StyleBooks

- Simplificación de las implementaciones de Citrix ADC en la nube pública a través de ADM
- 10 formas en que el servicio Citrix ADM admite actualizaciones más sencillas de Citrix ADC

Citrix ADM también proporciona API para sus diversas capacidades que integran Citrix ADM y Citrix ADC como parte de la automatización general de TI. Para obtener más información, consulte API de servicio Citrix ADM.

Automatice Citrix ADC con Terraform

Terraform es una herramienta que toma la infraestructura como un enfoque de código para aprovisionar y administrar la nube, la infraestructura o el servicio. Los recursos de terraform de Citrix ADC están disponibles en GitHub para su uso. Consulta GitHub para obtener documentación y uso detallados.

- Módulos Citrix ADC Terraform para configurar ADC para varios casos de uso, como el equilibrio de carga y GSLB
- Scripts en la nube de Terraform para implementar ADC en AWS
- Scripts en la nube de Terraform para implementar ADC en Azure
- Scripts en la nube de Terraform para implementar ADC en GCP
- Implementación azul-verde mediante procesos de Citrix ADC VPX y Azure

Blogs y vídeos sobre Terraform para la automatización de ADC

- Automatice sus implementaciones de Citrix ADC con Terraform
- Aprovisionar y configurar ADC en la configuración de alta disponibilidad en AWS mediante Terraform

Automatizar Citrix ADC mediante Consul-Terraform-Sync

El módulo Citrix ADC Consul-Terraform-Sync (CTS) permite a los equipos de aplicaciones agregar o eliminar automáticamente nuevas instancias de servicios en Citrix ADC. No es necesario generar tickets manuales a los administradores de TI o a los equipos de redes para realizar los cambios necesarios en las configuraciones de ADC.

- Módulo Citrix ADC Consul-Terraform-Sync para la automatización de la infraestructura de red
- Seminario web conjunto Citrix-HashiCorp: Redes dinámicas con Consul-Terraform-Sync para Terraform Enterprise y Citrix ADC

Automatice Citrix ADC con Ansible

Ansible es una herramienta de aprovisionamiento de software de código abierto, administración de configuración e implementación de aplicaciones que permite la infraestructura como código. Los

módulos y playbooks de muestra de Citrix ADC Ansible se pueden encontrar en GitHub para su uso. Consulta GitHub para obtener documentación y uso detallados.

- Módulos de Ansible para configurar ADC
- Documentación y guía de referencia de los módulos de ADC Ansible
- Informe técnico sobre automatización de ADC con Ansible
- Módulos de Ansible para ADM

Citrix es un socio de automatización certificado de Ansible. Los usuarios que tienen suscripción a Red Hat Ansible Automation Platform pueden acceder a las colecciones de Citrix ADC desde Red Hat Automation Hub.

Blogs de automatización de Terraform y Ansible

- Citrix nombrado socio de integración del año de HashiCorp
- Citrix ahora es un socio certificado de Red Hat Ansible Automation Platform
- Terraform y Ansible Automation para la entrega de aplicaciones y la seguridad

Plantillas de nube pública para implementaciones de ADC

Las plantillas de nube pública simplifican el aprovisionamiento de sus implementaciones en nubes públicas. Hay diferentes plantillas de Citrix ADC disponibles para varios entornos. Para obtener detalles de uso, consulta los repositorios GitHub respectivos.

CFT de AWS:

- CFT para aprovisionar Citrix ADC VPX en AWS

Plantillas de Azure Resource Manager (ARM):

- Plantillas ARM para aprovisionar Citrix ADC VPX en Azure

Plantillas de Google Cloud Deployment Manager (GDM):

- Plantillas de GDM para aprovisionar Citrix ADC VPX en Google

Vídeos en plantillas

- Implementación de Citrix ADC HA en AWS mediante la plantilla de CloudFormation
- Implemente Citrix ADC HA en las zonas de disponibilidad mediante AWS QuickStart
- Implementación de alta disponibilidad de Citrix ADC en GCP mediante plantillas de GDM

Inicio rápido de AWS

- Inicio rápido de Citrix WAF
- Inicio rápido de AWS para Citrix ADC VPX para aplicaciones web en AWS

API de NITRO

El protocolo Citrix ADC NITRO le permite configurar y supervisar mediante programación el dispositivo Citrix ADC mediante interfaces de transferencia de estado representacional (REST). Por lo tanto, las aplicaciones NITRO se pueden desarrollar en cualquier lenguaje de programación. Para las aplicaciones que deben desarrollarse en Java, .NET o Python, las API de NITRO se exponen a través de bibliotecas relevantes que se empaquetan como kits de desarrollo de software (SDK) separados.

- Documentación de NITRO API
- Referencia de la API de Citrix ADC
- Ejemplo de configuración de casos de uso de ADC mediante NITRO API de

Preguntas frecuentes

July 6, 2022

La siguiente sección le ayuda a clasificar las preguntas frecuentes según Citrix Application Delivery Controller (ADC) VPX.

- Función y funcionalidad
- Cifrado
- Precios y empaquetado
- Citrix ADC VPX Express
- Hipervisor
- Planificación o dimensionamiento de la capacidad
- Requisitos del sistema
- Otras preguntas frecuentes técnicas

Función y funcionalidad

¿Qué es Citrix ADC VPX?

Citrix ADC VPX es un dispositivo ADC virtual que se puede alojar en un hipervisor instalado en servidores estándar del sector.

¿Citrix ADC VPX incluye toda la funcionalidad de optimización de aplicaciones web como dispositivos ADC?

Sí. Citrix ADC VPX incluye todo el equilibrio de carga, la administración del tráfico, la aceleración de las aplicaciones, la seguridad de las aplicaciones (incluidos Citrix ADC Gateway y Citrix Application Firewall) y la funcionalidad de descarga. Para obtener una descripción completa de la función y funcionalidad de Citrix ADC, consulte Entrega de aplicaciones a su manera.

¿Existen limitaciones con Citrix Application Firewall al usarlo en Citrix ADC VPX?

Citrix Application Firewall en Citrix ADC VPX proporciona las mismas protecciones de seguridad que en los dispositivos Citrix ADC. El rendimiento o el rendimiento de Citrix Application Firewall varía según la plataforma.

¿Hay alguna diferencia entre Citrix ADC Gateway en Citrix ADC VPX y Citrix ADC Gateway en dispositivos Citrix ADC?

Funcionalmente, son idénticos. Citrix ADC Gateway en Citrix ADC VPX admite todas las funciones de Citrix ADC Gateway disponibles en la versión 9.1 del software Citrix ADC. Sin embargo, dado que los dispositivos Citrix ADC proporcionan hardware de aceleración SSL dedicado, ofrecen mayor escalabilidad SSL VPN que una instancia Citrix ADC VPX.

Aparte de la evidente diferencia de poder ejecutarse en un hipervisor, ¿en qué se diferencia Citrix ADC VPX de los dispositivos físicos Citrix ADC?

Hay dos áreas principales en las que los clientes ven diferencias de comportamiento. La primera es que Citrix ADC VPX no puede ofrecer el mismo rendimiento que muchos dispositivos Citrix ADC. La segunda es que, si bien los dispositivos Citrix ADC incorporan su propia funcionalidad de red L2, Citrix ADC VPX confía en el hipervisor para sus servicios de red L2. En general, no limita cómo se puede implementar Citrix ADC VPX. Puede haber cierta funcionalidad L2 configurada en un dispositivo Citrix ADC físico que debe configurarse en el hipervisor subyacente.

¿Qué papel desempeña Citrix ADC VPX en el mercado de la entrega de aplicaciones?

Citrix ADC VPX cambia las reglas del juego en el mercado de entrega de aplicaciones de las siguientes maneras:

- Al hacer que un dispositivo Citrix ADC sea aún más asequible, Citrix ADC VPX permite a cualquier organización de TI implementar un dispositivo Citrix ADC. No es solo para sus aplicaciones web más críticas, sino para todas sus aplicaciones web.

- Citrix ADC VPX permite a los clientes converger aún más las redes y la virtualización dentro de sus centros de datos. Citrix ADC VPX no solo se puede utilizar para optimizar las aplicaciones web alojadas en servidores virtualizados. También permite que la entrega de aplicaciones web se convierta en un servicio virtualizado que se puede implementar fácil y rápidamente en cualquier lugar. Las organizaciones de TI utilizan los procesos estándar del centro de datos para tareas tales como aprovisionamiento, automatización y devolución de cargo para la infraestructura de entrega de aplicaciones web.
- Citrix ADC VPX abre nuevas arquitecturas de implementación que no son prácticas si solo se utilizan dispositivos físicos. Los dispositivos Citrix ADC VPX y Citrix ADC MPX se pueden utilizar de base, adaptados a las necesidades individuales de cada aplicación respectiva para manejar acciones intensivas del procesador, como la compresión y la inspección del firewall de aplicaciones. En el perímetro del centro de datos, los dispositivos Citrix ADC MPX manejan tareas de gran volumen en toda la red, como la distribución inicial del tráfico, el cifrado o descifrado SSL, la prevención de ataques de denegación de servicio (DoS) y el equilibrio de carga global. La combinación de los dispositivos Citrix ADC MPX de alto rendimiento con el dispositivo virtual Citrix ADC VPX fácil de implementar brinda una flexibilidad y capacidades de personalización sin igual a los entornos de centros de datos modernos a gran escala y a la vez que reduce los costes generales del centro de datos.

¿Cómo encaja Citrix ADC VPX en nuestra estrategia de centro de entrega de Citrix?

Con la disponibilidad de Citrix ADC VPX, toda la oferta de centros de entrega de Citrix está disponible como una oferta virtualizada. Todo el centro de entrega de Citrix se beneficia de las potentes capacidades de administración, aprovisionamiento, supervisión y generación de informes disponibles en Citrix XenCenter. Esto se puede implementar rápidamente en casi cualquier entorno y administrarse de forma centralizada desde cualquier lugar. Con una infraestructura de entrega de aplicaciones virtualizada e integrada, las organizaciones pueden ofrecer escritorios, aplicaciones cliente-servidor y aplicaciones web.

Cifrado

¿Citrix ADC VPX admite la descarga SSL?

Sí. Sin embargo, Citrix ADC VPX realiza todo el procesamiento SSL en el software, por lo que Citrix ADC VPX no ofrece el mismo rendimiento SSL que los dispositivos Citrix ADC. Citrix ADC VPX puede admitir hasta 750 nuevas transacciones SSL por segundo.

¿Las tarjetas SSL de terceros instaladas en el servidor que aloja Citrix ADC VPX aceleran el cifrado o el descifrado SSL?

No. La compatibilidad con tarjetas SSL de terceros no puede asociar Citrix ADC VPX a implementaciones de hardware específicas. Disminuye en gran medida la capacidad de una organización de alojar de forma flexible Citrix ADC VPX en cualquier lugar del centro de datos. Los dispositivos Citrix ADC MPX deben utilizarse cuando se requiere un rendimiento SSL superior al que proporciona Citrix ADC VPX.

¿Admite Citrix ADC VPX los mismos cifrados de cifrado que los dispositivos Citrix ADC físicos?

VPX admite todos los cifrados de cifrado como dispositivos Citrix ADC físicos, excepto ECDSA.

¿Cuál es el rendimiento de las transacciones SSL de Citrix ADC VPX?

Consulte la hoja de datos de Citrix ADC VPX para obtener información sobre el rendimiento de las transacciones SSL.

Precios y empaquetado

¿Cómo se empaqueta Citrix ADC VPX?

La selección de Citrix ADC VPX es similar a la selección de dispositivos Citrix ADC. En primer lugar, el cliente selecciona la edición Citrix ADC en función de sus requisitos de funcionalidad. A continuación, el cliente selecciona el nivel de ancho de banda específico de Citrix ADC VPX en función de sus requisitos de rendimiento. Citrix ADC VPX está disponible en las ediciones Standard, Advanced y Premium. Citrix ADC VPX ofrece desde 10 Mbps (VPX 10) a 100 Gbps (VPX 100G). Puede encontrar más detalles en la hoja de datos de Citrix ADC VPX.

¿El precio de Citrix ADC VPX es el mismo para todos los hipervisores?

Sí.

¿Se utilizan los mismos SKU de Citrix ADC para VPX en todos los hipervisores?

Sí.

¿Se puede mover una licencia de Citrix ADC VPX de un hipervisor a otro (por ejemplo, de VMware a Hyper-V)?

Sí. Las licencias de Citrix ADC VPX son independientes del hipervisor subyacente. Si decide mover la máquina virtual Citrix ADC VPX de un hipervisor a otro, no necesita obtener una nueva licencia. Sin

embargo, es posible que deba volver a alojar la licencia existente de Citrix ADC VPX.

¿Se pueden actualizar las instancias Citrix ADC VPX?

Sí. Tanto los límites de rendimiento como la edición de la familia Citrix ADC se pueden actualizar. Hay disponibles SKU de actualización para ambos tipos de ascenso de clase.

Si quiero implementar Citrix ADC VPX en un par de alta disponibilidad, ¿cuántas licencias necesito?

Al igual que con los dispositivos físicos Citrix ADC, una configuración de alta disponibilidad de Citrix ADC requiere dos instancias activas. Por lo tanto, el cliente debe comprar dos licencias.

Citrix ADC VPX Express y prueba gratuita de 90 días

¿Citrix ADC VPX Express incluye toda la funcionalidad estándar de Citrix ADC? ¿Incluye Citrix ADC Gateway y equilibrio de carga para la interfaz web y el agente XML de Citrix Virtual Apps (anteriormente XenApp)?

Sí. Citrix ADC VPX Express incluye la funcionalidad completa de Citrix ADC Standard. A partir de las versiones 12.0 a 56.20 de Citrix ADC, Citrix modificó el comportamiento de VPX express.

¿Citrix ADC VPX Express incluye toda la funcionalidad estándar de Citrix ADC? ¿Incluye Citrix ADC Gateway y equilibrio de carga para la interfaz web de Citrix Virtual Apps y el broker XML?

A partir de las versiones 12.0 a 56.20 de Citrix ADC, VPX Express ofrece el conjunto de funciones de Citrix ADC Standard Edition, excepto la funcionalidad de Gateway. Anteriormente a la versión 12.0—56.20, VPX express incluye todas las funciones de la edición estándar.

¿Necesita una licencia Citrix ADC VPX Express?

Con la nueva versión de Citrix ADC VPX Express (12.0—56.20 y posteriores), VPX Express es gratuito y no requiere la instalación de archivos de licencias y no tiene ningún compromiso. Si ya tiene una licencia VPX Express, se conserva el comportamiento anterior de VPX Express. Si se quita el *archivo de licencias* VPX Express y se utiliza la versión 12.0—56.20 y posteriores, el nuevo comportamiento VPX express surte efecto.

¿Caduca la licencia de Citrix ADC VPX Express?

Con el nuevo VPX express, no. No hay licencia ni fecha de caducidad. Si ya tiene una licencia VPX express, la licencia caduca un año después de la descarga.

¿Citrix ADC VPX Express incluye las cinco licencias simultáneas gratuitas de Citrix ADC Gateway?

Sí, si tiene una licencia VPX express.

¿Existe un límite en cuanto a la cantidad de Citrix ADC VPX Express que un cliente puede descargar?

Cinco.

¿Admite Citrix ADC VPX Express los mismos cifrados de cifrado que los dispositivos Citrix ADC MPX?

Para disponibilidad general, los mismos cifrados de cifrado seguros compatibles con los dispositivos Citrix ADC están disponibles en Citrix ADC VPX y Citrix ADC VPX Express. Está sujeto a las mismas regulaciones de importación o exportación.

¿Puedo presentar casos de soporte técnico para Citrix ADC VPX Express?

No. Se requiere una licencia Citrix ADC VPX minorista como VPX-10, VPX-200, VPX-1000, VPX-3000 para presentar casos de soporte técnico. Sin embargo, los usuarios de Citrix ADC VPX Express pueden utilizar libremente el Knowledge Center de Citrix ADC VPX y solicitar ayuda a la comunidad a través de los foros de discusión Z.

¿Se puede actualizar Citrix ADC VPX Express a una versión comercial?

Sí. Simplemente compre la licencia minorista de Citrix ADC VPX que necesita y, a continuación, aplique la licencia correspondiente a la instancia Citrix ADC VPX Express.

Hipervisor

¿Qué versiones de VMware admite Citrix ADC VPX?

Citrix ADC VPX admite VMware ESX y ESXi para las versiones 3.5 o posterior. Para obtener más información, consulte Tabla de compatibilidad y directrices de uso

Para VMware, ¿cuántas interfaces de red virtual puede asignar a un VPX?

Puede asignar hasta 10 interfaces de red virtuales a un dispositivo Citrix ADC VPX.

Desde vSphere, ¿cómo podemos acceder a la línea de comandos de Citrix ADC VPX?

El cliente de VMware vSphere proporciona acceso integrado a la línea de comandos de Citrix ADC VPX a través de una ficha de consola. Además, puede utilizar cualquier cliente SSH o Telnet para acceder a la línea de comandos. Puede utilizar la dirección NSIP de Citrix ADC VPX en el cliente SSH o Telnet.

¿Cómo puede acceder a la GUI de Citrix ADC VPX?

Para acceder a la GUI de Citrix ADC VPX, escriba el NSIP de Citrix ADC VPX, por ejemplo, `http://NSIP address` en el campo de dirección de cualquier explorador.

¿Se pueden configurar dos instancias Citrix ADC VPX instaladas en el mismo VMware ESX en una configuración de alta disponibilidad?

Sí, pero no es recomendable. Un fallo de hardware afectaría a ambas instancias de Citrix ADC VPX.

¿Se pueden configurar dos instancias Citrix ADC VPX que se ejecutan en dos sistemas VMware ESX diferentes en una configuración de alta disponibilidad?

Sí. Se recomienda en una configuración de alta disponibilidad.

Para VMware, ¿los eventos relacionados con la interfaz son compatibles con Citrix ADC VPX?

No. No se admiten los eventos relacionados con la interfaz.

Para VMware, ¿las VLAN etiquetadas son compatibles con Citrix ADC VPX?

Sí. Las VLAN etiquetadas de Citrix ADC se admiten en Citrix ADC VPX desde la versión 11.0 y versiones posteriores. Para obtener más información, consulte la documentación de Citrix.

Para VMware, ¿se admite la agregación de enlaces y LACP en Citrix ADC VPX?

No. La agregación de vínculos y LACP no son compatibles con Citrix ADC VPX. La agregación de enlaces debe configurarse a nivel de VMware.

¿Cómo accedemos a la documentación de Citrix ADC VPX?

La documentación está disponible en la GUI de Citrix ADC VPX. Después de iniciar sesión, seleccione la ficha **Documentación**.

Planificación o dimensionamiento de la capacidad

¿Qué rendimiento puedo esperar con Citrix ADC VPX?

Citrix ADC VPX ofrece un buen rendimiento. Consulte la hoja de datos de Citrix ADC VPX para obtener un nivel de rendimiento específico alcanzable mediante Citrix ADC VPX.

Dado que la potencia de la CPU del servidor varía, ¿cómo podemos estimar el rendimiento máximo de una instancia de Citrix ADC?

El uso de una CPU más rápida puede dar lugar a un mayor rendimiento (hasta el máximo permitido por la licencia), mientras que usar una CPU más lenta puede limitar el rendimiento.

¿Existen límites de ancho de banda o rendimiento de Citrix ADC VPX para el tráfico entrante o para el tráfico entrante y saliente?

Los límites de ancho de banda de Citrix ADC VPX se aplican únicamente al tráfico entrante a Citrix ADC, independientemente de si se trata del tráfico de solicitud o de respuesta. Indica que un Citrix ADC VPX-1000 (por ejemplo) puede procesar simultáneamente 1 Gbps de tráfico entrante y 1 Gbps de tráfico saliente. El tráfico entrante y saliente no es lo mismo que el tráfico de solicitud y respuesta. Para Citrix ADC, tanto el tráfico procedente de los dispositivos de punto final (tráfico de solicitudes) como el tráfico procedente de los servidores de origen (tráfico de respuesta) es “entrante” (es decir, entra en Citrix ADC).

¿Se pueden ejecutar varias instancias de Citrix ADC VPX en el mismo servidor?

Sí. Sin embargo, asegúrese de que el servidor físico tenga suficiente capacidad de CPU y E/S para soportar la carga de trabajo total que se ejecuta en el host; de lo contrario, el rendimiento de Citrix ADC VPX podría verse afectado.

Si se ejecuta más de una instancia de Citrix ADC VPX en un servidor físico, ¿cuál es el requisito mínimo de hardware por instancia de Citrix ADC VPX?

A cada instancia de Citrix ADC VPX se le deben asignar 2 GB de RAM física, 20 GB de espacio en el disco duro y 2 vCPU.

¿Puedo alojar Citrix ADC VPX y otras aplicaciones en el mismo servidor?

Sí. Por ejemplo, Citrix ADC VPX, Citrix Virtual Apps Web Interface y Citrix Virtual Apps XML Broker se pueden virtualizar y ejecutar en el mismo servidor. Para obtener el mejor rendimiento, asegúrese de

que el host físico tenga suficiente capacidad de CPU y E/S para admitir todas las cargas de trabajo en ejecución.

¿Agregar núcleos de CPU a una única instancia de Citrix ADC VPX aumentará el rendimiento de esa instancia?

Dependiendo de la licencia, una instancia de Citrix ADC VPX puede usar hasta 4 vCPU en la actualidad. Agregar una CPU adicional a una instancia Citrix ADC VPX que puede utilizar más CPU aumenta el rendimiento.

¿Por qué Citrix ADC VPX parece consumir más del 90% de la CPU aunque esté inactiva?

Se trata de un comportamiento normal y los dispositivos Citrix ADC presentan el mismo comportamiento. Para ver la verdadera extensión de la utilización de CPU de Citrix ADC VPX, utilice el comando stat CPU en la CLI de Citrix ADC o vea el uso de CPU de Citrix ADC VPX desde la GUI de Citrix ADC. El motor de procesamiento de paquetes Citrix ADC siempre está "buscando trabajo", incluso cuando no hay trabajo por hacer. Por lo tanto, hace todo lo posible para tomar el control de la CPU y no liberarla. En un servidor instalado con Citrix ADC VPX y nada más, da como resultado (desde la perspectiva del hipervisor) que Citrix ADC VPX consume toda la CPU. Al examinar la utilización de la CPU desde "dentro de Citrix ADC" (mediante la CLI o la GUI) se proporciona una imagen de la capacidad de CPU Citrix ADC VPX que se está usando.

Requisitos del sistema

¿Cuál es el requisito mínimo de hardware para Citrix ADC VPX?

Consulte la hoja de datos de Citrix ADC VPX para conocer los requisitos del sistema.

Citrix ADC VPX requiere:

- Requisitos del procesador: servidor de doble núcleo con Intel Xeon y AMD (EPYC).
- Memoria disponible: 4 GB de RAM y disco duro de 20 GB. Para implementaciones críticas, Citrix no recomienda 2 GB de RAM para VPX porque el sistema funciona en un entorno con mucha limitación de memoria. Esto puede provocar problemas relacionados con la escala, el rendimiento o la estabilidad.
- Hipervisor: Citrix Hypervisor 5.6 o posterior; VMware ESX/ESXi 3.5 o posterior, Windows Server 2008 R2 con Hyper-V.
- Conectividad: 100 Mbps como mínimo. Se recomienda 1 Gbps.
- Una NIC compatible con el hipervisor.

> **Nota:**
>
> A partir de la versión 13.1 de Citrix ADC, la instancia de Citrix ADC VPX en el hipervisor VMware ESXi admite procesadores AMD (EPYC).

¿Qué es Intel VT-x?

Estas funciones, a veces denominadas “asistencia de hardware” o “asistencia de virtualización”, atrapan las instrucciones de CPU confidenciales o privilegiadas que ejecuta el SO invitado en el hipervisor. Esto simplifica el alojamiento de SO invitado (BSD para Citrix ADC VPX) en el hipervisor.

¿Qué tan comunes son las VT-x?

Prácticamente, todos los servidores enviados en los últimos dos años podrían admitir VT-x. Muchos servidores se envían con la asistencia de virtualización inhabilitada en el BIOS. Antes de asumir que no puede ejecutar Citrix ADC VPX, compruebe si necesita cambiar esta configuración en el servidor.

¿Existe una lista de compatibilidad de hardware (HCL) para Citrix ADC VPX?

Mientras el servidor sea compatible con Intel VT-x, Citrix ADC VPX debe ejecutarse en cualquier servidor compatible con el hipervisor subyacente. Consulte el HCL del hipervisor para obtener una lista completa de plataformas compatibles.

¿En qué versión del sistema operativo Citrix ADC se basa Citrix ADC VPX?

Citrix ADC VPX se basa en Citrix ADC 9.1 o versiones posteriores.

Dado que Citrix ADC VPX se ejecuta en BSD, ¿se puede ejecutar de forma nativa en un servidor con BSD Unix instalado?

No. Citrix ADC VPX requiere que se ejecute el hipervisor. Los soportes detallados de hipervisor se encuentran en la hoja de datos de Citrix ADC VPX.

Otras preguntas frecuentes técnicas

¿Funciona la agregación de enlaces en un servidor físico con varias NIC?

LACP no es compatible. Para Citrix Hypervisor, se admite la agregación de vínculos estáticos y tiene límites de cuatro canales y siete interfaces virtuales. En el caso de VMware, Citrix ADC VPX no admite la agregación de vínculos estáticos, pero se puede configurar a nivel de VMware.

¿VPX admite el reenvío basado en MAC (MBF)? ¿Hay algún cambio en la implementación del dispositivo Citrix ADC?

MBF es compatible y se comporta del mismo modo que con el dispositivo Citrix ADC. Básicamente, el hipervisor cambia todos los paquetes recibidos de Citrix ADC VPX al exterior y viceversa.

¿Cómo se lleva a cabo el proceso de actualización de Citrix ADC VPX?

Las actualizaciones se realizan de la misma manera que para los dispositivos Citrix ADC: Descargue un archivo de kernel y use install ns o la utilidad de actualización en la GUI.

¿Cómo se asigna el espacio flash y en disco? ¿Podemos cambiarlo?

/flash = 965M
/var = 14G
Se debe asignar un mínimo de 2 GB de memoria a cada instancia de Citrix ADC VPX. La imagen de disco Citrix ADC VPX tenía un tamaño de 20 GB para facilitar el mantenimiento, por ejemplo, espacio para tomar y almacenar volcados de memoria de hasta 4 GB y archivos de registro y seguimiento. Si bien sería posible generar una imagen de disco más pequeña, no hay planes de hacerlo en este momento. `/flash` y `/var` están en la misma imagen de disco. Se mantienen como sistemas de archivos separados para fines de compatibilidad.
Para obtener recomendaciones detalladas sobre la asignación de memoria, consulte la hoja de datos de Citrix ADC VPX.

¿Podemos agregar un nuevo disco duro para aumentar el espacio en la instancia de Citrix ADC VPX?

Sí. A partir de Citrix ADC versión 13.1 compilación 21.x, tiene la opción de aumentar el espacio en disco en la instancia de Citrix ADC VPX agregando un segundo disco. Esta función es compatible con todos los factores de forma VPX. Debe agregar el segundo disco durante el primer arranque del dispositivo Citrix ADC o después cuando se apague el dispositivo. Al conectar el segundo disco, el directorio "/var" se monta automáticamente en este disco. El segundo disco se utiliza para almacenar los archivos principales y el registro. Los directorios existentes que se utilizan para almacenar archivos principales y archivos de registro siguen funcionando como antes.

> **Nota:**
>
> Realice copias de seguridad externas al cambiar a una versión anterior del dispositivo Citrix ADC para evitar la pérdida de datos.

Para obtener información sobre cómo conectar una nueva unidad de disco duro (HDD) a una instancia de Citrix ADC VPX en una nube, consulte lo siguiente:

- Documentación de Azure
- Documentación de AWS
- Documentación de GCP

> **Advertencia:**
>
> Después de agregar una nueva unidad de disco duro a VPX, algunos de los scripts que funcionan en archivos que se mueven a la nueva unidad de disco duro pueden fallar en las siguientes condiciones:
>
> Si utiliza el comando shell “link” para crear enlaces físicos a los archivos, que se movieron a un disco duro nuevo.
>
> Todos estos comandos deben sustituirse por “ln -s” para utilizar un enlace simbólico. Además, modifique los scripts que fallan en consecuencia.

¿Qué podemos esperar de la numeración de compilaciones de Citrix ADC VPX y la interoperabilidad con otras compilaciones?

Citrix ADC VPX tiene una numeración de compilación similar a la 9.1. Cl (clásico) y 9.1. Versión de Nc (nCore), por ejemplo 9.1_97.3.vpx, 9.1_97.3.nc y 9.1_97.3.cl.

¿Puede Citrix ADC VPX formar parte de una configuración de alta disponibilidad con un dispositivo Citrix ADC?

No es una configuración compatible.

¿Todas las interfaces visibles en Citrix ADC VPX están directamente relacionadas con el número de interfaces del hipervisor?

No. Puede agregar hasta siete interfaces (10 para VMware) a través de la utilidad de configuración de Citrix ADC VPX con solo una NIC física en el hipervisor.

¿Se puede utilizar Citrix Hypervisor XenMotion o VMware VMotion o Hyper-V la migración en directo para mover instancias activas de Citrix ADC VPX?

Citrix ADC VPX no admite la migración en directo de XenMotion o Hyper-V. VMotion se admite a partir de la versión 12.1 de Citrix ADC. Para obtener más información, consulte Notas de la versión.

Descripción general del sistema de licencias

October 5, 2021

Citrix ofrece una amplia gama de ediciones de productos y modelos de licencias para dispositivos MPX y VPX, para satisfacer las necesidades de su organización.

Para que un dispositivo Citrix ADC funcione correctamente, debe tener una licencia de edición de la familia Citrix ADC. La línea de productos ADC tiene tres ediciones familiares:

- Standard Edition
- Advanced Edition
- Premium Edition

Para obtener más información, consulte la hoja de datos de Citrix ADC.

Después de seleccionar la edición Citrix ADC, puede seleccionar una de las ofertas de licencias MPX y VPX. Según criterios como perpetuidad y suscripción (suscripción anual y por hora), vCPU y ancho de banda, local y nube, etc.

Licencias de Citrix ADC VPX

Las siguientes son las licencias específicas de VPX.

Licencia Citrix ADC VPX Express

A partir de la versión 12.0 56.20 de Citrix ADC, VPX Express para implementaciones locales y en la nube no requiere un archivo de licencia y viene con las siguientes funciones:

- Ancho de banda 20 Mbps
- Todas las funciones de licencia estándar de ADC, excepto Citrix Gateway y defensas L4 y L7
- Máximo 250 sesiones SSL
- Rendimiento SSL de 20 Mbps

Puede actualizar la licencia VPX Express a las dos opciones siguientes:

1. Licencia independiente de Citrix ADC VPX
2. Licencia Citrix ADC Pooled Capacity para instancias VPX. Para obtener más información, consulte Capacidad agrupada de Citrix ADC.

> **Importante**
>
> La agrupación en clústeres está disponible en la edición Standard para la nube pública VPX y en la licencia VPX Express.

Licencia de capacidad agrupada de Citrix ADC VPX

Puede utilizar Citrix Application Delivery Management (ADM) para crear un marco de licencias que contenga un ancho de banda común y un grupo de instancias. Para obtener información completa, consulte Capacidad agrupada de Citrix ADC.

Recursos conexos

El sistema de licencias de Citrix

Cómo asignar licencias Citrix ADC VPX

Licencias VPX en la nube

La implementación VPX es compatible con proveedores de nube pública como Azure, AWS y Google. Para obtener más información, consulte los siguientes documentos:

- Licencia VPX-Azure
- Licencia VPX-AWS
- Licencia VPX-GCP

Asignar y aplicar una licencia

June 22, 2022

En la GUI de Citrix MPX y VPX ADC, puede utilizar el número de serie de hardware (HSN) o el código de acceso de licencia para asignar las licencias. De forma alternativa, si ya hay una licencia en el equipo local, puede cargarla en el dispositivo.

Para todas las demás funciones, como devolver o reasignar la licencia, debe utilizar el portal de licencias. Opcionalmente, puede seguir mediante el portal de licencias para la asignación de licencias. Para obtener más información, consulte Uso de administración de licencias en My Account en citrix.com.

Guía de licencias de Citrix

La guía de licencias de Citrix también incluye información sobre la instalación de licencias en un dispositivo Citrix ADC y la instalación de licencias en otros productos Citrix. Para obtener más información, consulte la Guía de licencias de Citrix.

Requisitos previos

> **Nota**
>
> Adquiera licencias independientes para cada dispositivo en un par de alta disponibilidad. Asegúrese de que los mismos tipos de licencias estén instalados en ambos dispositivos. Por ejemplo, si adquiere una licencia Premium para un dispositivo, debe comprar otra licencia Premium para el otro dispositivo.

Para utilizar el número de serie del hardware o el código de acceso de licencia para asignar las licencias:

- Debe poder acceder a los dominios públicos a través del dispositivo. Por ejemplo, el dispositivo debe poder acceder a www.citrix.com. El software de asignación de licencias accede internamente al portal de licencias de Citrix para su licencia. Para acceder a un dominio público:
  - Utilice un servidor proxy o configure un servidor DNS.
  - Configure una dirección IP de Citrix ADC (NSIP) o una dirección IP de subred (SNIP) en el dispositivo Citrix ADC.
- La licencia debe estar vinculada al hardware o debe tener un código de acceso de licencia válido. Citrix envía el código de acceso a la licencia por correo electrónico cuando compra una licencia.

Asignar una licencia mediante la interfaz gráfica de usuario

Si la licencia ya está vinculada al hardware, el proceso de asignación de licencias puede utilizar el número de serie del hardware. De lo contrario, debe escribir el código de acceso a la licencia.

Puede asignar licencias parcialmente según sea necesario para su implementación. Por ejemplo, si el archivo de licencia contiene 10 licencias, pero su requisito actual es solo para seis licencias, puede asignar seis licencias ahora y asignar más licencias más tarde. No puede asignar más del número total de licencias presentes en el archivo de licencia.

Para asignar su licencia

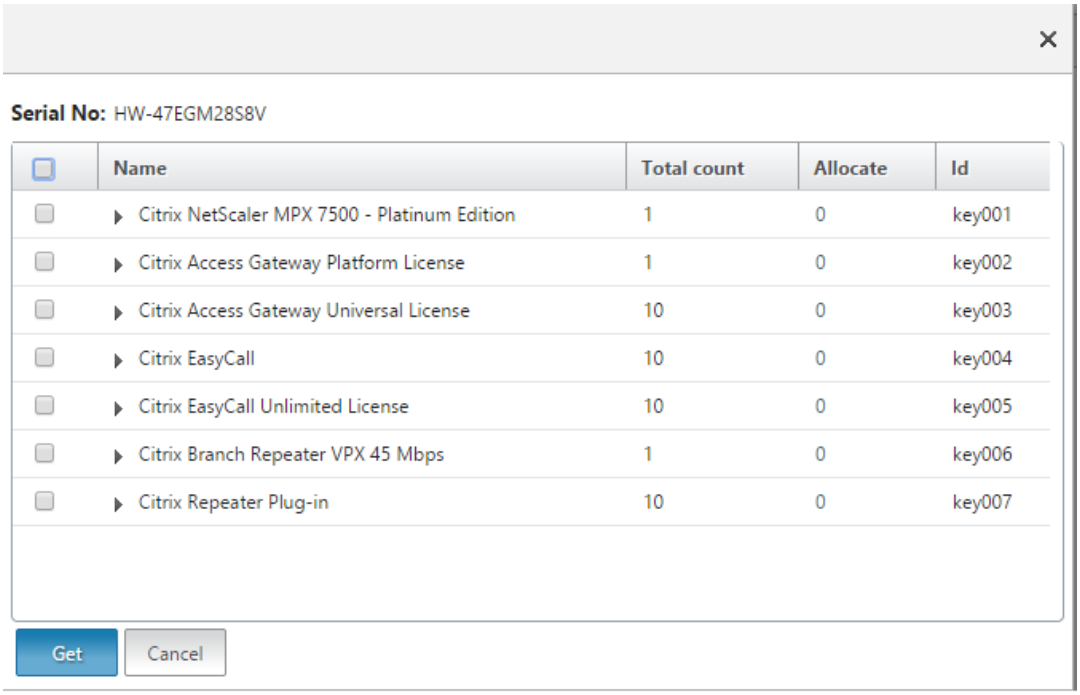
1. En un explorador web, escriba la dirección IP del dispositivo Citrix ADC (por ejemplo, `http://192.168.100.1`).
2. En Nombre de usuario y Contraseña, introduzca las credenciales de administrador.
3. En la ficha **Configuración**, vaya a **Sistema > Licencias**.
4. En el panel de detalles, haga clic en **Administrar licencias**, haga clic en **Agregar nueva licencia**, y a continuación, seleccione una de las siguientes opciones:
   - **Usar número de serie**: el software recupera internamente el número de serie del dispositivo y utiliza este número para mostrar las licencias.

- **Usar código de acceso de licencia**: Citrix envía por correo electrónico el código de acceso de licencia de la licencia que adquirió. Introduzca el código de acceso a la licencia en el cuadro de texto.

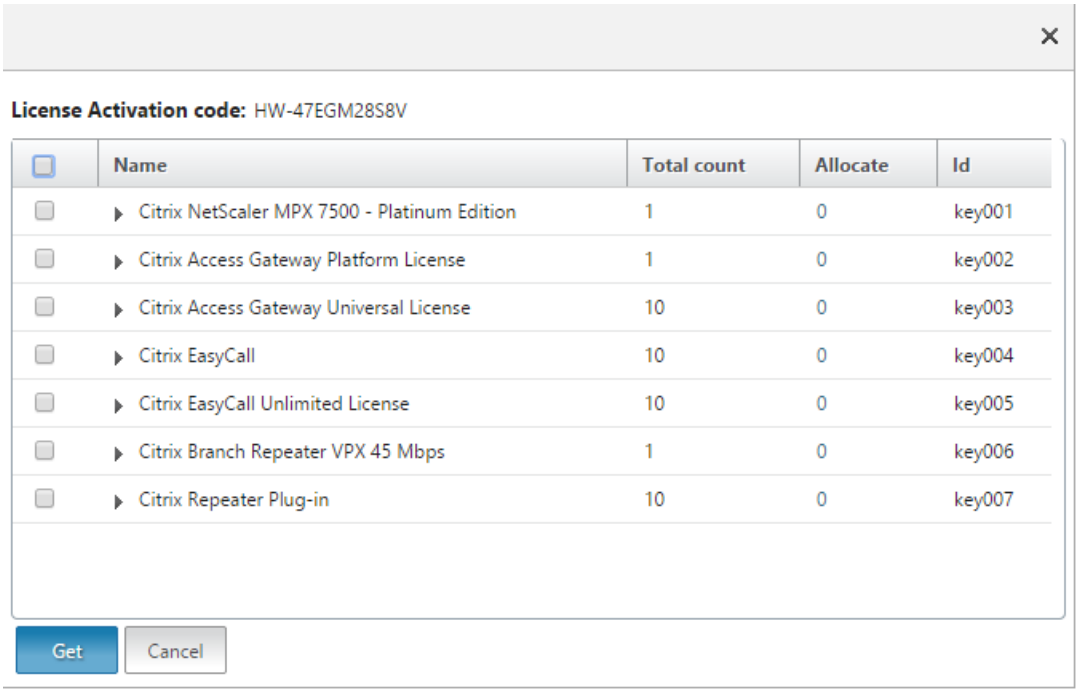
  Si no quiere configurar la conectividad a Internet en el dispositivo Citrix ADC, puede utilizar un servidor proxy. Marque la casilla de verificación **Conectar a través de un servidor proxy** y especifique la dirección IP y el puerto del servidor proxy.

5. Haga clic en **Obtener licencias**. En función de la opción seleccionada, aparece uno de los siguientes cuadros de diálogo.

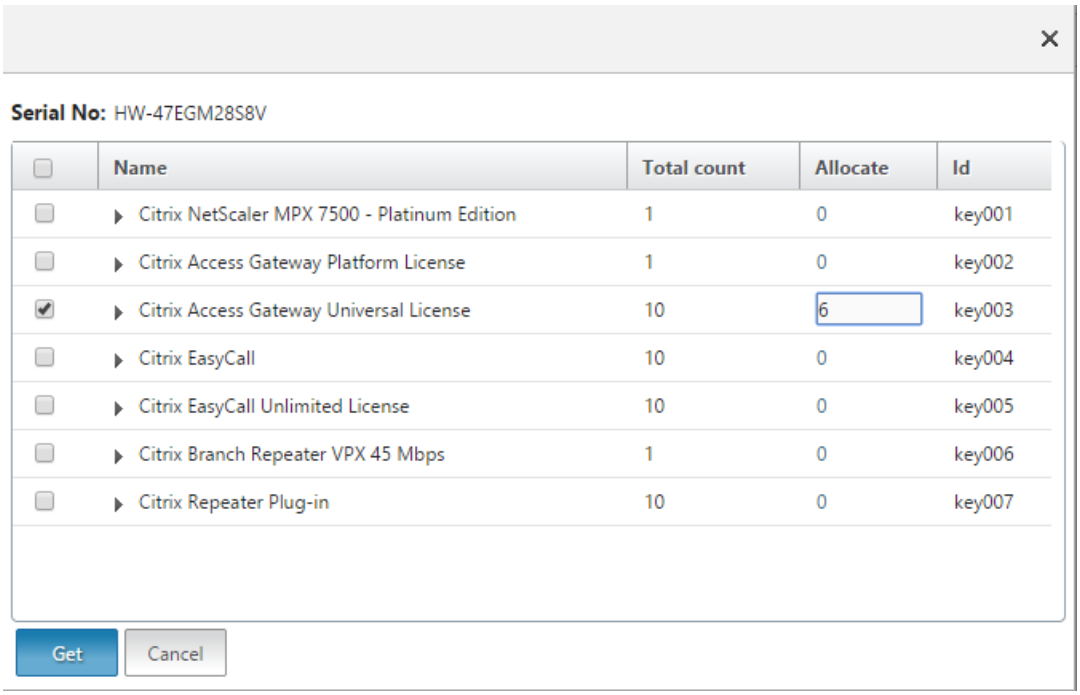
   - El siguiente cuadro de diálogo aparece si ha seleccionado Número de serie del hardware.



   - El siguiente cuadro de diálogo aparece si ha seleccionado el código de acceso de licencia.

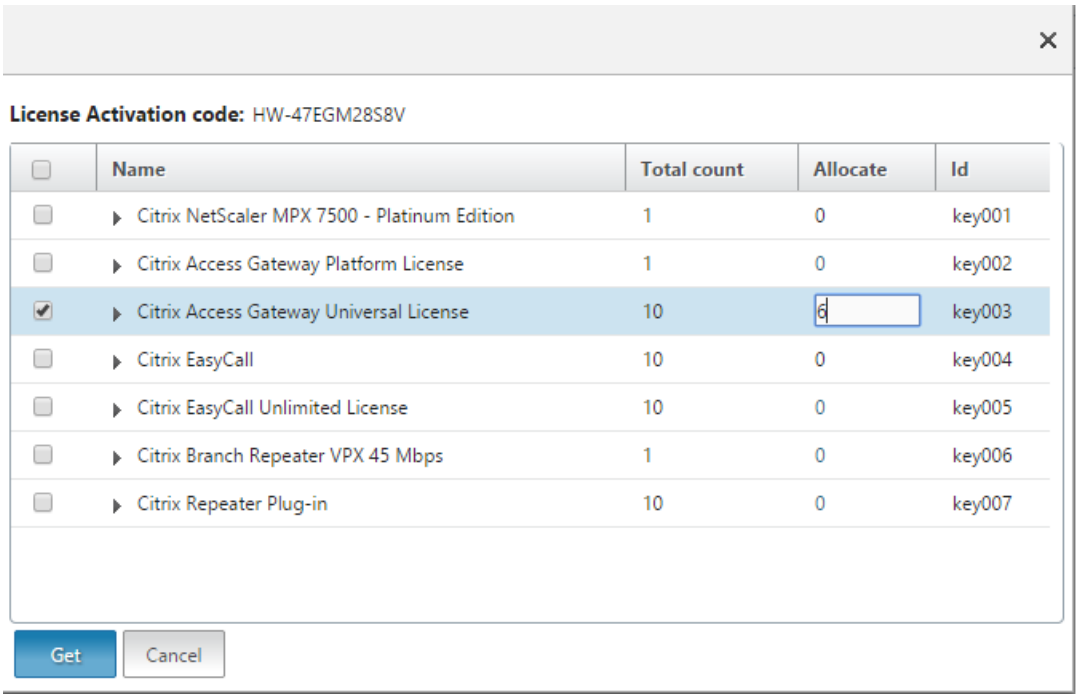


6. Seleccione el archivo de licencias que quiere utilizar para asignar las licencias.
7. En la columna **Asignar**, introduzca el número de licencias que se asignarán. Luego haga clic en **Obtener**.
   - Si ha seleccionado **Número de serie de hardware**, introduzca el número de licencias, como se muestra en la siguiente captura de pantalla.

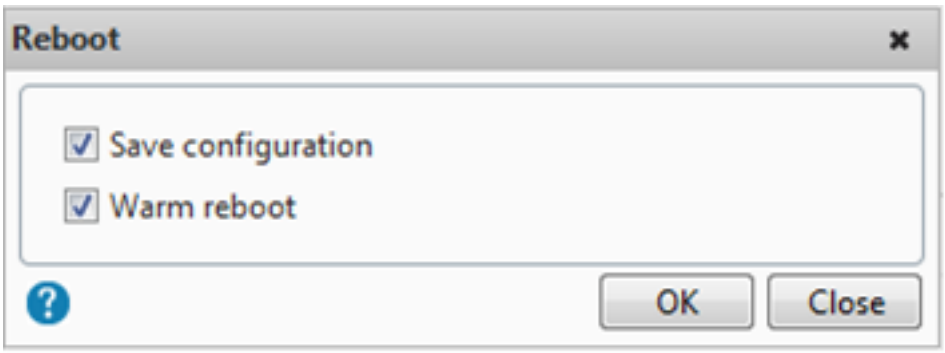


   - Si ha seleccionado el **código de acceso de licencia**, introduzca el número de licencias,

como se muestra en la siguiente captura de pantalla.



8. Haga clic en Reiniciar para que la licencia surta efecto.
9. En el cuadro de diálogo de reinicio, haga clic en **Aceptar** para continuar con los cambios o haga clic en **Cerrar** para cancelarlos.



Instalar una licencia

Si descargó el archivo de licencia en el equipo local accediendo al portal de licencias, debe cargar la licencia en el dispositivo.

Para instalar un archivo de licencia mediante la interfaz gráfica de usuario

1. En un explorador web, escriba la dirección IP del dispositivo Citrix ADC (por ejemplo, `http://192.168.100.1`).

2. En Nombre de usuario y Contraseña, introduzca las credenciales de administrador.
3. En la ficha **Configuración**, vaya a Licencias del sistema.
4. En el panel de detalles, haga clic en **Administrar licencias**.
5. Haga clic en **Agregar nueva licencia** y, a continuación, seleccione **Cargar archivos de licencias desde un equipo local**.
6. Haga clic en **Examinar**. Vaya a la ubicación de los archivos de licencias, seleccione el archivo de licencias y, a continuación, haga clic en **Abrir**.
7. Haga clic en Reiniciar para aplicar la licencia.
8. En el cuadro de diálogo de reinicio, haga clic en **Aceptar** para continuar con los cambios o haga clic en **Cerrar** para cancelarlos.

Para instalar las licencias mediante la CLI

1. Abra una **conexión SSH** con el dispositivo ADC mediante un cliente SSH, como PuTTY.
2. Inicie sesión en el dispositivo ADC con las credenciales de administrador.
3. Cambie al símbolo del shell, cree un subdirectorio de licencias en el directorio `nsconfig`, si no existe, y copie uno o varios archivos de licencia nuevos en este directorio.

   Ejemplo

```
login: nsroot
Password: nsroot
Last login: Mon Aug  4 03:37:27 2008 from 10.102.29.9
Done
> shell
Last login: Mon Aug  4 03:51:42 from 10.103.25.64
root@ns# mkdir /nsconfig/license
root@ns# cd /nsconfig/license
<!--NeedCopy-->
```

   Copie uno o varios archivos de licencia nuevos en este directorio.

> **Nota**
>
> El dispositivo Citrix ADC no solicita una opción de reinicio cuando utiliza la interfaz de línea de comandos para instalar las licencias. Ejecute el comando reboot -w para reiniciar el sistema en caliente o ejecute el comando restart para reiniciar el sistema normalmente.

Comprobar las funciones con licencia

Antes de utilizar una función, asegúrese de que su licencia sea compatible con la función.

Para comprobar las funciones con licencia mediante la CLI

1. Abra una **conexión SSH** con el dispositivo ADC mediante un cliente SSH, como PuTTY.
2. Inicie sesión en el dispositivo ADC con las credenciales de administrador.
3. En el símbolo del sistema, introduzca el comando sh ns license para mostrar las funciones admitidas por la licencia.

   Ejemplo

```
sh ns license
        License status:
                            Web Logging: YES
                        Surge Protection: YES
                          .......

                          Responder: YES
 Done
<!--NeedCopy-->
```

Para comprobar las funciones con licencia mediante la interfaz gráfica de usuario

1. En un explorador web, escriba la dirección IP del dispositivo ADC, como `http://192.168.100.1` .
2. En Nombre de usuario y Contraseña, introduzca las credenciales de administrador.
3. Proporcione el nombre de usuario y la contraseña y haga clic en **Iniciar sesión**.
4. En el panel de navegación, expanda **Sistema**y haga clic en **Licencias**. Verá una marca de verificación verde junto a las funciones con licencia.

Habilitar o inhabilitar una función

Al utilizar el dispositivo Citrix ADC por primera vez, debe habilitar una función para poder utilizarla. Si configura una función antes de activarla, aparece un mensaje de advertencia. La configuración se guarda pero solo se aplica después de habilitar la función.

Para habilitar una función mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para habilitar una función y verificar la configuración:

- enable feature <FeatureName>

- show feature

  Ejemplo

```
enable feature lb cs
done
 >show feature

        Feature                        Acronym
           Status
        -------                        -------
           ------
 1)     Web Logging                    WL                     OFF
 2)     Surge Protection               SP                     ON
 3)     Load Balancing                 LB                     ON
 4)     Content Switching              CS                     ON
 5)     Cache Redirection              CR                     ON
 .
 .
 .
 24)    NetScaler Push                 push                   OFF
 Done
<!--NeedCopy-->
```

  En el ejemplo se muestra cómo habilitar el equilibrio de carga (lb) y el cambio de contenido (cs).

  Si la clave de licencia no está disponible para una función concreta, aparece el siguiente mensaje de error para esa función:

  ERROR: funciones sin licencia

  Nota: Para habilitar una función opcional, debe tener una licencia específica de la función. Por ejemplo, ha adquirido e instalado la licencia de Citrix NetScaler Advanced Edition. Sin embargo, para habilitar la función Almacenamiento en caché integrado, debe comprar e instalar la licencia de AppCache.

Para inhabilitar una función mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para inhabilitar una función y verificar la configuración:

- disable feature <FeatureName>
- show feature

  Ejemplo

En el siguiente ejemplo se muestra cómo inhabilitar el equilibrio de carga (LB).

```
> disable feature lb
 Done
> show feature

        Feature                        Acronym
           Status
        -------                        -------
           ------
 1)     Web Logging                    WL                     OFF
 2)     Surge Protection               SP                     ON
 3)     Load Balancing                 LB                     OFF
 4)     Content Switching              CS                     ON
 .
 .
 .
 24)    NetScaler Push                 push                   OFF
 Done
>
<!--NeedCopy-->
```

Configurar alertas de caducidad de licencias de Citrix ADC

De forma predeterminada, aparece una alerta de GUI cuando la fecha de caducidad de la licencia de ADC es inferior o igual a 30 días.

Puede configurar el dispositivo Citrix ADC para que realice las siguientes operaciones de alerta durante un número específico de días antes de que caduque una licencia de Citrix ADC:

- Muestre un anuncio de alerta de caducidad de licencia en la GUI de Citrix ADC.
- Envíe capturas SNMP que contengan la información de caducidad de la licencia a intervalos regulares a los detectores de capturas configurados si la alarma SNMP “NS_LICENSE_EXPIRY” está habilitada.

Al caducar la licencia, el dispositivo Citrix ADC se reinicia automáticamente para revocar la licencia. Si un dispositivo Citrix ADC utiliza licencias de proveedores de servicios (CSP) de Citrix, el dispositivo no se reinicia automáticamente para revocar la licencia. Sin embargo, si el usuario reinicia el dispositivo, se reinicia sin licencia.

Para especificar el número de días para las alertas de caducidad de licencias de Citrix ADC mediante la CLI:
En el símbolo del sistema, escriba:

- **set license parameters** [-**tiempo de alerta de caducidad de licencia**]
- **parámetros de licencia sh**

Ejemplo:

```
> set licenseparameters -licenseexpiryalerttime 200
Done

> sh licenseparameters
...
    Licenseexpiryalerttime:  200
<!--NeedCopy-->
```

Para especificar el número de días para las alertas de caducidad de licencias de Citrix ADC mediante la GUI de Citrix ADC:

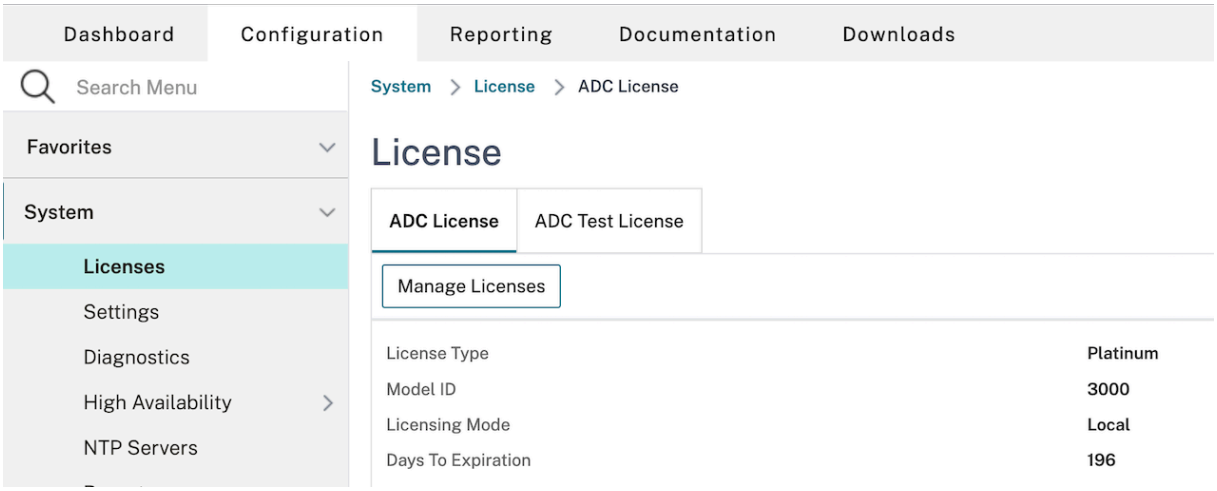
1. Vaya a **Configuración** > **Sistema** > **Licencias**.
2. En **Configuración de notificaciones**, haga clic en el botón modificar para especificar el número de días para las alertas de caducidad de licencias de Citrix ADC.

Comprobar información de caducidad de licencia

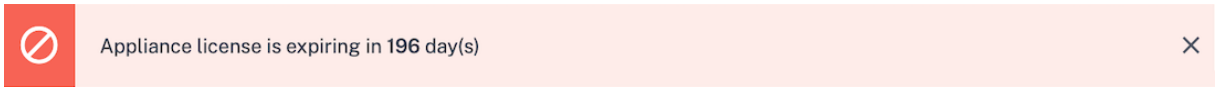
Puede comprobar la información de caducidad de la licencia de Citrix ADC a través de la GUI o la CLI.

Para comprobar la información de caducidad de licencias de Citrix ADC mediante la GUI:

Vaya a **Configuración > Sistema > Licencias**.



Aparece una alerta de GUI cuando la fecha de caducidad de la licencia de ADC es inferior o igual al número de días especificado para la alerta de caducidad de la licencia de Citrix ADC.



Para comprobar la información de caducidad de la licencia a través de CLI:

Escriba el comando “show ns license”.

```
> sh license
    License status:

    Web Logging: YES
    Surge Protection: YES

    Web Logging: YES
    Surge Protection: YES

    ...

Days to expiry: 196

Done
>
<!--NeedCopy-->
```

Actualizar una licencia

Puede actualizar un dispositivo Citrix ADC de una edición de familia a otra y de un rango de capacidad a otro adquiriendo una licencia de mayor capacidad.

Las actualizaciones son de dos tipos:

- Actualizaciones de edición: Estándar a Avanzado, Estándar a Premium y Avanzado a Premium. Las actualizaciones de edición deben estar dentro del mismo ancho de banda.
- Actualizaciones de capacidad: Puede actualizar de menor a mayor capacidad, tanto para vCPU como para ancho de banda. Las actualizaciones de capacidad solo se pueden realizar en la misma edición (Standard, Advanced o Premium).

Si quiere actualizar tanto la capacidad como la edición, actualice primero la capacidad, reinicie el dispositivo y, a continuación, actualice la edición.

Ejemplo: Para actualizar una licencia VPX 10 Mbps Standard Edition a VPX 200 Mbps Premium Edition, la actualización debe realizarse en dos pasos.

- Actualización VPX de 10 Mbps Standard Edition a 200 Mbps Standard Edition.

- Actualización VPX de 200 Mbps Standard Edition a 200 Mbps Premium Edition.

> Nota
>
> Puede utilizar Citrix Application Delivery Management (ADM) para crear un marco de licencias que contenga un ancho de banda común y un grupo de instancias. Para obtener información completa, consulte Capacidad agrupada de Citrix ADC.

Recursos conexos

- El sistema de licencias de Citrix
- Cómo asignar licencias Citrix ADC VPX

Gobierno de datos

March 9, 2022

¿Qué es la conexión de servicio Citrix ADM?

La conexión del servicio Citrix Application Delivery Management (ADM) es una función que permite la incorporación sin problemas de las instancias MPX, SDX y VPX de Citrix ADC y los dispositivos Citrix Gateway en el servicio Citrix ADM. Esta función permite que la instancia Citrix ADC o el dispositivo Citrix Gateway se conecten de forma automática y segura con el servicio Citrix ADM y le envíen datos del sistema, el uso y la telemetría. Con base en estos datos, obtiene información y recomendaciones para su infraestructura Citrix ADC en el servicio Citrix ADM.

Mediante el uso de la función de conexión del servicio Citrix ADM y la incorporación de las instancias Citrix ADC o los dispositivos Citrix Gateway al servicio Citrix ADM. También puede administrar todos los activos de Citrix ADC y Citrix Gateway, ya sean locales o en la nube. Además, se beneficia del acceso a un amplio conjunto de funciones de visibilidad que ayudan a identificar rápidamente los problemas de rendimiento, el uso elevado de recursos, los errores críticos, etc. El servicio Citrix ADM proporciona una amplia gama de capacidades para las instancias y aplicaciones de Citrix ADC. Para obtener más información sobre el servicio Citrix ADM, consulte Citrix Application Delivery Management Service

> **Importante**
>
> - El dispositivo Citrix Gateway también admite la función de conexión de servicio de Citrix ADM. Para mayor facilidad, el dispositivo Citrix Gateway no se llama explícitamente en las secciones consecutivas.

¿Qué es el servicio Citrix ADM?

El servicio Citrix ADM es una solución basada en la nube que le ayuda a administrar, supervisar, orquestar, automatizar y solucionar problemas de las instancias de Citrix ADC. También proporciona información analítica y recomendaciones basadas en aprendizaje automático sobre las instancias de Citrix ADC y sobre el estado, el rendimiento y la seguridad de las aplicaciones. Para obtener más información, consulte Descripción general del servicio Citrix ADM.

¿Cómo se habilita la conexión al servicio Citrix ADM?

La conexión del servicio Citrix ADM está habilitada de forma predeterminada, después de instalar o actualizar Citrix ADC o Gateway a la versión 13.0 compilación 61.xx y superior.

¿Qué datos se capturan mediante Citrix ADM service connect?

Los siguientes detalles se capturan mediante Citrix ADM service connect:

- **Detalles de Citrix ADC**
  - Identificación de serie
  - ID de serie codificada
  - ID de host
  - UUID
  - Dirección IP de administración
  - Nombre de host
  - Versión
  - Tipo de construcción
  - Build
  - Tipo de licencia
  - Hipervisor
  - Tipo de implementación (autónoma/HA)
  - Tipo de plataforma
  - Descripción de la plataforma
  - ID del sistema
  - Modos habilitados en ADC
  - Funciones habilitadas en ADC
- **Información de licencia**
  - Funciones con licencia en Citrix ADC
  - Número de licencia
- **Métricas de uso clave**

  - Fecha y hora del sistema
  - Porcentaje de uso de CPU
  - Porcentaje de CPU de gestión
  - Rendimiento
  - Nuevas sesiones SSL
  - Rendimiento de cifrado SSL
  - Rendimiento de descifrado de SSL
  - Tiempo de actividad del sistema

- **Configuración**

  - archivo ns.conf

    > **Nota**
    >
    > Antes de que la conexión del servicio Citrix ADM envíe el archivo `ns.conf` desde el dispositivo Citrix ADC al servicio Citrix ADM, anonimiza las contraseñas cifradas o con hash. La conexión del servicio Citrix ADM comprueba los parámetros `-encrypted` o `-passcrypt` y reemplaza el valor cifrado o hash asociado por `XXXX`. El servicio Citrix ADM se conecta a continuación codifica y comprime el archivo `ns.conf` y lo envía al dispositivo de punto final del servicio Citrix ADM.

- **Detalles de errores críticos**

  - Fallos del disco duro
  - Fallos en la tarjeta SSL
  - Fallos en la unidad de fuente de alimentación (PSU)
  - Fallo de la unidad flash
  - Reinicio en caliente
  - Uso sostenido de memoria superior al 90% o pérdida de memoria
  - Cae el límite de velocidad

- **Uso de herramientas de automatización NITRO**

  - Uso de herramientas de automatización como los SDK de Ansible, Terraform o NITRO.

- **Detalles de diagnóstico**

  > Nota:
  >
  > La herramienta de diagnóstico ADM utiliza los siguientes detalles de diagnóstico. Para obtener más información, consulte el tema Herramienta de diagnóstico en Citrix ADM.

  - Estado de CLI de ADC
  - Estado DNS de ADC
  - estado de la conexión de red al extremo de ADM “adm.cloud.com”
  - estado de la conexión de red al extremo de ADM “agent.adm.cloud.com”

- estado de la conexión de red al servicio de confianza de ADM “trust.citrixnetworkapi.net”
- estado de la conexión de red al sitio de descarga de ADM “download.citrixnetworkapi.net”

¿Cómo se utilizan los datos?

Al recopilar los datos, Citrix puede proporcionarle información oportuna y detallada sobre sus instalaciones de Citrix ADC, que incluyen lo siguiente:

- **Métricas clave**. Detalles de las métricas clave sobre CPU, memoria, rendimiento, rendimiento SSL y comportamiento anómalo destacado en instancias de Citrix ADC.
- **Errores críticos**. Cualquier error crítico que pudiera haberse producido en las instancias de Citrix ADC.
- **Asesoramiento de implementación**. Identifique las instancias de Citrix ADC que se implementan en modo independiente pero que tienen un alto rendimiento y son vulnerables a un único punto de falla.
- **Herramienta de diagnóstico**. Cuando incorpora una instancia de ADC en Citrix ADM, es posible que experimente algunos problemas que impidan que la instancia de ADC se incorpore correctamente. Para solucionar los problemas, puede utilizar manualmente la herramienta de diagnóstico o ver la información de diagnóstico en la GUI de ADM. Para obtener más información, consulte Herramienta de diagnóstico.

¿Cuánto tiempo se conservan los datos recopilados?

Los datos recopilados se conservan durante no más de 13 meses.

Si decide terminar el uso del servicio inhabilitando la función de conexión del servicio de Citrix ADM de Citrix ADC, todos los datos recopilados anteriormente se eliminarán después de un período de 30 días.

¿Dónde se almacenan los datos y qué tan seguros son?

Todos los datos recopilados por Citrix ADM service connect se almacenan en una de las tres regiones: Estados Unidos, Unión Europea y Australia y Nueva Zelanda (ANZ). Para obtener más información, consulte Consideraciones geográficas.

Los datos se almacenan de forma segura con estricto aislamiento de arrendatarios en la capa de base de datos.

¿Cómo inhabilitar la conexión del servicio Citrix ADM?

Si quiere inhabilitar la recopilación de datos mediante la conexión del servicio Citrix ADM, consulte Cómo habilitar y inhabilitar la conexión del servicio Citrix ADM.

Introducción a Citrix ADM Service connect para dispositivos Citrix ADC

February 19, 2022

El servicio Citrix ADM es una solución basada en la nube que le ayuda a administrar, supervisar, orquestar, automatizar y solucionar problemas de las instancias de Citrix ADC. También proporciona información analítica y recomendaciones basadas en aprendizaje automático para el estado, el rendimiento y la seguridad de sus aplicaciones. Para obtener más información, consulte Citrix Application Delivery Management Service.

El servicio de conexión de Citrix Application Delivery Management (ADM) es una función que permite la integración perfecta de instancias de Citrix ADC en el servicio de Citrix ADM. Esta función ayuda a las instancias de Citrix ADC y al servicio Citrix ADM a funcionar como una solución integral, que ofrece a los clientes múltiples beneficios.

La función de conexión de servicio de Citrix ADM permite que la instancia de Citrix ADC se conecte automáticamente con el servicio de Citrix ADM y le envíe datos de sistema, uso y telemetría. En base a estos datos, el servicio Citrix ADM le proporciona información y recomendaciones sobre su infraestructura Citrix ADC y Gateway, como la siguiente:

- Información sobre asesoramiento de seguridad que destaca sus dispositivos ADC vulnerables.
- Información de asesoramiento de actualización que destaca los dispositivos ADC que han alcanzado o están a punto de llegar al final del mantenimiento y al final de su vida útil.
- Identificación rápida de problemas de rendimiento, uso elevado de recursos y errores críticos.

Para aprovechar la potencia del servicio Citrix ADM, puede optar por incorporarse las instancias de Citrix ADC al servicio de Citrix ADM. El proceso de incorporación utiliza ADM service connect y hace que la experiencia sea fluida y rápida para usted.

> **Puntos que tener en cuenta**
>
> - Citrix ADM Service connect ya está disponible en instancias de Citrix ADC MPX, SDX y VPX y en dispositivos Citrix Gateway.
> - La iniciativa del servicio Citrix ADM que utiliza esta función de conexión de servicio Citrix ADM es la incorporación de baja pulsación basada en conexión de servicio ADM. Para obtener más información, consulte Incorporación con poco toque de instancias Citrix ADC mediante Citrix ADM service connect.
> - Si la conexión del servicio ADM está habilitada en una instancia ADC, ciertos detalles de diagnóstico se envían automáticamente al servicio ADM.

Para obtener más información, consulte Gobernanza de datos.

> **Importante**
>
> Citrix ADM service connect no recopila los datos del sondeo y no puede ayudar a incorporar el dispositivo ADC al servicio ADM si se cumplen las siguientes condiciones:
>
> - `NSinternal` cuenta de usuario está inhabilitada.
> - La clave pública SSH no está configurada.
>
> Para superar el caso anterior, Citrix recomienda seguir cualquiera de las siguientes opciones:
>
> - Habilite la cuenta de usuario `internaluser` mediante `set ns param -internaluserlogin ENABLED`.
> - Configure la autenticación de clave pública. Para obtener más información, consulte Acceso a un dispositivo Citrix ADC mediante claves SSH y sin contraseña.

¿Cómo conecta el servicio Citrix ADM la asistencia con el servicio Citrix ADM?

A continuación se muestra un flujo de trabajo de alto nivel sobre cómo la función de conexión de servicio de Citrix ADM en Citrix ADC interactúa con el servicio Citrix ADM.

1. La función de conexión del servicio Citrix ADM en el dispositivo Citrix ADC se conecta automáticamente con el servicio Citrix ADM mediante una solicitud de sonda periódica.
2. Esta solicitud tiene datos de sistema, uso y telemetría, mediante los cuales el servicio Citrix ADM le brinda información y recomendaciones sobre su infraestructura Citrix ADC. Por ejemplo, identificación rápida de problemas de rendimiento, uso elevado de recursos y errores críticos.
3. Puede ver los conocimientos y las recomendaciones y decidir incorporar sus instancias de ADC al servicio Citrix ADM para comenzar a administrar sus instancias de Citrix ADC.
4. Cuando decide incorporar, la función de conexión del servicio Citrix ADM ayuda a completar la incorporación sin problemas.

¿En qué versiones de Citrix ADC se admite la conexión del servicio Citrix ADM?

La conexión del servicio Citrix ADM se admite en todas las plataformas Citrix ADC y en todos los modelos de dispositivos (MPX, VPX y SDX). A partir de la versión 13.0 compilación 61.xx de Citrix ADC, la conexión al servicio Citrix ADM está habilitada de forma predeterminada para los dispositivos Citrix ADC.

¿Cómo habilitar la conexión del servicio Citrix ADM?

Si ya es cliente de Citrix ADC y actualiza a Citrix ADC versión 13.0 build 61.xx, la conexión del servicio Citrix ADM está habilitada de forma predeterminada como parte del proceso de actualización.

Si es un cliente nuevo de Citrix ADC, al instalar Citrix ADC versión 13.0 compilación 61.xx, la conexión del servicio Citrix ADM está habilitada de forma predeterminada como parte del proceso de instalación.

> **Nota**
>
> A diferencia de los nuevos dispositivos Citrix ADC, los dispositivos Citrix ADC existentes encuentran la ruta a través de Citrix Insight Service (CIS) o Call Home.

¿Cómo habilitar y inhabilitar la conexión del servicio Citrix ADM?

Puede habilitar y inhabilitar la conexión del servicio Citrix ADM desde los métodos CLI, GUI o API de NITRO.

Uso de CLI

Para habilitar la conexión del servicio Citrix ADM mediante la CLI

En el símbolo del sistema, escriba:

```
set adm parameter -admserviceconnect ENABLED
```

Para inhabilitar la conexión del servicio Citrix ADM mediante la CLI

En el símbolo del sistema, escriba:

```
set adm parameter -admserviceconnect DISABLED
```

> **Importante**
>
> Si Citrix ADC se encuentra en la versión 13.0 compilación 61.xx, el nombre del parámetro para habilitar o inhabilitar la conexión del servicio Citrix ADC es “autoconnect”. Por ejemplo, para habilitar la conexión de servicio, utilice el comando `set adm parameter -autoconnect ENABLED`.

Uso de la GUI

Para inhabilitar la conexión del servicio Citrix ADM mediante la GUI de Citrix ADC

1. En un explorador web, escriba la dirección IP del dispositivo Citrix ADC (por ejemplo, http://192.0.2.10).
2. En **Nombre de usuario** y **Contraseña**, introduzca las credenciales de administrador.

3. Vaya a **Sistema > Configuración > Configurar parámetros de ADM**.
4. En la página **Configurar parámetros de ADM**, desactive el cuadro de diálogo **Habilitar conexión del servicio Citrix ADM** y haga clic en **Aceptar**.

Uso de la API de NITRO

Puede inhabilitar la conexión del servicio Citrix ADM mediante el comando **NITRO**.

- En Citrix ADC versión 13.0 compilación 61.xx, puede habilitar o inhabilitar la conexión del servicio Citrix ADM mediante el siguiente comando:
  - `curl -X PUT -H "Content-Type:application/json"http://192.0.2.10/nitro/v1/config/admparameter> -d '{ "admparameter":{ "autoconnect":"enabled" } } ' -u nsroot:Test@1`
- A partir de Citrix ADC versión 13.0 compilación 64.xx, el nombre del parámetro "autoconnect" cambia el nombre a `admserviceconnect`. Puede inhabilitar la conexión del servicio Citrix ADM mediante el siguiente comando:
  - `curl -X PUT -H "Content-Type:application/json" http://192.0.2.10/nitro/v1/config/admparameter -d '{ "admparameter":{ "admserviceconnect":"disabled" } } ' -u nsroot:Test@1`

Herramienta de diagnóstico

Cuando incorpora una instancia de ADC en Citrix ADM, es posible que experimente algunos problemas que impidan que la instancia de ADC se incorpore correctamente. Para solucionar los problemas, puede utilizar manualmente la herramienta de diagnóstico o ver la información de diagnóstico en la GUI de ADM.

- Para obtener más información sobre los detalles capturados mediante la conexión del servicio ADM, consulte Gobierno de datos.
- Para obtener más información sobre la herramienta de diagnóstico, consulte Herramienta de diagnóstico.

Comportamiento del agente integrado de Citrix ADM

A partir de Citrix ADC versión 13.0 compilación 61.xx y superior, el agente integrado de Citrix ADM disponible en instancias de Citrix ADC se comunica con el servicio ADM. Se comunica sin necesidad de inicialización manual en la instancia de ADC respectiva. Después de establecer la comunicación con el servicio ADM, el agente integrado se mantiene siempre verde actualizándose automáticamente a la última versión de software regularmente.

Anteriormente, tenía que inicializar el agente integrado en las instancias de ADC, mediante comandos `mastools`, para establecer la comunicación con el servicio ADM y para realizar actualizaciones automáticas periódicas.
Para obtener más información, consulte Configurar el agente integrado de ADC para administrar instancias.

Referencias

Para obtener más información acerca de Citrix ADM Service connect, consulte los siguientes temas:

- Gobierno de datos: gobernanza de datos.
- Servicio Citrix ADM: Citrix Application Delivery Management Service.

Actualización y degradación de un dispositivo Citrix ADC

January 31, 2022

Citrix ADC 13.1 ofrece funciones nuevas y actualizadas con mayor funcionalidad. En las notas de la versión que acompañan al anuncio de la versión se incluye una lista completa de mejoras. Lea el documento de notas de la versión antes de actualizar el software.

En esta sección se proporciona información sobre la **actualización y la degradación del firmware de un dispositivo Citrix ADC** (MPX y VPX) **mediante la GUI o CLI de Citrix ADC**.

También puede **utilizar Citrix ADM para actualizar un dispositivo Citrix ADC**. Para obtener más información, consulte:

- 10 formas en que el servicio Citrix ADM admite actualizaciones más sencillas de Citrix ADC
- Usar el servicio Citrix ADM para actualizar instancias de Citrix ADC
- Utilice el software Citrix ADM para actualizar las instancias de Citrix ADC

Para obtener información sobre **la actualización de un dispositivo Citrix ADC SDX**, consulteActualización de paquete único.

> **Nota**
>
> A partir de la versión 13.1 de Citrix ADC, las funciones y funciones clásicas basadas en directivas obsoletas se quitan del dispositivo Citrix ADC. Para obtener más información, consulte la tabla Preguntas frecuentes sobre la desuso de directivas clásicas .

Antes de comenzar

July 8, 2022

Antes de iniciar el proceso de actualización o degradación, asegúrese de comprobar lo siguiente:

- Tiempo asignado para actualizar los dispositivos Citrix ADC. Siga el procedimiento de control de cambios de su organización. Asigne el doble de tiempo para realizar las actualizaciones. Asigne tiempo suficiente para actualizar cada dispositivo Citrix ADC.
- Evalúe el acuerdo de asistencia de su organización. Documente el número de serie del dispositivo, el acuerdo de asistencia y los detalles de los contactos para obtener asistencia de la asistencia técnica de Citrix o del socio autorizado de Citrix.
- El marco de licencias y los tipos de licencias. La actualización de una edición de software puede requerir licencias nuevas, como:
  - actualizar de la edición estándar a la edición avanzada, o
  - la edición estándar de la edición Premium, o
  - la edición avanzada de la edición Premium.

  Las licencias de Citrix ADC existentes continúan funcionando al actualizar a la versión 13.1. Para obtener más información, consulte Licencias
- Compruebe si hay comandos, parámetros y OID SNMP nuevos y obsoletos.
- Compruebe la tabla de compatibilidad de hardware y software Citrix ADC MPX.
- Si la página de inicio de sesión de Citrix ADC Gateway está personalizada, asegúrese de que el tema de la interfaz de usuario está configurado como predeterminado.
- Si va a actualizar LOM, consulte la página Actualización del firmware de LOM.
- Descargue el firmware de Citrix ADC de las descargas de Citrix ADC. Para obtener los pasos detallados para descargar el firmware de Citrix ADC, consulte Descargar un paquete de versión de Citrix ADC.
- Realízate los archivos. Realice una copia de seguridad del archivo de configuración, archivo de personalización, certificados, scripts de supervisión, archivos de licencias, etc. manualmente o consulte la siguiente documentación para realizar copias de seguridad mediante la CLI o GUI de Citrix ADC - Copia de seguridad y restauración.
  - Consulte la lista siguiente para obtener más archivos personalizados comunes para realizar copias de seguridad.
    * `/nsconfig/monitors/*.pl`
    * `/nsconfig/rc.netscaler`

  - Cree una copia de reserva de la carpeta de personalización. Esto suele estar por debajo /`var`/`customizations`. Un ejemplo de personalización es una página de inicio de sesión con un logotipo. Una vez copiada la carpeta de personalizaciones, debe eliminarla del dispositivo Citrix ADC antes de actualizar el dispositivo. La actualización con la personalización implementada podría ocasionar algunos problemas.

    > **Importante:**
    > Citrix recomienda encarecidamente revisar los procedimientos de copia de seguridad anteriores. Tenga un plan de acción en caso de que la actualización no se complete en el dispositivo Citrix ADC.

- Compruebe que hay espacio suficiente en el directorio /var y /flash para el dispositivo Citrix ADC antes de realizar la actualización. El /var requiere 5 GB de espacio libre (1 GB para el paquete de actualización y 4 GB para el proceso de actualización)
  /flash requiere espacio suficiente para copiar sobre el nuevo kernel, que varía entre 140 MB y 160 MB aproximadamente, asegúrese de que haya al menos 250 MB de espacio libre disponible.
  Para obtener más información sobre cómo liberar espacio en disco en /var, consulte Cómo liberar espacio en el directorio /var para problemas de registro con un dispositivo Citrix ADC.
  Para obtener más información sobre cómo borrar los espacios en disco de /flash, consulte, https://support.citrix.com/article/CTX133587.
- Validar la integridad del dispositivo Citrix ADC. Si tiene un dispositivo de hardware Citrix ADC, Citrix recomienda encarecidamente ejecutar `fsck` para realizar una comprobación de disco y validar la integridad del disco duro Citrix ADC. En caso de error, restablezca la unidad de disco duro y repita el comando de comprobación del disco. Si vuelve a aparecer el mensaje de error, póngase en contacto con la asistencia técnica de Citrix para investigar más a fondo el problema.
  - Valide la integridad del disco duro mediante un comando fsck. Para obtener más información, consulte CTX122845.
  - Valide la integridad de un dispositivo Citrix ADC mediante los archivos de paquetes de diagnóstico y carga de los registros en Citrix Insight Service para su análisis. Para obtener más información, consulte Cómo recopilar un paquete de asistencia técnica.
- Consulte la tabla de compatibilidad de Citrix ADC VPX y las directrices de uso.
- Consulta la sección Preguntas frecuentes.
- Es una práctica recomendada actualizar a una versión principal a la vez. No actualice directamente a la última versión.

  Por ejemplo, si el dispositivo Citrix ADC está en la versión 12.1 y quiere actualizar a la versión 13.1, primero debe actualizar el dispositivo a la versión 13.0 y, a continuación, a la versión 13.1.
- Compruebe los procedimientos de actualización con un entorno de prueba.

Para obtener más información acerca de los requisitos previos para actualizar o revertir la versión del dispositivo Citrix ADC, consulte estos artículos de asistencia técnica:

- CTX220371: Debe leer artículos antes y después de actualizar Citrix ADC

Consideraciones sobre la actualización de los archivos de configuración personalizados en el directorio /etc

July 27, 2022

Si ha modificado algún archivo de configuración del directorio `/etc` y lo ha copiado en el directorio `/nsconfig`, para mantener la persistencia, el dispositivo Citrix ADC crea un enlace simbólico en `/etc` que apunta al archivo de `/nsconfig`.

Por ejemplo: `/etc/httpd.conf -> /nsconfig /httpd.conf`

Un paquete de versión puede contener su propia versión de los archivos de configuración del directorio `/etc`. Estos archivos de configuración incluyen actualizaciones importantes que se requieren para que el dispositivo Citrix ADC funcione correctamente. La actualización de un dispositivo Citrix ADC a una versión reemplaza los archivos de configuración del directorio `/etc` por los archivos de configuración que contienen las actualizaciones de la versión.

Considere un ejemplo de un archivo de configuración personalizado, `example.conf`, que está presente en el directorio `/etc`. El archivo `example.conf` se copia en el directorio `/nsconfig` para mantener la persistencia. El dispositivo Citrix ADC crea un enlace simbólico que `/etc` apunta al archivo en `/nsconfig`: `/etc/example.conf -> / nsconfig /example.conf`

Además, un paquete de versión incluye su propia versión de `example.conf`, que contiene actualizaciones importantes. Se observa el siguiente comportamiento al actualizar el dispositivo Citrix ADC a la versión:

Como el enlace simbólico `/etc/example.conf` ya está presente, el dispositivo Citrix ADC no coloca la copia del paquete de versión de `example.conf` en el directorio `/etc` durante el proceso de actualización.

Como la copia del paquete de versión de `example.conf` contiene actualizaciones importantes, su ausencia en el directorio `/etc` puede provocar que el dispositivo Citrix ADC falle o no funcione correctamente.

Pasos para conservar los cambios de actualización y la personalización

Para asegurarse de que no se pierdan ni las actualizaciones de la versión ni las personalizaciones, lleve a cabo los siguientes pasos:

- Pasos previos a la actualización:
  - Realizar una copia de seguridad del archivo personalizado antes de la actualización
  - Eliminar la persistencia del archivo personalizado antes de la actualización
- Pasos posteriores a la actualización:
  - Aplicar personalizaciones al archivo actualizado y agregar persistencia tras la actualización

    > **Importante:**
    > NO sustituya directamente el archivo personalizado de la carpeta `/etc`. Al reemplazar directamente un archivo `/etc` por el archivo personalizado de copia de seguridad, se eliminan las actualizaciones de versión agregadas al archivo durante el proceso de actualización.

Realizar una copia de seguridad del archivo personalizado antes de la actualización

Realice una copia de seguridad de los archivos personalizados presentes en el directorio `/nsconfig` antes de actualizar el dispositivo.

Cree un directorio `/var/nsconfig_backup` y mueva los archivos personalizados a este directorio. Es decir, mueva los archivos que haya modificado en el directorio `/etc` y que haya copiado en `/nsconfig` ejecutando el siguiente comando en el intérprete de comandos:

```
mv /nsconfig/<filename> /var/nsconfig_backup/
<!--NeedCopy-->
```

Ejemplo:

```
mv /nsconfig/httpd.conf /var/nsconfig_backup/
<!--NeedCopy-->
```

Eliminar la persistencia del archivo personalizado antes de la actualización

Elimine los enlaces simbólicos `/etc` que apuntan a los archivos `/nsconfig` antes de actualizar el dispositivo.

1. Compruebe los enlaces simbólicos existentes en el directorio `/etc` ejecutando el siguiente comando en el símbolo del shell:

```
ls -la /etc
```



```
2 <!--NeedCopy-->
```

2. Para eliminar un enlace simbólico /etc que apunte a un archivo /nsconfig, ejecuta el siguiente comando en el símbolo del shell:

```
1 unlink /etc/<filename>
2 <!--NeedCopy-->
```

Ejemplo:

```
1 unlink /etc/httpd.conf
2 <!--NeedCopy-->
```

3. Verifique que el enlace simbólico se haya eliminado ejecutando el siguiente comando en el indicador de shell:

```
1 cat /etc/<filename>
2 <!--NeedCopy-->
```

Ejemplo:

```
1 cat /etc/httpd.conf
2 <!--NeedCopy-->
```

Este comando no muestra ningún contenido si se quita el enlace simbólico.

Aplicar personalizaciones al archivo actualizado y agregar persistencia tras la actualización

Si ha realizado una copia de seguridad de cualquier archivo de configuración /nsconfig modificado en /var/nsconfig_backup, haga lo siguiente después de actualizar el dispositivo:

1. Compare el archivo presente en los directorios /var/nsconfig_backup y /etc. Agregue manualmente los cambios correspondientes al archivo /etc que ya contiene las actualizaciones de la versión.

> **Importante:**
>
> Al reemplazar directamente el archivo `/etc` por el archivo `/var/nsconfig_backup`, se eliminarán las actualizaciones de versión agregadas al archivo durante el proceso de actualización. Esta eliminación de actualizaciones puede provocar que las funcionalidades relacionadas de Citrix ADC fallen o no funcionen correctamente.

2. Para mantener la persistencia, copie el archivo actualizado presente en el directorio `/etc` en el directorio `/nsconfig` ejecutando el siguiente comando en el símbolo del shell:

```
cp /etc/<filename> /nsconfig/
<!--NeedCopy-->
```

Ejemplo:

```
cp /etc/httpd.conf /nsconfig/
<!--NeedCopy-->
```

3. Repita los dos pasos anteriores para cada archivo personalizado presente en el directorio `/var/nsconfig_backup`.
4. Reinicie el dispositivo para aplicar los cambios.

Consideraciones de actualización: Configuración SNMP

January 12, 2021

El parámetro de tiempo de espera para una alarma SNMP es una opción interna que no afecta a la configuración de la alarma.

El parámetro Timeout puede aparecer en las configuraciones de alarma SNMP en la configuración en ejecución (sh running) y la configuración guardada (ns.conf) incluso si no ha realizado ningún cambio en estas configuraciones de alarma SNMP.

Al actualizar a una compilación de versión con la corrección del problema de configuración de tiempo de espera, las configuraciones SNMP se restablecen erróneamente a los valores predeterminados.

Las siguientes alarmas SNMP (si están configuradas) se ven afectadas durante una actualización:

- APPFW-BUFFER-DESBORDAMIENTO
- APPFW-COOKIE
- APPFW-CSRF-TAG

- APPFW-DENY-URL
- CONSISTENCIA DE CAMPO APPFW-
- FORMATO APPFW-FIELD-
- APPFW-POLICY-HIT
- ENCABEZADO APPFW-REFERER-
- APPFW-SAFE-COMMERCE
- APPFW-SAFE-OBJECT
- APPFW-SQL
- APPFW-START-URL
- APPFW-VIOLATIONS-TYPE
- APPFW-XML-ADJUNTO
- APPFW-XML-DOS
- APPFW-XML-SCHEMA-COMPILAR
- APPFW-XML-SOAP-FAULT
- APPFW-XML-SQL
- VALIDACIÓN APPFW-XML-
- APPFW-XML-WSI
- APPFW-XML-XSS
- APPFW-XSS
- CLUSTER-BACKPLANE-HB-FALTA
- CLUSTER-NODO-SALUD
- CLUSTER-NODO-QUÓRUM
- DISCORDANCIA DE VERSIÓN-CLÚSTER
- COMPACT-FLASH-ERRORS
- CONFIG-CHANGE
- CONFIG-SAVE
- HA-MAL-SECUNDARIO-ESTADO
- HA-NO-LATIDOS
- FALLO HA-SYNC-
- HA-VERSIÓN-DISCORDANCIA
- HARD-DISK-DRIVE-ERRORS
- HA-STATE-CHANGE
- HA-PEGAJO-PRIMARIO
- ERROR DE ASIGNACIÓN DE PUERTO
- SINFLOOD

Estas configuraciones de alarmas SNMP se ven afectadas al actualizar Citrix ADC a las versiones siguientes:

- Versión 11.1 compilación 61.2 o posterior
- Versión 12.0 compilación 61.0 o posterior

- Versión 12.1 compilación 30.1 o posterior
- Versión 13.0 compilación 51.4 o posterior

Ejemplo

Consideremos un ejemplo de alarma SNMP CLUSTER-NODE-HEALTH.

```
CLUSTER-NODE-HEALTH SNMP alarm is set up by using the Citrix ADC
    command line:

> set snmp alarm CLUSTER-NODE-HEALTH -time 111 -state DISABLED -
    severity Major

> save config
<!--NeedCopy-->
```

Esta configuración de alarma SNMP aparece en el archivo de configuración guardado (`ns.conf`) como:

```
set snmp alarm CLUSTER-NODE-HEALTH -time 111 -state DISABLED -severity
    Major -timeout 86400

<!--NeedCopy-->
```

Durante una actualización a cualquiera de las versiones de versión mencionadas anteriormente, aparece el siguiente error en el archivo ns.log:

```
May 23 09:14:46 <local0.err> ns nsconfigd: __init_config_filter(): (
    null) line 0: No such argument [-timeout]>> set snmp alarm CLUSTER-
    NODE-HEALTH -time 111 -state DISABLED -severity Major -timeout
    86400.
<!--NeedCopy-->
```

Después de la actualización, las configuraciones de alarma SNMP se restablecen a los valores predeterminados.

Solución temporal

Ponga en marcha alguna de las siguientes soluciones alternativas:

- Antes de la actualización, quite la configuración de tiempo de espera de las configuraciones SNMP en el archivo de configuración guardado (ns.conf).
- Después de la actualización, vuelva a configurar las alarmas SNMP sin el parámetro timeout.

Descargue un paquete de versión de Citrix ADC

August 20, 2021

Complete los siguientes pasos para descargar un paquete de versión de Citrix ADC:

1. Abra la página Descargas de Citrix ADC en un explorador web.
2. En la página Descargas de Citrix ADC, expanda la **versión de Citrix ADC** a la que quiere actualizar.
3. Expanda una de las categorías adecuadas y haga clic en el vínculo de compilación de Citrix ADC. Por ejemplo, para descargar una versión del firmware de Citrix ADC, expanda **Firmware** y haga clic en la compilación de Citrix ADC que quiere descargar.
4. En la página de compilación de Citrix ADC seleccionada, expanda la sección **Generar**, haga clic en **Descargar archivo** para descargar el paquete de compilación de Citrix ADC.

> **Nota:**
> La suma de comprobación se proporciona para asegurarse de que coincide el paquete de compilación descargado con el paquete real que está alojado en el sitio web. Checksum es una comprobación importante para asegurarse de que tiene los bits correctos.

Actualizar un dispositivo independiente de Citrix ADC

July 27, 2022

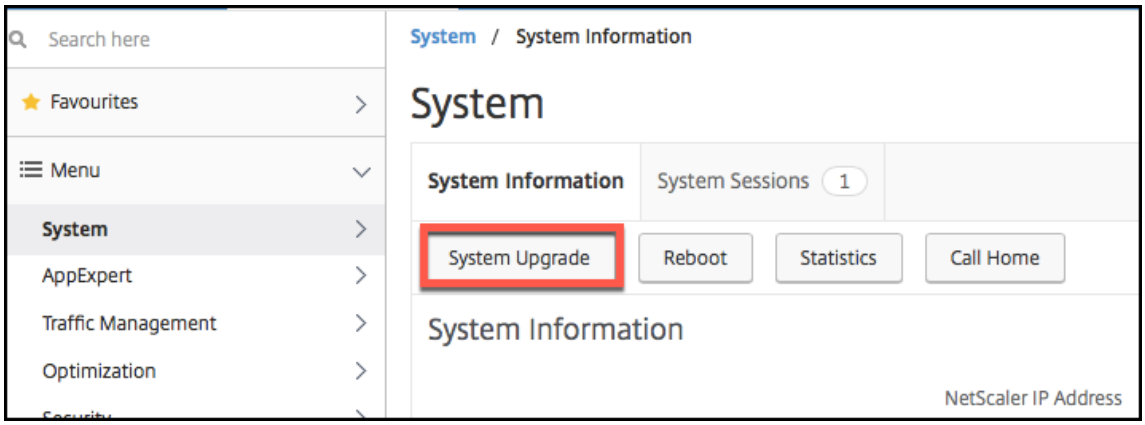
Antes de actualizar el software del sistema, asegúrese de leer la sección Antes de comenzar y completar los requisitos previos, tales como hacer una copia de seguridad de los archivos necesarios y descargar el firmware de Citrix ADC.

Actualizar un dispositivo independiente de Citrix ADC mediante la interfaz gráfica de usuario

Siga estos pasos para actualizar un Citrix ADC independiente a la versión 13.1 mediante la GUI.

1. En un explorador web, escriba la dirección IP de Citrix ADC, por ejemplo `http://10.102.29.50`.

2. En Nombre de usuario y contraseña, escriba las credenciales de administrador (nsroot/nsroot) y, a continuación, haga clic **en Iniciar sesión**.
3. En la GUI, haga clic en **Actualización del sistema**.



4. En el menú **Elegir archivo**, seleccione la opción adecuada: **Local** o **Appliance**. Si quiere utilizar la opción Appliance, primero debe cargar el firmware en Citrix ADC. Puede utilizar cualquier método de transferencia de archivos, como WinSCP, para cargar el firmware de Citrix ADC en el dispositivo.
5. Seleccione el archivo correcto y haga clic en **Actualizar**.
6. Siga las instrucciones para actualizar el software.
7. Cuando se le solicite, seleccione **Reiniciar**.

Tras la actualización, cierre todas las instancias del explorador y borre la memoria caché del equipo antes de acceder al dispositivo.

Actualizar un dispositivo independiente Citrix ADC mediante la CLI

Siga estos pasos para actualizar un Citrix ADC independiente a la versión 13.1 mediante la CLI:

En el siguiente procedimiento, `<release>` y `<releasenumber>` representan la versión de lanzamiento a la que va a actualizar y `<targetbuildnumber>` representa el número de compilación a la que va a actualizar. El procedimiento incluye pasos opcionales para evitar perder las actualizaciones que se insertan en el directorio /etc durante la actualización.

1. Utilice un cliente SSH, como PuTTY, para abrir una conexión SSH con el dispositivo.
2. Inicie sesión en el dispositivo con las credenciales de administrador. Guarda la configuración en ejecución. En el símbolo del sistema, escriba:

   ```
   save config
   ```

3. Cambie al símbolo del shell ejecutando el siguiente comando:

   ```
   shell
   ```


4. Cree una copia del archivo ns.conf. En el símbolo del shell, escriba:

   - `cd /nsconfig`
   - `cp ns.conf ns.conf.NS<currentreleasenumber><currentbuildnumber>`

   Debe hacer una copia de seguridad del archivo de configuración en otro equipo.

5. **IMPORTANTE:**

   Es importante que tanto los cambios de actualización como las personalizaciones se apliquen a un dispositivo Citrix ADC actualizado. Por lo tanto, si tiene archivos de configuración personalizados en el directorio `/etc`, realice los **pasos previos a la actualización** en Consideraciones sobre la actualización para los archivos de configuración personalizados.

6. Cree una ubicación para el paquete de instalación. En el símbolo del shell, escriba:

   - `cd /var/nsinstall`
   - `cd <releasenumber>`

     Nota:

     Si el directorio de números de versión deseados no está presente, cree uno con el siguiente comando:

     `mkdir <releasenumber>`

     Ejemplo:

     `mkdir 13.1`

   - `mkdir build_<targetbuildnumber>`
   - `cd build_<targetbuildnumber>`

7. Copie el firmware Citrix ADC ya descargado en el directorio de compilación que ha creado en el paso anterior, mediante cualquier método de transferencia de archivos como WinSCP. Consulte la sección Antes de comenzar para obtener más información sobre la descarga del firmware de Citrix ADC.

8. Extraiga el contenido del paquete de instalación. Ejemplo:

   ```
   tar -xvzf build-13.1-37.2_nc_64.tgz
   ```

9. Ejecute el script installns para instalar la nueva versión del software del sistema.

   ```
   ./installns
   ```

10. Cuando se le solicite, reinicie Citrix ADC.

11. **IMPORTANTE:**

    Es importante que tanto los cambios de actualización como las personalizaciones se

> apliquen a un dispositivo Citrix ADC actualizado. Por lo tanto, si tiene archivos de configuración personalizados en el directorio `/etc`, realice los **pasos posteriores a la actualización** en Consideraciones sobre la actualización para los archivos de configuración personalizados.

A continuación se muestra un ejemplo de actualización del firmware de Citrix ADC.

```
login: nsroot

Password: nsroot

Last login: Mon Apr 17 15:05:05 2018 from 10.252.243.134

Done

> save config

> shell

Last login: Mon Apr 17 15:05:05 2018 from 10.252.243.134

root@NSnnn# cd /var/nsinstall

root@NSnnn# cd 13.1

root@NSnnn# mkdir build_43.1

root@NSnnn# cd build_43.1

root@NSnnn# ftp <FTP server IP address>

ftp> mget build-13.1-41.1_nc.tgz

ftp> bye

root@NSnnn# tar xzvf build-13.1-41.1_nc.tgz

root@NSnnn# ./installns

installns version (13.1-41.1) kernel (ns-13.1-41.1_nc.gz)

...

Copying ns-13.1-41.1_nc.gz to /flash/ns-13.1-41.1_nc.gz ...
```



```
38
39 ...
40
41 Installation has completed.
42
43 Reboot NOW? [Y/N] Y
```

Actualizar un dispositivo independiente de Citrix ADC mediante la API NITRO

Para utilizar la API de NITRO para actualizar o bajar de categoría un Citrix ADC, consulte Automatizar la actualización y la degradación de Citrix ADC con una única API.

Verifique el estado de las entidades en el dispositivo Citrix ADC después de actualizar

Una vez actualizado el dispositivo Citrix ADC, compruebe el estado de las siguientes entidades:

- Los servidores virtuales están en estado UP
- Los monitores están en estado UP
- Los sitios GSLB se sincronizan sin problemas
- Todos los certificados están presentes en el dispositivo
- Todas las licencias están presentes en el dispositivo

Comprobar e instalar la actualización del software Citrix ADC 13.1

Actualice el software Citrix ADC cuando haya una actualización disponible para obtener un mejor rendimiento. Una actualización de Citrix ADC puede incluir mejoras en las funciones, correcciones de rendimiento o mejoras. Asegúrese de leer las notas de la versión para ver qué correcciones y mejoras están disponibles en la actualización. Para comprobar e instalar una actualización de software, haga lo siguiente.

1. En la página principal de Citrix ADC, **haga clic en Buscar actualización** en el menú **nsroot** de la esquina superior derecha.
2. En la página **Últimas actualizaciones de software del sistema disponibles**, compruebe la actualización de software disponible que puede instalar.
3. Haga clic en **Descargar** para descargar el paquete de instalación del sitio web de descargas de Citrix .
4. Después de descargar el paquete de software, instale la actualización mediante el procedimiento CLI o GUI.

> **Nota**
>
> El enlace **Buscar actualización** solo está disponible si inicia sesión en la GUI a través del proto-

> colo HTTP y no mediante el protocolo HTTPS.

Recursos conexos

Los siguientes recursos proporcionan información relacionada con la actualización o la degradación de un dispositivo Citrix ADC:

- Tutorial en vídeo: cómo actualizar Citrix ADC mediante CLI

Bajar de categoría un dispositivo independiente Citrix ADC

October 5, 2021

Puede cambiar a cualquier versión anterior en un Citrix ADC independiente mediante la CLI o la GUI.

> **Nota:**
>
> Es posible que se produzca una pérdida de configuración al bajar de categoría. Compare las configuraciones antes y después de la degradación y, a continuación, vuelva a introducir manualmente las entradas que falten.

Bajar de categoría un dispositivo Citrix ADC mediante la CLI

Siga los pasos que se indican a continuación para degradar un dispositivo independiente Citrix ADC que ejecuta la versión 13.1 a una versión anterior.

En este procedimiento, <release> y <releasenumber> representan la versión de lanzamiento a la que va a bajar de categoría y <targetbuildnumber> representa el número de compilación al que va a bajar de categoría.

1. Abra una conexión SSH con Citrix ADC mediante un cliente SSH, como PuTTY.
2. Inicie sesión en Citrix ADC con las credenciales de administrador. Guarda la configuración en ejecución. En el símbolo del sistema, escriba:

   guardar configuración
3. Cree una copia del archivo ns.conf. En el símbolo del shell, escriba:

   a) `cd /nsconfig`
   b) `cp ns.conf ns.conf.NS<currentbuildnumber>`

   Debe hacer una copia de seguridad de una copia del archivo de configuración en otro equipo.
4. Copie el <releasenumber>archivo de configuración (NS.conf.ns<releasenumber>) en ns.conf. En el símbolo del shell, escriba:


```
cp ns.conf.NS<releasenumber> ns.conf
<!--NeedCopy-->
```

> **Nota:**
>
> ns.conf.NS<releasenumber> es el archivo de configuración de copia de seguridad que se crea automáticamente cuando el software del sistema se actualiza de la versión de lanzamiento <releasenumber> a la versión actual.
>
> Puede haber alguna pérdida en la configuración al bajar de categoría. Una vez reiniciado el dispositivo, compare la configuración guardada en el paso 3 con la configuración en ejecución y realice los ajustes necesarios para las funciones y entidades configuradas antes de la degradación. Guarde la configuración en ejecución después de realizar los cambios.
>
> **Importante:**
>
> Si la redirección está habilitado, realice el paso 5. De lo contrario, vaya al paso 6.

5. Si la redirección está habilitado, el archivo Zebos.conf contiene la configuración. En el símbolo del shell, escriba:

```
cd /nsconfig
cp ZebOS.conf ZebOS.conf.NS
cp ZebOS.conf.NS<targetreleasenumber> ZebOS.conf
<!--NeedCopy-->
```

6. Cambie el /var/nsinstall/<releasenumber>nsinstalldirectorio a o cree uno si no existe.
7. Cambie el build_<targetbuildnumber>directorio a o cree uno si no existe.
8. Descargue o copie el paquete de instalación (build-<release>-<targetbuildnumber>.tgz) en este directorio y extraiga el contenido del paquete de instalación.
9. Ejecute el script installns para instalar la nueva versión del software del sistema. El script actualiza el directorio /etc.

   Si el archivo de configuración de la compilación a la que va a bajar de categoría existe en el dispositivo, se le pedirá que cargue esa configuración:

   Ilustración 1. Menú de degradación si existe un archivo de configuración


```
 version build       size  last modified  file name
Copied to ns.conf    72545  Jun 18 04:42   ns.conf.NS10.1-112.13
  NS10.1  112.13     72545  Jun 18 04:42   ns.conf.NS10.1
  NS10.1  112.13     72545  Jun 18 04:42   ns.conf.4
  NS10.1  109.1      87219  Jun 18 04:42   ns.conf.NS10.1-109.1
  NS10.1  93.051     74443  Jun 18 04:42   ns.conf.NS10.1-93.051
  NS10.0  29.1.      62849  Jun 18 04:42   ns.conf.NS10.0-29.1.









Listed above are 5 configuration files, found in /nsconfig, that are
appropriate for use with build 112.13.

Use the arrow keys to select an item in the menu above, then type:
  'c' - copy file over ns.conf
  'v' - view file (with vi; type ':q!' to exit vi)
  '>' - more files
  '<' - fewer files
  'd' - done
```


Si el espacio libre disponible en la unidad flash no es suficiente para instalar la nueva compilación, Citrix ADC anula la instalación. Limpie manualmente la unidad flash y reinicie la instalación.

Ejemplo:

```
login: nsroot

Password: nsroot

Last login: Mon Apr 24 02:06:52 2017 from 10.102.29.9

Done

> save config

> shell

root@NSnnn# cp ns.conf.NS10.5 ns.conf

root@NSnnn# cd /var/nsinstall

root@NSnnn# mkdir 10.5nsinstall

root@NSnnn# cd 10.5nsinstall

root@NSnnn# mkdir build_57

root@NSnnn# cd build_57

root@NSnnn# ftp 10.102.1.1

ftp> mget build-10.5-57_nc.tgz

ftp> bye

root@NSnnn# tar -xzvf build-10.1-125_nc.tgz

root@NSnnn# ./installns

installns version (10.5-57) kernel (ns-10.5-57.gz)

...

```



```
...

...

Copying ns-10.5-57.gz to /flash/ns-10.5-57_nc.gz ...

Changing /flash/boot/loader.conf for ns-10.5-57 ...


Installation has completed.


Reboot NOW? [Y/N] Y
<!--NeedCopy-->
```

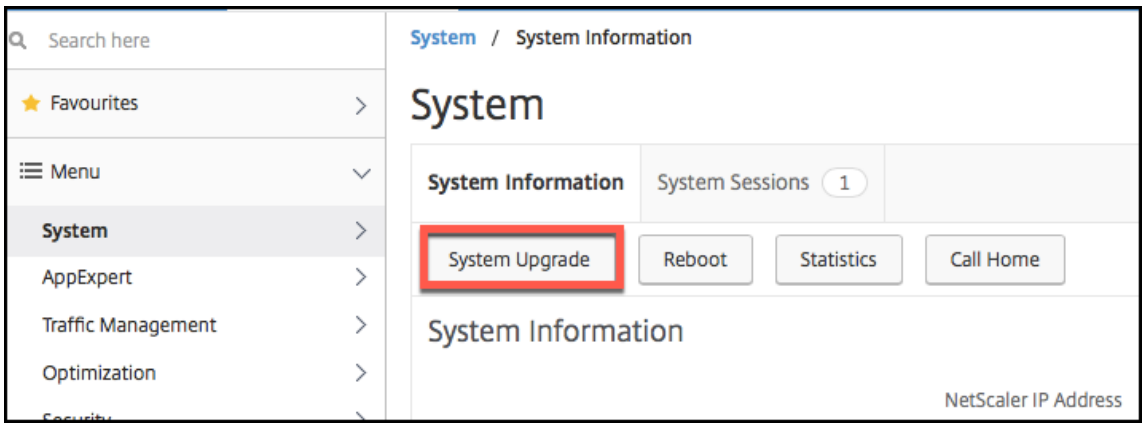
Bajar de categoría un dispositivo Citrix ADC mediante la interfaz gráfica de usuario

Puede utilizar el asistente de actualización de la GUI para degradar un dispositivo Citrix ADC que ejecuta la versión 13.1 a una versión anterior.

> **Notas:**
>
> No se puede degradar un dispositivo Citrix ADC que ejecuta la versión 13.1 directamente a la versión 10.5 o anterior mediante la interfaz gráfica de usuario. Citrix recomienda usar la CLI para degradar la categoría.
>
> Visite el sitio de Product Matrix para obtener más información sobre el ciclo de vida de la versión de Citrix ADC.
>
> Es una práctica recomendada bajar de categoría a una versión principal a la vez.
>
> Por ejemplo, si el dispositivo Citrix ADC está en la versión 13.1 y quiere bajar de categoría a la versión 12.1, primero debe degradar el dispositivo a la versión 13.0 y, a continuación, a la versión 12.1.

Siga los pasos que se indican a continuación para degradar un dispositivo Citrix ADC que ejecuta la versión 13.1 a una versión anterior mediante la interfaz gráfica de usuario.

1. En un explorador web, escriba la dirección IP de Citrix ADC, por ejemplo `http://10.102.29.50`.
2. En Nombre de usuario y contraseña, escriba las credenciales de administrador y, a continuación, haga clic **en Iniciar sesión**.
3. En la GUI, haga clic en **Actualización del sistema**.



4. En el menú **Elegir archivo**, seleccione la opción adecuada: **Local** o **Appliance**. Si quiere utilizar la opción Appliance, primero debe cargar el firmware en Citrix ADC. Puede utilizar cualquier método de transferencia de archivos, como WinSCP, para cargar el firmware de Citrix ADC en el dispositivo.
5. Seleccione el archivo correcto y haga clic en **Actualizar**.
6. Siga las instrucciones para degradar el software.
7. Cuando se le solicite, seleccione **Reiniciar**.

Tras la degradación, cierre todas las instancias del explorador y borre la memoria caché del equipo antes de acceder al dispositivo.

Recursos conexos

Los siguientes recursos proporcionan información relacionada con la actualización o la degradación de un dispositivo Citrix ADC:

- Tutorial en vídeo: cómo actualizar Citrix ADC mediante CLI

Actualizar un par de alta disponibilidad

July 27, 2022

Uno de los requisitos de los dispositivos Citrix ADC en una configuración de alta disponibilidad es instalar la misma versión de software Citrix ADC en ambos dispositivos de la configuración. Por lo tanto, cuando se actualiza el software de un dispositivo, asegúrese de que el software se actualice en ambos dispositivos.

Puede seguir el mismo procedimiento para actualizar un dispositivo independiente o cada uno de los dispositivos en un par de alta disponibilidad, aunque se aplican consideraciones adicionales a la actualización de un par de alta disponibilidad.

Antes de iniciar una actualización del firmware de Citrix ADC en un par de alta disponibilidad, lea los requisitos previos mencionados en la sección Antes de comenzar. Además, debe considerar algunos puntos específicos de HA.

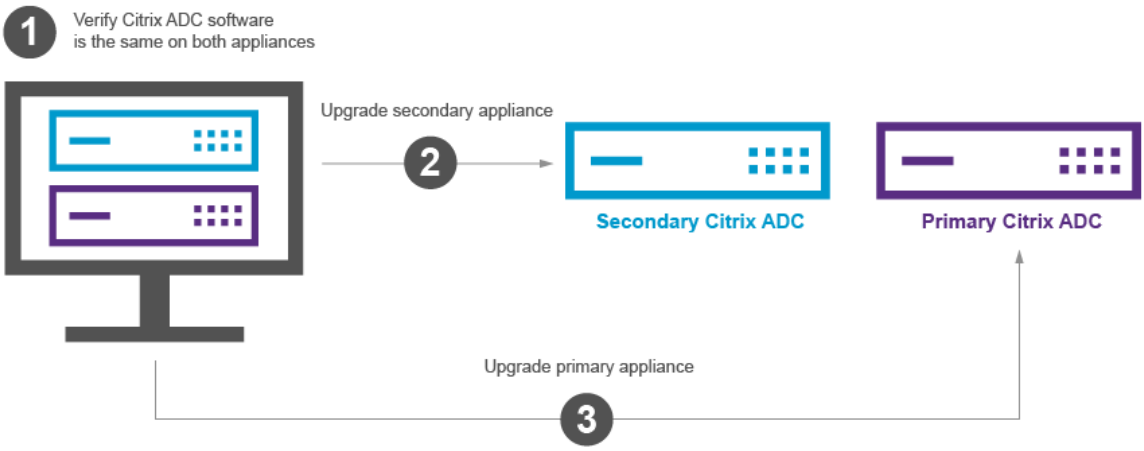
Puntos que tener en cuenta

> - **IMPORTANTE:**
>
> Es importante que tanto los cambios de actualización como las personalizaciones se apliquen a un dispositivo Citrix ADC actualizado. Por lo tanto, si tiene archivos de configuración personalizados en el directorio `/etc`, consulte Consideraciones sobre la actualización para los archivos de configuración personalizados antes de continuar con la actualización.

- Primero actualice el nodo secundario y, a continuación, el nodo principal. La actualización del software en el dispositivo secundario antes que el dispositivo principal garantiza que el proceso de actualización se complete sin problemas.
- Si ambos nodos en una configuración de alta disponibilidad (HA) ejecutan diferentes versiones de software Citrix ADC, se inhabilitan las siguientes funcionalidades:
  - Sincronización de configuración de alta disponibilidad
  - Propagación de comandos HA
  - Sincronización de alta disponibilidad de la información de servicios estatales
  - Duplicación de conexiones (conmutación por error de conexión) de sesiones
  - Sincronización de alta disponibilidad de información de sesiones de persistencia
- Las funcionalidades mencionadas anteriormente están inhabilitadas si ambos nodos en una configuración de alta disponibilidad (HA) ejecutan diferentes compilaciones de la misma versión, pero ambas compilaciones tienen diferentes versiones de HA internas. Las funcionalidades mencionadas anteriormente funcionan bien si ambos nodos en una configuración de alta disponibilidad (HA) ejecutan diferentes compilaciones de la misma versión, pero ambas compilaciones tienen las mismas versiones de alta disponibilidad internas.

  Consulte la sección Puntos a nota de las notas de la versión para comprobar si la versión interna de alta disponibilidad ha cambiado en la compilación de Citrix ADC.
- La sincronización de los archivos en el modo Todo del comando Sincronizar archivos HA funciona correctamente si los dos nodos de una configuración de HA ejecutan versiones de software Citrix ADC diferentes o si los dos nodos ejecutan compilaciones diferentes de la misma versión. Para obtener más información, consulte Sincronización de archivos de configuración en la configuración de alta disponibilidad.

Ilustración. Actualizar un par de alta disponibilidad



Puede realizar la actualización mediante la CLI o la GUI de Citrix ADC.

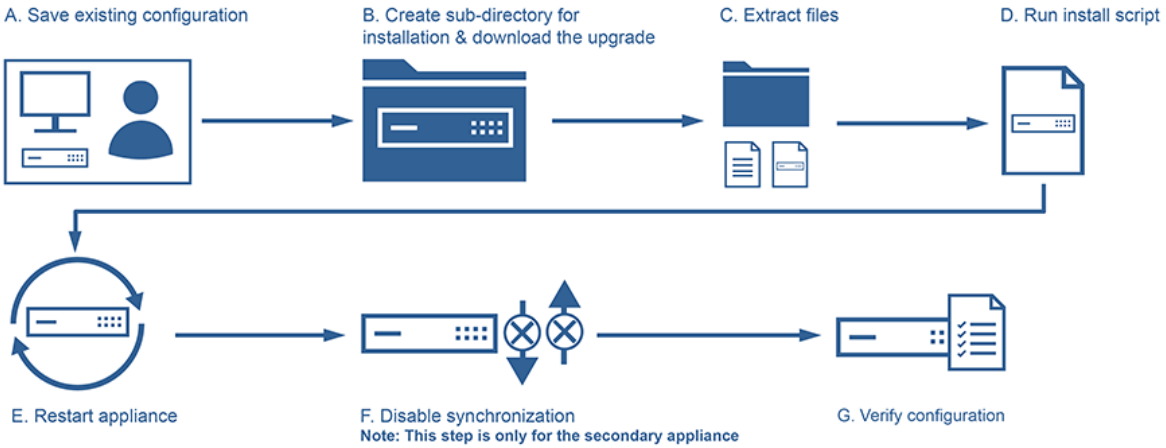
Actualizar un par de alta disponibilidad mediante la CLI

El proceso de actualización incluye los siguientes pasos:

1. Actualizar el software del dispositivo secundario
2. Actualizar el software del dispositivo principal
3. Sincronizar el dispositivo secundario

Actualizar el software del dispositivo secundario

La siguiente ilustración describe el procedimiento para actualizar el software en el dispositivo secundario:



1. Inicie sesión en el dispositivo secundario mediante una utilidad SSH, como PuTTY, y especificando la IP de Citrix ADC (NSIP). Use las credenciales `nsroot` para iniciar sesión en el dispositivo.

2. En la interfaz de línea de comandos del dispositivo, escriba el siguiente comando para guardar la configuración existente:

```
save config
<!--NeedCopy-->
```

3. Cambia al símbolo del shell:

```
shell
<!--NeedCopy-->
```

4. Ejecute el siguiente comando para cambiar al directorio de instalación predeterminado:

```
cd /var/nsinstall
<!--NeedCopy-->
```

5. Ejecute el siguiente comando para crear un subdirectorio temporal en el directorio `nsinstall`:

```
mkdir x_xnsinstall
<!--NeedCopy-->
```

> **Nota:**
>
> El texto x_x se usa para nombrar la versión de Citrix ADC para configuraciones futuras. Por ejemplo, el directorio para los archivos de instalación de Citrix ADC 13.1 se llama 13_1nsinstall. No utilice un punto (.) en el nombre de la carpeta, ya que puede provocar actualizaciones fallidas.

6. Cambie al directorio **x_xnsinstall**.
7. Descargue el paquete de instalación y el paquete de documentación necesarios, como “ns-x.0-xx.x-doc.tgz”, en el directorio temporal creado en el paso 4.

> **Nota:**
>
> Algunas compilaciones no tienen un paquete de documentación, ya que no tienen que instalarse.
>
> Haga clic en la ficha **Documentación** de la GUI para acceder a la documentación.

8. Antes de ejecutar el script de instalación, los archivos deben extraerse y colocarse en el dispositivo. Utilice el siguiente comando para descomprimir el paquete descargado del sitio web de Citrix: `tar -zxvf ns-x.0-xx.x-doc.tgz`. A continuación se ofrece una explicación rápida de los parámetros utilizados.

    - x - Extrae archivos.
    - v - Imprime los nombres de los archivos a medida que se extraen uno por uno.
    - z - El archivo es un archivo `gzipped`.
    - f - Utilice el siguiente archivo tar para la operación.

9. Ejecute el siguiente comando para instalar el software descargado:

```
./installns
<!--NeedCopy-->
```

> **Nota:**
>
> Si el dispositivo no tiene suficiente espacio en disco para instalar los nuevos archivos del núcleo, el proceso de instalación realiza una limpieza automática de la unidad flash.

10. Una vez finalizado el proceso de instalación, el proceso solicita que se reinicie el dispositivo. Presione `y` para reiniciar el dispositivo.
11. Inicie sesión en la interfaz de línea de comandos del dispositivo con las credenciales `nsroot`.
12. Ejecute el siguiente comando desde para mostrar el estado del dispositivo Citrix ADC. La salida del comando anterior debe indicar que el dispositivo es un nodo secundario y que la sincronización está inhabilitada.

```
show ha node
<!--NeedCopy-->
```

13. Ejecute el siguiente comando para realizar una conmutación por error forzada y una adquisición como dispositivo principal:

```
force failover
<!--NeedCopy-->
```

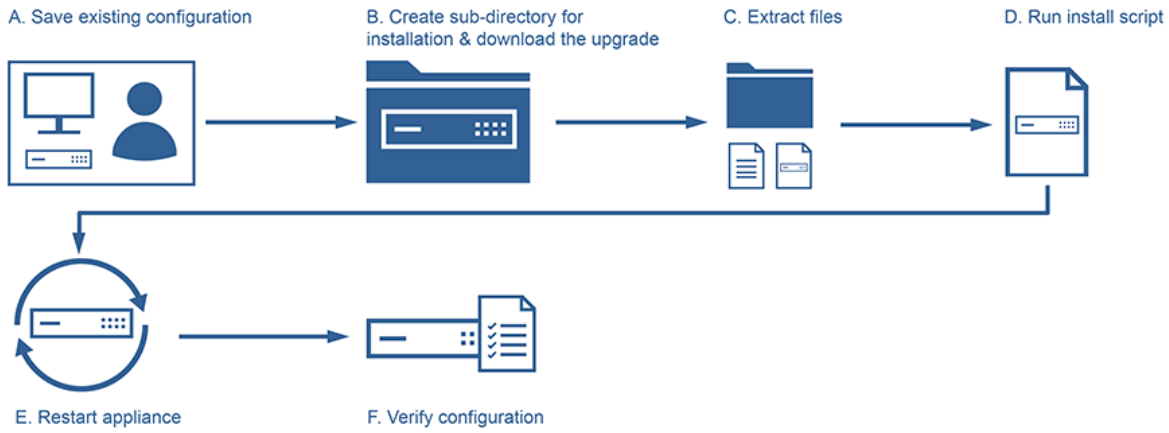
14. Compruebe que el dispositivo sea ahora un dispositivo principal.

    A continuación, se muestra una configuración de ejemplo en el nuevo nodo principal.


```
login: nsroot
Password: nsroot
Last login: Monday Apr  17 08:37:26 2017 from 10.102.29.9
Done
show ha node
        2 nodes:
1)      Node ID:      0
        IP:        10.0.4.2
        Node State: UP
        Master State: Primary
        ...
        Sync State: AUTO DISABLED
        Propagation: AUTO DISABLED
        ...
Done
<!--NeedCopy-->
```

Actualizar el software del dispositivo principal

La siguiente ilustración describe el procedimiento para actualizar el software del dispositivo principal:



> **Nota:**
>
> Tras completar el procedimiento “Actualizar el software en el dispositivo secundario”, el dispositivo principal original ahora es un dispositivo secundario.

1. Inicie sesión en el dispositivo secundario mediante una utilidad SSH, como PuTTY. Use las credenciales `nsroot` para iniciar sesión en el dispositivo. Siga los mismos pasos que se mencionan en la sección anterior para completar el proceso de instalación. Tenemos que seguir los mismos pasos que se mencionaron en el paso 2 al paso 9 de la sección anterior (Actualización del software del dispositivo secundario).

2. Una vez finalizado el proceso de instalación, el proceso solicita que se reinicie el dispositivo. Presione `y` para reiniciar el dispositivo.
3. Inicie sesión en la interfaz de línea de comandos del dispositivo con las credenciales `nsroot`.
4. Ejecute el siguiente comando para mostrar el estado del dispositivo NetScaler. La salida del comando anterior debe indicar que el dispositivo es un nodo secundario y que el estado del estado del nodo se marca como UP.

```
show ha node
<!--NeedCopy-->
```

5. Ejecute el siguiente comando para realizar una conmutación por error forzada a fin de garantizar que el dispositivo sea un dispositivo principal:

```
force failover
<!--NeedCopy-->
```

6. Compruebe que el dispositivo sea un dispositivo principal.

   A continuación, se muestra un ejemplo de configuración del nuevo nodo principal y el nuevo nodo secundario.

```
show ha node
    Node ID:      0
    IP:   10.0.4.11
    Node State: UP
    Master State: Primary
    ...
    ...
    INC State: DISABLED
    Sync State: ENABLED
    Propagation: ENABLED
    Enabled Interfaces : 1/1
    Disabled Interfaces : None
    HA MON ON Interfaces : 1/1
    ...
    ...
    Local node information
    Critical Interfaces: 1/1
Done
```



```
19
20 Show ha node
21     Node ID:      0
22     IP:   10.0.4.2
23     Node State: UP
24     Master State: Secondary
25     ..
26     ..
27     INC State: DISABLED
28     Sync State: SUCCESS
29     Propagation: ENABLED
30     Enabled Interfaces : 1/1
31     Disabled Interfaces : None
32     HA MON ON Interfaces : 1/1
33     . .
34     . .
35     Local node information:
36     Critical Interfaces: 1/1
37 Done
38 <!--NeedCopy-->
```

Actualizar un par de alta disponibilidad mediante la interfaz gráfica de usuario

Siga estos pasos para actualizar un par Citrix ADC en una configuración de alta disponibilidad, mediante la GUI de ADC. Considere un ejemplo de configuración de alta disponibilidad de los dispositivos Citrix ADC CITRIX-ADC-A (principal) y CITRIX-ADC-B (secundario).

1. **Actualice el nodo secundario**. Inicie sesión en la GUI del nodo secundario mediante credenciales de administrador y realice la actualización tal y como se describe en Actualizar un dispositivo independiente Citrix ADC mediante la GUI.

2. **Forzar la conmutación por error**. Realice una conmutación por error de fuerza en el nodo secundario mediante la GUI como se describe en Forzar a un nodo a la conmutación por error.

   Después de la operación de conmutación por error, el nodo secundario toma el control como principal y el nodo principal se convierte en el nuevo nodo secundario. Tras la operación de conmutación por error en el ejemplo de configuración de alta disponibilidad:

   - CITRIX-ADC-B se convierte en el nuevo principal
   - CITRIX-ADC-A se convierte en el nuevo secundario

3. **Actualice el nodo principal original (nuevo nodo secundario)**. Inicie sesión en la nueva GUI de nodo secundario (CITRIX-ADC-A) y realice la actualización tal y como se describe en Actualizar un dispositivo independiente Citrix ADC mediante la GUI.

4. **Forzar la conmutación por error**. Realice una conmutación por error de fuerza en el nuevo nodo secundario (CITRIX-ADC-A) mediante la GUI como se describe en Forzar la conmutación por error de un nodo.

   Después de esta segunda operación de conmutación por error, el estado de ambos nodos regresan al mismo estado que antes de iniciar la operación de actualización de HA. Tras la operación de conmutación por error en el ejemplo de configuración de alta disponibilidad:

   - CITRIX-ADC-A se convierte en principal
   - CITRIX-ADC-B se convierte en secundario

5. **Verifique el proceso de actualización**. Inicie sesión en la GUI de ambos nodos. Vaya a **Sistema > Alta disponibilidad**, en la página de detalles, verifique el estado de alta disponibilidad de ambos nodos. Además, compruebe los detalles de la versión actualizada que se muestran en el panel superior de la GUI.

Recursos conexos

Los siguientes recursos proporcionan información relacionada sobre la actualización de una configuración de alta disponibilidad de Citrix ADC:

- Tutorial en vídeo: Cómo actualizar el par Citrix ADC HA mediante la GUI

Soporte de actualización de software en servicio para alta disponibilidad para realizar actualizaciones sin tiempo de inactividad

March 9, 2022

Durante un proceso de actualización regular en una configuración de alta disponibilidad, en algún momento, ambos nodos ejecutan compilaciones de software diferentes. Estas dos compilaciones pueden tener números de versión de alta disponibilidad internos iguales o diferentes.

Si ambas compilaciones tienen números de versión de alta disponibilidad diferentes, no se admite la conmutación por error de conexión (incluso si está habilitada) para las conexiones de datos existentes. En otras palabras, se pierden todas las conexiones de datos existentes, lo que lleva a un tiempo de inactividad.

Para solucionar este problema, en Actualización de software de servicio (ISSU) se puede utilizar para configuraciones de alta disponibilidad. ISSU introduce una funcionalidad de migración, que reemplaza el paso de la operación de conmutación por error forzada en el proceso de actualización. La funcionalidad de migración se encarga de respetar las conexiones existentes e incluye la operación de conmutación por error forzada.

Después de realizar una operación de migración, el nuevo nodo principal siempre recibe tráfico (solicitud y respuesta) relacionado con las conexiones existentes, pero las dirige al nodo principal anterior. El nodo principal anterior procesa el tráfico de datos y, a continuación, lo envía directamente al destino.

Cómo funciona la ISSU mejorada

El proceso de actualización regular en una configuración de alta disponibilidad consiste en los siguientes pasos:

1. **Actualice el nodo secundario**. Este paso incluye la actualización del software del nodo secundario y el reinicio del nodo.
2. **Forzar conmutación por error**. La ejecución de la conmutación por error forzada convierte el nodo secundario actualizado en principal y el nodo principal en secundario.
3. **Actualice el nuevo nodo secundario**. Este paso incluye la actualización del software del nuevo nodo secundario y el reinicio del nodo.

Durante el período comprendido entre el paso 1 y el paso 3, ambos nodos ejecutan compilaciones de software diferentes. Estas dos compilaciones pueden tener versiones internas de alta disponibilidad iguales o diferentes.

Si ambas compilaciones tienen números de versión de alta disponibilidad diferentes, no se admite la conmutación por error de conexión (incluso si está habilitada) para las conexiones de datos existentes. En otras palabras, se pierden todas las conexiones de datos existentes, lo que lleva a un tiempo de inactividad.

El proceso de actualización de ISSU en una configuración de alta disponibilidad consiste en los siguientes pasos:

1. **Actualice el nodo secundario**. Este paso incluye la actualización del software del nodo secundario y el reinicio del nodo.
2. **Operación de migración de ISSU**. El paso incluye la operación de conmutación por error forzada y se ocupa de las conexiones existentes. Después de realizar la operación de migración, el nuevo nodo principal siempre recibe tráfico (solicitud y respuesta) relacionado con las conexiones existentes, pero las dirige al nodo principal anterior a través de la VLAN SYNC configurada en el túnel GRE. El nodo principal anterior procesa el tráfico de datos y, a continuación, lo envía directamente al destino. La operación de migración de ISSU se completa cuando se cierran todas las conexiones existentes.
3. **Actualice el nuevo nodo secundario**. Este paso incluye la actualización del software del nuevo nodo secundario y el reinicio del nodo.

Antes de comenzar

Antes de comenzar a realizar el proceso ISSU en una configuración de alta disponibilidad, siga los siguientes requisitos previos y limitaciones:

- Asegúrese de que `SYNC VLAN` esté configurado en ambos nodos de la configuración de alta disponibilidad. Para obtener más información, consulte Restricción del tráfico de sincronización de alta disponibilidad a una VLAN.
- ISSU no se admite en la nube de Microsoft Azure porque Microsoft Azure no admite la tunelización GRE.
- La propagación y sincronización de configuraciones de alta disponibilidad no funcionan durante la ISSU.
- No se admite ISSU para la configuración de alta disponibilidad de IPv6.
- ISSU no se admite en las siguientes sesiones:
  - Marcos Jumbo
  - Sesiones IPv6
  - NAT a gran escala (LSN)

Pasos de configuración

ISSU incluye una función de migración, que reemplaza la operación de conmutación por error forzada en el proceso de actualización regular de una configuración de alta disponibilidad. La funcionalidad de migración se encarga de respetar las conexiones existentes e incluye la operación de conmutación por error forzada.

Durante el proceso ISSU de una configuración de alta disponibilidad, ejecuta la operación de migración justo después de actualizar el nodo secundario. Puede realizar la operación de migración desde cualquiera de los dos nodos.

Procedimiento CLI

Para realizar la operación de migración de alta disponibilidad mediante la CLI:

En el símbolo del sistema, escriba:

```
start ns migration
<!--NeedCopy-->
```


Procedimiento GUI

Para realizar la operación de migración de alta disponibilidad mediante la GUI:

Vaya a **Sistema**, haga clic en la ficha **Información del sistema**, en **la ficha Migración**y, a continuación, en **Iniciar migración**.

Mostrar estadísticas de ISSU

Puede ver las estadísticas de ISSU para monitorear el proceso actual de ISSU en una configuración de alta disponibilidad. Las estadísticas de ISSU muestran la siguiente información:

- Estado actual de la operación de migración de ISSU
- Hora de inicio de la operación de migración de ISSU
- Hora de finalización de la operación de migración de ISSU
- Hora de inicio de la operación de reversión de ISSU
- Número total de conexiones que se procesan como parte de la operación de migración de ISSU
- Número de conexiones restantes que se están procesando como parte de la operación de migración de ISSU

Puede ver las estadísticas de ISSU en cualquiera de los nodos de alta disponibilidad mediante la CLI o la GUI.

Procedimiento CLI

Para mostrar las estadísticas de ISSU mediante la CLI:

En el símbolo del sistema, escriba:

```
1 show ns migration
2 <!--NeedCopy-->
```

Procedimiento GUI

Para mostrar las estadísticas de ISSU mediante la GUI:

Vaya a **Sistema**, haga clic en la ficha **Información del sistema**, haga clic en **la ficha Migración**y, **a continuación, haga clic en Haga clic para mostrar**

Mostrar estadísticas de ISSU: la lista de conexiones existentes que el nodo principal anterior está procesando

Puede mostrar la lista de conexiones existentes que el nodo principal anterior sirve actualmente como parte de la operación de migración de ISSU mediante la opción `dumpsession`(`Dump Session`) de la operación `show migration`.

La operación show migration con la opción `dumpsession` debe ejecutarse solo en el nuevo nodo principal durante la operación ISSU.

Procedimiento CLI

Para mostrar la lista de conexiones existentes que el nodo principal anterior está procesando actualmente mediante la CLI:

En el símbolo del sistema, escriba:

```
show ns migration  - dumpsession YES
<!--NeedCopy-->
```

```
> sh migration -dumpsession yes

Index   remote-IP-port          local-IP-port           idle-time(x 10
    ms)

1       192.0.2.10      22      192.0.2.1       15998       703
2       198.51.100.20   7375    98.51.100.2     22          687
3       203.0.113.30    5506    203.0.113.3     22          687


<!--NeedCopy-->
```

Procedimiento GUI

Para mostrar la lista de conexiones existentes que el nodo principal anterior está procesando actualmente mediante la interfaz gráfica de usuario:

Vaya a **Sistema**, haga clic en la ficha **Información del sistema**, en **la ficha Migración**y, a continuación, en **Haga clic para mostrar las conexiones de migración**

Reversión del proceso de ISSU

Las configuraciones de alta disponibilidad (HA) ahora admiten la reversión del proceso de actualización de software en servicio (ISSU). La función de reversión de ISSU es útil si observa que la configuración de HA durante la operación de migración de ISSU no es estable o no funciona en un nivel óptimo como se esperaba.

La reversión de ISSU se aplica cuando la operación de migración de ISSU está en curso. La reversión de ISSU no funciona si la operación de migración de ISSU ya se ha completado. En otras palabras, debe ejecutar la operación de reversión de ISSU cuando la operación de migración de ISSU esté en curso.

La reversión de ISSU funciona de manera diferente según el estado de la operación de migración de ISSU cuando se desencadena la operación de reversión de ISSU:

- **La conmutación por error forzada aún no se ha producido durante la operación de migración de ISSU**. La reversión de ISSU detiene la operación de migración de ISSU y elimina todos los datos internos relacionados con la migración de ISSU almacenados en ambos nodos. El nodo principal actual sigue siendo el nodo principal y continúa procesando el tráfico de datos relacionado con las conexiones existentes y las nuevas.
- Se**ha producido una conmutación por error forzada durante la operación de migración de ISSU**. Si la conmutación por error de alta disponibilidad se ha producido durante la operación de migración de ISSU, el nuevo nodo principal (digamos que es N1) procesa el tráfico relacionado con las nuevas conexiones. El nodo principal antiguo (nodo secundario nuevo, digamos que es N2) procesa el tráfico relacionado con las conexiones antiguas (conexiones existentes antes de la operación de migración de ISSU).

  La reversión de ISSU detiene la operación de migración de ISSU y desencadena una conmutación por error forzada. El nuevo nodo principal (N2) ahora comienza a procesar el tráfico relacionado con las nuevas conexiones. El nuevo nodo principal (N2) también continúa procesando el tráfico relacionado con las conexiones antiguas (conexiones existentes establecidas antes de la operación de migración de ISSU). En otras palabras, las conexiones existentes establecidas antes de la operación de migración de ISSU no se pierden.

  El nuevo nodo secundario (N1) elimina todas las conexiones existentes (conexiones nuevas creadas durante la operación de migración de ISSU) y no procesa ningún tráfico. En otras palabras, cualquier conexión existente que se haya establecido después de la conmutación por error forzada de la operación de migración de ISSU se pierde para siempre.

Pasos de configuración

Puede usar la CLI o la GUI de Citrix ADC para realizar la operación de reversión de ISSU.

Procedimiento CLI

Para realizar la operación de reversión de ISSU mediante la CLI:

En el símbolo del sistema, escriba:

```
stop ns migration
<!--NeedCopy-->
```

Procedimiento GUI

Para realizar la operación de reversión de ISSU mediante la GUI:

Vaya a **Sistema**, haga clic en la ficha **Información del sistema**, en **la ficha Migración**y, a continuación, en **Detener migración**.

Capturas SNMP para el proceso de actualización de software en servicio

El proceso de actualización de software en servicio (ISSU) para una configuración de alta disponibilidad admite los siguientes mensajes de captura SNMP al principio y al final de la operación de migración de ISSU.

Captura SNMP	Descripción
Migración iniciada	Esta captura SNMP se genera y se envía a los agentes de escucha de capturas SNMP configurados cuando se inicia la operación de migración ISSU.
Migración completa	Esta captura SNMP se genera y se envía a los agentes de escucha de capturas SNMP configurados cuando se completa la operación de migración ISSU.

El nodo principal (antes del inicio del proceso ISSU) siempre genera estas dos capturas SNMP y las envía a los agentes de escucha de capturas SNMP configurados.

No hay alarmas SNMP asociadas a las capturas SNMP de ISSU. En otras palabras, estas trampas se generan independientemente de cualquier alarma SNMP. Solo hay que configurar los detectores SNMP de captura.

Para obtener más información sobre la configuración de detectores de capturas SNMP, consulte Cap-

turas SNMP en Citrix ADC.

Descalificarlo de un par de alta disponibilidad

August 20, 2021

Puede degradar a cualquier versión en un par de alta disponibilidad mediante la interfaz de línea de comandos. La GUI no admite el proceso de cambio de versión.

Para degradar el software del sistema en un par de Citrix ADC en un par de alta disponibilidad, debe degradar el software primero en el nodo secundario y luego en el nodo primario. Para obtener instrucciones sobre la degradación de cada nodo por separado, consulte Rebaja de categoría de un dispositivo independiente Citrix ADC.

> **Importante**
>
> Puede producirse una pérdida en la configuración al degradar la categoría. Debe comparar las configuraciones antes y después de la rebaja y, a continuación, volver a introducir manualmente las entradas que falten.

Solución de problemas relacionados con los procesos de instalación, actualización y degradación

October 5, 2021

Si el dispositivo no funciona según lo esperado después de completar el proceso de instalación, actualización o degradación, lo primero que debe hacer es comprobar las causas más comunes del problema.

Recursos para solucionar problemas

Para obtener los mejores resultados, utilice los siguientes recursos para solucionar un problema relacionado con la instalación, actualización o degradación de Citrix ADC:

- Los archivos de configuración del dispositivo. En el caso de un par de alta disponibilidad, los archivos de configuración de ambos dispositivos.
- Los siguientes archivos de los dispositivos:
  - Los archivos newnslog relevantes.
  - El archivo ns.log.
  - El archivo de mensajes.

- Diagrama de topología de red.

Problemas y resoluciones

A continuación se presentan los problemas más comunes de instalación, actualización y degradación, así como sugerencias para resolverlos:

1. **Problema**

   La actualización de un dispositivo Citrix ADC MPX falla debido a una incompatibilidad de hardware y software.

   Solución:

   Consulte la tabla de compatibilidad de hardware y software de Citrix ADC MPX y compruebe si la versión de software es compatible con el hardware Citrix ADC MPX.

2. **Problema**

   La actualización de un dispositivo Citrix ADC VPX falla debido a la incompatibilidad del dispositivo Citrix ADC VPX y del hipervisor.

   Solución:

   Consulte la tabla de compatibilidad del dispositivo Citrix ADC VPX y el hipervisor y compruebe si el modelo de dispositivo Citrix ADC VPX es compatible con el hipervisor.

3. **Problema**

   La actualización de un dispositivo Citrix ADC falla debido a errores de hardware.

   Solución:

   Validar la integridad del dispositivo Citrix ADC. Si tiene un dispositivo de hardware Citrix ADC, Citrix recomienda que se ejecute `fsck` para ejecutar una comprobación de disco y validar la integridad del disco duro de Citrix ADC.

   Para obtener más información, consulte Cómo verificar la integridad del sistema de archivos de un dispositivo Citrix ADC.

4. **Problema**

   Actualización de un dispositivo Citrix ADC mediante las paradas de la GUI.

   Solución:

   Actualice el explorador para comprobar si la actualización está progresando o no.

5. **Problema**

   La actualización de un dispositivo Citrix ADC falla debido a la falta de espacio en el directorio /var

Solución:

Libere espacio en el directorio /var. Para obtener más información, consulte Cómo liberar espacio en el directorio /var.

6. **Problema**

   No se puede acceder a Citrix ADC después de la degradación del software

   Causa

   Durante el proceso de degradación de software, si el archivo de configuración de la versión y la compilación existentes no coincide con el archivo de configuración de la versión y la compilación anteriores, el dispositivo no puede cargar la configuración y la dirección IP predeterminada se asigna al dispositivo.

   Solución:

   - Compruebe que se pueda acceder al dispositivo desde la consola.
   - Compruebe la dirección NSIP y las rutas del dispositivo.
     - Si la dirección IP ha cambiado a la dirección IP predeterminada de 192.168.100.1, cambie la dirección IP según sea necesario.
     - Compruebe que se pueda acceder al dispositivo.

7. **Problema**

   Durante una actualización, si ejecuto el comando de sincronización, aparece el siguiente mensaje:

   Error del comando en el nodo secundario pero se ejecutó correctamente en el nodo principal.

   Solución:

   No ejecute ningún comando dependiente (set /unset /bind /unbind) cuando la sincronización de alta disponibilidad (HA) esté en curso.

8. **Problema**

   Durante un proceso de actualización, el tráfico no pasa por el nuevo nodo principal cuando ejecuta el comando forzar conmutación por error.

   Solución:

   - Compruebe si hay problemas con la topología de red y las configuraciones del conmutador.
   - Ejecute el comando set l2param -garpreply ENABLED para habilitar la respuesta GARP.
   - Intenta usar MAC virtual si aún no lo has usado.
   - Ejecute el comando sendarp —a desde el nodo principal.

9. **Problema**

Después de actualizar o bajar de categoría un dispositivo Citrix ADC, la conexión al dispositivo falla a través de SSH.

Solución:

Realice las siguientes operaciones en el dispositivo Citrix ADC:

- Elimine las claves de host antiguas o inseguras en `/nsconfig/ssh/ssh_host_*`.
- Revise la configuración de SSHD personalizada en `/nsconfig/sshd_config` y compruebe si sigue siendo relevante y compatible. Cambie el nombre o elimine la configuración personalizada de SSHD según corresponda.
- Reinicio en frío del dispositivo Citrix ADC

10. **Problema**

    En un par de alta disponibilidad, después de ejecutar el comando force HA failover, los dispositivos siguen reiniciándose. El dispositivo secundario no aparece tras una actualización.

    Solución:

    Compruebe si el directorio /var está lleno. Si es así, elimine los archivos de instalación antiguos. Ejecute el comando df —h para mostrar el espacio disponible en disco.

11. **Problema**

    Después de actualizar un par de alta disponibilidad, uno de los nodos aparece como estado DESCONOCIDO.

    Solución:

    - Comprueba si ambos nodos ejecutan la misma compilación. Si las compilaciones no son las mismas y los nodos de alta disponibilidad no coinciden con la versión, algunos de los campos se muestran como DESCONOCIDO al ejecutar el comando show ha node.
    - Compruebe si se puede acceder al dispositivo secundario.

12. **Problema**

    Después de actualizar Citrix ADC, la interfaz muestra que la mayoría de los servidores virtuales de equilibrio de carga y los servicios están INACTIVOS.

    Solución:

    Compruebe que la dirección SNIP está activa en el dispositivo secundario. Además, escriba el comando show service para ver si el servicio se está ejecutando.

13. **Problema**

    Tras realizar una actualización, todos los servidores virtuales no funcionan en el dispositivo secundario.

    Solución:

Habilite el estado de alta disponibilidad y la sincronización de alta disponibilidad ejecutando los siguientes comandos:

- set node hastate habilitar
- set node hasync enable

No se recomienda inhabilitar HA.

14. **Problema**

    Después de realizar una degradación, Citrix ADC no arranca correctamente.

    Solución:

    Compruebe si se ha instalado la licencia correcta.

15. **Problema**

    En un par de alta disponibilidad, algunas funciones no se sincronizan después de realizar una actualización.

    Solución:

    Ejecute el comando sync ha file misc para sincronizar los archivos de configuración del nodo principal al nodo secundario.

16. **Problema**

    Durante el reinicio, aparece el siguiente mensaje de error:

    Fallaron uno o más comandos en ns.conf ¿Qué debo hacer?

    Solución:

    Asegúrese de que ningún comando del archivo ns.conf exceda el límite de 255 bytes. En los comandos que crean directivas demasiado largas para el límite de 255 bytes, puede usar conjuntos de patrones para acortar las directivas.

    Ejemplo:

```
1 add cs policy p11 -rule 'HTTP.REQ.URL.ENDSWITH_ANY("
     ctx_file_extensions")'
2 Done
3 <!--NeedCopy-->
```

    ctx_file_extensions es un patset predeterminado que cubre un gran número de extensiones. Además de los conjuntos de patrones por defecto, puede crear conjuntos de patrones definidos por el usuario. Agregue un patset ejecutando el siguiente comando:


```
add patset <name>
<!--NeedCopy-->
```

Nota: Los patsets solo se admiten en la versión 9.3 o posterior.

17. **Problema**

    Al actualizar un dispositivo Citrix ADC VPX, se me dice que libere espacio en /var. ¿Qué archivos elimino?

    Solución:

    Elimine los archivos de instalación antiguos del directorio /var/tmp/. Elimine también los archivos no deseados de /flash.

18. **Problema**

    No hay conectividad con la interfaz gráfica de usuario (GUI) cuando ejecuta el comando forzar conmutación por error de alta disponibilidad en el dispositivo secundario.

    Solución:

    Inicie sesión en el dispositivo secundario mediante la interfaz de línea de comandos y habilite el acceso a la GUI ejecutando el comando set ns ip <IP> -gui habilitado.

19. **Problema**

    Después de realizar una actualización, y cuando hago clic en cualquier enlace de la GUI que tenga que cargar un applet java (Asistente para actualización o asistente de licencias), aparece el siguiente mensaje de error: **La versión de la GUI no coincide con la versión del kernel. Cierre esta instancia, borre la caché del complemento java y vuelva a abrirla**.

    Solución:

    - Inicie sesión en Citrix ADC mediante la GUI.
    - Vaya a Citrix ADC Gateway > Configuración global.
    - Haga clic en Cambiar configuración global en Configuración.
    - En el panel de detalles, en Experiencia del cliente, seleccione Predeterminado en la lista de temas de la interfaz de usuario.
    - Haga clic en OK.

20. **Problema**

    Si la actualización de un dispositivo Citrix ADC falló por cualquier motivo, ¿cómo restaurar el dispositivo mediante los archivos de los que se ha realizado una copia de seguridad?

    Solución:

Si la actualización no se realiza correctamente, restaure el dispositivo a la versión anterior del dispositivo Citrix ADC mediante los archivos de copia de seguridad. Para obtener más información, consulte Copia de seguridad y restauración de un dispositivo Citrix ADC.

Para obtener más información sobre la copia de seguridad y restauración de una configuración de clúster de Citrix ADC, consulte Copia de seguridad y restauración de una configuración de clúster.

21. **Problema**

    Si faltan licencias tras una actualización fallida de un dispositivo Citrix ADC, ¿cómo resolver el problema?

    Solución:

    Si falta alguna licencia o si quiere reasignar las licencias, consulte el siguiente tema Descripción general de licencias.

> **Nota**
>
> Estos pasos de solución de problemas también se aplican a los problemas de pérdida de configuración al bajar de categoría el software en varias versiones.
>
> Para cualquier otro problema, consulte las notas de la versión, los artículos del Knowledge Center y las preguntas frecuentes.

Preguntas frecuentes

August 20, 2021

Para obtener respuestas a las preguntas que podría tener sobre la actualización del firmware de Citrix ADC, consulte las preguntas frecuentes sobre instalación, actualización y degradación .

Comandos, parámetros y OID SNMP nuevos y obsoletos

July 8, 2022

En esta sección se enumeran los comandos, los parámetros y los OID de SNMP nuevos y en desuso.

Nuevos comandos

En la tabla siguiente se enumeran los nuevos comandos de la versión 13.1.

Grupo de comandos	Comando
Nube	nube de estadísticas

Nuevos parámetros

Grupo de comandos	Comandos y parámetros
Firewall de aplicaciones	`add appfw profile [-clientIpExpression <expression>];set appfw profile [-clientIpExpression <expression>];show appfw profile [-clientIpExpression <expression>]`
Bot	`add bot profile [-verboseLogLevel ( NONE | HTTP_FULL_HEADER )];set bot profile [-verboseLogLevel ( NONE | HTTP_FULL_HEADER )]show bot profile [verbose Log Level];set cloud ngsparameter [-csvserverTicketingDecouple ( YES | NO )];show cloud ngsparameter [-csvserverTicketingDecouple]`
GSLB	`set gslb parameter [-GSLBSyncSaveConfigCommand ( ENABLED | DISABLED )];show gslb parameter [GSLBSyncSaveConfigCommand]`
NS	`set ns tcpParam [-delinkClientServerOnRST ( ENABLED | DISABLED )];show ns tcpParam [delinkClientServerOnRST]`

Grupo de comandos	Comandos y parámetros
RDP	add rdp clientprofile [-rdpValidateClientIP (ENABLE | DISABLE)];set rdp clientprofile [-rdpValidateClientIP (ENABLE | DISABLE)]; show rdp clientprofile [-rdpValidateClientIP]

Comandos en desuso

Grupo de comandos	Comandos
NS	add ns trafficDomain; rm ns trafficDomain; bind ns trafficDomain; unbind ns trafficDomain; enable ns trafficDomain; disable ns trafficDomain; show ns trafficDomain; stat ns trafficDomain
WI	add wi site;rm wi siteset wi site; bind wi site; unbind wi siteshow wi site; install wi **package**; uninstall wi **package**; show wi **package**
WF	install wf **package**; uninstall wf **package**; show wf **package**;add wf site; rm wf site;set wf site;show wf site

Se han eliminado las funciones obsoletas

Se han eliminado las siguientes funciones obsoletas y ya no se pueden configurar a partir de la versión 13.1 de Citrix ADC.

- La función Filtro (también conocida como filtrado de contenido o CF): acciones, directivas y

vinculación.

- Las funciones SPDY, conexión segura (SC), cola prioritaria (PQ), denegación de servicio HTTP (DoS) e inyección de HTML.
- Directivas clásicas para SSL, cambio de contenido, redirección de caché, compresión y firewall de aplicaciones.
- Los parámetros `url` y `domain` de las directivas de conmutación de contenido.
- Expresiones clásicas en reglas de persistencia de equilibrio de cargas.
- El parámetro `pattern` de las acciones de reescritura.
- El parámetro `bypassSafetyCheck` de las acciones de reescritura.
- `SYS.EVAL_CLASSIC_EXPR` en Expresiones avanzadas.
- Entidad de configuración `patclass`.
- `HTTP.REQ.BODY` sin argumentos en las expresiones avanzadas.
- Prefijos Q y S en expresiones avanzadas.
- El parámetro `policyType` para la configuración del parámetro de compresión. (Comando `set cmp parameter` de la CLI)

Puede usar la herramienta `nspepi` para la conversión. Debe ejecutar la herramienta en un dispositivo Citrix ADC versión 13.0 o 12.1.

Para obtener más información, consulte Preguntas frecuentes sobre retirada de directivas clásicas.

Además, para usar la última versión de las herramientas para migrar de la configuración clásica a la avanzada, consulte Scripts de Citrix ADC en GitHub.

Nuevos OID SNMP

Para obtener más información, consulte la guía de referencia de OID de SNMP.

Soluciones para proveedores de servicios de telecomunicaciones

January 12, 2021

Tecnologías de la Información y la Comunicación (TIC) trata de acercar al usuario de Internet a las aplicaciones y los datos. Las últimas tecnologías de centros de datos han permitido que el usuario, las aplicaciones y los datos se encuentren en cualquier lugar. Un usuario puede acceder a aplicaciones y datos desde la oficina o desde casa, o desde una ubicación como un aeropuerto. Las aplicaciones y los datos se pueden ubicar en las instalaciones de la empresa, en una nube pública o privada o en un host híbrido. El resultado ha sido solo el aumento de la productividad, pero también la reducción de los costes de propiedad y mantenimiento.

El servicio ofrece la infraestructura básica necesaria para transportar las aplicaciones y los datos del usuario a través de la red. Debido a que la infraestructura principal atiende a millones de suscriptores

y a una amplia variedad de aplicaciones y datos, los requisitos de compatibilidad con escalabilidad y protocolo son muy altos. La infraestructura principal maneja dos tipos principales de tráfico: Plano de datos y plano de control. Cada uno de estos aviones tiene sus propios requisitos de escala y soporte de protocolo.

El plano de datos es la parte de la infraestructura principal que transporta aplicaciones de usuario y datos de extremo a extremo, es decir, entre el equipo del usuario final y el servidor de aplicaciones. El número de usuarios que acceden a aplicaciones y datos es de miles de millones, por lo que los requisitos de rendimiento y direccionamiento IP son muy altos. Cada usuario de la red debe ser identificable de forma única. Solo entonces el proveedor de servicios puede controlar el tráfico, supervisar el uso de la red, ofrecer servicios específicos del usuario y registrar correctamente la información. Muchos de los dispositivos cliente y servidores de aplicaciones actuales admiten IPv6 de forma nativa. La infraestructura principal no solo debe admitir una combinación de clientes y servidores IPv4 e IPv6, sino que también debe proporcionar las tecnologías para la comunicación cruzada entre IPv4 e IPv6. Por último, un proveedor de servicios se mide por la calidad del servicio (directamente relacionado con la experiencia del usuario final) y la disponibilidad del servicio sin interrupciones. El plano de datos debe ser lo suficientemente resistente como para proporcionar calidad y disponibilidad al mismo tiempo.

La infraestructura del plano de control gestiona el tráfico de usuarios y mantiene los servicios de negocio y operaciones de red. El más importante de los muchos protocolos que se ejecutan en este plano son Diameter, Radio y SMPP. Diameter es un protocolo base sobre el cual se han desarrollado varios otros protocolos específicos de función. Por ejemplo:

- Interfaz Gx entre la Función de Aplicación de Directivas y Cargos (PCEF) y la Función de Reglas de Directiva y Cargos (PCRF)
- Interfaz Gy entre el sistema de carga en línea (OCS) y la puerta de enlace de red de datos de paquetes de Cisco (PGW) /Función de cumplimiento de directivas y carga (PCEF)

El volumen de tráfico del avión de control está en proporción directa con la actividad del usuario. Para administrar el tráfico del plano de control, los proveedores de servicios utilizan varias funcionalidades ADC, como el equilibrio de carga y la conmutación de contenido. Necesitan un control de grano fino del tráfico del plano de control, lo que equivale al tráfico del plano de datos en complejidad.

Los proveedores de servicios deben cumplir con los exigentes acuerdos de nivel de servicio (SLA) y los reguladores examinan minuciosamente su cumplimiento. Cumplir con los requisitos mientras administra los datos y el tráfico del plano de control requiere que un proveedor de servicios mantenga su infraestructura ágil, dentro del presupuesto, fácilmente actualizable y flexible. Como los ADC más potentes y avanzados del mercado en la actualidad, los productos Citrix ADC son una opción natural para el entorno de proveedores de servicios.

NAT a gran escala

January 12, 2021

> **Nota**
>
> Esta función está disponible con una licencia Citrix ADC Advanced o Premium Edition.

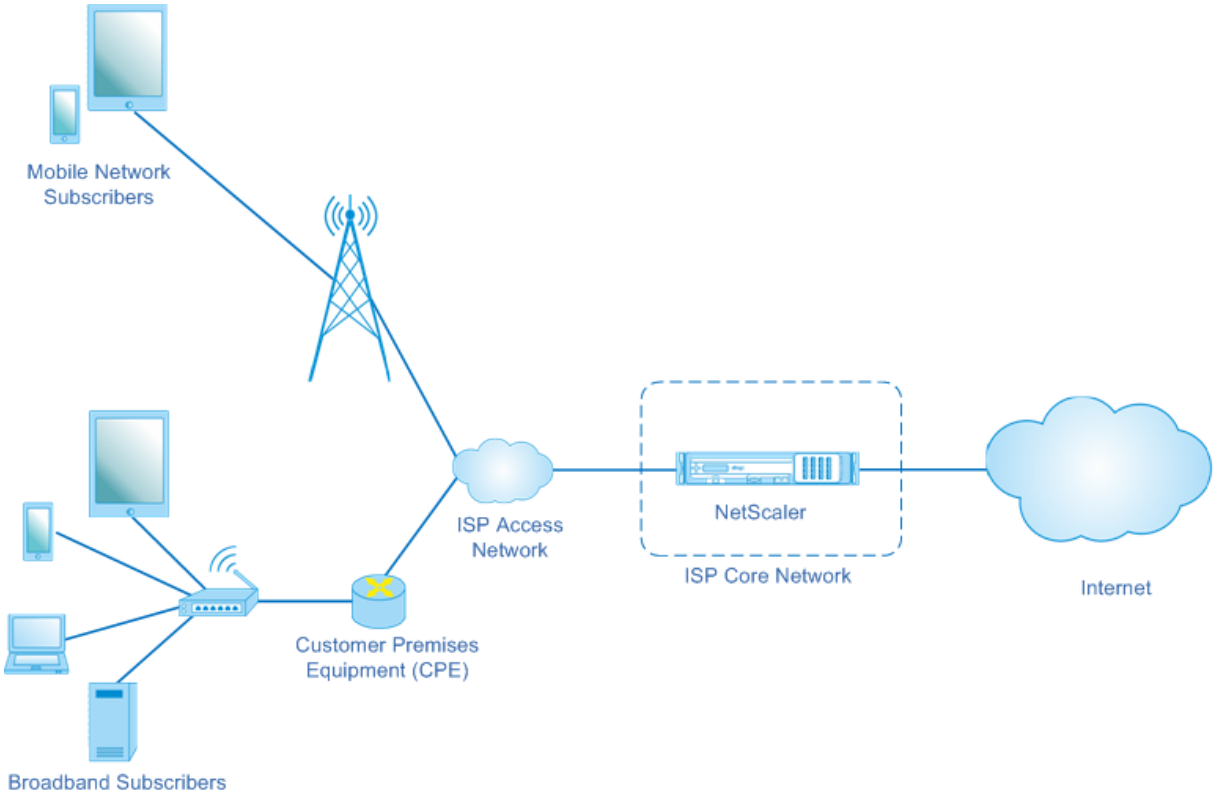
El crecimiento fenomenal de Internet ha dado lugar a una escasez de direcciones IPv4 públicas. La NAT de gran escala (LSN/CGNAT) proporciona una solución a este problema, maximizando el uso de direcciones IPv4 públicas disponibles al compartir algunas direcciones IPv4 públicas entre un gran grupo de usuarios de Internet.

LSN traduce direcciones IPv4 privadas en direcciones IPv4 públicas. Incluye métodos de traducción de direcciones de red y puertos para agregar muchas direcciones IP privadas en menos direcciones IPv4 públicas. LSN está diseñado para manejar NAT a gran escala. La función Citrix ADC LSN es muy útil para proveedores de servicios de Internet (ISP) y operadores que proporcionan millones de traducciones para admitir un gran número de usuarios (suscriptores) y con un rendimiento muy alto.

Arquitectura LSN

La arquitectura LSN de un ISP que utiliza productos Citrix consiste en suscriptores (usuarios de Internet) en espacios de direcciones privados que acceden a Internet a través de un dispositivo Citrix ADC implementado en la red principal del ISP. Los suscriptores están conectados al ISP a través de la red de acceso del ISP. Por lo general, los suscriptores para uso comercial de Internet están conectados directamente a la red de acceso del ISP. Para atender a esos suscriptores solo se requiere un nivel de NAT (NAT44).

Sin embargo, los suscriptores no comerciales suelen estar detrás de equipos locales del cliente (CPE), como enrutadores y módems, que también implementa NAT. Estos dos niveles de NAT crean el modelo NAT444. La implementación de un dispositivo Citrix ADC en la red principal de un ISP para la funcionalidad LSN es transparente para los suscriptores y no requiere cambios en la configuración de los suscriptores o los CPE.



Large Scale NAT

El dispositivo Citrix ADC recibe todos los paquetes de suscriptor destinados a Internet. El dispositivo se configura con un grupo de direcciones IP NAT predefinidas que se utilizarán para LSN. El dispositivo Citrix ADC utiliza su función LSN para traducir la dirección IP de origen (privada) y el puerto del paquete a la dirección IP NAT (pública) y al puerto NAT y, a continuación, envía el paquete a su destino en Internet. El dispositivo mantiene un registro de todas las sesiones activas que utilizan la función LSN. Estas sesiones se denominan sesiones LSN. El dispositivo Citrix ADC también mantiene las asignaciones entre la dirección IP y el puerto del suscriptor, y la dirección IP y el puerto NAT, para cada sesión. Estas asignaciones se denominan asignaciones LSN. Desde sesiones LSN y asignaciones LSN, el dispositivo Citrix ADC reconoce un paquete de respuesta (recibido de Internet) que pertenece a una sesión determinada. El dispositivo traduce la dirección IP de destino y el puerto del paquete de respuesta desde NAT IP address:port a la dirección IP del suscriptor:port y envía el paquete traducido al suscriptor.

Funciones LSN admitidas en el dispositivo Citrix ADC

A continuación se describen algunas de las funciones de LSN admitidas en el dispositivo Citrix ADC:

Asignación de recursos NAT

El dispositivo Citrix ADC asigna direcciones y puertos IP NAT, desde su grupo de recursos NAT predefinido, a los suscriptores para traducir sus paquetes para su transmisión a hosts externos (Internet). El dispositivo Citrix ADC admite los siguientes tipos de dirección IP NAT y asignación de puertos para los suscriptores:

- **Determinista.** El dispositivo Citrix ADC asigna una dirección IP NAT y un bloque de puertos a cada suscriptor. El dispositivo asigna secuencialmente recursos NAT a estos suscriptores. Asigna el primer bloque de puertos en la dirección IP NAT inicial a la dirección IP del suscriptor inicial. El siguiente rango de puertos se asigna al siguiente suscriptor, y así sucesivamente, hasta que la dirección NAT no tenga suficientes puertos para el siguiente suscriptor. En ese punto, el primer bloque de puerto de la siguiente dirección NAT se asigna al suscriptor, y así sucesivamente.

  El dispositivo Citrix ADC registra la dirección IP NAT asignada y el bloque de puertos para un suscriptor. Para una conexión, un suscriptor se puede identificar solo por su dirección IP NAT asignada y bloque de puerto. Por este motivo, el dispositivo Citrix ADC no registra ninguna sesión LSN creada o eliminada. Si se está usando todo el bloque de puertos, el dispositivo Citrix ADC elimina cualquier conexión nueva del suscriptor.

- **Dinámica.** El dispositivo Citrix ADC asigna una dirección IP NAT aleatoria y un puerto del grupo NAT LSN para la conexión de un suscriptor. Cuando la asignación de bloques de puertos está habilitada en la configuración, el dispositivo asigna una dirección IP NAT aleatoria y un bloque de puertos para un suscriptor cuando inicia una conexión por primera vez. A continuación, el dispositivo Citrix ADC asigna esta dirección IP NAT y uno de los puertos del bloque asignado a cada conexión posterior de este suscriptor. Si se está usando todo el bloque de puertos, el dispositivo asigna un nuevo bloque de puerto aleatorio al suscriptor cuando inicia una nueva conexión. Uno de los puertos del nuevo bloque de puertos se asigna para la nueva conexión.

Agrupación de IP

Las siguientes opciones de asignación de recursos NAT están disponibles para sesiones posteriores de un suscriptor al que se le asignó una dirección IP NAT aleatoria y un puerto para una sesión existente.

- **Emparejado.** El dispositivo Citrix ADC asigna la misma dirección IP NAT para todas las sesiones asociadas con el mismo suscriptor. Cuando no hay más puertos disponibles para esa dirección, el dispositivo elimina cualquier conexión nueva del suscriptor. Esta opción es necesaria para el correcto funcionamiento de ciertas aplicaciones que requieren la creación de varias sesiones en la misma dirección IP de origen (por ejemplo, en aplicaciones peer-to-peer que utilizan el protocolo RTP o RTCP.
- **Al azar.** El dispositivo Citrix ADC asigna direcciones IP NAT aleatorias, desde el grupo, para diferentes sesiones asociadas al mismo suscriptor.

Reutilización de Asignaciones LSN

El dispositivo Citrix ADC puede reutilizar una asignación LSN existente para nuevas conexiones que se originen desde el mismo puerto y dirección IP del suscriptor. La función Citrix ADC LSN admite los siguientes tipos de reutilización de asignación de LSN:

1. **Independiente del punto final.** El dispositivo Citrix ADC reutiliza la asignación LSN para los paquetes posteriores enviados desde la misma dirección IP del suscriptor y puerto (x:x) a cualquier dirección IP y puerto externos. Este tipo de reutilización de mapas LSN es útil para el correcto funcionamiento de las aplicaciones VOIP y peer-to-peer.
2. **Depende de la dirección.** El dispositivo Citrix ADC reutiliza la asignación LSN para los paquetes posteriores enviados desde la misma dirección IP del suscriptor y puerto (x:x) a la misma dirección IP externa (Y), independientemente del puerto externo.
3. **Depende del puerto de dirección.** El dispositivo Citrix ADC reutiliza la asignación LSN para los paquetes posteriores enviados desde la misma dirección IP interna y puerto (x:x) a la misma dirección IP externa y puerto (y:y) mientras la asignación sigue activa.

Filtrado LSN

El dispositivo Citrix ADC puede filtrar paquetes de hosts externos en función de las sesiones de LSN activas y las asignaciones de LSN. Considere un ejemplo de asignación LSN que incluye la asignación de IP del suscriptor (x:x), IP NAT: Puerto (n:n) y IP del host externo (y:y). La función Citrix ADC LSN admite los siguientes tipos de filtrado:

1. **Independiente del punto final.** El dispositivo Citrix ADC filtra solo aquellos paquetes que no están destinados a NAT IP:Port (N:n), que representa IP del suscriptor (X:x), independientemente de la dirección IP del host externo y el origen del puerto (Z:z). El dispositivo Citrix ADC reenvía los paquetes destinados a X:x. En otras palabras, enviar paquetes desde el suscriptor a cualquier dirección IP externa es suficiente para permitir paquetes desde cualquier host externo al suscriptor. Este tipo de filtrado es útil para el correcto funcionamiento de las aplicaciones VOIP y peer-to-peer.
2. **Depende de la dirección.** El dispositivo Citrix ADC filtra los paquetes no destinados a NAT IP:Port (N:n), que representa IP:Port del suscriptor (X:x). Además, el dispositivo filtra los paquetes de la dirección IP del host externo y del puerto (y:Y) destinados a n:n si el suscriptor no ha enviado previamente paquetes a y:AnyPort (independiente del puerto externo). En otras palabras, la recepción de paquetes de un host externo específico requiere que el suscriptor primero envíe paquetes a la dirección IP de ese host externo específico.
3. **Depende del puerto de dirección.** El dispositivo Citrix ADC filtra los paquetes no destinados a NAT IP:Port (N:n), que representa IP:Port del suscriptor (X:x). Además, el dispositivo filtra los paquetes de la dirección IP del host externo y del puerto (y:y) destinados a n:n si el suscriptor no ha enviado previamente paquetes a y:y. En otras palabras, la recepción de paquetes de un host

externo específico requiere que el suscriptor primero envíe paquetes a esa dirección IP externa y puerto específicos.

Cuotas

El dispositivo Citrix ADC puede limitar el número de puertos NAT y sesiones de cada suscriptor para garantizar una distribución justa de los recursos entre los suscriptores. El dispositivo Citrix ADC también puede limitar el número de sesiones de un grupo de suscriptores para garantizar una distribución justa de los recursos entre los diferentes grupos de suscriptores.

- **Cuota portuaria.** El dispositivo Citrix ADC puede limitar los puertos NAT LSN que cada suscriptor utilizará a la vez para un protocolo especificado. Por ejemplo, puede limitar cada suscriptor a un máximo de 500 puertos NAT TCP. Cuando las asignaciones NAT de LSN para un suscriptor alcanzan el límite, el dispositivo Citrix ADC no asigna puertos NAT adicionales del protocolo especificado a ese suscriptor.
- **Límite de sesión del suscriptor.** El número de sesiones simultáneas para un suscriptor puede ser mayor que su cuota de puerto. El dispositivo Citrix ADC puede limitar las sesiones LSN permitidas para cada suscriptor para un protocolo especificado. Cuando el número de sesiones LSN alcanza el límite para un suscriptor, el dispositivo Citrix ADC no permite que el suscriptor abra sesiones adicionales del protocolo especificado.
- **Límite de sesiones de grupo.** El dispositivo Citrix ADC puede limitar el número total de sesiones LSN permitidas para un grupo de suscriptores para un protocolo especificado. Cuando el número total de sesiones LSN alcanza el límite de un grupo para un protocolo especificado, el dispositivo Citrix ADC no permite que ningún suscriptor del grupo abra sesiones adicionales del protocolo especificado. Por ejemplo, limitar un grupo a un máximo de 10000 sesiones UDP. Cuando el número total de sesiones UDP para este grupo alcanza 10000, el dispositivo Citrix ADC no permite que ningún suscriptor del grupo abra sesiones UDP adicionales.

Puertas de enlace de capa de aplicación

Para algunos protocolos de capa de aplicación, las direcciones IP y los números de puerto de protocolo también se comunican en la carga útil del paquete. La puerta de enlace de capa de aplicación para un protocolo analiza la carga útil del paquete y realiza los cambios necesarios para garantizar que el protocolo continúa funcionando sobre LSN.

El dispositivo Citrix ADC admite ALG para los siguientes protocolos:

- FTP
- ICMP
- TFTP
- PPTP
- SIP

- RTSP

Soporte para horquilla

El dispositivo Citrix ADC admite la comunicación entre suscriptores o hosts internos mediante direcciones IP NAT. Este tipo de comunicación entre dos suscriptores que utilizan direcciones IP NAT se llama flujo de horquilla. El flujo de horquilla está habilitado de forma predeterminada y no puede inhabilitarlo.

Puntos a considerar antes de configurar LSN

August 20, 2021

Tenga en cuenta los siguientes puntos antes de configurar LSN en un dispositivo Citrix ADC:

- Asegúrese de que comprende los diferentes componentes de NAT de gran escala, descritos en RFC 6888, 5382, 5508 y 4787.
- La asignación independiente de endpoint (EIM) y el filtrado independiente de endpoint (EIF) están inhabilitados de forma predeterminada. Estas opciones deben estar habilitadas para el correcto funcionamiento de las aplicaciones VoIP y peer-to-peer (P2P).
- **Registro LSN**: A continuación se presentan los puntos de consideración para el registro de información LSN:
  - Citrix recomienda registrar la información LSN en servidores de registro externos en lugar de en el dispositivo Citrix ADC. El inicio de sesión en servidores externos facilita un rendimiento óptimo cuando el dispositivo crea un gran número de entradas de registro LSN (en orden de millones).
  - Citrix recomienda el uso de SYSLOG sobre TCP o NSLOG. De forma predeterminada, SYSLOG utiliza UDP y NSLOG solo utiliza TCP para transferir información de registro a los servidores de registro. TCP es más confiable que UDP para transferir datos completos.
  - Las siguientes limitaciones se aplican a SYSLOG sobre TCP:
    * La solución Syslog sobre TCP no proporciona autenticación, comprobación de integridad y privacidad.
    * El dispositivo Citrix ADC se basa en el protocolo TCP para proporcionar confirmación de la entrega de mensajes SYSLOG a servidores de registro externos.
- **Alta disponibilidad**: A continuación se presentan los puntos de consideración para la alta disponibilidad de los dispositivos Citrix ADC para LSN:
  - Citrix recomienda configurar la función LSN en una implementación de alta disponibilidad de dos dispositivos Citrix ADC para el funcionamiento sin interrupciones y sin interrupciones de todas las sesiones LSN.

  - En una implementación de alta disponibilidad, Citrix recomienda:
    * Establecer el parámetro SYNC VLAN para dedicar una VLAN para todas las comunicaciones relacionadas con HA.
    * Sincronización de la clave RSS simétrica del nodo principal con el nodo secundario para la sincronización con estado de un gran número de asignaciones y sesiones LSN.
    * Vinculación de la subred de direcciones IP LSN a una VLAN para evitar la inundación de transmisiones GARP en todas las VLAN después de una conmutación por error.
  - En una implementación de alta disponibilidad de dispositivos Citrix ADC, las sesiones relacionadas con ALG no se reflejan en el dispositivo secundario.
- **Gateways de capa de aplicación (ALG)**: A continuación se presentan los puntos de consideración relacionados con ALG en un dispositivo Citrix ADC:
  - Los siguientes no son compatibles con SIP ALG:
    * Direcciones IP de multidifusión
    * SDP cifrado
    * Mensajes SIP a través de TLS
    * Traducción de FQDN en mensajes SIP
    * Autenticación de mensajes SIP
    * Dominios de tráfico, particiones de administración y clústeres de ADC de Citrix.
    * Mensajes SIP con cuerpos con varias partes.
  - Los siguientes no son compatibles con RTSP ALG:
    * Sesiones RTSP multidifusión
    * Sesión RTSP sobre UDP
    * Dominios de tráfico Citrix ADC, particiones de administración y clústeres de ADC de Citrix
  - El dispositivo Citrix ADC no admite ALG para el protocolo IPSec.
- Si inhabilita la función LSN cuando existen algunas sesiones LSN en el dispositivo Citrix ADC, estas sesiones seguirán existiendo durante el intervalo de tiempo de espera configurado.
- LSN tiene prioridad sobre RNAT. Si un paquete de un suscriptor LSN especificado también coincide con una regla RNAT, el paquete se traduce de acuerdo con la configuración LSN.
- El reenvío de paquetes relacionados únicamente con las sesiones LSN se basa en la tabla de redirecciones del dispositivo Citrix ADC.
- A diferencia de las direcciones IP de subred, la selección de una dirección IP NAT LSN para la conexión de un suscriptor no se basa en la entrada de redirección de la dirección IP de destino.
- Para los paquetes entrantes, las asignaciones LSN estáticas tienen prioridad sobre las asignaciones LSN dinámicas.
- Para los paquetes salientes, los perfiles de aplicación LSN tienen prioridad sobre la asignación estática.
- Cuando existe un gran número de sesiones LSN (> 1 millón) en el dispositivo Citrix ADC, Citrix recomienda mostrar sesiones LSN seleccionadas en lugar de todas ellas. En la interfaz de línea

de comandos o en la utilidad de configuración, utilice los parámetros de selección para mostrar la operación de sesión LSN.

- Para reducir la cantidad de memoria activa asignada a la función LSN, debe reiniciar caliente el dispositivo Citrix ADC después de cambiar la configuración de memoria configurada. Sin un reinicio caliente, solo puede aumentar la cantidad de memoria activa.

Pasos de configuración para LSN

January 12, 2021

La configuración de LSN en un dispositivo Citrix ADC consta de las siguientes tareas:

1. **Establezca los parámetros globales de LSN.** Los parámetros globales incluyen la cantidad de memoria Citrix ADC reservada para la función LSN y la sincronización de sesiones LSN en una configuración de alta disponibilidad.
2. **Cree una entidad cliente LSN y vincule suscriptores a ella.** Una entidad cliente LSN es un conjunto de suscriptores en cuyo tráfico quiere que el dispositivo Citrix ADC realice LSN. La entidad cliente incluye direcciones IPv4 y reglas ACL extendidas para identificar suscriptores. Un cliente LSN se puede enlazar a un solo grupo LSN. La interfaz de línea de comandos tiene dos comandos para crear una entidad cliente LSN y vincular un suscriptor a la entidad cliente LSN. La utilidad de configuración combina estas dos operaciones en una sola pantalla.
3. **Cree un grupo LSN y vincule las direcciones IP NAT a él.** Un grupo LSN define un grupo de direcciones IP NAT que utilizará el dispositivo Citrix ADC para realizar LSN. Al grupo se le asignan parámetros, como la asignación de bloques de puertos y el tipo de NAT (Determinista o Dynamic). Un grupo LSN enlazado a un grupo LSN se aplica a todos los suscriptores de una entidad cliente LSN vinculada al mismo grupo. Solo se pueden enlazar grupos LSN y grupos LSN con la misma configuración de tipo NAT. Se pueden enlazar varios grupos LSN a un grupo LSN. Para NAT Dinámico, un grupo LSN se puede enlazar a varios grupos LSN. Para NAT determinista, los grupos enlazados a un grupo LSN no se pueden vincular a otros grupos LSN. La interfaz de línea de comandos tiene dos comandos para crear un grupo LSN y vincular direcciones IP NAT al grupo LSN. La utilidad de configuración combina estas dos operaciones en una sola pantalla.
4. **(Opcional) Cree un perfil de transporte LSN para un protocolo especificado.** Un perfil de transporte LSN define varios tiempos de espera y límites, como el máximo de sesiones LSN y el máximo uso de puertos, que un suscriptor puede tener para un protocolo determinado. Enlazar un perfil de transporte LSN para cada protocolo (TCP, UDP e ICMP) a un grupo LSN. Un perfil se puede enlazar a varios grupos LSN. Un perfil enlazado a un grupo LSN se aplica a todos los suscriptores de un cliente LSN vinculado al mismo grupo. De forma predeterminada, un perfil de transporte LSN con la configuración predeterminada para los protocolos TCP, UDP e ICMP está enlazado a un grupo LSN durante su creación. Este perfil se denomina perfil de transporte

predeterminado. Un perfil de transporte LSN que se vincula a un grupo LSN anula el perfil de transporte LSN predeterminado para ese protocolo.

5. **(Opcional) Cree un perfil de aplicación LSN para un protocolo especificado y enlazar un conjunto de puertos de destino a él.** Un perfil de aplicación LSN define la asignación LSN y los controles de filtrado LSN de un grupo para un protocolo determinado y para un conjunto de puertos de destino. Para un conjunto de puertos de destino, se vincula un perfil LSN para cada protocolo (TCP, UDP e ICMP) a un grupo LSN. Un perfil se puede enlazar a varios grupos LSN. Un perfil de aplicación LSN vinculado a un grupo LSN se aplica a todos los suscriptores de un cliente LSN vinculado al mismo grupo. De forma predeterminada, un perfil de aplicación LSN con configuración predeterminada para los protocolos TCP, UDP e ICMP para todos los puertos de destino está enlazado a un grupo LSN durante su creación. Este perfil se denomina perfil de aplicación predeterminado. Cuando vincula un perfil de aplicación LSN, con un conjunto especificado de puertos de destino, a un grupo LSN, el perfil enlazado reemplaza el perfil de aplicación LSN predeterminado para ese protocolo en ese conjunto de puertos de destino. La interfaz de línea de comandos tiene dos comandos para crear un perfil de aplicación LSN y vincular un conjunto de puertos de destino al perfil de aplicación LSN. La utilidad de configuración combina estas dos operaciones en una sola pantalla.
6. **Cree un grupo LSN y vincule grupos LSN, perfiles de transporte LSN (opcionales) y perfiles de aplicación LSN (opcionales) al grupo LSN.** Un grupo LSN es una entidad formada por un cliente LSN, grupos LSN, perfiles de transporte LSN y perfiles de aplicación LSN. A un grupo se le asignan parámetros, como el tamaño de bloque de puertos y el registro de sesiones LSN. La configuración de parámetros se aplica a todos los suscriptores de un cliente LSN enlazado al grupo LSN. Solo se pueden enlazar grupos LSN y grupos LSN con la misma configuración de tipo NAT. Los grupos LSN múltiples se pueden enlazar a un grupo LSN. Para NAT Dinámico, un grupo LSN se puede enlazar a varios grupos LSN. Para NAT determinista, los grupos enlazados a un grupo LSN no se pueden vincular a otros grupos LSN. Solo una entidad cliente LSN puede vincularse a un grupo LSN, y una entidad cliente LSN vinculada a un grupo LSN no puede vincularse a otros grupos LSN. La interfaz de línea de comandos tiene dos comandos para crear un grupo LSN y vincular grupos LSN, perfiles de transporte LSN, perfiles de aplicación LSN al grupo LSN. La utilidad de configuración combina estas dos operaciones en una sola pantalla.

En la siguiente tabla se enumeran los números máximos de diferentes entidades LSN y enlaces que se pueden crear en un dispositivo Citrix ADC. Estos límites también están sujetos a la memoria disponible en el dispositivo Citrix ADC.

Entidades y enlaces LSN	Límite
Clientes LSN	1024
Grupos LSN	128
Grupos LSN	1024

Entidades y enlaces LSN	Límite
Redes de suscriptor que se pueden enlazar a un cliente LSN	64
ACL extendidas que se pueden vincular a un cliente LSN	1024
Direcciones IP NAT en un grupo	4096
Grupos LSN que se pueden enlazar a un grupo LSN	8
Grupos LSN que pueden usar el mismo grupo LSN	16
Perfiles de transporte LSN que se pueden enlazar a un grupo LSN	3 (uno para cada protocolo TCP, UDP e ICMP)
Grupos LSN que pueden usar el mismo perfil de transporte LSN	8
Perfiles de aplicación LSN que se pueden enlazar a un grupo LSN	64
Grupos LSN que pueden usar el mismo perfil de aplicación LSN	8
Rangos de puertos que se pueden enlazar a un perfil de aplicación LSN	8

Configuración mediante la interfaz de línea de comandos

Para crear un cliente LSN mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
add lsn client <clientname>

show lsn client
<!--NeedCopy-->
```

Para enlazar una dirección de red o una regla de ACL a un cliente LSN mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:


```
bind lsn client <clientname> ((-network <ip_addr> [-netmask <netmask>]
    [-td<positive_integer>]) | -aclname <string>)

show lsn client
<!--NeedCopy-->
```

Para crear un grupo LSN mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
add lsn pool <poolname> [-nattype ( DYNAMIC | DETERMINISTIC )] [-
    portblockallocation ( ENABLED | DISABLED )] [-portrealloctimeout <
    secs>] [-maxPortReallocTmq <positive_integer>]

show lsn pool
<!--NeedCopy-->
```

Para enlazar un intervalo de direcciones IP a un grupo LSN mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
bind lsn pool <poolname> <lsnip>

show lsn pool
<!--NeedCopy-->
```

Nota: Para eliminar direcciones IP LSN de un grupo LSN, utilice el comando unbind lsn pool.

Para crear un perfil de transporte LSN mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
add lsn transportprofile <transportprofilename> <transportprotocol> [-
    sessiontimeout <secs>] [-finrsttimeout <secs>] [-portquota <
    positive_integer>] [-sessionquota <positive_integer>] [-
```



```
    portpreserveparity ( ENABLED | DISABLED )] [-portpreserverange (
    ENABLED | DISABLED )] [-syncheck ( ENABLED | DISABLED )]
2
3 show lsn transportprofile
4 <!--NeedCopy-->
```

Para crear un perfil de aplicación LSN mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
1 add lsn appsprofile <appsprofilename> <transportprotocol> [-ippooling (
    PAIRED | RANDOM )] [-mapping <mapping>] [-filtering <filtering>][-
    tcpproxy ( ENABLED | DISABLED )] [-td <positive_integer>]
2
3 show lsn appsprofile
4 <!--NeedCopy-->
```

Para enlazar un intervalo de puertos de protocolo de aplicación a un perfil de aplicación LSN mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
1 bind lsn appsprofile <appsprofilename> <lsnport>
2
3 show lsn appsprofile
4 <!--NeedCopy-->
```

Para crear un grupo LSN mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
1 add lsn group <groupname> -clientname <string> [-nattype ( DYNAMIC |
    DETERMINISTIC )] [-portblocksize <positive_integer>] [-logging (
    ENABLED | DISABLED )] [-sessionLogging ( ENABLED | DISABLED )][-
    sessionSync (ENABLED | DISABLED )] [-snmptraplimit <positive_integer
    >] [-ftp ( ENABLED | DISABLED )]
2
3 show lsn group
```



```
4 <!--NeedCopy-->
```

Para enlazar perfiles LSN y grupos LSN a un grupo LSN mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
1 bind lsn group <groupname> (-poolname <string> | -transportprofilename
     <string> | -appsprofilename <string>)
2
3 show lsn group
4 <!--NeedCopy-->
```

Configuración mediante la utilidad de configuración

Para configurar un cliente LSN y enlazar una dirección de red IPv4 o una regla ACL mediante la utilidad de configuración

Desplácese hasta **Sistema** > **NAT a gran escala** > **Clientes**, agregue un cliente y, a continuación, vincule una dirección de red IPv4 o una regla de ACL al cliente.

Para configurar un grupo LSN y enlazar direcciones IP NAT mediante la utilidad de configuración

Vaya a **Sistema > NAT de gran escala** > **Grupos**y agregue un grupo y, a continuación, vincule una dirección IP NAT o un rango de direcciones IP NAT al grupo.

Para configurar un perfil de transporte LSN mediante la utilidad de configuración

1. Vaya a **Sistema > NAT a gran escala > Perfiles**.
2. En el panel de detalles, haga clic en la ficha **Transporte** y, a continuación, agregue un perfil de transporte.

Para configurar un perfil de aplicación LSN mediante la utilidad de configuración

1. Vaya a **Sistema > NAT a gran escala > Perfiles**.
2. En el panel de detalles, haga clic en **la ficha Aplicación** y, a continuación, agregue un perfil de aplicación.

Para configurar un grupo LSN y enlazar un cliente LSN, grupos, perfiles de transporte y perfiles de aplicación mediante la utilidad de configuración

Desplácese hasta **Sistema > NAT a gran escala > Grupos**, agregue un grupo y, a continuación, vincule un cliente LSN, grupos, perfiles de transporte y perfiles de aplicación al grupo.

Descripciones de parámetros (de los comandos enumerados en el procedimiento CLI)

- add lsn client
  - nombre_cliente

    Nombre de la entidad cliente LSN. Debe comenzar con un carácter alfanumérico o de subrayado (_) ASCII y debe contener solo caracteres alfanuméricos ASCII, guión bajo, hash (#), punto (.), espacio, dos puntos (:), en (@), igual (=) y guión (-). No se puede cambiar después de crear el cliente LSN. El siguiente requisito solo se aplica a la CLI: Si el nombre incluye uno o más espacios, escriba el nombre entre comillas dobles o simples (por ejemplo, “lsn client1” o ‘lsn client1’).

    Este es un argumento obligatorio. Longitud máxima: 127

Descripciones de parámetros (de los comandos enumerados en el procedimiento CLI)

- bind lsn client
  - nombre_cliente

    Nombre de la entidad cliente LSN. Debe comenzar con un carácter alfanumérico o de subrayado (_) ASCII y debe contener solo caracteres alfanuméricos ASCII, guión bajo, hash (#), punto (.), espacio, dos puntos (:), en (@), igual (=) y guión (-). No se puede cambiar después de crear el cliente LSN. El siguiente requisito solo se aplica a la CLI: Si el nombre incluye uno o más espacios, escriba el nombre entre comillas dobles o simples (por ejemplo, “lsn client1” o ‘lsn client1’).

    Este es un argumento obligatorio. Longitud máxima: 127
  - red

    Direcciones IPv4 de los suscriptores LSN o redes de suscriptores en cuyo tráfico quiere que el dispositivo Citrix ADC realice NAT a gran escala.
  - máscara de red

    Máscara de subred para la dirección IPv4 especificada en el parámetro Network.

    Valor predeterminado: 255.255.255.255
  - td

    ID del dominio de tráfico al que pertenece este suscriptor o la red de suscriptor (según lo especificado por el parámetro de red).

    Si no especifica un ID, el suscriptor o la red del suscriptor pasan a formar parte del dominio de tráfico predeterminado.

    Valor predeterminado: 0

Valor mínimo: 0

Valor máximo: 4094

- aclname

  Nombre (s) de cualquier ACL extendida (s) configurada (s) cuya acción es ALLY. La condición especificada en la regla ACL extendida identifica el tráfico de un suscriptor LSN para el que el dispositivo Citrix ADC debe realizar NAT a gran escala. Longitud máxima: 127

Descripciones de parámetros (de los comandos enumerados en el procedimiento CLI)

- add lsn pool
  - poolname

    Nombre del grupo LSN. Debe comenzar con un carácter alfanumérico o de subrayado (_) ASCII y debe contener solo caracteres alfanuméricos ASCII, guión bajo, hash (#), punto (.), espacio, dos puntos (:), en (@), igual (=) y guión (-). No se puede cambiar después de crear el grupo LSN. El siguiente requisito solo se aplica a la CLI: Si el nombre incluye uno o más espacios, escriba el nombre entre comillas dobles o simples (por ejemplo, “lsn pool1” o ‘lsn pool1’).

    Este es un argumento obligatorio. Longitud máxima: 127

  - Tipo de natación

    Tipo de dirección IP NAT y asignación de puertos (de los grupos LSN enlazados a un grupo LSN) para suscriptores (de la entidad cliente LSN vinculada al grupo LSN):

    Las opciones disponibles funcionan de la siguiente manera:

    * **Determinista**: Asigne una dirección IP NAT y un bloque de puertos a cada suscriptor (del cliente LSN vinculado al grupo LSN). El dispositivo Citrix ADC asigna secuencialmente recursos NAT a estos suscriptores. El dispositivo Citrix ADC asigna el primer bloque de puertos (tamaño de bloque determinado por el parámetro de tamaño de bloque de puerto del grupo LSN) en la dirección IP NAT inicial a la dirección IP del suscriptor inicial. El siguiente rango de puertos se asigna al siguiente suscriptor, y así sucesivamente, hasta que la dirección NAT no tenga suficientes puertos para el siguiente suscriptor. En este caso, el primer bloque de puerto en la siguiente dirección NAT se utiliza para el suscriptor, y así sucesivamente. Dado que cada suscriptor recibe ahora una dirección IP NAT determinista y un bloque de puertos, se puede identificar un suscriptor sin necesidad de registro. Para una conexión, un suscriptor se puede identificar basándose únicamente en la dirección IP NAT y el puerto, así como en la dirección IP y el puerto de destino.

* **Dinámico**: Asigne una dirección IP NAT aleatoria y un puerto del grupo NAT de LSN para una conexión de suscriptores. Si la asignación de bloques de puertos está habilitada (en el grupo LSN) y se especifica un tamaño de bloque de puertos (en el grupo LSN), el dispositivo Citrix ADC asigna una dirección IP NAT aleatoria y un bloque de puertos para un suscriptor cuando inicia una conexión por primera vez. El dispositivo asigna esta dirección IP NAT y un puerto (del bloque de puertos asignado) para diferentes conexiones de este suscriptor. Si se asignan todos los puertos (para diferentes conexiones de suscriptores) desde el bloque de puertos asignado a los suscriptores, el dispositivo asigna un nuevo bloque de puertos aleatorio para el suscriptor. Solo se pueden enlazar grupos LSN y grupos LSN con la misma configuración de tipo NAT. Los grupos LSN múltiples se pueden enlazar a un grupo LSN.

  Valores posibles: DYNAMIC, DETERMINISTIC

  Valor predeterminado: DYNAMIC

- portblockallocation

  Asigne un bloque de puerto NAT aleatorio, desde el grupo de puertos NAT disponible de una dirección IP NAT, para cada suscriptor cuando la asignación NAT se establece como NAT dinámico. Para cualquier conexión iniciada desde un suscriptor, el dispositivo Citrix ADC asigna un puerto NAT desde el bloque de puertos NAT asignado a los suscriptores para crear la sesión LSN.

  Debe establecer el tamaño del bloque de puerto en el grupo LSN enlazado. Para un suscriptor, si todos los puertos se asignan desde el bloque de puertos asignado a los suscriptores, el dispositivo Citrix ADC asigna un nuevo bloque de puertos aleatorio para el suscriptor.

  Para NAT determinista, este parámetro está habilitado de forma predeterminada y no puede inhabilitarlo.

  Valores posibles: ENABLED, DISABLED

  Valor predeterminado: DISABLED

- portrealloctimeout

  El tiempo de espera, en segundos, entre la desasignación de puertos NAT LSN (cuando se quita una asignación LSN) y la reasignación de ellos para una nueva sesión LSN. Este parámetro es necesario para evitar colisiones entre asignaciones y sesiones antiguas y nuevas. Garantiza que todas las sesiones establecidas se rompen en lugar de redireccionarse a un suscriptor diferente. Esto no es aplicable a los puertos utilizados en:

  * NAT determinista
  * Filtrado dependiente de direcciones y filtrado dependiente del puerto de direcciones
  * NAT dinámico con asignación de bloques de puertos

En estos casos, los puertos se reasignan inmediatamente.

Valor predeterminado: 0

Valor máximo: 600

- maxPortReallocTmq

  Número máximo de puertos para los que se aplica el tiempo de espera de reasignación de puertos para cada dirección IP NAT. En otras palabras, el tamaño máximo de cola de puerto desasignado para el que se aplica el tiempo de espera de reasignación para cada dirección IP NAT.

  Cuando el tamaño de la cola está lleno, el siguiente puerto desasignado se reasigna inmediatamente para una nueva sesión LSN.

  Valor predeterminado: 65536

  Valor máximo: 65536

Descripciones de parámetros (de los comandos enumerados en el procedimiento CLI)

- bind lsn pool
  - poolname

    Nombre del grupo LSN. Debe comenzar con un carácter alfanumérico o de subrayado (_) ASCII y debe contener solo caracteres alfanuméricos ASCII, guión bajo, hash (#), punto (.), espacio, dos puntos (:), en (@), igual (=) y guión (-). No se puede cambiar después de crear el grupo LSN. El siguiente requisito solo se aplica a la CLI: Si el nombre incluye uno o más espacios, escriba el nombre entre comillas dobles o simples (por ejemplo, “lsn pool1” o ‘lsn pool1’).

    Este es un argumento obligatorio. Longitud máxima: 127

  - lsnip

    Dirección IPv4 o un rango de direcciones IPv4 que se utilizarán como direcciones IP NAT para LSN.

    Después de crear el grupo, estas direcciones IPv4 se agregan al dispositivo Citrix ADC como dirección IP propiedad de Citrix ADC de tipo LSN. Una dirección IP LSN asociada a un grupo LSN no se puede compartir con otros grupos LSN. Las direcciones IP especificadas para este parámetro no deben existir ya en el dispositivo Citrix ADC como cualquier dirección IP propiedad de Citrix ADC. En la interfaz de línea de comandos, separe el rango con un guión. Por ejemplo: 10.102.29.30-10.102.29.189. Posteriormente, puede quitar algunas o todas las direcciones IP de LSN del grupo y agregar direcciones IP al grupo LSN.

Descripciones de parámetros (de los comandos enumerados en el procedimiento CLI)

- agregar lsn transportprofile
  - transportprofilename

    Nombre del perfil de transporte LSN. Debe comenzar con un carácter alfanumérico o de subrayado (_) ASCII y debe contener solo caracteres alfanuméricos ASCII, guión bajo, hash (#), punto (.), espacio, dos puntos (:), en (@), igual (=) y guión (-). No se puede cambiar después de crear el perfil de transporte LSN. El siguiente requisito solo se aplica a la CLI: Si el nombre incluye uno o más espacios, escriba el nombre entre comillas dobles o simples (por ejemplo, “lsn transport profile1” o ‘lsn transport profile1’).

    Este es un argumento obligatorio. Longitud máxima: 127

  - transportprotocol

    Protocolo para el que establecer los parámetros del perfil de transporte LSN.

    Este es un argumento obligatorio.

    Valores posibles: TCP, UDP, ICMP

  - tiempo de espera de sesión

    Tiempo de espera, en segundos, para una sesión LSN inactiva. Si una sesión LSN está inactiva durante un tiempo que supera este valor, el dispositivo Citrix ADC quita la sesión.

    Este tiempo de espera no se aplica a una sesión TCP LSN cuando se recibe un mensaje FIN o RST desde cualquiera de los extremos.

    Valor predeterminado: 120

    Valor mínimo: 60

  - firsttimeout

    Tiempo de espera, en segundos, para una sesión TCP LSN después de recibir un mensaje FIN o RST desde uno de los extremos.

    Si una sesión TCP LSN está inactiva (después de que el dispositivo Citrix ADC reciba un mensaje FIN o RST) durante un tiempo que supere este valor, el dispositivo Citrix ADC quita la sesión.

    Dado que la función LSN del dispositivo Citrix ADC no mantiene la información de estado de ninguna sesión TCP LSN, este tiempo de espera admite la transmisión de FIN o RST y los mensajes ACK desde el otro extremo, de modo que ambos extremos puedan cerrar correctamente la conexión.

    Valor predeterminado: 30

- cuota de puerto

  Número máximo de puertos NAT LSN que se utilizarán cada vez por cada suscriptor para el protocolo especificado. Por ejemplo, cada suscriptor puede limitarse a un máximo de 500 puertos NAT TCP. Cuando las asignaciones NAT de LSN para un suscriptor alcanzan el límite, el dispositivo Citrix ADC no asigna puertos NAT adicionales para ese suscriptor.

  Valor predeterminado: 0

  Valor mínimo: 0

  Valor máximo: 65535

- cuota de sesión

  Número máximo de sesiones LSN simultáneas permitidas para cada suscriptor para el protocolo especificado. Cuando el número de sesiones LSN alcanza el límite para un suscriptor, el dispositivo Citrix ADC no permite que el suscriptor abra sesiones adicionales.

  Valor predeterminado: 0

  Valor mínimo: 0

  Valor máximo: 65535

- portpreserveparity

  Habilite la paridad de puertos entre un puerto de suscriptor y su puerto NAT LSN asignado. Por ejemplo, si un suscriptor inicia una conexión desde un puerto numerado impar, el dispositivo Citrix ADC asigna un puerto NAT LSN numerado impar para esta conexión. Debe establecer este parámetro para el correcto funcionamiento de los protocolos que requieren que el puerto de origen esté numerado par o impar, por ejemplo, en aplicaciones de punto a punto que utilizan el protocolo RTP o RTCP.

  Valores posibles: ENABLED, DISABLED

  Valor predeterminado: DISABLED

- portpreserverange

  Si un suscriptor inicia una conexión desde un puerto conocido (0-1023), asigne un puerto NAT desde el rango de puertos conocido (0-1023) para esta conexión. Por ejemplo, si un suscriptor inicia una conexión desde el puerto 80, el dispositivo Citrix ADC puede asignar el puerto 100 como puerto NAT para esta conexión.

  Este parámetro se aplica a NAT dinámico sin asignación de bloques de puertos. También se aplica a NAT determinista si el rango de puertos asignado incluye puertos conocidos.

  Cuando todos los puertos conocidos de todas las direcciones IP NAT disponibles se utilizan en diferentes conexiones de suscriptores (sesiones LSN) y un suscriptor inicia una conexión desde un puerto conocido, el dispositivo Citrix ADC interrumpe esta conexión.

Valores posibles: ENABLED, DISABLED

Valor predeterminado: DISABLED

- syncheck

  Suelte silenciosamente los paquetes que no sean SYN para las conexiones para las que no haya sesión LSN-NAT presente en el dispositivo Citrix ADC.

  Si inhabilita este parámetro, el dispositivo Citrix ADC acepta paquetes que no sean SYN y crea una nueva entrada de sesión LSN para esta conexión.

  A continuación se presentan algunos motivos para que el dispositivo Citrix ADC reciba dichos paquetes:

  * Existía sesión LSN para una conexión, pero el dispositivo Citrix ADC eliminó esta sesión porque la sesión LSN estuvo inactiva durante un tiempo que excedió el tiempo de espera de sesión configurado.
  * Dichos paquetes pueden ser parte de un ataque DoS.

  Valores posibles: ENABLED, DISABLED

  Valor predeterminado: ENABLED

Descripciones de parámetros (de los comandos enumerados en el procedimiento CLI)

- add lsn appsprofile
  - appsprofilename

    Nombre del perfil de aplicación LSN. Debe comenzar con un carácter alfanumérico o de subrayado (_) ASCII y debe contener solo caracteres alfanuméricos ASCII, guión bajo, hash (#), punto (.), espacio, dos puntos (:), en (@), igual (=) y guión (-). No se puede cambiar después de crear el perfil de aplicación LSN. El siguiente requisito solo se aplica a la CLI: Si el nombre incluye uno o más espacios, escriba el nombre entre comillas dobles o simples (por ejemplo, “lsn application profile1” o ‘lsn application profile1’).

    Este es un argumento obligatorio. Longitud máxima: 127

  - transportprotocol

    Nombre del protocolo al que se aplican los parámetros de este perfil de aplicación LSN.

    Este es un argumento obligatorio.

    Valores posibles: TCP, UDP, ICMP

  - ippooling

    Opciones de asignación de direcciones IP NAT para sesiones asociadas con el mismo suscriptor.

Las opciones disponibles funcionan de la siguiente manera:

* **Emparejado**: El dispositivo Citrix ADC asigna la misma dirección IP NAT para todas las sesiones asociadas con el mismo suscriptor. Cuando se utilizan todos los puertos de una dirección IP NAT en sesiones LSN (para los mismos suscriptores o varios), el dispositivo Citrix ADC elimina cualquier conexión nueva del suscriptor.
* **Random**: El dispositivo Citrix ADC asigna direcciones IP NAT aleatorias, desde el grupo, para diferentes sesiones asociadas con el mismo suscriptor.

Este parámetro solo es aplicable a la asignación NAT dinámica.

Valores posibles: PAIRED, RANDOM

Valor predeterminado: RANDOM

– mapeo

Tipo de asignación LSN para aplicar a los paquetes posteriores que se originan desde la misma dirección IP y puerto del suscriptor.

Considere un ejemplo de asignación LSN que incluye la asignación del suscriptor IP:Port (X:x), NAT IP:Port (N:n) y el host externo IP:Port (Y:y).

Las opciones disponibles funcionan de la siguiente manera:

* **ENDPOINT-INDEPENDIENTE**—Reutilice la asignación LSN para los paquetes posteriores enviados desde la misma dirección IP del suscriptor y puerto (x:x) a cualquier dirección IP externa y puerto.
* **ADDRESS-DEPENDIENTE**—Reutilice la asignación LSN para los paquetes posteriores enviados desde la misma dirección IP del suscriptor y puerto (x:x) a la misma dirección IP externa (Y), independientemente del puerto externo.
* **ADDRESS-PORT-DEPENDIENTE**—Reutilice la asignación LSN para los paquetes posteriores enviados desde la misma dirección IP interna y puerto (x:x) a la misma dirección IP externa y puerto (y:Y) mientras la asignación sigue activa.

Valores posibles: ENDPOINT-INDEPENDENT, ADDRESS-DEPENDENT, ADDRESS-PORT-DEPENDENT

Valor predeterminado: ADDRESS-PORT-DEPENDENT

– filtrado

Tipo de filtro que se aplicará a los paquetes procedentes de hosts externos.

Considere un ejemplo de asignación LSN que incluye la asignación de IP del suscriptor (x:x), IP NAT: Puerto (n:n) y IP del host externo (y:y).

Las opciones disponibles funcionan de la siguiente manera:

* **DISPOSITIVO DE PUNTO FINAL INDEPENDIENTE**—Filtra solo los paquetes no destinados a la dirección IP del suscriptor y al puerto x:x, independientemente de la dirección IP del host externo y el origen del puerto (z:z). El dispositivo Citrix ADC reenvía los paquetes destinados a X:x. En otras palabras, enviar paquetes desde el suscriptor a cualquier dirección IP externa es suficiente para permitir paquetes desde cualquier host externo al suscriptor.
* **DIRECCIÓN DEPENDIENTE**—Filtra los paquetes no destinados a la dirección IP del suscriptor y al puerto x:x. Además, el dispositivo filtra los paquetes de y:Y destinados al suscriptor (x:x) si el cliente no ha enviado previamente paquetes a y:AnyPort (independiente del puerto externo). En otras palabras, la recepción de paquetes de un host externo específico requiere que el suscriptor primero envíe paquetes a la dirección IP de ese host externo específico.
* **PUERTO DE DIRECCIÓN DEPENDIENTE** (valor predeterminado): Filtra los paquetes no destinados a la dirección IP del suscriptor y al puerto (x: X). Además, el dispositivo Citrix ADC filtra los paquetes de y:Y destinados al suscriptor (x:x) si el suscriptor no ha enviado previamente paquetes a y:y. En otras palabras, la recepción de paquetes de un host externo específico requiere que el suscriptor primero envíe paquetes a esa dirección IP externa y puerto.

Valores posibles: ENDPOINT-INDEPENDENT, ADDRESS-DEPENDENT, ADDRESS-PORT-DEPENDENT

Valor predeterminado: ADDRESS-PORT-DEPENDENT

– Tcpproxy

Habilite el proxy TCP, que permite al dispositivo Citrix ADC optimizar el tráfico TCP mediante funciones de capa 4.

Valores posibles: ENABLED, DISABLED

Valor predeterminado: DISABLED

– td

Id. del dominio de tráfico a través del cual el dispositivo Citrix ADC envía el tráfico saliente después de realizar LSN.

Si no especifica un identificador, el dispositivo envía el tráfico saliente a través del dominio de tráfico predeterminado, que tiene un identificador de 0.

Valor predeterminado: 65535

Valor máximo: 65535

Descripciones de parámetros (de los comandos enumerados en el procedimiento CLI)

- bind lsn appsprofile
  - appsprofilename

    Nombre del perfil de aplicación LSN. Debe comenzar con un carácter alfanumérico o de subrayado (_) ASCII y debe contener solo caracteres alfanuméricos ASCII, guión bajo, hash (#), punto (.), espacio, dos puntos (:), en (@), igual (=) y guión (-). No se puede cambiar después de crear el perfil de aplicación LSN. El siguiente requisito solo se aplica a la CLI: Si el nombre incluye uno o más espacios, escriba el nombre entre comillas dobles o simples (por ejemplo, “lsn application profile1” o ‘lsn application profile1’).

    Este es un argumento obligatorio. Longitud máxima: 127
  - lsnport

    Números de puerto o rango de números de puerto para que coincidan con el puerto de destino del paquete entrante de un suscriptor. Cuando se compara el puerto de destino, se aplica el perfil de aplicación LSN para la sesión LSN. Separe un intervalo de puertos con un guión. Por ejemplo, 40-90.

Descripciones de parámetros (de los comandos enumerados en el procedimiento CLI)

- agregar grupo lsn
  - groupname

    Nombre del grupo LSN. Debe comenzar con un carácter alfanumérico o de subrayado (_) ASCII y debe contener solo caracteres alfanuméricos ASCII, guión bajo, hash (#), punto (.), espacio, dos puntos (:), en (@), igual (=) y guión (-). No se puede cambiar después de crear el grupo LSN. El siguiente requisito solo se aplica a la CLI: Si el nombre incluye uno o más espacios, escriba el nombre entre comillas dobles o simples (por ejemplo, “lsn group1” o ‘lsn group1’).

    Este es un argumento obligatorio. Longitud máxima: 127
  - nombre_cliente

    Nombre de la entidad cliente LSN que se asociará con el grupo LSN. Solo puede asociar una entidad de cliente LSN a un grupo LSN. No puede quitar esta asociación ni reemplazarla con otra entidad cliente LSN una vez creado el grupo LSN.

    Este es un argumento obligatorio. Longitud máxima: 127
  - Tipo de natación

    Tipo de dirección IP NAT y asignación de puertos (de los grupos LSN enlazados) para los suscriptores:

Las opciones disponibles funcionan de la siguiente manera:

* **Determinista**: Asigne una dirección IP NAT y un bloque de puertos a cada suscriptor (del cliente LSN vinculado al grupo LSN). El dispositivo Citrix ADC asigna secuencialmente recursos NAT a estos suscriptores. El dispositivo Citrix ADC asigna el primer bloque de puertos (tamaño de bloque determinado por el parámetro de tamaño de bloque de puerto del grupo LSN) en la dirección IP NAT inicial a la dirección IP del suscriptor inicial. El siguiente rango de puertos se asigna al siguiente suscriptor, y así sucesivamente, hasta que la dirección NAT no tenga suficientes puertos para el siguiente suscriptor. En este caso, el primer bloque de puerto en la siguiente dirección NAT se utiliza para el suscriptor, y así sucesivamente. Dado que cada suscriptor recibe ahora una dirección IP NAT determinista y un bloque de puertos, se puede identificar un suscriptor sin necesidad de registro. Para una conexión, un suscriptor se puede identificar basándose únicamente en la dirección IP NAT y el puerto, así como en la dirección IP y el puerto de destino.
* **Dinámico**: Asigne una dirección IP NAT aleatoria y un puerto del grupo NAT LSN para la conexión de un suscriptor. Si la asignación de bloques de puertos está habilitada (en el grupo LSN) y se especifica un tamaño de bloque de puertos (en el grupo LSN), el dispositivo Citrix ADC asigna una dirección IP NAT aleatoria y un bloque de puertos para un suscriptor cuando inicia una conexión por primera vez. El dispositivo asigna esta dirección IP NAT y un puerto (del bloque de puertos asignado) para diferentes conexiones de este suscriptor. Si se asignan todos los puertos (para diferentes conexiones de suscriptores) desde el bloque de puertos asignado a los suscriptores, el dispositivo asigna un nuevo bloque de puertos aleatorio para el suscriptor.

Valores posibles: DYNAMIC, DETERMINISTIC

Valor predeterminado: DYNAMIC

– portblocksize

Tamaño del bloque de puerto NAT que se asignará para cada suscriptor.

Para establecer este parámetro para NAT dinámica, debe habilitar el parámetro de asignación de bloque de puerto en el grupo LSN enlazado. Para NAT determinista, el parámetro de asignación de bloque de puerto siempre está habilitado y no puede inhabilitarlo.

En NAT dinámica, el dispositivo Citrix ADC asigna un bloque de puerto NAT aleatorio, desde el grupo de puertos NAT disponible de una dirección IP NAT, para cada suscriptor. Para un suscriptor, si todos los puertos se asignan desde el bloque de puerto asignado a los suscriptores, el dispositivo asigna un nuevo bloque de puerto aleatorio para el suscriptor.

– logging

Entradas de asignación de registros y sesiones creadas o eliminadas para este grupo LSN. El dispositivo Citrix ADC registra las sesiones LSN para este grupo LSN solo cuando los parámetros de registro y registro de sesión están habilitados.

El dispositivo utiliza su marco de registro de auditoría y syslog existente para registrar la información de LSN. Debe habilitar el registro LSN de nivel global habilitando el parámetro LSN en las entidades de acción NSLOG y SYLOG relacionadas. Cuando se habilita el parámetro Logging, el dispositivo Citrix ADC genera mensajes de registro relacionados con asignaciones LSN y sesiones LSN de este grupo LSN. A continuación, el dispositivo envía estos mensajes de registro a los servidores asociados con la acción NSLOG y las entidades de acciones SYSLOG.

Un mensaje de registro para una entrada de asignación LSN consta de la siguiente información:

* Dirección NSIP del dispositivo Citrix ADC
* Marca de tiempo
* Tipo de entrada (MAPPING o SESSION)
* Si se crea o elimina la entrada de asignación LSN
* Dirección IP, puerto e ID de dominio de tráfico del suscriptor
* Dirección IP NAT y puerto
* Nombre del protocolo
* La dirección IP de destino, el puerto y el ID de dominio de tráfico pueden estar presentes, en función de las condiciones siguientes:
  - La dirección IP de destino y el puerto no se registran para la asignación independiente del punto final
  - Solo se registra la dirección IP de destino (y no el puerto) para la asignación dependiente de direcciones
  - La dirección IP de destino y el puerto se registran para la asignación dependiente del puerto de direcciones

Valores posibles: ENABLED, DISABLED

Valor predeterminado: DISABLED

– SessionLogging

Sesiones de registro creadas o eliminadas para el grupo LSN. El dispositivo Citrix ADC registra las sesiones LSN para este grupo LSN solo cuando los parámetros de registro y registro de sesión están habilitados.

Un mensaje de registro para una sesión LSN consta de la siguiente información:

* Dirección NSIP del dispositivo Citrix ADC
* Marca de tiempo

* Tipo de entrada (MAPPING o SESSION)
* Si se crea o elimina la sesión LSN
* Dirección IP, puerto e ID de dominio de tráfico del suscriptor
* Dirección IP NAT y puerto
* Nombre del protocolo
* Dirección IP de destino, puerto e ID de dominio de tráfico

Valores posibles: ENABLED, DISABLED

Valor predeterminado: DISABLED

- SessionSync

  En una implementación de alta disponibilidad (HA), sincronice la información de todas las sesiones LSN relacionadas con este grupo LSN con el nodo secundario. Después de una conmutación por error, las conexiones TCP establecidas y los flujos de paquetes UDP se mantienen activos y se reanudan en el nodo secundario (nuevo primario).

  Para que esta configuración funcione, debe habilitar el parámetro de sincronización de sesión global.

  Valores posibles: ENABLED, DISABLED

  Valor predeterminado: ENABLED

- snmptraplimit

  Número máximo de mensajes de captura SNMP que se pueden generar para el grupo LSN en un minuto.

  Valor predeterminado: 100

  Valor mínimo: 0

  Valor máximo: 10000

- ftp

  Habilite la puerta de enlace de capa de aplicación (ALG) para el protocolo FTP. Para algunos protocolos de capa de aplicación, las direcciones IP y los números de puerto de protocolo generalmente se comunican en la carga útil de los paquetes. Cuando actúa como ALG, el dispositivo cambia la carga útil de los paquetes para asegurarse de que el protocolo continúa funcionando sobre LSN.

  Nota: El dispositivo Citrix ADC también incluye ALG para protocolos ICMP y TFTP. ALG para el protocolo ICMP está habilitado de forma predeterminada, y no hay ninguna disposición para inhabilitarlo. ALG para el protocolo TFTP está inhabilitado de forma predeterminada. ALG se habilita automáticamente para un grupo LSN cuando se vincula un perfil de aplicación UDP LSN, con asignación independiente del punto final, filtrado independiente del punto final y puerto de destino como 69 (puerto conocido para TFTP), al grupo LSN.

Valores posibles: ENABLED, DISABLED

Valor predeterminado: ENABLED

Descripciones de parámetros (de los comandos enumerados en el procedimiento CLI)

- enlazar grupo lsn
  - groupname

    Nombre del grupo LSN. Debe comenzar con un carácter alfanumérico o de subrayado (_) ASCII y debe contener solo caracteres alfanuméricos ASCII, guión bajo, hash (#), punto (.), espacio, dos puntos (:), en (@), igual (=) y guión (-). No se puede cambiar después de crear el grupo LSN. El siguiente requisito solo se aplica a la CLI: Si el nombre incluye uno o más espacios, escriba el nombre entre comillas dobles o simples (por ejemplo, "lsn group1" o 'lsn group1').

    Este es un argumento obligatorio. Longitud máxima: 127

  - poolname

    Nombre del grupo LSN que se va a enlazar al grupo LSN especificado. Solo se pueden enlazar grupos LSN y grupos LSN con la misma configuración de tipo NAT. Los grupos LSN múltiples se pueden enlazar a un grupo LSN.

    Para NAT determinista, los grupos enlazados a un grupo LSN no se pueden vincular a otros grupos LSN. Para NAT dinámico, los grupos enlazados a un grupo LSN se pueden enlazar a varios grupos LSN. Longitud máxima: 127

  - transportprofilename

    Nombre del perfil de transporte LSN que se va a enlazar al grupo LSN especificado. Enlazar un perfil para cada protocolo para el que quiera especificar la configuración.

    De forma predeterminada, un perfil de transporte LSN con la configuración predeterminada para los protocolos TCP, UDP e ICMP está enlazado a un grupo LSN durante su creación. Este perfil se denomina transporte predeterminado.

    Un perfil de transporte LSN que se vincula a un grupo LSN anula el perfil de transporte LSN predeterminado para ese protocolo. Longitud máxima: 127

  - appsprofilename

    Nombre del perfil de aplicación LSN que se va a enlazar al grupo LSN especificado. Para cada conjunto de puertos de destino, vincule un perfil para cada protocolo para el que quiera especificar la configuración.

    De forma predeterminada, un perfil de aplicación LSN con configuración predeterminada para los protocolos TCP, UDP e ICMP para todos los puertos de destino está enlazado a un

grupo LSN durante su creación. Este perfil se denomina perfil de aplicación predeterminado.

Cuando vincula un perfil de aplicación LSN, con un conjunto especificado de puertos de destino, a un grupo LSN, el perfil enlazado reemplaza el perfil de aplicación LSN predeterminado para ese protocolo en ese conjunto de puertos de destino. Longitud máxima: 127

Configuraciones LSN de ejemplo

January 12, 2021

Los siguientes son ejemplos de configuración de LSN a través de la interfaz de línea de comandos.

Cree una configuración LSN simple con una única red de suscriptor, una sola dirección IP NAT LSN y una configuración predeterminada:

```
add lsn client LSN-CLIENT-1

Done

bind lsn client LSN-CLIENT-1 -network 192.0.2.0 -netmask 255.255.255.0

Done

add lsn pool LSN-POOL-1

Done

bind lsn pool LSN-POOL-1 203.0.113.3

Done

add lsn group LSN-GROUP-1 -clientname LSN-CLIENT-1

Done

bind lsn group LSN-GROUP-1 -poolname pool1 LSN-POOL-1

Done
<!--NeedCopy-->
```


Cree una configuración de LSN con una ACL extendida para identificar suscriptores de LSN:

```
add ns acl LSN-ACL-2 ALLOW -srcIP 192.0.2.10-192.0.2.20

Done

apply acls

Done

add lsn client LSN-CLIENT-2

Done

bind lsn client LSN-CLIENT-2  -aclname LSN-ACL-2

Done

add lsn pool LSN-POOL-2

Done

bind lsn pool LSN-POOL-2 203.0.113.5-203.0.113.10

Done

add lsn group LSN-GROUP-2 -clientname LSN-CLIENT-2

Done

bind lsn group LSN-GROUP-2 -poolname LSN-POOL-2

Done
<!--NeedCopy-->
```

Cree una configuración LSN con asignación independiente del punto final para el protocolo HTTP (puerto 80) y asignación dependiente del puerto de direcciones para el protocolo SSH (puerto 22). Además, restrinja a cada suscriptor para que utilice un máximo de 1000 puertos NAT para el protocolo TCP y 100 puertos NAT para el protocolo UDP. Restringir cada suscriptor para tener un máximo de 2000 sesiones simultáneas para el protocolo TCP. Restringir el grupo para que tenga un máximo de 30000 sesiones simultáneas para el protocolo TCP:


```
add lsn client LSN-CLIENT-3

Done

bind lsn client LSN-CLIENT-3 -network 192.0.3.0 -netmask 255.255.255.0

Done

add lsn pool LSN-POOL-3

Done

bind lsn pool LSN-POOL-3 203.0.113.11

Done

add lsn group LSN-GROUP-3 -clientname LSN-CLIENT-3

Done

bind lsn group LSN-GROUP-3 -poolname LSN-POOL-3

Done

add lsn appsprofile LSN-APPS-HTTPPROFILE-3 TCP -mapping ENDPOINT-
    INDEPENDENT

Done

bind lsn appsprofile LSN-APPS-HTTPPROFILE-3 80

Done

bind lsn group LSN-GROUP-3 -applicationprofilename LSN-APPS-HTTPPROFILE
    -3

Done

add lsn appsprofile LSN-APPS-SSHPROFILE-3 TCP -mapping ADDRESS-PORT-
    DEPENDENT

Done

bind lsn appsprofile LSN-APPS-SSHPROFILE-3 22
```



```
42
43 Done
44
45 bind lsn group LSN-GROUP-3 -applicationprofilename LSN-APPS-SSHPROFILE
       -3
46
47 Done
48
49 add lsn transportprofile LSN-TRANS-PROFILE-TCP-3 TCP -portquota 1000 -
       sessionquota 2000 -groupSessionLimit 30000
50
51 Done
52
53 bind lsn group LSN-GROUP-3 -transportprofilename LSN-TRANS-PROFILE-TCP
       -3
54
55 Done
56
57 add lsn transportprofile LSN-TRANS-PROFILE-UDP-3 UDP -portquota 100
58
59 Done
60
61 bind lsn group LSN-GROUP-3 -transportprofilename LSN-TRANS-PROFILE-UDP
       -3
62
63 Done
64 <!--NeedCopy-->
```

Cree una configuración de LSN para un gran conjunto de suscriptores:

```
1  add lsn client LSN-CLIENT-4
2
3  Done
4
5  bind lsn client LSN-CLIENT-4 -network 192.0.4.0 -netmask 255.255.255.0
6
7  Done
8
9  bind lsn client LSN-CLIENT-4 -network 192.0.5.0 -netmask 255.255.255.0
10
11 Done
12
13 bind lsn client LSN-CLIENT-4 -network 192.0.6.0 -netmask 255.255.255.0
```



```
14
15 Done
16
17 bind lsn client LSN-CLIENT-4 -network 192.0.7.0 -netmask 255.255.255.0
18
19 Done
20
21 bind lsn client LSN-CLIENT-4 -network 192.0.8.0 -netmask 255.255.255.0
22
23 Done
24
25 add lsn pool LSN-POOL-4
26
27 Done
28
29 bind lsn pool LSN-POOL-4 203.0.113.30-203.0.113.40
30
31 Done
32
33 bind lsn pool LSN-POOL-4 203.0.113.45-203.0.113.50
34
35 Done
36
37 bind lsn pool LSN-POOL-4 203.0.113.55-203.0.113.60
38
39 Done
40
41 add lsn group LSN-GROUP-4 -clientname LSN-CLIENT-4
42
43 Done
44
45 bind lsn group LSN-GROUP-4 -poolname LSN-POOL-4
46
47 Done
48
49 add lsn appsprofile LSN-APPS-WELLKNOWNPROFILE-4 TCP -mapping ENDPOINT-
      INDEPENDENT
50
51 Done
52
53 bind lsn appsprofile LSN-APPS-WELLKNOWN-PORTS-PROFILE-4 1- 1023
54
55 Done
56
57 bind lsn group LSN-GROUP-4 -applicationprofilename LSN-APPS-WELLKNOWN-
```



```
    PORTS-PROFILE-4

Done
<!--NeedCopy-->
```

Cree una configuración de LSN con el uso compartido de recursos NAT entre varios grupos LSN. En este ejemplo, el grupo LSN LSN-POOL-5 se comparte con los grupos LSN LSN-GROUP-5 y LSN-GROUP-6:

```
add lsn client LSN-CLIENT-5

Done

bind lsn client LSN-CLIENT-5 -network 192.0.15.0 -netmask 255.255.255.0

Done

add lsn pool LSN-POOL-5

Done

bind lsn pool LSN-POOL-5 203.0.113.12-203.0.113.14

Done

add lsn group LSN-GROUP-5 -clientname LSN-CLIENT-5

Done

bind lsn group LSN-GROUP-5 -poolname LSN-POOL-5

Done

add lsn client LSN-CLIENT-6

Done

bind lsn client LSN-CLIENT-6 -network 192.0.16.0 -netmask 255.255.255.0

Done

add lsn pool LSN-POOL-6

```



```
Done

bind lsn pool LSN-POOL-6 203.0.113.15-203.0.113.18

Done

add lsn group LSN-GROUP-6 -clientname LSN-CLIENT-6

Done

bind lsn group LSN-GROUP-6 -poolname LSN-POOL-6

Done

bind lsn group LSN-GROUP-6 -poolname LSN-POOL-5

Done
<!--NeedCopy-->
```

Cree una configuración LSN con asignación determinista de recursos NAT:

```
add lsn client LSN-CLIENT-7

Done

bind lsn client LSN-CLIENT-7 -network 192.0.17.0 -netmask 255.255.255.0

Done

add lsn pool LSN-POOL-7 -nattype DETERMINISTIC

Done

bind lsn pool LSN-POOL-7 203.0.113.19-203.0.113.23

Done

add lsn group LSN-GROUP-7 -clientname LSN-CLIENT-7 -nattype
   DETERMINISTIC -portblocksize 1024

Done

bind lsn group LSN-GROUP-7 -poolname LSN-POOL-7
```



```
22
23 Done
24 <!--NeedCopy-->
```

Cree una configuración LSN con varias redes de suscriptor que tengan la misma dirección de red pero cada red pertenezca a un dominio de tráfico diferente. Además, restrinja el tráfico saliente relacionado con el protocolo HTTP (puerto 80), enviándolo a través de un dominio de tráfico particular (td 5):

```
1  add lsn client LSN-CLIENT-8
2
3  Done
4
5  bind lsn client LSN-CLIENT-8 -network 192.0.18.0 -netmask 255.255.255.0
       -td 1
6
7  Done
8
9  bind lsn client LSN-CLIENT-8 -network 192.0.18.0 -netmask 255.255.255.0
       -td 2
10
11 Done
12
13 bind lsn client LSN-CLIENT-8 -network 192.0.18.0 -netmask 255.255.255.0
       -td 3
14
15 Done
16
17 add lsn pool LSN-POOL-8
18
19 Done
20
21 bind lsn pool LSN-POOL-8 203.0.113.80-203.0.113.86
22
23 Done
24
25 add lsn group LSN-GROUP-8 -clientname LSN-CLIENT-8
26
27 Done
28
29 bind lsn group LSN-GROUP-8 -poolname LSN-POOL-8
30
31 Done
```



```
32
33 add lsn appsprofile LSN-APPS-HTTP-PROFILE-8 TCP -td 5
34
35 Done
36
37 bind lsn appsprofile LSN-APPS-HTTP-PROFILE-8 80
38
39 Done
40
41 bind lsn group LSN-GROUP-8 -applicationprofilename LSN-APPS-HTTP-
      PROFILE-8
42
43 Done
44 <!--NeedCopy-->
```

Cree una configuración LSN que restrinja el tráfico saliente de un protocolo específico (TCP), enviándolo a través de un dominio de tráfico determinado (td 5). Con el filtrado independiente del punto final, reciba tráfico entrante relacionado con este protocolo (TCP) en cualquier dominio de tráfico:

```
1  add lsn client LSN-CLIENT-9
2
3  Done
4
5  bind lsn client LSN-CLIENT-9 -network 192.0.9.0 -netmask 255.255.255.0
       -td 1
6
7  Done
8
9  add lsn pool LSN-POOL-9
10
11 Done
12
13 bind lsn pool LSN-POOL-9 203.0.113.90
14
15 Done
16
17 add lsn group LSN-GROUP-9 -clientname LSN-CLIENT-9
18
19 Done
20
21 bind lsn group LSN-GROUP-9 -poolname LSN-POOL-9
22
```



```
Done

add lsn appsprofile LSN-APPS-PROFILE-9 TCP -filtering ENDPOINT-
    INDEPENDENT -td 5

Done

bind lsn group LSN-GROUP-9 -approfile LSN-APPS-PROFILE-9

Done
<!--NeedCopy-->
```

Cree una configuración LSN que restrinja el tráfico HTTP saliente (puerto 80), enviándolo a través de un dominio de tráfico determinado (td 10). Con el filtrado dependiente de la dirección, reciba el tráfico entrante relacionado con este protocolo (HTTP) en el dominio de tráfico especificado (td 10):

```
add lsn client LSN-CLIENT-10

Done

bind lsn client LSN-CLIENT-10 -network 192.0.10.0 -netmask
    255.255.255.0 -td 1

Done

add lsn pool LSN-POOL-10

Done

bind lsn pool LSN-POOL-10 203.0.113.100

Done

add lsn group LSN-GROUP-10 -clientname LSN-CLIENT-10

Done

bind lsn group LSN-GROUP-10 -poolname LSN-POOL-10

Done

add lsn appsprofile LSN-APPS-PROFILE-10 TCP -mapping ENDPOINT -
```



```
      INDEPENDENT -filtering ADDRESS-DEPENDENT -td 10

Done

bind lsn appsprofile LSN-APPS-PROFILE-10 80

Done

bind lsn group LSN-GROUP-10 -approfile LSN-APPS-PROFILE-10

Done
<!--NeedCopy-->
```

Configuración de mapas estáticos LSN

January 12, 2021

El dispositivo Citrix ADC admite la creación manual de una asignación de LSN uno a uno entre una dirección IP del suscriptor:puerto y una dirección IP NAT: Puerto. Las asignaciones LSN estáticas son útiles en los casos en que quiere asegurarse de que las conexiones iniciadas a un NAT IP: Port se asignan a la dirección IP del suscriptor:Port. Por ejemplo, servidores web ubicados en la red interna.

Para crear una asignación de LSN estática mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
add lsn static <name> <transportprotocol> <subscrIP> <subscrPort> [-td
    <positive_integer>] [<natIP> [<natPort>]] [-destIP <ip_addr> [-dsttd
     <positive_integer>]]
-  show lsn static
<!--NeedCopy-->
```

Para crear una asignación de LSN estática mediante la utilidad de configuración

Vaya a Sistema > NAT a gran escala > Estático y agregue una nueva asignación estática.

Descripciones de parámetros (de los comandos enumerados en el procedimiento CLI)

add lsn nombre estático

Nombre de la entrada de asignación estática LSN. Debe comenzar con un carácter alfanumérico o de subrayado (_) ASCII y debe contener solo caracteres alfanuméricos ASCII, guión bajo, hash (#), punto (.), espacio, dos puntos (:), en (@), igual (=) y guión (-). No se puede cambiar después de crear el grupo LSN. El siguiente requisito solo se aplica a la CLI: Si el nombre incluye uno o más espacios, escriba el nombre entre comillas dobles o simples (por ejemplo, “lsn static1” o ‘lsn static1’). Este es un argumento obligatorio. Longitud máxima: 127

transportprotocol

Protocolo para la entrada de asignación LSN. Este es un argumento obligatorio. Valores posibles: TCP, UDP, ICMP

subscrIP

Dirección IPv4 de un suscriptor LSN para la entrada de asignación LSN. Este es un argumento obligatorio.

subscrPort

Puerto del suscriptor LSN para la entrada de asignación LSN. Este es un argumento obligatorio. Valor máximo: 65535

td

ID del dominio de tráfico al que pertenece el suscriptor. Si no especifica un ID, se supone que el suscriptor forma parte del dominio de tráfico predeterminado. Valor predeterminado: 0, Valor mínimo: 0, Valor máximo: 4094

natIP

Dirección IPv4, ya existente en el dispositivo Citrix ADC como tipo LSN, que se utilizará como dirección IP NAT para esta entrada de asignación.

natPort

Puerto NAT para esta entrada de asignación LSN.

destIP

Dirección IP de destino para la entrada de asignación LSN.

Dsttd

Id. del dominio de tráfico a través del cual se puede acceder a la dirección IP de destino para esta entrada de asignación de LSN desde el dispositivo Citrix ADC. Si no especifica un ID, se supone que la dirección IP de destino es accesible a través del dominio de tráfico predeterminado, que tiene un ID de 0. Valor predeterminado: 0, Valor mínimo: 0, Valor máximo: 4094

Mapas estáticos de puerto comodín

Una entrada de asignación estática suele ser una asignación de LSN uno a uno entre una dirección IP del suscriptor:puerto y una dirección IP NAT: Puerto. Una entrada de asignación de LSN estática de uno a uno expone solo un puerto del suscriptor a Internet.

Algunas situaciones pueden requerir exponer todos los puertos (64K) de un suscriptor a Internet (por ejemplo, un servidor alojado en una red interna y ejecutar un servicio diferente en cada puerto). Para hacer que estos servicios internos sean accesibles a través de Internet, debe exponer todos los puertos del servidor a Internet.

Una forma de cumplir este requisito es agregar 64K entradas de asignación estática uno a uno, una entrada de asignación para cada puerto. Crear entradas de 64K es muy engorroso y una gran tarea. Además, este gran número de entradas de configuración puede provocar problemas de rendimiento en el dispositivo Citrix ADC.

Otro método simple es usar puertos comodín en una entrada de asignación estática. Solo necesita crear una entrada de mapeo estático con parámetros NAT-port y subscriber-port establecidos en el carácter comodín (*), y el parámetro de protocolo establecido en ALL, para exponer todos los puertos de un suscriptor a Internet. Para las conexiones entrantes o salientes de un suscriptor que coinciden con una entrada de asignación estática de comodín, el puerto del suscriptor no cambia después de la operación NAT.

Cuando una conexión a Internet iniciada por el suscriptor coincide con una entrada de asignación estática comodín, el dispositivo Citrix ADC asigna un puerto NAT que tiene el mismo número que el puerto del suscriptor desde el que se inicia la conexión. Del mismo modo, un host de Internet se conecta al puerto de un suscriptor mediante la conexión al puerto NAT que tiene el mismo número que el puerto del suscriptor.

Configuración del dispositivo Citrix ADC para proporcionar acceso a todos los puertos de un suscriptor IPv4

Para configurar el dispositivo Citrix ADC para proporcionar acceso a todos los puertos de un suscriptor IPv4, cree un mapa estático comodín con los siguientes parámetros obligatorios:

- Protocolo=Todos
- Puerto del suscriptor = *
- Puerto NAT = *

En un mapa estático comodín, a diferencia de un mapa estático uno a uno, establecer el parámetro IP NAT es obligatorio. Además, la dirección IP NAT asignada a un mapa estático de comodín no se puede utilizar para ningún otro suscriptor.

Para crear un mapa estático comodín mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
add lsn static <name> ALL <subscrIP> *  <natIP> * [-td <
   positive_integer>] [-destIP <ip_addr> [-dsttd <positive_integer>]]

show lsn static
<!--NeedCopy-->
```

Configuración de ejemplo

En el siguiente ejemplo de configuración de un mapa estático de comodín, todos los puertos de un suscriptor cuya dirección IP es 192.0.2.10 se hacen accesibles a través de NAT IP 203.0.11.33.

Configuración de ejemplo:

```
add lsn static NAT44-WILDCARD-STATIC-1 ALL  192.0.2.10 * 203.0.113.33 *

Done
<!--NeedCopy-->
```

Configuración de puertas de enlace de capa de aplicación

January 12, 2021

Para algunos protocolos de capa de aplicación, las direcciones IP y los números de puerto de protocolo también se comunican en la carga útil del paquete. La puerta de enlace de capa de aplicación para un protocolo analiza la carga útil del paquete y realiza los cambios necesarios para garantizar que el protocolo continúa funcionando sobre LSN.

El dispositivo Citrix ADC admite ALG para los siguientes protocolos:

- FTP
- ICMP
- TFTP
- PPTP
- SIP
- RTSP

Puerta de enlace de capa de aplicación para protocolos FTP, ICMP y TFTP

January 12, 2021

Puede habilitar o inhabilitar ALG para el protocolo FTP para una configuración LSN habilitando o inhabilitando la opción FTP del grupo LSN de la configuración LSN.

ALG para el protocolo ICMP está habilitado de forma predeterminada, y no hay ninguna disposición para inhabilitarlo.

ALG para el protocolo TFTP está inhabilitado de forma predeterminada. TFTP ALG se habilita automáticamente para una configuración LSN cuando se vincula un perfil de aplicación UDP LSN, con asignación independiente del punto final, filtrado independiente del punto final y puerto de destino como 69 (puerto conocido para TFTP), al grupo LSN.

Ejemplo de configuración LSN para ALG FTP:
En la siguiente configuración LSN de ejemplo, FTP ALG está habilitado para suscriptores que tienen dirección IP en el rango 192.0.2.30-192.0.2.100.

```
1 add ns acl LSN-ACL-1 ALLOW -srcIP 192.0.2.30-192.0.2.100
2
3 Done
4
5 apply acls
6
7 Done
8
9 add lsn client LSN-CLIENT-1
```



```
10
11 Done
12
13 bind lsn client LSN-CLIENT-1  - aclname LSN-ACL
14
15 Done
16
17 add lsn pool LSN-POOL-1
18
19 Done
20
21 bind lsn pool LSN-POOL-1 203.0.113.10
22
23 Done
24
25 add lsn group LSN-GROUP-1 -clientname LSN-CLIENT-1  -FTP ENABLED
26
27 Done
28
29 bind lsn group LSN-GROUP-1 -poolname pool1 LSN-POOL-1
30
31 Done
32 <!--NeedCopy-->
```

Ejemplo de configuración LSN para TFTP ALG:

En la siguiente configuración LSN de ejemplo, la asignación independiente del punto final y el filtrado independiente del punto final están habilitados para el protocolo TFTP (puerto UDP 69). El dispositivo Citrix ADC habilita automáticamente TFTP ALG para esta configuración de LSN.

```
1 add lsn client LSN-CLIENT-2
2
3 Done
4
5 bind lsn client LSN-CLIENT-2 -network 198.51.100.0 -netmask
     255.255.255.0
6
7 Done
8
9 add lsn pool LSN-POOL-2
10
11 Done
12
13 bind lsn pool LSN-POOL-2 203.0.113.10-203.0.113.11
```



```
14
15 Done
16
17 add lsn group LSN-GROUP-2 -clientname LSN-CLIENT-2
18
19 Done
20
21 bind lsn group LSN-GROUP-2 -poolname pool1 LSN-POOL-2
22
23 Done
24
25 add lsn appsprofile LSNAPPSPROFILE-TFTP-2 UDP -mapping ENDPOINT-
      INDEPENDENT  - filtering  ENDPOINT-INDEPENDENT
26
27 Done
28
29 bind lsn appsprofile LSNAPPSPROFILE-TFTP-2 69
30
31 Done
32
33 bind lsn group LSN-GROUP-1 -applicationprofilename LSNAPPSPROFILE-TFTP
      -2
34
35 Done
36 <!--NeedCopy-->
```

Puerta de enlace de capa de aplicación para protocolo PPTP

August 20, 2021

El dispositivo Citrix ADC admite puertas de enlace de capa de aplicación (ALG) para el Protocolo de túnel punto a punto (PPTP).

PPTP es un protocolo de red que permite la transferencia segura de datos desde un cliente remoto a un servidor empresarial mediante la creación de un túnel a través de redes de datos basadas en TCP/IP. PPTP encapsula paquetes PPP en paquetes IP para su transmisión a través de Internet. PPTP establece un túnel para cada par de servidores de red PPTP (PNS) comunicantes y concentrador de acceso PPTP (PAC). Una vez configurado el túnel, se utiliza la encapsulación de redirección genérica mejorada (GRE) para intercambiar paquetes PPP. Un ID de llamada en el encabezado GRE indica la sesión a la que pertenece un paquete PPP determinado.

El dispositivo Citrix ADC reconoce los paquetes PPTP que llegan al puerto TCP predeterminado, 1723.

El dispositivo analiza los paquetes de control PPTP, traduce el ID de llamada y asigna una dirección IP NAT. Para la comunicación de datos bidireccional entre el cliente y el servidor, el dispositivo Citrix ADC crea una entrada de sesión LSN basada en el ID de llamada del servidor y una sesión LSN basada en el ID de llamada del cliente. A continuación, el dispositivo analiza los paquetes de datos GRE y traduce los ID de llamada en función de las dos entradas de sesión LSN.

Para el protocolo PPTP, el dispositivo Citrix ADC también incluye la configuración de tiempo de espera para cualquier sesión PPTP LSN inactiva. Si una sesión PPTP LSN está inactiva durante un tiempo que supera el valor de tiempo de espera, el dispositivo Citrix ADC quita la sesión.

Limitaciones:

Las siguientes son las limitaciones de PPTP ALG en un dispositivo Citrix ADC:

- PPTP ALG no es compatible con el flujo LSN de horquilla.
- PPTP ALG no es compatible con ninguna configuración RNAT.
- PPTP ALG no es compatible con los clústeres de Citrix ADC.

Configuración de PPTP ALG

La configuración de PPTP ALG en el dispositivo Citrix ADC consta de las siguientes tareas:

- Cree una configuración LSN y habilite PPTP ALG en ella. En una configuración de LSN, el grupo LSN incluye la configuración PPTP ALG. Para obtener instrucciones sobre cómo crear una configuración LSN, consulte Pasos de configuración para LSN.
- (Opcional) Establezca el tiempo de espera global para las sesiones PPTP LSN inactivas.

Para habilitar PPTP ALG para una configuración LSN mediante la CLI

En el símbolo del sistema, escriba:

```
add lsn group <groupname> -clientname <string> [-pptp ( ENABLED |
   DISABLED )]

show lsn group
<!--NeedCopy-->
```

Para establecer el tiempo de espera global para las sesiones PPTP LSN inactivas mediante la CLI

En el símbolo del sistema, escriba:


```
set appAlgParam -pptpGreIdleTimeout <positive_integer>

show appAlgParam
<!--NeedCopy-->
```

Ejemplo:

En la siguiente configuración LSN de ejemplo, PPTP ALG está habilitado para suscriptores en la red 192.0.2.0/24.

También el tiempo de espera de la sesión PPTP LSN inactivo se establece en 200 segundos.

```
add lsn client LSN-CLIENT-1

Done

bind lsn client LSN-CLIENT-1 -network 192.0.2.0 -netmask 255.255.255.0

Done

add lsn pool LSN-POOL-1

Done

bind lsn pool LSN-POOL-1 203.0.113.3

Done

add lsn group LSN-GROUP-1 -clientname LSN-CLIENT-1  -pptp ENABLED

Done

bind lsn group LSN-GROUP-1 -poolname pool1 LSN-POOL-1

Done

set appAlgParam -pptpGreIdleTimeout 200

Done
<!--NeedCopy-->
```


Puerta de enlace de capa de aplicación para protocolo SIP

August 20, 2021

El uso de NAT de gran escala (LSN) con el Protocolo de inicio de sesión (SIP) es complicado, ya que los mensajes SIP contienen direcciones IP en los encabezados SIP, así como en el cuerpo SIP. Cuando LSN se utiliza con SIP, los encabezados SIP contienen información sobre la persona que llama y el receptor, y el dispositivo traduce esta información para ocultarla de la red externa. El cuerpo SIP contiene la información del Protocolo de descripción de la sesión (SDP), que incluye direcciones IP y números de puerto para la transmisión de los medios.

SIP ALG se adhiere a los siguientes RFC:

- RFC 3261
- RFC 3581
- RFC 4566
- RFC 4475

> **Nota**
>
> SIP ALG se admite en un dispositivo independiente de Citrix ADC, en una configuración de alta disponibilidad de Citrix ADC, así como en una configuración de clúster de Citrix ADC.

Cómo funciona SIP ALG

La forma en que se realiza la traducción de direcciones IP depende del tipo y la dirección del mensaje. Un mensaje puede ser cualquiera de los siguientes:

- Solicitud entrante
- Respuesta de salida
- Solicitud saliente
- Respuesta entrante

Para un mensaje saliente, la dirección IP privada y el número de puerto del cliente SIP se reemplazan por la dirección IP pública y el número de puerto propiedad de Citrix ADC, denominados *dirección IP del grupo LSN y número de puerto*, especificados durante la configuración de LSN. Para un mensaje entrante, la dirección IP del grupo LSN y el número de puerto se reemplazan por la dirección privada del cliente. Si el mensaje contiene direcciones IP públicas, Citrix ADC SIP ALG las conserva. Además, se crea un agujero de acceso en el:

- La dirección IP del grupo LSN y el puerto en nombre del cliente privado, de modo que los mensajes que llegan a esta dirección IP y puerto de la red pública se tratan como mensajes SIP.
- Dirección IP pública y puerto en nombre de los clientes públicos, de modo que los mensajes que llegan a esta dirección IP y puerto de la red privada se tratan como mensajes SIP.

Cuando se envía un mensaje SIP a través de la red, SIP Application Layer Gateway (ALG) recopila información del mensaje y traduce las direcciones IP de los siguientes encabezados en direcciones IP del grupo LSN:

- Vía
- Contacto
- Ruta
- Record-Route

En el siguiente mensaje de solicitud SIP de ejemplo, LSN reemplaza las direcciones IP en los campos de encabezado para ocultarlas de la red externa.

```
1 INVITE adam@10.102.185.156 SIP/2.0 Via: SIP/2.0/UDP 192.170.1.161:62914
      From: eve@10.120.210.3 To: adam@10.102.185.156 Call-ID: a12abcde@10
     .120.210.3 Contact: adam@10.102.185.156 Route: <sip:netscreen@10
     .150.20.3:5060> Record-Route: <sip:netscreen@10.150.20.3:5060>
2 <!--NeedCopy-->
```

Cuando llega un mensaje que contiene información SDP, SIP ALG recopila información del mensaje y traduce las direcciones IP de los siguientes campos en direcciones IP del grupo LSN y números de puerto:

- c= (información de conexión)

  Este campo puede aparecer en el nivel de sesión o de medios. Aparece en el siguiente formato:

  c=<network-type><address-type><connection-address>

  Si la dirección IP de destino es una dirección IP de unidifusión, el SIP ALG crea agujeros de acceso mediante la dirección IP y los números de puerto especificados en el campo m=.

- m= (anuncio de los medios)

  Este campo aparece en el nivel de medios y contiene la descripción del medio. Aparece en el siguiente formato:

  m=<media><port><transport><fmt list>

- a=(information about the media field)

  Este campo puede aparecer en el nivel de sesión o multimedia, con el siguiente formato:

  a=<attribute>

  a=<attribute>:<value>

En el siguiente extracto de una sección SDP de ejemplo se muestran los campos que se traducen para la asignación de recursos.

o=usuario 2344234 55234434 IN IP4 10.150.20.3

c=en IP4 10.150.20.3

m=audio 43249 RTP/AVP 0

La siguiente tabla muestra cómo se traduce la carga SIP.

Solicitud entrante (de público a privado)	A:	Ninguno
	De:	Ninguno
	Id. de llamada:	Ninguno
	Vía:	Ninguno
	URI de solicitud:	Reemplazar la dirección IP del grupo LSN por la dirección IP privada
	Contacto:	Ninguno
	Record-Route	Ninguno
	Ruta:	Ninguno
Respuesta saliente (de privado a público)	A:	Ninguno
	De:	Ninguno
	Id. de llamada:	Ninguno
	Vía:	Ninguno
	URI de solicitud:	Reemplazar la dirección IP privada con la dirección IP del grupo LSN
	Contacto:	Reemplazar la dirección IP privada con la dirección IP del grupo LSN
	Record-Route	Ninguno
	Ruta:	Ninguno
Solicitud saliente (de privado a público)	A:	Ninguno
	De:	Ninguno

	Id. de llamada:	Ninguno
	Vía:	Reemplazar la dirección IP privada con la dirección IP del grupo LSN
	URI de solicitud:	Ninguno
	Contacto:	Reemplazar la dirección IP privada con la dirección IP del grupo LSN
	Record-Route	Ninguno
	Ruta:	Ninguno
Respuesta entrante (de público a privado)	A:	Ninguno
	De:	Ninguno
	Id. de llamada:	Ninguno
	Vía:	Reemplazar la dirección IP del grupo LSN por la dirección IP privada
	URI de solicitud:	Ninguno
	Contacto:	Conservar la dirección IP pública, si está presente
	Record-Route	Ninguno
	Ruta:	Ninguno

Limitaciones de SIP ALG

Un SIP ALG tiene las siguientes limitaciones:

- Solo se admite la carga de SDP.
- Estas opciones no se admiten:
  - Direcciones IP de multidifusión
  - SDP cifrado
  - SIP TLS
  - Traducción FQDN
  - Autenticación de capa SIP

- TD/Partición
- Cuerpo con varias partes
- Mensajes SIP a través de una red IPv6
- Plegable de línea

Clientes SIP probados y servidores proxy

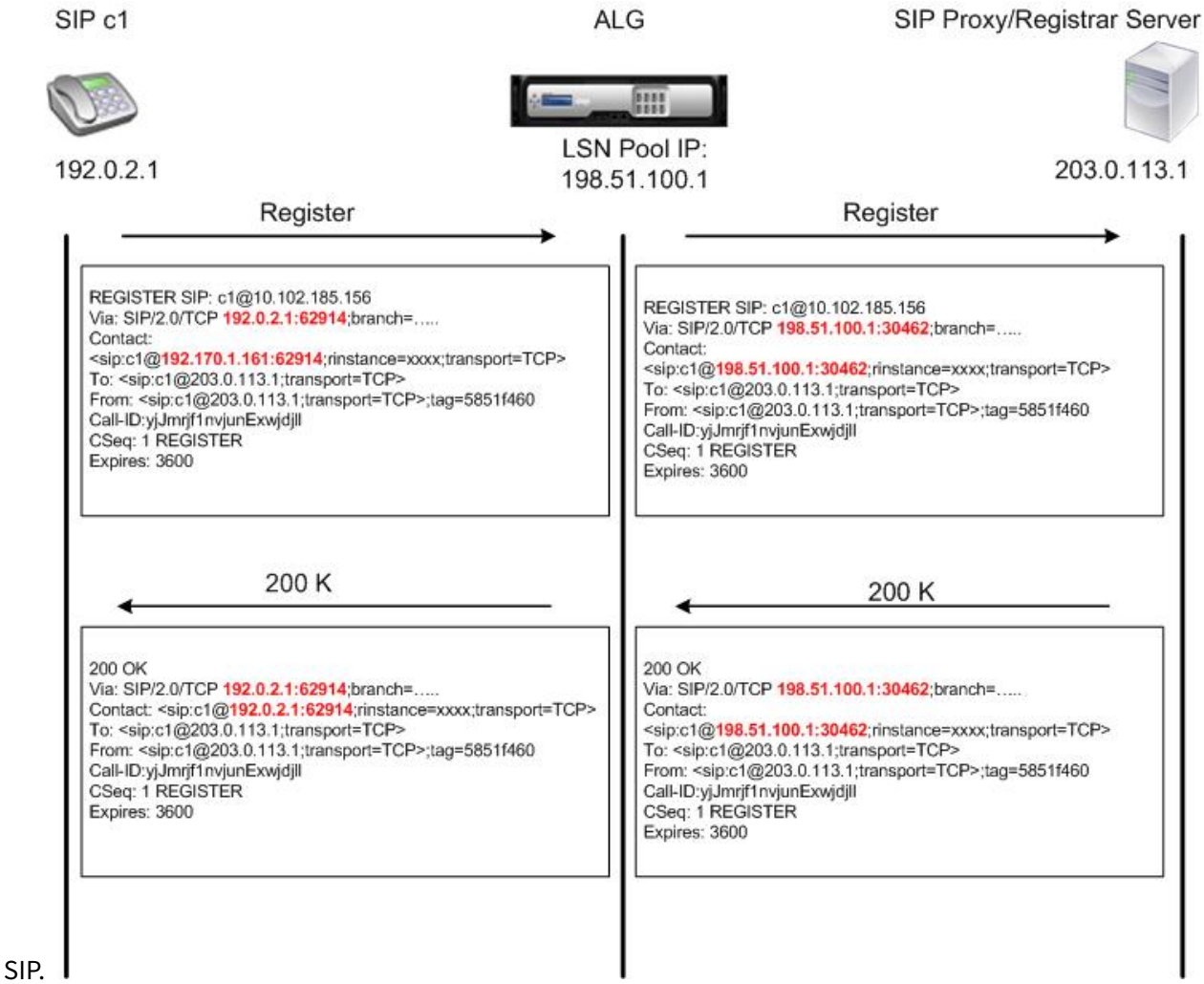
Los siguientes clientes SIP y servidor proxy se han probado con SIP ALG:

- **Clientes SIP:** X-Lite, Zoiper, Ekiga. Avaya
- **Servidor proxy:** OpenSIPS

Caso SIP LSN: Proxy SIP fuera de la red privada (red pública)

Registro de clientes SIP

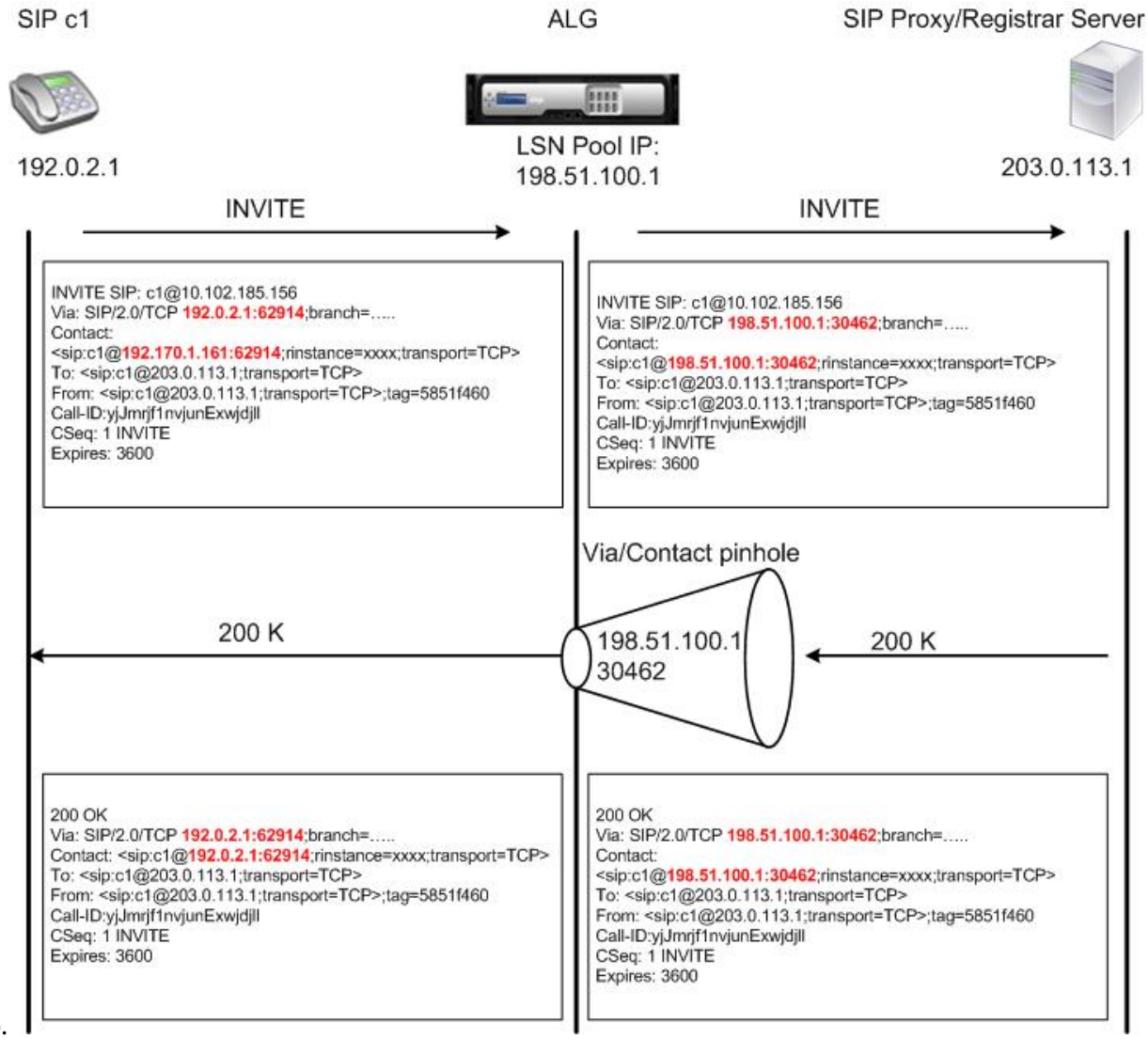
Para una llamada SIP típica, el cliente SIP debe registrarse con el registrador SIP componiendo una solicitud REGISTER y enviándola al registrador SIP. El SIP ALG del dispositivo Citrix ADC intercepta la solicitud, reemplaza la dirección IP y el número de puerto de la solicitud por la dirección IP del grupo LSN y el número de puerto proporcionados en la configuración de LSN, y reenvía la solicitud al registrador SIP. A continuación, el SIP ALG abre un agujero de acceso en la configuración de Citrix ADC para permitir una mayor comunicación SIP entre el cliente SIP y el registrador SIP. El registrador SIP envía una respuesta de 200 Aceptar al cliente SIP a través de la dirección IP del grupo LSN y el número de puerto. El dispositivo Citrix ADC captura esta respuesta en el agujero de acceso, y el SIP ALG reemplaza el encabezado SIP, volviendo a colocar los campos SIP Contacto, Vía, Ruta y Ruta de registro originales en el mensaje. A continuación, el SIP ALG reenvía el mensaje al cliente SIP. La siguiente ilustración muestra cómo SIP ALG utiliza LSN en un flujo de registro de llamadas



SIP.

Llamadas salientes

Una llamada SIP se inicia con un mensaje SIP INVITE enviado desde la red interna a la externa. El SIP ALG realiza NAT en las direcciones IP y los números de puerto en los campos de encabezado SIP Via, Contacto, Ruta y Record Route, reemplazándolos por la dirección IP del grupo LSN y el número de puerto. LSN almacena estas asignaciones para mensajes SIP posteriores en la llamada SIP. A continuación, el SIP ALG abre agujeros de acceso separados en la configuración de Citrix ADC para permitir SIP y medios a través del dispositivo Citrix ADC en los puertos asignados dinámicamente especificados en los encabezados SDP y SIP. Cuando un mensaje 200 Aceptar llega al Citrix ADC, se captura mediante uno de los agujeros de acceso creados. El SIP ALG reemplaza el encabezado SIP, restaurando los campos SIP Contacto, Vía, Ruta y Record Route SIP originales y, a continuación, reenvía el mensaje al cliente SIP in-

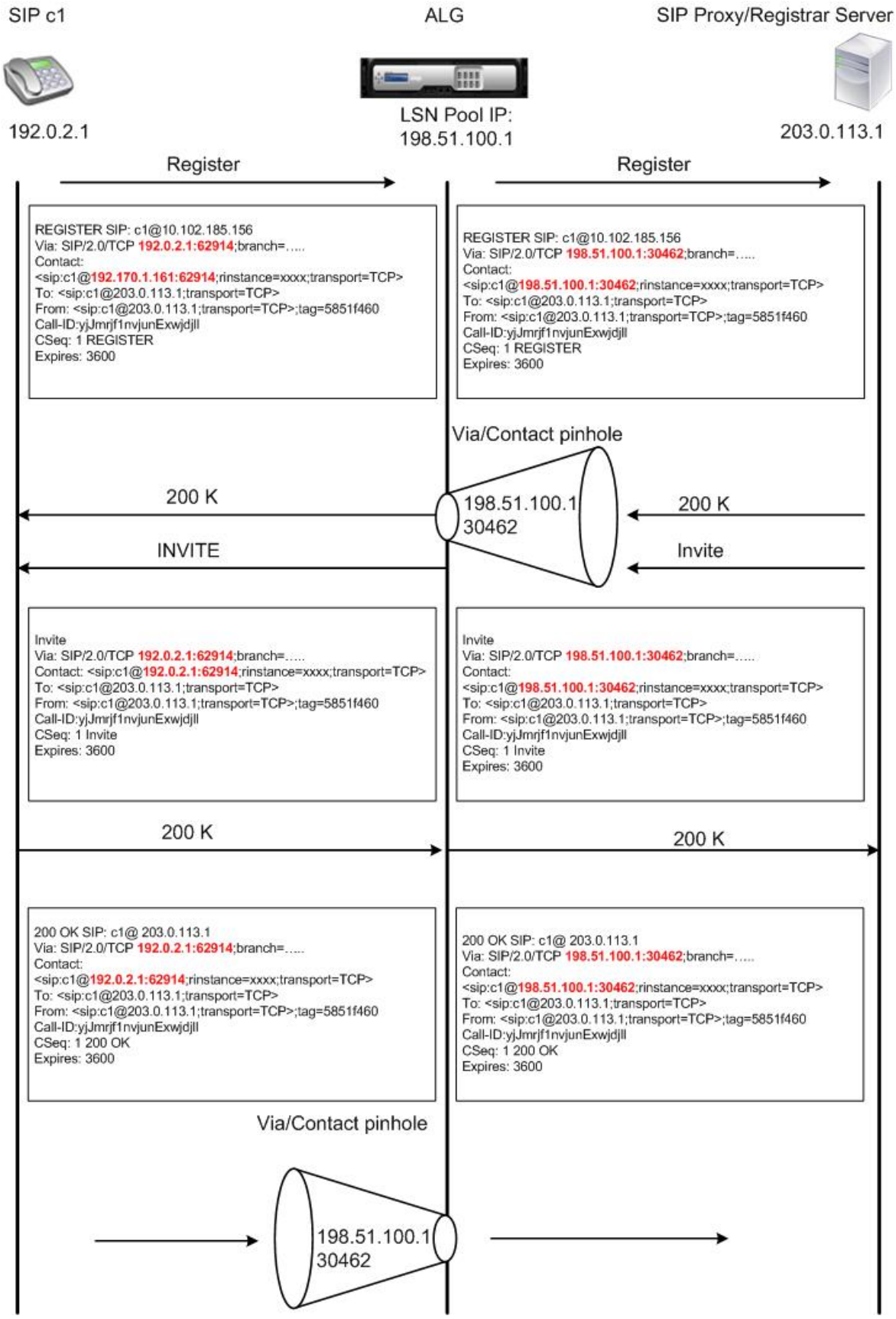


terno.

Llamadas entrantes

Una llamada entrante SIP se inicia con un mensaje SIP INVITE desde el cliente externo a la red interna. El registrador SIP reenvía el mensaje INVITE al cliente SIP en la red interna, mediante el agujero de acceso que se creó cuando el cliente SIP interno se registró con el registrador SIP.

El SIP ALG realiza NAT en las direcciones IP LSN y números de puerto en los campos de encabezado SIP Via, Contacto, Ruta y Record Route, traduciéndolos a la dirección IP y número de puerto del cliente SIP interno, y reenvía la solicitud al cliente SIP. Cuando el mensaje de respuesta 200 Aceptar enviado por el cliente SIP interno llega al dispositivo Citrix ADC, el SIP ALG realiza NAT en las direcciones IP y los números de puerto en los campos de encabezado SIP Via, Contacto, Ruta y Record Route, traduciéndolos a la dirección IP del grupo LSN y al número de puerto, reenvía la respuesta al registrador SIP y, a continuación, abre un agujero de acceso en la dirección de salida para una mayor comunicación



SIP.

Terminación de llamada

El mensaje BYE finaliza una llamada. Cuando el dispositivo recibe un mensaje BYE, traduce los campos de encabezado del mensaje tal como lo hace para cualquier otro mensaje. Pero debido a que un mensaje BYE debe ser reconocido por el receptor con un 200 Aceptar, el ALG retrasa el desmontaje de la llamada durante 15 segundos para permitir el tiempo de transmisión del 200 Aceptar.

Llamada entre clientes de la misma red

Cuando el cliente A y el cliente B de la misma red inician una llamada, los mensajes SIP se enrutan a través del proxy SIP en la red externa. El SIP ALG procesa el INVITE del cliente A como una llamada saliente normal. Dado que el cliente B está en la misma red, el proxy SIP envía INVITE de nuevo al dispositivo Citrix ADC. El SIP ALG examina el mensaje INVITE, determina que contiene la dirección IP NAT del cliente A y reemplaza esa dirección por la dirección IP privada del cliente A antes de enviar el mensaje al cliente B. Una vez establecida la llamada entre los clientes, el Citrix ADC no participa en la transmisión de medios. entre los clientes.

Más casos SIP LSN: Proxy SIP dentro de la red privada

Si quiere alojar el servidor proxy SIP dentro de la red privada, Citrix recomienda realizar una de las siguientes acciones:

- Configure una asignación LSN estática para el proxy SIP privado. Para obtener más información, consulte Configuración de mapas LSN estáticos. Asegúrese de que el puerto NAT es el mismo que el puerto configurado en el perfil SIP ALG.
- Configure el servidor proxy SIP dentro de una zona desmilitarizada (DMZ).

Ilustración 1. Registro de llamadas SIP

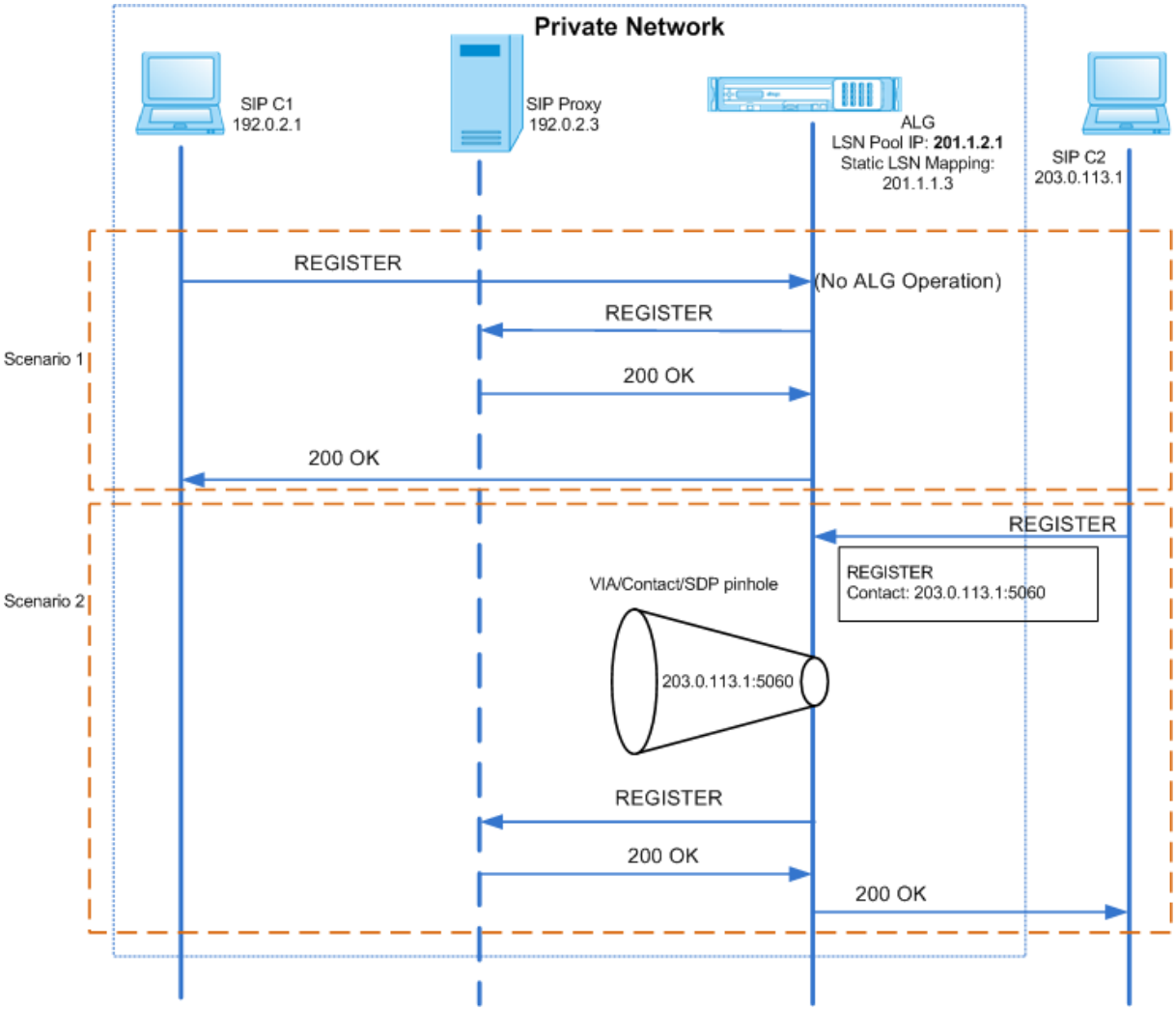
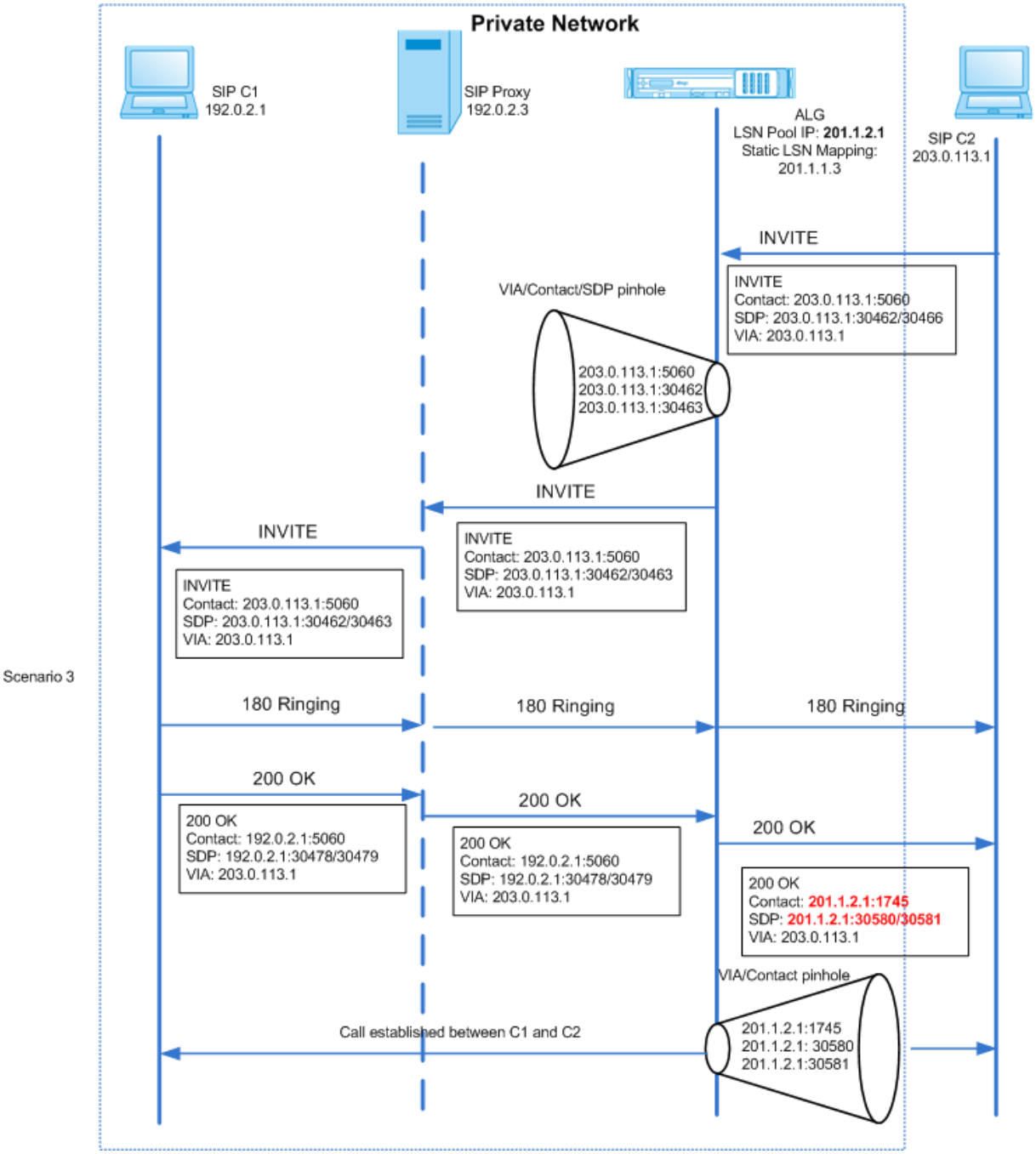


Ilustración 2. Flujo de llamadas entrantes SIP



Las ilustraciones 1 y 2 muestran los siguientes casos:

- Caso 1: El cliente SIP en la red privada se registra con el servidor proxy SIP en la misma red. Las operaciones ALG no se realizan porque el cliente SIP y el servidor proxy SIP están en la misma red.
- Caso 2: El cliente SIP en la red pública se registra con el servidor proxy SIP en la red privada. El mensaje REGISTER del cliente SIP público se envía al dispositivo Citrix ADC mediante la asignación de LSN estática configurada en el dispositivo, y el dispositivo crea un agujero de acceso

para otras operaciones SIP.

- Caso 3: Flujo de llamadas entrantes SIP. Una llamada entrante SIP se inicia con un mensaje SIP INVITE desde la red externa a la interna. El dispositivo Citrix ADC recibe el mensaje INVITE del cliente SIP C2, que se encuentra en la red externa, a través de los mapas LSN estáticos configurados en el dispositivo Citrix ADC.
  El dispositivo crea un agujero de acceso y reenvía el mensaje INVITE al proxy SIP. A continuación, el proxy SIP reenvía el mensaje INVITE al cliente SIP C1 en la red interna. El cliente SIP C1 envía 180 y 200 mensajes Aceptar al proxy SIP, que a su vez reenvía el mensaje al cliente SIP C2 a través del dispositivo Citrix ADC.
  Cuando el mensaje de respuesta 200 Aceptar enviado por el cliente SIP interno C1 llega al Citrix ADC, SIP ALG realiza NAT en las direcciones IP y los números de puerto en los campos de encabezado SIP Via, Contacto, Ruta y Record Route, y en los campos SDP, reemplazándolos por la dirección IP del grupo LSN y el número de puerto. A continuación, el SIP ALG reenvía el mensaje de respuesta al cliente SIP C2 y abre un agujero de acceso en la dirección de salida para una mayor comunicación SIP.

Compatibilidad con registros de auditoría

Puede registrar la información de ALG como parte del registro LSN habilitando ALG en la configuración de registro de auditoría de LSN. Para obtener más información sobre el registro de LSN, consulte Registro y supervisión de LSN. Un mensaje de registro para una entrada ALG en el registro LSN consta de la siguiente información:

- Marca de tiempo
- Tipo de mensaje SIP (por ejemplo, solicitud SIP)
- Dirección IP de origen y puerto del cliente SIP
- Dirección IP de destino y puerto del proxy SIP
- Dirección IP NAT y puerto
- SIP (método)
- Número de secuencia
- Si el cliente SIP está registrado o no
- Nombre de usuario y dominio de la persona que llama
- Nombre de usuario y dominio del receptor

Ejemplo de registro de auditoría:

Solicitar:

```
1 07/19/2013:09:49:19 GMT Informational 0-PPE-0 : default ALG
     ALG_SIP_INFO_PACKET_EVENT 169 0 : Infomsg: "SIP request" - Group: g2
      - Call_ID: NTY0YjYwMTJmYjNhNDU5ZjlhMmQxOTM5ZTE3Zjc3NjM. - Transport
```



```
      : TCP - Source_IP: 192.169.1.165 - Source_port: 57952 -
      Destination_IP: 10.102.185.156 - Destination_port: 5060 - Natted_IP:
       10.102.185.191 - Natted_port: 10313 - Method: REGISTER -
      Sequence_Number: 3060 - Register: YES - Content_Type: -
      Caller_user_name: 156_pvt_1 - Callee_user_name: 156_pvt_1 -
      Caller_domain_name: - Callee_domain_name: -
<!--NeedCopy-->
```

Respuesta:

```
07/19/2013:09:49:19 GMT Informational 0-PPE-0 : default ALG
    ALG_SIP_INFO_PACKET_EVENT 170 0 : Infomsg: "SIP response" - Group:
    g2 - Call_ID: NTY0YjYwMTJmYjNhNDU5ZjlhMmQxOTM5ZTE3Zjc3NjM. -
    Transport: TCP - Response_code 200 - Source_IP: 10.102.185.156 -
    Source_port: 5060 - Destination_IP: 192.169.1.165 - Destination_port
    : 57952 - Natted_IP: 10.102.185.191 - Natted_port: 10313 -
    Sequence_Number: 3060 - Content_Type: - Caller_user_name: 156_pvt_1
    - Callee_user_name: 156_pvt_1 - Caller_domain_name: -
    Callee_domain_name: -
<!--NeedCopy-->
```

Configuración de SIP ALG

Debe configurar el SIP ALG como parte de la configuración LSN. Para obtener instrucciones sobre cómo configurar LSN, consulte Pasos de configuración para LSN. Al configurar LSN, asegúrese de que:

- Defina los siguientes parámetros al agregar el perfil de aplicación LSN:
  - Agrupamiento de IP = PAIRED
  - Asignación de direcciones y puertos = ENDPOINT-INDEPENDENT
  - Filtrado = ENDPOINT-INDEPENDENT

Importante: Para que el SIP ALG funcione, es obligatoria una configuración de NAT de cono completo.

Ejemplo:

```
add lsn appsprofile app_tcp TCP -ippooling PAIRED -mapping ENDPOINT-
    INDEPENDENT -filtering ENDPOINT-INDEPENDENT
<!--NeedCopy-->
```

- Cree un perfil SIP ALG y asegúrese de definir el rango de puertos de origen o el rango de puertos de destino.

Ejemplo:

```
add lsn sipalgprofile sipalgprofile_tcp -sipsrcportrange 1-65535 -
    sipdstportrange 5060 -openViaPinhole ENABLED -openRecordRoutePinhole
     ENABLED  - sipTransportProtocol TCP
<!--NeedCopy-->
```

- Establezca SIP ALG = ENABLED, mientras crea el grupo LSN.

Ejemplo:

```
add lsn group g1 -clientname c1 -sipalg ENABLED
<!--NeedCopy-->
```

- Enlace el perfil SIP ALG al grupo LSN.

Ejemplo de configuración SIP ALG:

El siguiente ejemplo de configuración muestra cómo crear una configuración LSN simple con una única red de suscriptor, una sola dirección IP NAT LSN, una configuración específica de SIP ALG y configurar SIP ALG:

```
add lsn pool p1

Done

bind lsn pool p1 10.102.185.190

Done

add lsn client c1

Done

bind lsn client c1 -network 192.170.1.0 -netmask 255.255.255.0

Done

add lsn appsprofile app_tcp TCP -ippooling PAIRED -mapping ENDPOINT-
    INDEPENDENT -filtering ENDPOINT-INDEPENDENT

Done
```



```
20
21 add lsn appsprofile app_udp UDP -ippooling PAIRED -mapping ENDPOINT-
      INDEPENDENT -filtering ENDPOINT-INDEPENDENT
22
23 Done
24
25 bind lsn appsprofile app_tcp 1-65535
26
27 Done
28
29 bind lsn appsprofile app_udp 1-65535
30
31 Done
32
33 add lsn sipalgprofile sipalgprofile_tcp -sipdstportrange 5060 -
      openViaPinhole ENABLED -openRecordRoutePinhole ENABLED  -
      sipTransportProtocol TCP
34
35 Done
36
37 add lsn sipalgprofile sipalgprofile_udp -sipdstportrange 5060 -
      openViaPinhole ENABLED -openRecordRoutePinhole ENABLED -
      sipTransportProtocol UDP
38
39 Done
40
41 add lsn group g1 -clientname c1 -sipalg ENABLED
42
43 Done
44
45 bind lsn group g1 -poolname p1
46
47 Done
48
49 bind lsn group g1 -appsprofilename app_tcp
50
51 Done
52
53 bind lsn group g1 -appsprofilename app_udp
54
55 Done
56
57 bind lsn group g1 -sipalgprofilename sipalgprofile_tcp
58
59 Done
```



```
60
61 bind lsn group g1 -sipalgprofilename sipalgprofile_udp
62
63 Done
64 <!--NeedCopy-->
```

Puerta de enlace de capa de aplicación para protocolo RTSP

August 20, 2021

Real Time Streaming Protocol (RTSP) es un protocolo de nivel de aplicación para la transferencia de datos de medios en tiempo real. Utilizado para establecer y controlar sesiones de medios entre puntos finales, RTSP es un protocolo de canal de control entre el cliente de medios y el servidor de medios. La comunicación típica es entre un cliente y un servidor multimedia de streaming.

La transmisión de medios desde una red privada a una red pública requiere traducir direcciones IP y números de puerto a través de la red. La funcionalidad Citrix ADC incluye una puerta de enlace de capa de aplicación (ALG) para RTSP, que se puede utilizar con NAT de gran escala (LSN) para analizar la secuencia de medios y realizar los cambios necesarios para garantizar que el protocolo continúe funcionando a través de la red.

La forma en que se realiza la traducción de direcciones IP depende del tipo y la dirección del mensaje y del tipo de medios admitidos por la implementación cliente-servidor. Los mensajes se traducen de la siguiente manera:

- Solicitud saliente: Dirección IP privada a la dirección IP pública propiedad de Citrix ADC denominada dirección IP de grupo LSN.
- Respuesta entrante: Dirección IP de grupo LSN a dirección IP privada.
- Solicitud entrante: Sin traducción.
- Respuesta saliente: Dirección IP privada a la dirección IP del grupo LSN.

> **Nota**
>
> RTSP ALG se admite en un dispositivo independiente de Citrix ADC, en una configuración de alta disponibilidad de Citrix ADC, así como en una configuración de clúster de Citrix ADC.

Limitaciones de RTSP ALG

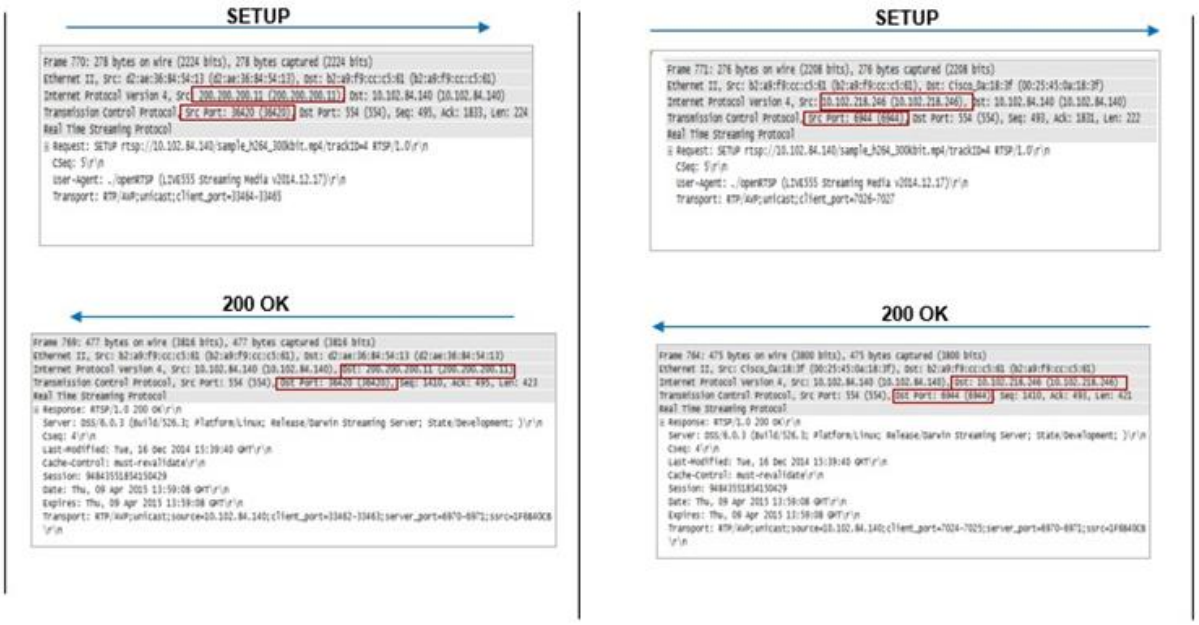
El RTSP ALG no admite lo siguiente:

- Sesiones RTSP multidifusión
- Sesión RTSP sobre UDP

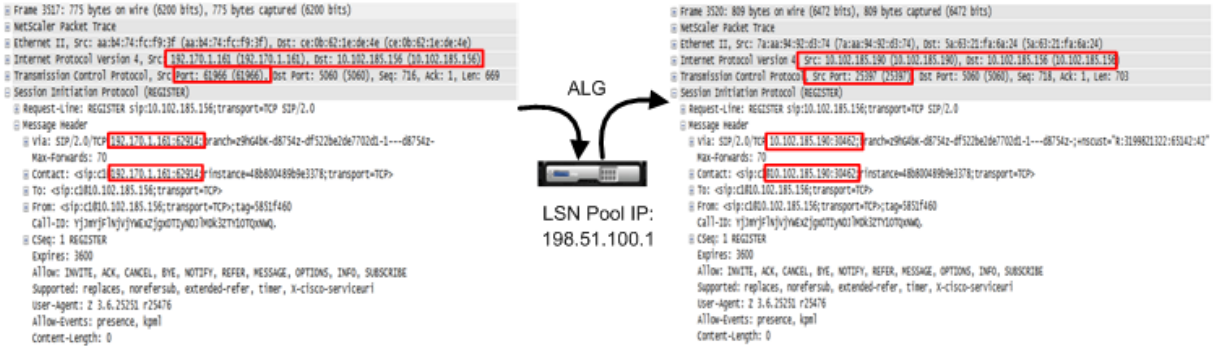
- TD/Admin partición
- Autenticación RSTP
- Tunelización HTTP

Caso RTSP y LSN

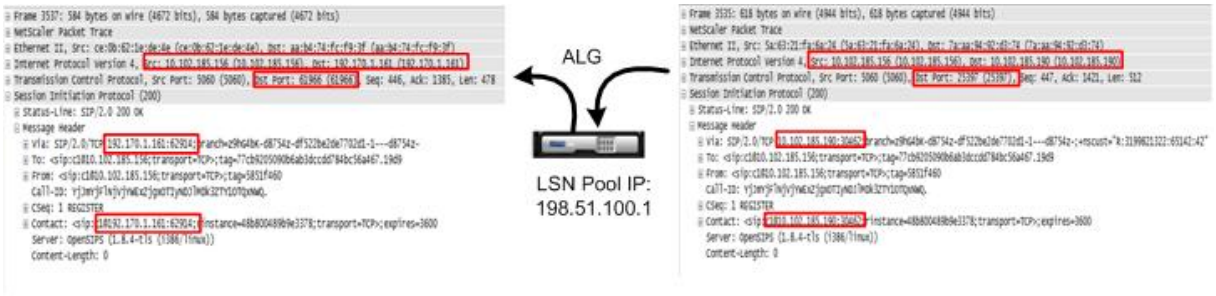
La siguiente ilustración muestra un flujo de solicitud RTSP SETUP. Normalmente, una solicitud SETUP especifica cómo se debe transportar una sola secuencia de medios. La solicitud contiene la URL de flujo de medios y un especificador de transporte. Este especificador normalmente incluye un puerto local para recibir datos RTP (audio o vídeo) y otro para recibir datos RTCP (metainformación). La respuesta del servidor generalmente confirma los parámetros elegidos y rellena las partes que faltan, como los puertos elegidos por el servidor. Cada secuencia de medios debe configurarse mediante el comando SETUP antes de que se pueda enviar una solicitud de reproducción agregada.



En una comunicación RTSP típica, el cliente de medios de la red pública envía una solicitud SETUP al servidor de medios de la red privada. RSTP ALG intercepta la solicitud y, en la secuencia de medios, reemplaza la dirección IP pública y el número de puerto por la dirección IP del grupo LSN y el número de puerto LSN. En la siguiente ilustración se muestra la traducción realizada por un dispositivo Citrix ADC en la secuencia de medios para una solicitud saliente:



El servidor de medios de la red privada utiliza la dirección IP del grupo LSN y el número de puerto LSN para enviar una respuesta 200 Aceptar al cliente de medios de la red pública. Citrix ADC RTSP ALG intercepta la respuesta y reemplaza la dirección IP del grupo LSN y el número de puerto LSN por la dirección IP pública y el número de puerto del cliente multimedia. En la siguiente ilustración se muestra la traducción realizada por un dispositivo Citrix ADC en la secuencia de medios para una respuesta entrante:



Configuración de RTSP ALG

Configure RTSP ALG como parte de la configuración LSN. Para obtener instrucciones sobre cómo configurar LSN, consulte Pasos de configuración para LSN. Al configurar LSN, asegúrese de que:

- Establezca el **tipo de NAT** como DETERMINISTIC o DYNAMIC mientras agrega el grupo LSN.
- Defina los siguientes parámetros al agregar el perfil de aplicación LSN:
  - Agrupamiento de IP = PAIRED
  - Asignación de direcciones y puertos = ENDPOINT-INDEPENDENT
  - Filtrado = ENDPOINT-INDEPENDENT
- Crear un perfil RTSP ALG y enlazar el perfil RTSP ALG al grupo LSN

Ejemplo de configuración RTSP ALG:

El siguiente ejemplo de configuración muestra cómo crear una configuración LSN simple con una única red de suscriptor, una sola dirección IP NAT LSN y una configuración RTSP ALG:

```
1 enable ns feature WL SP LB CS LSN
```



```
2
3  Done
4
5  add lsn pool pool1 -nattype DETERMINISTIC
6
7  Done
8
9  bind lsn pool pool1 10.102.218.246
10
11 Done
12
13 add lsn client client1
14
15 Done
16
17 bind lsn client client1 -network 200.200.200.11 -netmask 255.255.255.0
18
19 Done
20
21 add lsn appsprofile app1 TCP -ippooling PAIRED -mapping ENDPOINT-
      INDEPENDENT -filtering ENDPOINT-INDEPENDENT
22
23 Done
24
25 add lsn appsprofile app2 UDP -ippooling PAIRED -mapping ENDPOINT-
      INDEPENDENT -filtering ENDPOINT-INDEPENDENT
26
27 Done
28
29 bind lsn appsprofile app1 1-65535
30
31 Done
32
33 bind lsn appsprofile app2 1-65535
34
35 Done
36
37 add lsn rtspalgprofile rtspalgprofiledefault -rtspIdleTimeout 1000 -
      rtspportrange 554
38
39 Done
40
41 add lsn group group1 -clientname client1 -nattype DETERMINISTIC -
      portblocksize 512 -rtspalg ENABLED
42
```



```
Done

bind lsn group group1 -poolname pool1

Done

bind lsn group group1 -appsprofilename app1

Done

bind lsn group group1 -appsprofilename app2

Done

bind lsn group group1 -rtspalgprofilename rtspalgprofiledefault

Done
<!--NeedCopy-->
```

Puerta de enlace de capa de aplicación para protocolo IPSec

August 20, 2021

Si la comunicación entre dos dispositivos de red (por ejemplo, cliente y servidor) utiliza el protocolo IPSec, el tráfico IKE (que es sobre UDP) utiliza campos de puerto, pero el tráfico de carga de seguridad encapsuladora (ESP) no lo hace. Si un dispositivo NAT en la ruta asigna la misma dirección IP NAT (pero puertos diferentes) a dos o más clientes en el mismo destino, el dispositivo NAT no puede distinguir y enrutar correctamente el tráfico ESP de retorno no contiene información de puerto. Por lo tanto, el tráfico ESP IPSec falla en el dispositivo NAT.

Los extremos IPSec compatibles con NAT-T (NAT-T) detectan la presencia de un dispositivo NAT intermedio durante la fase 1 de IKE y conmutan al puerto UDP 4500 para todo el tráfico IKE y ESP subsiguiente (encapsulando ESP en UDP). Sin compatibilidad con NAT-T en los extremos IPSec del mismo nivel, el tráfico ESP protegido IPSec se transmite sin encapsulación UDP. Por lo tanto, el tráfico ESP IPSec falla en el dispositivo NAT.

El dispositivo Citrix ADC admite la funcionalidad de Gateway de capa de aplicación (ALG) IPSec para configuraciones NAT a gran escala. El ALG IPSec procesa el tráfico ESP IPSec y mantiene la información de sesión para que el tráfico no se produzca un error cuando los extremos IPSec no admiten NAT-T (encapsulación UDP del tráfico ESP).

Cómo funciona IPSec ALG

Un ALG IPSec supervisa el tráfico IKE entre un cliente y el servidor y permite solo un intercambio de mensajes IKE fase 2 entre el cliente y el servidor en un momento dado.

Una vez que se reciben los paquetes ESP bidireccionales para un flujo determinado, el ALG IPSec crea una sesión NAT para este flujo concreto de modo que el tráfico ESP posterior pueda fluir sin problemas. El tráfico ESP se identifica mediante índices de parámetros de seguridad (SPI), que son únicos para un flujo y para cada dirección. Un ALG IPSec utiliza SPI ESP en lugar de puertos de origen y destino para realizar NAT a gran escala.

Si una puerta no recibe tráfico, el tiempo de espera. Tras el tiempo de espera de ambas puertas, se permite otro intercambio de fase 2 de IKE.

Tiempos de espera IPSec ALG

IPSec ALG en un dispositivo Citrix ADC tiene tres parámetros de tiempo de espera:

- Tiempo de**espera de puerta ESP**. Tiempo máximo que el dispositivo Citrix ADC bloquea una puerta ALG IPSec para un cliente concreto en una dirección IP NAT específica para un servidor determinado si no se intercambia tráfico ESP bidireccional entre el cliente y el servidor.
- Tiempo de**espera de sesión IKE**. Tiempo máximo que el dispositivo Citrix ADC conserva la información de sesión IKE antes de quitarla si no hay tráfico IKE para esa sesión.
- Tiempo de**espera de la sesión ESP**. Tiempo máximo que el dispositivo Citrix ADC conserva la información de sesión ESP antes de eliminarla si no hay tráfico ESP para esa sesión.

Puntos a considerar antes de configurar IPSec ALG

Antes de comenzar a configurar IPSec ALG, tenga en cuenta los siguientes puntos:

- Debe comprender los diferentes componentes del protocolo IPSec.
- IPSec ALG no es compatible con las configuraciones DS-Lite y NAT64 de gran escala.
- IPsec ALG no es compatible con el flujo LSN de horquilla.
- IPSec ALG no funciona con configuraciones RNAT.
- IPsec ALG no es compatible con los clústeres de Citrix ADC.

Pasos de configuración

La configuración de IPSec ALG para NAT44 a gran escala en un dispositivo Citrix ADC consta de las siguientes tareas:

- **Cree un perfil de aplicación LSN y vincularlo a la configuración de LSN.** Defina los siguientes parámetros al configurar un perfil de aplicación:
  - Protocolo=UDP

  - Agrupamiento de IP = PAIRED
  - Port=500

Enlace el perfil de aplicación al grupo LSN de una configuración LSN. Para obtener instrucciones sobre cómo crear una configuración LSN, consulte Pasos de configuración para LSN.

- **Cree un perfil ALG IPSec**. Un perfil IPSec incluye varios tiempos de espera IPSec, como tiempo de espera de sesión IKE, tiempo de espera de sesión ESP y tiempo de espera de puerta ESP. Vincular un perfil ALG IPSec a un grupo LSN. Un perfil ALG IPSec tiene la siguiente configuración predeterminada:
  - Tiempo de espera de la sesión IKE = 60 minutos
  - Tiempo de espera de la sesión ESP = 60 minutos
  - Tiempo de espera de puerta ESP = 30 segundos
- **Enlace el perfil ALG IPSec a la configuración LSN**. IPSec ALG está habilitado para una configuración LSN cuando se vincula un perfil IPSec ALG a la configuración LSN. Enlace el perfil IPSec ALG a la configuración LSN estableciendo el parámetro de perfil IPSec ALG en el nombre del perfil creado en el grupo LSN. Un perfil ALG IPSec se puede enlazar a varios grupos LSN, pero un grupo LSN solo puede tener un perfil ALG IPSec.

Para crear un perfil de aplicación LSN mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
add lsn appsprofile <appsprofilename> UDP -ippooling PAIRED

show lsn appsprofile
<!--NeedCopy-->
```

Para enlazar el puerto de destino al perfil de aplicación LSN mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
bind lsn appsprofile <appsprofilename> <lsnport>

show lsn appsprofile
<!--NeedCopy-->
```


Para enlazar un perfil de aplicación LSN a un grupo LSN mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
bind lsn group <groupname> -appsprofilename <string>

show lsn group
<!--NeedCopy-->
```

Para crear un perfil ALG IPSec mediante la CLI

En el símbolo del sistema, escriba:

```
add ipsecalg profile <name> [-ikeSessionTimeout <positive_integer>] [-
    espSessionTimeout <positive_integer>] [-espGateTimeout <
    positive_integer>] [-connfailover ( ENABLED | DISABLED)

show ipsecalg profile <name>
<!--NeedCopy-->
```

Para enlazar un perfil ALG IPSec a una configuración LSN mediante la CLI

En el símbolo del sistema, escriba:

```
bind lsn group <groupname> -poolname <string> - ipsecAlgProfile <string
    >

show lsn group <name>
<!--NeedCopy-->
```

Para crear un perfil de aplicación LSN y vincularlo a una configuración LSN mediante la interfaz gráfica de usuario

Vaya a **Sistema** > **NAT a gran escala** > **Perfiles**, haga clic en la ficha **Aplicación**, agregue un perfil de aplicación LSN y enlácelo a un grupo LSN.

Para crear un perfil ALG IPSec mediante la interfaz gráfica de usuario

Vaya a **Sistema** > **NAT a gran escala** > **Perfiles**, haga clic en la ficha **ALG IPSEC** y, a continuación, agregue un perfil ALG IPSec.

Para enlazar un perfil ALG IPSec a una configuración LSN mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **NAT a gran escala** > **Grupo LSN**, abra el grupo LSN.
2. En **Configuración avanzada**, haga clic en **+ Perfil ALG IPSEC** para enlazar el perfil ALG IPSec creado al grupo LSN.

Configuración de ejemplo

En el siguiente ejemplo de configuración NAT44 a gran escala, IPSec ALG está habilitado para suscriptores en la red 192.0.2.0/24. IPSec ALG perfil IPSECALGPROFILE-1 con varias configuraciones de tiempo de espera IPSec se crea y se vincula al grupo LSN LSN Grupo -1.

Configuración de ejemplo:

```
add lsn client LSN-CLIENT-1

Done

bind lsn client LSN-CLIENT-1 -network 192.0.2.0 -netmask 255.255.255.0

Done

add lsn pool LSN-POOL-1

Done

bind lsn pool LSN-POOL-1 203.0.113.3-203.0.113.9

Done

add lsn appsprofile LSN-APPSPROFILE-1 UDP -ippooling PAIRED

Done

bind lsn appsprofile LSN-APPSPROFILE-1 500

Done
```



```
24
25 add ipsecalg profile  IPSECALGPROFILE-1 -ikeSessionTimeout 45  -
      espSessionTimeout 40  - espGateTimeout 20 -connfailover ENABLED
26
27 Done
28
29 bind lsn group LSN-GROUP-1 -appsprofilename LSN-APPSPROFILE-1
30
31 Done
32
33 bind lsn group LSN-GROUP-1 -poolname LSN-POOL-1
34
35 Done
36
37 bind lsn group LSN-GROUP-1 - ipsecAlgProfile IPSECALGPROFILE-1
38
39 Done
40 <!--NeedCopy-->
```

Registro y supervisión de LSN

October 5, 2021

Puede registrar la información de LSN para diagnosticar, solucionar problemas y cumplir los requisitos legales. Puede supervisar el rendimiento de la función LSN mediante contadores estadísticos LSN y mostrando las sesiones LSN actuales.

Registro LSN

El registro de la información LSN es una de las funciones importantes requeridas por los ISP para cumplir con los requisitos legales y para identificar el origen del tráfico en un momento dado.

Un dispositivo Citrix ADC registra las entradas de asignación de LSN y las sesiones LSN creadas o eliminadas para cada grupo LSN. Puede controlar el registro de información LSN para un grupo LSN mediante los parámetros de registro y registro de sesión del grupo LSN. Estos son parámetros de nivel de grupo y están inhabilitados de forma predeterminada. El dispositivo Citrix ADC registra las sesiones LSN para un grupo LSN solo cuando los parámetros de registro y registro de sesión están habilitados.

En la siguiente tabla se muestra el comportamiento de registro de un grupo LSN para varias configuraciones de parámetros de registro y registro de sesión.

Captura de registros	Registro de sesiones	Comportamiento de registro
Habilitado	Habilitado	Registra las entradas de asignación de LSN, así como las sesiones LSN.
Habilitado	Inhabilitada	Registra las entradas de asignación de LSN pero no las sesiones LSN.
Inhabilitada	Habilitado	No registra entradas de asignación ni sesiones LSN.

Un mensaje de registro para una entrada de asignación LSN consta de la siguiente información:

- Dirección IP propiedad de Citrix ADC (dirección NSIP o dirección SNIP) desde la que se origina el mensaje de registro.
- Marca de tiempo
- Tipo de entrada (MAPPING)
- Si se ha creado o eliminado la entrada de asignación LSN
- Dirección IP, puerto e ID de dominio de tráfico del suscriptor
- Dirección IP NAT y puerto
- Nombre del protocolo
- La dirección IP de destino, el puerto y el ID de dominio de tráfico pueden estar presentes, en función de las condiciones siguientes:
  - La dirección IP de destino y el puerto no se registran para la asignación independiente del punto final.
  - Solo se registra la dirección IP de destino para la asignación dependiente de direcciones. El puerto no está registrado.
  - La dirección IP de destino y el puerto se registran para la asignación dependiente del puerto de dirección.

Un mensaje de registro para una sesión LSN consta de la siguiente información:

- Dirección IP propiedad de Citrix ADC (dirección NSIP o dirección SNIP) desde la que se origina el mensaje de registro.
- Marca de tiempo
- Tipo de entrada (SESSION)
- Si se crea o elimina la sesión LSN
- Dirección IP, puerto e ID de dominio de tráfico del suscriptor
- Dirección IP NAT y puerto
- Nombre del protocolo
- Dirección IP de destino, puerto e ID de dominio de tráfico

El dispositivo utiliza su marco de registro de auditoría y syslog existente para registrar la información de LSN. Debe habilitar el registro LSN de nivel global habilitando el parámetro LSN en las entidades de acción NSLOG y SYLOG relacionadas. Cuando se habilita el parámetro Logging, el dispositivo Citrix ADC genera mensajes de registro relacionados con asignaciones LSN y sesiones LSN de este grupo LSN. A continuación, el dispositivo envía estos mensajes de registro a los servidores asociados con la acción NSLOG y las entidades de acción SYSLOG.

Para registrar la información de LSN, Citrix recomienda:

- Registrar la información de LSN en servidores de registro externos en lugar de en el dispositivo Citrix ADC. El inicio de sesión en servidores externos facilita un rendimiento óptimo cuando el dispositivo crea grandes cantidades de entradas de registro LSN (en orden de millones).
- Mediante SYSLOG sobre TCP, o NSLOG. De forma predeterminada, SYSLOG utiliza UDP y NSLOG solo utiliza TCP para transferir información de registro a los servidores de registro. TCP es más confiable que UDP para transferir datos completos.

  Nota:

  - El SYSLOG generado en el dispositivo Citrix ADC se envía dinámicamente a los servidores de registro externos.
  - Cuando se utiliza SYSLOG sobre TCP, si la conexión TCP está inactiva o el servidor SYSLOG está ocupado, los dispositivos Citrix ADC almacenan los registros en búfer y envían los datos una vez que la conexión está activa.

Para obtener más información sobre la configuración del registro, consulte Registro de auditoría.

La configuración del registro LSN consta de las siguientes tareas:

- **Configuración del dispositivo Citrix ADC para el registro.** Esta tarea implica la creación y configuración de varias entidades y parámetros del dispositivo Citrix ADC:
  - **Cree una configuración de registro de auditoría SYSLOG o NSLOG**. La creación de una configuración de registro de auditoría implica las siguientes tareas:
    * Cree una acción de auditoría NSLOG o SYSLOG y habilite el parámetro LSN. Las acciones de auditoría especifican las direcciones IP de los servidores de registro.
    * Cree una directiva de auditoría SYSLOG o NSLOG y vincule la acción de auditoría a la directiva de auditoría. Las acciones de auditoría especifican las direcciones IP de los servidores de registro. Opcionalmente, puede establecer el método de transporte para los mensajes de registro que se envían a los servidores de registro externos. Por defecto está seleccionado UDP, puede establecer el método de transporte como TCP para un mecanismo de transporte fiable.Enlazar la directiva de auditoría a global del sistema.
    * Cree una directiva de auditoría SYSLOG o NSLOG y vincule la acción de auditoría a la directiva de auditoría.

    * Vincular la directiva de auditoría a la global del sistema.
      Nota: Para una configuración de registro de auditoría existente, solo tiene que habilitar el parámetro LSN para registrar la información de LSN en el servidor especificado por la acción de auditoría.
  - **Habilitar los parámetros de registro y registro de sesión.** Habilite los parámetros de registro y registro de sesión al agregar grupos LSN o después de haber creado los grupos. El dispositivo Citrix ADC genera mensajes de registro relacionados con estos grupos LSN y los envía al servidor de las acciones de auditoría que tienen habilitado el parámetro LSN.
- **Configuración de servidores de registro.** Esta tarea implica instalar paquetes SYSLOG o NSLOG en los servidores deseados. Esta tarea también implica especificar la dirección NSIP del dispositivo Citrix ADC en el archivo de configuración de SYSLOG o NSLOG. Al especificar la dirección NSIP, el servidor puede identificar la información de registro enviada por el dispositivo Citrix ADC para almacenarla en un archivo de registro.

Para obtener más información sobre la configuración del registro, consulte Registro de auditoría.

Configuración SYSLOG mediante la interfaz de línea de comandos

Para crear una acción de servidor SYSLOG para el registro LSN mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
1 add audit syslogAction <name> <serverIP> [-serverPort <port>] -logLevel
      <logLevel>... [-transport (TCP)] [-lsn ( ENABLED | DISABLED )]
2 <!--NeedCopy-->
```

Para crear una directiva de servidor SYSLOG para el registro LSN mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
1 add audit syslogPolicy <name> <rule> <action>
2 <!--NeedCopy-->
```

Para enlazar una directiva de servidor SYSLOG al sistema global para el registro LSN mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:


```
bind system global [<policyName> [-priority <positive_integer>]]
<!--NeedCopy-->
```

Configuración SYSLOG mediante la utilidad de configuración

Para configurar una acción de servidor SYSLOG para el registro LSN mediante la utilidad de configuración

1. Vaya a **Sistemas** > **Auditoría** > **Syslog** y, en la ficha Servidores, agregue un nuevo servidor de auditoría o modifique un servidor existente.
2. Para habilitar el registro LSN, seleccione la opción **Registro NAT de gran escala**.
3. (Opcional) Para habilitar SYSLOG sobre TCP, seleccione la opción **Registro TCP**.

Para configurar una directiva de servidor SYSLOG para el registro LSN mediante la utilidad de configuración

Vaya a **Sistemas** > **Auditoría** > **Syslog** y, en la ficha **Directivas**, agregue una directiva nueva o modifique una directiva existente.

Para enlazar una directiva de servidor SYSLOG al sistema global para el registro LSN mediante la utilidad de configuración

1. Vaya a **Sistemas** > **Auditoría** > **Syslog**.
2. En la ficha **Directivas**, en la lista **Acción**, haga clic en **Enlaces globales** para enlazar las directivas globales de auditoría.

Configuración de NSLOG mediante la interfaz de línea de comandos

Para crear una acción de servidor NSLOG para el registro LSN mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
add audit nslogAction <name> <serverIP> [-serverPort <port>] -logLevel
    <logLevel> ... [-lsn ( ENABLED | DISABLED )]
<!--NeedCopy-->
```


Para crear una directiva de servidor NSLOG para el registro LSN mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
add audit nslogPolicy <name> <rule> <action>
<!--NeedCopy-->
```

Para enlazar una directiva de servidor NSLOG al sistema global para el registro LSN mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
bind system global [<policyName>]
<!--NeedCopy-->
```

Configuración de NSLOG mediante la utilidad de configuración

Para configurar una acción de servidor NSLOG para el registro LSN mediante la utilidad de configuración

1. Vaya a **Sistemas** > **Auditoría** > **Nslog** y, en la ficha **Servidores**, agregue un nuevo servidor de auditoría o modifique un servidor existente.
2. Para habilitar el registro LSN, seleccione la opción **Registro NAT de gran escala**.

Para configurar una directiva de servidor NSLOG para el registro LSN mediante la utilidad de configuración

Vaya a **Sistemas** > **Auditoría** > **Nslog** y, en la ficha **Directivas**, agregue una directiva nueva o modifique una directiva existente.

Para enlazar una directiva de servidor NSLOG al sistema global para el registro LSN mediante la utilidad de configuración

1. Vaya a **Sistemas** > **Auditoría** > **Nslog**.
2. En la ficha **Directivas**, en la lista **Acción**, haga clic en **Enlaces globales** para enlazar las directivas globales de auditoría.

Ejemplo

La siguiente configuración especifica dos servidores SYSLOG y dos servidores NSLOG para almacenar entradas de registro, incluidos los registros LSN. El registro LSN está configurado para los grupos LSN LSN-GROUP-2 y LSN-GROUP-3.

El dispositivo Citrix ADC genera mensajes de registro relacionados con asignaciones LSN y sesiones LSN de estos grupos LSN y los envía a los servidores de registro especificados.

```
add audit syslogAction SYS-ACTION-1 198.51.101.10 -logLevel ALL -lsn
    ENABLED
Done
add audit syslogPolicy SYSLOG-POLICY-1 ns_true SYS-ACTION-1
Done
bind system global SYSLOG-POLICY-1
Done

add audit syslogAction SYS-ACTION-2 198.51.101.20 -logLevel ALL -lsn
    ENABLED
Done
add audit syslogPolicy SYSLOG-POLICY-2 ns_true SYS-ACTION-2
Done
bind system global SYSLOG-POLICY-2
Done

add audit nslogAction NSLOG-ACTION-1 198.51.101.30 -logLevel ALL -lsn
    ENABLED
Done
add audit nslogPolicy NSLOG-POLICY-1 ns_true NSLOG-ACTION-1
Done
bind system global NSLOG-POLICY-1
Done
add audit nslogAction NSLOG-ACTION-2 198.51.101.40 -logLevel ALL -lsn
    ENABLED
Done
add audit nslogPolicy NSLOG-POLICY-2 ns_true NSLOG-ACTION-2
Done
bind system global NSLOG-POLICY-2
Done

add lsn group LSN-GROUP-3 -clientname LSN-CLIENT-2  -logging ENABLED  -
    sessionLogging ENABLED
Done
set lsn group LSN-GROUP-2   -logging ENABLED  -sessionLogging ENABLED
```



```
Done
<!--NeedCopy-->
```

La siguiente configuración especifica la configuración SYSLOG para enviar mensajes de registro al servidor SYSLOG externo 192.0.2.10 mediante TCP.

```
add audit syslogAction SYS-ACTION-1 192.0.2.10 -logLevel ALL -transport
    TCP
Done

add audit syslogPolicy SYSLOG-POLICY-1 ns_true SYS-ACTION-1
Done

bind system global SYSLOG-POLICY-1
Done
<!--NeedCopy-->
```

En la siguiente tabla se muestran las entradas de registro LSN de ejemplo de cada tipo almacenadas en los servidores de registro configurados. Estas entradas de registro LSN las genera un dispositivo Citrix ADC cuya dirección NSIP es 10.102.37.115.

Tipo de entrada de registro LSN	Entrada de registro de ejemplo
Creación de sesión LSN	Local4.Informational 10.102.37.115 08/05/2014:09:59:48 GMT 0-PPE-0: LSN LSN_SESSION 2581750: SESSION CREATED Client IP:Port:TD 192.0.2.10: 15136:0, NatIP:NatPort 203.0.113.6: 6234, Destination IP:Port:TD 198.51.100.9: 80:0, Protocol: TCP
Eliminación de sesión LSN	Local4.Informational 10.102.37.115 08/05/2014:10:05:12 GMT 0-PPE-0: LSN LSN_SESSION 3871790: SESSION DELETED Client IP:Port:TD 192.0.2.11: 15130:0, NatIP:NatPort 203.0.113.6: 7887, Destination IP:Port:TD 198.51.101.2:80:0, Protocol: TCP
Creación de mapeo LSN	Local4.Informational 10.102.37.115 08/05/2014:09:59:47 GMT 0-PPE-0: LSN LSN_MAPPING 2581580: EIM CREATED Client IP:Port 192.0.2.15: 14567, NatIP:NatPort 203.0.113.5: 8214, Protocol: TCP

Tipo de entrada de registro LSN	Entrada de registro de ejemplo
Eliminación de asignación de LSN	Local4.Informational 10.102.37.115 08/05/2014:10:05:12 GMT 0-PPE-0: LSN LSN_MAPPING 3871700: EIM DELETED Client IP:Port 192.0.3.15: 14565, NatIP:NatPort 203.0.113.11: 8217, Protocol: TCP

Registro mínimo

Las configuraciones de LSN deterministas y las configuraciones de LSN dinámicas con bloque de puertos reducen significativamente el volumen de registro LSN. Para estos dos tipos de configuración, el dispositivo Citrix ADC asigna una dirección IP NAT y un bloque de puertos a un suscriptor. El dispositivo Citrix ADC genera un mensaje de registro para un bloque de puerto en el momento de la asignación a un suscriptor. El dispositivo Citrix ADC también genera un mensaje de registro cuando se libera una dirección IP NAT y un bloque de puerto. Para una conexión, un suscriptor se puede identificar solo por su dirección IP NAT asignada y bloque de puerto. Por este motivo, el dispositivo Citrix ADC no registra ninguna sesión LSN creada o eliminada. El dispositivo tampoco registra ninguna entrada de asignación creada para una sesión ni cuando se quita la entrada de asignación.

La función de registro mínimo para las configuraciones deterministas LSN y las configuraciones dinámicas LSN con bloque de puertos está habilitada de forma predeterminada y no hay ninguna disposición para inhabilitarla. En otras palabras, el dispositivo Citrix ADC realiza automáticamente un registro mínimo para configuraciones de LSN deterministas y configuraciones de LSN dinámicas con bloque de puertos. No hay ninguna opción disponible para inhabilitar esta función. El dispositivo envía los mensajes de registro a todos los servidores de registro configurados.

Un mensaje de registro para cada bloque de puerto consta de la siguiente información:

- Dirección NSIP del dispositivo Citrix ADC
- Marca de tiempo
- Tipo de entrada como DETERMINISTIC o PORTBLOCK
- Si se asigna o se libera un bloque de puerto
- Dirección IP del suscriptor y la dirección IP NAT asignada y el bloque de puertos
- Nombre del protocolo

Registro mínimo para la configuración de LSN determinista

Considere un ejemplo de una configuración LSN determinista simple para cuatro suscriptores que tengan la dirección IP 192.0.17.1, 192.0.17.2, 192.0.17.3 y 192.0.17.4.

En esta configuración de LSN, el tamaño del bloque de puertos se establece en 32768 y el grupo de direcciones IP NAT de LSN tiene direcciones IP en el rango 203.0.113.19-203.0.113.23.

```
add lsn client LSN-CLIENT-7
Done
bind lsn client LSN-CLIENT-7 -network 192.0.17.0 -netmask
   255.255.255.253
Done
add lsn pool LSN-POOL-7 -nattype DETERMINISTIC
Done
bind lsn pool LSN-POOL-7 203.0.113.19-203.0.113.23
Done
add lsn group LSN-GROUP-7 -clientname LSN-CLIENT-7 -nattype
   DETERMINISTIC -portblocksize 32768
Done
bind lsn group LSN-GROUP-7 -poolname LSN-POOL-7
Done
<!--NeedCopy-->
```

El dispositivo Citrix ADC asigna de forma secuencial, desde el grupo IP NAT de LSN y sobre la base del tamaño de bloque de puerto establecido, una dirección IP NAT de LSN y un bloque de puertos a cada suscriptor. Asigna el primer bloque de puertos (1024-33791) en la dirección IP NAT inicial (203.0.113.19) a la dirección IP del suscriptor inicial (192.0.17.1). El siguiente rango de puertos se asigna al siguiente suscriptor, y así sucesivamente, hasta que la dirección NAT no tenga suficientes puertos para el siguiente suscriptor. En ese punto, el primer bloque de puerto de la siguiente dirección IP NAT se asigna al suscriptor, y así sucesivamente. El dispositivo registra la dirección IP NAT y el bloque de puertos asignados a cada suscriptor.

El dispositivo Citrix ADC no registra ninguna sesión LSN creada o eliminada para estos suscriptores. El dispositivo genera los siguientes mensajes de registro para la configuración de LSN.

```
1) 03/23/2015:00:30:56 GMT  Informational 0-PPE-0 : default LSN
   LSN_DETERMINISTIC 79201453 0 :  Dtrstc ALLOC Client 12.0.0.241,
   NatInfo 50.0.0.2:59904 to 60415
2) 03/23/2015:00:30:56 GMT  Informational 0-PPE-0 : default LSN
   LSN_DETERMINISTIC 79201454 0 :  Dtrstc ALLOC Client 12.0.0.242,
   NatInfo 50.0.0.2:60416 to 60927
3) 03/23/2015:00:30:56 GMT  Informational 0-PPE-0 : default LSN
   LSN_DETERMINISTIC 79201455 0 :  Dtrstc ALLOC Client 12.0.0.243,
   NatInfo 50.0.0.2:60928 to 61439
4) 03/23/2015:00:30:56 GMT  Informational 0-PPE-0 : default LSN
   LSN_DETERMINISTIC 79201455 0 :  Dtrstc ALLOC Client 12.0.0.243,
```



```
    NatInfo 50.0.0.2:60928 to 61439
<!--NeedCopy-->
```

Cuando quita la configuración de LSN, la dirección IP NAT asignada y el bloque de puertos se liberan de cada suscriptor. El dispositivo registra la dirección IP NAT y el bloque de puertos liberados de cada suscriptor. El dispositivo genera los siguientes mensajes de registro para cada suscriptor al quitar la configuración de LSN.

```
1) 03/23/2015:00:33:57 GMT  Informational 0-PPE-0 : default LSN
   LSN_DETERMINISTIC 79201706 0 :  Dtrstc FREE Client 12.0.0.238,
   NatInfo 50.0.0.2:58368 to 58879
2) 03/23/2015:00:33:57 GMT  Informational 0-PPE-0 : default LSN
   LSN_DETERMINISTIC 79201707 0 :  Dtrstc FREE Client 12.0.0.239,
   NatInfo 50.0.0.2:58880 to 59391
3) 03/23/2015:00:33:57 GMT  Informational 0-PPE-0 : default LSN
   LSN_DETERMINISTIC 79201708 0 :  Dtrstc FREE Client 12.0.0.240,
   NatInfo 50.0.0.2:59392 to 59903
<!--NeedCopy-->
```

Registro mínimo para la configuración dinámica de LSN con bloque de puertos

Considere un ejemplo de una configuración LSN dinámica simple con bloque de puerto para cualquier suscriptor en la red 192.0.2.0/24. En esta configuración de LSN, el tamaño del bloque de puertos se establece en 1024 y el grupo de direcciones IP NAT de LSN tiene direcciones IP en el rango 203.0.113.3-203.0.113.4.

```
set lsn parameter -memLimit 4000
Done
add lsn client LSN-CLIENT-1
Done
bind lsn client LSN-CLIENT-1 -network 192.0.2.0 -netmask 255.255.255.0
Done
add lsn pool LSN-POOL-1
Done
bind lsn pool LSN-POOL-1 203.0.113.3-203.0.113.4
Done
add lsn group LSN-GROUP-1 -clientname LSN-CLIENT-1 -portblocksize 1024
Done
bind lsn group LSN-GROUP-1 -poolname pool1 LSN-POOL-1
Done
```



```
<!--NeedCopy-->
```

El dispositivo Citrix ADC asigna una dirección IP NAT aleatoria y un bloque de puertos, desde el grupo IP NAT de LSN y sobre la base del tamaño de bloque de puertos establecido, para un suscriptor cuando inicia una sesión por primera vez. El Citrix ADC registra la dirección IP NAT y el bloque de puertos asignados a este suscriptor. El dispositivo no registra ninguna sesión LSN creada o eliminada para este suscriptor. Si todos los puertos se asignan (para diferentes sesiones del suscriptor) desde el bloque de puertos asignado del suscriptor, el dispositivo asigna una nueva dirección IP NAT aleatoria y un bloque de puertos para el suscriptor para sesiones adicionales. El Citrix ADC registra cada dirección IP NAT y bloque de puertos asignados a un suscriptor.

El dispositivo genera el siguiente mensaje de registro cuando el suscriptor, que tiene la dirección IP 192.0.2.1, inicia una sesión. El mensaje de registro muestra que el dispositivo ha asignado la dirección IP NAT 203.0.113.3 y el bloque de puerto 1024-2047 al suscriptor.

```
03/23/2015:00:07:12 GMT  Informational 0-PPE-3 : default LSN
   LSN_PORTBLOCK 106725793 0 :  Portblock ALLOC Client 12.0.2.72,
   NatInfo 203.0.113.3:1024 to 2047, Proto:TCP
<!--NeedCopy-->
```

Una vez que no quedan más sesiones que utilizan la dirección IP NAT asignada y uno de los puertos en el bloque de puertos asignado, la dirección IP NAT asignada y el bloque de puertos se liberan del suscriptor. El Citrix ADC registra que la dirección IP NAT y el bloque de puertos se liberan del suscriptor. El dispositivo genera los siguientes mensajes de registro para el suscriptor, que tiene la dirección IP 192.0.2.1, cuando no quedan más sesiones que utilicen la dirección IP NAT asignada (203.0.113.3) y un puerto del bloque de puertos asignado (1024-2047). El mensaje de registro muestra que la dirección IP NAT y el bloque de puerto se liberan del suscriptor.

```
03/23/2015:00:11:09 GMT Informational 0-PPE-3 : default LSN
   LSN_PORTBLOCK 106814342 0 :  Portblock FREE Client 12.0.3.122,
   NatInfo 203.0.113.3: 1024 to 2047, Proto:TC
<!--NeedCopy-->
```

Servidores SYSLOG de equilibrio de carga

El dispositivo Citrix ADC envía sus eventos SYSLOG y mensajes a todos los servidores de registro externos configurados. Esto da como resultado el almacenamiento de mensajes redundantes y dificulta la supervisión para los administradores del sistema. Para solucionar este problema, el dispositivo Citrix ADC ofrece algoritmos de equilibrio de carga que pueden equilibrar la carga de los mensajes SYS-

LOG entre los servidores de registro externos para mejorar el mantenimiento y el rendimiento. Los algoritmos de equilibrio de carga compatibles incluyen RoundRobin, LeastBandwidth, CustomLoad, LeastConnection, LeastPackets y AuditLogHash.

Equilibrio de carga de servidores SYSLOG mediante la interfaz de línea de comandos

Agregue un servicio y especifique el tipo de servicio como SYSLOGTCP o SYSLOGUDP.

```
add service <name>(<IP> | <serverName>) <serviceType (SYSLOGTCP |
    SYSLOGUDP)> <port>
<!--NeedCopy-->
```

Agregue un servidor virtual de equilibrio de carga, especifique el tipo de servicio como SYSLOGTCP o SYSLOGTCP y el método de equilibrio de carga como AUDITLOGHASH.

```
add lb vserver <name> <serviceType (SYSLOGTCP | SYSLOGUDP)> [-lbMethod
    <AUDITLOGHASH>]
<!--NeedCopy-->
```

Bing el servicio al servidor virtual de equilibrio de carga.

```
Bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Agregue una acción SYSLOG y especifique el nombre del servidor de equilibrio de carga que tiene SYSLOGTCP o SYSLOGUDP como tipo de servicio.

```
add syslogaction <name> <serverIP> [-lbVserverName <string>] [-logLevel
     <logLevel>]
<!--NeedCopy-->
```

Agregue una directiva SYSLOG especificando la regla y la acción.

```
add syslogpolicy <name> <rule> <action>
<!--NeedCopy-->
```


Enlace la directiva SYSLOG al global del sistema para que la directiva surta efecto.

```
bind system global <policyName>
<!--NeedCopy-->
```

Equilibrio de carga de servidores SYSLOG mediante la utilidad de configuración

1. Agregue un servicio y especifique el tipo de servicio como SYSLOGTCP o SYSLOGUDP.

   Vaya a Administración de Tráfico > Servicios, haga clic en Agregar y seleccione SYLOGTCP o SYSLOGUDP como protocolo.

2. Agregue un servidor virtual de equilibrio de carga, especifique el tipo de servicio como SYSLOGTCP o SYSLOGTCP y el método de equilibrio de carga como AUDITLOGHASH.

   Vaya a Administración del tráfico > Servidores virtuales, haga clic en Agregar y seleccione SYLOGTCP o SYSLOGUDP como protocolo.

3. Bing el servicio al servidor virtual de equilibrio de carga al servicio.

   Bing el servicio al servidor virtual de equilibrio de carga.

   Vaya a Administración del tráfico > Servidores virtuales, seleccione un servidor virtual y, a continuación, seleccione AuditLoghash en el método de equilibrio de carga.

4. Agregue una acción SYSLOG y especifique el nombre del servidor de equilibrio de carga que tiene SYSLOGTCP o SYSLOGUDP como tipo de servicio.

   Vaya a Sistema > Auditoría, haga clic en Servidores y agregue un servidor seleccionando la opción LB Vserver INSERVERS.

5. Agregue una directiva SYSLOG especificando la regla y la acción.

   Vaya a Sistema > Syslog, haga clic en Directivas y agregue una directiva SYSLOG.

6. Enlace la directiva SYSLOG al global del sistema para que la directiva surta efecto.

   Vaya a Sistema > Syslog, seleccione una directiva SYSLOG y haga clic en Acción y, a continuación, haga clic en Enlaces globales y vincule la directiva a global del sistema.

Ejemplo:

La siguiente configuración especifica el equilibrio de carga de los mensajes SYSLOG entre los servidores de registro externos mediante AUDITLOGHASH como método de equilibrio de carga. El dispositivo Citrix ADC genera eventos SYSLOG y mensajes equilibrados de carga entre los servicios, service1, service2 y service 3.


```
add service service1 192.0.2.10 SYSLOGUDP 514
Done

add service service2 192.0.2.11 SYSLOGUDP 514
Done

add service service3 192.0.2.11 SYSLOGUDP 514
Done

add lb vserver lbvserver1 SYSLOGUDP -lbMethod AUDITLOGHASH
Done

bind lb vserver lbvserver1 service1
Done

bind lb vserver lbvserver1 service2
Done

bind lb vserver lbvserver1 service3
Done

add syslogaction sysaction1 -lbVserverName lbvserver1 -logLevel All
Done

add syslogpolicy syspol1 ns_true sysaction1
Done

bind system global syspol1
Done
<!--NeedCopy-->
```

Registro de información de encabezado HTTP

El dispositivo Citrix ADC ahora puede registrar la información de encabezado de solicitud de una conexión HTTP que utiliza la funcionalidad LSN del Citrix ADC. Se puede registrar la siguiente información de encabezado de un paquete de solicitud HTTP:

- URL a la que está destinada la solicitud HTTP.
- Método HTTP especificado en la solicitud HTTP.
- Versión HTTP utilizada en la solicitud HTTP.
- Dirección IP del suscriptor que envió la solicitud HTTP.

Los registros de encabezado HTTP pueden ser utilizados por los ISP para ver las tendencias rela-

cionadas con el protocolo HTTP entre un conjunto de suscriptores. Por ejemplo, un ISP puede utilizar esta función para averiguar los sitios web más populares entre un conjunto de suscriptores.

Un perfil de registro de encabezado HTTP es una colección de atributos de encabezado HTTP (por ejemplo, URL y método HTTP) que se pueden habilitar o inhabilitar para el registro. El perfil de registro de encabezado HTTP se enlaza a un grupo LSN. A continuación, el dispositivo Citrix ADC registra los atributos de encabezado HTTP, que están habilitados en el perfil de registro de encabezado HTTP enlazado para el registro, de cualquier solicitud HTTP relacionada con el grupo LSN. A continuación, el dispositivo envía los mensajes de registro a los servidores de registro configurados.

Un perfil de registro de encabezado HTTP se puede enlazar a varios grupos LSN, pero un grupo LSN solo puede tener un perfil de registro de encabezado HTTP.

Para crear un perfil de registro de encabezado HTTP mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
add lsn httphdrlogprofile <httphdrlogprofilename> [-logURL ( ENABLED |
    DISABLED )] [-logMethod ( ENABLED | DISABLED )] [-logVersion (
    ENABLED | DISABLED )] [-logHost ( ENABLED | DISABLED )]

show lsn httphdrlogprofile
<!--NeedCopy-->
```

Para enlazar un perfil de registro de encabezado HTTP a un grupo LSN mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
bind lsn group <groupname> -httphdrlogprofilename <string>

show lsn group <groupname>
<!--NeedCopy-->
```

Ejemplo

En el siguiente ejemplo de una configuración LSN, el perfil de registro de encabezado HTTP HTTP-header-log-1 está enlazado al grupo LSN LSN-GROUP-1. El perfil de registro tiene todos los atributos HTTP (URL, método HTTP, versión HTTP y dirección IP HOST) habilitados para el registro, de modo que

todos estos atributos se registran para cualquier solicitud HTTP de suscriptores (en la red 192.0.2.0/24) relacionada con el grupo LSN.

```
add lsn httphdrlogprofile HTTP-HEADER-LOG-1
Done

set lsn parameter -memLimit 4000
Done

add lsn client LSN-CLIENT-1
Done

bind lsn client LSN-CLIENT-1 -network 192.0.2.0 -netmask 255.255.255.0
Done

add lsn pool LSN-POOL-1
Done

bind lsn pool LSN-POOL-1 203.0.113.3-203.0.113.4
Done

add lsn group LSN-GROUP-1 -clientname LSN-CLIENT-1 -portblocksize 1024
Done

bind lsn group LSN-GROUP-1 -poolname pool1 LSN-POOL-1
Done

bind lsn group  LSN-GROUP-1  -httphdrlogprofilename HTTP-HEADER-LOG-1
Done
<!--NeedCopy-->
```

El Citrix ADC genera el siguiente mensaje de registro de encabezado HTTP cuando uno de los suscriptores pertenecientes al ejemplo de configuración de LSN envía una solicitud HTTP.

El mensaje de registro nos dice que un cliente que tiene la dirección IP 192.0.2.33 envía una solicitud HTTP a URL example.com mediante el método HTTP GET y HTTP versión 1.1.

```
03/19/2015:16:24:04 GMT  Informational 0-PPE-1 : default LSN Message 59
    0 :  "LSN Client IP:TD 10.102.37.118:0 URL: example.com Host:
   192.0.2.33 Version: HTTP1.1 Method: GET"
<!--NeedCopy-->
```


Registro de información MSISDN

Un número de directorio integrado de suscriptor de Mobile Station (MSISDN) es un número de teléfono que identifica de forma única a un suscriptor a través de varias redes móviles. El MSISDN está asociado a un código de país y a un código de destino nacional que identifica al operador del suscriptor.

Puede configurar un dispositivo Citrix ADC para que incluya MSISSDN en entradas de registro LSN para suscriptores de redes móviles. La presencia de MSISSDN en los registros de LSN ayuda al administrador en un seguimiento más rápido y preciso de un suscriptor móvil que ha violado una directiva o ley, o cuya información es requerida por las agencias de interceptación legales.

Las siguientes entradas de registro LSN de ejemplo incluyen información MSISDN para una conexión de un suscriptor móvil en una configuración de LSN. Las entradas de registro muestran que un suscriptor móvil cuyo MSISDN es E 164:5556543210 se conectó al destino IP: Puerto 23.0.0. 1:80 a través de NAT IP: Puerto 203.0.113. 3:45195.

Tipo de entrada de registro	Entrada de registro de ejemplo
Creación de sesión LSN	Oct 14 15:37:30 10.102.37.77 10/14/2015:10:08:14 GMT 0-PPE-6: Default LSN LSN_SESSION 25012 0: SESSION CREATED E164:5556543210 Client IP:Port:TD 192.0.2.50:4649:0, NatIP:NatPort 203.0.113.3:45195, Destination IP:Port:TD 23.0.0.1:0:0, Protocol: TCP
Creación de mapeo LSN	Oct 14 15:37:30 10.102.37.77 10/14/2015:10:08:14 GMT 0-PPE-6: Default LSN LSN_ADDR_MAPPING 25013 0: ADM CREATED E164:5556543210 Client IP:Port:TD 192.0.2.50:4649:0, NatIP:NatPort 203.0.113.3:45195, Destination IP:Port:TD 23.0.0.1:0:0, Protocol: TCP
Eliminación de sesión LSN	Oct 14 15:40:30 10.102.37.77 10/14/2015:10:11:14 GMT 0-PPE-6: Default LSN LSN_SESSION 25012 0: SESSION CREATED E164:5556543210 Client IP:Port:TD 192.0.2.50:4649:0, NatIP:NatPort 203.0.113.3:45195, Destination IP:Port:TD 23.0.0.1:0:0, Protocol: TCP

Tipo de entrada de registro	Entrada de registro de ejemplo
Asignación de LSN	Oct 14 15:40:30 10.102.37.77 10/14/2015:10:11:14 GMT 0-PPE-6: Default LSN LSN_ADDR_MAPPING 25013 0: ADM CREATED E164:5556543210 Client IP:Port:TD 192.0.2.50:4649:0, NatIP:NatPort 203.0.113.3:45195, Destination IP:Port:TD 23.0.0.1:0:0, Protocol: TCP

Realice las siguientes tareas para incluir información de MSISDN en los registros LSN

- **Cree un perfil de registro LSN**. Un perfil de registro LSN incluye el parámetro ID de suscriptor de registro, que especifica si se debe incluir o no la información MSISDN en los registros de LSN de una configuración de LSN. Habilite el parámetro ID de suscriptor de registro al crear el perfil de registro LSN.
- **Enlazar el perfil de registro de LSN a un grupo LSN de una configuración LSN**. Vincular el perfil de registro LSN creado a un grupo LSN de una configuración LSN estableciendo el parámetro Nombre de perfil de registro en el nombre de perfil de registro LSN creado. Para obtener instrucciones sobre cómo configurar NAT a gran escala, consulte Pasos de configuración para LSN.

Para crear un perfil de registro LSN mediante la CLI

En el símbolo del sistema, escriba:

```
add lsn logprofile <logprofilename -logSubscriberID ( ENABLED |
    DISABLED )

show lsn logprofile
<!--NeedCopy-->
```

Para enlazar un perfil de registro LSN a un grupo LSN de una configuración de LSN mediante la CLI

En el símbolo del sistema, escriba:

```
bind lsn group <groupname>  -logProfileName <lsnlogprofilename>

```



```
show lsn group
<!--NeedCopy-->
```

Configuración de ejemplo:

En este ejemplo de configuración de LSN, el perfil de registro LSN tiene habilitado el parámetro ID de suscriptor de registro. El perfil está enlazado al grupo LSN LSN-GROUP-9. La información de MSISDN se incluye en la sesión de LSN y en los registros de asignación de LSN para conexiones de suscriptores móviles (en la red 192.0.2.0/24).

```
add lsn logprofile  LOG-PROFILE-MSISDN-9   -logSubscriberID ENABLED

Done
add lsn client LSN-CLIENT-9

Done
bind lsn client LSN-CLIENT-9 -network 192.0.2.0 -netmask 255.255.255.0

Done
add lsn pool LSN-POOL-9

Done
bind lsn pool LSN-POOL-9 203.0.113.3-203.0.113.4

Done
add lsn group LSN-GROUP-9 -clientname LSN-CLIENT-9

Done
bind lsn group LSN-GROUP-9 -poolname LSN-POOL-9

Done
bind lsn group  LSN-GROUP-9  -logprofilename LOG-PROFILE-MSISDN-9

Done
<!--NeedCopy-->
```

Visualización de sesiones LSN actuales

Puede mostrar las sesiones LSN actuales para detectar sesiones LSN no deseadas o ineficientes en el dispositivo Citrix ADC. Puede mostrar todas o algunas sesiones LSN sobre la base de parámetros de selección.

Nota: Cuando existen más de un millón de sesiones LSN en el dispositivo Citrix ADC, Citrix recomienda mostrar las sesiones LSN seleccionadas en lugar de todas mediante los parámetros de selección.

Configuración mediante la interfaz de línea de comandos

Para mostrar todas las sesiones LSN mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
show lsn session
<!--NeedCopy-->
```

Para mostrar sesiones LSN selectivas mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
show lsn session [-clientname <string>] [-network <ip_addr> [-netmask <
    netmask>] [-td <positive_integer>]] [-natIP <ip_addr> [-natPort <
    port>]]
<!--NeedCopy-->
```

Ejemplo

Para mostrar todas las sesiones LSN existentes en un dispositivo Citrix ADC

```
> show lsn session
        SubscrIP            SubscrPort      SubscrTD            DstIP                   DstPort DstTD     NatIP NatPort Proto   Dir
1.      192.0.2.10          15136           0           198.51.100.9            80          0       203.0.113.6     6234            TCP     OUT
2.      192.0.2.11          15130           0           198.51.101.2            80          0       203.0.113.6     7887            TCP     OUT
3.      192.0.2.12          16136           0           198.51.100.3            80          0       203.0.113.6     9807            TCP     OUT
4.      192.0.2.13          18148           0           198.51.101.6            80          0       203.0.113.6     4657            TCP     OUT
5.      192.0.2.14          13560           0           198.51.101.7            80          0       203.0.113.7     9341            TCP     OUT
6.      192.0.2.15          14567           0           198.51.100.8            80          0       203.0.113.5     8214            TCP     OUT
7.      192.0.2.15          16890           0           198.51.101.1            80          0       203.0.113.5     8214            TCP     OUT
8.      192.0.2.16          12345           0           198.51.102.9            80          0       203.0.113.5     1678            TCP     OUT
9.      192.0.2.19          19876           0           198.51.103.8            80          0       203.0.113.5     1567            TCP     OUT
10.     192.0.2.20          10989           0           198.51.104.19           80          0       203.0.113.11    1343            TCP     OUT
11.     192.0.3.13          18149           0           198.51.101.61           80          0       203.0.113.11    4653            TCP     OUT
12.     192.0.3.14          13510           0           198.51.101.74           80          0       203.0.113.11    9344            TCP     OUT
13.     192.0.3.15          14565           0           198.51.100.82           80          0       203.0.113.11    8217            TCP     OUT
14.     192.0.3.15          16899           0           198.51.101.12           80          0       203.0.113.11    8219            TCP     OUT
15.     192.0.3.16          12343           0           198.51.102.99           80          0       203.0.113.11    1673            TCP     OUT

Done
```

Para mostrar todas las sesiones LSN relacionadas con una entidad de cliente LSN LSN-CLIENT-2


```
> show lsn session -clientname LSN-CLIENT-2
        SubscrIP                SubscrPort      SubscrTD                DstIP                   DstPort DstTD     NatIP NatPort Proto   Dir
1.      192.0.2.10              15136           0               198.51.100.9            80              0       203.0.113.6     6ß234           TCP     OUT
2.      192.0.2.11              15130           0               198.51.101.2            80              0       203.0.113.6     7887            TCP     OUT
3.      192.0.2.12              16136           0               198.51.100.3            80              0       203.0.113.6     9807            TCP     OUT
4.      192.0.2.13              18148           0               198.51.101.6            80              0       203.0.113.6     4657            TCP     OUT
5.      192.0.2.14              13560           0               198.51.101.7            80              0       203.0.113.7     9341            TCP     OUT
6.      192.0.2.15              14567           0               198.51.100.8            80              0       203.0.113.5     8214            TCP     OUT
7.      192.0.2.15              16890           0               198.51.101.1            80              0       203.0.113.5     8214            TCP     OUT
8.      192.0.2.16              12345           0               198.51.102.9            80              0       203.0.113.5     1678            TCP     OUT
9.      192.0.2.19              19876           0               198.51.103.8            80              0       203.0.113.5     1567            TCP     OUT
10.     192.0.2.20              10989           0               198.51.104.19           80              0       203.0.113.11    1343            TCP     OUT

Done
```

Para mostrar todas las sesiones LSN que utilizan 203.0.113.5 como dirección IP NAT

```
> show lsn session –natIP 203.0.113.5
SubscrIP                SubscrPort      SubscrTD        DstIP                   DstPort DstTD     NatIP NatPort Proto   Dir
1.      192.0.2.15              14567           0               198.51.100.8            80              0       203.0.113.5     8214            TCP     OUT
2.      192.0.2.15              16890           0               198.51.101.1            80              0       203.0.113.5     8214            TCP     OUT
3.      192.0.2.16              12345           0               198.51.102.9            80              0       203.0.113.5     1678            TCP     OUT
4.      192.0.2.19              19876           0               198.51.103.8            80              0       203.0.113.5     1567            TCP     OUT
Done
```

Configuración mediante la utilidad de configuración

Para mostrar todas o seleccionadas sesiones LSN mediante la utilidad de configuración

1. Vaya a Sistema > NAT a gran escala > Sesiones y haga clic en la ficha NAT44.
2. Para mostrar sesiones LSN sobre la base de parámetros de selección, haga clic en Buscar.

Descripciones de parámetros (de los comandos enumerados en el procedimiento CLI)

- show lsn session
  - nombre_cliente

    Nombre de la entidad cliente LSN. Longitud máxima: 127
  - red

    Dirección IP o dirección de red del suscriptor (es).
  - máscara de red

    Máscara de subred para la dirección IP especificada por el parámetro de red.

    Valor predeterminado: 255.255.255.255
  - td

    Id. de dominio de tráfico de la entidad cliente LSN.

    Valor predeterminado: 0

    Valor mínimo: 0

    Valor máximo: 4094

- natIP

  Dirección IP NAT asignada utilizada en sesiones LSN.

Visualización de estadísticas de LSN

Puede mostrar estadísticas relacionadas con la función LSN para evaluar el rendimiento de la función LSN o para solucionar problemas. Puede mostrar un resumen de las estadísticas de la función LSN o de un grupo LSN determinado. Los contadores estadísticos reflejan los eventos desde que se reinició por última vez el dispositivo Citrix ADC. Todos estos contadores se restablecen a 0 cuando se reinicia el dispositivo Citrix ADC.

Para mostrar todas las estadísticas LSN mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
stat lsn
<!--NeedCopy-->
```

Para mostrar estadísticas de un grupo LSN especificado mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
stat lsn group [<groupname>]
<!--NeedCopy-->
```

Ejemplo

```
> stat lsn

Large Scale NAT statistics
                                                    Rate(/s)
                                                       Total
LSN TCP Received Packets                              0
    40
LSN TCP Received Bytes                                0
    3026
```



```
7  LSN TCP Transmitted Packets                          0
       40
8  LSN TCP Transmitted Bytes                            0
       3026
9  LSN TCP Dropped Packets                              0
                           0
10 LSN TCP Current Sessions                             0
                           0
11 LSN UDP Received Packets                             0
                           0
12 LSN UDP Received Bytes                               0
                           0
13 LSN UDP Transmitted Packets                          0
                           0
14 LSN UDP Transmitted Bytes                            0
                           0
15 LSN UDP Dropped Packets                              0
                           0
16 LSN UDP Current Sessions                             0
                           0
17 LSN ICMP Received Packets                            0
       982
18 LSN ICMP Received Bytes                              0
       96236
19 LSN ICMP Transmitted Packets                         0
                           0
20 LSN ICMP Transmitted Bytes                           0
                           0
21 LSN ICMP Dropped Packets                             0
       982
22 LSN ICMP Current Sessions                            0
                           0
23 LSN Subscribers                                      0
                           1
24
25 Done
26
27 > stat lsn group LSN-GROUP-1
28
29 LSN Group Statistics
30                                                   Rate (/s)
                                                        Total
31 TCP Translated Pkts                                  0
       40
32 TCP Translated Bytes                                 0
```



```
      3026
33 TCP Dropped Pkts                                    0
                         0
34 TCP Current Sessions                                0
                         0
35 UDP Translated Pkts                                 0
                         0
36 UDP Translated Bytes                                0
                         0
37 UDP Dropped Pkts                                    0
                         0
38 UDP Current Sessions                                0
                         0
39 ICMP Translated Pkts                                0
                         0
40 ICMP Translated Bytes                               0
                         0
41 ICMP Dropped Pkts                                   0
                         0
42 ICMP Current Sessions                               0
                         0
43 Current Subscribers                                 0
                         1
44
45 Done
46 <!--NeedCopy-->
```

Descripciones de parámetros (de los comandos enumerados en el procedimiento CLI)

- stat lsn grupo
  - groupname

    Nombre del grupo LSN. Longitud máxima: 127
  - detail

    Especifica la salida detallada (incluyendo más estadísticas). La salida puede ser bastante voluminosa. Sin este argumento, la salida mostrará solo un resumen.
  - fullValues

    Especifica que los números y cadenas deben mostrarse en su forma completa. Sin esta opción, las cadenas largas se acortan y los números grandes se abrevian.
  - ntimes

El número de veces, en intervalos de siete segundos, se deben mostrar las estadísticas.

Valor predeterminado: 1

- logFile

  Nombre del archivo de registro que se utilizará como entrada.

- clearstats

  Borrar los contadores de estadística/estadística

  Valores posibles: Básico, completo

Registro compacto

El registro de la información LSN es una de las funciones importantes que necesitan los ISP para cumplir con los requisitos legales y poder identificar el origen del tráfico en cualquier momento dado. Esto finalmente resulta en un gran volumen de datos de registro, lo que requiere que los ISP realicen grandes inversiones para mantener la infraestructura de registro.

El registro compacto es una técnica para reducir el tamaño del registro mediante el uso de un cambio notacional que implica códigos cortos para nombres de eventos y protocolos. Por ejemplo, C para cliente, SC para sesión creada y T para TCP. El registro compacto da como resultado una reducción media del 40 por ciento en el tamaño del registro.

Los siguientes ejemplos de entradas de registro de creación de mapas NAT44 muestran la ventaja del registro compacto.

Default logging format	02/02/2016:01:1 GMT Informational 0-PPE- 2: Default LSN LSN_ADDRPOR 85 0: A&PDM CREATED Clien- tIP:Port:TD1.1.1. Destina- tionIP:Port:TD2 Protocol: TCP

Compact logging format	02/02/2016:01:14:57 GMT Info 0-PE2:default LSN 87 0:A&PDMC	1.1.1.1:6500:0	N- 8.8.8.9:51066	D-2.2.2.2:80:0	T

Pasos de configuración

Realice las siguientes tareas para registrar la información de LSN en formato compacto:

- **Cree un perfil de registro LSN.** Un perfil de registro LSN incluye el parámetro Log Compact, que especifica si se va a registrar o no la información en formato compacto para una configuración de LSN.
- **Enlazar el perfil de registro LSN a un grupo LSN de una configuración LSN.** Vincular el perfil de registro LSN creado a un grupo LSN de una configuración de LSN estableciendo el parámetro Nombre de perfil de registro en el nombre de perfil de registro LSN creado. Todas las sesiones y asignaciones de este grupo LSN se registran en formato compacto.

Para crear un perfil de registro LSN mediante la CLI

En el símbolo del sistema, escriba:

```
add lsn logprofile <logprofilename> -logCompact (ENABLED|DISABLED)

show lsn logprofile
<!--NeedCopy-->
```

Para enlazar un perfil de registro LSN a un grupo LSN de una configuración de LSN mediante la CLI

En el símbolo del sistema, escriba:

```
bind lsn group <groupname> -logProfileName <lsnlogprofilename>

show lsn group
<!--NeedCopy-->
```


Configuración de ejemplo:

```
add lsn logprofile  LOG-PROFILE-COMPACT-9 -logCompact ENABLED

Done
add lsn client LSN-CLIENT-9
Done
bind lsn client LSN-CLIENT-9 -network 192.0.2.0 -netmask 255.255.255.0
Done
add lsn pool LSN-POOL-9
Done
bind lsn pool LSN-POOL-9 203.0.113.3-203.0.113.4
Done
add lsn group LSN-GROUP-9 -clientname LSN-CLIENT-9
Done
bind lsn group LSN-GROUP-9 -poolname LSN-POOL-9
Done
bind lsn group  LSN-GROUP-9  - logProfileName LOG-PROFILE-COMPACT-9
Done
<!--NeedCopy-->
```

Registro de IPFIX

El dispositivo Citrix ADC admite el envío de información sobre eventos LSN en formato de exportación de información de flujo de protocolo Internet (IPFIX) al conjunto configurado de recopiladores IPFIX. El dispositivo utiliza la función AppFlow existente para enviar eventos LSN en formato IPFIX a los recopiladores IPFIX.

El registro basado en IPFIX está disponible para los siguientes eventos relacionados con NAT44 a gran escala:

- Creación o eliminación de una sesión LSN.
- Creación o eliminación de una entrada de asignación LSN.
- Asignación o desasignación de bloques de puertos en el contexto de NAT determinista.
- Asignación o desasignación de bloques de puertos en el contexto de NAT dinámico.
- Siempre que se supere la cuota de sesión de suscriptor.

Puntos a tener en cuenta antes de configurar el registro IPFIX

Antes de comenzar a configurar IPSec ALG, tenga en cuenta los siguientes puntos:

- Debe configurar la función AppFlow y los recopiladores IPFIX en el dispositivo Citrix ADC. Para obtener instrucciones, consulte el tema Configuración de la función AppFlow.

Pasos de configuración

Realice las siguientes tareas para registrar la información LSN en formato IPFIX:

- **Habilite el registro LSN en la configuración de AppFlow**. Habilite el parámetro de registro LSN como parte de la configuración de AppFlow.
- **Cree un perfil de registro LSN**. Un perfil de registro LSN incluye el parámetro IPFIX que habilita o inhabilita la información de registro en formato IPFIX.
- **Enlazar el perfil de registro de LSN a un grupo LSN de una configuración LSN**. Enlace el perfil de registro LSN a uno o varios grupos LSN. Los eventos relacionados con el grupo LSN enlazado se registrarán en formato IPFIX.

Para habilitar el registro LSN en la configuración de AppFlow mediante la CLI

En el símbolo del sistema, escriba:

```
set appflow param -lsnLogging ( ENABLED | DISABLED )

show appflow param
<!--NeedCopy-->
```

Para crear un perfil de registro LSN mediante el comando CliAt, el símbolo del sistema

En el símbolo del sistema, escriba:

```
set lsn logprofile <logProfileName>  -logipfix ( ENABLED | DISABLED )

show lsn logprofile
<!--NeedCopy-->
```

Para enlazar el perfil de registro LSN a un grupo LSN de una configuración de LSN mediante la CLI

En el símbolo del sistema, escriba:

```
bind lsn group <groupname>  -logProfileName <lsnlogprofilename>

show lsn group
<!--NeedCopy-->
```


Para crear un perfil de registro LSN mediante la interfaz gráfica de usuario

Vaya a **Sistema** > **NAT a gran escala** > **Perfiles**, haga clic en la ficha **Registro** y, a continuación, agregue un perfil de registro.

Para enlazar el perfil de registro LSN a un grupo LSN de una configuración LSN mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **NAT a gran escala** > **Grupo LSN,** abra el grupo **LSN** .
2. En **Configuración avanzada,** haga clic en **+ Perfil de registro** para enlazar el perfil de registro creado al grupo LSN.

Tiempo de espera inactivo de TCP SYN

January 12, 2021

El tiempo de espera inactivo SYN es el tiempo de espera para establecer conexiones TCP que utilizan LSN en el dispositivo Citrix ADC. Si no se establece una sesión TCP dentro del período de tiempo de espera configurado, Citrix ADC quita la sesión. El tiempo de espera inactivo SYN es útil para proporcionar protección contra ataques de inundación SYN. En una configuración de LSN, la entidad del grupo LSN incluye la configuración de tiempo de espera inactivo SYN.

Ejemplo:

En la siguiente configuración LSN de ejemplo, el tiempo de espera inactivo SYN se establece en 30 segundos para las conexiones TCP relacionadas con suscriptores de la red 192.0.2.0/24.

```
add lsn client LSN-CLIENT-1

Done

bind lsn client LSN-CLIENT-1 -network 192.0.2.0 -netmask 255.255.255.0

Done

add lsn pool LSN-POOL-1

Done

bind lsn pool LSN-POOL-1 203.0.113.3

Done
```



```
16
17 add lsn group LSN-GROUP-1 -clientname LSN-CLIENT-1  - synidletimeout 30
18
19 Done
20
21 bind lsn group LSN-GROUP-1 -poolname pool1 LSN-POOL-1
22
23 Done
24 <!--NeedCopy-->
```

Anular la configuración de LSN con la configuración de equilibrio de carga

January 12, 2021

Una configuración LSN tiene prioridad sobre cualquier configuración de equilibrio de carga de forma predeterminada. Para anular la configuración de red a gran escala (LSN) con la configuración de equilibrio de carga para el tráfico que coincida con ambas configuraciones, cree un perfil de red con el parámetro Override LSN habilitado y vincule este perfil al servidor virtual de la configuración de equilibrio de carga. La configuración de USNIP o USIP de la configuración de equilibrio de carga se aplica al tráfico, en lugar de aplicar la dirección IP de LSN de la configuración de LSN.

Esta opción es útil en una implementación de LSN que incluye dispositivos Citrix ADC y servicios de valor agregado, como firewall y dispositivos de optimización. En este tipo de implementación, se requiere el tráfico de entrada en el dispositivo Citrix ADC para pasar a través de estos servicios de valor agregado antes de aplicar una configuración LSN en el dispositivo al tráfico. Para que el dispositivo Citrix ADC envíe el tráfico de entrada a un servicio de valor agregado, se crea una configuración de equilibrio de carga y se habilita la sustitución de LSN en el dispositivo. La configuración de equilibrio de carga incluye servicios de valor agregado, representados como servicios de equilibrio de carga, enlazados a un servidor virtual de tipo ANY. El servidor virtual está configurado con directivas de escucha para identificar el tráfico que se va a enviar al servicio de valor agregado.

Para habilitar override lsn en un perfil de red mediante la CLI

Para habilitar override lsn al agregar un perfil de red, en el símbolo del sistema, escriba

```
1 add netProfile <name> -overrideLsn ( ENABLED | DISABLED )
2
3 show netprofile <name>
4 <!--NeedCopy-->
```


Para habilitar override lsn al agregar un perfil de red, en el símbolo del sistema, escriba

```
set netProfile <name> -overrideLsn ( ENABLED | DISABLED )

show netprofile <name>
<!--NeedCopy-->
```

Para habilitar la anulación de lsn en un perfil de red mediante GUI

1. Vaya a **Sistema** > **Red** > **Perfiles de red**.
2. Defina el parámetro **Override LSN** al agregar o modificar perfiles de red.

En la siguiente configuración de ejemplo, el perfil de red NETPROFILE-OVERRIDELSN-1 tiene habilitada la opción LSN y está enlazado al servidor virtual de equilibrio de carga LBVS-1.

Configuración de ejemplo:

```
add netprofile NETPROFILE-OVERRIDELSN-1 -overrideLsn ENABLED

Done

set lb vserver LBVS-1 -netprofile NETPROFILE-OVERRIDELSN-1

Done
<!--NeedCopy-->
```

Borrado de sesiones LSN

January 12, 2021

Puede eliminar todas las sesiones LSN no deseadas o ineficientes del dispositivo Citrix ADC. El dispositivo libera inmediatamente los recursos (como la dirección IP NAT, el puerto y la memoria) asignados a estas sesiones, lo que hace que los recursos estén disponibles para las sesiones nuevas. El dispositivo también elimina todos los paquetes posteriores relacionados con estas sesiones eliminadas. Puede quitar todas las sesiones LSN o seleccionadas del dispositivo Citrix ADC.

Para borrar todas las sesiones LSN mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:


```
flush lsn session

show lsn session
<!--NeedCopy-->
```

Para borrar sesiones LSN selectivas mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
flush lsn session [-clientname <string>] [-network <ip_addr> [-netmask
   <netmask>] [-td <positive_integer>]] [-natIP <ip_addr> [-natPort <
   port>]]

show lsn session
<!--NeedCopy-->
```

Ejemplo

Borrar todas las sesiones LSN existentes en un dispositivo Citrix ADC

```
flush lsn session

Done
<!--NeedCopy-->
```

Borrar todas las sesiones LSN relacionadas con la entidad de cliente LSN LSN-CLIENT-1

```
flush lsn session -clientname LSN-CLIENT-1

Done
<!--NeedCopy-->
```

Borrar todas las sesiones LSN relacionadas con una red de suscriptor (192.0.2.0) de la entidad de cliente LSN LSN-CLIENT-2 perteneciente al dominio de tráfico 100


```
flush lsn session -clientname LSN-CLIENT-2 -network 192.0.2.0 -
    netmask 255.255.255.0 -td 100

Done
<!--NeedCopy-->
```

Para borrar todas las sesiones LSN mediante la utilidad de configuración

Vaya a Sistema > NAT a gran escala > Sesiones y haga clic en Vacía sesiones.

Descripciones de parámetros (de los comandos enumerados en el procedimiento CLI)

- flush lsn sesión
  - nombre_cliente

    Nombre de la entidad cliente LSN. Longitud máxima: 127
  - red

    Dirección IP o dirección de red del suscriptor (es).
  - máscara de red

    Máscara de subred para la dirección IP especificada por el parámetro de red.

    Valor predeterminado: 255.255.255.255
  - td

    Id. de dominio de tráfico de la entidad cliente LSN.

    Valor predeterminado: 0

    Valor mínimo: 0

    Valor máximo: 4094
  - natIP

    Dirección IP NAT asignada utilizada en sesiones LSN.
  - natPort

    Puerto NAT asignado utilizado en las sesiones LSN.

Servidores SYSLOG de equilibrio de carga

August 20, 2021

El dispositivo Citrix ADC envía sus eventos SYSLOG y mensajes a todos los servidores de registro externos configurados. Esto da como resultado el almacenamiento de mensajes redundantes y dificulta la supervisión para los administradores del sistema. Para solucionar este problema, el dispositivo Citrix ADC ofrece algoritmos de equilibrio de carga que pueden equilibrar la carga de los mensajes SYSLOG entre los servidores de registro externos para mejorar el mantenimiento y el rendimiento. Los algoritmos de equilibrio de carga compatibles incluyen RoundRobin, LeastBandwidth, CustomLoad, LeastConnection, LeastPackets y AuditLogHash.

Equilibrio de carga de servidores SYSLOG mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

Agregue un servicio y especifique el tipo de servicio como SYSLOGTCP o SYSLOGUDP.

```
add service <name>(<IP> | <serverName>) <serviceType (SYSLOGTCP |
    SYSLOGUDP)> <port>
<!--NeedCopy-->
```

Agregue un servidor virtual de equilibrio de carga, especifique el tipo de servicio como SYSLOGTCP o SYSLOGTCP y el método de equilibrio de carga como AUDITLOGHASH.

```
add lb vserver <name> <serviceType (SYSLOGTCP | SYSLOGUDP)> [-lbMethod
    <AUDITLOGHASH>]
<!--NeedCopy-->
```

Enlazar el servicio al servidor virtual de equilibrio de carga.

```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

1. Agregue una acción SYSLOG y especifique el nombre del servidor de equilibrio de carga que tiene SYSLOGTCP o SYSLOGUDP como tipo de servicio.

```
add syslogaction <name> <serverIP> [-lbVserverName <string>] [-logLevel
    <logLevel>]
```



```
<!--NeedCopy-->
```

Agregue una directiva SYSLOG especificando la regla y la acción.

```
add syslogpolicy <name> <rule> <action>
<!--NeedCopy-->
```

Enlace la directiva SYSLOG al global del sistema para que la directiva surta efecto.

```
bind system global <policyName>
<!--NeedCopy-->
```

Equilibrio de carga de servidores SYSLOG mediante la utilidad de configuración

1. Agregue un servicio y especifique el tipo de servicio como SYSLOGTCP o SYSLOGUDP.

   Vaya a Administración de Tráfico > Servicios, haga clic en Agregar y seleccione SYLOGTCP o SYSLOGUDP como protocolo.

2. Agregue un servidor virtual de equilibrio de carga, especifique el tipo de servicio como SYSLOGTCP o SYSLOGTCP y el método de equilibrio de carga como AUDITLOGHASH.

   Vaya a Administración del tráfico > Servidores virtuales, haga clic en Agregar y seleccione SYLOGTCP o SYSLOGUDP como protocolo.

3. Bing el servicio al servidor virtual de equilibrio de carga al servicio.

   Bing el servicio al servidor virtual de equilibrio de carga.

   Vaya a Administración del tráfico > Servidores virtuales, seleccione un servidor virtual y, a continuación, seleccione AuditLoghash en el método de equilibrio de carga.

4. Agregue una acción SYSLOG y especifique el nombre del servidor de equilibrio de carga que tiene SYSLOGTCP o SYSLOGUDP como tipo de servicio.

   Vaya a Sistema > Auditoría, haga clic en Servidores y agregue un servidor seleccionando la opción LB Vserver INSERVERS.

5. Agregue una directiva SYSLOG especificando la regla y la acción.

   Vaya a Sistema > Syslog, haga clic en Directivas y agregue una directiva SYSLOG.

6. Enlace la directiva SYSLOG al global del sistema para que la directiva surta efecto.

   Vaya a Sistema > Syslog, seleccione una directiva SYSLOG y haga clic en Acción y, a continuación, haga clic en Enlaces globales y vincule la directiva a global del sistema.

Ejemplo:

La siguiente configuración especifica el equilibrio de carga de los mensajes SYSLOG entre los servidores de registro externos mediante AUDITLOGHASH como método de equilibrio de carga. El dispositivo Citrix ADC genera eventos SYSLOG y mensajes equilibrados de carga entre los servicios, service1, service2 y service 3.

```
add service service1 192.0.2.10 SYSLOGUDP 514

add service service2 192.0.2.11 SYSLOGUDP 514

add service service3 192.0.2.11 SYSLOGUDP 514

add lb vserver lbvserver1 SYSLOGUDP -lbMethod AUDITLOGHASH

bind lb vserver lbvserver1 service1

bind lb vserver lbvserver1 service2

bind lb vserver lbvserver1 service3

add syslogaction sysaction1 -lbVserverName lbvserver1 -logLevel All

add syslogpolicy syspol1 ns_true sysaction1

bind system global syspol1
<!--NeedCopy-->
```

Limitaciones:

El dispositivo Citrix ADC no admite un servidor virtual de equilibrio de carga externo que equilibra la carga de los mensajes SYSLOG entre los servidores de registro.

Protocolo de control de puertos

January 12, 2021

Los dispositivos Citrix ADC ahora admiten Port Control Protocol (PCP) para NAT (LSN) a gran escala. Muchas de las aplicaciones de suscriptor de un ISP deben ser accesibles desde Internet (por ejemplo, dispositivos de Internet de las cosas (IOT), como una cámara IP que proporciona vigilancia a través de Internet). Una forma de cumplir este requisito es crear mapas estáticos de NAT (LSN) a gran es-

cala. Pero para una gran cantidad de suscriptores, crear mapas NAT LSN estáticos no es una solución factible.

Port Control Protocol (PCP) permite a un suscriptor solicitar asignaciones NAT LSN específicas para sí mismo y/o para otros dispositivos de terceros. El dispositivo NAT a gran escala crea un mapa LSN y lo envía al suscriptor. El suscriptor envía a los dispositivos remotos en Internet la dirección IP NAT: Puerto NAT en el que pueden conectarse al suscriptor.

Las aplicaciones suelen enviar mensajes de mantenimiento activo frecuentes al dispositivo NAT a gran escala para que sus asignaciones LSN no agoten el tiempo de espera. PCP ayuda a reducir la frecuencia de dichos mensajes keep-alive al permitir que las aplicaciones aprendan la configuración de tiempo de espera de las asignaciones LSN. Esto ayuda a reducir el consumo de ancho de banda en la red de acceso del ISP y el consumo de batería en dispositivos móviles.

PCP es un modelo cliente-servidor y se ejecuta sobre el protocolo de transporte UDP. Un dispositivo Citrix ADC implementa el componente del servidor PCP y cumple con RFC 6887.

Pasos de configuración

Realice las siguientes tareas para configurar PCP:

- (Opcional) Cree un perfil de PCP. Un perfil PCP incluye configuraciones para parámetros relacionados con PCP (por ejemplo, para escuchar solicitudes PCP de mapeo y de pares). Un perfil PCP se puede enlazar a un servidor PCP. Un perfil PCP enlazado a un servidor PCP aplica toda su configuración al servidor PCP. Un perfil PCP puede enlazarse a varios servidores PCP. De forma predeterminada, un perfil PCP con parámetros predeterminados está enlazado a todos los servidores PCP. Un perfil PCP que se vincula a un servidor PCP anula la configuración predeterminada del perfil PCP para ese servidor. Un perfil PCP predeterminado tiene los siguientes parámetros:
  - Asignación: Activada
  - Peer: Activado
  - Vida útil mínima del mapa: 120 segundos
  - Vida máxima máxima: 86400 segundos.
  - Número de anunciaciones: 10
  - Terceros: Inhabilitado
- Cree un servidor PCP y vincule un perfil PCP a él. Cree un servidor PCP en el dispositivo Citrix ADC para escuchar solicitudes y mensajes relacionados con PCP de los suscriptores. Se debe asignar una dirección IP de subred (SNIP) a un servidor PCP para tener acceso a ella. De forma predeterminada, un servidor PCP escucha en el puerto 5351.
- Enlace el servidor PCP a un grupo LSN de una configuración LSN. Vincular el servidor PCP creado a un grupo LSN de una configuración LSN estableciendo el parámetro PCP Server para especificar el servidor PCP creado. Solo los suscriptores de este grupo LSN pueden acceder al servidor

PCP creado.

> **Nota**
>
> Un servidor PCP para una configuración NAT a gran escala no atiende solicitudes de suscriptores identificados a partir de reglas de ACL.

Para crear un perfil PCP mediante la CLI

En el símbolo del sistema, escriba:

```
add pcp profile <name> [-mapping ( ENABLED | DISABLED )] [-peer (
    ENABLED | DISABLED )] [-minMapLife <secs>]  [-maxMapLife <secs>] [-
    announceMultiCount <positive_integer>][-thirdParty ( ENABLED |
    DISABLED )]

show pcp profile <name>
<!--NeedCopy-->
```

Para crear un servidor PCP mediante la CLI

En el símbolo del sistema, escriba:

```
add pcp server <name> <IPAddress> [-port <portNum|*>] [-pcpProfile <
    string>]

show pcp server <name>
<!--NeedCopy-->
```

Configuración de ejemplo para NAT44

En la siguiente configuración de ejemplo, el servidor PCP PCP-SERVER-9, con la configuración predeterminada de PCP, está enlazado al grupo LSN LSN-GROUP-9. PCP-SERVER-9 atiende solicitudes PCP de suscriptores en la red 192.0.2.0/24.

Configuración de ejemplo:

```
add pcp server PCP-SERVER-9 192.0.3.9

```



```
Done

add lsn client LSN-CLIENT-9

Done

bind lsn client LSN-CLIENT-9 -network 192.0.2.0 -netmask 255.255.255.0

Done

add lsn pool LSN-POOL-9

Done

bind lsn pool LSN-POOL-9 203.0.113.3-203.0.113.4

Done

add lsn group LSN-GROUP-9 -clientname LSN-CLIENT-9

Done

bind lsn group LSN-GROUP-9 -poolname LSN-POOL-9

Done

bind lsn group  LSN-GROUP-9  -pcpServer PCP-SERVER-9

Done
<!--NeedCopy-->
```

LSN44 en una configuración de clúster

January 12, 2021

Las configuraciones NAT44 de gran escala se admiten en una configuración de clúster de Citrix ADC.

Un clúster de Citrix ADC es un grupo de dispositivos Citrix ADC que se configuran y administran como un único sistema. Un clúster de Citrix ADC proporciona escalabilidad y disponibilidad. Cada dispositivo Citrix ADC en una configuración de clúster actúa como una entidad LSN independiente y se administra como un único sistema.

La configuración de LSN en una configuración de clúster es la misma que en un dispositivo indepen-

diente, excepto que un grupo específico de direcciones IP de LSN es propiedad de un nodo cada vez. En otras palabras, una entidad de grupo IP LSN se configura como una entidad manchada en un nodo particular. Todos los nodos de una configuración de clúster pueden tener una entidad de grupo IP LSN específica. Para asegurarse de que los paquetes relacionados con una sesión LSN se reciben en el mismo nodo de clúster que realizó la operación NAT, se configura la dirección del backplane basado en directivas (PBS). PBS dirige los paquetes relacionados recibidos de una sesión LSN al mismo nodo de clúster.

Configuración de ejemplo:

```
add lsn client LSN-CLIENT-1

Done

bind lsn client LSN-CLIENT-1 -network 192.0.2.0 -netmask 255.255.255.0

Done

add lsn pool LSN-POOL-1

Done

bind lsn pool LSN-POOL-1 -ownerNode 1 203.0.113.3

Done

bind lsn pool LSN-POOL-1 -ownerNode 2 203.0.113.3

Done

add lsn group LSN-GROUP-1 -clientname LSN-CLIENT-1

Done

bind lsn group LSN-GROUP-1 -poolname pool1 LSN-POOL-1

Done

add ns acl b1 ALLOW -srcIP = 192.0.2.0-192.0.2.255 -type DFD -dfdhash
    SIP


Done
```



```
33
34 apply ns acls -type DFD
35
36 Done
37 <!--NeedCopy-->
```

Dual-Stack Lite

January 12, 2021

Debido a la escasez de direcciones IPv4 y a las ventajas de IPv6 sobre IPv4, muchos ISP han comenzado a realizar la transición a la infraestructura IPv6. Sin embargo, durante la transición, los ISP deben seguir soportando IPv4 junto con IPv6, porque la mayor parte de Internet público todavía utiliza solo IPv4, y muchos suscriptores no admiten IPv6.

Dual Stack Lite (DS-Lite) es una solución de transición IPv6 para ISP con infraestructura IPv6 para conectar sus suscriptores IPv4 a Internet. DS-Lite utiliza la tunelización IPv4 en IPv6 para enviar el paquete IPv4 de un suscriptor a través de un túnel en la red de acceso IPv6 al ISP. El paquete IPv6 se descapsuló para recuperar el paquete IPv4 del suscriptor y luego se envía a Internet después de la traducción de direcciones NAT y puertos y otro procesamiento relacionado con LSN. Los paquetes de respuesta atraviesan la misma ruta al suscriptor.

El dispositivo Citrix ADC implementa el componente AFTR de una implementación de DS-Lite y cumple con RFC 6333.

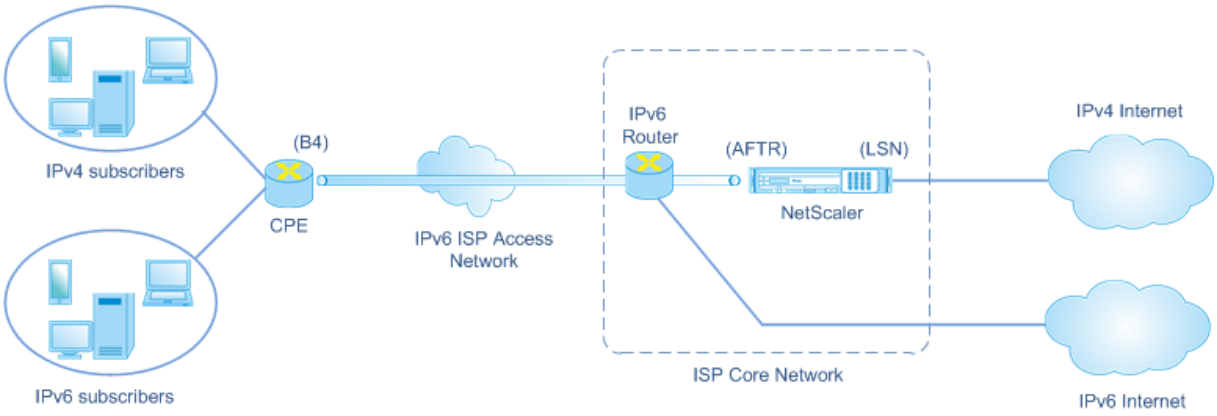
Arquitectura

La arquitectura Dual-Stack Lite para un ISP consta de los siguientes componentes:

- **Banda ancha básica en puente (B4).** La banda ancha básica en puente, o B4, es un dispositivo o componente que reside en las instalaciones del suscriptor. Normalmente, B4 es un componente en los dispositivos CPE en las instalaciones del suscriptor. Los suscriptores IPv4 están conectados a la red de acceso ISP solo IPv6 a través del dispositivo CPE que contiene el componente B4. La función principal del B4 es iniciar un túnel IPv6 entre B4 y un router de transición de familia de direcciones (AFTR) para enviar o recibir paquetes de solicitud o respuesta IPv4 del suscriptor a través del túnel. B4 incluye una dirección IPv6 conocida como dirección de extremo del túnel B4. B4 utiliza esta dirección para enviar paquetes IPv6 a AFTR y recibir paquetes de AFTR.
- **Enrutador de transición de la familia de direcciones (AFTR).** AFTR es un dispositivo o componente que reside en la red principal del ISP. AFTR termina el túnel IPv6 desde el dispositivo B4. En otras palabras, el túnel IPv6 se forma entre B4 en la premisa del suscriptor y AFTR en la red

principal del ISP. AFTR decapsula los paquetes IPv6 recibidos de B4 para recuperar los paquetes IPv4 originales de los suscriptores. AFTR envía los paquetes IPv4 al dispositivo o componente LSN. LSN enruta los paquetes IPv4 a su destino después de realizar la traducción de direcciones NAT y puertos (NAT 44) y otro procesamiento relacionado con LSN. AFTR incluye una dirección IPv6 conocida como dirección de extremo del túnel AFTR. AFTR utiliza esta dirección para enviar paquetes IPv6 a B4 y recibir paquetes IPv6 desde B4. El dispositivo Citrix ADC implementa el componente AFTR.

- **Softwire.** El túnel IPv6 creado entre B4 y AFTR se denomina softwire.



La arquitectura DS-Lite de un ISP que utiliza un dispositivo Citrix ADC consiste en suscriptores en espacios de direcciones privados que acceden a Internet a través de un dispositivo Citrix ADC implementado en la red principal del ISP. Los suscriptores IPv4 están conectados a un dispositivo CPE que incluye la funcionalidad DS-Lite B4. El dispositivo CPE está conectado a la red principal del ISP a través de la red de acceso solo IPv6 del ISP. El dispositivo Citrix ADC contiene la funcionalidad AFTR y LSN de DS-Lite.

A los suscriptores IPv4 conectados al dispositivo CPE se les asignan direcciones IPv4 privadas manualmente o a través del servidor DHCP que se ejecuta en el dispositivo CPE. En el dispositivo CPE, la dirección de extremo del túnel AFTR se especifica manualmente o a través de DHCPv6. La configuración de los dispositivos CPE es específica del proveedor y, por lo tanto, está fuera del alcance de esta documentación.

Al recibir un paquete de solicitud procedente de un suscriptor IPv4 y destinado a una ubicación en Internet, el componente B4 del dispositivo CPE encapsula el paquete IPv4 en un paquete IPv6 y lo envía al dispositivo Citrix ADC en la red principal del ISP. La funcionalidad AFTR del dispositivo Citrix ADC decapsula el paquete IPv6 para recuperar el paquete IPv4 original del suscriptor. La funcionalidad LSN del dispositivo Citrix ADC traduce la dirección IP de origen y el puerto del paquete IPv4 a una dirección IP NAT y puerto NAT seleccionados del grupo NAT configurado y, a continuación, envía el paquete a su destino en Internet.

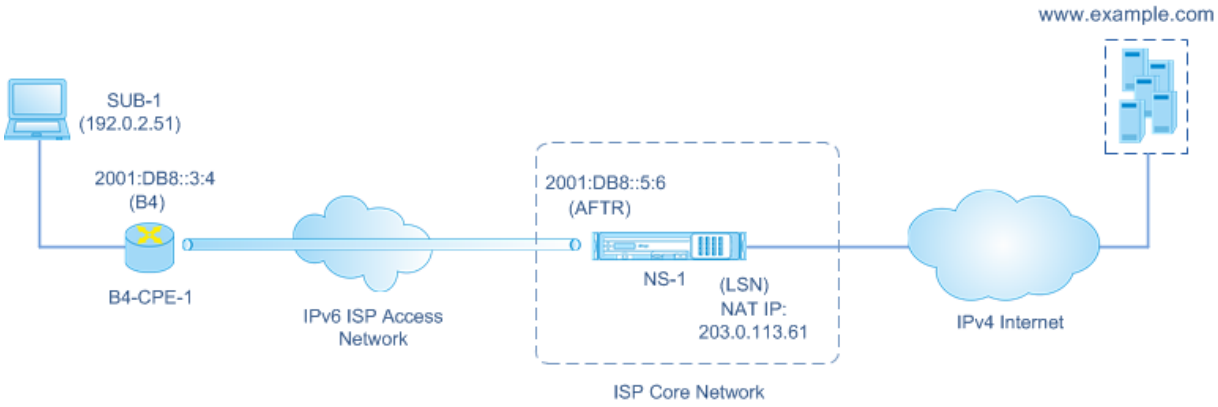
El dispositivo mantiene un registro de todas las sesiones activas que utilizan las funcionalidades AFTR y LSN. Estas sesiones se llaman sesiones DS-Lite. El dispositivo Citrix ADC también mantiene las asig-

naciones entre la dirección IPv6 B4, la dirección IPv4 del suscriptor y el puerto y la dirección y puerto NAT IPv4, para cada sesión de DS-Lite. Estas asignaciones se denominan asignaciones LSN de DS-Lite. A partir de las entradas de sesión de DS-Lite y las entradas de asignación de LSN de DS-Lite, el dispositivo Citrix ADC reconoce que un paquete de respuesta (recibido de Internet) pertenece a una sesión de DS-Lite determinada.

Cuando el dispositivo Citrix ADC recibe un paquete de respuesta perteneciente a una sesión DS-Lite determinada, la funcionalidad LSN del dispositivo traduce la dirección IP de destino y el puerto del paquete de respuesta desde la dirección IP NAT y el puerto a la dirección IP del suscriptor y al puerto, la funcionalidad AFTR encapsula el resultante en un paquete IPv6 y lo envía al dispositivo CPE. La funcionalidad B4 del dispositivo CPE decapsula el paquete IPv6 para recuperar el paquete de respuesta IPv4 y, a continuación, envía el paquete IPv4 al suscriptor.

Ejemplo

Considere un ejemplo de implementación de DS-Lite que consiste en Citrix ADC NS-1 en la red principal de un ISP, el dispositivo CPE B4-CPE-1 en una premisa de suscriptor y un único suscriptor IPv4 SUB-1. B4-CPE-1 admite la funcionalidad B4 de la función DS-Lite.



En la tabla siguiente se enumeran los parámetros utilizados en este ejemplo.

Entidad	Nombre	Detalles
Dirección IPv4 del suscriptor SUB-1		192.0.2.51
Dirección IPv6 del extremo softwire en el dispositivo B4 (B4-CPE-1)		2001:DB8::3:4
Dirección IPv6 del extremo softwire en el dispositivo AFTR (NS-1)		2001:DB8::5:6

Configuración del dispositivo Citrix ADC NS-1:

Entidad	Nombre	Detalles
Cliente LSN	LSN-DSLITE-CLIENT-1	Red6 (Identificación del tráfico de dispositivos B4) = 2001:DB8:: 3:0/100
grupo LSN	LSN-DSLITE-POOL-1	IP LSN (IP NAT) = 203.0.113.61: 203.0.113.70
Perfil IPv6	LSN-DSLITE-PROFILE-1	Type = DS-LITE; IPv6 address (AFTR IPv6 address) = Una de las direcciones IPv6 propiedad de Citrix ADC del tipo SNIP6 = 2001:DB8:: 5:6
Grupo LSN	LSN-DSLITE-GROUP-1	Cliente LSN = LSN-DSLITE-CLIENT-1; grupo LSN = LSN-DSLITE-POOL-1; perfil IPv6 = LSN-DSLITE-PROFILE-1

A continuación se presenta el flujo de tráfico en este ejemplo:

1. El suscriptor IPv4 SUB-1 envía una solicitud a (`http://www.example.com/`). El paquete IPv4 tiene:
    - Dirección IP de origen = 192.0.2.51
    - Puerto de origen = 2552
    - Dirección IP de destino = 198.51.100.250
    - Puerto de destino = 80
2. Al recibir el paquete de solicitud IPv4, B4-CPE-1 lo encapsula en la carga útil de un paquete IPv6 y, a continuación, envía el paquete IPv6 a NS-1. El paquete IPv6 tiene:
    - Dirección IP de origen = 2001:DB8:: 3:4
    - Dirección IP de destino = 2001:DB8:: 5:6
3. Cuando NS-1 recibe el paquete IPv6, el módulo AFTR decapsulará el paquete quitando los encabezados IPv6. El paquete resultante es el paquete de solicitud IPv4 original de SUB-1.
4. El módulo LSN de NS-1 traduce la dirección IP de origen y el puerto del paquete a una dirección IP NAT y puerto NAT seleccionados del grupo NAT configurado. El paquete IPv4 traducido tiene:
    - Dirección IP de la fuente = 203.0.113.61

- Puerto de origen = 3002
- Dirección IP de destino = 198.51.100.250
- Puerto de destino = 80

5. El módulo LSN también crea una asignación LSN y una entrada de sesión para esta sesión de DS Lite. La asignación incluye la siguiente información:
   - Dirección IP de origen del paquete IPv6 (dirección IPv6 de B4-CPE-1) = 2001:DB8:: 3:4
   - Dirección IP de origen del paquete IPv4 (dirección IPv4 de SUB-1) = 192.0.2.51
   - Puerto de origen del paquete IPv4 = 2552
   - Dirección IP NAT = 203.0.113.61
   - Puerto NAT = 3002
6. NS-1 envía el paquete IPv4 resultante a su destino en Internet.
7. El servidor de www.example.com procesa el paquete de solicitud y envía un paquete de respuesta. El paquete de respuesta IPv4 tiene:
   - Dirección IP de la fuente = 198.51.100.250
   - Puerto de origen = 80
   - Dirección IP de destino = 203.0.113.61
   - Puerto de destino = 3002
8. Al recibir el paquete IPv4, NS-1 examina la asignación de LSN y las entradas de sesión y descubre que el paquete de respuesta IPv4 pertenece a una sesión de DS Lite. El módulo LSN de NS-1 traduce la dirección IP de destino y el puerto. El paquete IPv4 ahora tiene:
   - Dirección IP de la fuente = 198.51.100.250
   - Puerto de origen = 80
   - Dirección IP de destino = 192.0.2.51
   - Puerto de destino = 2552
9. El módulo AFTR de NS-1 encapsula el paquete IPv4 en un paquete IPv6 y, a continuación, envía el paquete IPv6 a B4-CPE-1. El paquete IPv6 tiene:
   - Dirección IP de origen = 2001:DB8:: 5:6
   - Dirección IP de destino = 2001:DB8:: 3:4
10. Al recibir el paquete, B4-CPE-1 descapsula el paquete IPv6 quitando los encabezados IPv6 y, a continuación, envía el paquete IPv4 resultante a CL-1.

Puntos a considerar antes de configurar DS-Lite

August 20, 2021

Tenga en cuenta los siguientes puntos antes de configurar DS-Lite en un dispositivo Citrix ADC:

1. Debe comprender los diferentes componentes de DS-Lite, descritos en RFC 6333.
2. Una configuración de DS-Lite en un dispositivo Citrix ADC utiliza los conjuntos de comandos LSN. En una configuración de DS-Lite, la entidad cliente LSN especifica la dirección IPv6 o la dirección de red IPv6 o las reglas ACL6 para identificar el tráfico desde el dispositivo B4. Una configuración de DS-Lite también incluye un perfil IPv6, que especifica el componente AFTR de dirección IPv6 en un dispositivo Citrix ADC. Para obtener más información sobre la función LSN de Citrix ADC, consulte NAT a gran escala.
3. Para una configuración DS-Lite, el dispositivo Citrix ADC admite LSN para paquetes IPv4 que pertenecen únicamente a uno de los siguientes protocolos. El dispositivo Citrix ADC descarta paquetes IPv4 pertenecientes a otros protocolos:
    - TCP
    - UDP
    - ICMP
4. El dispositivo Citrix ADC admite los siguientes ALGs DS-Lite:
    - ICMP
    - FTP
    - TFTP
    - Protocolo de inicio de sesión (SIP)
    - Protocolo de transmisión en tiempo real (RTSP)

Configuración de DS-Lite

August 20, 2021

Una configuración de DS-Lite en un dispositivo Citrix ADC utiliza los conjuntos de comandos LSN. En una configuración de DS-Lite, la entidad cliente LSN especifica la dirección IPv6 o la dirección de red IPv6 o las reglas ACL6 para identificar el tráfico desde el dispositivo B4. Para obtener más información sobre la función Citrix ADC LSN, consulte NAT a gran escala. Una configuración de DS-Lite también incluye un perfil IPv6, que especifica la dirección IPv6 (de tipo SNIP6) del componente AFTR de DS-Lite en un dispositivo Citrix ADC.

La configuración de DS-Lite en un dispositivo Citrix ADC consta de las siguientes tareas:

- **Establezca los parámetros LSN globales**. Los parámetros globales incluyen la cantidad de memoria Citrix ADC reservada para la función LSN y la sincronización de sesiones LSN en una configuración de alta disponibilidad.

- **Cree una entidad cliente LSN para identificar el tráfico de dispositivos CPE B4**. La entidad cliente LSN se refiere a un conjunto de dispositivos DS-Lite B4. La entidad cliente incluye direcciones IPv6 o direcciones de red IPv6 o reglas ACL6 para identificar el tráfico de estos dispositivos B4. Un cliente LSN se puede enlazar a un solo grupo LSN. La interfaz de línea de comandos tiene dos comandos para crear una entidad cliente LSN y vincular un suscriptor a la entidad cliente LSN. La utilidad de configuración combina estas dos operaciones en una sola pantalla.
- **Cree un grupo LSN y vincule direcciones IP NAT a él**. Un grupo LSN define un grupo de direcciones IP NAT que utilizará el dispositivo Citrix ADC para realizar LSN. La interfaz de línea de comandos tiene dos comandos para crear un grupo LSN y vincular direcciones IP NAT al grupo LSN. La utilidad de configuración combina estas dos operaciones en una sola pantalla.
- **Cree un perfil LSN IP6.** Un perfil LSN IP6 define la dirección IPv6 del componente AFTR de DS-Lite en el dispositivo Citrix ADC. La dirección IPv6 debe ser una de las direcciones IPv6 propiedad de Citrix ADC del tipo SNIP6.
- **(Opcional) Cree un perfil de transporte LSN para un protocolo especificado**. Un perfil de transporte LSN define varios tiempos de espera y límites, como el máximo de sesiones LSN y el máximo uso de puertos que un suscriptor puede tener para un protocolo determinado. Enlazar un perfil de transporte LSN para cada protocolo (TCP, UDP e ICMP) a un grupo LSN. Un perfil se puede enlazar a varios grupos LSN. Un perfil enlazado a un grupo LSN se aplica a todos los suscriptores de un cliente LSN vinculado al mismo grupo. De forma predeterminada, un perfil de transporte LSN con la configuración predeterminada para los protocolos TCP, UDP e ICMP está enlazado a un grupo LSN durante su creación. Este perfil se denomina perfil de transporte predeterminado. Un perfil de transporte LSN que se vincula a un grupo LSN anula el perfil de transporte LSN predeterminado para ese protocolo.
- **(Opcional) Cree un perfil de aplicación LSN para un protocolo especificado y vincule un conjunto de puertos de destino a él**. Un perfil de aplicación LSN define la asignación LSN y los controles de filtrado LSN de un grupo para un protocolo determinado y para un conjunto de puertos de destino. Para un conjunto de puertos de destino, se vincula un perfil LSN para cada protocolo (TCP, UDP e ICMP) a un grupo LSN. Un perfil se puede enlazar a varios grupos LSN. Un perfil de aplicación LSN vinculado a un grupo LSN se aplica a todos los suscriptores de un cliente LSN vinculado al mismo grupo. De forma predeterminada, un perfil de aplicación LSN con configuración predeterminada para los protocolos TCP, UDP e ICMP para todos los puertos de destino está enlazado a un grupo LSN durante su creación. Este perfil se denomina perfil de aplicación predeterminado. Cuando vincula un perfil de aplicación LSN, con un conjunto especificado de puertos de destino, a un grupo LSN, el perfil enlazado reemplaza el perfil de aplicación LSN predeterminado para ese protocolo en ese conjunto de puertos de destino. La interfaz de línea de comandos tiene dos comandos para crear un perfil de aplicación LSN y vincular un conjunto de puertos de destino al perfil de aplicación LSN. La utilidad de configuración combina estas dos operaciones en una sola pantalla.

- **Cree un grupo LSN y vincule grupos LSN, perfil LSN IPv6, perfiles de transporte LSN (opcionales) y perfiles de aplicación LSN (opcionales) al grupo LSN**. Un grupo LSN es una entidad formada por un cliente LSN, un perfil IPv6 LSN, grupos LSN, perfiles de transporte LSN y perfiles de aplicación LSN. A un grupo se le asignan parámetros, como el tamaño de bloque de puertos y el registro de sesiones LSN. La configuración de parámetros se aplica a todos los suscriptores de un cliente LSN enlazado al grupo LSN. Solo se puede enlazar un perfil IPv6 de LSN a un grupo LSN, y un perfil IPv6 de LSN vinculado a un grupo LSN no puede vincularse a otros grupos LSN. Solo se pueden enlazar grupos LSN y grupos LSN con la misma configuración de tipo NAT. Los grupos LSN múltiples se pueden enlazar a un grupo LSN. Solo una entidad cliente LSN puede vincularse a un grupo LSN, y una entidad cliente LSN vinculada a un grupo LSN no puede vincularse a otros grupos LSN. La interfaz de línea de comandos tiene dos comandos para crear un grupo LSN y vincular grupos LSN, perfiles de transporte LSN y perfiles de aplicación LSN al grupo LSN. La utilidad de configuración combina estas dos operaciones en una sola pantalla.

Configuración mediante la línea de comandos

Para crear un cliente LSN mediante la interfaz de línea de comandos:

En el símbolo del sistema, escriba:

```
add lsn client <clientname>

show lsn client
<!--NeedCopy-->
```

Para enlazar una red IPv6 o una regla ACL6 a un cliente LSN mediante la interfaz de línea de comandos:

En el símbolo del sistema, escriba:

```
bind lsn client <clientname> (-network6 <ipv6_addr|*>| -acl6name <
   string>)

show lsn client
<!--NeedCopy-->
```

Para crear un grupo LSN mediante la interfaz de línea de comandos:

En el símbolo del sistema, escriba:


```
add lsn pool <poolname> [-nattype ( DYNAMIC )] [-portblockallocation (
    ENABLED | DISABLED )] [-portrealloctimeout <secs>] [-
    maxPortReallocTmq <positive_integer>]

show lsn pool
<!--NeedCopy-->
```

Para enlazar un intervalo de direcciones IP a un grupo LSN mediante la interfaz de línea de comandos:

En el símbolo del sistema, escriba:

```
bind lsn pool <poolname> <lsnip>

show lsn pool
<!--NeedCopy-->
```

Nota: Para eliminar direcciones IP LSN de un grupo LSN, utilice el comando unbind lsn pool.

Para configurar un perfil IPv6 de LSN mediante la interfaz de línea de comandos:

En el símbolo del sistema, escriba:

```
add lsn ip6profile <name>  -type DS-Lite  -network6 < ipv6_addr|*s >

show lsn ip6profile
<!--NeedCopy-->
```

Para crear un perfil de transporte LSN mediante la interfaz de línea de comandos:

En el símbolo del sistema, escriba:

```
add lsn transportprofile <transportprofilename> <transportprotocol> [-
    sessiontimeout <secs>] [-finrsttimeout <secs>] [-portquota <
    positive_integer>] [-sessionquota <positive_integer>] [-
    portpreserveparity ( ENABLED | DISABLED )] [-portpreserverange (
    ENABLED | DISABLED )] [-syncheck ( ENABLED | DISABLED )]

show lsn transportprofile
<!--NeedCopy-->
```


Para crear un perfil de aplicación LSN mediante la interfaz de línea de comandos:

En el símbolo del sistema, escriba:

```
add lsn appsprofile <appsprofilename> <transportprotocol> [-ippooling (
    PAIRED | RANDOM )] [-mapping <mapping>] [-filtering <filtering>][-
    tcpproxy ( ENABLED | DISABLED )] [-td <positive_integer>]

show lsn appsprofile
<!--NeedCopy-->
```

Para enlazar un rango de puertos de protocolo de aplicación a un perfil de aplicación LSN mediante la interfaz de línea de comandos:

En el símbolo del sistema, escriba:

```
bind lsn appsprofile <appsprofilename> <lsnport>

show lsn appsprofile
<!--NeedCopy-->
```

Para crear un grupo LSN mediante la interfaz de línea de comandos:

En el símbolo del sistema, escriba:

```
add lsn group <groupname> -clientname <string> [-nattype ( DYNAMIC )]
    [-portblocksize <positive_integer>] [-logging (ENABLED | DISABLED )]
     [-sessionLogging ( ENABLED | DISABLED )][-sessionSync ( ENABLED |
    DISABLED )] [-snmptraplimit<positive_integer>] [-ftp ( ENABLED |
    DISABLED )] [-pptp ( ENABLED |DISABLED )] [-sipalg ( ENABLED |
    DISABLED )] [-rtspalg ( ENABLED |DISABLED )] [-ip6profile <string>]

show lsn group
<!--NeedCopy-->
```

Para enlazar perfiles de protocolo LSN y grupos LSN a un grupo LSN mediante la interfaz de línea de comandos:

En el símbolo del sistema, escriba:


```
bind lsn group <groupname> (-poolname <string> | -transportprofilename
    <string> | -httphdrlogprofilename <string> | -appsprofilename <
    string> | -sipalgprofilename <string> | rtspalgprofilename <string>)

show lsn group
<!--NeedCopy-->
```

Configuración mediante la utilidad de configuración

Para configurar un cliente LSN y enlazar una dirección de red IPv6 o una regla ACL6 mediante la utilidad de configuración:

Desplácese hasta **Sistema** > **NAT a gran escala** > **Clientes**, agregue un cliente y, a continuación, vincule una dirección de red IPv6 o una regla ACL6 al cliente.

Para configurar un grupo LSN y enlazar direcciones IP NAT mediante la utilidad de configuración:

Vaya a **Sistema** > **NAT a gran escala** > **Grupos**y agregue un grupo y, a continuación, vincule una dirección IP NAT o un rango de direcciones IP NAT al grupo.

Para configurar un perfil IPv6 de LSN mediante la utilidad de configuración:

Vaya a **Sistema** > **NAT de gran escala** > **Perfiles**, haga clic en la ficha **IPv6** y asigne una dirección IPv6 para DS-Lite AFTR.

Para configurar un perfil de transporte LSN mediante la utilidad de configuración:

1. Vaya a **Sistema** > **NAT a gran escala** > **Perfiles**.
2. En el panel de detalles, haga clic en **Transporte** y, a continuación, agregue un perfil de transporte.

Para configurar un perfil de aplicación LSN mediante la utilidad de configuración:

1. Vaya a **Sistema** > **NAT a gran escala** > **Perfiles**.
2. En el panel de detalles, haga clic en **Aplicación** y, a continuación, agregue un perfil de aplicación.

Para configurar un grupo LSN y enlazar un cliente LSN, un perfil IPv6 LSN, grupos, perfiles de transporte y perfiles de aplicación mediante la utilidad de configuración:

Desplácese hasta **Sistema** > **NAT a gran escala** > **Grupos**, agregue un grupo y, a continuación, vincule un cliente LSN, un perfil IPv6 de LSN, grupos, perfiles de transporte y perfiles de aplicación al grupo.

```
> add lsn client LSN-DSLITE-CLIENT-1
Done
> bind lsn client LSN-DSLITE-CLIENT-1 -network6 2001:DB8::3:0/100
```



```
4  Done
5  > add lsn pool LSN-DSLITE-POOL-1
6  Done
7  > bind lsn pool LSN-DSLITE-POOL-1 203.0.113.61 - 203.0.113.70
8  Done
9  > add lsn ip6profile LSN-DSLITE-PROFILE-1 -type DS-Lite -network6 2001:
       DB8::5:6
10 Done
11 > add lsn group LSN-DSLITE-GROUP-1 -clientname LSN-DSLITE-CLIENT-1 -
       portblocksize 1024 -ip6profile LSN-DSLITE-PROFILE-1
12 Done
13 > add lsn group LSN-DSLITE-GROUP-1 -poolname LSN-DSLITE-POOL-1
14 Done
```

Registro y supervisión DS-Lite

Puede registrar la información de DS-Lite para diagnosticar o solucionar problemas y para cumplir los requisitos legales. El dispositivo Citrix ADC admite todas las funciones de registro LSN para registrar información de DS-Lite. Para configurar el registro de DS-Lite, utilice los procedimientos para configurar el registro LSN, descritos en Registro y supervisión de LSN.

Un mensaje de registro para una entrada de asignación de LSN de DS-Lite consta de la siguiente información:

- Dirección IP propiedad de Citrix ADC (dirección NSIP o dirección SNIP) desde la que se origina el mensaje de registro
- Marca de tiempo
- Tipo de entrada (MAPPING)
- Si se ha creado o eliminado la entrada de asignación LSN de DS-Lite
- Dirección IPv6 de B4
- Dirección IP, puerto e ID de dominio de tráfico del suscriptor
- Dirección IP NAT y puerto
- Nombre del protocolo
- La dirección IP de destino, el puerto y el ID de dominio de tráfico pueden estar presentes, en función de las condiciones siguientes:
  - La dirección IP de destino y el puerto no se registran para la asignación independiente del punto final.
  - Solo se registra la dirección IP de destino para la asignación dependiente de direcciones. El puerto no está registrado.
  - La dirección IP de destino y el puerto se registran para la asignación dependiente del puerto de dirección.

Un mensaje de registro para una sesión de DS-Lite consta de la siguiente información:

- Dirección IP propiedad de Citrix ADC (dirección NSIP o dirección SNIP) desde la que se origina el mensaje de registro
- Marca de tiempo
- Tipo de entrada (SESSION)
- Si se crea o elimina la sesión de DS-Lite
- Dirección IPv6 de B4
- Dirección IP, puerto e ID de dominio de tráfico del suscriptor
- Dirección IP NAT y puerto
- Nombre del protocolo
- Dirección IP de destino, puerto e ID de dominio de tráfico

En la tabla siguiente se muestran las entradas de registro DS-Lite de ejemplo de cada tipo almacenadas en los servidores de registro configurados. Estas entradas de registro las genera un dispositivo Citrix ADC cuya dirección NSIP es 10.102.37.115.Puede registrar información de DS-Lite para diagnosticar o solucionar problemas y cumplir los requisitos legales. El dispositivo Citrix ADC admite todas las funciones de registro LSN para registrar información de DS-Lite. Para configurar el registro de DS-Lite, utilice los procedimientos para configurar el registro LSN, descritos en Registro y supervisión de LSN.

Un mensaje de registro para una entrada de asignación de LSN de DS-Lite consta de la siguiente información:

- Dirección IP propiedad de Citrix ADC (dirección NSIP o dirección SNIP) desde la que se origina el mensaje de registro
- Marca de tiempo
- Tipo de entrada (MAPPING)
- Si se ha creado o eliminado la entrada de asignación LSN de DS-Lite
- Dirección IPv6 de B4
- Dirección IP, puerto e ID de dominio de tráfico del suscriptor
- Dirección IP NAT y puerto
- Nombre del protocolo
- La dirección IP de destino, el puerto y el ID de dominio de tráfico pueden estar presentes, en función de las condiciones siguientes:
  - La dirección IP de destino y el puerto no se registran para la asignación independiente del punto final.
  - Solo se registra la dirección IP de destino para la asignación dependiente de direcciones. El puerto no está registrado.
  - La dirección IP de destino y el puerto se registran para la asignación dependiente del puerto de dirección.

Un mensaje de registro para una sesión de DS-Lite consta de la siguiente información:

- Dirección IP propiedad de Citrix ADC (dirección NSIP o dirección SNIP) desde la que se origina

el mensaje de registro
- Marca de tiempo
- Tipo de entrada (SESSION)
- Si se crea o elimina la sesión de DS-Lite
- Dirección IPv6 de B4
- Dirección IP, puerto e ID de dominio de tráfico del suscriptor
- Dirección IP NAT y puerto
- Nombre del protocolo
- Dirección IP de destino, puerto e ID de dominio de tráfico

En la tabla siguiente se muestran las entradas de registro DS-Lite de ejemplo de cada tipo almacenadas en los servidores de registro configurados. Estas entradas de registro las genera un dispositivo Citrix ADC cuya dirección NSIP es 10.102.37.115.

Tipo de entrada de registro LSN	Entrada de registro de ejemplo
Creación de sesiones de DS-Lite	Local4.Informational 10.102.37.115 08/14/2015:13:35:38 GMT 0-PPE-1: Default LSN LSN_SESSION 37647607 0: SESSION CREATED 2001:DB8::3:4 Client IP:Port:TD 192.0.2.51:2552:0, NatIP:NatPort 203.0.113.61:3002, Destination IP:Port:TD 198.51.100.250:80:0, Protocol:TCP
Eliminación de sesión de DS-Lite	Local4.Informational 10.102.37.115 08/14/2015:13:38:22 GMT 0-PPE-1: Default LSN LSN_SESSION 37647617 0: SESSION DELETED 2001:DB8::3:4 Client IP:Port:TD 192.0.2.51:2552:0, NatIP:NatPort 203.0.113.61:3002, Destination IP:Port:TD 198.51.100.250:80:0, Protocol: TCP
Creación de mapeo LSN de DS-Lite	Local4.Informational 10.102.37.115 08/14/2015:13:35:39 GMT 0-PPE-1: Default LSN LSN_EIM_MAPPING 37647610 0: EIM CREATED 2001:DB8::3:4 Client IP:Port:TD 192.0.2.51:2552:0, NatIP:NatPort 198.51.100.250:80, Protocol: TCP

Eliminación de asignación de LSN de DS-Lite	Local4.Informational 10.102.37.115 08/14/2015:13:38:25 GMT 0-PPE-1: Default LSN LSN_EIM_MAPPING 37647618 0: EIM DELETED 2001:DB8::3:4 Client IP:Port:TD 192.0.2.51:2552:0, NatIP:NatPort 198.51.100.250:80, Protocol: TCP

Visualización de sesiones DS-Lite actuales

Puede mostrar las sesiones DS-Lite actuales para detectar sesiones no deseadas o ineficientes en el dispositivo Citrix ADC. Puede mostrar todas o algunas sesiones de DS-Lite, sobre la base de los parámetros de selección.

Configuración mediante la interfaz de línea de comandos

Para mostrar todas las sesiones de DS-Lite mediante la interfaz de línea de comandos:

En el símbolo del sistema, escriba:

```
show lsn session  - nattype DS-Lite
<!--NeedCopy-->
```

Para mostrar las sesiones DS-Lite seleccionadas mediante la interfaz de línea de comandos:

En el símbolo del sistema, escriba:

```
show lsn session  - nattype DS-Lite [-clientname <string>] [-network <
    ip_addr> [-netmask <netmask>] [-td <positive_integer>]] [-natIP <
    ip_addr> [-natPort <port>]]
<!--NeedCopy-->
```

Ejemplo:

La salida de ejemplo siguiente muestra todas las sesiones DS-Lite existentes en un dispositivo Citrix ADC:


```
show lsn session  - nattype DS-Lite
  B4-Address SubscrIP SubscrPort SubscrTD DstIP DstPort DstTD NatIP
     NatPort Proto Dir

1.  2001:DB8::3:4 192.0.2.51 2552 0 198.51.100.250 80 0 203.0.113.61
    3002 TCP OUT

2.  2001:DB8::3:4 192.0.2.51 3551 0 198.51.100.300 80 0 203.0.113.61
    52862 TCP OUT

3.  2001:DB8::3:4 192.0.2.100 4556 0 198.51.100.250 0 0 203.0.113.61
    48116 ICMP OUT

4.  2001: DB8::190 192.0.2.150 3881 0 198.51.100.199 80 0 203.0.113.69
    48305 TCP OUT

Done
<!--NeedCopy-->
```

Configuración mediante la utilidad de configuración

Para mostrar todas las sesiones DS-Lite o seleccionadas mediante la utilidad de configuración

1. **Vaya a Sistema** > **NAT a gran escala** > **Sesiones**y haga clic en la ficha **DS-Lite** .
2. Para mostrar sesiones de DS-Lite sobre la base de parámetros de selección, haga clic en **Buscar**.

Borrar sesiones de DS-Lite

Puede eliminar todas las sesiones DS-Lite no deseadas o ineficientes del dispositivo Citrix ADC. El dispositivo libera inmediatamente los recursos (como la dirección IP de NAT, el puerto y la memoria) asignados para estas sesiones, lo que hace que los recursos estén disponibles para las sesiones nuevas. El dispositivo también elimina todos los paquetes posteriores relacionados con estas sesiones eliminadas. Puede quitar todas las sesiones DS-Lite o seleccionadas del dispositivo Citrix ADC.

Para borrar todas las sesiones de DS-Lite mediante la interfaz de línea de comandos:

En el símbolo del sistema, escriba:

```
flush lsn session -nattype DS-Lite
show lsn session -nattype DS-Lite
```

Para borrar sesiones DS-Lite seleccionadas mediante la interfaz de línea de comandos:

En el símbolo del sistema, escriba:


```
flush lsn session  - nattype DS-Lite [-clientname <string>] [-network <
    ip_addr> [-netmask <netmask>] [-td <positive_integer>]] [-natIP <
    ip_addr> [-natPort <port>]]

show lsn session  - nattype DS-Lite
<!--NeedCopy-->
```

Para borrar todas las sesiones DS-Lite o seleccionadas mediante la utilidad de configuración:

1. Vaya a **Sistema** > **NAT a gran escala** > **Sesiones**y haga clic en la ficha **DS-Lite**.
2. Haga clic en **Vaciar sesiones**.

Configuración de mapas estáticos DS-Lite

August 20, 2021

El dispositivo Citrix ADC admite la creación manual de asignaciones LSN de DS-Lite, que contienen la asignación entre la siguiente información:

- Dirección IP y puerto del suscriptor, y dirección IPv6 del dispositivo o componente B4
- Dirección IP NAT y puerto

Las asignaciones estáticas de LSN DS-Lite son útiles en los casos en que quiere asegurarse de que las conexiones iniciadas a una dirección IP NAT y puerto se asignan a la dirección IP del suscriptor y al puerto a través del dispositivo B4 especificado (por ejemplo, servidores web ubicados en la red interna).

Nota: Esta función se admite en la versión 11.0 compilación 64.x y versiones posteriores.

Para crear una asignación de LSN estática de DS-Lite mediante la línea de comandos

En el símbolo del sistema, escriba:

```
add lsn static <name> <transportprotocol> <subscrIP> <subscrPort> [-td
    <positive_integer>] [-network6 <B4_ADDR>] [<natIP> [<natPort>]] [-
    destIP<ip_addr> [-dsttd <positive_integer>]]

show lsn static
<!--NeedCopy-->
```


Descripciones de parámetros

agregar lsn estática

- nombre

Nombre de la entrada de asignación estática LSN. Debe comenzar con un carácter alfanumérico o de subrayado (_) ASCII y debe contener solo caracteres alfanuméricos ASCII, guión bajo, hash (#), punto (.), espacio, dos puntos (:), en (@), igual (=) y guión (-). No se puede cambiar después de crear el grupo LSN. El siguiente requisito solo se aplica a la CLI: Si el nombre incluye uno o más espacios, escriba el nombre entre comillas dobles o simples (por ejemplo, “ds-lite lsn static1” o ‘ds-lite lsn static1’). Este es un argumento obligatorio. Longitud máxima: 127

- transportprotocol

Protocolo para la entrada de asignación LSN DS-Lite.

- subscrIP

Dirección IPv4 de un suscriptor para la entrada de asignación LSN DS-Lite.

- subscrPort

Puerto del suscriptor para la entrada de asignación LSN DS-Lite.

- Network6

Dirección IPv6 del dispositivo o componente B4.

- td

Id. del dominio de tráfico al que pertenece el dispositivo B4. La dirección IPv6 del dispositivo B4 se especifica en el parámetro network6. Si no especifica un ID, se supone que el dispositivo B4 forma parte del dominio de tráfico predeterminado.

- natIP

Dirección IPv4, ya existente en el dispositivo Citrix ADC como tipo LSN, que se utilizará como dirección IP NAT para esta entrada de asignación.

- natPort

Puerto NAT para esta entrada de asignación LSN DS-Lite.

- destIP

Dirección IP de destino para la entrada de asignación LSN DS-Lite.

- Dsttd

Id. del dominio de tráfico a través del cual se puede acceder a la dirección IP de destino para esta entrada de asignación de LSN de DS-Lite desde el dispositivo Citrix ADC. Si no especifica un ID, se supone que la dirección IP de destino es accesible a través del dominio de tráfico predeterminado, que tiene un ID de 0.

Para crear una asignación de LSN estática de DS-Lite mediante la utilidad de configuración

Vaya a Sistema > NAT a gran escala > Estático y agregue una nueva asignación de LSN estática de DS-Lite.

Configuración de la asignación de NAT determinista para DS-Lite

January 19, 2021

La asignación de NAT determinista para implementaciones de LSN DS-Lite es un tipo de asignación de recursos NAT en el que el dispositivo Citrix ADC asigna previamente, desde el grupo de IP NAT de LSN y sobre la base del tamaño de bloque de puertos especificado, una dirección IP NAT de LSN y un bloque de puertos a cada suscriptor (suscriptor detrás del dispositivo B4).

Nota: Esta función se admite en la versión 11.0 compilación 64.x y versiones posteriores.

El dispositivo asigna secuencialmente recursos NAT a estos suscriptores. Asigna el primer bloque de puertos en la dirección IP NAT inicial a la dirección IP del suscriptor inicial. El siguiente rango de puertos se asigna al siguiente suscriptor, y así sucesivamente, hasta que la dirección NAT no tenga suficientes puertos para el siguiente suscriptor. En ese punto, el primer bloque de puerto de la siguiente dirección NAT se asigna al suscriptor, y así sucesivamente.

El dispositivo Citrix ADC registra la dirección IP NAT asignada y el bloque de puertos para un suscriptor. Para una conexión, un suscriptor puede ser identificado solo por su dirección IP NAT asignada y bloque de puerto. Por este motivo, el dispositivo Citrix ADC no registra la creación o eliminación de una sesión LSN.

Un suscriptor de DS-Lite solo puede tener un bloque de puerto determinista. Si se está usando todo el bloque de puertos, el dispositivo Citrix ADC elimina cualquier conexión nueva del suscriptor.

Ejemplo: DS-Lite determinista

En este ejemplo, una configuración determinista DS-Lite incluye cuatro suscriptores con direcciones IP 192.0.17.5, 192.0.17.6, 192.0.17.7 y 192.0.17.8. Estos suscriptores IPv4 están detrás de un dispositivo B4 que tiene la dirección IPv6 2001:DB8:: 3:4. En esta configuración, el tamaño del bloque de puerto se establece en 20480 y el grupo de direcciones IP NAT LSN tiene direcciones IP en el rango 203.0.113.41-203.0.113.42.

El dispositivo Citrix ADC asigna de forma secuencial, desde el grupo IP NAT de LSN y sobre la base del tamaño de bloque de puerto establecido, una dirección IP NAT de LSN y un bloque de puertos a cada suscriptor. Asigna el primer bloque de puertos (1024-21503) en la dirección IP NAT inicial (203.0.113.41)

a la dirección IP del suscriptor inicial (192.0.17.5). El siguiente rango de puertos se asigna al siguiente suscriptor, y así sucesivamente, hasta que la dirección NAT no tenga suficientes puertos para el siguiente suscriptor. En ese punto, el primer bloque de puerto de la siguiente dirección IP NAT se asigna al suscriptor, y así sucesivamente. El Citrix ADC registra la dirección IP NAT y el bloque de puertos asignados para cada suscriptor.

El dispositivo Citrix ADC no registra ninguna sesión LSN creada o eliminada para estos suscriptores.

En la siguiente tabla se enumeran la dirección IP NAT y los bloques de puertos asignados a cada suscriptor en este ejemplo:

Dirección IP del suscriptor	Dirección IP NAT asignada	Bloque de puertos asignado	Dirección IPv6 de B4
192.0.17.5	203.0.113.41	1024: 21503	2001:DB8::3:4
192.0.17.6	203.0.113.41	21504: 41983	2001:DB8::3:4
192.0.17.7	203.0.113.41	41984: 62463	2001:DB8::3:4
192.0.17.8	203.0.113.42	1024: 21503	2001:DB8::3:4

Pasos de configuración

Debe configurar NAT determinista como parte de la configuración DS-Lite. Para obtener instrucciones sobre cómo configurar DS-Lite, consulte Configuración de DS-Lite.

Al configurar DS-Lite, asegúrese de que:

- Establezca el parámetro Tipo de NAT en Determinista al agregar el grupo LSN y el grupo LSN.
- Establezca el parámetro de tamaño de bloque de puerto deseado al agregar el grupo LSN, a menos que pueda aceptar el valor predeterminado.

Puntos a considerar antes de configurar DS-Lite determinista

Considere los siguientes puntos antes de configurar DS-Lite determinista:

- La dirección IP completa de cada suscriptor debe especificarse en un comando add lsn client independiente, estableciendo los parámetros Network y Netmask. (Establezca la máscara de red en 255.255.255.255.) También la dirección IPv4 del dispositivo B4 especificado en el parámetro Network6 debe estar completa (/128 prefijo). En otras palabras, los parámetros Network y Network6 no aceptan direcciones distintas de /32 bit mask y /128 prefijo, respectivamente.

- El dispositivo Citrix ADC elimina las conexiones de los suscriptores que no se especifican en ninguna configuración determinista de DS-Lite, pero que están detrás de dispositivos B4 especificados en una configuración determinista de DS-Lite.
- El dispositivo Citrix ADC reconoce a los suscriptores que tienen la misma dirección IPv4 que los suscriptores diferentes si están detrás de diferentes dispositivos B4. Una combinación de dirección IPv4 del suscriptor y dispositivo B4 define un suscriptor único en la entidad cliente LSN de una configuración DS-Lite.

Ejemplo de configuración determinista DS-Lite:

La siguiente configuración utiliza los parámetros enumerados en la sección Ejemplo: Determinista DS-Lite.

```
add lsn client LSN-DSLITE-CLIENT-10

Done
bind lsn client LSN-DSLITE-CLIENT-10 -network 192.0.17.5 -netmask
    255.255.255.255 -network6 2001:DB8::3:4/128

Done
bind lsn client LSN-DSLITE-CLIENT-10 -network 192.0.17.6 -netmask
    255.255.255.255 -network6 2001:DB8::3:4/128

Done
bind lsn client LSN-DSLITE-CLIENT-10 -network 192.0.17.7 -netmask
    255.255.255.255 -network6 2001:DB8::3:4/128

Done
bind lsn client LSN-DSLITE-CLIENT-10 -network 192.0.17.8 -netmask
    255.255.255.255 -network6 2001:DB8::3:4/128

Done
add lsn pool LSN-DSLITE-POOL-10 -nattype DETERMINISTIC

Done
bind lsn pool LSN-DSLITE-POOL-10  203.0.113.41-203.0.113.42

Done
add lsn ip6profile LSN-DSLITE-PROFILE-10 -type DS-Lite -network6 2001:
    DB8::5:6

Done
add lsn group LSN-DSLITE-GROUP-10 -clientname LSN-DSLITE-CLIENT-10 -
    nattype DETERMINISTIC -portblocksize 20480 -ip6profile LSN-DSLITE-
```



```
      PROFILE-10
26
27 Done
28 bind lsn group LSN-DSLITE-GROUP-10 -poolname LSN-DSLITE-POOL-10
29
30 Done
31 <!--NeedCopy-->
```

Configuración de puertas de enlace de capa de aplicación para DS-Lite

January 12, 2021

Para algunos protocolos de capa de aplicación, las direcciones IP y los números de puerto de protocolo también se comunican en la carga útil del paquete. Application Layer Gateway (AGL) para un protocolo analiza la carga útil del paquete y realiza los cambios necesarios para garantizar que el protocolo continúa funcionando sobre DS-Lite.

El dispositivo Citrix ADC admite ALG para los siguientes protocolos para DS-Lite:

- FTP
- ICMP
- TFTP
- SIP
- RTSP

Puerta de enlace de capa de aplicación para protocolos FTP, ICMP y TFTP

January 12, 2021

Puede habilitar o inhabilitar ALG para el protocolo FTP para una configuración DS-Lite habilitando o inhabilitando la opción FTP ALG del grupo LSN de la configuración.

ALG para el protocolo ICMP está habilitado de forma predeterminada, y no hay ninguna disposición para inhabilitarlo.

ALG para el protocolo TFTP está inhabilitado de forma predeterminada. TFTP ALG se habilita automáticamente para una configuración DS-Lite cuando se vincula un perfil de aplicación UDP LSN, con asignación independiente del punto final, filtrado independiente del punto final y puerto de destino como 69 (puerto conocido para TFTP), al grupo LSN.

Puerta de enlace de capa de aplicación para protocolo SIP

August 20, 2021

El uso de DS-Lite con el Protocolo de Iniciación de Sesión (SIP) es complicado, ya que los mensajes SIP contienen direcciones IP en los encabezados SIP, así como en el cuerpo SIP. Cuando LSN se utiliza con SIP, los encabezados SIP contienen información sobre la persona que llama y el receptor, y el dispositivo traduce esta información para ocultarla de la red externa. El cuerpo SIP contiene la información del Protocolo de descripción de la sesión (SDP), que incluye direcciones IP y números de puerto para la transmisión de los medios. SIP ALG para DS-Lite es compatible con RFC 3261, RFC 3581, RFC 4566 y RFC 4475.

> **Nota**
>
> SIP ALG se admite en un dispositivo independiente de Citrix ADC, en una configuración de alta disponibilidad de Citrix ADC, así como en una configuración de clúster de Citrix ADC.

Limitaciones de SIP ALG

SIP ALG para DS-Lite tiene las siguientes limitaciones:

- Solo se admite la carga de SDP.
- Estas opciones no se admiten:
  - Direcciones IP de multidifusión
  - SDP cifrado
  - SIP TLS
  - Traducción FQDN
  - Autenticación de capa SIP
  - Particiones de administración
  - Cuerpo con varias partes
  - Plegable de línea

Configuración de SIP ALG

Debe configurar el SIP ALG como parte de la configuración LSN. Para obtener instrucciones sobre cómo configurar LSN, consulte Configuración de DS-Lite. Al configurar LSN, asegúrese de que:

- Defina los siguientes parámetros al agregar un perfil de aplicación LSN:
  - Agrupamiento de IP = PAIRED
  - Asignación de direcciones y puertos = ENDPOINT-INDEPENDENT
  - Filtrado = ENDPOINT-INDEPENDENT

- Cree un perfil SIP ALG y asegúrese de definir el rango de puertos de origen o el rango de puertos de destino. Enlace el perfil SIP ALG al grupo LSN
- Habilitar SIP ALG en el grupo LSN

Para habilitar SIP ALG para una configuración LSN mediante la CLI

En el símbolo del sistema, escriba:

```
add lsn group <groupname> -clientname <string>[-sipalg ( ENABLED |
    DISABLED )]

show lsn group<groupname>
<!--NeedCopy-->
```

Para habilitar SIP ALG para una configuración LSN mediante la CLI

En el símbolo del sistema, escriba:

```
add lsn sipalgprofile<sipalgprofilename>[-dataSessionIdleTimeout<
    positive_integer>][-sipSessionTimeout<positive_integer>][-
    registrationTimeout<positive_integer>][-sipsrcportrange<port[-port
    ]>][-sipdstportrange<port[-port]>][-openRegisterPinhole ( ENABLED |
    DISABLED )][-openContactPinhole ( ENABLED | DISABLED )][-
    openViaPinhole ( ENABLED | DISABLED )][-openRecordRoutePinhole (
    ENABLED | DISABLED )]-sipTransportProtocol ( TCP | UDP )[-
    openRoutePinhole ( ENABLED | DISABLED )][-rport ( ENABLED | DISABLED
     )]

show lsn sipalgprofile<sipalgprofilename>
<!--NeedCopy-->
```

Configuración de ejemplo

El siguiente ejemplo de configuración DS-Lite, SIP ALG está habilitado para el tráfico TCP desde dispositivos B4 en la red 2001:DB8:: 3:0/96.

```
add lsn client LSN-DSLITE-CLIENT-1
Done
```



```
bind lsn client LSN-DSLITE-CLIENT-1 -network6 2001:DB8::3:0/96
Done
add lsn pool LSN-DSLITE-POOL-1
Done
bind lsn pool LSN-DSLITE-POOL-1 203.0.113.61 - 203.0.113.70
Done
add lsn ip6profile LSN-DSLITE-PROFILE-1 -type DS-Lite -network6 2001:
   DB8::5:6
Done
add lsn appsprofile LSN-DSLITE-APPS-PROFILE-1 TCP -ippooling PAIRED -
   mapping ENDPOINT-INDEPENDENT -filtering ENDPOINT-INDEPENDENT
Done
add lsn sipalgprofile SIPALGPROFILE-1  -sipdstportrange 5060 -
   sipTransportProtocol TCP
Done
add lsn group LSN-DSLITE-GROUP-1 -clientname LSN-DSLITE-CLIENT-1 -
   portblocksize 1024 -ip6profile LSN-DSLITE-PROFILE-1 -sipalg ENABLED
Done
bind lsn group LSN-DSLITE-GROUP-1 -poolname LSN-DSLITE-POOL-1
Done
bind lsn group LSN-DSLITE-GROUP-1 -appsprofilename LSN-DSLITE-APPS-
   PROFILE-1
Done
bind lsn group LSN-DSLITE-GROUP-1 -sipalgprofilename SIPALGPROFILE-1
Done
<!--NeedCopy-->
```

Puerta de enlace de capa de aplicación para protocolo RTSP

January 19, 2021

Real Time Streaming Protocol (RTSP) es un protocolo de nivel de aplicación para la transferencia de datos de medios en tiempo real. Utilizado para establecer y controlar sesiones de medios entre puntos finales, RTSP es un protocolo de canal de control entre el cliente de medios y el servidor de medios. La comunicación típica es entre un cliente y un servidor multimedia de streaming.

La transmisión de medios desde una red privada a una red pública requiere traducir direcciones IP y números de puerto a través de la red. La funcionalidad Citrix ADC incluye una puerta de enlace de capa de aplicación (ALG) para RTSP, que se puede utilizar con NAT de gran escala (LSN) para analizar la secuencia de medios y realizar los cambios necesarios para garantizar que el protocolo continúe funcionando a través de la red.

La forma en que se realiza la traducción de direcciones IP depende del tipo y la dirección del mensaje y del tipo de medios admitidos por la implementación cliente-servidor. Los mensajes se traducen de la siguiente manera:

- Solicitud saliente: Dirección IP privada a la dirección IP pública propiedad de Citrix ADC llamada dirección IP LSN.
- Respuesta entrante: Dirección IP LSN a dirección IP privada.
- Solicitud entrante: Sin traducción.
- Respuesta saliente: Dirección IP privada a la dirección IP del grupo LSN.

> **Nota**
>
> RTSP ALG se admite en un dispositivo independiente de Citrix ADC, en una configuración de alta disponibilidad de Citrix ADC, así como en una configuración de clúster de Citrix ADC.

Limitaciones de RTSP ALG

El RTSP ALG no admite lo siguiente:

- Sesiones RTSP multidifusión
- Sesión RTSP sobre UDP
- Particiones de administración
- Autenticación RTSP
- Tunelización HTTP

Configuración de RTSP ALG

Configure RTSP ALG como parte de la configuración LSN. Para obtener instrucciones sobre cómo configurar LSN, consulte Configuración de DS-Lite. Al configurar LSN, asegúrese de que:

- Defina los siguientes parámetros al agregar un perfil de aplicación LSN:
  - Agrupamiento de IP = PAIRED
  - Asignación de direcciones y puertos = ENDPOINT-INDEPENDENT
  - Filtrado = ENDPOINT-INDEPENDENT
- Habilitar RTSP ALG en el grupo LSN
- Crear un perfil RTSP ALG y enlazar el perfil RTSP ALG al grupo LSN

Para habilitar RTSP ALG para una configuración LSN mediante la CLI

En el símbolo del sistema, escriba:


```
add lsn group <groupname> -clientname <string> [-rtspalg ( ENABLED |
    DISABLED )]

show lsn group <groupname>
<!--NeedCopy-->
```

Para habilitar RTSP ALG para una configuración LSN mediante la CLI

En el símbolo del sistema, escriba:

```
add lsn rtspalgprofile <rtspalgprofilename> [-rtspIdleTimeout <
    positive_integer>] -rtspportrange <port[-port]> [-
    rtspTransportProtocol (TCP|UDP)]

show lsn rtspalgprofile <rtspalgprofilename>
<!--NeedCopy-->
```

Ejemplo de configuración RTSP ALG

El siguiente ejemplo de configuración DS-Lite, RTSP ALG está habilitado para el tráfico TCP desde dispositivos B4 en la red 2001:DB8:: 4:0/96.

Ejemplo de configuración RTSP ALG:

```
add lsn client LSN-DSLITE-CLIENT-5
Done
bind lsn client LSN-DSLITE-CLIENT-5 -network6 2001:DB8::4:0/96
Done
add lsn pool LSN-DSLITE-POOL-5
Done
bind lsn pool LSN-DSLITE-POOL-5 203.0.113.61 - 203.0.113.70
Done
add lsn ip6profile LSN-DSLITE-PROFILE-5 -type DS-Lite -network6 2001:
    DB8::5:6
Done
add lsn appsprofile LSN-DSLITE-APPS-PROFILE-5 TCP -ippooling PAIRED -
    mapping ENDPOINT-INDEPENDENT -filtering ENDPOINT-INDEPENDENT
Done
add lsn rtspalgprofile RTSPALGPROFILE-5 -rtspIdleTimeout 1000 -
    rtspportrange 554
```



```
14 Done
15 add lsn group LSN-DSLITE-GROUP-5 -clientname LSN-DSLITE-CLIENT-5 -
      portblocksize 1024 -ip6profile LSN-DSLITE-PROFILE-5 -rtspalg ENABLED
16 Done
17 bind lsn group LSN-DSLITE-GROUP-5 -poolname LSN-DSLITE-POOL-5
18 Done
19 bind lsn group LSN-DSLITE-GROUP-5 -appsprofilename LSN-DSLITE-APPS-
      PROFILE-5
20 Done
21 bind lsn group LSN-DSLITE-GROUP-5 -rtspalgprofilename RTSPALGPROFILE-5
22 Done
23 <!--NeedCopy-->
```

Registro y supervisión DS-Lite

August 20, 2021

Puede registrar la información de DS-Lite para diagnosticar o solucionar problemas y para cumplir los requisitos legales. El dispositivo Citrix ADC admite todas las funciones de registro LSN para registrar información de DS-Lite. Para configurar el registro de DS-Lite, utilice los procedimientos para configurar el registro LSN, descritos en Registro y supervisión de LSN.

Un mensaje de registro para una entrada de asignación de LSN de DS-Lite consta de la siguiente información:

- Dirección IP propiedad de Citrix ADC (dirección NSIP o dirección SNIP) desde la que se origina el mensaje de registro
- Marca de tiempo
- Tipo de entrada (MAPPING)
- Si se ha creado o eliminado la entrada de asignación LSN de DS-Lite
- Dirección IPv6 de B4
- Dirección IP, puerto e ID de dominio de tráfico del suscriptor
- Dirección IP NAT y puerto
- Nombre del protocolo
- La dirección IP de destino, el puerto y el ID de dominio de tráfico pueden estar presentes, en función de las condiciones siguientes:
  - La dirección IP de destino y el puerto no se registran para la asignación independiente del punto final.
  - Solo se registra la dirección IP de destino para la asignación dependiente de direcciones. El puerto no está registrado.

  - La dirección IP de destino y el puerto se registran para la asignación dependiente del puerto de dirección.

Un mensaje de registro para una sesión de DS-Lite consta de la siguiente información:

- Dirección IP propiedad de Citrix ADC (dirección NSIP o dirección SNIP) desde la que se origina el mensaje de registro
- Marca de tiempo
- Tipo de entrada (SESSION)
- Si se crea o elimina la sesión de DS-Lite
- Dirección IPv6 de B4
- Dirección IP, puerto e ID de dominio de tráfico del suscriptor
- Dirección IP NAT y puerto
- Nombre del protocolo
- Dirección IP de destino, puerto e ID de dominio de tráfico

En la tabla siguiente se muestran las entradas de registro DS-Lite de ejemplo de cada tipo almacenadas en los servidores de registro configurados. Estas entradas de registro las genera un dispositivo Citrix ADC cuya dirección NSIP es 10.102.37.115.Puede registrar información de DS-Lite para diagnosticar o solucionar problemas y cumplir los requisitos legales. El dispositivo Citrix ADC admite todas las funciones de registro LSN para registrar información de DS-Lite. Para configurar el registro de DS-Lite, utilice los procedimientos para configurar el registro LSN, descritos en Registro y supervisión de LSN.

Un mensaje de registro para una entrada de asignación de LSN de DS-Lite consta de la siguiente información:

- Dirección IP propiedad de Citrix ADC (dirección NSIP o dirección SNIP) desde la que se origina el mensaje de registro
- Marca de tiempo
- Tipo de entrada (MAPPING)
- Si se ha creado o eliminado la entrada de asignación LSN de DS-Lite
- Dirección IPv6 de B4
- Dirección IP, puerto e ID de dominio de tráfico del suscriptor
- Dirección IP NAT y puerto
- Nombre del protocolo
- La dirección IP de destino, el puerto y el ID de dominio de tráfico pueden estar presentes, en función de las condiciones siguientes:
  - La dirección IP de destino y el puerto no se registran para la asignación independiente del punto final.
  - Solo se registra la dirección IP de destino para la asignación dependiente de direcciones. El puerto no está registrado.
  - La dirección IP de destino y el puerto se registran para la asignación dependiente del

puerto de dirección.

Un mensaje de registro para una sesión de DS-Lite consta de la siguiente información:

- Dirección IP propiedad de Citrix ADC (dirección NSIP o dirección SNIP) desde la que se origina el mensaje de registro
- Marca de tiempo
- Tipo de entrada (SESSION)
- Si se crea o elimina la sesión de DS-Lite
- Dirección IPv6 de B4
- Dirección IP, puerto e ID de dominio de tráfico del suscriptor
- Dirección IP NAT y puerto
- Nombre del protocolo
- Dirección IP de destino, puerto e ID de dominio de tráfico

En la tabla siguiente se muestran las entradas de registro DS-Lite de ejemplo de cada tipo almacenadas en los servidores de registro configurados. Estas entradas de registro las genera un dispositivo Citrix ADC cuya dirección NSIP es 10.102.37.115.

Tipo de entrada de registro LSN	Entrada de registro de ejemplo
Creación de sesiones de DS-Lite	Local4.Informational 10.102.37.115 08/14/2015:13:35:38 GMT 0-PPE-1: Default LSN LSN_SESSION 37647607 0: SESSION CREATED 2001:DB8::3:4 Client IP:Port:TD 192.0.2.51:2552:0, NatIP:NatPort 203.0.113.61:3002, Destination IP:Port:TD 198.51.100.250:80:0, Protocol:TCP
Eliminación de sesión de DS-Lite	Local4.Informational 10.102.37.115 08/14/2015:13:38:22 GMT 0-PPE-1: Default LSN LSN_SESSION 37647617 0: SESSION DELETED 2001:DB8::3:4 Client IP:Port:TD 192.0.2.51:2552:0, NatIP:NatPort 203.0.113.61:3002, Destination IP:Port:TD 198.51.100.250:80:0, Protocol: TCP

Creación de mapeo LSN de DS-Lite	Local4.Informational 10.102.37.115 08/14/2015:13:35:39 GMT 0-PPE-1: Default LSN LSN_EIM_MAPPING 37647610 0: EIM CREATED 2001:DB8::3:4 Client IP:Port:TD 192.0.2.51:2552:0, NatIP:NatPort 198.51.100.250:80, Protocol: TCP
Eliminación de asignación de LSN de DS-Lite	Local4.Informational 10.102.37.115 08/14/2015:13:38:25 GMT 0-PPE-1: Default LSN LSN_EIM_MAPPING 37647618 0: EIM DELETED 2001:DB8::3:4 Client IP:Port:TD 192.0.2.51:2552:0, NatIP:NatPort 198.51.100.250:80, Protocol: TCP

Visualización de sesiones DS-Lite actuales

Puede mostrar las sesiones DS-Lite actuales para detectar sesiones no deseadas o ineficientes en el dispositivo Citrix ADC. Puede mostrar todas o algunas sesiones de DS-Lite, sobre la base de los parámetros de selección.

Para mostrar todas las sesiones de DS-Lite mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
show lsn session -nattype DS-Lite
<!--NeedCopy-->
```

Para mostrar sesiones DS-Lite seleccionadas mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
show lsn session -nattype DS-Lite [-clientname <string>] [-network <
    ip_addr> [-netmask <netmask>] [-td <positive_integer>]] [-natIP <
    ip_addr> [-natPort <port>]]
<!--NeedCopy-->
```


La salida de ejemplo siguiente muestra todas las sesiones DS-Lite existentes en un dispositivo Citrix ADC:

> show lsn session —nattype DS-Lite

```
1   B4-Address SubscrIP SubscrPort SubscrTD DstIP DstPort DstTD NatIP
       NatPort Proto Dir
2
3  1. 2001:DB8::3:4 192.0.2.51 2552 0 198.51.100.250 80 0 203.0.113.61
      3002 TCP OUT
4
5  2. 2001:DB8::3:4 192.0.2.51 3551 0 198.51.100.300 80 0 203.0.113.61
      52862 TCP OUT
6
7  3. 2001:DB8::3:4 192.0.2.100 4556 0 198.51.100.250 0 0 203.0.113.61
      48116 ICMP OUT
8
9  4. 2001: DB8::190 192.0.2.150 3881 0 198.51.100.199 80 0 203.0.113.69
      48305 TCP OUT
10 Done
11 <!--NeedCopy-->
```

Configuración mediante la utilidad de configuración

Para mostrar todas las sesiones DS-Lite o seleccionadas mediante la utilidad de configuración

1. **Vaya a Sistema** > **NAT a gran escala** > **Sesiones**y haga clic en la ficha **DS-Lite** .
2. Para mostrar sesiones de DS-Lite sobre la base de parámetros de selección, haga clic en **Buscar**.

Borrar sesiones de DS-Lite

Puede eliminar todas las sesiones DS-Lite no deseadas o ineficientes del dispositivo Citrix ADC. El dispositivo libera inmediatamente los recursos (como la dirección IP de NAT, el puerto y la memoria) asignados para estas sesiones, lo que hace que los recursos estén disponibles para las sesiones nuevas. El dispositivo también elimina todos los paquetes posteriores relacionados con estas sesiones eliminadas. Puede quitar todas las sesiones DS-Lite o seleccionadas del dispositivo Citrix ADC.

Para borrar todas las sesiones de DS-Lite mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:


```
flush lsn session  -nattype DS-Lite

show lsn session  -nattype DS-Lite
<!--NeedCopy-->
```

Para borrar sesiones DS-Lite seleccionadas mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
flush lsn session  -nattype DS-Lite [-clientname <string>] [-network <
   ip_addr> [-netmask <netmask>] [-td <positive_integer>]] [-natIP <
   ip_addr> [-natPort <port>]]

show lsn session  -nattype DS-Lite
<!--NeedCopy-->
```

Para borrar todas o seleccionadas sesiones de DS-Lite mediante la utilidad de configuración

1. Vaya a **Sistema** > **NAT a gran escala** > **Sesiones**y haga clic en la ficha **DS-Lite**.
2. Haga clic en **Vaciar sesiones**.

Registro de información de encabezado HTTP

El dispositivo Citrix ADC puede registrar la información de encabezado de solicitud de una conexión HTTP que utiliza la funcionalidad DS-Lite. Se puede registrar la siguiente información de encabezado de un paquete de solicitud HTTP:

- URL a la que está destinada la solicitud HTTP
- Método HTTP especificado en la solicitud HTTP
- Versión HTTP utilizada en la solicitud HTTP
- Dirección IPv4 del suscriptor que envió la solicitud HTTP

Los registros de encabezado HTTP pueden ser utilizados por los ISP para ver las tendencias relacionadas con el protocolo HTTP entre un conjunto de suscriptores. Por ejemplo, un ISP puede utilizar esta función para averiguar el sitio web más popular entre un conjunto de suscriptores.

Pasos de configuración

Realice las siguientes tareas para configurar el dispositivo Citrix ADC para registrar la información de encabezado HTTP:

- **Cree un perfil de registro de encabezado HTTP**. Un perfil de registro de encabezado HTTP es una colección de atributos de encabezado HTTP (por ejemplo, URL y método HTTP) que se pueden habilitar o inhabilitar para el registro.
- **Enlazar el encabezado HTTP a un grupo LSN de una configuración de DS-Lite LSN**. Enlace el perfil de registro de encabezado HTTP a un grupo LSN de una configuración LSN estableciendo el parámetro de nombre de perfil de registro de encabezado HTTP en el nombre del perfil de registro de encabezado HTTP creado. A continuación, el dispositivo Citrix ADC registra la información de encabezado HTTP de cualquier solicitud HTTP relacionada con el grupo LSN. Un perfil de registro de encabezado HTTP se puede enlazar a varios grupos LSN, pero un grupo LSN solo puede tener un perfil de registro de encabezado HTTP.

Para crear un perfil de registro de encabezado HTTP mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
add lsn httphdrlogprofile <httphdrlogprofilename> [-logURL ( ENABLED |
    DISABLED )] [-logMethod ( ENABLED | DISABLED )] [-logVersion (
    ENABLED | DISABLED )] [-logHost ( ENABLED | DISABLED )]

show lsn httphdrlogprofile
<!--NeedCopy-->
```

Para enlazar un perfil de registro de encabezado HTTP a un grupo LSN mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
bind lsn group <groupname> -httphdrlogprofilename <string>

show lsn group <groupname>
<!--NeedCopy-->
```

Configuración de ejemplo

En la siguiente configuración de LSN de DS-Lite, el perfil de registro de encabezado HTTP HTTP-header-log-1 está enlazado al grupo LSN LSN-DSLITE-GROUP-1. El perfil de registro tiene todos los atributos HTTP (URL, método HTTP, versión HTTP y dirección IP HOST) habilitados para el registro,

de modo que todos estos atributos se registran para cualquier solicitud HTTP desde dispositivos B4 (en la red 2001:DB 8:5001: :/96).

Configuración de ejemplo:

```
add lsn httphdrlogprofile HTTP-HEADER-LOG-1

Done

add lsn client LSN-DSLITE-CLIENT-1

Done

bind lsn client LSN-DSLITE-CLIENT-1 -network6 2001:DB8::3:0/100

Done

add lsn pool LSN-DSLITE-POOL-1

Done

bind lsn pool LSN-DSLITE-POOL-1 203.0.113.61 - 203.0.113.70

Done

add lsn ip6profile LSN-DSLITE-PROFILE-1 -type DS-Lite -network6 2001:
   DB8::5:6

Done

add lsn group LSN-DSLITE-GROUP-1 -clientname LSN-DSLITE-CLIENT-1 -
   portblocksize 1024 -ip6profile LSN-DSLITE-PROFILE-1

Done

bind lsn group LSN-DSLITE-GROUP-1 -poolname LSN-DSLITE-POOL-1

Done

bind lsn group LSN-DSLITE-GROUP-1 -httphdrlogprofilename HTTP-HEADER-
   LOG-1

Done
<!--NeedCopy-->
```


Registro de IPFIX

El dispositivo Citrix ADC admite el envío de información sobre eventos LSN en formato de exportación de información de flujo de protocolo Internet (IPFIX) al conjunto configurado de recopiladores IPFIX. El dispositivo utiliza la función AppFlow existente para enviar eventos LSN en formato IPFIX a los recopiladores IPFIX.

El registro basado en IPFIX está disponible para los siguientes eventos relacionados con DS_Lite:

- Creación o eliminación de una sesión LSN.
- Creación o eliminación de una entrada de asignación LSN.
- Asignación o desasignación de bloques de puertos en el contexto de NAT determinista.
- Asignación o desasignación de bloques de puertos en el contexto de NAT dinámico.
- Siempre que se supere la cuota de sesión de suscriptor.

Puntos a tener en cuenta antes de configurar el registro IPFIX

Antes de comenzar a configurar IPSec ALG, tenga en cuenta los siguientes puntos:

- Debe configurar la función AppFlow y los recopiladores IPFIX en el dispositivo Citrix ADC. Para obtener instrucciones, consulte Configuración de la función AppFlow.

Pasos de configuración

Realice las siguientes tareas para registrar la información LSN en formato IPFIX:

- **Habilite el registro LSN en la configuración de AppFlow**. Habilite el parámetro de registro LSN como parte de la configuración de AppFlow.
- **Cree un perfil de registro LSN**. Un perfil de registro LSN incluye el parámetro IPFIX que habilita o inhabilita la información de registro en formato IPFIX.
- **Enlazar el perfil de registro de LSN a un grupo LSN de una configuración LSN**. Enlace el perfil de registro LSN a uno o varios grupos LSN. Los eventos relacionados con el grupo LSN enlazado se registrarán en formato IPFIX.

Para habilitar el registro LSN en la configuración de AppFlow mediante la CLI

En el símbolo del sistema, escriba:

```
1 set appflow param -lsnLogging (ENABLED |DISABLED )
2
3 show appflow param
4 <!--NeedCopy-->
```


Para crear un perfil de registro LSN mediante el comando CliAt el símbolo del sistema, escriba

En el símbolo del sistema, escriba:

```
set lsn logprofile <logProfileName>  -logipfix ( ENABLED | DISABLED )

show lsn logprofile
<!--NeedCopy-->
```

Para enlazar el perfil de registro LSN a un grupo LSN de una configuración de LSN mediante la CLI

En el símbolo del sistema, escriba:

```
bind lsn group <groupname>  -logProfileName <lsnlogprofilename>

show lsn group
<!--NeedCopy-->
```

Para crear un perfil de registro LSN mediante la interfaz gráfica de usuario

Vaya a **Sistema** > **NAT a gran escala** > **Perfiles**, haga clic en la ficha **Registro** y, a continuación, agregue un perfil de registro.

Para enlazar el perfil de registro LSN a un grupo LSN de una configuración LSN mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **NAT a gran escala** > **Grupo LSN,** abra el grupo **LSN** .
2. En **Configuración avanzada,** haga clic en **+ Perfil de registro** para enlazar el perfil de registro creado al grupo LSN.

Protocolo de control de puertos para DS-Lite

January 12, 2021

Los dispositivos Citrix ADC ahora admiten Port Control Protocol (PCP) para NAT (LSN) a gran escala. Muchas de las aplicaciones de suscriptor de un ISP deben ser accesibles desde Internet (por ejemplo, dispositivos de Internet de las cosas (IOT), como una cámara IP que proporciona vigilancia a través

de Internet). Una forma de cumplir este requisito es crear mapas estáticos de NAT (LSN) a gran escala. Pero para una gran cantidad de suscriptores, crear mapas NAT LSN estáticos no es una solución factible.

Port Control Protocol (PCP) permite a un suscriptor solicitar asignaciones NAT LSN específicas para sí mismo y/o para otros dispositivos de terceros. El dispositivo NAT a gran escala crea un mapa LSN y lo envía al suscriptor. El suscriptor envía a los dispositivos remotos en Internet la dirección IP NAT: Puerto NAT en el que pueden conectarse al suscriptor.

Las aplicaciones suelen enviar mensajes de mantenimiento activo frecuentes al dispositivo NAT a gran escala para que sus asignaciones LSN no agoten el tiempo de espera. PCP ayuda a reducir la frecuencia de dichos mensajes keep-alive al permitir que las aplicaciones aprendan la configuración de tiempo de espera de las asignaciones LSN. Esto ayuda a reducir el consumo de ancho de banda en la red de acceso del ISP y el consumo de batería en dispositivos móviles.

PCP es un modelo cliente-servidor y se ejecuta sobre el protocolo de transporte UDP. Un dispositivo Citrix ADC implementa el componente del servidor PCP y cumple con RFC 6887.

Pasos de configuración

Realice las siguientes tareas para configurar PCP:

- (Opcional) Cree un perfil de PCP. Un perfil PCP incluye configuraciones para parámetros relacionados con PCP (por ejemplo, para escuchar solicitudes PCP de mapeo y de pares). Un perfil PCP se puede enlazar a un servidor PCP. Un perfil PCP enlazado a un servidor PCP aplica toda su configuración al servidor PCP. Un perfil PCP puede enlazarse a varios servidores PCP. De forma predeterminada, un perfil PCP con parámetros predeterminados está enlazado a todos los servidores PCP. Un perfil PCP que se vincula a un servidor PCP anula la configuración predeterminada del perfil PCP para ese servidor. Un perfil PCP predeterminado tiene los siguientes parámetros:
  - Asignación: Activada
  - Peer: Activado
  - Vida útil mínima del mapa: 120 segundos
  - Vida máxima máxima: 86400 segundos.
  - Número de anunciaciones: 10
  - Terceros: Inhabilitado
- Cree un servidor PCP y vincule un perfil PCP a él. Cree un servidor PCP en el dispositivo Citrix ADC para escuchar solicitudes y mensajes relacionados con PCP de los suscriptores. Se debe asignar una dirección IP de subred (SNIP) a un servidor PCP para tener acceso a ella. De forma predeterminada, un servidor PCP escucha en el puerto 5351.
- Enlace el servidor PCP a un grupo LSN de una configuración LSN. Vincular el servidor PCP creado a un grupo LSN de una configuración LSN estableciendo el parámetro PCP Server para

especificar el servidor PCP creado. Solo los suscriptores de este grupo LSN pueden acceder al servidor PCP creado.

Nota: Un servidor PCP para una configuración NAT a gran escala no atiende solicitudes de suscriptores identificados a partir de reglas de ACL.

Para crear un perfil PCP mediante la CLI

En el símbolo del sistema, escriba:

```
add pcp profile <name> [-mapping ( ENABLED | DISABLED )] [-peer (
    ENABLED | DISABLED )] [-minMapLife <secs>]  [-maxMapLife <secs>] [-
    announceMultiCount <positive_integer>][-thirdParty ( ENABLED |
    DISABLED )]

show pcp profile <name>
<!--NeedCopy-->
```

Para crear un servidor PCP mediante la CLI

En el símbolo del sistema, escriba:

```
add pcp server <name> <IPAddress> [-port <portNum|*>] [-pcpProfile <
    string>]

show pcp server <name>
<!--NeedCopy-->
```

Configuración de ejemplo para DS-LITE

En la siguiente configuración de ejemplo, el servidor PCP PCP-SERVER-1, con la configuración PCP de PCP-DSLITE-PROFILE-1, está enlazado al grupo LSN LSN-DSLITE-GROUP-1. PCP-SERVER-9 atiende solicitudes PCP de suscriptores IPv4 detrás de dispositivos B4 de la red 2001:DB8:: 3:0/100.

Configuración de ejemplo:

```
add pcp profile PCP-DSLITE-PROFILE-1 -minMapLife 300
Done
add pcp server PCP-DSLITE-SERVER-1 192.0.3.10  -pcpProfile PCP-DSLITE-
    PROFILE-1
```



```
4  Done
5  add lsn client LSN-DSLITE-CLIENT-1
6  Done
7  bind lsn client LSN-DSLITE-CLIENT-1 -network6 2001:DB8::3:0/100
8  Done
9  add lsn pool LSN-DSLITE-POOL-1
10 Done
11 bind lsn pool LSN-DSLITE-POOL-1 203.0.113.61 - 203.0.113.70
12 Done
13 add lsn ip6profile LSN-DSLITE-PROFILE-1 -type DS-Lite -network6 2001:
      DB8::5:6
14 Done
15 add lsn group LSN-DSLITE-PROFILE-1 -clientname LSN-NAT64-CLIENT-1  -
      ip6profile LSN-NAT64-PROFILE-1
16 Done
17 bind lsn group LSN-DSLITE-GROUP-1 -poolname LSN-NAT64-POOL-1
18 Done
19 bind lsn group LSN-DSLITE-GROUP-1 -poolname  PCP-NAT64-SERVER-1
20 Done
21 <!--NeedCopy-->
```

Gran escala NAT64

August 20, 2021

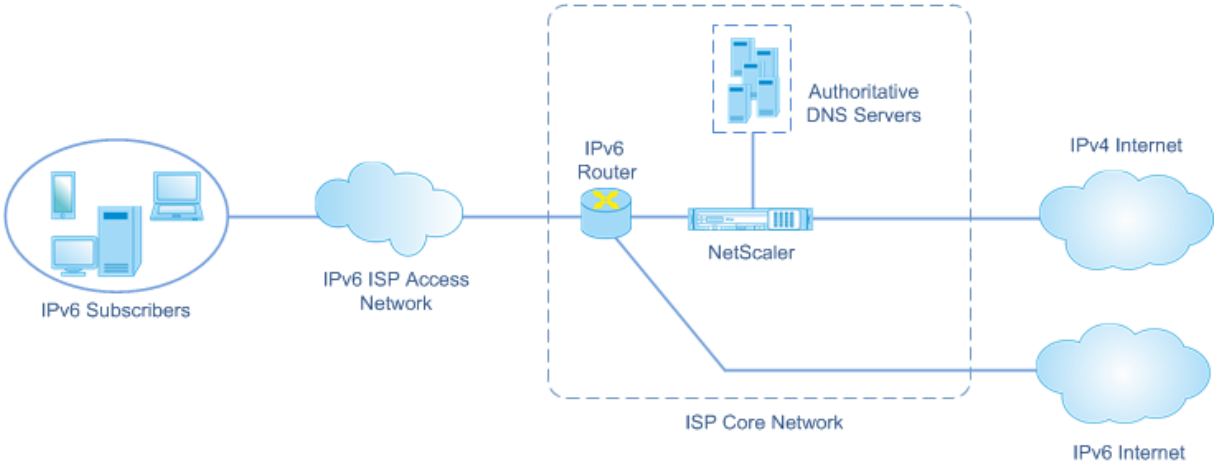
Debido al agotamiento inminente de las direcciones IPv4, los ISP han comenzado a realizar la transición a la infraestructura IPv6. Sin embargo, durante la transición, los ISP deben seguir soportando IPv4 junto con IPv6, porque la mayor parte de Internet público todavía utiliza IPv4. NAT64 a gran escala es una solución de transición IPv6 para ISP con infraestructura IPv6 para conectar a sus suscriptores solo IPv6 a Internet IPv4. DNS64 es una solución para permitir la detección de dominios solo IPv4 por parte de clientes solo IPv6. DNS64 se utiliza con NAT64 a gran escala para permitir una comunicación perfecta entre los clientes solo IPv6 y los servidores solo IPv4.

Un dispositivo Citrix ADC implementa NAT64 y DNS64 a gran escala y cumple con los RFC 6145, 6146, 6147, 6052, 3022, 2373, 2765 y 2464.

Arquitectura

La arquitectura NAT64 de un ISP que utiliza un dispositivo Citrix ADC consiste en suscriptores IPv6 que acceden a Internet IPv4 a través de un dispositivo Citrix ADC implementado en la red principal del ISP.

Los suscriptores IPv6 están conectados a la red principal del ISP a través de la red de acceso solo IPv6 del ISP.



La funcionalidad NAT64 a gran escala de un dispositivo Citrix ADC permite la comunicación entre los clientes IPv6 y los servidores IPv4 a través de la traducción de paquetes IPv6 a IPv4, y viceversa, mientras mantiene la información de sesión en el dispositivo Citrix ADC. La funcionalidad Citrix ADC DNS64 representa dominios solo IPv4 a IPv6. mediante la síntesis de registros DNS AAAA para dominios solo IPv4 y el envío a los suscriptores.

NAT64 a gran escala tiene dos componentes principales: Prefijo NAT64 y grupo NAT IPv4. DNS64 tiene un componente principal, el prefijo DNS64, que tiene el mismo valor que el prefijo NAT64.

Al recibir una solicitud AAAA de un suscriptor solo IPv6 para un nombre de dominio alojado en un servidor web solo IPv4 en Internet, la funcionalidad Citrix ADC DNS64 sintetiza un registro AAAA para el nombre de dominio y lo envía al suscriptor. El registro AAAA se sintetiza concatenando el prefijo DNS64 (que se establece en el prefijo NAT64) y la dirección IPv4 real del nombre de dominio.

El suscriptor ahora tiene una dirección de destino IPv6 que corresponde al nombre de dominio deseado. El suscriptor envía la solicitud a la dirección IPv6 sintetizada. Al recibir la solicitud IPv6, la funcionalidad de Citrix ADC NAT64 a gran escala traduce el paquete de solicitud IPv6 en un paquete de solicitud IPv4. NAT64 a gran escala establece la dirección de destino de la solicitud IPv4 en la dirección IPv4, que se extrae de la dirección de destino de la solicitud IPv6 mediante la eliminación del prefijo NAT64 de la dirección IPv6. El puerto de destino se conserva de la solicitud IPv6. NAT64 de gran escala también establece la dirección IP de origen:puerto de origen del paquete IPv4 en la dirección IP NAT:puerto NAT seleccionado del grupo NAT configurado.

El dispositivo mantiene un registro de todas las sesiones activas que utilizan la funcionalidad NAT64 a gran escala. Estas sesiones se llaman sesiones NAT64 a gran escala. El dispositivo también mantiene las asignaciones entre la dirección IPv6 del suscriptor y el puerto, y la dirección y el puerto NAT IPv4, para cada sesión NAT64 a gran escala. Estas asignaciones se denominan asignaciones NAT64 a gran escala. Desde entradas de sesión NAT64 a gran escala y entradas de asignación NAT64 a gran escala, el dispositivo Citrix ADC reconoce que un paquete de respuesta (recibido de Internet) pertenece a una

sesión NAT64 concreta.

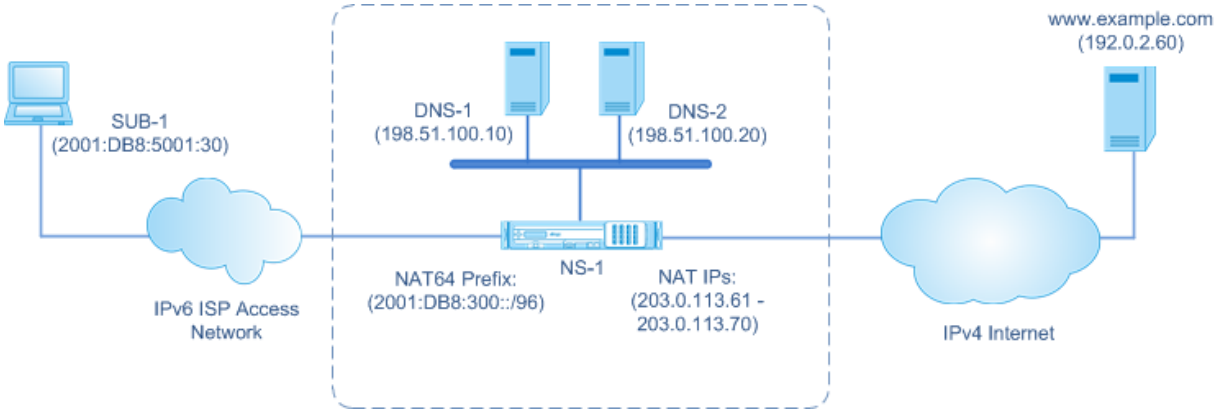
Cuando el dispositivo recibe un paquete de respuesta IPv4 perteneciente a una sesión NAT64 concreta, utiliza la información almacenada en la sesión NAT64 para traducir el paquete IPv4 en un paquete IPv6 y, a continuación, envía el paquete de respuesta IPv6 al suscriptor.

Ejemplo: Flujo de tráfico de implementación NAT64 y DNS64

Considere un ejemplo de implementación NAT64 y DNS64 a gran escala que consiste en el dispositivo Citrix ADC NS-1 y dos servidores DNS locales, DNS-1 y DNS-2, en la red principal de un ISP y suscriptor IPv6 SUB-1. SUB-1 está conectado a NS-1 a través de la red de acceso IPv6 del ISP. NS-1 incluye configuraciones NAT64 y DNS64 a gran escala para habilitar la comunicación entre el suscriptor IPv6 SUB-1 y los hosts IPv4 (internos y externos).

La configuración NAT64 a gran escala incluye un prefijo NAT64 (2001:DB 8:300: :/96) y un grupo NAT IPv4 para la traducción de solicitudes IPv6 a solicitudes IPv4 y respuestas IPv4 a respuestas IPv6.

La configuración de DNS64 incluye un servidor virtual de equilibrio de carga DNS LBVS-DNS64-1 (2001:DB 8:9999: :99) y un prefijo DNS64 (2001:DB 8:300: :/96). LBVS-DNS64-1 representa el servidor DNS local DNS-1 y DNS-2 a los suscriptores del ISP. El prefijo DNS64, que tiene el mismo valor que el prefijo NAT64, se utiliza para sintetizar registros DNS AAAA a partir de registros DNS A recibidos de servidores DNS DNS-1 y DNS-2. NS-1 responde con un registro AAAA sintetizado a SUB-1 para una solicitud DNS para resolver un host IPv4.



Flujo de tráfico DNS64

Fluye el tráfico entre el suscriptor IPv6 SUB-1 y el sitio `www.example.com`, que reside en un servidor web solo IPv4 en Internet, de la siguiente manera:

1. El suscriptor IPv6 SUB-1 envía una solicitud AAAA DNS para `www.example.com` a su servidor DNS designado (2001:DB 8:9999: :99).

2. El servidor virtual de equilibrio de carga DNS LBVS-DNS64-1 (2001:DB 8:9999: :99) en el dispositivo Citrix ADC NS1 recibe la solicitud AAAA. El algoritmo de equilibrio de carga de LBVS-DNS64-1 selecciona el servidor DNS DNS-1 y reenvía la solicitud AAAA a él.
3. DNS-1 devuelve un registro vacío o un mensaje de error, porque no hay ningún registro AAAA disponible para `www.example.com`.
4. Dado que la opción DNS64 está habilitada en LBVS-DNS64-1 y la solicitud AAAA de CL1 coincide con la condición especificada en DNS64-Directiva-1, NS1 envía una solicitud DNS A a DNS-1 para la dirección IPv4 de `www.example.com`.
5. DNS-1 responde con el registro A de 192.0.2.60 para `www.example.com`.
6. El módulo DNS64 en NS1 sintetiza un registro AAAA para `www.example.com` encadenar el prefijo DNS64 (2001:DB 8:300: :/96) asociado a LBVS-DNS64-1, y la dirección IPv4 (192.0.2.60) para `www.example.com` = 2001:DB 8:300: :192.0.2.60
7. NS1 envía el registro AAAA sintetizado al cliente IPv6 CL1. NS1 también almacena en caché el registro A en su memoria. NS1 utiliza el registro A almacenado en caché para sintetizar registros AAAA para solicitudes AAAA posteriores.

Flujo de tráfico NAT64

1. El suscriptor IPv6 SUB-1 envía una solicitud a 2001:DB8:5001:30 `www.example.com`. El paquete IPv6 tiene:
   - Dirección IP de origen = 2001:DB 8:5001:30
   - Puerto de origen = 2552
   - Dirección IP de destino = 2001:DB 8:300: :192.0.2.60
   - Puerto de destino = 80
2. El suscriptor IPv6 SUB-1 envía una solicitud a 2001:DB8:5001:30 `www.example.com`. El paquete IPv6 tiene:
   - Dirección IP de origen = 2001:DB 8:5001:30
   - Puerto de origen = 2552
   - Dirección IP de destino = 2001:DB 8:300: :192.0.2.60
   - Puerto de destino = 80
3. Cuando NS-1 recibe el paquete IPv6, el módulo NAT64 a gran escala crea un paquete de solicitud IPv4 traducido con:
   - Dirección IP de origen = Una de las direcciones IPv4 disponibles en el grupo NAT configurado (203.0.113.61)
   - Puerto de origen = Uno de los puertos disponibles con la dirección NAT IPv4 asignada (3002)
   - Dirección IP de destino = dirección IPv4 extraída de la dirección de destino de la solicitud IPv6 mediante la eliminación del prefijo NAT64 (2001:DB 8:300: :/96) de la dirección IPv6

(192.0.2.60)
- Puerto de destino = puerto de destino de la solicitud IPv6 (80)

4. El módulo NAT64 a gran escala también crea entradas de asignación y sesión para este flujo NAT64 a gran escala. Las entradas de sesión y asignación incluyen la siguiente información:
   - Dirección IP de origen del paquete IPv6 = 2001:DB 8:5001:30
   - Puerto de origen del paquete IPv6 = 2552
   - Dirección IP NAT = 203.0.113.61
   - Puerto NAT = 3002
   - NS-1 envía el paquete IPv4 resultante a su destino en Internet.
5. Al recibir el paquete de solicitud, el servidor de `www.example.com` procesa el paquete y envía un paquete de respuesta a NS-1. El paquete de respuesta IPv4 tiene:
   - Dirección IP de la fuente = 192.0.2.60
   - Puerto de origen = 80
   - Dirección IP de destino = 203.0.113.61
   - Puerto de destino = 3002
6. Al recibir el paquete de respuesta IPv4, NS-1 examina la asignación NAT64 a gran escala y las entradas de sesión y descubre que el paquete de respuesta IPv4 pertenece a una sesión NAT64 a gran escala. El módulo NAT64 a gran escala crea un paquete de respuesta IPv6 traducido:
   - Dirección IP de origen = 2001:DB 8:300: :192.0.2.60
   - Puerto de origen = 80
   - Dirección IP de destino = 2001:DB 8:5001:30
   - Puerto de destino = 2552
7. NS-1 envía la respuesta IPv6 traducida al cliente SUB-1.

Funciones NAT64 de gran escala compatibles con dispositivos Citrix ADC

NAT64 a gran escala en un dispositivo Citrix ADC admite el conjunto de funciones LSN estándar. Para obtener más información sobre estas funciones de LSN, consulte Arquitectura LSN.

A continuación se presentan algunas de las funciones NAT64 a gran escala compatibles con los dispositivos Citrix ADC:

- ALG. Soporte de aplicación Layer Gateway (ALG) para protocolos SIP, RTSP, FTP, ICMP y TFTP.
- NAT determinista/Fijo. Soporte para preasignación de bloques de puertos a suscriptores para minimizar el registro.
- Mapeo. Compatibilidad con la asignación independiente del punto final (EIM), la asignación dependiente de direcciones (ADM) y la asignación dependiente del puerto de direcciones (APDM).
- Filtrado. Compatibilidad con el filtrado independiente del punto final (EIF), el filtrado dependiente de direcciones (ADF) y el filtrado dependiente del puerto de direcciones (APDF).

- Cuotas. Límites configurables en el número de puertos, sesiones por suscriptor y sesiones por grupo LSN.
- Asignación estática. Soporte para definir manualmente una asignación NAT64 a gran escala.
- Flujo de horquilla. Soporte para la comunicación entre suscriptores o hosts internos mediante direcciones IP NAT.
- 464XLAT conexiones. Compatibilidad con la comunicación entre aplicaciones solo IPv4 en hosts de suscriptor IPv6 y hosts IPv4 en Internet a través de una red IPv6.
- Prefijos NAT64 y DNS64 de longitud variable. El dispositivo Citrix ADC admite la definición de prefijos NAT64 y DNS64 de longitudes de 32, 40, 48, 56, 64 y 96.
- Múltiples prefijos NAT64 y DNS64. El dispositivo Citrix ADC admite varios prefijos NAT64 y DNS64.
- Clientes LSN. Soporte para especificar o identificar suscriptores para NAT64 a gran escala mediante prefijos IPv6 y reglas ACL6 ampliadas.
- Registro. Soporte para el registro de sesiones NAT64 para la aplicación de la ley. Además, los siguientes también son compatibles para el registro.
  - **SYSLOG fiable**. Soporte para enviar mensajes SYSLOG a través de TCP a servidores de registro externos para un mecanismo de transporte más confiable.
  - **Equilibrio de carga de servidores de registro**. Compatibilidad con el equilibrio de carga de servidores de registro externos para evitar el almacenamiento de mensajes de registro redundantes.
  - **Registro mínimo**. Las configuraciones deterministas LSN o las configuraciones dinámicas LSN con bloque de puertos reducen significativamente el volumen de registro NAT64 a gran escala.
  - **Registro de información MSISDN**. Soporte para incluir información MSISDN de los suscriptores en registros NAT64 a gran escala para identificar y rastrear la actividad del suscriptor a través de Internet.

Puntos a considerar para configurar NAT64 a gran escala

January 12, 2021

Antes de comenzar a configurar NAT64 y DNS64 a gran escala, tenga en cuenta estos puntos:

1. Asegúrese de comprender los diferentes componentes de NAT64 a gran escala, descritos en RFC.
2. El dispositivo Citrix ADC admite solo los siguientes ALG para NAT64 de gran escala:
   - FTP
   - TFTP
   - ICMP

- SIP
- RTSP

3. En una configuración de alta disponibilidad de dos dispositivos Citrix ADC, no se admite la sincronización de sesión NAT64 grande (duplicación de conexiones).

Configuración de DNS64

January 19, 2021

La creación de las entidades necesarias para la configuración NAT64 con estado en el dispositivo Citrix ADC implica los siguientes procedimientos:

- Agregar servicios DNS. Los servicios DNS son representaciones lógicas de servidores DNS para los que el dispositivo Citrix ADC actúa como servidor proxy DNS. Para obtener más información sobre la configuración de parámetros opcionales de un servicio, consulte Equilibrio de carga.
- Agregue la acción DNS64 y la directiva DNS64 y, a continuación, vincule la acción DNS64 a la directiva DNS64. Una directiva DNS64 especifica las condiciones que deben coincidir con el tráfico para el procesamiento DNS64 de acuerdo con la configuración de la acción DNS64 asociada. La acción DNS64 especifica el prefijo DNS64 obligatorio y la configuración opcional de reglas de exclusión y reglas mapped-rule.
- Cree un servidor virtual de equilibrio de carga DNS y vincule los servicios DNS y la directiva DNS64 a él. El servidor virtual de equilibrio de carga DNS actúa como un servidor proxy DNS para los servidores DNS representados por los servicios DNS enlazados. El tráfico que llega al servidor virtual coincide con la directiva DNS64 vinculada para el procesamiento DNS64. Para obtener más información sobre la configuración de parámetros opcionales de un servidor virtual de equilibrio de carga, consulte Equilibrio de carga.

> **Nota**
>
> La interfaz de línea de comandos tiene comandos separados para estas dos tareas, pero la GUI los combina en un solo cuadro de diálogo.

- Habilitar el almacenamiento en caché de registros DNS. Habilite el parámetro global para el dispositivo Citrix ADC para almacenar en caché los registros DNS, que se obtienen mediante operaciones de proxy DNS. Para obtener más información sobre cómo habilitar el almacenamiento en caché de registros DNS, consulte Habilitación del almacenamiento en caché de registros DNS.

Para crear un servicio de tipo DNS mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:


```
add service <name> <IP> <serviceType> <port> …
<!--NeedCopy-->
```

Para crear una acción DNS64 mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
add dns action64 <actionName> -Prefix <ipv6_addr|*> [-mappedRule <
    expression>] [-excludeRule <expression>]
<!--NeedCopy-->
```

Para crear una directiva DNS64 mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
add dns policy64 <name> -rule <expression> -action <string>
<!--NeedCopy-->
```

Para crear un servidor virtual de equilibrio de carga DNS mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
add lb vserver <name> DNS <IPAddress> <port> -dns64 (ENABLED | DISABLED
    ) [-bypassAAAA ( YES | NO)] …
<!--NeedCopy-->
```

Para enlazar los servicios DNS y la directiva DNS64 al servidor virtual de equilibrio de carga DNS mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
bind lb vserver <name> <serviceName> ...

```



```
3 bind lb vserver <name> -policyName <string> -priority <positive_integer
     > ...
4 <!--NeedCopy-->
```

Configuración de ejemplo:

```
1  add service SVC-DNS-1 203.0.113.50 DNS 53
2  Done
3  add service SVC-DNS-2 203.0.113.60 DNS 53
4  Done
5  add dns Action64 DNS64-Action-1 -Prefix 2001:DB8:300::/96
6  Done
7  add dns Policy64 DNS64-Policy-1 -rule "CLIENT.IPv6.SRC.IN_SUBNET(2001:
      DB8:5001::/64)" -action DNS64-Action-1
8  Done
9  add lb vserver LBVS-DNS64-1 DNS 2001:DB8:9999::99 53 -dns64 ENABLED
10 Done
11 bind lb vserver LBVS-DNS64-1 SVC-DNS-1
12 Done
13 bind lb vserver LBVS-DNS64-1 SVC-DNS-2
14 Done
15 bind lb vserver LBVS-DNS64-1 -policyname DNS64-Policy-1 -priority 2
16 Done
17 <!--NeedCopy-->
```

Configuración de Large Scaler NAT64

August 20, 2021

Una configuración NAT64 a gran escala en un dispositivo Citrix ADC utiliza los conjuntos de comandos LSN. En una configuración NAT64 a gran escala, la entidad cliente LSN especifica la dirección IPv6 o la dirección de red IPv6, o las reglas ACL6, para identificar suscriptores IPv6. Una configuración NAT64 también incluye un perfil IPv6, que especifica un prefijo NAT64.

La configuración de NAT64 en un dispositivo Citrix ADC consta de las siguientes tareas:

- Establezca los parámetros globales de LSN. Los parámetros globales incluyen la cantidad de memoria Citrix ADC reservada para la función LSN y la sincronización de sesiones LSN en una configuración de alta disponibilidad.
- Cree una entidad cliente LSN para identificar el tráfico de suscriptores IPv6. La entidad cliente LSN hace referencia a un conjunto de suscriptores IPv6. La entidad cliente incluye direcciones

IPv6 o prefijos de red IPv6, o reglas ACL6, para identificar el tráfico de estos suscriptores. Un cliente LSN se puede enlazar a un solo grupo LSN. La interfaz de línea de comandos tiene dos comandos para crear una entidad cliente LSN y vincular un suscriptor a la entidad cliente LSN. La GUI combina estas dos operaciones en una sola pantalla.

- Cree un grupo LSN y vincule las direcciones IP NAT a él. Un grupo LSN define un grupo de direcciones IP NAT que utilizará el dispositivo Citrix ADC para realizar NAT64 a gran escala. La interfaz de línea de comandos tiene dos comandos para crear un grupo LSN y vincular direcciones IP NAT al grupo LSN. La GUI combina estas dos operaciones en una sola pantalla.
- Cree un perfil LSN IP6. Un perfil LSN IP6 define el prefijo NAT64 para una configuración NAT64 a gran escala.
- (Opcional) Cree un perfil de transporte LSN para un protocolo especificado. Un perfil de transporte LSN define varios tiempos de espera y límites, como sesiones NAT64 máximas a gran escala y el uso máximo de puertos que un suscriptor puede tener para un protocolo determinado. Enlazar un perfil de transporte LSN para cada protocolo (TCP, UDP e ICMP) a un grupo LSN. Un perfil se puede enlazar a varios grupos LSN. Un perfil enlazado a un grupo LSN se aplica a todos los suscriptores de un cliente LSN vinculado al mismo grupo. De forma predeterminada, un perfil de transporte LSN con la configuración predeterminada para los protocolos TCP, UDP e ICMP está enlazado a un grupo LSN durante su creación. Este perfil se denomina perfil de transporte predeterminado. Un perfil de transporte LSN que se vincula a un grupo LSN anula el perfil de transporte LSN predeterminado para ese protocolo.
- (Opcional) Cree un perfil de aplicación LSN para un protocolo especificado y enlazar un conjunto de puertos de destino a él. Un perfil de aplicación LSN define la asignación LSN y los controles de filtrado LSN de un grupo para un protocolo determinado y para un conjunto de puertos de destino. Para un conjunto de puertos de destino, se vincula un perfil LSN para cada protocolo (TCP, UDP e ICMP) a un grupo LSN. Un perfil se puede enlazar a varios grupos LSN. Un perfil de aplicación LSN vinculado a un grupo LSN se aplica a todos los suscriptores de un cliente LSN vinculado al mismo grupo. De forma predeterminada, un perfil de aplicación LSN con configuración predeterminada para los protocolos TCP, UDP e ICMP para todos los puertos de destino está enlazado a un grupo LSN durante su creación. Este perfil se denomina perfil de aplicación predeterminado. Cuando vincula un perfil de aplicación LSN, con un conjunto especificado de puertos de destino, a un grupo LSN, el perfil enlazado reemplaza el perfil de aplicación LSN predeterminado para ese protocolo en ese conjunto de puertos de destino. La interfaz de línea de comandos tiene dos comandos para crear un perfil de aplicación LSN y vincular un conjunto de puertos de destino al perfil de aplicación LSN. La GUI combina estas dos operaciones en una sola pantalla.
- Cree un grupo LSN y vincule grupos LSN, perfil LSN IPv6, perfiles de transporte LSN (opcionales) y perfiles de aplicación LSN (opcionales) al grupo LSN. Un grupo LSN es una entidad formada por un cliente LSN, un perfil IPv6 LSN, grupos LSN, perfiles de transporte LSN y perfiles de aplicación LSN. A un grupo se le asignan parámetros, como el tamaño de bloque de puertos y el

registro de sesiones LSN. La configuración de parámetros se aplica a todos los suscriptores de un cliente LSN enlazado al grupo LSN. Solo se puede enlazar un perfil IPv6 de LSN a un grupo LSN, y un perfil IPv6 de LSN vinculado a un grupo LSN no puede vincularse a otros grupos LSN. Solo se pueden enlazar grupos LSN y grupos LSN con la misma configuración de tipo NAT. Los grupos LSN múltiples se pueden enlazar a un grupo LSN. Solo una entidad cliente LSN puede vincularse a un grupo LSN, y una entidad cliente LSN vinculada a un grupo LSN no puede vincularse a otros grupos LSN. La interfaz de línea de comandos tiene dos comandos para crear un grupo LSN y vincular grupos LSN, perfiles de transporte LSN y perfiles de aplicación LSN al grupo LSN. La GUI combina estas dos operaciones en una sola pantalla.

Configuración mediante la línea de comandos

Puede crear diferentes configuraciones mediante la interfaz de línea de comandos. Siga los pasos que se indican a continuación.

Para crear un cliente LSN mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
add lsn client <clientname

show lsn client
<!--NeedCopy-->
```

Para enlazar una red IPv6 o una regla ACL6 a un cliente LSN mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
bind lsn client <clientname> (-network6 <ipv6_addr|*>| -acl6name <
   string>)

show lsn client
<!--NeedCopy-->
```

Para crear un grupo LAN mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:


```
add lsn pool <poolname>

show lsn pool <poolname>
<!--NeedCopy-->
```

Para enlazar direcciones IP NAT a un grupo LSN mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
bind lsn pool <poolname> <lsnip>

show lsn pool
<!--NeedCopy-->
```

> **Nota**
>
> Para eliminar direcciones IP NAT (direcciones IP LSN) de un grupo LSN, utilice el comando unbind lsn pool.

Para configurar un perfil IPv6 de LSN mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
add lsn ip6profile <name>  -type NAT64 -natprefix <ipv6_addr|*>

show lsn ip6profile
<!--NeedCopy-->
```

Para crear un perfil de transporte LSN mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
add lsn transportprofile <transportprofilename> <transportprotocol> [-
    sessiontimeout <secs>] [-finrsttimeout <secs>] [-portquota <
    positive_integer>] [-sessionquota <positive_integer>] [-
    portpreserveparity ( ENABLED | DISABLED )] [-portpreserverange (
    ENABLED | DISABLED )] [-syncheck ( ENABLED | DISABLED )]
```



```
2
3 show lsn transportprofile
4 <!--NeedCopy-->
```

Para crear un perfil de aplicación LSN mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
1 add lsn appsprofile <appsprofilename> <transportprotocol> [-ippooling (
     PAIRED | RANDOM )] [-mapping <mapping>] [-filtering <filtering>][-
     tcpproxy ( ENABLED | DISABLED )]
2
3 show lsn appsprofile
4 <!--NeedCopy-->
```

Para enlazar un intervalo de puertos de protocolo de aplicación a un perfil de aplicación LSN mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
1 bind lsn appsprofile <appsprofilename> <lsnport>
2
3 show lsn appsprofile
4 <!--NeedCopy-->
```

Para crear un grupo LSN mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
1 add lsn group <groupname> -clientname <string> [-nattype ( DYNAMIC |
     DETERMINISTIC )] [-portblocksize <positive_integer>] [-logging(
     ENABLED | DISABLED )] [-sessionLogging ( ENABLED | DISABLED )][-
     sessionSync ( ENABLED | DISABLED )] [-snmptraplimit<positive_integer
     >] [-ftp ( ENABLED | DISABLED )] [-sipalg ( ENABLED | DISABLED )] [-
     rtspalg ( ENABLED |DISABLED )] [-ip6profile <string>]
2
3 show lsn group
4 <!--NeedCopy-->
```


Para enlazar perfiles de protocolo LSN y grupos LSN a un grupo LSN mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
bind lsn group <groupname> (-poolname <string> | -transportprofilename
    <string> | -httphdrlogprofilename <string> | -appsprofilename <
    string> | -sipalgprofilename <string> | rtspalgprofilename <string>)

show lsn group
<!--NeedCopy-->
```

Ejemplo de configuraciones NAT64 a gran escala

Aquí hay algunas configuraciones de ejemplo de NAT64 a gran escala:

Configuración simple de NAT64 a gran escala con ajustes predeterminados:

```
add lsn client LSN-NAT64-CLIENT-1

bind lsn client LSN-NAT64-CLIENT-1 -network6 2001:DB8:5001::/96

add lsn pool LSN-NAT64-POOL-1

bind lsn pool LSN-NAT64-POOL-1 203.0.113.61 - 203.0.113.70

add lsn ip6profile LSN-NAT64-PROFILE-1 -type NAT64 -natprefix 2001:DB8
    :300::/96

add lsn group LSN-NAT64-GROUP-1 -clientname LSN-NAT64-CLIENT-1  -
    ip6profile LSN-NAT64-PROFILE-1

bind lsn group LSN-NAT64-GROUP-1 -poolname LSN-NAT64-POOL-1

<!--NeedCopy-->
```

Configuración NAT64 simple a gran escala con una regla ACL6 extendida para identificar suscriptores:

```
add ns acl6 LSN-NAT64-ACL-2 ALLOW  - srcIPv6 = 2001:DB8:5002::20 - 2001:
    DB8:5002::200
```



```
2
3 apply acl6s
4
5 add lsn client LSN-NAT64-CLIENT-2
6
7 bind lsn client LSN-NAT64-CLIENT-2  -acl6name LSN-NAT64-ACL-2
8
9 add lsn pool LSN-NAT64-POOL-2
10
11 bind lsn pool LSN-NAT64-POOL-2 203.0.113.5-203.0.113.10
12
13 add lsn ip6profile LSN-NAT64-PROFILE-2 -type NAT64 -natprefix 2001:DB8
    :302::/96
14
15 add lsn group LSN-NAT64-GROUP-2 -clientname LSN-NAT64-CLIENT-2 -
    ip6profile LSN-NAT64-PROFILE-2
16
17 bind lsn group LSN-NAT64-GROUP-2 -poolname LSN-NAT64-POOL-2
18
19 <!--NeedCopy-->
```

Configuración NAT64 a gran escala con asignación determinista de recursos NAT:

```
1 add lsn client LSN-NAT64-CLIENT-7
2
3 bind lsn client LSN-NAT64-CLIENT-7 -network6 2001:DB8:1002::7/128
4
5 add lsn pool LSN-NAT64-POOL-7 -nattype DETERMINISTIC
6
7 bind lsn pool LSN-NAT64-POOL-7 203.0.113.24-203.0.113.27
8
9 add lsn ip6profile LSN-NAT64-PROFILE-7 -type NAT64 -natprefix 2001:DB8
    :307::/96
10
11 add lsn group LSN-NAT64-GROUP-7 -clientname LSN-NAT64-CLIENT-7 -
    ip6profile LSN-NAT64-PROFILE-7 -nattype DETERMINISTIC -portblocksize
     256
12
13 bind lsn group LSN-NAT64-GROUP-7 -poolname LSN-POOL-7
14
15 <!--NeedCopy-->
```


Configuración de puertas de enlace de capa de aplicación para NAT64 a gran escala

January 12, 2021

Para algunos protocolos de capa de aplicación, las direcciones IP y los números de puerto de protocolo también se comunican en la carga útil del paquete. Application Layer Gateway para un protocolo analiza la carga útil del paquete y realiza los cambios necesarios para garantizar que el protocolo continúa funcionando en NAT64 a gran escala.

El dispositivo Citrix ADC admite ALG para los siguientes protocolos para NAT64 a gran escala:

- FTP
- ICMP
- TFTP
- SIP
- RTSP

Puerta de enlace de capa de aplicación para protocolos FTP, ICMP y TFTP

January 12, 2021

Puede habilitar o inhabilitar ALG para el protocolo FTP para una configuración NAT64 a gran escala habilitando o inhabilitando la opción ALG FTP del grupo LSN de la configuración.

ALG para el protocolo ICMP está habilitado de forma predeterminada, y no hay ninguna disposición para inhabilitarlo.

ALG para el protocolo TFTP está inhabilitado de forma predeterminada. TFTP ALG se habilita automáticamente para una configuración NAT64 a gran escala cuando se vincula un perfil de aplicación UDP LSN, con asignación independiente del punto final, filtrado independiente del punto final y puerto de destino como 69 (puerto conocido para TFTP), al grupo LSN.

Puerta de enlace de capa de aplicación para protocolo SIP

August 20, 2021

El uso de NAT64 a gran escala con protocolo de inicio de sesión (SIP) es complicado, ya que los mensajes SIP contienen direcciones IP en los encabezados SIP, así como en el cuerpo SIP. Cuando LSN se utiliza con SIP, los encabezados SIP contienen información sobre la persona que llama y el receptor,

y el dispositivo traduce esta información para ocultarla de la red externa. El cuerpo SIP contiene la información del Protocolo de descripción de la sesión (SDP), que incluye direcciones IP y números de puerto para la transmisión de los medios. SIP ALG para NAT64 a gran escala es compatible con RFC 3261, RFC 3581, RFC 4566 y RFC 4475.

> **Nota**
>
> SIP ALG se admite en un dispositivo independiente de Citrix ADC, en una configuración de alta disponibilidad de Citrix ADC, así como en una configuración de clúster de Citrix ADC.

Limitaciones de SIP ALG

SIP ALG para NAT64 a gran escala tiene las siguientes limitaciones:

- Solo se admite la carga de SDP.
- Estas opciones no se admiten:
  - Direcciones IP de multidifusión
  - SDP cifrado
  - SIP TLS
  - Traducción FQDN
  - Autenticación de capa SIP
  - Dominios de tráfico
  - Particiones de administración
  - Cuerpo con varias partes
  - Plegable de línea

Configuración de SIP ALG

Debe configurar el SIP ALG como parte de la configuración LSN. Para obtener instrucciones sobre la configuración de LSN, consulte Configuración de gran escala NAT64. Al configurar LSN, asegúrese de que:

- Defina los siguientes parámetros al agregar un perfil de aplicación LSN:
  - Agrupamiento de IP = PAIRED
  - Asignación de direcciones y puertos = ENDPOINT-INDEPENDENT
  - Filtrado = ENDPOINT-INDEPENDENT
- Cree un perfil SIP ALG y asegúrese de definir el rango de puertos de origen o el rango de puertos de destino. Enlace el perfil SIP ALG al grupo LSN.
- Habilite SIP ALG en el grupo LSN.

Para habilitar SIP ALG para una configuración LSN mediante la CLI

En el símbolo del sistema, escriba:


```
add lsn group <groupname> -clientname <string> [-sipalg ( ENABLED |
    DISABLED )]

show lsn group <groupname>
<!--NeedCopy-->
```

Para habilitar SIP ALG para una configuración LSN mediante la CLI

En el símbolo del sistema, escriba:

```
add lsn sipalgprofile <sipalgprofilename>[-dataSessionIdleTimeout <
    positive_integer>][-sipSessionTimeout <positive_integer>] [-
    registrationTimeout <positive_integer>] [-sipsrcportrange <port[-
    port]>] [-sipdstportrange <port[-port]>] [-openRegisterPinhole (
    ENABLED | DISABLED )] [-openContactPinhole ( ENABLED | DISABLED )]
    [-openViaPinhole ( ENABLED | DISABLED )] [-openRecordRoutePinhole (
    ENABLED | DISABLED )]-sipTransportProtocol ( TCP | UDP ) [-
    openRoutePinhole ( ENABLED | DISABLED )] [-rport ( ENABLED |
    DISABLED )]

show lsn sipalgprofile <sipalgprofilename
<!--NeedCopy-->
```

Configuración de ejemplo

El siguiente ejemplo de configuración NAT64 a gran escala, SIP ALG está habilitado para el tráfico TCP desde dispositivos de suscriptor en la red 2001:DB 8:1003: :/96.

```
add lsn client LSN-NAT64-CLIENT-9

Done
bind lsn client LSN-NAT64-CLIENT-9 -network6 2001:DB8:1002::/96

Done
add lsn pool LSN-NAT64-POOL-9

Done
bind lsn pool LSN-NAT64-POOL-9 203.0.113.90
```



```
11
12 Done
13 add lsn ip6profile LSN-NAT64-PROFILE-9 -type NAT64 -natprefix 2001:DB8
      :309::/96
14
15 Done
16 add lsn appsprofile LSN-NAT64-APPS-PROFILE-9 TCP -ippooling PAIRED -
      mapping ENDPOINT-INDEPENDENT -filtering ENDPOINT-INDEPENDENT
17
18 Done
19 add lsn sipalgprofile SIPALGPROFILE-9  -sipdstportrange 5060  -
      sipTransportProtocol TCP
20
21 Done
22 add lsn group LSN-NAT64-GROUP-9 -clientnameLSN-NAT64-CLIENT-9 -
      ip6profile LSN-NAT64-PROFILE-7 -sipalg ENABLED
23
24 Done
25 bind lsn group LSN-NAT64-GROUP-9 -poolnameLSN-NAT64-POOL-9
26 Done
27 bind lsn group LSN-NAT64-GROUP-9 -appsprofilename LSN-NAT64-APPS-
      PROFILE-9
28 Done
29 bind lsn group LSN-NAT64-GROUP-9 -sipalgprofilename SIPALGPROFILE-9
30 Done
31 <!--NeedCopy-->
```

Puerta de enlace de capa de aplicación para protocolo RTSP

January 12, 2021

Real Time Streaming Protocol (RTSP) es un protocolo de nivel de aplicación para la transferencia de datos de medios en tiempo real. Utilizado para establecer y controlar sesiones de medios entre puntos finales, RTSP es un protocolo de canal de control entre el cliente de medios y el servidor de medios. La comunicación típica es entre un cliente y un servidor multimedia de streaming.

La transmisión de medios desde una red privada a una red pública requiere traducir direcciones IP y números de puerto a través de la red. La funcionalidad Citrix ADC incluye una puerta de enlace de capa de aplicación (ALG) para RTSP, que se puede utilizar con NAT de gran escala (LSN) para analizar la secuencia de medios y realizar los cambios necesarios para garantizar que el protocolo continúe funcionando a través de la red.

La forma en que se realiza la traducción de direcciones IP depende del tipo y la dirección del mensaje y del tipo de medios admitidos por la implementación cliente-servidor. Los mensajes se traducen de la siguiente manera:

- Solicitud saliente: Dirección IP privada a la dirección IP pública propiedad de Citrix ADC llamada dirección IP LSN.
- Respuesta entrante: Dirección IP LSN a dirección IP privada.
- Solicitud entrante: Sin traducción.
- Respuesta saliente: Dirección IP privada a la dirección IP del grupo LSN.

> **Nota**
>
> RTSP ALG se admite en un dispositivo independiente de Citrix ADC, en una configuración de alta disponibilidad de Citrix ADC, así como en una configuración de clúster de Citrix ADC.

Limitaciones de RTSP ALG

El RTSP ALG no admite lo siguiente:

- Sesiones RTSP multidifusión
- Sesión RTSP sobre UDP
- Particiones de administración
- Autenticación RTSP
- Tunelización HTTP

Configuración de RTSP ALG

Configure RTSP ALG como parte de la configuración LSN. Para obtener instrucciones sobre la configuración de LSN, consulte Configuración de gran escala NAT64. Durante la configuración, asegúrese de que:

- Defina los siguientes parámetros al agregar un perfil de aplicación LSN:
  - Agrupamiento de IP = PAIRED
  - Asignación de direcciones y puertos = ENDPOINT-INDEPENDENT
  - Filtrado = ENDPOINT-INDEPENDENT
- Habilitar RTSP ALG en el grupo LSN
- Crear un perfil RTSP ALG y enlazar el perfil RTSP ALG al grupo LSN

Para habilitar RTSP ALG para una configuración LSN mediante la CLI

En el símbolo del sistema, escriba:


```
add lsn group <groupname> -clientname <string> [-rtspalg ( ENABLED |
    DISABLED )]

show lsn group <groupname>
<!--NeedCopy-->
```

Para habilitar RTSP ALG para una configuración LSN mediante la CLI

En el símbolo del sistema, escriba:

```
add lsn rtspalgprofile <rtspalgprofilename> [-rtspIdleTimeout <
    positive_integer>] -rtspportrange <port[-port]> [-
    rtspTransportProtocol (TCP|UDP)]

show lsn rtspalgprofile <rtspalgprofilename>
<!--NeedCopy-->
```

Ejemplo de configuración RTSP ALG

El siguiente ejemplo de configuración NAT64 a gran escala, RTSP ALG está habilitado para el tráfico TCP desde dispositivos de suscriptor en la red 2001:DB 8:1002: :/96.

```
add lsn client LSN-NAT64-CLIENT-9
Done
bind lsn client LSN-NAT64-CLIENT-9 -network6 2001:DB8:1002::/96
Done
add lsn pool LSN-NAT64-POOL-9
Done
bind lsn pool LSN-NAT64-POOL-9 203.0.113.90
Done
add lsn ip6profile LSN-NAT64-PROFILE-9 -type NAT64 -natprefix 2001:DB8
    :309::/96
Done
add lsn appsprofile LSN-NAT64-APPS-PROFILE-9 TCP -ippooling PAIRED -
    mapping ENDPOINT-INDEPENDENT -filtering ENDPOINT-INDEPENDENT
Done
add lsn rtspalgprofile RTSPALGPROFILE-9 -rtspIdleTimeout 1000 -
    rtspportrange 554
Done
```



```
15 add lsn group LSN-NAT64-GROUP-9 -clientname LSN-NAT64-CLIENT-9 -
      ip6profile LSN-NAT64-PROFILE-7 -rtspalg ENABLED
16 Done
17 bind lsn group LSN-NAT64-GROUP-9 -poolname LSN-NAT64-POOL-9
18 Done
19 bind lsn group LSN-NAT64-GROUP-9 -appsprofilename LSN-NAT64-APPS-
      PROFILE-9
20 Done
21 bind lsn group LSN-NAT64-GROUP-9  -rtspalgprofilename RTSPALGPROFILE-9
22 Done
23 <!--NeedCopy-->
```

Configuración de mapas NAT64 estáticos de gran escala

January 12, 2021

El dispositivo Citrix ADC admite la creación manual de asignaciones NAT64, que contienen la asignación entre la siguiente información:

- Dirección IP y puerto del suscriptor
- Dirección IP NAT y puerto

Las asignaciones NAT64 estáticas a gran escala son útiles en los casos en que quiere asegurarse de que las conexiones IPv4 iniciadas a una dirección IP NAT:puerto se traducen IPv6 y se asignan a la dirección IP del suscriptor:puerto (por ejemplo, servidores web ubicados en la red interna).

Para crear una asignación NAT64 a gran escala mediante la línea de comandos

En el símbolo del sistema, escriba:

```
1 add lsn static <name> <transportprotocol> <subscrIP> <subscrPort>  [<
      natIP> [<natPort>]] [-destIP <ip_addr> [-dsttd <positive_integer>]]
2
3 show lsn static
4 <!--NeedCopy-->
```

Mapas NAT64 estática de gran escala de puerto comodín

Una entrada de asignación NAT64 estática a gran escala suele ser una asignación uno a uno entre una dirección IPv6 de suscriptor: Puerto y una dirección IPv4 NAT: Puerto. Una entrada de asignación

NAT64 estática a gran escala de uno a uno expone solo un puerto de la dirección IP del suscriptor a Internet.

Algunas situaciones pueden requerir exponer todos los puertos (64K: Limitado al número máximo de puertos de una dirección NAT IPv4) de una dirección IP de suscriptor a Internet (por ejemplo, un servidor alojado en una red interna y ejecutando un servicio diferente en cada puerto). Para hacer que estos servicios internos sean accesibles a través de Internet, debe exponer todos los puertos del servidor a Internet.

Una forma de cumplir este requisito es agregar 64 mil entradas de mapeo estático uno a uno, una entrada de mapeo para cada puerto. Crear esas entradas es muy engorroso y una gran tarea. Además, este gran número de entradas de configuración puede provocar problemas de rendimiento en el dispositivo Citrix ADC.

Un método más simple es usar puertos comodín en una entrada de asignación estática. Solo necesita crear una entrada de mapeo estático con parámetros NAT-port y subscriber-port establecidos en el carácter comodín (*), y el parámetro de protocolo establecido en ALL, para exponer todos los puertos de una dirección IP de suscriptor para todos los protocolos a Internet.

Para las conexiones entrantes o salientes de un suscriptor que coinciden con una entrada de asignación estática de comodín, el puerto del suscriptor no cambia después de la operación NAT. Cuando una conexión a Internet iniciada por el suscriptor coincide con una entrada de asignación estática comodín, el dispositivo Citrix ADC asigna un puerto NAT que tiene el mismo número que el puerto del suscriptor desde el que se inicia la conexión. Del mismo modo, un host de Internet se conecta al puerto de un suscriptor mediante la conexión al puerto NAT que tiene el mismo número que el puerto del suscriptor.

Para configurar el dispositivo Citrix ADC para proporcionar acceso a todos los puertos de una dirección IPv6 de suscriptor, cree un mapa estático comodín con los siguientes parámetros obligatorios:

- Protocolo=Todos
- Puerto del suscriptor = *
- Puerto NAT = *

En un mapa estático comodín, a diferencia de un mapa estático uno a uno, establecer el parámetro IP NAT es obligatorio. Además, la dirección IP NAT asignada a un mapa estático de comodín no se puede utilizar para ningún otro suscriptor.

Para crear un mapa estático comodín mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
1 add lsn static <name> ALL <subscrIP> *  <natIP> * [-td <
     positive_integer>] [-destIP <ip_addr>
2
```



```
3 show lsn static
4 <!--NeedCopy-->
```

En la siguiente configuración de ejemplo de un mapa estático de comodín, todos los puertos de un suscriptor cuya dirección IP es 2001:DB 8:5001: :3 se hacen accesibles a través de NAT IP 203.0.11.33.

```
1 add lsn static NAT64-WILDCARD-STATIC-1 ALL 2001:DB8:5001::3 *
     203.0.113.33 *
2 Done
3 <!--NeedCopy-->
```

Registro y supervisión de NAT64 a gran escala

August 20, 2021

Puede registrar información NAT64 a gran escala para diagnosticar y solucionar problemas y cumplir los requisitos legales. Puede supervisar el rendimiento de la implementación NAT64 a gran escala mediante contadores estadísticos y mostrando las sesiones actuales relacionadas.

Registro de gran escala NAT64

El registro de información NAT64 a gran escala es necesario para que los ISP cumplan los requisitos legales e identifiquen el origen del tráfico en un momento dado.

Un mensaje de registro para una entrada de asignación NAT64 a gran escala consta de la siguiente información:

- Dirección IP propiedad de Citrix ADC (dirección NSIP o dirección SNIP) desde la que se origina el mensaje de registro.
- Marca de tiempo.
- Tipo de entrada (MAPPING).
- Si se ha creado o eliminado la entrada de asignación.
- Dirección IP, puerto e ID de dominio de tráfico del suscriptor.
- Dirección IP NAT y puerto.
- Nombre del protocolo.
- La dirección IP de destino, el puerto y el ID de dominio de tráfico pueden estar presentes, en función de las condiciones siguientes:
  - La dirección IP de destino y el puerto no se registran para la asignación independiente del punto final.

- Solo se registra la dirección IP de destino para la asignación dependiente de la dirección. El puerto no está registrado.
- La dirección IP de destino y el puerto se registran para la asignación dependiente del puerto de dirección.

Un mensaje de registro para una sesión NAT64 a gran escala consta de la siguiente información:

- Dirección IP propiedad de Citrix ADC (dirección NSIP o dirección SNIP) desde la que se origina el mensaje de registro
- Marca de tiempo
- Tipo de entrada (SESSION)
- Si se crea o elimina la sesión
- Dirección IP, puerto e ID de dominio de tráfico del suscriptor
- Dirección IP NAT y puerto
- Nombre del protocolo
- Dirección IP de destino, puerto e ID de dominio de tráfico

La tabla siguiente muestra entradas de registro NAT64 a gran escala de ejemplo de cada tipo almacenadas en los servidores de registro configurados. Las entradas de registro muestran que un suscriptor cuya dirección IPv6 es 2001:db8:5001: :9 estaba conectado al destino IP: Puerto 23.0.0.1:80 a través de NAT IP: Puerto 203.0.113.63:45195 el 7 de abril de 2016, de 14:07:57 GMT a 14:10:59 GMT.

Tipo de entrada de registro	Entrada de registro de ejemplo
Creación de sesiones	04/07/2016:14:07:57 GMT Informational 0-PPE-10: Default LSN LSN_SESSION 5532 0: SESSION CREATED Client IP-Port:TD **2001:db8:5001::9-34937:0**, NatIP:NatPort 203.0.113.63:45195, Destination IP:Port:TD 23.0.0.1:0:80, Protocol: TCP
Creación de mapas	04/07/2016:14:07:57 GMT Informational 0-PPE-10: Default LSN LSN_ADDR_MAPPING 5533 0: ADM CREATED Client IP-Port:TD **2001:db8:5001::9-34937:0**, NatIP:NatPort 203.0.113.63:45195, Destination IP:TD 23.0.0.1:80, Protocol: TCP
Eliminación de sesión	04/07/2016:14:10:59 GMT 0-PPE-10: Default LSN LSN_SESSION 25012 0: SESSION DELETED Client IP-Port:TD **2001:db8:5001::9-34937:0**, NatIP:NatPort 203.0.113.63:45195, Destination IP:Port:TD 23.0.0.1:0:80, Protocol: TCP

Tipo de entrada de registro	Entrada de registro de ejemplo
Eliminación de asignación	04/07/2016:14:10:59 GMT 0-PPE-10: Default LSN LSN_ADDR_MAPPING 25013 0: ADM DELETED Client IP-Port:TD **2001:db8:5001::9-34937:0**, NatIP:NatPort 203.0.113.63:45195, Destination IP:Port:TD 23.0.0.1:0:80, Protocol: TCP

Pasos de configuración

Puede configurar el registro de información NAT64 a gran escala para una configuración NAT64 a gran escala estableciendo los parámetros de registro y registro de sesión de los grupos LSN. Estos son parámetros de nivel de grupo y están inhabilitados de forma predeterminada. El dispositivo Citrix ADC registra sesiones NAT64 a gran escala para un grupo LSN solo cuando los parámetros de registro y registro de sesión están habilitados.

En la siguiente tabla se muestra el comportamiento de registro de un grupo LSN para varias configuraciones de parámetros de registro y registro de sesión.

Captura de registros	Registro de sesiones	Comportamiento de registro
Habilitado	Habilitado	Registra las entradas de asignación de LSN así como las sesiones LSN
Habilitado	Inhabilitada	Registra las entradas de asignación de LSN pero no las sesiones LSN
Inhabilitada	Habilitado	Registra ni entradas de asignación ni sesiones LSN

Para registrar información NAT64 a gran escala mediante la CLI

Para establecer los parámetros de registro y registro de sesión al agregar un grupo LSN, en el símbolo del sistema, escriba:

```
1 add lsn group <groupname> -clientname <string> [-logging (ENABLED|
     DISABLED)] [-sessionLogging (ENABLED|DISABLED)]
2
3 show lsn group
```



```
<!--NeedCopy-->
```

Para establecer los parámetros de registro y registro de sesión para un grupo LSN existente, en el símbolo del sistema, escriba:

```
set lsn group <groupname> [-logging (ENABLED|DISABLED)] [-
   sessionLogging (ENABLED|DISABLED)]

show lsn group
<!--NeedCopy-->
```

Configuración de ejemplo

En este ejemplo de configuración NAT64 a gran escala, los parámetros de registro y registro de sesión están habilitados para el grupo LSN LSN-NAT64-GROUP-1.

El dispositivo Citrix ADC registra información de asignación y sesión NAT64 a gran escala para conexiones de suscriptores (en la red 2001:DB 8:5001: :/96).

Configuración de ejemplo:

```
add lsn client LSN-NAT64-CLIENT-1 Done
Done
bind lsn client LSN-NAT64-CLIENT-1 -network6 2001:DB8:5001::/96
Done
add lsn pool LSN-NAT64-POOL-1
Done
bind lsn pool LSN-NAT64-POOL-1 203.0.113.61 - 203.0.113.70
Done
add lsn ip6profile LSN-NAT64-PROFILE-1 -type NAT64 -natprefix 2001:DB8
   :300::/96
Done
add lsn group LSN-NAT64-GROUP-1 -clientname LSN-NAT64-CLIENT-1  -
   ip6profile LSN-NAT64-PROFILE-1  -logging ENABLED -sessionLogging
   ENABLED
Done
bind lsn group LSN-NAT64-GROUP-1 -poolname LSN-NAT64-POOL-1
Done
<!--NeedCopy-->
```


Registro de información MSISDN para NAT64 de gran escala

Un número de directorio integrado de suscriptor de Mobile Station (MSISDN) es un número de teléfono que identifica de forma única a un suscriptor a través de varias redes móviles. El MSISDN está asociado a un código de país y a un código de destino nacional que identifica al operador del suscriptor.

Puede configurar un dispositivo Citrix ADC para que incluya MSISSDN en entradas de registro NAT64 LSN a gran escala para suscriptores en redes móviles. La presencia de MSISDN en los registros de LSN facilita el rastreo más rápido y preciso de un suscriptor móvil que ha infringido una directiva o ley, o cuya información es requerida por agencias de interceptación legales.

Las siguientes entradas de registro LSN de ejemplo incluyen información MSISDN para una conexión de un suscriptor móvil en una configuración de LSN. Las entradas de registro muestran que un suscriptor móvil cuyo MSISDN es E164:5556543210 y dirección IPv6 es 2001:db8:5001::9 se conectó al destino IP: Puerto 23.0.0.1:80 a través de NAT IP: Puerto 203.0.113.63:45195 el 7 de abril de 2016, de 14:07:57 GMT a 14:10:59 GMT.

Tipo de entrada de registro	Entrada de registro de ejemplo
Creación de sesiones	04/07/2016:14:07:57 GMT Informational 0-PPE-10: Default LSN LSN_SESSION 5532 0: SESSION CREATED **E164:5556543210** Client IP-Port:TD **2001:db8:5001::9-34937:0**, NatIP:NatPort 203.0.113.63:45195, Destination IP:Port:TD 23.0.0.1:0:80, Protocol: TCP
Creación de mapas	04/07/2016:14:07:57 GMT Informational 0-PPE-10: Default LSN LSN_ADDR_MAPPING 5533 0: ADM CREATED **E164:5556543210** Client IP-Port:TD **2001:db8:5001::9-34937:0**, NatIP:NatPort 203.0.113.63:45195, Destination IP:TD 23.0.0.1:80, Protocol: TCP
Eliminación de sesión	04/07/2016:14:10:59 GMT 0-PPE-10: Default LSN LSN_SESSION 25012 0: SESSION DELETED **E164:5556543210** Client IP-Port:TD **2001:db8:5001::9-34937:0**, NatIP:NatPort 203.0.113.63:45195, Destination IP:Port:TD 23.0.0.1:0:80, Protocol: TCP

Tipo de entrada de registro	Entrada de registro de ejemplo
Eliminación de asignación	04/07/2016:14:10:59 GMT 0-PPE-10: Default LSN LSN_ADDR_MAPPING 25013 0: ADM DELETED **E164:5556543210** Client IP-Port:TD **2001:db8:5001::9-34937:0**, NatIP:NatPort 203.0.113.63:45195, Destination IP:Port:TD 23.0.0.1:0:80, Protocol: TCP

Pasos de configuración

Realice las siguientes tareas para incluir información de MSISDN en los registros LSN:

- **Cree un perfil de registro LSN**. Un perfil de registro LSN incluye el parámetro ID de suscriptor de registro, que especifica si se debe incluir o no la información MSISDN en los registros de LSN de una configuración de LSN.
- Enlace el perfil de registro LSN a un grupo LSN de una configuración LSN.Enlazar el perfil de registro LSN creado a un grupo LSN de una configuración LSN estableciendo el parámetro de nombre de perfil de registro en el nombre de perfil de registro LSN creado. La información MSISDN se incluye en todos los registros de LSN relacionados con suscriptores móviles de este grupo LSN.

Para crear un perfil de registro LSN mediante la CLI

En el símbolo del sistema, escriba:

```
add lsn logprofile <logprofilename> -logSubscriberID ( ENABLED |
   DISABLED )

show lsn logprofile
<!--NeedCopy-->
```

Para enlazar un perfil de registro LSN a un grupo LSN de una configuración de LSN NAT64 mediante la CLI

En el símbolo del sistema, escriba:

```
bind lsn group <groupname>  -logProfileName <lsnlogprofilename>
```



```
2
3 show lsn group
4 <!--NeedCopy-->
```

Configuración de ejemplo

En este ejemplo de configuración de NAT64 LSN, el perfil de registro LSN LOG-PROFILE-MSISDN-1 tiene habilitado el parámetro ID de suscriptor de registro. LOG-PROFILE-MSISDN-1 está vinculado al grupo LSN LSN-NAT64-GROUP-1. La información de MSISDN se incluye en la sesión de LSN y en los registros de asignación de LSN para conexiones de suscriptores móviles (en la red 2001:DB 8:5001: :/96).

```
1 add lsn logprofile  LOG-PROFILE-MSISDN-1  -logSubscriberID ENABLED
2 Done
3 add lsn client LSN-NAT64-CLIENT-1
4 Done
5 bind lsn client LSN-NAT64-CLIENT-1 -network6 2001:DB8:5001::/96
6 Done
7 add lsn pool LSN-NAT64-POOL-1
8 Done
9 bind lsn pool LSN-NAT64-POOL-1 203.0.113.61 - 203.0.113.70
10 Done
11 add lsn ip6profile LSN-NAT64-PROFILE-1 -type NAT64 -natprefix 2001:DB8
      :300::/96
12 Done
13 add lsn group LSN-NAT64-GROUP-1 -clientname LSN-NAT64-CLIENT-1  -
      ip6profile LSN-NAT64-PROFILE-1
14 Done
15 bind lsn group LSN-NAT64-GROUP-1 -poolname LSN-NAT64-POOL-1
16 Done
17 bind lsn group LSN-NAT64-GROUP-1 -logprofilename  LOG-PROFILE-MSISDN-1
18 Done
19 <!--NeedCopy-->
```

Registro compacto para NAT a gran escala

El registro de la información LSN es una de las funciones importantes que necesitan los ISP para cumplir con los requisitos legales y poder identificar el origen del tráfico en cualquier momento dado. Esto finalmente resulta en un gran volumen de datos de registro, lo que requiere que los ISP realicen grandes inversiones para mantener la infraestructura de registro.

El registro compacto es una técnica para reducir el tamaño del registro mediante el uso de un cambio notacional que implica códigos cortos para nombres de eventos y protocolos. Por ejemplo, C para cliente, SC para sesión creada y T para TCP. El registro compacto da como resultado una reducción media del 40 por ciento en el tamaño del registro.

Pasos de configuración

Realice las siguientes tareas para registrar la información de LSN en formato compacto:

1. Cree un perfil de registro LSN. Un perfil de registro LSN incluye el parámetro Log Compact, que especifica si se va a registrar o no la información en formato compacto para una configuración de LSN.
2. Enlazar el perfil de registro LSN a un grupo LSN de una configuración LSN. Vincular el perfil de registro LSN creado a un grupo LSN de una configuración de LSN estableciendo el parámetro Nombre de perfil de registro en el nombre de perfil de registro LSN creado. Todas las sesiones y asignaciones de este grupo LSN se registran en formato compacto.

Para crear un perfil de registro LSN mediante la CLI

En el símbolo del sistema, escriba:

```
add lsn logprofile <logprofilename> -logCompact (ENABLED|DISABLED)

show lsn logprofile
<!--NeedCopy-->
```

Para enlazar un perfil de registro LSN a un grupo LSN de una configuración de LSN mediante la CLI

En el símbolo del sistema, escriba:

```
bind lsn group <groupname> -logProfileName <lsnlogprofilename>

show lsn group
<!--NeedCopy-->
```

Ejemplo de configuración para NAT64:


```
add lsn logprofile  LOG-PROFILE-COMPACT-1 -logCompact ENABLED
Done
add lsn client LSN-NAT64-CLIENT-1
Done
bind lsn client LSN-NAT64-CLIENT-1 -network6 2001:DB8:5001::/96
Done
add lsn pool LSN-NAT64-POOL-1
Done
bind lsn pool LSN-NAT64-POOL-1 203.0.113.61 - 203.0.113.70
Done
add lsn ip6profile LSN-NAT64-PROFILE-1 -type NAT64 -natprefix 2001:DB8
   :300::/96
Done
add lsn group LSN-NAT64-PROFILE-1 -clientname LSN-NAT64-CLIENT-1  -
   ip6profile LSN-NAT64-PROFILE-1
Done
bind lsn group LSN-NAT64-GROUP-1 -poolname LSN-NAT64-POOL-1
Done
bind lsn group LSN-NAT64-GROUP-1  - logProfileName LOG-PROFILE-COMPACT-1
Done
<!--NeedCopy-->
```

Registro de información de encabezado HTTP

El dispositivo Citrix ADC puede registrar la información de encabezado de solicitud de una conexión HTTP que utiliza la funcionalidad NAT64 de gran escala de Citrix ADC. Se puede registrar la siguiente información de encabezado de un paquete de solicitud HTTP:

- URL a la que está destinada la solicitud HTTP
- Método HTTP especificado en la solicitud HTTP
- Versión HTTP utilizada en la solicitud HTTP
- Dirección IPv6 del suscriptor que envió la solicitud HTTP

Los registros de encabezado HTTP pueden ser utilizados por los ISP para ver las tendencias relacionadas con el protocolo HTTP entre un conjunto de suscriptores. Por ejemplo, un ISP puede utilizar esta función para averiguar el sitio web más popular entre un conjunto de suscriptores.

Pasos de configuración

Realice las siguientes tareas para configurar el dispositivo Citrix ADC para registrar la información de encabezado HTTP:

- Cree un perfil de registro de encabezado HTTP. Un perfil de registro de encabezado HTTP es una colección de atributos de encabezado HTTP (por ejemplo, URL y método HTTP) que se pueden habilitar o inhabilitar para el registro.
- Enlazar el encabezado HTTP a un grupo LSN de una configuración NAT64 a gran escala. Enlace el perfil de registro de encabezado HTTP a un grupo LSN de una configuración LSN estableciendo el parámetro de nombre de perfil de registro de encabezado HTTP en el nombre del perfil de registro de encabezado HTTP creado. A continuación, el dispositivo Citrix ADC registra la información de encabezado HTTP de cualquier solicitud HTTP relacionada con el grupo LSN. Un perfil de registro de encabezado HTTP se puede enlazar a varios grupos LSN, pero un grupo LSN solo puede tener un perfil de registro de encabezado HTTP.

Para crear un perfil de registro de encabezado HTTP mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
add lsn httphdrlogprofile <httphdrlogprofilename> [-logURL ( ENABLED |
    DISABLED )] [-logMethod ( ENABLED | DISABLED )] [-logVersion (
    ENABLED | DISABLED )] [-logHost ( ENABLED | DISABLED )]

show lsn httphdrlogprofile
<!--NeedCopy-->
```

Para enlazar un perfil de registro de encabezado HTTP a un grupo LSN mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
bind lsn group <groupname> -httphdrlogprofilename <string>

show lsn group <groupname>
<!--NeedCopy-->
```

Configuración de ejemplo

```
add lsn httphdrlogprofile HTTP-HEADER-LOG-1
Done
add lsn client LSN-NAT64-CLIENT-1 Done
```



```
4  Done
5  bind lsn client LSN-NAT64-CLIENT-1 -network6 2001:DB8:5001::/96
6  Done
7  add lsn pool LSN-NAT64-POOL-1
8  Done
9  bind lsn pool LSN-NAT64-POOL-1 203.0.113.61 - 203.0.113.70
10 Done
11 add lsn ip6profile LSN-NAT64-PROFILE-1 -type NAT64 -natprefix 2001:DB8
       :300::/96
12 Done
13 add lsn group LSN-NAT64-GROUP-1 -clientname LSN-NAT64-CLIENT-1  -
       ip6profile LSN-NAT64-PROFILE-1
14 Done
15 bind lsn group LSN-NAT64-GROUP-1 -poolname LSN-NAT64-POOL-1
16 Done
17 bind lsn group LSN-NAT64-GROUP-1 -httphdrlogprofilename HTTP-HEADER-LOG
       -1
18 Done
19 <!--NeedCopy-->
```

Visualización de sesiones NAT64 actuales a gran escala

Puede mostrar las sesiones NAT64 a gran escala actuales para detectar sesiones no deseadas o ineficientes en el dispositivo Citrix ADC. Puede mostrar todas o algunas sesiones NAT64 a gran escala sobre la base de parámetros de selección.

> **Nota**
>
> Cuando existen más de un millón de sesiones NAT64 a gran escala en el dispositivo Citrix ADC, Citrix recomienda utilizar los parámetros de selección para mostrar las sesiones NAT64 a gran escala seleccionadas en lugar de mostrarlas todas.

Para mostrar todas las sesiones NAT64 a gran escala mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
1 show lsn session  - nattype NAT64
2 <!--NeedCopy-->
```

Para mostrar sesiones NAT64 selectivas a gran escala mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:


```
show lsn session  -nattype NAT64 [-network6 <ipv6_addr|*>] [-clientname
    <string>] [-natIP <ip_addr> [-natPort <port>]]
<!--NeedCopy-->
```

Visualización de estadísticas NAT64 a gran escala

Puede mostrar estadísticas relacionadas con el módulo NAT64 a gran escala y evaluar su rendimiento o solucionar problemas. Puede mostrar un resumen de las estadísticas de todas las configuraciones NAT64 a gran escala o de una configuración NAT64 a gran escala concreta. Los contadores estadísticos reflejan los eventos desde que se reinició por última vez el dispositivo Citrix ADC. Todos estos contadores se restablecen a 0 cuando se reinicia el dispositivo Citrix ADC.

Para mostrar estadísticas totales de NAT64 a gran escala mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
stat lsn nat64
<!--NeedCopy-->
```

Para mostrar estadísticas para una configuración NAT64 a gran escala especificada mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
stat lsn group <groupname>
<!--NeedCopy-->
```

Eliminación de sesiones NAT64 a gran escala

Puede eliminar cualquier sesión NAT64 a gran escala no deseada o ineficiente del dispositivo Citrix ADC. El dispositivo libera inmediatamente los recursos (como la dirección IP NAT, el puerto y la memoria) asignados a estas sesiones, lo que hace que los recursos estén disponibles para las sesiones nuevas. El dispositivo también elimina todos los paquetes posteriores relacionados con estas sesiones eliminadas. Puede quitar todas las sesiones NAT64 a gran escala o seleccionadas del dispositivo Citrix ADC.

Para borrar todas las sesiones NAT64 a gran escala mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
flush lsn session  -nattype NAT64

show lsn session  -nattype NAT64
<!--NeedCopy-->
```

Para borrar sesiones NAT64 selectivas a gran escala mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
flush lsn session  -nattype NAT64 [-network6 <ipv6_addr|*>] [-
   clientname <string>] [-natIP <ip_addr> [-natPort <port>]]

show lsn session  -nattype NAT64 [-network6 <ipv6_addr|*>] [-clientname
    <string>] [-natIP <ip_addr> [-natPort <port>]]
<!--NeedCopy-->
```

Configuración de ejemplo:

Borrar todas las sesiones NAT64 a gran escala existentes en un dispositivo Citrix ADC

```
flush lsn session   -nattype NAT64
Done
<!--NeedCopy-->
```

Borrar todas las sesiones NAT64 a gran escala relacionadas con la entidad cliente LSN-NAT64-CLIENT-1

```
flush lsn session  -nattype NAT64 -clientname LSN-NAT64-CLIENT-1
Done
<!--NeedCopy-->
```

Borrar todas las sesiones NAT64 a gran escala relacionadas con una red de suscriptor (2001:DB 8:5001::/96) de la entidad de cliente LSN LSN-NAT64-CLIENT-2


```
flush lsn session -nattype NAT64 -network6 2001:DB8:5001::/96 -
   clientname LSN-NAT64-CLIENT-2
Done
<!--NeedCopy-->
```

Registro de IPFIX

El dispositivo Citrix ADC admite el envío de información sobre eventos LSN en formato de exportación de información de flujo de protocolo Internet (IPFIX) al conjunto configurado de recopiladores IPFIX. El dispositivo utiliza la función AppFlow existente para enviar eventos LSN en formato IPFIX a los recopiladores IPFIX.

El registro basado en IPFIX está disponible para los siguientes eventos relacionados con NAT64:

- Creación o eliminación de una sesión LSN.
- Creación o eliminación de una entrada de asignación LSN.
- Asignación o desasignación de bloques de puertos en el contexto de NAT determinista.
- Asignación o desasignación de bloques de puertos en el contexto de NAT dinámico.
- Siempre que se supere la cuota de sesión de suscriptor.

Puntos a tener en cuenta antes de configurar el registro IPFIX

Antes de comenzar a configurar IPSec ALG, tenga en cuenta los siguientes puntos:

- Debe configurar la función AppFlow y los recopiladores IPFIX en el dispositivo Citrix ADC. Para obtener instrucciones, consulte Configuración de la función AppFlow.

Pasos de configuración

Realice las siguientes tareas para registrar la información LSN en formato IPFIX:

- **Habilite el registro LSN en la configuración de AppFlow**. Habilite el parámetro de registro LSN como parte de la configuración de AppFlow.
- **Cree un perfil de registro LSN**. Un perfil de registro LSN incluye el parámetro IPFIX que habilita o inhabilita la información de registro en formato IPFIX.
- **Enlazar el perfil de registro de LSN a un grupo LSN de una configuración LSN**. Enlace el perfil de registro LSN a uno o varios grupos LSN. Los eventos relacionados con el grupo LSN enlazado se registrarán en formato IPFIX.

Para habilitar el registro LSN en la configuración de AppFlow mediante la CLI

En el símbolo del sistema, escriba:


```
set appflow param -lsnLogging ( ENABLED | DISABLED )

show appflow param
<!--NeedCopy-->
```

Para crear un perfil de registro LSN mediante el comando CliAt el símbolo del sistema, escriba

En el símbolo del sistema, escriba:

```
set lsn logprofile <logProfileName>  -logipfix ( ENABLED | DISABLED )

show lsn logprofile
<!--NeedCopy-->
```

Para enlazar el perfil de registro LSN a un grupo LSN de una configuración de LSN mediante la CLI

En el símbolo del sistema, escriba:

```
bind lsn group <groupname>  -logProfileName <lsnlogprofilename>

show lsn group
<!--NeedCopy-->
```

Para crear un perfil de registro LSN mediante la interfaz gráfica de usuario

Vaya a **Sistema** > **NAT a gran escala** > **Perfiles**, haga clic en la ficha **Registro** y, a continuación, agregue un perfil de registro.

Para enlazar el perfil de registro LSN a un grupo LSN de una configuración LSN mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **NAT a gran escala** > **Grupo LSN,** abra el grupo **LSN** .
2. En **Configuración avanzada,** haga clic en **+ Perfil de registro** para enlazar el perfil de registro creado al grupo LSN.

Protocolo de control de puertos para NAT64 a gran escala

January 12, 2021

Los dispositivos Citrix ADC ahora admiten Port Control Protocol (PCP) para NAT (LSN) a gran escala. Muchas de las aplicaciones de suscriptor de un ISP deben ser accesibles desde Internet (por ejemplo, dispositivos de Internet de las cosas (IOT), como una cámara IP que proporciona vigilancia a través de Internet). Una forma de cumplir este requisito es crear mapas estáticos de NAT (LSN) a gran escala. Pero para una gran cantidad de suscriptores, crear mapas NAT LSN estáticos no es una solución factible.

Port Control Protocol (PCP) permite a un suscriptor solicitar asignaciones NAT LSN específicas para sí mismo y/o para otros dispositivos de terceros. El dispositivo NAT a gran escala crea un mapa LSN y lo envía al suscriptor. El suscriptor envía a los dispositivos remotos en Internet la dirección IP NAT: Puerto NAT en el que pueden conectarse al suscriptor.

Las aplicaciones suelen enviar mensajes de mantenimiento activo frecuentes al dispositivo NAT a gran escala para que sus asignaciones LSN no agoten el tiempo de espera. PCP ayuda a reducir la frecuencia de dichos mensajes keep-alive al permitir que las aplicaciones aprendan la configuración de tiempo de espera de las asignaciones LSN. Esto ayuda a reducir el consumo de ancho de banda en la red de acceso del ISP y el consumo de batería en dispositivos móviles.

PCP es un modelo cliente-servidor y se ejecuta sobre el protocolo de transporte UDP. Un dispositivo Citrix ADC implementa el componente del servidor PCP y cumple con RFC 6887.

Pasos de configuración

Realice las siguientes tareas para configurar PCP:

- **(Opcional) Cree un perfil de PCP**. Un perfil PCP incluye configuraciones para parámetros relacionados con PCP (por ejemplo, para escuchar solicitudes PCP de mapeo y de pares). Un perfil PCP se puede enlazar a un servidor PCP. Un perfil PCP enlazado a un servidor PCP aplica toda su configuración al servidor PCP. Un perfil PCP puede enlazarse a varios servidores PCP. De forma predeterminada, un perfil PCP con parámetros predeterminados está enlazado a todos los servidores PCP. Un perfil PCP que se vincula a un servidor PCP anula la configuración predeterminada del perfil PCP para ese servidor. Un perfil PCP predeterminado tiene los siguientes parámetros:
  - Asignación: Activada
  - Peer: Activado
  - Vida útil mínima del mapa: 120 segundos
  - Vida máxima máxima: 86400 segundos.
  - Número de anunciaciones: 10

  - Terceros: Inhabilitado
- **Cree un servidor PCP y vincule un perfil PCP a él**. Cree un servidor PCP en el dispositivo Citrix ADC para escuchar solicitudes y mensajes relacionados con PCP de los suscriptores. Se debe asignar una dirección IP de subred (SNIP) o (SNIP6) a un servidor PCP para tener acceso a ella. De forma predeterminada, un servidor PCP escucha en el puerto 5351.
- **Enlace el servidor PCP a un grupo LSN de una configuración LSN**. Vincular el servidor PCP creado a un grupo LSN de una configuración LSN estableciendo el parámetro PCP Server para especificar el servidor PCP creado. Solo los suscriptores de este grupo LSN pueden acceder al servidor PCP creado.

> **Nota**
>
> Un servidor PCP para una configuración NAT a gran escala no atiende solicitudes de suscriptores identificados a partir de reglas de ACL.

Para crear un perfil PCP mediante la CLI

En el símbolo del sistema, escriba:

```
add pcp profile <name> [-mapping ( ENABLED | DISABLED )] [-peer (
    ENABLED | DISABLED )] [-minMapLife <secs>]  [-maxMapLife <secs>] [-
    announceMultiCount <positive_integer>][-thirdParty ( ENABLED |
    DISABLED )]

show pcp profile <name>
<!--NeedCopy-->
```

Para crear un servidor PCP mediante la CLI

En el símbolo del sistema, escriba:

```
add pcp server <name> <IPAddress> [-port <portNum|*>] [-pcpProfile <
    string>]

show pcp server <name>
<!--NeedCopy-->
```


Configuración de ejemplo para NAT64

En la siguiente configuración de ejemplo, el servidor PCP PCP-SERVER-1, con la configuración PCP de PCP-PROFILE-1, está enlazado al grupo LSN LSN-NAT64-GROUP-1. PCP-SERVER-1 atiende solicitudes PCP de suscriptores IPv6 en la red 2001:DB 8:5001: :/96.

Configuración de ejemplo:

```
add pcp profile PCP-PROFILE-1 -minMapLife 400
Done
add pcp server PCP-SERVER-1 2001:DB8:6001::90  -pcpProfile PCP-PROFILE
    -1
Done
add lsn client LSN-NAT64-CLIENT-1
Done
bind lsn client LSN-NAT64-CLIENT-1 -network6 2001:DB8:5001::/96
Done
add lsn pool LSN-NAT64-POOL-1
Done
bind lsn pool LSN-NAT64-POOL-1 203.0.113.61 - 203.0.113.70
Done
add lsn ip6profile LSN-NAT64-PROFILE-1 -type NAT64 -natprefix 2001:DB8
    :300::/96
Done
add lsn group LSN-NAT64-PROFILE-1 -clientname LSN-NAT64-CLIENT-1  -
    ip6profile LSN-NAT64-PROFILE-1
Done
bind lsn group LSN-NAT64-GROUP-1 -poolname LSN-NAT64-POOL-1
Done
bind lsn group LSN-NAT64-GROUP-1  - pcpServer PCP-NAT64-SERVER-1
Done
<!--NeedCopy-->
```

LSN64 en una configuración de clúster

January 12, 2021

Las configuraciones NAT64 de gran escala se admiten en una configuración de clúster de Citrix ADC.

Un clúster de Citrix ADC es un grupo de dispositivos Citrix ADC que se configuran y administran como un único sistema. Un clúster de Citrix ADC proporciona escalabilidad y disponibilidad. Cada dispos-

itivo Citrix ADC en una configuración de clúster actúa como una entidad LSN independiente y se administra como un único sistema.

La configuración de LSN en una configuración de clúster es la misma que en un dispositivo independiente, excepto en el caso de que un grupo específico de direcciones IP de LSN sea propiedad de un nodo cada vez. En otras palabras, una entidad de grupo IP LSN se configura como una entidad manchada en un nodo particular. Todos los nodos de una configuración de clúster pueden tener una entidad de grupo IP LSN específica. Para asegurarse de que los paquetes relacionados con una sesión LSN se reciben en el mismo nodo de clúster que realizó la operación NAT, se configura la dirección del backplane basado en directivas (PBS). PBS dirige los paquetes relacionados recibidos de una sesión LSN al mismo nodo de clúster.

Configuración de ejemplo:

```
add lsn client LSN-NAT64-CLIENT-1

Done

bind lsn client LSN-NAT64-CLIENT-1 -network6 2001:DB8:5001::/96

Done

add lsn pool LSN-NAT64-POOL-1

Done

bind lsn pool LSN-NAT64-POOL-1 -ownerNode 1  203.0.113.61 -
    203.0.113.70

Done

bind lsn pool LSN-NAT64-POOL-1 -ownerNode 2  203.0.113.101 -
    203.0.113.110

Done

add lsn ip6profile LSN-NAT64-PROFILE-1 -type NAT64 -natprefix 2001:DB8
    :300::/96

Done

add lsn group LSN-NAT64-GROUP-1 -clientname LSN-NAT64-CLIENT-1  -
    ip6profile LSN-NAT64-PROFILE-1
```



```
26
27 Done
28
29 bind lsn group LSN-NAT64-GROUP-1 -poolname LSN-NAT64-POOL-1
30
31 Done
32
33 add ns acl6 NAT64-DFD ALLOW -srcIPv6 = 2001:DB8:5001:: -type DFD -
      dfdhash SIP -dfdprefix 64
34
35 Done
36
37 apply ns acls6 -type DFD
38
39 Done
40 <!--NeedCopy-->
```

Asignación de direcciones y puertos mediante traducción

January 12, 2021

Mapping Address and Port using Translation (MAP-T) es una solución de transición IPv6 para los ISP con infraestructura IPv6 para conectar sus suscriptores IPv4 a la Internet IPv4_.MAP-T se basa en tecnologías de traducción de direcciones IPv4 e IPv6 sin estado. MAP-T es un mecanismo que realiza doble traducción (IPv4 a IPv6 y viceversa) en dispositivos de borde del cliente (CE) y enrutadores de borde (en la red principal del ISP).

En una implementación MAP-T, el dispositivo CE implementa una combinación de traducción NAPT44 con estado y traducción NAT46 sin estado. El dispositivo CE obtiene NAT-IP y el bloque de puertos que se utilizará para la traducción a través de DHCPv6 o cualquier otro método.

Cuando un paquete IPv4 de un dispositivo de suscriptor llega al dispositivo CE, el dispositivo CE realiza NAPT44 y almacena la información de enlace NAPT44. Después de la traducción NAT44, el paquete se somete a la traducción NAT46 y luego se reenvía al dispositivo del router de frontera (BR) ubicado en la red principal del ISP. El dispositivo BR recibe los paquetes IPv6 del dispositivo CE, extrae y valida el NAT-IP y el bloque de puerto incrustados en el encabezado IPv6, y reenvía el paquete IPv4 a Internet IPv4. Cuando BR recibe el paquete IPv4 de Internet, traduce el paquete IPv4 a un paquete IPv6 y envía el paquete IPv6 al dispositivo CE.

MAP-T es sin estado en un dispositivo BR, por lo que no requiere que el dispositivo BR realice NAT en el tráfico. En su lugar, la funcionalidad NAT se delega en los dispositivos CE. Esta funcionalidad de delegación y sin estado en dispositivos BR permite que la implementación de BR se escale en proporción

al volumen de tráfico.

El dispositivo Citrix ADC implementa la funcionalidad BR de una solución MAP-T como se describe en RFC 7599.

Configuración de MAP-T

La configuración de MAP-T en un dispositivo Citrix ADC consta de las siguientes tareas:

- Agregar una regla de asignación predeterminada
- Agregar una regla de asignación básica
- Vincular un rango de direcciones NAT IPv4 de dispositivos CE a una regla de asignación básica
- Agregar un dominio de mapa y enlazar una regla de asignación básica y una regla de asignación predeterminada al dominio

Para agregar una regla de asignación predeterminada mediante la CLI

En el símbolo del sistema, escriba:

```
add MapDmr <name> -BRIpv6Prefix ( <ipv6_addr> | <*> )

show MapDmr <name>
<!--NeedCopy-->
```

Para agregar una regla de asignación básica mediante la CLI

En el símbolo del sistema, escriba:

```
add MapBmr <name> -RuleIpv6Prefix <ipv6_addr> | <*>  [-psidoffset <
    positive_integer>] [-EAbitLength <positive_integer>]  [-psidlength <
    positive_integer>]

show MapBmr <name>
<!--NeedCopy-->
```

Para enlazar el intervalo de direcciones NAT IPv4 de dispositivos CE a una regla de asignación básica mediante la CLI

En el símbolo del sistema, escriba:


```
bind MapBmr <name> (-network <ip_addr>  [-netmask <netmask>])

show MapBmr <name>
<!--NeedCopy-->
```

Para agregar un dominio de mapa mediante la CLI

En el símbolo del sistema, escriba:

```
add MapDomain <name> -MapDmrName <string>

show MapDomain <name>
<!--NeedCopy-->
```

Para enlazar una regla de asignación básica a un dominio de mapa mediante la CLI

En el símbolo del sistema, escriba:

```
bind MapDomain <name> -MapBmrName <string>

show MapDomain <name>
<!--NeedCopy-->
```

Configuración de ejemplo

```
add mapdmr DMR-1 -BRIpv6Prefix 2002:db8::/64

Done

add mapbmr BMR-1 -ruleIpv6Prefix 2002:db8:89ab::/48 -eAbitLength 16 -
    psidlength 8 -psidoffset 6

Done

bind mapbmr BMR-1 -network 192.0.1.0 -netmask 255.255.255.0

```



```
Done

add MapDomain MAP-DOMAIN-1 -mapdmrname DMR-1

Done

bind MapDomain MAP-DOMAIN-1 -mapbmrname BMR-1
Done
<!--NeedCopy-->
```

Gestión de suscriptores de telecomunicaciones

August 20, 2021

El número de suscriptores de una red de telecomunicaciones está aumentando a un ritmo sin precedentes, y su gestión se está convirtiendo en un reto para los proveedores de servicios. Los dispositivos más nuevos, más rápidos e inteligentes están poniendo una gran demanda en la red y en los sistemas de gestión de suscriptores. Ya no es factible proporcionar a cada suscriptor el mismo nivel de servicio, y la necesidad de procesar el tráfico en base a cada suscriptor es imperiosa.

El dispositivo Citrix ADC proporciona inteligencia para perfilar a los suscriptores en función de la información almacenada en la Función de reglas de carga y directivas (PCRF). Cuando un suscriptor móvil se conecta a Internet, la Gateway de paquetes asocia una dirección IP con el suscriptor y reenvía el paquete de datos al dispositivo. El dispositivo recibe la información del suscriptor dinámicamente o puede configurar suscriptores estáticos. Esta información permite al dispositivo aplicar sus capacidades de administración de tráfico enriquecidas, como la conmutación de contenido, el almacenamiento en caché integrado, la reescritura y el respondedor, por suscriptor para administrar el tráfico.

Antes de configurar el dispositivo Citrix ADC para administrar suscriptores, debe asignar memoria al módulo que almacena las sesiones de suscriptor. Para los suscriptores dinámicos, debe configurar una interfaz a través de la cual el dispositivo reciba información de sesión. Los suscriptores estáticos deben tener identificadores asignados, y puede asociarlos con directivas.

También puede hacer lo siguiente:

- Aplicación y gestión de directivas de suscriptor.
- Configure el dispositivo para que identifique de forma única a un suscriptor mediante solo el prefijo IPv6 en lugar de la dirección IPv6 completa.
- Use directivas para optimizar el tráfico TCP para suscriptores dinámicos y estáticos. Estas directivas asocian diferentes perfiles TCP con diferentes tipos de usuarios.
- Administrar sesiones inactivas en un dispositivo Citrix ADC.

- Habilitar el registro en un servidor de registro.
- Elimine las sesiones LSN para las sesiones de suscriptor eliminadas.

Asignación de memoria para el módulo de almacenamiento de sesión de suscriptor

Cada entrada de sesión de suscriptor consume 1 KB de memoria. Almacenar 500.000 sesiones de suscriptor en cualquier momento requiere 500 MB de memoria. Este valor debe agregarse al requisito mínimo de memoria, que se muestra como parte de la salida del comando “show extendedmemoryparam”. En el ejemplo siguiente, el resultado es para una instancia de Citrix ADC VPX con 3 motores de paquetes y 8 GB de memoria.

Para almacenar 500.000 sesiones de suscriptor en este dispositivo, la memoria configurada debe ser 2058+500 MB (500.000 x 1 KB = 500 MB).

> **Nota**
>
> La memoria configurada debe estar en múltiplos de 2 MB y no debe exceder el límite máximo de uso de memoria. El dispositivo debe reiniciarse para que los cambios surtan efecto.

Ejemplo

```
show extendedmemoryparam
       Extended Memory Global Configuration. This memory is utilized by
           LSN and Subscriber Session Store Modules:
        Active Memory Usage: 0 MBytes
        Configured Memory Limit: 0 MBytes
        Minimum Memory Required: 2058 MBytes
        Maximum Memory Usage Limit: 2606 MBytes
    Done
    set extendedmemoryparam -memLimit 2558
    Done
    show extendedmemoryparam
            Extended Memory Global Configuration. This memory is
               utilized by LSN and Subscriber Session Store Modules:

            Active Memory Usage: 2558 MBytes
            Configured Memory Limit: 2558 MBytes
            Minimum Memory Required: 2058 MBytes
            Maximum Memory Usage Limit: 2606 MBytes
    Done
<!--NeedCopy-->
```


Configurar una interfaz para suscriptores dinámicos

El dispositivo Citrix ADC recibe dinámicamente la información del suscriptor a través de cualquiera de los siguientes tipos de interfaz:

- Interfaz Gx
- Interfaz RADIUS
- Interfaz RADIUS y Gx

> **Nota**
>
> - A partir de NetScaler versión 12.0, compilación 57.19, la interfaz de Gx es compatible con una implementación de clúster. Para obtener más información, consulte Interfaz Gx en una topología de clúster.
> - En una configuración de alta disponibilidad, las sesiones de suscriptor se sincronizan continuamente en el nodo secundario. En caso de una conmutación por error, la información del suscriptor sigue estando disponible en el nodo secundario.

Interfaz Gx

Una interfaz Gx (como se especifica en 3GPP 29.212) es una interfaz estándar basada en el protocolo Diameter que permite el intercambio de reglas de control de directivas y carga entre un PCRF y una entidad de la Función de Aplicación de Directivas y Carga (PCEF) en una red de telecomunicaciones.

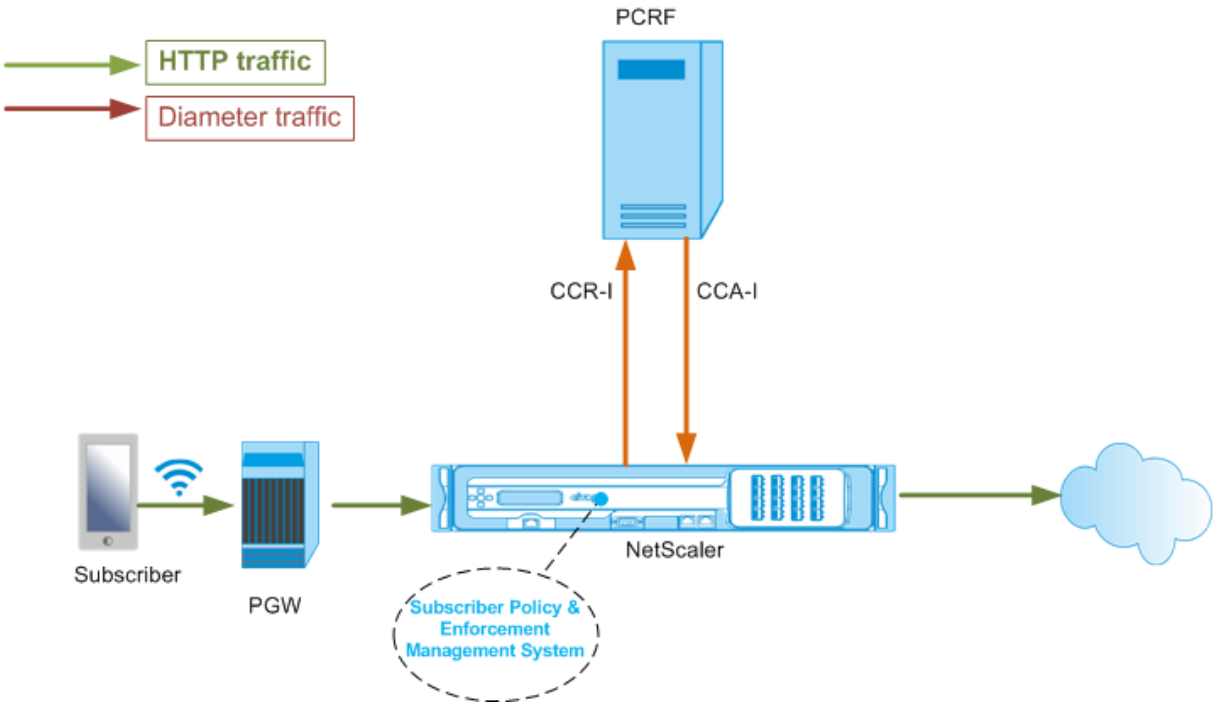
Cuando se establece una sesión IP-CAN, la Gateway de paquetes reenvía el ID del suscriptor, como el MSISDN, y la información de dirección IP enmarcado sobre el suscriptor al PCRF como mensaje Diameter. Cuando el paquete de datos llega al dispositivo desde la Gateway de paquetes (PGW), el dispositivo utiliza la dirección IP del suscriptor para consultar el PCRF para obtener la información del suscriptor. Esto también se conoce como funcionalidad PCEF secundaria.

Las reglas de directiva y control de carga (PCC) recibidas por el dispositivo a través de la interfaz Gx se almacenan en el dispositivo durante la sesión del suscriptor, es decir, hasta que el PCRF envía un mensaje de solicitud de reautenticación (RAR) con un AVP de causa de lanzamiento de sesión o la sesión del suscriptor finaliza desde la CLI o desde el utilidad de configuración. Si hay actualizaciones para un suscriptor existente, el PCRF envía las actualizaciones en un mensaje RAR. Una sesión de suscriptor se inicia cuando un suscriptor inicia sesión en la red y finaliza cuando el suscriptor cierra la sesión.

> **Nota**: Si el servidor PCRF está inactivo, el dispositivo Citrix ADC crea sesiones negativas para las solicitudes de suscriptor Gx pendientes o entrantes. Cuando el servidor PCRF vuelve a realizar una copia de seguridad, el dispositivo Citrix ADC evita una tormenta de solicitudes al esperar a que caduquen las sesiones negativas antes de realizar las solicitudes de suscriptor específicas.

La siguiente ilustración muestra el flujo de tráfico de alto nivel. Se supone que el tráfico del plano de datos es HTTP. El dispositivo envía una solicitud de control de crédito (CCR) a través de una interfaz

Gx al servidor PCRF y, en la respuesta de control de crédito (CCA), recibe las reglas PCC y, opcionalmente, otra información, como el tipo Tecnología de acceso de radio (RAT), que se aplica al suscriptor concreto. Las reglas PCC incluyen uno o más nombres de directivas (reglas) y otros parámetros. El dispositivo utiliza esta información para recuperar las reglas predefinidas almacenadas en el dispositivo y para dirigir el flujo de tráfico. También almacena esta información en el sistema de administración de directivas de suscriptor y cumplimiento durante la sesión de suscriptor. Una vez finalizada una sesión de suscriptor, el dispositivo descarta toda la información sobre el suscriptor.



El siguiente ejemplo muestra los comandos para configurar una interfaz Gx. Los comandos están en negrita.

Para configurar una interfaz Gx, realice las siguientes tareas

Agregue un servicio DIAMETER para cada interfaz Gx. Por ejemplo:

```
1 add service pcrf-svc1 203.0.113.1 DIAMETER 3868
2
3 add service pcrf-svc2 203.0.113.2 DIAMETER 3868
4 <!--NeedCopy-->
```

Agregue un servidor virtual de equilibrio de carga DIAMETER no direccionable y vincule los servicios creados en el paso 1 a este servidor virtual. Para más de un servicio, especifique PersistenceType y PersistaVPno para que las sesiones específicas sean manejadas por el mismo servidor PCRF. Por ejemplo:


```
add lb vserver vdiam DIAMETER 0.0.0.0 0 -persistenceType DIAMETER -
    persistAVPno 263

bind lb vserver vdiam pcrf-svc1

bind lb vserver vdiam pcrf-svc2
<!--NeedCopy-->
```

Configure la identidad y el dominio del diameter Citrix ADC. La identidad y el dominio se utilizan como AVP origin-Host y origin-Realm en los mensajes de diameter enviados por el cliente Gx. Por ejemplo:

```
set ns diameter  - identity netscaler.com  - realm com
<!--NeedCopy-->
```

Configure la interfaz Gx para utilizar el servidor virtual creado en el paso 2 como servidor virtual PCRF. Especifique el dominio PCRF que se utilizará como AVP Destination-Realm en los mensajes de diameters enviados por el cliente Gx. Por ejemplo:

```
set subscriber gxInterface -vServer vdiam -pcrfRealm pcrf.com
<!--NeedCopy-->
```

Establezca el tipo de interfaz de suscriptor en GXOnly. Por ejemplo:

```
set subscriber param -interfaceType GxOnly
<!--NeedCopy-->
```

Para ver la configuración y el estado de la interfaz de Gx, escriba:

```
show subscriber gxinterface
<!--NeedCopy-->
```

Ejemplo

```
show subscriber gxinterface
```



```
    Gx Interface parameters:
        PCRF Vserver: vdiam (DOWN)
        Gx Client Identity...:  netscaler1.com
        Gx Client Realm ..........:  com
        PCRF Realm: epc.mnc030.mcc234.3gppnetwork.org
        Hold Packets On Subscriber Absence: YES
        CCR Request Timeout: 4 Seconds
        CCR Request Retry Attempts: 1
        Gx HealthCheck enabled: NO
        Gx HealthCheck TTL : 30 Seconds
        CER Request Timeout: 10 Seconds
        RevalidationTimeout: 30 Seconds
        NegativeTTL: 60 Seconds
        NegativeTTL Limited Success: NO
        Purge SDB on Gx Failure: YES
        ServicePath AVP code: 262099    ServicePath AVP VendorID: 3845
        PCRF Connection State: PCRF is not ready
    Done

<!--NeedCopy-->
```

ARGUMENTOS

vServer

Nombre del servidor virtual de equilibrio de carga o de conmutación de contenido al que se establecen las conexiones Gx. El tipo de servicio del servidor virtual debe ser DIAMETER o SSL_DIAMETER. Este parámetro es mutuamente exclusivo con el parámetro de servicio. Por lo tanto, no puede establecer tanto el servicio como el servidor virtual en la interfaz Gx.

Servicio

Nombre del servicio DIAMETER o SSL_DIAMETER correspondiente a PCRF al que se establece la conexión Gx. Este parámetro es mutuamente exclusivo con el parámetro vserver. Por lo tanto, no puede establecer tanto el servicio como el servidor virtual en la interfaz Gx.

PCRFALM

El ámbito del PCRF al que se va a dirigir el mensaje. Este es el dominio utilizado en Destination-Realm AVP por el cliente Citrix ADC Gx (como nodo Diameter).

holdOnSubscriberAbsence

Establezca en Sí para retener los paquetes hasta que se obtenga la información de la sesión del suscriptor del servidor PCRF. Si se establece en No, se aplica el perfil de suscriptor predeterminado hasta que se obtenga la información de la sesión del suscriptor del servidor PCRF. Si no se configura un perfil de suscriptor predeterminado, se genera un UNDEF para las expresiones que utilizan atributos de suscriptor.

RequestTimeout

Tiempo, en segundos, dentro del cual debe completarse la solicitud Gx CCR. Si la solicitud no se completa en este tiempo, la solicitud se vuelve a transmitir por el número de veces especificado en el parámetro RequestTryAttempts. Si la solicitud no se completa incluso después de retransmitir, entonces el perfil de suscriptor predeterminado se aplica a este suscriptor. Si no se configura un perfil de suscriptor predeterminado, se genera un UNDEF para las expresiones que utilizan atributos de suscriptor. Zero inhabilita el tiempo de espera. Valor predeterminado: 10

requestRetryAttempts

Especifique el número de veces que debe retransmitirse una solicitud si la solicitud no se completa dentro del valor especificado en el parámetro RequestTimeout. Valor predeterminado: 3.

healthCheck

Establezca en Sí para habilitar la comprobación de estado en línea del par Gx. Cuando está habilitado, Citrix ADC envía paquetes DWR al servidor PCRF. Cuando la sesión Gx está inactiva, el temporizador HealthCheck caduca y se inician los paquetes DWR para comprobar si el servidor PCRF está activo. Valor predeterminado: No.
Nota: Este parámetro es compatible con Citrix ADC 12.1, compilación 51.xx y versiones posteriores.

healthCheckTTL

Tiempo en segundos definido para la supervisión del guardián. Después de que expire el tiempo TTL de comprobación de estado, se envía DWR para comprobar el estado del servidor PCRF. Cualquier mensaje CCR, CCA, RAR o RAA restablece el temporizador.
Valor mínimo: 6 segundos. Valor predeterminado: 30 segundos.
Nota: Este parámetro es compatible con Citrix ADC 12.1, compilación 51.xx y versiones posteriores.

CerRequestTimeout

Tiempo en segundos definido para la retransmisión de la solicitud de intercambio de capacidades. Citrix ADC inicia un nuevo mensaje CER si no recibe un CEA del PCRF en este tiempo configurado.

Si no se recibe respuesta del servidor PCRF, el dispositivo intenta enviar el mensaje CER 5 veces. Si no hay respuesta incluso después de 5 mensajes CER, el dispositivo cierra la conexión TCP e informa de un error. Si el valor de tiempo de espera se establece en 0, la función de comprobación de estado de la aplicación está inhabilitada.
Valor mínimo: 0 segundos. Valor predeterminado: 0 segundos.
Nota: Este parámetro es compatible con Citrix ADC 12.1, compilación 51.xx y versiones posteriores.

RevalidationTimeout

Tiempo, en segundos, después del cual la solicitud Gx CCR-U se envía después de cualquier actividad PCRF en una sesión. Cualquier mensaje RAR o CCA restablece el temporizador. El valor cero inhabilita el tiempo de espera inactivo.

negativeTTL

Tiempo, en segundos, después del cual se reenvía la solicitud Gx CCR-I para sesiones que no han sido resueltas por PCRF porque el servidor está inactivo o no hay respuesta o se recibe una respuesta fallida. En lugar de sondear constantemente el servidor PCRF, un TTL negativo hace que el dispositivo se mantenga en una sesión no resuelta. En el caso de las sesiones negativas, el dispositivo hereda los atributos del perfil de suscriptor predeterminado, si se configura uno, y del mensaje de contabilidad RADIUS, si se recibe uno. El valor cero inhabilita las sesiones negativas. El dispositivo no instala sesiones negativas aunque no se haya podido obtener una sesión de suscriptor. Valor predeterminado: 600

negativeTTLLimitedSuccess

Establezca en Sí para crear sesión negativa para el código de respuesta parcial de éxito (2002). Si se establece en No, se creará una sesión regular. Valor predeterminado: No.

Este parámetro es compatible con Citrix ADC 12.1, compilación 49.xx y versiones posteriores.

purgeSDBonGxFailure

Establezca en Sí para vaciar la base de datos del suscriptor cuando se produzca un error en la interfaz de Gx. El error de la interfaz Gx incluye tanto la supervisión DWR (si está activada) como la comprobación de estado de la red (si está activada). Cuando se establece en Sí, se borran todas las sesiones del suscriptor.
Valor predeterminado: No.
Nota: Este parámetro es compatible con Citrix ADC 12.1, compilación 51.xx y versiones posteriores.

ServicePathAVP

El código AVP en el que PCRF envía la ruta de servicio aplicable a un suscriptor.

ServicePathVendorid

Id. de proveedor del AVP en el que PCRF envía la ruta de servicio aplicable a un suscriptor.

Para configurar la interfaz Gx mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico** > **Suscriptor** > **Parámetros**.
2. Haga clic en **Configurar parámetros de suscriptor**.
3. En Tipo de interfaz, seleccione **GXOnly**.
4. Especifique los valores para todos los parámetros necesarios.
5. Haga clic en **Aceptar**.

Detectar fallos de transporte sobre conexiones Gx establecidas

Nota: Esta función es compatible con Citrix ADC 12.1, compilación 51.xx y versiones posteriores.

Un dispositivo Citrix ADC se puede configurar para detectar errores de transporte en conexiones Gx establecidas mediante mensajes de solicitud de control de dispositivos (DWR) y de respuesta de control de dispositivos (DWA).

Después de establecer una sesión Gx, se activa un temporizador predefinido para detectar si una sesión está inactiva. Se envía un mensaje DWR después de que expire el temporizador de tiempo de inactividad. El temporizador de tiempo de inactividad se restablece cada vez que el dispositivo Citrix ADC recibe un mensaje a través de una sesión Gx establecida. La disponibilidad del par se confirma en función del mensaje DWA después de enviar un mensaje DWR.

- Si se recibe el DWA, se confirma la disponibilidad de un par y se restablece el temporizador de vigilancia.
- Si no se recibe el DWA y el temporizador de vigilancia caduca dos veces consecutivamente, la sesión se considera inactiva y no está disponible del mismo nivel. El dispositivo cierra la sesión e intenta establecer una nueva sesión con el par Gx.

Cuando el temporizador de vigilancia caduca dos veces sin respuesta, el dispositivo Citrix ADC considera que la conexión Gx es defectuosa e inicia un cierre de conexión. Una vez cerrada la conexión, no se envía ninguna otra solicitud de control al par Gx. El dispositivo Citrix ADC utiliza la siguiente sesión de Gx disponible para cualquier solicitud PCRF.

Para detectar fallos de transporte sobre conexiones Gx establecidas mediante la CLI

En el símbolo del sistema, escriba:


```
set subscriber gxInterface [-vServer <string>] [-service <string>] [-
    healthCheck ( YES | NO )] [-healthCheckTTL<positive_integer>][-
    cerRequestTimeout <positive_integer>] [-purgeSDBonGxFailure ( YES |
    NO )]
<!--NeedCopy-->
```

Ejemplo:

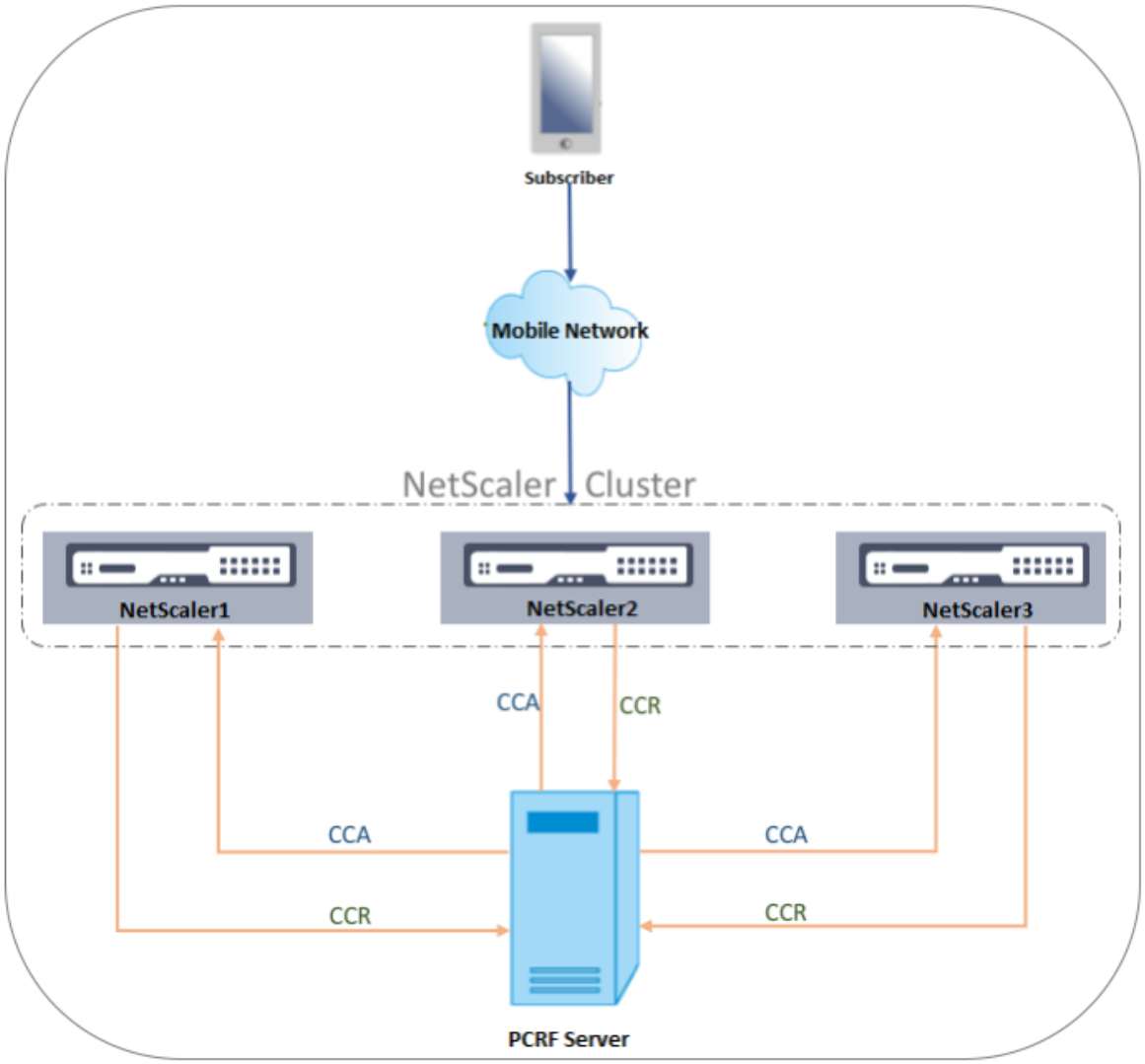
```
set subscriber gxInterface set subscriber gxInterface -vServer vdiam -
    healthCheck YES -healthCheckTTL 31 -cerRequestTimeout 15
    purgeSDBonGxFailure  YES
<!--NeedCopy-->
```

Para detectar fallos de transporte sobre conexiones Gx establecidas mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico** > **Suscriptor** > **Parámetros**.
2. Haga clic en **Configurar parámetros de suscriptor**.
3. En **Tipo de interfaz**, seleccione **GxOnly**.
4. Especifique los valores para todos los parámetros necesarios.
5. Seleccione **Comprobación de estado** y especifique valores para **TTL de comprobación** de estado y tiempo de **espera de solicitud CER**.
6. Haga clic en **Aceptar**.

Interfaz Gx en una topología de clúster

El dispositivo Citrix ADC admite la interfaz Gx en una topología de clúster.



Los nodos Citrix ADC en el clúster se comunican con un servidor PCRF externo a través de la interfaz Gx. Cuando un nodo recibe tráfico de cliente, el dispositivo realiza lo siguiente:

- Envía una solicitud CCR-I al servidor PCRF para obtener información del suscriptor.
- El servidor PCRF responde con un CCR-A.
- A continuación, el nodo Citrix ADC almacena la información del suscriptor recibido en su almacén de suscriptores y aplica las reglas al tráfico del cliente.

Cada nodo mantiene un almacén de suscriptor independiente y las sesiones de suscriptor no se sincronizan con otros nodos.

Según el protocolo de base de diámetro RFC 6733, cada par debe configurarse con una identidad de diámetro única para comunicarse con otros pares a través del protocolo de diámetro. Por lo tanto, en una implementación de clúster, se detecta la configuración de la identidad del diameter. Los parámetros de diámetro (identidad, dominio, propagación de cierre del servidor) para cada nodo se pueden configurar individualmente mediante la GUI o la CLI.

Cuando se agrega un nodo a un clúster, asume los parámetros de diameter predeterminados (identity=netscaler.com, realm=com, serverClosePropaogation=No). Después de agregar los nodos, se deben configurar los parámetros de diameter para cada nodo.

Para configurar los parámetros de diameter mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **Configuración**.
2. En el panel de detalles, haga clic en **Cambiar parámetros de diámetro**.
3. En la página Parámetros de diameter, seleccione el nodo Citrix ADC para el que quiere configurar los parámetros de diameter y, a continuación, haga clic en **Configurar**.
4. En la página Configurar parámetros de diámetro, configure la identidad de diámetro, el dominio de diámetro y la propagación de cierre del servidor para el nodo seleccionado.
5. Haga clic en **Aceptar**.

Para configurar los parámetros de diameter mediante la CLI

En el símbolo del sistema, escriba:

```
set ns diameter [-identity <string>] [-ownerNode <positive_integer>]
<!--NeedCopy-->
```

ARGUMENTOS

Identidad

Identidad de diameter se utiliza para identificar un nodo de diameter de forma única. Antes de configurar la configuración del diameter, se debe asignar al dispositivo Citrix ADC (como nodo Diameter) una identidad de diameter única.

Por ejemplo, establezca ns diameter -identity netscaler.com -ownerNode 1. Por lo tanto, siempre que el sistema Citrix ADC necesite usar la identidad en mensajes de diámetro, utiliza 'netscaler.com' como Origin-Host AVP tal como se define en RFC3588.

Longitud máxima: 255

OwnerNode

OwnerNode representa el identificador del nodo de clúster para el que se establece el identificador de diameter. OwnerNode solo se puede configurar a través de CLIP.

Valor mínimo: 0

Valor máximo: 31

Ejemplo:

set ns diámetro -identity netscaler1.com -OwnerNode 1

Nota:

La opción OwnerNode también se agrega al comando show ns diameter.

Ejemplo:

```
show diameter -ownerNode <0-31>
<!--NeedCopy-->
```

Cuando se ejecuta el comando show ns diameter, muestra los parámetros de diameter para un nodo determinado.

Para configurar una interfaz Gx para la implementación de clústeres

Para configurar una interfaz Gx, realice las siguientes tareas:

Agregue un servicio DIAMETER para cada interfaz Gx.

Ejemplo:

```
add service pcrf-svc1 203.0.113.1 DIAMETER 3868
add service pcrf-svc2 203.0.113.2 DIAMETER 3868
<!--NeedCopy-->
```

Agregue un servidor virtual de equilibrio de carga DIAMETER y vincule los servicios creados en el paso 1 a este servidor virtual.

Ejemplo:

```
add lb vserver vdiam DIAMETER 0.0.0.0 0 -persistenceType DIAMETER -
    persistAVPno 263

bind lb vserver vdiam pcrf-svc1

bind lb vserver vdiam pcrf-svc2
<!--NeedCopy-->
```


Configure la identidad y el dominio del diameter Citrix ADC en todos los nodos del clúster. La identidad y el dominio se utilizan como AVP origin-Host y origin-Realm en los mensajes de diameter enviados por el cliente Gx.

Ejemplo:

```
set ns diameter -identity node0.netscaler.com -realm netscaler.com -
    ownerNode 0

set ns diameter -identity node1.netscaler.com -realm netscaler.com -
    ownerNode 1
<!--NeedCopy-->
```

Configure la interfaz Gx para utilizar el servidor virtual creado en el paso 2 como servidor virtual PCRF y establezca también el dominio PCRF.

Ejemplo:

```
set subscriber gxInterface -vServer vdiam -pcrfRealm pcrf.com

Set the subscriber interface type to GxOnly.
<!--NeedCopy-->
```

Ejemplo:

```
set subscriber param -interfaceType GxOnly
<!--NeedCopy-->
```

Para ver la configuración y el estado de la interfaz de Gx, escriba:

```
show subscriber gxinterface
<!--NeedCopy-->
```

Interfaz RADIUS

Con una interfaz RADIUS, la Gateway de paquetes reenvía la información del suscriptor en un mensaje de inicio de cuentas RADIUS al dispositivo a través de la interfaz RADIUS cuando se establece una sesión IP-CAN. Un servicio de tipo RadiusListener procesa los mensajes de RADIUS Accounting.

Agregue un secreto compartido para el cliente RADIUS. Si no se configura un secreto compartido, el mensaje RADIUS se elimina silenciosamente. En el ejemplo siguiente se muestran los comandos para configurar una interfaz RADIUS. Los comandos están en negrita.

Para configurar una interfaz RADIUS, realice las siguientes tareas:

Cree un servicio de escucha RADIUS en la dirección SNIP donde se reciben los mensajes RADIUS. Por ejemplo:

```
1 add service srad1 192.0.0.206 RADIUSLISTENER 1813
2 <!--NeedCopy-->
```

Configure la interfaz RADIUS del suscriptor para utilizar este servicio. Por ejemplo:

```
1 set subscriber radiusInterface -listeningService srad1
2 <!--NeedCopy-->
```

Establezca el tipo de interfaz del suscriptor en RadiusOnly. Por ejemplo:

```
1 set subscriber param -interfaceType RadiusOnly
2 <!--NeedCopy-->
```

Agregue un cliente RADIUS especificando una subred y un secreto compartido. Por ejemplo:

```
1 add radius client 192.0.2.0/24 -radkey client123
2 <!--NeedCopy-->
```

Una subred de 0.0.0.0/0 implica que es el secreto compartido predeterminado para todos los clientes. Para ver la configuración y el estado de la interfaz RADIUS, escriba:

```
1 show subscriber radiusInterface
2 <!--NeedCopy-->
```

Parámetros de interfaz RADIUS:

Servicio de escucha de radio: Srad1 (UP)

Completado

Ejemplo:

```
add service pcrf-svc1 203.0.113.1 DIAMETER 3868

add service pcrf-svc2 203.0.113.2 DIAMETER 3868
<!--NeedCopy-->
```

ARGUMENTOS

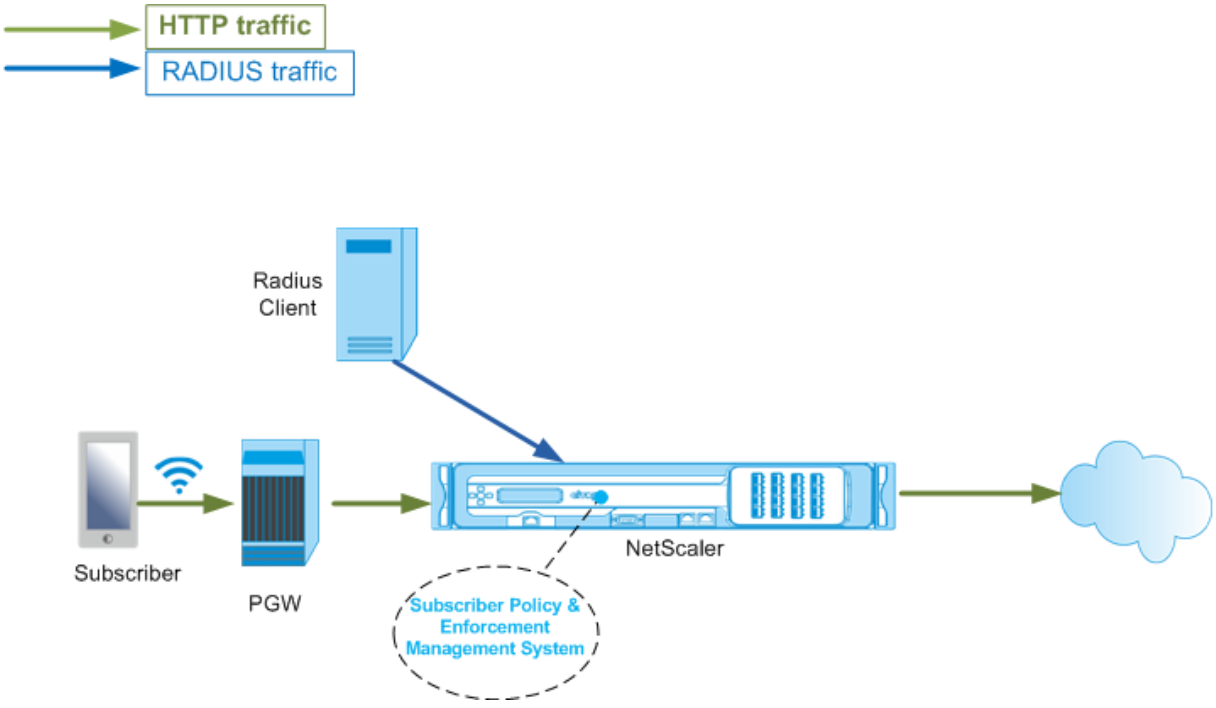
Servicio de escucha

Nombre del servicio de escucha RADIUS que procesa las solicitudes de contabilidad RADIUS.

SVRState

El estado del servicio de escucha RADIUS.

La siguiente ilustración muestra el flujo de tráfico de alto nivel.



Para configurar la interfaz RadiusOnly mediante la interfaz GUI

1. Vaya a **Administración del tráfico** > **Suscriptor** > **Parámetros**.
2. Haga clic en **Configurar parámetros de suscriptor**.

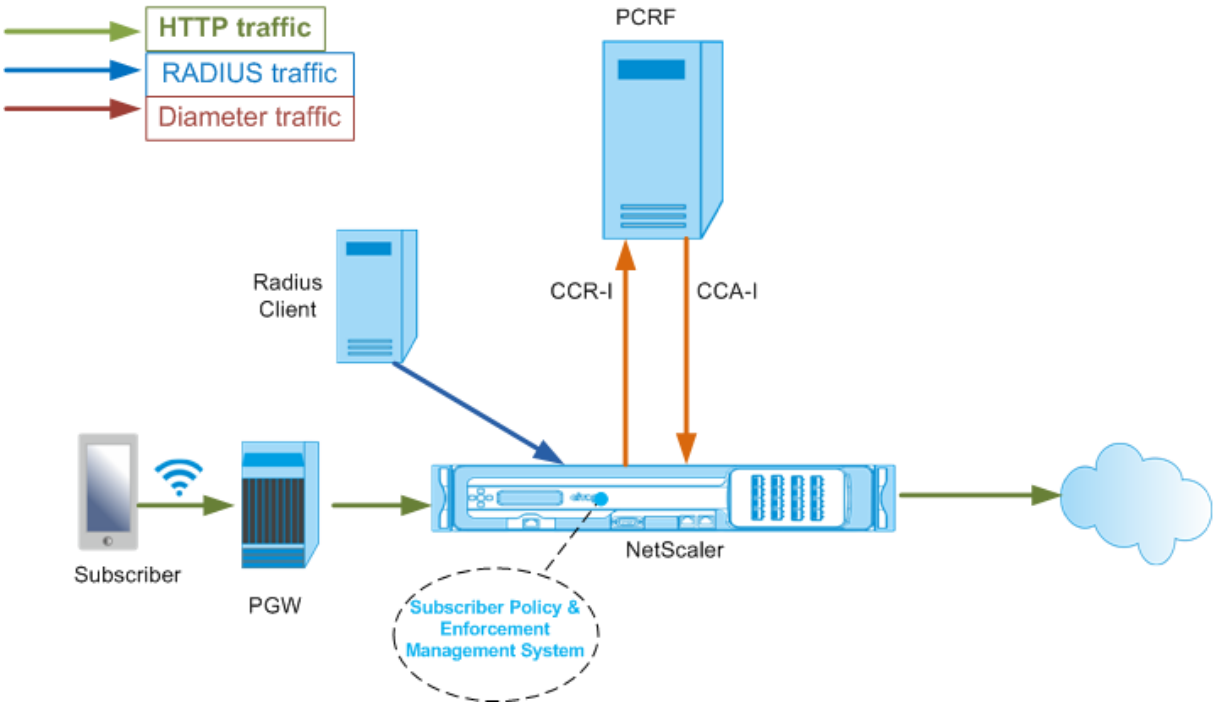
3. En Tipo de interfaz, seleccione **RadiusOnly**.
4. Especifique los valores para todos los parámetros necesarios.
5. Haga clic en **Aceptar**.

Interfaz RADIUS y Gx

Con una interfaz RADIUS y Gx, cuando se establece una sesión IP-CAN, la Gateway de paquetes reenvía el ID del suscriptor, como MSISDN, y la información de dirección IP tramed-IP del suscriptor al dispositivo a través de la interfaz RADIUS. El dispositivo utiliza este ID de suscriptor para consultar el PCRF en la interfaz de Gx para obtener la información del suscriptor. Esto se conoce como funcionalidad primaria de PCEF. En el ejemplo siguiente se muestran los comandos para configurar una interfaz RADIUS y Gx.

```
1 set subscriber param -interfaceType RadiusandGx
2 add service pcrf-svc 203.0.113.1 DIAMETER 3868
3 add lb vserver vdiam DIAMETER 0.0.0.0 0 -persistenceType DIAMETER -
     persistAVPno 263
4 bind lb vserver vdiam pcrf-svc
5 set subscriber gxInterface -vServer vdiam -pcrfRealm testrealm1.net -
     holdOnSubscriberAbsence YES -revalidationTimeout 60 -negativeTTL 120
6 add service srad1 192.0.0.206 RADIUSLISTENER 1813    set subscriber
     radiusInterface -listeningService srad1
7 <!--NeedCopy-->
```

La siguiente ilustración muestra el flujo de tráfico de alto nivel.



Para configurar la interfaz RadiusAndGX mediante la interfaz GUI

1. Vaya a **Administración del tráfico** > **Suscriptor** > **Parámetros**.
2. Haga clic en **Configurar parámetros de suscriptor**.
3. En Tipo de interfaz, seleccione **RadiusAndGX**.
4. Especifique los valores para todos los parámetros necesarios.
5. Haga clic en **Aceptar**.

Configurar suscriptores estáticos

Puede configurar manualmente los suscriptores en el dispositivo Citrix ADC mediante la línea de comandos o la utilidad de configuración. Para crear suscriptores estáticos, asigne un identificador de suscriptor único y, opcionalmente, asocie una directiva con cada suscriptor. Los siguientes ejemplos muestran los comandos para configurar un suscriptor estático.

En los ejemplos siguientes, **SubscriptionIdValue** especifica el número de teléfono internacional y **SubscriptionIdType** (E164 en este ejemplo) especifica el formato general de los números de teléfono internacionales.

```
1    add subscriber profile 203.0.113.6 -subscriberRules policy1 policy2
         -subscriptionIdType E164 -subscriptionIdvalue 98767543211
```



```
2     add subscriber profile 2002::a66:e8d3/64 -subscriberRules policy1
         policy3 -subscriptionIdtype E164 -subscriptionIdvalue
         98767543212
3     add subscriber profile 203.0.24.2 10 -subscriberRules policy2
         policy3 -subscriptionIdtype E164 -subscriptionIdvalue
         98767543213
4 <!--NeedCopy-->
```

Para ver los perfiles de suscriptor configurados, escriba:

> mostrar perfil de suscriptor

```
1     > show subscriber profile
2
3     1)  Subscriber IP: 203.0.24.2 VLAN:10
4         Profile Attributes:
5                 Active Rules: policy2, policy3
6                 Subscriber Id Type: E164
7                 Subscriber Id Value: 98767543213
8     2)  Subscriber IP: 2002::/64
9         Profile Attributes:
10                Active Rules: policy1, policy3
11                Subscriber Id Type: E164
12                Subscriber Id Value: 98767543212
13    3)  Subscriber IP: 203.0.113.6
14        Profile Attributes:
15                Active Rules: policy1, policy2
16                Subscriber Id Type: E164
17                Subscriber Id Value: 98767543211
18
19     Done
20 <!--NeedCopy-->
```

Perfil de suscriptor predeterminado

Se utiliza un perfil de suscriptor predeterminado si no se encuentra la dirección IP del suscriptor en el almacén de sesión del suscriptor en el dispositivo. En el ejemplo siguiente, se agrega un perfil de suscriptor predeterminado con la directiva de regla de suscriptor1.

```
1     > add subscriber profile * -subscriberRules policy1
2 <!--NeedCopy-->
```


Ver y borrar sesiones de suscriptor

Utilice el siguiente comando para mostrar todas las sesiones de suscriptor estáticas y dinámicas.

> mostrar sesiones de suscriptor

```
    > show subscriber sessions
    1)  Subscriber IP: 2002::/64
        Session Attributes:
                Active Rules: policy1, policy3
                Subscriber Id Type: E164
                Subscriber Id Value: 98767543212
    2)  Subscriber IP: *
        Session Attributes:
                Active Rules: policy1
    3)  Subscriber IP: 203.0.24.2 VLAN:10
        Session Attributes:
                Active Rules: policy2, policy3
                Subscriber Id Type: E164
                Subscriber Id Value: 98767543213
    4)  Subscriber IP: 203.0.113.6
        Session Attributes:
                Active Rules: policy1, policy2
                Subscriber Id Type: E164
                Subscriber Id Value: 98767543211
    5)  Subscriber IP: 192.168.0.11
        Session Attributes:
                Idle TTL remaining: 361 Seconds
                Active Rules: policy1
                Subscriber Id Type: E164
                Subscriber Id Value: 1234567811
                Service Path: policy1
                AVP(44): 34 44 32 42 42 38 41 43  2D 30 30 30 30 30 30
                   31 31
                AVP(257): 00 01 C0 A8 0A 02
                PCRF-Host: host.pcrf.com
                AVP(280): 74 65 73 74 2E 63 6F 6D

    Done
<!--NeedCopy-->
```

Utilice el siguiente comando para borrar una sola sesión o el almacén de sesiones completo. Si no especifica una dirección IP, se borra el almacén completo de sesión del suscriptor.


```
clear subscriber sessions <ip>
<!--NeedCopy-->
```

Sistema de gestión y aplicación de directivas de suscriptor

El dispositivo Citrix ADC utiliza la dirección IP del suscriptor como clave para el sistema de administración y aplicación de directivas del suscriptor.

Puede agregar expresiones de suscriptor para leer la información de suscriptor disponible en el Sistema de administración y cumplimiento de directivas de suscriptor. Estas expresiones se pueden utilizar con las reglas y acciones de directivas configuradas para las funciones de Citrix ADC, como el almacenamiento en caché integrado, la reescritura, el respondedor y la conmutación de contenido.

Los siguientes comandos son un ejemplo de cómo agregar una acción y una directiva de respuesta basada en suscriptores. La directiva se evalúa como true si el valor de la regla de suscriptor es “pol1”.

```
    add responder action error_msg respondwith '"HTTP/1.1 403 OKrnrn" +
        " You are  not authorized to access Internet"'
    add responder policy no_internet_access "SUBSCRIBER.RULE_ACTIVE("
       pol1")" error_msg
<!--NeedCopy-->
```

En el ejemplo siguiente se muestran los comandos para agregar una acción y una directiva de reescritura basada en suscriptores. La acción inserta un encabezado HTTP “X-Nokia-MSISDN” mediante el valor de AVP (45) en la sesión de suscriptor.

```
    > add rewrite action AddHDR-act insert_http_header X-Nokia-MSISDN "
       SUBSCRIBER.AVP(45).VALUE"
    > add rewrite policy AddHDR-pol "HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.
       URL).EQUALS_ANY("patset-test")" AddHDR-act
<!--NeedCopy-->
```

En el ejemplo siguiente, se configuran dos directivas en el dispositivo. Cuando el dispositivo comprueba la información del suscriptor y la regla del suscriptor es cache_enable, realiza el almacenamiento en caché. Si la regla de suscriptor es cache_disable, el dispositivo no realiza el almacenamiento en caché.


```
1      > add cache policy nocachepol -rule "SUBSCRIBER.RULE_ACTIVE("
          cache_disable")" - action NOCACHE
2      > add cache policy cachepol -rule "SUBSCRIBER.RULE_ACTIVE("
          cache_enable")" - action CACHE -storeInGroup cg1
3  <!--NeedCopy-->
```

Para obtener una lista completa de expresiones que empiecen por "SUSCRIPTOR", consulte la Guía de configuración de directivas.

> **Importante**
>
> La versión 12.1 del software Citrix ADC admite el método de búsqueda de claves IPANDVLAN cuando la interfaz del suscriptor está establecida en GXOnly. Para obtener más información, consulte Método de búsqueda de claves de ID de VLAN y dirección IP.

Sesiones de suscriptor basadas en prefijos IPv6

Un usuario de telecomunicaciones se identifica por el prefijo IPv6 en lugar de por la dirección IPv6 completa. El dispositivo Citrix ADC ahora utiliza el prefijo en lugar de la dirección IPv6 completa (/128) para identificar a un suscriptor en la base de datos (almacén de suscriptores). Para comunicarse con el servidor PCRF (por ejemplo, en un mensaje CCR-I), el dispositivo utiliza ahora el AVP con prefijo IPv6-frame en lugar de la dirección IPv6 completa. La longitud predeterminada del prefijo es /64, pero puede configurar el dispositivo para que utilice un valor diferente.

Para configurar el prefijo IPv6 mediante la línea de comandos

```
set subscriber param [-ipv6PrefixLookupList <positive_integer> ...]
```

El primer comando de ejemplo a continuación establece un único prefijo y el segundo comando de ejemplo establece varios prefijos.

```
1      set subscriber param -ipv6PrefixLookupList 64
2      set subscriber param -ipv6PrefixLookupList 64 72 96
3  <!--NeedCopy-->
```

Para configurar el prefijo IPv6 mediante la utilidad de configuración

1. Vaya a **Administración del tráfico** > **Suscriptor** > **Parámetros**.
2. En el panel de detalles, en **Configuración**, haga clic en **Configurar parámetros de suscriptor** y, en **Lista de búsqueda de prefijos IPv6**, especifique uno o varios prefijos.

Método de búsqueda de claves de ID de VLAN y dirección IP

El dispositivo Citrix ADC utiliza la dirección IP del suscriptor como método de búsqueda de claves para el sistema de administración y aplicación de directivas de suscriptor. Este método no es efectivo si las direcciones IP se superponen. En tales casos, puede utilizar el ID de VLAN como un tipo de búsqueda de suscriptor adicional. El método de búsqueda de claves IPANDVLAN solo se admite cuando la interfaz del suscriptor está establecida en GXOnly. Cuando IPANDVLAN está configurado como método de búsqueda, el dispositivo Citrix ADC realiza lo siguiente:

- Incluye el ID de VLAN de origen en la consulta Gx para suscriptores IPv4.
- Incluye Gx VLAN AVP en todas las respuestas de Gx. Sin embargo, si hay un ID de VLAN no coincide, el dispositivo ignora las respuestas.

Por ejemplo, si el dispositivo envía un CCR-I con GXSessionID-A:IPV4-B:VLAN-C y la respuesta contiene GXSessionID-A:IPV4-B:VLAN-D, se elimina la respuesta y se crea una entrada de suscriptor predeterminada.

> **Nota**
>
> - El tipo de interfaz RadiusAndGX y RadiusOnly no se pueden configurar junto con el tipo de clave IPANDVLAN.
> - Si el tráfico proviene de una dirección IPv6, el dispositivo Citrix ADC utiliza el método de búsqueda IP.

Para configurar IP o IPANDVLAN como método de búsqueda de claves mediante la CLI

En el símbolo del sistema, escriba:

```
set subscriber param [-keytype ( IP | IPANDVLAN )] [-interfaceType <
   interfaceType>]
<!--NeedCopy-->
```

Ejemplo:

```
set subscriber param -keytype IPANDVLAN -interfaceType GxOnly

set subscriber param -keytype IP -interfaceType GxOnly
<!--NeedCopy-->
```

> **Nota**
>
> Cambiar el parámetro keytype de IP a IPANDVLAN y, por el contrario, borra todos los datos del

> suscriptor.

Parámetro de VLAN

El parámetro VLAN también se agrega para los siguientes comandos.

```
add subscriber profile <ip>@ [-vlan]

set subscriber profile <ip>@ [-vlan] [-subscriptionIdType  <
   subscriptionIdType>]

show subscriber profile [<ip>@] [-vlan]

rm subscriber profile <ip>@ [-vlan <positive_integer>]
<!--NeedCopy-->
```

Argumentos

ip

Representa la dirección IP del suscriptor. Este es un argumento obligatorio y no se puede cambiar después de agregar el perfil de suscriptor.

Vlan

Representa el número de VLAN en el que se encuentra el suscriptor. El número de VLAN no se puede cambiar después de agregar el perfil de suscriptor.

Valor mínimo: 1

Valor máximo: 4096

```
add subscriber profile 192.0.2.23 10

set subscriber profile 192.0.2.23 10 -subscriptionIdtype E164

show subscriber profile 192.0.2.23 10

rm subscriber profile 192.0.2.23 10

<!--NeedCopy-->
```


Para configurar IP o IPANDVLAN como método de búsqueda de claves mediante la interfaz gráfica de usuario

1. Vaya a **Gestión del Tráfico** > **Suscriptor** > **Parámetros.**
2. Haga clic en **Configurar parámetros de suscriptor**.
3. En **Tipo de clave**, seleccione **IP**o **IPANDVLAN** según sus requisitos.
4. Complete la configuración y haga clic en **Aceptar**.

Gestión de sesiones inactivas de sesiones de suscriptor en una red de telecomunicaciones

La limpieza de sesión de suscriptor en un dispositivo Citrix ADC se basa en eventos del plano de control, como un mensaje de detención de cuentas RADIUS, un mensaje RAR de diameter (liberación de sesión) o un comando "borrar sesión de suscriptor". En algunas implementaciones, es posible que los mensajes de un cliente RADIUS o de un servidor PCRF no lleguen al dispositivo. Además, durante el tráfico intenso, es posible que los mensajes se pierdan. Una sesión de suscriptor que está inactiva durante mucho tiempo continúa consumiendo memoria y recursos IP en el dispositivo Citrix ADC. La función de administración de sesiones inactivas proporciona temporizadores configurables para identificar las sesiones inactivas y las limpia en función de la acción especificada.

Una sesión se considera inactiva si no se recibe tráfico de este suscriptor en el plano de datos o en el plano de control. Puede especificar una acción de actualización, finalizar (informar al PCRF y, a continuación, eliminar la sesión) o eliminar (sin informar al PCRF). La acción solo se realiza después de que la sesión esté inactiva durante el tiempo especificado en el parámetro de tiempo de espera inactivo.

Para configurar el tiempo de espera de la sesión inactiva y la acción asociada mediante la línea de comandos

```
set subscriber param [-idleTTL <positive_integer>] [-idleAction <
   idleAction>]
<!--NeedCopy-->
```

Ejemplos:

```
set subscriber param -idleTTL 3600 -idleAction ccrTerminate

set subscriber param -idleTTL 3600 -idleAction ccrUpdate

set subscriber param -idleTTL 3600 -idleAction delete
<!--NeedCopy-->
```


Para inhabilitar el tiempo de espera de la sesión inactiva, establezca el tiempo de espera inactivo en cero.

set subscriber param –idleTTL 0

Para configurar el tiempo de espera de la sesión inactiva y la acción asociada mediante la utilidad de configuración

1. Vaya a **Administración del tráfico** > **Suscriptor** > **Parámetros**.
2. En el panel de detalles, en **Configuración**, haga clic en **Configurar parámetros de suscriptor** y especifique un **tiempo de inactividad** y **acción de inactividad**.

Registro de sucesos de sesión de suscriptor

Si habilita el registro de suscriptores, puede realizar un seguimiento de los mensajes del plano de control RADIUS y Gx específicos de un suscriptor y utilizar los datos históricos para analizar las actividades del suscriptor. Algunos de los atributos clave son MSISDN y marca de tiempo. También se registran los siguientes atributos:

- Evento de sesión (instalación, actualización, eliminación, error)
- Tipo de mensaje Gx (CCR-I, CCR-U, CCR-T, RAR)
- Tipo de mensaje de radio (inicio, parada)
- IP del suscriptor
- Tipo de ID de suscripción (MSISDN (E164), IMSI)
- Valor SubscribId

Mediante estos registros, puede realizar un seguimiento de los usuarios por dirección IP y, si está disponible, MSISDN.

Puede habilitar el registro de sesión de suscriptor en un servidor syslog o nslog local o remoto. El siguiente ejemplo muestra cómo habilitar el registro de suscriptor en un servidor syslog remoto.

```
1     > add syslogAction sysact1 192.0.2.0 -loglevel EMERGENCY ALERT
        CRITICAL ERROR WARNING NOTICE INFORMATIONAL -subscriberlog
        enabled
2  <!--NeedCopy-->
```

A partir de estos registros, puede obtener información sobre cualquier actividad relacionada con un usuario, como la hora en que se actualizó, eliminó o creó una sesión (se instaló). Además, también se registran mensajes de error.

Ejemplos:

1. Las siguientes entradas de registro son ejemplos de creación de sesión de RadiusAndGX, actualización de sesión y eliminación de sesión.

   > 09/30/2015:16:29:18 GMT Informational 0-PPE-0: Default SUBSCRIBER SESSION_EVENT 147 0: Session Install, GX MsgType: CCR-I, RADIUS MsgType: Start, IP: 100.10.1.1, ID: E164: 30000000001
   >
   > 09/30/2015:16:30:18 GMT Informational 0-PPE-0: Default SUBSCRIBER SESSION_EVENT 148 0: Session Update, GX MsgType: CCR-U, IP: 100.10.1.1, ID: E164: 30000000001
   >
   > 09/30/2015:17:27:56 GMT Informational 0-PPE-0: Default SUBSCRIBER SESSION_EVENT 185 0: Session Delete, GX MsgType: CCR-T, RADIUS MsgType: Stop, IP: 100.10.1.1, ID: E164: 30000000001

2. Las siguientes entradas de registro son ejemplos de mensajes de error, como cuando no se encuentra un suscriptor en el servidor PCRF y cuando el dispositivo no puede conectarse al servidor PCRF.

   > 09/30/2015:16:44:15 GMT Error 0-PPE-0: Default SUBSCRIBER SESSION_FAILURE 169 0: Failure Reason: PCRF failure response, GX MsgType: CCR-I, IP: 100.10.1.1
   >
   > Sep 30 13:03:01 09/30/2015:16:49:08 GMT 0-PPE-0: Default SUBSCRIBER SESSION_FAILURE 176 0: Failure Reason: Unable to connect to PCRF, GX MsgType: CCR-I, RADIUS MsgType: Start, IP: 100.10.1.1, ID: E164: 30000000001#000#000#000#000#000#000#000#000#000#000#000#000#0

Finalización de sesión LSN con reconocimiento de suscriptor

En versiones anteriores, si se elimina una sesión de suscriptor cuando se recibe un mensaje STOP de contabilidad RADIUS o PCRF-RAR, o como resultado de cualquier otro evento, como la caducidad o vaciado de TTL, las sesiones LSN correspondientes del suscriptor se quitan solo después del período de tiempo de espera de LSN configurado. Las sesiones LSN que se mantienen abiertas hasta que caduque este tiempo de espera continúan consumiendo recursos en el dispositivo.

Desde la versión 11.1, se agrega un nuevo parámetro (SubscrSessionRemoval). Si este parámetro está habilitado y la información del suscriptor se elimina de la base de datos del suscriptor, también se quitan las sesiones LSN correspondientes a ese suscriptor. Si este parámetro está inhabilitado, las sesiones de suscriptor agotan el tiempo de espera especificado por la configuración de tiempo de espera de LSN.

Para configurar la terminación de sesión LSN con reconocimiento de suscriptor mediante la CLI

En el símbolo del sistema, escriba:


```
set lsn parameter -subscrSessionRemoval (          DISABLED )
ENABLED
```

```
1      > set lsn parameter -subscrSessionRemoval ENABLED
2      Done
3      > sh lsn parameter
4                  LSN Global Configuration:
5
6                  Active Memory Usage: 0 MBytes
7                  Configured Memory Limit: 0 MBytes
8                  Maximum Memory Usage Limit: 912 MBytes
9                  Session synchronization: ENABLED
10                 Subscriber aware session removal: ENABLED
11 <!--NeedCopy-->
```

Para configurar la terminación de sesión LSN con reconocimiento de suscriptor mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **NAT a gran escala**.
2. En **Introducción**, haga clic en **Establecer parámetro LSN**.
3. Defina el **parámetro Eliminación de sesión con reconocimiento del suscriptor**.

Solucionar problemas

Si la implementación no funciona como se esperaba, utilice los siguientes comandos para solucionar problemas:

- show subscriber gxinterface La salida de
  este comando puede incluir los siguientes mensajes de error (mostrados aquí con respuestas sugeridas):
  - Gx Interface Not Configured-Use set subscriber param comando para configurar el tipo de interfaz correcto.
  - PCRF no configurado: Configure un servidor virtual de diameter o servicio en GXInterface use el comando set subscriber gx interface para asignar un servicio o servidor virtual de diameter a esta interfaz.
  - PCRF no está Ready-check correspondiente vserver/service para obtener más detalles: Use el comando show LB vserver o show service para comprobar el estado del servicio.

  - Citrix ADC está esperando que el CEA de la negociación de la capacidad de PCRF entre el PCRF y el Citrix ADC podría estar fallando. Esto podría ser un estado intermitente. Si persiste, compruebe la configuración DIAMETER en su servidor PCRF.
  - La memoria no está configurada para almacenar sesiones de suscriptor. Utilice 'set extendedmemoryparam -memlimit <>'-Use el comando set extendedmemoryparam para configurar la memoria extendida.
- show subscriber radiusinterface
  Si "No configurado" es la salida de este comando, utilice el comando set subscriber radiusinterface para especificar un servicio RadiusListener.

Si el registro de suscriptor está habilitado, puede obtener información más detallada de los archivos de registro.

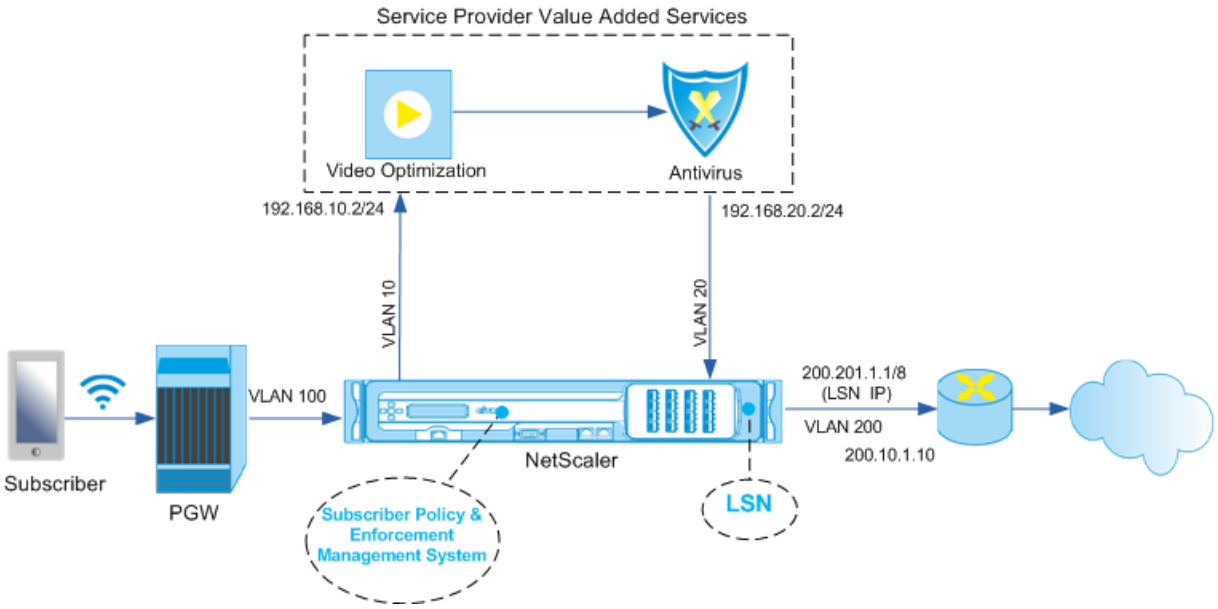
Dirección de tráfico consciente del suscriptor

August 20, 2021

La dirección del tráfico dirige el tráfico del suscriptor de un punto a otro. Cuando un suscriptor se conecta a la red, la Gateway de paquetes asocia una dirección IP con el suscriptor y reenvía el paquete de datos al dispositivo Citrix ADC. El dispositivo se comunica con el servidor PCRF a través de la interfaz Gx para obtener la información de directiva. En función de la información de directiva, el dispositivo realiza una de las siguientes acciones:

- Reenvíe el paquete de datos a otro conjunto de servicios (como se muestra en la siguiente ilustración).
- Suelta el paquete.
- Realice solo NAT a gran escala (LSN), si LSN está configurado en el dispositivo.

Los valores que se muestran en la siguiente ilustración se configuran en el procedimiento CLI que sigue a la ilustración. Un servidor virtual de conmutación de contenido en el dispositivo Citrix ADC dirige las solicitudes a los servicios de valor agregado o las omite, en función de la regla definida, y, a continuación, envía el paquete a Internet después de realizar LSN.



Para configurar la dirección del tráfico para la implementación anterior mediante la CLI

Agregue las direcciones IP de subred (SNIP) del dispositivo.

Ejemplo:

```
add ns ip 192.168.10.1 255.255.255.0 -type snip

add ns ip 192.168.20.1 255.255.255.0 -type snip

add ns ip 100.100.100.1 255.0.0.0 -type snip

add ns ip 200.200.200.1 255.0.0.0 -type snip

add ns ip 100.1.1.1 255.0.0.0 -type snip

add ns ip 200.201.1.1 255.0.0.0 -type snip
<!--NeedCopy-->
```

Agregue las VLAN. Las VLAN ayudan al dispositivo a identificar el origen del tráfico. Enlazar las VLAN a las interfaces y direcciones IP de subred.

Ejemplo:

```
add vlan 10

```



```
add vlan 20

add vlan 100

add vlan 200

bind vlan 10 -ifnum 1/4 -tagged -IPAddress 192.168.10.1 255.255.255.0

bind vlan 20 -ifnum 1/4 -tagged -IPAddress 192.168.20.1 255.255.255.0

bind vlan 100 -ifnum 1/2 -tagged -IPAddress 100.1.1.1 255.0.0.0

bind vlan 200 -ifnum 1/3 -tagged -IPAddress 200.1.1.1 255.0.0.0
<!--NeedCopy-->
```

Especifique la VLAN a la que llega el tráfico de suscriptor al dispositivo. Especifique la ruta de servicio AVP que indica al dispositivo dónde buscar el nombre de la ruta de servicio en la sesión del suscriptor. Para la funcionalidad principal de PCEF, especifique InterfaceType como RadiusAndGX.

Ejemplo:

```
set ns param -servicePathIngressVLAN 100

set subscriber gxinterface -servicepathAVP 1001 1005 -
   servicepathVendorid 10415

set subscriber param -interfaceType RadiusAndGx
<!--NeedCopy-->
```

Configure un servicio y un servidor virtual de tipo Diameter y vincule el servicio al servidor virtual. A continuación, especifique el dominio PCRF y los parámetros de interfaz Gx del suscriptor. Para la funcionalidad principal de PCEF, configure un servicio de escucha RADIUS y una interfaz RADIUS.

Ejemplo:

```
add service sd1 10.102.232.200 DIAMETER 3868

add lb vserver vdiam DIAMETER 0.0.0.0 0 -persistenceType DIAMETER -
   persistAVPno 263

bind lb vserver vdiam sd1

```



```
set ns diameter -identity netscaler.sc1.net -realm pcrf1.net

set subscriber gxInterface -vServer vdiam -pcrfRealm pcrf1.net -
    holdOnSubscriberAbsence YES -idleTTL 1200 -negativeTTL 120

add service srad1 10.102.232.236 RADIUSListener 1813

set subscriber radiusInterface -listeningService srad1
<!--NeedCopy-->
```

Agregue funciones de servicio para asociar un VAS con una VLAN de entrada. Agregue una ruta de servicio para definir la cadena, es decir, especifique el VAS al que debe enviarse el paquete y el orden en el que debe ir a ese VAS. El nombre de la ruta de servicio suele ser enviado por el PCRF. Sin embargo, la ruta de servicio del perfil de suscriptor predeterminado (*) se aplica si se cumple alguna de las siguientes condiciones:

- PCRF no tiene la información del suscriptor.
- La información del suscriptor no incluye este AVP.
- El dispositivo no puede consultar el PCRF. Por ejemplo, el servicio que representa el PCRF es DOWN.

La ruta de servicio AVP que contiene este nombre ya debe configurarse como parte de la configuración global. Enlazar la función de servicio a la ruta de servicio. El índice de servicio especifica el orden en el que se agrega el VAS a la cadena. El número más alto (255) indica el comienzo de la cadena.

Ejemplo:

```
add ns servicefunction SF1 -ingressVLAN 20

add ns servicepath pol1

bind ns servicepath pol1 -servicefunction SF1 -index 255

add subscriber profile * -subscriberrules default_path
<!--NeedCopy-->
```

Agregue la configuración de LSN. Es decir, defina el grupo NAT e identifique los clientes para los que el dispositivo debe realizar LSN.

```
add lsn pool pool1

bind lsn pool pool1 200.201.1.1
```



```
4
5 add lsn client client1
6
7 bind lsn client client1 -network 100.0.0.0 -netmask 255.0.0.0
8
9 add lsn group group1 -clientname client1
10
11 bind lsn group group1 -poolname pool1
12 <!--NeedCopy-->
```

El dispositivo realiza LSN de forma predeterminada. Para anular LSN, debe crear un perfil de red con el parámetro OverridelSN habilitado y enlazar este perfil a todos los servidores virtuales de equilibrio de carga configurados para servicios de valor agregado (VASs).

Ejemplo:

```
1 add netprofile np1
2
3 set netprofile np1 -overrideLsn ENABLED
4
5 set lb vserver vs1 -netprofile np1
6 <!--NeedCopy-->
```

Configure el VAS en el dispositivo. Esto incluye crear los servicios y servidores virtuales y, a continuación, vincular los servicios a los servidores virtuales.

```
1 add service vas1 192.168.10.2 ANY 80 -usip YES
2
3 add service sint 200.10.1.10 ANY 80 -usip YES
4
5 add lb vserver vs1 ANY -m MAC -l2Conn ON
6
7 add lb vserver vint ANY -m MAC -l2Conn ON
8
9 bind lb vserver vs1 vas1
10
11 bind lb vserver vint sint
12 <!--NeedCopy-->
```

Agregue la configuración de conmutación de contenido (CS). Esto incluye servidores virtuales, directivas y sus acciones asociadas. El tráfico llega al servidor virtual CS y, a continuación, se redirige al

servidor virtual de equilibrio de carga adecuado. Defina expresiones que asocien un servidor virtual con una función de servicio.

Ejemplo:

```
add cs vserver cs1 ANY * 80 -l2Conn ON

add cs action csact1 -targetLBVserver vs1

add cs action csactint -targetLBVserver vint

add cs policy cspol1 -rule  SUBSCRIBER.SERVICEPATH.IS_NEXT("SF1") &&
    SYS.VSERVER("vs1").STATE.EQ(UP)" -action csact1

bind cs vserver cs1 -policyName cspol1 -priority 110

bind cs vserver cs1 -lbvserver vint
<!--NeedCopy-->
```

Para configurar la dirección del tráfico en el dispositivo mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **Red** > **IPs** y agregue las direcciones IP de la subred.
2. Vaya a Sistema > Red > **VLAN** y agregue VLAN, vincule las VLAN a las interfaces y direcciones IP de subred.
3. Vaya a **Administración del tráfico** > Conexión **de servicio** > **Configurar VLAN de entrada de ruta de servicio** y especifique una VLAN de entrada.
4. Vaya a **Gestión del Tráfico** > **Suscriptor** > **Parámetros** > **Configurar Parámetros del Suscriptor** y especifique lo siguiente:
   - Tipo de interfaz: Especifique **RadiusAndGX**.
   - Configure un servidor virtual de diameter, un dominio PCRF y los parámetros de interfaz GX del suscriptor.
   - Especifique los parámetros de interfaz RADIUS.
5. Vaya a **Administración del tráfico** > Conexión **de servicios** > **Función de servicio** y agregue funciones de servicio para asociar un servicio de valor agregado a una VLAN de entrada.
6. Vaya a **Sistema** > **Red** > **NAT a gran escala**. Haga clic en **Grupos** y agregue un grupo. Haga clic en **Clientes** y agregue un cliente. Haga clic en **Grupos**, agregue un grupo y especifique el cliente. Modifique el grupo y vincule el grupo a este grupo.
7. Vaya a **Sistema** > **Red** > **Perfiles de red** y agregue un perfil de red. Seleccione **Reemplazar LSN**. Si lo quiere, vaya a **Sistema** > **Red** > **Configuración** > **Configurar parámetros de capa 3** y

compruebe que no está seleccionado **Anular LSN**.

8. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales** y configure los servidores virtuales y los servicios de valor agregado del dispositivo. Enlace los servicios y el perfil de red al servidor virtual.
9. Vaya a **Administración del tráfico** > **Cambio de contenido** > **Servidores virtuales** y configure un servidor virtual, una directiva y una acción. Especifique el servidor virtual de equilibrio de carga de destino.

Para configurar el encadenamiento de servicios en el dispositivo mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **Red** > **IPs** y agregue las direcciones IP de la subred.
2. Vaya a Sistema > Red > **VLAN** y agregue VLAN, vincule las VLAN a las interfaces y direcciones IP de subred.
3. Vaya a **Administración del tráfico** > Conexión **de servicio** > **Configurar VLAN de entrada de ruta de servicio** y especifique una VLAN de entrada.
4. Vaya a **Gestión del Tráfico** > **Suscriptor** > **Parámetros** > **Configurar Parámetros del Suscriptor** y especifique lo siguiente:
   - Tipo de interfaz: Especifique **RadiusAndGX**.
   - Configure un servidor virtual de diameter, un dominio PCRF y los parámetros de interfaz GX del suscriptor.
   - Especifique los parámetros de interfaz RADIUS.
5. Vaya a **Administración del tráfico** > Conexión **de servicios** > **Función de servicio** y agregue funciones de servicio para asociar un servicio de valor agregado a una VLAN de entrada.
6. Vaya a **Sistema** > **Red** > **NAT a gran escala**. Haga clic en **Grupos** y agregue un grupo. Haga clic en **Clientes** y agregue un cliente. Haga clic en **Grupos**, agregue un grupo y especifique el cliente. Modifique el grupo y vincule el grupo a este grupo.
7. Vaya a **Sistema** > **Red** > **Perfiles de red** y agregue un perfil de red. Seleccione **Reemplazar LSN**. Si lo quiere, vaya a **Sistema** > **Red** > **Configuración** > **Configurar parámetros de capa 3** y compruebe que no está seleccionado **Anular LSN**.
8. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales** y configure los servidores virtuales y los servicios de valor agregado del dispositivo. Enlace los servicios y el perfil de red al servidor virtual.
9. Vaya a **Administración del tráfico** > **Cambio de contenido** > **Servidores virtuales** y configure un servidor virtual, una directiva y una acción. Especifique el servidor virtual de equilibrio de carga de destino.

Encadenamiento del servicio de reconocimiento del suscriptor

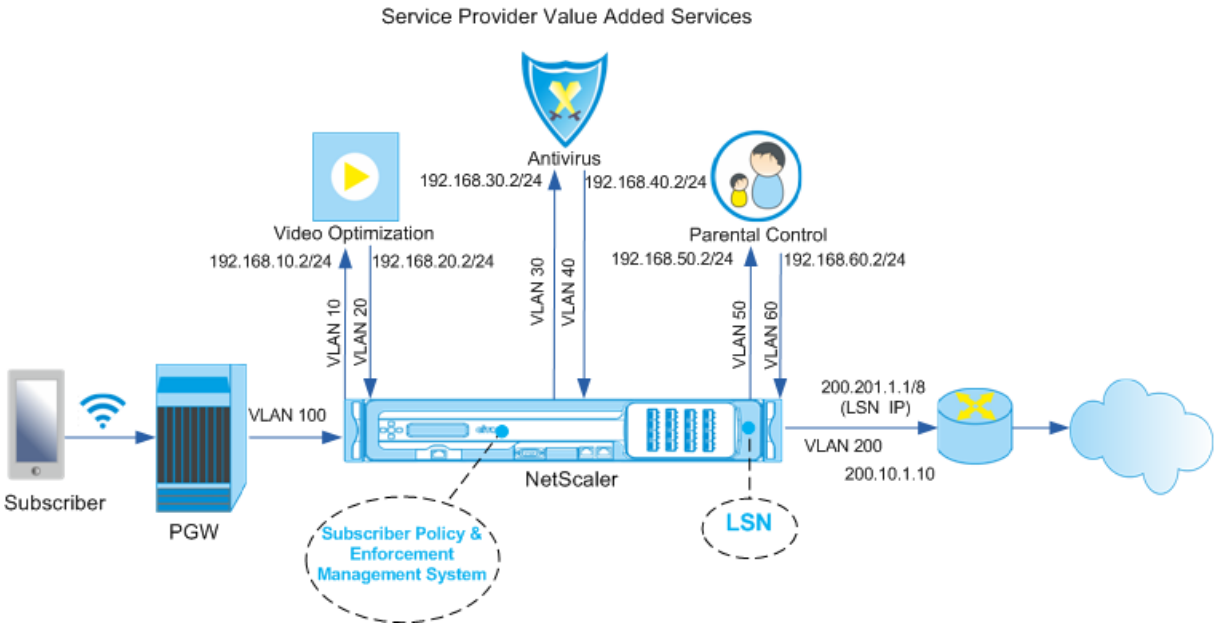
August 20, 2021

Con el enorme aumento del tráfico de datos que pasa a través de las redes de telecomunicaciones, ya no es factible que los proveedores de servicios dirijan todo el tráfico a través de todos los servicios de valor agregado (VAS). Un proveedor de servicios debe ser capaz de optimizar el uso del VAS y dirigir el tráfico de manera inteligente para mejorar la experiencia del usuario. Por ejemplo, la optimización de vídeo no es necesaria para el tráfico que no incluye un vídeo. Además, si un suscriptor está conectado a una red 4G, el contenido puede transmitirse en alta definición (HD) y puede que no sea necesaria la optimización del vídeo. Sin embargo, la optimización de vídeo mejora la experiencia de un usuario en una red 3G. Del mismo modo, el almacenamiento en caché proporciona una experiencia de usuario más rápida y mejor y se puede habilitar en función del plan de suscriptor. Otro ejemplo de VAS es el control parental. Si los principales proporcionan un teléfono móvil a un niño menor, les gustaría algún tipo de control sobre los sitios web que visita su secundario.

Para hacer lo anterior y más, los proveedores de servicios deben poder proporcionar servicios de valor agregado por suscriptor. En otras palabras, las entidades de la red de proveedores de servicios deben ser capaces de extraer la información del suscriptor y dirigir inteligentemente el paquete sobre la base de esta información.

El encadenamiento de servicios determina el conjunto de servicios a través del cual debe pasar el tráfico de un suscriptor antes de ir a Internet. En lugar de enviar todo el tráfico a todos los servicios, Citrix ADC enruta de manera inteligente todas las solicitudes de un suscriptor a un conjunto específico de servicios sobre la base de la directiva definida para ese suscriptor.

La siguiente ilustración muestra las entidades involucradas en el encadenamiento de servicios. Los valores mostrados se configuran en el procedimiento que sigue a la ilustración. Un servidor virtual de conmutación de contenido en el dispositivo Citrix ADC dirige las solicitudes a los servicios de valor agregado o las omite, en función de la regla definida, y, a continuación, envía el paquete a Internet después de realizar LSN.



Para configurar el encadenamiento de servicios para la implementación anterior mediante la CLI

Agregue las direcciones IP de subred (SNIP) del dispositivo.

Ejemplo:

```
add ns ip 192.168.10.1 255.255.255.0 -type snip

add ns ip 192.168.20.1 255.255.255.0 -type snip

add ns ip 192.168.30.1 255.255.255.0 -type snip

add ns ip 192.168.40.1 255.255.255.0 -type snip

add ns ip 192.168.50.1 255.255.255.0 -type snip

add ns ip 192.168.60.1 255.255.255.0 -type snip

add ns ip 100.1.1.1 255.0.0.0 -type snip

add ns ip 200.201.1.1 255.0.0.0 -type snip
<!--NeedCopy-->
```

Agregue las VLAN. Las VLAN ayudan al dispositivo a identificar el origen del tráfico. Enlazar las VLAN a las interfaces y direcciones IP de subred. Agregue una VLAN de entrada y salida para cada VAS.

Ejemplo:

```
add vlan 10

add vlan 20

add vlan 30

add vlan 40

add vlan 50

add vlan 60

add vlan 100

add vlan 200

bind vlan 10 -ifnum 1/4 -tagged -IPAddress 192.168.10.1 255.255.255.0

bind vlan 20 -ifnum 1/4 -tagged -IPAddress 192.168.20.1 255.255.255.0

bind vlan 20 -ifnum 1/4 -tagged -IPAddress 192.168.30.1 255.255.255.0

bind vlan 20 -ifnum 1/4 -tagged -IPAddress 192.168.40.1 255.255.255.0

bind vlan 20 -ifnum 1/4 -tagged -IPAddress 192.168.50.1 255.255.255.0

bind vlan 20 -ifnum 1/4 -tagged -IPAddress 192.168.60.1 255.255.255.0

bind vlan 100 -ifnum 1/2 -tagged -IPAddress 100.1.1.1 255.0.0.0

bind vlan 200 -ifnum 1/3 -tagged -IPAddress 200.201.1.1 255.0.0.0
<!--NeedCopy-->
```

Especifique la VLAN a la que llega el tráfico de suscriptor al dispositivo. Especifique la ruta de servicio AVP que indica al dispositivo dónde buscar el nombre de la ruta de servicio en la sesión del suscriptor. Para la funcionalidad principal de PCEF, especifique InterfaceType como RadiusAndGX.

Ejemplo:

```
set ns param -servicePathIngressVLAN 100
```



```
2
3 set subscriber gxinterface -servicepathAVP 1001 1005 -
     servicepathVendorid 10415
4
5 set subscriber param -interfaceType RadiusAndGx
6 <!--NeedCopy-->
```

Configure un servicio y un servidor virtual de tipo Diameter y vincule el servicio al servidor virtual. A continuación, especifique el dominio PCRF y los parámetros de interfaz Gx del suscriptor. Para la funcionalidad principal de PCEF, configure un servicio de escucha RADIUS y una interfaz RADIUS.

Ejemplo:

```
1 add service sd1 10.102.232.200 DIAMETER 3868
2
3 add lb vserver vdiam DIAMETER 0.0.0.0 0 -persistenceType DIAMETER -
     persistAVPno 263
4
5 bind lb vserver vdiam sd1
6
7 set ns diameter -identity netscaler.sc1.net -realm pcrf1.net
8
9 set subscriber gxInterface -vServer vdiam -pcrfRealm pcrf1.net -
     holdOnSubscriberAbsence YES -idleTTL 1200 -negativeTTL 120
10
11 add service srad1 10.102.232.236 RADIUSListener 1813
12
13 set subscriber radiusInterface -listeningService srad1
14 <!--NeedCopy-->
```

Agregue funciones de servicio para asociar un VAS con una VLAN de entrada. Agregue una ruta de servicio para definir la cadena, es decir, especifique el VAS al que debe enviarse el paquete y el orden en el que debe ir a ese VAS. El nombre de la ruta de servicio suele ser enviado por el PCRF. Sin embargo, la ruta de servicio del perfil de suscriptor predeterminado (*) se aplica si se cumple alguna de las siguientes condiciones:

- PCRF no tiene la información del suscriptor.
- La información del suscriptor no incluye este AVP.
- El dispositivo no puede consultar el PCRF. Por ejemplo, el servicio que representa el PCRF es DOWN.

La ruta de servicio AVP que contiene este nombre debe configurarse como parte de la configuración global anterior. Enlazar la función de servicio a la ruta de servicio. El índice de servicio especifica

el orden en el que se agrega el VAS a la cadena. El número más alto (255) indica el comienzo de la cadena.

Ejemplo:

```
add ns servicefunction SF1 -ingressVLAN 20

add ns servicefunction SF2 -ingressVLAN 40

add ns servicefunction SF3 -ingressVLAN 60

add ns servicepath pol1

bind ns servicepath pol1 -servicefunction SF1 -index 255

bind ns servicepath pol1 -servicefunction SF2 -index 254

bind ns servicepath pol1 -servicefunction SF3 -index 253

add ns servicepath pol2

bind ns servicepath pol2 -servicefunction SF2 -index 255

add ns servicepath pol3

bind ns servicepath pol3 -servicefunction SF1 -index 255

add subscriber profile * -subscriberrules default_path
<!--NeedCopy-->
```

Agregue la configuración de LSN. Es decir, defina el grupo NAT e identifique los clientes para los que el dispositivo debe realizar LSN.

Ejemplo:

```
add lsn pool pool1

bind lsn pool pool1 200.201.1.1

add lsn client client1

bind lsn client client1 -network 100.0.0.0 -netmask 255.0.0.0

```



```
add lsn group group1 -clientname client1

bind lsn group group1 -poolname pool1
<!--NeedCopy-->
```

El dispositivo realiza LSN de forma predeterminada. Para anular LSN, debe crear un perfil de red con el parámetro OverrideISN habilitado y enlazar este perfil a todos los servidores virtuales de equilibrio de carga configurados para servicios de valor agregado (VASs).

Ejemplo:

```
add netprofile np1

set netprofile np1 -overrideLsn ENABLED

set lb vserver vs1 -netprofile np1
<!--NeedCopy-->
```

Configure el VAS en el dispositivo. Esto incluye crear los servicios y servidores virtuales y, a continuación, vincular los servicios a los servidores virtuales.

Ejemplo:

```
add service vas1 192.168.10.2 ANY 80 -usip YES

add service vas2 192.168.30.2 ANY 80 -usip YES

add service vas3 192.168.50.2 ANY 80 -usip YES

add service sint 200.10.1.10 ANY 80 -usip YES

add lb vserver vs1 ANY -m MAC -l2Conn ON

add lb vserver vs2 ANY -m MAC -l2Conn ON

add lb vserver vs3 ANY -m MAC -l2Conn ON

add lb vserver vint ANY -m MAC -l2Conn ON

bind lb vserver vs1 vas1

bind lb vserver vs2 vas2

```



```
bind lb vserver vs3 vas3

bind lb vserver vint sint
<!--NeedCopy-->
```

Agregue la configuración de conmutación de contenido (CS). Esto incluye servidores virtuales, directivas y sus acciones asociadas. El tráfico llega al servidor virtual CS y, a continuación, se redirige al servidor virtual de equilibrio de carga adecuado. Defina expresiones que asocien un servidor virtual con una función de servicio.

Ejemplo:

```
add cs vserver cs1 ANY * 80 -l2Conn ON

add cs action csact1 -targetLBVserver vs1

add cs action csact2 -targetLBVserver vs2

add cs action csact3 -targetLBVserver vs3

add cs action csactint -targetLBVserver vint

add cs policy cspol1 -rule "SUBSCRIBER.SERVICEPATH.IS_NEXT("SF1") &&
   SYS.VSERVER("vs1").STATE.EQ(UP)" -action csact1

add cs policy cspol2 -rule "SUBSCRIBER.SERVICEPATH.IS_NEXT("SF2") &&
   SYS.VSERVER("vs2").STATE.EQ(UP)" -action csact2

add cs policy cspol3 -rule "SUBSCRIBER.SERVICEPATH.IS_NEXT("SF3") &&
   SYS.VSERVER("vs3").STATE.EQ(UP)" -action csact3

bind cs vserver cs1 -policyName cspol1 -priority 110

bind cs vserver cs1 -policyName cspol2 -priority 120

bind cs vserver cs1 -policyName cspol3 -priority 130

bind cs vserver cs1 -lbvserver vint
<!--NeedCopy-->
```


Para configurar el encadenamiento de servicios en el dispositivo mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **Red** > **IPs** y agregue las direcciones IP de la subred.
2. Vaya a **Sistema** > **Red** > **VLAN** y agregue VLAN, Vincule las VLAN a las interfaces y direcciones IP de subred.
3. Vaya a **Administración del tráfico** > Conexión **de servicio** > **Configurar VLAN de entrada de ruta de servicio** y especifique una VLAN de entrada.
4. Vaya a **Gestión del Tráfico** > **Suscriptor** > **Parámetros** > **Configurar Parámetros del Suscriptor** y especifique lo siguiente:
   - Tipo de interfaz: Especifique **RadiusAndGX**.
   - Configure un servidor virtual de diameter, un dominio PCRF y los parámetros de interfaz GX del suscriptor.
   - Especifique los parámetros de interfaz RADIUS.
5. Vaya a **Administración del tráfico** > Conexión **de servicios** > **Función de servicio** y agregue funciones de servicio para asociar un servicio de valor agregado a una VLAN de entrada.
6. Vaya a **Sistema** > **Red** > **NAT a gran escala**. Haga clic en **Grupos** y agregue un grupo. Haga clic en **Clientes** y agregue un cliente. Haga clic en **Grupos**, agregue un grupo y especifique el cliente. Modifique el grupo y vincule el grupo a este grupo.
7. Vaya a **Sistema** > **Red** > **Perfiles de red** y agregue un perfil de red. Seleccione **Reemplazar LSN**. Si lo quiere, vaya a **Sistema** > **Red** > **Configuración** > **Configurar parámetros de capa 3** y compruebe que no está seleccionado **Anular LSN**.
8. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales** y configure los servidores virtuales y los servicios de valor agregado del dispositivo. Enlace los servicios y el perfil de red al servidor virtual.
9. Vaya a **Administración del tráfico** > **Cambio de contenido** > **Servidores virtuales** y configure un servidor virtual, una directiva y una acción. Especifique el servidor virtual de equilibrio de carga de destino.

Dirección de tráfico consciente del suscriptor con optimización TCP

August 20, 2021

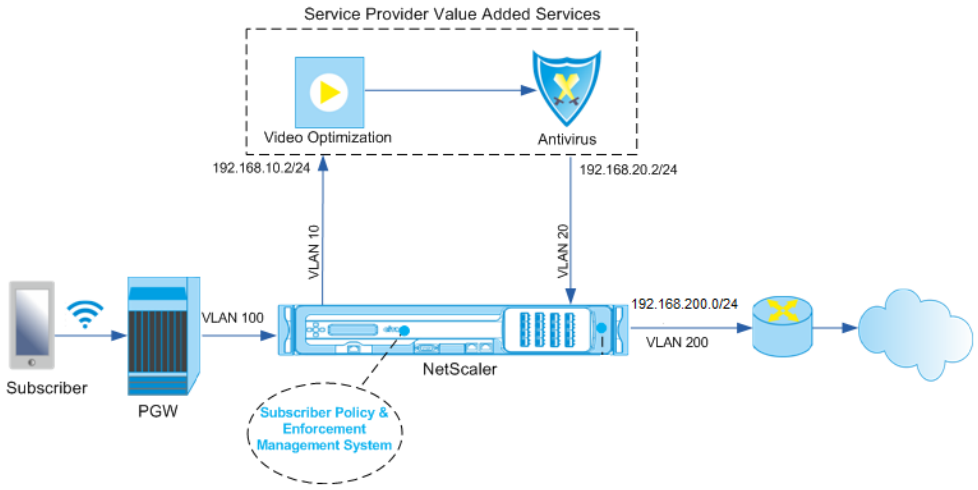
La dirección del tráfico dirige el tráfico del suscriptor de un punto a otro. Cuando un suscriptor se conecta a la red, la Gateway de paquetes asocia una dirección IP con el suscriptor y reenvía el paquete de datos al dispositivo Citrix ADC. El dispositivo se comunica con el servidor PCRF a través de la interfaz Gx para obtener la información de directiva de suscriptor. En función de la información de directiva, el dispositivo realiza una de las siguientes acciones:

- Reenvíe el paquete de datos a otro conjunto de servicios (como se muestra en la siguiente ilus-

tración).

- Realice solo la optimización TCP.

Los valores que se muestran en la siguiente ilustración se configuran en el procedimiento CLI que sigue a la ilustración. Un servidor virtual de conmutación de contenido en el dispositivo Citrix ADC dirige las solicitudes a los servicios de valor agregado o las omite y realiza la optimización TCP, según la regla definida, y, a continuación, envía el paquete a Internet.



> **Nota**
>
> El soporte para la configuración que se muestra a continuación se introdujo en la versión 11.1, compilación 50.10.

Para configurar la dirección de tráfico para la implementación anterior mediante la CLI:

1. Agregue las direcciones IP de subred (SNIP) del dispositivo.

```
add ns ip 192.168.10.1 255.255.255.0 -type snip

add ns ip 192.168.20.1 255.255.255.0 -type snip

add ns ip 192.168.100.1 255.255.255.0 -type snip

add ns ip 192.168.200.1 255.255.255.0 -type snip

add ns ip 10.102.232.236 255.255.255.0  - type snip
<!--NeedCopy-->
```

2. Agregue las VLAN. Las VLAN ayudan al dispositivo a identificar el origen del tráfico. Enlazar las VLAN a las interfaces y direcciones IP de subred.


```
add vlan 10

add vlan 20

add vlan 100

add vlan 200

add vlan 102

bind vlan 10 -ifnum 1/4 -tagged -IPAddress 192.168.10.1
    255.255.255.0

bind vlan 20 -ifnum 1/4 -tagged -IPAddress 192.168.20.1
    255.255.255.0

bind vlan 100 -ifnum 1/2 -tagged -IPAddress 192.168.100.1
    255.255.255.0

bind vlan 200 -ifnum 1/2 -tagged -IPAddress 192.168.200.1
    255.255.255.0

bind vlan 102  - ifnum 1/1  - tagged  - IPAddress 10.102.232.236
    255.255.255.0
<!--NeedCopy-->
```

3. Configure un servicio y un servidor virtual de tipo Diameter y vincule el servicio al servidor virtual. Especifique el dominio PCRF y los valores para los parámetros de interfaz Gx del suscriptor. Especifique también la ruta de servicio AVP que indica dónde puede encontrar el dispositivo el nombre de la ruta de servicio dentro de la sesión del suscriptor. Para la funcionalidad principal de PCEF, configure un servicio de escucha RADIUS y una interfaz RADIUS y especifique el tipo de interfaz como “RadiusAndGX”.

```
add service sd1 10.102.232.200 DIAMETER 3868

add lb vserver vdiam DIAMETER 0.0.0.0 0 -persistenceType DIAMETER
    -persistAVPno 263

bind lb vserver vdiam sd1

set ns diameter -identity netscaler.sc1.net -realm pcrf1.net
```



```
8
9  set extendedmemoryparam -memLimit 2558
10
11 set subscriber gxInterface -vServer vdiam -pcrfRealm pcrf1.net
12
13 set subscriber gxinterface -servicepathAVP 1001 1005 -
       servicepathVendorid 10415
14
15 add service srad1 10.102.232.236 RADIUSListener 1813
16
17 set subscriber radiusInterface -listeningService srad1
18
19 set subscriber param -interfaceType RadiusAndGx
20 <!--NeedCopy-->
```

4. Especifique un perfil de suscriptor predeterminado (*) que se aplicará si se cumple alguna de las siguientes condiciones:

   - PCRF no tiene la información del suscriptor.
   - La información del suscriptor no incluye la ruta de servicio AVP.
   - El dispositivo no puede consultar el PCRF. Por ejemplo, el servicio que representa el PCRF es DOWN.

```
1 add subscriber profile * -subscriberrules default_path
2 <!--NeedCopy-->
```

5. Cree perfiles TCP para la ruta de optimización VAS y TCP, respectivamente. El tráfico dirigido a VAS no sufrirá ninguna optimización TCP antes o después de salir del VAS. Por lo tanto, el modo TCP del perfil VAS debe establecerse en TRANSPARENTE mientras que el modo TCP del perfil TCPOPT debe establecerse en ENDpoint.

   add ns TCPProfile VAS —TCPMode TRANSPARENTE

   add ns TCPProfile TCPOpt -WS ENABLED -SACK ENABLED -WSVal 8 -mss 1460 -MaxBurst 30 -InitialCwnd 16 -OOOQSize 15000 -minRto 800 -BufferSize 4000000 -flavor BIC -dynamicReceiveBuffering ENABLED -KA ENABLED -SendBuffSize 4000000 -RSTWindowAttenuate ENABLED -spoofSyndrop ENABLED -wnto d 1000000 -fack ENABLED -RstMaxack ENABLED -tcpmode ENDpoint

6. Configure el equilibrio de carga para los servidores VAS. Cree un servidor virtual no direccionable de tipo TCP. Cree servicios TCP con las direcciones IP de los servidores VAS y vincule los servicios al servidor virtual. El servidor virtual y los servicios utilizarán el perfil TCP transparente creado para la ruta del VAS:


```
add service vas1 192.168.10.2 TCP * -usip YES -useproxyport NO -
    TCPB NO -tcpProfileName VAS

add service vas2 192.168.10.3 TCP * -usip YES -useproxyport NO -
    TCPB NO -tcpProfileName VAS

add lb vserver vs1 TCP -m MAC -l2Conn ON  - tcpProfileName VAS

bind lb vserver vs1 vas1

bind lb vserver vs1 vas2
<!--NeedCopy-->
```

7. Agregue un servidor virtual de equilibrio de carga para capturar el tráfico de salida del VAS. Este servidor virtual supervisará la VLAN de salida del VAS y utilizará el perfil TCP transparente:

```
add lb vserver vsint TCP * * -Listenpolicy "CLIENT.VLAN.ID.EQ(20)"
     - Listenpriority 30  - l2Conn ON  - tcpProfileName VAS
<!--NeedCopy-->
```

8. Agregue un servidor virtual de optimización TCP que escuche cualquier tráfico en la VLAN del lado inalámbrico y use el perfil TCP del extremo creado para la ruta de optimización TCP:

```
add lb vserver vs-TcpOpt TCP * * -Listenpolicy "client.vlan.id.eq
    (100)"  - Listenpriority 20 -l2Conn ON -tcpProfileName TCPOpt
<!--NeedCopy-->
```

9. Agregue la configuración de conmutación de contenido (CS). Esto incluye servidores virtuales, directivas y sus acciones asociadas. El servidor virtual CS recibe el tráfico y lo redirige al servidor virtual de equilibrio de carga adecuado de acuerdo con las directivas de CS definidas. Cree un servidor virtual CS TCP que escuche cualquier tráfico en la VLAN del lado inalámbrico con la máxima prioridad y utilice el perfil TCP del extremo. Cree una directiva de CS que se evalúe como TRUE cuando “vas” es la regla del suscriptor y especifique una acción de CS que dirija el tráfico a VAS. Haga que el servidor virtual de optimización TCP sea el vserver LB predeterminado. Cualquier tráfico de suscriptor con una regla que no sea “vas” pasará por el vserver LB predeterminado.


```
add cs vserver cs1 TCP * * -Listenpolicy "client.vlan.id.eq(100)"
    - Listenpriority 10 -l2Conn ON  - tcpProfileName TCPOpt

add cs action csact1 -targetLBVserver vs1

add cs policy cspol1 -rule  SUBSCRIBER.RULE_ACTIVE("vas") && SYS.
   VSERVER("vs1").STATE.EQ(UP)" -action csact1

bind cs vserver cs1 -policyName cspol1

bind cs vserver cs1 -lbvserver vs-TcpOpt
<!--NeedCopy-->
```

10. Agregue rutas estáticas o basadas en directivas a Internet. También se admite el redirección dinámica en esta configuración. En el ejemplo siguiente se utilizan rutas basadas en directivas:

```
add ns pbr pbr-vlan100-to-vlan200 ALLOW -nextHop 192.168.200.10 -
   vlan 100 -priority 10

add ns pbr pbr-vlan20-to-vlan200 ALLOW -nextHop 192.168.200.10 -
   vlan 20 -priority 11

apply ns pbrs
<!--NeedCopy-->
```

Nota

- Las directivas CS pueden contener direcciones IP y números de puerto además de las expresiones de suscriptor, por ejemplo, SUBSCRIPBER.RULE_ACTIVE ("vas") && & (CLIENT.TCP.DSTPORT.EQ (80) || CLIENT.TCP.DSTPORT.EQ (443). También pueden contener expresiones basadas en HTTP, por ejemplo, HTTP.REQ.HOSTNAME.DOMAIN.EQ ("somedomain.com"). En este caso, reemplace las entidades TCP (vserver, service, etc.) con HTTP. La configuración del perfil TCP sigue siendo la misma.
- Agregue la configuración IPv6 (direcciones, rutas, PBRs) para admitir suscriptores IPv6. Las aplicaciones cliente de Happy Eyeballs funcionarán sin problemas tanto para rutas de optimización VAS como TCP.
- Agregue VLAN, direcciones IP, PBRs y servidores virtuales LB delante del VAS (vs1, vs2, etc.) para admitir múltiples flujos de suscriptores. Modifique las directivas de escucha de CS vserver "cs1" y LB vserver "vsint" para incluir las VLAN adicionales.

Selección de perfiles TCP basada en directivas

January 31, 2022

Puede configurar el dispositivo Citrix ADC para que realice la optimización de TCP en función de los atributos del suscriptor. Por ejemplo, el dispositivo puede seleccionar diferentes perfiles TCP en tiempo de ejecución, en función de la red a la que está conectado el equipo de usuario (UE). Como resultado, puede mejorar la experiencia de un usuario móvil estableciendo algunos parámetros en los perfiles TCP y, a continuación, mediante una directiva para seleccionar el perfil apropiado.

Cree perfiles TCP separados para los suscriptores que se conectan a través de una red 4G y para los usuarios que se conectan a través de cualquier otra red Defina una regla de directiva que se seleccione en función de un parámetro de suscriptor, como el tipo de tecnología de acceso por radio (tipo RAT). En los siguientes ejemplos, si el tipo RAT es EUTRAN, se selecciona un perfil TCP que admita una conexión más rápida (Ejemplo 1). Para todos los demás valores de tipo RAT, se selecciona un perfil TCP diferente (Ejemplo 2).

Para obtener más información sobre la tecnología de acceso de radio y su configuración de directivas, consulte RFC 29.212.

> **Nota**
>
> El AVP de tipo RAT (código AVP 1032) es de tipo “enumerado” y se usa para identificar la tecnología de acceso por radio que sirve al UE.
>
> El valor “1004” indica que la RAT es EUTRAN.

Ejemplo 1:

```
add ns tcpProfile tcp2 -WS ENABLED -SACK ENABLED -WSVal 8 -initialCwnd
    16 - oooQSize 15000 -slowStartIncr 1 -bufferSize 1000000 -flavor BIC
     - dynamicReceiveBuffering DISABLED -sendBuffsize 1000000 -dsack
    DISABLED -maxcwnd 4000000 -fack ENABLED -minRTO 500 -maxburst 15

add appqoe action appact2 -priority HIGH -tcpprofile tcp2

add appqoe policy apppol2 -rule ”SUBSCRIBER.AVP(1032).VALUE.
    GET_UNSIGNED32(0, BIG_ENDIAN).EQ(1004)” -action appact2

bind cs vserver <name>  -policyname apppol2 -priority 20 -type request
<!--NeedCopy-->
```

Ejemplo 2:


```
add ns tcpProfile tcp1 -WS ENABLED -SACK ENABLED -WSVal 8 -initialCwnd
    16 - oooQSize 15000 -slowStartIncr 1 -bufferSize 150000 -flavor BIC
    - dynamicReceiveBuffering DISABLED -sendBuffsize 150000 -dsack
    DISABLED -maxcwnd 4000000 -fack ENABLED -minRTO 200 -maxburst 15

add appqoe action appact1 -priority HIGH -tcpprofile tcp1

add appqoe policy apppol1 -rule "SUBSCRIBER.AVP(1032).VALUE.
    GET_UNSIGNED32(0, BIG_ENDIAN).NE(1004)" -action appact1

bind cs vserver <name>  -policyname apppol1 -priority 10 -type request
<!--NeedCopy-->
```

Tráfico de plano de control de equilibrio de carga basado en los protocolos de diameter, SIP y SMPP

August 20, 2021

Con el aumento del tráfico del plano de control, los servidores pueden convertirse en un cuello de botella porque el tráfico no se distribuye de manera óptima entre los servidores. Por lo tanto, los mensajes deben estar equilibrados de carga. El dispositivo Citrix ADC admite el equilibrio de carga de Diameter, SIP y SMPP.

SIP

Citrix ADC le permite equilibrar la carga de mensajes SIP a través de UDP o a través de TCP (incluido TLS) en un grupo de servidores proxy. Citrix ADC también proporciona persistencia basada en ID de llamada y método de equilibrio de carga hash ID de llamada mediante el cual se dirigen los paquetes para una sesión SIP concreta al mismo servidor SIP equilibrado de carga.
El lenguaje de expresiones predeterminadas de Citrix ADC contiene varias expresiones que operan en conexiones SIP (Protocolo de inicio de sesión). Estas expresiones están pensadas para ser utilizadas en directivas para el protocolo SIP que opera sobre una base de solicitud/respuesta. Estas expresiones se pueden utilizar en directivas de conmutación de contenido, limitación de velocidad, respuesta y reescritura.

Para obtener más información, consulte Equilibrio de carga de un grupo de servidores SIP.

SMPP

Millones de mensajes cortos se intercambian diariamente entre individuos y proveedores de servicios de valor agregado, como bancos, anunciantes y servicios de directorio, mediante el protocolo de mensajes cortos peer to peer (SMPP). A menudo, la entrega de mensajes se retrasa porque los servidores están sobrecargados y el tráfico no se distribuye de manera óptima entre los servidores.
El dispositivo Citrix ADC proporciona una distribución óptima de los mensajes entre los servidores, lo que evita el rendimiento deficiente y las interrupciones. El dispositivo Citrix ADC:

- Balanza de carga los mensajes que se originan desde el servidor y desde el cliente
- Supervisa el estado de los centros de mensajes
- Proporciona compatibilidad con el cambio de contenido para los centros de mensajes
- Maneja mensajes concatenados

Limitación: No se admiten los ID de mensaje, desde el centro de mensajes, de más de 59 bytes. Si la longitud del identificador del mensaje devuelto por el centro de mensajes es superior a 59 bytes, las operaciones auxiliares fallan y el dispositivo Citrix ADC responde con un mensaje de error.

Para obtener más información, consulte Equilibrio de carga de SMPP

Diameter

Diameter es un protocolo base con más de 50 protocolos (también llamados aplicaciones) construidos sobre él. Por lo tanto, el tráfico de diameter generado en una red de telecomunicaciones es alto. Para mantener de forma óptima este tráfico de diameter, el dispositivo Citrix ADC realiza el equilibrio de carga, la conmutación de contenido y actúa como agente de retransmisión. Además, el dispositivo ofrece funciones de reescritura y respuesta. El dispositivo admite la limitación de velocidad de los mensajes de diameter.

Para obtener más información, consulte Configuración del equilibrio de carga de diámetro.

Proporcionar servicios de infraestructura y tráfico DNS, como equilibrio de carga, almacenamiento en caché y registro para proveedores de servicios de telecomunicaciones

January 19, 2021

Los proveedores de servicios de telecomunicaciones pueden configurar el dispositivo Citrix ADC para que funcione como proxy DNS. El almacenamiento en caché de registros DNS, que es una función importante de un proxy DNS, está habilitado de forma predeterminada en el dispositivo Citrix ADC. Esto permite que el dispositivo Citrix ADC proporcione respuestas rápidas para traducciones repetidas

y, por lo tanto, mejora la experiencia del cliente y también ahorra el ancho de banda. La caché de las respuestas de los servidores de nombres DNS. Cuando el dispositivo recibe una consulta DNS, comprueba el dominio consultado en su caché. Si la dirección del dominio consultado está presente en su caché, el dispositivo Citrix ADC devuelve la dirección correspondiente al cliente. De lo contrario, reenvía la consulta a un servidor de nombres DNS que comprueba la disponibilidad de la dirección y la devuelve al dispositivo Citrix ADC. A continuación, el dispositivo Citrix ADC devuelve la dirección al cliente.

Para las solicitudes de un dominio que se ha almacenado en caché anteriormente, el dispositivo Citrix ADC sirve el registro de direcciones del dominio desde la caché sin consultar el servidor DNS configurado y, por lo tanto, guarda el ancho de banda.

A partir de la versión 11.0, Citrix ADC también registra las solicitudes DNS que recibe y también las respuestas que envía al cliente. Los proveedores de servicios de telecomunicaciones pueden usar este registro para:

- Auditar las respuestas DNS al cliente
- Auditar clientes DNS
- Detectar y prevenir ataques DNS
- Solucionar problemas

Para obtener más información, consulte Sistema de nombres de dominio.

Proporcionar distribución de carga de suscriptor mediante GSLB a través de redes de núcleo de un proveedor de servicios de telecomunicaciones

January 19, 2021

La escalabilidad, la alta disponibilidad y el rendimiento son fundamentales para las implementaciones de proveedores de servicios. Aunque muchos proveedores de servicios implementan infraestructura en una sola ubicación o en varias ubicaciones, estas implementaciones están sujetas a una serie de limitaciones inherentes, como:

- Si el sitio pierde conectividad a la totalidad o parte de Internet público, será inaccesible para los usuarios y clientes, lo que puede tener un impacto significativo en el negocio.
- Los usuarios que acceden al sitio desde ubicaciones geográficamente distantes pueden experimentar retrasos grandes y muy variables, que se ven agravados por el gran número de viajes de ida y vuelta que HTTP requiere para transferir contenido.

El equilibrio global de carga de servidores (GSLB) del dispositivo Citrix ADC supera estos problemas distribuyendo tráfico entre sitios implementados en varias ubicaciones geográficas. Al servir con-

tenido de muchos puntos diferentes en Internet, GSLB alivia el impacto de los cuellos de botella de ancho de banda de red y proporciona robustez en caso de fallas de red en un sitio determinado. Los usuarios pueden ser dirigidos automáticamente al sitio más cercano o menos cargado en el momento de la solicitud, minimizando la probabilidad de retrasos prolongados en la descarga y/o interrupciones en el servicio.

Puede utilizar el equilibrio de carga global del servidor del dispositivo Citrix ADC para:

- Recuperación ante desastres o alta disponibilidad mediante la configuración de un centro de datos activo en espera que consta de un centro de datos activo y un centro de datos en espera. Cuando se produce una conmutación por error como resultado de un evento de desastre, el centro de datos en espera entra en funcionamiento.
- Alta disponibilidad y velocidad mediante la configuración de un centro de datos activo-activo que consta de varios centros de datos activos. Las solicitudes de los clientes se equilibran la carga entre los centros de datos activos.
- Dirigir las solicitudes del cliente al centro de datos más cercano en distancia geográfica o distancia de red mediante la configuración de proximidad.
- Resoluciones DNS completas, GSLB procesa consultas DNS de los tipos A, AAAA y CNAME, y la opción de función DNS puede procesar consultas DNS de todos los demás tipos, como MX y PTR. Además, si la resolución recursiva está habilitada, el dispositivo reenviará consultas DNS para nombres de dominio que no estén configurados en el dispositivo Citrix ADC.

Para obtener más información, consulte Equilibrio de carga global del servidor.

Utilización del ancho de banda mediante la funcionalidad de redirección de caché

January 19, 2021

El volumen de tráfico web en Internet es enorme y un gran porcentaje de ese tráfico es redundante. Varios clientes piden a los servidores web el mismo contenido repetidamente, lo que lleva a un uso ineficiente del ancho de banda. Para evitar que el servidor web de origen procese cada solicitud, los proveedores de servicios de Internet (ISP) pueden utilizar la función de redirección de caché del dispositivo Citrix ADC y servir el contenido desde un servidor de caché en lugar de desde el servidor de origen. El dispositivo Citrix ADC analiza las solicitudes entrantes, envía solicitudes de datos en caché a servidores de caché y envía solicitudes no en caché y solicitudes HTTP dinámicas a servidores de origen. La función de redirección de caché de Citrix ADC está basada en directivas y, de forma predeterminada, las solicitudes que coinciden con una directiva se envían al servidor de origen y todas las demás solicitudes se envían a un servidor de caché. Puede combinar el cambio de contenido con la redirección de caché para almacenar contenido selectivo en caché y servir contenido desde servi-

dores de caché específicos para tipos específicos de contenido solicitado.

Para obtener más información, consulte Redirección de caché.

Optimización TCP de Citrix ADC

January 19, 2021

El dispositivo Citrix ADC proporciona técnicas y capacidades avanzadas de optimización y optimización TCP que se adaptan perfectamente a las redes 3.5 y 4G modernas, lo que mejora significativamente la experiencia del usuario y las velocidades de descarga percibidas.

Esta sección se centra en instrucciones detalladas relacionadas con:

- Elegir e insertar un modelo apropiado de Citrix ADC T1000 Series en una red móvil para optimizar TCP
- Instrucciones de configuración completas relacionadas no solo con la optimización TCP, sino también con la configuración apropiada de Capa 2 y Capa 3 del dispositivo T1

La sección incluye los siguientes temas:

- Introducción
- Red de administración
- Licencias
- Alta disponibilidad
- Integración de Gi-LAN
- Configuración de optimización TCP
- Optimización del rendimiento TCP mediante TCP NILE
- Análisis e informes
- Estadísticas en tiempo real
- SNMP
- Recetas técnicas
- Pautas de solución de problemas
- Preguntas frecuentes

Introducción

August 20, 2021

Hardware

Citrix proporciona una gran cantidad de modelos de Citrix ADC que pueden estar basados en dos factores:

- Capacidad, que actualmente oscila entre cientos de Mbps para el dispositivo VPX de gama baja y 160 Gbps para el dispositivo de gama alta de la serie MPX de 25000
- Grado de telecomunicaciones, con la disponibilidad de la serie T1000 para centros de datos de telecomunicaciones.

Su representante de ventas o soporte técnico de Citrix puede ayudarle a seleccionar el hardware adecuado para sus necesidades de demostración, prueba o producción.

El resto de esta sección utiliza un dispositivo Citrix ADC T1200 como hardware de referencia. Tenga en cuenta que dejando de lado las diferencias superficiales relacionadas con el número y la notación de interfaces disponibles (ver * en la nota) o las limitaciones bien documentadas de Citrix ADC VPX (ver * en la nota), las instrucciones deben aplicarse mayormente verbatim, independientemente del modelo de Citrix ADC seleccionado.

> **Nota**
>
> * Por ejemplo, un modelo T1010 solo tiene 12x1GbE normalmente marcado como 1/1-1/12 en lugar de la notación 10/x utilizada en este documento.
>
> ** Por lo general, una instancia de Citrix ADC VPX no admite la agregación LACP; también es posible que no admita el etiquetado VLAN.

Configuración inicial

A través de la consola serie

Después de conectar un cable serie, puede iniciar sesión en el dispositivo Citrix ADC con las siguientes credenciales:

- Nombre de usuario: nsroot
- Contraseña: Nsroot

Una vez iniciada la sesión, configure los detalles básicos del dispositivo Citrix ADC como se muestra en la captura de pantalla que aparece a continuación.

Ejemplo:

```
set ns config  - IPAddress <ip_addr> -netmask <netmask>

saveconfig

```



```
reboot -warm
<!--NeedCopy-->
```

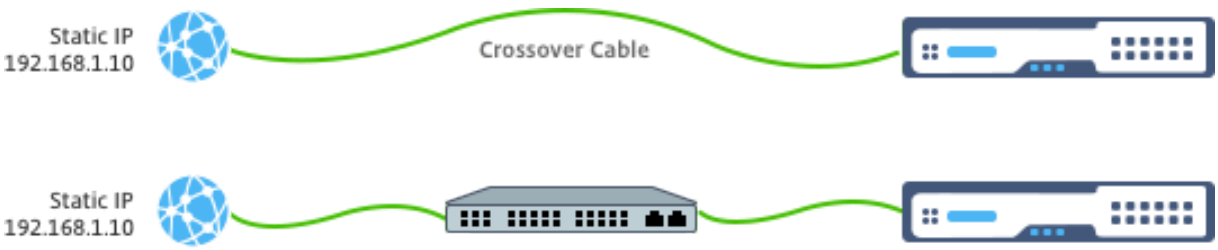
Después de reiniciar el dispositivo, puede utilizar SSH para una configuración adicional de los nodos T1100.

A través de LOM

El puerto de administración de luces (LOM) en el panel frontal del dispositivo Citrix ADC permite al operador supervisar y administrar remotamente el dispositivo independientemente del sistema operativo. El operador puede cambiar la dirección IP, el ciclo de alimentación y realizar un volcado de código conectándose al dispositivo Citrix ADC a través del puerto LOM.

La dirección IP predeterminada del puerto LOM es 192.168.1.3

Ilustración. Configuración inicial del módulo LOM



Establezca una IP estática en su portátil y conéctela directamente a la interfaz LOM con un cable cruzado o a un conmutador en el mismo dominio de difusión que la interfaz LOM.

Para la configuración inicial, escriba la dirección predeterminada del puerto: http://192.168.1.3 en un explorador web y cambie la dirección IP predeterminada del puerto LOM.

Consulte las Guías de configuración para obtener más detalles.

Software

La optimización TCP de Citrix ADC para redes móviles está en constante evolución. Las capacidades y ajustes descritos en este documento requieren una compilación de Citrix ADC Telco. A continuación se muestra un ejemplo que muestra la compilación de Citrix ADC Telco.

Ejemplo:

```
show ver

NetScaler NS11.0: Build 64.957.nc, Date: Aug 26 2016, 02:00:23
<!--NeedCopy-->
```


Si el T1000 no se ha enviado con la revisión de compilación adecuada, póngase en contacto con el servicio de atención al cliente de Citrix ADC.

> **Importante**
>
> Ambos dispositivos deben tener la misma imagen de software.

Cliente SSH

Un dispositivo Citrix ADC se puede configurar mediante la CLI o la GUI HTML5. Sin embargo, esta sección solo proporciona instrucciones basadas en CLI.

Aunque se puede acceder a la CLI a través de la consola serie de Citrix ADC, normalmente se recomienda un cliente SSH para permitir la configuración remota de Citrix ADC.

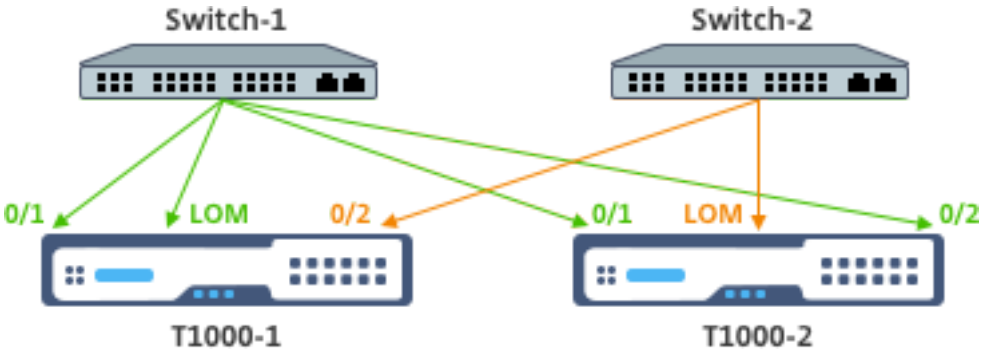
Red de gestión

January 12, 2021

Conectividad

La mayoría de los dispositivos Citrix ADC ofrecen puertos OAM redundantes de 1 GbE, anotados como 0/1 y 0/2. Para proporcionar redundancia en caso de fallo del conmutador, debe conectar los puertos relevantes a diferentes conmutadores ascendentes.

En el siguiente diagrama se describe una descripción general de alto nivel de la conectividad recomendada:



Una vez conectado el dispositivo Citrix ADC a la red de administración, los pasos de configuración posteriores se pueden realizar de forma remota mediante SSH o conectividad web a la CLI y la GUI, respectivamente.

Redirección

El comando add route puede utilizarse para configurar las rutas apropiadas para la red de administración. La Gateway pertinente debe ser accesible en la subred NSIP, como se muestra a continuación.

Ejemplo:

```
add route <network>  <netmask>  <gateway>
<!--NeedCopy-->
```

Licencias

January 12, 2021

Debe instalarse un archivo de licencia válido en el dispositivo Citrix ADC. La licencia debe admitir al menos tantos Gbps como el rendimiento máximo de GI-LAN esperado.

Los archivos de licencia deben copiarse a través de un cliente SCP en /nsconfig/license del dispositivo, como se muestra en la captura de pantalla que aparece a continuación.

Ejemplo:

```
shell ls /nsconfig/license/

CNS_V3000_SERVER_PLT_Retail.lic ssl
<!--NeedCopy-->
```

Realice un reinicio caliente para aplicar la nueva licencia, como se muestra en la captura de pantalla a continuación.

Ejemplo:

```
reboot -warm

Are you sure you want to restart NetScaler (Y/N)? [N]:y

Done
<!--NeedCopy-->
```


Una vez completado el reinicio, compruebe que la licencia se ha aplicado correctamente mediante la CLI show license.

En el ejemplo siguiente se ha instalado correctamente una licencia Premium de 3Gbps.

Ejemplo:

```
> show license

              License status:

                                    Web Logging: YES

                                              ...

                                 Model Number ID: 3000

                                    License Type: Premium License

Done

<!--NeedCopy-->
```

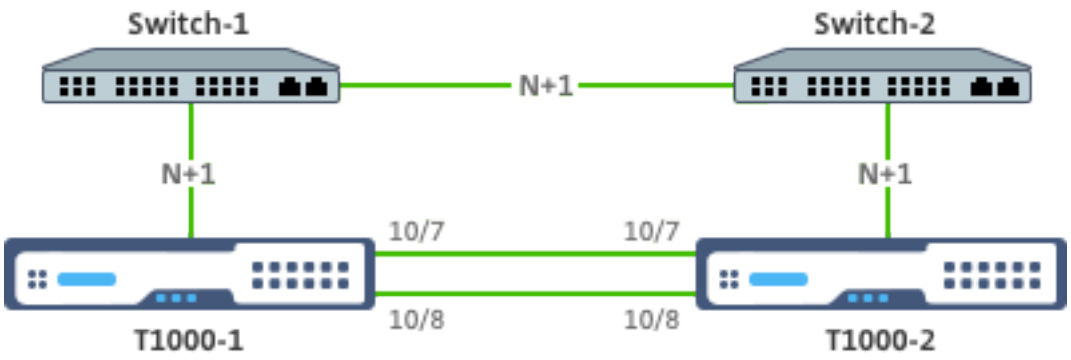
Alta disponibilidad

January 19, 2021

Alta disponibilidad (HA) hace referencia a un modo operativo activo y en espera de un par de dispositivos Citrix ADC. Cada dispositivo tiene su propia dirección IP de administración dedicada. Todas las demás direcciones IP son propiedad del dispositivo activo del par.

Conectividad

Si bien existen varias opciones de conectividad para un par Citrix ADC HA, la más recomendada se muestra en el siguiente diagrama:



En el diagrama anterior, los enlaces rojos N+1 entre cada T1000 y el conmutador respectivo implican redundancia N+1, como se explica en Conectividad. Por ejemplo, considerar una Gi-LAN de 45 Gbps N=5 es un valor apropiado, con canales LACP de 6x10GbE entre cada switch y el T1000 respectivo, así como entre los dos switches.

Se recomienda un par adicional de vínculos entre el par Citrix ADC, para proporcionar aislamiento de comunicación de alta disponibilidad de la red OAM.

Integración de GI-LAN

December 2, 2021

Por lo general, un dispositivo Citrix ADC se inserta como un nodo en línea L3 separado en la GI-LAN, de forma similar a un enrutador L3.

Ilustración: Una representación simple de un Gi-LAN

Conectividad

Se recomienda una conectividad física de Citrix ADC a los conmutadores ascendentes para proporcionar suficiente redundancia. Por ejemplo, suponiendo que un dispositivo Citrix ADC se inserte en una GI-LAN que gestiona un total (enlace ascendente+enlace descendente) de 24 Gbps, se recomienda la conectividad con 4 x 10 GbE o más interfaces. Esto proporciona efectivamente redundancia N+1 en caso de un fallo de enlace.

Los puertos relevantes del conmutador ascendente deben configurarse para la agregación de puertos LACP. La configuración relevante en Citrix ADC se describe a continuación:

Configuración de conectividad:

```
set interface 10/1 -tagall ON -lacpMode ACTIVE -lacpKey 1

set interface 10/2 -tagall ON -lacpMode ACTIVE -lacpKey 1

set interface 10/3 -tagall ON -lacpMode ACTIVE -lacpKey 1

set interface 10/4 -tagall ON -lacpMode ACTIVE -lacpKey 1
<!--NeedCopy-->
```

Puede verificar la funcionalidad adecuada de LACP mediante el comando “show interface”:

mostrar interfaz:

```
sh interface LA/1

    1)      Interface LA/1 (802.3ad Link Aggregate) #39

             flags=0x4100c020 <ENABLED, UP, AGGREGATE, UP, HAMON, 802.1
                q>

             MTU=1500, native vlan=1, MAC=02:e0:ed:33:88:b0, uptime 340
                h11m56s

             Requested: media NONE, speed AUTO, duplex NONE, fctl NONE,

             throughput 0

             Actual: throughput 4000

             LLDP Mode: NONE,

             RX: Pkts(918446) Bytes(110087414) Errs(0) Drops(795989)
                Stalls(0)

             TX: Pkts(124113) Bytes(15255532) Errs(0) Drops(0) Stalls
                (0)

```



```
21              NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0)
                   Muted(0)
22
23              Bandwidth thresholds are not set.
24
25 Disable the remaining unused interfaces and turn off the monitor.
26
27 set interface 10/5  -haMonitor OFF
28 <!--NeedCopy-->
```

Comando:

```
1 set interface 10/24  -haMonitor OFF
2
3 disable interface 10/5
4
5 disable interface 10/24
6 <!--NeedCopy-->
```

La configuración de las interfaces físicas no se comparte en las dos unidades Citrix ADC. Por lo tanto, los comandos anteriores deben ejecutarse en ambos nodos de Citrix ADC en caso de una implementación de par de alta disponibilidad.

Configuración de alta disponibilidad

Todos los demás parámetros de configuración se comparten entre los nodos Citrix ADC de un par de alta disponibilidad. Por lo tanto, la sincronización de alta disponibilidad debe habilitarse antes de que se ejecute cualquier otro comando de configuración. La configuración de alta disponibilidad básica implica los siguientes pasos:

1. Mediante exactamente el mismo hardware, software y licencia de Citrix ADC: Los pares de HA no se admiten entre diferentes modelos (es decir, un T1100 y un MPX21550) ni los mismos modelos con diferentes niveles de firmware. Consulte las instrucciones adecuadas sobre cómo actualizar un par de HA existente - Actualización a la versión 11.1.

2. Establecimiento del par HA.

Ejemplo:

```
1 netscaler-1> add HA node 1 <netscaler-2-NSIP>
2
3 netscaler-2> add HA node 1 <netscaler-1-NSIP>
```



```
<!--NeedCopy-->
```

3. Verifique que el establecimiento del par HA ejecute el siguiente comando en cualquiera de los nodos; ambos nodos deben estar visibles, uno de ellos como Primario (activo) y el otro como secundario (en espera).

Ejemplo:

```
show HA node
<!--NeedCopy-->
```

4. Active el modo a prueba de fallos y MaxFlips Esto garantiza que, en caso de un fallo del monitor de ruta en ambos nodos, al menos un nodo permanezca activo sin que el estado activo/en espera cambie constantemente.

Ejemplo:

```
set HA node  - failsafe ON

set HA node -maxFlips 3 -maxFlipTime 1200
<!--NeedCopy-->
```

5. Por último, habilite la sincronización de alta disponibilidad en los puertos dedicados dentro de Citrix ADC en lugar de en la red OAM.

Ejemplo:

```
add vlan 4080 -aliasName syncVlan

set HA node -syncvlan 4080
<!--NeedCopy-->
```

> **Nota**
>
> La VLAN 4080 en los comandos del ejemplo anterior no debe tomarse literalmente. Es posible que se reserve cualquier ID de VLAN no utilizada.

Configuración de VLAN

Una vez que las interfaces físicas se hayan configurado correctamente, puede configurar las VLAN GI-LAN apropiadas. Por ejemplo, considere un entorno GI-LAN bastante simple con un par de VLAN de

entrada/salida con un identificador de VLAN 100/101 respectivamente.

Los siguientes comandos configuran las VLAN relevantes sobre el canal LACP creado en el paso anterior.

```
add vlan 100
add vlan 101
bind vlan 100 -ifnum LA/1 -tagged
bind vlan 101 -ifnum LA/1 -tagged
<!--NeedCopy-->
```

Configuración de IPv4

Por lo general, un dispositivo Citrix ADC requiere un SNIP por VLAN. En el ejemplo siguiente se supone que las redes descritas en el diagrama de integración de GI-LAN, dado al principio de esta página, tienen una máscara de subred /24:

```
add ns ip 192.168.1.254 255.255.255.0 -vserver DISABLED -mgmtAccess
   DISABLED
add ns ip 192.168.2.254 255.255.255.0 -vserver DISABLED -mgmtAccess
   DISABLED
<!--NeedCopy-->
```

Una vez configurados los SNIP, deben asociarse a la VLAN adecuada:

```
bind vlan 100 -IPAddress 192.168.1.254 255.255.255.0
bind vlan 101 -IPAddress 192.168.2.254 255.255.255.0
<!--NeedCopy-->
```

Redirección estática IPv4

El ejemplo descrito en la sección Red de administración requiere solo un par de reglas de redirección estáticas:

- Una ruta estática 10.0.0.0/8 a los clientes a través del router de entrada
- Una ruta predeterminada a Internet a través del enrutador de salida

Ejemplo:


```
add route 0.0.0.0 0.0.0.0 192.168.2.1
add route 10.0.0.0 255.0.0.0 192.168.1.1
<!--NeedCopy-->
```

Redirección basada en directivas IPv4 (VLAN: VLAN)

Un dispositivo Citrix ADC permite la redirección basada en directivas en lugar de redirección estática, con decisiones de redirección generalmente basadas en la interfaz entrante y/o VLAN en lugar de la IP de destino. La redirección basada en directivas es una alternativa conveniente, en caso de que el rango de direcciones IP de origen del cliente esté sujeto a cambios periódicos, o una consideración obligatoria, en caso de que la dirección IP de destino de un paquete no sea suficiente por sí misma para llegar a una decisión de redirección (es decir, en caso de superposición de direcciones IP de cliente en varias VLAN).

Ejemplo:

```
add ns pbr fromWirelessToInternet ALLOW -nextHop 192.168.2.1 -vlan
    100 -priority 10

Done

 add ns pbr fromInternetToWireless ALLOW -nextHop 192.168.1.1 -vlan
     200 -priority 20

Done

apply ns pbrs
<!--NeedCopy-->
```

Configuración de IPv6

Los siguientes comandos asignan SNIP IPv6 por vlan. En el ejemplo siguiente se supone que las redes descritas en la Ilustración: Una representación simple de una Gi-LAN en esta página tienen una máscara de subred /64:

Comando:

```
add ns ip6 fd00:192:168:1::254/64 -vServer DISABLED -mgmtAccess
    DISABLED
```



```
2 add ns ip6 fd00:192:168:2::254/64 -vServer DISABLED  - mgmtAccess
     DISABLED
3 bind vlan 100 -IPAddress fd00:192:168:1::254/64
4 bind vlan 200 -IPAddress fd00:192:168:2::254/64
5 <!--NeedCopy-->
```

Redirección de IPv6

Una vez completado el direccionamiento IPv6, se puede configurar la redirección estático IPv6:

- Una ruta estática fd 00:10: :/64 a los clientes a través del enrutador de entrada
- Una ruta predeterminada a Internet a través del enrutador de salida

Ejemplo:

```
1 add route6 fd00:10::/64 fd00:192:168:1::1
2 add route6 ::/0 fd00:192:168:2::1
3 <!--NeedCopy-->
```

O el uso de redirección basada en directivas:

Ejemplo:

```
1 add ns pbr6 fromWirelessToInternetv6 ALLOW -vlan 100 -priority 10 -
     nextHop fd00:192:168:2::1
2
3 add ns pbr6 fromInternetToWirelessv6 ALLOW -vlan 200 -priority 20 -
     nextHop fd00:192:168:1::1
4
5 apply ns pbr6
6 <!--NeedCopy-->
```

Redundancia y conmutación por error de LACP

En el caso de una configuración de alta disponibilidad, se recomienda aprovechar la opción de rendimiento para configurar un umbral bajo para el canal LACP. Por ejemplo, considere una Gi-LAN de 25 Gbps y un canal de 4 x 10 GbE entre cada dispositivo Citrix ADC del par de alta disponibilidad y el conmutador ascendente para proporcionar redundancia de enlace N+1:

Ejemplo:


```
set interface LA/1 -haMonitor ON -throughput 29000
<!--NeedCopy-->
```

En caso de una falla de doble enlace entre el dispositivo principal y el conmutador ascendente, el rendimiento máximo de GI-LAN que se puede admitir caería a 20 Gbps. Un umbral bajo de 29 Gbps según el ejemplo anterior daría como resultado un evento de conmutación de redundancia en el dispositivo secundario (que no ha sufrido fallos de enlace similares), de modo que el tráfico GI-LAN no se vea afectado.

Monitores de ruta

Además de la redundancia LACP, las comprobaciones del monitor de ruta pueden configurarse y asociarse con la configuración del par de alta disponibilidad. Las comprobaciones del monitor de rutas pueden ser útiles para detectar fallas entre el dispositivo Citrix ADC y los enrutadores de siguiente salto, especialmente si dichos enrutadores no están conectados directamente, sino a través de un conmutador ascendente.

A continuación se describe una configuración típica del monitor de ruta de alta disponibilidad según la Gi-LAN de muestra en la sección 2.5.1:

```
add route 192.168.1.0 255.255.255.0 192.168.1.1 -msr ENABLED -monitor
    arp
add route 192.168.2.0 255.255.255.0 192.168.2.1 -msr ENABLED -monitor
    arp
bind HA node -routeMonitor 192.168.1.0 255.255.255.0
bind HA node -routeMonitor 192.168.2.0 255.255.255.0
<!--NeedCopy-->
```

Configuración de optimización TCP

August 20, 2021

Antes de configurar la optimización TCP, aplique las siguientes opciones de configuración básicas en el dispositivo Citrix ADC:

Configuración inicial:

```
enable ns feature LB IPv6PT
```



```
enable ns mode FR L3 USIP MBF Edge USNIP PMTUD
disable ns feature SP
disable ns mode TCPB
set lb parameter -preferDirectRoute NO
set lb parameter -vServerSpecificMac ENABLED
set l4param -l2ConnMethod Vlan
set rsskeytype -rsstype SYMMETRIC
set ns param -useproxyport DISABLED
<!--NeedCopy-->
```

> **Nota**
>
> Reinicie el dispositivo Citrix ADC si cambia el parámetro del sistema rsskeytype.

Terminación TCP

Para que Citrix ADC T1 aplique la optimización TCP, primero debe terminar el tráfico TCP entrante. Con este fin, se debe crear y configurar un vserver TCP comodín para interceptar el tráfico de entrada y luego reenviarlo al enrutador de Internet.

Entorno de redirección estática o dinámica

Para entornos con redirección estática o dinámica en su lugar, vserver puede confiar en la información de la tabla de redirecciones para reenviar paquetes hacia el enrutador de Internet. La ruta predeterminada debe apuntar al enrutador de Internet y también las entradas de redirección para las subredes del cliente hacia el enrutador inalámbrico deben estar en su lugar:

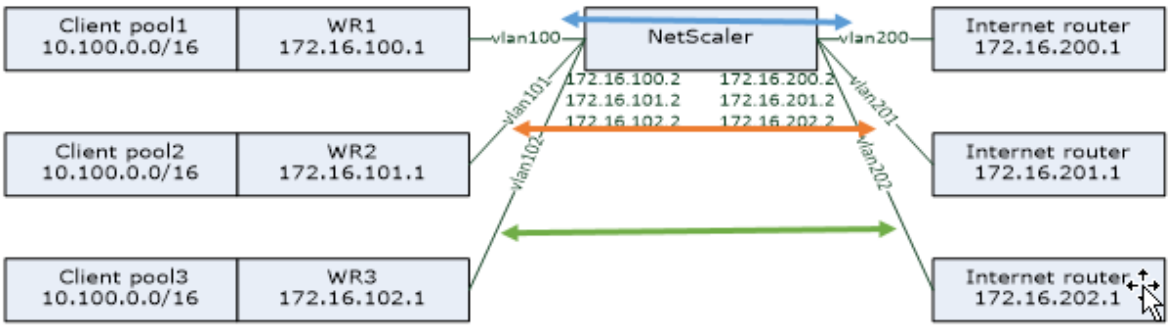
Ejemplo:

```
add lb vserver vsrv-wireless TCP * * -persistenceType NONE -
    Listenpolicy "CLIENT.VLAN.ID.EQ(100) && SYS.VSERVER("vsrv-wireless")
    .STATE.EQ(UP)" -m IP -cltTimeout 9000
add route 0.0.0.0 0.0.0.0 192.168.2.1
add route 10.0.0.0 255.0.0.0 192.168.1.1
<!--NeedCopy-->
```

Entorno de VLAN a VLAN (PBR)

Existen entornos de clientes en los que el tráfico de suscriptor se segmenta a múltiples flujos y necesita ser reenviado a diferentes enrutadores en función de los parámetros de tráfico entrante. La redirección basado en directivas (PBR) se puede utilizar para enrutar paquetes basados en parámetros de

paquetes entrantes, como VLAN, dirección MAC, interfaz, IP de origen, puerto de origen, dirección IP de destino y puerto de destino.



Ejemplo:

```
add lb vserver vsrv-wireless TCP * * -m IP -l2Conn ON -listenpolicy "
    CLIENT.VLAN.ID.EQ(100) || CLIENT.VLAN.ID.EQ(101) || CLIENT.VLAN.ID.
    EQ(102)"

add ns pbr pbr-vlan100-to-vlan200 ALLOW -vlan 100 -nexthop 172.16.200.1

add ns pbr pbr-vlan101-to-vlan201 ALLOW -vlan 101 -nexthop 172.16.201.1

add ns pbr pbr-vlan102-to-vlan202 ALLOW -vlan 102 -nexthop 172.16.202.1
<!--NeedCopy-->
```

El uso de redirección basada en directivas para enrutar el tráfico optimizado TCP es una nueva función agregada en la versión 11.1 50.10. Para versiones anteriores, tener varias entidades vserver MAC "modo" por VLAN es una solución alternativa para entornos multi-VLAN. Cada servidor virtual tiene un servicio vinculado que representa el enrutador de Internet para el flujo en particular.

Ejemplo:

```
add server internet_router_1 172.16.200.1

add server internet_router_2 172.16.201.1

add server internet_router_3 172.16.202.1

add service svc-internet-1 internet_router_1 TCP * -usip YES -
    useproxyport NO

```



```
9  add service svc-internet-2 internet_router_2 TCP * -usip YES -
       useproxyport NO
10
11 add service svc-internet-3 internet_router_3 TCP * -usip YES -
       useproxyport NO
12
13 bind service svc-internet-1 -monitorName arp
14
15 bind service svc-internet-2 -monitorName arp
16
17 bind service svc-internet-3 -monitorName arp
18
19 add lb vserver vsrv-wireless-1 TCP * * -Listenpolicy "CLIENT.VLAN.ID.EQ
       (100) && SYS.VSERVER("vsrv-wireless-1").STATE.EQ(UP)" -m MAC -l2Conn
        ON
20
21 add lb vserver vsrv-wireless-2 TCP * * -Listenpolicy "CLIENT.VLAN.ID.EQ
       (101) && SYS.VSERVER("vsrv-wireless-2").STATE.EQ(UP)" -m MAC -l2Conn
        ON
22
23 add lb vserver vsrv-wireless-3 TCP * * -Listenpolicy "CLIENT.VLAN.ID.EQ
       (102) && SYS.VSERVER("vsrv-wireless-3").STATE.EQ(UP)" -m MAC -l2Conn
        ON
24
25 bind lb vserver vsrv-wireless-1 svc-internet-1
26
27 bind lb vserver vsrv-wireless-2 svc-internet-2
28
29 bind lb vserver vsrv-wireless-3 svc-internet-3
30 <!--NeedCopy-->
```

> **Nota:**
>
> El modo vserver es MAC en contraste con ejemplos anteriores donde es el modo IP. Esto es necesario para conservar la información IP de destino cuando tenemos servicio (s) enlazado (s) a vserver. Además, la configuración de PBR adicional necesita enrutar el tráfico no optimizado.

Optimización TCP

La terminación TCP de Citrix ADC listo para usar está configurada para la funcionalidad de paso a través de TCP. El paso a través de TCP significa esencialmente que Citrix ADC T1 puede interceptar de forma transparente una secuencia TCP cliente-servidor, pero no retiene búferes de cliente/servidor independientes ni aplica ninguna técnica de optimización.

Para habilitar la optimización TCP, se utiliza un perfil TCP, denominado nstcpprofile, para especificar las configuraciones TCP que se utilizan si no se proporcionan configuraciones TCP en el nivel de servicio o servidor virtual y debe modificarse de la siguiente manera:

Comando:

```
add ns tcpProfile nstcpprofile -WS ENABLED -SACK ENABLED -WSVal 8 -mss
    1460 -maxBurst 30 -initialCwnd 16 -oooQSize 15000 -minRTO 800 -
    bufferSize 4000000 -flavor BIC -dynamicReceiveBuffering ENABLED -KA
    ENABLED -sendBuffsize 4000000 -rstWindowAttenuate ENABLED -
    spoofSynDrop ENABLED -ecn ENABLED -frto ENABLED -maxcwnd 1000000 -
    fack ENABLED -rstMaxAck enABLED -tcpmode ENDPOINT
<!--NeedCopy-->
```

> **Nota:**
>
> Si no hay ningún perfil explícitamente creado y enlazado a vserver y servicio, el perfil nstcp_default_profile está enlazado de forma predeterminada.
>
> En caso de necesidad de múltiples perfiles TCP, se pueden crear perfiles TCP adicionales y asociarlos con el servidor virtual apropiado

Comando:

```
add ns tcpProfile custom_profile -WS ENABLED -SACK ENABLED -WSVal 8 -
    mss 1460 -maxBurst 30 -initialCwnd 16 -oooQSize 15000 -minRTO 800 -
    bufferSize 4000000 -flavor BIC -dynamicReceiveBuffering ENABLED -KA
    ENABLED -sendBuffsize 4000000 -rstWindowAttenuate ENABLED -
    spoofSynDrop ENABLED -ecn ENABLED -frto ENABLED -maxcwnd 1000000 -
    fack ENABLED -rstMaxAck enABLED -tcpmode ENDPOINT

set lb vserver vsrv-wireless -tcpProfileName custom_profile
<!--NeedCopy-->
```

> **Nota:**
>
> Para implementaciones con MAC y servicio vserver -m, el mismo perfil debe estar asociado con el servicio.

```
set service svc-internet -tcpProfileName custom_profile
<!--NeedCopy-->
```


Capacidades de optimización de TCP

La mayoría de las capacidades de optimización TCP relevantes de un dispositivo Citrix ADC se exponen a través de un perfil TCP correspondiente. Los parámetros típicos de CLI que deben tenerse en cuenta al crear un perfil TCP son los siguientes:

1. **Escala de ventana (WS)**: Escalado de ventana TCP permite aumentar el tamaño de ventana de recepción TCP más allá de 65535 bytes. Ayuda a mejorar el rendimiento TCP en general y especialmente en redes de alto ancho de banda y largo retardo. Ayuda a reducir la latencia y mejorar el tiempo de respuesta a través de TCP.
2. **Reconocimiento selectivo (SACK)**: TCP SACK aborda el problema de la pérdida de múltiples paquetes que reduce la capacidad de rendimiento general. Con el acuse de recibo selectivo, el receptor puede informar al remitente sobre todos los segmentos que se reciben correctamente, permitiendo al remitente solo retransmitir los segmentos que se perdieron. Esta técnica ayuda a T1 a mejorar el rendimiento general y reducir la latencia de conexión.
3. **Factor de escala de ventana (WsVal)**: Factor utilizado para calcular el nuevo tamaño de ventana. Debe configurarse con un valor alto para permitir que la ventana anunciada por NS sea al menos igual al tamaño del búfer.
4. **Tamaño máximo del segmento (MSS)**: MSS de un único segmento TCP. Este valor depende de la configuración de MTU en enrutadores intermedios y clientes finales. Un valor de 1460 corresponde a una MTU de 1500.
5. **MaxBurst**: Número máximo de segmentos TCP permitidos en una ráfaga.
6. **Tamaño de la ventana de congestión inicial (InitialCwnd)**: El tamaño de la ventana de congestión inicial TCP determina el número de bytes que pueden estar pendientes al comienzo de la transacción. Permite a T1 enviar esos muchos bytes sin preocuparse por la congestión en el cable.
7. **Tamaño máximo de cola de paquetes OOO (OOQSize)**: TCP mantiene la cola Fuera de orden para mantener los paquetes OOO en la comunicación TCP. Esta configuración afecta a la memoria del sistema si el tamaño de la cola es largo, ya que los paquetes deben mantenerse en la memoria en tiempo de ejecución. Por lo tanto, esto debe mantenerse en un nivel optimizado basado en el tipo de funciones de la red y la aplicación.
8. **RTO mínimo (minRto)**: El tiempo de espera de retransmisión TCP se calcula en cada ACK recibido según la lógica de implementación interna. El tiempo de espera de retransmisión predeterminado ocurre en 1 segundo para empezar y esto se puede ajustar con esta configuración. Para la segunda retransmisión de estos paquetes RTO se calculará por N*2 y luego N*4… N*8… continúa hasta el último intento de retransmisión.
9. **BufferSize/sendBuffSize**: Se refieren a la cantidad máxima de datos que el T1 puede recibir del servidor y búfer internamente sin enviarlo al cliente. Deben establecerse en un valor mayor (al menos doble) que el producto de demora de ancho de banda del canal de transmisión subyacente.
10. **sabor**: Esto se refiere al algoritmo de control de congestión TCP. Los valores válidos son Default,

BIC, CUBIC, Westwood y Nile.

11. Almacenamiento en **búfer de recepción dinámico**: Permite que el búfer de recepción se ajuste dinámicamente en función de las condiciones de memoria y red. Llenará el búfer tanto como sea necesario para mantener el proceso de descarga del cliente llena en lugar de llenar, leyendo con anticipación desde el servidor, un búfer de tamaño fijo, ya que este último se especifica en el perfil TCP y normalmente se basa en criterios como 2* BDP, para una conexión. Citrix ADC T1 supervisa las condiciones de red para el cliente y calcula cuánto debe leer con anticipación desde el servidor.
12. **Keep-Alive (KA)**: Envíe sondeos TCP keep-alive (KA) periódicos para comprobar si el par sigue activo.
13. RstWindowAttenuate: Defender TCP contra ataques de suplantación. Responderá con ACK correctivo cuando un número de secuencia no es válido.
14. **RstMaxack**: Habilita o inhabilita la aceptación de RST que está fuera de la ventana pero hace eco del número de secuencia ACK más alto.
15. **SpoofSynDrop**: Caída de paquetes SYN no válidos para proteger contra la suplantación de identidad.
16. **Notificación explícita de congestión (ecn)**: Envía una notificación del estado de congestión de la red al remitente de los datos y toma medidas correctivas para la congestión de los datos o la corrupción de los datos.
17. **Reenviar RTO-recuperación**: En caso de retransmisiones falsas, las configuraciones de control de congestión se revierten a su estado original.
18. **Ventana de congestión máxima TCP (maxcwnd)**: Tamaño máximo de ventana de congestión TCP configurable por el usuario.
19. **Reconocimiento directo (FACK)**: Para evitar la congestión TCP midiendo explícitamente el número total de bytes de datos pendientes en la red y ayudando al remitente (ya sea T1 o cliente) a controlar la cantidad de datos inyectados en la red durante los tiempos de espera de retransmisión.
20. **tcpmode**: Modos de optimización TCP para perfil específico. Hay dos modos de optimización TCP: Transparente y Endpoint.

    - Punto final. En este modo, el dispositivo administra las conexiones de cliente y servidor por separado.
    - Transparente. En el modo transparente, los clientes necesitan acceder directamente a los servidores, sin ningún servidor virtual que intervenga. Las direcciones IP del servidor deben ser públicas porque los clientes necesitan poder acceder a ellas. En el ejemplo que se muestra en la siguiente ilustración, se coloca un dispositivo NetScaler entre el cliente y el servidor, de modo que el tráfico debe pasar por el dispositivo.

Dejar silenciosamente las conexiones inactivas

En una red de telecomunicaciones, casi el 50% de las conexiones TCP de un dispositivo Citrix ADC quedan inactivas y el dispositivo envía paquetes RST para cerrarlos. Los paquetes enviados a través de canales de radio activan esos canales innecesariamente, lo que causa un flujo de mensajes que a su vez hacen que el dispositivo genere un flujo de mensajes de rechazo de servicio. El perfil TCP predeterminado ahora incluye los parámetros DropAlfClosedConnonTimeout y DropestConnonTimeout, que de forma predeterminada están inhabilitados. Si habilita ambos, ni una conexión medio cerrada ni una conexión establecida hacen que se envíe un paquete RST al cliente cuando se agote el tiempo de espera de la conexión. El dispositivo solo deja caer la conexión.

```
set ns tcpProfile nstcpprofile  -DropHalfClosedConnOnTimeout ENABLED
set ns tcpProfile nstcpprofile  -DropEstConnOnTimeout ENABLED
<!--NeedCopy-->
```

Análisis e informes

October 5, 2021

TCP Speed Reporting es una función de Citrix ADC que extrae estadísticas de conexión TCP, como medida del rendimiento de descarga y carga de TCP, y se utiliza en los informes TCP Insight de Citrix Application Delivery Management (ADM). Para lograrlo, Citrix ADC supervisa cada conexión TCP, localiza ráfagas de paquetes en función del tiempo de espera inactivo e informa de métricas clave (como el recuento de bytes, el recuento de bytes retransmitidos y la duración) para la ráfaga máxima identificada. La función de informes de velocidad TCP está habilitada de forma predeterminada, admite servidores virtuales TCP y HTTP y depende de la infraestructura de informes de AppFlow/ULFD.

Estadísticas en tiempo real

August 20, 2021

El comando stat puede utilizarse para verificar que la optimización TCP se aplica correctamente:

Comando:

```
> stat lb vserver vsrv-wireless
Virtual Server Summary
```



```
3                        vsvrIP  port     Protocol        State   Health
                            actSvcs
4  vsrv...eless               *     0          TCP           UP      100
           1
5
6             inactSvcs
7  vsrv...eless       0
8  Virtual Server Statistics
9                                            Rate (/s)
                                                Total
10 Vserver hits                                      0
       10
11 Requests                                          0
                         0
12 Responses                                         0
                         0
13 Request bytes                                     0
       1580
14 Response bytes                                    0
       532594360
15 Total Packets rcvd                                0
       216463
16 Total Packets sent                                0
       369898
17 Current client connections                       --
                         0
18 Current Client Est connections                   --
                         0
19 Current server connections                       --
                         0
20 Requests in surge queue                          --
                         0
21 Requests in vserver's surgeQ                     --
                         0
22 Requests in service's surgeQs                    --
                         0
23 Spill Over Threshold                             --
                         0
24 Spill Over Hits                                  --
                         0
25 Labeled Connection                               --
                         0
26 Push Labeled Connection                          --
                         0
27 Deferred Request                                  0
```



```
                          0
Invalid Request/Response                          --
                          0
Invalid Request/Response Dropped                  --
                          0
Bound Service(s) Summary
                             IP  port         Type        State     Hits
                                   Hits/s
svc-internet     192.168.2.2     0           TCP           UP       10
         0/s

                 Req    Req/s      Rsp    Rsp/s Throughp ClntConn
                    SurgeQ
svc-internet       0      0/s        0      0/s        0        0
            0
                  SvrConn   ReuseP  MaxConn ActvTran  SvrTTFB     Load
svc-internet         0        0        0        0        0        0
```

Los contadores Totales deben aumentar constantemente para el sistema operativo. Además, los contadores Tasa deben ser distintos de cero.

> **Nota**
>
> La salida anterior proviene de un sistema de laboratorio operativo pero inactivo, explicando la tasa cero.

SNMP

January 12, 2021

El agente SNMP se puede consultar para obtener información específica del sistema desde un dispositivo remoto (SNMP Manager). En función de la consulta, el agente busca el identificador de objeto igual (OID) en la base de información de administración (MIB) para los datos solicitados y envía la información al administrador SNMP. Los siguientes son los OID SNMP más útiles para implementaciones de telecomunicaciones:

Memoria

- **resMemUsage (1.3.6.1.4.1.5951.4.1.1.41.2)**

Porcentaje de utilización de memoria en Citrix ADC.

CPU del motor de paquetes

- **resCpuUsage (1.3.6.1.4.1.5951.4.1.1.41.1)**

Porcentaje de utilización de CPU.

- **nsCPUTable (1.3.6.1.4.1.5951.4.1.1.41.6)**

Esta tabla contiene información sobre cada CPU en Citrix ADC.

Indexado en: NSCPUname

- **nsCPUname (1.3.6.1.4.1.5951.4.1.1.41.6.1.1)**

El nombre de la CPU.

- **nsCPUusage (1.3.6.1.4.1.5951.4.1.1.41.6.1.2)**

Porcentaje de utilización de CPU.

Rendimiento

- **allNicTotRxMbits (1.3.6.1.4.1.5951.4.1.1.71.1)**

Número de megabits recibidos por el dispositivo Citrix ADC.

- **allNicTotTxMbits (1.3.6.1.4.1.5951.4.1.1.71.2)**

Número de megabits transmitidos por el dispositivo Citrix ADC.

- **ipTotRxPkts (1.3.6.1.4.1.5951.4.1.1.43.25)**

Paquetes IP recibidos.

- **ipTotRxMbits (1.3.6.1.4.1.5951.4.1.1.43.27)**

Megabits de datos IP recibidos.

- **ipTotTxPkts (1.3.6.1.4.1.5951.4.1.1.43.28)**

Paquetes IP transmitidos.

- **ipTotTxMbits (1.3.6.1.4.1.5951.4.1.1.43.30)**

Megabits de datos IP transmitidos.

Conexiones

Conexiones activas:

- **tcpActiveServerConn (1.3.6.1.4.1.5951.4.1.1.46.8)**

Conexiones a un servidor que responde actualmente a las solicitudes.

Total de conexiones:

- **tcpCurServerConn (1.3.6.1.4.1.5951.4.1.1.46.1)**

Conexiones de servidor, incluidas las conexiones en los estados Apertura, Establecida y Cierre.

- **tcpCurClientConn (1.3.6.1.4.1.5951.4.1.1.46.2)**

Conexiones de cliente, incluidas las conexiones en los estados Apertura, Establecida y Cierre.

Nota: Debido a Syn Cookie, esto no incluye al cliente en estado de apertura

- **tcpTotZombieCltConnFlushed (1.3.6.1.4.1.5951.4.1.1.46.26)**

Conexiones de cliente que se vacían porque el cliente ha estado inactivo durante algún tiempo.

- **tcpTotZombieSvrConnFlushed (1.3.6.1.4.1.5951.4.1.1.46.27)**

Conexiones de servidor que se vacían porque no ha habido solicitudes de cliente en la cola durante algún tiempo.

Errores

- **tcpErrSynGiveUp (1.3.6.1.4.1.5951.4.1.1.46.37)**

Intenta establecer una conexión en el Citrix ADC que se agotó el tiempo de espera.

- **tcpErrRetransmitGiveUp (1.3.6.1.4.1.5951.4.1.1.46.60)**

Número de veces que Citrix ADC termina una conexión después de retransmitir el paquete siete veces en esa conexión. La retransmisión ocurre cuando el final de recepción no reconoce el paquete.

- **ifInDiscards (1.3.6.1.2.1.2.2.1.13)**

El número de paquetes entrantes que se eligieron para ser descartados aunque no se habían detectado errores para evitar que fueran entregables a un protocolo de capa superior. Una posible razón para descartar un paquete de este tipo podría ser liberar espacio en el búfer.

- **ifOutDiscards (1.3.6.1.2.1.2.2.1.19)**

El número de paquetes salientes que se eligieron para ser descartados aunque no se habían detectado errores para evitar su transmisión. Una posible razón para descartar un paquete de este tipo podría ser liberar espacio en el búfer.

- **ifErrTxOverflow (1.3.6.1.4.1.5951.4.1.1.54.1.36)**

Número de paquetes que han pasado a través de las colas de desbordamiento durante la transmisión en la interfaz especificada, desde que se inició el dispositivo Citrix ADC o se borraron las estadísticas de la interfaz. Esto se incrementa solo en puertos congestionados.

Conexiones optimizadas/de omisión

- **tcpOptimizationEnabled (1.3.6.1.4.1.5951.4.1.1.46.131)**

Número total de conexiones habilitadas con optimización TCP.

- **tcpOptimizationBypassed (1.3.6.1.4.1.5951.4.1.1.46.132)**

Número total de conexiones omitirse Optimización TCP.

Recetas técnicas

August 20, 2021

Los modelos Citrix ADC T1 proporcionan funciones avanzadas y un lenguaje de configuración de directivas potente que permiten evaluar decisiones complejas en tiempo de ejecución.

Aunque no es posible evaluar todas las capacidades potencialmente desbloqueadas por las funciones de T1000 y la guía de configuración de directivas, los receptores técnicos consideran la implementación de varios requisitos presentados por los operadores de telecomunicaciones. Siéntase libre de reutilizar las "recetas" tal como están o adaptarse a su entorno.

Límite de conexión por usuario

El modelo Citrix ADC T1 se puede configurar para limitar el número de conexiones por IP de suscriptor único. Con la configuración siguiente, se permiten N conexiones TCP simultáneas por IP (CLIENT.IP.SRC). Por cada intento de conexión más allá del umbral configurado, T1 envía un RST. Para un máximo de 2 conexiones simultáneas por usuario:

Comando:

```
1 add stream selector streamSel_usrlimit CLIENT.IP.SRC
2 add ns limitIdentifier limitId_usrlimit -threshold 2 -mode CONNECTION -
     selectorName streamSel_usrlimit
3 add responder policy respPol_usrlimit "SYS.CHECK_LIMIT("
     limitId_usrlimit")" RESET
4 bind lb vserver vsrv-wireless -policyName respPol_usrlimit -priority 1
     -gotoPriorityExpression END
5 <!--NeedCopy-->
```

Inserción/eliminación suave de Vserver

Muchos operadores se preocupan por la interrupción de las conexiones TCP cuando el modelo Citrix ADC T1 se activa en línea para la optimización TCP o cuando se inhabilita para fines de mantenimiento.

Para evitar romper las conexiones existentes cuando se introduce vserver, se debe aplicar la siguiente configuración antes de configurar o activar vserver para la optimización TCP:

Comando:

```
add ns acl acl-ingress ALLOW -vlan 100
add forwardingSession fwd-ingress -aclname acl-ingress
apply ns acls
<!--NeedCopy-->
```

Las sesiones de reenvío son efectivas sobre la redirección (estático o dinámico o PBR) y crean entradas de sesión para el tráfico enrutado (modo L3). Cualquier conexión existente se maneja mediante reenvío de sesión debido a las sesiones correspondientes, y después de la introducción del servidor virtual comienza a capturar solo nuevas conexiones TCP.

Las ACL se pueden configurar para capturar solo puertos específicos como vserver, a fin de evitar la creación de sesiones para tráfico innecesario, que consume memoria. Otra opción es eliminar la configuración específica después de la activación de vserver.

Para fines de mantenimiento, vserver debe estar inhabilitado y su estado aparece como OUT ODE SERVICIO. Cuando esto sucede, el servidor vserver termina todas las conexiones inmediatamente de forma predeterminada. Para que vserver siga sirviendo las conexiones existentes y no acepte nuevas, se debe aplicar la siguiente configuración:

Comando:

```
set lb vserver vsrv-wireless -downStateFlush DISABLED
<!--NeedCopy-->
```

Las nuevas conexiones pasan por la tabla de redirecciones y las entradas de sesión correspondientes se crean debido a las sesiones de reenvío.

Perfiles TCP basados en directivas

La selección de perfiles TCP basada en directivas permite a los operadores configurar el perfil TCP dinámicamente para clientes procedentes de diferentes dominios de tráfico (es decir, 3G o 4G). Algunas de las métricas QoS son diferentes para estos dominios de tráfico, y para lograr un mejor rendimiento, necesita cambiar parte del parámetro TCP dinámicamente. Considere un caso en el que los clientes procedentes de 3G y 4G golpean el mismo servidor virtual y usan el mismo perfil TCP, lo que tiene un impacto negativo en el rendimiento de algunos clientes. La funcionalidad AppQoE puede clasificar estos clientes y cambiar dinámicamente el perfil TCP en vserver.

Ejemplo:

```
enable feature AppQoE

add ns tcpProfile nstcpprofile1 -WS ENABLED -SACK ENABLED -WSVal 8 -mss
     1460 -maxBurst 30 -initialCwnd 16 -oooQSize 15000 -minRTO 800 -
    slowStartIncr 1 -bufferSize 4000000 -flavor BIC -KA ENABLED -
    sendBuffsize 4000000 -rstWindowAttenuate ENABLED -spoofSynDrop
    ENABLED -frto ENABLED -maxcwnd 1000000 -fack ENABLED -tcpmode
    ENDPOINT

add ns tcpProfile nstcpprofile2 -WS ENABLED -SACK ENABLED -WSVal 8 -mss
     1460 -maxBurst 15 -initialCwnd 16 -oooQSize 15000 -minRTO 800 -
    slowStartIncr 1 -bufferSize 128000 -flavor BIC -KA ENABLED -
    sendBuffsize 6000000 -rstWindowAttenuate ENABLED -spoofSynDrop
    ENABLED -frto ENABLED -maxcwnd 64000 -fack ENABLED -tcpmode ENDPOINT

add appqoe action action_1 -priority HIGH -tcpprofile nstcpprofile1

add appqoe action action_2 -priority HIGH -tcpprofile nstcpprofile2

add appqoe policy appqoe_4G -rule "CLIENT.VLAN.ID.EQ(100)" -action
    action_1

add appqoe policy appqoe_3G -rule "CLIENT.VLAN.ID.EQ(200)" -action
    action_2

bind lb vserver vsrv-wireless -policyName appqoe_4G -priority 100

bind lb vserver vsrv-wireless -policyName appqoe_3G -priority 110
<!--NeedCopy-->
```

El modelo Citrix ADC T1 es capaz de recibir la información del suscriptor dinámicamente a través de la interfaz Gx o Radius o y Gx y aplicar diferentes perfiles TCP por suscriptor.

Comando:

```
add appqoe action action_1 -priority HIGH -tcpprofile nstcpprofile1

add appqoe action action_2 -priority HIGH -tcpprofile nstcpprofile2

add appqoe policy appqoe_4G -rule "SUBSCRIBER.RULE_ACTIVE("3G")" -
    action action_1
```



```
6
7 add appqoe policy appqoe_3G -rule "SUBSCRIBER.RULE_ACTIVE("4G")" -
     action action_2
8 <!--NeedCopy-->
```

Para la integración del modelo Citrix ADC T1 con la red del plano de control del operador, consulte Administración de suscriptores de telecomunicaciones.

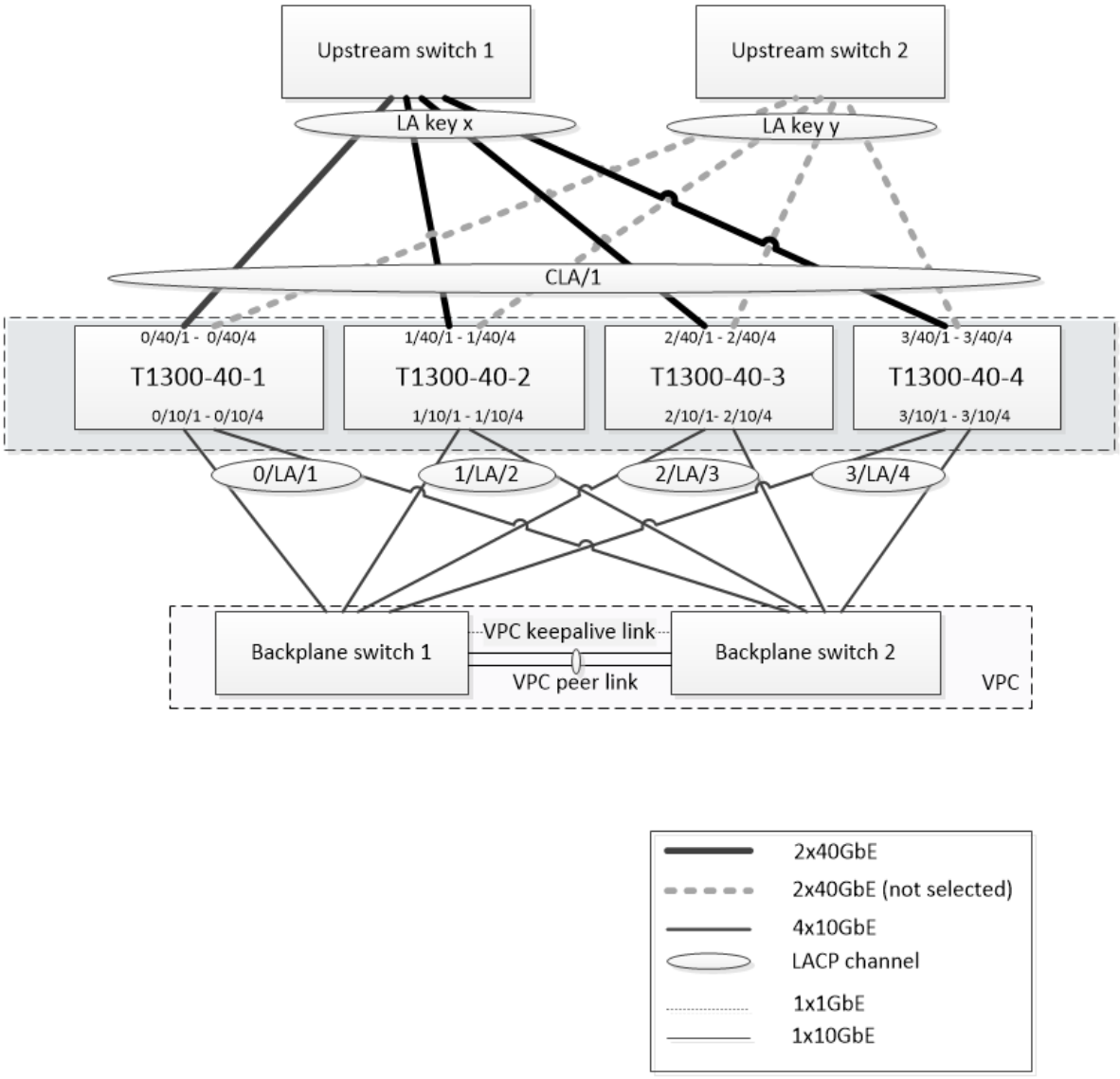
Escalabilidad

August 20, 2021

Debido a que la optimización TCP requiere muchos recursos, es posible que un único dispositivo Citrix ADC, incluso un dispositivo —de gama alta, no pueda soportar altos rendimientos de GI-LAN. Para ampliar la capacidad de la red, puede implementar dispositivos Citrix ADC en una formación de clúster N+1. En una implementación de clúster, los dispositivos Citrix ADC funcionan juntos como una única imagen del sistema. El tráfico del cliente se distribuye a través de los nodos del clúster con la ayuda de un dispositivo de conmutador externo.

Topología

La ilustración 1 es un ejemplo de un clúster que consta de cuatro nodos T1300-40G.



La configuración mostrada en la Imagen 1 tiene las siguientes propiedades:

1. Todos los nodos del clúster pertenecen a la misma red (también conocida como clúster L2).
2. El tráfico del plano de datos y del backplane se maneja mediante diferentes conmutadores.
3. Suponiendo que el rendimiento de GI-LAN es de 200 Gbps y que un dispositivo T1300-40G puede soportar 80 Gbps de rendimiento, necesitamos tres dispositivos T1300-40G. Para proporcionar redundancia en caso de fallo de nodo de clúster único, implementamos cuatro dispositivos en total.
4. Cada nodo recibirá hasta 67 Gbps de tráfico (50 Gbps en condiciones normales de funcionamiento y 67 Gbps en caso de fallo de nodo de clúster único), por lo que necesita conexiones de 2 x 40 Gbps al conmutador ascendente. Para proporcionar redundancia en caso de falla del switch, implementamos un par de switches ascendentes y duplicamos el número de conexiones.

5. La agregación de vínculos de clúster (CLAG) se utiliza para distribuir el tráfico entre los nodos de clúster. Un único CLAG maneja tanto el tráfico de cliente como el de servidor. La redundancia de enlaces está habilitada en el CLAG, por lo que solo se selecciona un "subcanal" en un momento dado y se encarga del tráfico. Si algún enlace falla o el rendimiento cae por debajo del umbral especificado, se selecciona el otro subcanal.
6. El conmutador ascendente realiza un equilibrio de carga de canal de puerto simétrico (por ejemplo, el algoritmo de origen dest-ip de solo IP de Cisco IOS 7.0 (8) N1 (1)) de modo que los flujos de tráfico hacia adelante y hacia atrás sean manejados por el mismo nodo de clúster. Esta propiedad es deseable porque elimina el reordenamiento de paquetes, lo que degradaría el rendimiento TCP.
7. Se espera que el cincuenta por ciento del tráfico de datos se dirigirá al plano anterior, lo que significa que cada nodo conducirá hasta 34 Gbps a otros nodos de clúster (25 Gbps en condiciones normales de funcionamiento y 34 Gbps en caso de fallo de nodo de clúster único). Por lo tanto, cada nodo necesita al menos 4x10G conexiones al conmutador de plano anterior. Para proporcionar redundancia en caso de error del conmutador, implementamos un par de conmutadores de plano anterior y duplicamos el número de conexiones. Actualmente, la redundancia de enlace no es compatible con el plano anterior, por lo que se quiere Cisco VPC o tecnología equivalente para lograr la redundancia a nivel de conmutador.
8. El tamaño de MTU de los paquetes dirigidos es de 1578 bytes, por lo que los conmutadores de plano anterior deben admitir una MTU de más de 1500 bytes.

Nota: El diseño representado en la ilustración 1 también es aplicable a los dispositivos T1120 y T1310. Para T1310 usaríamos interfaces 40GbE para las conexiones de plano anterior, ya que carece de puertos 10GbE.

Nota: Si bien en este documento se utiliza Cisco VPC como ejemplo, si se trabaja con conmutadores que no son de Cisco podrían utilizarse soluciones equivalentes alternativas, como el MLAG de Juniper.

Nota: Aunque otras topologías como ECMP en lugar de CLAG son posibles, actualmente no se admiten para este caso de uso particular.

Configuración de la optimización TCP en un clúster Citrix ADC T1000

Una vez completadas la instalación física, la conectividad física, la instalación de software y las licencias, puede continuar con la configuración del clúster real. Las configuraciones descritas a continuación se aplican al clúster representado en la Imagen 1.

Nota: Para obtener más información sobre la configuración del clúster, consulte Configuración de un clúster de Citrix ADC.

Suponga que los cuatro nodos T1300 de la Imagen 1 tienen las siguientes direcciones NSIP:

Cuatro nodos T1300 con dirección NSIP:


```
T1300-40-1: 10.102.29.60
T1300-40-2: 10.102.29.70
T1300-40-3: 10.102.29.80
T1300-40-4: 10.102.29.90
```

El clúster se administrará a través de la dirección IP del clúster (CLIP), que se supone que es 10.78.16.61.

Configuración del clúster

Para comenzar a configurar el clúster que se muestra en la Imagen 1, inicie sesión en el primer dispositivo que quiera agregar al clúster (por ejemplo, T1300-40-1) y haga lo siguiente.

1. En la solicitud de comando, escriba los siguientes comandos:

   Comando:

```
> add cluster instance 1
> add cluster node 0 10.102.29.60 -state ACTIVE
> add ns ip 10.102.29.61 255.255.255.255 -type clip
> enable cluster instance 1
> save ns config
> reboot  - warm
```

2. Después de reiniciar el dispositivo, conéctese a la dirección IP del clúster (CLIP) y agregue el resto de los nodos al clúster:

   Comando:

```
> add cluster node 1 10.102.29.70 -state ACTIVE
> add cluster node 2 10.102.29.80 -state ACTIVE
> add cluster node 3 10.102.29.90  - state ACTIVE
> save ns config
```

3. Conéctese a la dirección NSIP de cada uno de los nodos recién agregados y únase al clúster:

   Comando:

```
> join cluster -clip 10.102.29.61 -password nsroot
> save ns config
> reboot  - warm
```


4. Después de reiniciar los nodos, continúe con la configuración del plano posterior. En la dirección IP del clúster, escriba los siguientes comandos para crear un canal LACP para el vínculo de backplane de cada nodo del clúster:

   Comando:

```
> set interface 0/10/[1-8] -lacpkey 1 -lacpmode ACTIVE
> set interface 1/10/[1-8] -lacpkey 2 -lacpmode ACTIVE
> set interface 2/10/[1-8] -lacpkey 3 -lacpmode ACTIVE
> set interface 3/10/[1-8] -lacpkey 4 -lacpmode ACTIVE
```

5. Del mismo modo, configure LA dinámica y VPC en los conmutadores del plano posterior. Asegúrese de que la MTU de las interfaces del conmutador de backplane tenga al menos 1578 bytes.
6. Verifique que los canales estén operativos:

   Comando:

```
> show channel 0/LA/1
> show channel 1/LA/2
> show channel 2/LA/3
> show channel 3/LA/4
```

7. Configure las interfaces del plano posterior del nodo del clúster.

   Comando:

```
> set cluster node 0 -backplane 0/LA/1
> set cluster node 1 -backplane 1/LA/2
> set cluster node 2 -backplane 2/LA/3
> set cluster node 3 -backplane 3/LA/4
```

8. Compruebe el estado del clúster y compruebe que el clúster está operativo:

```
> show cluster instance
> show cluster node
```

Para obtener más información sobre la configuración del clúster, consulte Configuración de un clúster de Citrix ADC

Distribuir tráfico entre nodos de clúster

Después de haber formado el clúster Citrix ADC, implemente la Agregación de vínculos de clúster (CLAG) para distribuir el tráfico entre los nodos de clúster. Un único enlace CLAG manejará tanto el tráfico de cliente como el de servidor.

En la dirección IP del clúster, ejecute los siguientes comandos para crear el grupo de agregación de vínculos de clúster (CLAG) que se muestra en la Imagen 1:

Comando:

```
> set interface 0/40/[1-4] -lacpMode active -lacpKey 5 -lagType Cluster
> set interface 1/40/[1-4] -lacpMode active -lacpKey 5 -lagType Cluster
> set interface 2/40/[1-4] -lacpMode active -lacpKey 5 -lagType Cluster
> set interface 3/40/[1-4] -lacpMode active -lacpKey 5 -lagType Cluster
```

Configure la agregación de vínculos dinámicos en los conmutadores externos.

A continuación, habilite Redundancia de vínculos de la siguiente manera:

Código:

```
> set channel CLA/1 -linkRedundancy ON -lrMinThroughput 240000
```

Por último, compruebe el estado del canal introduciendo:

Comando:

```
> show channel CLA/1
```

El canal debe estar UP y el rendimiento real debe ser 320000.

Para obtener más información acerca de la agregación de vínculos de clúster, consulte los temas siguientes:

- Agregación dinámica de vínculos de clúster
- Redundancia de vínculos en un clúster con LACP.

Debido a que vamos a utilizar el reenvío basado en MAC (MBF), configurar un conjunto de vínculos y vincularlo al grupo CLAG de la siguiente manera:

Comando:


```
> add linkset LS/1
> bind linkset LS/1 -ifnum CLA/1
```

Para obtener más información acerca de los conjuntos de vínculos, consulte los siguientes temas:

- Configuración de conjuntos de vínculos
- Uso del canal LA de clúster con conjuntos de enlaces

Configuración de direcciones VLAN e IP

Utilizaremos la configuración IP de rayas, lo que significa que las direcciones IP están activas en todos los nodos (configuración predeterminada). Consulte Configuraciones rayadas, parcialmente rayadas y manchadas para obtener más información sobre este tema.

1. Agregue los SNIP de entrada y salida:

   Comando:

```
> add ns ip 172.16.30.254 255.255.255.0 -type SNIP
> add ns ip 172.16.31.254 255.255.255.0 -type SNIP
> add ns ip6 fd00:172:16:30::254/112 -type SNIP
> add ns ip6 fd00:172:16:31::254/112 -type SNIP
```

2. Agregue las VLAN de entrada y salida correspondientes:

   Comando:

```
> add vlan 30 -aliasName wireless
> add vlan 31 -aliasName internet
```

3. Vincular VLAN con IPs y conjunto de vínculos:

   Comando:

```
> bind vlan 31 -ifnum LS/1 -tagged
> bind vlan 30 -ifnum LS/1 -tagged
> bind vlan 30 -IPAddress 172.16.30.254 255.255.255.0
> bind vlan 31 -IPAddress 172.16.31.254 255.255.255.0
> bind vlan 30 -IPAddress fd00:172:16:30::254/112
> bind vlan 31 -IPAddress fd00:172:16:31::254/112
```

Se pueden agregar más VLAN de entrada y salida si es necesario.

Configuración de Optimización TCP

En este punto, hemos aplicado todos los comandos específicos del clúster. Para completar la configuración, siga los pasos descritos en Configuración de optimización TCP.

Configuración de redirección dinámica

Un clúster de Citrix ADC se puede integrar en el entorno de redirección dinámica de la red del cliente. A continuación se muestra un ejemplo de configuración de redirección dinámica mediante el protocolo de redirección BGP (también se admite OSPF).

1. Desde la dirección CLIP, habilite BGP y el redirección dinámica en las direcciones IP de entrada y salida:

   Comando:

```
> enable ns feature bgp
> set ns ip 172.16.30.254 -dynamicRouting ENABLED
> set ns ip 172.16.31.254 -dynamicRouting ENABLED
```

2. Abra vtysh y configure BGP para el lado de salida:

   Código:

```
> shell
root@ns# vtysh
ns# configure terminal
ns(config)# router bgp 65531
ns(config-router)# network 10.0.0.0/24
ns(config-router)# neighbor 172.16.31.100 remote-as 65530
ns(config-router)# neighbor 172.16.31.100 update-source
    172.16.31.254
ns(config-router)# exit
ns(config)# ns route-install propagate
ns(config)# ns route-install default
ns(config)# ns route-install bgp
ns(config)# exit
```

3. Configure el peer BGP del lado de salida para anunciar la ruta predeterminada al clúster de Citrix ADC. Por ejemplo:

   Comando:


```
router bgp 65530
 bgp router-id 172.16.31.100
 network 0.0.0.0/0
 neighbor 172.16.31.254 remote-as 65531
```

4. Siga pasos similares para configurar el lado de entrada.
5. Desde vtysh, compruebe que la configuración se propaga a todos los nodos del clúster, introduciendo:

   Comando:

```
ns# show running-config
```

6. Finalmente, inicie sesión en la dirección NSIP de cada nodo del clúster y verifique las rutas anunciadas desde el peer BGP:

   Comando:

```
> show route | grep BGP
```

Optimización del rendimiento TCP mediante TCP Nile

August 20, 2021

TCP utiliza las siguientes técnicas de optimización y estrategias de control de congestión (o algoritmos) para evitar la congestión de red en la transmisión de datos.

Estrategias de control de congestión

El Protocolo de control de transmisión (TCP) se ha utilizado durante mucho tiempo para establecer y administrar conexiones a Internet, manejar errores de transmisión y conectar aplicaciones web sin problemas con dispositivos cliente. Pero el tráfico de red se ha vuelto más difícil de controlar, porque la pérdida de paquetes no depende solo de la congestión en la red, y la congestión no necesariamente causa la pérdida de paquetes. Por lo tanto, para medir la congestión, un algoritmo TCP debe centrarse tanto en la pérdida de paquetes como en el ancho de banda.

Algoritmo NILE

Citrix Systems ha desarrollado un nuevo algoritmo de control de congestión, NILE, un algoritmo de optimización TCP diseñado para redes de alta velocidad como LTE, LTE avanzado y 3G. Nile aborda desafíos únicos causados por la decoloración, pérdidas aleatorias o congestivas, retransmisiones de capa de enlace y agregación de portadoras.

El algoritmo NILE:

- Basa las estimaciones de latencia de cola en mediciones de tiempo de ida y vuelta.
- Utiliza una función de aumento de la ventana de congestión que es inversamente proporcional a la latencia de la cola medida. Este método resulta en acercarse al punto de congestión de red más lentamente que el método TCP estándar, y reduce las pérdidas de paquetes durante la congestión.
- Puede distinguir entre pérdida aleatoria y pérdida basada en congestión en la red mediante el uso de la latencia de cola estimada.

Los proveedores de servicios de telecomunicaciones pueden utilizar el algoritmo NILE en su infraestructura TCP para:

- Optimice las redes móviles y de larga distancia: El algoritmo NILE logra un rendimiento superior en comparación con TCP estándar. Esta función es especialmente importante para redes móviles y de larga distancia.
- Disminuir la latencia percibida por las aplicaciones y mejorar la experiencia del suscriptor: El algoritmo de Nile utiliza información de pérdida de paquetes para determinar si el tamaño de la ventana de transmisión debe aumentarse o reducirse, y utiliza información de demora en la cola para determinar el tamaño del incremento o disminución. Esta configuración dinámica del tamaño de la ventana de transmisión disminuye la latencia de la aplicación en la red.

Para configurar la compatibilidad con NILE mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba lo siguiente:

```
set ns tcpProfile <name> [-flavor NILE]
<!--NeedCopy-->
```

Configuración de la compatibilidad con NILE mediante la utilidad de configuración

1. Vaya a **Sistema** > **Perfiles** > **Perfiles TCP** y haga clic en **Perfiles TCP**.
2. En la lista desplegable **TCP Flavor**, seleccione **NILE**.

Ejemplo:


```
set ns tcpProfile tcpprofile1 -flavor NILE
<!--NeedCopy-->
```

Algoritmo de Recuperación de Tasa Proporcional (PRR)

Los mecanismos de recuperación rápida TCP reducen la latencia web causada por pérdidas de paquetes. El nuevo algoritmo de recuperación proporcional de velocidad (PRR) es un algoritmo de recuperación rápida que evalúa los datos TCP durante una recuperación de pérdidas. Se modela después de Rate-Halving, mediante el uso de la fracción que es apropiada para la ventana de destino elegida por el algoritmo de control de congestión. Minimiza el ajuste de la ventana y el tamaño real de la ventana al final de la recuperación está cerca del umbral de inicio lento (ssthresh).

Apertura rápida TCP (TFO)

TCP Fast Open (TFO) es un mecanismo TCP que permite el intercambio de datos rápido y seguro entre un cliente y un servidor durante el protocolo de enlace inicial de TCP. Esta función está disponible como opción TCP en el perfil TCP enlazado a un servidor virtual de un dispositivo Citrix ADC. TFO utiliza una cookie TCP Fast Open (una cookie de seguridad) que genera el dispositivo Citrix ADC para validar y autenticar al cliente que inicia una conexión TFO al servidor virtual. Mediante el mecanismo TFO, puede reducir la latencia de red de una aplicación en el tiempo necesario para un viaje completo de ida y vuelta, lo que reduce significativamente el retraso experimentado en las transferencias TCP cortas.

Cómo funciona el TFO

Cuando un cliente intenta establecer una conexión TFO, incluye una cookie TCP Fast Open con el segmento SYN inicial para autenticarse. Si la autenticación se realiza correctamente, el servidor virtual del dispositivo Citrix ADC puede incluir datos en el segmento SYN-ACK aunque no haya recibido el segmento ACK final del protocolo de enlace de tres vías. Esto ahorra hasta un viaje completo de ida y vuelta en comparación con una conexión TCP normal, que requiere un protocolo de enlace de tres vías antes de que se puedan intercambiar datos.

Un cliente y un servidor back-end realizan los siguientes pasos para establecer una conexión TFO e intercambiar datos de forma segura durante el protocolo de enlace TCP inicial.

1. Si el cliente no tiene una cookie TCP Fast Open para autenticarse, envía una solicitud Fast Open Cookie en el paquete SYN al servidor virtual del dispositivo Citrix ADC.
2. Si la opción TFO está habilitada en el perfil TCP enlazado al servidor virtual, el dispositivo genera una cookie (cifrando la dirección IP del cliente bajo una clave secreta) y responde al cliente con un SYN-ACK que incluye la cookie de apertura rápida generada en un campo de opción TCP.

3. El cliente almacena en caché la cookie para futuras conexiones TFO al mismo servidor virtual del dispositivo.
4. Cuando el cliente intenta establecer una conexión TFO al mismo servidor virtual, envía SYN que incluye la cookie de apertura rápida en caché (como opción TCP) junto con los datos HTTP.
5. El dispositivo Citrix ADC valida la cookie y, si la autenticación se realiza correctamente, el servidor acepta los datos del paquete SYN y reconoce el evento con SYN-ACK, cookie TFO y respuesta HTTP.

Nota: Si la autenticación del cliente falla, el servidor elimina los datos y reconoce el evento solo con un SYN que indica un tiempo de espera de la sesión.

1. En el lado del servidor, si la opción TFO está habilitada en un perfil TCP enlazado a un servicio, el dispositivo Citrix ADC determina si la cookie de apertura rápida TCP está presente en el servicio al que está intentando conectarse.
2. Si la cookie TCP Fast Open no está presente, el dispositivo envía una solicitud de cookie en el paquete SYN.
3. Cuando el servidor back-end envía la cookie, el dispositivo almacena la cookie en la caché de información del servidor.
4. Si el dispositivo ya tiene una cookie para el par IP de destino dado, reemplaza la cookie antigua por la nueva.
5. Si la cookie está disponible en la caché de información del servidor cuando el servidor virtual intenta volver a conectarse al mismo servidor back-end mediante la misma dirección SNIP, el dispositivo combina los datos del paquete SYN con la cookie y los envía al servidor back-end.
6. El servidor back-end reconoce el evento con datos y un SYN.

Nota: Si el servidor reconoce el evento con solo un segmento SYN, el dispositivo Citrix ADC reenvía inmediatamente el paquete de datos después de quitar el segmento SYN y las opciones TCP del paquete original.

Configuración de TCP Fast Open

Para utilizar la función TCP Fast Open (TFO), habilite la opción TCP Fast Open en el perfil TCP pertinente y establezca el parámetro TFO Cookie Timeout en un valor que se ajuste al requisito de seguridad para ese perfil.

Para habilitar o inhabilitar TFO mediante la línea de comandos

En el símbolo del sistema, escriba uno de los siguientes comandos para habilitar o inhabilitar TFO en un perfil nuevo o existente.

Nota: El valor predeterminado es DISABLED.


```
add tcpprofile <TCP Profile Name> - tcpFastOpen ENABLED | DISABLED
set tcpprofile <TCP Profile Name> - tcpFastOpen ENABLED | DISABLED
unset tcpprofile <TCP Profile Name> - tcpFastOpen
<!--NeedCopy-->
```

Ejemplos:

add tcpprofile Profile1: TcpFastOpen
Set tcpprofile Profile1: TcpFastOpen Enabled
unset tcpprofile Profile1: TcpFastOpen

Para establecer el valor de tiempo de espera de la cookie de apertura rápida TCP mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
set tcpparam  - tcpfastOpenCookieTimeout <Timeout Value>
<!--NeedCopy-->
```

Ejemplo:

```
set tcpprofile  - tcpfastOpenCookieTimeout 30secs
<!--NeedCopy-->
```

Para configurar el TCP Fast Open mediante la interfaz gráfica de usuario

1. Vaya a **Configuración** > **Sistema** > **Perfiles** > y, a continuación, haga clic en **Modificar** para modificar un perfil TCP.
2. En la página **Configurar perfil TCP**, marque la casilla **TCP Fast Open**.
3. Haga clic en **Aceptar** y, a continuación, **Listo**.

Para configurar el valor de tiempo de espera de TCP Fast Cookie mediante la interfaz gráfica de usuario

Vaya a **Configuración** > **Sistema** > **Configuración** > **Cambiar parámetros TCP** y, a continuación, **Configurar parámetros TCP** para establecer el valor de tiempo de espera TCP Fast Open Cookie.

TCP Hystart

Un nuevo parámetro de perfil TCP, hystart, habilita el algoritmo Hystart, que es un algoritmo de inicio lento que determina dinámicamente un punto seguro en el que terminar (ssthresh). Permite una transición a evitar la congestión sin grandes pérdidas de paquetes. Este nuevo parámetro está inhabilitado de forma predeterminada.

Si se detecta congestión, Hystart entra en una fase de prevención de congestión. Si lo habilita, obtendrá un mejor rendimiento en redes de alta velocidad con una alta pérdida de paquetes. Este algoritmo ayuda a mantener el ancho de banda cercano al máximo durante el procesamiento de transacciones. Por lo tanto, puede mejorar el rendimiento.

Configuración de TCP Hystart

Para utilizar la función Hystart, habilite la opción Cubic Hystart en el perfil TCP correspondiente.

Para configurar Hystart mediante la interfaz de línea de comandos (CLI)

En el símbolo del sistema, escriba uno de los siguientes comandos para habilitar o inhabilitar Hystart en un perfil TCP nuevo o existente.

```
add tcpprofile <profileName> -hystart ENABLED
set tcpprofile <profileName> -hystart ENABLED
unset tcprofile <profileName> -hystart
<!--NeedCopy-->
```

Ejemplos:

```
add tcpprofile Profile1 - tcpFastOpen
Set tcpprofile Profile1 - tcpFastOpen Enabled
unset tcpprofile Profile1 - tcpFastOpen
<!--NeedCopy-->
```

Para configurar la compatibilidad con Hystart mediante la interfaz gráfica de usuario

1. Vaya a **Configuración** > **Sistema** > **Perfiles** > y haga clic en **Modificar** para modificar un perfil TCP.
2. En la página **Configurar perfil TCP**, active la casilla de verificación **Hystart cúbico**.
3. Haga clic en **Aceptar** y, a continuación, **Listo**.

Técnicas de optimización

TCP utiliza las siguientes técnicas y métodos de optimización para controles de flujo optimizados.

Selección de perfil TCP basada en directivas

Hoy en día, el tráfico de red es más diverso y requiere mucho ancho de banda que nunca. Con el aumento del tráfico, el efecto que la calidad de servicio (QoS) tiene en el rendimiento TCP es significativo. Para mejorar la calidad de servicio, ahora puede configurar directivas de AppQoE con diferentes perfiles TCP para diferentes clases de tráfico de red. La directiva AppQoE clasifica el tráfico de un servidor virtual para asociar un perfil TCP optimizado para un tipo concreto de tráfico, como 3G, 4G, LAN o WAN.

Para utilizar esta función, cree una acción de directiva para cada perfil TCP, asocie una acción con directivas AppQoE y vincule las directivas a los servidores virtuales de equilibrio de carga.

Configuración de la selección de perfiles TCP basada en directivas

La configuración de la selección de perfiles TCP basada en directivas consta de las siguientes tareas:

- Activando AppQoE. Antes de configurar la función de perfil TCP, debe habilitar la función AppQoE.
- Agregar acción AppQoE. Después de habilitar la función AppQoE, configure una acción AppQoE con un perfil TCP.
- Configuración de la selección de perfiles TCP basada en AppQoE. Para implementar la selección de perfiles TCP para diferentes clases de tráfico, debe configurar directivas AppQoE con las que su dispositivo Citrix ADC pueda distinguir las conexiones y enlazar la acción AppQoE correcta a cada directiva.
- Vinculación de la directiva AppQoE con el servidor virtual. Una vez que haya configurado las directivas de AppQoE, debe vincularlas a uno o más servidores virtuales de equilibrio de carga, conmutación de contenido o redirección de caché.

Configurar mediante la interfaz de línea de comandos

Para habilitar AppQoE mediante la interfaz de línea de comandos:

En el símbolo del sistema, escriba los siguientes comandos para habilitar la función y compruebe que está habilitada:

```
1 enable ns feature appqoe
2
3 show ns feature
```



```
<!--NeedCopy-->
```

Para enlazar un perfil TCP al crear una acción AppQoE mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba el siguiente comando de acción AppQoE con la opción tcpprofile-tobind.

Enlazar un perfil TCP:

```
add appqoe action <name> [-priority <priority>] [-respondWith ( ACS |
    NS ) [<CustomFile>] [-altContentSvcName <string>] [-altContentPath <
    string>] [-maxConn <positive_integer>] [-delay <usecs>]] [-polqDepth
     <positive_integer>] [-priqDepth <positive_integer>] [-
    dosTrigExpression <expression>] [-dosAction ( SimpleResponse |
    HICResponse )] [-tcpprofiletobind <string>]

show appqoe action
<!--NeedCopy-->
```

Para configurar una directiva AppQoE mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
add appqoe policy <name> -rule <expression> -action <string>
<!--NeedCopy-->
```

Para vincular una directiva de AppQoE al equilibrio de carga, la redirección de caché o la conmutación de contenido de servidores virtuales mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
bind cs vserver cs1 -policyName <appqoe_policy_name> -priority <
    priority>
bind lb vserver <name> - policyName <appqoe_policy_name> -priority <
    priority>
bind cr vserver <name> -policyName <appqoe_policy_name> -priority <
    priority>
```



```
<!--NeedCopy-->
```

Ejemplo:

```
add ns tcpProfile tcp1 -WS ENABLED -SACK ENABLED -WSVal 8 -nagle
    ENABLED -maxBurst 30 -initialCwnd 16 -oooQSize 15000 -minRTO 500 -
    slowStartIncr 1 -bufferSize 4194304 -flavor BIC -KA ENABLED -
    sendBuffsize 4194304 -rstWindowAttenuate ENABLED -spoofSynDrop
    ENABLED -dsack enabled -frto ENABLED -maxcwnd 4000000 -fack ENABLED
    -tcpmode ENDPOINT

add appqoe action appact1 -priority HIGH -tcpprofile tcp1

add appqoe policy apppol1 -rule "client.ip.src.eq(10.102.71.31)" -
    action appact1

bind lb vserver lb2 -policyName apppol1 -priority 1 -
    gotoPriorityExpression END -type REQUEST

bind cs vserver cs1 -policyName apppol1 -priority 1 -
    gotoPriorityExpression END -type REQUEST
<!--NeedCopy-->
```

Configuración de perfiles TCP basados en directivas mediante la GUI

Para habilitar AppQoE mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **Configuración**.
2. En el panel de detalles, haga clic en **Configurar funciones avanzadas**.
3. En el cuadro de diálogo **Configurar funciones avanzadas**, active la casilla de verificación **AppQoE**.
4. Haga clic en **Aceptar**.

Para configurar la directiva AppQoE mediante la interfaz gráfica de usuario

1. Vaya a **App-Expert** > **AppQoE** > **Acciones**.
2. En el panel de detalles, realice una de las acciones siguientes:
3. Para crear una nueva acción, haga clic en **Agregar**.
4. Para modificar una acción existente, selecciónela y, a continuación, haga clic en **Modificar**.

5. En la pantalla **Crear acción AppQoE** o **Configurar acción AppQoE**, escriba o seleccione valores para los parámetros. El contenido del cuadro de diálogo corresponde a los parámetros descritos en “Parámetros para configurar la acción AppQoE” de la siguiente manera (asterisco indica un parámetro obligatorio):
   a) Nombre: Name
   b) Tipo de acción: RespondWith
   c) Prioridad: Priority
   d) Profundidad de cola de directivas: PolqDepth
   e) Profundidad de la cola: PriqDepth
   f) Acción de DOS: DosAction
6. Haga clic en **Crear**.

Para enlazar la directiva de AppQoE mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**, seleccione un servidor y, a continuación, haga clic en **Modificar**.
2. En la sección **Directivas** y haga clic en (+) para enlazar una directiva de AppQoE.
3. En el control deslizante **Directivas**, haga lo siguiente:
   a) Seleccione un tipo de directiva como AppQoE en la lista desplegable.
   b) Seleccione un tipo de tráfico en la lista desplegable.
4. En la sección **Enlace de directivas**, haga lo siguiente:
   a) Haga clic en **Nuevo** para crear una nueva directiva de AppQoE.
   b) Haga clic en **Directiva existente** para seleccionar una directiva de AppQoE en la lista desplegable.
5. Establezca la prioridad de enlace y haga clic en **Vincular** a la directiva al servidor virtual.
6. Haga clic en **Done**.

Generación de bloques SACK

El rendimiento TCP se ralentiza cuando se pierden varios paquetes en una ventana de datos. En este caso, un mecanismo de reconocimiento selectivo (SACK) combinado con una directiva de retransmisión selectiva de repetición supera esta limitación. Para cada paquete entrante fuera de pedido, debe generar un bloque SACK.

Si el paquete fuera de pedido encaja en el bloque de cola de reensamblaje, inserte la información del paquete en el bloque y establezca la información del bloque completa como SACK-0. Si un paquete fuera de pedido no encaja en el bloque de reensamblaje, envíe el paquete como SACK-0 y repita los bloques SACK anteriores. Si un paquete fuera de orden es un duplicado y la información del paquete se establece como SACK-0, entonces D-SACK el bloque.

Nota: Un paquete se considera como D-SACK si es un paquete reconocido, o un paquete fuera de servicio que ya se ha recibido.

Incumplimiento del cliente

Un dispositivo Citrix ADC puede manejar el renegamiento del cliente durante la recuperación basada en SACK.

Las comprobaciones de memoria para marcar end_point en PCB no consideran la memoria total disponible

En un dispositivo Citrix ADC, si el umbral de uso de memoria se establece en el 75% en lugar de utilizar la memoria total disponible, las nuevas conexiones TCP evitan la optimización TCP.

Retransmisiones innecesarias debido a la falta de bloques SACK

En un modo no endpoint, cuando envía DUPACKS, si faltan bloques SACK para pocos paquetes fuera de servicio, desencadena retransmisiones adicionales desde el servidor.

SNMP para la optimización del número de conexiones omitirse debido a la sobrecarga

Los siguientes identificadores SNMP se han agregado a un dispositivo Citrix ADC para realizar un seguimiento del número de conexiones que se han omitido la optimización TCP debido a la sobrecarga.

1. 1.3.6.1.4.1.5951.4.1.1.46.13 (tcpOptimizationEnabled). Para realizar un seguimiento del número total de conexiones habilitadas con la optimización TCP.
2. 1.3.6.1.4.1.5951.4.1.1.46.132 (tcpOptimizationBypassed). Para realizar un seguimiento del número total de conexiones que se omite TCP Optimization.

Buffer de recepción dinámica

Para maximizar el rendimiento TCP, un dispositivo Citrix ADC ahora puede ajustar dinámicamente el tamaño del búfer de recepción TCP.

Pautas de solución de problemas

August 20, 2021

Asistencia técnica

Todas las consultas de solución de problemas y escalación requieren un paquete de soporte técnico de Citrix ADC reciente, que captura la configuración actual, la versión del firmware instalada, los archivos de registro, los núcleos sobresalientes y otros.

Ejemplo:

```
show techsupport

showtechsupport data collector tool - $Revision: #5 $!
...
<!--NeedCopy-->
```

Todos los datos serán recogidos bajo

```
...
Archiving all the data into "/var/tmp/support/collector_P_192
   .168.121.117_18Jun2015_09_53.tar.gz" ....
Created a symbolic link for the archive with /var/tmp/support/support.
   tgz
/var/tmp/support/support.tgz  ---- points to ---> /var/tmp/support/
   collector_P_192.168.121.117_18Jun2015_09_53.tar.gz
<!--NeedCopy-->
```

Después de generar un paquete de soporte técnico, es posible que se copie mediante SCP.

Rastros

Los problemas de optimización TCP de Citrix ADC normalmente requieren rastros de Citrix ADC para solucionar correctamente los problemas. Tenga en cuenta que uno debe tratar de capturar rastros en condiciones similares, es decir, en la misma celda, durante la misma hora del día, mediante el mismo equipo de usuario y aplicación, y otros.

Los comandos start nstrace y stop nstrace pueden utilizarse para capturar trazas:

- Se recomienda encarecidamente que se utilice el filtro apropiado para evitar la captura de paquetes extraños e innecesarios en el rastreo. Por ejemplo, use start nstrace -filter 'IP == 10.20.30.40' para capturar solo los paquetes enviados o recibidos desde la dirección IP 10.20.30.40, que es la dirección IP del equipo del usuario.
- No utilice la opción -tcpdump, ya que elimina los encabezados nstrace necesarios para la depuración.

Análisis de rastros

Después de capturar un seguimiento Citrix ADC, es posible que se vea con Wireshark 1.12 o posterior. Compruebe que los rastros capturados incluyan los encabezados de seguimiento de paquetes de Citrix ADC apropiados, como se muestra en la captura de pantalla siguiente:

Los encabezados de depuración adicionales también están visibles según la ilustración siguiente:

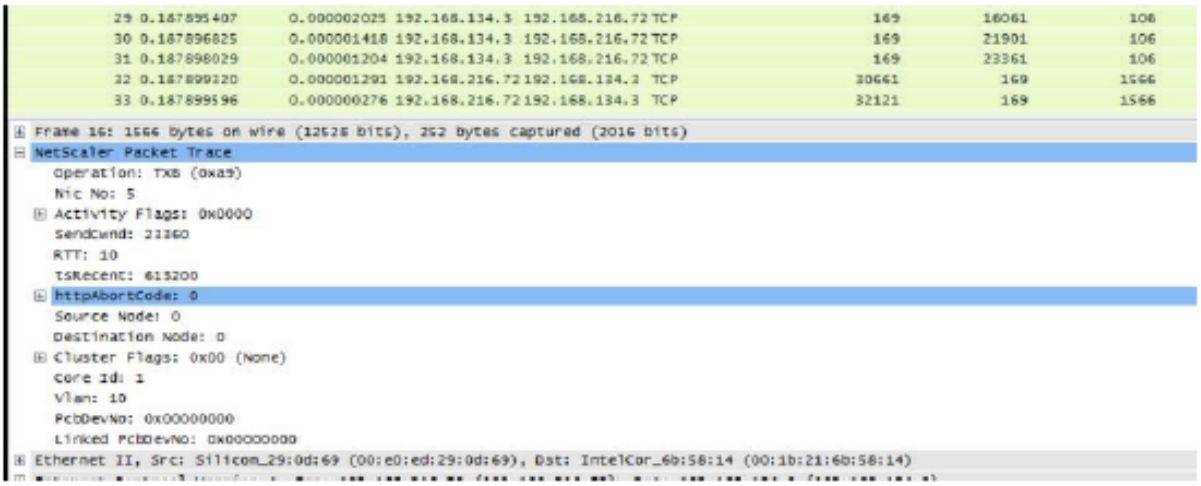


Tabla de conexiones

Cuando el problema está relacionado con la optimización TCP y se puede reproducir o está en curso, lo mejor es obtener también la tabla de conexión cuando el problema se produce desde el nodo T1 primario.

Para obtener la tabla deberá cambiar al shell BSD y ejecutar el siguiente comando:

```
shell
...

nscli -U 127.0.0.1:nsroot:nsroot show connectiontable -detail full link
    > /var/tmp/contable.log
<!--NeedCopy-->
```


> **Nota**
>
> El comando podría ejecutarse durante más tiempo y la CPU de administración podría estar estresada en ese momento (depende del número de entradas de la tabla de conexión), pero no afecta el servicio.

Preguntas frecuentes

August 20, 2021

Tiempos de espera

> **Importante**
>
> Antes de utilizar *cualquier mando nsapimgr*, consulte con el servicio de atención al cliente de Citrix.

A continuación se muestra una lista de diferentes tiempos de espera de conexión inactiva que se pueden establecer en servidores y servicios virtuales Citrix ADC T1. El tiempo de espera inactivo establecido para las conexiones de cliente o servidor en el nivel de servidor o servicio son aplicables solo para las conexiones en el estado TCP ESTABLISHED y están inactivas.

- El parámetro CLTTimeout del servidor virtual de Equilibrio de carga especifica el tiempo en segundos que una conexión de un cliente a un servidor virtual de Equilibrio de carga debe estar inactiva, antes de que el dispositivo cierre la conexión.
- El parámetro Service SvrTimeout especifica el tiempo en segundos que una conexión desde el dispositivo a un servicio o servidor debe estar inactiva antes de que el dispositivo cierre la conexión.
- El parámetro Service CLTTimeout especifica el tiempo en segundos que una conexión de un cliente a un servicio debe estar inactiva antes de que el dispositivo cierre la conexión.

Cuando un servicio está enlazado a un servidor virtual de equilibrio de carga, el CLTTimeout para el servidor virtual de equilibrio de carga tiene prioridad y se omite el servicio CLTTimeout para el servicio.

En caso de que no haya servicio vinculado al servidor virtual de equilibrio de carga, el tiempo de espera inactivo global, es decir, TCPServer, se utiliza para las conexiones del lado del servidor. Se puede configurar de la siguiente manera:

Comando:

```
set ns timeout -tcpServer 9000
```



```
<!--NeedCopy-->
```

Las conexiones en otro estado tienen valores de tiempo de espera diferentes:

- Tiempo de espera de inactividad de conexiones medio abiertas: 120 segundos (valor codificado)
- Time_WAIT conexiones inactivas: 40 segundos (valor codificado)
- Tiempo de espera inactivo de conexiones medio cierre. Por defecto es 10s y se puede configurar entre 1s y 600s mediante el fragmento

Comando:

```
 set ns timeout -halfclose 10
<!--NeedCopy-->
```

Cuando se activa el tiempo de espera de medio cierre, la conexión se mueve al estado zombie. Cuando caduca el tiempo de espera zombie, la limpieza zombie se inicia y T1 envía RST tanto en el cliente como en el servidor para la conexión dada de forma predeterminada.

- Tiempo de espera zombi: Intervalo en el que debe ejecutarse el proceso de limpieza zombie para limpiar las conexiones TCP inactivas. El valor de tiempo de espera predeterminado es 120s y se puede configurar entre 1s y 600s.

Comando:

```
set ns timeout -zombie 120
<!--NeedCopy-->
```

Tabla de tamaño máximo de segmento

Un dispositivo Citrix ADC T1 se defiende contra ataques de inundación SYN mediante el uso de cookies SYN en lugar de mantener conexiones semiabiertas en la pila de memoria del sistema. El dispositivo envía una cookie a cada cliente que solicita una conexión TCP, pero no mantiene los estados de conexiones semiabiertas. En su lugar, el dispositivo asigna memoria del sistema para una conexión solo al recibir el paquete ACK final o, para el tráfico HTTP, al recibir una solicitud HTTP. Esto evita los ataques SYN y permite que las comunicaciones TCP normales con clientes legítimos continúen ininterrumpidas. La función específica está habilitada por defecto sin opción de inhabilitar.

Sin embargo, hay una advertencia ya que las cookies SYN estándar limitan las conexiones al uso de solo ocho valores de tamaño máximo de segmento (MSS). Si la conexión MMS no coincide con ningún valor predefinido, recogerá el siguiente valor inferior disponible tanto para el cliente como para el servidor.

Los valores predefinidos TCP Maximum Segment Size (MSS) son los siguientes y se pueden configurar a través de una nueva perilla nsapimgr.

1460	1440	1330	1220	956	536	384	128

La nueva tabla MSS:

- No es necesario contener compatibilidad con Jumbo-Frame. Aunque de forma predeterminada 8 valores están reservados en la tabla MSS para tramas jumbo, la configuración de la tabla se puede modificar para incluir solo fotogramas estándar de tamaño Ethernet.
- Debe tener 16 valores
- Debería tener valores en orden descendente
- Debe incluir 128 como último valor

Si la nueva tabla MSS es válida, la tabla se almacena y los valores antiguos se cambian en el tiempo de rotación SYN Cookie. De lo contrario, la nueva tabla devuelve un error. Los cambios se aplican a las nuevas conexiones, mientras que las conexiones existentes conservan la tabla MSS anterior hasta que las conexiones caduquen o terminen.

Para mostrar la tabla MSS actual en un dispositivo Citrix ADC, escriba el comando siguiente.

Comando:

```
>shell

#nsapimgr -d mss_table
```

Ejemplo:

```
#nsapimgr -d mss_table

MSS table

{
 9176,9156,8192,7168,6144,4196,3072,2048,1460,1440,1330,1212,956,536,384,128
     }


Done.
```


Para cambiar la tabla mss, escriba el siguiente comando:

Comando:

```
>shell

#nsapimgr -s mss_table=<16 comma seperated values>
```

Ejemplo:

```
#nsapimgr -ys mss_table
   =9176,9156,8192,7168,6144,4196,3072,2048,1460,1400,1330,1212,956,536,384,128


# nsapimgr -d mss_table

MSS table

{
 9176,9156,8192,7168,6144,4196,3072,2048,1460,1400,1330,1212,956,536,384,128
     }


Done.
```

A continuación se muestra un ejemplo que utiliza valores estándar de tamaño Ethernet:

Ejemplo:

```
#nsapimgr -ys mss_table
   =1460,1440,1420,1400,1380,1360,1340,1320,1300,1280,1260,1212,956,536,384,128


# nsapimgr -d mss_table

MSS table

{
 1460,1440,1420,1400,1380,1360,1340,1320,1300,1280,1260,1212,956,536,384,128
     }


```



```
Done.
```

Para que este cambio sea permanente incluso después de que se reinicie el dispositivo Citrix ADC, incluya el comando##`nsapimgr -ys mss_table=<16 comma seperated values>` en el archivo "/nsconfig/rc.netscaler". Si el archivo "rc.netscaler" no existe, créelo en la carpeta "/nsconfig" y, a continuación, agregue el comando.

Protección contra sobrecarga de memoria

Un motor de procesamiento de paquetes (PPE) de Citrix ADC comienza a omitir las conexiones de la optimización TCP si la memoria utilizada por ese PPE es superior a un valor de marca de agua alto especificado. Si una utilización de memoria PPE supera los ~ 2,6 GB, entonces comienza a omitir *cualquier conexión nueva* de la optimización. Las conexiones existentes (las admitidas anteriormente para la optimización) continúan obteniendo optimización. Este valor de marca de agua se ha seleccionado a propósito y no se recomienda para afinar.

> **Nota**
>
> Si crees que hay una buena razón para cambiar ese valor de marca de agua, ponte en contacto con Atención al cliente.

Soporte para clientes de Happy Eyeballs

Si el dispositivo Citrix ADC recibe un SYN para un destino cuyo estado es desconocido, el dispositivo comprueba primero la accesibilidad del servidor y, a continuación, reconoce el cliente. Este mecanismo de sondeo permite a los clientes con pilas IP duales descubrir la accesibilidad de servidores de Internet de doble pila. Si el cliente descubre que tanto el acceso IPv6 como IPv4 están disponibles, establece una conexión con el servidor que responde más rápidamente y restablece la otra. Para que la conexión para el dispositivo Citrix ADC reciba un restablecimiento, restablecerá la conexión del lado del servidor correspondiente.

Nota: Esta función no tiene configuraciones TCP configurables por el usuario para inhabilitarlas o habilitarlas en el dispositivo Citrix ADC.

Para obtener más información sobre el soporte de Happy Eyeballs, consulte RFC 6555.

Optimización de vídeo Citrix ADC

January 19, 2021

El dispositivo Citrix ADC proporciona técnicas y capacidades de optimización para optimizar el tráfico de vídeo ABR para el tráfico de vídeo a través de redes móviles. Esto mejora la experiencia del usuario y reduce el consumo general de ancho de banda de la red.

La sección incluye los siguientes temas:

- Introducción
- Licencias
- Configuración de optimización de vídeo a través de TCP
- Configuración de optimización de vídeo a través de UDP

Introducción

August 20, 2021

Los archivos multimedia han estado impulsando una cantidad cada vez mayor de tráfico a través de las redes móviles, y la migración a tecnologías de redes más rápidas ha aumentado drásticamente el volumen de tráfico de vídeo cifrado. La tecnología tradicional de entrega de medios (descarga progresiva) está fallando en ofrecer una calidad aceptable de experiencia (QoE) a una alta velocidad de transmisión. Esto ha llevado a la introducción del protocolo Adaptive Bit Rate (ABR). Puede adaptar la velocidad de bits de transmisión al ancho de banda de red disponible y restringir la calidad de transmisión para que coincida con la capacidad del auricular que recibe el vídeo. Sin embargo, el protocolo ABR no funciona tan bien en redes móviles como lo hace a través de Internet. Por lo tanto, los operadores móviles deben optimizar el tráfico ABR.

Un dispositivo Citrix ADC tiene capacidades únicas para detectar el tráfico de vídeo entrante y optimizar selectivamente los vídeos ABR.

Cómo funciona la optimización de vídeo de Citrix ADC

Un dispositivo Citrix ADC puede identificar y optimizar el tráfico ABR cifrado (incluido el tráfico de vídeo de Facebook) a través de TCP, y el tráfico ABR de YouTube a través de QUIC. El dispositivo tiene las siguientes capacidades:

1. Detecta vídeos de descarga progresiva (PD) a través de HTTP.
2. Detecta y optimiza los vídeos ABR a través de HTTP.
3. Detecta y optimiza vídeos ABR a través de HTTPS.
4. Detecta y optimiza vídeos ABR de YouTube a través de QUIC.

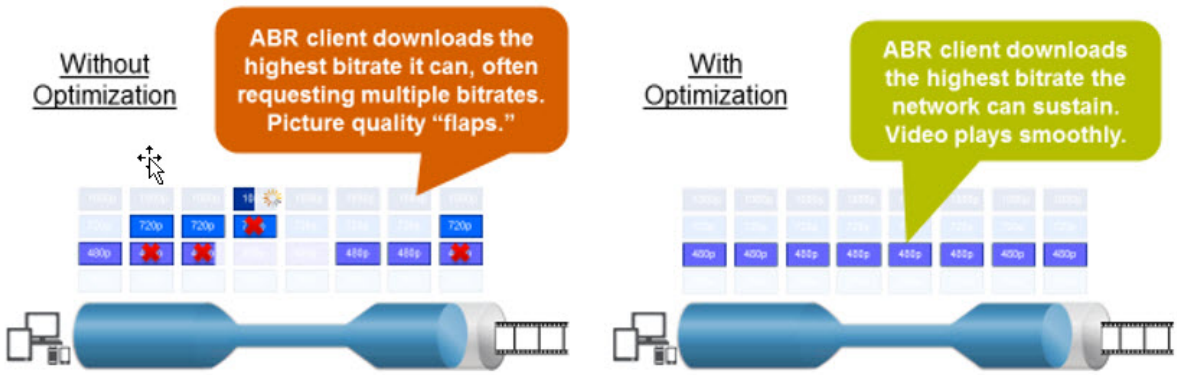
Además, el dispositivo utiliza los siguientes dominios de soporte para detectar tráfico de vídeo a través de protocolos TCP y QUIC.

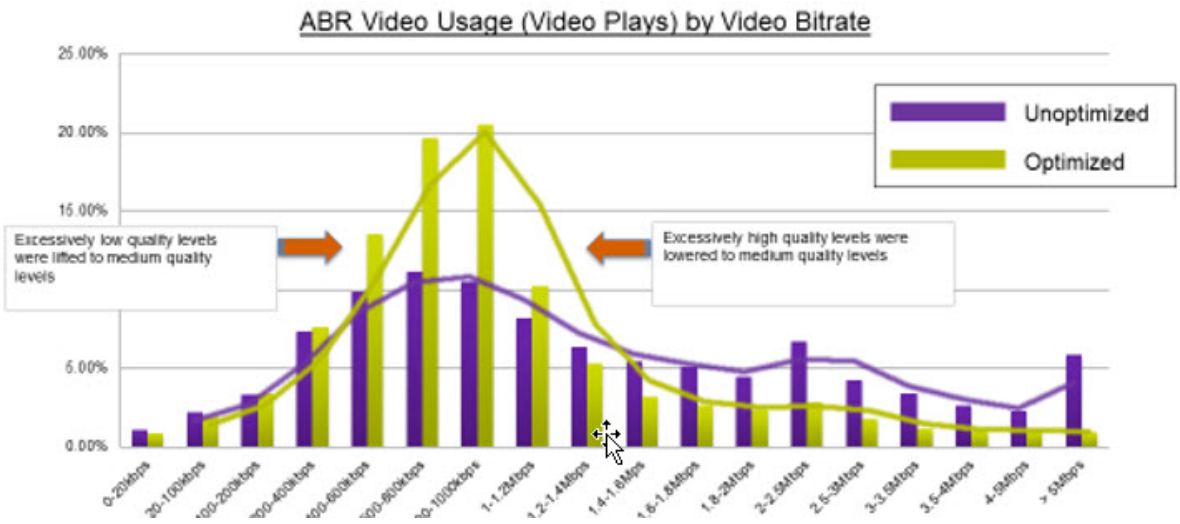
- Vídeos ABR sin cifrar a través de TCP. El dispositivo detecta todos los sitios web de streaming de vídeo compatibles con los estándares. El dispositivo detecta sesiones ABR inspeccionando el encabezado de carga de vídeo de respuesta, la URL y los encabezados HTTP.
- Vídeo ABR encriptado a través de TCP. El dispositivo detecta sesiones ABR mediante un algoritmo genérico y heurístico basado en patrones de dominio, encabezado SSL y tráfico. Con esto, el dispositivo cuenta con un soporte integrado para detectar sitios web de vídeo de primera calidad, con una precisión del 95% y seguimos agregando compatibilidad para nuevos tipos de vídeo. Citrix ADC también tiene un programa para proporcionar verificación adicional para los principales sitios ABR cifrados para una región o país a fin de garantizar la cobertura de la red.
- Vídeos ABR encriptados a través de QUIC. El dispositivo detecta sesiones ABR para el proveedor de vídeo basado en QUIC, como YouTube. El algoritmo de detección se basa en una heurística aprovechando los encabezados y el dominio QUIC. Citrix ADC continuará agregando compatibilidad con sitios de vídeo más recientes mediante QUIC.

Ventajas

Optimizar el tráfico de vídeo ABR puede proporcionar los siguientes beneficios:

- Gestione la red durante la congestión en horas punta.
- Mejora la consistencia de reproducción de vídeo y reduce el estancamiento de vídeo.
- Habilite nuevas ofertas de servicios de vídeo (por ejemplo, servicios de vídeo Binge-on).
- Permita a los clientes seleccionar la mejor calidad de vídeo sostenible.
- Proporcionar una experiencia de usuario coherente para el suscriptor.





Optimización de vídeo a través de TCP

La optimización Citrix ADC del tráfico ABR a través de TCP funciona de la siguiente manera:

1. El tráfico HTTP o HTTPS que recibe el dispositivo a través de TCP se envía al servidor virtual de equilibrio de carga correspondiente.
2. Las directivas de detección integradas enlazadas al servidor virtual combinadas con otros algoritmos de detección propietarios evalúan el tráfico.
3. Las directivas utilizan un conjunto de firmas de detección de vídeo integradas para detectar el tipo de vídeo. La directiva que coincide con el tráfico aplica una acción que clasifica el tipo de vídeo como una de las siguientes:
   a) PD de texto claro
   b) ABR de texto claro
   c) ABR cifrado
   d) Otros
4. Las directivas de optimización vinculadas al mismo servidor virtual evalúan el tráfico y determinan la velocidad de bits de optimización que se aplicará al tráfico.
5. La velocidad de bits de optimización se aplica si el tráfico es ABR de texto claro o ABR cifrado.

Un proveedor de servicios móviles puede mejorar la calidad de la experiencia (QoE) estableciendo la velocidad de descarga para el tráfico móvil 2G, 3G y 4G. Esto reduce los tiempos de inicio del vídeo o los eventos de almacenamiento en búfer. La optimización también puede reducir la cantidad de ancho de banda de red consumida por las sesiones de vídeo.

Las técnicas de optimización incluyen control dinámico de ráfagas y muestreo aleatorio.

Control dinámico de ráfagas

La optimización de Citrix ADC ABR se adapta dinámicamente a las condiciones cambiantes de la red. Permite una velocidad de ráfaga inicial de 1,3 veces la velocidad de ritmo configurada durante 15 segundos. La velocidad de ráfaga inicial se aplica al comienzo de cada sesión de vídeo ABR optimizada, incluso cuando varias sesiones usan la misma conexión TCP o grupo de conexiones TCP.

El dispositivo también admite ráfagas de recuperación en caso de que la velocidad de bits admitida por la red se sitúe por debajo de la velocidad de ritmo configurada. Por ejemplo, si la velocidad de bits efectiva cae en el 7º segundo y se recupera en el 15º segundo de la ráfaga inicial, el dispositivo recupera la pérdida durante el siguiente ciclo de ráfaga. Al hacerlo, el dispositivo optimiza dinámicamente el ancho de banda de red para todos los suscriptores, de modo que la calidad del vídeo siga siendo coherente por píxel.

Nota: Cuando se produce una ráfaga de recuperación durante una ráfaga inicial, la velocidad de bits de ritmo no debe exceder las tasas máximas de recuperación-ráfaga y ráfaga inicial (no debe agregar el factor Explosión de recuperación encima del factor Explosión inicial). De lo contrario, podría ser tan rápido que el reproductor multimedia cambia a un modo de mayor calidad. Sin embargo, si es necesario, puede ampliar la duración de la ráfaga inicial para compensar el ancho de banda no utilizado.

Muestreo aleatorio

Para estimar los ahorros derivados de la optimización de vídeo, el dispositivo Citrix ADC implementa el muestreo aleatorio. Con esta técnica, el dispositivo selecciona aleatoriamente un porcentaje configurable del tráfico de vídeo detectado (el parámetro de muestreo aleatorio es un número entero comprendido entre 0 y 100, por lo que no es posible menos del 1 por ciento). Estas transacciones (y sesiones) seleccionadas aleatoriamente y no optimizadas se convierten en un grupo de referencia y se identifican en los registros de transacciones (junto con otras funciones, como el tamaño de byte y los campos de temporizador. También se registran las funciones de las sesiones optimizadas, y el motor de generación de informes compara las estadísticas de los grupos optimizados y de referencia para estimar los ahorros derivados de la optimización (incluidos los ahorros de ABR Optimization).

Optimización de vídeo sobre UDP

Google ha introducido un nuevo protocolo de transporte llamado QUIC. El protocolo QUIC de Google es muy similar a TCP+TLS+HTTP/2 y se implementa en la parte superior de UDP. Citrix ADC puede detectar vídeos ABR de YouTube transmitidos a través del protocolo QUIC y aplicar la optimización de vídeo ABR de manera similar a ABR sobre TCP.

Licencias

August 20, 2021

La función Optimización de vídeo funciona en plataformas Telco con la compra de una licencia CBM básica y una licencia CBM Premium, y para otras plataformas Citrix ADC, la función funciona con la compra de una licencia CNS Premium. Antes de configurar la función de optimización de vídeo, el dispositivo debe tener una licencia adecuada.

Soporte de licencia para plataformas de telecomunicaciones:

- **CBM_TXXX_SERVER_Retail.lic**
- **CBM_TPRE_SERVER_Retail.lic**
- **CNS_WebF_SServer_Retail.lic**

Donde XXX es el rendimiento, por ejemplo, Citrix ADC T1000.

Compatibilidad con licencias para otras plataformas Citrix ADC:

- **CNS_XXX_SERVER_PLT_Retail.lic**

Donde XXX es el rendimiento.

Para cargar un archivo de licencia Premium, sigue los pasos que se indican a continuación:

1. Debe instalarse un archivo de licencia válido en el dispositivo Citrix ADC. La licencia debe admitir al menos tantos Gbps como el rendimiento máximo de GI-LAN esperado.

   Los archivos de licencia deben copiarse a través de un cliente SCP en /nsconfig/license del dispositivo, como se muestra en la captura de pantalla que aparece a continuación.

```
1 > shell ls /nsconfig/license/
2 CNS_V3000_SERVER_PLT_Retail.lic ssl
3 <!--NeedCopy-->
```

2. Realice un reinicio caliente para solicitar la nueva licencia, como se muestra en la captura de pantalla a continuación.

```
1 > reboot -warm
2 Are you sure you want to restart NetScaler (Y/N)? [N]:y
3  Done
4 <!--NeedCopy-->
```

3. Una vez completado el reinicio, compruebe que la licencia se ha aplicado correctamente mediante la CLI show license.

En el ejemplo siguiente se ha instalado correctamente una licencia Premium con edición Premium.

```
    > show license

                License status:

                                        Video Optimization: YES

                                                    ...

                                    Model Number ID: 110050

                                       License Type: Premium License
<!--NeedCopy-->
```

Configuración de la optimización de vídeo a través de TCP

October 5, 2021

> **Advertencia:**
>
> Como parte de la optimización de vídeo, la funcionalidad de ritmo de vídeo está obsoleta y se quitará del dispositivo Citrix ADC en las próximas versiones.

Para optimizar el tráfico de vídeo a través de TCP, comience por habilitar la función de optimización de vídeo. A continuación, el dispositivo activa las directivas de detección integradas para detectar el tráfico de vídeo entrante e identificar el tipo de vídeo. Las directivas de optimización configurables por el usuario para cada tipo de vídeo especifican la velocidad de bits de optimización necesaria para optimizar el tráfico.

Configuración de la optimización de vídeo a través de TCP mediante la CLI

Para configurar la optimización de vídeo en un dispositivo Citrix ADC, realice las siguientes tareas:

1. Activa la función de optimización de vídeo.
2. Agregue servidores virtuales para el tráfico HTTP y HTTPS.
3. Enlazar todas las directivas de detección integradas a un servidor virtual de equilibrio de carga para el tráfico HTTP.
4. Enlazar todas las directivas de detección integradas a un servidor virtual de equilibrio de carga de puente SSL para el tráfico HTTPS.

5. Agregue las directivas de optimización deseadas para el tráfico HTTP y HTTPS.
6. Enlazar directivas de optimización a un servidor virtual de equilibrio de carga para tráfico HTTP.
7. Enlazar directivas de optimización a un servidor virtual de equilibrio de carga de puente SSL para el tráfico HTTPS.

Activación de optimización de vídeo

Si quiere que el dispositivo Citrix ADC detecte, optimice e informe sobre el tráfico de vídeo, debe habilitar la función Optimización de vídeo y establecer la optimización en ON. Después de habilitar la función, puede utilizar directivas de detección integradas para identificar el tráfico de vídeo entrante y configurar directivas de optimización para optimizar el tráfico ABR cifrado. Para optimizar el tráfico de vídeo ABR, debe configurar la velocidad de bits de descarga (también llamada *velocidad de ritmo*).

También debe habilitar la función de equilibrio de carga y, si quiere utilizar la optimización de vídeo para el tráfico HTTPS, debe habilitar la función SSL.

Para habilitar la función de optimización de vídeo

En el símbolo del sistema, escriba el siguiente comando:

```
enable ns feature VideoOptimization
<!--NeedCopy-->
```

> **Nota**
>
> Si quiere supervisar el rendimiento de optimización de vídeo y los informes de información de vídeo, debe habilitar la función AppFlow y, a continuación, acceder a la función Vídeo Analytics en Citrix Application Delivery Management (ADM). Para obtener más información, consulte la documentación de Video Insight .

Creación de servidores virtuales para tráfico de vídeo HTTP y HTTPS

Un dispositivo Citrix ADC utiliza distintos servidores virtuales para detectar y optimizar los distintos tipos de tráfico de vídeo entrante. El dispositivo admite los siguientes tipos de servidores virtuales para el tráfico TCP.

- **Servidor virtual de equilibrio de carga HTTP**. Para detectar el tráfico de vídeo HTTP, el dispositivo utiliza un servidor virtual de equilibrio de carga HTTP. Administra las solicitudes de vídeo HTTP que recibe el dispositivo de los clientes.
- **Servidor virtual de equilibrio de carga de puente SSL**. Para detectar el tráfico de vídeo cifrado, debe configurar un servidor virtual puente SSL en el dispositivo.

Para agregar un servidor virtual de equilibrio de carga HTTP para detectar tráfico de vídeo HTTP

En el símbolo del sistema, escriba lo siguiente:

```
add lb vserver <name> HTTP * 80 -persistenceType NONE
<!--NeedCopy-->
```

Ejemplo:

```
add lb vserver ProxyVserver-HTTP HTTP * 80 -persistenceType NONE -
    cltTimeout 120
<!--NeedCopy-->
```

Para agregar un servidor virtual SSL Bridge para detectar tráfico de vídeo HTTPS

En el símbolo del sistema, escriba lo siguiente:

```
add lb vserver <name> SSL_BRIDGE * 443 -persistenceType NONE
<!--NeedCopy-->
```

Ejemplo:

```
add lb vserver ProxyVserver-SSL SSL_BRIDGE * 443 -persistenceType NONE
    -cltTimeout 180
<!--NeedCopy-->
```

Vinculación de directivas de detección integradas a un servidor virtual de equilibrio de carga HTTP

Para detectar el tráfico de vídeo a través de una conexión HTTP, debe vincular todas las directivas de detección integradas a un servidor virtual de equilibrio de carga. Debe vincular las directivas al procesamiento de tiempo de solicitud o de tiempo de respuesta, dependiendo del tipo de directiva.

> **Nota:**

> La directiva de optimización de vídeo `ns_videoopt_http_body_detection` no admite el método de solicitud HTTP `CONNECT`.

Para enlazar directivas de detección para diferentes tipos de vídeo a un servidor virtual de equilibrio de carga HTTP

En el símbolo del sistema, escriba el comando adecuado para cada tipo. Los comandos disponibles son los siguientes:

```
bind lb vserver <name> -policyName ns_videoopt_http_abr_netflix -
    priority <integer> -type (REQUEST | RESPONSE)

bind lb vserver <name>   -policyName ns_videoopt_http_abr_netflix2 -
    priority <integer> -type (REQUEST | RESPONSE)

bind lb vserver <name>   -policyName ns_videoopt_http_abr_youtube -
    priority <integer>  -type (REQUEST | RESPONSE)

bind lb vserver <name>    -policyName ns_videoopt_http_pd_youtube -
    priority <integer>  -type (REQUEST | RESPONSE)

bind lb vserver <name>    -policyName ns_videoopt_http_pd_youtube2  -
    priority <integer>  -type (REQUEST | RESPONSE)

bind lb vserver  <name>   -policyName ns_videoopt_http_pd_youtube3 -
    priority <integer>  -type (REQUEST | RESPONSE)

bind lb vserver  <name>  -policyName ns_videoopt_http_abr_generic -
    priority <integer> -type (REQUEST | RESPONSE)
<!--NeedCopy-->
```

Ejemplo:

```
bind lb vserver ProxyVserver-HTTP    -policyName
    ns_videoopt_http_abr_netflix -priority 400  type RESPONSE

bind lb vserver ProxyVserver-HTTP    -policyName
    ns_videoopt_http_abr_netflix2 -priority 500 -type RESPONSE

bind lb vserver ProxyVserver-HTTP    -policyName
    ns_videoopt_http_abr_youtube -priority 600  -type RESPONSE
```



```
6
7 bind lb vserver ProxyVserver-HTTP    -policyName
     ns_videoopt_http_pd_youtube -priority 800  -type RESPONSE
8
9 bind lb vserver ProxyVserver-HTTP    -policyName
     ns_videoopt_http_pd_youtube2 -priority 900 -type RESPONSE
10
11 bind lb vserver  ProxyVserver-HTTP   -policyName
     ns_videoopt_http_pd_youtube3 -priority 1000 -type REQUEST
12
13 bind lb vserver  ProxyVserver-HTTP   -policyName
     ns_videoopt_http_abr_generic -priority 1100 -type RESPONSE
14 <!--NeedCopy-->
```

Vinculación de la directiva de detección de contenido de cuerpo HTTP al servidor virtual de equilibrio de carga

Para detectar el tráfico de vídeo a través de HTTP, debe vincular la directiva de detección de contenido corporal al servidor virtual de equilibrio de carga. Puede usar el siguiente comando:

```
1 bind lb vserver <name> -policyName ns_videoopt_http_body_detection -
     priority <integer> -type (REQUEST | RESPONSE)
2 <!--NeedCopy-->
```

Ejemplo:

```
1 bind lb vserver ProxyVserver-HTTP -policyName
     ns_videoopt_http_body_detection -priority 1500 -type REQUEST
2 <!--NeedCopy-->
```

Enlace de directivas de detección integradas a un servidor virtual de equilibrio de carga de puente SSL

Para detectar el tráfico de vídeo a través de una conexión HTTPS, debe vincular directivas de detección integradas a un servidor virtual de equilibrio de carga SSL Bridge.

Para enlazar una directiva de detección a un servidor virtual de equilibrio de carga de puente SSL

En el símbolo del sistema, escriba el comando adecuado para cada tipo. Los comandos disponibles son los siguientes:

```
bind lb vserver <name> -policyName ns_videoopt_https_abr_netflix -
    priority <positive_integer> -type (REQUEST | RESPONSE)

bind lb vserver <name> -policyName ns_videoopt_https_abr_youtube -
    priority <positive_integer> -type (REQUEST | RESPONSE)

bind lb vserver <name> -policyName ns_videoopt_https_abr_generic -
    priority <positive_integer> -type (REQUEST | RESPONSE)
<!--NeedCopy-->
```

Ejemplo:

```
bind lb vserver ProxyVserver-SSL -policyName
    ns_videoopt_https_abr_netflix -priority 120 -type REQUEST

bind lb vserver ProxyVserver-SSL -policyName
    ns_videoopt_https_abr_youtube -priority 140 -type REQUEST

bind lb vserver ProxyVserver-SSL -policyName
    ns_videoopt_https_abr_generic -priority 150 -type REQUEST
<!--NeedCopy-->
```

Adición de directivas de optimización para el ritmo del tráfico ABR

Para optimizar el tráfico ABR, debe configurar las directivas de optimización y las acciones asociadas. A continuación, enlaza las directivas a los mismos servidores virtuales de equilibrio de carga a los que vincula las directivas de detección. Para cada directiva, cree primero la acción para poder incluirla al crear la directiva.

Para agregar una acción de optimización

En el símbolo del sistema, escriba:


```
add videooptimization pacingaction <action Name> -rate <integer> [-
    comment <string>]
<!--NeedCopy-->
```

Donde el parámetro **rate** especifica la velocidad en Kbps a la que se enviará el tráfico (velocidad de ritmo).

Ejemplo:

```
add videooptimization pacingaction MyOptAct2000 -rate 2000
<!--NeedCopy-->
```

Para agregar una directiva de optimización

En el símbolo del sistema, escriba:

```
add videooptimization pacingpolicy <name> -rule <expression> -action <
    string>
<!--NeedCopy-->
```

Ejemplo:

```
add videooptimization pacingpolicy myOptPolicy2000 -rule TRUE -action
    MyOptAct2000
<!--NeedCopy-->
```

Vinculación de directivas de optimización a un servidor virtual de equilibrio de carga HTTP

Para optimizar el tráfico de vídeo ABR a través de una conexión HTTP, debe vincular las directivas de optimización a un servidor virtual de equilibrio de carga al que están vinculadas las directivas de detección.

Para enlazar una directiva de optimización a un servidor virtual de equilibrio de carga

En el símbolo del sistema, escriba el siguiente comando:


```
bind lb vserver <name> -policyName <policy_name> -priority <
    positive_integer> -type  (REQUEST | RESPONSE)
<!--NeedCopy-->
```

Ejemplo:

```
bind lb vserver ProxyVserver-HTTP -policyName myOptPolicy2000 -priority
     3400 -type  REQUEST
<!--NeedCopy-->
```

Vinculación de directivas de optimización a servidores virtuales de puente SSL

Para optimizar el tráfico de vídeo ABR a través de una conexión HTTPS, debe vincular las directivas de optimización al servidor virtual SSL Bridge al que están vinculadas las directivas de detección integradas.

Para enlazar una directiva de optimización al servidor virtual SSL Bridge para el ritmo del tráfico cifrado

En el símbolo del sistema, escriba el siguiente comando:

```
bind lb vserver <name> -policyName <policy_name> -priority <
    positive_integer> -type  (REQUEST |RESPONSE)
<!--NeedCopy-->
```

Ejemplo:

```
bind lb vserver ProxyVserver-SSL -policyName myOptPolicy2000 -priority
    3400 -type  REQUEST
<!--NeedCopy-->
```

Configuración de parámetros de ritmo de optimización de vídeo

La CLI le permite establecer los parámetros de ritmo de optimización de vídeo, como el porcentaje de muestreo aleatorio.

Para establecer el porcentaje de muestreo aleatorio

En el símbolo del sistema, escriba el siguiente comando:

```
set videooptimization parameter  - RandomSamplingPercentage <realNumber>
<!--NeedCopy-->
```

Donde un número real es un valor comprendido entre 0,0 y 100,0.

Ejemplo:

```
set videooptimization parameter -RandomSamplingPercentage 50
<!--NeedCopy-->
```

Configuración de la optimización de vídeo a través de TCP mediante la interfaz gráfica de usuario

La interfaz gráfica de usuario le permite:

- Active la función de optimización de vídeo
- Cree un servidor virtual de equilibrio de carga HTTP.
- Cree un servidor virtual de equilibrio de carga de puente SSL.
- Enlazar directivas de detección integradas al servidor virtual de equilibrio de carga HTTP.
- Vincular las directivas de detección integradas al servidor virtual de equilibrio de carga del puente SSL.
- Cree una directiva de optimización.
- Cree una acción de optimización.
- Configuración del parámetro de optimización de ritmo.
- Enlazar la directiva de optimización al servidor virtual de equilibrio de carga para el tráfico HTTP.
- Enlazar la directiva de optimización al servidor virtual de equilibrio de carga de puente SSL para el tráfico HTTPS.

Para activar la función de optimización de vídeo

1. En el panel de navegación, expanda **Sistema**y, a continuación, haga clic en **Configuración**.
2. En la página **Configuración**, haga clic en el enlace **Configurar funciones avanzadas** .
3. En la página **Configurar funciones avanzadas**, active la casilla de verificación **Optimización de vídeo** .
4. Haga clic en **Aceptar** y, a continuación, haga clic en **Cerrar**.

Para crear un servidor virtual de equilibrio de carga para el tráfico HTTP

1. Inicie sesión en el dispositivo Citrix ADC y vaya a la página **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales** .
2. En el panel de detalles, haga clic en **Agregar**.
3. En la pantalla Servidor virtual de equilibrio de carga, defina los siguientes parámetros:
   a) **Name**. Nombre del servidor virtual de equilibrio de carga.
   b) **Protocolo**. Seleccione el tipo de protocolo como HTTP
   c) **Tipo de dirección IP**. Tipo de dirección IP: IPv4 o IPv6.
   d) **Dirección IP**. Dirección IPv4 o IPv6 asignada al servidor virtual.
   e) **Puerto**. Número de puerto del servidor virtual.
4. Haga clic en **Aceptar** para continuar con la configuración de otros parámetros opcionales. Para obtener más información, consulte Creación de un servidor virtual.
5. Haga clic en **Crear** y **cerrar**.

Para crear un servidor virtual de equilibrio de carga para el tráfico HTTPS

1. Inicie sesión en el dispositivo Citrix ADC y vaya a la página **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales** .
2. En el panel de detalles, haga clic en **Agregar**.
3. En la pantalla **Servidor virtual de equilibrio de carga**, defina los siguientes parámetros:
   a) **Name**. Nombre del servidor virtual de equilibrio de carga.
   b) **Protocolo**. Seleccione el tipo de protocolo como puente SSL.
   c) **Tipo de dirección IP**. Tipo de dirección IP: IPv4 o IPv6.
   d) **Dirección IP**. Dirección IPv4 o IPv6 asignada al servidor virtual.
   e) **Puerto**. Número de puerto del servidor virtual.
4. Haga clic en **Aceptar** para continuar con la configuración de otros parámetros opcionales. Para obtener más información, consulte Creación de un servidor virtual.
5. Haga clic en **Crear** y, a continuación, en **Cerrar**.

Para enlazar una directiva de detección integrada a un servidor virtual de equilibrio de carga

1. Inicie sesión en el dispositivo Citrix ADC y vaya a la pantalla **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales** .
2. En el panel de detalles, seleccione el servidor virtual de equilibrio de carga y haga clic en **Modificar**.
   a) En la sección **Configuración avanzada**, haga clic en **Directivas**.
   b) En la sección **Directivas**, haga clic en el icono **+** para acceder al control deslizante **Directivas** .
   c) En la sección **Directivas**, defina los siguientes parámetros.

d) Elija Directiva. Seleccione una directiva de detección de optimización de vídeo de la lista desplegable.
e) Seleccione Tipo. Seleccione el tipo de directiva como Solicitud.
f) Haga clic en **Continue**.

3. Seleccione la directiva de detección de vídeo de la lista y haga clic en **Cerrar**.

Para enlazar una directiva de detección integrada a un servidor virtual de equilibrio de carga de puente SSL

1. Inicie sesión en el dispositivo Citrix ADC y vaya a la pantalla **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales** .
2. En el panel de detalles, seleccione el servidor virtual de equilibrio de carga de puente SSL y haga clic en **Modificar**.
3. En la sección **Configuración avanzada**, haga clic en **Directivas**.
4. En la sección **Directivas**, haga clic en el icono **+** para acceder al control deslizante **Directivas** .
5. En la sección **Directivas**, defina los siguientes parámetros.
   a) Elija Directiva. Seleccione la directiva de detección de optimización de vídeo en la lista desplegable.
   b) Seleccione Tipo. Seleccione el tipo de directiva como Solicitud.
6. Haga clic en **Continue**.
7. Seleccione la directiva de detección de vídeo de la lista y haga clic en **Cerrar**.

Para crear una acción de optimización de vídeo

1. Inicie sesión en el dispositivo Citrix ADC y vaya a **Configuración > Optimización > Optimización de vídeo > RitMO > Acciones**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En la página **Crear acción de ritmo de optimización de vídeo**, defina los siguientes parámetros.
   a) **Name**. Nombre de la acción de optimización.
   b) **Tasa de optimización de ABR (Kbps).** Velocidad de ritmo a la que se envía el tráfico de vídeo ABR. La tasa predeterminada para la optimización de ABR es de 1000 Kbps. El valor mínimo es 1 y el valor máximo es 2147483647.
   c) **Comentario**. Breve descripción de la acción.
4. Haga clic en **Crear** y **cerrar**.

Para crear una directiva de optimización de vídeo

1. Inicie sesión en el dispositivo Citrix ADC y vaya a **Configuración > Optimización > Optimización de vídeo > RitMO > Directivas**.

2. En el panel de detalles, haga clic en **Agregar**.
3. En la página **Crear directiva de ritmo de optimización de vídeo**, defina los siguientes parámetros.
   a) **Name**. Nombre de la directiva de optimización
   b) **Expresión**. Expresiones regulares personalizadas que implementan la directiva.
   c) **Acción**. Acción de optimización asociada a la directiva para gestionar el tráfico de vídeo entrante.
   d) **Acción del FNUD.** Evento indefinido si la solicitud entrante no coincide con la directiva de optimización.
   e) **Comentario**. Breve descripción de la directiva.
   f) **Acción de registro.** Seleccione la acción de registro de auditoría que crea los mensajes de registro deseados.
4. Haga clic en **Crear**y, a continuación, en **Cerrar.**

Para establecer los parámetros de ritmo de optimización de vídeo

1. Inicie sesión en el dispositivo Citrix ADC y vaya a **Configuración** > **Optimización > Optimizaciónde vídeo.**
2. En la página **Optimización de vídeo**, haga clic en **Cambiar configuración de optimización de vídeo** .
3. En la página **Configuración de optimización de vídeo**, defina el siguiente parámetro.
   a) **Porcentaje de muestreo aleatorio (%)**. Porcentaje de paquetes seleccionados para muestreo aleatorio.
4. Haga clic en **Aceptar** y **cerrar**.

Para enlazar una directiva de optimización de vídeo a un servidor virtual de equilibrio de carga HTTP

1. Inicie sesión en el dispositivo Citrix ADC y vaya a **Configuración** > **Optimización > Optimizaciónde vídeo**.
2. En la página **Optimización de vídeo**, haga clic en el enlace **Administrador de directivas de ritmo de optimización de vídeo** .
3. Defina los siguientes parámetros.
   a) **Punto de enlace**. Punto en el que se debe aplicar la directiva de optimización durante el procesamiento de solicitudes o respuestas.
   b) **Tipo de conexión**. Tipo de conexión como solicitud o respuesta.
   c) **Servidor virtual**. El servidor virtual de equilibrio de carga al que se va a vincular la directiva.
   d) Haga clic en **Continue**.
4. En la sección **Punto de enlace**, realice una de las siguientes acciones:

a) Seleccione una directiva de la lista.
b) Haga clic en **Agregar enlace** para acceder al deslizador **Enlace de directivas** .
   i. Seleccione una directiva existente o agregue una nueva directiva.
   ii. Introduzca los detalles del enlace y haga clic en **Enlazar**.
5. Haga clic en **Cerrar**.

Para enlazar una directiva de optimización de vídeo a un servidor virtual de equilibrio de carga de puente SSL

1. Inicie sesión en el dispositivo Citrix ADC y vaya a **Configuración > Optimización > Optimización de vídeo**.
2. En la página **Optimización de vídeo**, haga clic en el enlace **Administrador de directivas de ritmo de optimización de vídeo** .
3. En la página **Administrador de directivas de optimización de vídeo**, defina los siguientes parámetros.
   a) Punto de enlace. Punto en el que se debe aplicar la directiva de optimización durante el procesamiento de la solicitud/respuesta.
   b) Tipo de conexión. Tipo de conexión como solicitud o respuesta.
   c) Servidor virtual. El servidor virtual de equilibrio de carga de puente SSL al que se va a vincular la directiva.
4. Haga clic en **Continue**.
5. En la sección **Punto de enlace**, realice una de las siguientes acciones:
   a) Seleccione un enlace de directiva de la lista.
   b) Haga clic en **Agregar enlace** para acceder al deslizador **Enlace de directivas** .
      i. Seleccione una directiva existente o agregue una nueva directiva.
      ii. Introduzca los detalles del enlace y haga clic en **Enlazar**.
6. Haga clic en **Cerrar**.

Configuración de optimización de vídeo a través de UDP

August 20, 2021

Para optimizar el tráfico de vídeo ABR de QUIC a través de UDP, comience habilitando la función de optimización de vídeo. Una vez completada la configuración, el dispositivo detecta el tráfico de vídeo ABR basado en QUIC y aplica la velocidad de bits de optimización configurada en el dispositivo.

Configuración de la optimización de vídeo para QUIC mediante la CLI

Para configurar la optimización de vídeo para el tráfico de vídeo QUIC a través de UDP, debe realizar las siguientes tareas:

1. Habilite la optimización de vídeo.
2. Cree un servicio QUIC.
3. Cree un servidor virtual de equilibrio de carga QUIC.
4. Enlace el servicio web QUIC al servidor virtual de equilibrio de carga.
5. Cree una directiva de optimización de vídeo para el ritmo del tráfico UDP basado en QUIC.
6. Vincular la directiva de optimización a un servidor virtual de equilibrio de carga basado en QUIC.

Habilitar la optimización de vídeo para el tráfico de QUIC

Si quiere que el dispositivo Citrix ADC detecte, optimice e informe del tráfico de vídeo, debe habilitar la función Optimización de vídeo y establecer la optimización ON.

> **Nota**
>
> Si quiere utilizar la optimización de vídeo para el tráfico de QUIC, debe habilitar las funciones de equilibrio de carga y AppFlow.

Para habilitar la optimización de vídeo

En el símbolo del sistema, escriba el siguiente comando:

```
1 enable ns feature VideoOptimization
2 <!--NeedCopy-->
```

Creación de un servicio para el tráfico de QUIC

Un dispositivo Citrix ADC utiliza un servicio QUIC para que el servidor virtual de equilibrio de carga se conecte al enrutador de salida en el modo de redirección estática.

> **Nota**
>
> Actualmente, no se admite el redirección dinámica.

Para crear un servicio web de equilibrio de carga para el tráfico de vídeo QUIC

En el símbolo del sistema, escriba:


```
add service <name> <router-IP> <serviceType> <port> -usip yes -
   useproxyport  [yes | no]
<!--NeedCopy-->
```

Ejemplo:

```
add service svc-quic 10.102.29.200 QUIC 443  -usip yes  -useproxyport
   no

where IP address is the internet router address.
<!--NeedCopy-->
```

Creación de un servidor virtual de equilibrio de carga para el tráfico QUIC

Un dispositivo Citrix ADC utiliza un servidor virtual de equilibrio de carga para detectar y optimizar el tráfico de vídeo QUIC a través de UDP.

Para crear un servidor virtual de equilibrio de carga para el tráfico de vídeo QUIC

En el símbolo del sistema, escriba:

```
add lb vserver <name> <serviceType> <ip> <port> -m MAC
<!--NeedCopy-->
```

Ejemplo:

```
add lb vserver vs-quic QUIC * 443 -persistenceType NONE -m MAC -
   cltTimeout 120
<!--NeedCopy-->
```

Vinculación de un servicio web QUIC al servidor virtual de equilibrio de carga

Después de crear los servicios web y el servidor virtual de equilibrio de carga para el tráfico QUIC, debe vincular los servicios al servidor virtual.

Para enlazar un servicio web al servidor virtual de equilibrio de carga para el tráfico de vídeo QUIC

En el símbolo del sistema, escriba:

```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Ejemplo:

```
bind lb vserver vs-quic svc-quic
<!--NeedCopy-->
```

Creación de una directiva de optimización de vídeo para el tráfico UDP basado en QUIC

Para optimizar el tráfico UDP basado en QUIC, debe configurar las directivas de optimización de ritmo y sus acciones. A continuación, debe vincular las directivas a los servidores virtuales de equilibrio de carga basados en QUIC. Para cada directiva, cree primero una acción para que pueda asociarla a la directiva.

Para agregar una acción de optimización

En el símbolo del sistema, escriba:

```
add videooptimization pacingaction <action Name> -rate <integer> [-
   comment <string>]
<!--NeedCopy-->
```

Donde el parámetro **de velocidad** especifica la velocidad en Kbps a la que enviar el tráfico (la velocidad de ritmo).

Ejemplo:

```
set videooptimization parameter -QUICPacingRate 1000
<!--NeedCopy-->
```

donde 1000 representa la velocidad de ritmo deseada en Kbits/seg.

Para agregar una directiva de optimización

En el símbolo del sistema, escriba:

```
add videooptimization pacingpolicy <name> -rule <expression> -action <
    string>
<!--NeedCopy-->
```

Ejemplo:

```
add videooptimization pacingpolicy myOptPolicy2000 -rule TRUE -action
    MyOptAct2000
<!--NeedCopy-->
```

Vinculación de directivas de optimización a un servidor virtual de equilibrio de carga QUIC

Para optimizar el tráfico de vídeo QUIC a través de una conexión UDP, debe vincular las directivas de optimización a un servidor virtual de equilibrio de carga QUIC.

Para enlazar una directiva de optimización a un servidor virtual de equilibrio de carga QUIC

En el símbolo del sistema, escriba el siguiente comando:

```
bind lb vserver <name> -policyName <policy_name> -priority <
    positive_integer> -type (REQUEST)
<!--NeedCopy-->
```

> **Nota**
>
> Las directivas de ritmo deben estar enlazadas a un servidor virtual de equilibrio de carga QUIC solo en el momento de la solicitud.

Ejemplo:

```
bind lb vserver vs-quic -policyName myOptPolicy2000 -priority 3400 -
    type  REQUEST
<!--NeedCopy-->
```


Configuración de la optimización de vídeo para QUIC mediante la interfaz gráfica de usuario

Para configurar la función en el dispositivo a través de la interfaz gráfica de usuario, debe realizar las siguientes tareas:

1. Habilitar optimización de vídeo
2. Configurar servidores QUIC
3. Configurar el servicio QUIC
4. Configurar un servidor virtual de equilibrio de carga QUIC
5. Vincular el servicio web QUIC al servidor virtual de equilibrio de carga
6. Cree una directiva de optimización.
7. Crear acción de optimización.
8. Configuración del parámetro de optimización de ritmo.
9. Vincular la directiva de optimización al servidor virtual de equilibrio de carga para el tráfico QUIC.

Para habilitar la optimización de vídeo

1. Inicie sesión en el dispositivo Citrix ADC y vaya a **Sistema** > **Configuración.**
2. En la página de detalles, seleccione el vínculo **Configurar funciones avanzadas**.
3. En la página **Configurar funciones avanzadas**, active la casilla **Optimización de vídeo**.

Para crear servidores QUIC

1. Inicie sesión en el dispositivo Citrix ADC y vaya a la pantalla **Administración del tráfico** > **Equilibrio de carga** > **Servidores**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En la página **Crear servidor**, establezca los siguientes parámetros:
   a) Name. Nombre del servidor QUIC.
   b) Dirección IP. Dirección IP del servidor QUIC
   c) Dominio de tráfico. Nombre de dominio del servidor.
   d) Activación después de la creación. Estado inicial del servidor.
   e) Comentarios. Breve información sobre el servidor.
4. Haga clic en **Crear.**

Para crear un servicio QUIC

1. Inicie sesión en el dispositivo Citrix ADC y vaya a la pantalla **Administración del tráfico** > **Equilibrio de carga** > **Servicios**.
2. En el panel de detalles, haga clic en **Agregar**.

3. En la página **Servicio de equilibrio de carga**, defina los siguientes parámetros:
   a) **Nombre del servicio**. Nombre del servicio QUIC.
   b) **Dirección IP**. Dirección IP asignada al servicio QUIC.
   c) **Protocolo**. Seleccione el protocolo como QUIC.
   d) **Puerto**. Número de puerto del servicio web.
4. Haga clic en **Aceptar** para continuar. A continuación, puede configurar otros parámetros opcionales. Para obtener más información, consulte Configuración de servicios.
5. Una vez configurados los parámetros opcionales, haga clic en **Aceptar** y **Cerrar**.

Para crear un servidor virtual de equilibrio de carga

1. Inicie sesión en el dispositivo Citrix ADC y vaya a la pantalla **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En la página **Servidor virtual de equilibrio de carga**, establezca los siguientes parámetros:
   a) **Name**. Nombre del servidor virtual de equilibrio de carga.
   b) **Protocolo**. Protocolo utilizado por el servicio para enviar solicitudes QUIC.
   c) Tipo de dirección IP. Tipo de dirección IP: IPv4 o IPv6.
   d) **Dirección IP**. Dirección IP 4 o IP6 asignada al servidor virtual.
   e) **Puerto**. Número de puerto del servidor virtual.
4. Haga clic en Aceptar para continuar con la configuración de otros parámetros opcionales. Para obtener más información, consulte Creación de un servidor virtual.

Para enlazar un servidor virtual de equilibrio de carga a un servicio QUIC

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**y seleccione un servidor virtual.
2. Haga clic en **Servicios y grupos de servicios** para acceder a la pantalla **Enlace de servicio de servidor virtual de equilibrio de carga**.
3. Seleccione un servicio web basado en QUIC y haga clic en **Vincular**.
4. Haga clic en **Done**.

Para enlazar un servidor virtual de equilibrio de carga a un servicio QUIC

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**y seleccione un servidor virtual.
2. Haga clic en **Servicios y grupos de servicios** para acceder a la pantalla **Enlace de servicio de servidor virtual de equilibrio de carga**.
3. Seleccione un servicio web basado en QUIC y haga clic en **Vincular**.
4. Haga clic en **Done**.

Para crear una acción de optimización de vídeo para el tráfico de QUIC

1. Inicie sesión en el dispositivo Citrix ADC y vaya a **Configuración** > **Optimización** > **Vídeo Optimización** > **Ritmo** > **Acciones**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En la página **Crear acción de ritmo de optimización de vídeo**, establezca los siguientes parámetros.
   a) **Name**. Nombre de la acción de optimización.
   b) **Velocidad de optimización ABR (Kbps).** Velocidad de ritmo a la que enviar el tráfico de vídeo ABR. La velocidad predeterminada para la optimización ABR es 1000 Kbps. El valor mínimo es 1 y el valor máximo es 2147483647.
   c) **Comentario**. Una breve descripción de la acción.
4. Haga clic en **Crear** y **cerrar**.

Para crear una directiva de optimización de vídeo para el tráfico de QUIC

1. Inicie sesión en el dispositivo Citrix ADC y vaya a **Configuración** > **Optimización** > **Vídeo Optimización** > **Ritmo** > **Directivas**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En la página **Crear directiva de ritmo de optimización de vídeo**, establezca los siguientes parámetros.
   a) Name. Nombre de la directiva de optimización
   b) Expresión. Expresiones regex personalizadas que implementan la directiva.
   c) Acción. Acción de optimización asociada a la directiva para gestionar el tráfico de vídeo entrante.
   d) Acción del UNDEF. Evento indefinido si la solicitud entrante no coincide con la directiva de optimización.
   e) Comentario. Una breve descripción de la directiva.
   f) Acción de registro. Seleccione la acción de registro de auditoría que crea los mensajes de registro deseados.
4. Haga clic en **Crear** y, a continuación, en **Cerrar**.

Para enlazar una directiva de optimización de vídeo a un servidor virtual de equilibrio de carga QUIC

1. Inicie sesión en el dispositivo Citrix ADC y vaya a **Configuración** > **Optimización > Optimización devídeo**.
2. En la página **Optimización de vídeo**, haga clic en el enlace **Administrador de directivas de ritmo de optimización de vídeo**.
3. En la página **Administrador de directivas de optimización de vídeo**, establezca los siguientes parámetros.

a) Punto de enlace. Punto en el que se aplica la directiva de optimización durante el procesamiento de solicitudes. **Nota**: Las directivas de ritmo deben estar enlazadas a un servidor virtual de equilibrio de carga QUIC solo en el momento de la solicitud.
b) Tipo de conexión. Tipo de conexión como Solicitud o Respuesta.
c) Servidor virtual. El servidor virtual de equilibrio de carga al que se va a enlazar la directiva.

4. Haga clic en **Continuar**.
5. En la sección **Punto de enlace**, siga uno de estos procedimientos:
   a) Seleccione una directiva de la lista.
   b) Haga clic en **Agregar enlace** para acceder al control deslizante **Enlace de directivas**.
      i. Seleccione una directiva existente o agregue una directiva nueva.
      ii. Introduzca los detalles del enlace y haga clic en **Enlazar**.
6. Haga clic en **Cerrar**.

Filtrado de URL Citrix ADC

August 20, 2021

El filtrado de URL proporciona un control basado en directivas de sitios web mediante el uso de la información contenida en las URL. Esta función ayuda a los administradores de red a supervisar y controlar el acceso de los usuarios a sitios web maliciosos en redes móviles.

Como administrador, puede configurar una directiva de filtrado de URL mediante la función Categorización de URL o la función Lista de URL.

Lista de URL. Controla el acceso a sitios web y páginas web de la lista de prohibidos bloqueando el acceso a direcciones URL que se encuentren en un conjunto de direcciones URL importadas en el dispositivo.

Categorización de URL. Controla el acceso a sitios web y páginas web filtrando el tráfico sobre la base de una lista predefinida de categorías.

Lista de URL

August 20, 2021

La función Lista de URL permite controlar el acceso a listas de URL personalizadas (hasta un millón de entradas). La función filtra sitios web aplicando una directiva de filtrado de URL enlazada a un servidor virtual.

Como administrador, debe importar la lista de direcciones URL al dispositivo Citrix ADC. Esta lista importada se almacena internamente como un conjunto de datos de directiva denominado conjunto

de *direcciones URL*. A continuación, el dispositivo aplica un algoritmo único de coincidencia rápida de URL a las solicitudes de URL entrantes. Si la solicitud de dirección URL entrante coincide con una entrada del conjunto, el dispositivo aplica la acción de directiva asociada para controlar el acceso.

Tipos de lista de direcciones URL

Cada entrada de un conjunto de URL puede incluir una URL y, opcionalmente, sus metadatos (categoría de URL, grupos de categorías o cualquier otro dato relacionado). Para las direcciones URL con metadatos, el dispositivo utiliza una expresión de directiva que evalúa los metadatos. Para obtener más información, consulte Conjuntos de URL.

Lista de URL personalizada. Puede crear un conjunto de direcciones URL personalizado de hasta 1.000.000 entradas de URL e importarlo como un archivo de texto en el dispositivo. La lista puede contener URL con o sin metadatos (que podrían ser como una categoría de URL). La plataforma Citrix ADC detecta automáticamente si los metadatos están presentes. También es compatible con el almacenamiento de las listas importadas de forma segura. Para obtener más información, consulte Conjunto de URL.

Puede alojar la lista de direcciones URL y configurar el dispositivo Citrix ADC para que actualice periódicamente la lista sin necesidad de intervención manual. Una vez actualizada la lista de direcciones URL, el dispositivo puede detectar automáticamente los metadatos y las categorías mediante expresiones de directiva para evaluar cada dirección URL entrante y, a continuación, aplicar acciones como permitir, bloquear, redirigir o notificar al usuario.

Expresiones de directiva de lista de direcciones URL

En la tabla siguiente se describen las expresiones básicas que puede utilizar para evaluar el tráfico entrante. Después de importar una lista de direcciones URL al dispositivo, se denomina *conjunto de direcciones URL*.

Expresión	Operación
`<URL expression>.URLSET_MATCHES_ANY (<URLSET>)`	Evalúa como TRUE si la URL coincide exactamente con cualquier entrada del conjunto de URL.
`<URL expression>. GET_URLSET_METADATA(<URLSET>)`	La expresión GET_URLSET_METADATA() devuelve los metadatos asociados si la URL coincide exactamente con cualquier patrón dentro del conjunto de URL. Se devuelve una cadena vacía si no hay coincidencia.

Expresión	Operación
<URL expression>.GET_URLSET_METADATA(<URLSET>).EQ(<METADATA>)	Evalúa como TRUE si los metadatos coincidentes son iguales a <METADATA>.
<URLexpression>.GET_URLSET_METADATA(<URLSET>).TYPECAST_LIST_T(‘,’).GET(0).EQ(<CATEGORY>)	Evalúa como TRUE si los metadatos coincidentes están al principio de la categoría. Este patrón se puede utilizar para codificar campos separados dentro de los metadatos, pero solo coinciden con el campo 1st.
HTTP.REQ.HOSTNAME.APPEND (HTTP.REQ.URL)	Se une a los parámetros host y URL, que luego se pueden utilizar como un <URL expression> para la coincidencia.

Acciones de directiva de lista de direcciones URL

La acción de aplicación más común para las direcciones URL que coinciden con una lista de direcciones URL es restringir el acceso. Cree una directiva de lista de direcciones URL con una expresión coincidente de lista de direcciones URL deseada y una acción de aplicación. El uso del grupo de directivas depende del tipo de tráfico entrante (HTTP o HTTPS) y del servidor virtual configurado en el dispositivo. Puede utilizar una directiva Responder para el tráfico HTTP o una directiva de Optimización de vídeo para el tráfico HTTPS. Especifique las acciones que se aplicarán a las direcciones URL que coincidan con las expresiones de las directivas. En la siguiente tabla se enumeran las acciones disponibles.

Tipo de acción	Directiva	Descripción
ALLOW	Responder	Permitir que la solicitud acceda a la URL de destino.
REDIRECT	Responder	Redirigir la solicitud a la URL especificada como destino.
DENY	Responder	Denegar la solicitud.
RESTABLECER	Responder, VideoOptimization	Restablezca la conexión.
DROP	Responder, VideoOptimization	Suelta la conexión.

Requisitos previos

Para configurar la función Lista de URL, asegúrese de haber configurado el siguiente servidor.

Servidor DNS para solicitudes DNS

Debe configurar un servidor DNS si importa un conjunto de direcciones URL desde una dirección URL de nombre de host.

En el símbolo del sistema, escriba:

```
add dns nameServer ((<IP> [-local]) | <dnsVserverName>) [-state (
    ENABLED | DISABLED )] [-type <type>] [-dnsProfileName <string>]
<!--NeedCopy-->
```

Ejemplo:

```
add dns nameServer 10.140.50.5
<!--NeedCopy-->
```

Importar una lista de URL personalizada

Para importar un conjunto de URL, consulte el tema Conjunto de URL .

Configuración de una lista de direcciones URL para el tráfico HTTP

El dispositivo Citrix ADC admite tráfico HTTP y HTTPS. Para configurar un servidor virtual de equilibrio de carga para el tráfico HTTP y vincular directivas de lista de URL al servidor, haga lo siguiente:

- Agregar acciones de lista de URL.
- Agregar directivas de lista de direcciones URL.
- Agregar un servidor virtual de equilibrio de carga HTTP para el tráfico HTTP
- Enlazar las directivas de la lista de direcciones URL al servidor virtual de equilibrio de carga HTTP para el tráfico HTTP

Para agregar una acción de lista de URL

En el símbolo del sistema, escriba lo siguiente:


```
add responder action <name> <type> (<target> | <htmlpage>) [-comment <
    string>] [-responseStatusCode <positive_integer>] [-reasonPhrase <
    string>]
<!--NeedCopy-->
```

Para agregar un servidor virtual de equilibrio de carga HTTP para el tráfico HTTP

En el símbolo del sistema, escriba lo siguiente:

```
add lb vserver <name> [-td <positive_integer>] <serviceType> [-cltT
    imeout <secs>]
<!--NeedCopy-->
```

Ejemplo:

```
add lb vserver vsrv-HTTP HTTP * 80 -persistenceType NONE -cltTimeout
    120
<!--NeedCopy-->
```

Para enlazar la directiva de lista de URL al servidor virtual de equilibrio de carga HTTP

En el símbolo del sistema, escriba lo siguiente:

```
bind lb vserver <vServerName> -policyName <string> [-priority <
    positive_integer>]
<!--NeedCopy-->
```

Configuración de la lista de URL para el tráfico HTTPS

El dispositivo Citrix ADC admite tráfico HTTP y HTTPS. Para configurar un servidor virtual de equilibrio de carga de puente SSL para el tráfico HTTPS y las directivas de lista de URL de enlace al servidor, haga lo siguiente:

- Agregar acciones de lista de URL.
- Agregar directivas de lista de direcciones URL.
- Agregar un servidor virtual de equilibrio de carga de puente SSL para el tráfico HTTP

- Enlazar las directivas de la lista de direcciones URL al servidor virtual de equilibrio de carga del puente SSL para el tráfico HTTP

Para agregar una directiva de lista de direcciones URL para el tráfico HTTPS

En el símbolo del sistema, escriba:

```
add videooptimization detectionpolicy <name> -rule <expression> -action
     <string> [-undefAction <string>] [-comment <string>] [-logAction <
    string>]
<!--NeedCopy-->
```

Para agregar un servidor virtual de equilibrio de carga de puente SSL

En el símbolo del sistema, escriba:

```
add lb vserver <name> [-td <positive_integer>] <serviceType> [-cltT
    imeout <secs>]
<!--NeedCopy-->
```

Ejemplo:

```
add lb vserver vsrv-HTTPS SSL_BRIDGE * 443 -persistenceType NONE -
    cltTimeout 180
<!--NeedCopy-->
```

Para enlazar la directiva de lista de URL con el equilibrio de carga del puente SSL mediante la CLI

En el símbolo del sistema, escriba:

```
bind lb vserver <vServerName> -policyName <string> [-priority <
    positive_integer>]
<!--NeedCopy-->
```


Configuración de una lista de direcciones URL mediante la interfaz gráfica de usuario

La GUI le permite:

- Importar una lista de direcciones URL.
- Agregar una lista de direcciones URL.
- Configurar acciones de lista de URL.
- Configurar directivas de lista de URL para el tráfico HTTP.
- Agregue un servidor virtual de equilibrio de carga HTTP para el tráfico HTTP.
- Agregue un servidor virtual de equilibrio de carga de puente SSL para el tráfico HTTPS.
- Vincular directivas de lista de URL al servidor virtual de equilibrio de carga HTTP.
- Enlazar directivas de lista de direcciones URL al servidor virtual de equilibrio de carga del puente SSL.

Para importar una lista de direcciones URL

1. En el panel de navegación, expanda **AppExpert** > **Conjuntos de URL**.
2. En el panel de detalles, haga clic en **Importar**.
3. En la página **Configurar conjunto de direcciones URL**, establezca los siguientes parámetros.
   a) **Name**. Nombre del conjunto de direcciones URL.
   b) **URL**. Dirección web de la ubicación en la que se accede al conjunto de direcciones URL.
   c) **Sobrescribir**. Sobrescribir un conjunto de direcciones URL previamente importado.
   d) **Delimitador**. Secuencia de caracteres que delimita un registro de archivo CSV.
   e) **Separador de filas**. Separador de filas utilizado en el archivo CSV. Se permite un valor de carácter único, por ejemplo “/n”.
   f) **Intervalo**. Intervalo en segundos, redondeado a los 15 minutos más próximos, en los que se actualiza el conjunto de direcciones URL.
   g) **Conjunto privado.** Opción para impedir la exportación del conjunto de direcciones URL
   h) **URL Canary**. URL interna para comprobar si el contenido del conjunto de URL debe mantenerse confidencial. La longitud máxima de la URL es de 2047 caracteres
4. Haga clic en **Crear** y, a continuación, en **Cerrar**.

Para agregar una lista de direcciones URL

1. En el panel de navegación, expanda **AppExpert** > **Conjuntos de URL**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En la página **Crear conjunto de direcciones URL**, establezca los siguientes parámetros.
   a) **Name**. Nombre del conjunto de direcciones URL que se dio al importarlo.
   b) **Comentarios**. Una breve descripción sobre el conjunto de URL.
4. Haga clic en **Crear**.

Para configurar una acción de lista de URL

1. Inicie sesión en el dispositivo Citrix ADC y vaya a la página **de la ficha Configuración**.
2. En el panel de menús, vaya a **AppExpert** > **Respondedor** > **Acciones**.
3. En el panel de detalles, haga clic en **Agregar**.
4. En la página **Crear acción del respondedor**, establezca los siguientes parámetros.
   a) **Name**. Nombre de la acción de directiva Lista de URL.
   b) **Tipo**. Seleccione un tipo de acción.
   c) **Expresión**. Utilice el editor de expresiones para crear la expresión de directiva.
   d) **Comentarios**. Una breve descripción de la acción de directiva.
5. Haga clic en **Crear** y **cerrar**.

Para configurar una directiva de lista de direcciones URL

1. En el panel de navegación, expanda **AppExpert** > **Respondedor** > **Directivas**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En la página **Crear Directiva de Respondedor**, establezca los siguientes parámetros.
   a) **Name**. Nombre de la acción de directiva Lista de URL.
   b) **Acción**. Seleccione la acción Lista de direcciones URL que prefiera asociar a la directiva.
   c) **Acción de registro**. Seleccione la acción de registro.
   d) **AppFlow**. Seleccione una acción de AppFlow.
   e) **Expresión**. Utilice el editor de expresiones para crear la expresión de directiva.
   f) **Comentarios**. Una breve descripción de la directiva.
4. Haga clic en **Crear** y **cerrar**.

Para agregar un servidor virtual de equilibrio de carga HTTP

1. Acceda a la página **Gestión del Tráfico** > **Equilibrio de Carga** > **Servidores Virtuales**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En la pantalla **Servidor virtual de equilibrio de carga**, establezca los siguientes parámetros:
   a) **Name**. Nombre del servidor virtual de equilibrio de carga.
   b) **Protocolo**. Elija el tipo de protocolo como HTTP.
   c) **Tipo de dirección IP**. Tipo direccionable IP.
   d) **Dirección IP**. Dirección IP 4 o IP6 asignada al servidor virtual.
   e) **Puerto**. Número de puerto del servidor virtual.
4. Haga clic en **Aceptar** para continuar con la configuración de otros parámetros opcionales. Para obtener más información, vea Creación de un servidor virtual.

Para enlazar una directiva de lista de direcciones URL al servidor virtual de equilibrio de carga HTTP

1. Vaya a la pantalla **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**.
2. En el panel de detalles, seleccione el servidor virtual de equilibrio de carga y haga clic en **Modificar**.
3. En la sección **Configuración avanzada**, haga clic en **Directivas**.
4. En la sección **Directivas**, haga clic en el icono **+** para acceder al control deslizante **Directivas**.
5. En la sección **Directivas**, establezca los siguientes parámetros.
   a) Seleccione Directiva. Seleccione una directiva de categorización de URL en la lista desplegable.
   b) Elija Tipo. Seleccione el tipo de directiva como Solicitud.
6. Haga clic en **Continuar**.
7. En la página Directivas, seleccione la directiva Lista de URL de la lista y haga clic en **Seleccionar**.
8. En el control deslizante **Directivas**, haga clic en **Vincular** y **cerrar**.

Para agregar directiva de lista de URL para el tráfico HTTPS

1. Inicie sesión en el dispositivo Citrix ADC y vaya a **Configuración** > **Optimización** > **Vídeo Optimización** > **Detección**.
2. En la página **Detección**, haga clic en el enlace **Directivas de detección de optimización de vídeo**.
3. En la página **Directivas de detección de optimización de vídeo**, haga clic en **Agregar**.
4. En la página **Crear directiva de detección de optimización de vídeo**, establezca los siguientes parámetros.
   a) **Name**. Nombre de la directiva de optimización
   b) **Expresión**. Configure la directiva mediante expresiones personalizadas.
   c) **Acción**. Acción de optimización asociada a la directiva para gestionar el tráfico de vídeo entrante.
   d) **Acción del FNUD**. Evento indefinido si la solicitud entrante no coincide con la directiva de optimización.
   e) **Comentario**. Una breve descripción de la directiva.
   f) **Acción de registro**. Seleccione una acción de registro de auditoría que especifique la acción que se va a realizar para los mensajes de registro.
5. Haga clic en **Crear** y **cerrar**.

Para agregar un servidor virtual de equilibrio de carga de puente SSL para el tráfico HTTPS

1. Acceda a la página **Gestión del Tráfico** > **Equilibrio de Carga** > **Servidores Virtuales**.
2. En el panel de detalles, haga clic en **Agregar**.

3. En la pantalla **Servidor virtual de equilibrio de carga**, establezca los siguientes parámetros:
   a) **Name**. Nombre del servidor virtual de equilibrio de carga.
   b) **Protocolo**. Seleccione el tipo de protocolo como puente SSL.
   c) **Tipo de dirección IP**. Tipo de dirección IP: IPv4 o IPv6.
   d) **Dirección IP**. Dirección IPv4 o IP6vip asignada al servidor virtual.
   e) **Puerto**. Número de puerto del servidor virtual.
4. Haga clic en **Aceptar** para continuar con la configuración de otros parámetros opcionales. Para obtener más información, consulte el tema "Creación de un servidor virtual".

Para enlazar una directiva de lista de direcciones URL al servidor virtual de equilibrio de carga del puente SSL

1. Vaya a la pantalla **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**.
2. En el panel de detalles, seleccione el servidor virtual de equilibrio de carga del puente SSL y haga clic en **Modificar**.
3. En la sección **Configuración avanzada**, haga clic en **Directivas**.
4. En la sección **Directivas**, haga clic en el icono **+** para acceder al control deslizante **Directivas**.
5. Defina los siguientes parámetros.
   a) **Elija Directiva.** Seleccione la directiva de detección de vídeo en la lista desplegable.
   b) **Elija Tipo**. Seleccione el tipo de directiva como Solicitud.
6. Haga clic en **Continuar**.
7. Seleccione la directiva de detección de vídeo de la lista y haga clic en **Cerrar**.

Configuración de la mensajería del registro de auditoría

El registro de auditoría le permite revisar una condición o una situación en cualquier fase del proceso de lista de direcciones URL. Cuando un dispositivo Citrix ADC recibe una dirección URL entrante, si la directiva de respondedor tiene una expresión avanzada de directiva de conjunto de direcciones URL, la función de registro de auditoría recopila información de conjunto de direcciones URL en la URL y almacena los detalles como un mensaje de registro para cualquier destino permitido por el registro de auditoría.

El mensaje de registro contiene la siguiente información:

1. Marca de tiempo.
2. Tipo de mensaje de registro.
3. Niveles de registro predefinidos (Crítico, Error, Aviso, Advertencia, Informativo, Depuración, Alerta y Emergencia).
4. Información del mensaje de registro, como el nombre del conjunto de direcciones URL, la acción de directiva o la dirección URL.

Para configurar el registro de auditoría para la función Lista de URL, debe completar las siguientes tareas:

1. Habilitar registros de auditoría.
2. Acción de mensaje Crear registro de auditoría.
3. Establecer la directiva de respuesta de lista de URL con la acción de mensaje Registro de auditoría.

Para obtener más información, consulte Registro de auditoría.

Semántica de lista de URL

En la tabla siguiente se enumeran los patrones de coincidencia de URL y se describe cómo las direcciones URL de una lista de URL coinciden con las direcciones URL de solicitudes entrantes. Por ejemplo, el patrón www.example.com/bar solo coincide con una página en www.example.com/bar. Para que coincidan todas las páginas cuya URL comience por 'www.example.com/bar', debe agregar un asterisco (*) al final de la URL.

Semántica	Patrón de URL	Coincidido	Incomparable
Coincidencia de subdominios	dominio.com	dominio.com; www.domain.com; sub.one.domain.com	tudominio.com; www.dominio.com
Coincidencia de URL, ruta exacta	dominio.com/ejemplo/bar/index.html	dominio.com/ejemplo/bar/index.html; www.domain.com/example/bar/index.html; s.domain.com/example/bar/index.html	wwwdomaincom/ejemplo/bar/index.html; dominio.com/ejemplo/bar/index.html/
Coincidencia de URL, ruta exacta	dominio.com/ejemplo/	domain.com/example/index.html?key=value; www.domain.com/example/bar; s.domain.com/example	wwwdomaincom/ejemplo/bar/index.html; dominio.com/ejemplo/bar/index.html/
Coincidencia de URL, coincidencia de subrutas	dominio.com/ejemplo/bar/	domain.com/ejemplo/bar/; dominio.com/ejemplo/bar/index.html; www.domain.com/example/bar/index.html; dominio.com/ejemplo/bar/index.html/one.jpg	wwwdomaincom/ejemplo/bar/index.html;

Categorización de URL

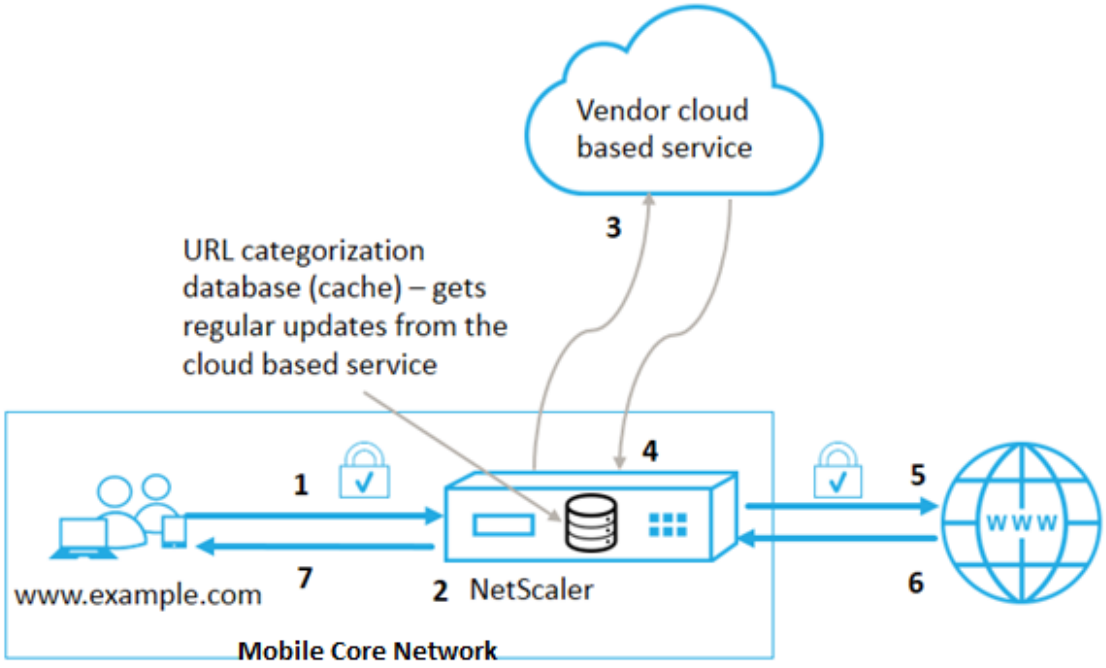
August 20, 2021

La categorización de URL restringe el acceso de los usuarios a sitios web específicos y categorías de sitios web. Como servicio suscrito en colaboración conNetSTAR, la función permite a los clientes empresariales filtrar el tráfico web mediante una base de datos de categorización comercial. LaNetSTAR base de datos tiene un gran número (miles de millones) de URL clasificadas en diferentes categorías, como redes sociales, juegos de azar, contenido para adultos, nuevos medios y compras. Además de la categorización, cada URL tiene una puntuación de reputación actualizada basada en el perfil de riesgo histórico del sitio. Podemos utilizarNetSTAR los datos para filtrar el tráfico mediante la configuración de directivas avanzadas basadas en categorías, grupos de categorías (como Terrorismo, Drogas ilegales) o puntuaciones de reputación de sitio.

Por ejemplo, puede bloquear el acceso a sitios peligrosos, como sitios infectados con malware, o restringir selectivamente el acceso a contenido para adultos o contenido multimedia de entretenimiento en streaming.

Cómo funciona la categorización de URL

En la siguiente ilustración se muestra cómo se integra el servicio de filtrado de URL de Citrix ADC con una base de datos comercial de categorización de URL y servicios en la nube para actualizaciones frecuentes.



Los componentes interactúan de la siguiente manera:

1. El cliente envía una solicitud de URL enlazada a Internet.
2. Una directiva Citrix ADC intenta evaluar la solicitud en términos de detalles de categorización (como categoría, grupo de categorías y puntuación de reputación de sitio) recuperados de la base de datos de categorización de URL. Si la base de datos devuelve los detalles de la categoría, el proceso salta al paso 5.
3. Si la base de datos no devuelve detalles de categorización, la solicitud se envía a un servicio de búsqueda basado en la nube mantenido por un proveedor de categorización de URL. Sin embargo, el dispositivo no espera una respuesta. En su lugar, marca la URL como Sin categoría y salta al paso 5. Sin embargo, continúa supervisando los comentarios de las consultas en la nube y lo utiliza para actualizar la caché de modo que las futuras solicitudes puedan beneficiarse de la búsqueda en la nube.
4. El dispositivo Citrix ADC recibe los detalles de la categoría de URL (categoría, grupo de categorías y puntuación de reputación) del servicio basado en la nube y los almacena en la caché de la nube.
5. Si la directiva permite la URL, la solicitud se envía al servidor de origen. De lo contrario, el dispositivo descarta o redirige la solicitud o responde con una página HTML personalizada.
6. El servidor de origen responde con los datos solicitados al dispositivo Citrix ADC.
7. El dispositivo envía la respuesta al cliente.

Puede utilizar la función de filtrado de URL para detectar sitios que infrinjan los mandatos de uso seguro de Internet emitidos por el gobierno e implementar directivas para bloquear estos sitios. Sitios que alojan contenido para adultos, medios de transmisión o redes sociales identificados como inseguros para niños o prohibidos como ilegales.

Requisitos previos

La función funciona en plataformas Telco con la compra de una licencia CBM básica y una licencia CBM Premium, y para otras plataformas Citrix ADC, la función funciona con la compra de una licencia CNS Premium.

Nota: Además de una licencia Basic CBM y una licencia CBM Premium, el dispositivo debe tener una licencia de URL Threat Intelligence con un servicio de suscripción durante 1 o 3 años. Antes de habilitar y configurar la función, debe instalar las siguientes licencias:

Soporte de licencia para plataformas de telecomunicaciones:

- **CBM_TXXX_SERVER_Retail.lic**
- **CBM_TPRE_SERVER_Retail.lic**
- **CNS_WebF_SServer_Retail.lic**

Donde XXX es el rendimiento, por ejemplo, Citrix ADC T1000.

Compatibilidad con licencias para otras plataformas Citrix ADC:

- **CNS_XXX_SERVER_PLT_Retail.lic**

Donde XXX es el rendimiento.

Expresiones de directiva de categorización de URL

En la tabla siguiente se enumeran las diferentes expresiones de directiva de categorización de URL para identificar direcciones URL entrantes y se aplica una acción configurada.

Expresión	Operación
<text>. URL_CATEGORIZE (<min_reputation>, <max_reputation>)	Devuelve un objeto URL_CATEGORY. La puntuación de la reputación es un número del 1 al 4. Para obtener objetos, todas las puntuaciones de reputación utilizan 0.0 como <min reputation> y <max_reputation>. Si <min_reputation> es mayor que 0, el objeto devuelto no contiene una categoría con reputación inferior a <min_reputation>. Si <max_reputation> es mayor que 0, el objeto devuelto no contiene una categoría con reputación superior a <max_reputation>. Si la categoría no se resuelve de manera oportuna, se devuelve el valor undef.
<url_category>. CATEGORÍA	Devuelve la cadena de categoría de este objeto. Si la URL no tiene una categoría, o si la URL tiene un formato incorrecto, el valor devuelto es “Sin categoría”.
<url_category>. GRUPO	Devuelve una cadena que identifica el grupo de categorías del objeto. Se trata de una agrupación de categorías de nivel superior, que es útil en operaciones que requieren información menos detallada sobre la categoría de URL. Si la URL no tiene una categoría, o si la URL tiene un formato incorrecto, el valor devuelto es “Sin categoría”.

Expresión	Operación
<url_category>. REPUTACIÓN	Devuelve la puntuación de reputación como un número de 1 a 4, donde 4 indica la reputación más riesgosa. Si la categoría es “Sin categoría”, el valor de reputación es 2.

Expresiones de directiva de ejemplo

Directiva	Expresiones de directiva
Directiva para seleccionar las solicitudes de direcciones URL que se encuentran en la categoría Motor de búsqueda	add responder policy p1 ‘HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGO CATEGORY.EQ(“Search Engine”)
Directiva para seleccionar solicitudes de URL que se encuentren en el grupo de categoría Adulto	add responder policy p1 ‘HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGO GROUP.EQ(“Adult”)’
Directiva para seleccionar solicitudes de direcciones URL del motor de búsqueda con una puntuación de reputación igual a 4.	add responder policy p2 ‘HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGO CATEGORY.EQ(“Search Engine”)’
Directiva para seleccionar solicitudes de URL del motor de búsqueda y de Shopping	add policy patset good_categories; bind policy good_categories “Search Engine”; bind policy good_categories “Shopping”; add responder policy p3 ‘HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGO CATEGORY .EQUALS_ANY(“good_categories”)
Directiva para seleccionar solicitudes de direcciones URL del motor de búsqueda con una puntuación de reputación igual a 4.	add responder policy p5 ‘CLIENT.SSL.DETECTED_DOMAIN.URL_CATEGORIZE(4,0). CATEGORY.EQ(“Search Engine”)

Acciones de directiva de categorización de URL

Una directiva de filtrado de URL evalúa el tráfico para identificar las solicitudes que pertenecen a una categoría determinada. En la tabla siguiente se enumeran las acciones que puede asignar a una directiva de filtrado de URL.

Directiva de acción	Grupo de directivas	Descripción
ALLOW	Responder	Permitir que la solicitud entrante acceda a la URL de destino
REDIRECT	Responder	Redirigir la solicitud entrante a la URL especificada como destino.
DENY	Responder	Denegar solicitud entrante.
RESTABLECER	Responder, VideoOptimization	Restablecer conexión.
DROP	Responder, VideoOptimization	Suelta la conexión.

> **Nota**
>
> Para el tráfico cifrado, la directiva VideoOptimization incluye acciones que implementan las acciones de filtrado de URL.

Configuración de categorización de URL

Para configurar la categorización de URL, comience habilitando la función Filtrado de URL. A continuación, debe configurar los límites de memoria caché, la directiva de categorización y los servidores virtuales para el tráfico HTTP y HTTPS. Configuración de la categorización de URL mediante la CLI.

Para utilizar la categorización de URL de configuración de la CLI en un dispositivo Citrix ADC, haga lo siguiente:

- Configurar categorización de URL.
  - Habilite la función de filtrado de URL.
  - Configure la memoria compartida para limitar la memoria caché.
  - Configure los parámetros de categorización de URL.
- Configure la categorización de URL para el tráfico HTTP.
  - Agregar acciones de categorización de URL.
  - Agregar directivas de categorización de URL.
  - Agregue un servidor virtual de equilibrio de carga para el tráfico HTTP.
  - Vincular las directivas de categorización de URL al servidor virtual de equilibrio de carga.
- Configure la categorización de URL para el tráfico HTTPS.
  - Agregar directivas de categorización de URL.
  - Agregue un servidor virtual de equilibrio de carga de puente SSL.

- Vincular las directivas de categorización de URL al servidor virtual de equilibrio de carga.

Configuración de categorización de URL

Para configurar la función, debe habilitar la función Categorización de URL, configurar los parámetros de filtrado y establecer el límite de memoria compartida.

Para habilitar la función Filtrado de URL

En el símbolo del sistema, escriba:

```
enable ns feature URLFiltering VideoOptimization Responder IC SSL AppFlow
```

Para configurar el límite de memoria compartida

En el símbolo del sistema, escriba:

```
1 set cache parameter [-memLimit <megaBytes>]
2 <!--NeedCopy-->
```

Donde MemLimit es el límite de memoria para el almacenamiento en caché.

Ejemplo:

```
set cache parameter -memLimit 10
```

Para configurar los parámetros de categorización de URL

En el símbolo del sistema, escriba:

```
1 set urlfiltering parameter [-HoursBetweenDBUpdates <positive_integer>]
     [-TimeOfDayToUpdateDB <HH:MM>]
2 <!--NeedCopy-->
```

***Ejemplo:**

```
set urlfiltering parameter -HoursBetweenDBUpdates 3 -TimeOfDayToUpdateDB
03:00
```


Configuración de la categorización de URL para el tráfico HTTP

Para configurar la función de categorización de URL para el tráfico HTTP, debe configurar un servidor virtual de equilibrio de carga, agregar directivas de categorización de URL y enlazar las directivas al servidor virtual. Al hacerlo, el servidor virtual recibe el tráfico HTTP y, en función de la evaluación de directivas, el sistema asigna una acción de filtrado.

Para agregar acción de categorización de URL para el tráfico HTTP

En el símbolo del sistema, escriba:

```
add responder action <name> <type> (<target> | <htmlpage>)[-comment <string
>] [-responseStatusCode <positive_integer>] [-reasonPhrase <string>]
```

Ejemplo:

```
add responder action act_url_categorize respondwith "\"HTTP/1.1 200 OK\r\n\
r\n\" + HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGORIZE(0,0).CATEGORY
 + \"\n\""
```

Para agregar directiva de categorización de URL para el tráfico HTTP

En el símbolo del sistema, escriba:

```
add responder policy <name> <rule> <action> [<undefAction>] [-comment <
string>] [-logAction <string>] [-appflowAction <string>]
```

Ejemplo:

```
add responder policy pol_url_categorize_http "HTTP.REQ.HOSTNAME.APPEND(
HTTP.REQ.URL).URL_CATEGORIZE(0,0).GROUP.EQ(\"Adult\")|| HTTP.REQ.HOSTNAME.
APPEND(HTTP.REQ.URL).URL_CATEGORIZE(0,0).GROUP.EQ(\"Gambling\")"RESET
```

Para agregar un servidor virtual de equilibrio de carga HTTP

Si un servidor virtual para el tráfico HTTP aún no está configurado, en el símbolo del sistema, escriba:

```
add lb vserver <name> [-td <positive_integer>] <serviceType> [-clt Timeout
<secs>]
```

Ejemplo:

```
add lb vserver vsrv-HTTP HTTP * 80 -persistenceType NONE -cltTimeout 120
```


Para enlazar la directiva de categorización de URL con el servidor virtual de equilibrio de carga

En el símbolo del sistema, escriba:

```
bind lb vserver <name> -policyName <string> [-priority <positive_integer>]
```

Ejemplo:

```
bind lb vserver vsrv-HTTP -policyName pol_url_categorize_http -priority 10
-gotoPriorityExpression END -type REQUEST
```

Configuración de la categorización de URL para el tráfico HTTPS

Para configurar la función de categorización de URL para el tráfico HTTPS, debe configurar un servidor virtual de equilibrio de carga de puente SSL, agregar directivas de categorización de URL y enlazar las directivas al servidor virtual de puente SSL. Al hacerlo, el servidor recibe el tráfico HTTPS y, en función de la evaluación de directivas, el sistema asigna una acción de filtrado.

Para agregar directiva de categorización de URL para el tráfico HTTPS

En el símbolo del sistema, escriba:

```
add videooptimization detectionpolicy <name> -rule <expression> -action <
string> [-undefAction <string>] [-comment <string>] [-logAction <string>]
```

Ejemplo:

```
add videooptimization detectionpolicy pol_url_categorize_https_block_adult -
rule "CLIENT.SSL.DETECTED_DOMAIN.URL_CATEGORIZE(0,0).CATEGORY.EQ("Adult")' -
action RESET
```

Para agregar un servidor virtual de equilibrio de carga de puente SSL

En el símbolo del sistema, escriba:

```
add lb vserver <name> [-td <positive_integer>] <serviceType> [-cltT imeout
<secs>]
```

Ejemplo:

```
add lb vserver vsrv-HTTPS SSL_BRIDGE * 443 -persistenceType NONE -cltTimeout
 180
```

Para enlazar la directiva de categorización con el servidor virtual de puente SSL

En el símbolo del sistema, escriba:


```
bind lb vserver <name> -policyName <string> [-priority <positive_integer>]
```

Ejemplo:

```
bind lb vserver vsrv-HTTPS -policyName pol_url_categorize_https_block_adult
 -priority 20 -type REQUEST
```

Configuración de la categorización de URL mediante la interfaz gráfica de usuario

La GUI le permite:

- Habilite la función de categorización de URL.
- Agregar acciones de categorización de URL para el tráfico HTTP.
- Agregar directivas de categorización de URL para el tráfico HTTP.
- Agregar directivas de categorización de URL para el tráfico HTTPS.
- Agregue un servidor virtual de equilibrio de carga para el tráfico HTTP.
- Agregue un servidor virtual de equilibrio de carga de puente SSL para el tráfico HTTPS.
- Vincular las directivas de categorización de URL al servidor virtual de equilibrio de carga.
- Vincular las directivas de categorización de URL al servidor virtual de equilibrio de carga del puente SSL.
- Configure el límite de memoria compartida.
- Configure los parámetros de categorización de URL.

Para habilitar la categorización de URL

1. En el panel de navegación, expanda **Sistema** y, a continuación, haga clic en **Configuración**.
2. En la página **Configuración**, haga clic en el vínculo **Configurar funciones avanzadas**.
3. En la página **Configurar funciones avanzadas**, active la casilla de verificación **Filtrado de URL**.
4. Haga clic en **Aceptar** y **Cerrar**.

Para agregar una acción de categorización de URL

1. En el panel de navegación, expanda **AppExpert** > Respondedor >**** **Acción**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En la página **Crear acción del respondedor**, establezca los siguientes parámetros.
   a) **Name**. Nombre de la acción de directiva de categorización de URL.
   b) **Tipo**. Seleccione un tipo de acción.
   c) **Expresión**. Utilice el editor de expresiones para crear la expresión de directiva.
   d) **Comentarios**. Una breve descripción de la acción de directiva.
4. Haga clic en **Crear** y **cerrar**.

Para agregar una directiva de categorización de URL para el tráfico HTTP

1. En el panel de navegación, expanda **AppExpert** > **Respondedor** > **Directivas**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En la página **Crear Directiva de Respondedor**, establezca los siguientes parámetros.
   a) **Name**. Nombre de la acción de directiva de categorización de URL.
   b) **Acción**. Seleccione la acción Categorización de URL que prefiera asociar a la directiva.
   c) **Acción de registro**. Seleccione la acción de registro.
   d) **AppFlow**. Seleccione una acción de AppFlow.
   e) **Expresión**. Utilice el editor de expresiones para crear la expresión de directiva.
   f) **Comentarios**. Una breve descripción de la acción de directiva.
4. Haga clic en **Crear** y **cerrar**.

Para agregar una directiva de categorización para el tráfico HTTPS

1. Inicie sesión en el dispositivo Citrix ADC y vaya a **Configuración** > **Optimización** > **Vídeo Optimización** > **Detección**.
2. En la página **Detección**, haga clic en el enlace **Directivas de detección de optimización de vídeo**.
3. En la página Directivas de detección de optimización de vídeo, haga clic en **Agregar**.
4. En la página **Crear directiva de detección de optimización de vídeo**, establezca los siguientes parámetros.
   a) **Name**. Nombre de la directiva de optimización
   b) **Expresión**. Configure la directiva mediante expresiones personalizadas.
   c) **Acción**. Acción de optimización asociada a la directiva para gestionar el tráfico de vídeo entrante.
   d) **Acción del FNUD**. Evento indefinido si la solicitud entrante no coincide con la directiva de optimización.
   e) **Comentario**. Una breve descripción de la directiva.
   f) **Acción de registro.** Seleccione una acción de registro de auditoría que especifique la acción que se va a realizar para los mensajes de registro.
5. Haga clic en **Crear** y **cerrar**.

Para agregar un servidor virtual de equilibrio de carga para el tráfico HTTP

1. Acceda a la página **Gestión del Tráfico** > **Equilibrio de Carga** > **Servidores Virtuales**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En la página **Servidor virtual de equilibrio de carga**, establezca los siguientes parámetros:
   a) **Name**. Nombre del servidor virtual de equilibrio de carga.
   b) **Protocolo**. Elija el tipo de protocolo como HTTP.

c) **Tipo de dirección IP.** IPv4 o IPv6.
d) **Dirección IP.** IPv4 o IPv6, dirección VIP asignada al servidor virtual.
e) **Puerto**. Número de puerto del servidor virtual.

4. Haga clic en **Aceptar** para continuar con la configuración de otros parámetros opcionales.
5. Haga clic en **Crear** y **cerrar**.

Para agregar un servidor virtual de equilibrio de carga de puente SSL

1. Acceda a la página **Gestión del Tráfico** > **Equilibrio de Carga** > **Servidores Virtuales**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En la página **Servidor virtual de equilibrio de carga**, establezca los siguientes parámetros:
   a) **Name**. Nombre del servidor virtual de equilibrio de carga.
   b) **Protocolo**. Seleccione el tipo de protocolo como puente SSL.
   c) **Tipo de dirección IP**. Tipo direccionable IP.
   d) **Dirección IP**. Dirección IP 4 o IP6 asignada al servidor virtual.
   e) **Puerto**. Número de puerto del servidor virtual.
4. Elija **Aceptar** para continuar con la configuración de otros parámetros opcionales.
5. Haga clic en **Crear** y, a continuación, en **Cerrar**.

Para enlazar una directiva de categorización de URL al servidor virtual de equilibrio de carga HTTP

1. Acceda a la página **Administración de Tráfico** > **Equilibrio de Carga** > **Servidores Virtuales**.
2. En el panel de detalles, seleccione el servidor virtual de equilibrio de carga y haga clic en **Modificar**.
3. En la sección **Configuración avanzada**, haga clic en **Directivas**.
4. En la sección **Directivas**, haga clic en el icono **+** para acceder al control deslizante **Directivas**.
5. Defina los siguientes parámetros.
   a) **Seleccione Directiva**. Seleccione la directiva de categorización de URL en la lista desplegable.
   b) **Elija Tipo**. Seleccione el tipo de directiva como Solicitud.
6. Haga clic en **Continuar**.
7. Seleccione la directiva de categorización de URL de la lista y haga clic en **Cerrar**.

Para enlazar una directiva de categorización al servidor virtual de equilibrio de carga del puente SSL

1. Vaya a la pantalla **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**.
2. En el panel de detalles, seleccione el servidor virtual de equilibrio de carga del puente SSL y haga clic en **Modificar**.

3. En la sección **Configuración avanzada**, haga clic en **Directivas**.
4. En la sección **Directivas**, haga clic en el icono **+** para acceder al control deslizante **Directivas**.
5. En la sección **Directivas**, establezca los siguientes parámetros.
   a) **Seleccione Directiva**. Seleccione la directiva de detección de vídeo en la lista desplegable.
   b) **Elija Tipo**. Seleccione el tipo de directiva como Solicitud.
6. Haga clic en **Continuar**.
7. Seleccione la directiva de detección de vídeo de la lista y haga clic en **Cerrar**.

Para configurar el límite de memoria compartida

1. Inicie sesión en el dispositivo y vaya a **Optimización** > Almacenamiento en **caché integrado**.
2. En el panel de detalles, haga clic en **el vínculo Cambiar configuración de caché**.
3. En la página **Configuración global de caché**, establezca los siguientes parámetros.
   a) **Límite de uso de memoria (MB).**
   b) **Límite de uso de memoria activa**.
   c) **Vía Encabezado**.
   d) **Longitud máxima del cuerpo del poste que se almacenará en caché**
   e) **Acción global de resultados no definidos**
   f) **Habilitar la persistencia de objetos HA**
   g) **Verificar la persistencia de objetos almacenados en caché**
   h) **Prerecuperaciones**
4. Haga clic en **Aceptar** y **Cerrar**.

Para configurar los parámetros de categorización de URL

1. Inicie sesión en el dispositivo y vaya a **Seguridad**.
2. En el panel de detalles, haga clic en **el vínculo Cambiar configuración de filtrado de URL**.
3. En la página **Configuración de parámetros de filtrado de URL**, establezca los siguientes parámetros.
   a) Horas entre actualizaciones de base de datos. Horas de filtrado de URL entre las actualizaciones de la base de datos. Valor mínimo: 0 y Valor máximo: 720.
   b) Hora del día para actualizar la base de datos. URL Filtrado hora del día para actualizar la base de datos.
4. Haga clic en **Aceptar** y **Cerrar.**

Configuración de la mensajería del registro de auditoría

Cuando un dispositivo Citrix ADC recibe una dirección URL entrante, si la directiva de respuesta tiene una expresión de filtrado de URL, la función de registro de auditoría recopila información de cate-

gorización y la muestra como mensajes de registro en cualquier servidor de registro de auditoría de destino configurado. La información se registra.

- Dirección IP de origen (la dirección IP del cliente que realizó la solicitud).
- Dirección IP de destino (la dirección IP del servidor solicitado).
- URL solicitada que contiene el esquema, el host y el nombre de dominio (`http://www.example.com`).
- Categoría de URL que devuelve el marco de filtrado de URL.
- Grupo de categoría de URL devuelto por el marco de filtrado de URL.
- Número de reputación de URL devuelto por el marco de filtrado de URL.
- Acción de registro de auditoría realizada por la directiva de categorización de URL.

Para configurar el registro de auditoría para la función Lista de URL, debe completar las siguientes tareas:

1. Habilitar registros de auditoría.
2. Acción de mensaje Crear registro de auditoría.
3. Establecer la directiva de respuesta de lista de URL con la acción de mensaje Registro de auditoría.

Para obtener más información, consulte el tema Registro de auditoría .

Almacenamiento de errores mediante mensajería SYSLOG

En cualquier etapa del proceso de filtrado de URL, si se produce un error a nivel del sistema, el dispositivo Citrix ADC utiliza el mecanismo de registro de auditoría para almacenar registros en el archivo ns.log. Los errores se almacenan como mensajes de texto en formato SYSLOG para que un administrador pueda verlo más adelante en un orden cronológico de ocurrencia de eventos. Estos registros también se envían a un servidor SYSLOG externo para su archivado. Para obtener más información, consulte el artículo CTX229399.

Por ejemplo, si se produce un error al inicializar el SDK de filtrado de URL, el mensaje de error se almacena en el siguiente formato de mensajería.

3 de octubre 15:43:40 <local0.err> ns URLFiltering[1349]: Error al inicializar NetStar SDK (error del SDK = -1). (estado=1).

El dispositivo Citrix ADC almacena los mensajes de error en cuatro categorías de error diferentes:

- Error de descarga. Si se produce un error al intentar descargar la base de datos de categorización.
- Fallo de integración. Si se produce un error al integrar una actualización en la base de datos de categorización existente.
- Error de inicialización. Si se produce un error al inicializar la función de categorización de URL, establecer parámetros de categorización o finalizar un servicio de categorización.

- Error de recuperación. Si se produce un error cuando el dispositivo recupera los detalles de categorización de la solicitud.

Puntuación de reputación de URL

La función Categorización de URL proporciona un control basado en directivas para restringir las direcciones URL incluidas en la lista de prohibidos. Puede controlar el acceso a sitios web en función de la categoría de URL, la puntuación de reputación o la categoría de URL y la puntuación de reputación. Si un administrador de red supervisa a un usuario que accede a sitios web de alto riesgo, puede utilizar una directiva de respuesta vinculada a la puntuación de reputación de URL para bloquear dichos sitios web de riesgo.

Al recibir una solicitud de dirección URL entrante, el dispositivo recupera la puntuación de categoría y reputación de la base de datos de categorización de direcciones URL. En función de la puntuación de reputación devuelta por la base de datos, el dispositivo asigna una calificación de reputación a los sitios web. El valor puede variar de 1 a 4, donde 4 es el tipo de sitios web más arriesgado, como se muestra en la siguiente tabla.

Clasificación de reputación de URL	Comentario de reputación
1	Sitio limpio.
2	Sitio desconocido.
3	Potencialmente peligroso o afiliado a un sitio peligroso.
4	Sitio malicioso.

Preguntas frecuentes

August 20, 2021

En esta sección se proporcionan las preguntas frecuentes sobre las siguientes funciones de Citrix ADC

- Partición de administración
- AppFlow
- Call Home
- Agrupar en clústeres
- Administración de conexiones

- Conmutación de contenido
- Depuración
- Hardware
- Alta disponibilidad
- Almacenamiento en caché integrado
- Instalación, actualización y desactualización
- Equilibrio de carga
- GUI de NetScaler
- SSL

Partición de administración

August 20, 2021

¿Dónde puedo obtener el archivo de configuración de Citrix ADC para una partición?

El archivo de configuración (*ns.conf*) para la partición predeterminada está disponible en el directorio */nsconfig*. Para particiones admin, el archivo está disponible en el directorio */nsconfig/partitions/<partitionName>*.

¿Cómo puedo configurar el almacenamiento en caché integrado en un dispositivo Citrix ADC con particiones?

> **Nota**
>
> El almacenamiento en caché integrado en particiones de administración es compatible a partir de NetScaler 11.0.

Para configurar el almacenamiento en caché integrado (IC) en un dispositivo Citrix ADC particionado, después de definir la memoria IC en la partición predeterminada, el superusuario puede configurar la memoria IC en cada partición de administración de modo que la memoria IC total asignada a todas las particiones de administración no supere la memoria IC definida en la partición predeterminada. La memoria que no está configurada para las particiones admin permanece disponible para la partición predeterminada.

Por ejemplo, si un dispositivo Citrix ADC con dos particiones de administrador tiene 10 GB de memoria IC asignados a la partición predeterminada y la asignación de memoria IC para las dos particiones de administración es la siguiente:

- Partición1: 4 GB
- Partición2: 3 GB

Luego, la partición predeterminada tiene 10 - (4 + 3) = 3 GB de memoria IC disponible para su uso.

> **Nota**
>
> Si las particiones de administrador utilizan toda la memoria IC, no hay memoria IC disponible para la partición predeterminada.

¿Cuál es el alcance de los parámetros L2 y L3 en particiones administrativas?

> **Nota**
>
> - Aplicable a partir de NetScaler 11.0.
> - Para que ARP funcione en una partición no predeterminada, debe habilitar el parámetro "ProxYarp" en el comando "set l2param".

En un dispositivo Citrix ADC con particiones, el ámbito de actualización de los parámetros L2 y L3 es el siguiente:

- Para los parámetros L2 que se establecen mediante el comando "set L2Param", los siguientes parámetros solo se pueden actualizar desde la partición predeterminada, y sus valores son aplicables a todas las particiones admin:

  MaxBridgeCollision, BDGSetting, GarponvridinTF, Garpreply, ProxYarp, ResetInterfaceOnhaFailover y skip_proxying_bsd_traffic.

  Los otros parámetros L2 se pueden actualizar en particiones administrativas específicas, y sus valores son locales para esas particiones.

- Para los parámetros L3 que se establecen mediante el comando "set L3Param", todos los parámetros se pueden actualizar en particiones administrativas específicas, y sus valores son locales para esas particiones. Del mismo modo, los valores que se actualizan en la partición predeterminada se aplican solo a la partición predeterminada.

¿Cómo habilitar el redirección dinámica en una partición de administración?

> **Nota**
>
> El redirección dinámica en particiones de administración es compatible a partir de NetScaler 11.0.

Mientras que el redirección dinámica (OSPF, RIP, BGP, ISIS, BGP+) está habilitado de forma predeterminada en la partición predeterminada, en una partición admin, debe habilitarse mediante el siguiente comando:

```
> set L3Param -dynamicRouting ENABLED
```


> **Nota**
>
> Un máximo de 63 particiones pueden ejecutar redirección dinámica (62 particiones de administración y 1 partición predeterminada).

Al habilitar el redirección dinámica en una partición de administración, se crea un enrutador virtual (VR).

- Cada VR mantiene su propio vlan0 que se mostrará como vlan0_<partition-name>.
- Todas las direcciones IP independientes que están expuestas a ZEBO están enlazadas a vlan0.
- La VR predeterminada (de la partición predeterminada) muestra todos los VR configurados.
- La VR predeterminada muestra las VLAN enlazadas a estas VR (excepto las VLAN predeterminadas).

¿Dónde puedo encontrar los registros de una partición?

Los registros Citrix ADC no son específicos de partición. Las entradas de registro para todas las particiones deben almacenarse en el directorio */var/log/*.

¿Cómo puedo obtener registros de auditoría para una partición de administrador?

En un dispositivo Citrix ADC particionado, no puede tener servidores de registro específicos para una partición específica. Los servidores definidos en la partición predeterminada son aplicables en todas las particiones administrativas. Por lo tanto, para ver los registros de auditoría de una partición específica, debe utilizar el comando "show audit messages".

> **Nota**
>
> Los usuarios de una partición de administrador no tienen acceso al shell y, por lo tanto, no pueden acceder a los archivos de registro.

¿Cómo puedo obtener registros web para una partición de administración?

Puede obtener los registros web para una partición de administración de la siguiente manera:

- **Para NetScaler 11.0 y versiones posteriores**

  La función de registro web debe estar habilitada en cada una de las particiones que requieren registro web. Mediante el cliente Citrix ADC Web Logging (NSWL), Citrix ADC recupera los registros web de todas las particiones con las que está asociado el usuario.

- **Para versiones anteriores a NetScaler 11.0**

  Los registros web solo pueden ser obtenidos por `nsroot` y otros superusuarios. Además, aunque el registro web está habilitado en la partición predeterminada, el cliente Citrix ADC Web Logging (NSWL) obtiene registros web para todas las particiones.

Para ver la partición de cada entrada de registro, personalice el formato de registro para incluir la opción %P. A continuación, puede filtrar los registros para ver los registros de una partición específica.

¿Cómo puedo obtener el seguimiento de una partición de administración?

Puede obtener el seguimiento de una partición de administrador de la siguiente manera:

- **Para NetScaler 11.0 y versiones posteriores**

  En un dispositivo Citrix ADC con particiones, la `nstrace` operación se puede realizar en particiones de administrador individuales. Los archivos de seguimiento se almacenan en el directorio */var/partitions/<partitionName>/nstrace/*.

  Nota: No se puede obtener el seguimiento de una partición de administrador mediante el uso de la GUI. Debe usar la CLI.

- **Para versiones anteriores a NetScaler 11.0**

  La `nstrace` operación solo se puede realizar en la partición predeterminada. Por lo tanto, las capturas de paquetes están disponibles para todo el sistema Citrix ADC. Para obtener capturas de paquetes específicas de partición, utilice filtros basados en VLAN-ID.

¿Cómo puedo obtener el paquete de soporte técnico específico de una partición de administrador?

Para obtener el paquete de soporte técnico para una partición específica, debe ejecutar el siguiente comando desde la partición predeterminada:

```
> show techsupport -scope partition -partitionname <string>
```

Nota: Este comando también proporciona información específica del sistema.

AppFlow

August 20, 2021

- **¿Qué compilación de Citrix ADC admite AppFlow?**

  AppFlow es compatible con dispositivos Citrix ADC que ejecutan la versión 9.3 y superior con la compilación nCore.

- **¿Cuál es el formato utilizado por AppFlow para transmitir datos?**

  AppFlow transmite información en el formato de Internet Protocol Flow Information Export (IPFIX), que es un estándar abierto de Internet Engineering Task Force (IETF) definido en RFC 5101.

IPFIX (la versión estandarizada de NetFlow de Cisco) se utiliza ampliamente para supervisar la información de flujo de red.

- **¿Qué contienen los registros de AppFlow?**

  Los registros de AppFlow contienen información estándar de NetFlow o IPFIX, como marcas de tiempo para el inicio y el final de un flujo, recuento de paquetes y recuento de bytes. Los registros de AppFlow también contienen información de nivel de aplicación (como direcciones URL HTTP, métodos de solicitud HTTP y códigos de estado de respuesta, tiempo de respuesta del servidor y latencia). Los registros de flujo IPFIX se basan en plantillas que se deben enviar antes de enviar registros de flujo.

- **Después de una actualización a NetScaler Versión 9.3 Build 48.6 Cl, ¿por qué un intento de abrir un servidor virtual desde la GUI produce el mensaje de error "La función AppFlow solo está disponible en Citrix ADC Ncore"?**

  AppFlow solo se admite en dispositivos nCore. Cuando abra la ficha de configuración del servidor virtual, desactive la casilla de verificación **AppFlow** .

- **¿Qué contiene el ID de transacción en los registros de AppFlow?**

  Un Id. de transacción es un número de 32 bits sin firmar que identifica una transacción a nivel de aplicación. Para HTTP, una transacción corresponde a un par de solicitudes y respuestas. Todos los registros de flujo que corresponden a este par de solicitudes y respuestas tienen el mismo identificador de transacción. Una transacción típica tiene cuatro registros de flujo. Si Citrix ADC genera la respuesta por sí mismo (desde la caché integrada o mediante una directiva de seguridad), es posible que solo haya dos registros de flujo para la transacción.

- **¿Qué es una acción AppFlow?**

  Una acción de AppFlow es un conjunto de recopiladores a los que se envían los registros de flujo si coincide la directiva de AppFlow asociada.

- **¿Qué comandos puedo ejecutar en el dispositivo Citrix ADC para comprobar que la acción AppFlow es un éxito?**

  La acción show AppFlow. Por ejemplo:

```
> show appflow action
1) Name: aFL-act-collector-1
   Collectors: collector-1
   Hits: 0
   Action Reference Count: 2
  2) Name: apfl-act-collector-2-and-3
   Collectors: collector-2, collecter-3
   Hits: 0
```



```
    Action Reference Count: 1
  3) Name: apfl-act-collector-1-and-3
    Collectors: collector-1, collecter-3
    Hits: 0
    Action Reference Count: 1
<!--NeedCopy-->
```

- **¿Qué es un colector AppFlow?**

Un recopilador recibe registros de flujo generados por el dispositivo Citrix ADC. Para poder enviar registros de flujo, debe especificar al menos un recopilador. Puede especificar hasta cuatro. Puede eliminar los colectores no utilizados.

- **¿Qué versión de Citrix ADC se requiere para usar AppFlow?**

  Utilice NetScaler versión 9.3.49.5 o superior, y recuerde que AppFlow solo está disponible en las compilaciones de nCore.

- **¿Qué protocolo de transporte utiliza AppFlow?**

  AppFlow utiliza UDP como protocolo de transporte.

- **¿Qué puertos se deben abrir si tengo un firewall en la red?**

  Puerto 4739. Es el puerto UDP predeterminado que el colector AppFlow utiliza para escuchar mensajes IPFIX. Si el usuario cambia el puerto predeterminado, ese puerto debe abrirse en el firewall.

- **¿Cómo puedo cambiar el puerto predeterminado que AppFlow usa?**

  Cuando se agrega un recopilador AppFlow mediante el comando add appflowCollector, se puede especificar el puerto que se va a utilizar.

```
> add appflowCollector coll1 -IPAddress 10.102.29.251 -port 8000
 Done
<!--NeedCopy-->
```

- **¿Qué hace la configuración clientTrafficOnly?**

  Citrix ADC genera registros de AppFlow solo para el tráfico del lado del cliente.

- **¿Cuántos colectores se pueden configurar a la vez?**

  Puede configurar hasta cuatro recopiladores AppFlow a la vez en el dispositivo Citrix ADC. Tenga en cuenta que el número máximo de recopiladores que se pueden configurar en un dispositivo Citrix ADC es de cuatro.

Call Home

August 20, 2021

- **¿Qué es Call Home en un dispositivo Citrix ADC?**

  Call Home supervisa y notifica eventos críticos en un dispositivo Citrix ADC. Al habilitar Call Home, puede automatizar el proceso de notificación de errores. No solo evita llamar al soporte técnico de Citrix, plantear una solicitud de servicio y cargar datos del sistema antes de que el soporte técnico de Citrix pueda solucionar el problema, sino que también identifique y resuelva los problemas antes de que ocurra.

- **¿Call Home está habilitado de forma predeterminada en un dispositivo Citrix ADC?**

  Sí, Call Home está habilitado de forma predeterminada en el dispositivo. Si actualiza al software más reciente desde una versión anterior en la que Call Home estaba inhabilitado de forma predeterminada, el proceso de actualización activa automáticamente la función. Si posteriormente decide inhabilitarlo, la configuración actualizada se recordará para todas las actualizaciones posteriores. Para obtener información, consulte Call Home.

- **¿Cuáles son los requisitos previos para que Call Home funcione?**

  Acceso a una conexión a Internet.

  Nota: Si el dispositivo Citrix ADC no tiene conectividad a Internet, puede configurar un servidor proxy mediante el cual Citrix ADC puede generar registros del sistema y cargarlos en el servidor de soporte técnico de Citrix (CIS).

- **¿Cuáles son las ventajas de usar Call Home?**

  - Supervisar las condiciones de error de hardware y software.
  - Notificar la ocurrencia de eventos críticos que afectan a la red.
  - Envíe datos de rendimiento y registros del sistema a Citrix para:
    * Analizar y mejorar la calidad del producto.
    * Proporcione información de solución de problemas en tiempo real para la identificación proactiva de problemas y una resolución más rápida de problemas.

- **¿Qué versión del software Citrix ADC admite Call Home?**

  Citrix ADC versión 10.0 y posterior.

- **¿Qué modelos de plataforma Citrix ADC admiten Call Home?**

  La función Call Home está habilitada de forma predeterminada en todas las plataformas Citrix ADC y en todos los modelos de dispositivos (MPX, VPX y SDX).

  - Citrix ADC MPX: Todos los modelos MPX.

  - Citrix ADC VPX: Todos los modelos VPX. Además, es compatible con dispositivos VPX que obtienen sus licencias de grupos de licencias externos o centrales. Sin embargo, la función sigue siendo la misma que para un dispositivo VPX estándar.
  - Citrix ADC SDX: Supervisa la unidad de disco y los chips SSL asignados en busca de errores o fallas. Sin embargo, las instancias VPX no tienen acceso a la unidad de fuente de alimentación (PSU) y, por lo tanto, su estado no se supervisa. En una plataforma SDX, puede configurar Call Home directamente en una instancia individual o a través del SVM.

- **¿Debo configurar la alarma SNMP para Call Home para notificar las condiciones de error?**

  No, no es necesario configurar SNMP para Call Home para supervisar las condiciones de error, ya que las cargas SNMP y Call Home son independientes entre sí. Si quiere recibir una notificación cada vez que se produzca una condición de error, puede configurar la alarma CALLHOME-UPLAD-EVENT SNMP para generar una alerta SNMP siempre que se produzca una carga de Call Home. La alerta SNMP notifica al administrador local acerca de las ocurrencias de eventos críticos.

- **¿Cómo me pongo en contacto con asistencia técnica?**

  Para todos los eventos críticos relacionados con el hardware, Call Home crea automáticamente una solicitud de servicio a Citrix. En caso de otros errores, después de revisar los registros del sistema, puede ponerse en contacto con el equipo de soporte técnico de Citrix para abrir una solicitud de servicio para una investigación más detallada. Para obtener más información, consulte http://support.citrix.com/article/CTX200021.

- **¿Qué condiciones de error supervisa Call Home en un dispositivo Citrix ADC?**

  Call Home admite la supervisión de los siguientes eventos en un dispositivo Citrix ADC:

  - Errores de unidad flash compacta
  - Errores de la unidad de disco duro
  - Fallo de la unidad de alimentación
  - Error en la tarjeta SSL
  - Reinicio en caliente
  - Anomalías de memoria
  - Caídas límite de velocidad

- **¿Necesita una licencia separada para Call Home?**

  No, Call Home no requiere una licencia separada. Puede habilitarlo en todas las licencias de la plataforma Citrix ADC.

- **¿Qué datos envía Call Home al servidor de asistencia de Citrix y con qué frecuencia se envían?**

  Call Home recopila y envía dos tipos de datos al CIS. Se trata de:

  - Información básica del sistema (ejecución de la versión Citrix ADC, modo de implementación (independiente, HA, clúster), detalles de hardware, etc.). Se envía en el momento del registro de Call Home y como parte de latidos cardíacos periódicos. El latido se envía una vez cada 30 días, pero puede configurar este intervalo entre 1 y 30 días. Sin embargo, no se recomienda un valor de menos de 5 días, porque las cargas frecuentes generalmente no son muy útiles.
  - Versión abreviada de `show tech support bundle` cuando hay una condición de error. Se envía en la primera aparición de una condición de error particular desde la última vez que se inició el dispositivo. Es decir, la repetición de la misma condición de error no desencadena otra carga a menos que el dispositivo se haya reiniciado después de la ocurrencia anterior.

- **¿Puede Call Home generar y cargar registros del sistema a través de un servidor proxy?**

  Sí. Si el dispositivo Citrix ADC no tiene conectividad directa a Internet, puede configurar un servidor proxy y cargar los registros del sistema en el servidor de soporte técnico de Citrix (CIS).

- **¿Puedo revisar los datos de Call Home antes de enviarlos a CIS?**

  Lamentablemente, no puede revisar los datos de Call Home antes de enviarlos a CIS. Call Home no recopila ningún otro dato además de los datos que proporcionará cuando se ponga en contacto con el equipo de soporte de Citrix.

- **¿Qué tan seguras y privadas son las cargas de Call Home?**

  Call Home proporciona seguridad y privacidad de los datos de las siguientes maneras:

  - Utiliza un canal seguro SSL/TLS para transferir datos a servidores Citrix.
  - Los datos cargados son revisados únicamente por personal autorizado y no se comparten con terceros.

Agrupar en clústeres

August 20, 2021

Haga clic aquí para obtener preguntas frecuentes sobre agrupación en clústeres

Administración de conexiones

August 20, 2021

- **¿Qué es una conexión de administrador?**

Una conexión de administrador establece una conexión con la dirección NSIP y permite a los administradores configurar y supervisar el dispositivo Citrix ADC.

- **¿Cuáles son los tipos de conexiones de administración?**

  Hay dos tipos de conexiones de administración:

  - Conexión SSH: los usuarios administradores utilizan un cliente SSH para iniciar sesión a través de la dirección NSIP.
  - Conexión a la API de NITRO: los usuarios administradores utilizan las API de NITRO para automatizar el proceso de inicio de sesión en el dispositivo Citrix ADC.

> **Nota**
>
> Los usuarios administradores también pueden iniciar sesión a través de la GUI para iniciar sesión, mediante un explorador para conectarse a la dirección NSIP. La interfaz gráfica de usuario abre internamente una conexión API NITRO. Por lo tanto, una sesión de GUI equivale a una conexión API de NITRO y las preguntas frecuentes relacionadas con la API de NITRO se aplican a la GUI.

- **¿Cuántas conexiones de administración simultáneas se permiten en un dispositivo Citrix ADC?**

  El dispositivo permite hasta 20 conexiones de administración simultáneas.

- **¿Qué credenciales de inicio de sesión son necesarias para un inicio de sesión de administrador?**

  El inicio de sesión del administrador requiere un nombre de usuario y una contraseña.

  Nota: Se puede utilizar una clave de autenticación en lugar de una contraseña.

- **¿Qué métodos de autenticación externa admite un dispositivo Citrix ADC?**

  El dispositivo admite los siguientes métodos de autenticación externa:

  - RADIUS
  - LDAP
  - TACACS

- **¿Qué es un cliente?**

  Un cliente es un dispositivo (portátil o de escritorio) que utiliza el usuario administrador para abrir una conexión de administrador.

- **¿Qué es un token de sesión?**

  Un token de sesión es un identificador único que el dispositivo Citrix ADC emite a un cliente que envía una solicitud de inicio de sesión de la API NITRO.

  - Los clientes de API pueden reutilizar el token de sesión, si no ha expirado, para solicitudes de API posteriores en nuevas conexiones TCP

  - Los clientes de GUI abren internamente las conexiones API de NITRO y mantienen activo el token de sesión durante la sesión GUI.

- **¿Qué es una sesión activa en un dispositivo Citrix ADC?**

  Una sesión CLI se considera activa si la sesión no ha expirado y tiene una conexión SSH abierta con un dispositivo Citrix ADC.

  Una sesión de API NITRO se considera activa si el tiempo de espera del token de sesión no ha expirado en el dispositivo Citrix ADC.

- **¿Cómo aplica Citrix ADC el límite de conexión concurrente?**

  Cada vez que el dispositivo Citrix ADC recibe una solicitud de conexión de administrador (SSH o API NITRO), comprueba el número de conexiones de administración abiertas. Si el número es inferior a 20, se abre una nueva conexión.

- **¿Qué contador refleja el número de conexiones de administración en un dispositivo Citrix ADC?**

  El contador de conexiones (nsconfigd_cur_clients) refleja el número de conexiones activas. Este contador aumenta cuando un cliente abre una nueva conexión al dispositivo y disminuye cuando se cierra una conexión.

- **¿Qué contador refleja el número de tokens activos en el dispositivo Citrix ADC?**

  El contador *configd_cur_tokens* refleja el número de tokens activos en el dispositivo Citrix ADC.

- **¿Cómo gestiona el dispositivo Citrix ADC los errores en una conexión?**

  El dispositivo Citrix ADC cierra inmediatamente la conexión del cliente (CLI, API y GUI) si encuentra errores en una conexión.

- **¿Una sesión de CLI o GUI en una conexión a la dirección de administración cuenta en relación con el límite de conexión de administrador?**

  Sí, todas las conexiones CLI y GUI son conexiones basadas en TCP, y cada conexión TCP a la dirección de administración cuenta con respecto al límite de conexión de administrador.

- **¿Cuenta una sesión NITRO contra el límite de conexión del administrador?**

  Una sesión NITRO cuenta con el límite de conexión de administrador si hay una conexión TCP abierta que use el token de sesión emitido por el dispositivo Citrix ADC.

- **¿Cuál es el período de tiempo de espera predeterminado para las sesiones API, GUI y CLI en el dispositivo Citrix ADC?**

  En la tabla siguiente se muestra el período de tiempo de espera predeterminado para las sesiones de API, GUI y CLI en el dispositivo Citrix ADC:

Versiones de Citrix ADC	Período de tiempo de espera predeterminado de CLI (min)	Período de tiempo de espera predeterminado de la API (min)	Período de tiempo de espera predeterminado de la GUI (min)
NetScaler 9.3	Ninguno	30 Minutos	30 Minutos
NetScaler 10.1	Ninguno	30 Minutos	30 Minutos
NetScaler 10.5 en adelante	15 Minutos	30 Minutos	15 Minutos

- **¿Cómo se puede establecer el tiempo de espera de las sesiones CLI en un dispositivo Citrix ADC?**

  El tiempo de espera de sesión de CLI se puede configurar ejecutando el siguiente comando en el símbolo de la CLI:

  ```
  set cli mode -timeout \<xx seconds>
  ```

- **¿Cómo se anula el período de tiempo de espera predeterminado cuando se usa la API NITRO?**

  Puede anular el período de tiempo de espera predeterminado para una API NITRO estableciendo la duración del tiempo de espera en el campo “tiempo de espera” del objeto de inicio de sesión. Si el tiempo de espera de la sesión se establece en cero, el token de sesión tiene un tiempo de espera infinito.

  Nota: No se recomienda un tiempo de espera infinito, ya que las sesiones que no se agota el tiempo de espera continúan contando con el recuento de conexiones de administrador.

- **¿Qué sucede si se elimina una cuenta de usuario del dispositivo Citrix ADC después de crear una sesión de administración?**

  Para los usuarios internos del sistema, el dispositivo Citrix ADC cierra la sesión de la CLI o NITRO API existente.

  Para los usuarios externos del sistema, la sesión permanece activa hasta que caduca.

- **¿Pueden los clientes de la API NITRO utilizar un token de sesión único para abrir varias conexiones de administración en el dispositivo Citrix ADC?**

  Sí. Cada una de estas conexiones cuenta con el límite de conexión de administrador.

- **Si el acceso de administración está habilitado para una dirección de SNIP, ¿las conexiones de administrador a esa dirección cuentan con el límite para el número de conexiones de administrador?**

Sí, las conexiones de administrador a la dirección de administración (SNIP) cuentan con el límite de conexión de administrador en Citrix ADC.

- **¿Puede un administrador de Citrix ADC iniciar sesión en el dispositivo Citrix ADC una vez alcanzado el límite máximo de conexiones?**

  Sí. Se permite una conexión de administrador más después de alcanzar el límite máximo de conexión.

- **¿Pueden los puntos finales de la API NITRO abrir varias conexiones de administración en Citrix ADC el dispositivo?**

  Sí, los puntos finales de la API de NITRO pueden abrir varias conexiones de administración y agotar el límite de conexión de administración simultánea en un dispositivo Citrix ADC. En tales situaciones, se permite una conexión SSH/CLI adicional y el administrador puede forzar el cierre de sesiones de API antiguas o reducir el tiempo de espera de la sesión de las sesiones API existentes.

- **¿Puede el mismo cliente abrir varias sesiones de API en un dispositivo Citrix ADC?**

  Sí, un cliente puede abrir varias sesiones de API iniciando sesión repetidamente. Por ejemplo, el cliente podría volver a iniciar sesión después de reiniciar.
  Nota: Los inicios de sesión repetidos de clientes se comparan con el límite de conexión de administración en el dispositivo Citrix ADC.

- **¿Pueden los clientes API usar todo el límite de token de sesión de API?**

  Sí, los clientes API pueden usar todo el límite de token de sesión de API, proporcionado al iniciar sesión repetidamente sin usar un token emitido previamente.

  Nota: Si el tiempo de espera de sesión de un cliente es cero, el token es válido para siempre. Los inicios de sesión repetidos con nuevos tokens de sesión pueden contar para el límite de tokens de sesión de API.

- **¿Las sesiones CLI cuentan con el límite de token de sesión de API?**

  No, las sesiones CLI no se cuentan en el límite de token de sesión de API.

- **¿Pueden los usuarios de administración usar telnet para abrir una sesión CLI?**

  No. Solo un cliente SSH puede abrir una sesión CLI.

- **¿Cuál es el límite de conexión y el límite de sesión de API aplicables a varias versiones de Citrix ADC?**

  En la siguiente tabla se enumeran los límites máximos de conexión de administración simultánea y de sesión de API activa aplicables a varias versiones de Citrix ADC:

Versiones de Citrix ADC	9,3	10.1 (antes de 130.x)	10.1 (antes de 130.10)	10.1 (a partir de 130.10)
Número máximo de conexiones de administración simultáneas	20	20	20	20
Número máximo de sesiones de API activas*	1000	20	1000	1000

Nota:

- Las sesiones de API se consideran activas si no se ha agotado el tiempo de espera. Por ejemplo, si se crearon 500 sesiones de API pero 100 han caducado, 400 sesiones de API están activas.
- Una sesión de API no necesita abrir una conexión TCP al dispositivo Citrix ADC.

Conmutación de contenido

October 5, 2021

- **He instalado un dispositivo de equilibrio de carga que no es de Citrix ADC en la red. Sin embargo, me gustaría utilizar la función de cambio de contenido del dispositivo Citrix ADC para dirigir las solicitudes del cliente al dispositivo de equilibrio de carga. ¿Es posible utilizar la función de cambio de contenido del dispositivo Citrix ADC con un dispositivo de equilibrio de carga que no sea Citrix ADC?**

  Sí. Puede utilizar la función Cambio de contenido del dispositivo Citrix ADC con la función de equilibrio de carga del dispositivo Citrix ADC o de un dispositivo de equilibrio de carga que no sea Citrix ADC. Sin embargo, al utilizar el dispositivo de equilibrio de carga que no es de Citrix ADC, asegúrese de crear un servidor virtual de equilibrio de carga en el dispositivo Citrix ADC y vincularlo al dispositivo de equilibrio de carga que no es de Citrix ADC como servicio.

- **¿En qué se diferencia un servidor virtual de conmutación de contenido de un servidor virtual de equilibrio de carga?**

  Un servidor virtual de conmutación de contenido solo puede enviar solicitudes de cliente a otros servidores virtuales. No se comunica con los servidores.

Un servidor virtual de equilibrio de carga equilibra la carga del cliente entre los servidores y se comunica con los servidores. Supervisa la disponibilidad del servidor y se puede utilizar para aplicar diferentes algoritmos de equilibrio de carga para distribuir la carga de tráfico.

La conmutación de contenido es un método que se utiliza para dirigir las solicitudes de los clientes de tipos específicos de contenido a los servidores de destino mediante el equilibrio de carga de los servidores virtuales. Puede dirigir las solicitudes de los clientes a los servidores más adecuados para gestionarlas. Esto reduce los gastos generales para procesar las solicitudes de los clientes en los servidores.

- **Deseo implementar la función de cambio de contenido del dispositivo Citrix ADC para dirigir las solicitudes de los clientes. ¿Qué tipos de solicitudes de clientes puedo dirigir mediante la función Content switching?**

  Solo puede dirigir solicitudes de cliente HTTP, HTTPS, FTP, TCP, Secure TCP y RTSP mediante la función de conmutación de contenido. Para dirigir las solicitudes de clientes HTTPS, debe configurar la función de descarga SSL en el dispositivo.

- **Quiero crear reglas de conmutación de contenido en el dispositivo Citrix ADC. ¿Cuáles son los distintos elementos de la solicitud del cliente en los que puedo crear una regla de cambio de contenido?**

  Puede crear reglas de cambio de contenido en función de los siguientes elementos y sus valores en la solicitud del cliente:

  - URL
  - Tokens URL
  - versión HTTP
  - Encabezados HTTP
  - Dirección IP de origen del cliente
  - Versión cliente
  - Puerto TCP de destino

- **Entiendo que la función de cambio de contenido del dispositivo Citrix ADC ayuda a mejorar el rendimiento de la red. ¿Es correcto?**

  Sí. Puede dirigir las solicitudes del cliente a los servidores más adecuados para gestionarlas. El resultado es una reducción de la sobrecarga para procesar las solicitudes de los clientes en los servidores.

- **¿Qué función del dispositivo Citrix ADC debo configurar en el dispositivo Citrix ADC para mejorar la capacidad de administración del sitio y el tiempo de respuesta a las solicitudes del cliente?**

  Puede configurar la función de cambio de contenido del dispositivo Citrix ADC para mejorar la capacidad de administración del sitio y el tiempo de respuesta a la solicitud del cliente. Esta

función permite crear grupos de contenido dentro del mismo nombre de dominio y dirección IP. Este enfoque es flexible, a diferencia del enfoque común de dividir explícitamente el contenido en diferentes nombres de dominio y direcciones IP, que son visibles para el usuario.

Varias particiones que dividen un sitio web en varios nombres de dominio y direcciones IP obligan al explorador a crear una conexión independiente para cada dominio que encuentre al procesar y recuperar el contenido de una página web. Estas conexiones WAN adicionales degradan el tiempo de respuesta de la página web.

- **He alojado un sitio web en una comunidad de servidores web. ¿Qué ventajas ofrece la función de cambio de contenido de Citrix ADC para este tipo de configuración?**

  La función de cambio de contenido proporciona las siguientes ventajas en un dispositivo Citrix ADC de un sitio basado en una comunidad de servidores web:

  - Administre el contenido del sitio mediante la creación de un grupo de contenido dentro del mismo dominio y dirección IP.
  - Mejore el tiempo de respuesta a las solicitudes de los clientes mediante el grupo de contenido dentro del mismo dominio y dirección IP.
  - Evite la necesidad de replicar el contenido completo en todos los dominios.
  - Habilite la partición de contenido específica de la aplicación. Por ejemplo, puede dirigir las solicitudes de los clientes a un servidor que solo gestiona contenido dinámico o solo contenido estático, según corresponda para la solicitud.
  - Admite el alojamiento múltiple de varios dominios en el mismo servidor y usa la misma dirección IP.
  - Reutilice las conexiones a los servidores.

- **Deseo implementar la función de cambio de contenido en el dispositivo Citrix ADC. Quiero dirigir las solicitudes de los clientes a los distintos servidores después de evaluar los distintos parámetros de cada solicitud. ¿Qué enfoque debo seguir para implementar esta configuración al configurar la función de cambio de contenido?**

  Puede utilizar expresiones de directiva para crear directivas para la función de cambio de contenido. Una expresión es una condición que se evalúa comparando los calificadores de la solicitud del cliente con un operando mediante un operador. Puede utilizar los siguientes parámetros de la solicitud del cliente para crear una expresión:

  - **Method**: Método de solicitud HTTP.
  - **URL**: URL en el encabezado HTTP.
  - **URL TOKENS**: Tokens especiales en la URL.
  - **VERSION**: Versión de solicitud HTTP.
  - **URL QUERY**: Contiene el encabezado URL Query LEN, URL LEN y HTTP.
  - **SOURCEIP**: Dirección IP del cliente.

  A continuación se muestra una lista completa de los operadores que se pueden utilizar para

crear una expresión:

- == (igual a)
- ! = (no es igual)
- EXISTS
- NOT EXISTS
- CONTAINS
- NOT CONTAINS
- GT (mayor que)
- LT (menor que)

También puede crear varias reglas, que son agregaciones lógicas de un conjunto de expresiones. Puede combinar varias expresiones para crear reglas. Para combinar expresiones, puede usar los operadores && (AND) y	(OR). También puede usar paréntesis para crear reglas anidadas y complejas.

- **Quiero configurar una directiva basada en reglas junto con una directiva basada en URL para el mismo servidor virtual de conmutación de contenido. ¿Es posible crear ambos tipos de directivas para el mismo servidor virtual de conmutación de contenido?**

  Sí. Puede crear ambos tipos de directivas para el mismo servidor virtual de conmutación de contenido. Sin embargo, asegúrese de asignar prioridades para establecer una prioridad adecuada para las directivas.

- **Quiero crear directivas de cambio de contenido que evalúen el nombre de dominio, junto con un prefijo y un sufijo de una URL, y dirijan las solicitudes del cliente en consecuencia. ¿Qué tipo de directiva de cambio de contenido debo crear?**

  Puede crear una directiva de dominio y URL exacta. Cuando se evalúa este tipo de directiva, el dispositivo Citrix ADC selecciona un grupo de contenido si el nombre de dominio completo y la URL de la solicitud del cliente coinciden con los configurados. La solicitud del cliente debe coincidir con el nombre de dominio configurado y coincidir exactamente con el prefijo y el sufijo de la URL si están configurados.

- **Quiero crear directivas de cambio de contenido que evalúen el nombre de dominio, junto con un prefijo parcial y un sufijo de URL, y dirijan las solicitudes del cliente en consecuencia. ¿Qué tipo de directiva de cambio de contenido debo crear?**

  Puede crear una directiva URL de dominio y comodín para el servidor virtual de conmutación

de contenido. Cuando se evalúa este tipo de directiva, el dispositivo Citrix ADC selecciona un grupo de contenido si la solicitud coincide con el nombre de dominio completo y coincide parcialmente con el prefijo de URL.

- **¿Qué es una directiva de URL comodín?**

  Puede utilizar caracteres comodín para evaluar URL parciales en las solicitudes de cliente a la URL que ha configurado en el dispositivo Citrix ADC. Puede utilizar comodines en los siguientes tipos de directivas basadas en URL:

  - Solo prefijo. Por ejemplo, la expresión /sports/* coincide con todas las URL disponibles en la URL /sports. Del mismo modo, la expresión /sports * coincide con todas las URL cuyo prefijo es /sports.
  - Solo sufijo. Por ejemplo, la expresión /*.jsp coincide con todas las URL con una extensión de nombre de archivo jsp.
  - Prefijo y sufijo. Por ejemplo, la expresión /sports/ *.jsp coincide con todas las URL de /sports/ que también tienen la extensión de nombre de archivo jsp. Del mismo modo, la expresión /sports *.jsp coincide con todas las URL con un prefijo /sports * y una extensión de nombre de archivo jsp.

- **¿Qué es una directiva de dominio y regla?**

  Al crear una directiva de dominio y reglas, la solicitud del cliente debe coincidir con el dominio completo y con la regla configurada en el dispositivo Citrix ADC.

- **¿Cuál es la prioridad predeterminada establecida para evaluar las directivas?**

  De forma predeterminada, las directivas basadas en reglas se evalúan en primer lugar.

- **Si parte del contenido es el mismo para todas las solicitudes de clientes, ¿qué tipo de prioridad debería usar para evaluar directivas?**

  Si parte del contenido es el mismo para todos los usuarios y se debe publicar contenido diferente sobre la base de los atributos del cliente, puede utilizar la prioridad basada en URL para la evaluación de directivas.

- **¿Qué sintaxis de expresiones de directiva se admiten en el cambio de contenido?**

  El cambio de contenido admite dos tipos de expresiones de directiva:

  - **Sintaxis clásica:** la sintaxis clásica en el cambio de contenido comienza con la palabra clave REQ y es más avanzada que la directiva Avanzada. Las directivas clásicas no pueden estar vinculadas a una acción. Por lo tanto, el servidor virtual de equilibrio de carga de destino solo se puede agregar después de vincular el servidor virtual de conmutación de contenido.
  - **Directiva avanzada:** La directiva avanzada suele comenzar con la palabra clave HTTP y es más fácil de configurar. Una acción de servidor virtual de equilibrio de carga de destino se

puede enlazar a una directiva avanzada y la directiva se puede utilizar en varios servidores virtuales de conmutación de contenido.

- **¿Puedo vincular una única directiva de conmutación de contenido a varios servidores virtuales?**

  Sí. Puede enlazar una única directiva de conmutación de contenido a varios servidores virtuales mediante directivas con acciones definidas. Las directivas de conmutación de contenido que utilizan una acción se pueden enlazar a varios servidores virtuales de conmutación de contenido porque el servidor virtual de equilibrio de carga de destino ya no se especifica en la directiva de conmutación de contenido. La capacidad de vincular una sola directiva a varios servidores virtuales de conmutación de contenido ayuda a reducir aún más el tamaño de la configuración de conmutación de contenido.

  Para obtener más información, consulte los siguientes artículos de Knowledge Center y los temas de documentación de Citrix:

  - Consulte CTX122918: Cómo vincular la misma directiva de conmutación de contenido a dos servidores virtuales Content Switching en un dispositivo Citrix ADC.
  - Consulte CTX122736: Cómo vincular la misma directiva avanzada a varios servidores virtuales de conmutación de contenido mediante etiquetas de directiva.
  - Configuración de la conmutación de contenido básica.

- **¿Puedo crear una directiva basada en acciones mediante expresiones clásicas?**

  No. A partir de ahora, Citrix ADC no admite directivas que utilicen expresiones de sintaxis clásicas con acciones. El servidor virtual de equilibrio de carga de destino debe agregarse al vincular la directiva en lugar de definirla en una acción.

Depuración

January 12, 2021

- **¿Cómo puedo determinar la interfaz (CLI, GUI o API) a través de la cual se realizó una operación?**

  Citrix ADC realiza un seguimiento de las interfaces a través de las cuales se realizan las operaciones. Puede ver esta información en syslogs (en la GUI, vaya a
  Configuración > Sistema > Auditoría > Mensajes de auditoría > Mensajes de syslog) o en el archivo ns.log (ubicado en el directorio /var/log/).

  Por ejemplo, las operaciones que se realizan a través de la API se marcan como “API CMD_EXECUTED.”

Hardware

August 20, 2021

Haga clic aquí para ver las preguntas frecuentes sobre el hardware MPX.

Alta disponibilidad

August 20, 2021

- **¿Cuáles son los diversos puertos utilizados para intercambiar información relacionada con HA entre los nodos en una configuración de HA?**

  En una configuración de alta disponibilidad, ambos nodos utilizan los siguientes puertos para intercambiar información HareLated:

  - Puerto UDP 3003, para intercambiar paquetes de latidos
  - Puerto 3010, para sincronización y propagación de comandos

- **¿Qué configuraciones no se sincronizan o propagan en una configuración de alta disponibilidad en modo INC o no INC?**

  Las configuraciones implementadas con los siguientes comandos no se propagan ni sincronizan con el nodo secundario:

  - Todos los comandos de configuración de HA específicos del nodo. Por ejemplo `add ha node`, `set ha node`, y `bind ha node`.
  - Todos los comandos de configuración relacionados con la interfaz. Por ejemplo, set interface y unset interface.
  - Todos los comandos de configuración relacionados con el canal. Por ejemplo, agregue canal, establezca canal y enlace canal.

  Para obtener más información sobre la configuración de alta disponibilidad en modo INC, consulte Configuración de nodos de alta disponibilidad en diferentes subredes.

- **¿Qué configuraciones no se sincronizan o propagan en una configuración de alta disponibilidad en modo INC?**

  Las siguientes configuraciones no se sincronizan ni propagan. Cada nodo tiene su propio.

  - MIP
  - SNIP
  - VLAN
  - Rutas (excepto rutas LLB)

- Monitores de ruta
- Reglas RNAT (excepto cualquier regla RNAT con VIP como IP NAT)
- Configuraciones de redirección dinámica.

- **¿Cuáles son las condiciones que desencadenan la sincronización?**

  La sincronización se activa por cualquiera de las siguientes condiciones:

  - El número de encarnación del nodo primario, recibido por el secundario, no coincide con el del nodo secundario.
    Nota: Ambos nodos en una configuración de HA mantienen un contador llamado *número de encarnación*, que cuenta el número de configuraciones en el archivo de configuración del nodo. Cada nodo envía su número de encarnación entre sí nodo en los mensajes de latido. El número de encarnación no se incrementa para los siguientes comandos:
    * Todos los comandos relacionados con la configuración de HA. Por ejemplo `add ha node`, `set ha node`, y `bind ha node`.
    * Todos los comandos relacionados con la interfaz. Por ejemplo, set interface y unset interface.
    * Todos los comandos relacionados con el canal. Por ejemplo, agregue canal, establezca canal y enlace canal.
  - El nodo secundario aparece después de reiniciar.
  - El nodo principal se convierte en secundario después de una conmutación por error.

- **¿Se sincroniza una configuración agregada al nodo secundario en el primario?**

  No, una configuración agregada al nodo secundario no se sincroniza con el primario.

- **¿Cuál podría ser la razón por la que ambos nodos afirman ser el principal en una configuración de alta disponibilidad?**

  La razón más probable es que los nodos primario y secundario están en buen estado, pero el secundario no recibe los paquetes de latido del primario. El problema puede estar en la red entre los nodos.

- **¿Una configuración de alta disponibilidad tiene algún problema si implementa los dos nodos con diferentes configuraciones de reloj del sistema?**

  Diferentes configuraciones de reloj del sistema en los dos nodos pueden causar los siguientes problemas:

  - Las marcas de tiempo de las entradas del archivo de registro no coinciden. Esta situación hace que sea difícil analizar las entradas de registro para cualquier problema.
  - Después de una conmutación por error, es posible que tenga problemas con cualquier tipo de persistencia basada en cookies para el equilibrio de carga. Una diferencia significativa entre los tiempos puede hacer que una cookie caduque antes de lo esperado, lo que resulta en la terminación de la sesión de persistencia.

  - Consideraciones similares se aplican a cualquier decisión relacionada con el tiempo en los nodos.

- **¿ Cuáles son las condiciones para el fallo del comando *force HA sync* ?**

  La sincronización forzada falla en cualquiera de las siguientes circunstancias:

  - Fuerza la sincronización cuando la sincronización ya está en curso.
  - El nodo secundario está inhabilitado.
  - La sincronización de HA está inhabilitada en el nodo secundario actual.
  - La propagación de HA está inhabilitada en el nodo principal actual y se fuerza la sincronización desde el primario.

- **¿ Cuáles son las condiciones para la falla del comando *sync HA files* ?**

  La sincronización de archivos de configuración falla si el nodo secundario está inhabilitado.

- **En una configuración de alta disponibilidad, si el nodo secundario toma el control como primario, ¿cambia de nuevo al estado secundario si el primario original vuelve a conectarse?**

  No. Después de que el nodo secundario toma el control como principal, permanece como primario incluso si el nodo primario original vuelve a conectarse de nuevo. Para intercambiar el estado primario y secundario de los nodos, ejecute el comando *force failover*.

- **¿ Cuáles son las condiciones para el fallo del comando *force failover* ?**

  Una conmutación por error forzada falla en cualquiera de las siguientes circunstancias:

  - El nodo secundario está inhabilitado.
  - El nodo secundario está configurado para permanecer secundario.
  - El nodo principal está configurado para que siga siendo primario.
  - El estado del nodo del mismo nivel es desconocido.

Almacenamiento en caché integrado

August 20, 2021

Grupos de contenido

- **¿En qué se diferencia un grupo de contenido DEFAULT de otros grupos de contenido?**

  El comportamiento del grupo de contenido DEFAULT es el mismo que cualquier otro grupo. El único atributo que hace que el grupo de contenido DEFAULT sea especial es que si un objeto se está almacenando en caché y no se ha creado ningún grupo de contenido. El objeto se almacena en caché en el grupo DEFAULT.

- **¿Cuál es la opción 'Cache-Control' del nivel de grupo de contenido?**

  Puede enviar cualquier encabezado de control de caché al explorador. Hay una opción de nivel de grupo de contenido, -CacheControl, que le permite especificar el encabezado de control de caché que quiere insertar en la respuesta al explorador.

- **¿Cuál es la opción 'Minhit' en el nivel de grupo de contenido?**

  `Minhit` es un valor entero que especifica el número mínimo de selección de una directiva de caché antes de que el objeto se almacene en caché. Este valor se puede configurar en el nivel de grupo de contenido. A continuación se muestra la sintaxis para configurar este valor desde la CLI.

  ```
  add/set cache contentGroup \<Content_Group_Name> [-minHits \<Integer>]
  ```

- **¿Cuál es el uso de la opción ExpireAtlastByte?**

  La opción ExpireAtLastByte permite que la caché integrada caduque el objeto cuando se descarga. Solo las solicitudes que son solicitudes pendientes se sirven desde la caché. Las solicitudes nuevas se envían al servidor. Esta configuración es útil cuando el objeto se modifica con frecuencia, como en el caso de las cotizaciones de valores. Este mecanismo de caducidad funciona junto con la función Flash Cache. Para configurar una opción ExpireatLastByte, ejecute el siguiente comando desde la CLI:

  ```
  add cache contentGroup \<Group_Name> -expireAtLastByte YES
  ```

Directiva de caché

- **¿Qué es una directiva de almacenamiento en caché?**

  Las directivas determinan qué transacciones se pueden almacenar en caché y cuáles no. Además, las directivas agregan o anulan el comportamiento estándar de almacenamiento en caché HTTP. Las directivas determinan una acción, como CACHE o NOCACHE, según las funciones específicas de la solicitud o respuesta. Si una respuesta coincide con las reglas de directiva, el objeto de la respuesta se agrega al grupo de contenido configurado en la directiva. Si no ha configurado un grupo de contenido, el objeto se agrega al grupo de contenido DEFAULT.

- **¿Qué es una directiva acción?**

  Una selección se produce cuando una solicitud o respuesta coincide con una directiva de caché.

- **¿Qué es un error?**

  Se produce un error cuando una solicitud o respuesta no coincide con ninguna directiva de caché. También puede producirse una falla si la solicitud o respuesta coincide con una directiva de caché, pero alguna anulación del comportamiento de RFC impide que el objeto se almacene en la caché.

- **He configurado la función de almacenamiento en caché integrado del dispositivo Citrix ADC. Al agregar la directiva siguiente, aparece un mensaje de error. ¿Hay algún error en el comando?**

  ```
  add cache policy image_caching -rule exp1 | ns_ext_not_jpeg -action
  cache
  ```

  ```
  \> ERROR: No such command
  ```

  En el comando anterior, la expresión debe estar entre comillas. Sin comillas, se considera que el operador es el operador de proceso.

Requisitos de memoria

- **¿Cuáles son los comandos que puedo ejecutar en el dispositivo Citrix ADC para comprobar la memoria asignada a la caché?**

  Para mostrar la memoria asignada para la caché en el dispositivo Citrix ADC, ejecute cualquiera de los siguientes comandos desde la CLI:

  - `show cache parameter`

    En la salida, compruebe el valor del parámetro de límite de uso de memoria. Esta es la memoria máxima asignada para la caché.

  - `show cache \<Content_Group_Name>`

    En la salida, compruebe los valores de los parámetros Uso de memoria y Límite de uso de memoria que indican la memoria utilizada y asignada para el grupo de contenido individual.

- **Mi dispositivo Citrix ADC tiene 2 GB de memoria. ¿Hay algún límite de memoria recomendado para la caché?**

  Para cualquier modelo del dispositivo Citrix ADC, puede asignar la mitad de la memoria a la caché. Sin embargo, Citrix recomienda asignar un poco menos de la mitad de la memoria, debido a la dependencia interna de la memoria. Puede ejecutar el siguiente comando para asignar 1 GB de memoria a la caché:

  ```
  set cache parameter -memLimit 1024
  ```

- **¿Es posible asignar memoria para grupos de contenido individuales?**

  Sí. Aunque asigne memoria para la caché integrada globalmente ejecutando el parámetro set cache —memlimit <Integer>, puede asignar memoria a grupos de contenido individuales ejecutando el <Content_Group_Name> <Integer> comando set cache —memLimit. La memoria máxima que puede asignar a grupos de contenido (combinada) no puede exceder la memoria asignada a la caché integrada.

- **¿Cuál es la dependencia de la memoria entre la caché integrada y el búfer TCP?**

  Si el dispositivo Citrix ADC tiene 2 GB de memoria, el dispositivo reserva entre 800 MB y 900 MB de memoria y el resto se asigna al sistema operativo FreeBSD. Por lo tanto, puede asignar hasta 512 MB de memoria a la caché integrada y el resto se asigna al búfer TCP.

- **¿Afecta al proceso de almacenamiento en caché si no asigno memoria global a la caché integrada?**

  Si no asigna memoria a la caché integrada, todas las solicitudes se envían al servidor. Para asegurarse de que ha asignado memoria a la caché integrada, ejecute el comando show cache parameter. En realidad, ningún objeto se almacena en caché si la memoria global es 0, por lo que debe establecerse primero.

Comandos de verificación

- **¿Cuáles son las opciones para mostrar estadísticas de caché?**

  Puede utilizar cualquiera de las siguientes opciones para mostrar las estadísticas de la caché:

  - `stat cache`

    Para mostrar el resumen de las estadísticas de caché.

  - `stat cache -detail`

    Para mostrar todos los detalles de las estadísticas de caché.

- **¿Cuáles son las opciones para mostrar el contenido almacenado en caché?**

  Para mostrar el contenido almacenado en caché, puede ejecutar el comando `show cache object`.

- **¿Cuál es el comando que puedo ejecutar para mostrar las funciones de un objeto almacenado en caché?**

  Si el objeto almacenado en la caché es, por ejemplo, GET //10.102.12.16:80/index.html, puede mostrar los detalles sobre el objeto ejecutando el siguiente comando desde la CLI del dispositivo:

  ```
  show cache object -url '/index.html'-host 10.102.3.96 -port 80
  ```

- **¿Es obligatorio especificar el nombre del grupo como parámetro para mostrar los objetos parametrizados en la memoria caché?**

  Sí. Es obligatorio especificar el nombre del grupo como parámetro para mostrar los objetos parametrizados en la caché. Por ejemplo, considere que ha agregado las siguientes directivas con la misma regla:


```
add cache policy p2 -rule ns_url_path_cgibin -action CACHE -
    storeInGroup g1
add cache policy p1 -rule ns_url_path_cgibin -action CACHE -
    storeInGroup g2
<!--NeedCopy-->
```

En este caso, para las múltiples solicitudes, si se evalúa la directiva p1, su contador de selección se incrementa y la directiva almacena el objeto en el grupo g1, que tiene parámetros de selección. Por lo tanto, debe ejecutar el siguiente comando para mostrar los objetos de la caché:

```
show cache object -url "/cgi-bin/setCookie.pl"-host 10.102.18.152
groupName g1
```

Del mismo modo, para otro conjunto de solicitudes múltiples, si se evalúa la directiva p2, su contador de selección se incrementa y la directiva almacena el objeto en el grupo g2, que no tiene parámetros de selección. Por lo tanto, debe ejecutar el siguiente comando para mostrar los objetos de la caché:

```
show cache object -url "/cgi-bin/setCookie2.pl"-host 10.102.18.152
```

- **Hay algunas entradas en blanco en la salida del comando nscachemgr. ¿Cuáles son esas entradas?**

  Considere el siguiente ejemplo de salida del `nscachemgr` comando. Las entradas en blanco de esta salida se resaltan en negrita para su referencia:

```
root@ns# /netscaler/nscachemgr -a
//10.102.3.89:80/image8.png
//10.102.3.97:80/staticdynamic.html
//10.102.3.97:80/
//10.102.3.89:80/image1.png
//10.102.3.89:80/file5.html
//10.102.3.96:80/
//10.102.3.97:80/bg_logo_segue.png
//10.102.3.89:80/file500.html
//10.102.3.92:80/
//10.102.3.96:80/cgi-bin/rfc/ccProxyReval.pl
Total URLs in IC = 10
<!--NeedCopy-->
```

  Las entradas en blanco en la salida se deben a las propiedades de almacenamiento en caché predeterminadas para GET/HTTP/1.1.

Lavado de objetos

- **¿Cómo puedo vaciar un objeto selectivo de la caché?**

  Puede identificar un objeto de forma única por su dirección URL completa. Para vaciar un objeto de este tipo, puede realizar cualquiera de las siguientes tareas:

  - Caché de vaciado
  - Grupo de contenido de vaciado
  - Vacar el objeto específico

  Para vaciar el objeto específico, debe especificar los parámetros de consulta. Especifique el parámetro InvalParam para vaciar el objeto. Este parámetro solo se aplica a una consulta.

- **¿Algún cambio en la configuración de la caché activa el vaciado de la caché?**

  Sí. Al cambiar a la configuración de caché, todos los comandos de caché SET vacian de forma inherente los grupos de contenido adecuados.

- **He actualizado los objetos en el servidor. ¿Necesito vaciar los objetos almacenados en caché?**

  Sí. Al actualizar objetos en el servidor, debe vaciar los objetos almacenados en caché, o al menos los objetos y grupos de contenido relevantes. La memoria caché integrada no se ve afectada por una actualización del servidor. Continúa sirviendo los objetos almacenados en caché hasta que caduquen.

Caché Flash

- **¿Qué es la función Flash Cache del dispositivo Citrix ADC?**

  El fenómeno de las multitudes de Flash ocurre cuando muchos clientes acceden al mismo contenido. El resultado es un aumento repentino del tráfico hacia el servidor. La función Flash Cache permite que el dispositivo Citrix ADC mejore el rendimiento en tal situación mediante el envío de una sola solicitud al servidor. Todas las demás solicitudes se ponen en cola en el dispositivo y la respuesta única se sirve a las solicitudes. Puede utilizar cualquiera de los siguientes comandos para habilitar la función Caché rápida:

  - `add cache contentGroup \<Group_Name> -flashCache YES`
  - `set cache contentGroup \<Group_Name> -flashCache YES`

- **¿Cuál es el límite para los clientes de Flash Cache?**

  El número de clientes de Flash Cache depende de la disponibilidad de recursos en el dispositivo Citrix ADC.

Comportamiento predeterminado

- **¿El dispositivo Citrix ADC recibe objetos de forma proactiva al caducar?**

  El dispositivo Citrix ADC nunca recibe objetos de forma proactiva al caducar. Esto es cierto incluso para los objetos negativos. El primer acceso después de la expiración desencadena una solicitud al servidor.

- **¿La caché integrada agrega clientes a la cola para servir incluso antes de que comience a recibir la respuesta?**

  Sí. La caché integrada agrega clientes a la cola para servir incluso antes de que comience a recibir la respuesta.

- **¿Cuál es el valor predeterminado para Verify cached object using parameter of the cache configuration?**

  HOSTNAME_AND_IP es el valor predeterminado.

- **¿El dispositivo Citrix ADC crea entradas de registro en los archivos de registro?**

  Sí. El dispositivo Citrix ADC crea entradas de registro en los archivos de registro.

- **¿Los objetos comprimidos se almacenan en la caché?**

  Sí. Los objetos comprimidos se almacenan en la caché.

Interoperabilidad con otras funciones

- **¿Qué sucede con los objetos almacenados actualmente en caché y a los que se accede a través de SSL VPN?**

  Los objetos almacenados en la caché y a los que se accede regularmente se sirven como caché, selecciónelo cuando se accede a través de SSL VPN.

- **¿Qué sucede con los objetos almacenados en la caché cuando se accede a través de SSL VPN y posteriormente se accede a través de una conexión regular?**

  Los objetos almacenados a través del acceso SSL VPN se sirven como selección cuando se accede a través de la conexión normal.

- **Cuando uso el registro web, ¿cómo diferencio las entradas que indican la respuesta servida de la caché de las servidas por el servidor?**

  Para las respuestas servidas desde la caché integrada, el campo de registro del servidor contiene el valor IC. Para las respuestas servidas desde un servidor, el campo de registro del servidor contiene el valor enviado por el servidor. A continuación se muestra una entrada de registro de ejemplo para una transacción de almacenamiento en caché integrada:


```
”10.102.1.52 - ”Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 4.0; .NET
 CLR 1.0.3705)””GET /”200 0 ”IC”10.102.1.45”
```

Junto con una solicitud de cliente, la respuesta registrada es la enviada al cliente y no necesariamente la enviada por el servidor.

> **Nota**
>
> Cuando se utiliza el registro web, las respuestas de la caché integrada contienen el IC de valor en el campo de registro del servidor. El campo de registro del servidor está presente en el cliente NSWL con el especificador de formato “%o1”.

Otros

- **¿Qué significa configurar relexpiry y absexpiry?**

  Al configurar `relexpiry` y `absexpiry`, significa que va a anular el encabezado independientemente de lo que aparezca en el encabezado. Puede configurar una configuración de caducidad diferente y el nivel de grupo de contenido. Con `relexpiry`, la caducidad del encabezado se basa en el momento en que Citrix ADC recibe el objeto. Con `absexpiry`, la caducidad se basa en el tiempo configurado en Citrix ADC. `Relexpiry` se configura en segundos. `Absexpiry` es una hora del día.

- **¿Qué significa configurar weakpos y heuristic?**

  La heurística `weakpos` y la heurística son como valores de reserva. Si hay un encabezado de caducidad, solo se considera si el encabezado modificado por última vez está presente. El dispositivo Citrix ADC establece la caducidad en función de la última cabecera modificada y el parámetro heurístico. El cálculo de caducidad heurístico determina el tiempo de caducidad mediante la comprobación del encabezado modificado por última vez. Un porcentaje de la duración desde la última modificación del objeto se utiliza como tiempo de caducidad. La heurística de un objeto que permanece sin modificar durante períodos de tiempo más largos y es probable que tenga períodos de caducidad más largos. —heurExpiryParam especifica el valor porcentual que se va a utilizar en este cálculo. De lo contrario, el dispositivo utiliza el `weakpos` valor.

- **¿Qué debo considerar antes de configurar el almacenamiento en caché dinámico?**

  Si hay algún parámetro que está en formato nombre-valor y no tiene la consulta URL completa, o si el dispositivo recibe el parámetro en un encabezado de cookie o en un cuerpo POST, considere la posibilidad de configurar el almacenamiento en caché dinámico. Para configurar el almacenamiento en caché dinámico, debe configurar el parámetro HitParams.

- **¿Cómo se admite la codificación hexadecimal en los nombres de los parámetros?**

En el dispositivo Citrix ADC, la codificación %HEXHEX se admite en los nombres de los parámetros. En los nombres que especifique para HitParams o InvalParams, puede especificar un nombre que contiene la codificación %HEXHEX en los nombres. Por ejemplo, el nombre, el nombre%65 y n%61m%65 son equivalentes.

- **¿Cuál es el proceso para seleccionar un parámetro HitParam?**

  Considere el siguiente extracto de un encabezado HTTP para una solicitud POST:

```
POST /data2html.asp?param1=value1&param2=&param3&param4=value4
HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,
application/vnd.ms-powerpoint, application/vnd.ms-excel,
application/msword, application/x-shockwave-flash, \*/\*
Referer: http://10.102.3.97/forms.html
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Host: 10.102.3.97
Content-Length: 153
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: ASPSESSIONIDQGQGGRNY=NNLLKDADEENOAFLCCDGFGDMO
S1=This+text+is+only+text%2C+not+more+and+not+less%2C+%0D%0Ajust+
   text+to+be+itself%2C+namely+%22Text%22+to+be+posted+as+text
   +%28what+else...%29&B1=Submit
<!--NeedCopy-->
```

  En la solicitud anterior, puede utilizar S1 y B1, resaltados en negrita para su referencia, como HitParams dependiendo de sus necesidades. Además, si utiliza -MatchCookies YES en el grupo de contenido ASPSESSIONIDQGQGGRNY, entonces también puede usar estos parámetros como HitParams.

- **¿Qué sucede con los clientes en cola si la respuesta no se almacena en caché?**

  Si la respuesta no se puede almacenar en caché, todos los clientes de la cola reciben la misma respuesta que recibe el primer cliente.

- **¿Puedo habilitar las funciones Poll every time (PET) y Flash Cache en el mismo grupo de contenido?**

  No. No puede habilitar PET y Flash Cache en el mismo grupo de contenido. La caché integrada no realiza la función AutoPet en grupos de contenido de Flash Cache. La función PET garantiza que la caché integrada no sirve a un objeto almacenado sin consultar al servidor. Puede

configurar PET explícitamente para un grupo de contenido.

- **¿Cuándo se crean las entradas de registro para los clientes en cola?**

  Las entradas de registro se crean para los clientes en cola poco después de que el dispositivo reciba el encabezado de respuesta. Las entradas de registro se crean solo si el encabezado de respuesta no hace que el objeto no se pueda almacenar en caché.

- **¿Cuál es el significado de los valores DNS, HOSTNAME y HOSTNAME_AND_IP de Verify cached object using parameter of the cache configuration?**

  Los significados son los siguientes:

  - `set cache parameter -verifyUsing HOSTNAME`

    El comando ignora la dirección IP de destino.

  - `set cache parameter -verifyUsing HOSTNAME_AND_IP`

    El comando coincide con la dirección IP de destino.

  - `set cache parameter -verifyUsing DNS`

    El comando utiliza el servidor DNS.

- **He establecido WeakNegreLexpiry en 600, que son 10 minutos. Noté que las respuestas 404 no se están almacenando en caché. ¿Cuál es la razón?**

  Esto depende completamente de su configuración. De forma predeterminada, 404 respuestas se almacenan en caché durante 10 minutos. Si quiere que todas las respuestas 404 se obtenan del servidor, especifique: weaknegrelExpiry 0. Puede ajustar el —weaknegrelExpiry a un valor deseado, como superior o inferior para obtener las 404 respuestas almacenadas en caché adecuadamente. Si ha configurado —AbsExpiry para respuestas positivas, entonces es posible que no produzca los resultados deseados.

- **Cuando el usuario accede al sitio mediante el explorador Mozilla Firefox, se muestra el contenido actualizado. Sin embargo, cuando el usuario accede al sitio mediante el explorador Microsoft Internet Explorer, se muestra contenido obsoleto. ¿Cuál podría ser la razón?**

  Es posible que el explorador Microsoft Internet Explorer esté tomando el contenido de su caché local en lugar de la caché integrada de Citrix ADC. La razón puede ser que el explorador Microsoft Internet Explorer no respeta el encabezado relacionado con la caducidad en la respuesta.

  Para resolver este problema, puede inhabilitar la caché local de Internet Explorer y borrar el contenido sin conexión. Después de borrar el contenido sin conexión, el explorador debe mostrar el contenido actualizado.

- **¿Qué pasa si los hits son cero?**

  Compruebe si la hora del servidor y la hora NS están sincronizadas. Y el límite de WeakPosrelExpiry debe soportar la diferencia horaria entre NS y servidor de la siguiente manera:


```
root@ns180# date
Tue May 15 18:53:52 IST 2012
<!--NeedCopy-->
```

- **¿Por qué las directivas reciben visitas pero no se está almacenando en caché?**

  Compruebe que la memoria esté asignada a la caché integrada y que la asignación sea mayor que cero.

- **¿Es posible poner a cero los contadores de caché?**

  No hay línea de comandos ni opción GUI para establecer los contadores de caché en cero, y el vaciado de la caché tampoco lo hace. Reiniciar el cuadro establece automáticamente estos contadores en cero.

Instalación, actualización de versiones y reversión de versiones

August 20, 2021

Instalación y actualización

¿Cómo descargar un paquete específico de compilación de versión de Citrix ADC?

Para obtener información sobre cómo descargar un paquete de compilación de versiones de Citrix ADC específico, consulte Descargar un paquete de versión de Citrix ADC.

¿Cómo actualizar el software del sistema de un dispositivo Citrix ADC?

Para obtener información sobre la actualización del software del sistema de un dispositivo Citrix ADC, consulte Actualización de un dispositivo independiente Citrix ADC.

¿Dónde puedo encontrar las notas de la versión de una versión de Citrix ADC?

El documento de notas de la versión de una compilación de versión de Citrix ADC enumera lo siguiente para la compilación de la versión:

- Mejoras
- Problemas resueltos
- Problemas conocidos

El documento de notas de la versión de una compilación de versión de Citrix ADC se encuentra en las siguientes ubicaciones:

- Página de descargas de firmware o dispositivo virtual de Citrix ADC de una compilación de versión específica.
- Página de notas de la versión de Citrix ADC en el sitio de documentos de Citrix

¿Dónde puedo encontrar actualizaciones de seguridad para los dispositivos Citrix ADC?

El equipo de seguridad de Citrix publica periódicamente boletines de seguridad sobre vulnerabilidades y exposiciones comunes (CVE) para todos los productos Citrix relacionados. Esta información se encuentra en el boletín de seguridad de Citrix. Alternativamente, puede buscar un CVE específico en el sitio de soporte de Citrix.

¿Para qué sirve el archivo zebos.conf disponible en una versión de Citrix ADC?

Un dispositivo Citrix ADC utiliza ZeBO como conjunto de redirección. El archivo zebos.conf disponible en una versión de Citrix ADC es el archivo de configuración de ZEBO.

Quiero cambiar el puerto SSH (22) del dispositivo Citrix ADC a otro puerto. ¿Es posible cambiar el puerto SSH en el dispositivo?

Sí. Puede cambiar el puerto SSH en el dispositivo Citrix ADC modificando el archivo sshd_config en el directorio /nsconfig. Si el archivo no existe en el directorio /nsconfig, cópielo desde el directorio /etc.

En el archivo sshd_config, modifique la entrada del puerto 22 al puerto <Number>, donde <Number> es el número de puerto de destino. Si no quiere reiniciar el dispositivo y hacer efectivos los cambios, finalice el `sshd` proceso mediante el comando kill y, a continuación, reinicie el proceso.

Falta el directorio flash en el dispositivo Citrix ADC. ¿Qué procedimiento debo seguir para montar el directorio flash?

Para montar el directorio flash, haga lo siguiente:

1. Inicie el dispositivo Citrix ADC en modo de usuario único.

   Cuando se inicia el dispositivo, aparece el siguiente mensaje:

   Seleccione [Entrar] para arrancar inmediatamente o cualquier otra tecla del símbolo del sistema. Arrancar [el núcleo] en 10 segundos…" Seleccione el espacio y debe ver el siguiente mensaje:

   Escriba "?" para obtener una lista de comandos, "help" para obtener ayuda más detallada.

2. Introduzca el siguiente comando para iniciar FreeBSD en modo de usuario único:

   boot –s

   Una vez iniciado el dispositivo, aparece el siguiente mensaje:

   Introduzca el nombre de ruta completo de shell o RETURN para /bin/sh:

3. Pulse Intro para mostrar la solicitud #.
4. Ejecute el siguiente comando para montar el directorio flash:

```
mount /dev/ad0s1a /flash

Note: If the preceding command displays an error message about
   permissions, run the following command to check the disk for
   consistency:

fsck /dev/ad0s1a

Run the mount command again to mount the flash directory.
```

5. Reinicie el dispositivo.
6. Desde el símbolo del shell, ejecute el siguiente comando para comprobar que el directorio flash está montado:

```
df -kh
```

Deseo iniciar sesión en el dispositivo Citrix ADC sin introducir la contraseña. ¿Es posible configurar SSH en el dispositivo para permitir eso?

Sí. Puede configurar SSH en el dispositivo Citrix ADC para que inicie sesión sin contraseña. Sin embargo, debe proporcionar su nombre de usuario. Para configurar SSH para iniciar sesión sin contraseña, haga lo siguiente:

1. Ejecute el siguiente comando para generar las claves públicas y privadas:

```
\# ssh-keygen -t rsa
```

2. Ejecute el siguiente comando para copiar el archivo id_rsa.pub en el directorio.ssh del host remoto en el que quiere iniciar sesión:


```
\# scp id_dsa.pub \<user>@\<remote_host>/.ssh/id_dsa.pub
```

3. Inicie sesión en el host remoto.
4. Cambie al directorio .ssh.
5. Ejecute los siguientes comandos para agregar la clave pública del cliente a las claves públicas conocidas:

```
\# cat id_dsa.pub >> authorized_keys2

\# chmod 640 authorized_keys2

\# rm id_dsa.pub
```

¿Cuál es el procedimiento para restablecer el BIOS del dispositivo Citrix ADC? ¿En qué circunstancias debo restablecer el BIOS?

Para restablecer el BIOS del dispositivo Citrix ADC, realice el siguiente procedimiento:

1. Conéctese al dispositivo a través del puerto serie.
2. Inicie el dispositivo y presione Supr cuando se inicie el proceso de arranque.

   Al pulsar Suprimir durante el proceso POST se muestra la configuración del BIOS del dispositivo.
3. Active la página Salir de la configuración del BIOS.
4. Seleccione la opción Cargar valores predeterminados óptimos. Aparece el cuadro de mensaje Cargar configuración óptima.
5. Seleccione Aceptar.
6. Realice los siguientes cambios en la configuración del BIOS en las diferentes fichas:

   Tabulador
7. Active la página Salir de la configuración del BIOS.
8. Seleccione Guardar cambios y Salir.
9. Seleccione Aceptar para confirmar.
10. Compruebe que el dispositivo se inicia de forma limpia y que la consola serie muestra la salida después de que se inicie el dispositivo.

Debe restablecer el BIOS cuando la consola serie no responda. Esto suele ocurrir después de actualizar el dispositivo y la consola serie está inhabilitada. Sin embargo, aún puede acceder al dispositivo mediante la utilidad telnet o SSH.

Necesito restablecer el dispositivo Citrix ADC a los valores predeterminados de fábrica. ¿Qué procedimiento debo seguir?

Para restablecer el dispositivo Citrix ADC a los valores predeterminados de fábrica, debe restablecer dos entornos: El entorno de aplicaciones Citrix ADC y el entorno básico de FreeBSD.
Para restablecer el entorno de aplicación Citrix ADC del dispositivo a los valores predeterminados de fábrica, haga lo siguiente:

1. Realizar una copia de seguridad del dispositivo /nsconfig/ns.conf.
2. Elimine el archivo /nsconfig/ns.conf.
3. Reinicie el dispositivo. Para restablecer el entorno FreeBSD del dispositivo a los valores predeterminados de fábrica, haga lo siguiente:
   a) Instale una nueva imagen de código Citrix ADC en el dispositivo. Esto sobrescribe varios archivos de configuración de nivel FreeBSD con valores predeterminados.
   b) Elimine los usuarios y grupos que se agregan al dispositivo, es decir, todos excepto los usuarios predeterminados.
   c) Elimine el archivo /etc/resolv.conf.
   d) Elimine las entradas que ha agregado al archivo /etc/hosts.
   e) Si existe el archivo /etc/rc.netscaler, elimínelo.
   f) Abra el archivo /etc/nsperm_group_suser y asegúrese de que todas las entradas IOCTL sean entradas de comentarios.
   g) Abra el archivo /etc/rc.conf y asegúrese de que la entrada SysLogd_Enable=No se cambie a SysLogd_Enable=Yes.
   h) Abra el archivo /etc/syslog.conf y asegúrese de que no haya entradas adicionales en el archivo.
   i) Elimine el contenido de los archivos /var/nslog, /var/nstrace y /var/crash.
   j) Si el proceso syslog está habilitado en el dispositivo y éste crea archivos de registro localmente, elimine el contenido de los archivos de registro enumerados en el archivo /etc/syslog.conf. Los archivos se crean en el directorio /var/log. Por ejemplo, si el proceso syslog escribe eventos del sistema en el archivo /var/log/events y `sslvpn` accede a eventos al archivo /var/log/sslvpnevents, elimine estos archivos.

El dispositivo muestra un mensaje similar al mensaje "21 de junio 12:20:18 ns /flash/ns-10.0-47.15: [1/2]dc0: NIC cuelga la condición #663: TX 10000/10000, RX 0, HF 0" en la consola. ¿Cuál es el significado de este mensaje?

El mensaje consta de los siguientes componentes (mostrados aquí como ejemplos):

- #663: Número de veces que se ha producido esta condición en el dispositivo.
- TX 10000/10000: Número de paquetes que el dispositivo intentó transmitir y número de paquetes transmitidos. Si ambos números son iguales, como en este ejemplo, la NIC transmitió todos los paquetes que el dispositivo intentó transmitir.
- RX 0: Número de paquetes recibidos. En este ejemplo, no se recibió ningún paquete.
- HF0: Número de problemas de hardware notificados por la NIC. En este ejemplo, la NIC no informó ningún problema de hardware.

Si el dispositivo no recibe ningún paquete, informa de una condición de bloqueo, ya que en una red es poco probable que no reciba ningún paquete. Sin embargo, si el dispositivo está conectado a la interfaz bastante, puede ignorar este mensaje de error.

Después de actualizar la versión de Citrix ADC en el dispositivo, el dispositivo sigue mostrando la versión o compilación anteriores. ¿Cuál puede ser la razón?

El dispositivo muestra el número de versión de software del archivo /flash/boot/loader.conf. Si la entrada del núcleo de la versión actual de Citrix ADC no se encuentra en ese archivo, el dispositivo muestra la última versión de Citrix ADC para la que la entrada estaba disponible.
Para resolver este problema, haga lo siguiente:

1. Compruebe que el archivo del núcleo existe en el directorio /nsconfig.
2. Compruebe el archivo /flash/boot/loader.conf para una entrada para el núcleo.

   (Puede esperar que la entrada del kernel de la versión o compilación que instaló falte en el archivo).
3. Abra el archivo loader.conf en un editor de texto, como el editor vi, y actualice la entrada del kernel para la nueva versión o compilación.
4. Guarde el archivo y ciérrelo.
5. Repita los pasos 2 a 4 para el archivo /flash/boot/loader.conf.local.
6. Actualice la entrada de release/build en el archivo ns.conf.
7. Reinicie el dispositivo.

Desde que actualicé la versión Citrix ADC en el dispositivo, la pantalla LCD del panel frontal del dispositivo muestra el mensaje de falta de servicio o no muestra nada. ¿Cómo puedo resolver este problema?

Ejecute el siguiente comando desde el símbolo del shell del dispositivo:

```
1 /netscaler/nslcd -k
```


He actualizado la versión o compilación de Citrix ADC. Sin embargo, después del proceso de actualización, el dispositivo no se inicia. ¿Puedo degradar el software del dispositivo a la versión anterior o compilación?

Sí. Puede iniciar el dispositivo con el archivo kernel kernel.old. Cuando reinicie el dispositivo, presione la tecla F1 cuando la consola del dispositivo muestre el mensaje Press F1. Escriba kernel.old y pulse **Intro**.

Después de actualizar la versión de Citrix ADC en el dispositivo, eliminé accidentalmente el archivo del kernel del directorio /flash. Como resultado, no puedo iniciar el dispositivo. ¿Hay algún método para iniciar el dispositivo en esta situación?

Sí. Puede iniciar el dispositivo mediante el archivo `kernel.GENERIC` kernel, como se indica a continuación:

1. Cuando reinicie el dispositivo, presione la tecla F1 cuando la consola del dispositivo muestre el mensaje Press F1.
2. Escriba kernel. GENERIC y pulse Intro.
3. Inicie sesión como usuario raíz.
4. Vuelva a instalar la versión Citrix ADC.
5. Reinicie el dispositivo.

Después de actualizar el software del dispositivo, no puedo iniciar sesión en el dispositivo y aparece el siguiente mensaje. Intenté resolver este problema mediante el procedimiento de recuperación de contraseña, pero no funcionó. ¿He hecho algo incorrectamente?

```
```
login: nsroot
Password:
connect: No such file or directory
nsnet_connect: No such file or directory
Login incorrect
<!--NeedCopy--> ```
```

No puede resolver este problema mediante el procedimiento de recuperación de contraseña. Citrix ADC versión 12.1 o posterior utiliza el nuevo sistema de licencias, basado en el `Imgrd` demonio, que se ejecuta durante el procedimiento de inicio. Para que este demonio funcione correctamente, el nombre de host del dispositivo Citrix ADC, que se establece en el archivo /nsconfig/rc.conf, debe resolverse mediante un servidor de nombres a la dirección NSIP. Alternativamente, puede crear un archivo hosts en el directorio /nsconfig y agregar la <Host_Name> entrada 127.0.0.1 en el archivo.

Además, asegúrese de haber copiado los archivos de licencia en el directorio /nsconfig/license/.

 
```

Durante una actualización de un par de alta disponibilidad, el siguiente mensaje aparece repetidamente. ¿Cuál puede ser la razón?

ns sshd[5035]: error: nombre de usuario o contraseña no válidos
Este mensaje de error aparece cuando los dispositivos involucrados en el emparejamiento de alta disponibilidad tienen instalada una versión de Citrix ADC diferente o una compilación diferente de la misma versión. Los dispositivos pueden tener una versión diferente instalada si ha actualizado o degradado un dispositivo pero no el otro.
Deseo cambiar la máscara de red de la dirección NSIP en un dispositivo Citrix ADC. ¿Puedo hacerlo sin provocar una interrupción?
Cambiar la máscara de red de la IP de Citrix ADC podría provocar una interrupción breve. Asegúrese de cambiar la máscara de red en el dispositivo secundario y, a continuación, romper el emparejamiento de alta disponibilidad. Compruebe la funcionalidad del dispositivo. Si todo funciona como se esperaba, reconstruya el emparejamiento de alta disponibilidad.
Para cambiar la máscara de red en el dispositivo, ejecute el 'config ns' comando desde el indicador de CLI y, a continuación, elija la segunda opción en el menú.
He configurado un par de dispositivos Citrix ADC de alta disponibilidad. Después de actualizar la versión de software de una versión preliminar a una versión final, me di cuenta de que faltan algunas de las configuraciones del dispositivo. ¿Puedo recuperar las configuraciones perdidas?
Puede utilizar el siguiente procedimiento para restaurar la configuración:
1. Inicie sesión en la línea de comandos de Citrix ADC del dispositivo principal.
2. Ejecute los comandos siguientes:
save config
shell
\#cp /nsconfig/ns.conf /nsconfig/ns.conf.bkup
The ns.conf.bkup file is a backup for the running configuration.
3. Actualice el software de ambos dispositivos a la versión final.
4. Inicie sesión en la línea de comandos de Citrix ADC del dispositivo principal.
¿Pueden el dispositivo principal y el dispositivo secundario tener compilaciones independientes?
La práctica recomendada es utilizar la misma versión y el mismo número de compilación tanto en el dispositivo primario como en el secundario.
¿Se pueden actualizar ambos dispositivos en un par de alta disponibilidad (HA) al mismo tiempo?
No. En un par HA, primero actualice el nodo secundario y, a continuación, actualice el nodo primario. Para obtener más información, consulte [Actualización de un par de alta disponibilidad](/es-es/citrix-adc/current-release/upgrade-downgrade-citrix-adc-appliance/upgrade-downgrade-HA-pair.html).
¿Citrix admite actualizaciones de firmware en la nube de Amazon Web Services?
Sí.
¿Puedo actualizar la instancia de Citrix ADC independientemente de la versión SDX?
No es necesario actualizar la versión SDX cuando se actualiza el dispositivo Citrix ADC. Sin embargo, es posible que algunas funciones no funcionen.

¿Puedo usar el servidor FTP para actualizar el dispositivo Citrix ADC?
No. Primero debe descargar el firmware del sitio de descargas de Citrix, guardarlo en el equipo local y, a continuación, actualizar el dispositivo.
¿Es diferente el procedimiento para actualizar el dispositivo Citrix ADC con configuraciones GSLB de una actualización de un dispositivo que no está involucrado en GSLB?
No. El procedimiento de actualización es similar al procedimiento básico de actualización. La única diferencia es que puede actualizar los dispositivos autónomos o de alta disponibilidad en diferentes sitios de manera gradual.
Degradar
He recibido un dispositivo Citrix ADC con la versión más reciente de Citrix ADC instalada en él. Sin embargo, quiero degradar la versión de software. ¿Puedo hacerlo?
No. Si intenta degradar la versión de software, es posible que el dispositivo no funcione como se esperaba, ya que el archivo ns.conf de la versión posterior podría no ser compatible con la versión anterior y que el dispositivo podría restaurar la configuración de fábrica.
Al degradar la versión de Citrix ADC, seguí las instrucciones. Sin embargo, el dispositivo muestra el siguiente mensaje. ¿Cómo se realiza el procedimiento de reversión en un dispositivo Citrix ADC?
root@LBCOL03B# ./installns
installns version (10.0-47.7) kernel (ns-10.0-47.7.gz)
Note:
Installation may pause for up to 3 minutes while data is written to the flash.
Caution:
Do not interrupt the installation process.
Doing so may cause the system to become unusable.
Installation will proceed in 5 seconds, CTRL-C to abort
No Valid Citrix ADC Version Detected
root@LBCOL03B#
El procedimiento de reversión es similar al procedimiento básico de actualización. Seleccione la compilación de destino en la que desea revertir y realice la degradación. Antes de volver a otra versión, Citrix recomienda crear una copia de los archivos de configuración actuales. Para bajar de categoría desde una versión, consulte [Desactualización de un dispositivo independiente Citrix ADC](/es-es/citrix-adc/current-release/upgrade-downgrade-citrix-adc-appliance/downgrade-standalone-appliance.html).

Equilibrio de carga

August 20, 2021

- **¿Cuáles son las diversas directivas de equilibrio de carga que puedo crear en el dispositivo Citrix ADC?**

Puede crear los siguientes tipos de directivas de equilibrio de carga en el dispositivo Citrix ADC:

- Menos conexiones
- Round Robin
- Tiempo de respuesta mínimo
- Ancho de banda mínimo
- Menos paquetes
- hash de URL
- Hash de nombres de dominio
- Hashing de direcciones IP de origen
- Hashing de direcciones IP de destino
- IP de origen: Hash IP de destino
- Token
- LRTM

- **¿Puedo lograr la seguridad de la comunidad de servidores web implementando el equilibrio de carga con el dispositivo Citrix ADC?**

  Sí. Puede lograr la seguridad de la comunidad de servidores web implementando el equilibrio de carga mediante el dispositivo Citrix ADC. El dispositivo Citrix ADC permite implementar las siguientes opciones de la función de equilibrio de carga:

  - Ocultación de direcciones IP: Permite instalar los servidores reales para estar en el espacio de direcciones IP privado por razones de seguridad y para la conservación de direcciones IP. Este proceso es transparente para el usuario final porque el dispositivo Citrix ADC acepta solicitudes en nombre del servidor. Mientras se encuentra en el modo de ocultación de direcciones, el dispositivo aísla completamente las dos redes. Por lo tanto, un cliente puede acceder a un servicio que se ejecuta en la subred privada, como FTP o un servidor Telnet, a través de un VIP diferente en el dispositivo para ese servicio.
  - Asignación de puertos: Permite que los servicios TCP reales se hospeden en puertos no estándar por razones de seguridad. Este proceso es transparente para el usuario final, ya que el dispositivo Citrix ADC acepta solicitudes en nombre del servidor en la dirección IP anunciada estándar y el número de puerto.

- **¿Cuáles son los distintos dispositivos que puedo utilizar para equilibrar la carga con un dispositivo Citrix ADC?**

  Puede equilibrar la carga de los siguientes dispositivos con un dispositivo Citrix ADC:

  - Comunidades de servidores
  - Cachés o proxy inverso
  - Dispositivos Firewall
  - Sistemas de detección de intrusiones
  - Dispositivos de descarga SSL

  - Dispositivos de compresión
  - Servidores de inspección de contenido

- **¿Por qué debería implementar la función de equilibrio de carga para el sitio web?**

  Puede implementar la función de equilibrio de carga para que el sitio web tenga las siguientes ventajas:

  - Reducir el tiempo de respuesta: Cuando implementa la función de equilibrio de carga para el sitio web, uno de los principales beneficios es el impulso que puede esperar en el tiempo de carga. Con dos o más servidores que comparten la carga del tráfico web, cada uno de los servidores ejecuta menos carga de tráfico que un solo servidor. Esto significa que hay más recursos disponibles para satisfacer las solicitudes del cliente. Esto da como resultado un sitio web más rápido.
  - Redundancia: La implementación de la función de equilibrio de carga introduce un poco de redundancia. Por ejemplo, si el sitio web está equilibrado en tres servidores y uno de ellos no responde en absoluto, los otros dos pueden seguir funcionando y los visitantes del sitio web ni siquiera notan ningún tiempo de inactividad. Cualquier solución de equilibrio de carga deja de enviar inmediatamente tráfico al servidor back-end que no está disponible.

- **¿Por qué necesito desactivar la opción de reenvío basado en Mac (MBF) para el equilibrio de carga de enlace (LLB)?**

  - Si habilita la opción MBF, el dispositivo Citrix ADC considera que el tráfico entrante del cliente y el tráfico saliente al mismo cliente fluyen a través del mismo enrutador ascendente. Sin embargo, la función LLB requiere que se elija la mejor ruta para el tráfico de retorno.
  - Habilitar la opción MBF rompe este diseño de topología al enviar el tráfico saliente a través del enrutador que reenvió el tráfico de cliente entrante.

- **¿Cuáles son los distintos tipos de persistencia disponibles en el dispositivo Citrix ADC?**

  El dispositivo Citrix ADC admite los siguientes tipos de persistencia:

  - IP de origen
  - Inserción de cookies
  - ID de sesión SSL
  - URL pasiva
  - ID de servidor personalizado
  - Regla
  - DESTIP

Interfaz gráfica (GUI)

January 31, 2022

- **Cuando uso Firefox para comparar dos configuraciones de Citrix ADC, ¿el explorador parece bloquearse?**

  Firefox finalmente muestra la diferencia en las configuraciones, pero el proceso lleva una cantidad considerable de tiempo si hay más de 1000 diferencias. Usa Chrome para obtener una respuesta más rápida.

- **Estoy usando un explorador Safari MAC para actualizar un Citrix ADC. En el asistente de actualización, cuando hago clic en el botón Examinar para elegir el archivo de compilación del dispositivo, el cuadro de diálogo no muestra ningún archivo o carpeta. Además, cuando vuelvo a la carpeta raíz, el cuadro de diálogo muestra la carpeta de nivel superior, pero no puedo explorarla. ¿Qué debo hacer?**

  En el explorador Safari, haga clic en el icono Configuración y vaya a **Preferencias > Seguridad > Administrar la configuración del sitio web > Java**. Cambie el valor de la configuración **Al visitar otros sitios web** a Ejecutar en modo inseguro.

- **¿Qué debo hacer antes de acceder a la GUI?**

  Antes de acceder a una nueva versión del software Citrix ADC:

  - Borrar la caché del explorador, incluidas las cookies
  - Accede a la GUI en modo incógnito del explorador.
  - Acceda a GUI en algún otro explorador.
  - Desactive la opción **Usar aceleración de software** en la configuración y reinicie el explorador.
  - Accede a **chrome: extensions**, desmarca la casilla **Habilitar** y reinicia el explorador Chrome.

- **¿Qué puerto debo abrir para acceder a la GUI mediante HTTP o HTTPS?**

  A continuación se enumeran los números de puerto predeterminados para los servicios de administración (GUI) HTTP y HTTPS en los dispositivos Citrix ADC MPX, VPX y CPX:

  - Dispositivos Citrix ADC MPX y VPX: 80 (HTTP) y 443 (HTTPS)
  - Dispositivos Citrix ADC CPX: 9080 (HTTP) y 9443 (HTTPS)

  Además, puede configurar puertos para los servicios de administración (GUI) HTTP y HTTPS distintos de los puertos 80 y 443. Para obtener más información, consulte Configurar puertos de administración HTTP y HTTPS.

- **¿Con qué exploradores es compatible la GUI para diferentes sistemas operativos?**

En la siguiente tabla se enumeran los exploradores compatibles para la GUI de NetScaler versión 12.0, 12.1 y 13.0:

Sistema operativo	Explorador web	Versiones
Windows 7 y versiones posteriores	Internet Explorer	11, Edge y versiones posteriores
Windows 7 y versiones posteriores	Mozilla Firefox	45 y posteriores
Windows 7 y versiones posteriores	Chrome	60 y posteriores
MAC	Mozilla Firefox	45 y posteriores
MAC	Safari	10.1.1 y posteriores

SSL

August 20, 2021

Haga clic aquí para ver las preguntas frecuentes sobre SSL.

Autenticación, autorización y auditoría del tráfico de aplicaciones

December 2, 2021

Muchas empresas restringen el acceso al sitio web solo a usuarios válidos y controlan el nivel de acceso permitido a cada usuario. La función de autenticación, autorización y auditoría permite al administrador del sitio administrar los controles de acceso con el dispositivo Citrix ADC en lugar de administrar estos controles por separado para cada aplicación. La autenticación en el dispositivo también permite compartir esta información en todos los sitios web del mismo dominio que están protegidos por el dispositivo.

Para utilizar la autenticación, autorización y auditoría, debe configurar los servidores virtuales de autenticación para gestionar el proceso de autenticación y los servidores virtuales de administración del tráfico para gestionar el tráfico hacia las aplicaciones web que requieren autenticación. También configura su DNS para asignar FQDN a cada servidor virtual. Después de configurar los servidores virtuales, configura una cuenta de usuario para cada usuario que se autenticará mediante el dispositivo Citrix ADC y, de forma opcional, creará grupos y asignará cuentas de usuario a grupos. Después de

crear grupos y cuentas de usuario, se configuran directivas que indican al dispositivo cómo autenticar a los usuarios, a qué recursos se les permite acceder y cómo registrar las sesiones de usuario. Para aplicar las directivas, debe vincular cada directiva de forma global, a un servidor virtual específico o a las cuentas de usuario o grupos adecuados. Después de configurar las directivas, puede personalizar las sesiones de usuario configurando los ajustes de sesión y vinculando las directivas de sesión al servidor virtual de administración del tráfico. Por último, si la intranet utiliza certificados de cliente, debe configurar la configuración del certificado de cliente.

Para comprender cómo funcionan la autenticación, la autorización y la auditoría en un entorno distribuido, considere una organización con una intranet a la que acceden sus empleados en la oficina, en casa y cuando viajan. El contenido de la intranet es confidencial y requiere acceso seguro. Cualquier usuario que quiera acceder a la intranet debe tener un nombre de usuario y una contraseña válidos. Para cumplir estos requisitos, el ADC hace lo siguiente:

- Redirige al usuario a la página de inicio de sesión si accede a la intranet sin haber iniciado sesión.
- Recopila las credenciales del usuario, las entrega al servidor de autenticación y las almacena en caché en un directorio al que se puede acceder mediante el Protocolo ligero de acceso a directorios (LDAP). Para obtener más información, consulte Determinación de atributos en el directorio LDAP.
- Comprueba que el usuario esté autorizado a acceder al contenido específico de la intranet antes de entregar la solicitud del usuario al servidor de aplicaciones.
- Mantiene un tiempo de espera de la sesión tras el cual los usuarios deben volver a autenticarse para recuperar el acceso a la intranet. (Puede configurar el tiempo de espera).
- Registra el acceso del usuario, incluidos los intentos de inicio de sesión no válidos, en un registro de auditoría.

Tipos de autenticación admitidos

- Locales
- LDAP
- RADIUS
- SAML
- TACACOS+
- Autenticación de certificado de cliente (incluida la autenticación con tarjeta inteligente)
- Web
- Autentificación avanzada
- Autentificación basada en formularios
- Autentificación basada en 401
- OTP nativo
- Notificación push

- Correo electrónico OTP
- reCAPTCHA

Citrix Gateway también admite RSA SecurID, Gemalto Protiva y SafeWord. Se utiliza un servidor RADIUS para configurar estos tipos de autenticación.

Antes de configurar la autenticación, autorización y auditoría, debe estar familiarizado y comprender cómo configurar el equilibrio de carga, el cambio de contenido y SSL en el dispositivo Citrix ADC.

Autenticación sin autorización

La autorización especifica los recursos de red a los que tienen acceso los usuarios cuando inician sesión en el dispositivo. La configuración predeterminada de la autorización es denegar el acceso a todos los recursos de red. Citrix recomienda utilizar la configuración global predeterminada y, a continuación, crear directivas de autorización para definir los recursos de red a los que pueden acceder los usuarios.

La autorización se configura en el dispositivo mediante expresiones y directivas de autorización. Después de crear una directiva de autorización, puede vincularla a los usuarios o grupos que haya configurado en el dispositivo.

Puede configurar el dispositivo para que utilice únicamente la autenticación, sin autorización. Al configurar la autenticación sin autorización, el dispositivo no realiza una comprobación de autorización de grupo. Las directivas que configura para el usuario o el grupo se asignan al usuario.

Habilitación de autenticación, autorización y auditoría

Para utilizar la función de autenticación, autorización y auditoría, debe habilitarla. Puede configurar entidades de autenticación, autorización y auditoría, como los servidores virtuales de autenticación y administración del tráfico, antes de habilitar la función de autenticación, autorización y auditoría, pero las entidades no funcionan hasta que se habilita la función.

Para habilitar la autenticación, autorización y auditoría mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para habilitar la autenticación, la autorización y la auditoría y compruebe la configuración:

```
1 enable ns feature AAA
2 <!--NeedCopy-->
```


Para habilitar la autenticación, autorización y auditoría mediante la interfaz gráfica de usuario

1. Vaya a **Sistema > Configuración**.
2. En el panel de detalles, en **Modos y funciones**, haga clic en **Cambiar funciones básicas**.
3. En el cuadro de diálogo **Configurar funciones básicas**, active la casilla de verificación **Autenticación, autorización y auditoría** .
4. Haga clic en **OK**.

Inhabilitar la autenticación

Si la implementación no requiere autenticación, puede inhabilitarla. Puede inhabilitar la autenticación para cada servidor virtual que no requiera autenticación.

> **Importante:**
>
> **Importante:** Citrix recomienda inhabilitar la autenticación con precaución. Si no utiliza un servidor de autenticación externo, cree usuarios y grupos locales para permitir que el dispositivo autentique a los usuarios. Al inhabilitar la autenticación se detiene el uso de las funciones de autenticación, autorización y contabilidad que controlan y supervisan las conexiones al dispositivo. Cuando los usuarios escriban una dirección web para conectarse al dispositivo, la página de inicio de sesión no aparece.

Para inhabilitar la autenticación

1. Vaya a **Configuración > Citrix Gateway > Servidores virtuales**.
2. En el panel de detalles, haga clic en un servidor virtual y, a continuación, haga clic en **Abrir**.
3. En la página **Configuración básica**, desactive la casilla de verificación **Habilitar autenticación** .

Cómo funciona la autenticación, la autorización y la auditoría

December 2, 2021

La autenticación, autorización y auditoría proporcionan seguridad para un entorno de Internet distribuido al permitir que cualquier cliente con las credenciales adecuadas se conecte de forma segura a servidores de aplicaciones protegidos desde cualquier lugar de Internet. Esta función incorpora las tres funciones de seguridad de autenticación, autorización y auditoría. La autenticación permite que Citrix ADC compruebe las credenciales del cliente, ya sea de forma local o con un servidor de autenticación de terceros, y permite que solo los usuarios aprobados accedan a los servidores protegidos. La autorización permite al ADC verificar a qué contenido de un servidor protegido permite el acceso

de cada usuario. La auditoría permite al ADC mantener un registro de la actividad de cada usuario en un servidor protegido.

Para comprender cómo funcionan la autenticación, la autorización y la auditoría en un entorno distribuido, considere una organización con una intranet a la que acceden sus empleados en la oficina, en casa y cuando viajan. El contenido de la intranet es confidencial y requiere acceso seguro. Cualquier usuario que quiera acceder a la intranet debe tener un nombre de usuario y una contraseña válidos. Para cumplir estos requisitos, el ADC hace lo siguiente:

- Redirige al usuario a la página de inicio de sesión si accede a la intranet sin haber iniciado sesión.
- Recopila las credenciales del usuario, las entrega al servidor de autenticación y las almacena en caché en un directorio accesible a través de LDAP. Para obtener más información, consulte Determinación de atributos en el directorio LDAP.
- Comprueba que el usuario esté autorizado a acceder al contenido específico de la intranet antes de entregar la solicitud del usuario al servidor de aplicaciones.
- Mantiene un tiempo de espera de la sesión tras el cual los usuarios deben volver a autenticarse para recuperar el acceso a la intranet. (Puede configurar el tiempo de espera).
- Registra el acceso del usuario, incluidos los intentos de inicio de sesión no válidos, en un registro de auditoría.

Configurar directivas de auditoría y autorización de autenticación

Después de configurar los usuarios y los grupos, debe configurar las directivas de autenticación, las directivas de autorización y las directivas de auditoría para definir a qué usuarios se les permite acceder a la intranet, a qué recursos puede acceder cada usuario o grupo y qué nivel de detalle autenticación, autorización y auditoría se conservará en los registros de auditoría. Una directiva de autenticación define el tipo de autenticación que se debe aplicar cuando un usuario intenta iniciar sesión. Si se utiliza la autenticación externa, la directiva también especifica el servidor de autenticación externo. Las directivas de autorización especifican los recursos de red a los que pueden acceder los usuarios y los grupos después de iniciar sesión. Las directivas de auditoría definen el tipo y la ubicación del registro de auditoría.

Debe vincular cada directiva para que se aplique. Enlaza directivas de autenticación a servidores virtuales de autenticación, directivas de autorización a una o más cuentas o grupos de usuarios y directivas de auditoría de forma global y a una o más cuentas o grupos de usuarios.

Cuando vincula una directiva, le asigna una prioridad. La prioridad determina el orden en que se evalúan las directivas que defina. Puede establecer la prioridad en cualquier número entero positivo. En el sistema operativo Citrix ADC, las prioridades de las directivas funcionan en orden inverso: cuanto mayor sea el número, menor será la prioridad. Por ejemplo, si tiene tres directivas con prioridades de 10, 100 y 1000, la directiva asignada a una prioridad de 10 se ejecuta primero, luego a la directiva se

le asigna una prioridad de 100 y, por último, a la directiva se le asigna un orden de 1000. La función de autenticación, autorización y auditoría implementa solo la primera de cada tipo de directiva con la que coincide una solicitud, no ninguna directiva adicional de ese tipo con la que una solicitud también pueda coincidir, por lo que la prioridad de las directivas es importante para obtener los resultados deseados.

Puede dejar suficiente espacio para agregar otras directivas en cualquier orden y configurarlas para que se evalúen en el orden que quiera, estableciendo prioridades con intervalos de 50 o 100 entre cada directiva al vincular las directivas. A continuación, puede agregar directivas adicionales en cualquier momento sin tener que reasignar la prioridad de una directiva existente.

Para obtener información adicional sobre las directivas de enlace en el dispositivo Citrix ADC, consulte la documentación del producto Citrix ADC.

Configurar la directiva No_Auth para omitir cierto tráfico

Ahora puede configurar la directiva No_Auth para omitir cierto tráfico de la autenticación cuando la autenticación basada en 401 está habilitada en el servidor virtual de administración del tráfico. Para este tipo de tráfico, debe vincular una directiva de "No_Auth".

Para configurar la directiva No_Auth para evitar cierto tráfico mediante la CLI

En el símbolo del sistema, escriba:

```
add authentication policy <name> -rule <expression> -action <string>
<!--NeedCopy-->
```

Ejemplo:

```
add authentication policy ldap -rule ldapAct1 -action No_Auth
<!--NeedCopy-->
```

Componentes básicos de configuración de autenticación, autorización y auditoría

August 20, 2021

Los componentes básicos de la configuración de autenticación, autorización y auditoría son los siguientes:

- **Servidor virtual de autenticación**: Todas las solicitudes de autenticación son redirigidas por el servidor virtual de administración del tráfico (equilibrio de carga o cambio de contenido) al servidor virtual de autenticación. Este servidor virtual procesa las directivas de autenticación asociadas y, en consecuencia, proporciona acceso a la aplicación. Para obtener más información, consulte Servidor virtual de autenticación.
- **Perfiles** de autenticación: un perfil de autenticación especifica el servidor virtual de autenticación, el host de autenticación, el dominio de autenticación y un nivel de autenticación.

Puede crear uno o más perfiles de autenticación para especificar diferentes configuraciones de autenticación y enlazar estos perfiles de autenticación a servidores de administración de tráfico relevantes según sus requisitos. Para obtener más información, consulte Perfiles de autenticación.

- **Directivas de autenticación**: Cuando los usuarios inician sesión en el dispositivo Citrix ADC o Citrix Gateway, se autentican de acuerdo con una directiva que cree. Una directiva de autenticación comprende una expresión y una acción. Las directivas de autenticación utilizan expresiones Citrix ADC. Para obtener más información, consulte Directivas de autenticación.
- **Directivas de autorización**: Al configurar una directiva de autorización, puede configurarla para permitir o denegar el acceso a los recursos de red de la red interna. Para obtener más información, consulte Directivas de autorización.
- **Usuarios y grupos:** después de configurar la configuración básica de autenticación, autorización y auditoría, se crean usuarios y grupos. Primero debe crear una cuenta de usuario para cada persona que se autentique a través del dispositivo Citrix ADC. Si utiliza autenticación local controlada por el propio dispositivo Citrix ADC, cree cuentas de usuario locales y asigne contraseñas a cada una de esas cuentas. Para obtener más información, consulte Usuarios y grupos.

Servidor virtual de autenticación

October 5, 2021

El servidor virtual de administración del tráfico (equilibrio de carga o conmutación de contenido) redirige todas las solicitudes de autenticación al servidor virtual de autenticación. Este servidor virtual procesa las directivas de autenticación asociadas y, en consecuencia, proporciona acceso a la aplicación.

Nota: No se pueden vincular las directivas de administración del tráfico a servidores virtuales de autenticación, autorización y auditoría.

Configurar servidor virtual de autenticación

Los pasos necesarios para configurar un servidor virtual de autenticación son:

1. Habilite la función de autenticación, autorización y auditoría.

```
enable ns feature AAA
<!--NeedCopy-->
```

2. Configure un servidor virtual de autenticación. Debe ser de tipo SSL y asegúrese de vincular el par de claves de certificado SSL al servidor virtual.

```
add authentication vserver <name> SSL <ipaddress> <port>

bind ssl certkey <auth-vserver-name> <certkey>
<!--NeedCopy-->
```

3. Especifique el FQDN del dominio del servidor virtual de autenticación.

```
set authentication vserver <name> -authenticationDomain <FQDN>
<!--NeedCopy-->
```

4. Asocie el servidor virtual de autenticación al servidor virtual de administración de tráfico correspondiente.

   Puntos a tener en cuenta:

   - El FQDN del servidor virtual de administración de tráfico debe estar en el mismo dominio que el FQDN del servidor virtual de autenticación para que la cookie de sesión de dominio funcione correctamente. En el servidor virtual de administración del tráfico:
     - Habilite la autenticación.
     - Especifique el FQDN del servidor virtual de autenticación como host de autenticación del servidor virtual de administración de tráfico.
     - [Opcional] Especifique el dominio de autenticación en el servidor virtual de administración del tráfico.
     - Si no configura el dominio de autenticación, el dispositivo asigna un FQDN que consiste en el FQDN del servidor virtual de autenticación sin la parte del nombre de host. Por ejemplo, si el nombre de dominio del servidor virtual de autenticación es **tm.xyz.bar.com**, el dispositivo asigna **xyz.bar.com** como dominio de autenticación.
       * Para equilibrio de carga:


```
set lb vserver <name> -authentication ON -
   authenticationhost <FQDN> [-authenticationdomain <
   authdomain>]
<!--NeedCopy-->
```

* Para el cambio de contenido:

```
set cs vserver <name> <protocol> <IPAddress> <port>
<!--NeedCopy-->
```

- Si tiene que configurar una cookie de todo el dominio para un dominio de autenticación, debe habilitar el perfil de autenticación en un servidor virtual de equilibrio de carga.

5. Compruebe que ambos servidores virtuales estén activos y estén configurados correctamente.

```
show authentication vserver <name>
<!--NeedCopy-->
```

Para configurar un servidor virtual de autenticación mediante la interfaz gráfica de usuario

1. Habilite la función de autenticación, autorización y auditoría.

   Vaya a **Sistema > Configuración**, haga clic en **Configurar funciones básicas**y habilite **Autenticación, autorización y auditoría**.

2. Configure el servidor virtual de autenticación.

   Vaya a **Seguridad > AAA - Tráfico de aplicaciones > Servidores virtuales**y configúrelos según sea necesario.

3. Configure el servidor virtual de administración de tráfico para la autenticación.

   - **Para equilibrio de carga:**

     Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**y configure el servidor virtual según sea necesario.

   - **Para el cambio de contenido:**

     Vaya a **Administración del tráfico > Cambio de contenido > Servidores virtuales**y configure el servidor virtual según sea necesario.

4. - Compruebe la configuración de autenticación.

Vaya a **Seguridad > AAA - Tráfico de aplicaciones > Servidores virtuales**y compruebe los detalles del servidor virtual de autenticación correspondiente.

Configurar el servidor virtual de autenticación

Para configurar la autenticación, autorización y auditoría, primero configure un servidor virtual de autenticación para gestionar el tráfico de autenticación. A continuación, vincule un par de claves de certificado SSL al servidor virtual para que pueda manejar las conexiones SSL.
Para obtener información adicional sobre la configuración de SSL y la creación de un par de claves de certificado, consulte Certificados SSL.

Configurar un servidor virtual de autenticación mediante la CLI

Para configurar un servidor virtual de autenticación y verificar la configuración, en el símbolo del sistema escriba los siguientes comandos en el mismo orden:

```
add authentication vserver <name> ssl <ipaddress>

show authentication vserver <name>

bind ssl certkey <certkeyName>

show authentication vserver <name>

set authentication vserver <name>

show authentication vserver <name>
<!--NeedCopy-->
```

Ejemplo:

```
add authentication vserver Auth-Vserver-2 SSL 10.102.29.77 443 Done

show authentication vserver Auth-Vserver-2 Auth-Vserver-2
    (10.102.29.77:443) - SSL Type: CONTENT State: DOWN[Certkey not bound
    ] Client Idle Timeout: 180 sec Down state flush: DISABLED Disable
    Primary Vserver On Down : DISABLED Authentication : ON Current AAA
    Users: 0 Done

bind ssl certkey Auth-Vserver-2 Auth-Cert-1 Done
```



```
6
7  show authentication vserver Auth-Vserver-2 Auth-Vserver-2
       (10.102.29.77:443) - SSL Type: CONTENT State: UP Client Idle Timeout
       : 180 sec Down state flush: DISABLED Disable Primary Vserver On Down
        : DISABLED Authentication : ON Current AAA Users: 0 Done
8
9  set authentication vserver Auth-Vserver-2
10
11 show authentication vserver Auth-Vserver-2 Auth-Vserver-2
       (10.102.29.77:443) - SSL Type: CONTENT State: DOWN[Certkey not bound
       ] Client Idle Timeout: 180 sec Down state flush: DISABLED Disable
       Primary Vserver On Down : DISABLED Authentication : ON Current AAA
       Users: 0 Done
12 <!--NeedCopy-->
```

> **Nota**
>
> El parámetro Dominio de autenticación está obsoleto. Utilice el perfil de autenticación para configurar cookies de todo el dominio.

Configurar un servidor virtual de autenticación mediante la interfaz gráfica de usuario

1. Vaya a **Seguridad > AAA - Tráfico de aplicaciones > Servidores virtuales**.
2. En el panel de detalles, realice una de las acciones siguientes:
   - Para crear un nuevo servidor virtual de autenticación, haga clic en **Agregar**.
   - Para modificar un servidor virtual de autenticación existente, seleccione el servidor virtual y, a continuación, haga clic en **Modificar**. El cuadro de diálogo Configuración se abre con el área Configuración básica expandida.
3. Especifique los valores de los parámetros de la siguiente manera (el asterisco indica un parámetro obligatorio):
   - nombre*: nombre (no se puede cambiar para un servidor virtual creado anteriormente)
   - Tipo de dirección IP*: tipo de dirección IP del servidor virtual de autenticación
   - Dirección IP*: dirección IP del servidor virtual de autenticación
   - puerto*: puerto TCP en el que el servidor virtual acepta conexiones.
   - Tiempo de espera de inicio de sesión fallido: failedLoginTimeout (se permiten segundos antes de que se produzca un error en el inicio de sesión y el usuario debe volver a iniciar el proceso de inicio
   - Número máximo de intentos de inicio de sesión: MaxLoginAttentes (número de intentos de inicio de sesión permitidos antes de bloquear al usuario)

> **Nota:**
>
> El servidor virtual de autenticación utiliza solo el protocolo SSL y el puerto 443, por lo que estas opciones aparecen atenuadas. Cualquier opción que no se mencione se puede ignorar.

4. Haga clic en **Continuar** para mostrar el área Certificados.
5. En el área **Certificados**, configure los certificados SSL que quiera utilizar con este servidor virtual.
    - Para configurar un certificado de CA, haga clic en la flecha situada a la derecha de Certificado de CA para mostrar el cuadro de diálogo Clave de certificado de CA, seleccione el certificado que quiere vincular a este servidor virtual y haga clic en **Guardar**.
    - Para configurar un certificado de servidor, haga clic en la flecha situada a la derecha de Certificado de servidor y siga el mismo proceso que para el certificado de CA.
6. Haga clic en **Continuar** para mostrar el área **Directivas de autenticación avanzada** .
7. Si quiere enlazar una directiva de autenticación avanzada al servidor virtual, haga clic en la flecha situada a la derecha de la línea para mostrar el cuadro de diálogo **Directiva de autenticación**, elija la directiva que quiere enlazar al servidor, establezca la prioridad y, a continuación, haga clic en **Aceptar**.
8. Haga clic en **Continuar** para mostrar el área **Directivas de autenticación básica** .
9. Si quiere crear una directiva de autenticación básica y vincularla al servidor virtual, haga clic en el signo más para mostrar el cuadro de diálogo **Directivas** y siga las instrucciones para configurar la directiva y vincularla a este servidor virtual.
10. Haga clic en **Continuar** para mostrar el área Servidores virtuales basados en 401.
11. En el área Servidores virtuales basados en 401, configure los servidores virtuales de equilibrio de carga o conmutación de contenido que quiera enlazar a este servidor virtual.
    - Para enlazar un servidor virtual de equilibrio de carga, haga clic en la flecha situada a la derecha del servidor virtual de equilibrio de carga para mostrar el cuadro de diálogo Servidores virtuales de equilibrio de carga y siga las instrucciones.
    - Para enlazar un servidor virtual de conmutación de contenido, haga clic en la flecha situada a la derecha del servidor virtual de conmutación de contenido para mostrar el cuadro de diálogo Servidores virtuales de conmutación de contenido y siga el mismo proceso que para enlazar un servidor virtual LB.
12. Si quiere crear o configurar un grupo, en el área Grupos, haga clic en la flecha para mostrar el cuadro de diálogo Grupos y siga las instrucciones.
13. Revisa su configuración y, cuando hayas terminado, haga clic en **Listo**. El cuadro de diálogo se cierra. Si ha creado un nuevo servidor virtual de autenticación, ahora aparece en la lista de la

ventana **Configuración** .

Servidor virtual de administración del tráfico

Después de crear y configurar el servidor virtual de autenticación, debe crear o configurar un servidor virtual de administración de tráfico y asociar el servidor virtual de autenticación con él. Puede utilizar un servidor virtual de equilibrio de carga o de conmutación de contenido para un servidor virtual de administración de tráfico.
Para obtener más información sobre cómo crear y configurar cualquiera de los tipos de servidor virtual, consulte la *Guía de administración de tráfico de Citrix Traffic Management* en Traffic Management.

> **Nota:**
>
> El FQDN del servidor virtual de administración de tráfico debe estar en el mismo dominio que el FQDN del servidor virtual de autenticación para que la cookie de sesión de dominio funcione correctamente.

Para configurar un servidor virtual de administración de tráfico para la autenticación, autorización y auditoría, habilite la autenticación y, a continuación, asigne el FQDN del servidor de autenticación al servidor virtual de administración de tráfico. También puede configurar el dominio de autenticación en el servidor virtual de administración de tráfico actualmente. Si no configura esta opción, el dispositivo Citrix ADC asigna al servidor virtual de administración de tráfico un FQDN que consiste en el FQDN del servidor virtual de autenticación sin la parte del nombre de host. Por ejemplo, si el nombre de dominio del servidor virtual de autenticación es tm.xyz.bar.com, el dispositivo asigna xyz.bar.com. como dominio de autenticación.

Para configurar un servidor virtual de administración del tráfico mediante la CLI

En el símbolo del sistema, escriba uno de los siguientes conjuntos de comandos:

```
set lb vserver <name>  -authentication ON -authenticationhost <FQDN> [-
    authenticationdomain <authdomain>]
show lb vserver <name>
set cs vserver <name>  -authentication ON -authenticationhost <FQDN> [-
    authenticationdomain <authdomain>]
show cs vserver <name>
<!--NeedCopy-->
```

Ejemplo:


```
1 set lb vserver vs-cont-sw -Authentication ON -AuthenticationHost mywiki
     .index.com Done
2
3 show lb vserver vs-cont-sw vs-cont-sw (0.0.0.0:0) - TCP Type: ADDRESS
     State: DOWN Last state change was at Wed Aug 19 10:03:15 2009 (+410
     ms) Time since last state change: 5 days, 20:00:40.290 Effective
     State: DOWN Client Idle Timeout: 9000 sec Down state flush: ENABLED
     Disable Primary Vserver On Down : DISABLED No. of Bound Services : 0
      (Total) 0 (Active) Configured Method: LEASTCONNECTION Mode: IP
     Persistence: NONE Connection Failover: DISABLED Authentication: ON
     Host: mywiki.index.com
4 Done
5 <!--NeedCopy-->
```

Para configurar un servidor virtual de administración del tráfico mediante la interfaz gráfica de usuario

1. En el panel de navegación, realice una de las acciones siguientes.
   - Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
   - Vaya a **Administración del tráfico > Conmutación de contenido > Servidores virtuales**
   - En el panel de detalles, seleccione el servidor virtual en el que quiere habilitar la autenticación y, a continuación, haga clic en **Modificar**.
   - En el cuadro de texto Dominio, escriba el dominio de autenticación.
   - En el menú **Avanzado** de la derecha, seleccione **Autenticación**.
   - Elija **Autenticación basada en formularios** o **Autenticación basada en 401**y rellene la información de autenticación.
     - En Autenticación basada en formularios, introduzca el FQDN de autenticación (el nombre de dominio completo del servidor de autenticación), el servidor virtual de autenticación (la dirección IP del servidor virtual de autenticación) y el perfil de autenticación (el perfil que se utilizará para la autenticación).
     - Para Autenticación basada en 401, introduzca únicamente el servidor virtual de autenticación y el perfil de autenticación.
   - Haga clic en **OK**. Aparece un mensaje en la barra de estado que indica que el servidor virtual se ha configurado correctamente.

Compatibilidad con protocolos de inicio de sesión simplificados para autenticación, autorización y auditoría

El protocolo de inicio de sesión entre los servidores virtuales de autenticación, autorización y auditoría de administración del tráfico y los servidores virtuales de autenticación, autorización y auditoría se simplifica para utilizar mecanismos internos en lugar de enviar los datos cifrados a través de parámetros de consulta. Con esta función, se impide la repetición de solicitudes.

Configurar DNS

Para que la cookie de sesión de dominio utilizada en el proceso de autenticación funcione correctamente, debe configurar DNS para asignar tanto la autenticación como los servidores virtuales de administración de tráfico a los FQDN del mismo dominio. Para obtener información sobre cómo configurar los registros de direcciones DNS, consulte Sistema de nombres de dominio.

Verificar servidor virtual de autenticación

Después de configurar los servidores virtuales de autenticación y administración del tráfico y antes de crear cuentas de usuario, debe comprobar que ambos servidores virtuales están configurados correctamente y que están en estado UP.

Configurar una autenticación NoAuth mediante la CLI

En el símbolo del sistema, escriba el siguiente comando:

```
show authentication vserver <name>
<!--NeedCopy-->
```

Ejemplo:

```
show authentication vserver Auth-Vserver-2
Auth-Vserver-2 (10.102.29.77:443) - SSL Type: CONTENT
State: UP
Client Idle Timeout: 180 sec
Down state flush: DISABLED
Disable Primary Vserver On Down : DISABLED
Authentication : ON
Current AAA Users: 0
Authentication Domain: myCompany.employee.com
Done
```



```
<!--NeedCopy-->
```

Configurar una autenticación NoAuth mediante la interfaz gráfica de usuario

1. Vaya a **Seguridad > Citrix ADC AAA - Tráfico de aplicaciones > Servidores virtuales**.
   Nota: En Citrix Gateway, vaya a **Citrix Gateway > Servidores virtuales**.
2. Revise la información del panel **Servidores virtuales AAA** para comprobar que la configuración es correcta y que el servidor virtual de autenticación acepta tráfico. Puede seleccionar un servidor virtual específico para ver información detallada en el panel de detalles.

Directivas de autorización

August 20, 2021

Al configurar una directiva de autorización, puede configurarla para permitir o denegar el acceso a los recursos de red de la red interna. Por ejemplo, para permitir que los usuarios tengan acceso a la red 10.3.3.0, utilice la expresión siguiente:

CLIENT.IP.DST.IN_SUBNET(10.3.0.0/16)

Las directivas de autorización se aplican a usuarios y grupos. Después de autenticar un usuario, Citrix Gateway realiza una comprobación de autorización de grupo obteniendo la información de grupo del usuario de un servidor RADIUS, LDAP o TACACS+. Si la información de grupo está disponible para el usuario, Citrix Gateway comprueba los recursos de red permitidos para el grupo.

Para controlar a qué recursos pueden acceder los usuarios, debe crear directivas de autorización. Si no necesita crear directivas de autorización, puede configurar la autorización global predeterminada.

Si crea una expresión dentro de la directiva de autorización que deniegue el acceso a una ruta de archivo, solo puede utilizar la ruta de acceso del subdirectorio y no el directorio raíz. Por ejemplo, use fs.path contiene “dir1dir2” en lugar de fs.path contiene “rootdirdir1dir2”. Si utiliza la segunda versión de este ejemplo, se producirá un error en la directiva.

Después de configurar la directiva de autorización, la enlaza a un usuario o grupo.

De forma predeterminada, las directivas de autorización se validan primero con las directivas vinculadas al servidor virtual y, a continuación, con las directivas enlazadas globalmente. Si vincula una directiva globalmente y quiere que la directiva global tenga prioridad sobre una directiva que vincule a un usuario, grupo o servidor virtual, puede cambiar el número de prioridad de la directiva. Los números de prioridad comienzan en cero. Un número de prioridad más bajo otorga a la directiva mayor prioridad.

Por ejemplo, si la directiva global tiene un número de prioridad de uno y el usuario tiene una prioridad de dos, la directiva de autenticación global se aplica primero.

> **Importante:**
>
> - Las directivas de autorización clásicas se aplican solo en el tráfico TCP.
> - La directiva de autorización avanzada se puede aplicar a todos los tipos de tráfico (TCP/UDP/ICMP/DNS).
>   - To apply policy on UDP/ICMP/DNS traffic, policies must be bound at type UDP_REQUEST, ICMP_REQUEST, and DNS_REQUEST respectively.
>   - While binding, if “type” is not explicitly mentioned or “type” is set to REQUEST, the behavior does not change from earlier builds, that is these policies are applied only to TCP traffic.
>   - The policies bound at UDP_REQUEST do not apply for DNS traffic. For DNS, policies must be explicitly bound to DNS_REQUEST TCP_DNS is similar to other TCP requests.

Para obtener más información sobre las directivas de autorización avanzadas, consulte el artículo https://support.citrix.com/article/CTX232237.

Configurar y enlazar una directiva de autorización

Configurar una directiva de autorización mediante la interfaz gráfica de usuario

1. Vaya a **Citrix Gateway > Directivas > Autorización.**
2. En el panel de detalles, haga clic en **Agregar**.
3. En **Nombre**, escriba un nombre para la directiva.
4. En **Acción**, seleccione **Permitir** o **Denegar**.
5. En **Expresión**, haga clic en **Editor de expresiones**.
6. Para empezar a configurar la expresión, haga clic en **Seleccionar** y elija los elementos necesarios.
7. Haga clic en **Listo** cuando se complete la expresión.
8. Haga clic en **Crear**.

Vincular una directiva de autorización a un usuario mediante la GUI

1. Vaya a **Citrix Gateway > Administración de usuarios.**
2. Haga clic en **Usuarios AAA**.
3. En el panel de detalles, seleccione un usuario y, a continuación, haga clic en **Modificar**.
4. En **Configuración avanzada**, haga clic en **Directivas de autorización**.
5. En la página **Enlace de directivas**, seleccione una directiva o cree una.
6. En **Prioridad**, establezca el número de prioridad.

7. En **Tipo**, seleccione el tipo de solicitud y, a continuación, haga clic en **Aceptar**.

Enlazar una directiva de autorización a un grupo mediante la GUI

1. Vaya a **Citrix Gateway > Administración de usuarios**.
2. Haga clic en **Grupos AAA**.
3. En el panel de detalles, seleccione un grupo y, a continuación, haga clic en **Modificar**.
4. En **Configuración avanzada**, haga clic en **Directivas de autorización**.
5. En la página **Enlace de directivas**, seleccione una directiva o cree una.
6. En **Prioridad**, establezca el número de prioridad.
7. En **Tipo**, seleccione el tipo de solicitud y, a continuación, haga clic en **Aceptar**.

Autorización especifica los recursos de red a los que tienen acceso los usuarios cuando inician sesión en Citrix Gateway. La configuración predeterminada para la autorización es denegar el acceso a todos los recursos de red. Citrix recomienda utilizar la configuración global predeterminada y, a continuación, crear directivas de autorización para definir los recursos de red a los que pueden acceder los usuarios.

Puede configurar la autorización en Citrix Gateway mediante una directiva de autorización y expresiones. Después de crear una directiva de autorización, puede vincularla a los usuarios o grupos configurados en el dispositivo.

Autorización global predeterminada

Para definir los recursos a los que tienen acceso los usuarios en la red interna, puede configurar la autorización global predeterminada. Puede configurar la autorización global permitiendo o denegando el acceso a los recursos de red globalmente en la red interna.

Cualquier acción de autorización global que cree se aplica a todos los usuarios que aún no tengan una directiva de autorización asociada a ellos, ya sea directamente o a través de un grupo. Una directiva de autorización de usuario o grupo siempre anula la acción de autorización global. Si la acción de autorización predeterminada está establecida en Denegar, debe aplicar directivas de autorización para todos los usuarios o grupos para que los recursos de red sean accesibles para esos usuarios o grupos. Este requisito ayuda a mejorar la seguridad.

Para establecer la autorización global predeterminada:

1. En la utilidad de configuración, en la ficha Configuration, en el panel de navegación, expanda Citrix Gateway y, a continuación, haga clic en Global Settings.
2. En el panel de detalles, en Configuración, haga clic en Cambiar configuración global.
3. En la ficha Seguridad, junto a Acción de autorización predeterminada, seleccione Permitir o Denegar y haga clic en Aceptar.

Perfiles de autenticación

January 31, 2022

Cuando quiera que varios servidores virtuales de administración de tráfico utilicen la misma configuración de autenticación, puede crear un perfil de autenticación que especifique el servidor virtual de autenticación, el host de autenticación, el dominio de autenticación y el nivel de autenticación.

Este perfil de autenticación se puede asociar con los servidores virtuales de administración de tráfico relevantes.

Configurar un perfil de autenticación

Configurar un perfil de autenticación mediante la CLI

- Cree el perfil de autenticación y establezca los parámetros necesarios.

  Por ejemplo, para crear un perfil con un servidor virtual de autenticación denominado “AuthVs”.

```
add authentication authnProfile authProfile1 -authnVsName authVS
   -authenticationHost authnVS.example.com -authenticationDomain
   example.com -authenticationLevel
<!--NeedCopy-->
```

> **Nota:**
>
> El peso o nivel de autenticación depende del servidor virtual al que está vinculado el tráfico. Una sesión que se crea autenticando contra el servidor virtual de administración de tráfico en un nivel determinado no se puede utilizar para acceder al servidor virtual de administración del tráfico en un nivel superior.

- Enlazar el perfil de autenticación a los servidores virtuales de administración de tráfico pertinentes.

  Por ejemplo, para enlazar AuthProfile1 a un servidor virtual de equilibrio de carga denominado “vserver1”.

```
set lb vserver vserver1 -authnProfile authProfile1
<!--NeedCopy-->
```


Configurar un perfil de autenticación mediante la interfaz gráfica de usuario

En la ficha **Configuración**, vaya a **Seguridad > AAA: Tráfico de aplicaciones > Perfil de autenticación** y configure el perfil de autenticación según sea necesario.

> **Nota:**
>
> - Puede crear un perfil de autenticación mediante también el asistente de Citrix Gateway. El perfil contiene toda la configuración de la directiva de autenticación. Configurar el perfil al crear la directiva de autenticación.
> - Con el asistente de Citrix Gateway, puede utilizar el tipo de autenticación elegido para configurar la autenticación. Si quiere configurar otras directivas de autenticación después de ejecutar el asistente, puede utilizar la utilidad de configuración. Para obtener más información sobre el asistente de Citrix Gateway, consulte Configuración de la configuración mediante Citrix Gateway Wizard].

Directivas de autenticación

February 19, 2022

Cuando los usuarios inician sesión en el dispositivo Citrix ADC o Citrix Gateway, se autentican de acuerdo con una directiva que cree. Una directiva de autenticación comprende una expresión y una acción. Las directivas de autenticación utilizan expresiones Citrix ADC.

Después de crear una acción de autenticación y una directiva de autenticación, enlácela a un servidor virtual de autenticación y asígnele una prioridad. Cuando lo vincule, desígnelo también como directiva primaria o secundaria. Las directivas primarias se evalúan antes que las directivas secundarias. En configuraciones que usan ambos tipos de directivas, las directivas principales suelen ser directivas más específicas, mientras que las directivas secundarias suelen ser directivas más generales. Su objetivo es gestionar la autenticación de cualquier cuenta de usuario que no cumpla con los criterios más específicos. La directiva define el tipo de autenticación. Una única directiva de autenticación se puede utilizar para necesidades de autenticación sencillas y suele estar vinculada a nivel global. También puede utilizar el tipo de autenticación predeterminado, que es local. Si configura la autenticación local, también debe configurar usuarios y grupos en el dispositivo.

Puede configurar varias directivas de autenticación y vincularlas para crear un procedimiento de autenticación detallado y servidores virtuales. Por ejemplo, puede configurar la autenticación en cascada y en dos fases mediante la configuración de varias directivas. También puede establecer la prioridad de las directivas de autenticación para determinar qué servidores y el orden en que el dispositivo comprueba las credenciales de los usuarios. Una directiva de autenticación incluye una expresión y una acción. Por ejemplo, si establece la expresión en True value, cuando los usuarios inician sesión,

la acción evalúa el inicio de sesión del usuario como true y, a continuación, los usuarios tienen acceso a los recursos de red.

Después de crear una directiva de autenticación, la vincula a nivel global o a servidores virtuales. Cuando vincula al menos una directiva de autenticación a un servidor virtual, las directivas de autenticación enlazadas al nivel global no se utilizan cuando los usuarios inician sesión en el servidor virtual, a menos que el tipo de autenticación global tenga una prioridad más alta que la directiva enlazada al servidor virtual.

Cuando un usuario inicia sesión en el dispositivo, la autenticación se evalúa en el siguiente orden:

- Se comprueba si hay directivas de autenticación vinculadas en el servidor virtual.
- Si las directivas de autenticación no están enlazadas al servidor virtual, el dispositivo comprueba las directivas de autenticación globales.
- Si una directiva de autenticación no está vinculada a un servidor virtual ni de forma global, el usuario se autentica mediante el tipo de autenticación predeterminado.

Si configura directivas de autenticación LDAP y RADIUS y quiere enlazar las directivas de forma global para la autenticación de dos factores, puede seleccionar la directiva en la utilidad de configuración y, a continuación, seleccionar si la directiva es el tipo de autenticación principal o secundaria. También puede configurar una directiva de extracción de grupos.

> **Nota:**
>
> El dispositivo Citrix ADC o Citrix Gateway codifican solo caracteres UTF-8 para la autenticación y no son compatibles con los servidores que usan caracteres ISO-8859-1.

Crear una directiva de autenticación

Crear una directiva de autenticación mediante la interfaz gráfica de usuario

1. Vaya a **Seguridad > AAA - Tráfico de aplicaciones > Directivas > Autenticación**y, a continuación, seleccione el tipo de directiva que quiere crear.
   Para Citrix Gateway, vaya a **Citrix Gateway > Directivas > Autenticación**.
2. En el panel de detalles, en la ficha **Directivas**, realice una de las siguientes acciones:
   - Para crear una nueva directiva, haga clic en **Agregar**.
   - Para modificar una directiva existente, seleccione la acción y, a continuación, haga clic en **Modificar**.
3. En el cuadro de diálogo Crear directiva de autenticación o Configurar directiva de autenticación, escriba o seleccione los valores de los parámetros.
   - **Nombre: nombre** de la directiva (no se puede cambiar para una acción configurada previamente)

- **Tipo de autenticación** — `authtype`
- **Servidor** — `authVsName`
- **Expresión**: Regla (para introducir expresiones, primero debe elegir el tipo de expresión en la lista desplegable situada más a la izquierda, debajo de la ventana Expresión y, a continuación, escribir la expresión directamente en el área de texto de la expresión o hacer clic en Agregar para abrir el cuadro de diálogo Agregar expresión y utilizar el menú desplegable listas en él para construir su expresión.)

4. Haga clic en **Crear** o **Aceptar**. La directiva que creó aparece en la página Directivas.
5. Haga clic en la ficha **Servidores** y, en el panel de detalles, realice una de las siguientes acciones:
   - Para usar un servidor existente, selecciónelo y, a continuación, haga clic en.
   - Para crear un servidor, haga clic en Agregar y siga las instrucciones.
6. Si quiere designar esta directiva como directiva de autenticación secundaria, en la ficha Autenticación, haga clic en Secundaria. Si quiere designar esta directiva como directiva de autenticación principal, omita este paso.
7. Haga clic en **Insertar directiva**.
8. Elija la directiva que quiere vincular al servidor virtual de autenticación en la lista desplegable.
9. En la columna **Prioridad** de la izquierda, modifique la prioridad predeterminada para asegurarse de que la directiva se evalúa en el orden correcto.
10. Haga clic en **OK**. Aparece un mensaje en la barra de estado que indica que la directiva se ha configurado correctamente.

Modificar una directiva de autenticación mediante la interfaz gráfica de usuario

Puede modificar las directivas y los perfiles de autenticación configurados, como la dirección IP del servidor de autenticación o la expresión.

1. En la utilidad de configuración, en la ficha Configuración, expanda **Citrix Gateway > Directivas > Autenticación**.
   Nota: También puede configurar la directiva desde **Seguridad > AAA - Tráfico de aplicaciones > Directivas > Autenticación**y, a continuación, seleccionar el tipo de directiva que quiere modificar.
2. En el panel de navegación, en Autenticación, seleccione un tipo de autenticación.
3. En el panel de detalles, en la ficha Servidores, seleccione un servidor y, a continuación, haga clic en Abrir.

Eliminar una directiva de autenticación mediante la interfaz gráfica de usuario

Si ha cambiado o quitado un servidor de autenticación de la red, quite la directiva de autenticación correspondiente de Citrix Gateway.

1. En la utilidad de configuración, en la ficha Configuración, expanda **Citrix Gateway > Directivas > Autenticación**.
   Nota: Para configurar desde ADC, vaya a **Seguridad > AAA - Tráfico de aplicaciones > Directivas > Autenticación**y, a continuación, seleccione el tipo de directiva que quiere eliminar.
2. En el panel de navegación, en Autenticación, seleccione un tipo de autenticación.
3. En el panel de detalles, en la ficha Directivas, seleccione una directiva y, a continuación, haga clic en Quitar.

Crear una directiva de autenticación mediante la CLI

En el símbolo del sistema, escriba los comandos siguientes:

```
add authentication negotiatePolicy <name> <rule> <reqAction>

show authentication localPolicy <name>

bind authentication vserver <name> -policy <policyname> [-priority <
    priority>][-secondary]]

show authentication vserver <name>
<!--NeedCopy-->
```

Ejemplo:

```
add authentication localPolicy Authn-Pol-1 ns_true
Done

show authentication localPolicy
1)      Name: Authn-Pol-1       Rule: ns_true          Request action:
    LOCAL   Done

bind authentication vserver Auth-Vserver-2 -policy Authn-Pol-1
Done

show authentication vserver Auth-Vserver-2
Auth-Vserver-2 (10.102.29.77:443) - SSL Type: CONTENT State: UP Client
    Idle
```



```
Timeout: 180 sec Down state flush: DISABLED
Disable Primary Vserver On Down : DISABLED
Authentication : ON
Current AAA Users: 0
Authentication Domain: myCompany.employee.com
1)  Primary authentication policy name:  Authn-Pol-1 Priority: 0
Done
<!--NeedCopy-->
```

Modificar una directiva de autenticación mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para modificar una directiva de autenticación existente:

```
set authentication localPolicy <name> <rule> [-reqaction <action>]
<!--NeedCopy-->
```

Ejemplo

```
set authentication localPolicy Authn-Pol-1 'ns_true'
<!--NeedCopy-->
```

Eliminar una directiva de autenticación mediante la CLI

En el símbolo del sistema, escriba el siguiente comando para eliminar una directiva de autenticación:

```
rm authentication localPolicy <name>
<!--NeedCopy-->
```

Ejemplo

```
rm authentication localPolicy Authn-Pol-1
<!--NeedCopy-->
```


Enlazar una directiva de autenticación

Después de configurar las directivas de autenticación, la vincula de forma global o a un servidor virtual. Puede utilizar la utilidad de configuración para enlazar una directiva de autenticación.

Para vincular una directiva de autenticación de forma global mediante la utilidad de configuración:

1. En la utilidad de configuración, en la ficha Configuración, expanda **Citrix Gateway > Directivas > Autenticación**.
   Nota: Para configurar desde ADC, vaya a **Seguridad > AAA - Tráfico de aplicaciones > Directivas > Autenticación**
2. Haga clic en un tipo de autenticación.
3. En el panel de detalles, en la ficha Directivas, haga clic en un servidor y, a continuación, en Acción, haga clic en **Enlaces globales**.
4. En la ficha Primaria o Secundaria, en Detalles, haga clic en **Insertar directiva**.
5. En Nombre de directiva, seleccione la directiva y, a continuación, haga clic en **Aceptar**.

   Nota: Al seleccionar la directiva, Citrix Gateway establece la expresión en True value automáticamente.

Para desvincular una directiva de autenticación global mediante la utilidad de configuración:

1. En la utilidad de configuración, en la ficha Configuración, expanda **Citrix Gateway > Directivas > Autenticación**.
   Nota: Para configurar desde ADC, vaya a **Seguridad > AAA - Tráfico de aplicaciones > Directivas > Autenticación**
2. En la ficha Directivas, en Acción, haga clic en **Enlaces globales**.
3. En el cuadro de diálogo Vincular/desvincular directivas de autenticación a globales, en la ficha Primaria o Secundaria, en Nombre de directiva, seleccione la directiva, haga clic en **Desvincular directiva**y, a continuación, haga clic en **Aceptar**.

Agregar una acción de autenticación

Agregar una acción de autenticación mediante la CLI

Si no usa la autenticación LOCAL, debe agregar una acción de autenticación explícita. En el símbolo del sistema, escriba el siguiente comando:

```
add authentication tacacsAction <name> -serverip <IP> [-serverPort <
    port>][-authTimeout <positive_integer>][ ... ]
<!--NeedCopy-->
```


Ejemplo

```
add authentication tacacsaction Authn-Act-1 -serverip 10.218.24.65 -
    serverport 1812 -authtimeout 15 -tacacsSecret ”minotaur” -
    authorization OFF -accounting ON -auditFailedCmds OFF -
    defaultAuthenticationGroup ”users”
<!--NeedCopy-->
```

Configurar una acción de autenticación mediante la CLI

Para configurar una acción de autenticación existente, en el símbolo del sistema, escriba el siguiente comando:

```
set authentication tacacsAction <name> -serverip <IP> [-serverPort <
    port>][-authTimeout <positive_integer>][ ... ]
<!--NeedCopy-->
```

Ejemplo

```
set authentication tacacsaction Authn-Act-1 -serverip 10.218.24.65 -
    serverport 1812 -authtimeout 15 -tacacsSecret ”minotaur” -
    authorization OFF -accounting ON -auditFailedCmds OFF -
    defaultAuthenticationGroup ”users”
<!--NeedCopy-->
```

Eliminar una acción de autenticación mediante la interfaz de línea de comandos

Para eliminar una acción RADIUS existente, en el símbolo del sistema, escriba el siguiente comando:

```
rm authentication radiusAction <name>
<!--NeedCopy-->
```

Ejemplo

```
rm authentication tacacsaction Authn-Act-1
<!--NeedCopy-->
```


La autenticación noAuth

El dispositivo Citrix ADC admite la capacidad de autenticación noAuth que permite al cliente configurar un parámetro defaultAuthenticationGroup en el comando `noAuthAction`, cuando un usuario ejecuta esta directiva. El administrador puede comprobar la presencia de este grupo en el grupo del usuario para determinar la navegación del usuario a través de la directiva noAuth.

Para configurar una autenticación noAuth mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba;

```
add authentication noAuthAction <name> [-defaultAuthenticationGroup <
    string>]
<!--NeedCopy-->
```

Ejemplo

```
add authentication noAuthAction noauthact  - defaultAuthenticationGroup
    mynoauthgroup
<!--NeedCopy-->
```

Tipos de autenticación globales predeterminados

Al instalar Citrix Gateway y ejecutar el asistente de Citrix Gateway, configuró la autenticación en el asistente. Esta directiva de autenticación está vinculada automáticamente al nivel global de Citrix Gateway. El tipo de autenticación que configura en el asistente de Citrix Gateway es el tipo de autenticación predeterminado. Puede cambiar el tipo de autorización predeterminado ejecutando de nuevo el asistente de Citrix Gateway o modificar la configuración de autenticación global en la utilidad de configuración.

Si necesita agregar otros tipos de autenticación, puede configurar directivas de autenticación en Citrix Gateway y vincular las directivas a Citrix Gateway mediante la utilidad de configuración. Al configurar la autenticación de forma global, se define el tipo de autenticación, se configuran los valores y se establece el número máximo de usuarios que se pueden autenticar.

Después de configurar y vincular la directiva, puede establecer la prioridad para definir qué tipo de autenticación tiene prioridad. Por ejemplo, se configuran las directivas de autenticación LDAP y RADIUS. Si la directiva LDAP tiene un número de prioridad de 10 y la directiva RADIUS tiene un número de prioridad de 15, la directiva LDAP tiene prioridad, independientemente de dónde vincule cada directiva. Esto se denomina autenticación en cascada.

Puede elegir entregar páginas de inicio de sesión desde la memoria caché en memoria de Citrix Gateway o desde el servidor HTTP que se ejecuta en Citrix Gateway. Si elige entregar la página de inicio de sesión desde la memoria caché en memoria, la entrega de la página de inicio de sesión desde Citrix Gateway es más rápida que desde el servidor HTTP. La elección de entregar la página de inicio de sesión desde la memoria caché en memoria reduce el tiempo de espera cuando muchos usuarios inician sesión al mismo tiempo. Solo puede configurar la entrega de páginas de inicio de sesión desde la caché como parte de una directiva de autenticación global.

También puede configurar la dirección IP de traducción de direcciones de red (NAT) que es una dirección IP específica para la autenticación. Esta dirección IP es única para la autenticación y no es la subred de Citrix Gateway, las direcciones IP asignadas ni las direcciones IP virtuales. Este es un parámetro opcional.

> **Nota:**
>
> - No puede usar el asistente de Citrix Gateway para configurar la autenticación SAML.
> - Puede utilizar el Asistente de configuración rápida para configurar la autenticación de certificados de cliente, LDAP y RADIUS. Al ejecutar el asistente, puede seleccionar entre un servidor LDAP o RADIUS existente configurado en Citrix Gateway. También puede configurar los ajustes de LDAP o RADIUS. Si utiliza la autenticación de dos factores, Citrix recomienda utilizar LDAP como tipo de autenticación principal.

Configurar los tipos de autenticación globales predeterminados

1. En la GUI, en la ficha Configuración, en el panel de navegación, expanda **Citrix Gateway y,** a continuación, haga clic en **Configuración global**.
2. En el panel de detalles, en Configuración, haga clic en **Cambiar la configuración de autenticación**.
3. En **Número máximo de usuarios**, escriba el número de usuarios que se pueden autenticar mediante este tipo de autenticación.
4. En **Dirección IP NAT**, escriba la dirección IP única para la autenticación.
5. Seleccione Activar almacenamiento en**caché estático para entregar las páginas de inicio de sesión más rápido**.
6. Seleccione **Habilitar comentarios de autenticación mejorada para enviar un mensaje a los usuarios si la autenticación falla**. El mensaje que reciben los usuarios incluye los errores de contraseña, la cuenta inhabilitada o bloqueada, o el usuario no se encuentra, por nombrar algunos.
7. En **Tipo de autenticación predeterminado**, seleccione el tipo de autenticación.
8. Configure los ajustes de su tipo de autenticación y, a continuación, haga clic en **Aceptar**.

Función para recuperar los intentos de inicio de sesión actuales para un usuario

El dispositivo Citrix ADC proporciona una opción para recuperar el valor de los intentos de inicio de sesión actuales de un usuario mediante una nueva expresión `aaa.user.login_attempts`. La expresión acepta un argumento (nombre de usuario) o ningún argumento. Si no hay ningún argumento, la expresión obtiene el nombre de usuario de `aaa_session` o `aaa_info`.

Puede usar la expresión `aaa.user.login_attempts` con directivas de autenticación para su posterior procesamiento.

Para configurar el número de intentos de inicio de sesión por usuario mediante la CLI

En el símbolo del sistema, escriba:

```
add expression er aaa.user.login_attempts
```

Grupos y usuarios

August 20, 2021

Después de configurar la configuración básica de autenticación, autorización y auditoría, se crean usuarios y grupos. Primero debe crear una cuenta de usuario para cada persona que se autentica a través del dispositivo Citrix ADC. Si utiliza autenticación local controlada por el propio dispositivo Citrix ADC, cree cuentas de usuario locales y asigne contraseñas a cada una de esas cuentas.

También puede crear cuentas de usuario en el dispositivo Citrix ADC si utiliza un servidor de autenticación externo. Sin embargo, en este caso, cada cuenta de usuario debe coincidir exactamente con una cuenta para ese usuario en el servidor de autenticación externo y no debe asignar contraseñas a las cuentas de usuario que cree en Citrix ADC. El servidor de autenticación externo administra las contraseñas de los usuarios que se autentican con el servidor de autenticación externo.

Si utiliza un servidor de autenticación externo, puede crear cuentas de usuario locales en el dispositivo Citrix ADC si, por ejemplo, quiere permitir que los usuarios temporales (como los visitantes) inicien sesión pero no quiere crear entradas para esos usuarios en el servidor de autenticación. Asigna una contraseña a cada cuenta de usuario local, tal como lo haría si estuviera mediante la autenticación local para todas las cuentas de usuario.

Cada cuenta de usuario debe estar vinculada a directivas de autenticación y autorización. Para simplificar esta tarea, puede crear uno o más grupos y asignarles cuentas de usuario. A continuación, puede enlazar directivas a grupos en lugar de cuentas de usuario individuales.

Configurar directivas con grupos

Después de configurar los grupos, puede utilizar el cuadro de diálogo **Grupo** para aplicar directivas y opciones que especifican el acceso de los usuarios. Si utiliza la autenticación local, cree usuarios y los agregue a grupos configurados en Citrix Gateway. A continuación, los usuarios heredan la configuración de ese grupo.

Puede configurar las siguientes directivas u opciones para un grupo de usuarios en el cuadro de diálogo **Grupo** :

- Usuarios
- Directivas de autorización
- Directivas de auditoría
- Directivas de sesión
- Directivas de tráfico
- Marcadores
- Aplicaciones de intranet
- Direcciones IP de intranet

En la configuración, es posible que tenga usuarios que pertenezcan a más de un grupo. Además, cada grupo puede tener una o más directivas de sesión enlazadas, con diferentes parámetros configurados. Los usuarios que pertenecen a más de un grupo heredan las directivas de sesión asignadas a todos los grupos a los que pertenece el usuario. Para asegurarse de que la evaluación de directivas de sesión tiene prioridad sobre la otra, debe establecer la prioridad de la directiva de sesión.

Por ejemplo, tiene group1 enlazado con una directiva de sesión configurada con la página principal www.homepage1.com. Group2 está vinculado con una directiva de sesión configurada con la página principal www.homepage2.com. Cuando estas directivas están enlazadas a grupos respectivos sin un número de prioridad o con un mismo número de prioridad, la página principal que aparece a los usuarios que pertenecen a ambos grupos depende de la directiva que se procese primero. Al establecer un número de prioridad más bajo, que da mayor prioridad, para la directiva de sesión con la página principal www.homepage1.com, puede asegurarse de que los usuarios que pertenecen a ambos grupos reciban la página principal www.homepage1.com.

Si las directivas de sesión no tienen asignado un número de prioridad o tienen el mismo número de prioridad, la prioridad se evalúa en el orden siguiente:

- Usuario
- Grupo
- Servidor virtual
- Global

Si las directivas están enlazadas al mismo nivel, sin un número de prioridad o si las directivas tienen el mismo número de prioridad, el orden de evaluación es según el orden de enlace de directiva. Las

directivas que están enlazadas primero a un nivel reciben prioridad sobre las directivas enlazadas más adelante.

Si tenemos un usuario vinculado a varios grupos con cada grupo con IIP enlazado, el usuario puede obtener IP libre de cualquiera de los grupos enlazados.

Crear usuarios y grupos

Configurar la autenticación, la autorización y la auditoría de usuarios locales mediante la GUI

1. Vaya a **Seguridad > AAA: Tráfico de aplicaciones > Usuarios**
   de Citrix Gateway, expanda **Citrix Gateway > Administración de usuarios**y, a continuación, haga clic en **Usuarios AAA**.
2. En el panel de detalles, realice una de las acciones siguientes:
   - Para crear una nueva cuenta de usuario, haga clic en **Agregar**.
   - Para modificar una cuenta de usuario existente, seleccione la cuenta de usuario y, a continuación, haga clic en **Abrir**.
3. En el cuadro de diálogo **Crear usuario AAA**, en el cuadro de texto **Nombre de usuario**, escriba un nombre para el usuario.
4. Si crea una cuenta de usuario autenticada localmente, desactive la casilla **Autenticación externa** y proporcione una contraseña local que el usuario utilice para iniciar sesión.
5. Haga clic en **Crear** o **Aceptar**y, a continuación, en **Cerrar**. Aparece un mensaje en la barra de estado que indica que el usuario se ha configurado correctamente.

Configure la autenticación, la autorización y la auditoría de grupos locales y agregue usuarios a ellos mediante la utilidad de configuración

1. Vaya a **Seguridad > AAA: Tráfico de aplicaciones > Grupos**
   de Citrix Gateway, expanda **Citrix Gateway > Administración de usuarios**y, a continuación, haga clic en **Grupos AAA**.
2. En el panel de detalles, realice una de las acciones siguientes:
   - Para crear un nuevo grupo, haga clic en **Agregar**.
   - Para modificar un grupo existente, selecciónelo y, a continuación, haga clic en **Modificar**.
3. Si va a crear un grupo nuevo, en el cuadro de diálogo **Crear grupo AAA**, en el cuadro de texto **Nombre de grupo**, escriba un nombre para el grupo.
4. En el área **Avanzadas** a la derecha, haga clic en **Usuarios AAA**.
   - Para agregar un usuario al grupo, selecciónelo y, a continuación, haga clic en **Agregar**.

- Para quitar un usuario del grupo, selecciónelo y, a continuación, haga clic en **Quitar**.
- Para crear una nueva cuenta de usuario y agregarla al grupo, haga clic en el icono **Plus** y, a continuación, siga las instrucciones de "Para configurar la autenticación, la autorización y la auditoría de los usuarios locales mediante la utilidad de configuración".

5. Haga clic en **Crear** o **Aceptar**. El grupo que ha creado aparece en la página **Grupos AAA**.

Eliminar un grupo mediante la interfaz gráfica de usuario

También puede eliminar grupos de usuarios de Citrix Gateway.

1. Vaya a **Seguridad > AAA: Tráfico de aplicaciones > Grupos**
   desde Citrix Gateway, ExpandCitrix **Gateway > Administración de usuarios y,** a continuación, haga clic en **Grupos AAA**.
   En el panel de detalles, seleccione el grupo y, a continuación, haga clic en Quitar.

Configurar la autenticación, la autorización y la auditoría de usuarios locales mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos:

```
add aaa group <groupname>

bind aaa group <groupname> -username <username>
<!--NeedCopy-->
```

Ejemplo:

```
add aaa group group-2

bind aaa group group-2 -username user-2
<!--NeedCopy-->
```

Quitar usuarios de un grupo de autenticación, autorización y auditoría mediante la interfaz de línea de comandos

En el símbolo del sistema, desenlazar usuarios del grupo escribiendo el siguiente comando una vez para cada cuenta de usuario enlazada al grupo:

```
unbind aaa group <groupname> -username <username><!--NeedCopy-->
```



```
**Ejemplo:**

<!--NeedCopy-->
```

unbind aaa group group-hr -username user-hr-1

```
### Quitar un grupo de autenticación, autorización y auditoría mediante
    la interfaz de línea de comandos

Primero elimine todos los usuarios del grupo. A continuación, en el sí
   mbolo del sistema, escriba el siguiente comando para quitar un grupo
    Citrix ADC AAA y verificar la configuración:

<!--NeedCopy-->
```

rm aaa group

```
**Ejemplo:**

<!--NeedCopy-->
```

rm aaa group group-hr

```
> **Nota**
>
>No se puede agregar un nombre de usuario con dominio si el nombre de
   usuario ya se ha agregado sin dominio. Si el nombre de usuario con
   dominio se agrega primero seguido del mismo nombre de usuario sin
   dominio, el dispositivo Citrix ADC agrega el nombre de usuario a la
   lista de usuarios.

En el ejemplo siguiente se muestra que no se permite agregar un nombre
   de usuario con dominio si se agrega el mismo nombre de usuario sin
   dominio.

<!--NeedCopy-->
```



```
add aaa user u47985
Done
show aaa users
1) UserName: u47985
Done
add aaa user u47985@domain.com
ERROR: User already exists
```

En el ejemplo siguiente se muestra si el nombre de usuario con dominio se agrega primero seguido del mismo nombre de usuario sin dominio, el dispositivo Citrix ADC agrega el nombre de usuario a la lista de usuarios.

```
> add aaa user u47985@domain.com
Done
> add aaa user u47985
Done
> sh aaa user
1)   UserName: u47985@domain.com
2)   UserName: u47985
```

Métodos de autenticación

August 20, 2021

El dispositivo Citrix ADC puede autenticar usuarios con cuentas de usuario locales o mediante un servidor de autenticación externo. El dispositivo admite los siguientes tipos de autenticación:

- **LOCAL:** se autentica en el dispositivo Citrix ADC mediante una contraseña, sin referencia a un servidor de autenticación externo. Los datos de usuario se almacenan localmente en el dispositivo Citrix ADC.
- **RADIUS:** Autenticar en un servidor RADIUS externo.
- **LDAP:** se autentica en un servidor de autenticación LDAP externo.
- **TACACS:** se autentica en un servidor de autenticación externo del sistema de control de acceso del controlador de acceso de terminal (TACACS).
- **CERT:** se autentica en el dispositivo Citrix ADC mediante un certificado de cliente, sin referencia a un servidor de autenticación externo.

- **NEGOCIATE:** se autentica en un servidor de autenticación Kerberos. Si hay un error en la autenticación Kerberos, Citrix ADC utiliza la autenticación NTLM.
- **SAML:** se autentica en un servidor que admite el lenguaje de marcado de aserción de seguridad (SAML).
- **SAML IDP:** configura Citrix ADC para que funcione como proveedor de identidades (IdP) de lenguaje de marcado de aserción de seguridad (SAML).
- **WEB:** se autentica en un servidor web, proporcionando las credenciales que requiere el servidor web en una solicitud HTTP y analiza la respuesta del servidor web para determinar que la autenticación del usuario se realizó correctamente.
- **OTP nativo:** el dispositivo Citrix ADC admite contraseñas de un solo uso (OTP) sin tener que utilizar un servidor de terceros.
- **Notificación push:** Citrix Gateway admite notificaciones push para OTP. Los usuarios no tienen que introducir manualmente el OTP recibido en sus dispositivos registrados para iniciar sesión en Citrix Gateway. Los administradores pueden configurar Citrix Gateway de modo que las notificaciones de inicio de sesión se envíen a los dispositivos registrados de los usuarios mediante servicios de notificación push.
- **Email OTP:** el método Email OTP le permite autenticarse mediante la contraseña de un solo uso (OTP) que se envía a la dirección de correo electrónico registrada. Cuando intenta autenticarse en cualquier servicio, el servidor envía una OTP a la dirección de correo electrónico registrada del usuario.
- **Autenticación reCAPTCHA**: Citrix Gateway admite una nueva acción de primera clase 'CaptChaAction' que simplifica la configuración de reCAPTCHA. Como reCAPTCHA es una acción de primera clase, puede ser un factor propio. Puede inyectar reCAPTCHA en cualquier lugar del flujo de nFactor.
- **Autenticación de nFactor:** La autenticación multifactor mejora la seguridad de una aplicación al requerir a los usuarios que proporcionen varias pruebas de identificación para obtener acceso. El dispositivo Citrix ADC proporciona un enfoque extensible y flexible para configurar la autenticación multifactor. Este enfoque se denomina autenticación nFactor.
- **Autenticación OAuth:** la autenticación OAuth autoriza y autentica a los usuarios en servicios alojados en aplicaciones como Google, Facebook y Twitter.

Autentificación nFactor

December 2, 2021

> **Importante**
>
> - La autenticación nFactor se admite desde NetScaler 11.0 Build 62.x en adelante.
> - Para que la autenticación nFactor funcione con Citrix ADC, se requiere una licencia Advanced o una licencia Premium.
> - A partir de la versión 13.0 compilación 67.x, la autenticación de nFactor se admite con licencia estándar solo para el servidor virtual Gateway/VPN. Para obtener más información sobre la autenticación nFactor con Citrix Gateway, consulte nFactor for Gateway Authentication.
> - La autenticación nFactor no es compatible con el cliente Linux.

La autenticación multifactor mejora la seguridad de una aplicación al requerir que los usuarios proporcionen múltiples pruebas de identidad para obtener acceso. El dispositivo Citrix ADC proporciona un enfoque extensible y flexible para configurar la autenticación multifactor. Este enfoque se denomina *autenticación nFactor*.

Cómo funciona la autenticación nFactor

Cada factor de autenticación realiza las siguientes tareas:

- Recopila las credenciales del usuario. Los mecanismos de autenticación compatibles con Citrix ADC incluyen LDAP, RADIUS, aserción SAML, certificado de cliente, OAuth OpenID Connect, Kerberos, etc.
- Evalúa las credenciales proporcionadas para decidir si la autenticación se realizó correctamente, falló o si se realizarán acciones como la extracción de grupo o la extracción de atributos.
- En función de los resultados de la evaluación, el acceso se concede, se deniega o se selecciona un factor siguiente.
- Repita estos pasos hasta que no haya más factores que evaluar.

Con la autenticación nFactor puede:

- Configure cualquier número de factores de autenticación.
- Basar la selección del siguiente factor en el resultado de la ejecución del factor anterior.
- Personaliza la interfaz de inicio de sesión Por ejemplo, puede personalizar los nombres de las etiquetas, los mensajes de error y el texto de ayuda.
- Extraiga la información del grupo de usuarios sin realizar la autenticación.
- Configure PassThrough para un factor de autenticación. Esto significa que no se requiere ninguna interacción de inicio de sesión explícita para ese factor.
- Configure el orden en que se aplican los diferentes tipos de autenticación. Cualquiera de los mecanismos de autenticación admitidos en el dispositivo Citrix ADC se puede configurar como

cualquier factor de la configuración de la autenticación nFactor. Estos factores se ejecutan en el orden en que se configuran.

- Configure Citrix ADC para que proceda a un factor de autenticación que se debe ejecutar cuando se produce un error en la autenticación. Para ello, configure otra directiva de autenticación con la misma condición exacta, pero con la siguiente prioridad más alta y con la acción establecida en "NO_AUTH". Debe configurar el siguiente factor, que debe especificar el mecanismo de autenticación alternativo que se aplicará.

Cifrado de información de inicio de sesión de Citrix Gateway para la autenticación

Citrix Gateway con autenticación nFactor puede cifrar los campos de solicitud de inicio de sesión enviados por un cliente (explorador o aplicaciones SSO) durante el proceso de autenticación. Los campos de solicitud de inicio de sesión encriptados proporcionan una capa adicional de seguridad para proteger los datos confidenciales del usuario contra la divulgación.

Exploradores compatibles

La siguiente tabla muestra los exploradores junto con los detalles de la versión que admiten el cifrado de inicio de sesión.

Exploradores web	Versión
Chrome	78 y superior
Firefox	69 y superior
Internet Explorer	11
Borde	42 y superior
Safari	11.0 y superior
Ópera	66

Clientes compatibles

La siguiente sección enumera los clientes junto con los detalles de la versión que admiten el cifrado de la información de inicio de sesión de Citrix Gateway.

- La aplicación Citrix Workspace en Mac solo admite el cifrado cuando la versión del sistema operativo es 10.14.x o superior.
- La aplicación Citrix SSO en Mac solo admite el cifrado cuando la versión del sistema operativo es 10.14.x y superior.
- La aplicación SSO de Windows no tiene restricciones de compatibilidad.

- El cifrado de contraseñas en los clientes de la aplicación Citrix Workspace para Windows solo se admite en la versión de Internet Explorer 11.

Para habilitar el cifrado de inicio de sesión mediante la CLI

En el símbolo del sistema, escriba:

```
set aaa parameter [-loginEncryption (ENABLED | DISABLED)]
```

> **Nota**
>
> El parámetro LoginEncryption está DISABLED de forma predeterminada. Debe HABILITARLO.

Para habilitar el cifrado de inicio de sesión mediante la interfaz gráfica de usuario

1. Vaya a **Seguridad > AAA — Tráfico de aplicaciones**, haga clic en **Cambiar la configuración de AAA** de **autenticación en la sección Configuración** de autenticación.
2. En la página **Configurar parámetro AAA**, desplácese hacia abajo hasta la opción **Cifrado de inicio de sesión** y habilite esta opción.

Conceptos, entidades y terminología de nFactor

March 9, 2022

Este tema captura algunas de las principales entidades involucradas en la autenticación de nFactor y su importancia.

Esquema de inicio de sesión

nFactor desacopla la “vista”, la interfaz de usuario, con el “modelo” que es el manejo en tiempo de ejecución. La vista de nFactor está definida por el esquema de inicio de sesión. El esquema de inicio de sesión es una entidad que define lo que ve el usuario y especifica cómo extraer los datos del usuario.

Para definir una vista, el esquema de inicio de sesión apunta a un archivo en el disco que define el formulario de inicio de sesión. Este archivo debe cumplir con la especificación del “Protocolo de formularios comunes de Citrix”. Este archivo es esencialmente una definición XML del formulario de inicio de sesión.

Además del archivo XML, el esquema de inicio de sesión contiene expresiones de directiva avanzadas para obtener el nombre de usuario y la contraseña de la solicitud de inicio de sesión del usuario. Estas

expresiones son opcionales y se pueden omitir si el nombre de usuario y la contraseña del usuario llegan con los nombres de variables de formulario esperados.

El esquema de inicio de sesión también define si el conjunto actual de credenciales se debe usar como credenciales SingleSignOn predeterminadas.

El esquema de inicio de sesión se puede crear ejecutando el siguiente comando de la CLI:

```
1    add authentication loginSchema <name> -authenticationSchema <string>
         [-userExpression <string>] [-passwdExpression <string>] [-
        userCredentialIndex <positive_integer>] [-passwordCredentialIndex
         <positive_integer>] [-authenticationStrength <positive_integer>]
         [-SSOCredentials ( YES | NO )]
2 <!--NeedCopy-->
```

> **Nota:**
>
> **Las credenciales SSOCredentials** indican si las credenciales de los factores actuales son las credenciales SSO predeterminadas. El valor por defecto es NO.
>
> En la configuración de autenticación nFactor, las credenciales del último factor se utilizan para el SSO de forma predeterminada. Al usar la configuración de **SsoCredentials**, se pueden usar las credenciales de factor actuales. En caso de que esta configuración se establezca en diferentes factores, el factor final que tiene esta configuración establecida toma la prioridad.

Para obtener más información sobre cada parámetro, consulte https://developer-docs.citrix.com/projects/citrix-adc-command-reference/en/latest/authentication/authentication-loginSchema/#add-authentication-loginschema.

Etiqueta de directiva

Una etiqueta de directiva es un conjunto de directivas. Es una construcción que no es ajena a la infraestructura de directivas de Citrix ADC. Etiqueta de directiva define un factor de autenticación. Es decir, contiene todas las directivas necesarias para determinar si se cumplen las credenciales del usuario. Todas las directivas de una etiqueta de directiva pueden considerarse homogéneas. La etiqueta de directiva para la autenticación no puede tomar directivas de tipo diferente, por ejemplo, reescribir. En otras palabras, todas las directivas de una etiqueta de directiva validan la misma contraseña/credencial del usuario, en su mayoría. El resultado de las directivas en una policyLabel sigue la condición lógica OR. Por lo tanto, si la autenticación especificada por la primera directiva tiene éxito, se omiten las demás directivas que la siguen.

La etiqueta de directiva se puede crear ejecutando el siguiente comando de la CLI:


```
add authentication policy label mylabel  - loginSchema <>
<!--NeedCopy-->
```

Una etiqueta de directiva toma el esquema de inicio de sesión como propiedad. El esquema de inicio de sesión define la vista de esa etiqueta de directiva. Si no se especifica el esquema de inicio de sesión, se asocia un esquema de inicio de sesión implícito, LSCHEMA_INT, a esa etiqueta de directiva. El esquema de inicio de sesión decide si una etiqueta de directiva se convierte en un acceso directo o no.

Etiqueta de servidor virtual

En la infraestructura de directivas avanzada de Citrix ADC, un servidor virtual también es una etiqueta de directiva implícita. Esto se debe a que el servidor virtual también se puede vincular a más de una directiva. Sin embargo, un servidor virtual es especial porque es el punto de entrada para el tráfico del cliente y puede tomar directivas de un tipo diferente. Cada una de las directivas que pone bajo su propia etiqueta dentro del servidor virtual. Por lo tanto, el servidor virtual es un conglomerado de etiquetas.

Siguiente factor

Siempre que una directiva esté vinculada a un servidor virtual o a una etiqueta de directiva, se puede especificar con el siguiente factor. El siguiente factor determina lo que se debe hacer si una autenticación determinada tiene éxito. Si no hay un factor siguiente, se concluye el proceso de autenticación para ese usuario.

Cada directiva enlazada a un servidor virtual o etiqueta de directiva puede tener un factor siguiente diferente. Esto permite la máxima flexibilidad en la que el éxito de cada directiva puede definir una nueva ruta para la autenticación del usuario. El administrador puede aprovechar este hecho y crear factores de reserva inteligentes para los usuarios que no cumplen ciertas directivas.

Directiva de exclusión de autenticación

nFactor introduce una directiva integrada especial llamada NO_AUTHN. La directiva NO_AUTHN siempre devuelve el éxito como resultado de la autenticación. La directiva `No-auth` se puede crear ejecutando el siguiente comando de la CLI:

```
add authentication policy noauthpolicy  - rule <> -action NO_AUTHN
<!--NeedCopy-->
```


Según el comando, la directiva `no-authentication` toma una regla que puede ser cualquier expresión de directiva avanzada. El resultado de la autenticación siempre es correcto desde NO_AUTHN.

Una directiva `no-auth` en sí misma no parece agregar valor. Sin embargo, cuando se utiliza junto con etiquetas de directivas de paso a través, ofrece una gran flexibilidad para tomar decisiones lógicas para impulsar el flujo de autenticación de usuarios. La directiva NO_AUTHN y los factores de paso ofrecen una nueva dimensión a la flexibilidad de nFactor.

Nota: Consulte los ejemplos que describen el uso de `no-auth` y el acceso directo en las secciones posteriores.

Factor/etiqueta de paso

Una vez que el usuario ha pasado la autenticación en el servidor virtual (para el primer factor), las autenticaciones posteriores se producen en las etiquetas de directiva o en los factores definidos por el usuario (secundarios).
Cada etiqueta/factor de directiva se asocia a una entidad de esquema de inicio de sesión para mostrar la vista de ese factor. Esto permite personalizar las vistas en función de la ruta que el usuario habría tomado para llegar a un factor determinado.

Existen tipos especializados de etiquetas de directiva que no apuntan explícitamente a un esquema de inicio de sesión. Las etiquetas de directivas especializadas apuntan a un esquema de inicio de sesión que en realidad no apunta al archivo XML de la vista. Estas etiquetas/factores de directivas se denominan factores de “transferencia”.

Los factores de acceso directo se pueden crear ejecutando los siguientes comandos de la CLI:

Ejemplo 1:

```
1 add authentication policylabel example1
2 <!--NeedCopy-->
```

Ejemplo 2:

```
1 add loginschema passthrough_schema  - authenticationSchema noschema
2
3 add authentication policylabel example2  - loginschema
     passthrough_schema
4 <!--NeedCopy-->
```

El factor de acceso directo implica que el subsistema de autenticación, autorización y auditoría no debe volver al usuario para obtener la credencial establecida para ese factor. En su lugar, es una

sugerencia para que la autenticación, la autorización y la auditoría continúen con las credenciales ya obtenidas. Esto es útil en casos en los que no se quiere la intervención del usuario. Por ejemplo:

- Cuando al usuario se le presentan dos campos de contraseña, después del primer factor, el segundo factor no necesita la intervención del usuario.
- Cuando se realiza la autenticación de un tipo (por ejemplo, certificado) y el administrador debe extraer grupos para ese usuario.

El factor de paso se puede usar con la directiva `NO_AUTH` para realizar saltos condicionales.

Flujo de autenticación nFactor

La autenticación siempre comienza en el servidor virtual de nFactor. El servidor virtual define el primer factor para el usuario. El servidor virtual sirve el primer formulario que ve el usuario. El formulario de inicio de sesión que ve el usuario se puede personalizar en el servidor virtual mediante directivas de esquema de inicio de sesión. Si no hay directivas de esquema de inicio de sesión, se muestra al usuario un solo campo de nombre de usuario y contraseña.

Si se debe mostrar al usuario más de un campo de contraseña en un formulario personalizado, se deben usar directivas de esquema de inicio de sesión. Permiten mostrar diferentes formularios basados en las reglas configuradas (como usuario de intranet frente al usuario externo, proveedor de servicios A frente al proveedor de servicios B).

Una vez que se publican las credenciales de usuario, la autenticación comienza en el servidor virtual de autenticación, el primer factor. Como el servidor virtual de autenticación se puede configurar con varias directivas, cada una de ellas se evalúa en una secuencia. En cualquier momento dado, si una directiva de autenticación tiene éxito, se toma el siguiente factor especificado contra ella. Si no hay otro factor, el proceso de autenticación finaliza. Si existe el siguiente factor, se comprueba si ese factor es un factor de paso o un factor regular. Si se trata de transferencia, las directivas de autenticación de ese factor se evalúan sin intervención del usuario. De lo contrario, el esquema de inicio de sesión asociado a ese factor se muestra al usuario.

Ejemplo de uso de directivas de factor de paso y sin autenticación para tomar decisiones lógicas

El administrador quiere decidir nextFactor en función de los grupos.

```
1 add authentication policylabel group check
2
3 add authentication policy admin group  -rule http.req.user.is_member_of
    ("Administrators")  -action NO_AUTHN
4
5 add authentication policy nonadmins  -rule true  -action NO_AUTHN
```



```
6
7  bind authentication policy label group check  - policy admingroup  - pri
       1  - nextFactor factor-for-admin
8
9  bind authentication policy label groupcheck  - policy nonadmins  - pri 10
        - nextfactor factor-for-others
10
11 add authentication policy first_factor_policy  - rule <> -action <>
12
13 bind authentication vserver <> -policy first_factor_policy  - priority
       10  - nextFactor groupcheck
14 <!--NeedCopy-->
```

Configuración de la autenticación nFactor

January 21, 2022

Puede configurar varios factores de autenticación mediante la configuración de nFactor. La configuración de nFactor solo se admite en las ediciones Citrix ADC Advanced y Premium.

Métodos para configurar nFactor

Puede configurar la autenticación nFactor mediante uno de los métodos siguientes:

- **nFactor Visualizer:** el visualizador nFactor le permite vincular fácilmente factores o etiquetas de directivas en un solo panel y también cambiar la vinculación de los factores en el mismo panel. Puede crear un flujo nFactor mediante el visualizador y vincular ese flujo a un servidor virtual de autenticación, autorización y auditoría. Para obtener más información sobre nFactor Visualizer y un ejemplo de configuración de nFactor mediante el visualizador, consulte nFactor Visualizer para obtener una configuración simplificada.
- **Citrix ADC GUI:** Para obtener más información, consulte la sección **Elementos de configuración involucrados en la configuración de nFactor**.
- **CLI de Citrix ADC:** Para obtener un fragmento de ejemplo en la configuración de nFactor mediante la CLI de Citrix ADC, consulte Fragmento de ejemplo en la configuración de nFactor mediante la CLI de Citrix ADC.

> **Importante:** Este tema contiene detalles sobre la configuración de nFactor mediante la GUI de Citrix ADC.

Elementos de configuración implicados en la configuración nFactor

Los siguientes elementos participan en la configuración de nFactor. Para ver los pasos detallados, consulte las secciones correspondientes de este tema.

Elemento de configuración	Tareas que deben realizarse
Servidor virtual AAA	Creación de un servidor virtual AAA
	Enlazar el tema del portal al servidor virtual AAA
	Activar autenticación de certificados de cliente
Esquema de inicio de sesión	Configuración de un perfil de esquema de inicio
	Crear y enlazar una directiva de esquema de inicio de sesión
Directivas de autenticación avanzada	Creación de directivas de autenticación avanzadas
	Vincular la directiva de autenticación avanzada de primer factor al servidor virtual AAA de Citrix ADC
	Utilizar grupos LDAP extraídos para seleccionar el siguiente factor de autenticación
Etiqueta de directiva de autenticación	Crear etiqueta de directiva de autenticación
	Etiqueta de directiva de autenticación de enlace
nFactor para Citrix Gateway	Crear perfil de autenticación para vincular un servidor virtual Citrix ADC AAA con el servidor virtual Citrix Gateway
	Configuración de parámetros SSL y certificado de CA para Citrix Gateway
	Configurar directiva de tráfico de Citrix Gateway para el inicio de sesión único de nFactor en StoreFront

Cómo funciona nFactor

Cuando un usuario se conecta al servidor virtual de autenticación, autorización y auditoría o Citrix Gateway, la secuencia de eventos que se producen es la siguiente:

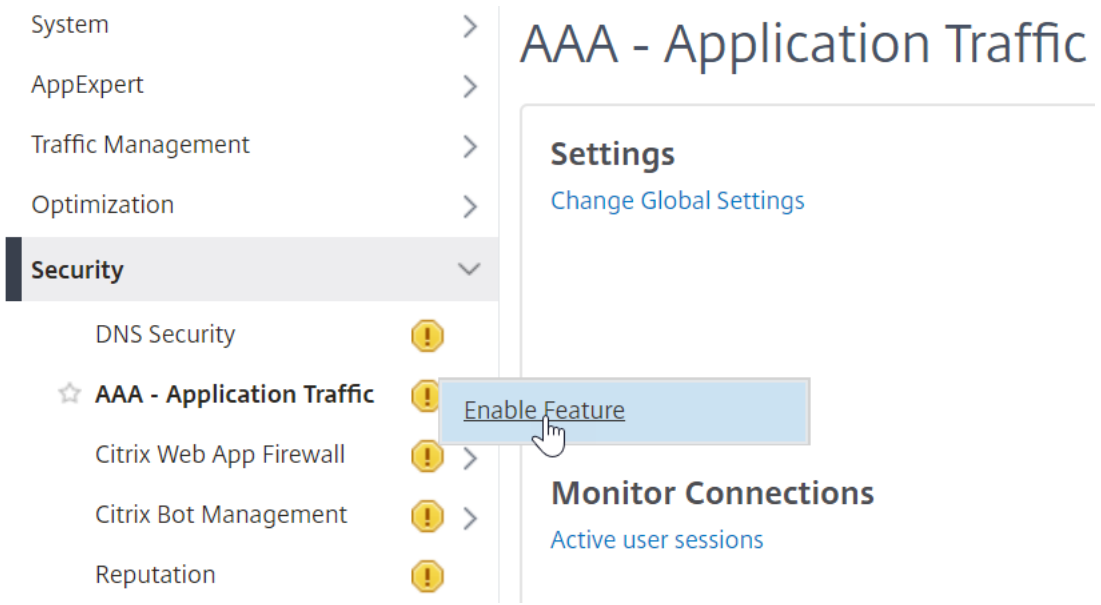
1. Si se utiliza la autenticación basada en formularios, se muestra el esquema de inicio de sesión enlazado al servidor virtual de autenticación, autorización y auditoría.
2. Se evalúan las directivas de autenticación avanzada enlazadas al servidor virtual de autenticación, autorización y auditoría.
    - Si la directiva de autenticación avanzada tiene éxito y si se configura el siguiente factor (etiqueta de directiva de autenticación), se evalúa el siguiente factor. Si Next Factor no está configurado, la autenticación se ha completado y se ha realizado correctamente.
    - Si se produce un error en la directiva de autenticación avanzada y si Goto Expression se establece en Siguiente, se evalúa la siguiente directiva de autenticación avanzada enlazada. Si ninguna de las directivas de autenticación avanzada tiene éxito, se produce un error en la autenticación.
3. Si la etiqueta de directiva de autenticación de siguiente factor tiene un esquema de inicio de sesión enlazado, se muestra al usuario.
4. Se evalúan las directivas de autenticación avanzadas enlazadas a la etiqueta de directiva de autenticación de siguiente factor.
    - Si la directiva de autenticación avanzada tiene éxito y si se configura el siguiente factor (etiqueta de directiva de autenticación), se evalúa el siguiente factor.
    - Si Next Factor no está configurado, la autenticación se ha completado y se ha realizado correctamente.
5. Si se produce un error en la directiva de autenticación avanzada y si Goto Expression es Siguiente, se evalúa la siguiente directiva de autenticación avanzada vinculada.
6. Si las directivas tienen éxito, se produce un error en la autenticación.

Servidor virtual de autenticación, autorización y auditoría

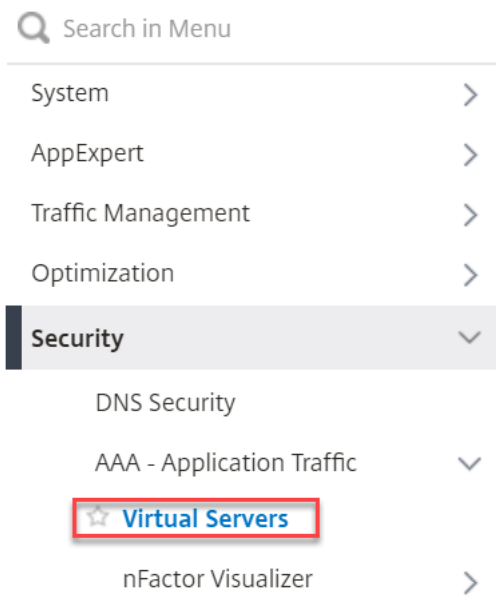
Para usar nFactor con Citrix Gateway, primero debe configurarlo en un servidor virtual de autenticación, autorización y auditoría. A continuación, vincula el servidor virtual de autenticación, autorización y auditoría al servidor virtual de Citrix Gateway.

Crear servidor virtual de autenticación, autorización y auditoría

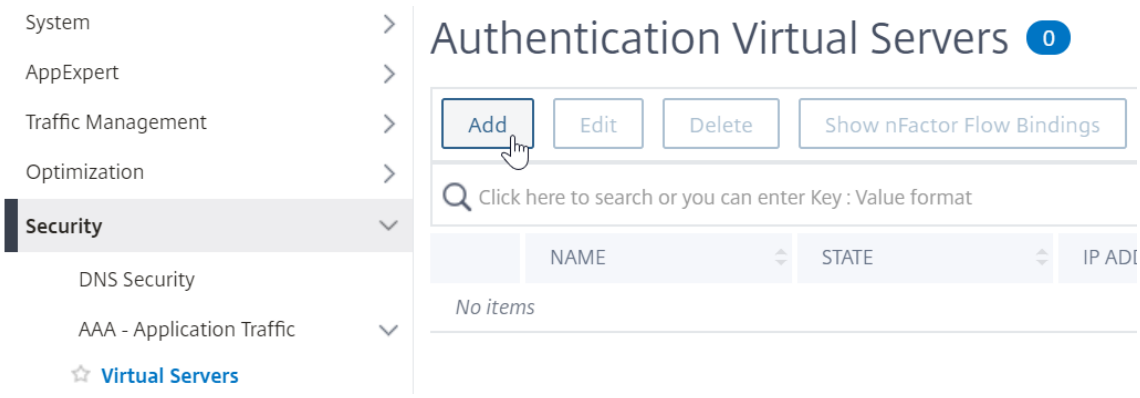
1. Si la función Autenticación, autorización y auditoría aún no está habilitada, vaya a **Seguridad > AAA: tráfico de aplicaciones**y haga clic con el botón derecho para habilitar la función.



2. Vaya a **Configuración > Seguridad > AAA - Tráfico de aplicaciones > Servidores virtuales**.

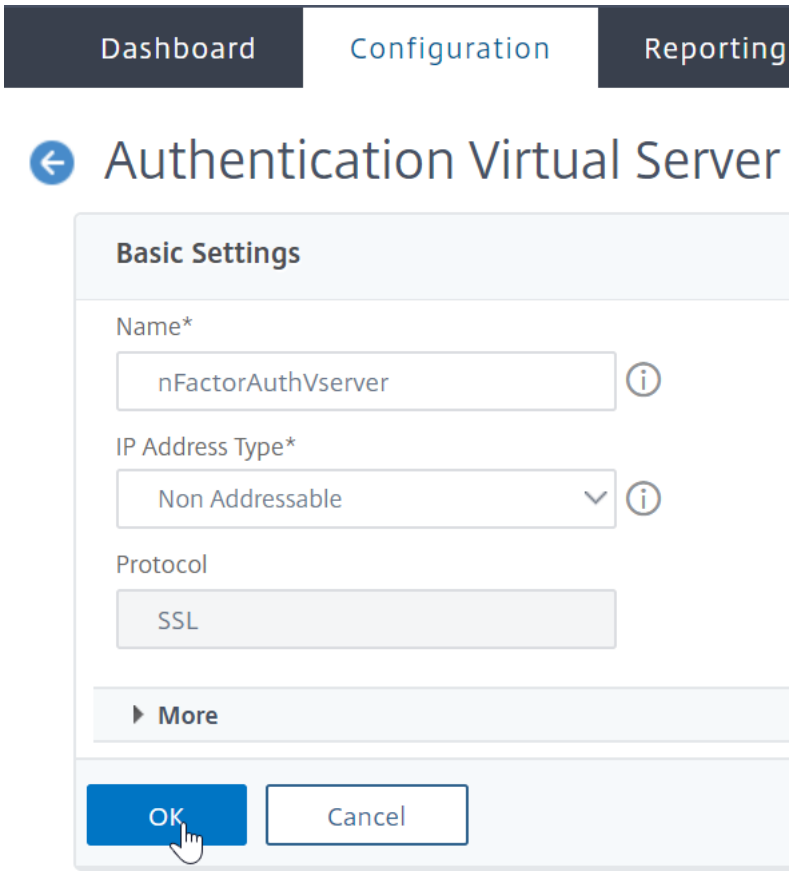


3. Haga clic en **Agregar** para crear un servidor virtual de autenticación.

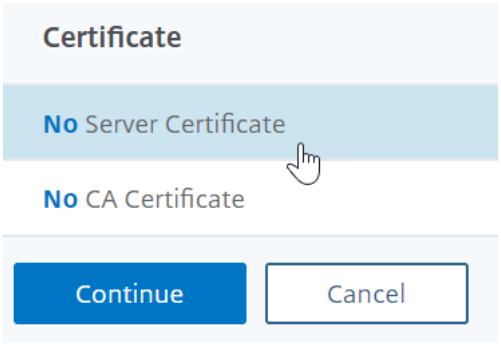


4. Introduzca la siguiente información y haga clic en **Aceptar**.

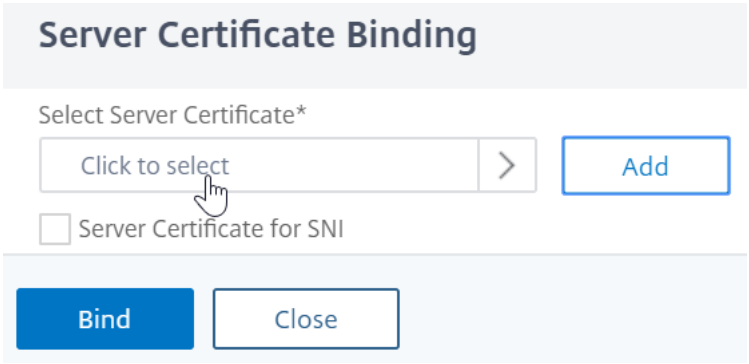
Nombre del parámetro	Descripción del parámetro
Nombre	Nombre del servidor virtual de autenticación, autorización y auditoría.
Tipo de dirección IP	Cambie el tipo de dirección IP a **No direccionable** si este servidor virtual se utiliza solo para Citrix Gateway.



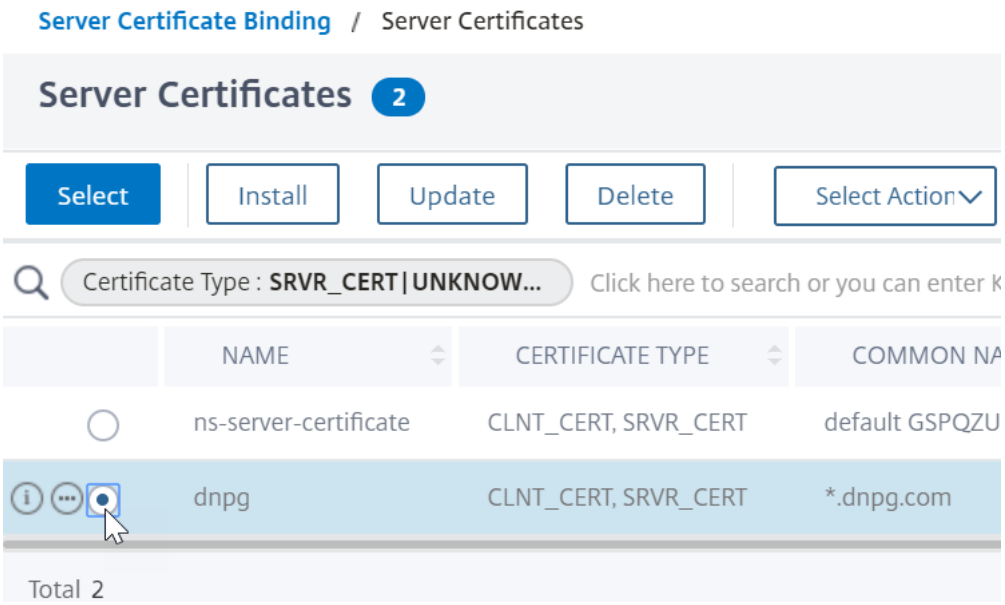
5. En Certificado, seleccione **Sin certificado de servidor**.



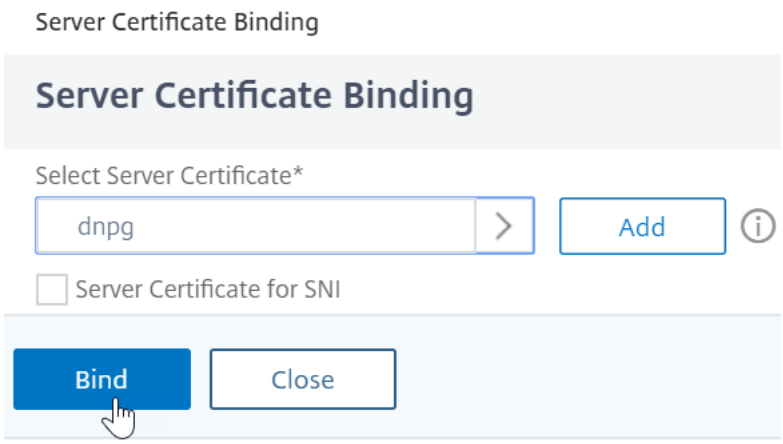
6. Haga clic en el texto, **haga clic para seleccionar** para seleccionar el certificado del servidor.



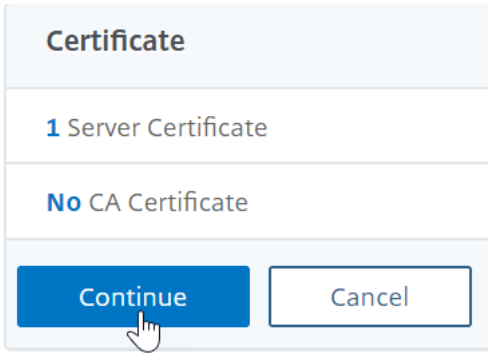
7. Haga clic en el botón de opción situado junto a un certificado para el servidor virtual de autenticación, autorización y auditoría y, a continuación, haga clic en **Seleccionar**. El certificado elegido no importa porque no se puede acceder directamente a este servidor.



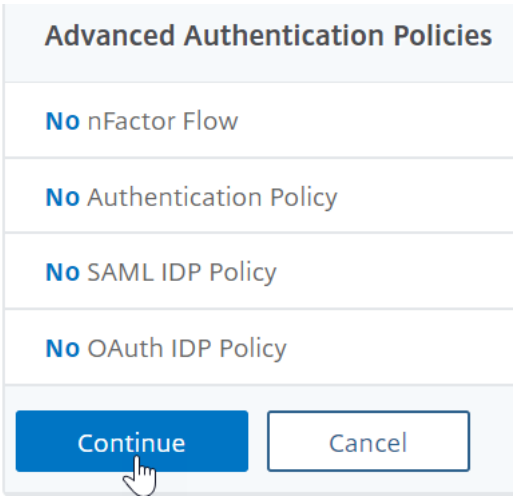
8. Haga clic en **Bind**.



9. Haga clic en **Continuar** para cerrar la sección **Certificado**.

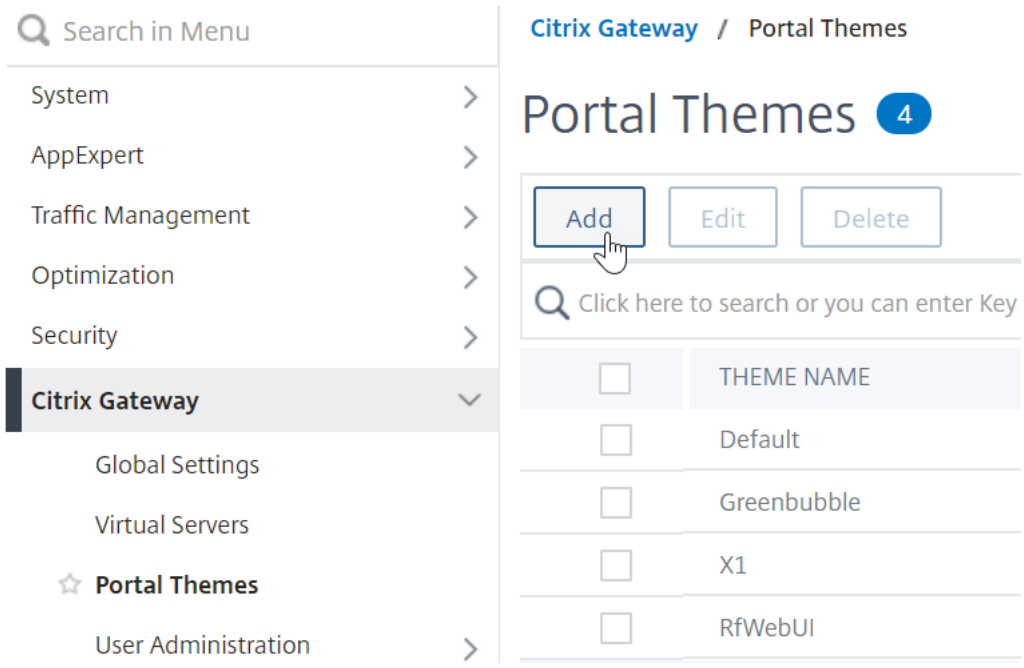


10. Haga clic en **Continuar**.

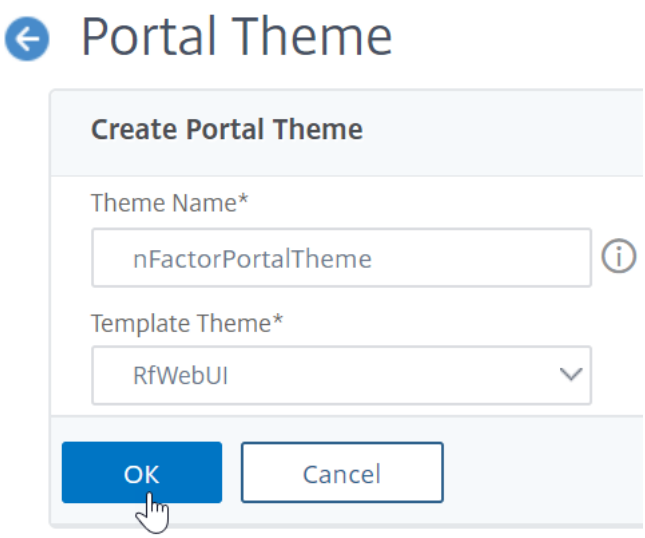


Enlazar el tema del portal al servidor virtual de autenticación, autorización y auditoría

1. Vaya a **Citrix Gateway > Temas del portal**y agregue un tema. Cree el tema en Citrix Gateway y, a continuación, lo vincule al servidor virtual de autenticación, autorización y auditoría.

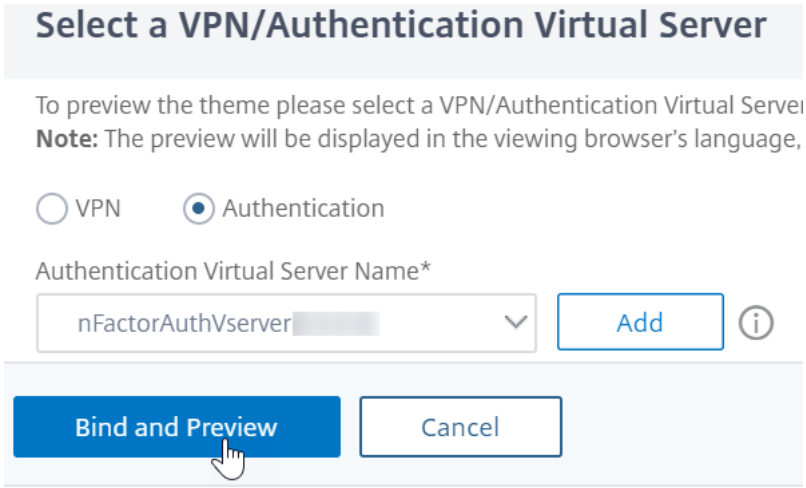


2. Crea un tema basado en el tema de plantilla RFWebUI.



3. Después de ajustar el tema según lo quiera, en la parte superior de la página de edición del tema del portal, haga clic en **Hacer clic para enlazar y ver el tema configurado**.

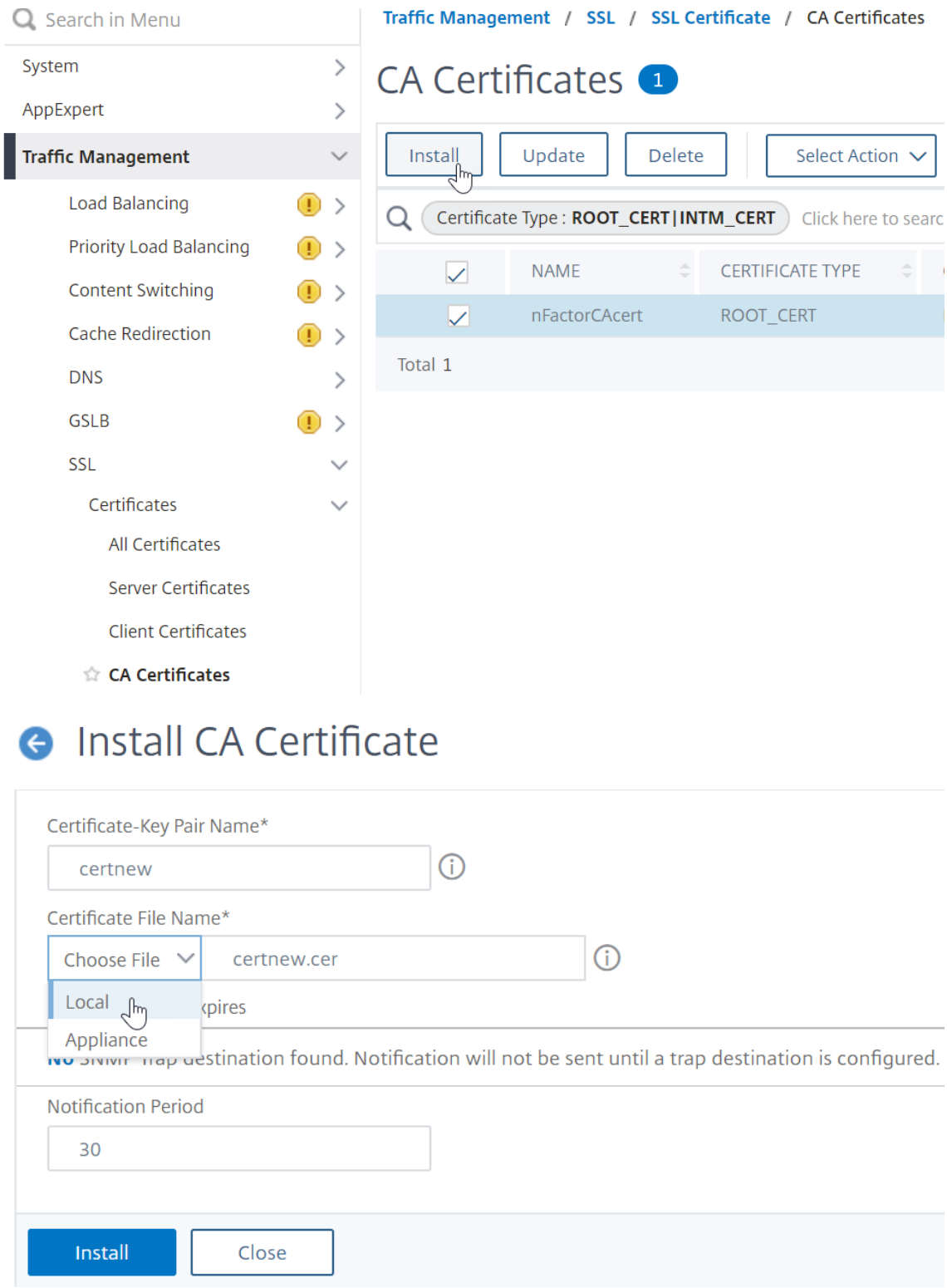
4. Cambie la selección a Autenticación. En el menú desplegable **Nombre del servidor virtual de autenticación**, seleccione el servidor virtual de autenticación, autorización y auditoría, y haga clic en Vincular **y vista previa** y cierre la ventana de vista previa.



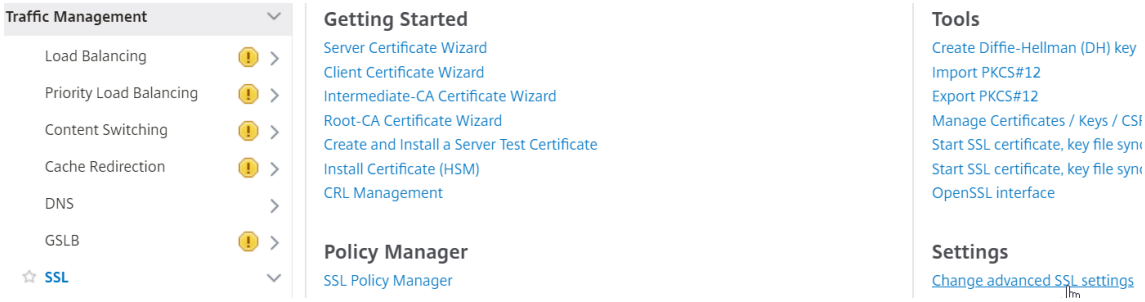
Habilitar la autenticación de certificados de cliente

Si uno de sus factores de autenticación es el certificado de cliente, debe realizar alguna configuración de SSL en el servidor virtual de autenticación, autorización y auditoría:

1. Vaya a **Administración del tráfico > SSL > Certificados > Certificados de CA**e instale el certificado raíz del emisor de los certificados de cliente. Los certificados raíz no tienen archivo de claves.



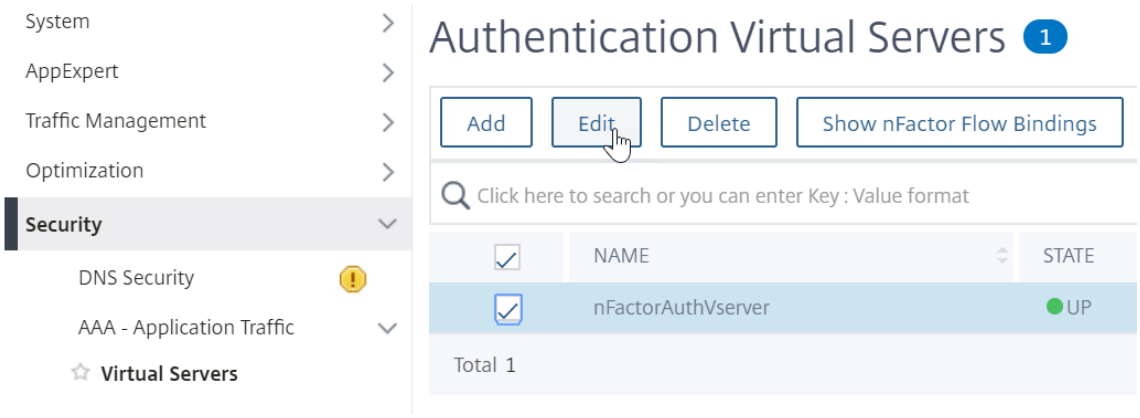
2. Vaya a **Administración del tráfico > SSL > Cambiar la configuración avanzada de SSL**.



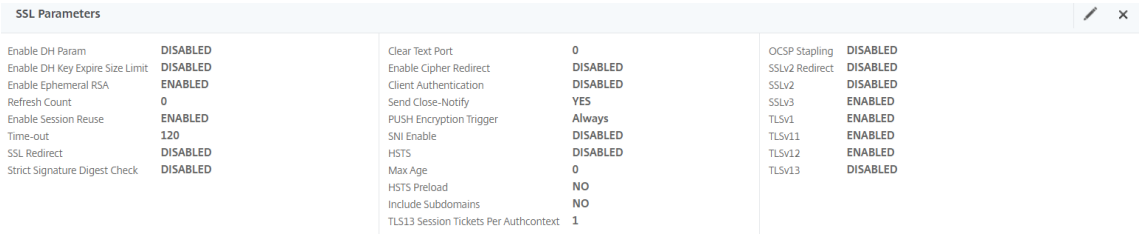
a) Desplácese hacia abajo para comprobar si **el perfil predeterminado** está **HABILITADO**. En caso afirmativo, debe utilizar un perfil SSL para habilitar la autenticación de certificados de cliente. De lo contrario, puede habilitar la autenticación de certificados de cliente directamente en el servidor virtual de autenticación, autorización y auditoría en la sección Parámetros SSL.

3. Si los perfiles SSL predeterminados no están habilitados:

a) Vaya a **Seguridad > AAA - Aplicación > Servidores virtuales**y modifique un servidor virtual de autenticación, autorización y auditoría existente.

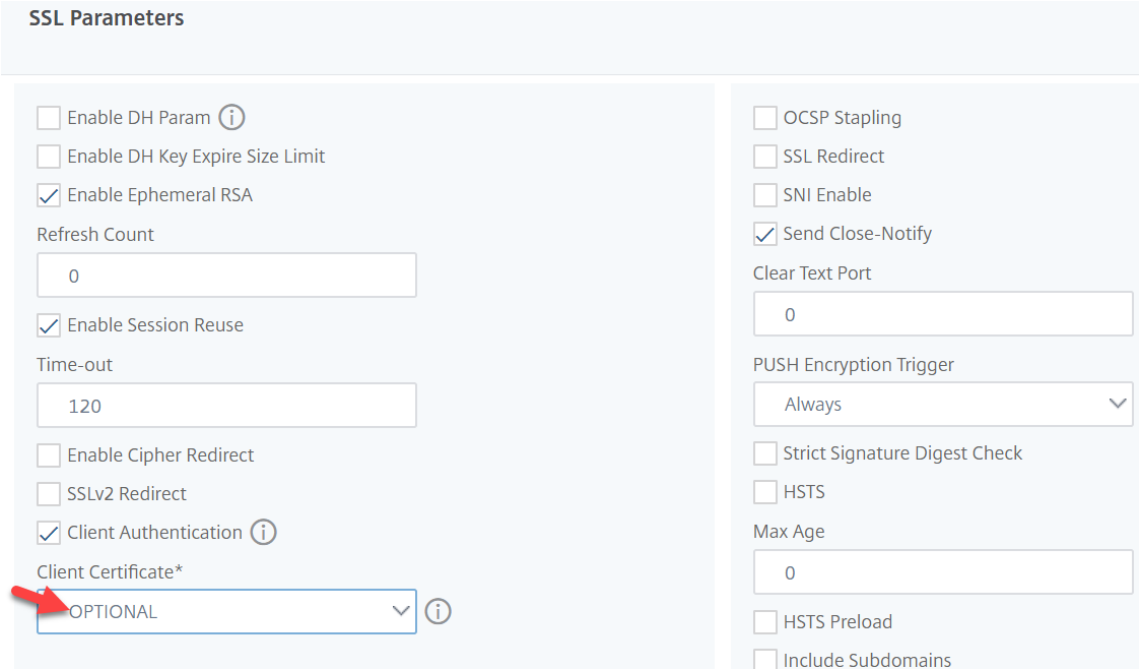


a) A la izquierda, en la sección **Parámetros SSL**, haga clic en el icono del lápiz.



a) Marque la casilla junto a **Autenticación de clientes**

b) Asegúrese de que está seleccionado **Opcional** en el menú desplegable **Certificado de cliente** y haga clic en **Aceptar**.



4. Si los perfiles SSL predeterminados están habilitados, cree un perfil SSL con la autenticación de cliente habilitada:

   a) En el menú de la izquierda, expanda Sistema y haga clic en Perfiles.

   b) En la parte superior derecha, cambia a la ficha Perfil SSL.

   c) Haga clic con el botón derecho en el perfil ns_default_ssl_profile_frontend y haga clic en Agregar. Esto copia la configuración del perfil predeterminado.

   d) Asigna un nombre al perfil. El propósito de este perfil es habilitar los certificados de cliente.

   e) Desplácese hacia abajo y busque la casilla Autenticación de clientes Marca la casilla.

   f) Cambie el menú desplegable Certificado de cliente a OPCIONAL.

   g) Al copiar el perfil SSL predeterminado, no se copian los cifrados SSL. Debe volver a hacerlas.

   h) Haga clic en Listo cuando haya terminado de crear el perfil SSL.

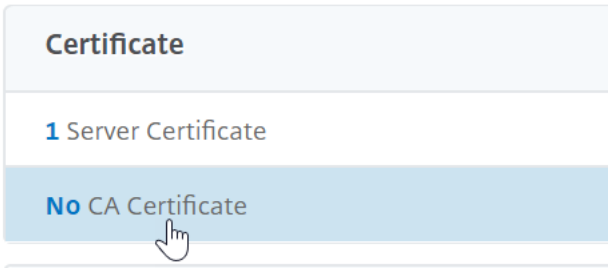
   i) Vaya a **Seguridad > AAA — Tráfico de aplicaciones > Servidores virtuales**y modifique un servidor virtual de autenticación, autorización y auditoría.

   j) Vaya hacia abajo hasta la sección Perfil SSL y haga clic en el lápiz.

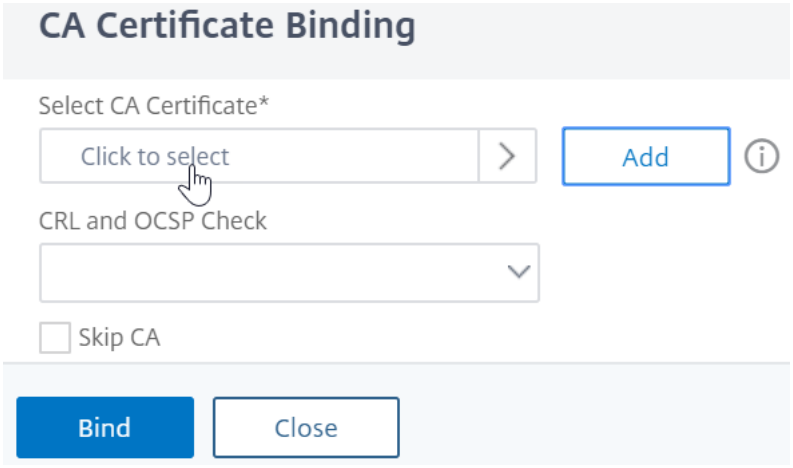
   k) Cambie el menú desplegable Perfil SSL por el perfil que tiene habilitados los certificados de cliente. Haga clic en OK.

   l) Desplácese hacia abajo en este artículo hasta llegar a las instrucciones para vincular el certificado de CA.

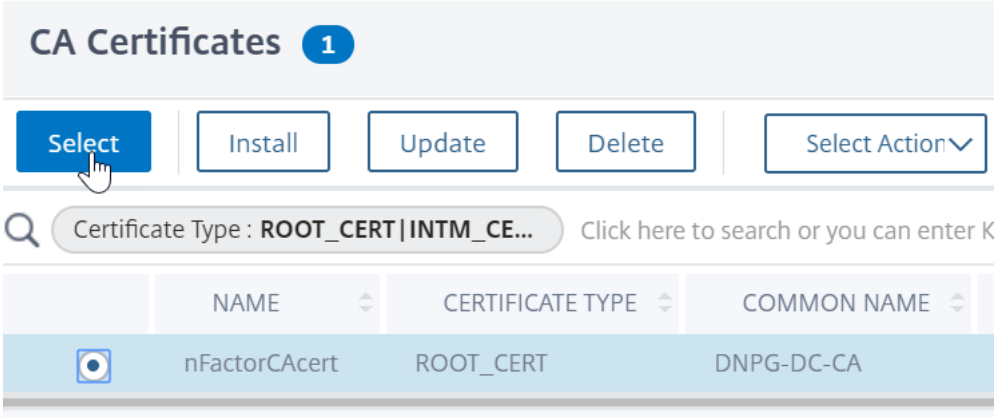
5. A la izquierda, en la sección **Certificados**, haga clic en donde dice **Sin certificado de CA**.



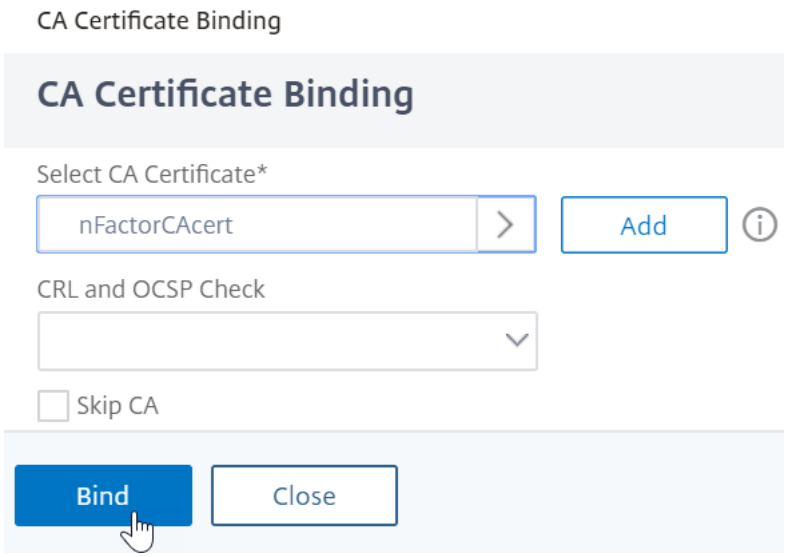
6. Haga clic en el texto, **haga clic para seleccionarlo**.



7. Haga clic en el botón de opción situado junto al certificado raíz del emisor de los certificados de cliente y haga clic en **Seleccionar**.



8. Haga clic en **Bind**.



Archivo XML de esquema de inicio de sesión

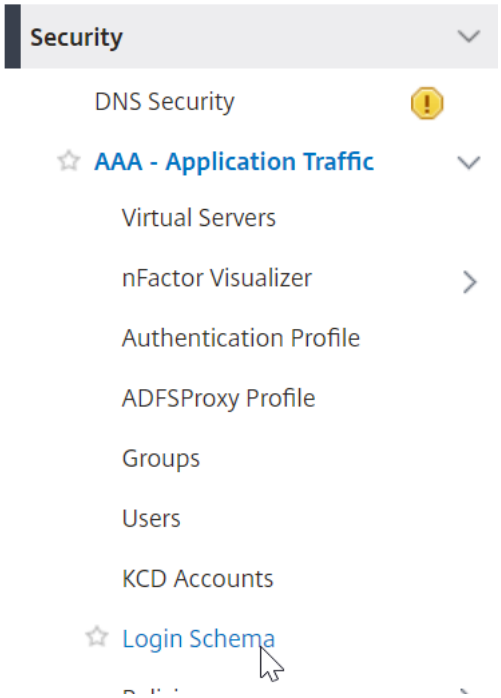
El esquema de inicio de sesión es un archivo XML que proporciona la estructura de las páginas de inicio de sesión de autenticación basadas en formularios.

nFactor implica múltiples factores de autenticación que están encadenados entre sí. Cada factor puede tener páginas o archivos de esquema de inicio de sesión diferentes. En algunos casos de autenticación, a los usuarios se les pueden presentar varias pantallas de inicio de sesión.

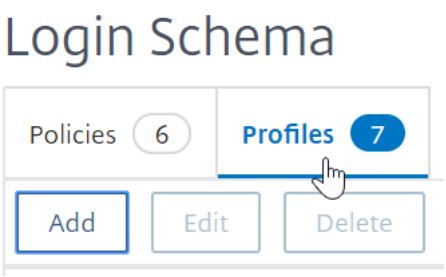
Configurar un perfil de esquema de inicio de sesión

Para configurar un perfil de esquema de inicio de sesión:

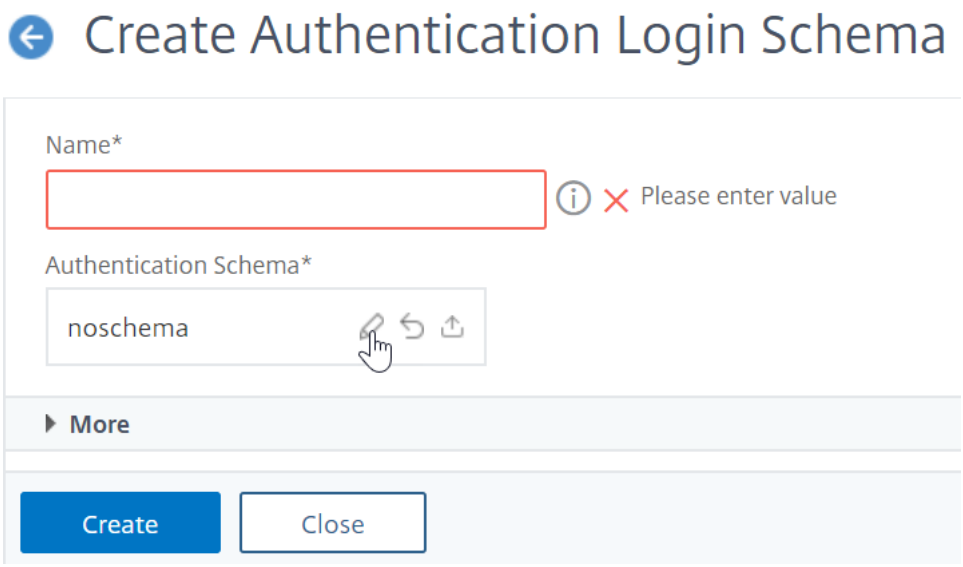
1. Cree o modifique un archivo.XML de esquema de inicio de sesión basado en el diseño de nFactor.
2. Vaya a **Seguridad > AAA: Tráfico de aplicaciones > Esquema de inicio**de sesión.



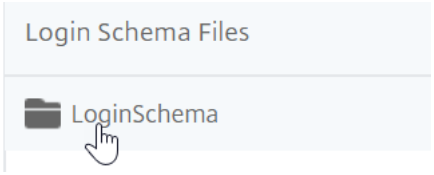
3. A la derecha, cambia a la ficha **Perfiles** y haga clic en **Agregar**.



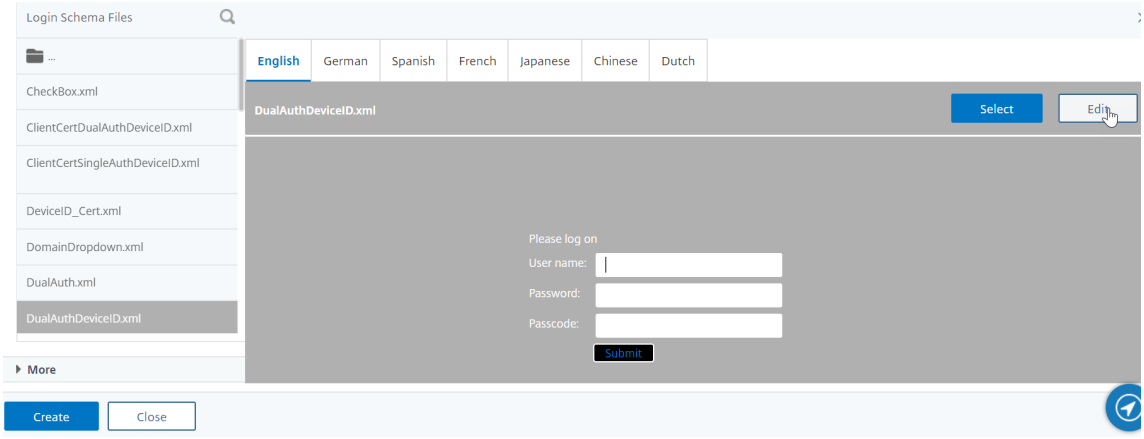
4. En el campo **Esquema de autenticación**, haga clic en el icono del lápiz.



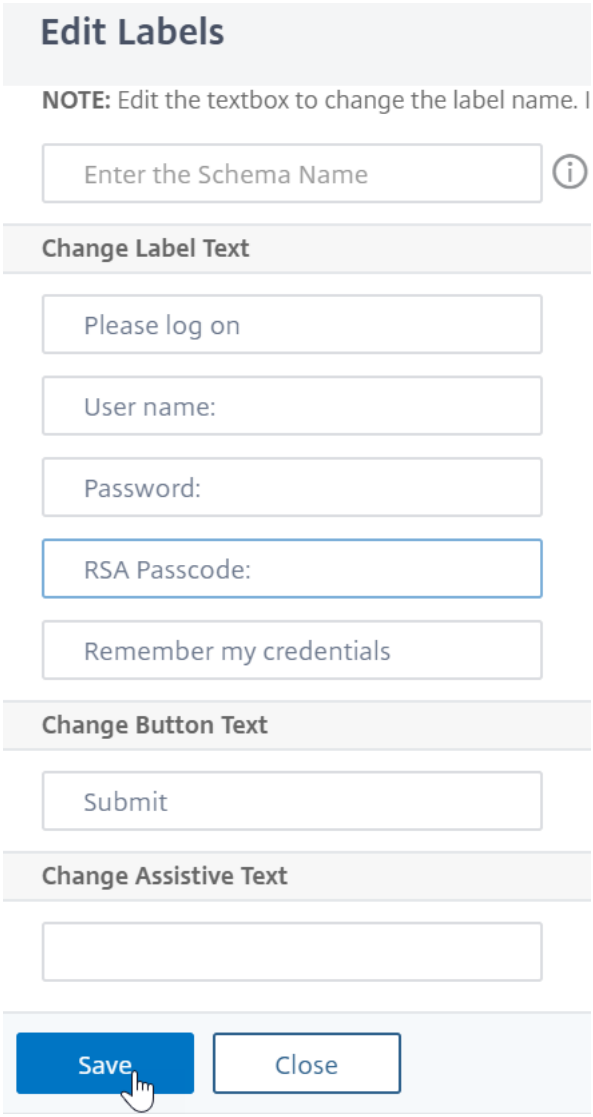
5. Haga clic en la carpeta LoginSchema para ver los archivos que contiene.



6. Seleccione uno de los archivos. Puede ver una vista previa a la derecha. Las etiquetas se pueden cambiar haciendo clic en el botón **Modificar** de la parte superior derecha.

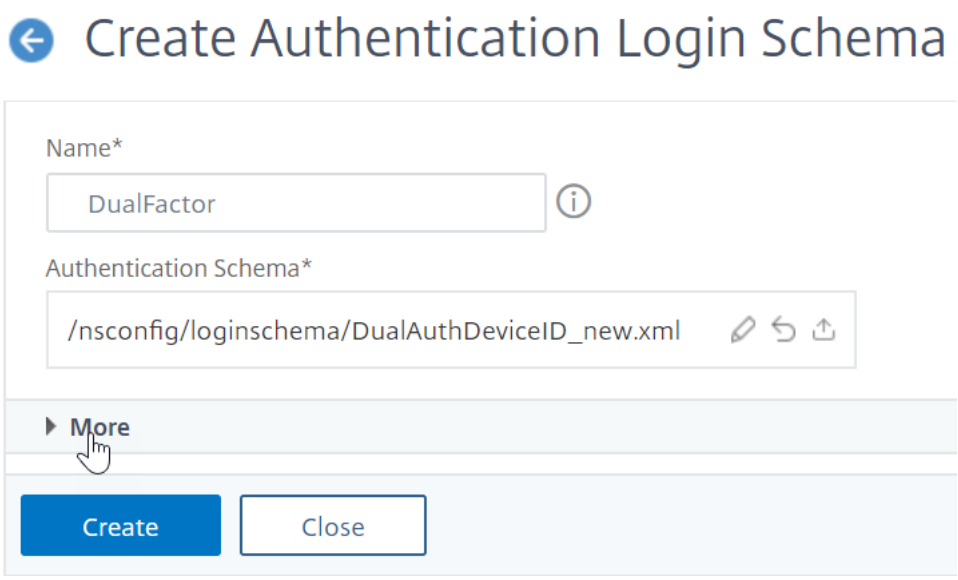


7. Al guardar los cambios, se crea un archivo en /nsconfig/LoginSchema.



8. En la parte superior derecha, haga clic en **Seleccionar**.

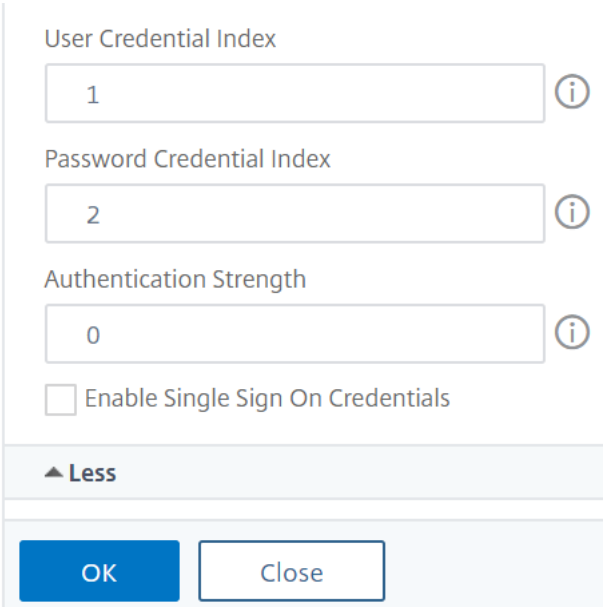
9. Asigne un nombre al esquema de inicio de sesión y haga clic en **Más**.



10. Use el nombre de usuario y la contraseña introducidos en el esquema de inicio de sesión para el inicio de sesión único (SSO) en un servicio de back-end, por ejemplo, StoreFront.

    Puede utilizar las credenciales introducidas en el esquema de inicio de sesión como credenciales de inicio de sesión único mediante cualquiera de los métodos siguientes.

    - Haga clic en **Más** en la parte inferior de la página **Crear esquema de inicio de sesión de autenticación** y seleccione **Activar credenciales de inicio de sesión único**.
    - Haga clic en **Más** en la parte inferior de la página **Crear esquema de inicio de sesión de autenticación** e introduzca valores únicos para el índice de credenciales de usuario y el índice de credenciales de contraseña. Estos valores pueden estar entre 1 y 16. Más adelante, haga referencia a estos valores de índice en una directiva/perfil de tráfico mediante la expresión AAA.USER.ATTRIBUTE (#).



11. Haga clic en **Aceptar** para crear el perfil de esquema de inicio de sesión.

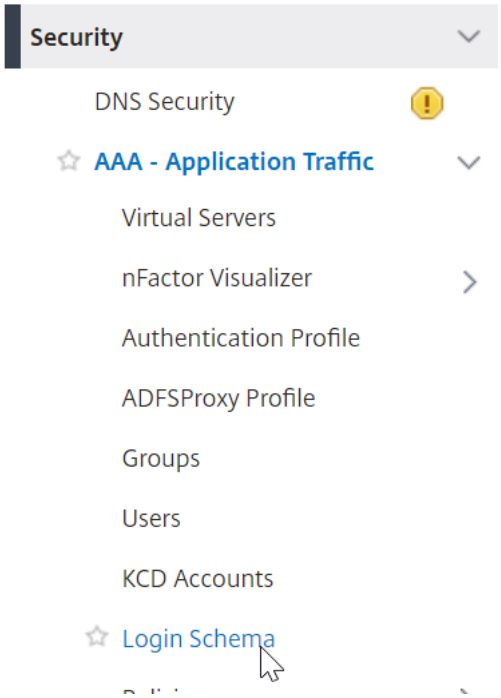
> **Nota:** Si modifica el archivo de esquema de inicio de sesión (.xml) más adelante, para que los cambios se reflejen, debe modificar el perfil del esquema de inicio de sesión y volver a seleccionar el archivo de esquema de inicio de sesión (.xml).

Crear y enlazar una directiva de esquema de inicio de sesión

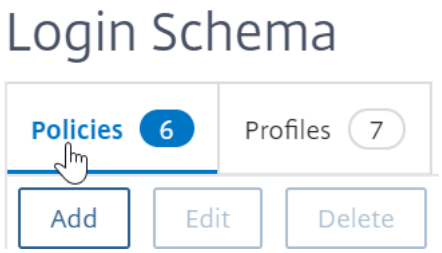
Para enlazar un perfil de esquema de inicio de sesión a un servidor virtual de autenticación, autorización y auditoría, primero debe crear una directiva de esquema de inicio de sesión. Las directivas de esquema de inicio de sesión no son necesarias al vincular el perfil del esquema de inicio de sesión a una etiqueta de directiva de autenticación, como se detalla más adelante.

Para crear y vincular una directiva de esquema de inicio de sesión:

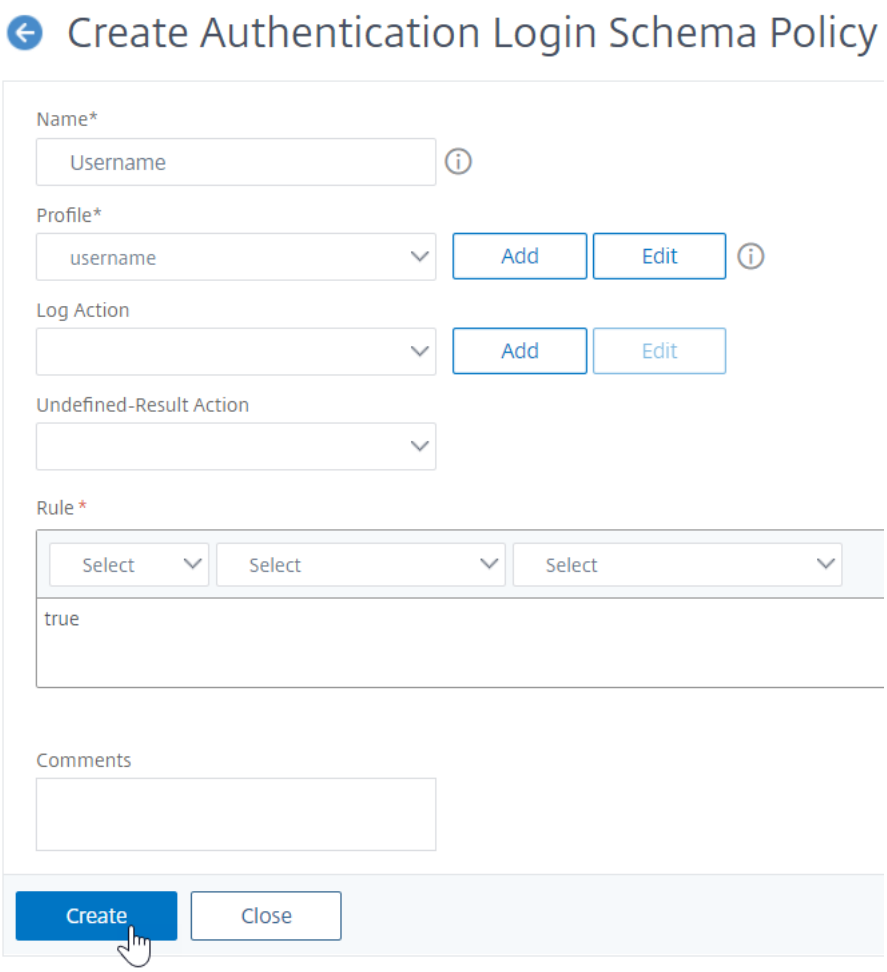
1. Vaya a **Seguridad > AAA: Tráfico de aplicaciones > Esquema de inicio**de sesión.



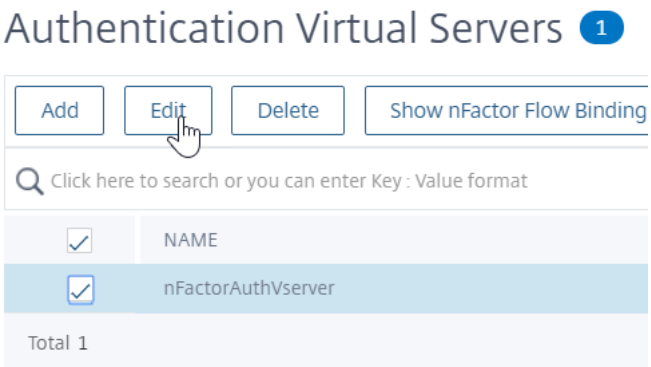
2. En la ficha **Policies**, haga clic en **Add**.



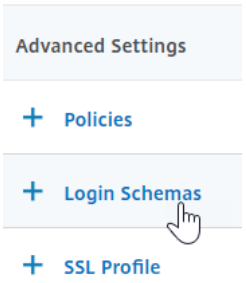
3. Utilice el menú desplegable **Perfil** para seleccionar el perfil de esquema de inicio de sesión que ya ha creado.
4. Introduzca una expresión de directiva avanzada en el cuadro **Regla** y haga clic en **Crear**.



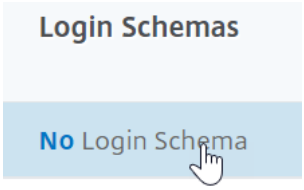
5. A la izquierda, vaya a **Seguridad > AAA - Tráfico de aplicaciones > Servidores virtuales**y modifique un servidor virtual de autenticación, autorización y auditoría existente.



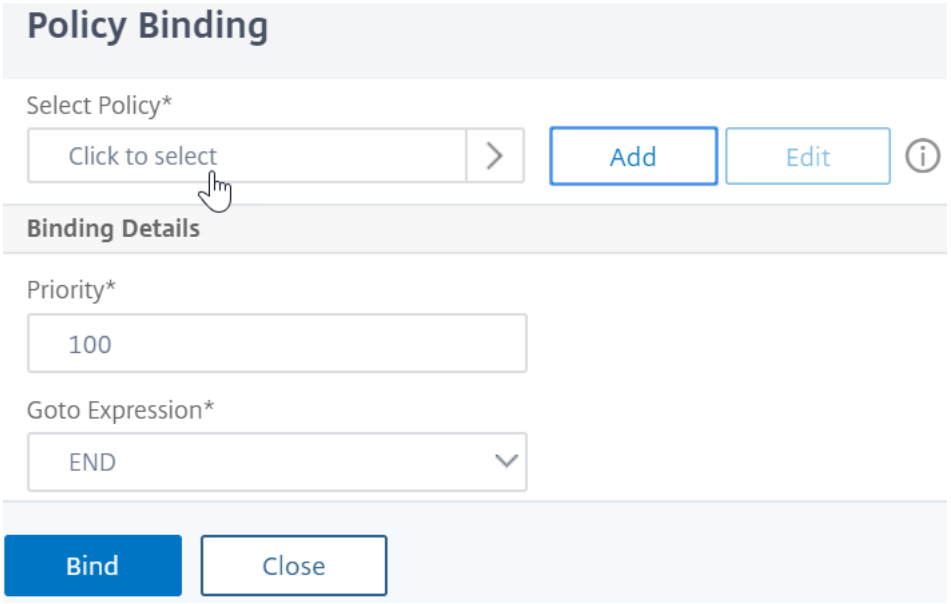
6. En la columna Configuración avanzada, haga clic en **Esquemas de inicio**de sesión.



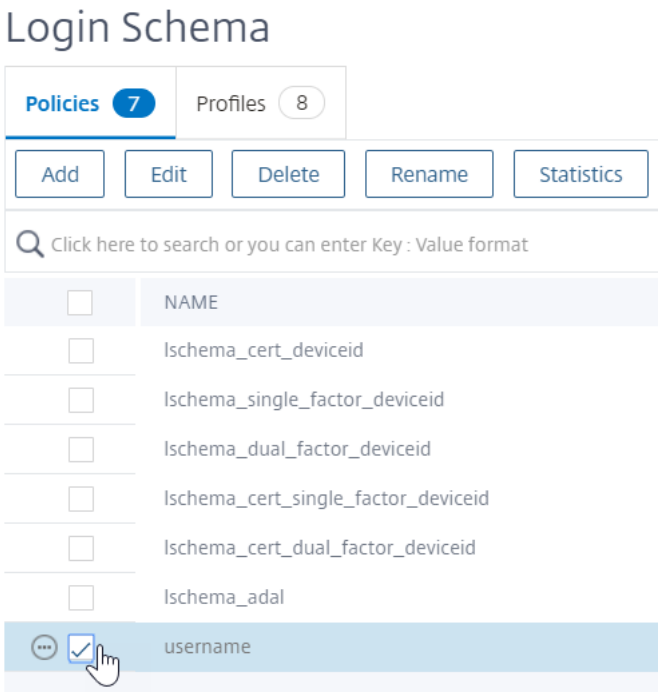
7. En la sección Esquemas de inicio de sesión, haga clic en el texto **Sin esquema de inicio**de sesión.



8. Haga clic en el texto, **haga clic para seleccionarlo**.



9. Haga clic en el botón de opción situado junto a la directiva de esquema de inicio de sesión y haga clic en **Seleccionar**. En esta lista solo aparecen las directivas de esquema de inicio de sesión. Los perfiles de esquema de inicio de sesión (sin directiva) no aparecen.



10. Haga clic en **Bind**.

Directivas de autenticación avanzada

Las directivas de autenticación son una combinación de expresión de directiva y acción de directiva. Si la expresión es verdadera, evalúe la acción de autenticación.

Creación de directivas de autenticación avanzadas

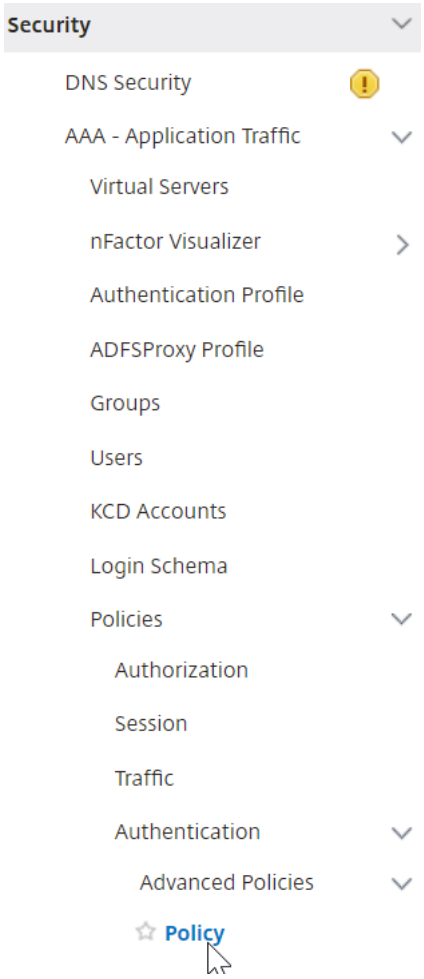
Las directivas de autenticación son una combinación de expresión de directivas y acción de directivas. Si la expresión es verdadera, evalúe la acción de autenticación.

Necesita acciones/servidores de autenticación (por ejemplo, LDAP, RADIUS, CERT, SAML, etc.)
Al crear una directiva de autenticación avanzada, hay un icono más (Agregar) que le permite crear acciones/servidores de autenticación.

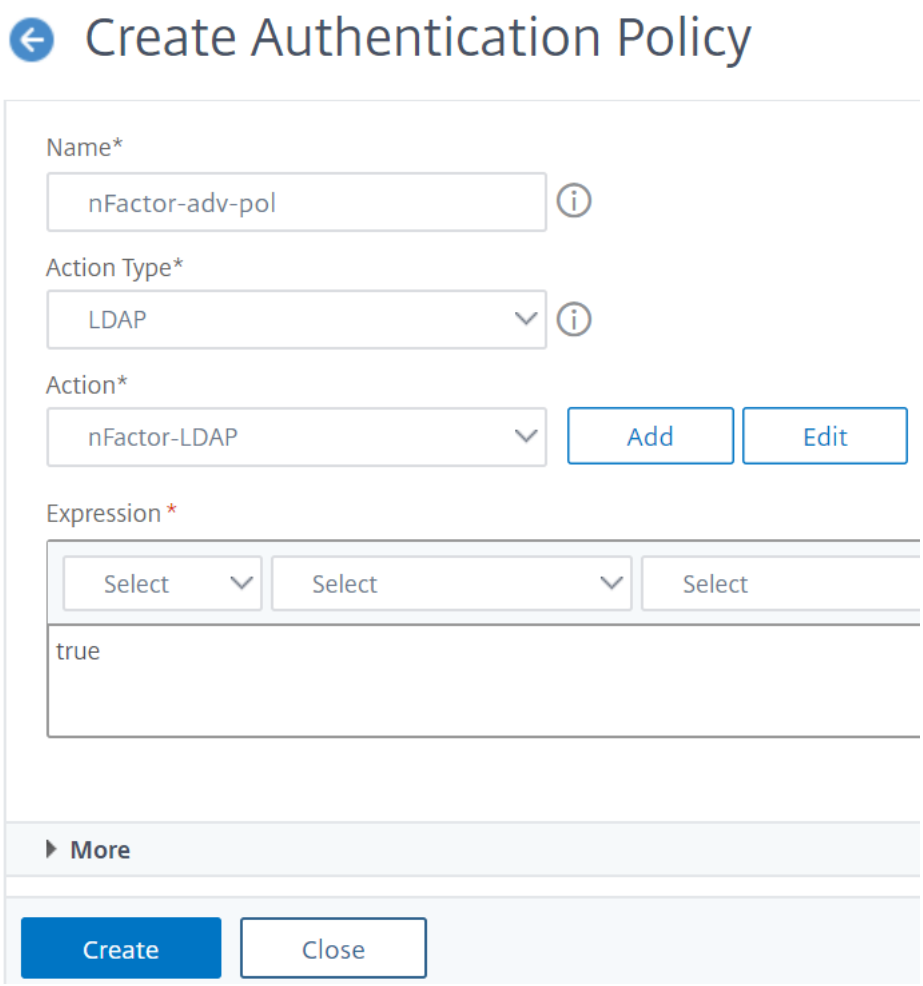
O bien, puede crear acciones de autenticación (servidores) antes de crear la directiva de autenticación avanzada. Los servidores de autenticación se encuentran en **Autenticación > Panel de control**. A la derecha, haga clic en Agregar y seleccione un tipo de servidor. Las instrucciones para crear estos servidores de autenticación no se detallan aquí. Consulte los procedimientos Autenticación: NetScaler 12/Citrix ADC 12.1.

Para crear una directiva de autenticación avanzada:

1. Vaya a **Seguridad > AAA - Tráfico de aplicaciones > Directivas > Autenticación > Directivas avanzadas > Directiva**



2. En el panel de detalles, realice una de las siguientes acciones:
   - Para crear una directiva, haga clic en **Agregar**.
   - Para modificar una directiva existente, selecciónela y, a continuación, haga clic en **Modificar**.
3. En el cuadro de diálogo **Crear directiva** de **autenticación o Configurar directiva** de autenticación, escriba o seleccione valores para los parámetros.



- **Nombre: nombre** de la directiva. No se puede cambiar para una directiva configurada previamente.
- **Tipo de acción**: Tipo de directiva: Cert, Negotiate, LDAP, RADIUS, SAML, SAMLIDP, TACACS o WEBAUTH.
- **Acción: acción** de autenticación (perfil) que se va a asociar a la directiva. Puede elegir una acción de autenticación existente o hacer clic en el signo más y crear una acción del tipo adecuado.
- **Acción de registro: acción** de auditoría que se va a asociar a la directiva. Puede elegir una acción de auditoría existente o hacer clic en el signo más y crear una acción.
  No tiene ninguna acción configurada o, para crear una acción, haga clic en **Agregar** y complete los pasos.
- **Expresión**: Regla que selecciona las conexiones a las que quiere aplicar la acción especificada. La regla puede ser simple ("true" selecciona todo el tráfico) o compleja. Las expresiones se introducen seleccionando primero el tipo de expresión en la lista desplegable situada más a la izquierda debajo de la ventana Expresión y, a continuación, escribiendo la expresión directamente en el área de texto de la expresión o haciendo clic en Agregar

para abrir el cuadro de diálogo Agregar expresión y mediante las listas desplegables que contiene para crear el expresión.)

- **Comentario**: Puede escribir un comentario que describa el tipo de tráfico al que se aplica esta directiva de autenticación. Opcional.

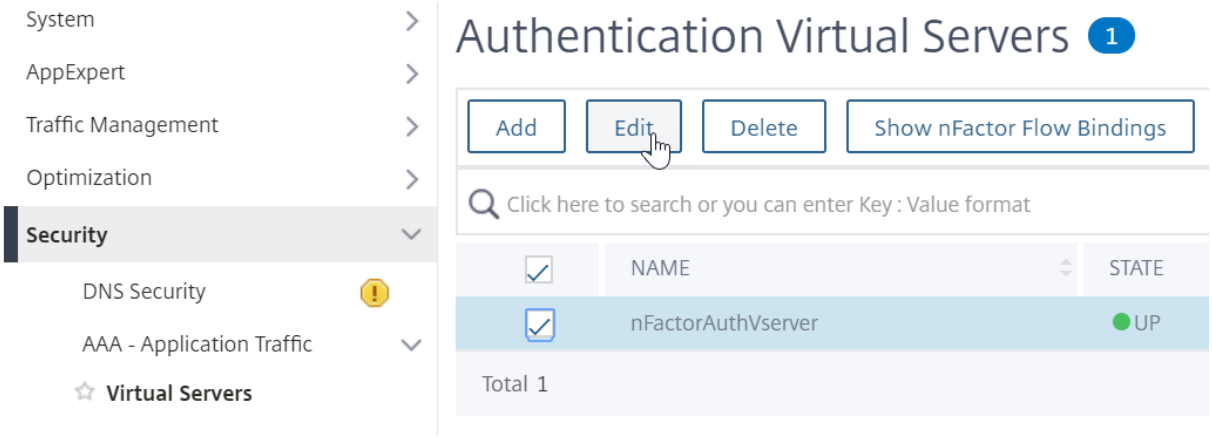
4. Haga clic en **Create** y, luego, en **Close**. Si ha creado una directiva, esa directiva aparece en la página Directivas y servidores de autenticación.

Cree directivas de autenticación avanzadas adicionales según sea necesario en función de su diseño de nFactor.

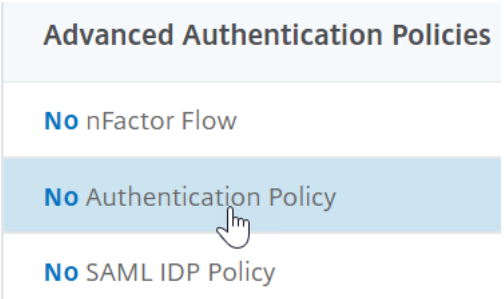
Vincular la directiva de autenticación avanzada de primer factor a la autenticación, la autorización y la auditoría

Puede vincular directamente directivas de autenticación avanzadas para el primer factor: el servidor virtual de autenticación, autorización y auditoría. Para los siguientes factores, debe vincular las directivas de autenticación avanzada a las etiquetas de la directiva de autenticación.

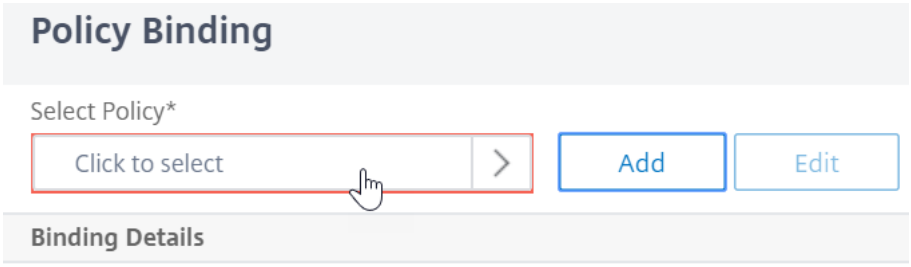
1. Vaya a **Seguridad > AAA - Tráfico de aplicaciones > Servidores virtuales**. Modificar un servidor virtual existente.



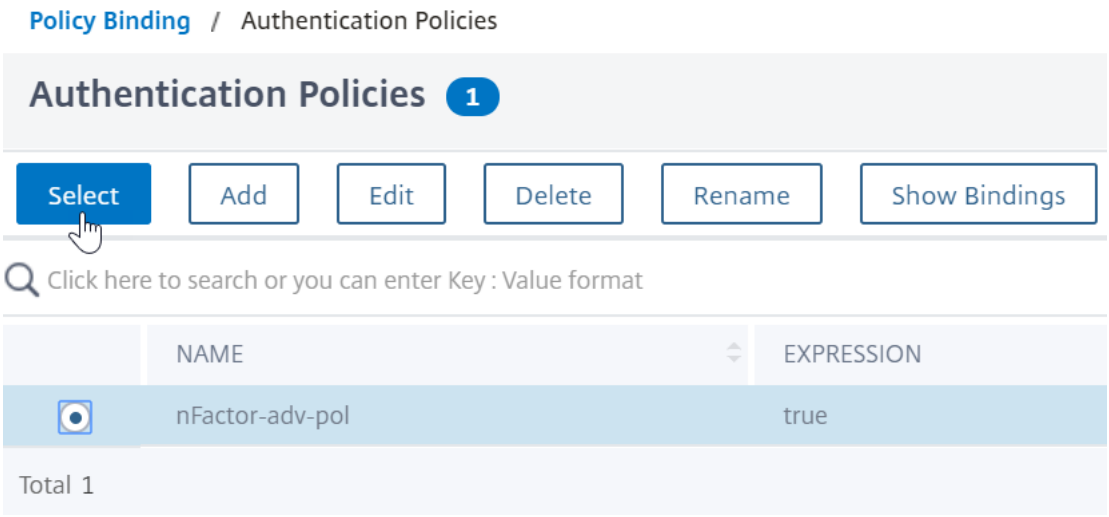
1. A la izquierda, en la sección Directivas de autenticación avanzada, haga clic en **Sin directiva de autenticación**.



2. En **Seleccionar directiva**, haga clic en el texto, **haga clic para seleccionar**.

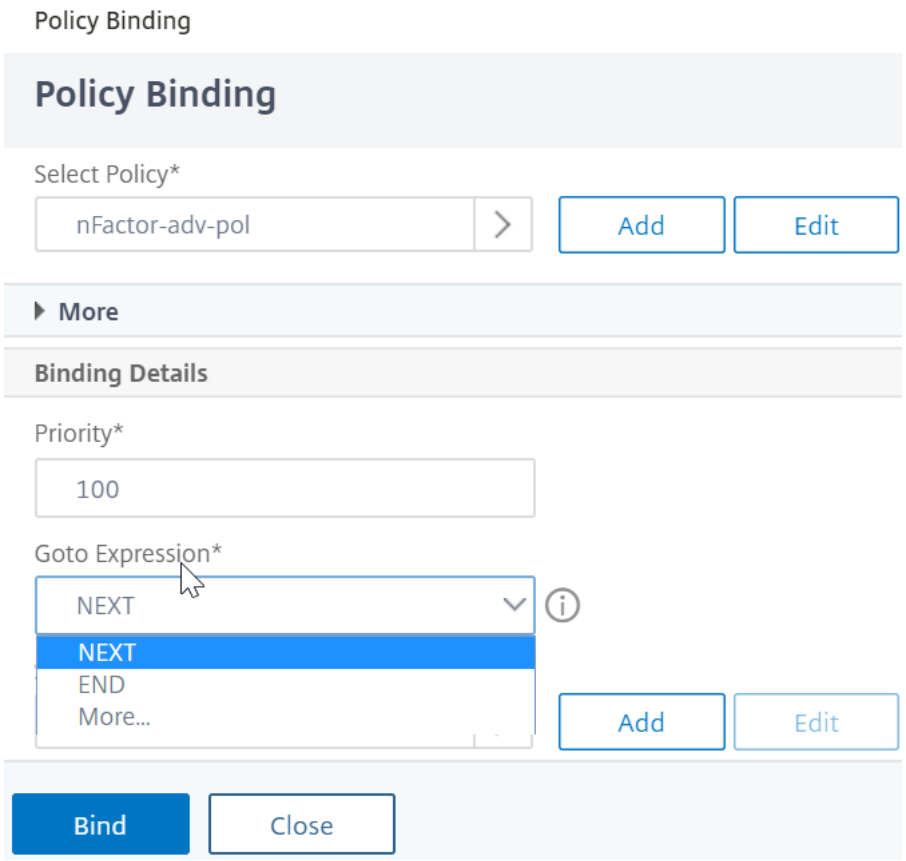


3. Haga clic en el botón de opción situado junto a la **Directiva de autenticación avanzada**y, a continuación, haga clic en **Seleccionar**.

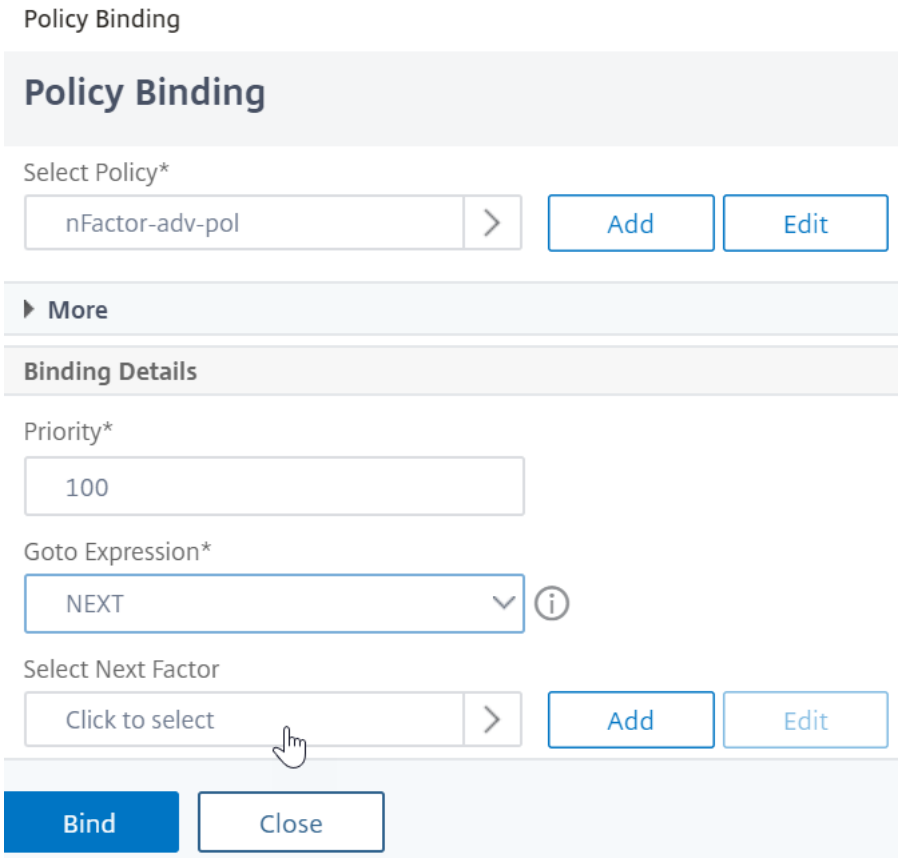


4. En la sección Detalles de enlace, la **expresión Goto** determina qué sucede a continuación si se produce un error en esta directiva de autenticación avanzada.

   - Si **Goto Expression** se establece en **SIGUIENTE**, se evalúa la siguiente directiva de autenticación avanzada enlazada a este servidor virtual de autenticación, autorización y auditoría.
   - Si **Goto Expression** se establece en **END**o si no hay directivas de autenticación más avanzadas enlazadas a este servidor virtual de autenticación, autorización y auditoría, la autenticación se completa y se marca como fallida.



5. En **Seleccionar factor siguiente**, puede seleccionar puede apuntar a una etiqueta de directiva de autenticación. El siguiente factor se evalúa solo si la directiva de autenticación avanzada tiene éxito. Por último, haga clic en **Enlazar**.



Utilizar grupos LDAP extraídos para seleccionar el siguiente factor de autenticación

Puede utilizar grupos LDAP extraídos para seleccionar el siguiente factor de autenticación sin autenticación real con LDAP.

1. Al crear o modificar un servidor LDAP o una acción LDAP, desactive la casilla **Autenticación**.
2. En **Otros ajustes**, seleccione los valores apropiados en **Atributo de grupo** y **Nombre de subatributo**.

Autenticar la etiqueta de directiva

Cuando vincula una directiva de autenticación avanzada al servidor virtual de autenticación, autorización y auditoría y ha seleccionado un factor siguiente, el siguiente factor se evalúa solo si la directiva de autenticación avanzada. El siguiente factor que se evalúa es una etiqueta de directiva de autenticación.

La etiqueta de directiva de autenticación especifica un conjunto de directivas de autenticación para un factor concreto. Cada etiqueta de directiva corresponde a un único factor. También especifica el formulario de inicio de sesión que debe presentarse al usuario. La etiqueta de directiva de autenticación debe estar vinculada como el siguiente factor de una directiva de autenticación o de otra

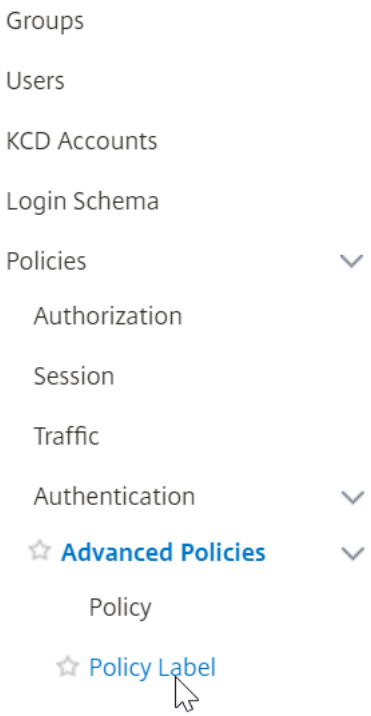
etiqueta de directiva de autenticación.

Nota: No todos los factores necesitan un esquema de inicio de sesión. El perfil de esquema de inicio de sesión solo es necesario si vincula un esquema de inicio de sesión a una etiqueta de directiva de autenticación.

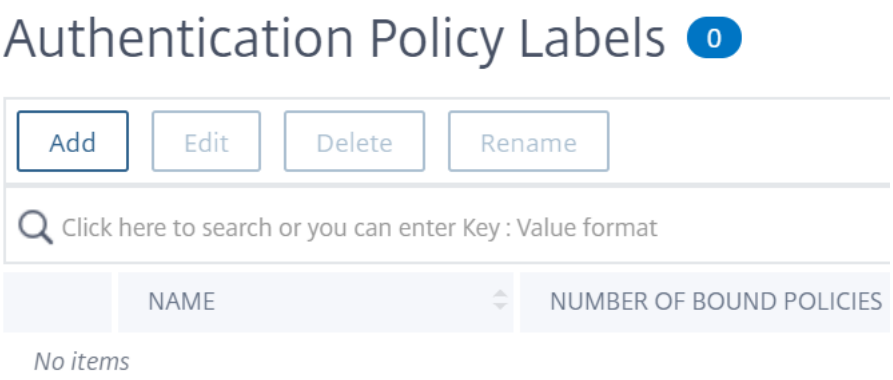
Crear una etiqueta de directiva de autenticación

Una etiqueta de directiva especifica las directivas de autenticación de un factor concreto. Cada etiqueta de directiva corresponde a un único factor. La etiqueta de directiva especifica el formulario de inicio de sesión que debe presentarse al usuario. La etiqueta de directiva debe estar vinculada como el siguiente factor de una directiva de autenticación o de otra etiqueta de directiva de autenticación. Normalmente, una etiqueta de directiva incluye directivas de autenticación para un mecanismo de autenticación específico. Sin embargo, también puede tener una etiqueta de directiva que tenga directivas de autenticación para distintos mecanismos de autenticación.

1. Vaya a **Seguridad > AAA — Tráfico de aplicaciones > Directivas > Autenticación > Directivas avanzadas > Etiqueta de directiva**.



2. Haga clic en el botón **Agregar**.

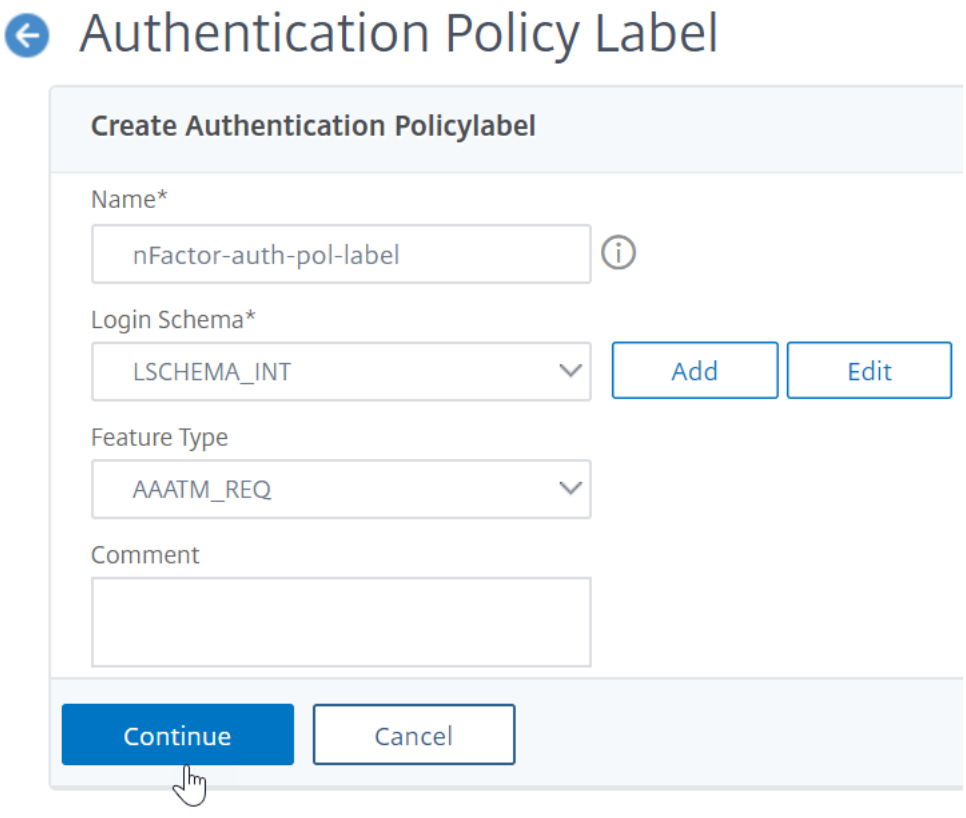


3. Complete los campos siguientes para crear una etiqueta de directiva de autenticación:

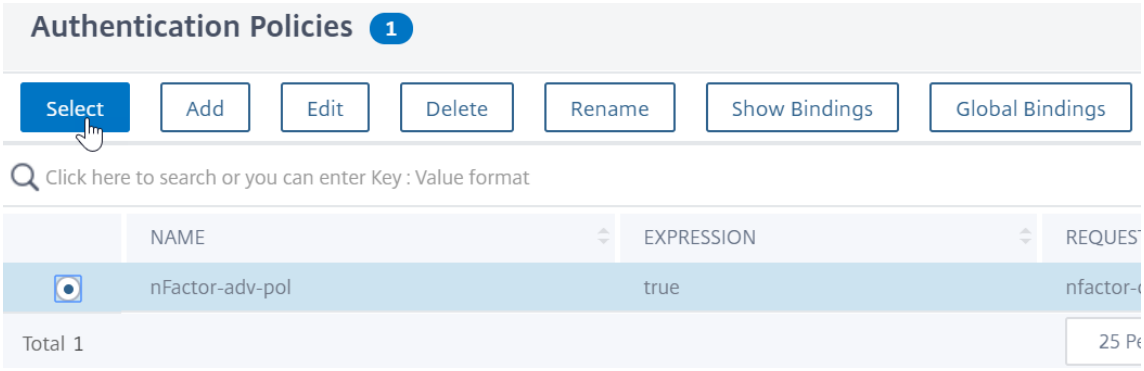
   a) Introduzca el **nombre** de la nueva etiqueta de directiva de autenticación.

   b) Seleccione el **esquema de inicio** de sesión asociado a la etiqueta de directiva de autenticación. SI no quiere mostrar nada al usuario, puede seleccionar un perfil de esquema de inicio de sesión que esté configurado como ningún esquema (LSCHEMA_INT).

   c) Haga clic en **Continuar**.



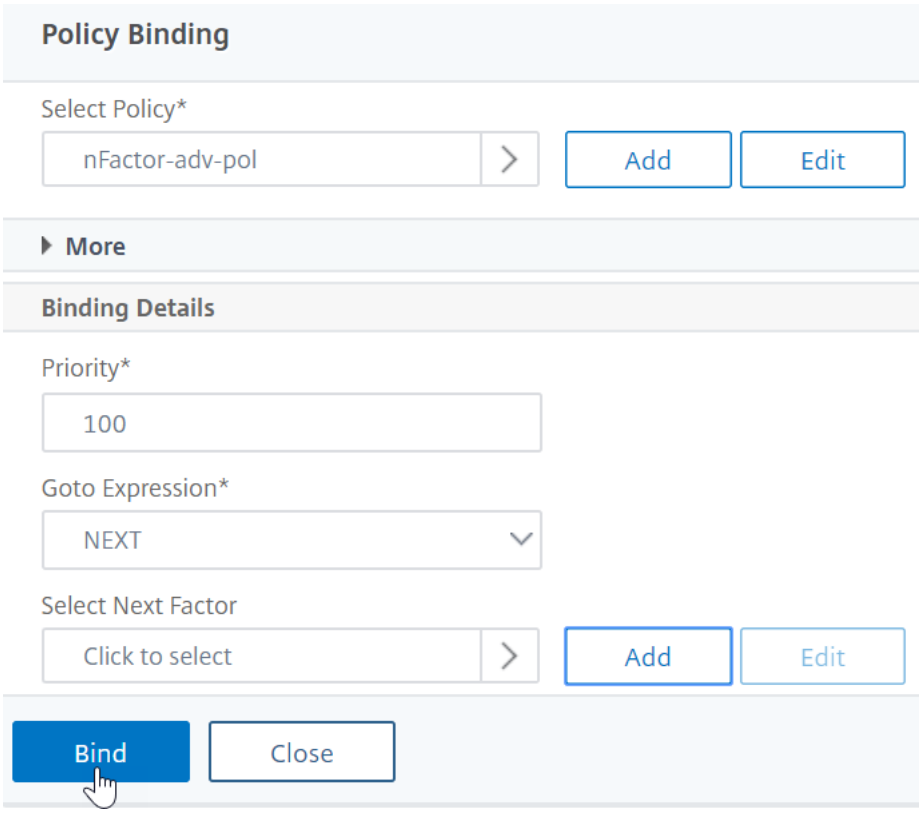
4. En la sección **Vinculación de directivas**, haga clic en donde dice **Haga clic para seleccionar**.
5. Seleccione la directiva de autenticación que evalúa este factor.



6. Rellene los campos siguientes:

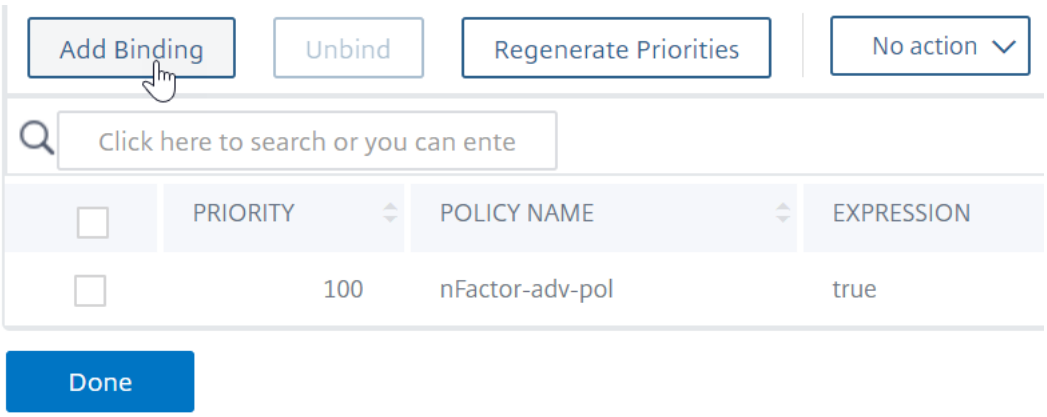
   a) Introduzca la **prioridad** de la vinculación de la directiva.

   b) En **Goto Expression**, seleccione **SIGUIENTE** si quiere enlazar directivas de autenticación más avanzadas a este factor o seleccione **END**.



7. En **Seleccionar siguiente factor**, si quiere agregar otro factor, haga clic para seleccionar y enlazar la siguiente etiqueta de directiva de autenticación (factor siguiente).
   Si no selecciona el siguiente factor y esta directiva de autenticación avanzada tiene éxito, la autenticación se realiza correctamente y se ha completado.
8. Haga clic en **Bind**.
9. Puede hacer clic en **Agregar enlace** para agregar directivas de autenticación más avanzadas a

esta etiqueta de directiva (factor). Haga clic en **Listo** al finalizar.



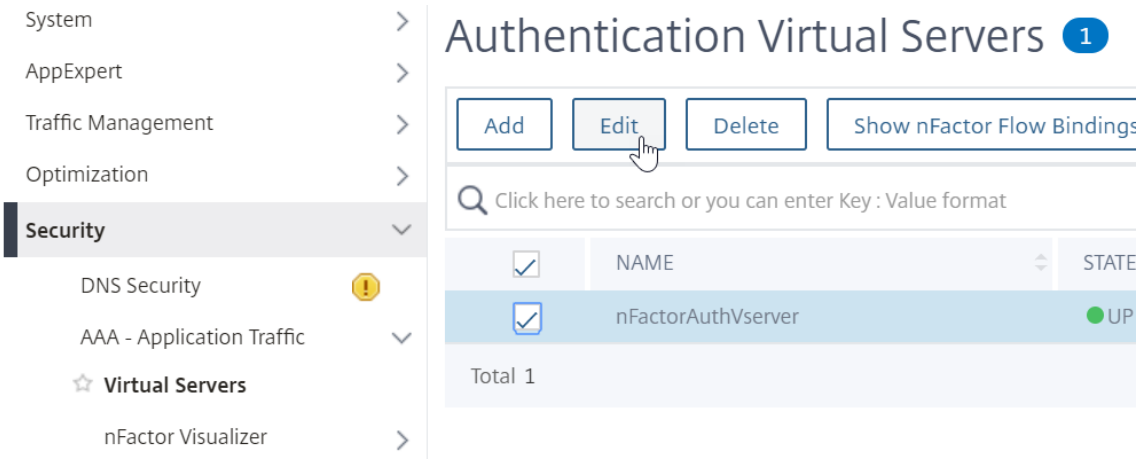
Etiqueta de directiva de autenticación de enlace

Después de crear la etiqueta de directiva, la vincula a un enlace de directiva de autenticación avanzada existente para encadenar los factores.

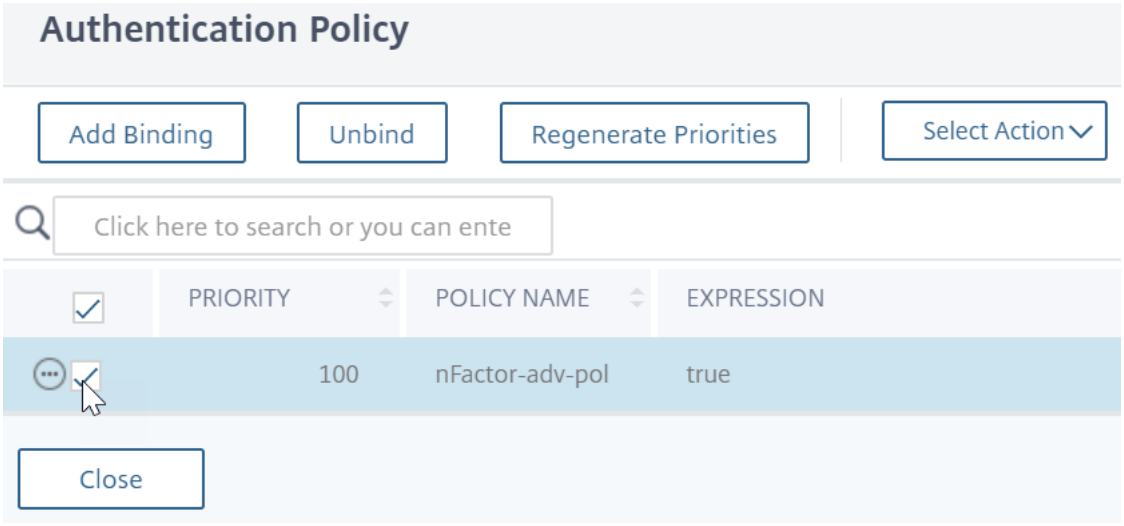
Puede seleccionar el siguiente factor al modificar un servidor virtual de autenticación, autorización y auditoría existente que tenga un límite de directiva de autenticación avanzada o al modificar una etiqueta de directiva diferente para incluir el siguiente factor.

Para modificar un servidor virtual de autenticación, autorización y auditoría existente que ya tiene una directiva de autenticación avanzada enlazada a él

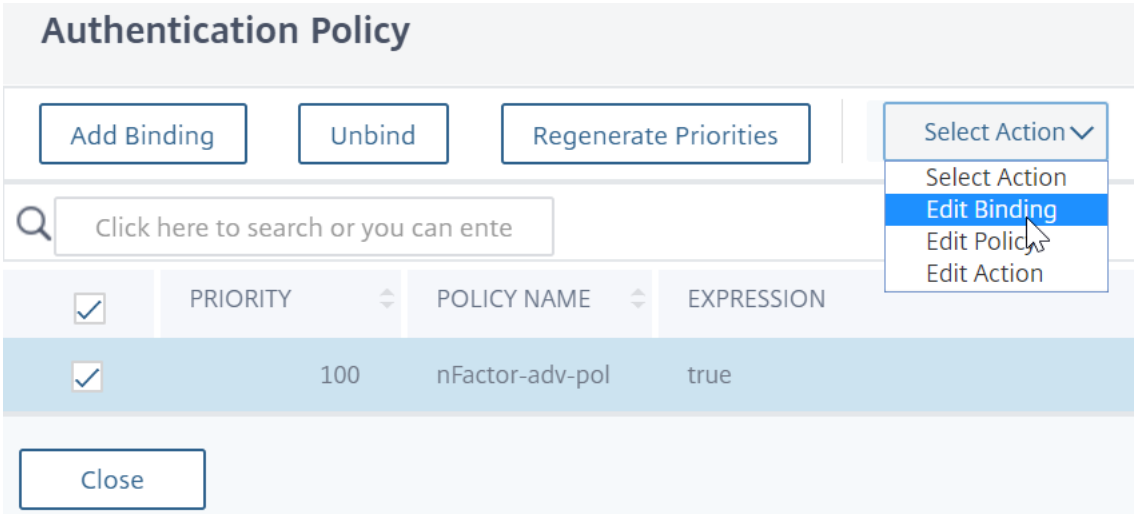
1. Vaya a **Seguridad > AAA — Tráfico de aplicaciones > Servidores virtuales.** Seleccione el servidor virtual y haga clic en **Modificar**.



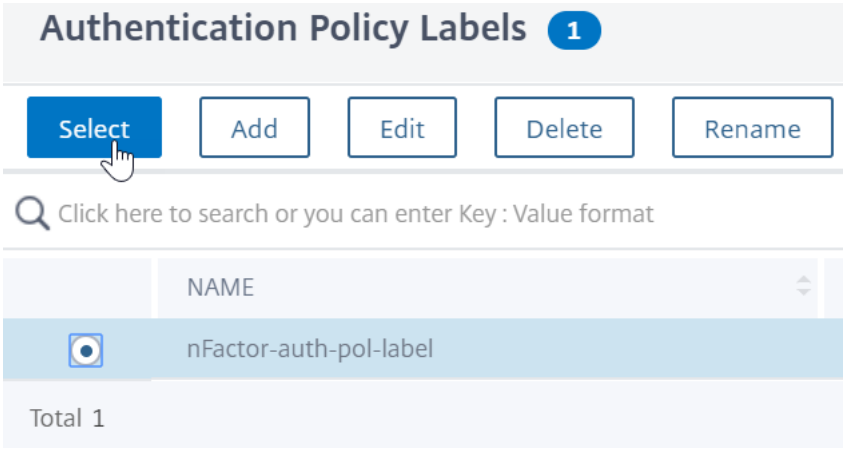
2. A la izquierda, en la sección **Directivas de autenticación avanzada**, haga clic en un enlace de directiva de autenticación existente.



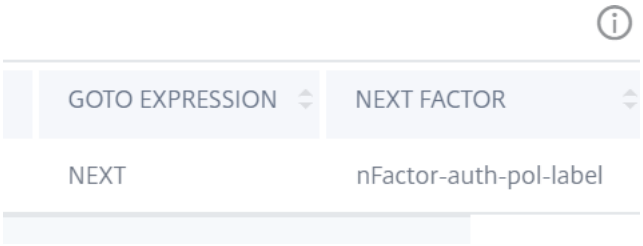
3. En **Seleccionar acción**, haga clic en **Modificar enlace**.



4. En **Seleccionar factor siguiente**, haga clic en y seleccione una etiqueta de directiva de autenticación existente (factor siguiente).

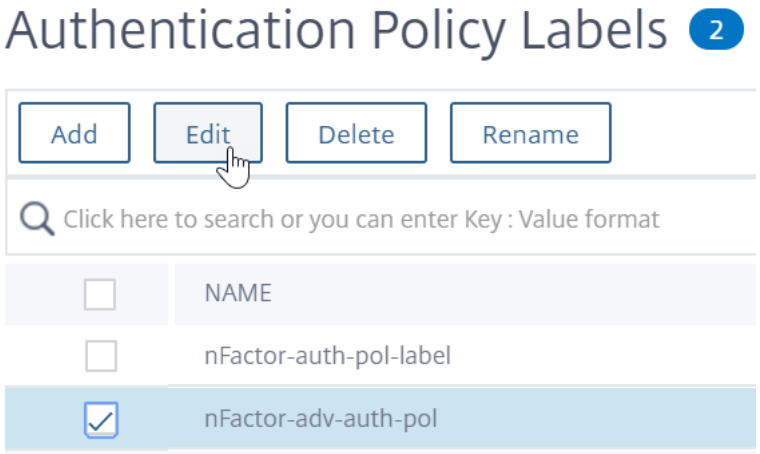


5. Haga clic en **Bind**. Puede ver el siguiente factor en el extremo derecho.

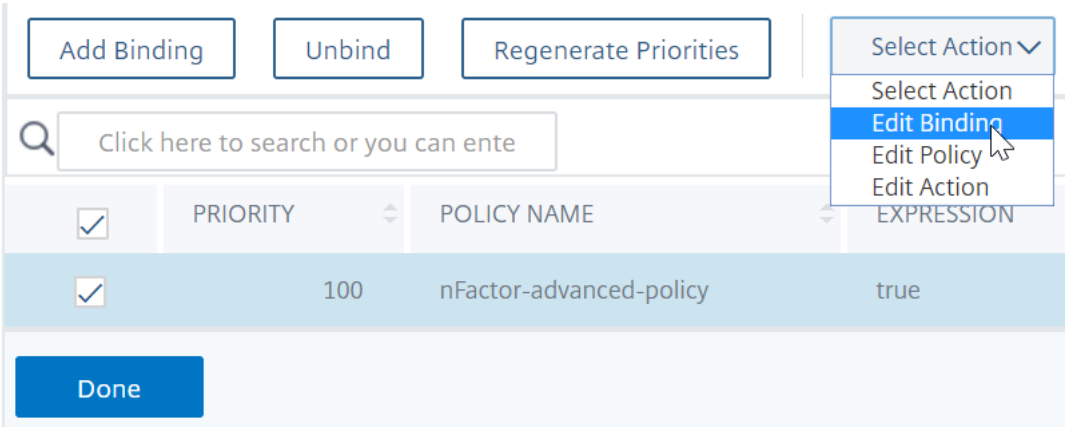


Para agregar un factor siguiente de etiqueta de directiva a otro rótulo de directiva

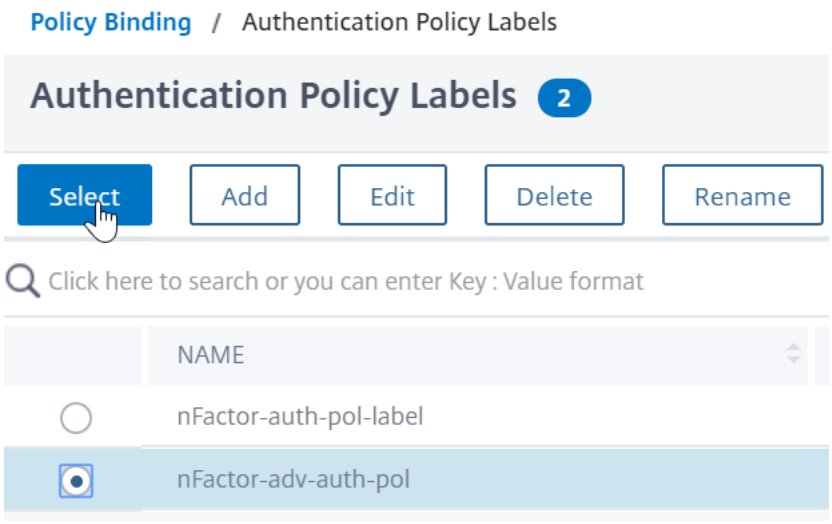
1. Vaya a **Seguridad > AAA — Tráfico de aplicaciones > Directivas > Autenticación > Directivas avanzadas > Etiqueta de directiva**. Seleccione una etiqueta de directiva diferente y haga clic en **Modificar.**



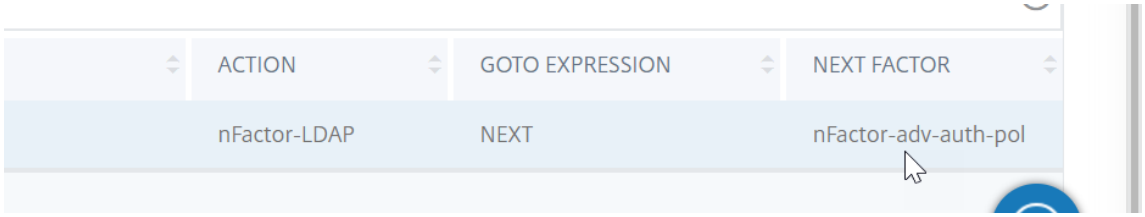
2. En **Seleccionar acción**, haga clic en **Modificar enlace**.



3. En **Detalles de enlace > Seleccionar factor siguiente**, haga clic para seleccionar el siguiente factor.
4. Elija la etiqueta de directiva para el siguiente factor y haga clic en el botón **Seleccionar**.



5. Haga clic en **Vincular**. Puede ver el siguiente factor a la derecha.

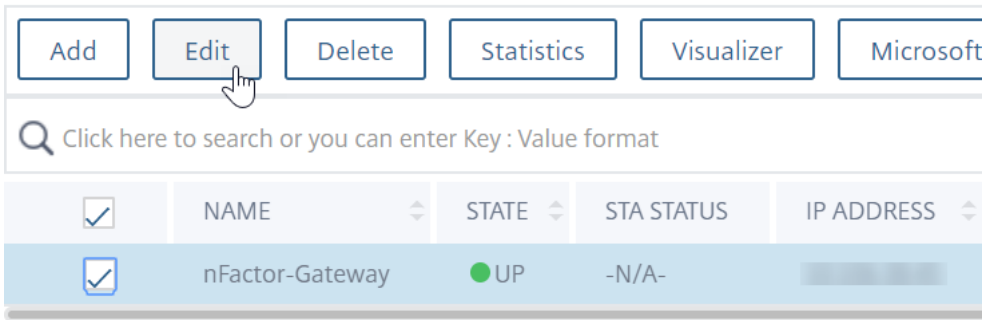


nFactor para Citrix Gateway

Para habilitar nFactor en Citrix Gateway, se debe vincular un perfil de autenticación a un servidor virtual de autenticación, autorización y auditoría.

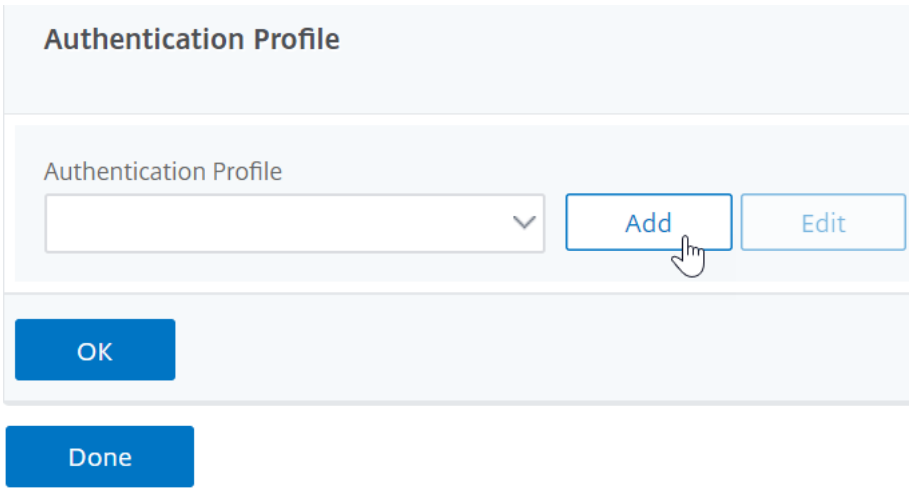
Crear un perfil de autenticación para vincular un servidor virtual de autenticación, autorización y auditoría con el servidor virtual Citrix Gateway

1. Vaya a **Citrix Gateway > Servidores virtuales** y seleccione un servidor virtual de puerta de enlace existente para modificarlo.

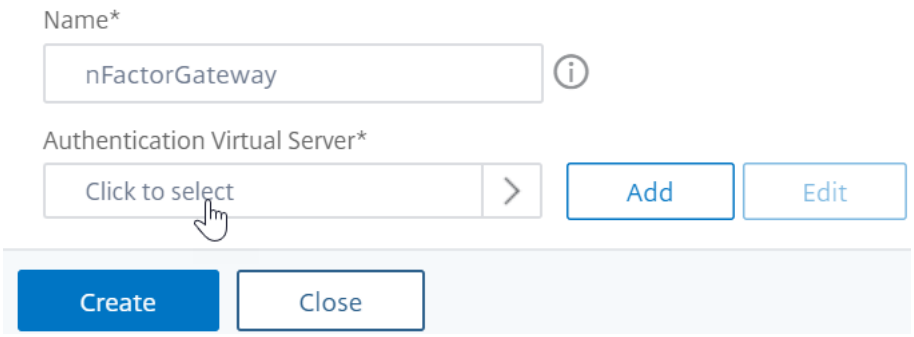


2. En **Configuración avanzada**, haga clic en **Perfil de autenticación**.

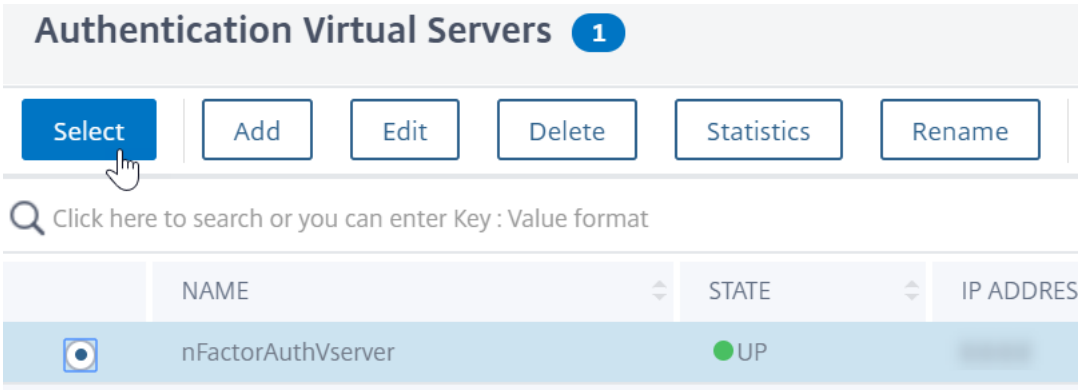
3. Haga clic en **Agregar** en **Perfil de autenticación**



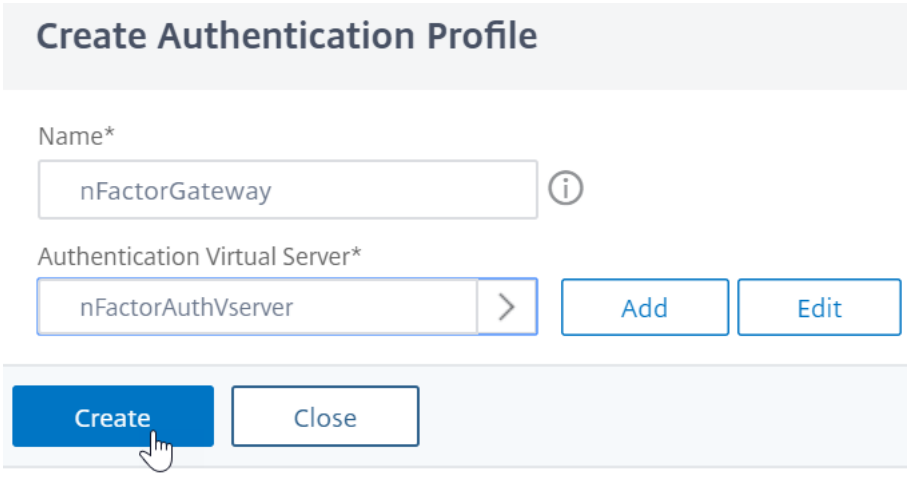
4. Introduzca el nombre del perfil de autenticación y haga clic donde dice **Haga clic para seleccionar**.



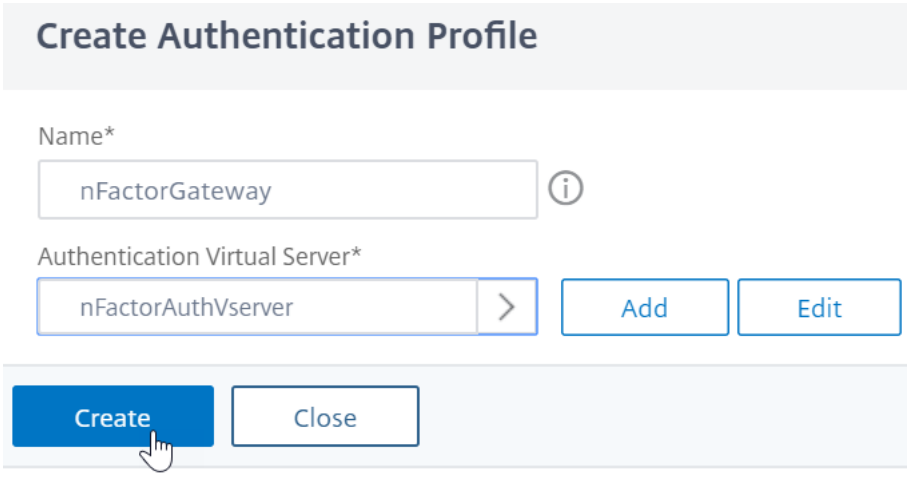
5. En **Servidor virtual de autenticación**, seleccione un servidor existente que tenga configurado el esquema de inicio de sesión, la directiva de autenticación avanzada y las etiquetas de directiva de autenticación. También puede crear un servidor virtual de autenticación. El servidor virtual de autenticación, autorización y auditoría no necesita una dirección IP. Haga clic en **Seleccionar**.



6. Haga clic en **Crear**.



7. Haga clic en **Aceptar** para cerrar la sección Perfil de autenticación.



Nota: Si ha configurado uno de los factores como certificados de cliente, debe configurar los parámetros SSL y el certificado de CA.

Después de haber completado la vinculación del perfil de autenticación a un servidor virtual de autenticación, autorización y auditoría, y cuando navega a su Citrix Gateway, puede ver las pantallas de autenticación de nFactor.

Configurar los parámetros SSL y el certificado de CA

Si uno de los factores de autenticación es un certificado, debe realizar alguna configuración SSL en el servidor virtual de Citrix Gateway.

1. Vaya a **Administración del tráfico > SSL > Certificados > Certificados de CA**e instale el certificado raíz del emisor de los certificados de cliente. Los certificados de la entidad emisora de certificados no necesitan archivos de claves.

   Si los perfiles SSL predeterminados están habilitados, significa que ya ha creado un perfil SSL

que tiene habilitada la autenticación de clientes.

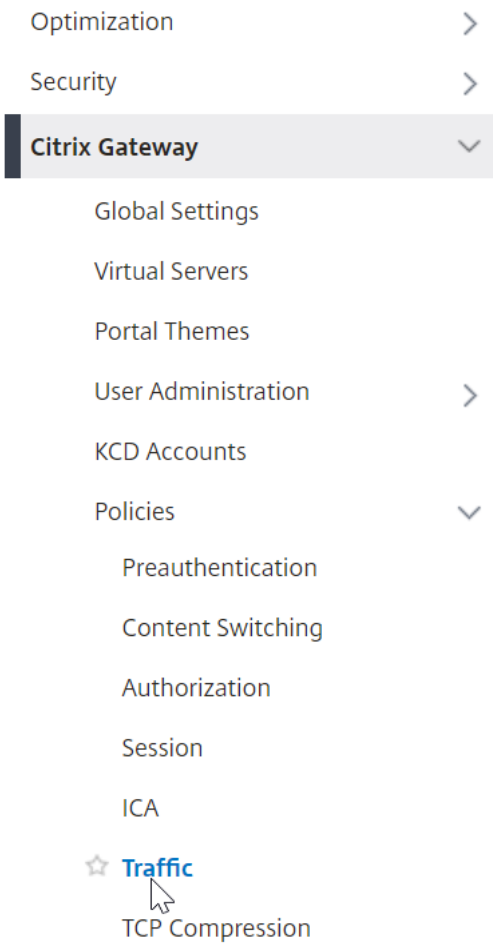
2. Vaya a **Citrix Gateway > Servidores virtuales** y modifique un servidor virtual Citrix Gateway existente habilitado para nFactor.
    - Si los perfiles SSL predeterminados están habilitados, haga clic en el icono de edición.
    - En la lista Perfil SSL, seleccione el perfil SSL que tiene habilitada la autenticación de cliente y defina el valor OPCIONAL.
    - Si los perfiles SSL predeterminados no están habilitados, haga clic en el icono de edición.
    - Marque la casilla Autenticación de cliente.
    - Asegúrese de que el certificado de cliente esté configurado en Opcional
3. Haga clic en OK.
4. En la sección Certificados, haga clic en **Sin certificado de CA.**
5. En Seleccionar certificado de CA, haga clic para seleccionar y seleccionar el certificado raíz del emisor de los certificados de cliente.
6. Haga clic en Bind.

Nota: Es posible que deba enlazar también cualquier certificado de CA intermedia que haya emitido los certificados de cliente.

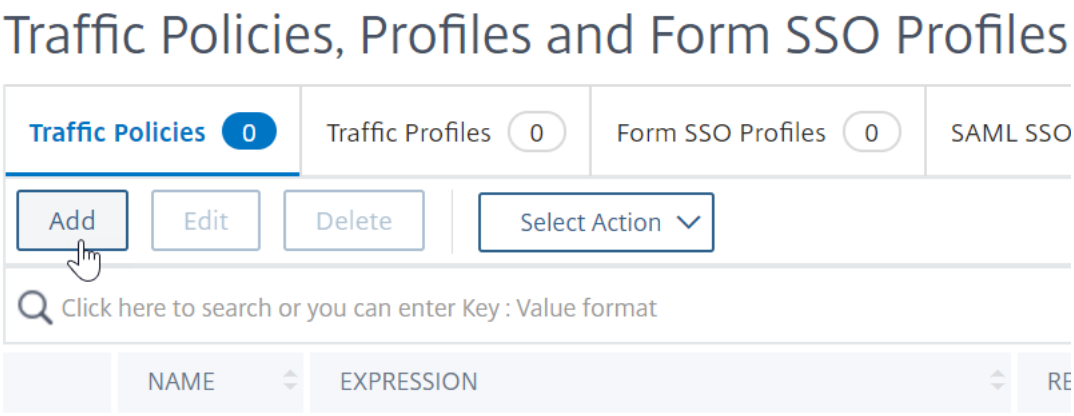
Configurar directiva de tráfico de Citrix Gateway para el inicio de sesión único de nFactor en StoreFront

Para el inicio de sesión único en StoreFront, nFactor utiliza de forma predeterminada la última contraseña introducida. Si LDAP no es la última contraseña introducida, debe crear una directiva/perfil de tráfico para anular el comportamiento predeterminado de nFactor.

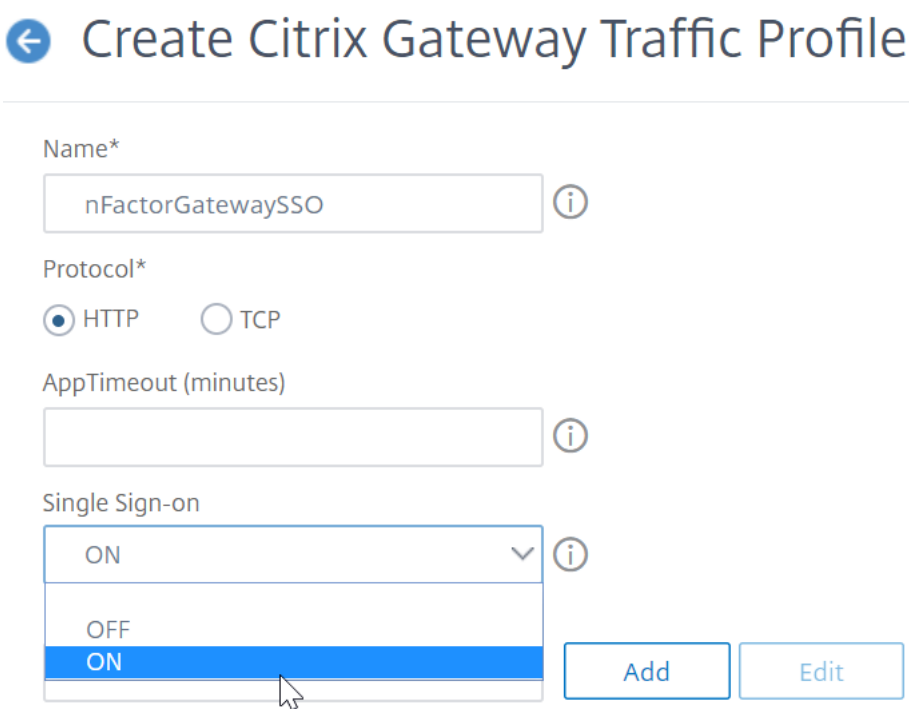
1. Vaya a **Citrix Gateway > Directivas > Tráfico**.



2. En la ficha **Perfiles de tráfico**, haga clic en **Agregar**.

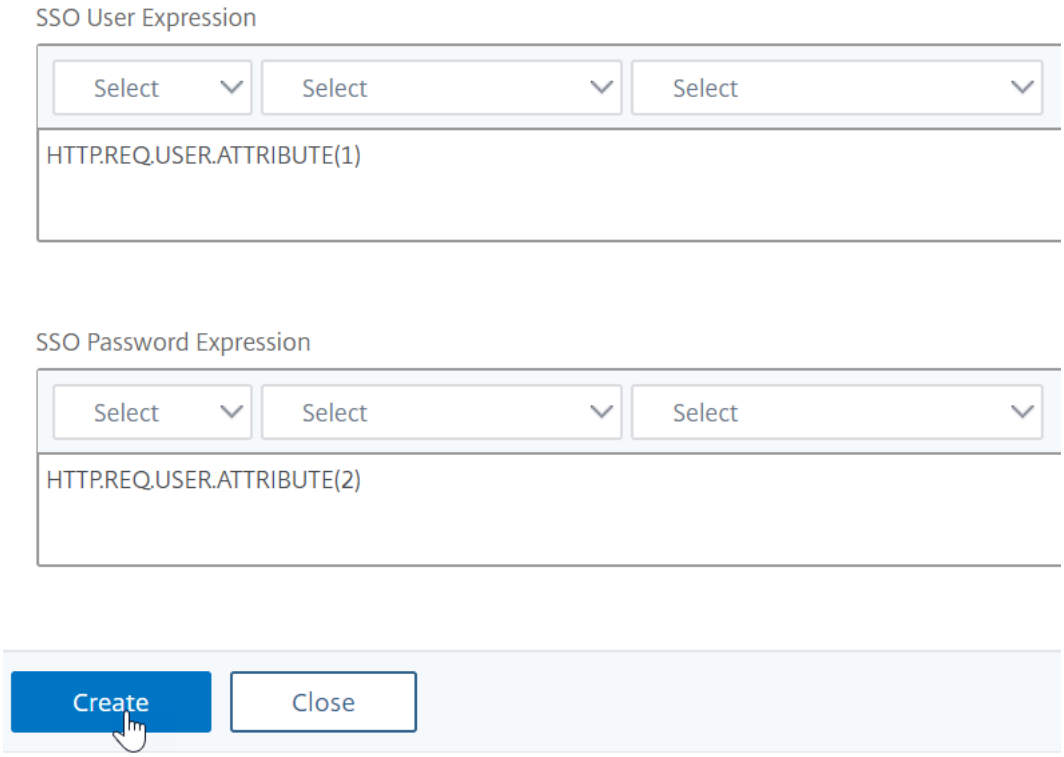


3. Introduzca un nombre para el perfil de tráfico. Seleccione el protocolo **HTTP**.
   En **Inicio de sesión único**, seleccione **ACTIVADO**.



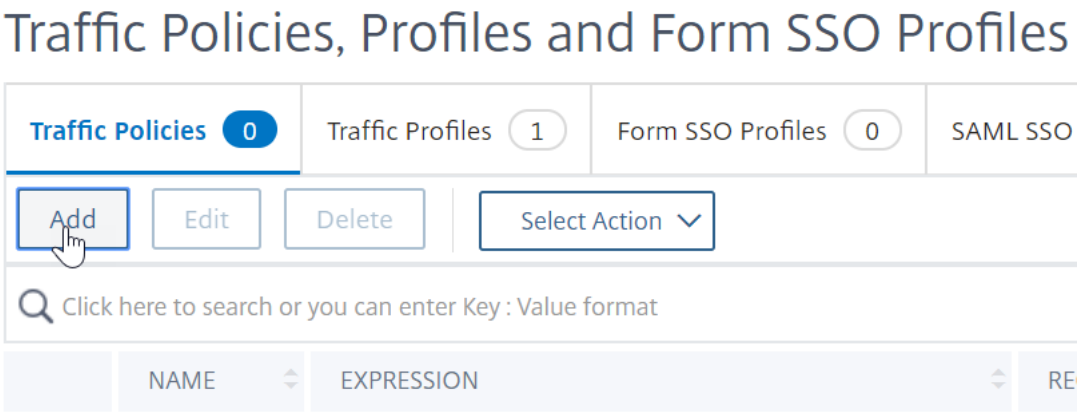
4. En la expresión de **SSO, introduzca una expresión**AAA.USER.ATTRIBUTE (#) que coincida con los índices especificados en el esquema de inicio de sesión y haga clic en **Crear**.

> **Nota**
>
> La expresión AAA.USER se ha implementado ahora para reemplazar las expresiones HTTP.REQ.USER obsoletas.



5. Haga clic en la ficha **Directivas de tráfico** y haga clic en **Agregar**.

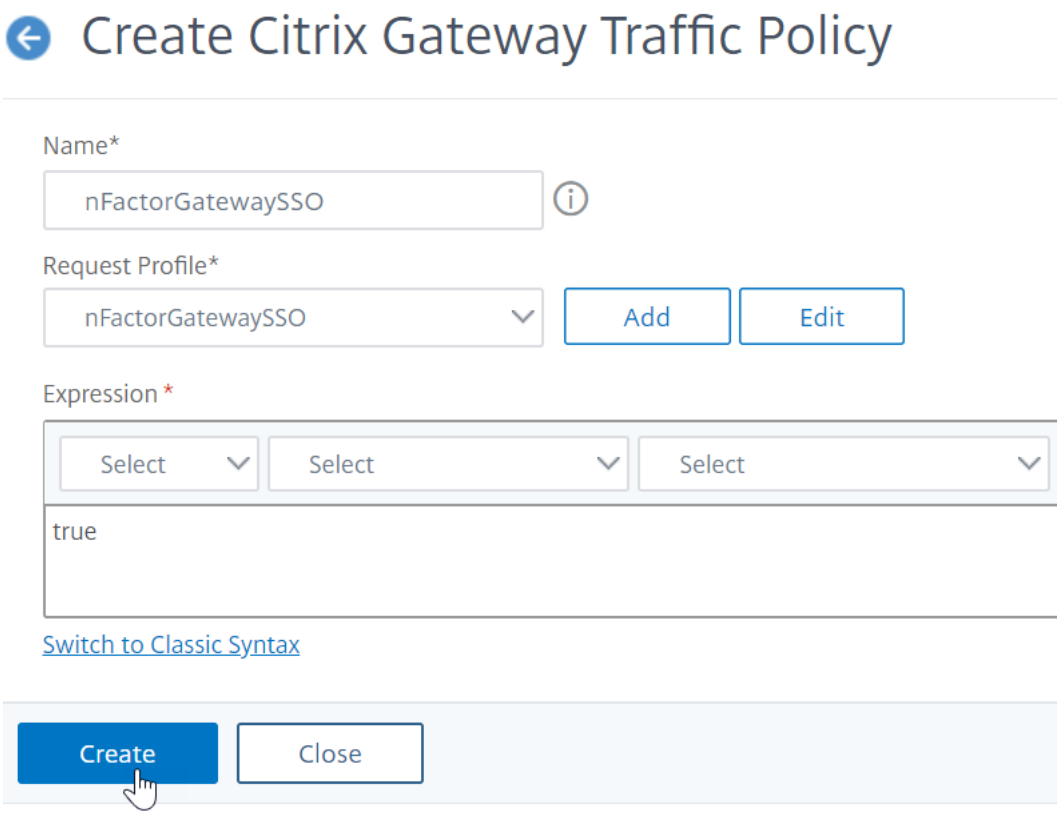
   Introduzca un nombre para la directiva.
   Seleccione el perfil de tráfico creado en el paso anterior.
   En **Expresión**, introduzca una expresión avanzada, por ejemplo true.
   Haga clic en **Crear**.



6. Vaya a **Citrix Gateway > Servidor virtual de Citrix Gateway**.

   - Seleccione un servidor virtual existente y haga clic en **Modificar**.
   - En la sección **Directivas**, haga clic en el signo **+**.
   - En **Elegir directiva**, seleccione **Tráfico**.
   - En **Elegir tipo**, seleccione **Solicitud**.

- Seleccione la directiva de tráfico que ha creado y, a continuación, haga clic en **Vincular**.



Fragmento de ejemplo sobre la configuración de nFactor mediante la CLI de Citrix ADC

Para comprender las configuraciones paso a paso para la autenticación nFactor, consideremos una implementación de autenticación de dos factores en la que el primer factor es la autenticación LDAP y el segundo factor es la autenticación RADIUS.

Esta implementación de ejemplo requiere que el usuario inicie sesión en ambos factores mediante un único formulario de inicio de sesión. Por lo tanto, definimos un único formulario de inicio de sesión que acepta dos contraseñas. La primera contraseña se utiliza para la autenticación LDAP y la otra para la autenticación RADIUS.
Estas son las configuraciones que se realizan:

1. Configurar el servidor virtual de equilibrio de carga para la autenticación

   add lb vserver lbvs89 HTTP 1.136.19.55 80 -AuthenticationHost auth56.aaatm.com -Autenticación ACTIVADA

2. Configure el servidor virtual de autenticación.

   agregar autenticación vserver auth56 SSL 10.106.30.223 443 -AuthenticationDomain aaatm.com

3. Configure el esquema de inicio de sesión para el formulario de inicio de sesión y enlácelo a una directiva de esquema de inicio de sesión.

   add authentication loginSchema login1 -authenticationSchema login-2passwd.xml -userCredentialIndex 1 -passwordCredentialIndex 2

   Nota:

   Use el nombre de usuario y una de las contraseñas introducidos en el esquema de inicio de sesión para el inicio de sesión único (SSO) en un servicio de back-end, por ejemplo, StoreFront. Puede hacer referencia a estos valores de índice en la acción de tráfico mediante la expresión AAA.USER.ATTRIBUTE (#). Los valores pueden estar entre 1 y 16.

   Como alternativa, puede utilizar las credenciales introducidas en el esquema de inicio de sesión como credenciales de inicio de sesión único mediante el siguiente comando.

```
add authentication loginSchema login1 -authenticationSchema login
   -2passwd.xml -SSOCredentials YES

 add authentication loginSchemaPolicy login1 -rule true -action
    login1
<!--NeedCopy-->
```

4. Configurar un esquema de inicio de sesión para la transferencia y vincularlo a una etiqueta de directiva

```
add authentication loginSchema login2 -authenticationSchema
   noschema

add authentication policylabel label1 -loginSchema login2
<!--NeedCopy-->
```

5. Configure las directivas LDAP y RADIUS.

```
add authentication ldapAction ldapAct1 -serverIP 10.17.103.28 -
   ldapBase "dc=aaatm, dc=com" -ldapBindDn administrator@aaatm.com
    -ldapBindDnPassword 81
   qw1b99ui971mn1289op1abc12542389b1f6c111n0d98e1d78ae90c8545901 -
   encrypted -encryptmethod ENCMTHD_3 -ldapLoginName
   samAccountName -groupAttrName memberOf -subAttributeName CN

add authentication Policy ldap -rule true -action ldapAct1
```



```
4
5 add authentication radiusAction radius -serverIP 10.101.14.3 -
      radKey
      n231d9a8cao8671or4a9ace940d8623babca0f092gfv4n5598ngc40b18876hj32
       -encrypted -encryptmethod ENCMTHD_3 -radNASip ENABLED -
      radNASid NS28.50 -radAttributeType 11 -ipAttributeType 8
6
7 add authentication Policy radius -rule true -action radius
8 <!--NeedCopy-->
```

6. Enlazar la directiva de esquema de inicio de sesión al servidor virtual de autenticación

```
1 bind authentication vserver auth56 -policy login1 -priority 1 -
      gotoPriorityExpression END
2 <!--NeedCopy-->
```

7. Enlazar la directiva LDAP (primer factor) al servidor virtual de autenticación.

```
1 bind authentication vserver auth56 -policy ldap -priority 1 -
      nextFactor label1 -gotoPriorityExpression next
2 <!--NeedCopy-->
```

8. Enlazar la directiva RADIUS (segundo factor) a la etiqueta de la directiva de autenticación.

```
1 bind authentication policylabel label1 -policyName radius -
      priority 2 -gotoPriorityExpression end
2 <!--NeedCopy-->
```

nFactor Visualizador para una configuración simplificada

February 19, 2022

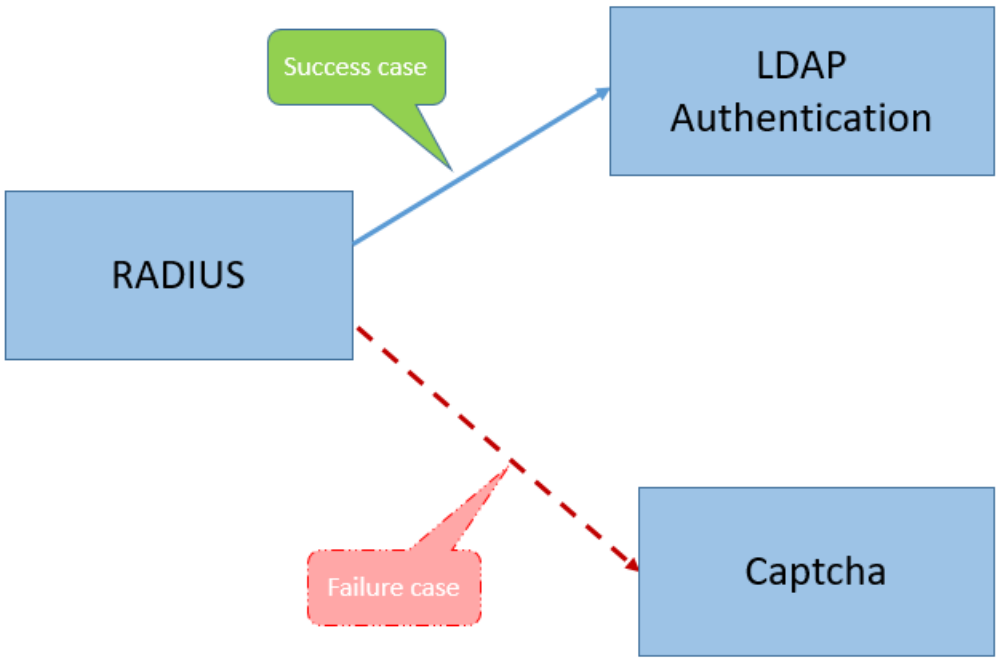
A partir de la versión 13.0 de Citrix ADC, compilación 36.27, la configuración de nFactor a través de la GUI se simplifica mediante el visualizador de nFactor. El visualizador nFactor ayuda a los administradores a agregar varios factores sin perder la noción de cada factor. El grupo de factores que se generan en el flujo se muestra en un solo lugar. Los administradores pueden agregar rutas de autenticación de éxito y error por separado. Después de crear el flujo, los administradores tienen que vincular el flujo de nFactor a un servidor virtual de autenticación.

> **Nota**
>
> - Todos los factores creados por un administrador en el flujo de nFactor se conservan para cualquier uso futuro.
> - Desde Citrix ADC, versión 13.0, compilación 64.35 y superior, mediante el visualizador nFactor, puede iniciar el flujo de nFactor con un bloque de decisión.

Anteriormente, la configuración nFactor era engorrosa, ya que los administradores tenían que visitar muchas páginas para configurarla. Si se requería un cambio, los administradores tenían que volver a visitar las secciones configuradas cada vez. Además, no había opción para ver la configuración completa en un solo lugar.

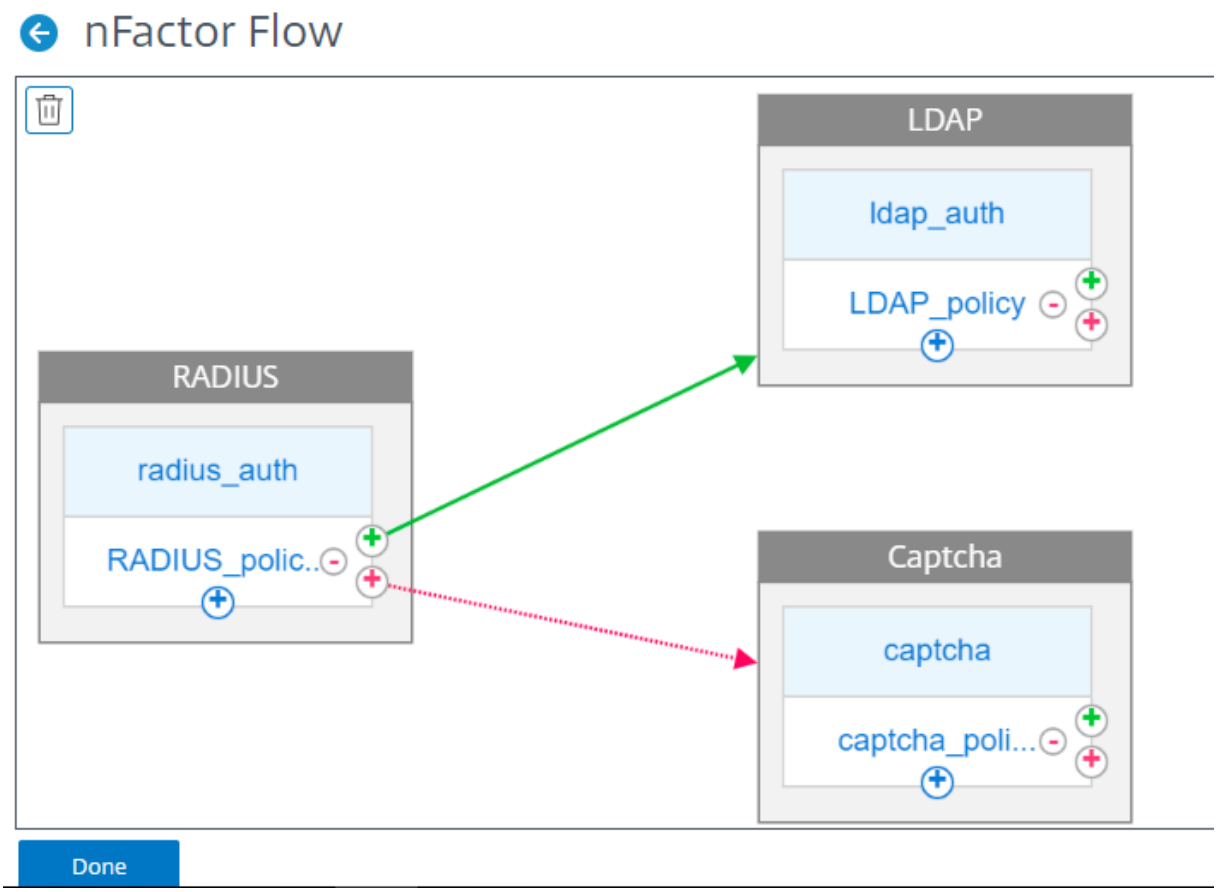
Caso de uso 1: RADIUS seguido de la autenticación LDAP; de lo contrario, se recurre a Captcha a través de Visualizador nFactor

Consiga la autenticación RADIUS como la autenticación de primer nivel seguida de la autenticación LDAP. En caso de que RADIUS falle, la autenticación debe volver a Captcha.



Para lograr este caso de uso, puede usar el visualizador nFactor. El Visualizador proporciona varios controles que se pueden utilizar para agregar este flujo y los elementos relacionados.

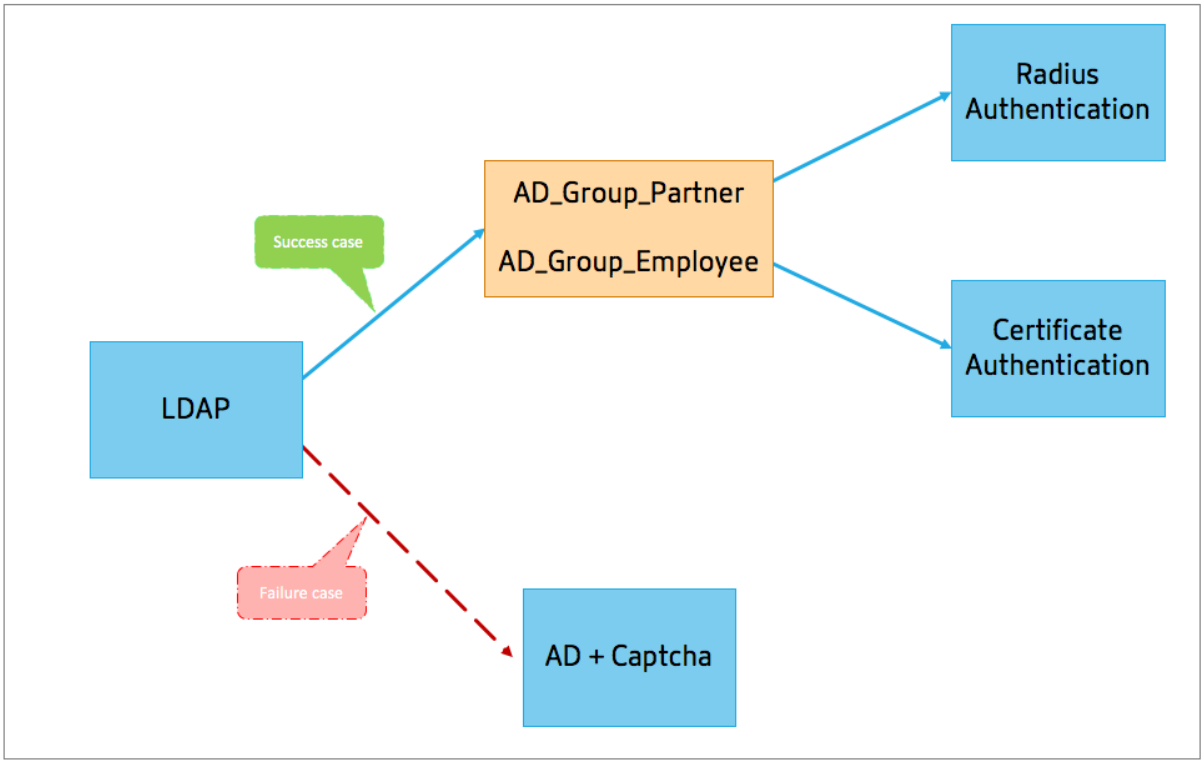
La siguiente ilustración muestra el flujo de nFactor creado para el caso de uso mencionado anteriormente mediante el visualizador.



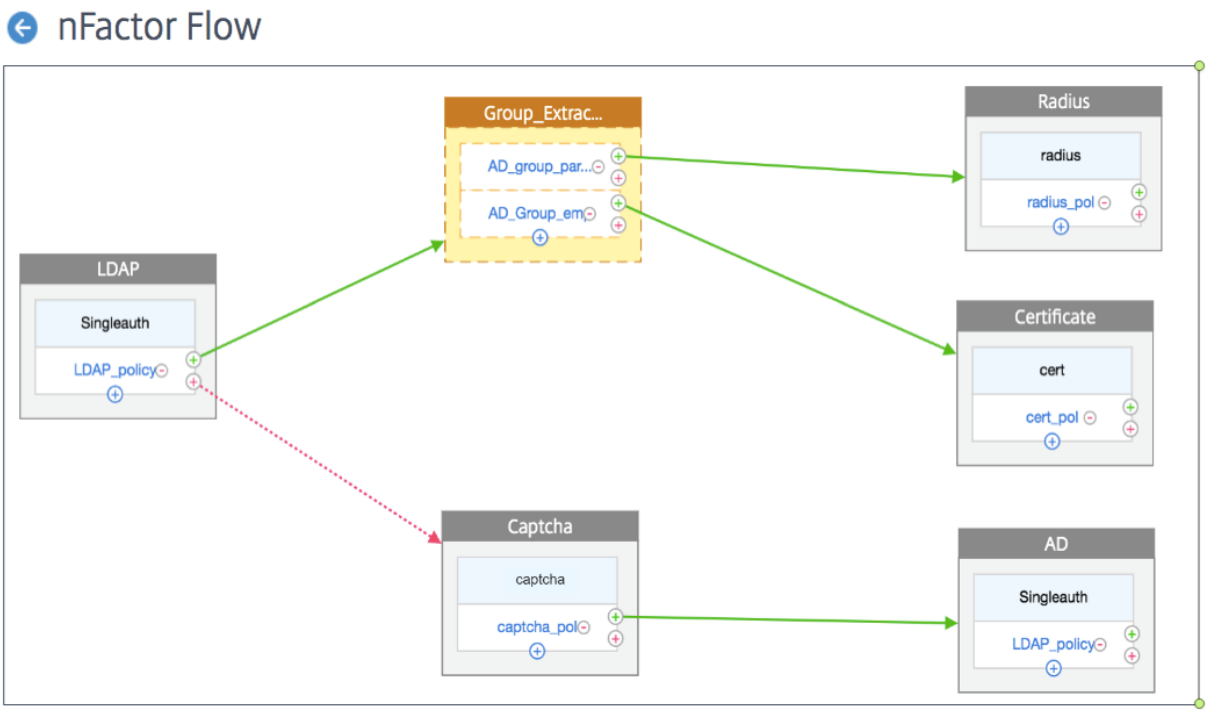
- **RADIO.** Configurar RADIUS como primer factor. Agregue un esquema de inicio de sesión y una directiva. En este ejemplo, radius_auth y Radius_Policy son el esquema de inicio de sesión y la directiva que se agregan. Para Radius_Policy, puede agregar otro factor para el caso de éxito. En este ejemplo, se agrega un bloque de factor LDAP para el caso de éxito. Para el caso de fallo, puede agregar un factor Captcha.
- **LDAP.** Configurar la autenticación LDAP como segundo factor. Agregue un esquema de inicio de sesión y una directiva. En este ejemplo, ldap_auth y LDAP_Policy son el esquema de inicio de sesión y la directiva que se agregan.
- **Captcha.** Para el caso de error de directiva RADIUS, se crea un factor Captcha. En este ejemplo, captcha y captcha_policy son el esquema de inicio de sesión y la directiva que se agregan.

Caso de uso 2: LDAP seguido de RADIUS/autenticación de certificados con Captcha basada en la pertenencia al grupo LDAP a través de Visualizador nFactor

Consiga la autenticación RADIUS como la autenticación de primer nivel seguida de la autenticación LDAP. En caso de que RADIUS falle, la autenticación debe volver a Captcha.



La siguiente ilustración muestra el flujo de nFactor creado para el caso de uso mencionado anteriormente mediante el visualizador.



- **LDAP.** Configurar LDAP como el primer factor. Agregue un esquema de inicio de sesión y una directiva. En este ejemplo, SingleAuth y LDAP_Policy son el esquema de inicio de sesión y la

directiva que se agregan. Para LDAP_Policy, puede agregar otro factor para el caso de éxito. En este ejemplo, se agrega un bloque de decisión para el caso de éxito. Para el caso de fallo, puede agregar Captcha seguido del factor AD.

- **LDAP de extracción de grupo.** Es el bloque de decisión agregado para el caso de éxito de LDAP. El bloque de decisión se utiliza como un factor de ramificación para ramificar los usuarios en función de las reglas de directiva. Visualizer permite configurar solo una directiva NO_AUTHN para el bloque de decisión.

  En este ejemplo, Group_Extraction_LDAP es el bloque de decisión. Agregue dos directivas (`AD_Group_Partner and AD_Group_Employee`) a este bloque de decisión. Como se explica en los casos de uso, todas las solicitudes enrutadas a través de la directiva AD_Group_Partner utilizan autenticación RADIUS. Por lo tanto, conecte el caso de éxito de esta directiva al siguiente factor que es el factor RADIUS. Del mismo modo, todas las solicitudes enrutadas a través de la directiva AD_Group_Employee utilizan autenticación de certificación. Por lo tanto, conecte el caso de éxito de esta directiva al siguiente factor que es el factor de autenticación de certificación.

  - **RADIO.** Para el caso de éxito de la directiva AD_Group_Partner, se crea el factor de autenticación RADIUS.
  - **Certificado.** Para el caso de éxito de la directiva AD_Group_Employee, se crea el factor de autenticación de certificado.

- **Captcha.** Para el caso de error de directiva LDAP, cree dos factores siguientes, Captcha y factor AD.

> **Nota**
>
> - Si tiene un caso de uso para ramificar como primera cosa, puede crear dos flujos y enlazar por separado o crear un flujo con el primero como rama de salida, y vincularlo al servidor virtual.
> - Si tiene varios bloques y para ver todo el flujo en la pantalla Flujo de nFactor, haga clic en el visualizador y arrastre el flujo hacia el extremo izquierdo.
> - Citrix recomienda modificar los flujos de nFactor mediante la página nFlujos de factor solamente.

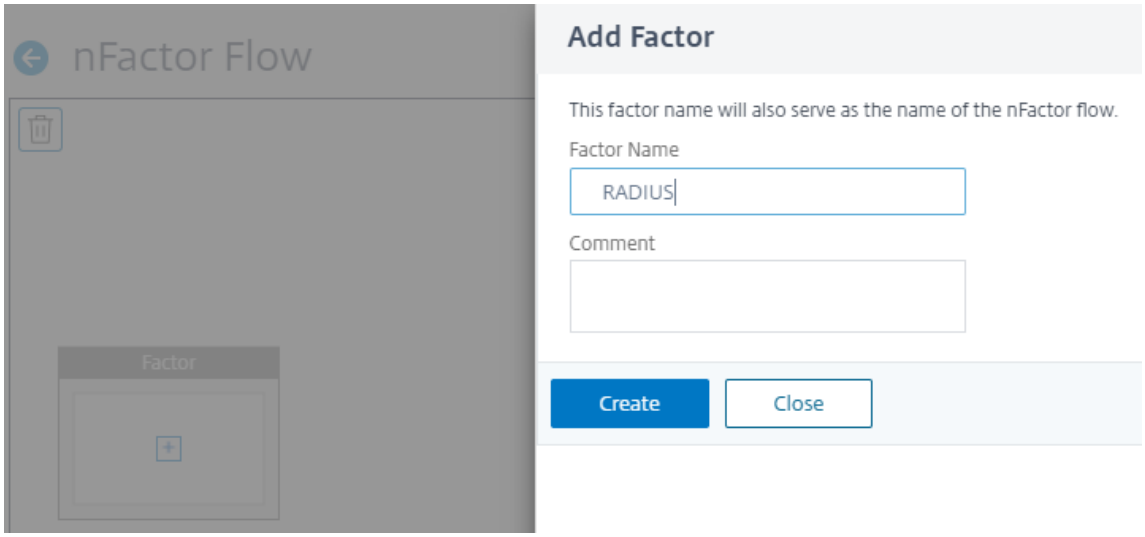
Para configurar nFactor mediante el visualizador nFactor

> **Nota**
>
> La siguiente configuración nFactor es un ejemplo sencillo que le ayuda a realizar las configuraciones de caso de caso de uso 1.

1. Vaya a **Seguridad > AAA: Tráfico de aplicaciones > Visualizador nFactor > Flujos de nFactor**.
2. Haga clic en **Agregar**.

3. En la **página Flujos de factor**, haga clic en **+** para agregar un primer factor para el flujo. El primer factor también sirve como un identificador para este flujo de nFactor.

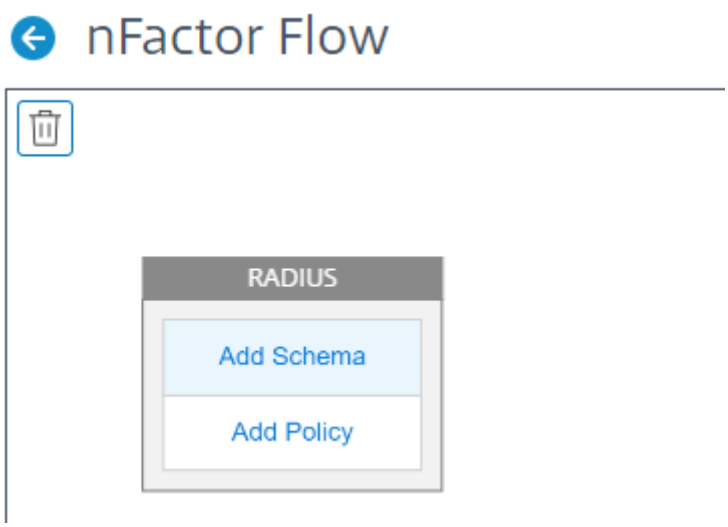
4. Introduzca el nombre del factor y haga clic en **Crear**.



El nombre del factor aparece en el bloque de factores en la página Flujo de nFactor.

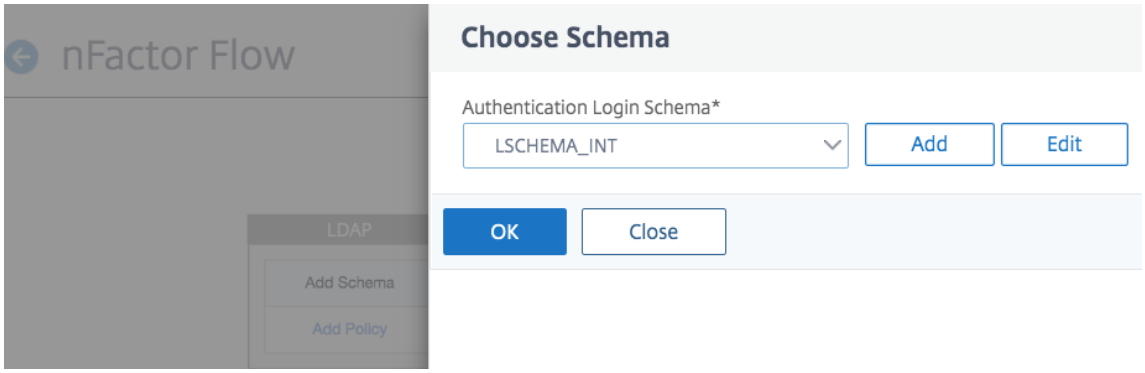
> **Nota**
>
> Citrix recomienda no utilizar nombres de etiqueta de directiva como,`__root` y `__<flow_name>`como sufijo y`_db_`prefijo. Se utiliza como los nombres de factores que se crean en el flujo de nFactor.

5. Una vez creado el factor RADIUS, se deben crear Agregar esquema y Agregar directiva.

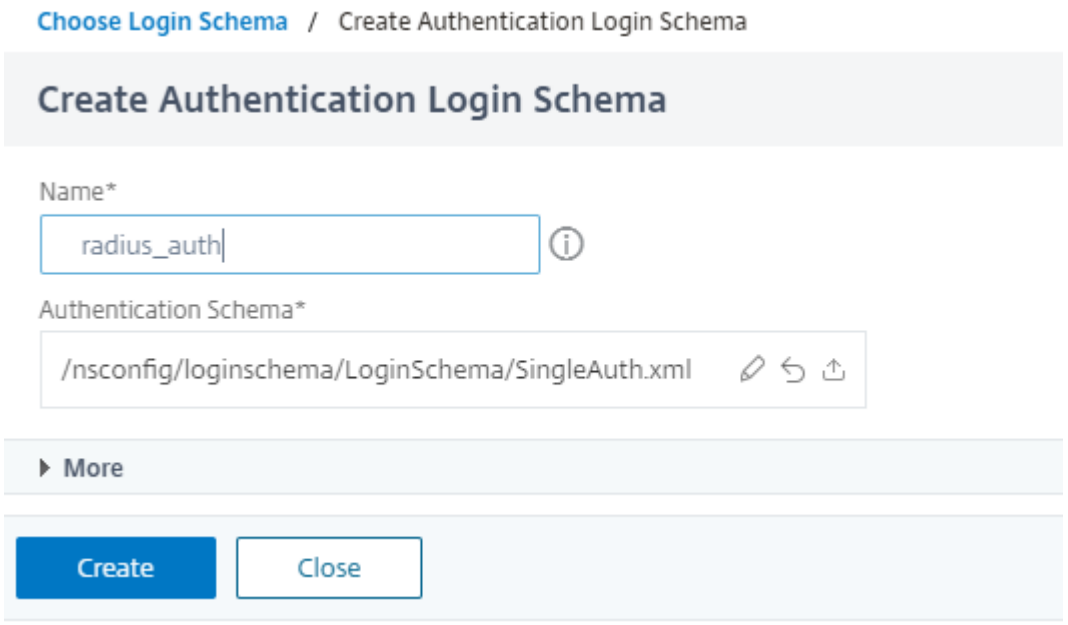


> **Nota**
>
> Para obtener más información, consulte Conceptos, entidades y terminología de nFactor.

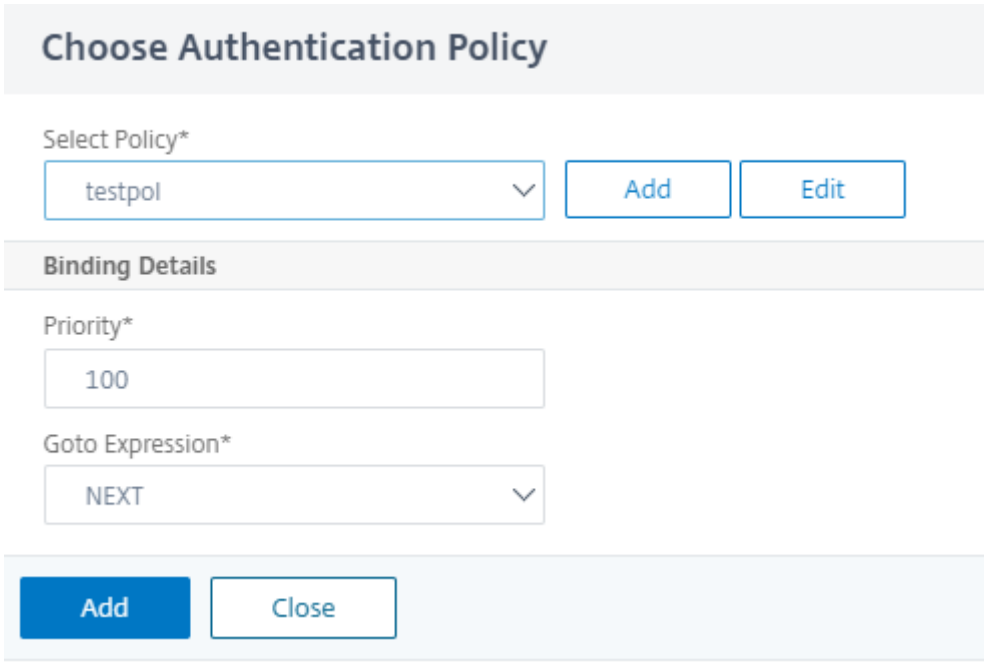
6. Haga clic en **Agregar esquema**. Puede agregar un nuevo esquema de inicio de sesión o seleccionar un esquema de inicio de sesión existente en la lista Esquema de **inicio de sesión de autenticación**.



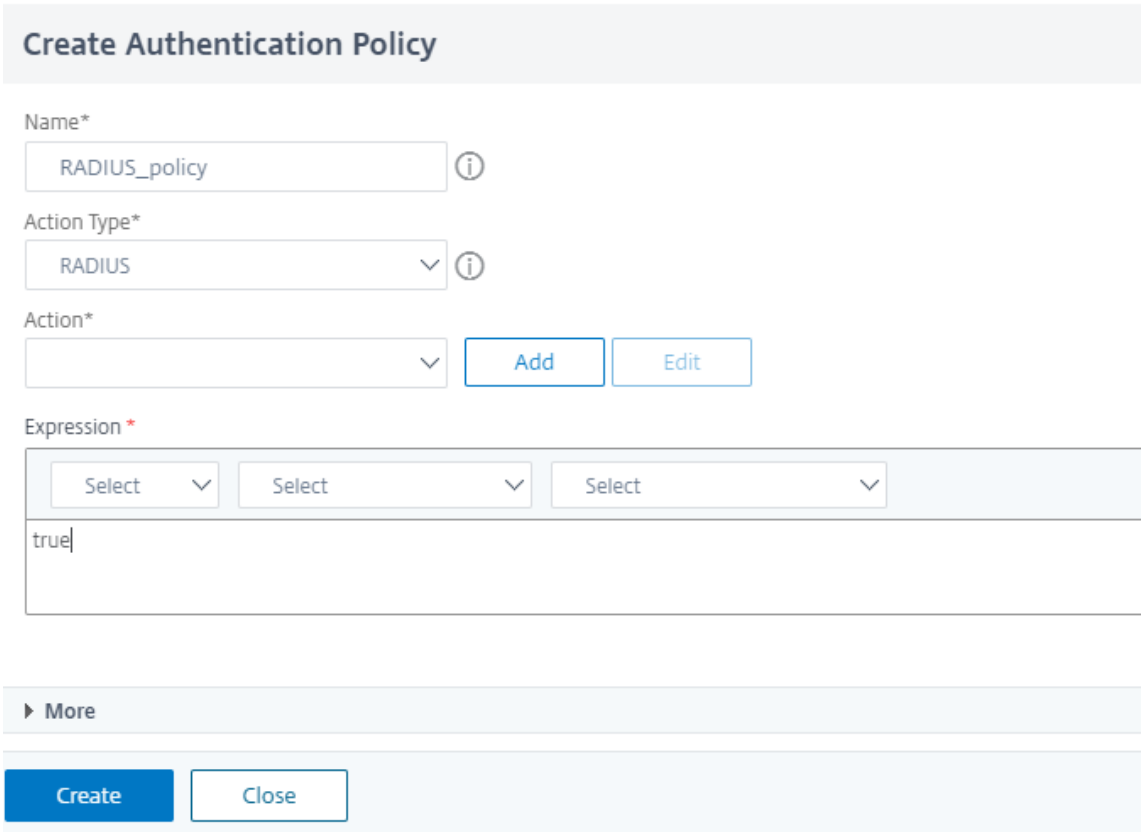
7. Para crear un esquema de inicio de sesión, haga clic en **Agregar** y, en la página **Crear esquema de inicio de sesión de autenticación**, escriba el nombre del esquema. Haga clic en **Modificar** (icono de lápiz) para seleccionar los **archivos de esquema de inicio** de sesión en la lista.



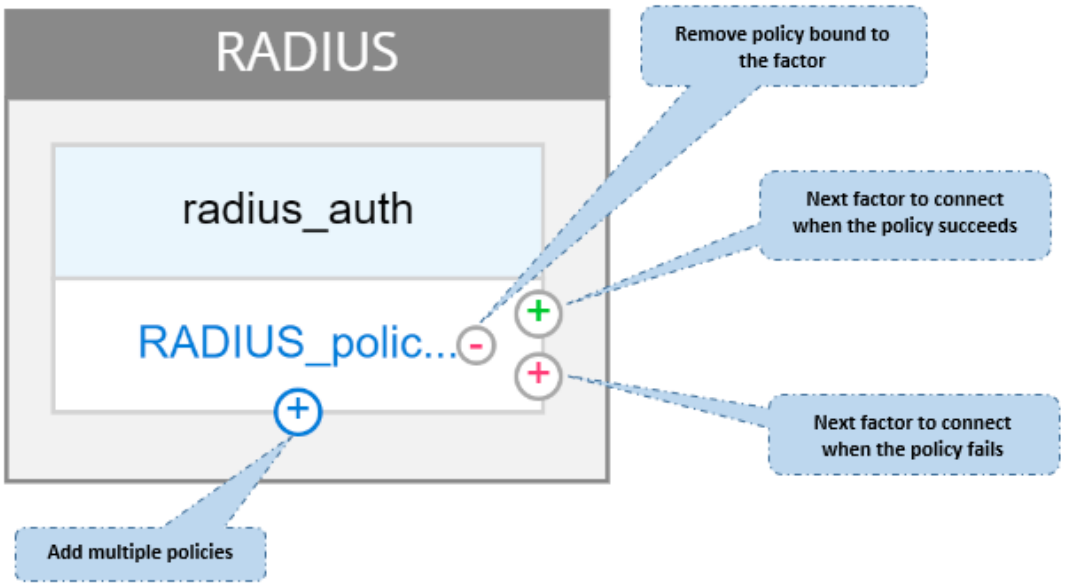
8. Haga clic en **Agregar directiva**. Puede crear una directiva de autenticación o seleccionar una directiva de autenticación existente.



9. Para crear una directiva nueva, haga clic en **Agregar** y, en la página **Crear directiva de autenticación**, escriba el nombre de la directiva y haga clic en **Crear**.



10. Después de agregar un esquema de inicio de sesión y una directiva al factor, el esquema de inicio de sesión y la directiva aparecen en el factor en el visualizador como se muestra en la siguiente ilustración. Para cualquier factor determinado, puede agregar varias directivas y definir el siguiente factor para el resultado correcto o incorrecto de cada directiva. También puede quitar las directivas que forman parte del factor.



11. Después de crear el flujo, puede enlazar el flujo de nFactor a un servidor virtual de autenticación.

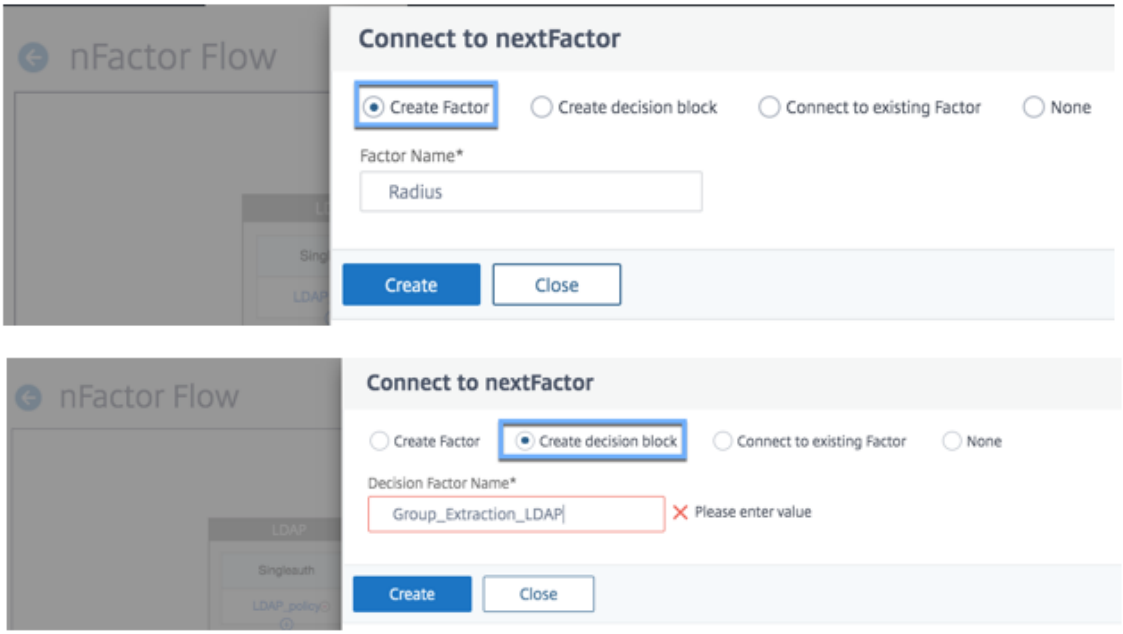
Agregar el siguiente factor

Para agregar el siguiente factor, puede seleccionar una de las siguientes opciones según su requisito:

- **Crear factor**. Cree un factor. Cada factor que se crea en un flujo es exclusivo de ese flujo.
- **Cree un bloque de decisión.** Cree un bloque de decisión que sirva como factor de ramificación. No puede agregar un esquema de inicio de sesión al bloque de decisión. Visualizer permite configurar solo una directiva NO_AUTHN para el bloque de decisión.

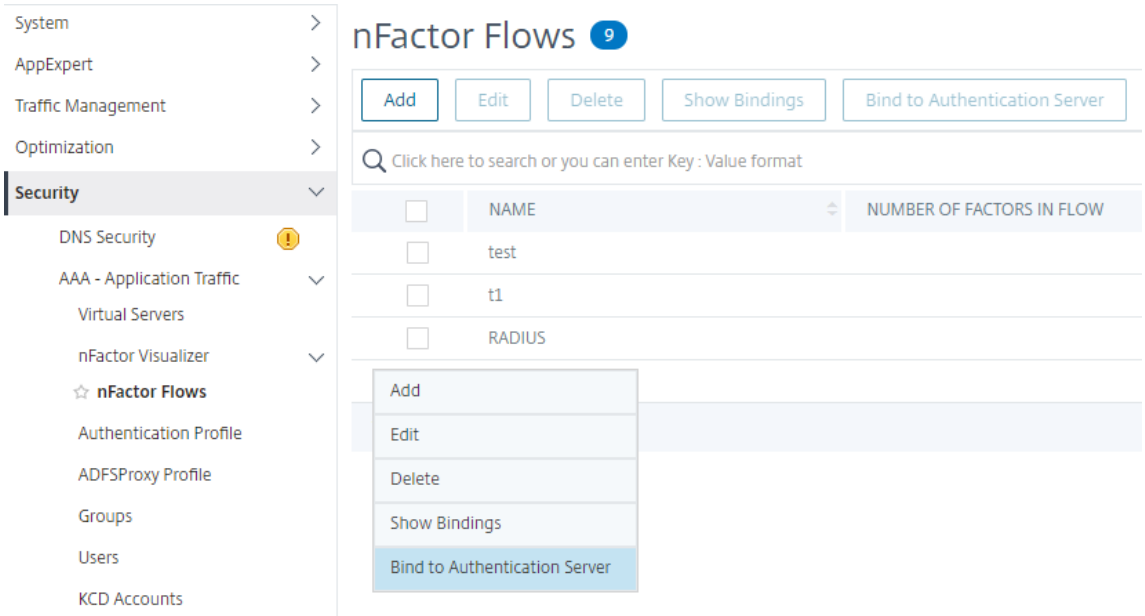
  > **Nota**
  >
  > Solo puede agregar o modificar el bloque de decisión a través de la GUI de Citrix ADC. No hay opción para configurar el bloque de decisión desde el comando CLI.

- **Conéctese a un factor existente**. Seleccione un factor existente como su siguiente factor. Todos los factores que aparecen en la lista existente se crean exclusivamente para ese flujo.
- **Ninguno.** Quitar una conexión existente.



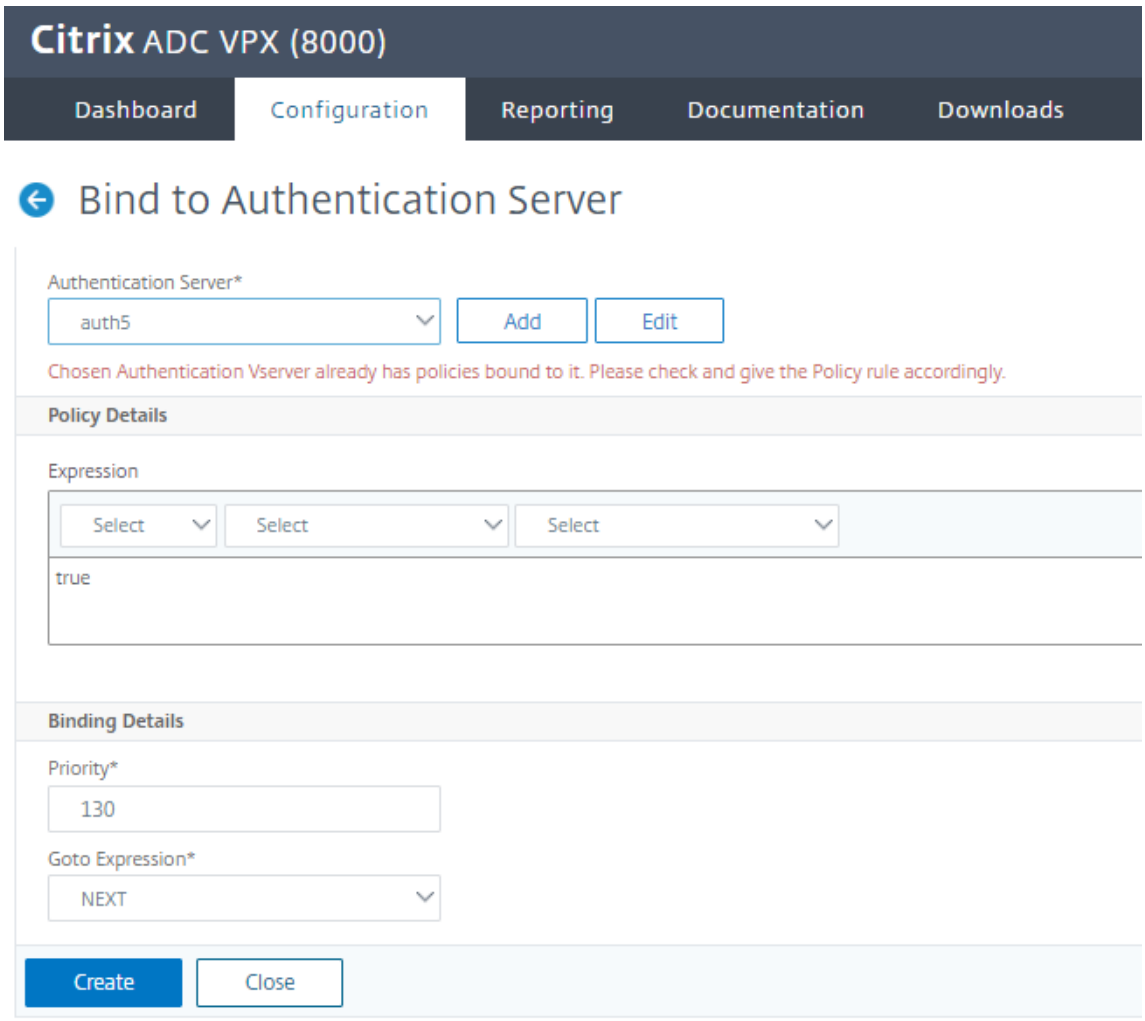
Para enlazar el flujo de nFactor al servidor de autenticación

1. En la página **Flujos de nFactor**, seleccione un flujo de nFactor que prefiera enlazar a un servidor virtual de autenticación.
2. Haga clic en el icono de tres líneas para seleccionar la opción **Vincular al servidor de autenticación** o, en el panel de detalles, haga clic en **Vincular al servidor de autenticación**.

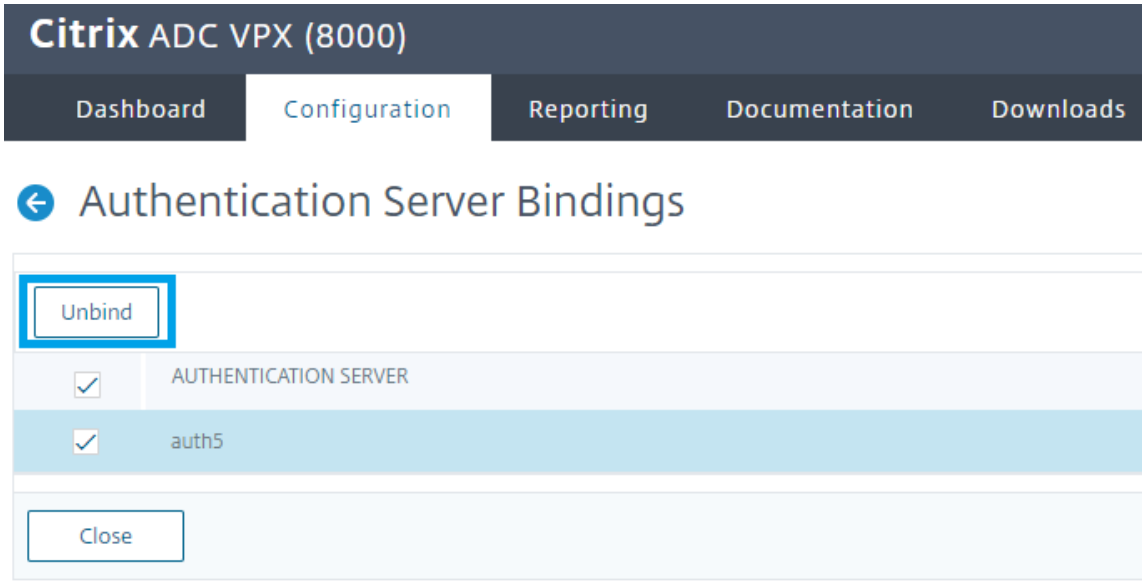


3. En la página **Vincular al servidor de autenticación**, puede realizar las siguientes acciones:
   - Para agregar un **servidor virtual de autenticación**, haga clic en **Agregar**.

- Para seleccionar un servidor de autenticación existente de la lista, haga clic en el campo **Servidor de autenticación**.



4. Haga clic en **Mostrar enlaces** en el icono de tres líneas para ver los enlaces.
5. Para desvincular el servidor de autenticación del flujo de nFactor específico, lleve a cabo los siguientes pasos:
   - En la página Flujo de **nFactor**, haga clic en **Mostrar enlaces** en el icono de hamburguesa.
   - En la página **Enlaces del servidor de autenticación**, seleccione el servidor de autenticación que quiere desenlazar y haga clic en **Desenlazar**. Haga clic en **Cerrar**.



Para obtener más información sobre la autenticación nFactor, consulte los temas siguientes:

- Concepto: Autenticación multifactor (nFactor).
- Flujo de trabajo: cómo funciona la autenticación nFactor.
- Configuración: configuración de la autenticación nFactor.

Mejoras en el visualizador nFactor

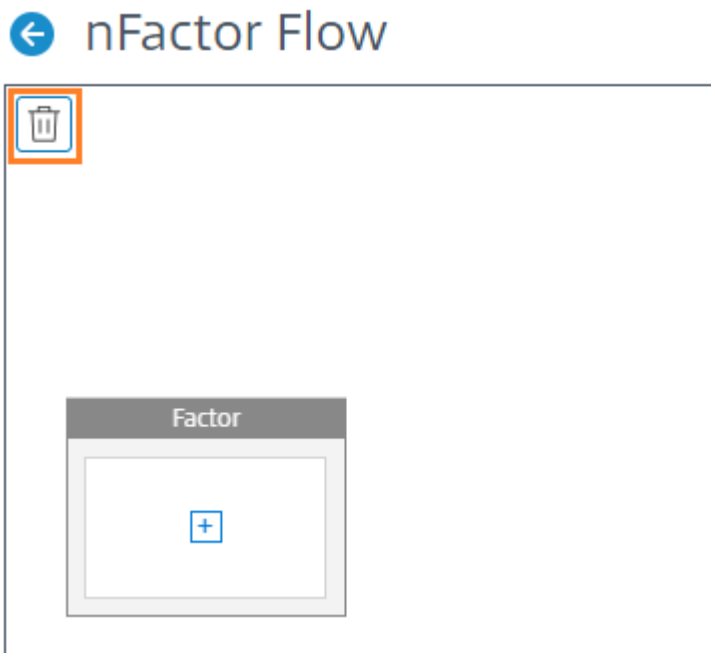
A partir de Citrix ADC versión 13.0 compilación 41.20, se realizan las siguientes mejoras en Visualizador nFactor.

- Los administradores pueden mover los factores creados al icono de la papelera.
- Vea los flujos nFactor en la página Servidor Virtual de Autenticación.

Icono de papelera. Los administradores solo pueden eliminar los nodos que no tienen conexiones. Sin embargo, las directivas subyacentes o los esquemas que se crean para el factor no se eliminan si el factor se mueve a la papelera.

Para ver el icono de papelera,

1. Vaya a **Seguridad > AAA: Tráfico de aplicaciones > Visualizador nFactor > Flujos de nFactor**.

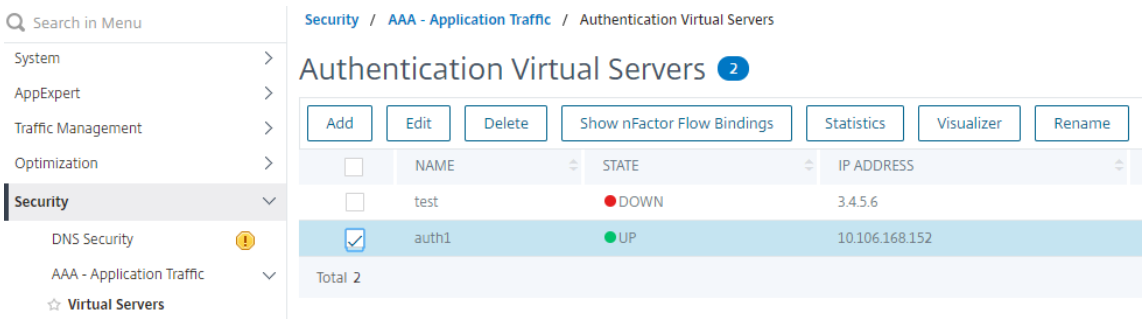


2. Para eliminar el factor, haga clic en el bloque de factores y arrástrelo a la papelera.

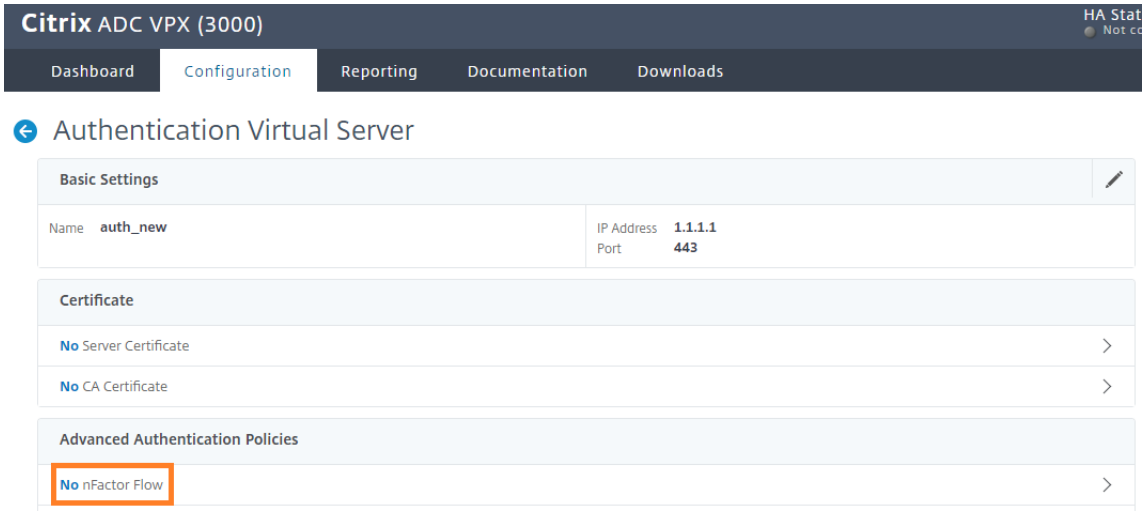
Ver el flujo de nFactor desde el servidor virtual de autenticación. Los administradores también pueden ver los flujos de NFactor creados desde la página Servidor Virtual de Autenticación.

Para ver el flujo de nFactor desde la página Servidor Virtual de Autenticación,

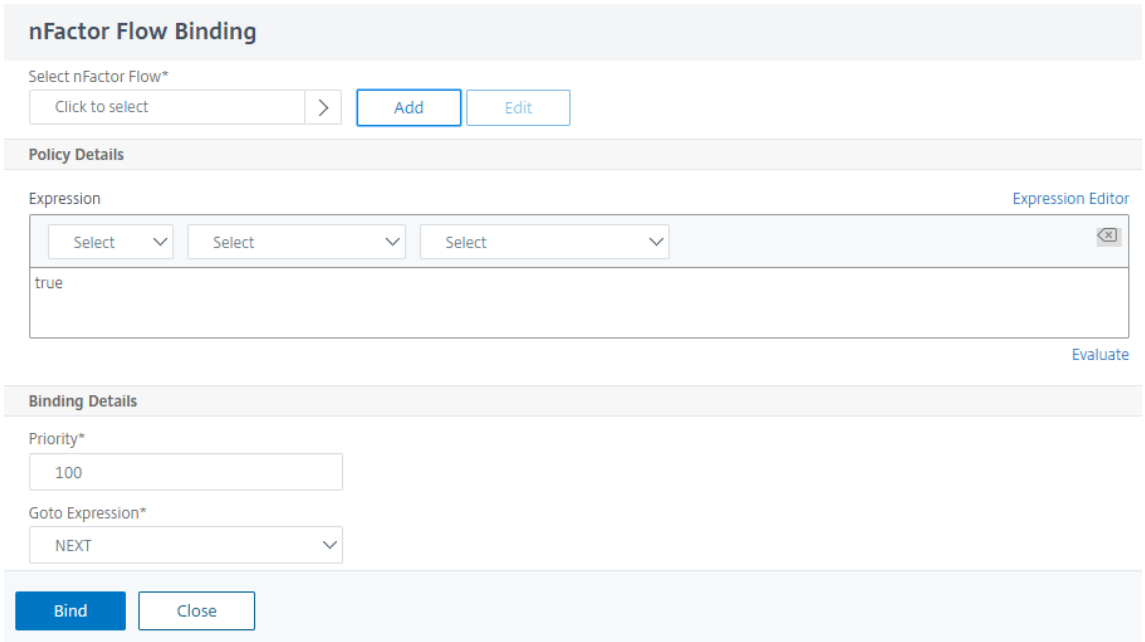
1. Vaya a **Seguridad > AAA — Tráfico de aplicaciones > Servidores virtuales**. En la página **Servidores virtuales de autenticación**, puede realizar los siguientes pasos:
   - Para agregar un servidor virtual de autenticación, haga clic en **Agregar**.
   - Para modificar un servidor virtual de autenticación existente, haga clic en la opción **Modificar** en el panel de detalles.



2. En la página **Servidor virtual de autenticación**, puede ver la opción **Flujo de nFactor** en **Directivas de autenticación avanzadas**.



3. Si no hay flujo de nFactor enlazado al servidor virtual, puede hacer clic en la opción **Sin flujo de nFactor** en la sección **Directivas de autenticación avanzadas** para agregar un nuevo flujo de nFactor o seleccionar el flujo de nFactor existente de la lista.



Extensibilidad nFactor

April 5, 2022

El marco de autenticación nFactor proporciona la flexibilidad de agregar personalizaciones para hacer que la interfaz de inicio de sesión sea más intuitiva para una experiencia de usuario enriquecida. Puede agregar etiquetas de inicio de sesión personalizadas, credenciales de inicio de sesión person-

alizadas, pantallas de interfaz de usuario personalizadas, etc.

Con nFactor, cada factor puede tener su propia pantalla de inicio de sesión. En cada pantalla de inicio de sesión puede presentar cualquier información de cualquiera de los factores anteriores o más información que sea invisible en otros factores. Por ejemplo, el último factor puede ser una página informativa en la que el usuario lea las instrucciones y haga clic en continuar.

Antes de nFactor, las páginas de inicio de sesión personalizadas eran limitadas y las personalizaciones necesitaban asistencia. Era posible reemplazar el archivo tmindex.html o aplicar reglas de reescritura para cambiar parte de su comportamiento. Sin embargo, no fue posible lograr la funcionalidad subyacente.

Las siguientes personalizaciones relacionadas con nFactor se capturan en detalle en este tema.

- Personalizar etiquetas de inicio
- Personalizar la interfaz de usuario para mostrar imágenes
- Personalizar el formulario de inicio de sesión de Citrix ADC

Supuestos

Conoce nFactor, comandos de Shell, XML y editores de texto.

Requisitos previos

- La personalización descrita en este tema solo es posible cuando el tema de la interfaz de usuario de RFweb (o basado en el tema) está configurado en Citrix ADC.
- La directiva de autenticación debe estar vinculada al servidor virtual de autenticación, autorización y auditoría; de lo contrario, el flujo no funciona según lo previsto.
- Tiene los siguientes artículos relacionados con nFactor
  - Esquema XML
  - JavaScript
  - Acciones de autenticación
  - Servidor virtual de autenticación
  - Citrix ADC versión 11.1 y posteriores

Personalizar las etiquetas de inicio

Para personalizar las etiquetas de inicio de sesión, necesita lo siguiente:

- El esquema XML que describe el aspecto de la página de inicio de sesión.
- El archivo script.js que contiene el JavaScript que se usa para cambiar el proceso de representación.

> **Nota:**
>
> El archivo script.js se encuentra en el directorio /var/netscaler/logon/themes/<custom_theme>/.

Funcionamiento

El JavaScript analiza el archivo XML y representa cada elemento dentro de la etiqueta <Requirements>. Cada elemento corresponde a una línea en el formulario HTML. Por ejemplo, un campo de inicio de sesión es una línea, el campo de contraseña es otra línea y también lo es el botón de inicio de sesión. Para introducir nuevas líneas, debe especificarlas en el archivo de esquema XML mediante el SDK de StoreFront. El SDK de StoreFront permite que la página de inicio de sesión con un esquema XML utilice la etiqueta <Requirement> y defina elementos en ella. Estos elementos permiten utilizar JavaScript para introducir en ese espacio los elementos HTML que se requieran. En este caso, se crea una línea con texto en forma de HTML.

El XML que se puede utilizar es el siguiente:

```
<Requirement>
<Credential>
<Type>nsg-custom-cred</Type>
<ID>passwd</ID>
</Credential>
<Label>
<Type>nsg-custom-label</Type>
</Label>
</Requirement>
<!--NeedCopy-->
```

<Requirement>: espacio proporcionado en la página de inicio de sesión. La credencial llena el espacio y las demás partes dirigen el motor a la información correcta. En este caso, escriba nsg-custom-cred. Se define como texto sin formato y la etiqueta se define para su cuerpo.
El XML requerido se combina con el código JavaScript para obtener los resultados requeridos.

```
// Custom Label Handler for Self Service Links
CTXS.ExtensionAPI.addCustomAuthLabelHandler({

getLabelTypeName: function () {
  return "nsg-custom-label";  }
 ,
getLabelTypeMarkup: function (requirements) {
```



```
8
9  return $("< Enter your HTML codes here>");
10  }
11  ,
12 // Instruction to parse the label as if it was a standard type
13 parseAsType: function () {
14
15 return "plain";
16  }
17
18  }
19  );
20 //Custom Credential Handler for Self Service Links
21 CTXS.ExtensionAPI.addCustomCredentialHandler({
22
23 getCredentialTypeName: function () {
24   return "nsg-custom-cred";  }
25  ,
26 getCredentialTypeMarkup: function (requirements) {
27
28 return $("<div/>");
29  }
30  ,
31  }
32  );
33 <!--NeedCopy-->
```

> **Importante:**
>
> Cuando agregue el código HTML, asegúrese de que el valor devuelto comienza con una etiqueta HTML.

La parte XML indica la página de inicio de sesión qué mostrar y el código JavaScript proporciona el texto real. El gestor de credenciales abre el espacio y la etiqueta llena el espacio. Como todo el tráfico de autenticación ahora es invisible para reescribir y responder, puede cambiar el aspecto de la página. Configuración para personalizar etiquetas de inicio de sesión

1. Crea y enlaza un tema basado en RfWeb.

```
1 add vpn portaltheme RfWebUI_MOD -basetheme RfWebUI
2
3 bind vpn vserver TESTAAA  - portaltheme RfWebUI_MOD
4 <!--NeedCopy-->
```


La ruta de los archivos basados en el tema está disponible en el directorio; /var/Netscaler/logon/themes/rfwebui_mod

2. Agrega el siguiente fragmento al final del archivo script.js:

> **Nota:**
>
> Si no se incluyen las líneas anteriores dentro del archivo correcto o si no se incluyen las funciones de JavaScript, se evita que se cargue el XML. El error solo se puede ver en la consola de desarrollador del explorador web con el siguiente texto: "Tipo sin definir `nsg-custom-cred`".

```
// Custom Label Handler for Self Service Links
CTXS.ExtensionAPI.addCustomAuthLabelHandler({

getLabelTypeName: function () {
  return "nsg-custom-label";  }
 ,
getLabelTypeMarkup: function (requirements) {

return $("<a href="https://identity.test.com/identity/faces/
   register" style="font-size: 16px;" style="text-align: center;">
   Self Registration</a><br><a href="https://identity.test.com/
   identity/faces/forgotpassword" style="font-size: 16px;" style="
   text-align: center;">Forgot Password</a><br><a href="https://
   identity.test.com/identity/faces/forgotuserlogin" style="font-
   size: 16px;" style="text-align: center;">Forgot User Login</a
   >");
 }
 ,
// Instruction to parse the label as if it was a standard type
parseAsType: function () {

return "plain";
 }

 }
 );
//Custom Credential Handler for Self Service Links
CTXS.ExtensionAPI.addCustomCredentialHandler({

getCredentialTypeName: function () {
  return "nsg-custom-cred";  }
 ,
```



```
getCredentialTypeMarkup: function (requirements) {

return $("<div/>");
 }
 ,
 }
 );
<!--NeedCopy-->
```

> **Importante:**
>
> Cuando agregue el código HTML, asegúrese de que el valor devuelto comienza con una etiqueta HTML.

Esquema de inicio de sesión utilizado en este ejemplo

```
<?xml version="1.0" encoding="utf-8"?>
<AuthenticateResponse xmlns="http://citrix.com/authentication/response
   /1">
<Status>success</Status>
<Result>more-info</Result>
<StateContext/>
<AuthenticationRequirements>
<PostBack>/nf/auth/doAuthentication.do</PostBack>
<CancelPostBack>/Citrix/Authentication/ExplicitForms/CancelAuthenticate
   </CancelPostBack>
<CancelButtonText>Cancel</CancelButtonText>
<Requirements>
<Requirement>
<Credential>
<ID>login</ID>
<SaveID>Username</SaveID>
<Type>username</Type>
</Credential>
<Label>
<Text>User name</Text>
<Type>plain</Type>
</Label>
<Input>
<AssistiveText>Please supply either domain\username or user@fully.
   qualified.domain</AssistiveText>
<Text>
<Secret>false</Secret>
<ReadOnly>false</ReadOnly>
```



```
<InitialValue></InitialValue>
<Constraint>.+</Constraint>
</Text>
</Input>
</Requirement>
<Requirement>
<Credential>
<ID>passwd</ID>
<SaveID>Password</SaveID>
<Type>password</Type>
</Credential>
<Label>
<Text>Password:</Text>
<Type>plain</Type>
</Label>
<Input>
<Text>
<Secret>true</Secret>
<ReadOnly>false</ReadOnly>
<InitialValue/>
<Constraint>.+</Constraint>
</Text>
</Input>
</Requirement>
<Requirement>
<Credential>
<Type>nsg-custom-cred</Type>
<ID>passwd</ID>
</Credential>
<Label>
<Type>nsg-custom-label</Type>
</Label>
</Requirement>
<Requirement>
<Credential>
<ID>loginBtn</ID>
<Type>none</Type>
</Credential>
<Label>
<Type>none</Type>
</Label>
<Input>
<Button>Please Log On</Button>
</Input>
</Requirement>
```

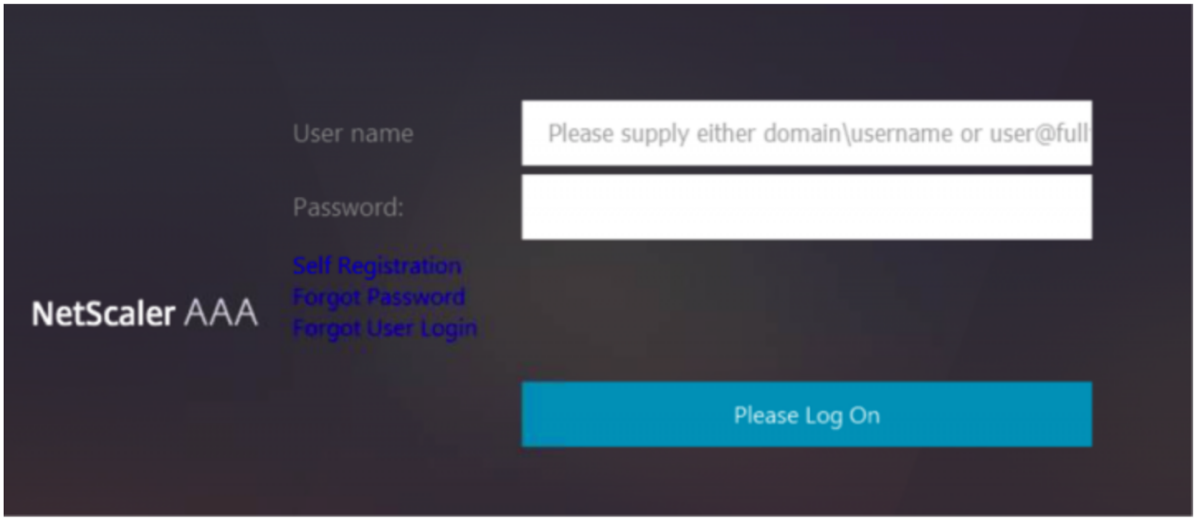


```
71 </Requirements>
72 </AuthenticationRequirements>
73 </AuthenticateResponse>
74 <!--NeedCopy-->
```

Ejecute los siguientes comandos para cargar el esquema personalizado en config.

```
1 add authentication loginSchema custom -authenticationSchema custom.xml
2
3 add authentication loginSchemaPolicy custom -rule true -action custom
4
5 bind authentication vserver AAATEST -policy custom -priority 100 -
     gotoPriorityExpression END
6 <!--NeedCopy-->
```

La siguiente ilustración muestra la página de inicio de sesión que se representa con esta configuración.



Personalizar la interfaz de usuario para mostrar imágenes

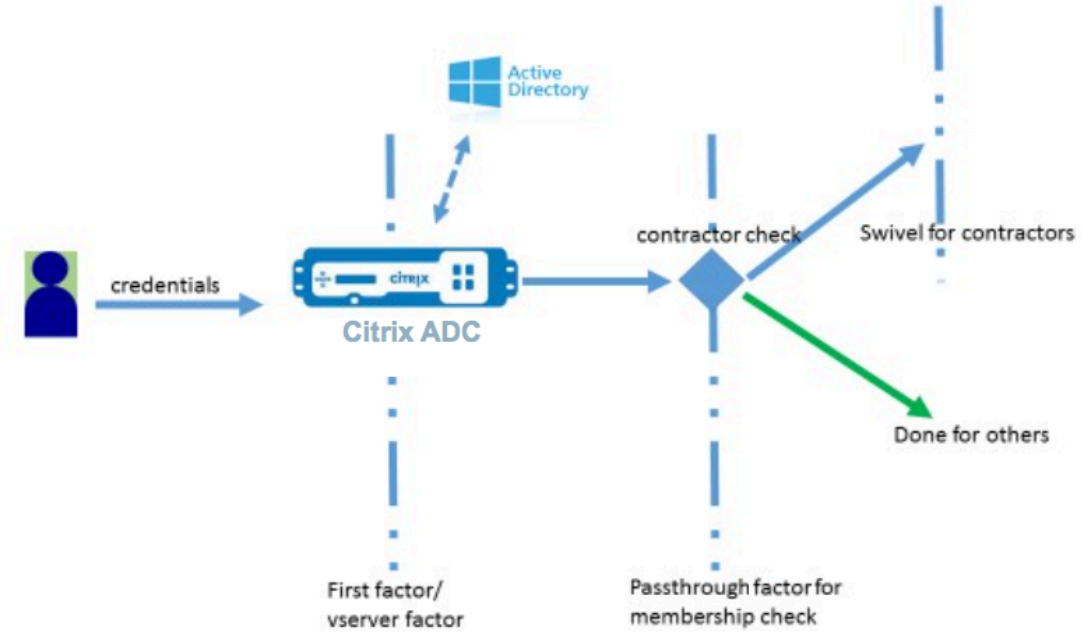
nFactor permite una visualización personalizada con el uso de archivos de esquema de inicio de sesión. Es posible que se requieran otras personalizaciones distintas de las que ofrecen los archivos de esquema de inicio de sesión integrados. Por ejemplo, mostrar un hipervínculo o escribir lógica personalizada en la interfaz de usuario. Esto se puede lograr mediante “credenciales personalizadas” que comprenden la extensión del esquema de inicio de sesión y el archivo javascript correspondiente.

Los archivos de esquema de inicio de sesión se pueden encontrar en el directorio `/nsconfig/loginschema/LoginSchema`.

Para que la personalización de la interfaz de usuario muestre imágenes, se utiliza como ejemplo un flujo de implementación en la integración “Citrix ADC-Swivel”.

Hay dos factores en este flujo.

- Primer factor: comprueba las credenciales de AD del usuario.
- Segundo factor: solicita el inicio de sesión del usuario en función de la pertenencia al grupo.



En este flujo, todos los usuarios pasan por el primer factor. Antes del segundo factor, hay un pseudo-factor para comprobar si algunos usuarios pueden omitirse del factor de “giro”. Si el usuario requiere el factor de “giro”, se muestran una imagen y un cuadro de texto para introducir el código.

Solución

La solución para personalizar la interfaz de usuario para mostrar imágenes contiene dos partes;

- Extensión esquema de inicio de sesión.
- Script personalizado para procesar la extensión del esquema de inicio de sesión.

Extensión esquema inicio de sesión

Para controlar la representación de formularios, se inyecta una “identificación” o “credencial” personalizada en el esquema de inicio de sesión. Esto se puede hacer reutilizando el esquema existente y modificándolo según el requisito.

En el ejemplo, se considera un esquema de inicio de sesión que solo tiene un campo de texto (como /nsconfig/loginschema/LoginSchema/OnlyPassword.xml).

El siguiente fragmento se agrega al esquema de inicio de sesión.

```
<Requirement><Credential><ID>swivel_cred</ID><Type>swivel_cred</Type><
   Input><Text><Hidden>true</Hidden><InitialValue>${
 http.req.user.name }
 </InitialValue></Text></Input></Credential></Requirement>
<!--NeedCopy-->
```

En el fragmento, “swivel_cred” se especifica como el “Tipo” de la credencial. Como esto no se reconoce como una “credencial” incorporada, la interfaz de usuario busca un controlador para este tipo y lo llama si existe.
Se envía un valor inicial para esta credencial, que es una expresión que Citrix ADC rellena dinámicamente. En el ejemplo, es el nombre del usuario utilizado para notificar el nombre de usuario al servidor giratorio. Puede que no sea necesario todo el tiempo o que se pueda aumentar con otros datos. Esos detalles deben agregarse según sea necesario.

Javascript para gestionar credenciales personalizadas

Cuando la IU encuentra una credencial personalizada, busca un controlador. Todos los controladores personalizados se escriben en /var/netscaler/logon/LogonPoint/custom/script.js para el tema del portal predeterminado.

Para los temas del portal personalizados, puede encontrar script.js en el directorio `/var/netscaler/logon/themes/<custom_theme>/`.

El siguiente script se agrega para renderizar el marcado de las credenciales personalizadas.

```
CTXS.ExtensionAPI.addCustomCredentialHandler({

    // The name of the credential, must match the type returned by the
       server
    getCredentialTypeName: function () {
  return "swivel_cred";  }
 ,
    // Generate HTML for the custom credential
    getCredentialTypeMarkup: function (requirements) {

        var div = $("<div></div>");
        var image = $("<img/>");
        var username = requirements.input.text.initialValue; //Get the
           secret from the response
        image.attr({
```



```
14
15              "style" : "width:200px;height:200px;",
16              "id" : "qrcodeimg",
17              "src" : "https://myswivelserver.citrix.com:8443/pinsafe/
                    SCImage?username=" + username
18           }
19   );
20          div.append(image);
21          return div;
22       }
23
24   }
25   );
26  <!--NeedCopy-->
```

Este fragmento es para manejar el marcado de "swivel_cred". El nombre de credencial resaltado debe coincidir con el "tipo" especificado anteriormente en la extensión del esquema de inicio de sesión. Para generar marcas, se debe agregar una imagen cuya fuente apunte al servidor giratorio. Una vez hecho esto, la interfaz de usuario carga la imagen desde la ubicación especificada. Como este esquema de inicio de sesión también tiene un cuadro de texto, la interfaz de usuario representa ese cuadro de texto.

> **Nota:**
>
> El administrador puede modificar el "estilo" del elemento de imagen para cambiar el tamaño de la imagen. Actualmente está configurado para 200x200 píxeles.

Configuración para personalizar la interfaz de usuario para mostrar imágenes

La configuración de nFactor se construye mejor de abajo hacia arriba, ese es el último factor primero porque cuando intenta especificar "nextFactor" para los factores anteriores, necesita el nombre del factor posterior.

Configuración del factor de giro:

```
1  add loginschema swivel_image  -authenticationSchema /nsconfig/
       loginschema/SwivelImage.xml
2
3  add authentication policylabel SwivelFactor  -loginSchema swivel_image
4
5  bind authentication policylabel SwivelFactor  -policy <policy-to-check-
       swivel-image> -priority 10
6  <!--NeedCopy-->
```


> **Nota:**
>
> Descargue SwivelImage.xml del esquema de inicio de sesión utilizado en el ejemplo.

Pseudo factor para la configuración de comprobación de grupo:

```
add authentication policylabel GroupCheckFactor

add authentication policy contractors_auth_policy -rule 'http.req.user.is_member_of( "contractors" )' -action NO_AUTHN

add authentication policy not_contractors _auth_policy -rule true -action NO_AUTHN

bind authentication policylabel GroupCheckFactor -policy contractors_auth_policy -pri 10 -nextFactor SwivelFactor

bind authentication policylabel GroupCheckFactor -policy not_contractors_auth_policy -pri 20
<!--NeedCopy-->
```

Primer factor para iniciar sesión en Active Directory:

```
add ldapAction <>

add authentication policy user_login_auth_policy -rule true -action <>

bind authentication vserver <> -policy user_login_auth_policy -pri 10 -nextFactor GroupCheckFactor
<!--NeedCopy-->
```

En la configuración, se especifican tres factores de los cuales uno está implícito/pseudo.

Esquema de inicio de sesión utilizado en este ejemplo

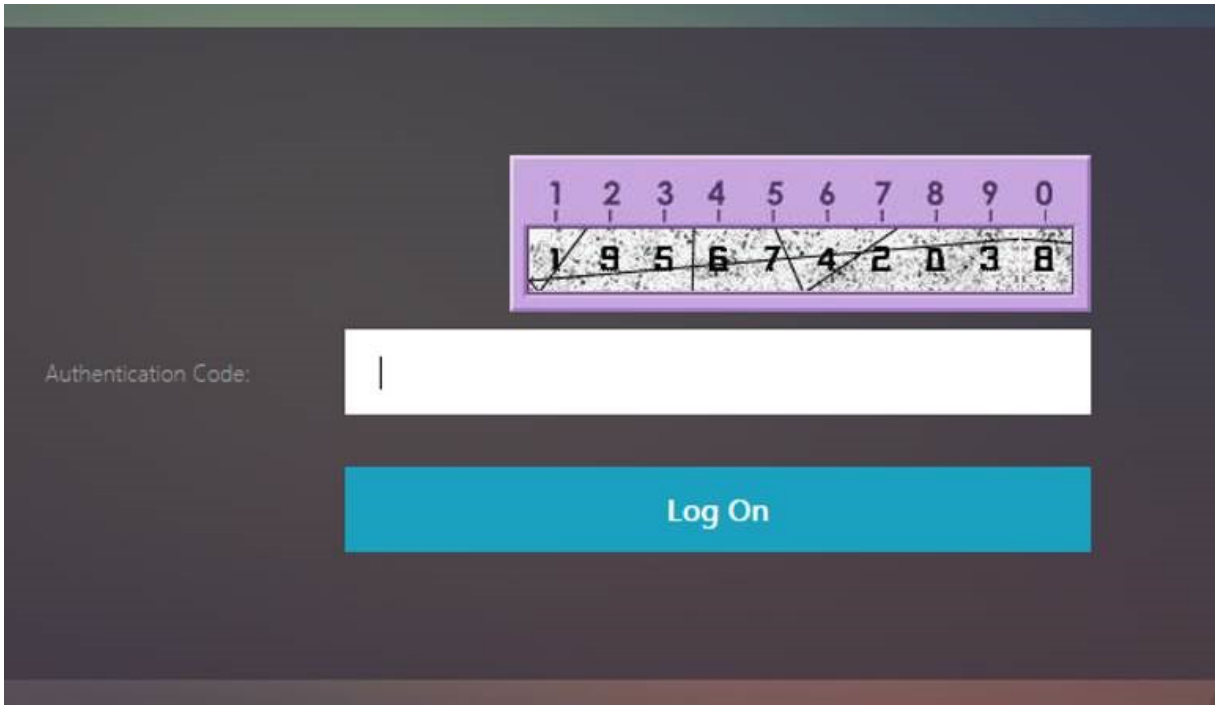
A continuación se muestra un esquema de ejemplo con credenciales giratorias y un cuadro de texto.

> **Nota:**
>
> Al copiar datos para un explorador web, las comillas pueden mostrarse de manera diferente. Copie los datos en los editores, como el bloc de notas, antes de guardarlos en archivos.


```
<?xml version="1.0" encoding="UTF-8"?>
<AuthenticateResponse xmlns="http://citrix.com/authentication/response/1">
<Status>success</Status>
<Result>more-info</Result>
<StateContext></StateContext>
<AuthenticationRequirements>
<PostBack>/nf/auth/doAuthentication.do</PostBack>
<CancelPostBack>/nf/auth/doLogoff.do</CancelPostBack>
<CancelButtonText>Cancel</CancelButtonText>
<Requirements>
<Requirement><Credential><ID>swivel_cred</ID><Type>swivel_cred</Type><Input><Text><Hidden>true</Hidden><InitialValue>${
 http.req.user.name }
 </InitialValue></Text></Input></Credential></Requirement>
<Requirement><Credential><ID>passwd</ID><SaveID>ExplicitForms-Password</SaveID><Type>password</Type></Credential><Label><Text>Password:</Text><Type>plain</Type></Label><Input><Text><Secret>true</Secret><ReadOnly>false</ReadOnly><InitialValue></InitialValue><Constraint>.+</Constraint></Text></Input></Requirement>
<Requirement><Credential><Type>none</Type></Credential><Label><Text>Hello ${
 http.req.user.name }
 , Please enter passcode from above image.</Text><Type>confirmation</Type></Label><Input /></Requirement>
<Requirement><Credential><ID>saveCredentials</ID><Type>savecredentials</Type></Credential><Label><Text>Remember my password</Text><Type>plain</Type></Label><Input><CheckBox><InitialValue>false</InitialValue></CheckBox></Input></Requirement>
<Requirement><Credential><ID>loginBtn</ID><Type>none</Type></Credential><Label><Type>none</Type></Label><Input><Button>Log On</Button></Input></Requirement>
</Requirements>
</AuthenticationRequirements>
</AuthenticateResponse>
<!--NeedCopy-->
```

Resultado

Una vez realizada la configuración, se muestra la siguiente imagen.



> **Nota:**
>
> La altura y la ubicación de la imagen se pueden modificar en JavaScript.

Personalizar el formulario de inicio de sesión nFactor de Citrix ADC para mostrar u ocultar

La interfaz de usuario RFweb de Citrix Gateway permite una amplia variedad de personalizaciones. Esta capacidad, cuando se combina con el marco de autenticación nFactor, permite a los clientes configurar flujos complejos sin comprometer los flujos de trabajo existentes.

En este ejemplo, hay dos opciones de autenticación, OAuth y LDAP disponibles en la lista Tipo de inicio de sesión. Cuando se carga el formulario por primera vez, se muestran los campos de nombre de usuario y contraseña (LDAP se muestra primero). Si se selecciona OAuth, todos los campos se ocultan porque OAuth implica una descarga de autenticación a un servidor de terceros. De esta manera, un administrador puede configurar flujos de trabajo intuitivos según la conveniencia del usuario.

> **Nota:**
>
> - Los valores de la lista Tipo de inicio de sesión se pueden modificar con modificaciones sencillas en el archivo de comandos.
> - En esta sección solo se describe la parte de la interfaz de usuario del flujo. La gestión en tiempo de ejecución de la autenticación queda fuera del alcance de este artículo. Se recomienda a los usuarios que consulten la documentación de nFactor para la configuración de la autenticación.

Cómo personalizar el formulario de inicio de sesión de nFactor

La personalización del formulario de inicio de sesión de nFactor se puede clasificar en dos partes

- Enviar el esquema de inicio de sesión correcto a la IU
- Escribir un controlador para interpretar el esquema de inicio de sesión y las selecciones del usuario

Enviar el esquema de inicio de sesión correcto a la IU

En este ejemplo, se envía una reclamación/requisito simple en el esquema de inicio de sesión.

Para ello, se modifica el archivo SingleAuth.xml. El archivo SingleAuth.xml se entrega con el firmware de Citrix ADC y se puede encontrar en el directorio `/nsconfig/loginschema/LoginSchema`.

Pasos para enviar el esquema de acceso:

1. Inicie sesión a través de SSH y coloque en shell (escriba 'shell').
2. Copie SingleAuth.xml en otro archivo para modificarlo.

   > **Nota:**
   >
   > La carpeta de destino es diferente de la carpeta de esquemas de inicio de sesión predeterminada de Citrix ADC.
   >
   > cp /nsconfig/loginschema/LoginSchema/SingleAuth.xml /nsconfig/loginschema/SingleAuthDynamic.xml

3. Agregue el siguiente reclamo a SingleAuthDynamic.xml.

```
<Requirement><Credential><ID>nsg_dropdown</ID><Type>nsg_dropdown</Type></Credential><Label><Text>Logon Type:</Text><Type>plain</Type></Label></Requirement>
<!--NeedCopy-->
```

4. Configure Citrix ADC para que envíe este esquema de inicio de sesión para cargar el primer formulario.

```
add loginschema single_auth_dynamic -authenticationSchema SingleAuthDynamic.xml

add loginschemaPolicy single_auth_dynamic -rule true -action single_auth_dynamic

```



```
bind authentication vserver aaa_nfactor -policy
    single_auth_dynamic -pri 10
<!--NeedCopy-->
```

Cambios en scripts para cargar formularios y gestionar eventos de usuario

Puede modificar el código JavaScript para que un administrador personalice la visualización del formulario de inicio de sesión. En este ejemplo, el campo de nombre de usuario y contraseña se muestran si se elige LDAP y se ocultan si se elige OAuth. El administrador también puede ocultar solo la contraseña.

Los administradores deben agregar el siguiente fragmento al directorio "script.js" que se encuentra en el directorio "/var/NetScaler/Logon/LogonPoint/Custom".

> **Nota:**
>
> Como este directorio es un directorio global, cree un tema de portal y modifique el archivo "script.js" dentro de esa carpeta, en "/var/netscaler/logon/themes/<THEME_NAME>".

```
CTXS.ExtensionAPI.addCustomCredentialHandler({

    // The name of the credential, must match the type returned by the
       server
    getCredentialTypeName: function () {
  return "nsg_dropdown";  }
 ,
    // Generate HTML for the custom credential
    getCredentialTypeMarkup: function (requirements) {

        var div = $("<div></div>");
        var select = $("<select name='nsg_dropdown'></select>").attr("
            id", "nsg_dropdown");

        var rsa = $("<option></option>").attr("selected", "selected").
            text("LDAP").val("LDAP");
        var OAuthID = $("<option></option>").text("OAuth").val("OAuth")
            ;
        select.append(rsa, OAuthID);

        select.change(function(e) {

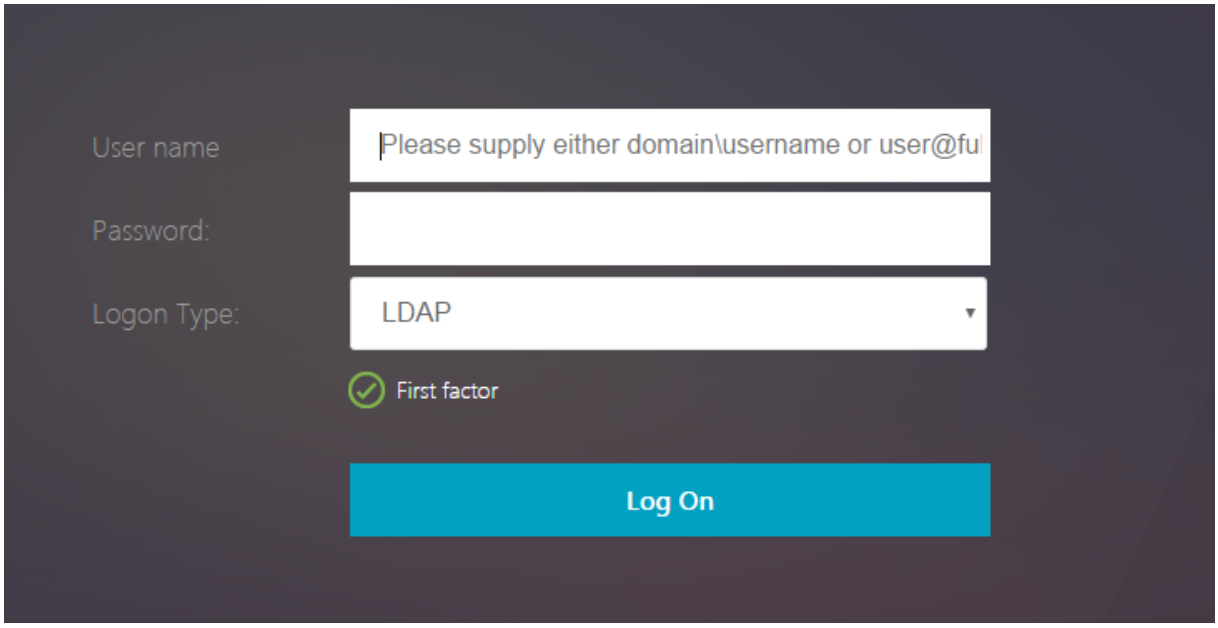
            var value = $(this).val();
```



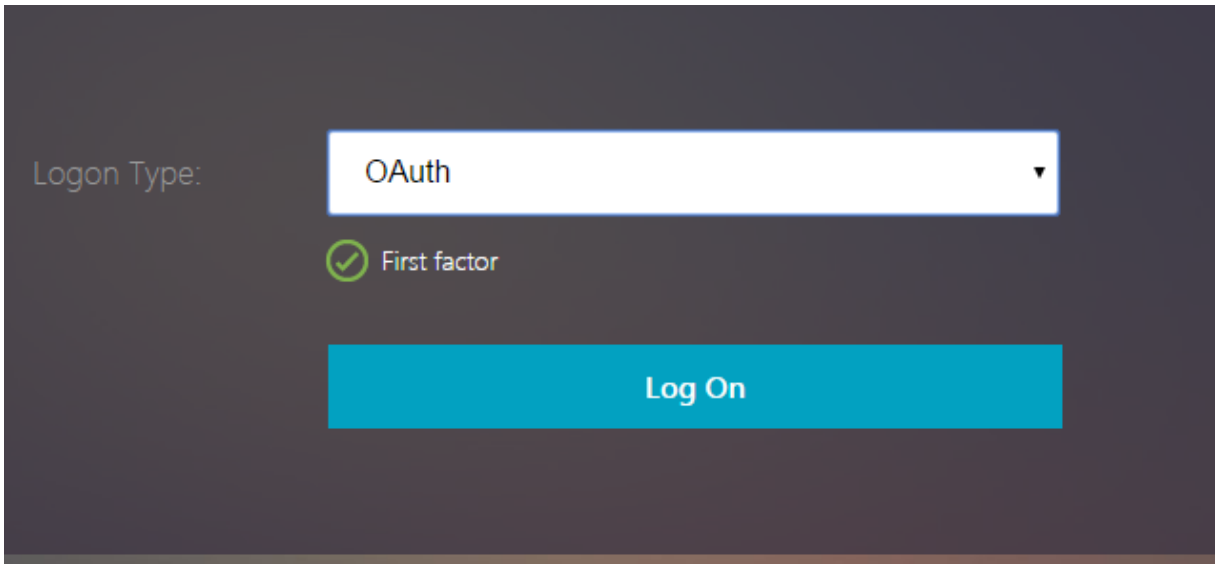
```
20              var ldapPwd = $($(".credentialform").find(".
                   CredentialTypepassword")[0]);
21              var ldapUname = $($(".credentialform").find(".
                   CredentialTypeusername"));
22              if(value == "OAuth") {
23
24                  if (ldapPwd.length)
25                          ldapPwd.hide();
26                  if (ldapUname.length)
27                          ldapUname.hide();
28               }
29    else if(value == "LDAP") {
30
31                  if (ldapPwd.length)
32                          ldapPwd.show();
33                  if (ldapUname.length)
34                          ldapUname.show();
35               }
36
37           }
38  );
39        div.append(select);
40         return div;
41      }
42
43  }
44  );
45 <!--NeedCopy-->
```

Experiencia del usuario final

Cuando un usuario final carga la página de inicio de sesión por primera vez, aparece la siguiente pantalla.



Si se selecciona **OAuth** en **Tipo de inicio de sesión**, se ocultan los campos de nombre de usuario y contraseña.



Si se selecciona **LDAP**, se muestran el nombre de usuario y la contraseña. De esta forma, la página de inicio de sesión se puede cargar dinámicamente en función de la selección del usuario.

Esquema de inicio de sesión utilizado en este ejemplo

```
<?xml version="1.0" encoding="UTF-8"?>
<AuthenticateResponse xmlns="http://citrix.com/authentication/response
   /1">
<Status>success</Status>
```



```
<Result>more-info</Result>
<StateContext></StateContext>
<AuthenticationRequirements>
<PostBack>/nf/auth/doAuthentication.do</PostBack>
<CancelPostBack>/nf/auth/doLogoff.do</CancelPostBack>
<CancelButtonText>Cancel</CancelButtonText>
<Requirements>
<Requirement><Credential><ID>login</ID><SaveID>ExplicitForms-Username</SaveID><Type>username</Type></Credential><Label><Text>User name</Text><Type>plain</Type></Label><Input><AssistiveText>Please supply either domain\username or user@fully.qualified.domain</AssistiveText><Text><Secret>false</Secret><ReadOnly>false</ReadOnly><InitialValue></InitialValue><Constraint>.+</Constraint></Text></Input></Requirement>
<Requirement><Credential><ID>passwd</ID><SaveID>ExplicitForms-Password</SaveID><Type>password</Type></Credential><Label><Text>Password:</Text><Type>plain</Type></Label><Input><Text><Secret>true</Secret><ReadOnly>false</ReadOnly><InitialValue></InitialValue><Constraint>.+</Constraint></Text></Input></Requirement>
<Requirement><Credential><ID>nsg_dropdown</ID><Type>nsg_dropdown</Type></Credential><Label><Text>Logon Type:</Text><Type>plain</Type></Label></Requirement>
<Requirement><Credential><Type>none</Type></Credential><Label><Text>First factor</Text><Type>confirmation</Type></Label><Input /></Requirement>
<Requirement><Credential><ID>saveCredentials</ID><Type>savecredentials</Type></Credential><Label><Text>Remember my password</Text><Type>plain</Type></Label><Input><CheckBox><InitialValue>false</InitialValue></CheckBox></Input></Requirement>
<Requirement><Credential><ID>loginBtn</ID><Type>none</Type></Credential><Label><Type>none</Type></Label><Input><Button>Log On</Button></Input></Requirement>
</Requirements>
</AuthenticationRequirements>
</AuthenticateResponse>
<!--NeedCopy-->
```

> **Nota:**
>
> Para obtener más información sobre varios temas relacionados con nFactor, consulte Autenticación nFactor.

Establecer una cookie mediante nFactor

February 19, 2022

Puede aplicar las etiquetas personalizadas nFactor y establecer una cookie como factor del flujo de autenticación. A través de etiquetas personalizadas, puede utilizar JavaScript para manipular el esquema de inicio de sesión.

Para establecer una cookie como factor, no es necesario mostrar ninguna información al usuario, que se realiza con un inicio de sesión sin esquema. En su lugar, debe interactuar con el explorador del usuario para indicar al esquema de inicio de sesión que almacene los datos deseados. Se requiere un esquema de inicio de sesión para establecer la cookie cuando se carga la página. La cookie se establece con una etiqueta personalizada y código JavaScript.

Para implementar un factor que establezca una cookie, cree un archivo XML llamado cookie.xml para almacenar el esquema en el directorio /nsconfig/loginschema/ con el siguiente contenido:

```
<?xml version="1.0" encoding="UTF-8"?>
<AuthenticateResponse xmlns="http://citrix.com/authentication/response
    /1">
<Status>success</Status>
<Result>more-info</Result>
<StateContext></StateContext>
<AuthenticationRequirements>
<PostBack>/nf/auth/doAuthentication.do</PostBack>
<CancelPostBack>/nf/auth/doLogoff.do</CancelPostBack>
<CancelButtonText>Cancel</CancelButtonText>
<Requirements>

<Requirement>
<Credential><ID>nsg_cookie</ID><Type>nsg_cookie</Type></Credential>
<Label><Text>Logon Type:</Text><Type>Plain</Type></Label>
</Requirement>

<Requirement>
<Credential><ID>loginBtn</ID><Type>none</Type></Credential>
<Label><Type>none</Type></Label><Input><Button>Log On</Button></Input>
</Requirement>

</Requirements>
</AuthenticationRequirements>
</AuthenticateResponse>
<!--NeedCopy-->
```


En este XML;

- La etiqueta personalizada nsg_cookie se utiliza para crear la cookie y enviar el formulario, y el botón formulario.
- El RfWebUI_custom es el nuevo tema del Portal basado en el tema RfWebUI.

Pasos para establecer una cookie mediante nFactor

1. Cree un tema del portal basado en el tema RfWebUI.

```
add vpn portaltheme RfWebUI_custom -basetheme RfWebUI
<!--NeedCopy-->
```

   Este comando crea una carpeta para este tema en /var/netscaler/logon/themes/RfWebUI_custom

2. Modifique el archivo /var/netscaler/logon/themes/RfWebUI_custom/script.js y agregue el siguiente script:

```
CTXS.ExtensionAPI.addCustomCredentialHandler({

    // The name of the credential, must match the type returned by the server
    getCredentialTypeName: function () {
  return "nsg_cookie";  }
 ,
    // Generate HTML for the custom credential
    getCredentialTypeMarkup: function (requirements) {

        var div = $("<div></div>");
        $(document).ready(function() {

        //Set cookie valid for 1000 days
        var exdays = 1000;
        var d = new Date();
        d.setTime(d.getTime() + (exdays\*24\*60\*60\*1000));
        var expires = "expires="+ d.toUTCString();
        document.cookie = "NSC_COOKIE_NAME=CookieValue;" + expires + ";path=/";

        //Submit form
        document.getElementById('loginBtn').click();
```



```
22             }
23   );
24           return div;
25       }
26
27   }
28   );
29  <!--NeedCopy-->
```

Este código realiza lo siguiente:

- Espera a que el explorador termine de cargar la página
- Establece una cookie llamada NSC_COOKIE_NAME con el valor CookieValue, válido durante 1000 días
- Envía automáticamente el formulario.

La cookie se crea y el usuario no necesita interactuar con la página.

3. Cree un esquema de inicio de sesión para enlazar a la etiqueta de directiva que representa el factor de cookie establecido.

```
1 add authentication loginSchema Cookie_LS -authenticationSchema "/
     nsconfig/loginschema/cookie.xml"
2 <!--NeedCopy-->
```

4. Cree una directiva de autenticación NO_AUTHN para enlazar a la etiqueta de directiva que representa el factor de cookie establecido.

```
1 add authentication Policy NO_AUTHN_POL -rule TRUE -action NO_AUTHN
2 <!--NeedCopy-->
```

Esta directiva siempre se evalúa como verdadera, moviendo al usuario al siguiente factor o completando el flujo de autenticación.

5. Enlazar el tema del portal RfWebUI_custom al servidor virtual Citrix Gateway o al servidor virtual AAA de Citrix ADC.

Implementaciones de ejemplo mediante autenticación nFactor

July 27, 2022

Estos son ejemplos de implementaciones que utilizan la autenticación nFactor:

- Obtener dos contraseñas por adelantado, PassThrough en el siguiente factor. Leer
- Extracción de grupos seguida de autenticación de certificado o LDAP, según la pertenencia al grupo. Leer
- SAML seguido de LDAP o autenticación de certificados, en función de los atributos extraídos durante SAML. Leer
- SAML en primer factor, seguido de la extracción de grupos y, a continuación, de la autenticación de certificados o LDAP, en función de los grupos extraídos. Leer
- Prerrellenar el nombre de usuario del certificado. Leer
- Autenticación de certificados seguida de extracción de grupos para 401 servidores virtuales de administración de tráfico habilitados. Leer
- Nombre de usuario y dos contraseñas con extracción de grupo en tercer factor. Leer
- Los certificados recurren a LDAP en la misma cascada; un servidor virtual para la autenticación de certificados y LDAP. Leer
- LDAP en primer factor y WebAuth en segundo factor. Leer
- Menú desplegable de dominio en primer factor, luego diferentes evaluaciones de directivas basadas en el grupo. Leer

Artículos “Cómo hacer…”

December 2, 2021

Los artículos “Cómo hacer” de autenticación, autorización y auditoría son artículos sencillos, relevantes y fáciles de implementar. Estos artículos contienen información sobre algunas de las funciones más populares de autenticación, autorización y auditoría, como la autenticación LDAP y la autenticación multifactor. Para obtener algunos de los artículos más populares sobre la configuración y la solución de problemas de autenticación mediante Citrix ADC, consulte Citrix ADC Authentication: ¿Cómo puedo?

Análisis de dispositivos de punto final

Configurar la exploración de Endpoint Analysis previa a la autenticación como factor en la autenticación nFactor

Configurar la exploración de Endpoint Analysis posterior a la autenticación como factor en la autenticación nFactor de Citrix ADC

Configurar la exploración EPA previa y posterior a la autenticación como factor en la autenticación nFactor

Configurar el análisis periódico de Endpoint Analysis como factor en la autenticación nFactor

Configurar la exploración EPA de autenticación previa de Citrix Gateway para la comprobación de dominio

Combinaciones de configuración de primer factor y segundo factor

Configurar nFactor para Citrix Gateway con WebAuth en primer factor y LDAP con cambio de contraseña en segundo factor

Configurar SAML seguido de la autenticación de certificados o LDAP basada en la extracción de atributos SAML en la autenticación nFactor

Configurar la autenticación de certificados como primer factor y LDAP como segundo factor en la autenticación nFactor de Citrix ADC

Configurar la autenticación de dos factores con un esquema de inicio de sesión y un esquema de acceso directo en la autenticación nFactor de Citrix ADC

Configurar nombre de usuario y dos contraseñas con extracción de grupo en tercer factor mediante autenticación nFactor

Configurar el menú desplegable del dominio, el nombre de usuario y el campo de contraseña en el primer factor y la evaluación de directivas en función de los grupos del siguiente factor

Configurar la extracción de grupos basada en la entrada de ID de correo electrónico (o nombre de usuario) en el primer factor para decidir el siguiente flujo de autenticación de factores

Configurar una lista desplegable de dominio para la entrada del usuario en el primer factor para decidir el siguiente flujo de autenticación de factores

CLUF como factor de autenticación

Configurar EULA como factor de autenticación en el sistema Citrix ADC nFactor

Rellenar previamente el nombre de usuario del certificado

Configurar el nombre de usuario de relleno previo del certificado en la autenticación nFactor de Citrix ADC

Autenticación intensificación

Configurar nFactor para aplicaciones con diferentes requisitos de sitio de inicio de sesión, incluida la autenticación escalonada

Autenticación SAML

January 12, 2021

Security Assertion Markup Language (SAML) es un mecanismo de autenticación basado en XML que proporciona capacidad de Single Sign-On y está definido por el Comité Técnico de Servicios de Seguridad de OASIS.

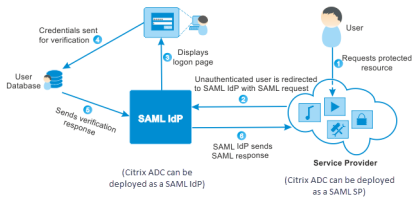
> Nota
>
> A partir de NetScaler 12.0, compilación 51.x, el dispositivo Citrix ADC utilizado como proveedor de servicios SAML (SP) con autenticación multifactor (nFactor) ahora rellena previamente el campo nombre de usuario en la página de inicio de sesión. El dispositivo envía un atributo NameID como parte de una solicitud de autorización SAML, recupera el valor del atributo NameID del proveedor de identidad (IdP) de Citrix ADC SAML y rellena previamente el campo nombre de usuario.

¿Por qué usar la autenticación SAML?

Considere un caso en el que un proveedor de servicios (LargeProvider) aloja varias aplicaciones para un cliente (BigCompany). BigCompany tiene usuarios que deben acceder sin problemas a estas aplicaciones. En una configuración tradicional, LargeProvider necesitaría mantener una base de datos de usuarios de BigCompany. Esto plantea algunas preocupaciones para cada una de las siguientes partes interesadas:

- LargeProvider debe garantizar la seguridad de los datos del usuario.
- BigCompany debe validar a los usuarios y mantener los datos del usuario actualizados, no solo en su propia base de datos, sino también en la base de datos de usuarios mantenida por LargeProvider. Por ejemplo, un usuario eliminado de la base de datos BigCompany también debe eliminarse de la base de datos LargeProvider.
- Un usuario tiene que iniciar sesión de forma individual en cada una de las aplicaciones alojadas.

El mecanismo de autenticación SAML proporciona un enfoque alternativo. El siguiente diagrama de implementación muestra cómo funciona SAML (flujo iniciado por SP).



Las preocupaciones planteadas por los mecanismos tradicionales de autenticación se resuelven de la siguiente manera:

- LargeProvider no tiene que mantener una base de datos para los usuarios de BigCompany. Liberado de la administración de identidades, LargeProvider puede concentrarse en proporcionar mejores servicios.
- BigCompany no soporta la carga de asegurarse de que la base de datos de usuarios de LargeProvider se mantenga sincronizada con su propia base de datos de usuarios.
- Un usuario puede iniciar sesión una vez, en una aplicación alojada en LargeProvider, e iniciar sesión automáticamente en las otras aplicaciones que están alojadas allí.

El dispositivo Citrix ADC se puede implementar como proveedor de servicios SAML (SP) y proveedor de identidades SAML (IdP). Lea los temas pertinentes para comprender las configuraciones que se deben realizar en el dispositivo Citrix ADC.

Un dispositivo Citrix ADC configurado como proveedor de servicios SAML ahora puede imponer una comprobación de restricción de audiencia. La condición de restricción de audiencia se evalúa como "Válido" solo si el grupo de respuesta SAML es miembro de al menos una de las audiencias especificadas.

Puede configurar un dispositivo Citrix ADC para analizar atributos en aserciones SAML como atributos de grupo. Al analizarlos como atributos de grupo, el dispositivo puede enlazar directivas a los grupos.

Citrix ADC como SP SAML

August 20, 2021

El proveedor de servicios SAML (SP) es una entidad SAML implementada por el proveedor de servicios. Cuando un usuario intenta acceder a una aplicación protegida, el SP evalúa la solicitud del cliente. Si el cliente no está autenticado (no tiene una cookie NSC_TMAA o NSC_TMAS válida), el SP redirige la solicitud al proveedor de identidad (IdP) SAML.

El SP también valida las aserciones SAML que se reciben del IdP.

Cuando el dispositivo Citrix ADC está configurado como SP, un servidor virtual de administración de tráfico recibe todas las solicitudes de usuario (equilibrio de carga o conmutación de contenido) asociado a la acción SAML pertinente.

El dispositivo Citrix ADC también admite enlaces POST y Redirect durante el cierre de sesión.

> **Nota**
>
> Un dispositivo Citrix ADC se puede utilizar como SP SAML en una implementación donde el IdP SAML está configurado en el dispositivo o en cualquier IdP SAML externo.

Cuando se utiliza como un SP SAML, un dispositivo Citrix ADC:

- Puede extraer la información de usuario (atributos) del token SAML. Esta información se puede utilizar en las directivas configuradas en el dispositivo Citrix ADC. Por ejemplo, si quiere extraer los atributos GroupMember y emailaddress, en SamlAction, especifique el parámetro **Attribute2** como GroupMember y el parámetro **Attribute3** como emailaddress.

  > **Nota**
  >
  > Los atributos predeterminados, como nombre de usuario, contraseña y dirección URL de cierre de sesión, no se deben extraer en los atributos 1 a 16, ya que se analizan y almacenan implícitamente en la sesión.

- Puede extraer nombres de atributos de hasta 127 bytes de una aserción SAML entrante. El límite anterior era de 63 bytes.
- Soporta enlaces de publicaciones, redireccionamiento y artefactos.

  > **Nota**
  >
  > El enlace de redirección no se debe utilizar para una gran cantidad de datos, cuando la aserción después de inflar o decodificar es mayor que 10K.

- Puede descifrar aserciones.
- Puede extraer atributos de varios valores de una aserción SAML. Estos atributos se envían son etiquetas XML anidadas tales como:

  <AttributeValue> <AttributeValue>Value1</AttributeValue>
  <AttributeValue>Value2</AttributeValue>
  </AttributeValue>

  > **Nota**
  >
  > Desde Citrix ADC 13.0 Build 63.x y superior, se ha aumentado la longitud máxima individual de los atributos SAML para permitir un máximo de 40k bytes. El tamaño de todos los atributos no debe exceder los 40k bytes.

  Cuando se presenta con XML anterior, el dispositivo Citrix ADC puede extraer Value1 y Value2 como valores de un atributo determinado, a diferencia del firmware antiguo que solo extrae Value1.

- Puede especificar la validez de una aserción SAML.

  Si la hora del sistema en Citrix ADC SAML IdP y el SP SAML del mismo nivel no está sincronizada, cualquiera de las partes podría invalidar los mensajes. Para evitar estos casos, ahora puede configurar la duración de tiempo para la que las aserciones son válidas.

  Esta duración, denominada “tiempo de sesgo”, especifica el número de minutos para los que debe aceptarse el mensaje. El tiempo de inclinación se puede configurar en el SP SAML y en el IdP de SAML.

- Puede enviar un atributo adicional llamado 'ForceAuth' en la solicitud de autenticación al IdP externo (proveedor de identidad). De forma predeterminada, ForceAuthN se establece en 'False'. Se puede establecer en 'True' para sugerir al IdP que forzar la autenticación a pesar del contexto de autenticación existente. Además, Citrix ADC SP realiza la solicitud de autenticación en el parámetro de consulta cuando se configura con enlace de artefactos.

Para configurar el dispositivo Citrix ADC como un SP SAML mediante la interfaz de línea de comandos

1. Configure una acción del SP SAML.

   Ejemplo

   El siguiente comando agrega una acción SAML que redirige las solicitudes de usuario no autenticadas.

   ```
   add authentication samlAction SamlSPAct1 -samlIdPCertName nssp -samlSigningCertNa
    nssp -samlRedirectUrl https://auth1.example.com -relaystateRule "AAA.
   LOGIN.RELAYSTATE.EQ(\"https://lb.example1.com/\")"
   ```

   Puntos a tener en cuenta

   - El certificado previsto `-samlIdPCertName` en el comando SAMLAction debe coincidir con el certificado correspondiente del proveedor de identidad para que la verificación de la firma se realce correctamente.
   - SAML solo admite certificado RSA. No se admiten otros certificados como HSM, FIPS, etc.
   - Citrix recomienda tener un nombre de dominio completo con '/' final en la expresión.
   - Los administradores deben configurar una expresión para **RelaysStateRule** en el comando SAMLAction. La expresión debe contener la lista de dominios publicados a los que se conecta el usuario antes de ser redirigido al servidor virtual de autenticación. Por ejemplo, la expresión debe contener los dominios del servidor virtual front-end (VPN, LB o CS) que utilizan esta acción SAML para la autenticación.

   Para obtener más información sobre el comando, consulte https://developer-docs.citrix.com/projects/citrix-adc-command-reference/en/latest/authentication/authentication-samlAction y https://support.citrix.com/article/CTX316577.

2. Configure la directiva SAML.

   Ejemplo

   El siguiente comando define una directiva SAML que aplica la acción SAML definida anteriormente a todo el tráfico.

   ```
   add authentication policy SamlSPPol1 -rule true -action SamlSPAct1
   ```


3. Enlazar la directiva SAML al servidor virtual de autenticación.

   Ejemplo

   El siguiente comando vincula la directiva SAML a un servidor virtual de autenticación denominado “av_saml”.

   ```
   bind authentication vserver av_saml -policy SamlSPPol1
   ```

4. Enlazar el servidor virtual de autenticación al servidor virtual de administración de tráfico adecuado.

   Ejemplo

   El siguiente comando agrega un servidor virtual de equilibrio de carga denominado “lb1_ssl” y asocia el servidor virtual de autenticación denominado “av_saml” al servidor virtual de equilibrio de carga.

   ```
   add lb vserver lb1_ssl SSL 10.217.28.224 443 -persistenceType NONE -
   cltTimeout 180 -AuthenticationHost auth1.example.com -Authentication ON
    -authnVsName av_saml
   ```

   Para obtener más detalles sobre el comando, consulte https://developer-docs.citrix.com/projects/citrix-adc-command-reference/en/latest/authentication/authentication-samlAction

Para configurar un dispositivo Citrix ADC como un SP SAML mediante la interfaz gráfica de usuario

1. Vaya a **Seguridad>Directivas AAA>Autenticación>Directivas básicas>SAML**.
2. Seleccione la ficha **Servidores**, haga clic en **Agregar**, introduzca valores para los siguientes parámetros y haga clic en **Crear**.

   Descripción del parámetro:

   Nombre: nombre del servidor

   URL de redirección: URL contra la que los usuarios se autenticarán. Algunos IdP tienen URL especiales a las que no se puede acceder a menos que se encuentre en la configuración de SAML.

   URL de cierre de sesión única: URL especificada para que Citrix ADC pueda reconocer cuándo debe devolver el cliente al IdP para completar el proceso de cierre de sesión. No lo usaremos en esta sencilla implementación.

   Enlace SAML: método que se utiliza para mover el cliente del SP al proveedor de identidades. Esto debe ser el mismo en el proveedor de identidad para que comprenda cómo se conectará el cliente a él.
   Cuando Citrix ADC actúa como SP, admite enlaces POST, REDIRECT y ARTIFACT.

   Enlace de cierre de sesión - REDIRECT

Nombre del certificado IDP - Certificado IDPCert (Base64) presente bajo Certificado de firma SAML.

Campo de usuario: sección del formulario de autenticación SAML del IdP que contiene el nombre de usuario para que SP lo extraiga si es necesario.

Nombre del certificado de firma: seleccione el certificado SP SAML (con clave privada) que Citrix ADC utiliza para firmar las solicitudes de autenticación al proveedor de identidad. El mismo certificado (sin clave privada) debe importarse al proveedor de identidad para que el proveedor de identidad pueda verificar la firma de la solicitud de autenticación. La mayoría de los desplazados internos no necesitan este campo.

Nombre del emisor: identificador. ID único que se especifica tanto en el SP como en el proveedor de servicios para ayudar a identificar el proveedor de servicios entre sí.

Rechazar afirmación sin firmar: opción que puede especificar si requiere que se firmen las afirmaciones del proveedor de identidad. Puede asegurarse de que solo se debe firmar (ON) la Afirmación (ON) o que sea necesario firmar la Afirmación y la Respuesta del IdP (ESTRICTA).

Audiencia: audiencia a la que se aplica la afirmación enviada por IdP. Normalmente se trata de un nombre de entidad o URL que representa ServiceProvider.

Algoritmo de firma - RSA-SHA256

Método de resumen - SHA256

Grupo de autenticación predeterminado: grupo predeterminado que se elige cuando la autenticación se realiza correctamente, además de los grupos extraídos.

Campo Nombre de grupo: nombre de la etiqueta en la afirmación que contiene grupos de usuarios.

Tiempo de sesgo (minutos): esta opción especifica el sesgo del reloj permitido en número de minutos que Citrix ADC ServiceProvider permite en una aserción entrante.

3. De forma similar, cree una directiva SAML correspondiente y enlazarla al servidor virtual de autenticación.

   Vaya a **Seguridad > AAA: Tráfico de aplicaciones > Servidores virtuales** y asocie la directiva SAML con el servidor virtual de autenticación.

4. Asocie el servidor de autenticación con el servidor virtual de administración de tráfico adecuado.

   Vaya a **Administración del tráfico > Equilibrio de carga** (o **Content Switching**) > **Servidores virtuales**, seleccione el servidor virtual y asocie el servidor virtual de autenticación con él.

Citrix ADC como proveedor de identidades SAML

December 2, 2021

El IdP de SAML (proveedor de identidad) es una entidad SAML que se implementa en la red del cliente. El IdP recibe solicitudes del SP SAML y redirige a los usuarios a una página de inicio de sesión, donde deben introducir sus credenciales. El IdP autentica estas credenciales con el directorio activo (servidor de autenticación externo, como LDAP) y, a continuación, genera una aserción SAML que se envía al SP.

El SP valida el token y el usuario obtiene acceso a la aplicación protegida solicitada.

Cuando el dispositivo Citrix ADC se configura como un IdP, todas las solicitudes se reciben en un servidor virtual de autenticación que está asociado con el perfil de IdP de SAML relevante.

> **Nota**
>
> Un dispositivo Citrix ADC se puede utilizar como IdP en una implementación en la que el SP SAML esté configurado en el dispositivo o en cualquier SP SAML externo.

Cuando se utiliza como proveedor de identidades SAML, un dispositivo Citrix ADC:

- Admite todos los métodos de autenticación que admite para los inicios de sesión tradicionales.
- Firma afirmaciones digitalmente.
- Admite la autenticación de un solo factor y de dos factores. SAML no debe configurarse como el mecanismo de autenticación secundario.
- Puede cifrar aserciones mediante la clave pública del SP SAML. Esto se recomienda cuando la afirmación incluye información confidencial.
- Puede configurarse para aceptar solo solicitudes firmadas digitalmente desde SAML SP.
- Puede iniciar sesión en el IdP de SAML mediante los siguientes mecanismos de autenticación basados en 401: Negociar, NTLM y Certificate.
- Se puede configurar para enviar 16 atributos además del atributo nameID. Los atributos se deben extraer del servidor de autenticación apropiado. Para cada uno de ellos, puede especificar el nombre, la expresión, el formato y un nombre descriptivo en el perfil del IdP de SAML.
- Si el dispositivo Citrix ADC está configurado como un IdP SAML para varios SP SAML, un usuario puede obtener acceso a las aplicaciones en los diferentes SPs sin autenticarse explícitamente cada vez. El dispositivo Citrix ADC crea una cookie de sesión para la primera autenticación y cada solicitud posterior utiliza esta cookie para la autenticación.
- Puede enviar atributos con varios valores en una aserción SAML.

- Admite enlaces posteriores y redireccionamientos. La compatibilidad con el enlace de artefactos se introduce en la versión 13.0 compilación 36.27 de Citrix ADC.
- Puede especificar la validez de una aserción SAML.

  Si la hora del sistema en el IdP SAML de Citrix ADC y el SP SAML del mismo par no están sincronizados, es posible que cualquiera de las partes invalide los mensajes. Para evitar estos casos, ahora puede configurar la duración de tiempo para la cual las afirmaciones son válidas.

  Esta duración, denominada "tiempo de desviación", especifica el número de minutos durante los que se debe aceptar el mensaje. El tiempo de inclinación se puede configurar en el SP de SAML y en el IdP de SAML.
- Se puede configurar para entregar aserciones solo a los SP SAML preconfigurados o confiables por el IdP. Para esta configuración, el IdP SAML debe tener el ID del proveedor de servicios (o el nombre del emisor) de los SP SAML relevantes.

  > **Nota**
  >
  > Antes de continuar, asegúrese de que tiene un servidor virtual de autenticación que esté vinculado a un servidor de autenticación LDAP.

Para configurar un dispositivo Citrix ADC como IdP de SAML mediante la interfaz de línea de comandos

1. Configure un perfil de IdP SAML.

   Ejemplo

   Agregar un dispositivo Citrix ADC como IdP con SiteMinder como SP.

   ```
   add authentication samlIdPProfile samlIDPProf1 -samlSPCertName siteminder
   -cert -encryptAssertion ON -samlIdPCertName ns-cert -assertionConsumerServiceURL
    http://sm-proxy.nsi-test.com:8080/affwebservices/public/saml2assertionconsumer
    -rejectUnsignedRequests ON -signatureAlg RSA-SHA256 -digestMethod
   SHA256 -acsUrlRule AAA.LOGIN.SAML_REQ_ACS_URL.REGEX_MATCH(re##^https://
   example2\.com/cgi/samlauth$##)
   ```

   Puntos a tener en cuenta

   - En el perfil de IdP de SAML, configure **acsurlRule** que toma una expresión de la lista de URL de proveedor de servicios aplicables para este IdP. Esta expresión depende del SP que se esté usando. Si Citrix ADC está configurado como SP, la URL de ACS será `https://<SP-domain_name>/cgi/samlauth`. Citrix recomienda tener una URL completa en la expresión para coincidir.
   - SAML solo admite certificado RSA. No se admiten otros certificados como HSM, FIPS, etc.

- Debe especificar el inicio del dominio con el signo "^" (ejemplo: ^https) junto con el signo de dólar "$" al final de la cadena (ejemplo: samlauth$).

Para obtener más información sobre el comando, consulte https://developer-docs.citrix.com/projects/citrix-adc-command-reference/en/latest/authentication/authentication-samlAction y https://support.citrix.com/article/CTX316577.

2. Configure la directiva de autenticación SAML y asocie el perfil de IdP de SAML como acción de la directiva.

```
add authentication samlIdPPolicy samlIDPPol1 -rule true -action samlIDPProf1
```

3. Enlazar la directiva al servidor virtual de autenticación.

```
bind authentication vserver saml-auth-vserver -policy samlIDPPol1 -
priority 100
```

Para obtener más información sobre el comando, consulte https://developer-docs.citrix.com/projects/citrix-adc-command-reference/en/latest/authentication/authentication-samlIdPProfile.

Para configurar un dispositivo Citrix ADC como IdP SAML mediante la interfaz gráfica de usuario

1. Vaya a **Seguridad>Directivas AAA>Autenticación>Directivas avanzadas>IdP SAML**.
2. Seleccione la ficha **Servidores**, haga clic en **Agregar**, introduzca valores para los siguientes parámetros y haga clic en **Crear**.

Descripción del parámetro:

URL de servicio al consumidor de aserción: URL a la que se redirigirá el usuario autenticado.

Nombre de certificado de IdP: par de claves de certificado utilizado para la página de autenticación.

Nombre del certificado SP: certificado del proveedor de servicios en este caso, la clave no es necesaria para ello.

Firmar aserción: la opción de firmar la afirmación y la respuesta al redirigir al cliente de nuevo al proveedor de servicios.

Nombre del emisor: un valor de cadena incluido en la aserción SAML emitida por el IdP.

ID del proveedor de servicios: ID único que se especifica en el SP para ayudar a identificar al proveedor de servicios. El identificador puede ser cualquier cosa y no necesita ser el URL que se especifica a continuación, sino que debe ser el mismo en el perfil SP y en los perfiles del IdP.

Rechazar solicitudes sin firmar: opción que puede especificar para garantizar que solo se acepten las afirmaciones firmadas con el certificado SP.

Algoritmo de firma: algoritmo utilizado para firmar y verificar las afirmaciones entre el IdP y el SP, debe ser el mismo en el perfil del IdP y el perfil del SP.

Método de resumen: algoritmo utilizado para verificar la integridad de las afirmaciones entre el IdP y el SP, esto debe ser igual en el perfil del IdP y el perfil del SP.

Vinculación SAML: igual que se describe en el perfil de SP, debe ser igual en el SP y el IdP.

3. Asocie la directiva IdP de SAML con un servidor virtual de autenticación.

   Vaya a **Seguridad > AAA: Tráfico de aplicaciones > Servidores virtuales** y asocie la directiva IdP SAML con el servidor virtual de autenticación.

Configurar el inicio de sesión único de SAML

May 8, 2022

Para proporcionar capacidades de inicio de sesión único en todas las aplicaciones alojadas en el proveedor de servicios, puede configurar el inicio de sesión único de SAML en el SP SAML.

Configuración del inicio de sesión único de SAML mediante la interfaz de línea de comandos

1. Configure el perfil de inicio de sesión único de SAML.

   Ejemplo

   En el siguiente comando, Ejemplo es el servidor virtual de equilibrio de carga que tiene un enlace web del portal de SharePoint. NSSP.example.com es el servidor virtual de administración de tráfico que equilibra la carga del servidor de SharePoint.

```
1  add tm samlSSOProfile tm-saml-sso -samlSigningCertName nssp -
      assertionConsumerServiceURL "https://nssp2.example.com/cgi/
      samlauth" -relaystateRule "\\"https://nssp2.example.com/
      samlsso.html\\"" -sendPassword ON -samlIssuerName nssp.example
      .com
2  <!--NeedCopy-->
```

2. Asocie el perfil de inicio de sesión único de SAML con la acción de tráfico.

   Ejemplo

El siguiente comando habilita el inicio de sesión único (SSO) y vincula el perfil de SSO SAML creado anteriormente a una acción de tráfico.

```
1 add tm trafficAction html_act -SSO ON -samlSSOProfile tm-saml-sso
2 <!--NeedCopy-->
```

3. Configure la directiva de tráfico que especifica cuándo debe ejecutarse la acción.

   Ejemplo

   El siguiente comando asocia la acción de tráfico a una directiva de tráfico.

```
1 add tm trafficPolicy html_pol "HTTP.REQ.URL.CONTAINS(\\"abc.html\\
     ")" html_act
2 <!--NeedCopy-->
```

4. Vincule la directiva de tráfico creada anteriormente a un servidor virtual de administración de tráfico (equilibrio de carga o conmutación de contenido). Alternativamente, la directiva de tráfico puede asociarse globalmente.

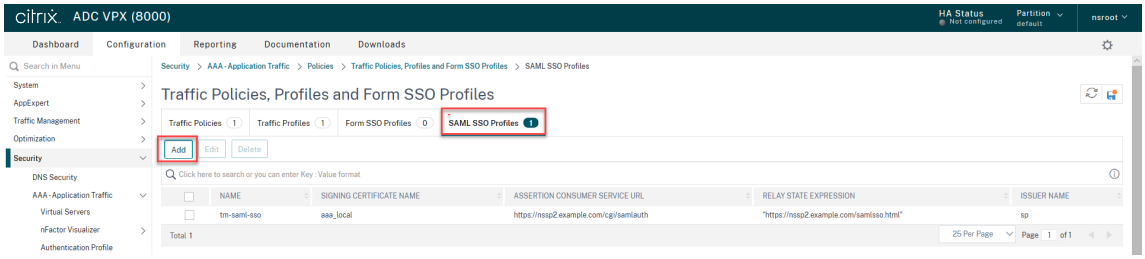
   > **Nota**
   >
   > Este servidor virtual de administración del tráfico debe estar asociado al servidor virtual de autenticación correspondiente asociado a la acción SAML.

```
1 bind lb vserver lb1_ssl -policyName html_pol -priority 100 -
     gotoPriorityExpression END -type REQUEST
2 <!--NeedCopy-->
```

Configuración del inicio de sesión único SAML mediante la GUI

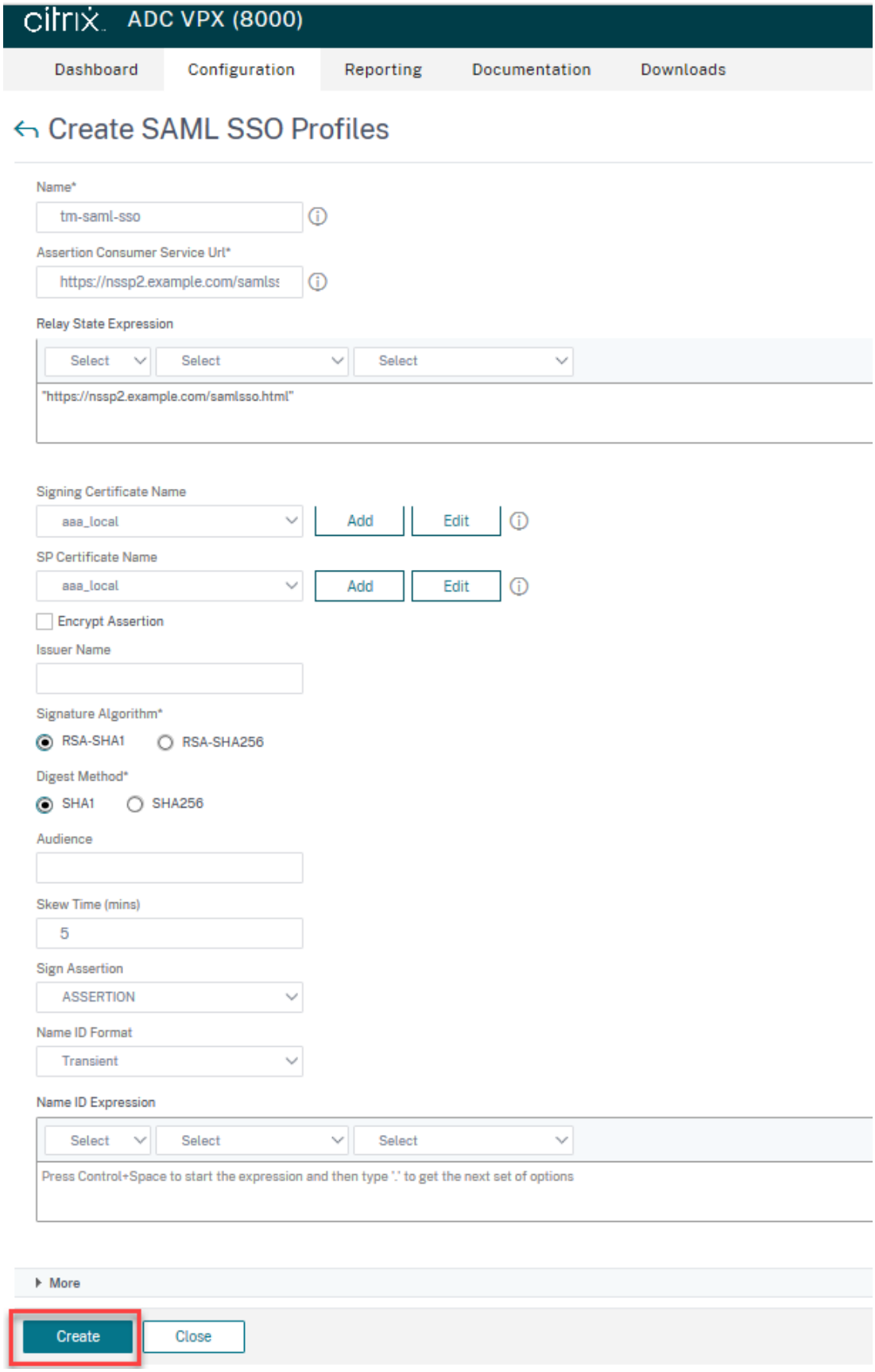
Para configurar el inicio de sesión único de SAML, debe definir el perfil de SSO de SAML, el perfil de tráfico y la directiva de tráfico y vincular la directiva de tráfico a un servidor virtual de administración de tráfico o globalmente al dispositivo Citrix ADC.

1. Vaya a **Seguridad > Tráfico de aplicaciones AAA-> Directivas > Tráfico > Perfiles de SSO SAML** y haga clic en **Agregar**.

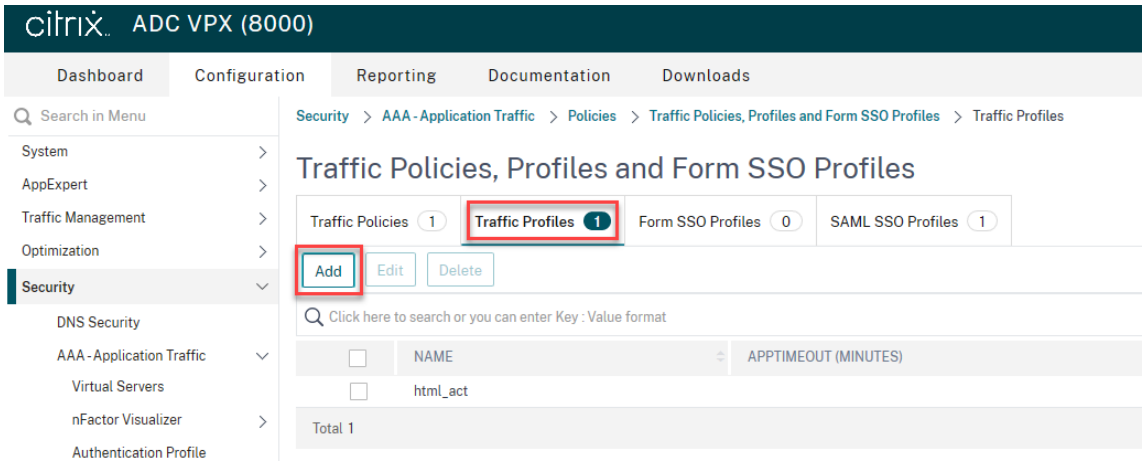


2. En la página **Crear perfiles de SSO SAML**, introduzca valores para los siguientes campos y haga clic en **Crear**.

   - Nombre: nombre del perfil de inicio único de SAML
   - Url del servicio de consumidor de aserción: URL a la que se va a enviar la afirmación
   - Nombre del certificado de firma: nombre del certificado SSL que se utiliza para firmar aserción
   - Nombre del certificado SP: nombre del certificado SSL de un par/parte receptora mediante el cual se cifra la aserción
   - Nombre del emisor: nombre que se utilizará en las solicitudes enviadas desde Citrix ADC al proveedor de identidad para identificar de forma exclusiva Citrix ADC
   - Algoritmo de firma: algoritmo que se utilizará para firmar/verificar transacciones SAML
   - Método de resumen: algoritmo que se utilizará para computar/verificar el resumen de las transacciones SAML
   - Audiencia: audiencia a la que se aplica una afirmación enviada por IdP. Normalmente se trata de un nombre de entidad o url que representa un ServiceProvider.
   - Audiencia: audiencia a la que se aplica una afirmación enviada por IdP. Normalmente se trata de un nombre de entidad o url que representa un ServiceProvider.
   - Tiempo de sesgo (minutos): el número de minutos en cada lado de la hora actual en que la afirmación sería válida
   - Firmar aserción: opción para firmar partes de aserción cuando el IdP de Citrix ADC envía una. Según la selección del usuario, se puede firmar Afirmación o Respuesta o Ambos o ninguno.
   - Formato de ID de nombre: formato del identificador de nombre enviado en aserción
   - Expresión de ID de nombre: expresión que se evalúa para obtener NameIdentifier que se enviará en la aserción

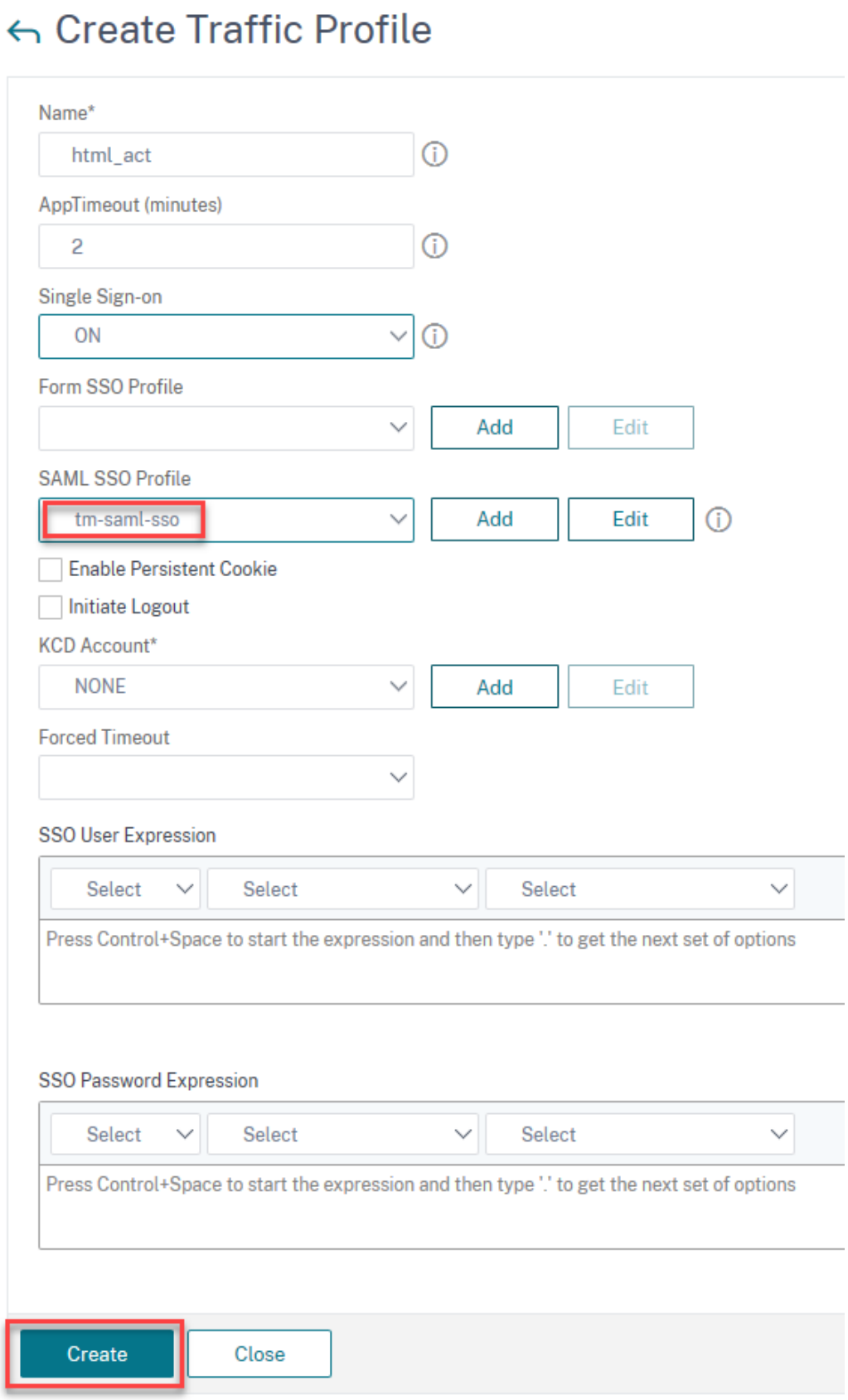


3. Vaya a **Seguridad > Tráfico de aplicaciones AAA-> Directivas> Tráfico > Perfiles de tráfico** y haga clic en **Agregar**.

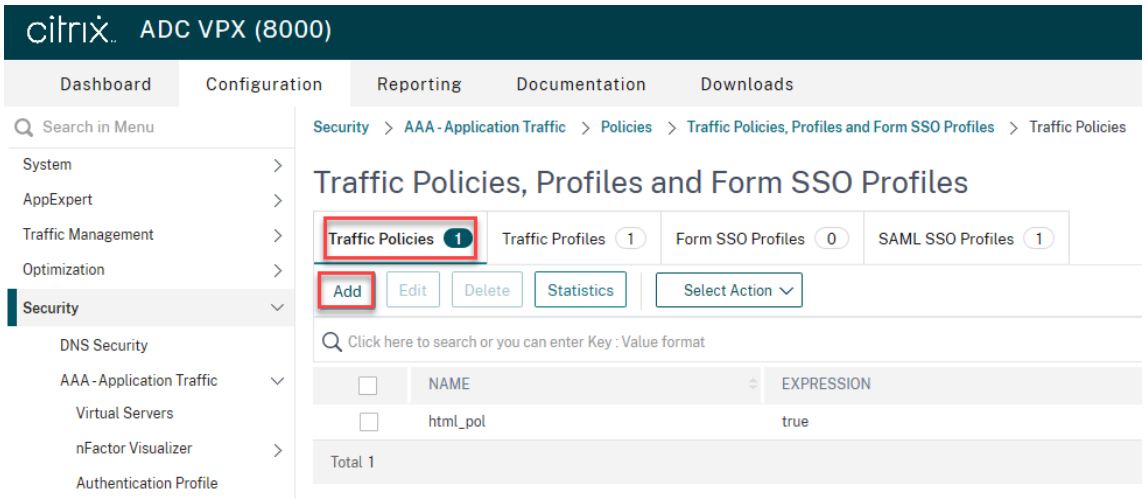


4. En la página **Crear perfil de tráfico**, introduzca valores para los siguientes campos y haga clic en **Crear**.

   - Nombre: nombre de la acción de tráfico.
   - appTimeout (minutos) - Intervalo de tiempo, en minutos, de inactividad del usuario tras el cual se cierra la conexión.
   - Inicio de sesión único - Seleccione ACTIVADO
   - Perfil de SSO SAML - Seleccione el perfil SSSO SAML creado
   - Cuenta KCD: nombre de cuenta de delegación restringida de Kerberos
   - Expresión de usuario de SSO: expresión que se evalúa para obtener el nombre de usuario de SingleSignOn
   - Expresión de contraseña de SSO: expresión que se evalúa para obtener la contraseña de SingleSignOn

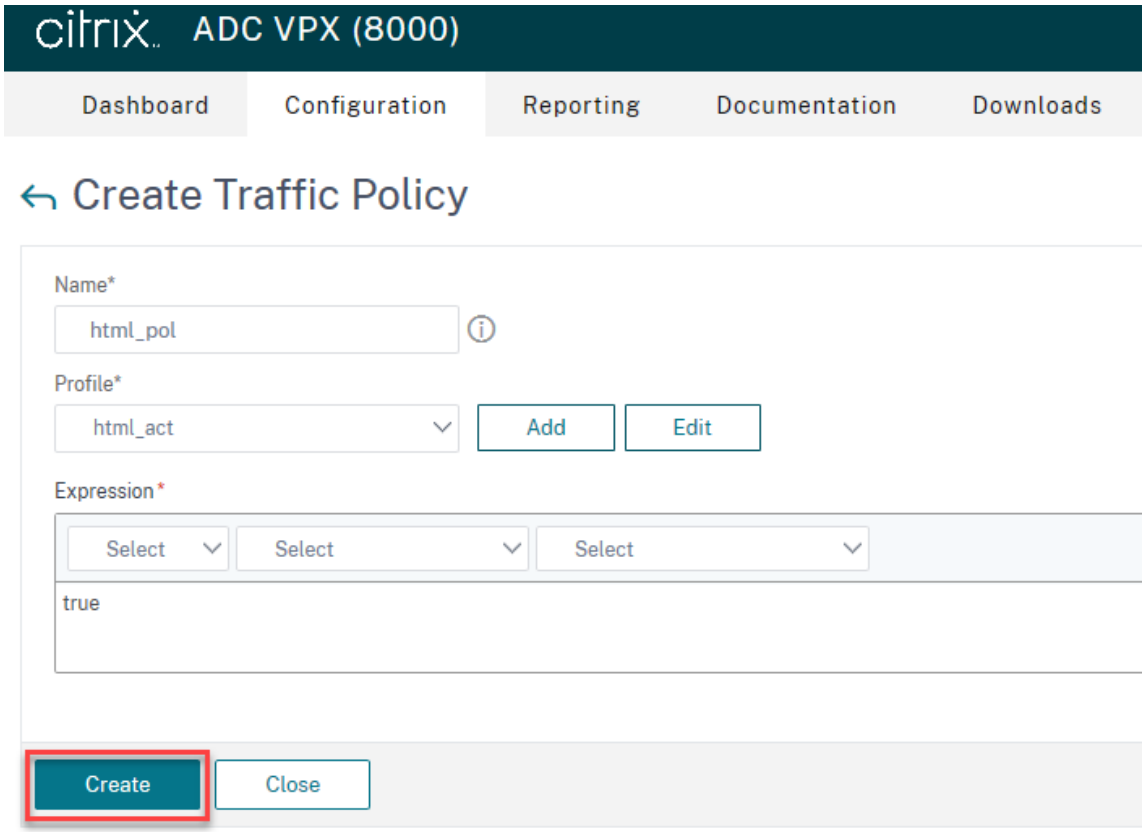


5. Vaya a **Seguridad > Tráfico de aplicaciones AAA-> Directivas > Tráfico > Directivas de tráfico** y haga clic en **Agregar**.

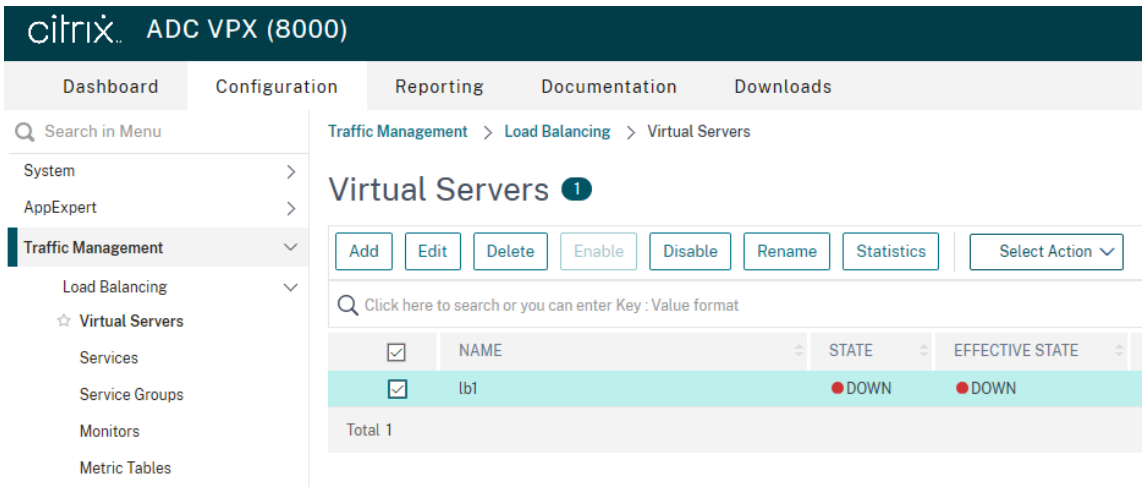


6. En la página **Crear directiva de tráfico**, introduzca valores para lo siguiente y haga clic en **Crear**.

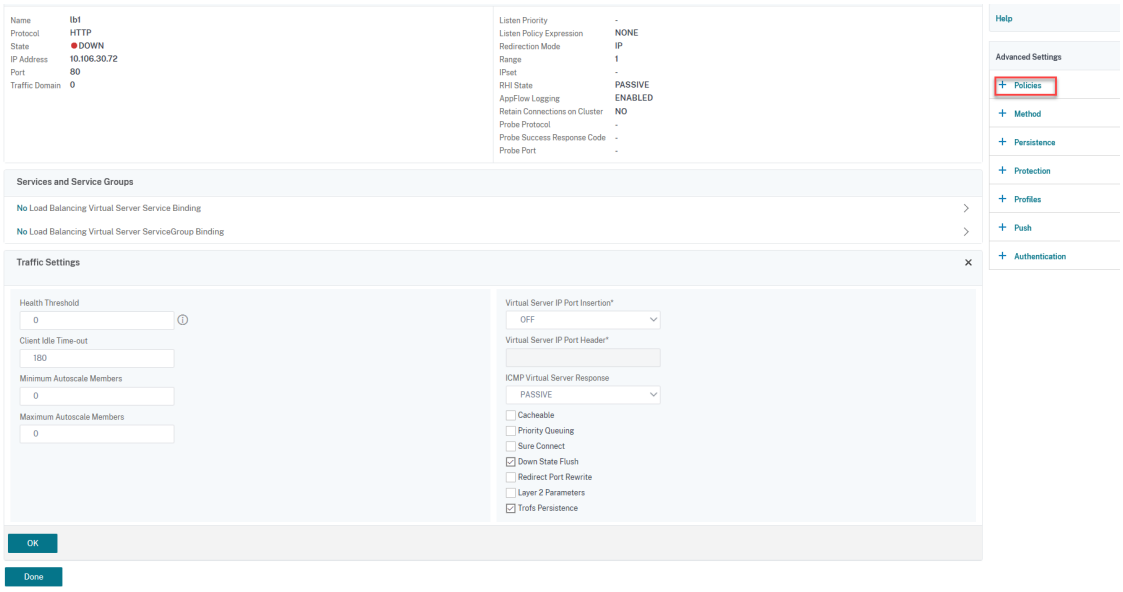
   - Nombre — Nombre de la directiva de tráfico que se va a crear
   - Perfil — Seleccione el perfil de tráfico creado
   - Expresión: Expresión de directiva avanzada que la directiva utiliza para responder a una solicitud específica. Por ejemplo, cierto.



7. Para vincular la directiva de tráfico a un servidor virtual de administración de tráfico, seleccione un servidor virtual.



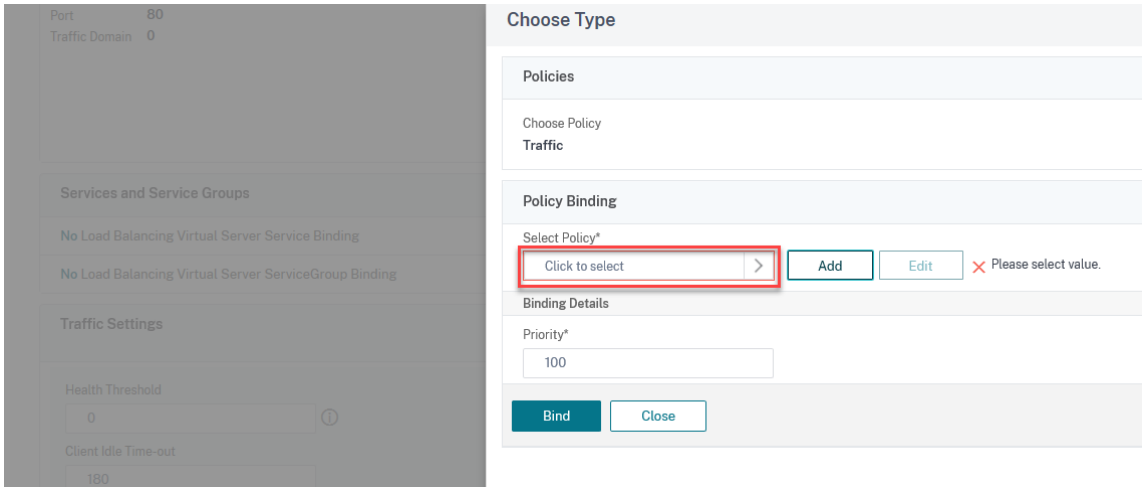
8. Haga clic en **Directivas**.



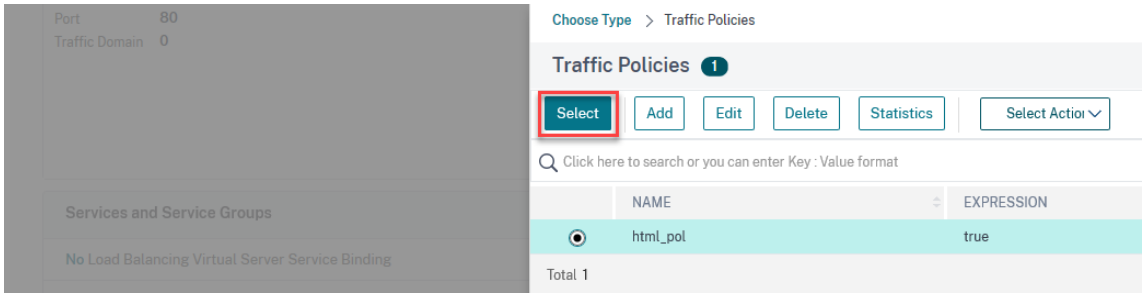
9. Seleccione **Tráfico** en el campo **Elegir directiva** y seleccione **Solicitud** en el campo **Elegir tipo** y haga clic en **Continuar**.

   ! [Haga clic aquí para agregar directiva (/en-us/citrix-adc/media/saml-9.png)

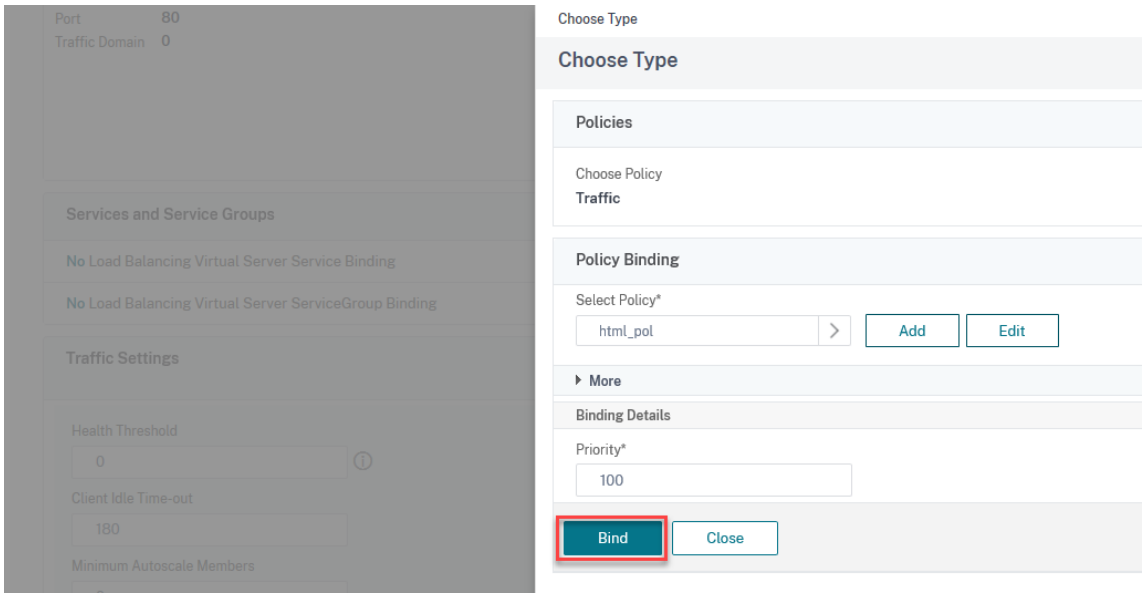
10. En **el campo Seleccionar directiva**, haga clic para seleccionar el tráfico creado.



11. Haga clic en **Seleccionar**.



12. Haga clic en **Vincular** para vincular la directiva de tráfico al servidor virtual.



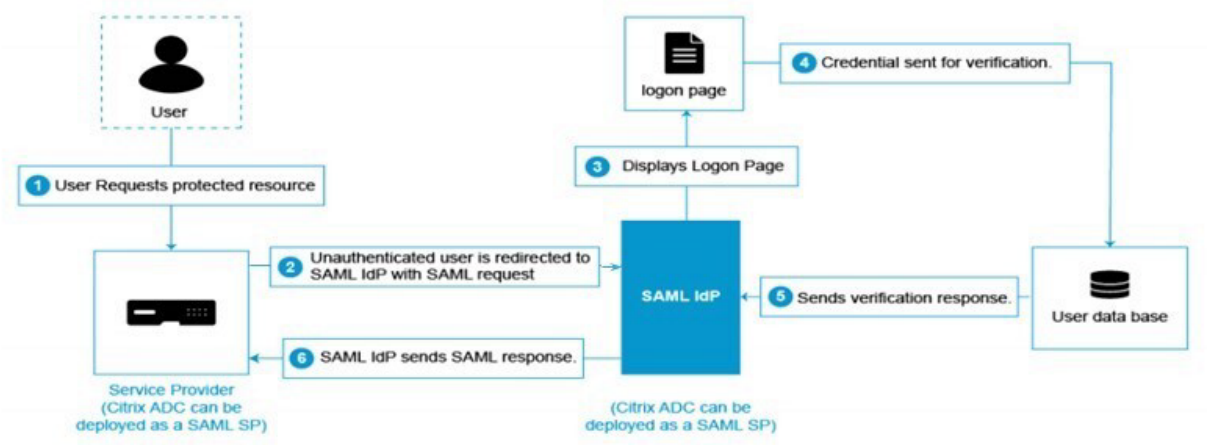
Configurar Azure AD como IdP de SAML y Citrix ADC como SP SAML

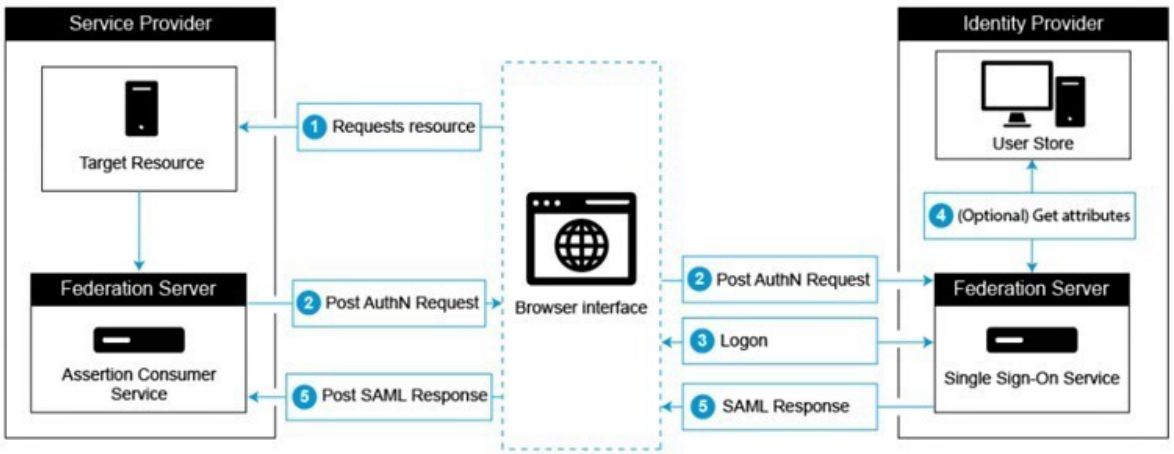
April 21, 2022

El proveedor de servicios (SP) de SAML es una entidad SAML implementada por el proveedor de servicios. Cuando un usuario intenta acceder a una aplicación protegida, el SP evalúa la solicitud del cliente. Si el cliente no está autenticado (no tiene una cookie NSC_TMAA o NSC_TMAS válida), el SP redirige la solicitud al proveedor de identidades (IdP) de SAML. El SP también valida las aserciones SAML que se reciben del IdP.

El IdP de SAML (proveedor de identidad) es una entidad SAML que se implementa en la red del cliente. El IdP recibe solicitudes del SP SAML y redirige a los usuarios a una página de inicio de sesión, donde deben introducir sus credenciales. El IdP autentica estas credenciales con el directorio de usuarios (servidor de autenticación externo, como LDAP) y, a continuación, genera una aserción SAML que se envía al SP. El SP valida el token y el usuario obtiene acceso a la aplicación protegida solicitada.

En el siguiente diagrama se muestra el mecanismo de autenticación SAML.

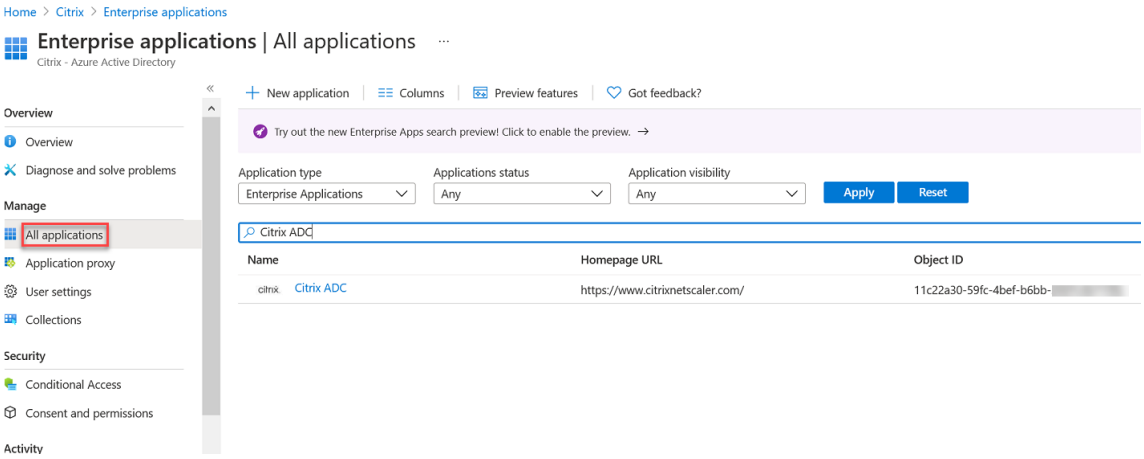




Configuraciones de Azure AD

Configurar los ajustes de inicio de sesión único:

1. En el portal de Azure, haga clic en **Azure Active Directory**.
2. En la sección **Administrar** del panel de navegación, haga clic en **Aplicaciones empresariales**. Aparece una muestra aleatoria de las aplicaciones de su arrendatario de Azure AD.
3. En la barra de búsqueda, escriba Citrix ADC.



4. En la sección **Administrar**, seleccione **Inicio de sesión único**.
5. Seleccione **SAML** para configurar el inicio de sesión único. Aparece la página **Configurar inicio de sesión único con SAML - Vista previa**. Aquí, Azure actúa como proveedor de identidad de SAML.
6. **Configurar las opciones de SAML básicas:**

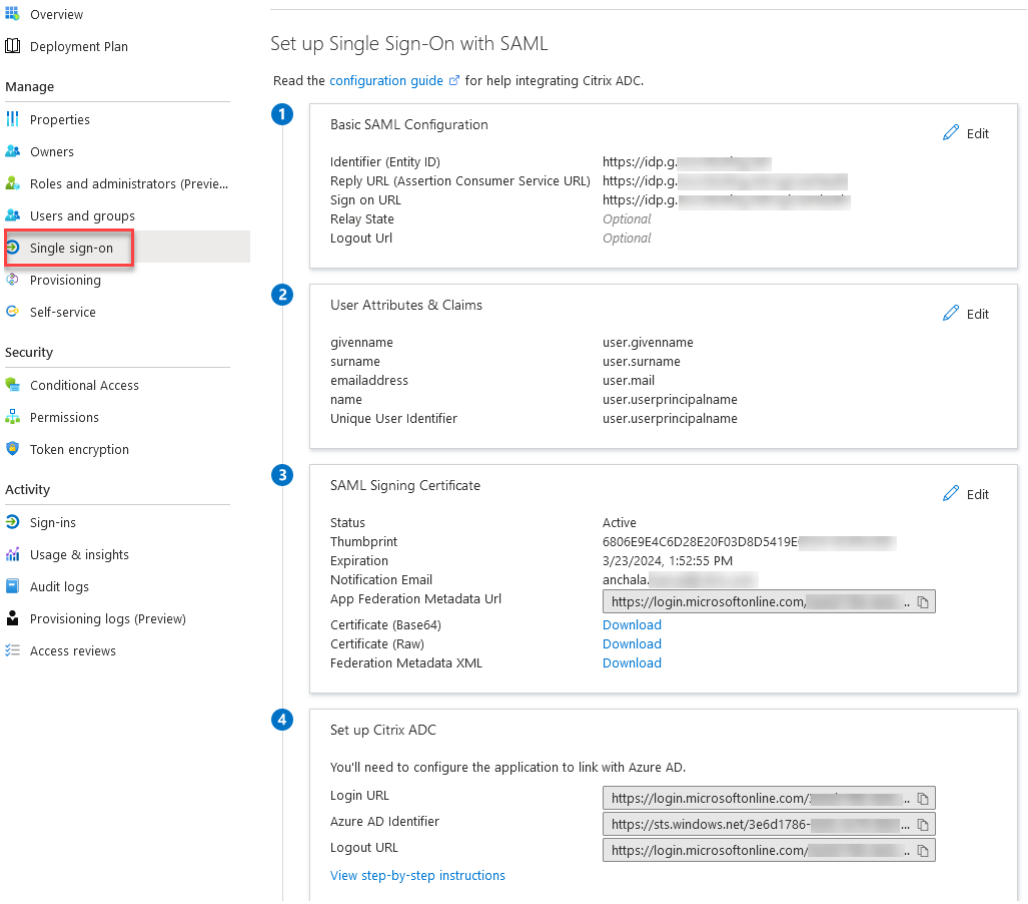
   Identificador (ID de entidad): Obligatorio para algunas aplicaciones. Identifica de forma exclusiva la aplicación para la que se está configurando el inicio de sesión único. Azure AD envía el identificador a la aplicación como parámetro de audiencia del token SAML. Se espera que la aplicación lo valide. Este valor también aparece como ID de entidad en cualquier metadato SAML proporcionado por la aplicación.

   URL de respuesta: Obligatoria. Especifica dónde espera recibir la aplicación el token SAML. La URL de respuesta también se denomina URL de Assertion Consumer Service (ACS).

   URL de inicio de sesión: Cuando un usuario abre esta URL, el proveedor de servicios redirige a Azure AD para autenticarlo e iniciar sesión en él.

   Estado de retransmisión: Especifica a la aplicación hacia dónde redirigir al usuario una vez finalizada la autenticación.

7. Descargue el certificado (Base64) presente en el **Certificado de firma SAML** para utilizarlo como SAMLIDPCertName mientras configura Citrix ADC como SP SAML.



Configuraciones laterales de Citrix ADC

1. Vaya a **Seguridad>Tráfico de aplicaciones AAA>Directivas>Autenticación>Directivas avanzadas>Acciones>SAML**.
2. Seleccione la ficha **Servidores**, haga clic en **Agregar**, introduzca valores para los siguientes parámetros y haga clic en **Crear**.

   Descripción del parámetro:

   El valor de los parámetros en negrita debe tomarse de las configuraciones del lado de Azure.

   Nombre: nombre del servidor

   URL de redirección: Introduzca la URL de inicio de sesión utilizada anteriormente en la sección “Configuración de Citrix ADC” de Azure AD. `https://login.microsoftonline.com/3e6d1786-4e0c-4c70-86d2-ae7811f97f79/saml2`

   URL de cierre de sesión única - `https://login.microsoftonline.com/3e6d1786-4e0c-4c70-86d2-ae7811f97f79/saml2`

   Vinculación SAML - POST

Vinculación de salida - REDIRECT

Nombre del certificado de IDP: Certificado IDPCert (Base64) presente en el Certificado de firma SAML.

Campo de usuario: Nombre principal de usuario. Tomado de la sección "Atributos de usuario y reclamaciones" de Azure IdP.

Nombre del certificado de firma: No es necesario para Azure AD. Seleccione el certificado SP SAML (con clave privada) que Citrix ADC utiliza para firmar solicitudes de autenticación al proveedor de identidad. El mismo certificado (sin clave privada) debe importarse al proveedor de identidad para que el proveedor de identidad pueda verificar la firma de la solicitud de autenticación. La mayoría de los desplazados internos no necesitan este campo.

issuerName: Identificador. `https://idp.g.nssvctesting.net`

Rechazar afirmación sin firmar - ACTIVADO

Público: Público al que se aplica la afirmación enviada por el IdP. Por lo general, se trata de un nombre de entidad o URL que representa el ServiceProvider.

Algoritmo de firma - RSA-SHA256

Método de resumen - SHA256

Grupo de autenticación predeterminado: el grupo predeterminado que se elige cuando la autenticación se realiza correctamente, además de los grupos extraídos.

Campo de nombre de grupo: nombre de la etiqueta en una aserción que contiene grupos de usuarios.

Tiempo sesgado (minutos): esta opción especifica el sesgo de reloj permitido en el número de minutos que Citrix ADC ServiceProvider permite en una aserción entrante.

Dos factores: OFF

Contexto de autenticación solicitado: exacto

Tipo de clase de autenticación: ninguno

Enviar huella digital - DESACTIVADO

Aplicar nombre de usuario - ACTIVADO

Forzar autenticación - DESACTIVADO

Respuesta SAML del almacén - DESACTIVADO

Del mismo modo, cree una directiva SAML correspondiente y enlácela al servidor virtual de autenticación.

Nota: Azure AD no espera el campo ID de asunto de la solicitud SAML. Para que Citrix ADC no envíe el campo ID de asunto, escriba el siguiente comando en el símbolo del sistema de **Citrix ADC**.


```
nsapimgr_wr.sh -ys call="ns_saml_dont_send_subject"
```

Más funciones compatibles con SAML

March 9, 2022

Las siguientes funciones se admiten para SAML.

Compatibilidad con lectura y generación de metadatos para la configuración del proveedor de identidades y SP SAML

El dispositivo Citrix ADC ahora admite archivos de metadatos como medio de entidades de configuración tanto para el proveedor de servicios (SP) SAML como para el proveedor de identidad (IdP). El archivo de metadatos es un archivo XML estructurado que describe la configuración de una entidad. Los archivos de metadatos para el SP y el IdP son independientes. Según la implementación y, en ocasiones, un SP o entidad de IdP puede tener varios archivos de metadatos.
Como administrador, puede exportar e importar archivos de metadatos (SAML SP e IdP) en Citrix ADC. La funcionalidad de exportación e importación de metadatos para el proveedor de identidad y el proveedor de identidad SAML se explica en las siguientes secciones.

Exportación de metadatos para el SP SAML

Considere un ejemplo en el que Citrix ADC está configurado como SP SAML y un IdP SAML quiere importar metadatos que contienen la configuración del SP de Citrix ADC. Suponga que el dispositivo Citrix ADC ya está configurado con un atributo “SAMLAction” que especifica la configuración del SP SAML.

Para exportar metadatos de usuarios o administradores, consulte el servidor virtual de autenticación o Citrix Gateway como se muestra a continuación:

```
1 https://vserver.company.com/metadata/samlsp/<action-name>
```

Importación de metadatos para SAML SP

Actualmente, la configuración de la acción SAML en el dispositivo Citrix ADC toma varios parámetros. El administrador especifica estos parámetros manualmente. Sin embargo, los administradores a menudo desconocen la nomenclatura si se trata de interoperar con diferentes sistemas SAML. Si los metadatos del IdP están disponibles, se puede evitar la mayor parte de la configuración en la entidad

“SAMLAction”. De hecho, es posible que se omita toda la configuración específica del IdP si se proporciona el archivo de metadatos del IdP. La entidad “SAMLAction” ahora toma un parámetro adicional para leer la configuración del archivo de metadatos.

Cuando importa un metadato en un dispositivo Citrix ADC, los metadatos no contienen ningún algoritmo de firma que se vaya a utilizar, sino que contienen los detalles del punto final. Un metadato se puede firmar con ciertos algoritmos que se pueden usar para verificar los metadatos en sí. Los algoritmos no se almacenan en la entidad “SAMLAction”.

Por lo tanto, lo que especifique en la entidad “SAMLAction” son los que se utilizan al enviar los datos. Los datos entrantes pueden contener un algoritmo diferente para que lo procese un dispositivo Citrix ADC.

Puede importar un tamaño máximo de 64 K bytes de metadatos.

Para obtener los archivos de metadatos mediante la interfaz de línea de comandos.

```
set samlAction <name> [-metadataUrl <url> [-metadataRefreshInterval <
    int>] https://idp.citrix.com/samlidp/metadata.xml
```

> **Nota**
>
> El parámetro metadataRefreshInterval es el intervalo en minutos para obtener información de metadatos de la URL de metadatos especificada. Valor por defecto 36000.

Importación de metadatos para IdP de SAML

El parámetro “SAMLIDPProfile” toma un nuevo argumento para leer toda la configuración específica del SP. La configuración del IdP SAML se puede simplificar sustituyendo las propiedades específicas del SP por un archivo de metadatos del SP. Este archivo se consulta a través de HTTP.

Para leer desde el archivo de metadatos mediante la interfaz de línea de comandos:

```
set samlIdPProfile <name> [-metadataUrl <url>] [-
    metadataRefreshInterval <int>]
```

Compatibilidad con atributos nombre-valor para la autenticación SAML

Ahora puede configurar los atributos de autenticación SAML con un nombre único junto con valores. Los nombres se configuran en el parámetro de acción SAML y los valores se obtienen consultando los nombres. Al especificar el valor del atributo name, los administradores pueden buscar fácilmente el

valor del atributo asociado al nombre del atributo. Además, los administradores ya no tienen que recordar el atributo solo por su valor.

> **Importante**
>
> - En el comando SAMLAction, puede configurar un máximo de 64 atributos separados por comas con un tamaño total inferior a 2048 bytes.
> - Citrix recomienda usar la lista de atributos. El uso del "atributo 1 al atributo 16" provocará un error en la sesión si el tamaño del atributo extraído es grande.

Para configurar los atributos nombre-valor mediante la CLI

En el símbolo del sistema, escriba:

```
1 add authentication samlAction <name> [-Attributes <string>]
```

Ejemplo:

```
1 add authentication samlAction samlAct1 -attributes  "mail,sn,
    userprincipalName"
```

Compatibilidad con URL de servicio al consumidor de aserción para IdP de SAML

Un dispositivo Citrix ADC configurado como proveedor de identidad (IdP) SAML ahora admite la indexación de Assertion Consumer Service (ACS) para procesar la solicitud del proveedor de servicios SAML (SP). El IdP SAML importa la configuración de indexación de ACS desde los metadatos del SP o permite introducir información de índices de ACS manualmente.
En la siguiente tabla se enumeran algunos artículos que son específicos de implementaciones en las que el dispositivo Citrix ADC se usa como SP SAML o IdP SAML.

En la siguiente tabla se enumeran algunos artículos que son específicos de implementaciones en las que el dispositivo Citrix ADC se usa como SP SAML o IdP SAML.

SP SAML	Proveedor de identidades SAML	Enlace de información
Citrix ADC	AD de Microsoft Azure	Citrix Support
Okta	Citrix ADC	Citrix Support
AWS	Citrix ADC	Citrix Support

Información sobre otras implementaciones específicas:

- NetScaler como SP SAML en dispositivo FIPS
- Configuración de Office365 para el inicio de sesión único con NetScaler como IdP SAML

Compatibilidad con tipos de credenciales WebView para mecanismos de autenticación

La autenticación de un dispositivo Citrix ADC ahora puede admitir el protocolo AuthV3. El tipo de credencial WebView en el protocolo AuthV3 admite todo tipo de mecanismos de autenticación (incluidos SAML y OAuth). El tipo de credencial WebView forma parte de AuthV3, que Citrix Receiver y el explorador implementan en las aplicaciones web.

En el siguiente ejemplo, se explica el flujo de eventos WebView a través de Citrix Gateway y Citrix Receiver:

1. Citrix Receiver negocia con Citrix Gateway para obtener compatibilidad con el protocolo AuthV3.
2. El dispositivo Citrix ADC responde positivamente y sugiere una URL de inicio específica.
3. A continuación, Citrix Receiver se conecta al endpoint (URL) específico.
4. Citrix Gateway envía una respuesta al cliente para iniciar WebView.
5. Citrix Receiver inicia WebView y envía la solicitud inicial al dispositivo Citrix ADC.
6. El dispositivo Citrix ADC redirige el URI al extremo de inicio de sesión del navegador.
7. Una vez que se completa la autenticación, el dispositivo Citrix ADC envía una respuesta de finalización a WebView.
8. WebView ahora se cierra y devuelve el control a Citrix Receiver para continuar con el protocolo AuthV3 para el establecimiento de la sesión.

Aumento del tamaño de SessionIndex en el SP SAML

El tamaño de SessionIndex del proveedor de servicios (SP) SAML aumenta a 96 bytes. Anteriormente, el tamaño máximo predeterminado de SessionIndex era de 63 bytes.

> **Nota**
>
> Soporte introducido en NetScaler 13.0 Build 36.x

Soporte de referencia de clase de autenticación personalizada para SAML SP

Puede configurar el atributo de referencia de clase de autenticación personalizado en el comando de **acción SAML**. Con el atributo de referencia de clase de autenticación personalizada, puede personalizar los nombres de las clases en las etiquetas SAML apropiadas. El atributo de referencia de clase de autenticación personalizada junto con el espacio de nombres se envía al IdP de SAML como parte de la solicitud de autenticación de SP de SAML.

Anteriormente, al usar el comando de acción SAML, podía configurar solo un conjunto de clases predefinidas definidas en el atributo AuthNctxClassRef.

> **Importante**
>
> Al configurar el atributo customAuthnctxClassRef, asegúrese de lo siguiente:

- Los nombres de las clases deben incluir caracteres alfanuméricos o una URL válida con etiquetas XML adecuadas.
- Si tiene que configurar varias clases personalizadas, cada clase debe estar separada por comas

Para configurar los atributos customAuthnctxClassRef mediante la CLI

En el símbolo del sistema, escriba:

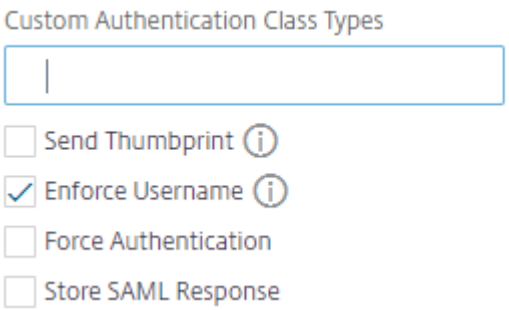
- add authentication samlAction <name> [-customAuthnCtxClassRef <string>]
- set authentication samlAction <name> [-customAuthnCtxClassRef <string>]

Ejemplo:

- `add authentication samlAction samlact1 -customAuthnCtxClassRef http://www.class1.com/LoA1,http://www.class2.com/LoA2`
- `set authentication samlAction samlact2 -customAuthnCtxClassRef http://www.class3.com/LoA1,http://www.class4.com/LoA2`

Para configurar los atributos customAuthnctxClassRef mediante la interfaz gráfica de usuario

1. Vaya a **Seguridad > AAA - Tráfico de aplicaciones > Directivas > Autenticación > Directivas avanzadas > Acciones > SAML**.
2. En la página SAML, seleccione la ficha **Servidores** y haga clic en **Agregar**.
3. En la página **Crear servidor SAML de autenticación**, introduzca el nombre de la acción SAML.
4. Desplácese hacia abajo para configurar los tipos de clase en la sección **Tipos de clase de autenticación personalizada**.



Compatibilidad con el enlace de artefactos en SAML IdP

El dispositivo Citrix ADC configurado como proveedor de identidad (IdP) SAML admite el enlace de artefactos. El enlace de artefactos mejora la seguridad del IdP SAML y evita que los usuarios malintencionados inspeccionen la afirmación.

Compatibilidad con URL de servicio al consumidor de aserción para IdP de SAML

Un dispositivo Citrix ADC configurado como proveedor de identidad (IdP) SAML ahora admite la indexación de Assertion Consumer Service (ACS) para procesar la solicitud del proveedor de servicios SAML (SP). El IdP SAML importa la configuración de indexación de ACS desde los metadatos del SP o permite introducir información de índices de ACS manualmente.

Soporte de descarga FIPS

Un dispositivo Citrix ADC MPX FIPS utilizado como proveedor de servicios SAML ahora admite aserciones cifradas. Además, un dispositivo Citrix ADC MPX FIPS que funcione como proveedor de servicios SAML o proveedor de identidad SAML ahora se puede configurar para usar los algoritmos SHA2 en hardware FIPS.

> **Nota**
>
> En el modo FIPS, solo se admite el algoritmo RSA-V1_5 como algoritmo de transporte de claves.

Configuración del soporte de descarga FIPS mediante la interfaz de línea de comandos:

1. Agregar SSL FIPS

   add ssl fipsKey fips-key

2. Cree una CSR y utilícela en el servidor de CA para generar un certificado. A continuación, puede copiar el certificado en **/nsconfig/ssl**. Supongamos que el archivo es *fips3cert.cer*.

   ```
   add ssl certKey fips-cert -cert fips3cert.cer -fipsKey fips-key<!--
   NeedCopy-->
   ```

3. Especificar este certificado en la acción SAML para el módulo SP SAML

   ```
   set samlAction <name> -samlSigningCertName fips-cert<!--NeedCopy-->
   ```

4. Usar el certificado en SAMLIDPProfile para el módulo IdP SAML

   ```
   set samlidpprofile fipstest -samlIdpCertName fips-cert<!--NeedCopy-->
   ```

Terminologías SAML comunes

A continuación, se muestran algunas terminologías SAML comunes:

- **Afirmación:** una aserción SAML es un documento XML devuelto por el proveedor de identidad al proveedor de servicios después de la autenticación del usuario. La afirmación tiene una estructura específica, tal como se define en el estándar SAML.
- **Tipos de afirmaciones:** Los siguientes son los tipos de afirmación.
  - Autenticación: el usuario se autentica por un medio determinado en un momento determinado
  - Autorización: se le concedió o denegó el acceso al usuario a un recurso específico
  - Atributos: el usuario está asociado a los atributos suministrados
- **Servicio al consumidor de aserciones (ACS):** el extremo (URL) del proveedor de servicios que es responsable de recibir y analizar una aserción SAML
- **Restricción de audiencia:** un valor dentro de la afirmación SAML que especifica a quién (y solo a quién) está destinada la afirmación. La "audiencia" será el proveedor de servicios y, por lo general, es una URL, pero técnicamente se puede formatear como cualquier cadena de datos.
- **Proveedor de identidad (IdP):** en términos de SAML, el proveedor de identidad es la entidad que verifica la identidad del usuario, en respuesta a una solicitud del proveedor de servicios.

  El proveedor de identidad es responsable de mantener y autenticar la identidad del usuario
- **Proveedor de servicios (SP):** en términos de SAML, el proveedor de servicios (SP) ofrece un servicio al usuario y le permite iniciar sesión mediante SAML. Cuando el usuario intenta iniciar sesión, el SP envía una solicitud de autenticación SAML al proveedor de identidad (IdP)
- **Vinculación de SAML:** los solicitantes y los respondedores de SAML se comunican mediante el intercambio de mensajes. El mecanismo para transportar estos mensajes se denomina enlace SAML.
- **Artefacto HTTP:** una de las opciones de enlace admitidas por el protocolo SAML. HTTP Artifact es útil en escenarios en los que el solicitante y el respondedor SAML utilizan un agente de usuario HTTP y no desean transmitir todo el mensaje, ya sea por razones técnicas o de seguridad. En su lugar, se envía un artefacto SAML, que es un identificador único para la información completa. El IdP puede usar el artefacto para recuperar la información completa. El emisor del artefacto debe mantener el estado mientras el artefacto está pendiente. Se debe configurar un Servicio de resolución de artefactos (ARS).

  HTTP Artifact envía el artefacto como un parámetro de consulta.
- **HTTP POST:** una de las opciones de enlace admitidas por el protocolo SAML.

  HTTP POST envía el contenido del mensaje como un parámetro POST, en la carga útil.
- **Redirección HTTP:** Una de las opciones de enlace admitidas por el protocolo SAML.

  Cuando se utiliza la redirección HTTP, el proveedor de servicios redirige al usuario al proveedor de identidades donde se produce el inicio de sesión, y el proveedor de identidades redirige al

usuario de vuelta al proveedor de servicios. La redirección HTTP requiere la intervención del agente de usuario (el navegador).

La redirección HTTP envía el contenido del mensaje en la URL. Por este motivo, no se puede usar para la respuesta SAML, ya que el tamaño de la respuesta normalmente superará la longitud de URL permitida por la mayoría de los navegadores.

Nota: El dispositivo Citrix ADC admite enlaces POST y Redirect durante el cierre de sesión.

- Metadatos: Los metadatos son los datos de configuración en SP e IdP para saber cómo comunicarse entre sí, lo que estará en los estándares XML

Otros artículos útiles de Citrix relacionados con la autenticación SAML

Puede que le resulten útiles los siguientes artículos relacionados con la autenticación SAML.

- https://support.citrix.com/article/CTX277558
- https://support.citrix.com/article/CTX259127
- https://support.citrix.com/article/CTX228135
- https://support.citrix.com/article/CTX221631
- https://support.citrix.com/article/CTX138988

Autenticación OAuth

October 5, 2021

La función de administración del tráfico de autenticación, autorización y auditoría admite la autenticación OAuth y OpenID Connect (OIDC). Autoriza y autentica a los usuarios en servicios alojados en aplicaciones como Google, Facebook y Twitter.

Puntos a tener en cuenta

- Se necesita Citrix ADC Advanced Edition y superiores para que la solución funcione.
- Un dispositivo Citrix ADC debe tener la versión 12.1 o posterior para que el dispositivo funcione como proveedor de identidades de OAuth mediante OIDC.
- OAuth en un dispositivo Citrix ADC está calificado para todos los IdP de SAML que cumplen con “OpenID connect 2.0”.

Un dispositivo Citrix ADC se puede configurar para que se comporte como proveedor de servicios (SP) o proveedor de identidad (IdP) mediante SAML y OIDC. Anteriormente, un dispositivo Citrix ADC configurado como IdP solo admitía el protocolo SAML. A partir de la versión 12.1 de Citrix ADC, Citrix ADC también admite el OIDC.

OIDC es una extensión de la autorización/delegación de OAuth. Un dispositivo Citrix ADC admite los protocolos OAuth y OIDC de la misma clase de otros mecanismos de autenticación. OIDC es un complemento de OAuth, ya que proporciona una forma de obtener información del usuario del servidor de autorización en lugar de OAuth que solo obtiene un token que no se puede obtener para obtener información del usuario.

El mecanismo de autenticación facilita la verificación en línea de los tokens OpenID. Un dispositivo Citrix ADC se puede configurar para obtener certificados y verificar firmas en el token.

Una ventaja importante de utilizar los mecanismos OAuth y OIDC es que la información del usuario no se envía a las aplicaciones alojadas. Por lo tanto, el riesgo de robo de identidad se reduce considerablemente.

El dispositivo Citrix ADC configurado para autenticación, autorización y auditoría ahora acepta tokens entrantes firmados mediante el algoritmo HMAC HS256. Además, las claves públicas del proveedor de identidades (IdP) SAML se leen de un archivo, en lugar de aprender de un extremo de URL.

En la implementación de Citrix ADC, el servidor virtual de administración del tráfico de autenticación, autorización y auditoría accede a la aplicación. Por lo tanto, para configurar OAuth, debe configurar una directiva de OAuth que debe asociarse a un servidor virtual de administración del tráfico de autenticación, autorización y auditoría.

Configurar el protocolo OpenID Connect

Un dispositivo Citrix ADC ahora se puede configurar como proveedor de identidad mediante el protocolo OIDC. El protocolo OIDC refuerza las capacidades de aportación de identidad del dispositivo Citrix ADC. Ahora puede acceder a la aplicación alojada en toda la empresa con un inicio de sesión único. El OIDC ofrece más seguridad al no transferir la contraseña del usuario, pero funciona con tokens con una duración específica. OIDC también está diseñado para integrarse con clientes que no son de explorador, como aplicaciones y servicios. Por lo tanto, muchas implementaciones adoptan ampliamente el OIDC.

Ventajas de contar con la compatibilidad con OpenID Connect

- OIDC elimina la sobrecarga de mantener varias contraseñas de autenticación, ya que el usuario tiene una identidad única en toda la organización.
- OIDC proporciona una seguridad sólida para su contraseña, ya que la contraseña solo se comparte con su proveedor de identidad y no con ninguna aplicación a la que acceda.
- OIDC tiene una amplia interoperabilidad con varios sistemas, lo que facilita que las aplicaciones alojadas acepten OpenID.
- OIDC es un protocolo sencillo que permite a los clientes nativos integrarse fácilmente con los servidores.

Para configurar un dispositivo Citrix ADC como proveedor de identidad mediante el protocolo OpenID Connect mediante la interfaz gráfica de usuario

1. Vaya a **Configuración > Seguridad > Tráfico de aplicaciones AAA > Directivas > Autenticación > Directivas avanzadas > IdP de OAuth**.
2. Haga clic en **Perfil** y haga clic en **Agregar.**

   En la pantalla **Crear perfil de proveedor de identidad de OAuth de autenticación**, defina los valores para los siguientes parámetros y haga clic en **Crear**.

   - **Nombre** : nombre del perfil de autenticación.
   - **ID de cliente** : cadena única que identifica al SP.
   - **Secreto del cliente** : secreto único que identifica al SP.
   - **URL de redirección** : punto final del SP en el que se debe publicar el código/token.
   - **Nombre del emisor** : cadena que identifica al IdP.
   - **Público** : destinatario objetivo del token que envía el IdP. El destinatario podría comprobarlo.
   - **Tiempo de sesgo** : el tiempo durante el cual el token sigue siendo válido.
   - Grupo de**autenticación predeterminado: grupo** agregado a la sesión de este perfil para simplificar la evaluación de directivas y ayudar a personalizar las directivas.
3. Haga clic en **Directivas** y en **Agregar.**
4. En la pantalla **Crear directiva de IDP de OAuth de autenticación**, defina los valores para los siguientes parámetros y haga clic en **Crear**.

   - **Nombre:** Nombre de la directiva de autenticación.
   - **Acción** : nombre del perfil creado anteriormente.
   - **Acción de registro** : nombre de la acción de registro de mensajes que se va a utilizar cuando una solicitud coincide con esta directiva. No es un archivo obligatorio.
   - Acción de**resultado indefinido: acción** a realizar si el resultado de la evaluación de directivas no está definido (UNDEF). No es un campo obligatorio.
   - **Expresión** : expresión de directiva avanzada que utiliza la directiva para responder a una solicitud específica. Por ejemplo, true.
   - **Comentarios** : cualquier comentario sobre la directiva.

Enlace de la directiva OAuthIdP y la directiva LDAP al servidor virtual de autenticación

1. Vaya a **Configuración > Seguridad > Tráfico de aplicaciones AAA > Directivas > Autenticación > Directivas avanzadas > Acciones > LDAP**.
2. En la pantalla **Acciones de LDAP**, haga clic en **Agregar**.
3. En la pantalla **Crear servidor LDAP de autenticación**, defina los valores de los siguientes parámetros y haga clic en **Crear**.

- **Nombre:** nombre de la acción LDAP
- **ServerName/ServerIP:** proporciona FQDN o IP del servidor LDAP
- Elija los valores adecuados **para Tipo de seguridad, Puerto, Tipo de servidor, Tiempo de espera**
- Asegúrese de que **la autenticación** esté marcada
- **DN base:** Base desde la que se inicia la búsqueda LDAP. Por ejemplo, dc=aaa, dc=local.
- **DN de enlace de administrador:** nombre de usuario del enlace al servidor LDAP. Por ejemplo, admin@aaa.local.
- **Contraseña de administrador/Confirmar contraseña: Contraseña para enlazar LDAP**
- Haga clic en **Probar conexión** para probar su configuración.
- **Atributo de nombre de inicio de sesión del servidor:** elija **"sAMAccountName"**
- Otros campos no son obligatorios y, por lo tanto, se pueden configurar según sea necesario.

4. Vaya a **Configuración > Seguridad > Tráfico de aplicaciones AAA > Directivas > Autenticación > Directivas avanzadas > Directiva.**
5. En la pantalla **Directivas de autenticación**, haga clic en **Agregar**.
6. En la página **Crear directiva de autenticación**, defina los valores de los siguientes parámetros y haga clic en **Crear.**

   - **Nombre:** nombre de la directiva de autenticación LDAP.
   - **Tipo de acción:** seleccione **LDAP.**
   - **Acción:** seleccione la acción LDAP.
   - **Expresión:** expresión de directiva avanzada que utiliza la directiva para responder a una solicitud específica. Por ejemplo, es cierto**.

Para configurar el dispositivo Citrix ADC como proveedor de identidad mediante el protocolo OpenID Connect mediante CLI

En el símbolo del sistema, escriba los siguientes comandos:

- `add authentication OAuthIDPProfile <name> [-clientID <string>][-clientSecret ][-redirectURL <URL>][-issuer <string>][-audience <string>][-skewTime <mins>] [-defaultAuthenticationGroup <string>]<!--NeedCopy-->`
- `add authentication OAuthIdPPolicy <name> -rule <expression> [-action <string> [-undefAction <string>] [-comment <string>][-logAction <string >]<!--NeedCopy-->`
- `add authentication ldapAction aaa-ldap-act -serverIP 10.0.0.10 -ldapBase "dc=aaa,dc=local"<!--NeedCopy-->`

- ldapBindDn <administrator@aaa.local> -ldapBindDnPassword <password> -ldapLoginName sAMAccountName<!--NeedCopy-->
- add authentication policy aaa-ldap-adv-pol -rule **true** -action aaa-ldap-act<!--NeedCopy-->
- bind authentication vserver auth_vs -policy <ldap_policy_name> -priority 100 -gotoPriorityExpression NEXT<!--NeedCopy-->
- bind authentication vserver auth_vs -policy <OAuthIDPPolicyName> -priority 5 -gotoPriorityExpression END<!--NeedCopy-->
- bind vpn global -certkey <><!--NeedCopy-->

> **Nota**
>
> Puede enlazar más de una tecla. Las partes públicas de los certificados enlazados se envían en respuesta ajwks_uri query (https://gw/oauth/idp/certs).

Citrix ADC como SP de OAuth

April 21, 2022

La función de administración del tráfico de autenticación, autorización y auditoría admite la autenticación de OAuth para autenticar a los usuarios en aplicaciones alojadas en aplicaciones como Google, Facebook y Twitter.

Puntos que tener en cuenta

- Se necesitan Citrix ADC Advanced Edition y versiones posteriores para que la solución funcione.
- OAuth en el dispositivo Citrix ADC está calificado para todos los IDP de SAML que cumplen con "OpenID connect 2.0".

> **Importante:**
>
> El dispositivo Citrix ADC puede responder con un error CSRF cuando un sitio web con mucho contenido envía varias solicitudes de autenticación al caducar la sesión. Como solución alternativa, se recomienda que cuando configure la directiva de OAuth, asegúrese de que la directiva esté configurada tanto para el nombre de host como para la ruta, que son los principales puntos de entrada.

Configurar OAuth mediante la interfaz gráfica de usuario

1. Configure la acción y la directiva de OAuth.

Vaya a **Seguridad > AAA - Tráfico de aplicaciones > Directivas > Autenticación > Directivas avanzadas > Directiva**, y cree una directiva con OAuth como tipo de acción y asocie la acción de OAuth requerida con la directiva.

2. Asocie la directiva de OAuth a un servidor virtual de autenticación.

   Vaya a **Seguridad > AAA - Tráfico de aplicaciones > Servidores virtuales** y asocie la directiva de OAuth con el servidor virtual de autenticación.

> **Nota:**
>
> Los atributos (1 a 16) se pueden extraer en la respuesta de OAuth. Actualmente, estos atributos no se evalúan. Se agregan para referencia futura.

Configurar OAuth mediante la CLI

1. Defina una acción de OAuth.

```
add authentication OAuthAction <name> -authorizationEndpoint <URL>
     -tokenEndpoint <URL> [-idtokenDecryptEndpoint <URL>] -clientID
     <string> -clientSecret <string> [-defaultAuthenticationGroup <
    string>][-tenantID <string>][-GraphEndpoint <string>][-
    refreshInterval <positive_integer>] [-CertEndpoint <string>][-
    audience <string>][-userNameField <string>][-skewTime <mins>][-
    issuer <string>][-Attribute1 <string>][-Attribute2 <string>][-
    Attribute3 <string>]
<!--NeedCopy-->
```

2. Asocie la acción a una directiva de autenticación avanzada.

```
add authentication Policy <name> -rule <expression> -action <
    string>
<!--NeedCopy-->
```

Ejemplo:

```
add authentication oauthAction a -authorizationEndpoint https://
    example.com/ -tokenEndpoint https://example.com/ -clientiD sadf
     -clientsecret df
<!--NeedCopy-->
```


Para obtener más información sobre los parámetros de autenticación OAuthAction, consulte autenticación OAuthAction.

> **Nota:**
>
> Cuando se especifica un CertEndPoint, el dispositivo Citrix ADC sondea ese punto final en la frecuencia configurada para aprender las claves.

Para configurar un Citrix ADC para que lea el archivo local y analice las claves de ese archivo, se introduce una nueva opción de configuración de la siguiente manera:

```
1 set authentication OAuthAction <> -CertFilePath <path to local file
     with jwks>
2 <!--NeedCopy-->
```

La función OAuth ahora admite las siguientes capacidades en la API de token desde el lado de la parte que confía (RP) y desde el lado del IdP de Citrix Gateway y Citrix ADC.

- Compatibilidad con PKCE (clave de prueba para intercambio de código)
- Soporte para client_assertion

Compatibilidad con atributos nombre-valor para la autenticación de OAuth

Ahora puede configurar los atributos de autenticación de OAuth con un nombre único junto con los valores. Los nombres se configuran en el parámetro de acción OAuth como “Atributos” y los valores se obtienen consultando los nombres. Los atributos extraídos se almacenan en la sesión de autenticación, autorización y auditoría. Los administradores pueden consultar estos atributos mediante `http.req.user.attribute("attribute name")` o `http.req.user.attribute(1)`, según el método elegido para especificar los nombres de los atributos.

Al especificar el nombre del atributo, los administradores pueden buscar fácilmente el valor del atributo asociado a ese nombre de atributo. Además, los administradores ya no tienen que recordar el atributo “atributo1 a atributo16” solo por su número.

> **Importante**
>
> En un comando de OAuth, puede configurar un máximo de 64 atributos separados por comas con un tamaño total inferior a 1024 bytes.
>
> **Nota**
>
> El error de sesión se puede evitar si el tamaño del valor total del “atributo 1 al atributo 16” y los valores de los atributos especificados en “Atributos” no superan los 10 KB.

Para configurar los atributos nombre-valor mediante la CLI

En el símbolo del sistema, escriba:

```
add authentication OAuthAction <name> [-Attributes <string>]

set authentication OAuthAction <name> [-Attributes <string>]
<!--NeedCopy-->
```

Ejemplos:

```
add authentication OAuthAction a1  - attributes ”email,company”  -
   attribute1 email

set authentication OAuthAction oAuthAct1 -attributes ”mail,sn,
   userprincipalName”
<!--NeedCopy-->
```

Citrix ADC como proveedor de identidad de OAuth

July 8, 2022

Ahora se puede configurar un dispositivo Citrix ADC como proveedor de identidad mediante el protocolo OpenID-Connect (OIDC). El protocolo OIDC refuerza las capacidades de aportación de identidad del dispositivo Citrix ADC. Ahora puede acceder a la aplicación alojada en toda la empresa con un inicio de sesión único, ya que OIDC ofrece más seguridad al no transferir la contraseña del usuario, sino al usar tokens con una duración específica. OpenID también está diseñado para integrarse con clientes que no son de explorador, como aplicaciones y servicios. Por lo tanto, muchas implementaciones adoptan ampliamente el protocolo OIDC.

> **Nota**
>
> Citrix ADC debe tener la versión 12.1 o posterior para que el dispositivo funcione como proveedor de identidad de OAuth mediante el protocolo OIDC.

Ventajas de tener Citrix ADC como proveedor de identidades de OAuth

- Elimina la sobrecarga de mantener varias contraseñas de autenticación, ya que el usuario tiene una identidad única en toda la organización.

- Proporciona una seguridad sólida para su contraseña, ya que la contraseña solo se comparte con su proveedor de identidad y no con ninguna aplicación a la que accedas.
- Proporcionó una amplia interoperabilidad con varios sistemas, lo que facilita que las aplicaciones alojadas acepten OpenID.

> **Nota**
>
> Se necesitan Citrix ADC Advanced Edition y versiones posteriores para que la solución funcione.

Para configurar el dispositivo Citrix ADC como IdP de OAuth mediante la GUI

1. Vaya a **Configuración > Seguridad > Tráfico de aplicaciones AAA > Directivas > Autenticación > Directivas avanzadas > IdP de OAuth**.
2. Haga clic en **Perfil** y haga clic en **Agregar.**

   En la pantalla **Crear perfil de proveedor de identidad de OAuth de autenticación**, defina los valores para los siguientes parámetros y haga clic en **Crear**.

   - **Nombre**: Nombre del perfil de autenticación. Debe comenzar con una letra, un número o un carácter de guión bajo (_) y debe contener solo letras, números y guión (-), punto (.), almohadilla (#), espacio ( ), en (@), igual a (=), dos puntos (:) y guión bajo. No se puede cambiar una vez creado el perfil.
   - **ID de cliente**: Cadena única que identifica al SP. El servidor de autorización infiere la configuración del cliente mediante este ID. Longitud máxima: 127.
   - **Client Secret**: Cadena secreta establecida por el usuario y el servidor de autorización. Longitud máxima: 239.
   - **URL de redirección**: Punto final del SP en el que se debe publicar el código/token.
   - **Nombre del emisor**: Identidad del servidor cuyos tokens se van a aceptar. Longitud máxima: 127.
   - **Público**: Destinatario objetivo del token que envía el IdP. El destinatario podría comprobarlo.
   - **Tiempo sesgado**: Esta opción especifica el sesgo de reloj permitido en minutos que Citrix ADC permite en un token entrante. Por ejemplo, si skewTime es 10, el token sería válido desde (tiempo actual - 10) min a (tiempo actual+ 10) min, es decir, 20 min en total. Valor por defecto: 5.
   - **Grupo de autenticación predeterminado**: Un grupo que se agrega a la lista de grupos internos de la sesión cuando el IdP elige este perfil y que se puede usar en el flujo nFactor. Se puede usar en la expresión (AAA.USER.IS_MEMBER_OF (“xxx”)) para que las directivas de autenticación
     identificar el flujo de nFactor relacionado con la parte de confianza. Longitud máxima: 63

A group added to the session for this profile to simplify policy evaluation and help in customizing policies. This is the default group that is chosen when the authentication succeeds in addition to the extracted groups. Maximum Length: 63.

3. Haga clic en **Directivas** y en **Agregar.**
4. En la pantalla **Crear directiva de IDP de OAuth de autenticación**, defina los valores para los siguientes parámetros y haga clic en **Crear**.
   - **Nombre**: Nombre de la directiva de autenticación.
   - **Acción**: Nombre del perfil creado anteriormente.
   - **Acción de registro**: Nombre de la acción de registro de mensajes que se utilizará cuando una solicitud coincida con esta directiva. No es un archivo obligatorio.
   - Acción de**resultado indefinido: acción** a realizar si el resultado de la evaluación de directivas no está definido (UNDEF). No es un campo obligatorio.
   - **Expresión**: Expresión de directiva avanzada que la directiva utiliza para responder a una solicitud específica. Por ejemplo, true.
   - **Comentarios**: Cualquier comentario sobre la directiva.

Enlace de la directiva OAuthIDP y la directiva LDAP al servidor virtual de autenticación

1. Vaya a **Configuración > Seguridad > Tráfico de aplicaciones AAA > Directivas > Autenticación > Directivas avanzadas > Acciones > LDAP**.
2. En la pantalla **Acciones de LDAP**, haga clic en **Agregar**.
3. En la pantalla **Crear servidor LDAP de autenticación**, defina los valores de los siguientes parámetros y haga clic en **Crear**.
   - **Nombre:** nombre de la acción LDAP
   - **ServerName/ServerIP:** proporciona FQDN o IP del servidor LDAP
   - Elija los valores adecuados **para Tipo de seguridad, Puerto, Tipo de servidor, Tiempo de espera**
   - Asegúrese de que **la opción de autenticación** esté marcada
   - **DN base:** Base desde la que se inicia la búsqueda LDAP. Por ejemplo, dc=aaa, dc=local.
   - **DN de enlace de administrador:** nombre de usuario del enlace al servidor LDAP. Por ejemplo, admin@aaa.local.
   - **Contraseña de administrador/Confirmar contraseña: Contraseña para enlazar LDAP**
   - Haga clic en **Probar conexión** para probar su configuración.
   - **Atributo de nombre de inicio de sesión del servidor:** elija **“sAMAccountName”**
   - Otros campos no son obligatorios y, por lo tanto, se pueden configurar según sea necesario.

4. Vaya a **Configuración > Seguridad > Tráfico de aplicaciones AAA > Directivas > Autenticación > Directivas avanzadas > Directiva.**
5. En la pantalla **Directivas de autenticación**, haga clic en **Agregar**.
6. En la página **Crear directiva de autenticación**, defina los valores de los siguientes parámetros y haga clic en **Crear.**
   - **Nombre:** nombre de la directiva de autenticación LDAP.
   - **Tipo de acción:** seleccione **LDAP.**
   - **Acción:** seleccione la acción LDAP.
   - **Expresión:** Expresión de directiva avanzada que la directiva utiliza para responder a una solicitud específica. Por ejemplo, true**.

La función OAuth ahora admite las siguientes capacidades en la API de token desde el lado de la parte que confía (RP) y desde el lado del IdP de Citrix Gateway y Citrix ADC.

- Compatibilidad con PKCE (clave de prueba para intercambio de código)
- Soporte para client_assertion

Para configurar el dispositivo Citrix ADC como un IdP mediante el protocolo OIDC mediante la CLI

En el símbolo del sistema, escriba los comandos siguientes:

```
add authentication OAuthIDPProfile <name> [-clientID <string>][-
    clientSecret ][-redirectURL <URL>][-issuer <string>][-audience <
    string>][-skewTime <mins>] [-defaultAuthenticationGroup <string>]

add authentication OAuthIdPPolicy <name> -rule <expression> [-action <
    string> [-undefAction <string>] [-comment <string>][-logAction <
    string>]

add authentication ldapAction aaa-ldap-act -serverIP 10.0.0.10 -
    ldapBase ”dc=aaa,dc=local”

ldapBindDn <administrator@aaa.local> -ldapBindDnPassword <password> -
    ldapLoginName sAMAccountName

add authentication policy aaa-ldap-adv-pol -rule true -action aaa-ldap-
    act

bind authentication vserver auth_vs -policy <ldap_policy_name> -
    priority 100 -gotoPriorityExpression NEXT
```



```
12
13 bind authentication vserver auth_vs -policy <OAuthIDPPolicyName> -
       priority 5 -gotoPriorityExpression END
14
15 bind vpn global  - certkey <>
16 <!--NeedCopy-->
```

Nota:

- Puede enlazar más de una tecla. Las partes públicas de los certificados enlazados se envían en respuesta a`jwks\\_uri query (https://gw/oauth/idp/certs).`
- El dispositivo de punto final introspectivo de IdP de OAuth admite la propiedad `active: true`.

Compatibilidad con tokens cifrados en el protocolo OIDC

El dispositivo Citrix ADC con el mecanismo OIDC ahora admite el envío de tokens cifrados junto con tokens firmados. El dispositivo Citrix ADC utiliza especificaciones de cifrado web JSON para calcular los tokens cifrados y solo admite la serialización compacta de tokens cifrados. Para cifrar un token OpenID, un dispositivo Citrix ADC necesita la clave pública de la parte que confía (RP). La clave pública se obtiene dinámicamente sondeando el punto final de configuración conocido de la parte que confía.

Se introduce una nueva opción “relyingPartyMetadataURL” en el perfil “authentication OAuthIDPProfile”.

Para configurar el punto final de la parte de confianza mediante la CLI

En el símbolo del sistema, escriba:

“‘set authentication OAuthIDPProfile [-relyingPartyMetadataURL] [-refreshInterval] [-status < >]

```
1 -  **relyingPartyMetadataURL**: Dispositivo de punto final en el que el
      proveedor de identidades de Citrix ADC puede obtener detalles sobre
      la parte que confía que se está configurando. La respuesta de
     metadatos debe incluir dispositivos de punto final para jwks_uri
     para claves públicas de RP.
2
3 -  **refreshInterval**: Define la velocidad a la que se debe sondear
     este extremo para actualizar los certificados en minutos.
4
5 -  **status**: Refleja el estado de la operación de sondeo. El estado
     se completa una vez que el dispositivo Citrix ADC obtiene
     correctamente las claves públicas.
```



```
6
7       **Ejemplo**
8
9       ```
10      set authentication OAuthIDPProfile sample_profile -
           relyingPartyMetadataURL https://rp.customer.com/metadata -
           refreshInterval 50 -status < >
11      <!--NeedCopy-->
```

Una vez configurado el punto final, un dispositivo Citrix ADC primero sondea el dispositivo de punto final conocido de la parte que confía para leer la configuración. Actualmente, el dispositivo Citrix ADC procesa solo el extremo 'jwks_uri'.

- Si 'jwks_uri' está ausente en la respuesta, el estado del perfil no está completo.
- Si el 'jwks_uri' está presente en la respuesta, Citrix ADC sondea ese punto final también para leer las claves públicas de la parte que confía.

> **Nota:**
>
> Solo se admiten los algoritmos de tipo de cifrado RSAES-OAEP y AES256 GCM para el cifrado de tokens.

Compatibilidad con atributos personalizados en OpenID Connect

Es posible que los usuarios de confianza de `OpenID` necesiten más que un nombre de usuario o un nombre principal de usuario (UPN) en el token para crear el perfil de usuario o tomar decisiones de autorización. Por lo general, los grupos de usuarios deben aplicar directivas de autorización para el usuario. A veces, se necesitan más detalles, como el nombre o el apellido, para aprovisionar una cuenta de usuario.

El dispositivo Citrix ADC configurado como IdP se puede utilizar para enviar atributos adicionales en el OidCID_token mediante expresiones. Las expresiones de directiva avanzadas se utilizan para enviar los atributos personalizados según el requisito. El IdP de Citrix evalúa las expresiones correspondientes a los atributos y, a continuación, calcula el token final.

El dispositivo Citrix ADC aplican automáticamente `JSONify` a los datos de salida. Por ejemplo, los números (como SSN) o los valores booleanos (true o false) no están rodeados de comillas. Los atributos con varios valores, como los grupos, se colocan dentro de un marcador de matriz ("[" y "]"). Los atributos de tipo complejo no se calculan automáticamente y puede configurar la expresión PI de esos valores complejos según su requisito.

Para configurar el punto final de la parte de confianza mediante la CLI

En el símbolo del sistema, escriba:


```
set oauthidpprofile <name> -attributes <AAA-custom-attribute-pattern>
<!--NeedCopy-->
```

El<AAA-custom-attribute-pattern> puede describirse como:

Attribute1=PI-Expresión@@@attribute2=PI-Expresión@@@

'attribute1', 'attribute2' son cadenas literales que representan el nombre del atributo que se insertará en id_token.

> **Nota:** Puede configurar hasta 2.000 bytes de atributos.

Ejemplo: `set oauthidpprofile sample_1 -attributes q{ myname=http.req.user.name@@@ssn="123456789"@@@jit="false"@@@groups=http.req.user.groups }`

- La expresión PI anterior es una expresión de directiva avanzada que representa el valor que se va a utilizar para el atributo. La expresión PI se puede usar para enviar un literal de cadena, como "'cadena codificada"'. El literal de cadena está rodeado de comillas dobles alrededor de comillas simples o comillas dobles alrededor de un inicio y un patrón (como se indicó anteriormente, el patrón de inicio es "q {"). Si el valor del atributo no es un literal de cadena, la expresión se evalúa en tiempo de ejecución y su valor se envía en token. Si el valor en tiempo de ejecución está vacío, el atributo correspondiente no se agrega al token de ID.
- Como se define en el ejemplo, "false" es una cadena literal para el atributo "jit". Además, "ssn" tiene un valor codificado como referencia. Los grupos y`myname`"" son expresiones PI que producen cadenas.

Compatibilidad con implementaciones de GSLB activo-activas en Citrix Gateway

Citrix Gateway configurado como proveedor de identidad (IdP) mediante el protocolo OIDC puede admitir implementaciones de GSLB activo-activas. La implementación activa y activa de GSLB en el IdP de Citrix Gateway proporciona la capacidad de equilibrar la carga de una solicitud de inicio de sesión de usuario entrante en varias ubicaciones geográficas.

> **Importante**
>
> Citrix recomienda vincular certificados de CA al servicio SSL y habilitar la validación de certificados en el servicio SSL para mejorar la seguridad.

Para obtener más información sobre cómo configurar la configuración de GSLB, consulte Ejemplo de configuración y configuración de GSLB.

Autenticación de API con el dispositivo Citrix ADC

August 20, 2021

Hay un cambio de paradigma en la forma en que las aplicaciones modernas interactúan con sus clientes. Tradicionalmente, los clientes de explorador se utilizaban para acceder a servicios. Las aplicaciones suelen establecer cookies de sesión para rastrear el contexto del usuario. Las aplicaciones modernas y distribuidas dificultan el mantenimiento de sesiones de usuario en los microservicios. Debido a esto, la mayoría de los accesos a la aplicación se han convertido en API.
Los clientes que se comunican con estos servicios distribuidos también han evolucionado. La mayoría de los clientes obtienen tokens de una entidad de confianza llamada Servidor de autorización para probar la identidad y el acceso del usuario. Estos clientes luego presentan el token a la aplicación con cada solicitud de acceso. Por lo tanto, los dispositivos proxy tradicionales como Citrix ADC deben evolucionar para admitir estos clientes. Un dispositivo Citrix ADC proporciona a los administradores una forma de manejar dicho tráfico. Citrix ADC se puede implementar como API Gateway para frontend todo el tráfico destinado a los servicios publicados. Una API Gateway se puede implementar para entornos nativos tradicionales (Hybrid Multi Cloud o HMC) o en la nube. API Gateway finaliza todo el tráfico entrante para ofrecer varios servicios como autenticación, autorización, limitación de velocidad, redirección, almacenamiento en caché, descarga SSL, firewall de aplicaciones, etc. Por lo tanto, se convierte en un componente crítico de la infraestructura.

Tipos de token

Los tokens intercambiados durante el acceso a la API se ajustan principalmente al protocolo OAuth/OpenID Connect (OIDC). Los tokens de acceso que se usan solo para 'acceso delegado' se ajustan al protocolo OAuth, mientras que los tokens de ID que cumplen con OIDC también llevan información de usuario.
Los tokens de acceso son normalmente un blob de datos opaco o aleatorio. Sin embargo, a veces pueden ser identificados tokens de acuerdo con los estándares JWT (Json Web Token). Los tokens de ID siempre están firmados JWT.

Acceso a API con OAuth

El tipo de autenticación OAuth en un dispositivo Citrix ADC se puede usar para manejar protocolos OAuth y OIDC. OIDC es una extensión del protocolo OAuth.

OAuthAction en un dispositivo Citrix ADC se puede utilizar para gestionar clientes interactivos, como exploradores y clientes nativos, como aplicaciones cliente. Los clientes interactivos se redirigen al proveedor de identidad para iniciar sesión mediante el protocolo OIDC. Los clientes nativos pueden obtener tokens fuera de banda y pueden presentarlos en un dispositivo Citrix ADC para acceder a ellos.

> **Nota:**
>
> El token de acceso obtenido de los dispositivos de punto final se puede almacenar en caché para solicitudes posteriores, mejorando así el rendimiento de la API.

Para configurar la compatibilidad con el almacenamiento en caché de tokens mediante la interfaz de línea de comandos, escriba el siguiente comando en el símbolo del sistema:

```
set aaaparameter  - apITokenCache <ENABLED>

<!--NeedCopy-->
```

En las secciones siguientes se describe el método de acceso API realizado por clientes nativos.

Servidor virtual para acceso a API

Para implementar un dispositivo Citrix ADC para un acceso API, se implementa un servidor virtual Traffic Management (TM) con la autenticación 401. Se asocia con un servidor virtual de autenticación (autenticación, autorización y auditoría) para contener las directivas de autenticación y sesión. El siguiente fragmento de configuración crea uno de estos servidores virtuales.

```
Add lb vserver lb-api-access SSL <IP> 443 -authn401 On -AuthnVsName
   auth-api-access

Bind ssl vserver lb-api-access -certkeyName <ssl-cert-entity>

Add authentication vserver auth-api-access SSL
<!--NeedCopy-->
```

> **Nota:**
>
> Tendría que vincular un servicio al servidor virtual de TM y una directiva de autenticación (con OAuthAction descrita de la siguiente manera) al servidor virtual de autenticación para completar la configuración.

Después de crear el servidor virtual, es necesario agregar una OAuthAction junto con la directiva correspondiente. Hay varias otras opciones dentro de una acción de OAuth dependiendo del tipo de token y otros mecanismos de seguridad.

Configuración de OAuth para tokens de ID

Los tokens de ID siempre están firmados JWT. Es decir, llevan encabezado, carga útil y firma. Dado que se trata de tokens independientes, un dispositivo Citrix ADC puede validar estos tokens localmente. Para validar estos tokens, el dispositivo necesitaría conocer la clave pública de la clave privada correspondiente utilizada para firmar estos tokens.

Lo que sigue es un ejemplo de OAuthAction con ciertos argumentos obligatorios junto con "CertendPoint".

```
1 Add authentication OAuthAction oauth-api-access -clientid <your-client-
    id> -clientsecret <your-client-secret> -authorizationEndpoint <URL
    to which users would be redirected for login> -tokenEndpoint <
    endpoint at which tokens could be obtained> -certEndpoint <uri at
    which public keys of IdP are published>
2 <!--NeedCopy-->
```

Donde:

- **ID de cliente**: Cadena única que identifica SP. El servidor de autorización deduce la configuración del cliente mediante este ID. Longitud máxima: 127.
- **Secreto del cliente**: Cadena secreta establecida por el usuario y el servidor de autorización. Longitud máxima: 239.
- **AuthorizationEndPoint**: URL en la que los usuarios normalmente iniciarían sesión (cuando usan clientes interactivos).
- **TokenEndPoint**: URL en el servidor de autorización en el que se obtienen/intercambian tokens/código
- **CertendPoint**: URL en la que el Servidor de autorización publica claves públicas utilizadas para firmar los tokens. El Servidor de autorización puede publicar más de una clave y elegir una de ellas para firmar tokens.

> **Nota: Identificación** de cliente/Secreto de client/AuthorizationEndPoint/TokenEndpoint son parámetros opcionales para API Access. Sin embargo, es una buena práctica proporcionar valores para estos parámetros, ya que la entidad de acción puede reutilizarse para diferentes propósitos.

En la configuración anterior 'CertPointPoint' es esencial para la validación de ID Token. Este extremo contiene claves públicas del certificado utilizado para firmar los tokens. Estas claves públicas deben corresponder a la especificación JWK (Json Web Keys).

Una vez configurado CertendPoint en el dispositivo Citrix ADC, sondea periódicamente el endpoint (con el intervalo predeterminado de 1 día que puede personalizarse en la configuración) para man-

tener actualizadas las claves públicas. Después de que las claves públicas estén disponibles, ADC puede realizar la validación local de los tokens de identificación entrantes.

Configuración de OAuth para tokens de acceso opaco

Los tokens opacos no se pueden verificar localmente en el dispositivo Citrix ADC. Estos deben validarse en el servidor de autorización. Un dispositivo Citrix ADC utiliza el "protocolo de introspección" mencionado en las especificaciones de OAuth para verificar estos tokens. Una nueva opción, IntrospectURL, se proporciona en la configuración de OAuth para verificar tokens opacos.

```
set oauthAction oauth-api-acccess -introspectURL <uri of the
    Authorization Server for introspection>

<!--NeedCopy-->
```

El formato de la API de introspección se ajusta a la especificación de la `https://tools.ietf.org/html/rfc7662##section-2.1` siguiente manera:

```
POST /introspect HTTP/1.1
Host: server.example.com
Accept: application/json
Content-Type: application/x-www-form-urlencoded
Authorization: Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW
token=mF_9.B5f-4.1JqM&token_type_hint=access_token

<!--NeedCopy-->
```

Directiva de enlace a Authentication vserver

Una vez creada OAuthAction, es necesario crear la directiva correspondiente para invocarla.

```
add authentication policy oauth-api-access -rule <> -action <oauth-api-
    access><!--NeedCopy-->
```

bind authentication vserver auth-api-access -policy oauth-api-access -pri 100

```
## Configuración de seguridad adicional en un dispositivo Citrix ADC
```



```
2
3 La validación de token incluye comprobaciones de duración del token.
    Los tokens fuera del tiempo aceptable se rechazan. A continuación se
     presentan los ajustes adicionales para mayor seguridad. Algunos de
    estos se recomiendan para ser configurados siempre.
4
5 **Audiencia**: OAuth Action se puede configurar con un destinatario
    previsto del token. Todos los tokens se comparan con esta URL
    configurada. Un dispositivo Citrix ADC tiene una capacidad adicional
     en la que el campo de audiencia apunta realmente a un patrón
    establecido en el dispositivo. Con este conjunto de patrones, un
    administrador puede configurar más de una URL para la audiencia.
6
7 <!--NeedCopy-->
```

add policy patset oauth_audiences

bind patset oauth_audiences https://app1.company.com

bind patset oauth_audiences https://app2.company.com

bind patset oauth_audiences httpsL//app1.company.com/path1

set oAuthAccess oauth-api-access -audience oauth_audiences

```
1 En el ejemplo anterior, se especifica más de una audiencia en un
    conjunto de patrones. Por lo tanto, solo se permite un token
    entrante si contiene cualquiera de las direcciones URL configuradas
    en el conjunto de patrones.
2
3 **Emisor**: Identidad del servidor cuyos tokens deben ser aceptados.
    Longitud máxima: 127. Es una buena práctica configurar el emisor de
    los tokens en la acción OAuth. Esto garantiza que los tokens
    emitidos por el Servidor de autorización incorrecto no están
    permitidos.
4
5 **SkewTime**: Especifica el sesgo de reloj permitido en el número de
    minutos que permite un dispositivo Citrix ADC en un token entrante.
    Por ejemplo, si SkewTime es 10, entonces el token sería válido desde
     (hora actual: 10) min hasta (hora actual + 10) min, es decir 20 min
     en total. Valor predeterminado: 5
6
7 **AllowedAlgorithms**: Esta opción permite al administrador restringir
    ciertos algoritmos en los tokens entrantes. De forma predeterminada,
     todos los métodos admitidos están permitidos. Sin embargo, estos se
```



```
      pueden controlar mediante esta opción.
8
9  La siguiente configuración garantiza que solo se permiten los tokens
       que utilizan RS256 y RS512:
10
11 <!--NeedCopy-->
```

set oAuthAction oauth-api-access -allowedAlgorithms RS256 RS512

```
1  Después de la configuración anterior, solo se permiten tokens que usan
       RS256 y RS512.
2
3  ## Omitir cierto tráfico de la autenticación
4
5  En muchos casos, hay algunas API de descubrimiento que son accesibles p
       úblicamente para los clientes. Estas API suelen revelar la
       configuración y las capacidades del propio servicio. Un
       administrador puede configurar el dispositivo Citrix ADC para que
       omita la autenticación de estas direcciones URL de metadatos
       mediante la directiva "Sin autenticación" que se describe a
       continuación:
6
7  <!--NeedCopy-->
```

add authentication policy auth-bypass-policy -rule <> -action NO_AUTHN

bind authentication vserver auth-api-access -policy auth-bypass-policy -pri 110

```
1  NO_AUTHN es una acción implícita que da como resultado que la
       autenticación se complete cuando la regla coincide. Hay otros usos
       de la acción NO_AUTHN más allá del alcance del acceso API.
2  <!--NeedCopy-->
```

Autenticación LDAP

April 5, 2022

Al igual que con otros tipos de directivas de autenticación, una directiva de autenticación de protocolo ligero de acceso a directorios (LDAP) comprende una expresión y una acción. Después de crear una directiva de autenticación, la enlaza a un servidor virtual de autenticación y le asigna una prioridad.

Al vincularlo, también lo designa como directiva principal o secundaria. Además de las funciones de autenticación estándar, LDAP puede buscar cuentas de usuario para usuarios que no existen localmente en otros servidores de Active Directory (AD). Esta función se denomina soporte de referencia o persecución de referencias.

Normalmente, se configura Citrix ADC para que use la dirección IP del servidor de autenticación durante la autenticación. Con los servidores de autenticación LDAP, también puede configurar el ADC para que use el FQDN del servidor LDAP en lugar de su dirección IP para autenticar a los usuarios. El uso de un FQDN puede simplificar una configuración de autenticación, autorización y auditoría mucho más compleja en entornos en los que el servidor de autenticación puede estar en cualquiera de varias direcciones IP, pero siempre usa un único FQDN. Para configurar la autenticación mediante el FQDN de un servidor en lugar de su dirección IP, siga el proceso de configuración normal, excepto cuando cree la acción de autenticación. Al crear la acción, se utiliza el parámetro **ServerName** en lugar del parámetro **ServerIP** y se sustituye el FQDN del servidor por su dirección IP.

Antes de decidir si desea configurar el ADC para que use la IP o el FQDN del servidor LDAP para autenticar a los usuarios, tenga en cuenta que configurar la autenticación, la autorización y la auditoría para autenticarse en un FQDN en lugar de en una dirección IP agrega un paso adicional al proceso de autenticación. Cada vez que el ADC autentica a un usuario, debe resolver el FQDN. Si muchos usuarios intentan autenticarse simultáneamente, las búsquedas de DNS resultantes pueden ralentizar el proceso de autenticación.

La compatibilidad con referencias LDAP está inhabilitada de forma predeterminada y no se puede habilitar de forma global Debe habilitarse de forma explícita para cada acción de LDAP. Asegúrese de que el servidor de AD acepte las mismas `binddn credentials` que se usa con el servidor de referencia (GC). Para habilitar la compatibilidad con referencias, configure una acción LDAP para seguir las referencias y especifique el número máximo de referencias a seguir.

Si la compatibilidad con referencias está habilitada y Citrix ADC recibe una respuesta LDAP_REFERRAL a una solicitud, la autenticación, la autorización y la auditoría siguen la referencia al servidor de active directory (AD) contenido en la referencia y realiza la actualización en ese servidor. En primer lugar, la autenticación, la autorización y la auditoría buscan el servidor de referencia en DNS y se conectan a ese servidor. Si la directiva de referencia requiere SSL/TLS, se conecta a través de SSL/TLS. A continuación, se vincula al nuevo servidor con las `binddn credentials` que usó con el servidor anterior y realiza la operación que generó la referencia. Esta función es transparente para el usuario.

Los números de puerto de las conexiones LDAP son:

- 389 para conexiones LDAP no seguras (para LDAP de texto sin formato)
- 636 para conexiones LDAP seguras (para SSL LDAP)
- 3268 para conexiones LDAP no seguras de Microsoft (para servidor de catálogo global de texto sin formato)
- 3269 para conexiones LDAP seguras de Microsoft (para SSL Global Catalog Server)

La tabla siguiente contiene ejemplos de campos de atributos de usuario para servidores LDAP:

Servidor LDAP	atributo de usuario	Sensible a may
Servidor Microsoft Active Directory	sAMAccountName	No
Directorio electrónico de Novell	ou	Sí
Servidor IBM Directory	uid	Sí
Dominó de loto	CN	Sí
Directorio Sun ONE (anteriormente iPlanet)	uid o cn	Sí

Esta tabla contiene ejemplos del DN base:

Servidor LDAP	DN base
Servidor Microsoft Active Directory	DC=citrix, DC = local
Directorio electrónico de Novell	ou=users, ou=dev
Servidor IBM Directory	cn=usuarios
Dominó de loto	OU=Ciudad, O=Citrix, C=US
Directorio Sun ONE (anteriormente iPlanet)	ou=Personas, dc=citrix, dc=com

La tabla siguiente contiene ejemplos de DN de enlace:

Servidor LDAP	Enlazar DN
Servidor Microsoft Active Directory	CN=Administrador, CN=Usuarios, DC=citrix, DC=local
Directorio electrónico de Novell	cn=admin, o=citrix
Servidor IBM Directory	LDAP_dn
Dominó de loto	CN=Administrador de notas, O=Citrix, C=US
Directorio Sun ONE (anteriormente iPlanet)	uid=admin, ou=Administradores, ou=topologyManagement, o=netscaperoot

Para obtener más información sobre la configuración de directivas de autenticación en general, consulte Directivas de autenticación. Para obtener más información sobre las expresiones Citrix ADC, que se utilizan en la regla de directiva, consulte Directivas y expresiones.

Para crear un servidor de autenticación LDAP mediante la CLI

En el símbolo del sistema, escriba los comandos siguientes:

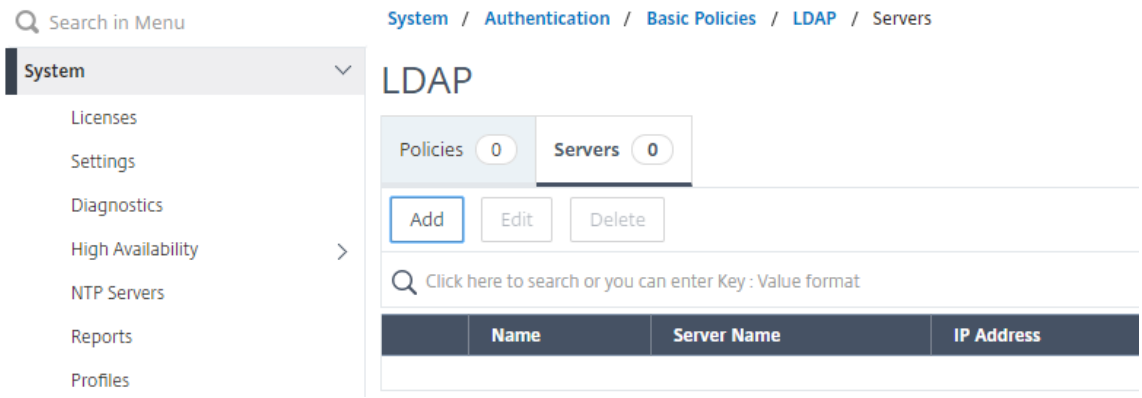
```
add authentication ldapAction <name> {
 -serverIP }
  <ip_addr|ipv6_addr|> | {
 -serverName <string> }
  }
```

Ejemplo

```
add authentication ldapAction ldap_server -serverip 1.1.1.1 -serverName
    ldap_test
```

Para crear un servidor de autenticación LDAP mediante la interfaz gráfica de usuario

1. Vaya a **Sistema > Autenticación > Directivas básicas > LDAP > Servidores > Agregar**.



2. En la página **Crear servidor LDAP de autenticación**, configure los parámetros del servidor LDAP.
3. Haga clic en **Create**.

Para habilitar una directiva de autenticación mediante la CLI

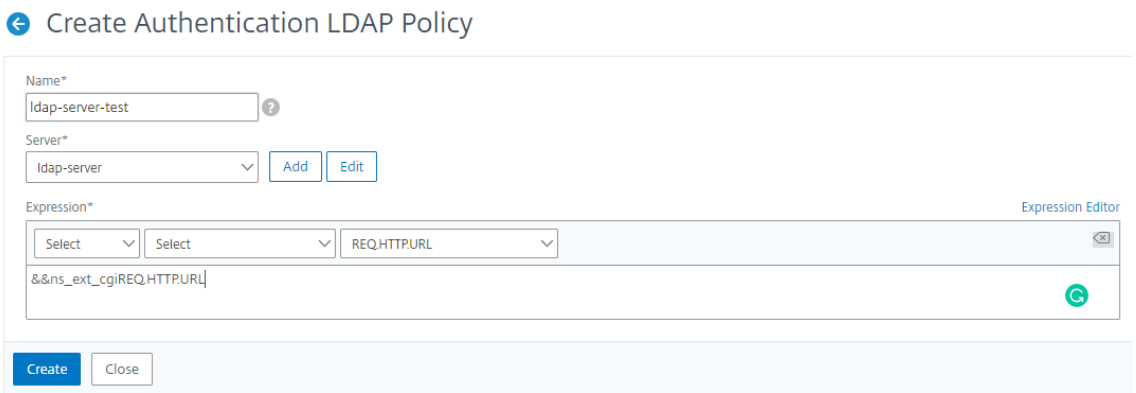
```
add authentication ldappolicy <name> <rule> [<reqAction>]
```

Ejemplo:

```
add authentication ldappolicy ldap-service-policy ns_true ldap_Server
```

Para crear una directiva de autenticación LDAP mediante la interfaz gráfica de usuario

1. Vaya a **Sistema > Autenticación > Directivas básicas > LDAP > Directivas > Agregar**
2. En la página **Crear directiva LDAP de autenticación**, configure los parámetros de la directiva LDAP.



3. Haga clic en **Create**.

> **Nota**
>
> Puede configurar servidores/directivas LDAP a través de la ficha **Seguridad**. Vaya a **Seguridad > AAA - Tráfico de aplicaciones > Directivas > Autenticación > Directivas básicas > LDAP > Servidores/Directivas**.

Para habilitar el soporte de referencia de LDAP mediante la CLI

En el símbolo del sistema, escriba los comandos siguientes:

```
set authentication ldapAction <name> -followReferrals ON
set authentication ldapAction <name> -maxLDAPReferrals <integer>
<!--NeedCopy-->
```


Ejemplo

```
set authentication ldapAction ldapAction-1 -followReferrals ON
set authentication ldapAction ldapAction-1 -maxLDAPReferrals 2
<!--NeedCopy-->
```

Soporte de autenticación basada en claves para los usuarios de LDAP

Con la autenticación basada en claves, ahora puede obtener la lista de claves públicas que se almacenan en el objeto de usuario en el servidor LDAP a través de SSH. El dispositivo Citrix ADC durante el proceso de autenticación basada en roles (RBA) debe extraer claves SSH públicas del servidor LDAP. La clave pública recuperada, que es compatible con SSH, debe permitirle iniciar sesión a través del método RBA.

Se introduce un nuevo atributo “sshPublicKey” en los comandos “add authentication ldapAction” y “set authentication ldapAction”. Al usar este atributo, puede obtener los siguientes beneficios:

- Puede almacenar la clave pública recuperada y la acción LDAP utiliza este atributo para recuperar la información de clave SSH del servidor LDAP.
- Puede extraer nombres de atributo de hasta 24 KB.

> Nota
>
> El servidor de autenticación externo, como LDAP, solo se usa para recuperar información de clave SSH. No se usa para fines de autenticación.

A continuación se muestra un ejemplo del flujo de eventos a través de SSH:

- El demonio SSH envía una solicitud AAA_AUTHENTICATE con el campo de contraseña vacío al puerto del demonio de autenticación, autorización y auditoría.
- Si LDAP está configurado para almacenar la clave pública SSH, la autenticación, la autorización y la auditoría responden con el atributo “sshPublicKey” junto con otros atributos.
- El demonio SSH verifica estas claves con las claves del cliente.
- El demonio SSH pasa el nombre de usuario en la carga útil de la solicitud, y la autenticación, la autorización y la auditoría devuelven las claves específicas de este usuario junto con las claves genéricas.

Para configurar el atributo sshPublicKey, en el símbolo del sistema, escriba los siguientes comandos:

- Con la operación add, puede agregar el atributo “sshPublicKey” mientras configura el comando `ldapAction`.


```
add authentication ldapAction <name> {
-serverIP <ip_addr|ipv6_addr|*> | {
-serverName <string> }
 }
 [-serverPort <port>] … [-Attribute1 <string>] … [-Attribute16
    <string>][-sshPublicKey <string>][-authentication off]
<!--NeedCopy-->
```

- Con la operación set, puede configurar el atributo “sshPublicKey” en un comando LDAPAction ya agregado.

```
set authentication ldapAction <name> [-sshPublicKey <string>][-
   authentication off]
<!--NeedCopy-->
```

Compatibilidad con atributos nombre-valor para la autenticación LDAP

Ahora puede configurar los atributos de la autenticación LDAP con un nombre único junto con valores. Los nombres se configuran en el parámetro de acción LDAP y los valores se obtienen consultando el nombre. Al usar esta función, un administrador de dispositivos Citrix ADC ahora puede lograr los siguientes beneficios:

- Minimiza el esfuerzo de los administradores al recordar el atributo por nombre (no solo por valor)
- Mejora la búsqueda para consultar el valor de atributo asociado a un nombre
- Proporciona una opción para extraer varios atributos

Para configurar esta función en el símbolo del sistema del dispositivo Citrix ADC, escriba:

```
add authentication ldapAction <name> [-Attribute1 <string>]
<!--NeedCopy-->
```

Ejemplo

```
add authentication ldapAction ldapAct1 attribute1 mail
<!--NeedCopy-->
```


Soporte para validar la autenticación LDAP de extremo a extremo

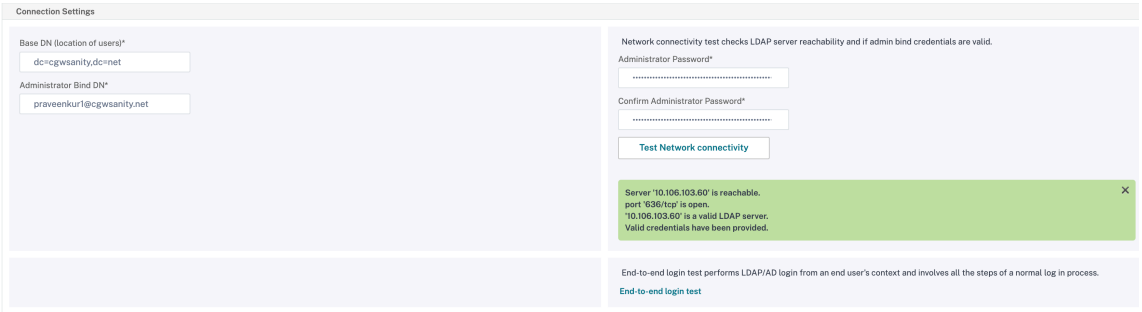
El dispositivo Citrix ADC ahora puede validar la autenticación LDAP de extremo a extremo a través de la GUI. Para validar esta función, se introduce un nuevo botón de "prueba" en la GUI. Un administrador del dispositivo Citrix ADC puede usar esta función para lograr los siguientes beneficios:

- Consolida el flujo completo (motor de paquetes, demonio AAA de Citrix ADC, servidor externo) para proporcionar un mejor análisis
- Reduce el tiempo de validación y resolución de problemas relacionados con casos individuales

Tiene dos opciones para configurar y ver los resultados de las pruebas de la autenticación de extremo a extremo LDAP mediante la interfaz gráfica de usuario.

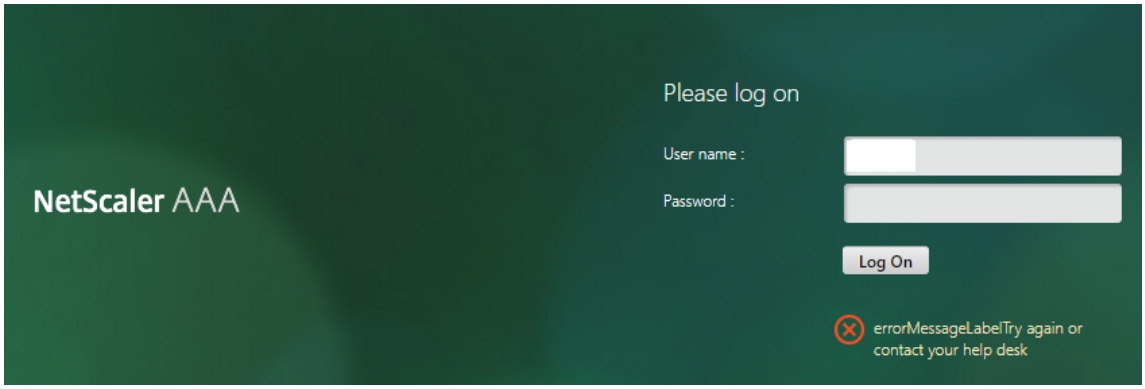
Desde la opción del sistema

1. Vaya a **Sistema > Autenticación > Directivas básicas > LDAP** y haga clic en la ficha **Servidores**.
2. Seleccione la **acción LDAP** disponible en la lista.
3. En la página **Configurar servidor LDAP de autenticación**, desplácese hacia abajo hasta la sección **Configuración de conexiones**.
4. Haga clic en **Probar conectividad de red** para comprobar la conexión del servidor LDAP. Puede ver un mensaje emergente de conexión correcta al servidor LDAP con los detalles del puerto TCP y la autenticidad de las credenciales válidas.



5. Para ver la autenticación LDAP de extremo a extremo, haga clic en el enlace **Prueba de inicio de sesión de extremo a extremo**.
6. En la página **Prueba de inicio de sesión integral**, haga clic en **Probar**.
    - En la página de autenticación, introduzca las credenciales válidas para iniciar sesión. Se muestra la pantalla de éxito.

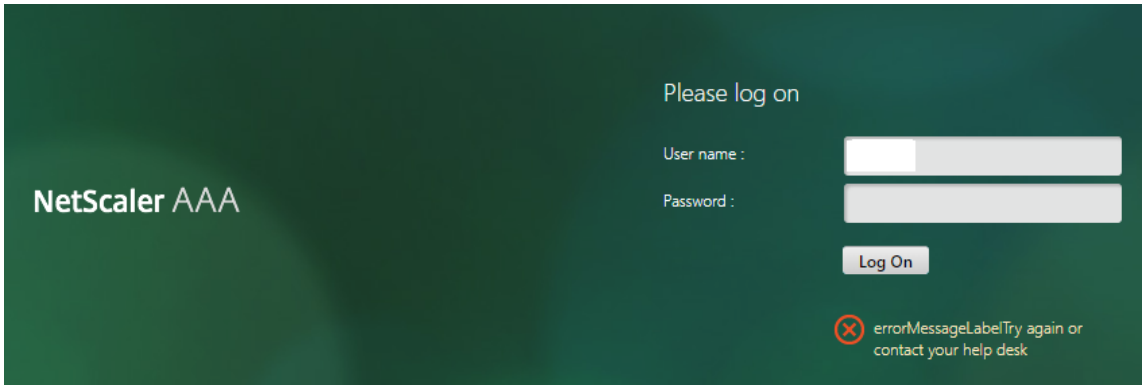
- Si la autenticación falla, se muestra la pantalla de error.



En la opción Autenticación

1. Vaya a **Autenticación > Panel de control**, seleccione la acción LDAP disponible en la lista.
2. En la página **Configurar servidor LDAP de autenticación**, tiene dos opciones en la sección **Configuración de conexiones**.
3. Para comprobar la conexión del servidor LDAP, haga clic en la ficha **Probar LDAP Reachability**. Puede ver un mensaje emergente de conexión correcta al servidor LDAP con los detalles del puerto TCP y la autenticidad de las credenciales válidas.
4. Para ver el estado de autenticación LDAP de extremo a extremo, haga clic en el enlace **Probar conexión de usuario final**.
5. En la página **Probar conexión de usuario final**, haga clic en **Probar**.
   - En la página de autenticación, introduzca las credenciales válidas para iniciar sesión. Se muestra la pantalla de éxito.

   - Si la autenticación falla, se muestra la pantalla de error.



Notificación de caducidad de contraseñas de 14 días para la autenticación LDAP

El dispositivo Citrix ADC ahora admite la notificación de caducidad de contraseñas de 14 días para la autenticación basada en LDAP. Al usar esta función, los administradores pueden notificar a los usuarios finales sobre el tiempo límite de caducidad de la contraseña en días. La notificación de caducidad de la contraseña de 14 días es precursora del restablecimiento de contraseña de autoservicio (SSPR).

> **Nota**
>
> El valor máximo o el tiempo límite en días para la notificación de caducidad de contraseñas es de 255 días.

Ventajas de la notificación de caducidad de contraseñas

- Permita a los usuarios restablecer sus contraseñas por sí mismos y brinde a los administradores una forma flexible de notificar al usuario final sobre la caducidad de su contraseña en días.
- Elimina la dependencia del usuario final para rastrear los días de caducidad de sus contraseñas.
- Envía notificaciones a la página del portal de VPN a los usuarios (en función del número de días) para que cambien su contraseña antes de que caduque.

> **Nota**
>
> Esta función solo se aplica a los esquemas de autenticación basados en LDAP, no a RADIUS o TACACS.

Comprender la notificación de contraseña de 14 días

El dispositivo Citrix ADC obtiene dos atributos (`Max-Pwd-Age and Pwd-Last-Set`) del servidor de autenticación LDAP.

- **Edad máxima de la almohadilla.** Este atributo indica la cantidad máxima de tiempo, en intervalos de 100 nanosegundos, hasta que la contraseña sea válida. El valor se almacena como un

entero grande que representa el número de intervalos de 100 nanosegundos desde el momento en que se estableció la contraseña antes de que caduque la contraseña.

- **Último juego de almohadillas.** Este atributo determina la fecha y la hora en que se cambió por última vez la contraseña de una cuenta.

Al obtener los dos atributos del servidor de autenticación LDAP, el dispositivo Citrix ADC determina el tiempo restante para que caduque la contraseña para un usuario en particular. Esta información se recopila cuando se validan las credenciales de usuario en el servidor de autenticación y se envía una notificación al usuario.

Se introduce un nuevo parámetro "pwdExpiryNotification" en el `set aaa parameter`comando. Al usar este parámetro, un administrador puede realizar un seguimiento del número de días que quedan para que caduque la contraseña. El dispositivo Citrix ADC ahora puede comenzar a notificar al usuario final sobre la caducidad de su contraseña.

> **Nota**
>
> Actualmente, esta función solo funciona para los servidores de autenticación que tienen servidores Microsoft AD con implementación LDAP. La compatibilidad con servidores basados en OpenLDAP se prevé más adelante.

A continuación se muestra un ejemplo del flujo de eventos para establecer una notificación de caducidad de contraseña de 14 días:

1. Un administrador, mediante el dispositivo Citrix ADC, establece un tiempo (14 días) para la caducidad de la contraseña.
2. El usuario envía una solicitud HTTP o HTTPS para acceder a un recurso en el servidor back-end.
3. Antes de proporcionar acceso, el dispositivo Citrix ADC valida las credenciales del usuario con lo que está configurado en el servidor de autenticación LDAP.
4. Junto con esta consulta al servidor de autenticación, el dispositivo Citrix ADC lleva la solicitud para obtener los detalles de los dos atributos (`Max-Pwd-Age and Pwd-Last-Set`).
5. Según el tiempo restante para que caduque la contraseña, se muestra una notificación de caducidad.
6. A continuación, el usuario toma las medidas apropiadas para actualizar la contraseña.

Para configurar la notificación de caducidad de 14 días mediante la interfaz de línea de comandos

> **Nota**
>
> La notificación de caducidad de 14 días se puede configurar para casos de uso de VPN sin cliente y VPN completa, y no para el proxy ICA.

En el símbolo del sistema, escriba los comandos siguientes:


```
set aaa parameter  - pwdExpiryNotificationDays <positive_integer>

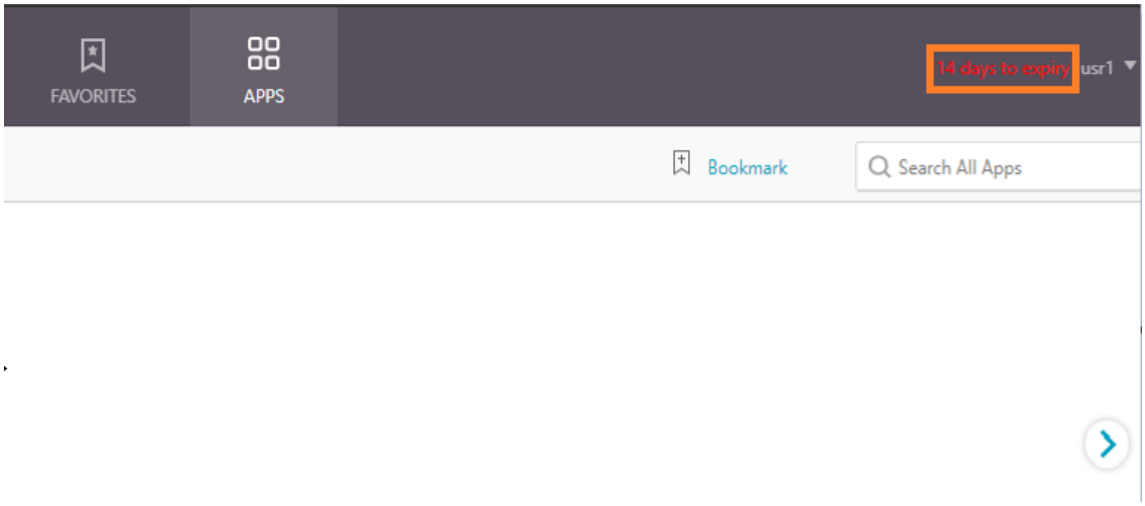
show aaa parameter
<!--NeedCopy-->
```

Ejemplo

```
    > set aaa parameter -pwdExpiryNotificationDays 14
    Done
    > show aaa parameter                              Configured AAA
       parameters  EnableStaticPageCaching: YES
       EnableEnhancedAuthFeedback: NO  DefaultAuthType: LOCAL
       MaxAAAUsers:           Unlimited
                                              AAAD nat ip: None
                  EnableSessionStickiness : NO  aaaSessionLoglevel :
       INFORMATIONAL               AAAD Log Level : INFORMATIONAL
                      Dynamic address: OFF
       GUI mode: ON
       Max Saml Deflate Size: 1024             Password Expiry
          Notification Days: 14
<!--NeedCopy-->
```

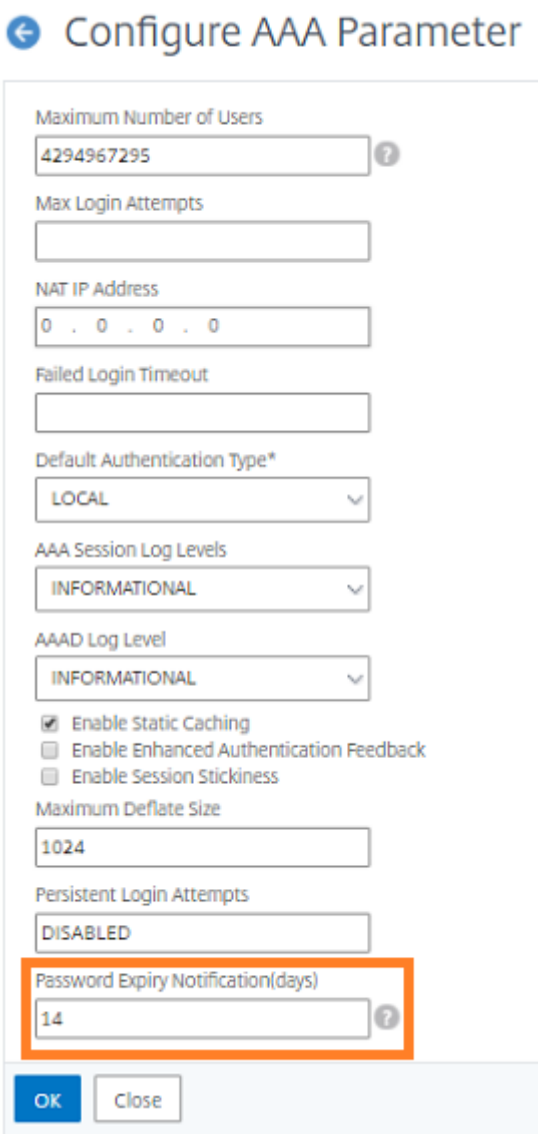
Para configurar la notificación de caducidad de 14 días mediante GUI

1. Vaya a **Seguridad > AAA - Tráfico de aplicaciones > Configuración de autenticación**.
2. Haga clic en **Cambiar configuración AAA de autenticación**.
3. En la página **Configurar parámetro AAA**, especifique los días en el campo **Notificación de caducidad de contraseña (días)**.



4. Haga clic en **Aceptar.**

   La notificación aparece en la esquina superior derecha de la página del portal de VPN.



Configurar la autenticación LDAP en el dispositivo Citrix ADC para fines de administración

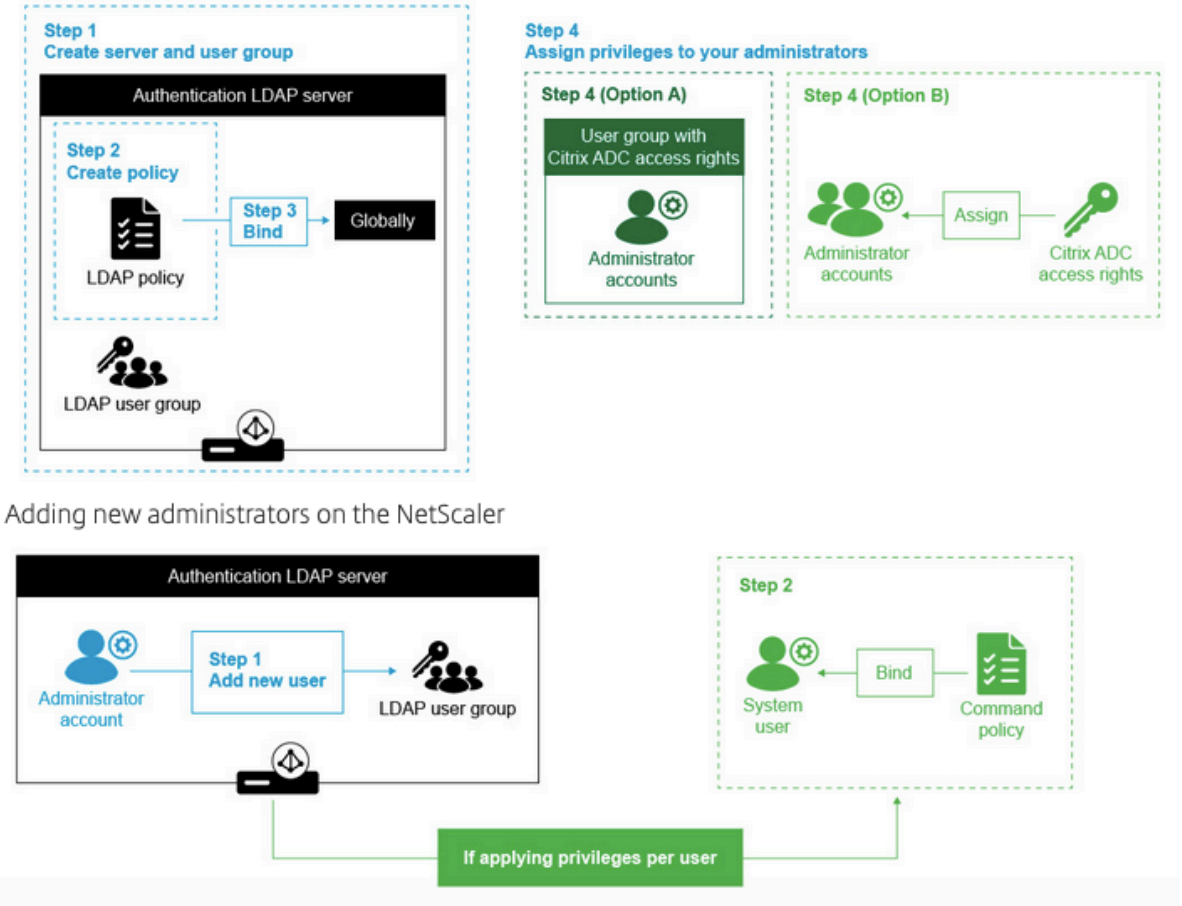
December 2, 2021

Puede configurar el inicio de sesión del usuario en el dispositivo Citrix ADC mediante las credenciales de active directory (nombre de usuario y contraseña) para fines de administración (superusuario, de solo lectura, privilegios de red y todos los demás).

Requisitos previos

- servidores de controladores de dominio de Windows Active Directory
- Un grupo de dominio dedicado para los administradores de NetScaler
- Citrix Gateway 10.1 y versiones posteriores

Las siguientes imágenes ilustran la autenticación LDAP en el dispositivo Citrix ADC.

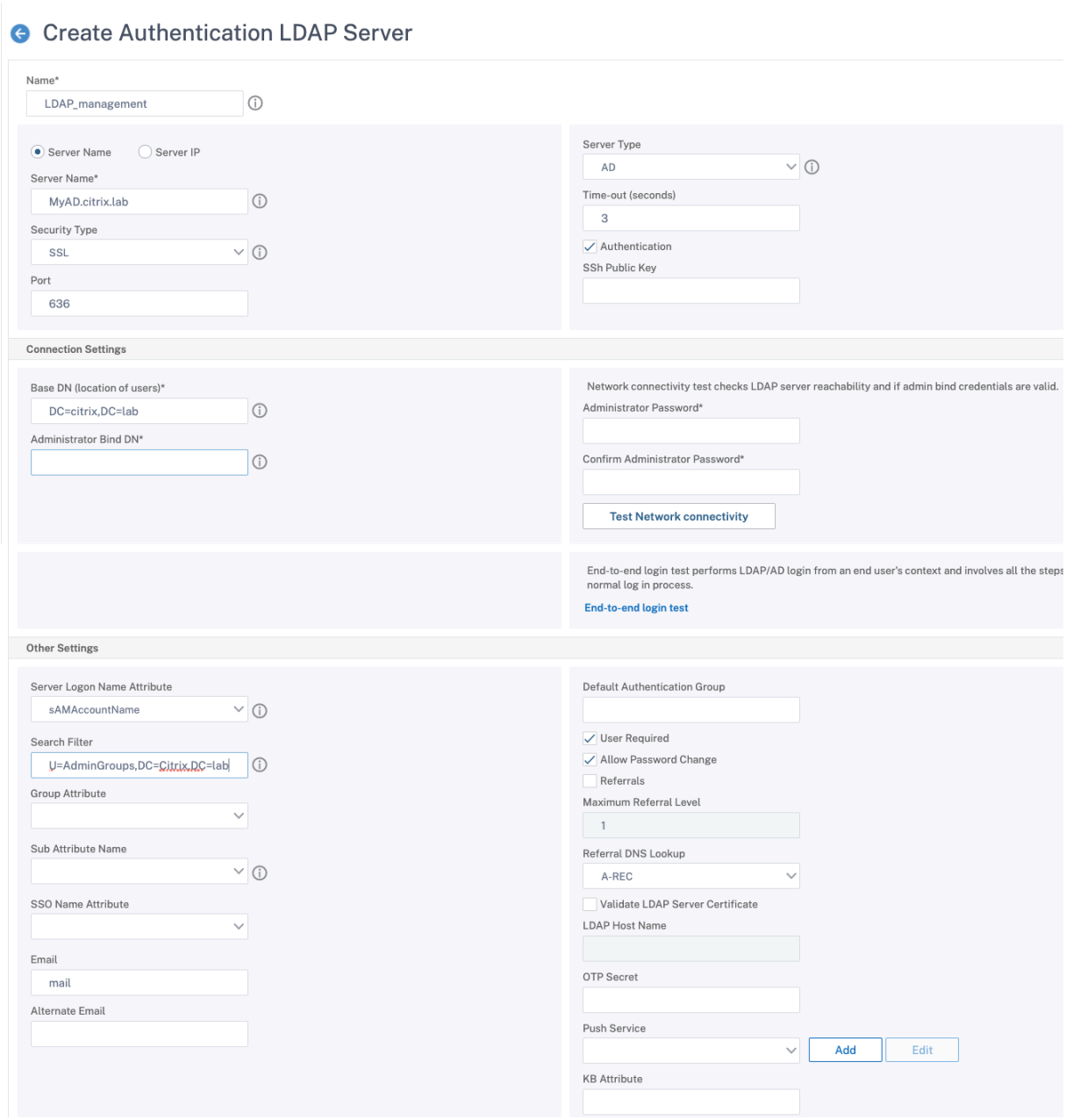


Pasos de configuración de alto nivel

1. Crear un servidor LDAP
2. Crear una directiva LDAP
3. Vincular la directiva LDAP
4. Asigne privilegios a sus administradores de una de las siguientes maneras
    - Aplicar privilegios en grupo
    - Aplicar privilegios individualmente para cada usuario

Crear un servidor LDAP de autenticación

1. Vaya a **Sistema > Autenticación > LDAP**.
2. Haga clic en la ficha **Servidor** y, a continuación, en **Agregar**.
3. Complete la configuración y, a continuación, haga clic en **Crear**.



> **Nota:**
>
> En este ejemplo, el acceso se limita al dispositivo Citrix ADC mediante el filtrado de la autenticación en la pertenencia al grupo de usuarios mediante la configuración de Filtro de búsqueda. El valor utilizado para este ejemplo es - & (memberof=CN=NSG_admin, ou=AdminGroups,

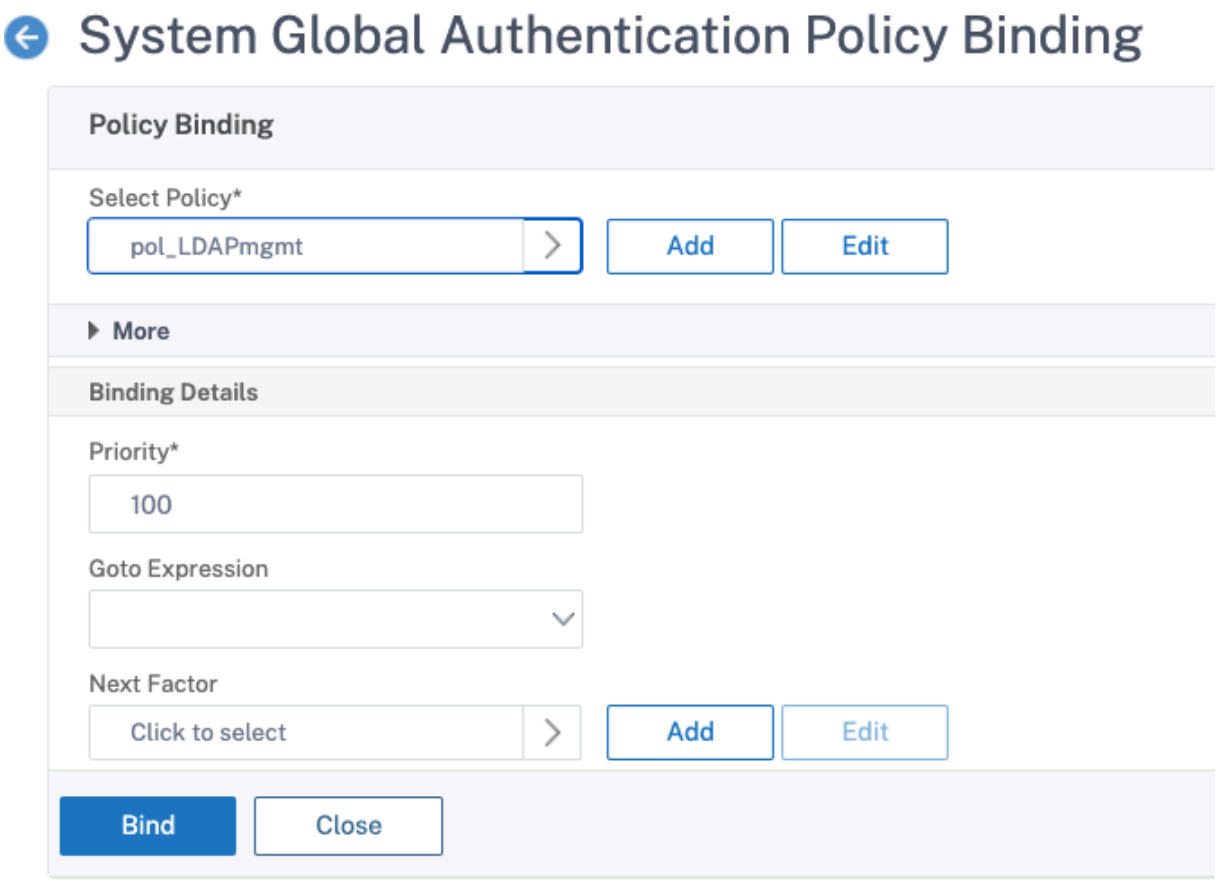
> DC=Citrix, DC=lab)

Crear una directiva LDAP

1. Vaya a **Sistema > Autenticación > Directivas avanzadas > Directiva**.
2. Haga clic en **Agregar**.
3. Introduzca un nombre para la directiva, seleccione el servidor que creó en los pasos anteriores.
4. En el campo de texto Expresión, introduzca la expresión adecuada y, a continuación, haga clic en **Crear**.

Vincular la directiva LDAP de forma global

1. Vaya a **Sistema > Autenticación > Directivas avanzadas > Directiva**.
2. En la página Directivas de autenticación, haga clic en **Enlaces globales**.
3. Seleccione la directiva que ha creado (en este ejemplo, pol_LDAPMgmt).
4. Elija una prioridad en consecuencia (cuanto menor sea el número, mayor será la prioridad)
5. Haga clic en **Enlazar y,** a continuación, en **Listo**. Aparece una marca de verificación verde en la columna **Vinculado globalmente**.



Asigne privilegios a sus administradores

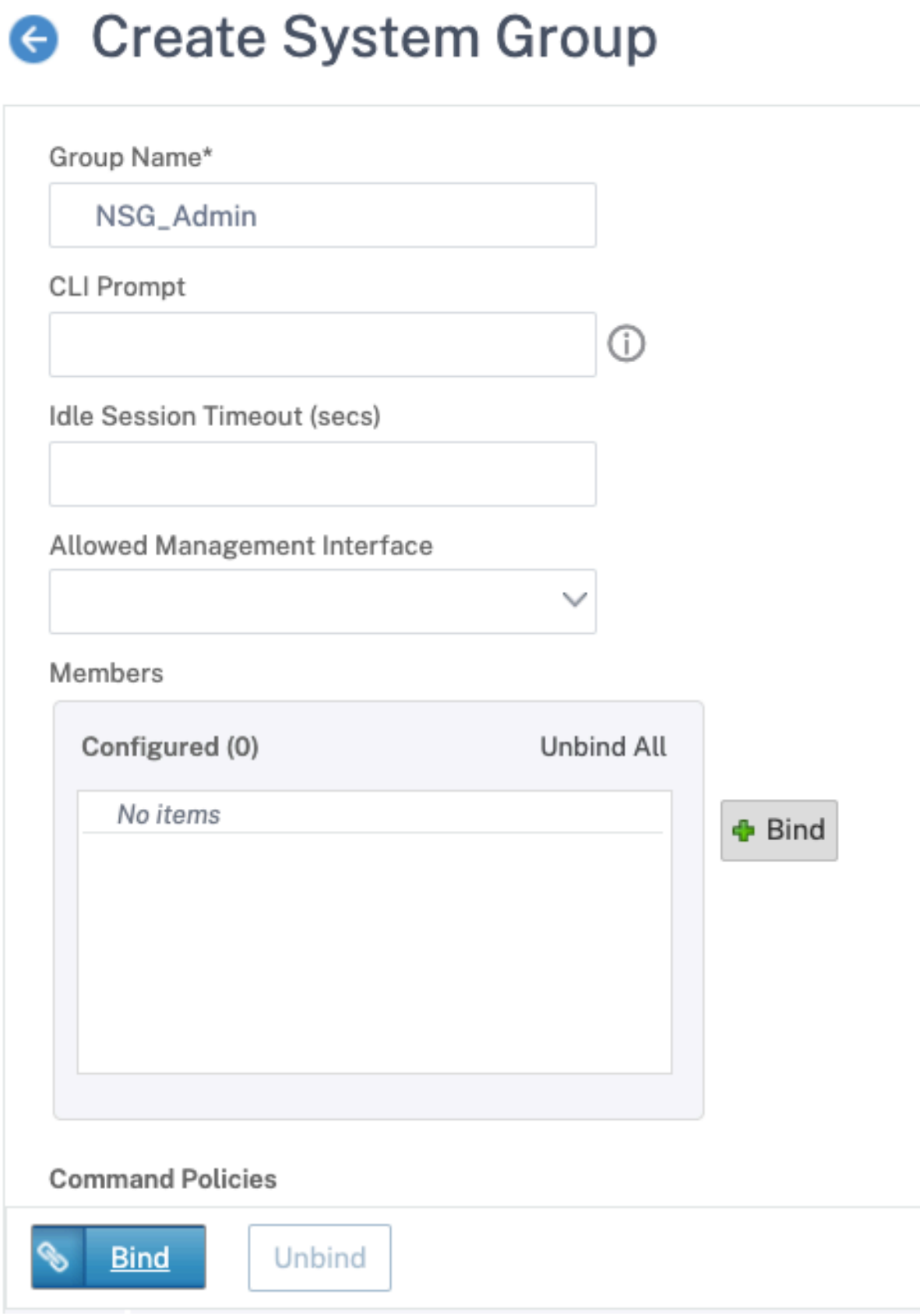
Puede elegir una de las dos opciones siguientes.

- **Aplicar privilegios a un grupo:** agregue un grupo en el dispositivo Citrix ADC y asigne los mismos derechos de acceso para cada usuario que sea miembro de este grupo.
- **Aplique privilegios individualmente para cada usuario:** cree la cuenta de administrador de cada usuario y asigne derechos para cada uno de ellos.

Aplicar privilegios a un grupo

Al aplicar privilegios a un grupo, los usuarios que son miembros del grupo de Active Directory configurado en el filtro de búsqueda (en este ejemplo, NSG_Admin) pueden conectarse a la interfaz de administración de Citrix ADC y tener una directiva de comandos de superusuario.

1. Vaya a **Sistema > Administración de usuarios > Grupos**.
2. Introduzca los detalles según el requisito y, a continuación, haga clic en **Crear**.



Ha definido el grupo de Active Directory al que pertenecen los usuarios y también el nivel de directiva de comandos que debe asociarse a la cuenta al iniciar sesión. Puede agregar nuevos usuarios administradores al grupo LDAP que configuró en el filtro de búsqueda.

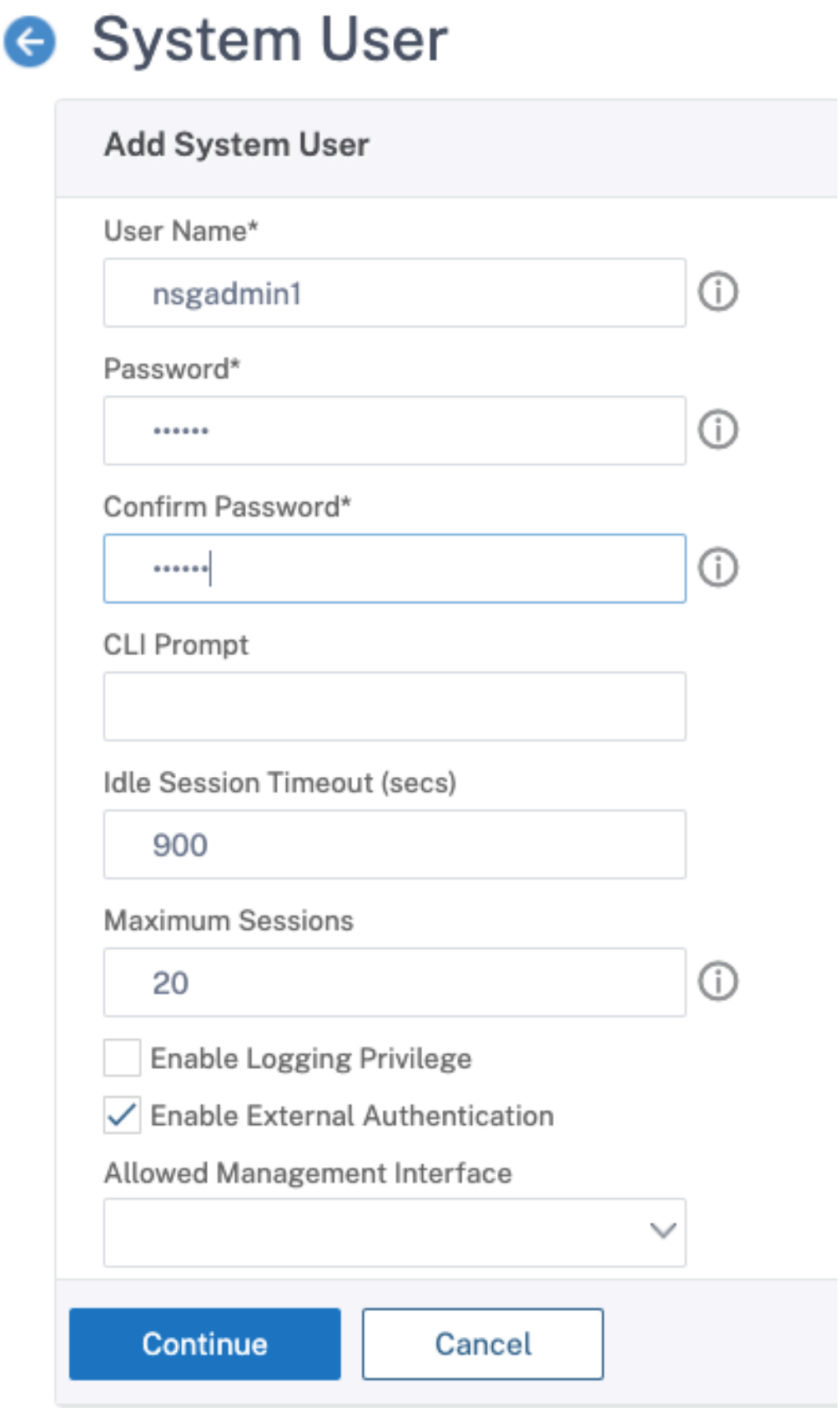
> **Nota:**
>
> El nombre del grupo debe coincidir con el registro de active directory.

Aplicar privilegios individualmente para cada usuario

En este caso, los usuarios que son miembros del grupo de Active Directory configurado en el filtro de búsqueda (en este ejemplo, NSG_Admin) pueden conectarse a la interfaz de administración de Citrix ADC, pero no tienen ningún privilegio hasta que cree el usuario específico en el dispositivo Citrix ADC y vincule la directiva de comando a él.

1. Vaya a **Sistema > Administración de usuarios > Usuarios**.
2. Haga clic en **Agregar**.
3. Introduzca los detalles según el requisito.

   Nota: Asegúrese de seleccionar **Habilitar autenticación externa**.



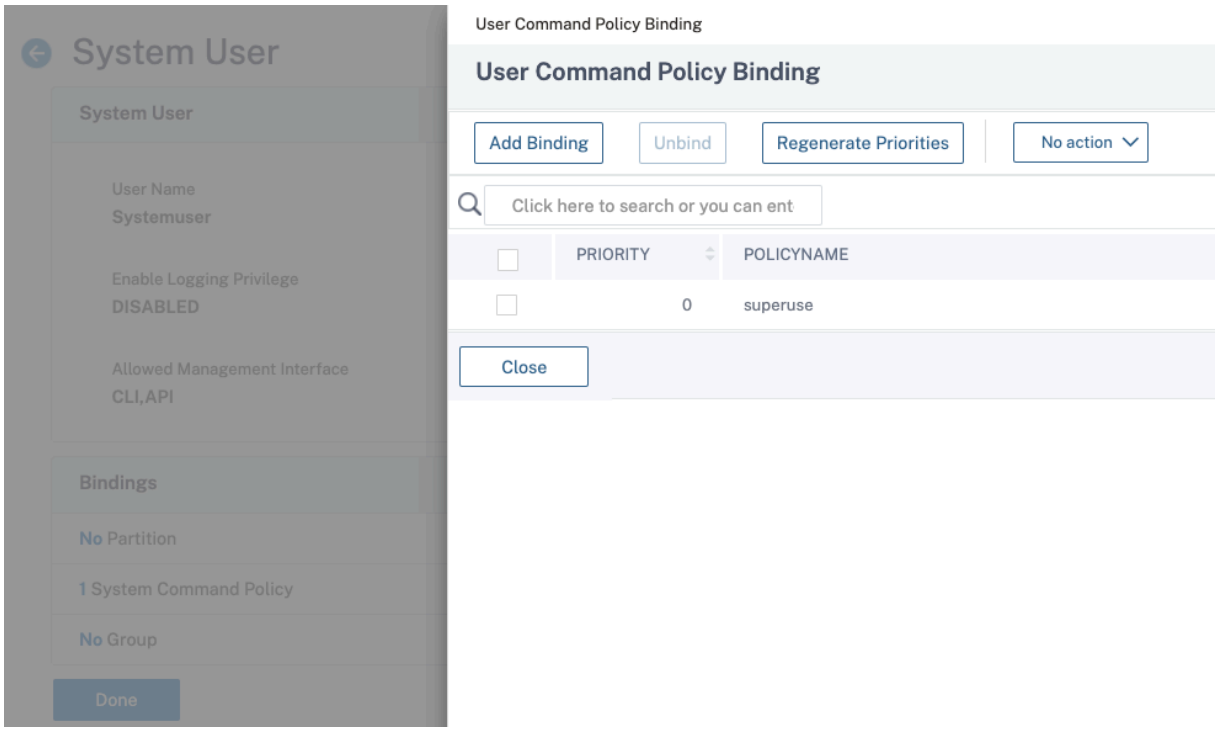
1. Haga clic en **Continue**.

Ha definido el usuario de Active Directory y el nivel de directiva de comandos que debe asociarse a la cuenta al iniciar sesión.

> **Nota:**
>
> - El nombre de usuario debe coincidir con el registro de active directory del usuario existente.
> - Cuando agrega un usuario a Citrix ADC para la autenticación externa, debe proporcionar una contraseña, si la autenticación externa no está disponible. Para que la autenticación externa funcione correctamente, la contraseña interna no debe ser la misma que la contraseña LDAP de la cuenta de usuario.

Agregar directiva de comandos al usuario

1. Vaya a **Sistema > Administración de usuarios > Usuarios**.
2. Seleccione el usuario que creó y, a continuación, haga clic en **Modificar.**
3. En Enlaces, haga clic en **Directiva de comandos del sistema**.
4. Seleccione la directiva de comandos correcta para aplicarla a su usuario.
5. Haga clic en **Vincular y, a continuación,** en **Cerrar**.



Para agregar más administradores;

- Agregue los usuarios administradores al grupo LDAP que configuró en el filtro de búsqueda.
- Cree el usuario del sistema en Citrix ADC y asigne la directiva de comandos correcta.

Para configurar la autenticación LDAP en el dispositivo Citrix ADC con fines de administración mediante la CLI

Utilice los siguientes comandos como referencia para configurar el inicio de sesión para un grupo con privilegios de superusuario en la CLI del dispositivo Citrix ADC.

1. Crear un servidor LDAP

```
add authentication ldapAction LDAP_mgmt -serverIP myAD.citrix.lab
    -serverPort 636 -ldapBase ”DC=citrix,DC=lab” -ldapBindDn
    readonly@citrix.lab -ldapBindDnPassword -ldapLoginName
    sAMAccountName -searchFilter ”&(memberof=CN=NSG_Admin,OU=
    AdminGroups,DC=citrix,DC=lab)” -groupAttrName memberOf
<!--NeedCopy-->
```

2. Directiva de creación y LDAP

```
add authentication ldapPolicy pol_LDAPmgmt ns_true LDAP_mgmt
<!--NeedCopy-->
```

3. Vinculación de la directiva LDAP

```
bind system global pol_LDAPmgmt -priority 110
<!--NeedCopy-->
```

4. Asigne privilegios a sus administradores

   - Para aplicar privilegios al grupo

```
add system group NSG_Admin
bind system group NSG_Admin -policyName superuser 100
<!--NeedCopy-->
```

   - Para aplicar privilegios individualmente a cada usuario

```
add system user admyoa
bind system user admyoa superuser 100
<!--NeedCopy-->
```


Autenticación RADIUS

August 20, 2021

Al igual que con otros tipos de directivas de autenticación, una directiva de autenticación del Servicio de usuario de marcado de autenticación remota (RADIUS) se compone de una expresión y una acción. Después de crear una directiva de autenticación, la vincula a un servidor virtual de autenticación y le asigna una prioridad. Al vincularlo, también se designa como directiva principal o secundaria. Sin embargo, la configuración de una directiva de autenticación RADIUS tiene ciertos requisitos especiales que se describen a continuación.

Normalmente, se configura Citrix ADC para que utilice la dirección IP del servidor de autenticación durante la autenticación. Con los servidores de autenticación RADIUS, ahora puede configurar el ADC para que utilice el FQDN del servidor RADIUS en lugar de su dirección IP para autenticar a los usuarios. El uso de un FQDN puede simplificar una configuración de autenticación, autorización y auditoría mucho más compleja en entornos en los que el servidor de autenticación podría estar en cualquiera de varias direcciones IP, pero siempre utiliza un único FQDN. Para configurar la autenticación mediante el FQDN de un servidor en lugar de su dirección IP, siga el proceso de configuración normal excepto al crear la acción de autenticación. Al crear la acción, se sustituye el parámetro **serverName** por el parámetro **serverIP**.

Antes de decidir si quiere configurar Citrix ADC para utilizar la IP o el FQDN de su servidor RADIUS para autenticar a los usuarios, tenga en cuenta que configurar la autenticación, la autorización y la auditoría para autenticarse en un FQDN en lugar de en una dirección IP agrega un paso adicional al proceso de autenticación. Cada vez que el ADC autentica a un usuario, debe resolver el FQDN. Si muchos usuarios intentan autenticarse simultáneamente, las búsquedas DNS resultantes podrían ralentizar el proceso de autenticación.

> **Nota**
>
> Estas instrucciones suponen que ya está familiarizado con el protocolo RADIUS y que ya ha configurado el servidor de autenticación RADIUS elegido.

Para agregar una acción de autenticación para un servidor RADIUS mediante la interfaz de línea de comandos

Si autentica en un servidor RADIUS, debe agregar una acción de autenticación explícita. Para ello, en el símbolo del sistema, escriba el siguiente comando:

```
1 add authentication radiusAction <name> [-serverip <IP> | -serverName] <
     FQDN>][-serverPort <port>] [-authTimeout <positive_integer>] {
```



```
 -radKey  }
  [-radNASip ( ENABLED | DISABLED )][-radNASid <string>] [-radVendorID
     <positive_integer>][-radAttributeType <positive_integer>][-
     radGroupsPrefix <string>] [-radGroupSeparator <string>][-
     passEncoding <passEncoding>][-ipVendorID <positive_integer>] [-
     ipAttributeType <positive_integer>][-accounting ( ON | OFF )][-
     pwdVendorID <positive_integer> [-pwdAttributeType <
     positive_integer>]] [-defaultAuthenticationGroup <string>] [-
     callingstationid ( ENABLED | DISABLED )]

<!--NeedCopy-->
```

En el ejemplo siguiente se agrega una acción de autenticación RADIUS denominada **Authn-Act-1**, con la IP de servidor **10.218.24.65**, el puerto de servidor **1812**, el tiempo de espera de autenticación de **15** minutos, la clave RADIUS **WareTheLorax**, la IP NAS inhabilitada y el ID NAS **NAS1**.

```
add authentication radiusaction Authn-Act-1 -serverip 10.218.24.65 -
   serverport 1812 -authtimeout 15 -radkey WareTheLorax -radNASip
   DISABLED -radNASid NAS1
Done

<!--NeedCopy-->
```

En el ejemplo siguiente se agrega la misma acción de autenticación RADIUS, pero se utiliza el servidor FQDN **rad01.example.com** en lugar de la IP.

```
add authentication radiusaction Authn-Act-1 -serverName rad01.example.
   com -serverport 1812 -authtimeout 15 -radkey WareTheLorax -radNASip
   DISABLED -radNASid NAS1
Done

<!--NeedCopy-->
```

Para configurar una acción de autenticación para un servidor RADIUS externo mediante la línea de comandos

Para configurar una acción RADIUS existente, en el símbolo del sistema, escriba el siguiente comando:


```
set authentication radiusAction <name> [-serverip <IP> | -serverName] <
    FQDN>][-serverPort <port>] [-authTimeout <positive_integer>] {
 -radKey  }
  [-radNASip ( ENABLED | DISABLED )][-radNASid <string>] [-radVendorID
     <positive_integer>][-radAttributeType <positive_integer>][-
     radGroupsPrefix <string>] [-radGroupSeparator <string>][-
     passEncoding <passEncoding>][-ipVendorID <positive_integer>] [-
     ipAttributeType <positive_integer>][-accounting ( ON | OFF )][-
     pwdVendorID <positive_integer> [-pwdAttributeType <
     positive_integer>]] [-defaultAuthenticationGroup <string>] [-
     callingstationid ( ENABLED | DISABLED )]

<!--NeedCopy-->
```

Para quitar una acción de autenticación para un servidor RADIUS externo mediante la interfaz de línea de comandos

Para quitar una acción RADIUS existente, en la solicitud de comando, escriba el siguiente comando:

```
rm authentication radiusAction <name>

<!--NeedCopy-->
```

Ejemplo

```
rm authentication radiusaction Authn-Act-1
Done

<!--NeedCopy-->
```

Para configurar un servidor RADIUS mediante la utilidad de configuración

> **Nota**
>
> En la utilidad de configuración, se utiliza el término servidor en lugar de acción, pero se refiere a la misma tarea.

1. Vaya a **Seguridad > AAA: Tráfico de aplicaciones > Directivas > Autenticación > Radio**
2. En el panel de detalles, en la ficha **Servidores**, realice una de las acciones siguientes:
   - Para crear un nuevo servidor RADIUS, haga clic en **Agregar**.

- Para modificar un servidor RADIUS existente, seleccione el servidor y, a continuación, haga clic en **Modificar**.

3. En el cuadro de diálogo **Crear servidor RADIUS de autenticación** o **Configurar servidor RADIUS** de autenticación, escriba o seleccione valores para los parámetros. Para completar los parámetros que aparecen debajo de **Send Calling Station ID**, expanda **Detalles**.
   - name*: RadiusActionName (no se puede cambiar para una acción configurada previamente)
   - Tipo de autenticación*: Authtype (Establecer en RADIUS, no se puede cambiar)
   - Nombre del servidor/Dirección IP*: Elija Nombre del servidor o IP del servidor
     - <FQDN>Nombre del servidor*: NombreServidor
     - Dirección IP*: ServerIP <IP> Si el servidor tiene asignada una dirección IP IPv6, active la casilla de verificación IPv6.
   - puerto*: ServerPort
   - Tiempo de espera (segundos) *: AuthTimeout
   - Clave secreta*: RadKey (secreto compartido RADIUS).
   - Confirmar clave secreta*: Escriba el secreto compartido RADIUS una segunda vez. (Sin equivalente de línea de comandos).
   - ID de estación de llamada de envío: ID de llamada
   - Identificador de proveedor de grupo: Radvendorid
   - Tipo de atributo de grupo: RadattributeType
   - Identificador de proveedor de direcciones IP: IPVendorid
   - pwdVendorid—pwdVendorid
   - Codificación de contraseñas: PassenCoding
   - Grupo de autenticación predeterminado: DefaultAuthenticationGroup
   - ID del NAS: RADNasid
   - Habilitar extracción de direcciones IP del NAS: RADNasip
   - Prefijo de grupo: RadGroupsPrefix
   - Separador de grupo: RadGroupSeparator
   - Tipo de atributo de dirección IP: IPattributeType
   - Tipo de atributo de contraseña: PWDateTributType
   - Contabilidad—Contabilidad
4. Haga clic en **Crear** o **Aceptar**. La directiva que ha creado aparece en la página Servidores.

Soporte para pasar a través del atributo 66 RADIUS (Tunnel-Client-Endpoint)

El dispositivo Citrix ADC ahora permite el paso a través del atributo RADIUS 66 (Tunnel-Client-Endpoint) durante la autenticación RADIUS. Al aplicar esta función, la dirección IP de los clientes se recibe mediante autenticación de segundo factor de confiar para tomar decisiones de autenticación basadas en riesgos.

Se introduce un nuevo atributo "TunnelEndPointClientIP" en el comando "add authentication RadiusAction" y "set RadiusParams".

Para utilizar esta función, en el símbolo del sistema del dispositivo Citrix ADC, escriba:

```
add authentication radiusAction <name> {
 -serverIP <ip_addr|ipv6_addr|*> | {
 -serverName <string> }
  }
  [-serverPort <port>] … [-tunnelEndpointClientIP (ENABLED|DISABLED)]

set radiusParams {
 -serverIP <ip_addr|ipv6_addr|*> |{
 -serverName <string> }
  }
  [-serverPort<port>] … [-tunnelEndpointClientIP(ENABLED|DISABLED)]

<!--NeedCopy-->
```

Ejemplo

```
add authentication radiusAction radius -severIP 1.217.22.20 -serverName
    FQDN -serverPort 1812 -tunnelEndpointClientIp ENABLED

set radiusParams -serverIp 1.217.22.20 -serverName FQDN1 -serverPort
   1812 -tunnelEndpointClientIP ENABLED

<!--NeedCopy-->
```

Compatibilidad con la validación de la autenticación RADIUS de extremo a extremo

El dispositivo Citrix ADC ahora puede validar la autenticación RADIUS de extremo a extremo mediante una GUI. Para validar esta función, se introduce un nuevo botón de "prueba" en la GUI. Un administrador de dispositivos Citrix ADC puede aprovechar esta función para obtener los siguientes beneficios:

- Consolida el flujo completo (motor de paquetes — daemon aaa — servidor externo) para proporcionar un mejor análisis
- Reduce el tiempo de validación y resolución de problemas relacionados con casos individuales

Tiene dos opciones para configurar y ver los resultados de las pruebas de autenticación de extremo a extremo RADIUS mediante la GUI.

Opción De sistema

1. Vaya a **Sistema > Autenticación > Directivas básicas > RADIUS,** haga clic en la ficha **Servidores**.
2. Seleccione la **acción RADIUS** disponible en la lista.
3. En la página **Configurar servidor RADIUS de autenticación**, tiene dos opciones en la sección **Configuración de conexiones**.
4. Para comprobar la conexión del servidor RADIUS, haga clic en la ficha **Probar RADIUS Accesibilidad**.
5. Para ver la autenticación RADIUS de extremo a extremo, haga clic en el vínculo **Probar conexión de usuario final**.

Desde la opción Autenticación

1. Vaya a **Autenticación > Panel de control**, seleccione la acción RADIUS disponible en la lista.
2. En la página **Configurar servidor RADIUS de autenticación**, tiene dos opciones en la sección **Configuración de conexiones**.
3. Para comprobar la conexión del servidor RADIUS, haga clic en la ficha **Probar RADIUS Accesibilidad**.
4. Para ver el estado de autenticación RADIUS de extremo a extremo, haga clic en el vínculo **Probar conexión de usuario final**.

Autenticación RADIUS mediante TCP o TLS

August 11, 2022

A partir de las versiones 13.1 a 27.59, la autenticación RADIUS también se admite en los protocolos TCP y TLS.

> **Nota:**
>
> La opción **Probar alcance RADIUS** no es compatible con RADIUS en los tipos de transporte TCP y TLS.

Configurar RADIUS sobre TCP mediante la CLI

En el símbolo del sistema, escriba:

```
add authentication radiusAction <name> [-serverIP] [-serverPort ] [-
    transport <transport>]
<!--NeedCopy-->
```

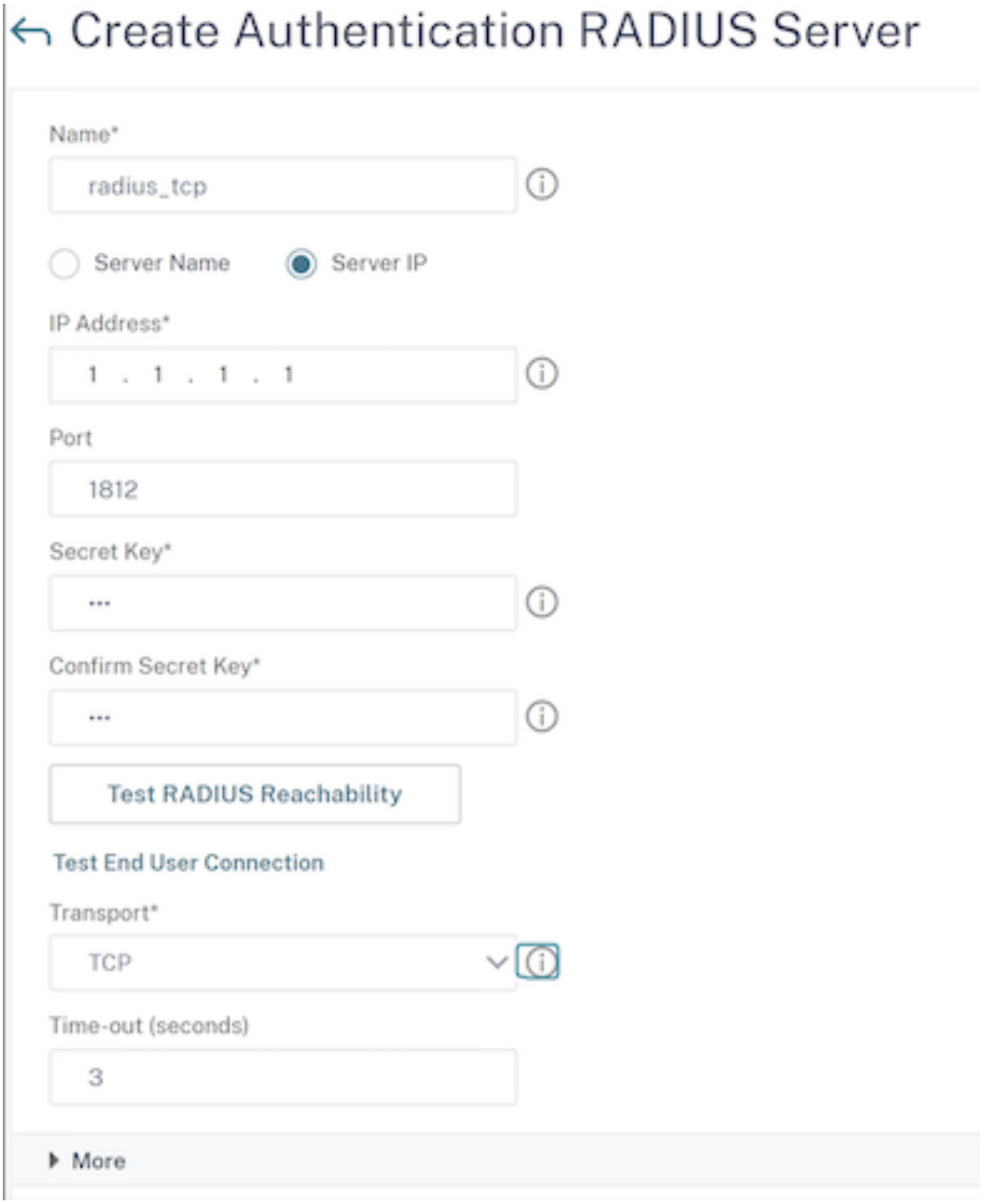
Ejemplo:

```
add authentication radiusAction RadAction -serverIP 1.1.1.1 -radkey 123
     -transport TCP
<!--NeedCopy-->
```

Configurar RADIUS a través de TCP mediante la GUI

1. Vaya a **Seguridad > AAA - Tráfico de aplicaciones > Directivas > Autenticación > Directivas avanzadas > Acciones > RADIUS**.
2. Seleccione un servidor existente o cree un servidor.

   Para obtener más información sobre la creación de un servidor, consulte Para configurar un servidor RADIUS mediante la GUI.



3. En **Transporte**, seleccione **TCP**.
4. Haga clic en **Crear**.

Configurar RADIUS sobre TLS mediante la CLI

En el símbolo del sistema, escriba:


```
add authentication radiusAction <name> [-serverIP] [-serverPort ] [-
    transport <transport>] [-targetLBVserver <string>]
<!--NeedCopy-->
```

Ejemplo

```
add authentication radiusAction RadAction -serverIP 1.1.1.1 -radkey 123
     -transport TLS -targetLBVserver rad-lb
<!--NeedCopy-->
```

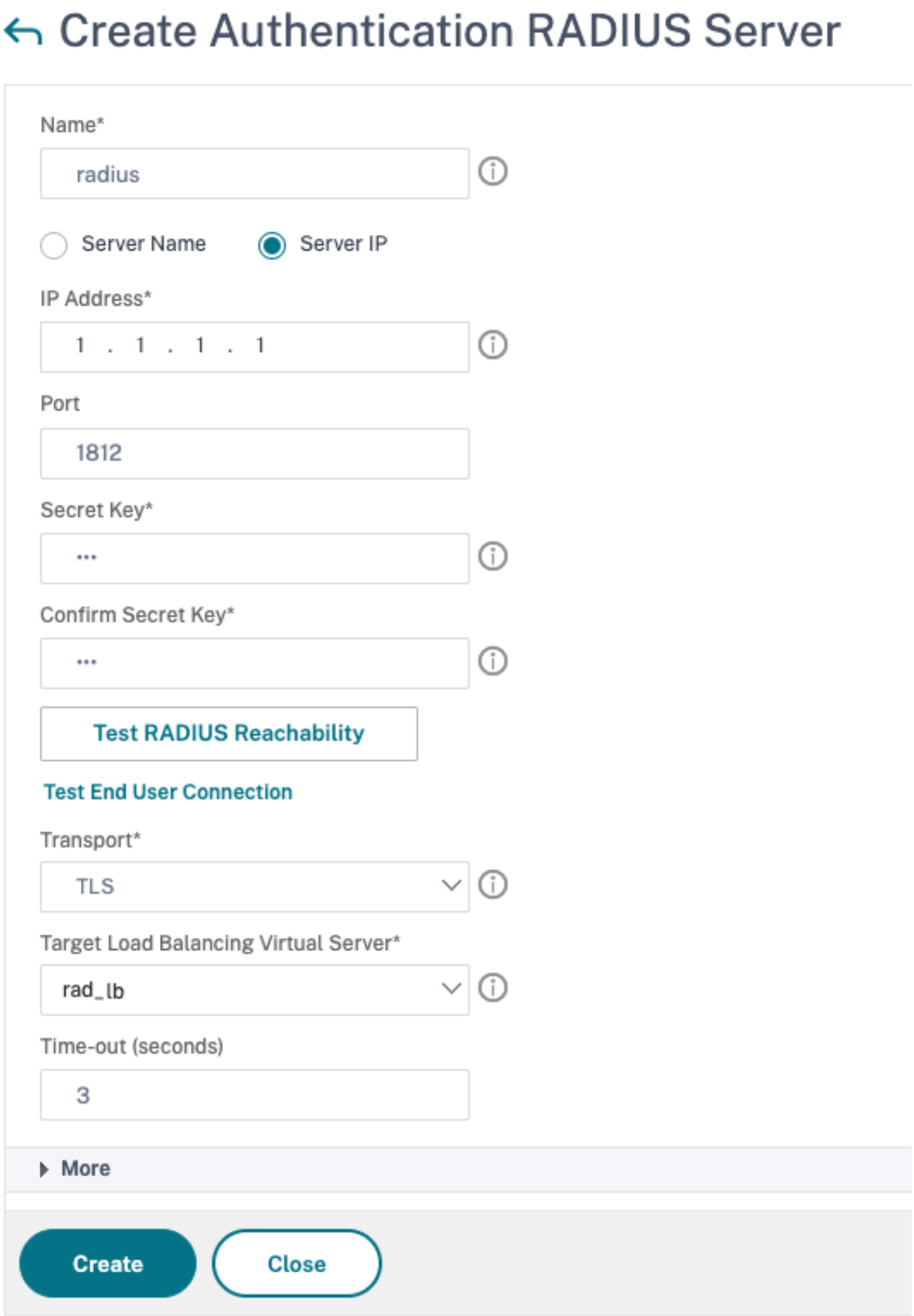
Nota:

- El nombre de servidor no se admite para el tipo de transporte TLS.
- Para el tipo de transporte TLS, configure un servidor virtual de equilibrio de carga de destino de tipo TCP y vincule un servicio de tipo SSL_TCP a este servidor virtual.
- La dirección IP y el número de puerto configurados para la acción RADIUS deben coincidir con la dirección IP y el número de puerto del servidor virtual de equilibrio de carga de destino configurado.

Configurar RADIUS a través de TLS mediante la GUI

1. Vaya a **Seguridad > AAA - Tráfico de aplicaciones > Directivas > Autenticación > Directivas avanzadas > Acciones > Servidores**.
2. Seleccione un servidor existente o cree un servidor.

   Para obtener más información sobre la creación de un servidor, consulte Para configurar un servidor RADIUS mediante la GUI.



3. En **Transporte**, seleccione **TLS**.
4. En **Servidor virtual de equilibrio de carga de destino**, seleccione el servidor virtual. Para obtener más información sobre la creación de un servidor virtual de equilibrio de carga, consulte Crear un servidor virtual.

   > **Nota:**
   >
   > - El nombre de servidor no se admite para el tipo de transporte TLS.
   > - Para el tipo de transporte TLS, configure un servidor virtual de equilibrio de carga de destino de tipo TCP y vincule un servicio de tipo SSL_TCP a este servidor virtual.
   > - La dirección IP y el número de puerto configurados para la acción RADIUS deben coincidir con la dirección IP y el número de puerto del servidor virtual de equilibrio de carga de destino configurado.

5. Haga clic en **Crear.**

Autenticación TACACS

January 12, 2021

La directiva de autenticación TACACS se autentica en un servidor externo de autenticación del sistema de control de acceso del controlador de acceso de Terminal Access Controller (TACACS).
Una vez que un usuario se autentica en un servidor TACACS, Citrix ADC se conecta al mismo servidor TACACS para todas las autorizaciones posteriores. Cuando un servidor TACACS principal no está disponible, esta función evita cualquier retraso mientras el ADC espera a que el primer servidor TACACS agote el tiempo de espera. Sucede antes de volver a enviar la solicitud de autorización al segundo servidor TACACS.

> **Nota: El**
>
> servidor de autorización TACACS no admite comandos cuya longitud de cadena supera los 255 caracteres.
>
> **Solución alternativa:** Utilice la autorización local en lugar de un servidor de autorización TACACS.

Al autenticarse a través de un servidor TACACS, los registros de administración de tráfico de autenticación, autorización y auditoría solo ejecutan correctamente los comandos TACACS. Impide que los registros muestren comandos TACACS introducidos por los usuarios que no estaban autorizados para ejecutarlos.

A partir de NetScaler 12.0, compilación 57.x, el sistema de control de acceso del controlador de acceso de Terminal Access (TACACS) no bloquea el demonio de autenticación, autorización y auditoría

mientras envía la solicitud TACACS. Permitir la autenticación LDAP y RADIUS para continuar con la solicitud. La solicitud de autenticación TACACS se reanuda una vez que el servidor TACACS reconoce la solicitud TACACS.

> **Importante:**
>
> - Citrix recomienda no modificar ninguna configuración relacionada con TACACS cuando ejecuta un comando “clear ns config”.
> - La configuración relacionada con TACACS relacionada con las directivas avanzadas se borra y se vuelve a aplicar cuando el parámetro “RbaConfig” se establece en NO en el comando “clear ns config” para la directiva avanzada.

Compatibilidad con atributos nombre-valor para la autenticación TACACS

Ahora puede configurar atributos de autenticación TACACS con un nombre único junto con valores. Los nombres se configuran en el parámetro de acción TACACS y los valores se obtienen consultando los nombres. Al especificar el valor del atributo name, los administradores pueden buscar fácilmente el valor del atributo asociado con el nombre del atributo. Además, los administradores ya no tienen que recordar el atributo solo por su valor.

> **Importante**
>
> - En el comando TacacsAction, puede configurar un máximo de 64 atributos separados por coma con un tamaño total inferior a 2048 bytes.

Para configurar los atributos nombre-valor mediante la CLI

En el símbolo del sistema, escriba:

```
1 add authentication tacacsAction <name> [-Attributes <string>]
2 <!--NeedCopy-->
```

Ejemplo:

```
1 add authentication tacacsAction tacacsAct1 -attributes  “mail,sn,
     userprincipalName”
2 <!--NeedCopy-->
```


Para agregar una acción de autenticación mediante la interfaz de línea de comandos

Si no utiliza la autenticación LOCAL, debe agregar una acción de autenticación explícita. En el símbolo del sistema, escriba el siguiente comando:

```
1 add authentication tacacsAction <name> -serverip <IP> [-serverPort <
     port>][-authTimeout <positive_integer>][ ... ]
2 <!--NeedCopy-->
```

Ejemplo

```
1 add authentication tacacsaction Authn-Act-1 -serverip 10.218.24.65 -
     serverport 1812                  -authtimeout 15 -tacacsSecret ”
     minotaur” -authorization OFF -accounting ON -auditFailedCmds OFF -
     defaultAuthenticationGroup ”users”
2 <!--NeedCopy-->
```

Para configurar una acción de autenticación mediante la interfaz de línea de comandos

Para configurar una acción de autenticación existente, en el símbolo del sistema, escriba el siguiente comando:

```
1 set authentication tacacsAction <name> -serverip <IP> [-serverPort <
     port>][-authTimeout <positive_integer>][ ... ]
2 <!--NeedCopy-->
```

Ejemplo

```
1     > set authentication tacacsaction Authn-Act-1 -serverip
        10.218.24.65 -serverport 1812                  -authtimeout 15
        -tacacsSecret ”minotaur” -authorization OFF -accounting ON -
        auditFailedCmds OFF -defaultAuthenticationGroup ”users”    Done
2 <!--NeedCopy-->
```

Para quitar una acción de autenticación mediante la interfaz de línea de comandos

Para quitar una acción RADIUS existente, en la solicitud de comando, escriba el siguiente comando:


```
rm authentication radiusAction <name>
<!--NeedCopy-->
```

Ejemplo

```
rm authentication tacacsaction Authn-Act-1
<!--NeedCopy-->
```

Autenticación de certificados de cliente

May 8, 2022

Los sitios web que contienen contenido confidencial, como los sitios web de banca en línea o los sitios web con información personal de los empleados, a veces requieren certificados de cliente para la autenticación. Para configurar la autenticación, la autorización y la auditoría para autenticar a los usuarios en función de los atributos del certificado del lado del cliente, primero debe habilitar la autenticación del cliente en el servidor virtual de administración de tráfico y vincular el certificado raíz al servidor virtual de autenticación. A continuación, implementa una de las dos opciones. Puede configurar el tipo de autenticación predeterminado en el servidor virtual de autenticación como CERT o puede crear una acción de certificado que defina lo que debe hacer Citrix ADC para autenticar a los usuarios en función de un certificado de cliente. En cualquier caso, el servidor de autenticación debe admitir CRL. Configure el ADC para extraer el nombre de usuario del campo **subjectCN** u otro campo especificado en el certificado de cliente.

Cuando el usuario intenta iniciar sesión en un servidor virtual de autenticación para el que no se ha configurado una directiva de autenticación y no se ha configurado una cascada global, la información del nombre de usuario se extrae del campo especificado del certificado. Si se extrae el campo obligatorio, la autenticación se realiza correctamente. Si el usuario no proporciona un certificado válido durante el protocolo de enlace SSL o si se produce un error en la extracción del nombre de usuario, se produce un error de autenticación. Después de validar el certificado de cliente, el ADC presenta una página de inicio de sesión al usuario.

Los siguientes procedimientos suponen que ya ha creado una configuración de autenticación, autorización y auditoría en funcionamiento y, por lo tanto, solo explican cómo habilitar la autenticación mediante certificados de cliente. Estos procedimientos también suponen que ha obtenido el certificado raíz y los certificados de cliente y los ha colocado en el ADC del directorio /nsconfig/ssl.

Configurar la autenticación con certificados del cliente

Para configurar los parámetros del certificado de cliente de autenticación, autorización y auditoría mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos, en el orden que se muestra, para configurar el certificado y verificar la configuración:

```
add ssl certKey <certkeyName> -cert <certFile> -key <keyFile> -password
    -inform <inform> -expiryMonitor <expiryMonitor> -notificationPeriod
    <notificationPeriod>

bind ssl certKey [<certkeyName>] [-ocspResponder <string>] [-priority <
   positive_integer>]

show ssl certKey [<certkeyName>]

set aaa parameter -defaultAuthType CERT

show aaa parameter

set aaa certParams -userNameField "Subject:CN"

show aaa certParams
<!--NeedCopy-->
```

Para configurar los parámetros del certificado de cliente de autenticación, autorización y auditoría mediante la utilidad de configuración

1. Vaya a **Seguridad > AAA - Tráfico de aplicaciones > Servidores virtuales.**
2. En el panel de detalles, seleccione el servidor virtual que desea configurar para gestionar la autenticación de certificados de cliente y, a continuación, haga clic en **Modificar.**
3. En la página **Configuración**, en **Certificados**, haga clic en la flecha hacia la derecha (>) para abrir el cuadro de diálogo de instalación de la clave de certificado de CA.
4. En el cuadro de diálogo **Clave de certificado de CA**, haga clic en **Insertar.**
5. En el cuadro de diálogo **Clave de certificado de CA - Certificados SSL**, haga clic en **Instalar.**
6. En el cuadro de diálogo **Instalar certificado**, defina los siguientes parámetros, cuyos nombres se correspondan con los nombres de los parámetros de la CLI, como se muestra:
   - Nombre del par de claves de certificado*: certKeyName
   - Nombre de archivo de certificado: certFile
   - Nombre de archivo de clave: keyFile

- Formato de certificado: inform
- Contraseña: password
- Paquete de certificados: bundle
- Notificar cuando caduque: expiryMonitor
- Período de notificación: notificationPeriod

7. Haga clic en **Instalar** y, después, en **Cerrar**.
8. En el cuadro de diálogo **Clave de certificado de CA**, en la lista **Certificado**, seleccione el certificado raíz.
9. Haga clic en **Guardar**.
10. Haga clic en **Atrás** para volver a la pantalla de configuración principal.
11. Vaya a **Seguridad > AAA - Tráfico de aplicaciones > Directivas > Autenticación > CERT**.
12. En el panel de detalles, seleccione la directiva que desea configurar para gestionar la autenticación de certificados de cliente y, a continuación, haga clic en **Modificar**.
13. En el cuadro de diálogo **Configurar directiva CERT de autenticación**, en la lista desplegable Servidor, seleccione el servidor virtual que configuró para gestionar la autenticación de certificados de cliente.
14. Haga clic en **Aceptar**. Aparece un mensaje en la barra de estado que indica que la configuración se ha completado correctamente.

Autenticación de certificados de cliente mediante

Los siguientes son los pasos para configurar la autenticación de certificados de cliente en Citrix ADC mediante directivas avanzadas.

1. Vaya a **Seguridad > AAA - Tráfico de aplicaciones > Servidores virtuales**.
2. En el panel de detalles, seleccione el servidor virtual que desea configurar para gestionar la autenticación de certificados de cliente y haga clic en **Modificar**.

   > **Nota:**
   >
   > Si ha importado un certificado de CA y un certificado de servidor válidos para el servidor virtual, puede pasar del **paso 3 al paso 10**.

3. En la página **Configuración**, en **Certificados**, haga clic en **>** para abrir el cuadro de diálogo de instalación **Clave de certificado de CA**.
4. En el cuadro de diálogo **Clave de certificado de CA**, haga clic en **Insertar**.
5. En el cuadro de diálogo **Clave de certificado de CA - Certificados SSL**, haga clic en **Instalar**.
6. En el cuadro de diálogo **Instalar certificado**, defina los siguientes parámetros, cuyos nombres se correspondan con los nombres de los parámetros de la CLI, como se muestra:

   - Nombre del par de claves de certificado: certkeyName

- Nombre de archivo de certificado: certFile
- Nombre de archivo de clave: keyFile
- Formato de certificado: inform
- Contraseña: password
- Paquete de certificados: bundle
- Notificar cuando caduque: expiryMonitor
- Período de notificación: notificationPeriod

7. Haga clic en **Instalar**y, a continuación, en Cerrar.
8. En el cuadro de diálogo **Clave de certificado de CA**, en la lista Certificado, seleccione el certificado raíz.
9. Haga clic en **Guardar**.
10. Haga clic en **Atrás** para volver a la pantalla de configuración principal.
11. Vaya a **Seguridad > AAA - Tráfico de aplicaciones > Directivas > Autenticación > Directivas avanzadas**y, a continuación, seleccione **Directiva**.
12. En el panel de detalles, realice una de las siguientes acciones:
    - Para crear una nueva directiva, haga clic en **Agregar**.
    - Para modificar una directiva existente, selecciónela y, a continuación, haga clic en **Modificar**.
13. En el cuadro de diálogo **Crear directiva** de **autenticación o Configurar directiva** de autenticación, escriba o seleccione valores para los parámetros.
    - Nombre: nombre de la directiva. No se puede cambiar para una directiva configurada previamente.
    - Tipo de acción: seleccionar certificado
    - Acción: acción de autenticación (perfil) que se va a asociar a la directiva. Puede elegir una acción de autenticación existente o hacer clic en el signo más y crear una nueva acción del tipo correcto.
    - Acción de registro: acción de auditoría que se va a asociar a la directiva. Puede elegir una acción de auditoría existente o hacer clic en el signo más y crear una nueva acción.
    - Expresión: Regla que selecciona las conexiones a las que quiere aplicar la acción especificada. La regla puede ser simple (“true” selecciona todo el tráfico) o compleja. Las expresiones se introducen seleccionando primero el tipo de expresión en la lista desplegable situada más a la izquierda debajo de la ventana Expresión y, a continuación, escribiendo la expresión directamente en el área de texto de la expresión o haciendo clic en Agregar para abrir el cuadro de diálogo Agregar expresión y mediante las listas desplegables que contiene para crear el expresión.)
    - Comentario: Puede escribir un comentario que describa el tipo de tráfico al que se aplica esta directiva de autenticación. Opcional.

14. Haga clic en **Crear** o **Aceptar**y, a continuación, en **Cerrar**. Si ha creado una directiva, esa directiva aparece en la página Directivas y servidores de autenticación.

Transferencia de certificados de cliente

El Citrix ADC ahora se puede configurar para pasar certificados de cliente a aplicaciones protegidas que requieren certificados de cliente para la autenticación de usuarios. El ADC primero autentica al usuario, luego inserta el certificado de cliente en la solicitud y lo envía a la aplicación. Esta función se configura mediante la adición de directivas de SSL adecuadas.

El comportamiento exacto de esta función cuando un usuario presenta un certificado de cliente depende de la configuración del servidor virtual VPN.

- Si el servidor virtual VPN está configurado para aceptar certificados de cliente pero no los necesita, el ADC inserta el certificado en la solicitud y, a continuación, reenvía la solicitud a la aplicación protegida.
- Si el servidor virtual VPN tiene inhabilitada la autenticación de certificados de cliente, el ADC renegocia el protocolo de autenticación y vuelve a autenticar al usuario antes de insertar el certificado de cliente en el encabezado y reenviar la solicitud a la aplicación protegida.
- Si el servidor virtual VPN está configurado para requerir la autenticación de certificados de cliente, el ADC utiliza el certificado de cliente para autenticar al usuario, luego inserta el certificado en el encabezado y reenvía la solicitud a la aplicación protegida.

En todos estos casos, se configura la transferencia de certificados de cliente de la siguiente manera.

Crear y configurar la transferencia de certificados de cliente mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los comandos siguientes:

```
add vpn vserver <name> SSL <IP> 443
<!--NeedCopy-->
```

En **nombre**, sustituya el servidor virtual por un nombre. El nombre debe contener entre uno y 127 caracteres ASCII, comenzando por una letra o un guión bajo (_), y que contenga solo letras, números y el guión bajo, hash (#), punto (.), espacio, dos puntos (:), arroba (@), igual (=) y guiones (-). Para <IP>, sustituya la dirección IP asignada al servidor virtual.

```
set ssl vserver <name> -clientAuth ENABLED -clientCert <clientcert>
<!--NeedCopy-->
```


Para <name>, sustituya el nombre del servidor virtual que creó. Para <clientCert>, sustituya uno de los valores siguientes:

- disabled: Inhabilita la autenticación de certificados de cliente en el servidor virtual VPN.
- mandatory: Configura el servidor virtual VPN para que requiera certificados de cliente para la autenticación.
- optional: Configura el servidor virtual VPN para permitir la autenticación de certificados de cliente, pero no para que la requiera.

```
1 bind vpn vserver <name> -policy local
2 <!--NeedCopy-->
```

Para <name>, sustituya el nombre del servidor virtual VPN que creó.

```
1 bind vpn vserver <name> -policy cert
2 <!--NeedCopy-->
```

Para <name>, sustituya el nombre del servidor virtual VPN que creó.

```
1 bind ssl vserver <name> -certkeyName <certkeyname>
2 <!--NeedCopy-->
```

Para <name>, sustituya el nombre del servidor virtual que creó. Para <certkeyName>, sustituya la clave de certificado de cliente.

```
1 bind ssl vserver <name> -certkeyName <cacertkeyname> -CA -ocspCheck
     Optional
2 <!--NeedCopy-->
```

Para <name>, sustituya el nombre del servidor virtual que creó. Para <cacertkeyName>, sustituya la clave de certificado de CA.

```
1 add ssl action <actname> -clientCert ENABLED -certHeader CLIENT-CERT
2 <!--NeedCopy-->
```

Para <actname>, sustituya la acción SSL por un nombre.


```
add ssl policy <polname> -rule true -action <actname>
<!--NeedCopy-->
```

Para <polname>, sustituya su nueva directiva de SSL por un nombre. Para <actname>, sustituya el nombre de la acción SSL que creó.

```
bind ssl vserver <name> -policyName <polname> -priority 10
<!--NeedCopy-->
```

Para <name>, sustituya el nombre del servidor virtual VPN.

Ejemplo

```
add vpn vserver vs-certpassthru SSL 10.121.250.75 443
set ssl vserver vs-certpassthru -clientAuth ENABLED -clientCert
   optional
bind vpn vserver vs-certpassthru -policy local
bind vpn vserver vs-certpassthru -policy cert
bind ssl vserver vs-certpassthru -certkeyName mycertKey
bind ssl vserver vs-certpassthru -certkeyName mycertKey -CA -ocspCheck
   Optional
add ssl action act-certpassthru -clientCert ENABLED -certHeader CLIENT-
   CERT
add ssl policy pol-certpassthru -rule true -action act-certpassthru
bind ssl vserver vs-certpassthru -policyName pol-certpassthru -priority
    10
<!--NeedCopy-->
```

Autenticación de negociación

August 20, 2021

Al igual que con otros tipos de directivas de autenticación, una directiva de autenticación de negociación se compone de una expresión y una acción. Después de crear una directiva de autenticación, la vincula a un servidor virtual de autenticación y le asigna una prioridad. Al vincularlo, también se designa como directiva principal o secundaria.

Además de las funciones de autenticación estándar, el comando Negociar acción ahora puede extraer información del usuario de un archivo keytab en lugar de requerir que introduzca esa información manualmente. Si una ficha clave tiene más de un SPN, la autenticación, la autorización y la auditoría seleccionará el SPN correcto. Puede configurar esta función en la línea de comandos o mediante la utilidad de configuración.

> **Nota**
>
> Estas instrucciones suponen que ya está familiarizado con el protocolo LDAP y que ya ha configurado el servidor de autenticación LDAP elegido.

Para configurar la autenticación, la autorización y la auditoría para extraer información de usuario de un archivo keytab mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba el comando apropiado:

```
add authentication negotiateAction <name> {
 -domain <string> }
  {
 -domainUser <string> }
  {
 -domainUserPasswd  }
  [-defaultAuthenticationGroup <string>] [-keytab <string>] [-NTLMPath
     <string>]

set authentication negotiateAction <name> {
 -domain <string> }
  {
 -domainUser <string> }
  {
 -domainUserPasswd }
  [-defaultAuthenticationGroup <string>] [-keytab <string>] [-NTLMPath
     <string>]
<!--NeedCopy-->
```

Parameter description

- **name**: Nombre de la acción de negociación que se va a utilizar.
- **domain**: Nombre de dominio del principal de servicio que representa Citrix ADC.
- **DomainUser**: Nombre de usuario de la cuenta asignada con Citrix ADC principal. Esto se puede dar junto con el dominio y la contraseña cuando el archivo keytab no está disponible. Si se da

nombre de usuario junto con el archivo keytab, entonces se buscarán las credenciales de este usuario en ese archivo keytab. Longitud máxima: 127

- **DomainUserPassWD** - Contraseña de la cuenta asignada a la entidad de Citrix ADC.
- **DefaultAuthenticationGroup** - Este es el grupo predeterminado que se elige cuando la autenticación se realiza correctamente además de los grupos extraídos. Longitud máxima: 63
- **keytab**: Ruta al archivo keytab que se utiliza para descifrar tíquets kerberos presentados a Citrix ADC. Si keytab no está disponible, se puede especificar el dominio/nombre de usuario/contraseña en la configuración de la acción de negociación. Longitud máxima: 127
- **NTLMPath**: Ruta de acceso al sitio habilitado para la autenticación NTLM, incluido el FQDN del servidor. Esto se utiliza cuando los clientes se remontan a NTLM. Longitud máxima: 127

Para configurar la autenticación, la autorización y la auditoría para extraer información de usuario de un archivo keytab mediante la utilidad de configuración

> Nota
>
> En la utilidad de configuración, se utiliza el término servidor en lugar de acción, pero se refiere a la misma tarea.

1. Vaya a **Seguridad > AAA - Tráfico de aplicaciones > Autenticación > Directivas avanzadas > Acciones > NEGOCIAR acciones**.
2. En el panel de detalles, en la ficha **Servidores**, realice una de las acciones siguientes:
   - Si quiere crear una nueva acción **Negociar**, haga clic en **Agregar**.
   - Si quiere modificar una acción **Negociar** existente, en el panel de datos seleccione la acción y, a continuación, haga clic en **Modificar**.
3. Si va a crear una nueva acción **Negociar**, en el cuadro de texto **Nombre**, escriba un nombre para la nueva acción. El nombre puede tener entre uno y 127 caracteres de longitud y puede consistir en letras mayúsculas y minúsculas, números y los caracteres de guión (-) y guión bajo (_). Si está modificando una acción Negociar existente, omita este paso. El nombre es de solo lectura; no se puede cambiar.
4. En **Negociar**, si la casilla de verificación Usar archivo Keytab aún no está activada, márquela.
5. En el cuadro de texto Ruta del archivo Keytab, escriba la ruta de acceso completa y el nombre de archivo del archivo keytab que quiere utilizar.
6. En el cuadro de texto Grupo de autenticación predeterminado, escriba el grupo de autenticación que quiere establecer como predeterminado para este usuario.
7. Haga clic en **Crear** o en **Aceptar** para guardar los cambios.

Puntos a tener en cuenta cuando se utilizan cifrados avanzados para la autenticación Kerberos

- **Ejemplo de configuración cuando se utiliza keytab:** agregar autenticación NegotiateAction neg_act_aes256 -keytab “/nsconfig/krb/lbvs_aes256.keytab”
- **Utilice el siguiente comando cuando keytab tenga varios tipos de cifrado.** El comando captura adicionalmente los parámetros de usuario del dominio: add authentication NegotiateAction neg_act_keytab_all -keytab “/nsconfig/krb/lbvs_all.keytab” -DomainUser “HTTP/LBVS.AAA.local”
- **Utilice los siguientes comandos cuando se utilicen credenciales de usuario:** add authentication NegotiateAction neg_act_user -domain AAA.LOCAL -DomainUser “HTTP/LBVS.AAA.local” -DomainUserPasswd <password>
- Asegúrese de que se proporciona la información correcta **del usuario del dominio**. Puede buscar el nombre de inicio de sesión del usuario en AD.

Autentificación web

October 5, 2021

La autenticación, autorización y auditoría ahora pueden autenticar a un usuario en un servidor web, proporcionando las credenciales que el servidor web requiere en una solicitud HTTP y analizando la respuesta del servidor web para determinar si la autenticación del usuario se ha realizado correctamente. Al igual que con otros tipos de directivas de autenticación, una directiva de autenticación web se compone de una expresión y una acción. Después de crear una directiva de autenticación, la enlaza a un servidor virtual de autenticación y le asigna una prioridad. Al vincularlo, también lo designa como directiva principal o secundaria.

Para configurar la autenticación basada en web con un servidor web específico, primero debe crear una acción de autenticación web. Dado que la autenticación en servidores web no utiliza un formato rígido, debe especificar exactamente qué información necesita el servidor web y en qué formato al crear la acción. Para ello, cree una expresión en la directiva avanzada del dispositivo Citrix ADC que contiene los siguientes elementos:

- **IP del servidor**: dirección IP del servidor web de autenticación.
- **Puerto del servidor**: puerto del servidor web de autenticación.
- **Regla de autenticación**: expresión de la directiva avanzada del dispositivo Citrix ADC que contiene las credenciales del usuario en el formato que espera el servidor web.
- **Esquema**: HTTP (para autenticación web sin cifrar) o HTTPS (para autenticación web cifrada).
- **Regla de éxito**: expresión de la directiva avanzada del dispositivo Citrix ADC que coincide con la cadena de respuesta del servidor web que indica que el usuario se ha autenticado correctamente.

Para todos los demás parámetros, siga las reglas normales del comando add authentication action.

A continuación, crea una directiva asociada a esa acción. La directiva es similar a una directiva LDAP y, al igual que las directivas LDAP, utiliza la sintaxis del dispositivo Citrix ADC.

> **Nota**
>
> En estas instrucciones se supone que ya está familiarizado con los requisitos de autenticación de los servidores web en los que quiere autenticarse y que ya ha configurado el servidor de autenticación web.

Para configurar una acción de autenticación web mediante la interfaz de línea de comandos

Para crear una acción de autenticación web en la línea de comandos, en la línea de comandos escriba el siguiente comando:

```
1 add authentication webAuthAction <name> -serverIP <ip_addr|ipv6_addr
    |\*> -serverPort <port|\*> [-fullReqExpr <string>] -scheme ( http |
    https ) -successRule <expression> [-defaultAuthenticationGroup <
    string>][-Attribute1 <string>][-Attribute2 <string>] [-Attribute3 <
    string>][-Attribute4 <string>] [-Attribute5 <string>][-Attribute6 <
    string>] [-Attribute7 <string>][-Attribute8 <string>] [-Attribute9 <
    string>][-Attribute10 <string>] [-Attribute11 <string>][-Attribute12
     <string>] [-Attribute13 <string>][-Attribute14 <string>] [-
    Attribute15 <string>][-Attribute16 <string>]
2 <!--NeedCopy-->
```

Ejemplo

```
1 add policy expression post_data ""username=" + http.REQ.BODY(1000).
    SET_TEXT_MODE(IGNORECASE).AFTER_STR("login=").BEFORE_STR("&") + "&
    passwort=" + http.REQ.BODY(1000).SET_TEXT_MODE(IGNORECASE).AFTER_STR
    ("passwd=")"
2
3 add policy expression length_post_data "("username= " + http.REQ.BODY
    (1000).SET_TEXT_MODE(IGNORECASE).AFTER_STR("login=").BEFORE_STR("&")
     + "passwort=" + http.REQ.BODY(1000).SET_TEXT_MODE(IGNORECASE).
    AFTER_STR("passwd=")).length"
4
5 add authentication webAuthAction webAuth_POST -serverIP 10.106.187.54 -
    serverPort 80 -fullReqExpr q{
6  "POST /MyPHP/auth.php HTTP/" + http.req.version.major + "." + http.req
     .version.major + "\r\nAccept:\*/\*\r\nHost: 10.106.187.54\r\
```



```
        nReferer: http://10.106.187.54/MyPHP/auth.php\r\nAccept-Language:
        en-US\r\nUser-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT
        6.1; Trident/5.0)\r\nContent-Type: application/x-www-form-
        urlencoded\r\n" + "Content-Length: " + length_post_data + "\r\
        nConnection: Keep-Alive\r\n\r\n" + post_data }
7     -scheme http -successRule "http.res.status.eq(200)"
8  <!--NeedCopy-->
```

Para configurar una acción de autenticación web mediante la utilidad de configuración

> **Nota**
>
> En la utilidad de configuración, se utiliza el término servidor en lugar de acción, pero se refiere a la misma tarea.

1. Vaya a **Seguridad > AAA - Tráfico de aplicaciones > Directivas > LDAP**.
2. En el panel de detalles, en la ficha **Servidores**, realice una de las siguientes acciones:
   - Si quiere crear una nueva acción de autenticación web, haga clic en **Agregar**.
   - Si quiere modificar una acción de autenticación web existente, en el panel de datos, seleccione la acción y, a continuación, haga clic en **Modificar**.
3. Si va a crear una nueva acción de autenticación web, en el cuadro de diálogo **Crear servidor web de autenticación**, en el cuadro de texto **Nombre**, escriba un nombre para la nueva acción de autenticación web. El nombre puede tener una longitud de entre uno y 127 caracteres y puede consistir en letras mayúsculas y minúsculas, números y guiones (-) y guiones bajos (_). Si va a modificar una acción de autenticación web existente, omita este paso. El nombre es de solo lectura; no se puede cambiar.
4. En el cuadro de texto **Dirección IP del servidor web**, escriba la dirección IP IPv4 o IPv6 del servidor web de autenticación. Si la dirección es una dirección IP IPv6, seleccione primero la casilla de verificación IPv6.
5. En el cuadro de texto Puerto, escriba el número de puerto en el que el servidor web acepta conexiones.
6. Seleccione **HTTP** o **HTTPS** en la lista desplegable **Protocolo** .
7. En el área de texto Expresión de solicitud HTTP, escriba una expresión regular con formato PCRE que cree la solicitud del servidor web que contiene las credenciales del usuario en el formato exacto que espera el servidor web de autenticación.
8. En el área de texto Expresión para validar la autenticación, escriba una expresión de directiva avanzada del dispositivo Citrix ADC que describa la información de la respuesta del servidor web que indica que la autenticación del usuario se ha realizado correctamente.

9. Rellene los campos restantes tal y como se describe en la documentación general de la acción de autenticación.
10. Haga clic en **OK**.

Autenticación OTP por SMS mediante autenticación web

June 2, 2022

Citrix ADC ahora se puede integrar con un proveedor de SMS de terceros para proporcionar una capa adicional de autenticación.

El dispositivo Citrix ADC se puede configurar para enviar un OTP en el móvil del usuario como segundo factor de autenticación. El dispositivo presenta al usuario un formulario de inicio de sesión para introducir al OTP después de iniciar sesión correctamente en AD. Solo después de la validación correcta de la autenticación OTP por SMS se presenta al usuario el recurso solicitado.

Para lograr la autenticación OTP por SMS, el dispositivo Citrix ADC se basa en los siguientes factores en el back-end.

1. Autentique al usuario mediante la autenticación LDAP y extraiga el número de teléfono móvil del usuario.
2. Cree OTP y almacénelo en la variable NS. Configuración y uso de variables.
3. Envíe la OTP mediante el método de autenticación WebAuth al número de teléfono móvil extraído de LDAP.
4. Valide la OTP.

Requisitos previos

Configurar el almacén de OTP

Los administradores configuran una base de datos o un almacén para guardar las OTP utilizadas para la autenticación por SMS mediante el siguiente comando de la CLI.

```
1 add ns variable otp_store -type ”map(text(65),text(6),100000)” -
     ifValueTooBig undef -ifNoValue undef -expires 5
2 <!--NeedCopy-->
```


Generar OTP aleatoria por sesión de usuario

Utilice el siguiente comando para generar una OTP aleatoria de 6 dígitos por sesión de usuario y guárdela en el almacén de OTP.

```
1 add ns assignment generate_otp -variable ”$otp_store[AAA.USER.SESSIONID
     ]” -set (”000000” + SYS.RANDOM.MUL(1000000).
     TYPECAST_UNSIGNED_LONG_AT.TYPECAST_TEXT_T).SUFFIX(6)
2 <!--NeedCopy-->
```

Configurar la autenticación OTP por SMS con Citrix ADC

- Antes de configurar la función de autenticación de dos factores de SMS, debe tener configurada una autenticación LDAP en un dispositivo Citrix ADC como primer factor con la autenticación habilitada. Para obtener instrucciones para configurar la autenticación LDAP, consulte Para configurar la autenticación LDAP mediante la utilidad de configuración.
- Configure LDAP y extraiga el número de teléfono móvil que se utilizará para la autenticación OTP por SMS.

Configuración de primer factor de ejemplo

```
1 add authentication ldapAction ldap_action -serverIP 1.1.1.1 -serverPort
      3268 -authTimeout 30 -ldapBase ”dc=nsi-test,dc=com” -ldapBindDn
     Administrator@nsi-test.com -ldapBindDnPassword freebsd -
     ldapLoginName samaccountname -groupAttrName memberOf -
     ssoNameAttribute samaccountname  -Attribute1 mobile -email mail
2
3 add authentication Policy ldap_policy -rule true -action ldap_action
4 <!--NeedCopy-->
```

> **Nota**
>
> El número de móvil se puede extraer con AAA.USER.ATTRIBUTE(1) y se puede incluir al enviarlo al servidor back-end.

Configuración de segundo factor de muestra

Con la siguiente configuración de ejemplo, se genera una OTP que se va a enviar al usuario final.


```
add authentication Policy set_otp -rule true -action generate_otp

add authentication policylabel set_otp -loginSchema LSCHEMA_INT

add authentication policy cascade_noauth -rule true -action NO_AUTHN

bind authentication policylabel set_otp -policyName set_otp -priority 1
    -gotoPriorityExpression NEXT
<!--NeedCopy-->
```

Ejemplo de configuración del tercer factor

Con la siguiente configuración de ejemplo, la OTP generada en la configuración del segundo factor se envía al usuario final mediante el método de autenticación web. Para obtener información sobre la autenticación web, consulte Autenticación web.

- Ejemplo de configuración de autenticación web cuando el servidor SMS expone la API mediante el método GET.

```
add policy expression otp_exp_get ""method=sendMessage&send_to="
    + AAA.USER.ATTRIBUTE(1) + "&msg=OTP is " + $otp_store[AAA.USER
    .SESSIONID] + "for login into secure access  gateway. Valid
    till EXPIRE_TIME. Do not share the OTP with anyone for
    security reasons.&userid=######&password=###=1.0""

add authentication webAuthAction webAuth_Get -serverIP
    10.106.168.210 -serverPort 8080 -fullReqExpr q{
"GET /GatewayAPI/rest?" + otp_exp_get + "HTTP/" + http.req.
    version.major + "." + http.req.version.minor.sub(1) + "\r\
    nAccept:\*/\*\r\nHost: <FQDN>\r\n" }
 -successRule "http.res.status.eq(200)" -scheme http
<!--NeedCopy-->
```

- Ejemplo de configuración de autenticación web cuando el servidor SMS expone la API mediante el método GET.

```
add policy expression otp_exp_post ""Message: OTP is " +
    $otp_store[AAA.USER.SESSIONID] + "for login into secure access
      gateway. Valid till EXPIRE_TIME. Do not share the OTP with
    anyone for security reasons&Mobile:" + AAA.USER.ATTRIBUTE(1)"
```



```
2
3  add authentication webAuthAction webAuth_POST -serverIP
      10.106.168.210 -serverPort 8080 -fullReqExpr q{
4  "POST /MyPHP/auth.php HTTP/" + http.req.version.major + "." +
      http.req.version.major + "\r\nAccept:\*/\*\r\nHost:
      10.106.168.210 \r\nContent-Length: 10\r\n\r\n" + otp_exp_post
      }
5   -scheme http -successRule true
6  <!--NeedCopy-->
```

```
1  add authentication webAuthAction webAuth_Get -serverIP
      10.106.168.210 -serverPort 8080 -fullReqExpr q{
2  "GET /GatewayAPI/rest?" + otp_exp_get + "HTTP/" + http.req.
      version.major + "." + http.req.version.minor.sub(1) + "\r\
      nAccept:/\r\nHost: <FQDN>\r\n" }
3   -successRule "http.res.status.eq(200)" -scheme http
4
5  add policy expression otp_exp_post "$otp_store[AAA.USER.SESSIONID
      ]"
6  <!--NeedCopy-->
```

- Por último, envíe la OTP.

```
1  add authentication Policy wpp -rule true -action webAuth_POST
2
3  add authentication policylabel send_otp -loginSchema LSCHEMA_INT
4  bind authentication policylabel send_otp -policyName wpp -
      priority 1 -gotoPriorityExpression NEXT
5  <!--NeedCopy-->
```

Ejemplo de configuración del cuarto factor

Con la siguiente configuración de ejemplo, valide la OTP enviada al usuario final.

En esta configuración, se utiliza una regla de directiva para validar la OTP con la que se envía al usuario final.

```
1  add authentication Policy otp_verify -rule "AAA.LOGIN.PASSWORD.EQ(
      $otp_store[AAA.USER.SESSIONID])" -action NO_AUTHN
```



```
2
3 add authentication policylabel otp_verify -loginSchema onlyPassword
4
5 bind authentication policylabel otp_verify -policyName otp_verify -
    priority 1 -gotoPriorityExpression NEXT
6
7 <!--NeedCopy-->
```

Utilice el siguiente comando para agregar el esquema de inicio de sesión OnlyPassword:

```
1 add authentication loginSchema onlypassword -authenticationschema /
    nsconfig/loginschema/LoginSchema/OnlyPassword.xml”
2 <!--NeedCopy-->
```

Vincule todos los factores para una autenticación OTP por SMS correcta

Utilice los siguientes comandos de la CLI para vincular todos los factores.

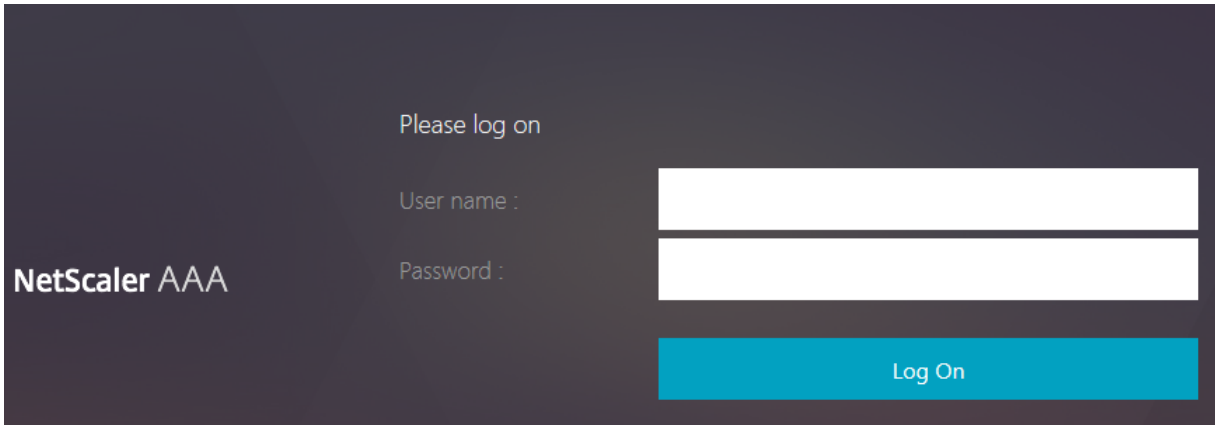
```
1 bind authentication policylabel send_otp -policyName wpp -priority 1 -
    gotoPriorityExpression NEXT -nextFactor otp_verify
2 <!--NeedCopy-->
```

> **Nota:**
>
> La directiva de autenticación en cascada se agrega para permitir una autenticación fiable y continua para los usuarios finales. Si el factor actual falla, se evalúa el siguiente factor de manera que no haya impacto en la experiencia del usuario.

Autentificación basada en formularios

August 20, 2021

Con la autenticación basada en formularios, se presenta un formulario de inicio de sesión al usuario final. Este tipo de formulario de autenticación admite la autenticación multifactor (nFactor) y la autenticación clásica.



Asegúrese de lo siguiente para que funcione la autenticación basada en formularios:

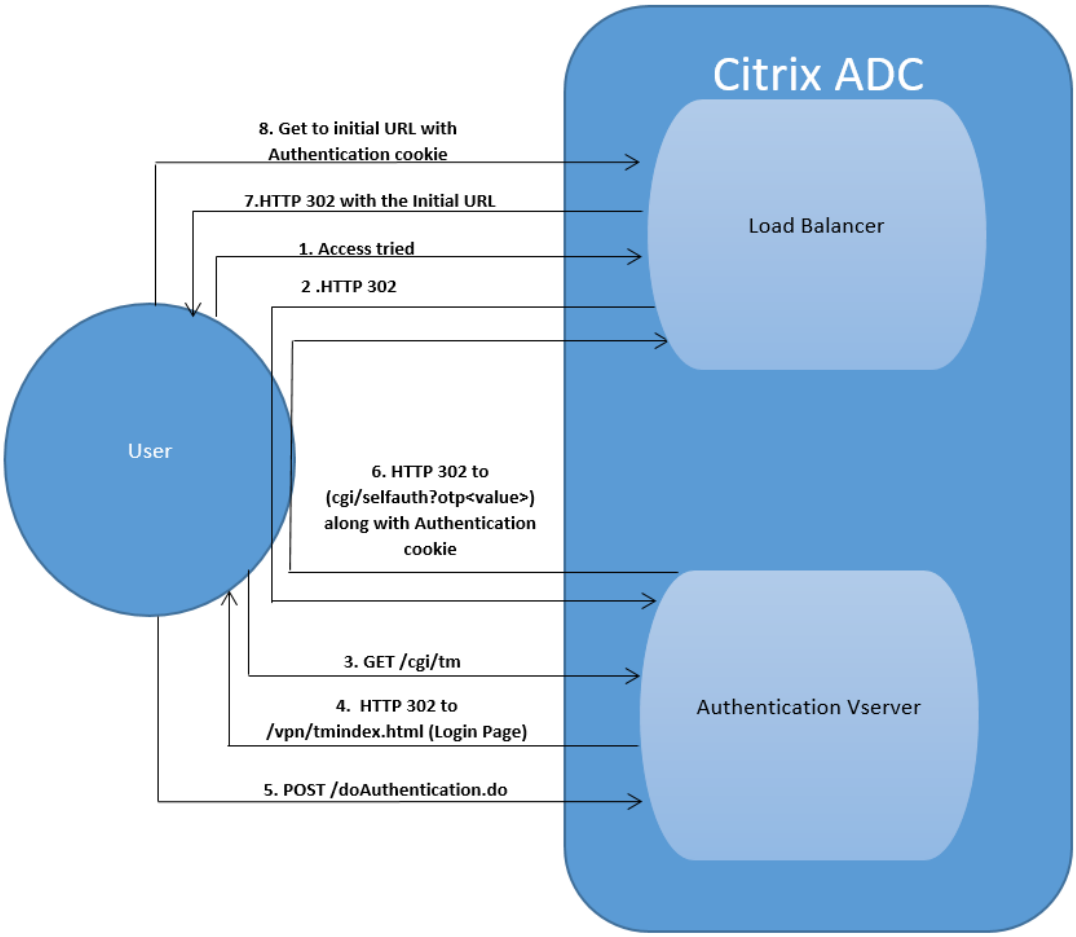
- El servidor virtual de equilibrio de carga debe tener **activada** la autenticación.
- Se debe especificar el parámetro 'AuthenticationHost' al que se debe redirigir el usuario para la autenticación. El comando para configurar el mismo es el siguiente:

```
1  set lb vs lb1 -authentication on  - authenticationhost aaavs-ip/
      fqdn
```

- La autenticación basada en formularios es compatible con el explorador que admite HTML

Los siguientes pasos describen cómo funciona la autenticación basada en formularios:

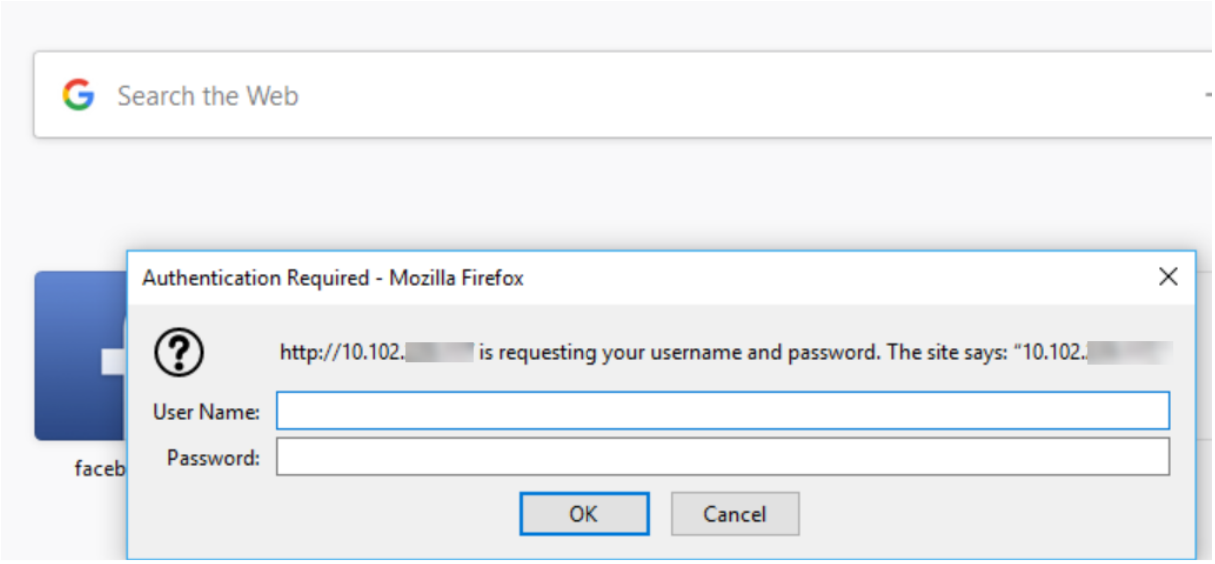
1. El cliente (explorador) envía una solicitud GET para una URL en el servidor virtual TM (equilibrio de carga/CS).
2. El servidor virtual TM determina que el cliente no se ha autenticado y envía una respuesta HTTP 302 al cliente. La respuesta contiene un script oculta que hace que el cliente emita una solicitud GET para /cgi/tm al servidor virtual de autenticación.
3. El cliente envía GET /cgi/tm que contiene la URL de destino al servidor virtual de autenticación.
4. El servidor virtual de autenticación envía una redirección a la página de inicio de sesión.
5. El usuario envía sus credenciales al servidor virtual de autenticación con un POST /doAuthentication.do. La autenticación la realiza el servidor virtual de autenticación.
6. Si las credenciales son correctas, el servidor virtual de autenticación envía una respuesta HTTP 302 a la URL cgi/selfauth en el servidor de equilibrio de carga con un token de una sola vez (OTP).
7. El servidor de equilibrio de carga envía HTTP 302 al cliente.
8. El cliente envía una solicitud GET para su URL de destino inicial junto con una cookie de 32 bytes.



Autentificación basada en 401

May 8, 2022

Con la autenticación basada en 401, el dispositivo Citrix ADC presenta un cuadro de diálogo emergente al usuario final.



El AAA-TM basado en formularios funciona en los mensajes de redireccionamiento. Algunas aplicaciones no admiten redireccionamientos, en tales casos se utiliza la autenticación 401 AAA-TM habilitada.

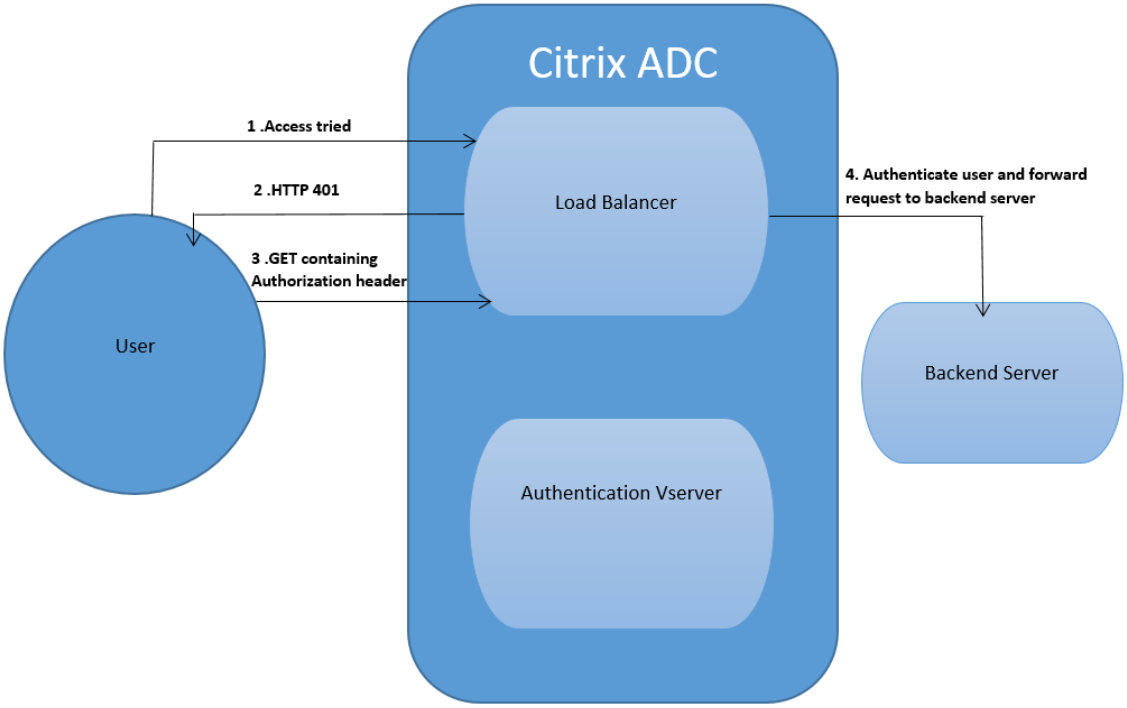
Habilite los siguientes parámetros para que funcione 401 Authentication AAA-TM.

- El valor del parámetro "authnVsName" para el servidor virtual de equilibrio de carga debe ser el nombre del servidor virtual de autenticación que se utilizará para autenticar a los usuarios.
- El parámetro "authn401" debe estar habilitado. El comando para configurar el mismo es el siguiente:

```
1  set lb vs lb1 -authn401 on -authnvsName <aaavs-name>
```

Los siguientes pasos describen cómo funciona la autenticación 401:

1. El usuario intenta acceder a una URL concreta mediante el servidor virtual de equilibrio de carga.
2. El servidor virtual de equilibrio de carga envía una respuesta HTTP 401 al usuario que indica que se requiere autenticación para el acceso.
3. El usuario envía sus credenciales al servidor virtual de equilibrio de carga en el encabezado de autorización.
4. El servidor virtual de equilibrio de carga autentica al usuario y, a continuación, lo conecta a los servidores back-end.



> **Importante:**
>
> Para un servidor virtual de equilibrio de carga con autenticación 401 activada, se pueden crear varias sesiones de autenticación y autorización para el mismo usuario en poco tiempo. Esta configuración puede provocar un pico en la memoria. Puede aplicar la siguiente configuración en el dispositivo Citrix ADC para depurar e identificar la aplicación del cliente final.

```
1 set syslogparams -userDefinedAuditlog yes
2
3 add audit messageaction 401_log_act InFORMATIONAL '"LB-401 accessed:
     User: <" + AAA.USER.NAME + "> SessionID <"+ AAA.USER.SESSIONID + ">
     Client :<" + CLIENT.IP.SRC + "> accessed URL: <" + HTTP.REQ.URL +
     ">"'
4
5 add rewritepolicy rewrite_401_log true NOREWRITE -logAction 401_log_act
6
7 bind lb vserver <lb_name> -policyName rewrite_401_log -priority 100 -
     type reqUEST
8 <!--NeedCopy-->
```


Configuración re-Captcha para autenticación nFactor

June 2, 2022

Citrix Gateway admite una nueva acción de primera clase `captchaAction` que simplifica la configuración de Re-Captcha. Como re-Captcha es una acción de primera clase, puede ser un factor en sí mismo. Puede inyectar re-Captcha en cualquier parte del flujo de nFactor.

Anteriormente, tenías que escribir directivas WebAuth personalizadas con cambios en la RfWebUI también. Con la introducción de `captchaAction`, no tiene que modificar el JavaScript.

> **Importante:**
>
> Si se usa re-Captcha junto con los campos de nombre de usuario o contraseña en el esquema, el botón **Enviar** se inhabilita hasta que se cumpla con re-Captcha.

Configuración de re-Captcha

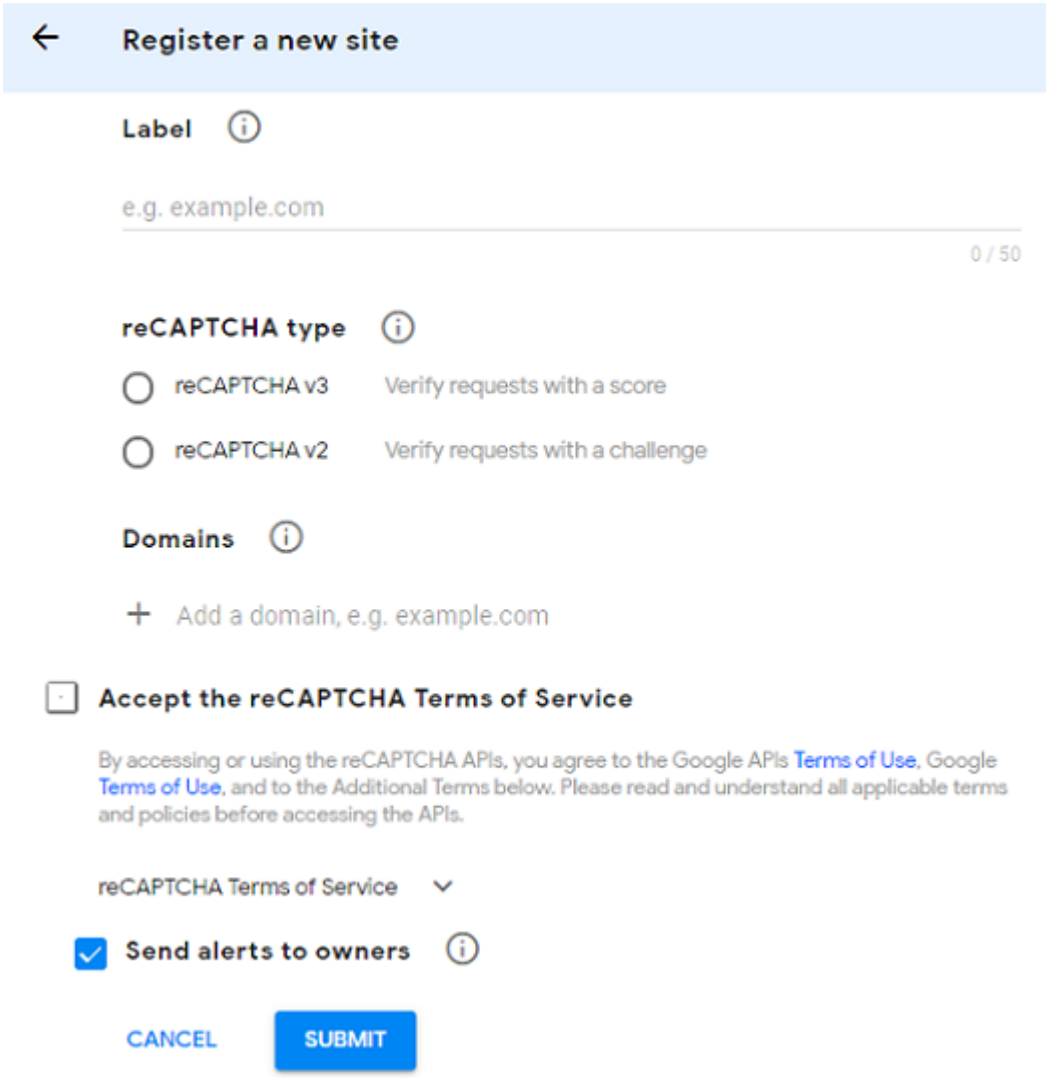
La configuración de re-Captcha consta de dos partes.

1. Configuración en Google para registrar re-Captcha.
2. Configuración en el dispositivo Citrix ADC para usar re-Captcha como parte del flujo de inicio de sesión.

Configuración de re-Captcha en Google

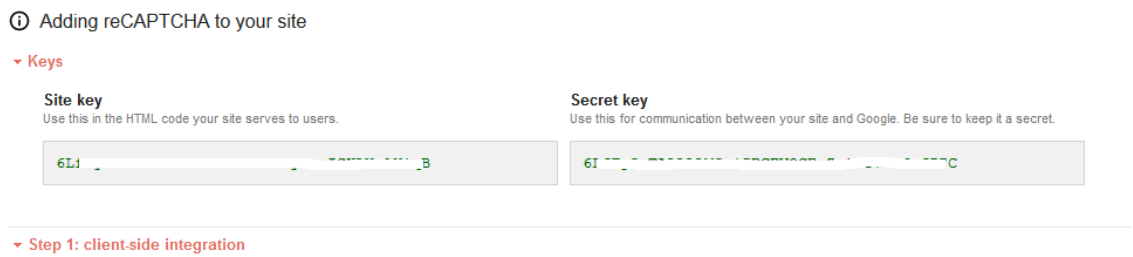
Registre un dominio para re-Captcha en https://www.google.com/recaptcha/admin#llist.

1. Al navegar a esta página, aparece la siguiente pantalla.



> **Nota**
>
> Utilice solo reCaptcha v2. Re-Captcha invisible aún está en Tech Preview.

2. Después de registrar un dominio, se muestran “SiteKey” y “SecretKey”.



> **Nota**
>
> Las teclas “SiteKey” y “SecretKey” aparecen atenuadas por motivos de seguridad. “Se-

> cretKey" debe mantenerse a salvo.

Configuración de re-Captcha en un dispositivo Citrix ADC

La configuración de re-Captcha en el dispositivo Citrix ADC se puede dividir en tres partes:

- Mostrar pantalla de re-Captcha
- Publicar la respuesta de re-Captcha en el servidor de Google
- La configuración LDAP es el segundo factor para el inicio de sesión del usuario (opcional)

Mostrar pantalla de re-Captcha

La personalización del formulario de inicio de sesión se realiza mediante el esquema de inicio de sesión SingleAuthCaptcha.xml. Esta personalización se especifica en el servidor virtual de autenticación y se envía a la interfaz de usuario para representar el formulario de inicio de sesión. El esquema de inicio de sesión integrado, SingleAuthCaptcha.xml, se encuentra en el directorio `/nsconfig/loginSchema/LoginSchema` del dispositivo Citrix ADC.

> **Importante**
>
> - El esquema de inicio de sesión de SingleAuthCaptcha.xml se puede usar cuando se configura LDAP como primer factor.
> - En función de su caso de uso y de los diferentes esquemas, puede modificar el esquema existente. Por ejemplo, si solo necesita el factor re-Captcha (sin nombre de usuario ni contraseña) o autenticación dual con re-Captcha.
> - Si se realizan modificaciones personalizadas o se cambia el nombre del archivo, Citrix recomienda copiar todos los loginSchemas del directorio `/nsconfig/loginschema/LoginSchema` al directorio principal, `/nsconfig/loginschema`.

Para configurar la visualización de re-Captcha mediante CLI

```
add authentication loginSchema singleauthcaptcha -authenticationSchema
    /nsconfig/loginschema/SingleAuthCaptcha.xml

add authentication loginSchemaPolicy singleauthcaptcha -rule true -
    action singleauthcaptcha

add authentication vserver auth SSL <IP> <Port>

add ssl certkey vserver-cert -cert <path-to-cert-file> -key <path-to-
    key-file>
```



```
8
9  bind ssl vserver auth -certkey vserver-cert
10
11 bind authentication vserver auth -policy singleauthcaptcha -priority 5
       -gotoPriorityExpression END
12 <!--NeedCopy-->
```

Publicar la respuesta de re-Captcha en el servidor de Google

Después de configurar el re-Captcha que debe mostrarse a los usuarios, los administradores agregan la configuración al servidor de Google para verificar la respuesta de re-Captcha del explorador.

Para verificar la respuesta de re-Captcha desde el explorador

```
1 add authentication captchaAction myrecaptcha -sitekey <sitekey-copied-
      from-google> -secretkey <secretkey-from-google>
2
3 add authentication policy myrecaptcha -rule true -action myrecaptcha
4
5 bind authentication vserver auth -policy myrecaptcha -priority 1
6 <!--NeedCopy-->
```

Los siguientes comandos son necesarios para configurar si se quiere la autenticación de AD. De lo contrario, puede ignorar este paso.

```
1 add authentication ldapAction ldap-new -serverIP x.x.x.x -serverPort
      636 -ldapBase "cn=users,dc=aaatm,dc=com" -ldapBindDn adminuser@aaatm
      .com -ldapBindDnPassword <password> -encrypted -encryptmethod
      ENCMTHD_3 -ldapLoginName sAMAccountName -groupAttrName memberof -
      subAttributeName CN -secType SSL -passwdChange ENABLED -
      defaultAuthenticationGroup ldapGroup
2
3 add authenticationpolicy ldap-new -rule true -action ldap-new
4 <!--NeedCopy-->
```

La configuración LDAP es el segundo factor para el inicio de sesión del usuario (opcional)

La autenticación LDAP ocurre después de volver a captcha, la agrega al segundo factor.


```
add authentication policylabel second-factor

bind authentication policylabel second-factor -policy ldap-new -
    priority 10

bind authentication vserver auth -policy myrecaptcha -priority 1 -
    nextFactor second-factor
<!--NeedCopy-->
```

El administrador debe agregar los servidores virtuales adecuados en función de si se utiliza el servidor virtual de equilibrio de carga o el dispositivo Citrix Gateway para el acceso. El administrador debe configurar el siguiente comando si se necesita un servidor virtual de equilibrio de carga:

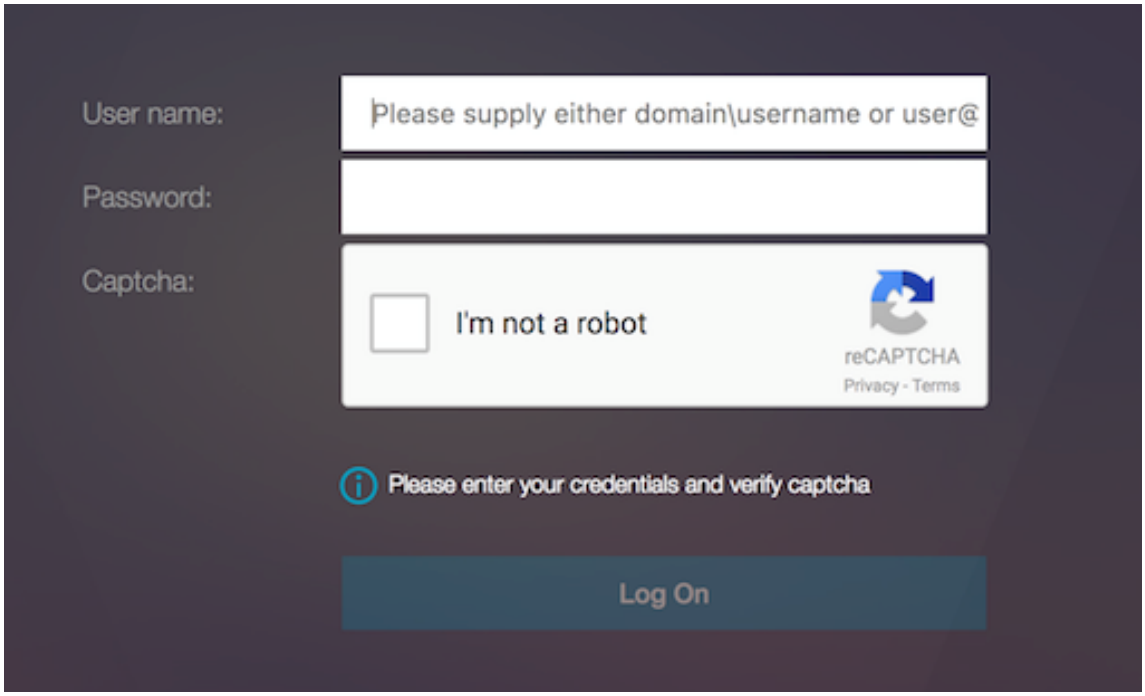
```
add lb vserver lbtest HTTP <IP> <Port> -authentication ON -
    authenticationHost nssp.aaatm.com
<!--NeedCopy-->
```

nssp.aaatm.com: Se resuelve en un servidor virtual de autenticación.

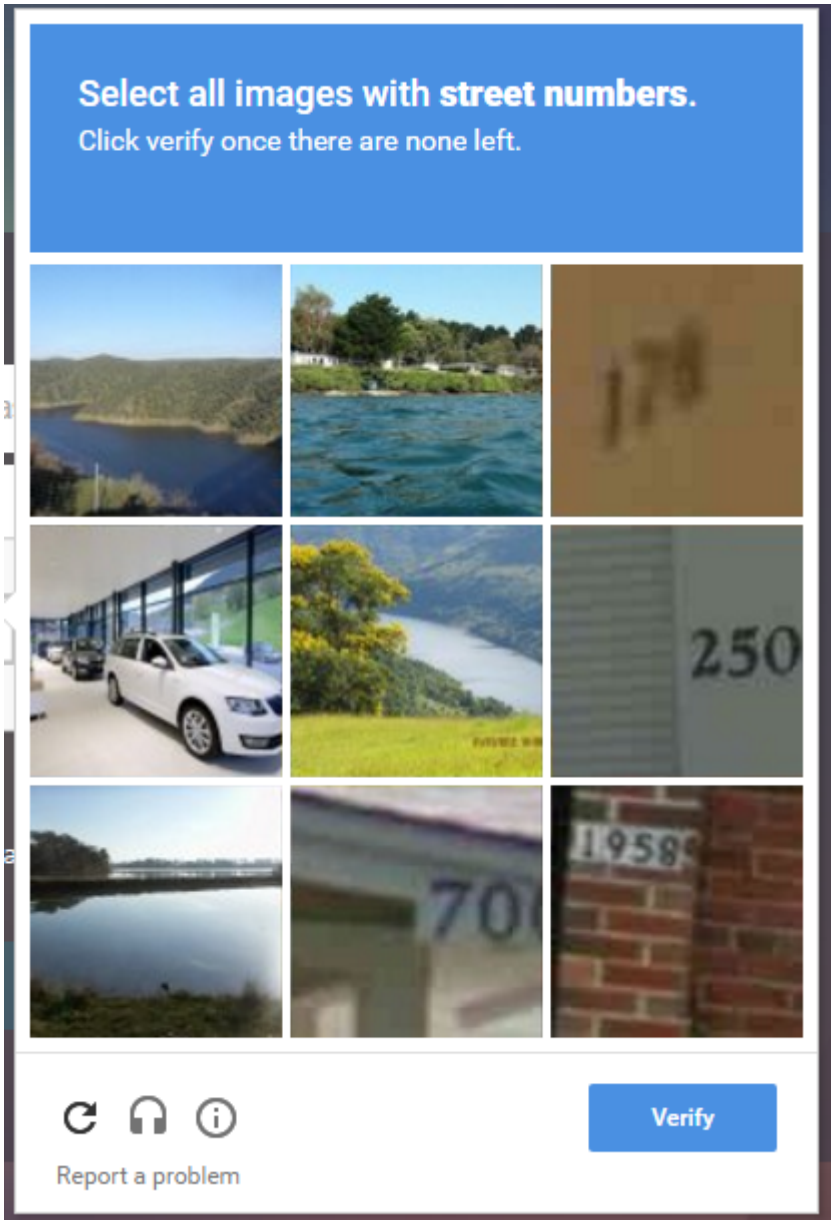
Validación de usuarios de re-Captcha

Una vez que haya configurado todos los pasos mencionados en las secciones anteriores, debe ver la siguiente interfaz de usuario.

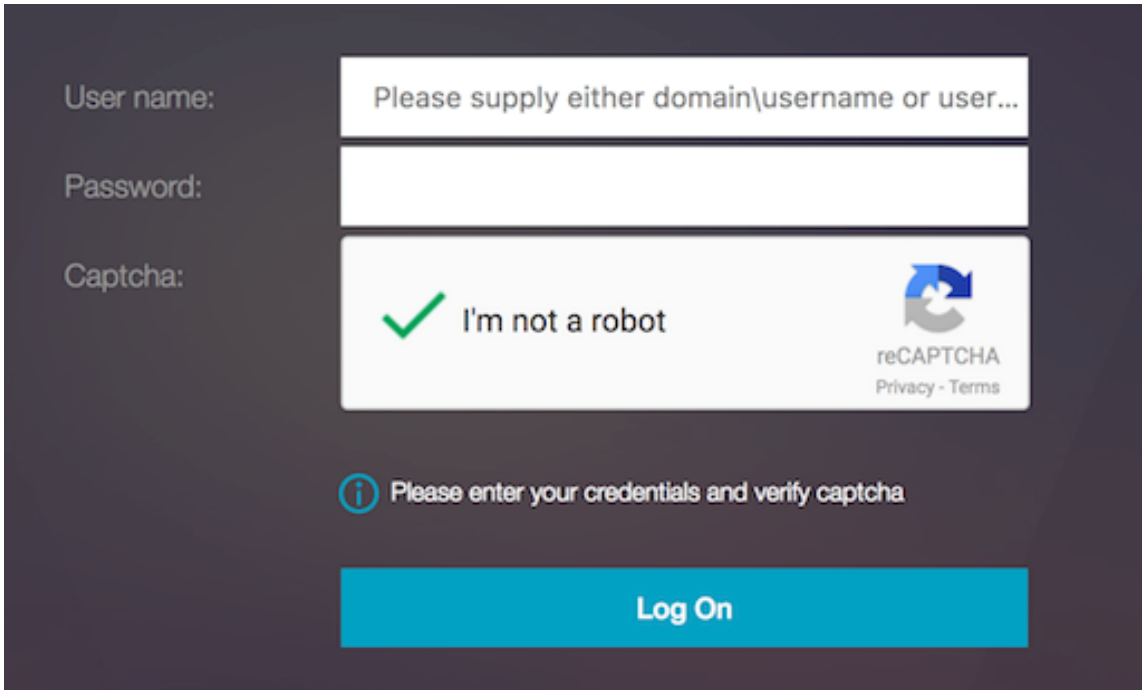
1. Una vez que el servidor virtual de autenticación carga la página de inicio de sesión, aparece la pantalla de inicio de sesión. El **inicio de sesión** está inhabilitado hasta que se complete Re-Captcha.



2. Selecciona la opción No soy un robot. Se muestra el widget re-Captcha.



3. Se le lleva a través de una serie de imágenes re-Captcha antes de que se muestre la página de finalización.
4. Introduzca las credenciales de AD, active la casilla de verificación **No soy un robot** y haga clic **en Iniciar sesión**. Si la autenticación se realiza correctamente, se le redirigirá al recurso deseado.



Notas:

- Si se usa re-Captcha con la autenticación de AD, el botón **Enviar** para las credenciales se inhabilita hasta que se complete re-Captcha.
- El re-Captcha ocurre en un factor propio. Por lo tanto, cualquier validación posterior como AD debe realizarse en re-Captcha. `nextfactor`

Compatibilidad con OTP nativa para la autenticación

July 8, 2022

Citrix ADC admite contraseñas de un solo uso (OTP) sin tener que usar un servidor de terceros. La contraseña de un solo uso es una opción muy segura para autenticarse en servidores seguros, ya que el número o código de acceso generado es aleatorio. Anteriormente, firmas especializadas, como RSA con dispositivos específicos que generan números aleatorios, ofrecían los OTP.

Además de reducir los gastos de capital y operativos, esta función mejora el control del administrador al mantener toda la configuración en el dispositivo Citrix ADC.

Nota:

Dado que ya no se necesitan servidores de terceros, el administrador de Citrix ADC tiene que configurar una interfaz para administrar y validar los dispositivos de usuario.

El usuario debe estar registrado con un servidor virtual Citrix ADC para utilizar la solución OTP. El reg-

istro solo es necesario una vez por dispositivo único y se puede restringir a determinados entornos. La configuración y validación de un usuario registrado es similar a la configuración de una directiva de autenticación adicional.

Ventajas de la función de OTP nativa

- Reduce los costes operativos al eliminar la necesidad de tener una infraestructura adicional en un servidor de autenticación además de Active Directory.
- Consolida la configuración solo en el dispositivo Citrix ADC, lo que ofrece un gran control a los administradores.
- Elimina la dependencia del cliente de un servidor de autenticación adicional para generar un número esperado por los clientes.

flujo de trabajo OTP nativo

La solución OTP nativa es un proceso doble y el flujo de trabajo se clasifica de la siguiente manera:

- Registro de dispositivos
- Inicio de sesión de usuario final

Importante:

> Puede omitir el proceso de registro si utiliza soluciones de terceros o administra otros dispositivos además del dispositivo Citrix ADC. La cadena final que agregue debe tener el formato especificado por Citrix ADC.

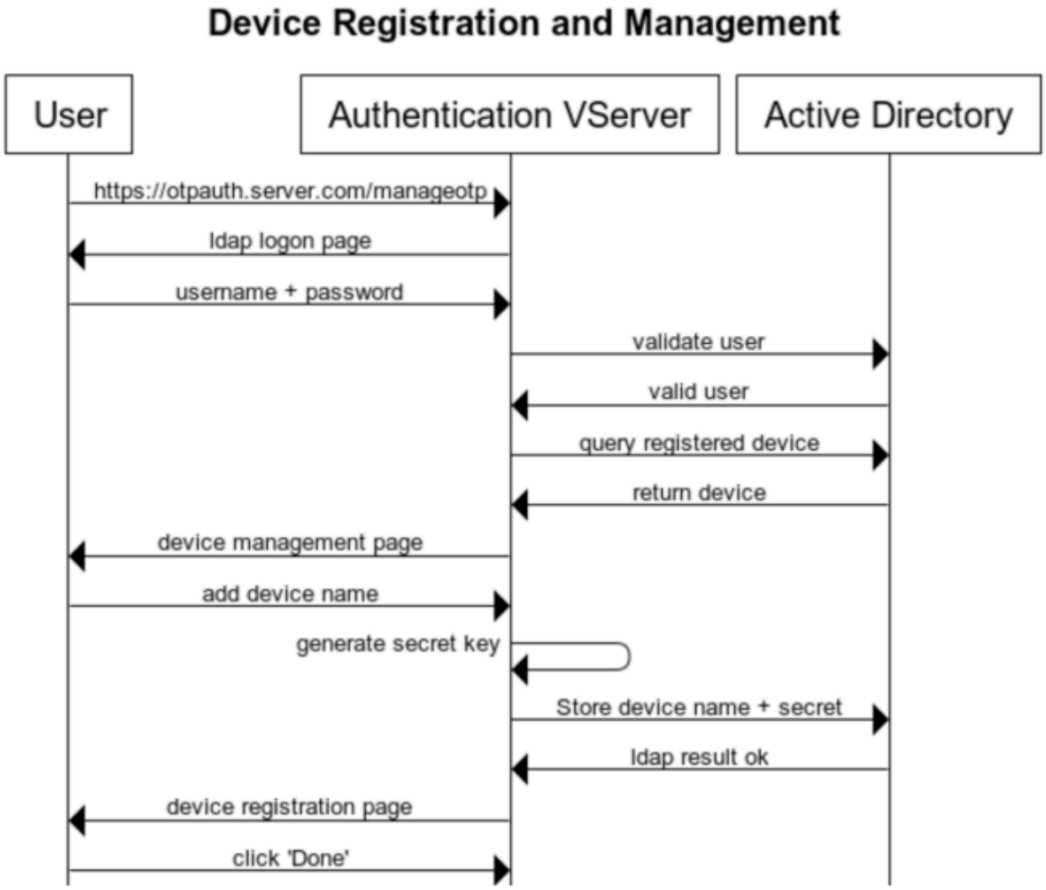
En la siguiente ilustración se muestra el flujo de registro de dispositivos para registrar un nuevo dispositivo para recibir OTP.

Nota:

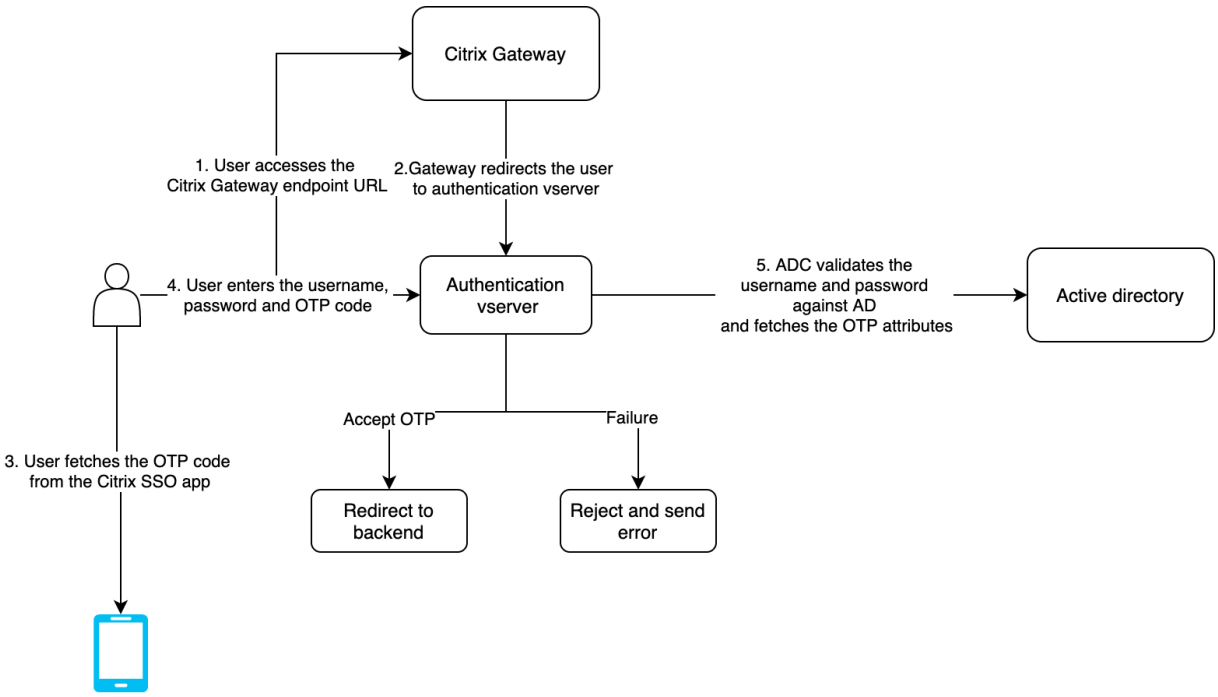
> El registro del dispositivo se puede realizar mediante cualquier número de factores. El factor único (como se especifica en la ilustración anterior) se utiliza como ejemplo para explicar el proceso de registro del dispositivo.

En la siguiente ilustración se muestra la verificación de OTP a través del dispositivo registrado.

En la siguiente ilustración se muestra el flujo de administración y registro de dispositivos.



En la siguiente ilustración se muestra el flujo de usuario final de la función OTP nativa.



Requisitos previos

Para utilizar la función OTP nativa, asegúrese de que se cumplen los siguientes requisitos previos.

- La versión de la función Citrix ADC es 12.0, compilación 51.24 y versiones posteriores.
- La licencia Advanced o Premium edition está instalada en Citrix Gateway.
- Citrix ADC está configurado con IP de administración y se puede acceder a la consola de administración mediante un explorador y una línea de comandos.
- Citrix ADC está configurado con un servidor virtual de autenticación, autorización y auditoría para autenticar a los usuarios. Para obtener más información, consulte Servidor virtual de autenticación.
- El dispositivo Citrix ADC se configura con Unified Gateway y el perfil de autenticación, autorización y auditoría se asigna al servidor virtual Gateway.
- La solución OTP nativa está restringida al flujo de autenticación nFactor. Se requieren directivas avanzadas para configurar la solución. Para obtener más información, consulte OTP nativo.

Asegúrese también de lo siguiente para Active Directory:

- Longitud mínima de atributo de 256 caracteres.
- El tipo de atributo debe ser “DirectoryString”, como UserParameters. Estos atributos pueden contener valores de cadena.
- El tipo de cadena de atributos debe ser Unicode, si el nombre del dispositivo no está escrito en inglés.
- El administrador LDAP de Citrix ADC debe tener acceso de escritura al atributo AD seleccionado.

- El dispositivo Citrix ADC y la máquina cliente deben sincronizarse con un servidor horario de red común.

Configurar OTP nativo mediante la GUI

El registro OTP nativo no es solo una autenticación de un solo factor. Las siguientes secciones le ayudan a configurar la autenticación de un solo factor y de segundo factor.

Crear esquema de inicio de sesión para el primer factor

1. Vaya a **Seguridad AAA > Tráfico de aplicaciones > Esquema de inicio**de sesión.
2. Vaya a **Perfiles** y haga clic en **Agregar**.
3. En la página **Crear esquema de inicio de sesión de autenticación**, escriba *lschema_single_auth_manage_ot* en el campo **Nombre** y haga clic en **Modificar** junto a **noschema**.
4. Haga clic en la carpeta **LoginSchema**.
5. Desplácese hacia abajo para seleccionar **SingleAuth.xml** y haga clic en **Seleccionar**.
6. Haga clic en **Crear**.
7. Haga clic en **Directivas** y haga clic en **Agregar**.
8. En la pantalla **Crear directiva de esquema de inicio de sesión de autenticación**, introduzca los siguientes valores.

   Nombre: lpol_single_auth_manage_otp_by_url

   Perfil: Seleccione lschema_single_auth_manage_otp de la lista.

   Regla: HTTP.REQ.COOKIE.VALUE(“NSC_TASS”).EQ(“manageotp”)

Configurar el servidor virtual de autenticación, autorización y auditoría

1. Vaya a **Seguridad > AAA — Tráfico de aplicaciones > Servidores virtuales de autenticación**. Haga clic para modificar el servidor virtual existente. Para obtener más información, consulte Servidor virtual de autenticación.
2. Haga clic en el icono **+** situado junto a **Esquemas de inicio** de sesión en **Configuración avanzada** en el panel derecho.
3. Seleccione **Sin esquema de inicio de sesión**.
4. Haga clic en la flecha y seleccione la directiva **lpol_single_auth_manage_otp_by_url**, haga clic en **Seleccionar**y, a continuación, en **Vincular**.

5. Desplácese hacia arriba y selecciona **1 Directiva de autenticación** en **Directiva de autenticación avanzada**.
6. Haga clic con el botón derecho en **la directiva nFactor** y seleccione **Modificar enlace**. Haga clic con el botón derecho en la directiva de nFactor ya configurada o consulte nFactor para crear una y seleccionar Modificar enlace.
7. Haga clic en la flecha de **Seleccionar siguiente factor** para seleccionar una configuración existente o haga clic en **Agregar** para crear un factor.
8. En la pantalla **Crear etiqueta de directiva de autenticación**, escriba lo siguiente y haga clic en **Continuar**:

   Nombre: manage_otp_flow_label

   Esquema de iniciode sesión: Lschema_Int
9. En la pantalla **Etiqueta de directiva de autenticación**, haga clic en **Agregar** para crear una directiva.

   ```
   Create a policy for a normal LDAP server.
   ```
10. En la pantalla **Crear directiva de autenticación**, introduzca lo siguiente:

    Nombre: auth_pol_ldap_native_otp
11. Seleccione el tipo de acción como **LDAP** mediante la lista **Tipo de acción**.
12. En el campo **Acción**, haga clic en **Agregar** para crear una acción.

    ```
    Create the first LDAP action with authentication enabled to be used for
     single factor.
    ```
13. En la página **Crear servidor LDAP de autenticación**, seleccione el botón de opción **IP del servidor**, desmarque la casilla situada junto a **Autenticación**, introduzca los siguientes valores y seleccione **Probar conexión**. A continuación se muestra un ejemplo de configuración.

    Nombre: ldap_native_otp

    Dirección IP: 192.8.xx.xx

    DN base: DC = formación, DC = laboratorio

    Administrador: Administrator@training.lab

    Contraseña: `xxxxx`

    ```
    Create a policy for OTP .
    ```
14. En la pantalla **Crear directiva de autenticación**, introduzca lo siguiente:

    Nombre: auth_pol_ldap_otp_action
15. Seleccione el tipo de acción como **LDAP** mediante la lista **Tipo de acción**.

16. En el campo **Acción**, haga clic en **Agregar** para crear una acción.

    `Create the second LDAP action to set OTP authenticator with OTP secret configuration and authentication unchecked.`

17. En la página **Crear servidor LDAP de autenticación**, seleccione el botón de opción **IP del servidor**, desmarque la casilla situada junto a **Autenticación**, introduzca los siguientes valores y seleccione **Probar conexión**. A continuación se muestra un ejemplo de configuración.

    Nombre: ldap_otp_action

    Dirección IP: 192.8.xx.xx

    DN base: DC = formación, DC = laboratorio

    Administrador: Administrator@training.lab

    Contraseña: `xxxxx`

18. Desplácese hacia abajo hasta la sección **Otros ajustes**. Utilice el menú desplegable para seleccionar las siguientes opciones.
    Atributo de nombre de inicio de sesión del servidor como **nuevo** y escriba **userprincipalname**.

19. Utilice el menú desplegable para seleccionar **Atributo de nombre de SSO** como **Nuevo** y escriba **userprincipalname**.

20. Introduzca “UserParameters” en el campo **OTP Secret** y haga clic en **Más**.

21. Introduzca los siguientes atributos.

    Atributo 1 = mail
    Atributo 2 =
    Atributo objectGUID 3 = immutableID

22. Haga clic en **Aceptar**.

23. En la página **Crear directiva de autenticación**, establezca la expresión en **true** y haga clic en **Crear**.

24. En la página **Crear etiqueta de directiva de autenticación**, haga clic en **Vincular** y haga clic en **Listo.**

25. En la página **Enlace de directivas**, haga clic en **Vincular**.

26. En la página **Directiva de autenticación**, haga clic en **Cerrar** y haga clic en **Listo**.

    `Create OTP for OTP verification.`

27. En la pantalla **Crear directiva de autenticación**, introduzca lo siguiente:

    Nombre: auth_pol_ldap_otp_verify

28. Seleccione el tipo de acción como **LDAP** mediante la lista **Tipo de acción**.
29. En el campo **Acción**, haga clic en **Agregar** para crear una acción.

    `Create the third LDAP action to verify OTP.`
30. En la página **Crear servidor LDAP de autenticación**, seleccione el botón de opción **IP del servidor**, desmarque la casilla situada junto a **Autenticación**, introduzca los siguientes valores y seleccione **Probar conexión**. A continuación se muestra un ejemplo de configuración.

    Nombre: ldap_verify_otp

    Dirección IP: 192.168.xx.xx

    DN base: DC = formación, DC = laboratorio

    Administrador: Administrator@training.lab

    Contraseña: `xxxxx`
31. Desplácese hacia abajo hasta la sección **Otros ajustes**. Utilice el menú desplegable para seleccionar las siguientes opciones.
    Atributo de nombre de inicio de sesión del servidor como **nuevo** y escriba **userprincipalname**.
32. Utilice el menú desplegable para seleccionar **Atributo de nombre de SSO** como **Nuevo** y escriba **userprincipalname**.
33. Introduzca “UserParameters” en el campo **OTP Secret** y haga clic en **Más**.
34. Introduzca los siguientes atributos.

    Atributo 1 = mail
    Atributo 2 =
    Atributo objectGUID 3 = immutableID
35. Haga clic en **Aceptar**.
36. En la página **Crear directiva de autenticación**, establezca la expresión en **true** y haga clic en **Crear**.
37. En la página **Crear etiqueta de directiva de autenticación**, haga clic en **Vincular** y haga clic en **Listo.**
38. En la página **Enlace de directivas**, haga clic en **Vincular**.
39. En la página **Directiva de autenticación**, haga clic en **Cerrar** y haga clic en **Listo**.

Probablemente no tenga ya una directiva de autenticación avanzada para su servidor LDAP normal. Cambie el tipo de acción a LDAP.
Seleccione su servidor LDAP normal, que es el que tiene la autenticación habilitada.

Introduzca true como expresión. Utiliza la directiva avanzada en lugar de la sintaxis clásica.
Haga clic en **Crear**.

> **Nota:**
>
> El servidor virtual de autenticación debe estar vinculado al tema del portal RFWebUI. Enlace un certificado de servidor al servidor. La IP del servidor "1.2.3.5" debe tener un FQDN correspondiente, es decir, otpauth.server.com, para su uso posterior.

Crear esquema de inicio de sesión para OTP de segundo factor

1. Vaya a **Seguridad > Tráfico de aplicaciones AAA > Servidores virtuales**. Seleccione el servidor virtual que va a modificar.
2. Vaya hacia abajo y seleccione **1 esquema de inicio de sesión**.
3. Haga clic en **Agregar enlace**.
4. En la sección **Vinculación de directivas**, haga clic en **Agregar** para agregar una directiva.
5. En la página **Crear directiva de esquema de inicio de sesión de autenticación**, escriba Nombre como OTP y haga clic en **Agregar** para crear un perfil.
6. En la página **Crear esquema de inicio de sesión de autenticación**, escriba Nombre como OTP y haga clic en el icono de lápiz junto a **noschema**.
7. Haga clic en la carpeta **LoginSchema**, seleccione **DualAuthManageOTP.xml**y, a continuación, haga clic en **Seleccionar**.
8. Haga clic en **Más** y desplácese hacia abajo.
9. En el campo **Índice de credenciales de contraseña**, escriba 1. Esto hace que nFactor guarde la contraseña del usuario en Citrix ADC AAA Attribute #1, que se puede usar más adelante en una directiva de tráfico para Single Sign-On en StoreFront. Si no lo hace, Citrix Gateway intentará usar el código de acceso para autenticarse en StoreFront, lo que no funciona.
10. Haga clic en **Crear**.
11. En la sección **Regla**, escriba **True**. Haga clic en **Crear**.
12. Haga clic en **Vincular**.
13. Observe los dos factores de autenticación. Haga clic en **Cerrar** y haga clic en **Listo**.

Directiva de tráfico para Single Sign-On

1. Vaya a **Citrix Gateway > Directivas > Tráfico**.
2. En la ficha **Perfiles de tráfico**, haga clic en **Agregar**.
3. Introduzca un nombre para el perfil de tráfico de OTP.
4. Desplácese hacia abajo, en el cuadro Expresión de contraseña de SSO, introduzca lo siguiente y haga clic en **Crear**. Aquí es donde usamos el atributo de contraseña del esquema de inicio de sesión especificado para el segundo factor OTP.


```
http.REQ.USER.ATTRIBUTE(1)
```

5. En la ficha **Directiva de tráfico**, haga clic en **Agregar**.
6. En el campo **Nombre**, introduzca un nombre para la directiva de tráfico.
7. En el campo **Solicitud de perfil**, seleccione el perfil de tráfico que ha creado.
8. En el cuadro Expresión, escriba **True**. Si su servidor virtual Citrix Gateway permite una VPN completa, cambie la expresión a la siguiente.

   ```
   http.req.method.eq(post)||http.req.method.eq(get)&& false
   ```

9. Haga clic en **Crear**.

Configurar la directiva de cambio de contenido para administrar OTP

Las siguientes configuraciones son necesarias si utiliza Unified Gateway.

1. Vaya a **Administración del tráfico > Cambio de contenido > Directivas**. Seleccione la directiva de cambio de contenido, haga clic con el botón derecho y seleccione **Modificar**.
2. Modifique la expresión para evaluar la siguiente instrucción OR y haga clic en **Aceptar**:

   ```
   is_vpn_url\|\|HTTP.REQ.URL.CONTAINS(”manageotp”)
   ```

Configurar OTP nativo mediante la CLI

Debe disponer de la siguiente información para configurar la página de administración de dispositivos OTP:

- IP asignada al servidor virtual de autenticación
- FQDN correspondiente a la IP asignada
- Certificado de servidor para servidor virtual de autenticación

> **Nota:**
>
> La OTP nativa es solo una solución basada en web.

Para configurar la página de registro y administración de dispositivos OTP

Crear servidor virtual de autenticación

```
1 ```
2 add authentication vserver authvs SSL 1.2.3.5 443
3 bind authentication vserver authvs -portaltheme RFWebUI
4 bind ssl vserver authvs -certkeyname otpauthcert
```



```
<!--NeedCopy--> ```
```

> **Nota:**
>
> El servidor virtual de autenticación debe estar enlazado al tema del portal RFWebUI. Enlace un certificado de servidor al servidor. La IP del servidor “1.2.3.5” debe tener un FQDN correspondiente, es decir, otpauth.server.com, para su uso posterior.

Para crear una acción de inicio de sesión LDAP

```
add authentication ldapAction <LDAP ACTION NAME> -serverIP <SERVER IP> -  serverPort <SERVER PORT> -ldapBase <BASE> -ldapBindDn <AD USER> -ldapBindDnPassword <PASSWO> -ldapLoginName <USER FORMAT>
```

Ejemplo:

```
add authentication ldapAction ldap_logon_action -serverIP 1.2.3.4 -serverPort 636 -ldapBase ”OU=Users,DC=server,DC=com” -ldapBindDn administrator@ctxnsdev.com -ldapBindDnPassword PASSWORD -ldapLoginName userprincipalname
```

Para agregar la directiva de autenticación para el inicio de sesión de LDAP

```
add authentication Policy auth_pol_ldap_logon -rule true -action ldap_logon_action
```

Para presentar la interfaz de usuario a través de LoginSchema

Mostrar campo de nombre de usuario y campo de contraseña a los usuarios al iniciar sesión

```
add authentication loginSchema lschema_single_auth_manage_otp -authenticationSchema ”/nsconfig/loginschema/LoginSchema/SingleAuthManageOTP.xml”
```

Mostrar la página de registro y administración de dispositivos

Citrix recomienda dos formas de mostrar la pantalla de registro y administración del dispositivo: URL o nombre de host.

- **Uso de URL**

  Cuando la URL contiene '/manageotp'

  - `add authentication loginSchemaPolicy lpol_single_auth_manage_otp_by_url -rule "http.req.cookie.value("NSC_TASS").contains("manageotp")"-action lschema_single_auth_manage_otp`
  - `bind authentication vserver authvs -policy lpol_single_auth_manage_otp_by_url -priority 10 -gotoPriorityExpression END`

- **Uso del nombre de host**

  Cuando el nombre de host es "alt.server.com"

  - `add authentication loginSchemaPolicy lpol_single_auth_manage_otp_by_host -rule "http.req.header("host").eq("alt.server.com")"-action lschema_single_auth_manage_otp`
  - `bind authentication vserver authvs -policy lpol_single_auth_manage_otp_by_host -priority 20 -gotoPriorityExpression END`

Para configurar la página de inicio de sesión de usuario mediante la CLI

Debe disponer de la siguiente información para configurar la página Inicio de sesión de usuario:

- IP de un servidor virtual de equilibrio de carga
- FQDN correspondiente para el servidor virtual de equilibrio de carga
- Certificado de servidor para el servidor virtual de equilibrio de carga

```
1 bind ssl virtual server lbvs_https -certkeyname lbvs_server_cert
2 <!--NeedCopy-->
```

El servicio back-end en el equilibrio de carga se representa de la siguiente manera:

```
1 ```
2 add service iis_backendsso_server_com 1.2.3.210 HTTP 80
3 bind lb vserver lbvs_https iis_backendsso_server_com
4 <!--NeedCopy--> ```
```

Para crear una acción de validación de código de acceso OTP


```
add authentication ldapAction <LDAP ACTION NAME> -serverIP <SERVER IP>
    -serverPort <SERVER PORT> -ldapBase <BASE> -ldapBindDn <AD USER> -
    ldapBindDnPassword <PASSWORD> -ldapLoginName <USER FORMAT> -
    authentication DISABLED -OTPSecret <LDAP ATTRIBUTE>`
```

Ejemplo:

```
add authentication ldapAction ldap_otp_action -serverIP 1.2.3.4 -
    serverPort 636 -ldapBase "OU=Users,DC=server,DC=com" -ldapBindDn
    administrator@ctxnsdev.com -ldapBindDnPassword PASSWORD -
    ldapLoginName userprincipalname -authentication DISABLED -OTPSecret
    userParameters
```

> **Importante:**
>
> La diferencia entre el inicio de sesión LDAP y la acción OTP es la necesidad de inhabilitar la autenticación e introducir un parámetro nuevo `OTPSecret`. No utilice el valor del atributo AD.

Para agregar directiva de autenticación para la validación de código de acceso OTP

```
add authentication Policy auth_pol_otp_validation -rule true -action
    ldap_otp_action
```

Para presentar la autenticación de dos factores a través de LoginSchema

Agregue la interfaz de usuario para la autenticación de dos factores.

```
add authentication loginSchema lscheme_dual_factor -
    authenticationSchema "/nsconfig/loginschema/LoginSchema/DualAuth.xml
    "
add authentication loginSchemaPolicy lpol_dual_factor -rule true -
    action lscheme_dual_factor
```

Para crear un factor de validación de código de acceso mediante la etiqueta de directiva

Crear una etiqueta de directiva de flujo OTP de administración para el siguiente factor (el primer factor es inicio de sesión LDAP)


```
add authentication loginSchema lschema_noschema -authenticationSchema
    noschema
add authentication policylabel manage_otp_flow_label -loginSchema
    lschema_noschema
```

Para enlazar la directiva OTP a la etiqueta de directiva

```
bind authentication policylabel manage_otp_flow_label -policyName
    auth_pol_otp_validation -priority 10 -gotoPriorityExpression NEXT
```

Para enlazar el flujo de la interfaz de usuario

Enlazar el inicio de sesión LDAP seguido de la validación OTP con el servidor virtual de autenticación.

```
bind authentication vserver authvs -policy auth_pol_ldap_logon -
    priority 10 -nextFactor  manage_otp_flow_label -
    gotoPriorityExpression NEXT
bind authentication vserver authvs -policy lpol_dual_factor -priority
    30 -gotoPriorityExpression END
```

Registre su dispositivo con Citrix ADC

1. Vaya a el FQDN de Citrix ADC (primera IP pública), con el sufijo /manageotp. Por ejemplo, inicie sesión en https://otpauth.server.com/manageotp con credenciales de usuario.
2. Haga clic en el ícono **+** para agregar un dispositivo.
3. Introduzca el nombre de un dispositivo y presione **Ir**. Aparece un código de barras en la pantalla.
4. Haga clic en **Iniciar configuración** y luego haga clic en **Escanear código de barras**
5. Coloque la cámara del dispositivo sobre el código QR. Si quiere, puede introducir el código.

   > **Nota**:
   >
   > El código QR que se muestra es válido durante 3 minutos.

6. Una vez escaneado correctamente, se le presenta un código sensible al tiempo de 6 dígitos que se puede utilizar para iniciar sesión.
7. Para realizar la prueba, haga clic en **Listo** en la pantalla QR y, a continuación, haga clic en la marca de verificación verde de la derecha.

8. Seleccione su dispositivo en el menú desplegable e introduzca el código de Google Authenticator (debe ser azul, no rojo) y haga clic en **Ir**.
9. Asegúrate de cerrar la sesión mediante el menú desplegable de la esquina superior derecha de la página.

Inicie sesión en Citrix ADC mediante la OTP

1. Navegue a la primera URL pública e introduzca su OTP desde Google Authenticator para iniciar sesión.
2. Autenticación en la página inicial de Citrix ADC.

Almacenar datos secretos de OTP en un formato cifrado

August 20, 2021

A partir de Citrix ADC versión 13.0 compilación 41.20, los datos secretos de OTP se pueden almacenar en un formato cifrado en lugar de texto sin formato.

Anteriormente, el dispositivo Citrix ADC almacenaba el secreto de OTP como texto sin formato en AD. Almacenar el secreto de OTP en texto sin formato supone una amenaza para la seguridad, ya que un atacante malintencionado o un administrador podría explotar los datos al ver el secreto compartido de otros usuarios.

El parámetro de cifrado habilita el cifrado del secreto OTP en AD. Cuando registra un nuevo dispositivo con Citrix ADC versión 13.0 compilación 41.20 y habilita el parámetro de cifrado, el secreto OTP se almacena de forma predeterminada en un formato cifrado. Sin embargo, si el parámetro de cifrado está inhabilitado, el secreto OTP se almacena en formato de texto sin formato.

Para los dispositivos registrados antes de la compilación 13.0 41.20, debe realizar lo siguiente como práctica recomendada:

1. Actualice el dispositivo Citrix ADC 13.0 a 13.0 compilación 41.20.
2. Habilite el parámetro de cifrado en el dispositivo.
3. Utilice la herramienta de migración secreta de OTP para migrar los datos secretos de OTP del formato de texto sin formato al formato cifrado.

Para obtener más información acerca de la herramienta de migración secreta OTP, consulte Herramienta de cifrado OTP.

> **Importante**
>
> Citrix le recomienda como administrador para asegurarse de que se cumplen los siguientes cri-

terios:

- Se debe configurar un nuevo certificado para cifrar los secretos de OTP si no está usando KBA como parte de la función de restablecimiento de contraseña de autoservicio.
  - To bind the certificate to VPN global, you can use the following command:

    ```
    bind vpn global -userDataEncryptionKey <certificate name>
    ```
- Si ya está usando un certificado para cifrar KBA, puede utilizar el mismo certificado para cifrar secretos OTP.

Para habilitar los datos de cifrado OTP mediante la CLI

En el símbolo del sistema, escriba:

```
set aaa otpparameter [-encryption ( ON | OFF )]
```

Ejemplo

```
set aaa otpparameter -encryption ON
```

Para configurar el cifrado OTP mediante la interfaz gráfica de usuario

1. Vaya a **Seguridad > AAA: Tráfico de aplicaciones** y haga clic en **Cambiar autenticación Parámetro OTP AAA** en la sección **Configuración de autenticación**.
2. En la página **Configurar parámetro OTP AAA**, seleccione **Cifrado secreto OTP**.
3. Haga clic en Aceptar.

Configuración del número de dispositivos de usuario final para recibir notificaciones de OTP

Ahora los administradores pueden configurar el número de dispositivos que un usuario final puede registrar para recibir una notificación o autenticación OTP.

Para configurar el número de dispositivos en OTP mediante la CLI

En el símbolo del sistema, escriba:

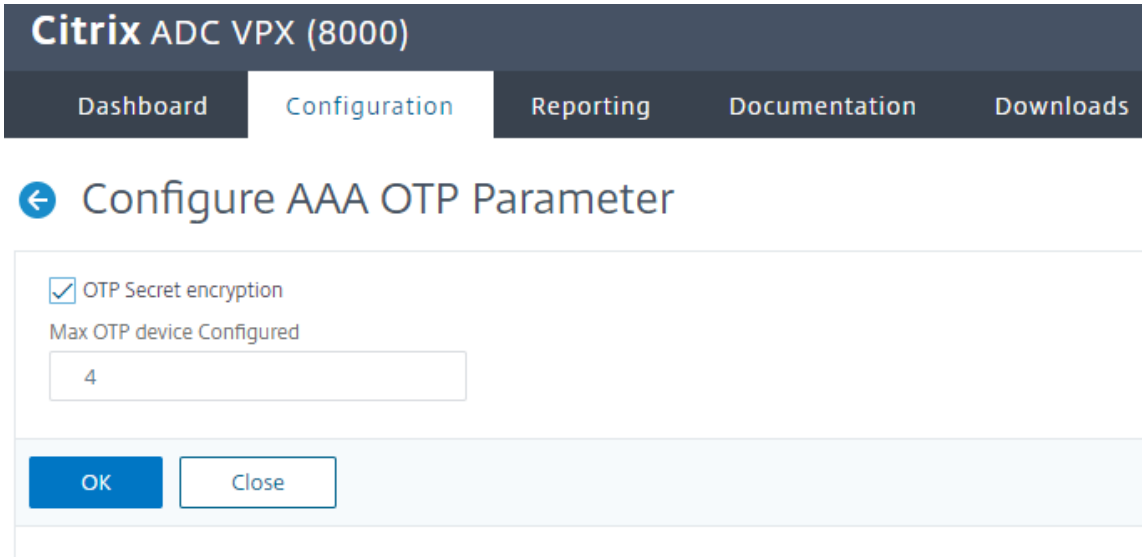
```
set aaa otpparameter [-maxOTPDevices <positive_integer>]
```

Ejemplo

```
set aaa otpparameter -maxOTPDevices 4
```


Para configurar el número de dispositivos mediante la interfaz gráfica de usuario

1. Vaya a **Seguridad > AAA: Tráfico de aplicaciones**, haga clic en **Cambiar autenticación Parámetro OTP AAA**en la sección **Configuración de autenticación**.
2. En la página **Configurar Parámetro OTP AAA**, introduzca el valor de **Dispositivo OTP Máximo configurado**.
3. Haga clic en **Aceptar**.



Herramienta de cifrado OTP

June 2, 2022

A partir de la versión 13.0 compilación 41.20 de Citrix ADC, los datos secretos de OTP se almacenan en un formato cifrado en lugar de texto sin formato para una mayor seguridad. El almacenamiento de un secreto OTP en formato cifrado es automático y no requiere intervención manual.

Anteriormente, el dispositivo Citrix ADC almacenaba un secreto OTP como texto sin formato en el directorio activo. Almacenar un secreto OTP en un formato de texto sin formato planteaba una amenaza para la seguridad, ya que un atacante malintencionado o un administrador podían explotar los datos al ver el secreto compartido de otros usuarios.

La herramienta de cifrado OTP ofrece las siguientes ventajas:

- No provoca ninguna pérdida de datos, incluso si tiene dispositivos antiguos que utilizan un formato antiguo (texto sin formato).
- La compatibilidad con versiones anteriores de Citrix Gateway ayuda a integrar y admitir los dispositivos existentes, junto con el nuevo dispositivo.

- La herramienta de cifrado OTP ayuda a los administradores a migrar todos los datos secretos de OTP de todos los usuarios a la vez.

> **Nota**
>
> La herramienta de cifrado OTP no cifra ni descifra los datos de registro de KBA ni de registro de correo electrónico.

Usos de la herramienta de cifrado OTP

La herramienta de cifrado OTP se puede utilizar para lo siguiente:

- **Cifrado**. Guarde el secreto OTP en formato cifrado. La herramienta extrae los datos OTP de los dispositivos registrados en Citrix ADC y, a continuación, convierte los datos OTP en formato de texto sin formato a formato cifrado.
- **Descifrado**. Revierte el secreto OTP al formato de texto sin formato.
- **Actualizar certificados**. Los administradores pueden actualizar el certificado a un nuevo certificado en cualquier momento. Los administradores pueden utilizar la herramienta para introducir el nuevo certificado y actualizar todas las entradas con los nuevos datos del certificado. La ruta de certificado debe ser una ruta absoluta o relativa.

> **Importante**
>
> - Debe habilitar el parámetro de cifrado en el dispositivo Citrix ADC para usar la herramienta de cifrado OTP.
> - Para los dispositivos registrados en Citrix ADC antes de la compilación 41.20, debe realizar lo siguiente:
>   - Upgrade the 13.0 Citrix ADC appliance to 13.0 build 41.20.
>   - Enable the encryption parameter on the appliance.
>   - Use the OTP Secret migration tool to migrate OTP secret data from plain text format to encrypted format.

Datos secretos OTP en formato de texto sin formato

Ejemplo:

```
##@devicename=<16 or more bytes>&tag=<64bytes>&,
```

Como puede ver, el patrón inicial de un formato antiguo siempre es “#@” y un patrón final siempre es “&”. Todos los datos entre “devicename=” y el patrón final constituyen datos OTP del usuario.

Datos secretos OTP en formato cifrado

El nuevo formato cifrado de los datos OTP tiene el siguiente formato:

Ejemplo:

```
    {

         ”otpdata” : {

          “devices” : {

                              “device1” :  “value1” ,
                              “device2” :  “value2” , ⋯
                         }

             }

      }

<!--NeedCopy-->
```

Donde, value1 es un valor codificado en base64 de datos de kid + IV +cifrado

Los datos cifrados se estructuran de la siguiente manera:

```
    {

      secret:<16-byte secret>,
      tag : <64-byte tag value>
      alg: <algorithm used> (not mandatory, default is sha1, specify
          the algorithm only if it is not default)
     }

<!--NeedCopy-->
```

- En “dispositivos”, tiene valor para cada nombre. El valor es base64encode(kid).base64encode(IV).base64enc
- En los algoritmos AES estándar, IV siempre se envía como los primeros 16 bytes o 32 bytes de datos cifrados. Puede seguir el mismo modelo.
- La IV es diferente para cada dispositivo, aunque la clave es la misma.

Configuración de la herramienta de cifrado OTP

> **Nota**
>
> Para ejecutar la herramienta de cifrado OTP, Citrix recomienda utilizar una plataforma alternativa

> con el entorno Python en lugar del dispositivo Citrix ADC.

La herramienta de cifrado OTP se encuentra en el directorio `\var\netscaler\otptool`. Debe descargar el código de la fuente de Citrix ADC y ejecutar la herramienta con las credenciales de AD requeridas.

- Requisitos previos para usar la herramienta de cifrado OTP:
  - Instale python 3.5 o una versión superior en el entorno en el que se ejecuta esta herramienta.
  - Instala pip3 o versiones posteriores.
- Ejecute los comandos siguientes:
  - **pip instala requirements.txt**. Instala automáticamente los requisitos
  - **python main.py que es**. Invoca la herramienta de cifrado OTP. Debe proporcionar los argumentos requeridos según su necesidad de migración de datos secretos OTP.
- La herramienta se puede ubicar en `\var\netscaler\otptool` desde un símbolo del shell.
- Ejecute la herramienta con las credenciales de AD requeridas.

Interfaz de herramienta de cifrado OTP

La siguiente ilustración muestra una interfaz de herramienta de cifrado OTP de ejemplo. La interfaz contiene todos los argumentos que se deben definir para la actualización de cifrado/descifrado/certificado. Además, se captura una breve descripción de cada argumento.

argumento OPERATION

Debe definir el argumento OPERATION para utilizar la herramienta de cifrado OTP para el cifrado, el descifrado o la actualización de certificados.

En la siguiente tabla se resumen algunos de los casos en los que se puede utilizar la herramienta de cifrado OTP y los valores de los argumentos OPERATION correspondientes.

Caso	Valor del argumento de operación y otros argumentos
Convierta el secreto OTP de texto sin formato a formato cifrado en el mismo atributo	Introduzca el valor del argumento OPERATION como 0 y proporcione el mismo valor para el atributo de origen y de destino. **Ejemplo:** `python3 main.py -Host 192.0.2.1 -Port 636 -username ldapbind_user@aaa.local -search_base cn=users,dc=aaa,dc=local -source_attribute unixhomedirectory -target_attribute unixhomedirectory -operation 0 -cert_path aaatm_wild_all.cert`
Convierta el secreto OTP de texto sin formato a formato cifrado en un atributo diferente	Introduzca el valor del argumento OPERATION como 0 y proporcione los valores correspondientes para el atributo de origen y de destino. **Ejemplo:** `python3 main.py -Host 192.0.2.1 -Port 636 -username ldapbind_user@aaa.local -search_base cn=users,dc=aaa,dc=local -source_attribute unixhomedirectory -target_attribute userparameters -operation 0 -cert_path aaatm_wild_all.cert`
Convertir las entradas cifradas de nuevo en texto sin formato	Introduzca el valor del argumento OPERATION como 1 y proporcione los valores correspondientes para el atributo de origen y de destino. **Ejemplo:** `python3 main.py -Host 192.0.2.1 -Port 636 -username ldapbind_user@aaa.local -search_base cn=users,dc=aaa,dc=local -source_attribute unixhomedirectory -target_attribute userparameters -operation 1 -cert_path aaatm_wild_all.cert`

Caso	Valor del argumento de operación y otros argumentos
Actualizar el certificado a un certificado nuevo	Introduzca el valor del argumento OPERATION como 2 y proporcione todos los detalles del certificado anterior y del nuevo certificado en los argumentos correspondientes. **Ejemplo:** `python3 main.py -Host 192.0.2.1 -Port 636 -username ldapbind_user@aaa.local -search_base cn=users,dc=aaa,dc=local -source_attribute unixhomedirectory -operation 2 -cert_path aaatm_wild_all.cert -new_cert_path aaatm_wild_all_new.cert`

Argumento CERT_PATH

El argumento CERT_PATH es un archivo que contiene el certificado que se utiliza en Citrix ADC para cifrar los datos. El usuario debe proporcionar este argumento para las tres operaciones, a saber, los **certificados de **cifrado, descifrado**y actualización**.

El archivo de argumentos CERT_PATH debe contener tanto el certificado como la clave privada asociada en el formato PEM o CERT (no se admite pfx).

Por ejemplo, si los archivos certificate.cert y certificate.key corresponden al archivo de certificado y su clave privada, en un sistema similar a Unix, el siguiente comando crea el archivo `certkey.merged` que se puede usar como valor para la marca cert_path.

```
$ cat certificate.cert certificate.key > certkey.merged
$
<!--NeedCopy-->
```

> **Puntos a tener en cuenta sobre el certificado**
>
> - El usuario debe proporcionar el mismo certificado que está enlazado globalmente en el dispositivo Citrix ADC para el cifrado de datos del usuario.
> - El certificado debe contener el certificado público codificado en Base64 y su correspondiente clave privada RSA en el mismo archivo.

> - El formato del certificado debe ser PEM o CERT. El certificado debe adherirse al formato X509.
> - Esta herramienta no acepta el formato de certificado protegido por contraseña ni el *archivo .pfx*. El usuario debe convertir los certificados PFX en *.cert* antes de proporcionar los certificados a la herramienta.

argumento SEARCH_FILTER

El argumento SEARCH_FILTER se utiliza para filtrar los dominios o usuarios de AD. El formato de este filtro de búsqueda es el mismo que el formato del filtro de búsqueda LDAP utilizado en el comando de **acción LDAP** en el dispositivo Citrix ADC.

Habilitar la opción de cifrado en el dispositivo Citrix ADC

Para cifrar el formato de texto sin formato, debe habilitar la opción de cifrado en el dispositivo Citrix ADC.

Para habilitar los datos de cifrado OTP mediante la CLI, en el símbolo del sistema, escriba:

```
set aaa otpparameter [-encryption ( ON | OFF )]
```

Ejemplo:

```
set aaa otpparameter -encryption ON
```

Casos de uso de la herramienta de cifrado OTP

La herramienta de cifrado OTP se puede utilizar para los siguientes casos de uso.

Registre nuevos dispositivos con el dispositivo Citrix ADC versión 13.0 compilación 41.20

Cuando registra su nuevo dispositivo con el dispositivo Citrix ADC versión 13.0 compilación 41.x, y si la opción de cifrado está habilitada, los datos OTP se guardan en un formato cifrado. Puede evitar la intervención manual.

Si la opción de cifrado no está habilitada, los datos OTP se almacenan en formato de texto sin formato.

Migrar los datos OTP para los dispositivos registrados antes de la versión 13.0 compilación 41.20

Debe realizar lo siguiente para cifrar los datos secretos de OTP para los dispositivos que están registrados en el dispositivo Citrix ADC antes de la 13.0 compilación 41.20.

- Use la herramienta de conversión para migrar datos OTP del formato de texto sin formato al formato cifrado.

- Habilite el parámetro “Cifrado” en el dispositivo Citrix ADC.
  - Para habilitar la opción de cifrado mediante la CLI:
    * `set aaa otpparameter -encryption ON`
  - Para habilitar las opciones de cifrado mediante la GUI:
    * Vaya a **Seguridad > AAA — Tráfico de aplicaciones** y haga clic en **Cambiar parámetro OTP AAA de autenticación** en la sección **Configuración de autenticación**.
    * En la página **Configurar parámetro OTP AAA**, seleccione **Cifrado secreto OTP**y haga clic en **Aceptar**.
  - Inicie sesión con las credenciales de AD válidas.
  - Si es necesario, registre más dispositivos (opcional).

Migrar datos cifrados del certificado antiguo al certificado nuevo

Si los administradores desean actualizar el certificado a un certificado nuevo, la herramienta ofrece una opción para actualizar las entradas de datos del nuevo certificado.

Para actualizar el certificado a un certificado nuevo mediante la CLI

En el símbolo del sistema, escriba:

Ejemplo:

```
python3 main.py -Host 192.0.2.1 -Port 636 -username ldapbind_user@aaa.local
-search_base cn=users,dc=aaa,dc=local -source_attribute unixhomedirectory -
target_attribute userparameters -operation 2 -cert_path aaatm_wild_all.cert
 -new_cert_path aaatm_wild_all_new.cert
```

> **Nota**
>
> - Los certificados deben tener claves públicas y privadas.
> - Actualmente, la funcionalidad solo se proporciona para OTP.

Vuelva a cifrar o migrar a un nuevo certificado para los dispositivos registrados después de que el dispositivo se actualice a 13.0 compilación 41.20 con cifrado

El administrador puede usar la herramienta en los dispositivos que ya están cifrados con un certificado y puede actualizar ese certificado con un certificado nuevo.

Convertir los datos cifrados a formato de texto sin formato

El administrador puede descifrar el secreto OTP y revertirlo al formato de texto sin formato original. La herramienta de cifrado OTP explora todos los usuarios en busca de un secreto OTP en formato cifrado y los convierte a formato descifrado.

Para actualizar el certificado a un certificado nuevo mediante la CLI

En el símbolo del sistema, escriba:

Ejemplo:

```
python3 main.py -Host 192.0.2.1 - Port 636 -username ldapbind_user@aaa
    .local -search_base cn=users,dc=aaa,dc=local -source_attribute
    unixhomedirectory -target_attribute userparameters -operation 1
<!--NeedCopy-->
```

Solución de problemas

La herramienta genera los siguientes archivos de registros.

- **app.log que es**. Registra todos los pasos principales de ejecución e información sobre errores, advertencias y fallas.
- **unmodified_users.txt que es**. Contiene una lista de DN de usuario que no se actualizaron de texto sin formato a formato cifrado. Estos registros se generan con un error de formato o pueden deberse a algún otro motivo.

Notificación push para OTP

May 8, 2022

Citrix Gateway admite notificaciones push para OTP. Los usuarios no tienen que introducir manualmente la OTP recibida en sus dispositivos registrados para iniciar sesión en Citrix Gateway. Los administradores pueden configurar Citrix Gateway para que las notificaciones de inicio de sesión se envíen a los dispositivos registrados de los usuarios mediante los servicios de notificaciones push. Cuando los usuarios reciben la notificación, simplemente tienen que tocar Permitir en la notificación para iniciar sesión en Citrix Gateway. Cuando la puerta de enlace recibe el acuse de recibo del usuario, identifica el origen de la solicitud y envía una respuesta a esa conexión del explorador.

Si la respuesta a la notificación no se recibe dentro del período de tiempo de espera (30 segundos), se redirige a los usuarios a la página de inicio de sesión de Citrix Gateway. A continuación, los usuarios pueden introducir la OTP manualmente o hacer clic en **Reenviar notificación** para volver a recibir la notificación en el dispositivo registrado.

Los administradores pueden hacer que la autenticación de notificaciones push sea la autenticación predeterminada mediante los esquemas de inicio de sesión creados para las notificaciones push.

> **Importante:**
>
> La función de notificaciones push está disponible con una licencia Citrix ADC Premium Edition.

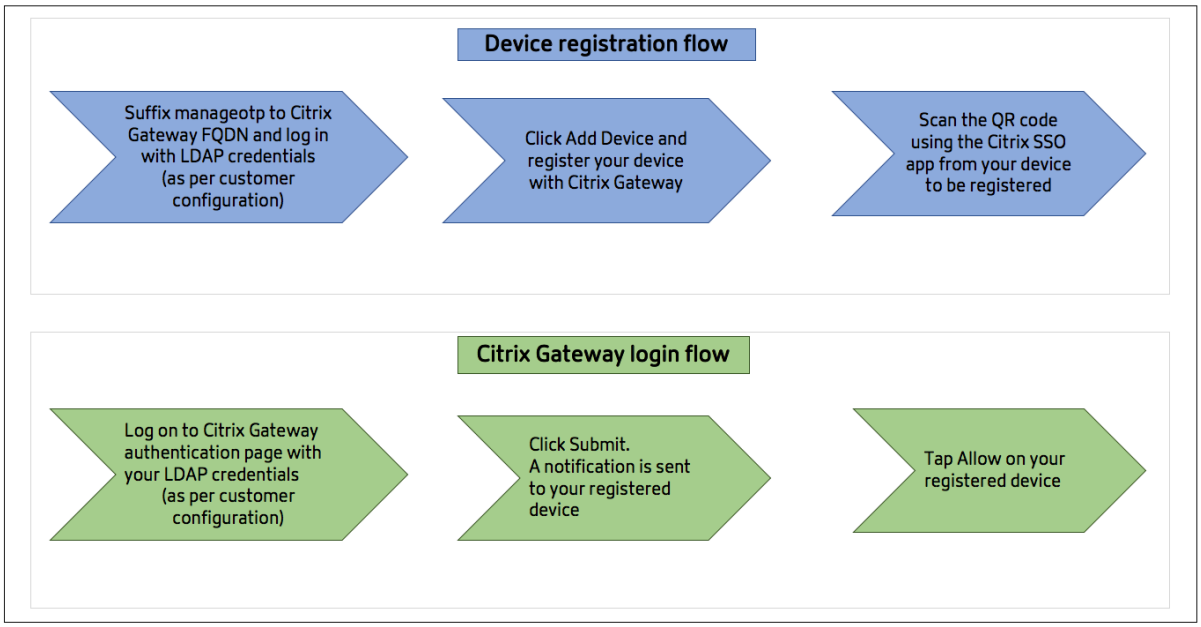
Ventajas de las notificaciones push

- Las notificaciones push proporcionan un mecanismo de autenticación multifactor más seguro. La autenticación en Citrix Gateway no se realiza correctamente hasta que el usuario aprueba el intento de inicio de sesión.
- Las notificaciones push son fáciles de administrar y usar. Los usuarios tienen que descargar e instalar la aplicación móvil Citrix SSO que no requiere asistencia de administrador.
- Los usuarios no tienen que copiar ni recordar el código. Simplemente tienen que tocar el dispositivo para autenticarse.
- Los usuarios pueden registrar varios dispositivos.

Cómo funcionan las notificaciones push

El flujo de trabajo de notificaciones push se puede clasificar en dos categorías:

- Registro de dispositivos
- Inicio de sesión de usuario final



Requisitos previos para utilizar las notificaciones push

- Complete el proceso de incorporación de Citrix Cloud.

1. Cree una cuenta de empresa de Citrix Cloud o únase a una existente. Para obtener instrucciones y procesos detallados sobre cómo proceder, consulte Registrarse en Citrix Cloud.
2. Inicie sesión en https://citrix.cloud.com y seleccione el cliente.
3. En Menú, seleccione **Administración de acceso e identidad** y, a continuación, vaya a la ficha **Acceso a API** para crear un cliente para la cuenta.
4. Copia el ID, el secreto y el ID de cliente. El ID y el secreto son necesarios para configurar el servicio push en Citrix ADC como “ClientID” y “ClientSecret” respectivamente.

> **Importante:**
>
> - Las mismas credenciales de API se pueden usar en varios centros de datos.
> - Los dispositivos Citrix ADC locales deben poder resolver las direcciones de servidor mfa.cloud.com y trust.citrixworkspacesapi.net y se puede acceder a ellos desde el dispositivo. Esto es para garantizar que no existan firewalls ni bloques de direcciones IP para estos servidores a través del puerto 443.

- Descargue la aplicación móvil Citrix SSO de App Store y Play Store para dispositivos iOS y Android, respectivamente. La notificación push es compatible con iOS desde la compilación 1.1.13 en Android a partir de la versión 2.3.5.
- Asegúrese de lo siguiente para Active Directory.
  - La longitud mínima del atributo debe ser de 256 caracteres como mínimo.
  - El tipo de atributo debe ser ‘DirectoryString’, como UserParameters. Estos atributos pueden contener valores de cadena.
  - El tipo de cadena de atributos debe ser Unicode, si el nombre del dispositivo no está escrito en inglés.
  - El administrador LDAP de Citrix ADC debe tener acceso de escritura al atributo AD seleccionado.
  - Citrix ADC y el equipo cliente deben sincronizarse con un servidor horario de red común.

Configuración de notificaciones push

A continuación se indican los pasos de alto nivel que se deben completar para utilizar la funcionalidad de notificaciones push.

- El administrador de Citrix Gateway debe configurar la interfaz para administrar y validar usuarios.
  1. Configure un servicio push.
  2. Configure Citrix Gateway para administración de OTP e inicio de sesión de usuario final.

     Los usuarios deben registrar sus dispositivos en la puerta de enlace para iniciar sesión en Citrix Gateway.

3. Registre el dispositivo con Citrix Gateway.
4. Inicie sesión en Citrix Gateway.

Crear un servicio push

1. Vaya a **Seguridad** > **Tráfico de aplicaciones AAA** > **Directivas** > **Autenticación** > **Directivas avanzadas** > **Acciones** > **Servicio de inserción** y haga clic en **Agregar**.
2. En **Nombre**, introduzca el nombre del servicio push.
3. En **ID de cliente**, introduzca la identidad única de la parte que confía para comunicarse con el servidor Citrix Push en la nube.
4. En **Client Secret**, introduzca el secreto único de la parte que confía para comunicarse con el servidor Citrix Push en la nube.
5. En **ID de cliente**, introduzca el ID de cliente o el nombre de la cuenta en la nube que se utiliza para crear el par ID de cliente y secreto de cliente.

> **Importante**
>
> La versión de TLS 1.2 es necesaria para el servicio push. Para obtener más información, consulte los detalles de configuración de TLS 1.2.

Configurar Citrix Gateway para la administración de OTP y el inicio de sesión del usuario final

Complete los siguientes pasos para la administración de OTP y el inicio de sesión del usuario final.

- Crear esquema de inicio de sesión para la administración de OTP
- Configurar el servidor virtual de autenticación, autorización y auditoría
- Configurar servidores virtuales de equilibrio de carga o VPN
- Configurar etiqueta de directiva
- Crear esquema de inicio de sesión para el inicio de sesión del usuario final

Para obtener más información sobre la configuración, consulte Compatibilidad con OTP nativa.

Importante: Para la notificación push, los administradores deben configurar explícitamente lo siguiente:

- Crea un servicio push.
- Al crear un esquema de inicio de sesión para la administración de OTP, seleccione el esquema de inicio de sesión SingleAuthManageOTP.xml o equivalente según sea necesario.
- Al crear un esquema de inicio de sesión para el inicio de sesión del usuario final, seleccione el esquema de inicio de sesión de DualAuthOrPush.xml o equivalente según sea necesario.

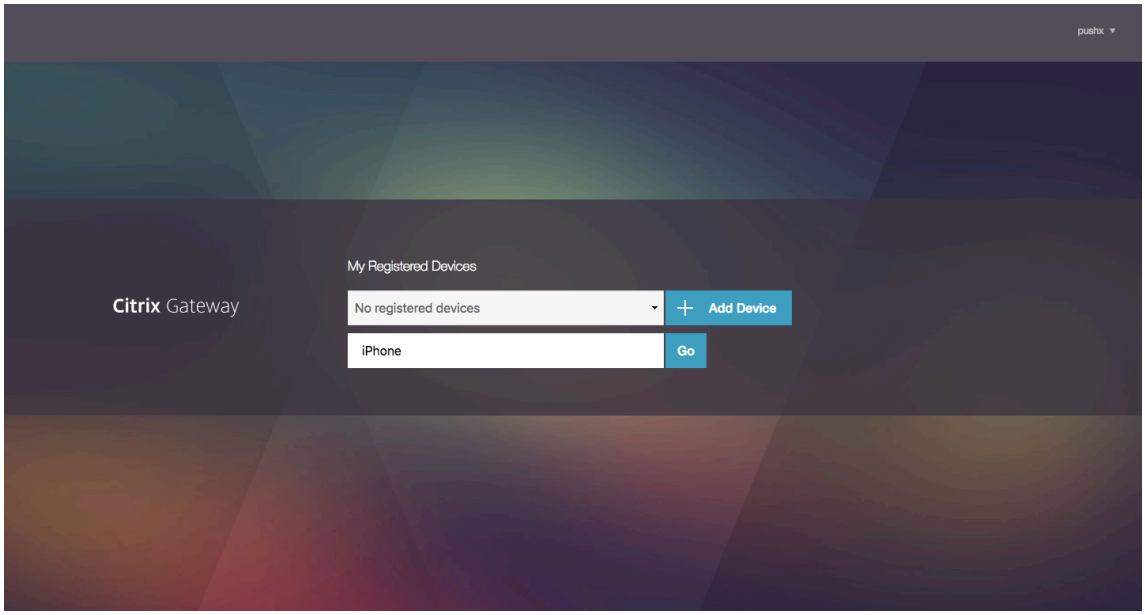
Registre su dispositivo con Citrix Gateway

Los usuarios deben registrar sus dispositivos en Citrix Gateway para utilizar la funcionalidad de notificaciones push.

1. En el explorador web, vaya al FQDN de Citrix Gateway y el sufijo **/manageotp** al FQDN.

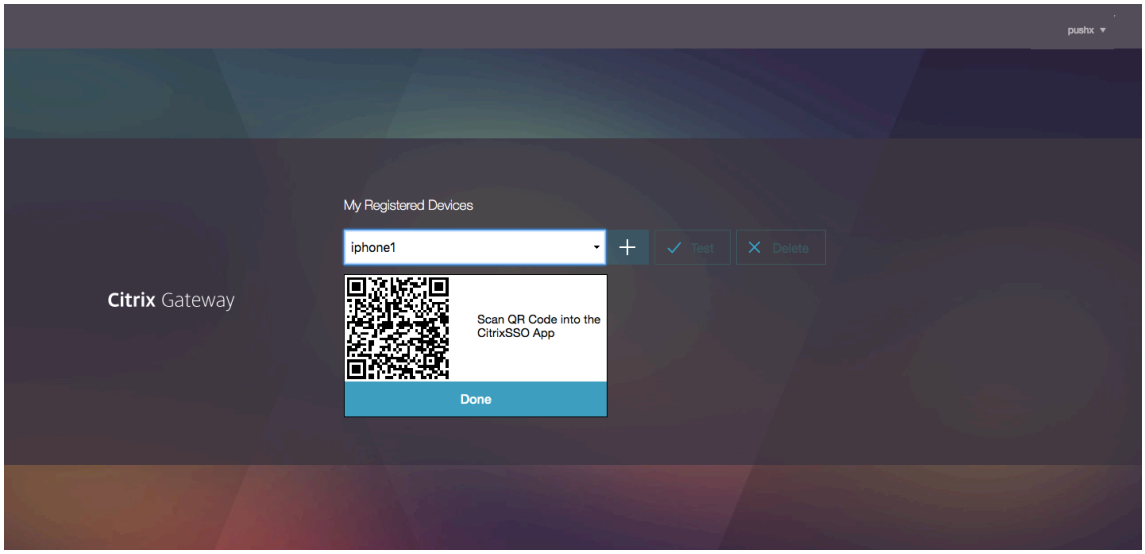
   Esto carga la página de autenticación.
   Ejemplo:https://gateway.company.com/manageotp

2. Inicie sesión con sus credenciales LDAP o los mecanismos de autenticación de dos factores adecuados, según sea necesario.



3. Haga clic en **Agregar dispositivo**.
4. Introduzca un nombre para el dispositivo y, a continuación, haga clic en **Ir**.

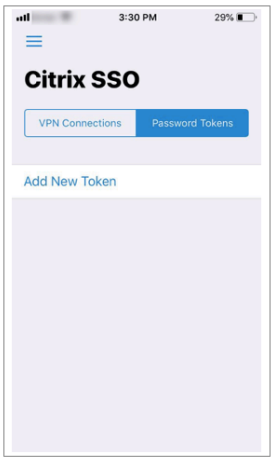
   Se muestra un código QR en la página del explorador de Citrix Gateway.

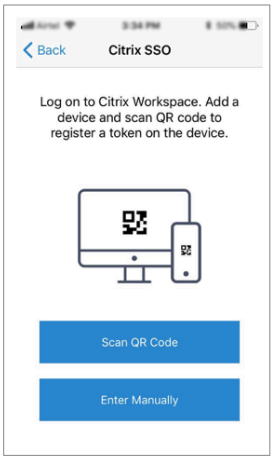


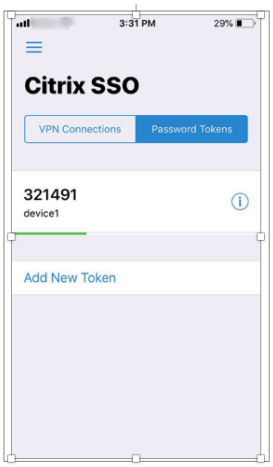
5. Escanee este código QR mediante la aplicación Citrix SSO desde el dispositivo que se va a registrar.

   Citrix SSO valida el código QR y, a continuación, se registra en la puerta de enlace para recibir notificaciones push. Si no hay errores en el proceso de registro, el token se agrega correctamente a la página de tokens de contraseña.

   > **Importante:**
   >
   > El inicio de sesión falla si introduce manualmente la clave secreta proporcionada en el código QR.







6. Si no hay dispositivos adicionales para agregar/administrar, cierre la sesión mediante la lista de la esquina superior derecha de la página.

Probar la autenticación de contraseña única

1. Para probar la OTP, haga clic en su dispositivo en la lista y, a continuación, haga clic en **Probar**.

2. Introduzca la OTP que ha recibido en su dispositivo y haga clic en **Ir**.

   Aparece el mensaje de verificación de OTP satisfactoria.

3. Cierre la sesión mediante la lista situada en la esquina superior derecha de la página.

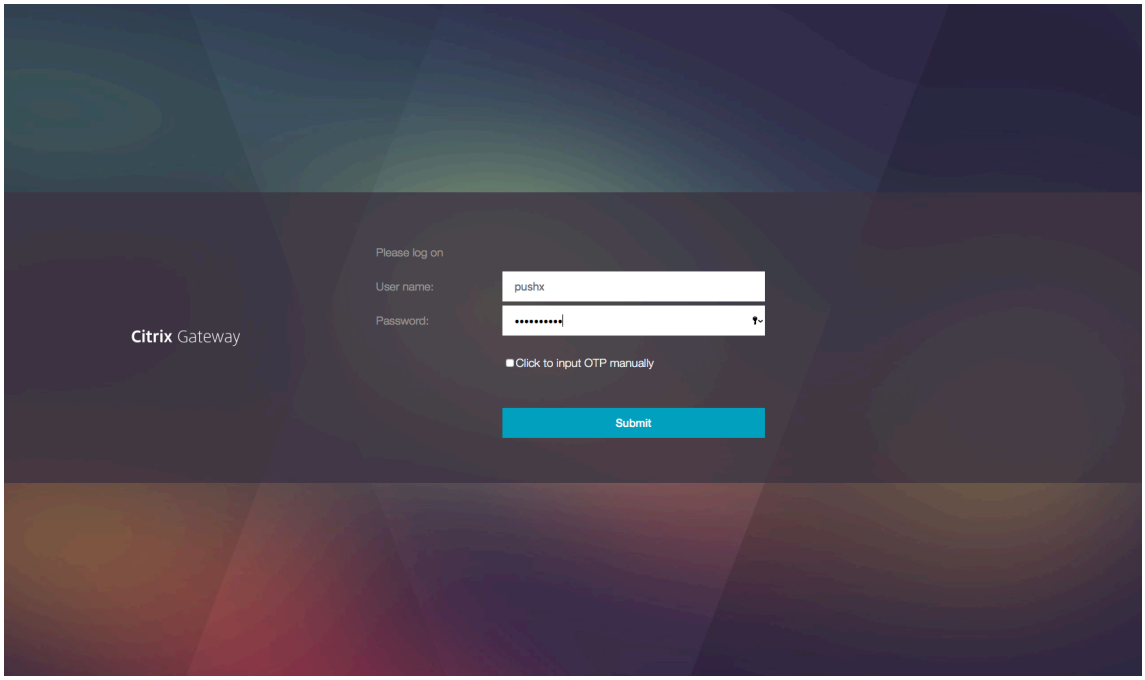
Nota: Puede utilizar el portal de administración de OTP en cualquier momento para probar la autenticación, eliminar dispositivos registrados o registrar más dispositivos.

Inicie sesión en Citrix Gateway

Después de registrar sus dispositivos en Citrix Gateway, los usuarios pueden utilizar la funcionalidad de notificaciones push para la autenticación.

1. Vaya a la página de autenticación de Citrix Gateway (por ejemplo: https://gateway.company.com)

   Se le pedirá que introduzca únicamente sus credenciales LDAP en función de la configuración del esquema de inicio de sesión.

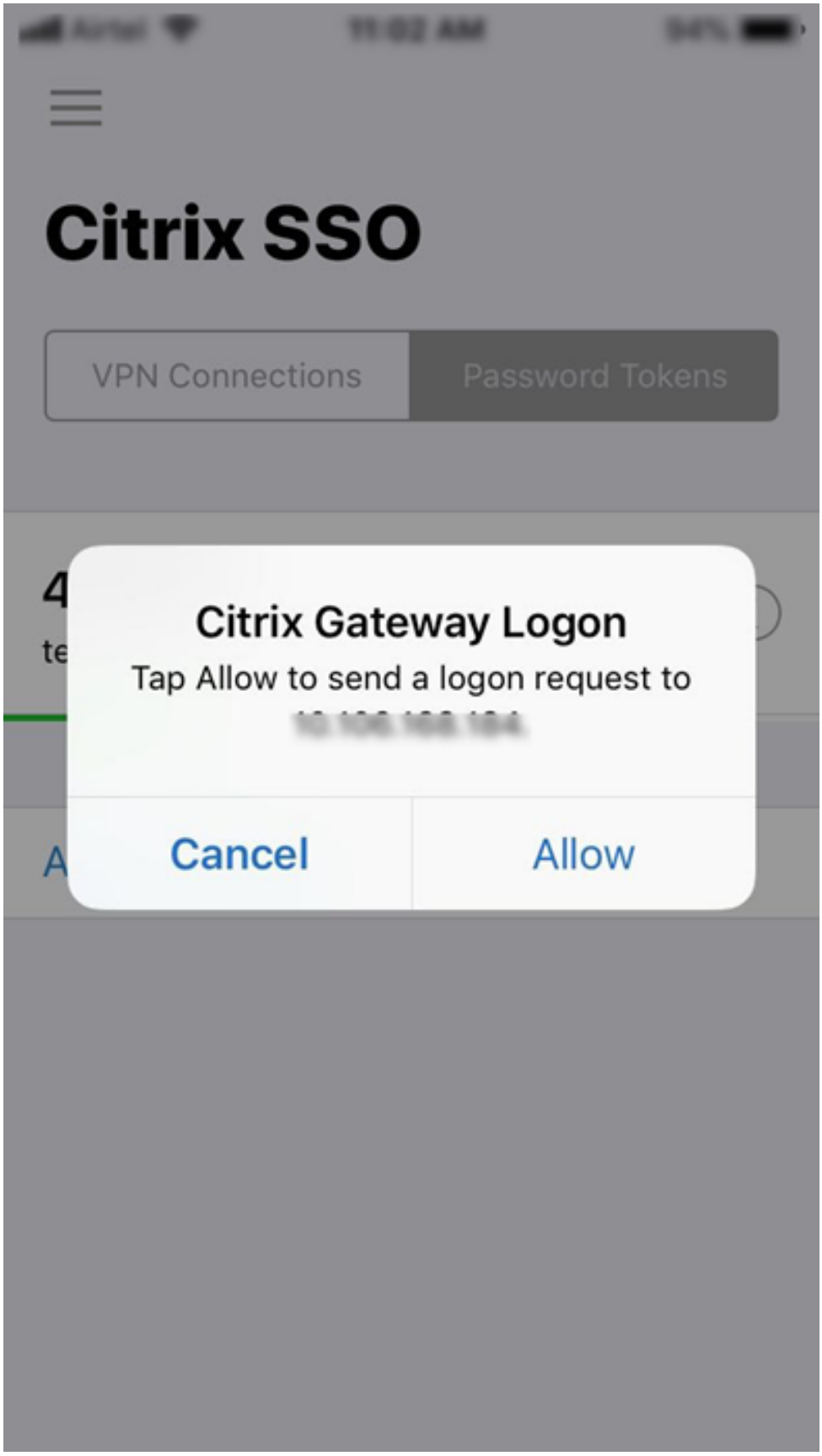


2. Introduzca su nombre de usuario y contraseña de LDAP y, a continuación, seleccione **Enviar**.

   Se envía una notificación al dispositivo registrado.

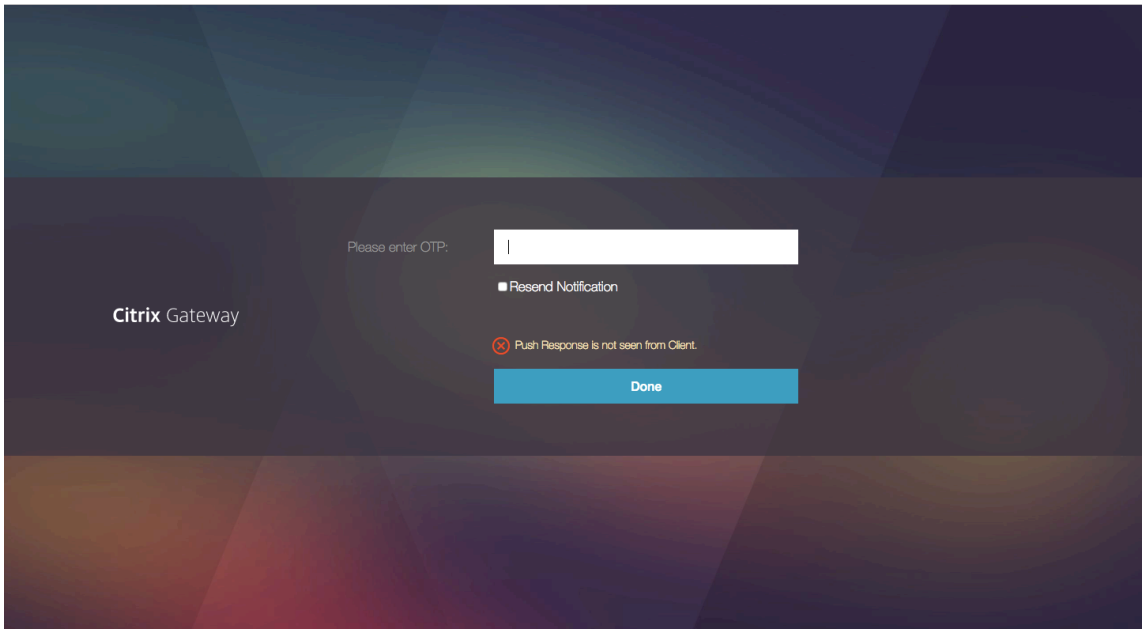
   Nota: Si quiere introducir la OTP manualmente, debe seleccionar **Haga clic** para introducir OTP manualmente e introducir la OTP en el campo **TOTP**.

3. Abra la aplicación Citrix SSO en el dispositivo registrado y toque **Permitir**.



Nota:

- En un dispositivo iOS, se le solicitará la identificación táctil/ID de cara/código de acceso como factor adicional de autenticación.
- El servidor de autenticación espera la respuesta de notificación del servidor push hasta que expire el período de tiempo de espera configurado. Tras el tiempo de espera, Citrix Gateway muestra la página de inicio de sesión. A continuación, los usuarios pueden introducir la OTP manualmente o hacer clic en **Reenviar notificación** para volver a recibir la notificación en el dispositivo registrado. Según la opción seleccionada, la puerta de enlace valida la OTP que ha introducido o vuelve a enviar la notificación en el dispositivo registrado.



- No se envía ninguna notificación a su dispositivo registrado en relación con un error de inicio de sesión.

Condiciones de fallo

- El registro del dispositivo puede fallar en los siguientes casos.
  - Es posible que el dispositivo del usuario final no confíe en el certificado del servidor.
  - El cliente no puede acceder a Citrix Gateway que se utiliza para registrarse en OTP.
- Las notificaciones pueden fallar en los siguientes casos.
  - El dispositivo del usuario no está conectado a Internet
  - Las notificaciones en el dispositivo del usuario están bloqueadas
  - El usuario no aprueba la notificación en el dispositivo

En estos casos, el servidor de autenticación espera hasta que caduque el período de tiempo de espera

configurado. Después del tiempo de espera, Citrix Gateway muestra una página de inicio de sesión con las opciones para introducir manualmente la OTP o volver a enviar la notificación en el dispositivo registrado. En función de la opción seleccionada, se realiza una validación adicional.

Registros de errores

A continuación se muestran los registros esperados cuando no se puede acceder al servicio push OTP.

- Error de notificación push cuando el dispositivo del usuario no está conectado a Internet - Push: no se pudo preparar la solicitud push para "`client name`" para el servicio Push.
- Registro de errores de registro de dispositivos - Push: No hay ningún dispositivo registrado para enviar solicitudes push a la nube para "`client name`".
- En caso de que el usuario no acepte el push - Push: No se ve la respuesta del cliente, para "`user name`", comprobando las opciones de reintento.

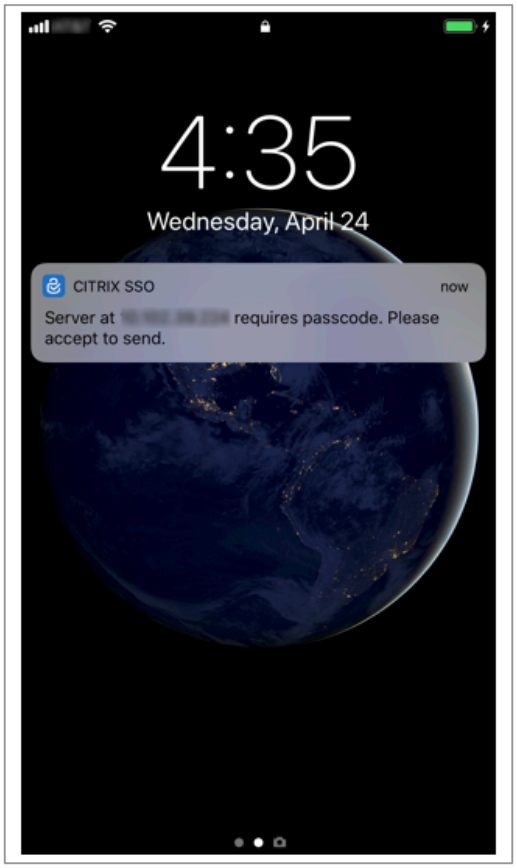
Comportamiento de la aplicación Citrix SSO en iOS: puntos a tener en cuenta

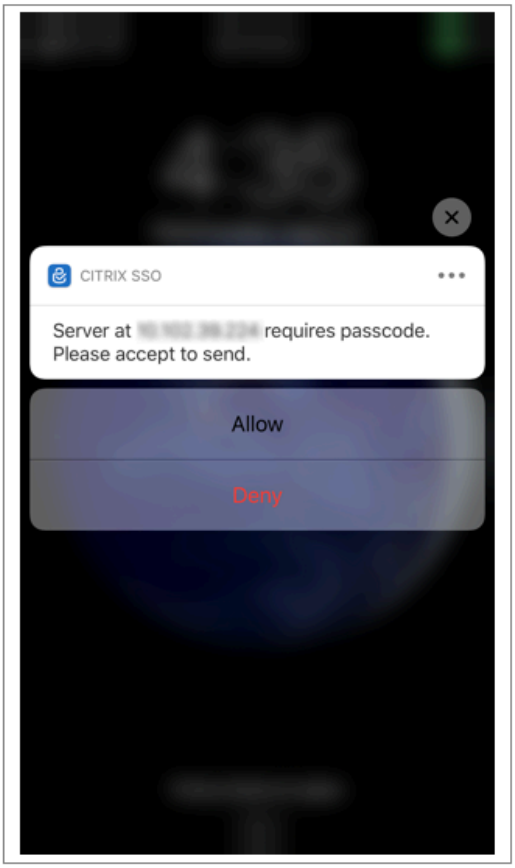
Accesos directos de notificación

La aplicación Citrix SSO iOS incluye soporte para notificaciones procesables para mejorar la experiencia del usuario. Una vez que se recibe una notificación en un dispositivo iOS, y si el dispositivo está bloqueado o la aplicación Citrix SSO no está en primer plano, los usuarios pueden usar los accesos directos integrados en la notificación para aprobar o denegar la solicitud de inicio de sesión.

Para acceder a los accesos directos de notificaciones, los usuarios deben forzar el toque (toque 3D) o presionar la notificación durante un tiempo prolongado en función del hardware del dispositivo. Al seleccionar la acción de acceso directo Permitir, se envía una solicitud de inicio de sesión a Citrix ADC. Según la configuración de la directiva de autenticación en el servidor virtual de autenticación, autorización y auditoría;

- La solicitud de inicio de sesión puede enviarse en segundo plano sin necesidad de iniciar la aplicación en primer plano ni de desbloquear el dispositivo.
- Es posible que la aplicación solicite ID de contacto, ID de rostro/código de acceso como factor adicional, en cuyo caso la aplicación se inicia en primer plano.



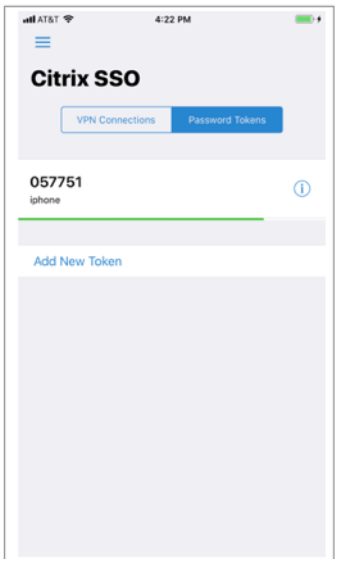


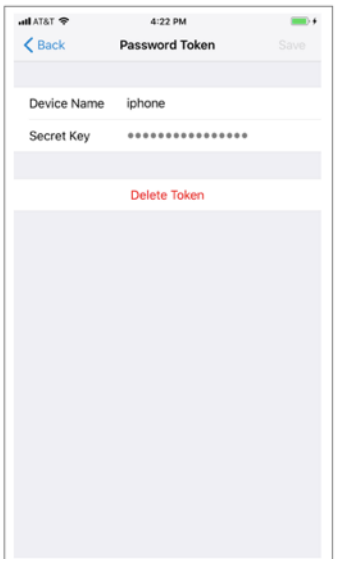
Eliminación de tokens de contraseña del Citrix SSO

1. Para eliminar un token de contraseña registrado para inserción en la aplicación Citrix SSO, los usuarios deben realizar los siguientes pasos:
2. Anular el registro (eliminar) del dispositivo iOS/Android en la puerta de enlace. Aparece el código QR para eliminar el registro del dispositivo.
3. Abra la aplicación Citrix SSO y pulse el botón de información del token de contraseña que quiere eliminar.
4. Presiona **Eliminar token** y escanea el código QR.

Nota:

- Si el código QR es válido, el token se quita correctamente de la aplicación Citrix SSO.
- Los usuarios pueden pulsar Forzar eliminación para eliminar un token de contraseña sin tener que escanear el código QR si el dispositivo ya se ha eliminado de la puerta de enlace. La eliminación forzada puede hacer que el dispositivo siga recibiendo notificaciones si el dispositivo no se ha quitado de Citrix Gateway.





Autenticación de OTP

March 9, 2022

La OTP de correo electrónico se presenta con Citrix ADC 12.1 compilación 51.x. El método OTP de correo electrónico le permite autenticarse con la contraseña de un solo uso (OTP) que se envía a la dirección de correo electrónico registrada. Cuando intenta autenticarse en cualquier servicio, el servidor envía una OTP a la dirección de correo electrónico registrada del usuario.

Para utilizar la función OTP de correo electrónico, primero debe registrar su ID de correo electrónico alternativo. Se necesita un registro de ID de correo electrónico alternativo para que la OTP se pueda enviar a ese ID de correo, ya que no podría acceder al ID de correo electrónico principal si hubiera un bloqueo de cuenta o en caso de que olvidara la contraseña de AD.

Puede utilizar la validación OTP de correo electrónico sin registro de ID de correo electrónico si ya ha proporcionado el ID de correo electrónico alternativo como parte de algún atributo de AD. Puede hacer referencia al mismo atributo en la acción de correo electrónico en lugar de especificar el ID de correo electrónico alternativo en la sección Dirección de correo electrónico.

Requisitos previos

Antes de configurar la función OTP de correo electrónico, revise los siguientes requisitos previos:

- Función Citrix ADC versión 12.1 compilación 51.28 y superior
- La función OTP de correo electrónico solo está disponible en el flujo de autenticación nFactor

- Para obtener más información, consulte https://support.citrix.com/pages/citrix-adc-authentication-how#nfactor
- Compatible con AAA-TM, Citrix Gateway (explorador, plug-in nativo y Receiver).

Configuración de Active Directory

- La versión admitida es el nivel de función de dominio de Active Directory 2016/2012 y 2008
- El nombre de usuario LDAPbind de Citrix ADC debe tener acceso de escritura a la ruta de AD del usuario

Servidor de correo

- Para que la solución OTP de correo electrónico funcione, asegúrese de que la autenticación basada en el inicio de sesión esté habilitada en el servidor SMTP. Citrix ADC solo admite la autenticación basada en AUTH LOGIN para que funcione la OTP de correo electrónico.
- Para asegurarse de que la autenticación basada en AUTH LOGIN esté habilitada, escriba el siguiente comando en el servidor SMTP. Si la autenticación basada en el inicio de sesión está habilitada, observará que el texto AUTH LOGIN aparece en **negrita** en la salida.

```
root@ns# telnet <IP address of the SMTP server><Port number of the server>
ehlo
root@ns# telnet 10.106.3.
Trying 10.106.
Connected to 10.106.
Escape character is '^]'.
220 E2K13.NSGSanity.com Microsoft ESMTP MAIL Service ready at Fri, 22 Nov
2019 16:24:17 +0530
ehlo
250-E2K13.NSGSanity.com Hello [10.221.
250-SIZE 37748736
250-PIPELINING
250-DSN
250-ENHANCEDSTATUSCODES
250-STARTTLS
250-X-ANONYMOUSTLS
250-AUTH LOGIN
250-X-EXPS GSSAPI NTLM
250-8BITMIME
250-BINARYMIME
250-CHUNKING
250 XRDST
For information on how to enable login based authentication, see
https://support.microfocus.com/kb/doc.php?id=7020367
```

Limitaciones

- Esta función solo se admite si el back-end de autenticación es LDAP.
- No se puede ver el ID de correo electrónico alternativo ya registrado.
- Solo el identificador de correo electrónico alternativo de la página de registro de KBA no se puede actualizar.

- La autenticación OTP de correo electrónico no puede ser el primer factor en el flujo de autenticación. Esto es por diseño para lograr una autenticación sólida.
- Si tanto el Id. de correo electrónico alternativo como el KBA se configuran con la misma acción de autenticación, el atributo debe ser el mismo para ambos.
- Para el complemento nativo y Receiver, el registro solo se admite a través de un navegador.

Configurar Active Directory

- La OTP de correo electrónico utiliza el atributo de Active Directory como almacenamiento de datos de usuario.
- Después de registrar el ID de correo electrónico alternativo, el ID de correo electrónico se envía al dispositivo Citrix ADC y el dispositivo lo almacena en el atributo KB configurado en el objeto de usuario de AD.
- El identificador de correo electrónico alternativo se cifra y se almacena en el atributo AD configurado.

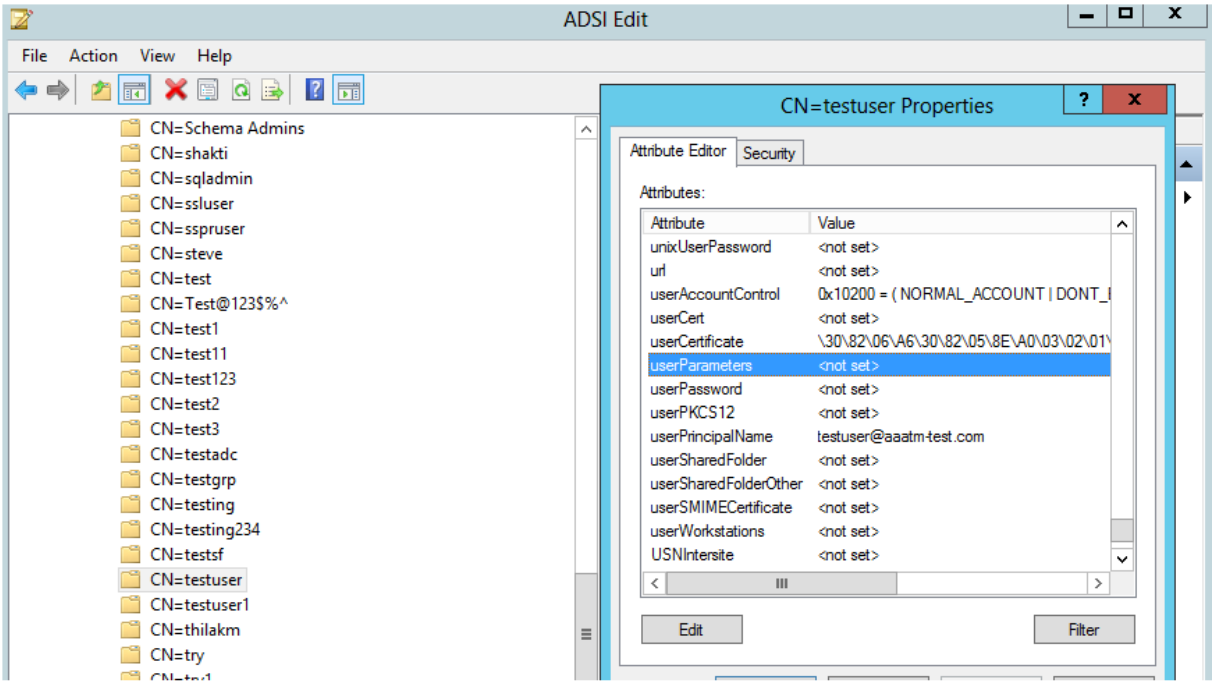
Al configurar un atributo de AD, tenga en cuenta lo siguiente:

- La longitud del nombre de atributo admitida debe tener al menos 128 caracteres.
- El tipo de atributo debe ser “DirectoryString”.
- Se puede usar el mismo atributo de AD para los datos de registro de OTP nativa y OTP de correo electrónico.
- El administrador de LDAP debe tener acceso de escritura al atributo de AD seleccionado.

Uso de atributos existentes

El atributo utilizado en este ejemplo es `Userparameters`. Como se trata de un atributo existente en el usuario de AD, no necesita realizar ningún cambio en el propio AD. Sin embargo, debe asegurarse de que el atributo no se está usando.

Para asegurarse de que el atributo no se utiliza, vaya a **ADSI** y seleccione usuario, haga clic con el botón derecho en el usuario y desplácese hacia abajo hasta la lista de atributos. Debe ver el valor de atributo de **userParameters** como **no establecido**. Esto indica que el atributo no se está usando en este momento.



Configurar OTP de correo electrónico

La solución OTP de correo electrónico consta de las dos partes siguientes:

- Registro por correo electrónico
- Validación de correo

Registro de ID de correo

Realice la siguiente configuración mediante la CLI después de que el esquema de registro de KBA se haya creado correctamente:

1. Enlace el tema del portal y el certificado a la VPN global.

```
bind authentication vserver authvs -portaltheme RfWebUI
bind vpn global -userDataEncryptionKey c1
<!--NeedCopy-->
```

> **Nota:**
>
> Se requiere un enlace de certificado anterior para cifrar los datos del usuario (KB Q&A e ID de correo alternativo registrado) almacenados en el atributo AD.

2. Cree una directiva de autenticación LDAP.


```
add authentication ldapAction ldap -serverIP 10.102.2.2 -
    serverPort 636 -ldapBase "dc=aaatm-test,dc=com" -ldapBindDn
    administrator@aaatm-test.com -ldapBindDnPassword freebsd -
    ldapLoginName samAccountName -secType SSL
add authentication Policy ldap -rule true -action ldap
<!--NeedCopy-->
```

3. Cree una directiva de autenticación LDAP para el registro de correo electrónico.

```
add authentication ldapAction ldap_email_registration -serverIP
    10.102.2.2 -serverPort 636 -ldapBase "dc=aaatm-test,dc=com" -
    ldapBindDn administrator@aaatm-test.com -ldapBindDnPassword
    freebsd -ldapLoginName samAccountName -secType SSL -KBAttribute
     userParameters -alternateEmailAttr userParameters
add authentication Policy ldap_email_registration -rule true -
    action ldap_email_registration
<!--NeedCopy-->
```

4. Cree un esquema de inicio de sesión de registro de correo electrónico y una etiqueta

```
add authentication loginSchema onlyEmailRegistration -
    authenticationSchema /nsconfig/loginschema/LoginSchema/
    AltEmailRegister.xml
add authentication policylabel email_Registration_factor -
    loginSchema onlyEmailRegistration
bind authentication policylabel email_Registration_factor -
    policyName ldap_email_registration -priority 1 -
    gotoPriorityExpression NEXT
<!--NeedCopy-->
```

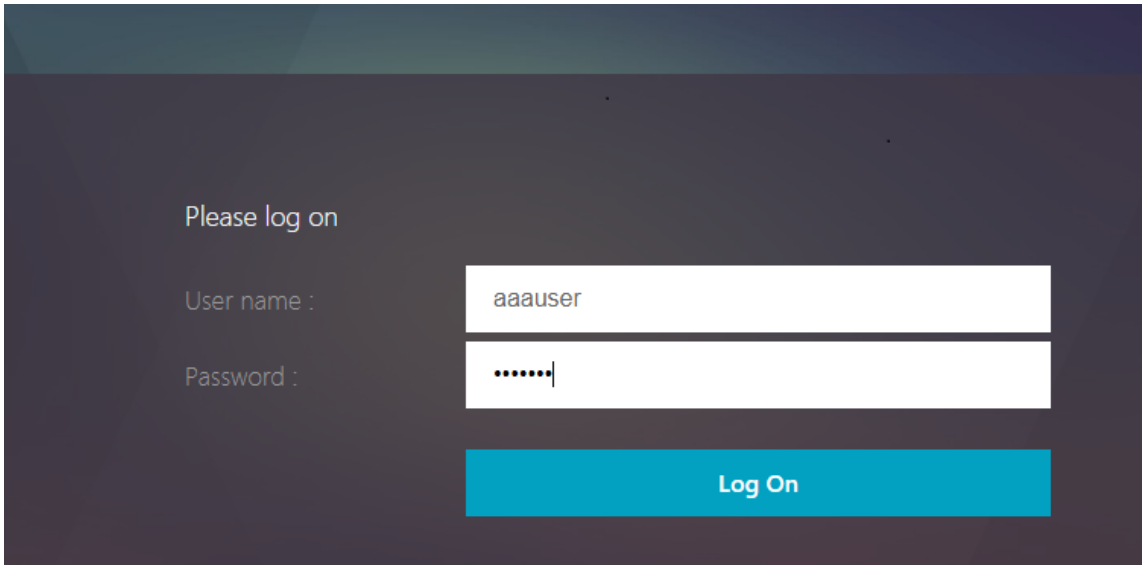
5. Enlazar la directiva de autenticación al servidor virtual de autenticación.

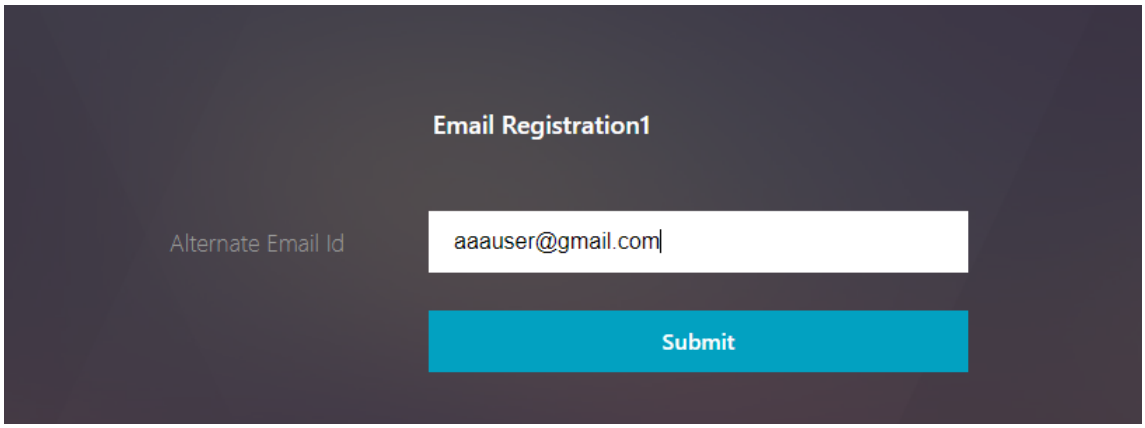
```
bind authentication vserver authvs  - policy ldap -priority 1 -
    nextFactor email_Registration_factor -gotoPriorityExpression
    NEXT
<!--NeedCopy-->
```

6. Una vez que haya configurado todos los pasos mencionados en las secciones anteriores, debe ver la siguiente pantalla GUI. Al acceder a través de la URL (por ejemplo,

https://lb1.server.com/), se le presenta una página de inicio de sesión inicial que solo requiere la credencial de inicio de sesión de LDAP seguida de una página de registro de correo electrónico alternativa.

Nota: El dominio https://lb1.server.com/ puede pertenecer a una puerta de enlace o a un servidor virtual de autenticación.





Nota:

- Puede usar el mismo esquema de autenticación tanto para el registro de KBA como para el registro de ID de correo electrónico.
- Al configurar el registro de KBA, puede seleccionar **Registrar correo electrónico alternativo** en la sección Registro de correo electrónico para registrar un ID de correo electrónico alternativo.

Validación de correo

Realice los siguientes pasos para la validación del correo electrónico.

1. Enlazar el tema del portal y el certificado a la VPN global

```
bind authentication vserver authvs -portaltheme RfWebUI
bind vpn global -userDataEncryptionKey c1
<!--NeedCopy-->
```

> **Nota:**
>
> Se requiere la vinculación del certificado anterior para descifrar los datos del usuario (preguntas y respuestas de la KB e ID de correo electrónico alternativo registrado) almacenados en el atributo AD.

2. Cree una directiva de autenticación LDAP. LDAP debe ser un factor anterior al factor de validación de correo electrónico porque necesita el ID de correo electrónico del usuario o el ID de correo electrónico alternativo para la validación OTP de correo electrónico.

```
add authentication ldapAction ldap1 -serverIP 10.102.2.2 -
    serverPort 636 -ldapBase "dc=aaatm-test,dc=com" -   ldapBindDn
    administrator@aaatm-test.com -ldapBindDnPassword freebsd -
    ldapLoginName samAccountName -secType SSL -KBAttribute
    userParameters -alternateEmailAttr userParameters
add authentication Policy ldap1 -rule true -action ldap1
<!--NeedCopy-->
```

3. Cree una directiva de autenticación de correo electrónico.

```
add authentication emailAction email -userName sqladmin@aaa.com -
    password freebsd-encrypted -encryptmethod ENCMTHD_3 -serverURL
    "smtps://10.2.3.3:25" -content "OTP is $code" -
    defaultAuthenticationGroup emailgrp -emailAddress "aaa.user.
    attribute("alternate_mail")"
add authentication Policy email -rule true  - action email
<!--NeedCopy-->
```

En el comando mencionado anteriormente, la **dirección de correo electrónico** es el usuario de ID de correo electrónico alternativo proporcionado durante el registro de KBA.

4. Cree una etiqueta de directiva de validación OTP de correo electrónico.

```
add authentication policylabel email_Validation_factor
```



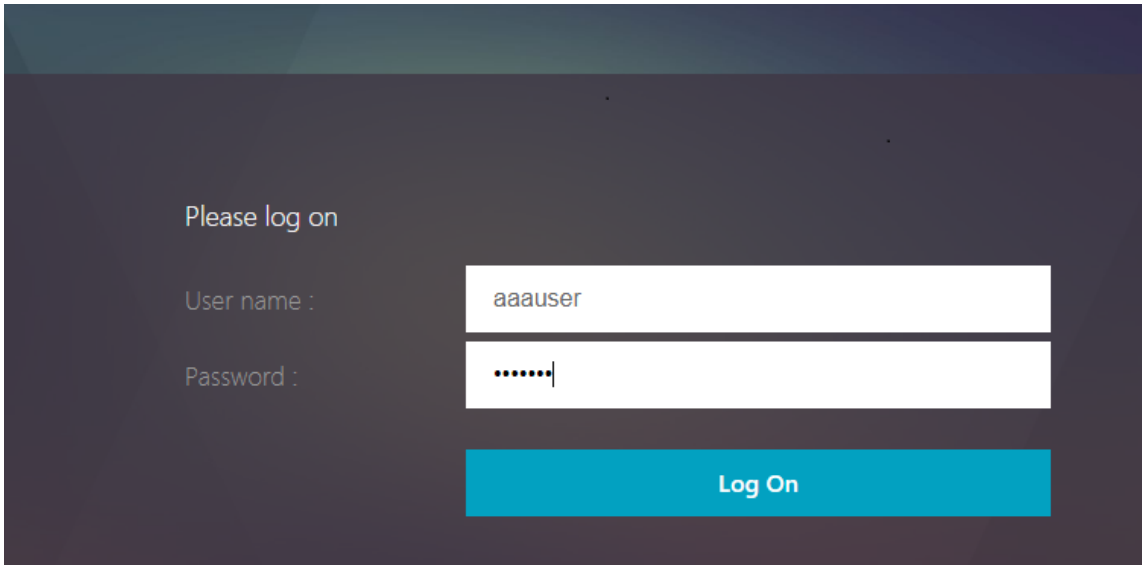
```
2 bind authentication policylabel email_Validation_factor -
    policyName email -priority 1 -gotoPriorityExpression NEXT
3 <!--NeedCopy-->
```

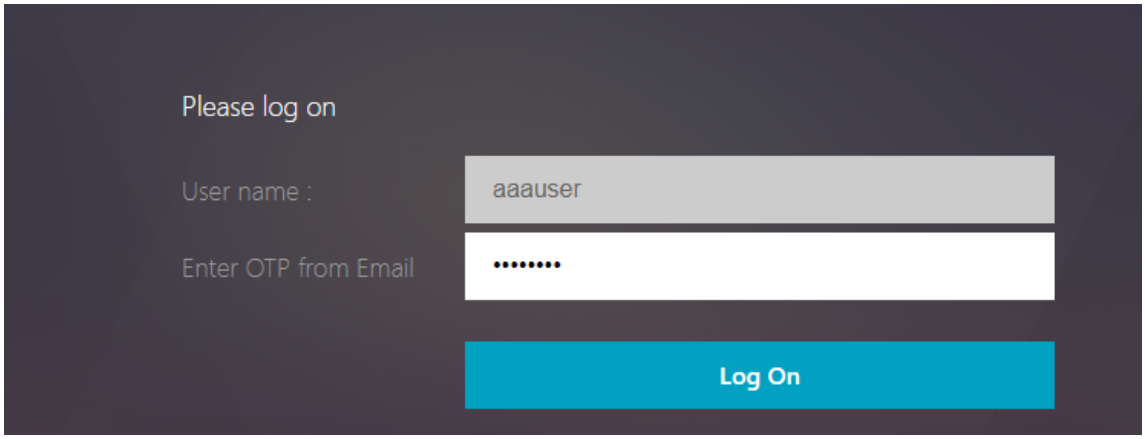
5. Enlazar la directiva de autenticación al servidor virtual de autenticación.

```
1 bind authentication vserver authvs - policy ldap1 -priority 1 -
    nextFactor email_Validation_factor -gotoPriorityExpression NEXT
2 <!--NeedCopy-->
```

6. Una vez que haya configurado todos los pasos mencionados en las secciones anteriores, debe ver la siguiente pantalla de GUI para la validación OTP de CORREO ELECTRÓNICO. Al acceder a través de la URL (por ejemplo, https://lb1.server.com/) se le presenta una página de inicio de sesión inicial que solo requiere la credencial de inicio de sesión de LDAP seguida de la página de validación de OTP de CORREO ELECTRÓNICO.

> **Nota:**
>
> En la directiva LDAP, es importante configurar `alternateEmailAttr` para poder consultar la identificación de correo electrónico del usuario desde el atributo AD.





Solución de problemas

Antes de analizar el registro, es mejor configurar el nivel de registro para depurar de la siguiente manera.

```
set syslogparams -loglevel DEBUG
<!--NeedCopy-->
```

Inscripción: escenario de éxito

Las siguientes entradas indican que el registro de usuario se ha realizado correctamente.

```
”ns_aaa_insert_hash_keyValue_entry key:kba_registered value:1”
Nov 14 23:35:51 <local0.debug> 10.102.229.76 11/14/2018:18:05:51 GMT
    0-PPE-1 : default SSLVPN Message 1588 0 :  ”
    ns_aaa_insert_hash_keyValue_entry key:alternate_mail value:
    eyJ2ZXJzaW9uIjoiMSIsICJraWQiOiIxbk1oWjN0T2NjLVVvZUx6NDRwZFhxdS01dTA9IiwgImtleS
    ==.oKmvOalaOJ3a9z7BcGCSegNPMw==”

<!--NeedCopy-->
```

Inscripción: escenario de fallo

En la página de inicio de sesión del usuario, aparece el siguiente mensaje de error: “No se puede completar la solicitud”. Esto indica que falta la clave de certificado que se vinculará a la VPN global para cifrar los datos del usuario.


```
Jul 31 08:51:46 <local0.info> 10.102.229.79 07/31/2020:03:21:4 6 GMT
    0-PPE-1 : default SSLVPN Message 696 0 :  "Encrypt UserData: No
    Encryption cert is bound to vpn global"
Jul 31 08:51:46 <local0.info> 10.102.229.79 07/31/2020:03:21:46 GMT  0-
    PPE-1 : default SSLVPN Message 697 0 :  "KBA Register: Alternate
    email id Encrypted blob length is ZERO aaauser"
<!--NeedCopy-->
```

Validación de correo electrónico: escenario exitoso

Las siguientes entradas indican que la validación OTP de correo electrónico se ha realizado correctamente.

```
"NFactor: Successfully completed email auth, nextfactor is pwd_reset"
<!--NeedCopy-->
```

Validación de correo electrónico: escenario de

En la página de inicio de sesión del usuario, se muestra el mensaje de error "No se puede completar su solicitud". Esto indica que la autenticación basada en el inicio de sesión no está habilitada en el servidor de correo electrónico y que lo mismo debe habilitarse.

```
" /home/build/rs_130_36_15_RTM/usr.src/netscaler/aaad/pocomail.cpp
    [100]: void ThreadWorker_SendMailJob(SMTPJob*) 0-215: [POCO][JobID:
    8]SMTP Configuration is Secure..
/home/build/rs_130_36_15_RTM/usr.src/netscaler/aaad/pocomail.cpp[108]:
    void ThreadWorker_SendMailJob(SMTPJob*) 0-215: [POCO][JobID: 8]
    First login succeeded
Wed Mar  4 17:16:28 2020
/home/build/rs_130_36_15_RTM/usr.src/netscaler/aaad/naaad.c[697]: main
    0-0: timer 2 firing...
/home/build/rs_130_36_15_RTM/usr.src/netscaler/aaad/pocomail.cpp[127]:
    void ThreadWorker_SendMailJob(SMTPJob*) 0-0: [POCO-ERROR][JobID: 8]
    Poco SMTP Mail Dispatch  Failed. SMTP TYPE:1, SMTPException:
    Exception occurs. SMTP Exception: The mail service does not support
    LOGIN authentication: 250-smtprelay.citrix.com Hello [10.9.154.239]
250-SIZE 62914560
250-PIPELINING
250-DSN
```



```
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-BINARYMIME
250 CHUNKING
<!--NeedCopy-->
```

Configuración re-Captcha para autenticación nFactor

June 2, 2022

Citrix Gateway admite una nueva acción de primera clase `captchaAction` que simplifica la configuración de Re-Captcha. Como re-Captcha es una acción de primera clase, puede ser un factor en sí mismo. Puede inyectar re-Captcha en cualquier parte del flujo de nFactor.

Anteriormente, tenías que escribir directivas WebAuth personalizadas con cambios en la RfWebUI también. Con la introducción de `captchaAction`, no tiene que modificar el JavaScript.

> **Importante:**
>
> Si se usa re-Captcha junto con los campos de nombre de usuario o contraseña en el esquema, el botón **Enviar** se inhabilita hasta que se cumpla con re-Captcha.

Configuración de re-Captcha

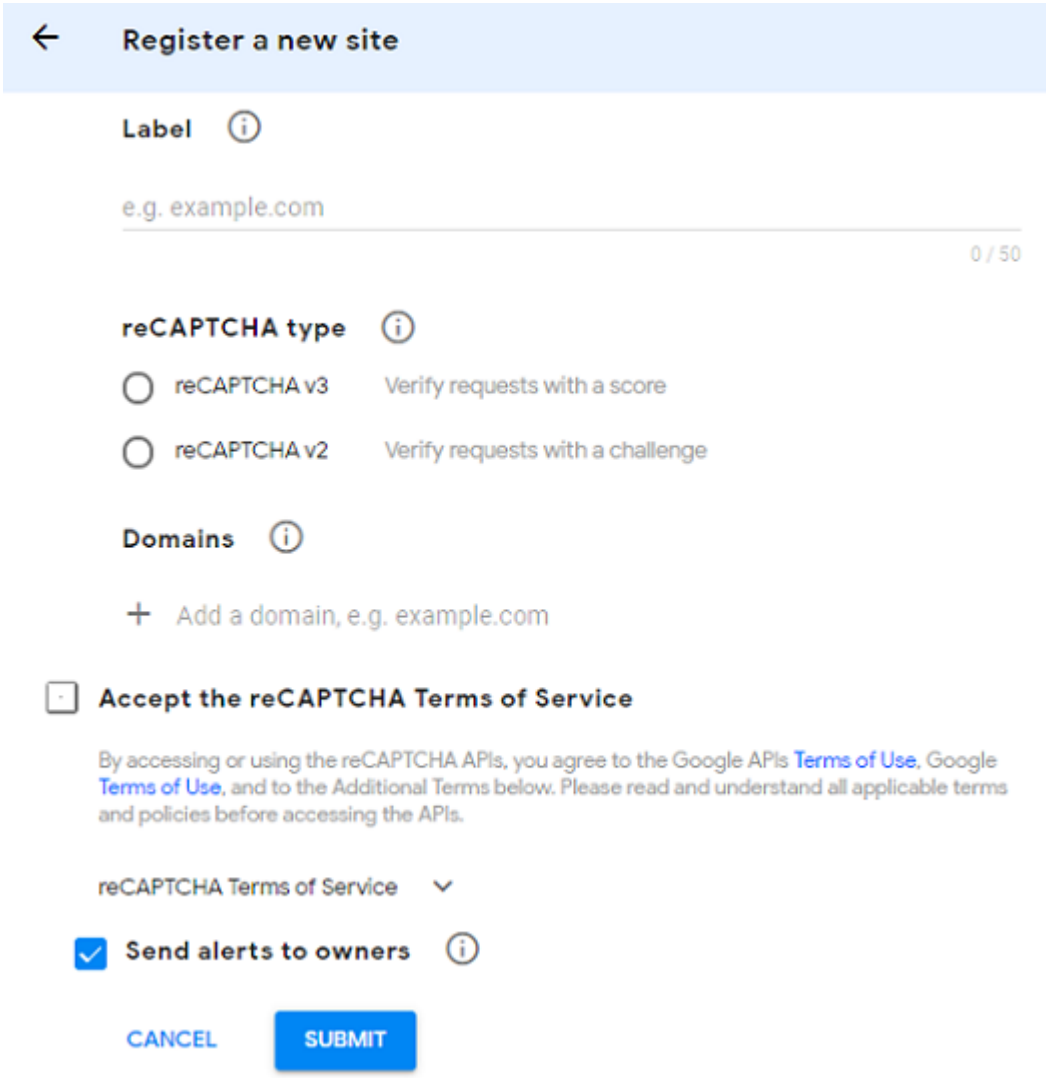
La configuración de re-Captcha consta de dos partes.

1. Configuración en Google para registrar re-Captcha.
2. Configuración en el dispositivo Citrix ADC para usar re-Captcha como parte del flujo de inicio de sesión.

Configuración de re-Captcha en Google

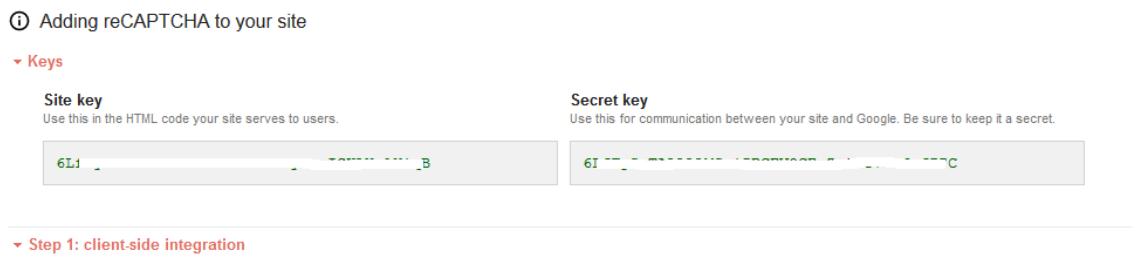
Registre un dominio para re-Captcha en https://www.google.com/recaptcha/admin#llist.

1. Al navegar a esta página, aparece la siguiente pantalla.



> **Nota**
>
> Utilice solo reCaptcha v2. Re-Captcha invisible aún está en Tech Preview.

2. Después de registrar un dominio, se muestran “SiteKey” y “SecretKey”.



> **Nota**
>
> Las teclas “SiteKey” y “SecretKey” aparecen atenuadas por motivos de seguridad. “Se-

> cretKey" debe mantenerse a salvo.

Configuración de re-Captcha en un dispositivo Citrix ADC

La configuración de re-Captcha en el dispositivo Citrix ADC se puede dividir en tres partes:

- Mostrar pantalla de re-Captcha
- Publicar la respuesta de re-Captcha en el servidor de Google
- La configuración LDAP es el segundo factor para el inicio de sesión del usuario (opcional)

Mostrar pantalla de re-Captcha

La personalización del formulario de inicio de sesión se realiza mediante el esquema de inicio de sesión SingleAuthCaptcha.xml. Esta personalización se especifica en el servidor virtual de autenticación y se envía a la interfaz de usuario para representar el formulario de inicio de sesión. El esquema de inicio de sesión integrado, SingleAuthCaptcha.xml, se encuentra en el directorio `/nsconfig/loginSchema/LoginSchema` del dispositivo Citrix ADC.

> **Importante**
>
> - El esquema de inicio de sesión de SingleAuthCaptcha.xml se puede usar cuando se configura LDAP como primer factor.
> - En función de su caso de uso y de los diferentes esquemas, puede modificar el esquema existente. Por ejemplo, si solo necesita el factor re-Captcha (sin nombre de usuario ni contraseña) o autenticación dual con re-Captcha.
> - Si se realizan modificaciones personalizadas o se cambia el nombre del archivo, Citrix recomienda copiar todos los loginSchemas del directorio `/nsconfig/loginschema/LoginSchema` al directorio principal, `/nsconfig/loginschema`.

Para configurar la visualización de re-Captcha mediante CLI

```
add authentication loginSchema singleauthcaptcha -authenticationSchema
    /nsconfig/loginschema/SingleAuthCaptcha.xml

add authentication loginSchemaPolicy singleauthcaptcha -rule true -
    action singleauthcaptcha

add authentication vserver auth SSL <IP> <Port>

add ssl certkey vserver-cert -cert <path-to-cert-file> -key <path-to-
    key-file>
```



```
8
9  bind ssl vserver auth -certkey vserver-cert
10
11 bind authentication vserver auth -policy singleauthcaptcha -priority 5
       -gotoPriorityExpression END
12 <!--NeedCopy-->
```

Publicar la respuesta de re-Captcha en el servidor de Google

Después de configurar el re-Captcha que debe mostrarse a los usuarios, los administradores agregan la configuración al servidor de Google para verificar la respuesta de re-Captcha del explorador.

Para verificar la respuesta de re-Captcha desde el explorador

```
1 add authentication captchaAction myrecaptcha -sitekey <sitekey-copied-
      from-google> -secretkey <secretkey-from-google>
2
3 add authentication policy myrecaptcha -rule true -action myrecaptcha
4
5 bind authentication vserver auth -policy myrecaptcha -priority 1
6 <!--NeedCopy-->
```

Los siguientes comandos son necesarios para configurar si se quiere la autenticación de AD. De lo contrario, puede ignorar este paso.

```
1 add authentication ldapAction ldap-new -serverIP x.x.x.x -serverPort
      636 -ldapBase "cn=users,dc=aaatm,dc=com" -ldapBindDn adminuser@aaatm
      .com -ldapBindDnPassword <password> -encrypted -encryptmethod
      ENCMTHD_3 -ldapLoginName sAMAccountName -groupAttrName memberof -
      subAttributeName CN -secType SSL -passwdChange ENABLED -
      defaultAuthenticationGroup ldapGroup
2
3 add authenticationpolicy ldap-new -rule true -action ldap-new
4 <!--NeedCopy-->
```

La configuración LDAP es el segundo factor para el inicio de sesión del usuario (opcional)

La autenticación LDAP ocurre después de volver a captcha, la agrega al segundo factor.


```
add authentication policylabel second-factor

bind authentication policylabel second-factor -policy ldap-new -
    priority 10

bind authentication vserver auth -policy myrecaptcha -priority 1 -
    nextFactor second-factor
<!--NeedCopy-->
```

El administrador debe agregar los servidores virtuales adecuados en función de si se utiliza el servidor virtual de equilibrio de carga o el dispositivo Citrix Gateway para el acceso. El administrador debe configurar el siguiente comando si se necesita un servidor virtual de equilibrio de carga:

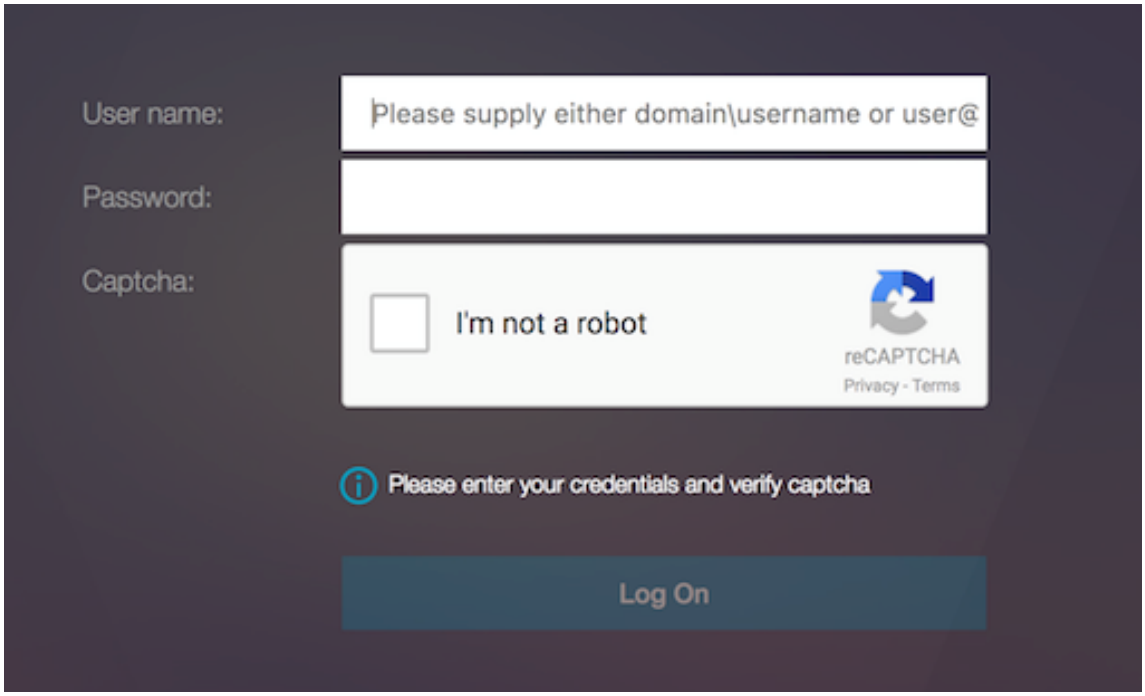
```
add lb vserver lbtest HTTP <IP> <Port> -authentication ON -
    authenticationHost nssp.aaatm.com
<!--NeedCopy-->
```

nssp.aaatm.com: Se resuelve en un servidor virtual de autenticación.

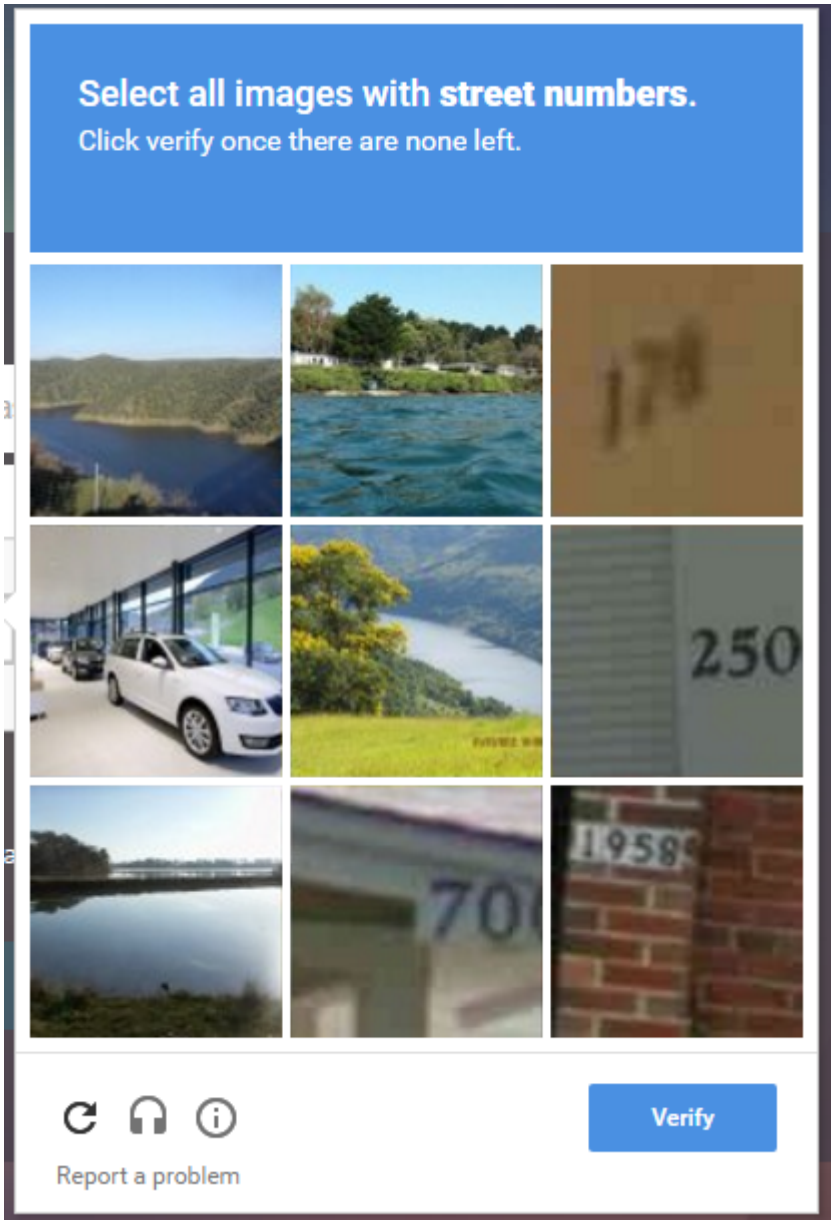
Validación de usuarios de re-Captcha

Una vez que haya configurado todos los pasos mencionados en las secciones anteriores, debe ver la siguiente interfaz de usuario.

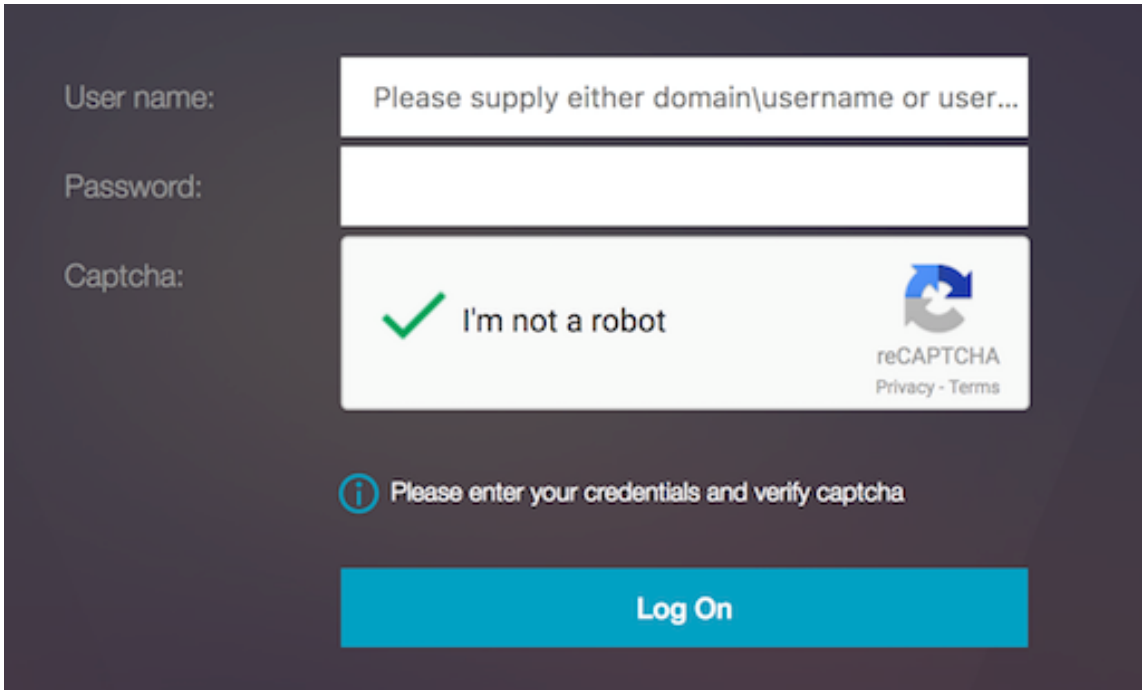
1. Una vez que el servidor virtual de autenticación carga la página de inicio de sesión, aparece la pantalla de inicio de sesión. El **inicio de sesión** está inhabilitado hasta que se complete Re-Captcha.



2. Selecciona la opción No soy un robot. Se muestra el widget re-Captcha.



3. Se le lleva a través de una serie de imágenes re-Captcha antes de que se muestre la página de finalización.
4. Introduzca las credenciales de AD, active la casilla de verificación **No soy un robot** y haga clic **en Iniciar sesión**. Si la autenticación se realiza correctamente, se le redirigirá al recurso deseado.



Notas:

- Si se usa re-Captcha con la autenticación de AD, el botón **Enviar** para las credenciales se inhabilita hasta que se complete re-Captcha.
- El re-Captcha ocurre en un factor propio. Por lo tanto, cualquier validación posterior como AD debe realizarse en re-Captcha. `nextfactor`

Configuración de autenticación, autorización y auditoría para protocolos de uso común

February 19, 2022

La configuración del dispositivo Citrix ADC para la autenticación, la autorización y la auditoría requiere una configuración específica en el dispositivo Citrix ADC y en los exploradores de los clientes. La configuración varía según el protocolo utilizado para la autenticación, autorización y auditoría.

Para obtener más información sobre la configuración del dispositivo Citrix ADC para la autenticación Kerberos, consulte Gestión de la autenticación, autorización y auditoría con Kerberos/NTLM.

Gestión de la autenticación, autorización y auditoría con Kerberos/NTLM

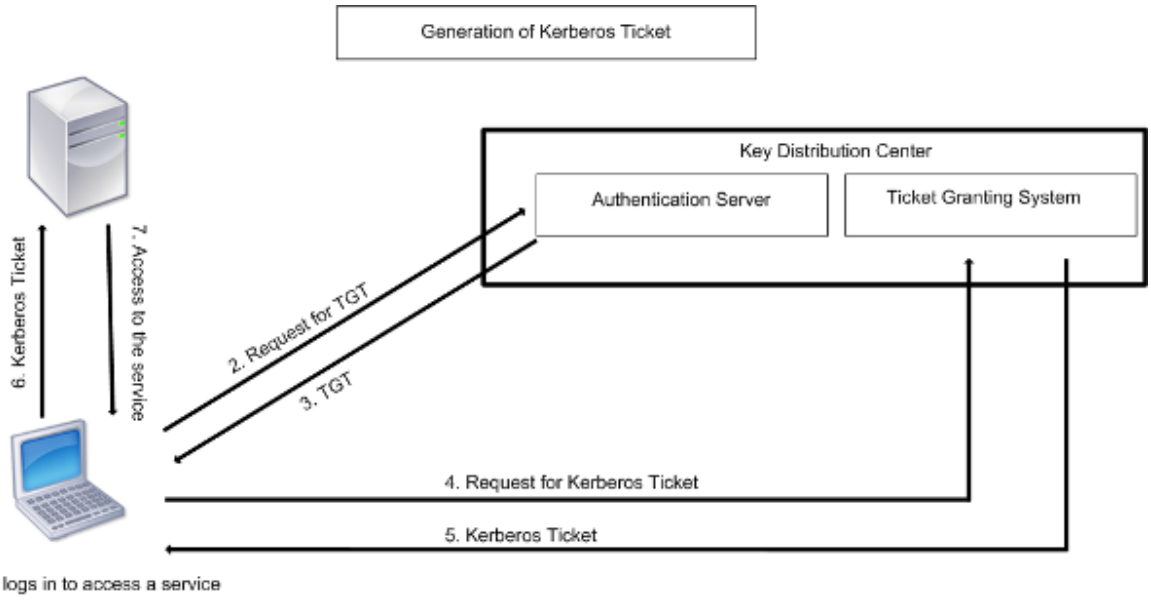
August 20, 2021

Kerberos, un protocolo de autenticación de red de equipos, proporciona una comunicación segura a través de Internet. Diseñado principalmente para aplicaciones cliente-servidor, proporciona una autenticación mutua mediante la cual el cliente y el servidor pueden garantizar la autenticidad del otro. Kerberos utiliza un tercero de confianza, denominado Centro de distribución de claves (KDC). Un KDC consta de un servidor de autenticación (AS), que autentica a un usuario, y un servidor de concesión de tíquets (TGS).

Cada entidad de la red (cliente o servidor) tiene una clave secreta que solo es conocida por sí misma y por el KDC. El conocimiento de esta clave implica la autenticidad de la entidad. Para la comunicación entre dos entidades de la red, el KDC genera una clave de sesión, denominada tíquet Kerberos o tíquet de servicio. El cliente realiza una solicitud al AS para obtener credenciales para un servidor específico. A continuación, el cliente recibe un tíquet, denominado Tíquet de concesión de tíquets (TGT). A continuación, el cliente se pone en contacto con el TGS, mediante el TGT que recibió del AS para demostrar su identidad, y solicita un servicio. Si el cliente puede usar el servicio, el TGS emite un tíquet Kerberos al cliente. A continuación, el cliente se pone en contacto con el servidor que aloja el servicio (denominado servidor de servicio), mediante el tíquet Kerberos para demostrar que está autorizado a recibir el servicio. El tíquet Kerberos tiene una vida útil configurable. El cliente se autentica con el AS solo una vez. Si se pone en contacto con el servidor físico varias veces, reutiliza el tíquet AS.

La siguiente ilustración muestra el funcionamiento básico del protocolo Kerberos.

Ilustración 1. **Funcionamiento de Kerberos**



La autenticación Kerberos tiene las siguientes ventajas:

- Autenticación más rápida. Cuando un servidor físico obtiene un tíquet Kerberos de un cliente, el servidor tiene suficiente información para autenticar el cliente directamente. No tiene que ponerse en contacto con un Controller de dominio para la autenticación del cliente y, por lo

tanto, el proceso de autenticación es más rápido.

- Autenticación mutua. Cuando el KDC emite un tíquet Kerberos a un cliente y el cliente utiliza el tíquet para acceder a un servicio, solo los servidores autenticados pueden descifrar el tíquet Kerberos. Si el servidor virtual del dispositivo Citrix ADC puede descifrar el tíquet Kerberos, puede concluir que tanto el servidor virtual como el cliente están autenticados. Por lo tanto, la autenticación del servidor ocurre junto con la autenticación del cliente.
- Inicio de sesión único entre Windows y otros sistemas operativos compatibles con Kerberos.

La autenticación Kerberos puede tener las siguientes desventajas:

- Kerberos tiene requisitos de tiempo estrictos; los relojes de los hosts involucrados deben sincronizarse con el reloj del servidor Kerberos para asegurarse de que la autenticación no falla. Puede mitigar esta desventaja mediante el uso de los daemons del Protocolo de hora de red para mantener sincronizados los relojes del host. Los tíquets Kerberos tienen un período de disponibilidad, que puede configurar.
- Kerberos necesita que el servidor central esté disponible continuamente. Cuando el servidor Kerberos está inactivo, nadie puede iniciar sesión. Puede mitigar este riesgo mediante el uso de varios servidores Kerberos y mecanismos de autenticación de reserva.
- Dado que toda la autenticación está controlada por un KDC centralizado, cualquier compromiso en esta infraestructura, como la contraseña del usuario para una estación de trabajo local que se está robando, puede permitir que un atacante suplante a cualquier usuario. Puede mitigar este riesgo hasta cierto punto mediante solo un equipo de escritorio o portátil en el que confíe, o aplicando la autenticación previa mediante un token de hardware.

Para utilizar la autenticación Kerberos, debe configurarla en el dispositivo Citrix ADC y en cada cliente.

Optimización de la autenticación Kerberos en la autenticación, autorización y auditoría

El dispositivo Citrix ADC optimiza y mejora el rendimiento del sistema mientras que la autenticación Kerberos. El demonio de autenticación, autorización y auditoría recuerda la solicitud Kerberos pendiente para el mismo usuario para evitar la carga en el Centro de distribución de claves (KDC), lo que evitará solicitudes duplicadas.

Cómo Citrix ADC implementa Kerberos para la autenticación de clientes

August 20, 2021

> **Importante**
>
> La autenticación Kerberos/NTLM solo se admite en la versión NetScaler 9.3 nCore o posterior, y

> solo se puede utilizar para la autenticación, autorización y auditoría de servidores virtuales de administración de tráfico.

Citrix ADC maneja los componentes involucrados en la autenticación Kerberos de la siguiente manera:

Centro de distribución de claves (KDC)

En Windows 2000 Server o versiones posteriores, el controlador de dominio y el KDC forman parte de Windows Server. Si Windows Server está UP y en ejecución, indica que el controlador de dominio y el KDC están configurados. El KDC es también el servidor de Active Directory.

> **Nota**
>
> Todas las interacciones Kerberos se validan con el controlador de dominio Kerberos de Windows.

Servicio de autenticación y negociación de protocolos

Un dispositivo Citrix ADC admite la autenticación Kerberos en los servidores virtuales de autenticación de administración de tráfico, autorización y auditoría. Si falla la autenticación Kerberos, Citrix ADC utiliza la autenticación NTLM.

De forma predeterminada, Windows 2000 Server y versiones posteriores de Windows Server utilizan Kerberos para la autenticación, la autorización y la auditoría. Si crea una directiva de autenticación con NEGOCIATE como tipo de autenticación, Citrix ADC intenta utilizar el protocolo Kerberos para la autenticación, autorización y auditoría y, si el explorador del cliente no recibe un tíquet Kerberos, Citrix ADC utiliza la autenticación NTLM. Este proceso se conoce como negociación.

El cliente puede no recibir un tíquet Kerberos en cualquiera de los siguientes casos:

- Kerberos no es compatible con el cliente.
- Kerberos no está habilitado en el cliente.
- El cliente está en un dominio distinto del KDC.
- El directorio de acceso del KDC no es accesible para el cliente.

Para la autenticación Kerberos/NTLM, Citrix ADC no utiliza los datos que están presentes localmente en el dispositivo Citrix ADC.

Autorización

El servidor virtual de administración de tráfico puede ser un servidor virtual de equilibrio de carga o un servidor virtual de conmutación de contenido.

Auditorías

El dispositivo Citrix ADC admite la auditoría de la autenticación Kerberos con el siguiente registro de auditoría:

- Seguimiento completo de auditoría de la actividad de usuario final de administración de tráfico
- Registro de SYSLOG y TCP de alto rendimiento
- Seguimiento completo de auditoría de los administradores del sistema
- Todos los eventos del sistema
- Formato de registro que permite ejecutar scripts

Entorno soportado

La autenticación Kerberos no necesita ningún entorno específico en Citrix ADC. El cliente (explorador) debe proporcionar soporte para la autenticación Kerberos.

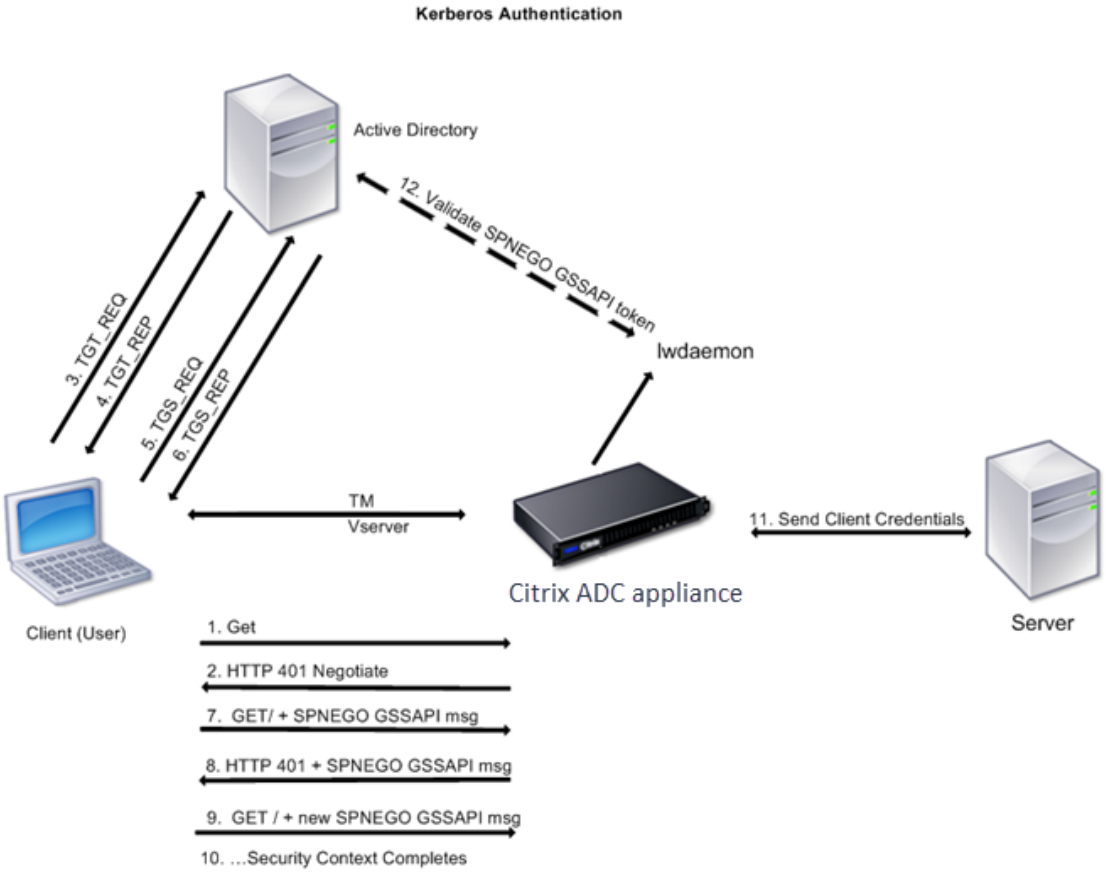
Alta disponibilidad

En una configuración de alta disponibilidad, solo el dispositivo Citrix ADC activo se une al dominio. En caso de una conmutación por error, el demonio Citrix ADC lwagent une el dispositivo Citrix ADC secundario al dominio. No se requiere ninguna configuración específica para esta funcionalidad.

Proceso de autenticación Kerberos

La siguiente ilustración muestra un proceso típico para la autenticación Kerberos en el entorno Citrix ADC.

Ilustración 1. Proceso de autenticación Kerberos en Citrix ADC



La autenticación Kerberos se produce en las etapas siguientes:

El cliente se autentica en el KDC

1. El dispositivo Citrix ADC recibe una solicitud de un cliente.
2. El servidor virtual de administración del tráfico (equilibrio de carga o conmutación de contenido) del dispositivo Citrix ADC envía un desafío al cliente.
3. Para responder al desafío, el cliente obtiene un tíquet Kerberos.
   - El cliente envía al servidor de autenticación del KDC una solicitud de un tíquet de concesión de tíquets (TGT) y recibe el TGT. (Consulte 3, 4 en la ilustración, Proceso de autenticación Kerberos.)
   - El cliente envía el TGT al servidor de concesión de tíquets del KDC y recibe un tíquet Kerberos. (Consulte 5, 6 en la ilustración, Proceso de autenticación Kerberos.)

> **Nota**
>
> El proceso de autenticación anterior no es necesario si el cliente ya tiene un tíquet Kerberos cuya vida útil no ha expirado. Además, los clientes como Servicios web, .NET o J2EE, que admiten SPNEGO, obtienen un tíquet Kerberos para el servidor de destino, crean un token SPNEGO e insertan el token en el encabezado HTTP cuando envían una solicitud HTTP. No pasan por el

> proceso de autenticación del cliente.

El cliente solicita un servicio.

1. El cliente envía el tíquet Kerberos que contiene el token SPNEGO y la solicitud HTTP al servidor virtual de administración de tráfico en Citrix ADC. El token SPNEGO tiene los datos GSSAPI necesarios.
2. El dispositivo Citrix ADC establece un contexto de seguridad entre el cliente y el dispositivo Citrix ADC. Si Citrix ADC no puede aceptar los datos proporcionados en el tíquet Kerberos, se le pedirá al cliente que obtenga otro tíquet. Este ciclo se repite hasta que los datos GSSAPI sean aceptables y se establezca el contexto de seguridad. El servidor virtual de administración de tráfico en Citrix ADC actúa como un proxy HTTP entre el cliente y el servidor físico.

El**dispositivo Citrix ADC completa la autenticación.**

1. Una vez completado el contexto de seguridad, el servidor virtual de administración de tráfico valida el token SPNEGO.
2. Desde el token SPNEGO válido, el servidor virtual extrae el ID de usuario y las credenciales de GSS, y las pasa al demonio de autenticación.
3. Una autenticación correcta completa la autenticación Kerberos.

Configuración de la autenticación kerberos en el dispositivo Citrix ADC

December 7, 2021

En este tema se proporcionan los pasos detallados para configurar la autenticación Kerberos en el dispositivo Citrix ADC mediante la CLI y la GUI.

Configuración de la autenticación Kerberos en la CLI

1. Habilite la función de autenticación, autorización y auditoría para garantizar la autenticación del tráfico en el dispositivo.

   ns-cli-prompt> **enable ns feature** AAA

2. Agregue el archivo keytab al dispositivo Citrix ADC. Se necesita un archivo keytab para descifrar el secreto recibido del cliente durante la autenticación Kerberos. Un único archivo keytab contiene detalles de autenticación para todos los servicios que están enlazados al servidor virtual de administración de tráfico en el dispositivo Citrix ADC.

   Primero genere el archivo keytab en el servidor de Active Directory y, a continuación, transfiéralo al dispositivo Citrix ADC.

- Inicie sesión en el servidor de Active Directory y agregue un usuario para la autenticación Kerberos mediante el siguiente comando.

```
net user <username> <password> /add
```

> **Nota**
>
> En la sección **Propiedades del usuario**, asegúrese de que la opción “Cambiar contraseña en el próximo inicio de sesión” no esté seleccionada y que la opción “La contraseña no caduca” esté seleccionada.

- Asigne el servicio HTTP al usuario anterior y exporte el archivo keytab. Por ejemplo, ejecute el siguiente comando en el servidor de Active Directory:

```
ktpass /out keytabfile /princ HTTP/owa.newacp.com@NEWACP.COM
   /pass <user password> /mapuser newacp\\dummy /ptype KRB5\
   _NT\_PRINCIPAL
```

> **Nota**
>
> Puede asignar más de un servicio si se requiere autenticación para más de un servicio. Si quiere asignar más servicios, repita el comando anterior para cada servicio. Puede dar el mismo nombre o nombres diferentes para el archivo de salida.

- Transfiera el archivo keytab al dispositivo Citrix ADC mediante el comando **ftp** de unix o cualquier otra utilidad de transferencia de archivos de su elección.

3. El dispositivo Citrix ADC debe obtener la dirección IP del controlador de dominio del nombre de dominio completo (FQDN). Por lo tanto, Citrix recomienda configurar Citrix ADC con un servidor DNS.

   ns-cli-prompt> **add dns nameserver** <ip-address>

   > **Nota**
   >
   > Como alternativa, puede agregar entradas de host estáticas o utilizar cualquier otro medio para que el dispositivo Citrix ADC pueda resolver el nombre FQDN del controlador de dominio en una dirección IP.

4. Configure la acción de autenticación y, a continuación, asociarla a una directiva de autenticación.

   - Configure la acción de negociación.

     ns-cli-prompt> **add authentication negotiateAction** <name> -domain <domain name> -domainUser <domain user name> -domainUserPasswd <domain user password> -

defaultAuthenticationGroup <default authentication group> -keytab <string> -NTLMPath <string>

Nota: Para la configuración de usuario de dominio y nombre de dominio, vaya al cliente y utilice el comando klist como se muestra en el siguiente ejemplo:

Cliente: nombre de usuario @ AAA.LOCAL

Servidor: http/onPrem_IDP.AAA.local @ AAA.LOCAL

agregar autenticación NegotiateAction <name>- dominio - Usuario de dominio <HTTP/onprem_idp.aaa.local>

- Configure la directiva de negociación y asocie la acción de negociación a esta directiva.

  ns-cli-prompt> **add authentication negotiatePolicy** <name> <rule> <reqAction>

5. Cree un servidor virtual de autenticación y asocie la directiva de negociación con él.
   - Cree un servidor virtual de autenticación.

     ns-cli-prompt> **add authentication vserver** <name> SSL <ipAuthVserver> 443 -authenticationDomain <domainName>
   - Enlace la directiva de negociación al servidor virtual de autenticación.

     ns-cli-prompt> **bind authentication vserver** <name> -policy <negotiatePolicyName>
6. Asocie el servidor virtual de autenticación con el servidor virtual de administración del tráfico (equilibrio de carga o conmutación de contenido).

   ns-cli-prompt> **set lb vserver** <name> -authn401 ON -authnVsName <string>

   > **Nota**
   >
   > También se pueden realizar configuraciones similares en el servidor virtual de conmutación de contenido.
7. Verifique las configuraciones haciendo lo siguiente:
   - Acceda al servidor virtual de administración de tráfico mediante el FQDN. Por ejemplo, Sample
   - Ver los detalles de la sesión en la CLI.

     ns-cli-prompt> **show aaa session**

Configuración de la autenticación Kerberos en la GUI

1. Habilite la función de autenticación, autorización y auditoría.

   Vaya a **Sistema** > **Configuración**, haga clic en **Configurar funciones básicas** y habilite la función de autenticación, autorización y auditoría.

2. Agregue el archivo keytab como se detalla en el paso 2 del procedimiento CLI mencionado anteriormente.
3. Agrega un servidor DNS.

   Vaya a **Administración del tráfico > DNS > Servidores**de nombres y especifique la dirección IP del servidor DNS.
4. Configure la acción y la directiva **Negociar**.

   Vaya a **Seguridad > AAA - Tráfico de aplicaciones > Directivas > Autenticación > Directivas avanzadas**> Directiva y cree una directiva con **Negociar** como tipo de acción. Haga clic en **AGREGAR** para crear un nuevo servidor de negociación de autenticación o haga clic en **Modificar** para configurar los detalles existentes.
5. Enlace la directiva de negociación al servidor virtual de autenticación.

   Vaya a **Seguridad > AAA - Tráfico de aplicaciones > Servidores virtuales**y asocie la directiva **Negotiate** con el servidor virtual de autenticación.
6. Asocie el servidor virtual de autenticación con el servidor virtual de administración del tráfico (equilibrio de carga o conmutación de contenido).

   Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**y especifique la configuración de autenticación relevante.

   > **Nota**
   >
   > También se pueden realizar configuraciones similares en el servidor virtual de conmutación de contenido.
7. Verifique las configuraciones como se detalla en el paso 7 del procedimiento CLI mencionado anteriormente.

Configurar la autenticación kerberos en un cliente

January 12, 2021

La compatibilidad con Kerberos debe configurarse en el explorador para usar Kerberos para la autenticación. Puede utilizar cualquier explorador compatible con Kerberos. Siga las instrucciones para configurar el soporte Kerberos en Internet Explorer y Mozilla Firefox. Para otros exploradores, consulte la documentación del explorador.

Para configurar Internet Explorer para la autenticación Kerberos

1. En el menú **Herramientas**, seleccione **Opciones de Internet**.

2. En la ficha **Seguridad**, haga clic en **Intranet local** y, a continuación, haga clic en **Sitios**.
3. En el cuadro de diálogo **Intranet local**, asegúrese de que la opción Detectar automáticamente la red de intranet está seleccionada y, a continuación, haga clic en **Avanzadas**.
4. En el cuadro de diálogo **Intranet local**, agregue los sitios web de los dominios del servidor virtual de administración de tráfico en el dispositivo Citrix ADC. Los sitios especificados se convierten en sitios de intranet local.
5. Haga clic en **Cerrar** o en **Aceptar** para cerrar los cuadros de diálogo.

Para configurar Mozilla Firefox para la autenticación Kerberos

1. Asegúrese de que tiene Kerberos configurado correctamente en su equipo.
2. Escriba about:config en la barra de URL.
3. En el cuadro de texto del filtro, escriba network.negotiate.
4. Cambie network.negotiate-auth.delegation-uris al dominio que quiere agregar.
5. Cambie network.negotiate-auth.trusted-uris al dominio que quiere agregar.

> **Nota:** Si está ejecutando Windows, también debe introducir sspi en el cuadro de texto del filtro y cambiar la opción network.auth.use-sspi a False.

Descarga de autenticación Kerberos desde servidores físicos

February 19, 2022

El dispositivo Citrix ADC puede descargar las tareas de autenticación de los servidores. En lugar de que los servidores físicos autentiquen las solicitudes de los clientes, Citrix ADC autentica todas las solicitudes de los clientes antes de reenviarlas a cualquiera de los servidores físicos vinculados a él. La autenticación de usuarios se basa en tokens de Active Directory.

No hay autenticación entre Citrix ADC y el servidor físico y la descarga de autenticación es transparente para los usuarios finales. Tras el inicio de sesión inicial en un equipo con Windows, el usuario final no tiene que introducir ninguna información de autenticación adicional en una ventana emergente o en una página de inicio de sesión.

En la versión actual del dispositivo Citrix ADC, la autenticación Kerberos solo está disponible para los servidores virtuales de administración del tráfico de autenticación, autorización y auditoría. La autenticación Kerberos no es compatible con SSL VPN en el dispositivo Citrix Gateway Advanced Edition ni en la administración de dispositivos Citrix ADC.

La autenticación Kerberos requiere configuración en el dispositivo Citrix ADC y en los exploradores cliente.

Para configurar la autenticación Kerberos en el dispositivo Citrix ADC

> **Nota**
>
> Las contraseñas utilizadas en la siguiente configuración de ejemplo son solo ejemplos y no las contraseñas de configuración reales.

1. Cree una cuenta de usuario en Active Directory. Al crear una cuenta de usuario, compruebe las siguientes opciones en la sección Propiedades de usuario:
   - Asegúrese de no seleccionar la opción Cambiar contraseña en el próximo inicio de sesión.
   - Asegúrese de seleccionar la opción La contraseña no caduca.
2. En el servidor de AD, en el símbolo del sistema de la CLI, escriba:
   - ktpass -princ HTTP/kerberos.crete.lab.net@crete.lab.net -ptype KRB5_NT_PRINCIPAL -mapuser kerbuser@crete.lab.net -mapop set -pass <password> -out C:\kerbtabfile.txt

   > **Nota**
   >
   > Asegúrese de escribir el comando anterior en una sola línea. El resultado del comando anterior se escribe en el archivo C:\kerbtabfile.txt.
3. Cargue el archivo kerbtabfile.txt en el directorio /etc del dispositivo Citrix ADC mediante un cliente de Secure Copy (SCP).
4. Ejecute el siguiente comando para agregar un servidor DNS al dispositivo Citrix ADC.
   - agregar servidor de nombres dns 1.2.3.4

   El dispositivo Citrix ADC no puede procesar solicitudes Kerberos sin el servidor DNS. Asegúrese de utilizar el mismo servidor DNS que se utiliza en el dominio de Microsoft Windows.
5. Cambie a la interfaz de línea de comandos de Citrix ADC.
6. Ejecute el siguiente comando para crear un servidor de autenticación Kerberos:
   - add authentication negotiateAction KerberosServer -domain “crete.lab.net” -domainUser kerbuser -domainUserPasswd <password> -keytab /var/mykcd.keytab

   > **Nota**
   >
   > Si keytab no está disponible, puede especificar los parámetros: domain, domainUser y -domainUserPasswd.
7. Ejecute el siguiente comando para crear una directiva de negociación:
   - `add authentication negotiatePolicy Kerberos-Policy ”REQ.IP.DESTIP == 192.168.17.200”KerberosServer<!--NeedCopy-->`
8. Ejecute el siguiente comando para crear un servidor virtual de autenticación.
   - `add authentication vserver Kerb-Auth SSL 192.168.17.201 443 -AuthenticationDomain crete.lab.net<!--NeedCopy-->`

9. Ejecute el siguiente comando para enlazar la directiva Kerberos al servidor virtual de autenticación:

   - `bind authentication vserver Kerb-Auth -policy Kerberos-Policy -priority 100<!--NeedCopy-->`

10. Ejecute el siguiente comando para enlazar un certificado SSL al servidor virtual de autenticación. Puede utilizar uno de los certificados de prueba, que puede instalar desde la interfaz gráfica de usuario del dispositivo Citrix ADC. Ejecute el siguiente comando para utilizar el certificado de muestra de ServerTestCert.

    - `bind ssl vserver Kerb-Auth -certkeyName ServerTestCert<!--NeedCopy-->`

11. Cree un servidor virtual de equilibrio de carga HTTP con la dirección IP 192.168.17.200.

    Asegúrese de crear un servidor virtual desde la interfaz de línea de comandos para las versiones de NetScaler 9.3 si son anteriores a la 9.3.47.8.

12. Ejecute el siguiente comando para configurar un servidor virtual de autenticación:

    - `set lb vserver <name>-authn401 ON -authnVsName Kerb-Auth<!--NeedCopy-->`

13. Introduzca el nombre de host Ejemplo en la barra de direcciones del explorador Web.

    El explorador web muestra un cuadro de diálogo de autenticación porque la autenticación Kerberos no está configurada en el explorador.

    > **Nota**
    >
    > La autenticación Kerberos requiere una configuración específica en el cliente. Asegúrese de que el cliente puede resolver el nombre de host, lo que hace que el explorador web se conecte a un servidor virtual HTTP.

14. Configure Kerberos en el explorador web del equipo cliente.

    - Para configurar en Internet Explorer, consulte Configuración de Internet Explorer para la autenticación Kerberos.
    - Para configurar en Mozilla Firefox, consulte Configuración de Internet Explorer para la autenticación Kerberos.

15. Compruebe si puede acceder al servidor físico back-end sin autenticación.

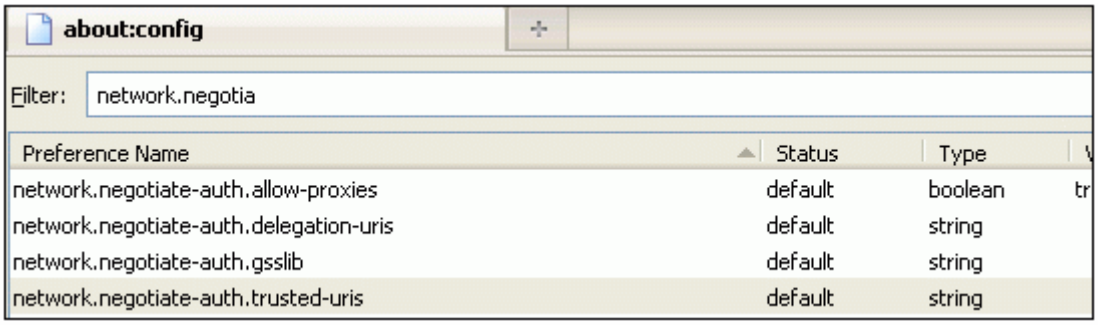
Para configurar Internet Explorer para la autenticación Kerberos

1. Seleccione **Opciones de Internet** en el menú **Herramientas** .
2. Activa la ficha **Seguridad** .

3. Seleccione **Intranet local en** la sección Seleccionar una zona para ver los cambios de configuración de seguridad.
4. Haga clic en **Sitios**.
5. Haga clic en **Avanzadas**.
6. Especifique la URL, el ejemplo y haga clic en **Agregar**.
7. Reinicie **Internet Explorer**.

Para configurar Mozilla Firefox para la autenticación Kerberos

1. Escriba about:config en la barra de direcciones del explorador.
2. Haga clic en la exención de responsabilidad de advertencia.
3. Escriba **network.negotiate-auth.trusted-URIS** en el cuadro **Filtro** .
4. Haga doble clic en **Network.negotiate-auth.trusted-URIS.** A continuación se muestra una pantalla de ejemplo.



5. En el cuadro de diálogo Introducir valor de cadena, especifique www.crete.lab.net.
6. Reinicia Firefox.

Tipos de inicio de sesión único

May 8, 2022

Las funciones de autenticación, autorización y auditoría de Citrix ADC admiten los siguientes tipos de inicio de sesión único.

- Inicio de**sesión único kerberos de Citrix ADC:** los dispositivos Citrix ADC ahora admiten el inicio de sesión único (SSO) mediante el protocolo Kerberos 5. Los usuarios inician sesión en un proxy, Application Delivery Controller (ADC), que proporciona acceso a recursos protegidos. Para obtener más información, consulte Inicio de sesión único kerberos de Citrix ADC.

- **SSO para autenticación básica, digest y NTLM:** la configuración de inicio de sesión único (SSO) en Citrix ADC y Citrix Gateway se puede habilitar a nivel global y también por nivel de tráfico. De forma predeterminada, la configuración de SSO está DESACTIVADA y un administrador puede habilitar el SSO por tráfico o globalmente. Desde el punto de vista de la seguridad, Citrix recomienda a los administradores que desactiven el SSO globalmente y lo habiliten por tráfico. Esta mejora tiene por objeto hacer que la configuración de SSO sea más segura mediante la inhabilitación de cierto tipo de métodos de SSO globalmente. Para obtener más información, consulte SSO para autenticación básica, resumen y NTLM.

Inicio de sesión único de Kerberos Citrix ADC

January 12, 2021

Los dispositivos Citrix ADC ahora admiten el inicio de sesión único (SSO) mediante el protocolo Kerberos 5. Los usuarios inician sesión en un proxy, Application Delivery Controller (ADC), que proporciona acceso a recursos protegidos.

La implementación de Citrix ADC Kerberos SSO requiere la contraseña del usuario para los métodos SSO que dependen de la autenticación básica, NTLM o basada en formularios. La contraseña del usuario no es necesaria para el SSO de Kerberos, aunque si el SSO de Kerberos falla y el dispositivo Citrix ADC tiene la contraseña del usuario, utiliza la contraseña para intentar SSO de NTLM.

Si la contraseña del usuario está disponible, la cuenta KCD se configura con un dominio y no hay información de usuario delegada, el motor de SSO de Citrix AD Kerberos suplanta al usuario para obtener acceso a los recursos autorizados. La suplantación también se denomina delegación sin restricciones.

El motor de SSO Kerberos de Citrix ADC también se puede configurar para usar una cuenta delegada para obtener acceso a recursos protegidos en nombre del usuario. Esta configuración requiere credenciales de usuario delegado, una ficha clave o un certificado de usuario delegado y un certificado de CA coincidente. La configuración que utiliza una cuenta delegada se denomina delegación restringida.

Introducción al inicio de sesión único de Kerberos de Citrix ADC

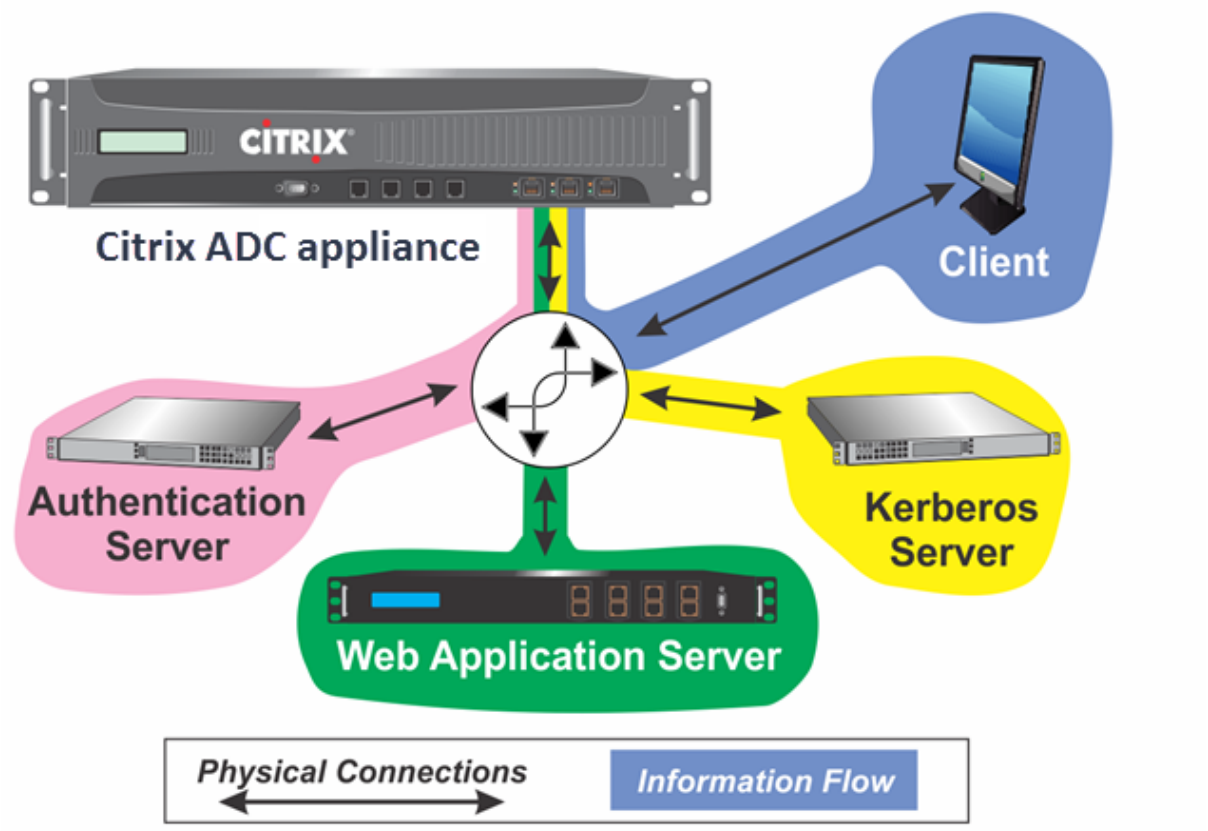
August 20, 2021

Para utilizar la función Citrix ADC Kerberos SSO, los usuarios primero se autentican con Kerberos o con un servidor de autenticación de terceros compatible. Una vez autenticado, el usuario solicita acceso a una aplicación web protegida. El servidor web responde con una solicitud de prueba de que el usuario está autorizado a acceder a esa aplicación web. El explorador del usuario se pone en contacto con el servidor Kerberos, que verifica que el usuario está autorizado para acceder a ese recurso y, a

continuación, proporciona al explorador del usuario un tíquet de servicio que proporciona pruebas. El explorador vuelve a enviar la solicitud del usuario al servidor de aplicaciones web con el tíquet de servicio adjunto. El servidor de aplicaciones web verifica el tíquet de servicio y, a continuación, permite al usuario acceder a la aplicación.

La administración de tráfico de autenticación, autorización y auditoría implementa este proceso como se muestra en el siguiente diagrama. El diagrama ilustra el flujo de información a través del dispositivo Citrix ADC y la administración de tráfico de autenticación, autorización y auditoría, en una red segura con autenticación LDAP y autorización Kerberos. Los entornos de administración de tráfico de autenticación, autorización y auditoría que utilizan otros tipos de autenticación tienen esencialmente el mismo flujo de información, aunque pueden diferir en algunos detalles.

Ilustración 1. Una red segura con LDAP y Kerberos



La administración de tráfico de autenticación, autorización y auditoría con autenticación y autorización en un entorno Kerberos requiere que se lleven a cabo las siguientes acciones.

1. El cliente envía una solicitud de un recurso al servidor virtual de administración de tráfico en el dispositivo Citrix ADC.
2. El servidor virtual de administración de tráfico pasa la solicitud al servidor virtual de autenticación, que autentica el cliente y, a continuación, devuelve la solicitud al servidor virtual de administración de tráfico.

3. El servidor virtual de administración de tráfico envía la solicitud del cliente al servidor de aplicaciones web.
4. El servidor de aplicaciones web responde al servidor virtual de administración de tráfico con un mensaje 401 no autorizado que solicita la autenticación Kerberos, la cual recurre a la autenticación NTLM si el cliente no admite Kerberos.
5. El servidor virtual de administración de tráfico se pone en contacto con el demonio SSO de Kerberos.
6. El demonio SSO de Kerberos se pone en contacto con el servidor Kerberos y obtiene un tíquet de concesión de tíquets (TGT) que le permite solicitar tíquets de servicio que autorizan el acceso a aplicaciones protegidas.
7. El demonio Kerberos SSO obtiene un tíquet de servicio para el usuario y lo envía al servidor virtual de administración de tráfico.
8. El servidor virtual de administración de tráfico adjunta el tíquet a la solicitud inicial del usuario y envía la solicitud modificada de nuevo al servidor de aplicaciones web.
9. El servidor de aplicaciones web responde con un mensaje de 200 OK.

Estos pasos son transparentes para el cliente, que solo envía una solicitud y recibe el recurso solicitado.

Integración de Citrix ADC Kerberos SSO con métodos de autenticación

Todos los mecanismos de autenticación de administración de tráfico de autenticación, autorización y auditoría son compatibles con Citrix ADC Kerberos SSO. La administración de tráfico de autenticación, autorización y auditoría admite el mecanismo de inicio de sesión único de Kerberos con los mecanismos de autenticación Kerberos, CAC (Smart Card) y SAML con cualquier forma de autenticación de cliente para el dispositivo Citrix ADC. También admite los mecanismos de SSO HTTP-Basic, HTTP-Digest, basados en formularios y NTLM (versiones 1 y 2) si el cliente utiliza autenticación HTTP-Basic o basada en formularios para iniciar sesión en el dispositivo Citrix ADC.

La tabla siguiente muestra cada método de autenticación del lado del cliente admitido y el método de autenticación del lado del servidor admitido para ese método del lado del cliente.

Cuadro 1 Métodos de autenticación admitidos

	Básico/Digest/NTLM	Delegación limitada de Kerberos	Suplantación de usuario
CAC (tarjeta inteligente): En la capa SSL/T LS		X	X
Basado en formularios (LDAP/RADIUS/TACACS)	X	X	X

	Básico/Digest/NTLM	Delegación limitada de Kerberos	Suplantación de usuario
HTTP básico (LDAP/RADIUS/TACACS)	X	X	X
Kerberos		X	
NT LM v1/v2		X	X
SAML		X	
SAML de dos factores	X	X	X
Certificado de dos factores	X	X	X

Configurar Citrix ADC SSO

February 19, 2022

Puede configurar el inicio de sesión único de Citrix ADC para que funcione de dos maneras: por suplantación de identidad o por delegación. El SSO por suplantación de identidad es una configuración más sencilla que el SSO por delegación y, por lo tanto, suele ser preferible cuando la configuración lo permite. Para configurar el SSO de Citrix ADC mediante suplantación de identidad, debe tener el nombre de usuario y la contraseña del usuario.

Para configurar el inicio de sesión único de Citrix ADC por delegación, debe tener las credenciales del usuario delegado en uno de los siguientes formatos: el nombre de usuario y la contraseña del usuario, la configuración keytab que incluye el nombre de usuario y una contraseña cifrada, o el certificado de usuario delegado y el certificado de entidad emisora de certificados correspondiente.

Requisitos previos para configurar Citrix ADC SSO

Antes de configurar el inicio de sesión único de Citrix ADC, debe tener el dispositivo Citrix ADC completamente configurado para administrar el tráfico y la autenticación de los servidores de aplicaciones web. Por lo tanto, debe configurar el equilibrio de carga o el cambio de contenido y, a continuación, la autenticación, la autorización y la auditoría para estos servidores de aplicaciones web. También debe verificar la redirección entre el dispositivo, el servidor LDAP y el servidor Kerberos.

Si su red aún no está configurada de esta manera, realice las siguientes tareas de configuración:

- Configure un servidor y un servicio para cada servidor de aplicaciones web.

- Configure un servidor virtual de administración del tráfico para gestionar el tráfico hacia y desde su servidor de aplicaciones web.

A continuación se presentan breves instrucciones y ejemplos para realizar cada una de estas tareas desde la línea de comandos de Citrix ADC. Para obtener más ayuda, consulte Configuración de un servidor virtual de autenticación.

> **Nota**
>
> A partir de la versión de Citrix ADC 13.1, el recorrido entre el dominio raíz y el dominio de árbol se admite durante la autenticación de SSO Kerberos para el servidor back-end desde el dispositivo Citrix ADC.

Para crear un servidor y un servicio mediante la CLI

Para que el SSO de Citrix ADC obtenga un TGS (tíquet de servicio) para un servicio, el FQDN asignado a la entidad del servidor en el dispositivo Citrix ADC debe coincidir con el FQDN del servidor de aplicaciones web o el nombre de la entidad del servidor debe coincidir con el nombre NetBIOS del servidor de aplicaciones web. Puede adoptar cualquiera de los siguientes enfoques:

- Configure la entidad del servidor Citrix ADC especificando el FQDN del servidor de aplicaciones web.
- Configure la entidad del servidor Citrix ADC especificando la dirección IP del servidor de aplicaciones web y asigne a la entidad del servidor el mismo nombre que el nombre NetBIOS del servidor de aplicaciones web.

En el símbolo del sistema, escriba los siguientes comandos:

```
1 -  add server name <serverFQDN>
2
3 -  add service name serverName serviceType port
4 <!--NeedCopy-->
```

Para las variables, sustituya los siguientes valores:

- **serverName**. Nombre del dispositivo Citrix ADC que se va a utilizar para hacer referencia a este servidor.
- **FQDN del servidor**. FQDN del servidor. Si el servidor no tiene ningún dominio asignado, utilice la dirección IP del servidor y asegúrese de que el nombre de la entidad del servidor coincida con el nombre NetBIOS del servidor de aplicaciones web.
- **serviceName**. Nombre del dispositivo Citrix ADC que se va a utilizar para hacer referencia a este servicio.
- **tipo**. Protocolo utilizado por el servicio, ya sea HTTP o MSSQLSVC.

- **puerto**. Puerto en el que escucha el servicio. Los servicios HTTP suelen escuchar en el puerto 80. Los servicios HTTPS seguros suelen escuchar en el puerto 443.

Ejemplo:

En los siguientes ejemplos se agregan entradas de servidor y servicio en el dispositivo Citrix ADC para el servidor de aplicaciones web was1.example.com. El primer ejemplo utiliza el FQDN del servidor de aplicaciones web; el segundo utiliza la dirección IP.

Para agregar el servidor y el servicio mediante el FQDN del servidor de aplicaciones web, was1.example.com, debe escribir los siguientes comandos:

```
add server was1 was1.example.com
add service was1service was1 HTTP 80
<!--NeedCopy-->
```

Para agregar el servidor y el servicio mediante la IP del servidor de aplicaciones web y el nombre NetBIOS, donde la IP del servidor de aplicaciones web es 10.237.64.87 y su nombre NetBIOS es WAS1, debe escribir los siguientes comandos:

```
add server WAS1 10.237.64.87
add service was1service WAS1 HTTP 8
<!--NeedCopy-->
```

Para crear un servidor virtual de administración del tráfico mediante la CLI

El servidor virtual de administración del tráfico administra el tráfico entre el cliente y el servidor de aplicaciones web. Puede utilizar un servidor virtual de equilibrio de carga o de conmutación de contenido como servidor de administración del tráfico. La configuración de SSO es la misma para cualquiera de los dos tipos.

Para crear un servidor virtual de equilibrio de carga, en el símbolo del sistema, escriba el siguiente comando:

```
add lb vserver <vserverName> <type> <IP> <port>
<!--NeedCopy-->
```

Para las variables, sustituya los siguientes valores:

- **vServerName**: nombre para el dispositivo Citrix ADC que se utilizará para hacer referencia a este servidor virtual.

- **type**: protocolo utilizado por el servicio, ya sea HTTP o MSSQLSVC.
- **IP**: dirección IP asignada al servidor virtual. Normalmente, se trata de una dirección IP no pública reservada por IANA en su LAN.
- **port**—Puerto en el que escucha el servicio. Los servicios HTTP suelen escuchar en el puerto 80. Los servicios HTTPS seguros suelen escuchar en el puerto 443.

Ejemplo:

Para agregar un servidor virtual de equilibrio de carga denominado tmvserver1 a una configuración que administra el tráfico HTTP en el puerto 80, asignarle una dirección IP de LAN 10.217.28.20 y, a continuación, vincular el servidor virtual de equilibrio de carga al servicio wasservice1, debe escribir los siguientes comandos:

```
1 add lb vserver tmvserver1 HTTP 10.217.28.20 80
2 bind lb vserver tmvserv1 wasservice1
3 <!--NeedCopy-->
```

Para crear un servidor virtual de autenticación mediante la CLI

El servidor virtual de autenticación administra el tráfico de autenticación entre el cliente y el servidor de autenticación (LDAP). Para crear un servidor virtual de autenticación, en el símbolo del sistema escriba los siguientes comandos:

```
1 add authentication vserver <authvserverName> SSL <IP> 443
2 <!--NeedCopy-->
```

Para las variables, sustituya los siguientes valores:

- **authvServerName** : nombre del dispositivo Citrix ADC que se utilizará para hacer referencia a este servidor virtual de autenticación. Debe comenzar con una letra, un número o un carácter de guión bajo (_) y debe contener solo letras, números y guión (-), punto (.), almohadilla (#), espacio ( ), en (@), igual a (=), dos puntos (:) y guión bajo. Se puede cambiar después de agregar el servidor virtual de autenticación mediante el comando rename authentication vserver.
- **IP**: dirección IP asignada al servidor virtual de autenticación. Al igual que con el servidor virtual de administración del tráfico, esta dirección normalmente sería una IP no pública reservada por IANA en su LAN.
- **domain**: dominio asignado al servidor virtual. Por lo general, este sería el dominio de la red. Es habitual, aunque no es obligatorio, introducir el dominio en mayúsculas al configurar el servidor virtual de autenticación.

Ejemplo:

Para agregar un servidor virtual de autenticación denominado authverver1 a su configuración y asignarle la IP LAN 10.217.28.21 y el dominio EXAMPLE.COM, debe escribir los siguientes comandos:

```
add authentication vserver authvserver1 SSL 10.217.28.21 443
<!--NeedCopy-->
```

Para configurar un servidor virtual de administración del tráfico para que utilice un perfil de autenticación

El servidor virtual de autenticación se puede configurar para gestionar la autenticación de un solo dominio o de varios dominios. Si está configurado para admitir la autenticación de varios dominios, también debe especificar el dominio de Citrix ADC SSO mediante la creación de un perfil de autenticación y, a continuación, la configuración del servidor virtual de administración de tráfico para que use ese perfil de autenticación.

> **Nota**
>
> El servidor virtual de administración del tráfico puede ser un servidor virtual de equilibrio de carga (lb) o conmutación de contenido (cs). En las instrucciones siguientes se supone que está usando un servidor virtual de equilibrio de carga. Para configurar un servidor virtual de conmutación de contenido, simplemente sustituya
> set cs vserver por set lb vserver. Por lo demás, el procedimiento es el mismo.

Para crear el perfil de autenticación y, a continuación, configurarlo en un servidor virtual de administración de tráfico, escriba los siguientes comandos:

```
-  add authentication authnProfile <authnProfileName> {
 -authvserverName <string> }
  {
 -authenticationHost <string> }
  {
 -authenticationDomain <string> }

-  set lb vserver <vserverName> -authnProfile <authnprofileName>
<!--NeedCopy-->
```

Para las variables, sustituya los siguientes valores:

- **authnProfileName**: nombre del perfil de autenticación. Debe comenzar con una letra, un número o un carácter de guión bajo (_) y debe constar de uno a treinta y un caracteres

alfanuméricos o de guión (-), punto (.), almohadilla (#), espacio ( ), en (@), igual (=), dos puntos (:) y guión bajo.

- **authvServerName**: nombre del servidor virtual de autenticación que utiliza este perfil para la autenticación.
- **AuthenticationHost**: nombre de host del servidor virtual de autenticación.
- **AuthenticationDomain**: dominio para el que Citrix ADC SSO gestiona la autenticación. Necesario si el servidor virtual de autenticación realiza la autenticación para más de un dominio, de modo que se incluya el dominio correcto cuando el dispositivo Citrix ADC establezca la cookie del servidor virtual de administración del tráfico.

Ejemplo:

Para crear un perfil de autenticación denominado AuthnProfile1 para la autenticación del dominio example.com y configurar el servidor virtual de equilibrio de carga vserver1 para utilizar el perfil de autenticación AuthnProfile1, escriba los siguientes comandos:

```
1 add authentication authnProfile authnProfile1 -authnvsName
     authvsesrver1
2       -authenticationHost authvsesrver1 -authenticationDomain example.
           com
3 set lb vserver vserver1 -authnProfile authnProfile1
4 <!--NeedCopy-->
```

Configurar Single Sign-On

July 8, 2022

Configurar Single Sign-On (SSO) de Citrix ADC para autenticar mediante suplantación es más sencillo que configurar SSO para autenticarse por delegación y, por lo tanto, es preferible cuando la configuración lo permite. Crea una cuenta en KCD. Puede usar la contraseña del usuario.

Si no tiene la contraseña del usuario, puede configurar Citrix ADC SSO para que se autentique por delegación. Aunque es más complejo que configurar el SSO para autenticarse mediante suplantación, el método de delegación proporciona flexibilidad en el sentido de que las credenciales de un usuario pueden no estar disponibles para el dispositivo Citrix ADC en todas las circunstancias.

Para la suplantación o la delegación, también debe habilitar la autenticación integrada en el servidor de aplicaciones web.

Habilitar la autenticación integrada en el servidor de aplicaciones web

Para configurar Citrix ADC Kerberos SSO en cada servidor de aplicaciones web que administra el SSO Kerberos, use la interfaz de configuración en ese servidor para configurar el servidor para que requiera autenticación. Seleccione la autenticación Kerberos (negociar) por preferencia, con opción de reserva NTLM para los clientes que no admiten Kerberos.

A continuación se presentan instrucciones para configurar Microsoft Internet Information Server (IIS) para que requiera autenticación. Si el servidor de aplicaciones web utiliza software distinto de IIS, consulte la documentación del software de ese servidor web para obtener instrucciones.

Para configurar Microsoft IIS de modo que utilice la autenticación integrada

1. Inicie sesión en el servidor IIS y abra el **Administrador de Internet Information Services.**
2. Seleccione el sitio web para el que quiere habilitar la autenticación integrada. Para habilitar la autenticación integrada para todos los servidores web de IIS administrados por IISM, configure los valores de autenticación para el sitio web predeterminado. Para habilitar la autenticación integrada para servicios individuales (como Exchange, Exadmin, ExchWeb y Public), configure estos ajustes de autenticación para cada servicio de forma individual.
3. Abra el cuadro de diálogo **Propiedades** del sitio web predeterminado o del servicio individual y haga clic en la ficha **Seguridad del directorio**.
4. Junto a **Autenticación** y **Control de acceso**, seleccione **Modificar**.
5. Inhabilite el acceso anónimo.
6. Habilite la autenticación integrada de Windows (solo). La habilitación de la autenticación de Windows integrada debe establecer automáticamente la negociación de protocolos para que el servidor web negocie, NTLM, que especifica la autenticación Kerberos con respaldo a NTLM para dispositivos que no sean compatibles con Kerberos. Si esta opción no se selecciona automáticamente, establezca manualmente la negociación del protocolo en Negociar, NTLM.

Configurar el SSO mediante suplantación

Puede configurar la cuenta KCD para Citrix ADC SSO mediante suplantación. En esta configuración, el dispositivo Citrix ADC obtiene el nombre de usuario y la contraseña del usuario cuando el usuario se autentica en el servidor de autenticación y utiliza esas credenciales para suplantar al usuario y obtener un tíquet de concesión de tíquets (TGT). Si el nombre del usuario está en formato UPN, el dispositivo obtiene el dominio del usuario de UPN. De lo contrario, obtiene el nombre y el dominio del usuario extrayéndolos del dominio SSO utilizado durante la autenticación inicial o del perfil de sesión.

> **Nota**
>
> No puede agregar un nombre de usuario con dominio si el nombre de usuario ya se agregó sin

> dominio. Si el nombre de usuario con dominio se agrega primero seguido del mismo nombre de usuario sin dominio, el dispositivo Citrix ADC agrega el nombre de usuario a la lista de usuarios.

Al configurar la cuenta KCD, debe establecer el parámetro realm en el dominio del servicio al que el usuario está accediendo. El mismo dominio también se usa como territorio del usuario si el dominio del usuario no se puede obtener de la autenticación con el dispositivo Citrix ADC o del perfil de sesión.

Para crear la cuenta KCD para el SSO mediante suplantación de identidad con una contraseña

En el símbolo del sistema, escriba el siguiente comando:

```
add aaa kcdaccount <accountname> -realmStr <realm>

<!--NeedCopy-->
```

Para las variables, sustituya los siguientes valores:

- **nombre_cuenta**. Nombre de la cuenta de KCD.
- **realm**. El dominio asignado al SSO de Citrix ADC.

Ejemplo

Para agregar una cuenta KCD denominada kcdccount1 y utilizar la ficha keytab denominada kcdvserver.keytab, escriba el siguiente comando:

```
add aaa kcdAccount kcdaccount1 -keytab kcdvserver.keytab

<!--NeedCopy-->
```

Para obtener información sobre cómo configurar la suplantación de Kerberos a través de la GUI de Citrix ADC, consulte Citrix Support.

Configurar SSO por delegación

Para configurar el SSO por delegación, debe realizar las siguientes tareas:

- Si configura la delegación por certificado de usuario delegado, instale los certificados de CA coincidentes en el dispositivo Citrix ADC y agréguelos a la configuración de Citrix ADC.
- Cree la cuenta KCD en el dispositivo. El dispositivo utiliza esta cuenta para obtener tickets de servicio para sus aplicaciones protegidas.
- Configure el servidor de Active Directory.

> **Nota**
>
> Para obtener más información sobre la creación de una cuenta KCD y la configuración en el dispositivo NetScaler, consulte los siguientes temas:
>
> - Gestionar la autenticación, la autorización y la auditoría con Kerberos/NTLM
> - Cómo Citrix ADC implementa Kerberos para la autenticación de clientes
> - Configuración de la autenticación kerberos en el dispositivo Citrix ADC

Instalación del certificado de CA cliente en el dispositivo Citrix ADC

Si configura el SSO de Citrix ADC con un certificado de cliente, debe copiar el certificado de CA coincidente para el dominio del certificado de cliente (el certificado de CA de cliente) en el dispositivo Citrix ADC y, a continuación, instalar el certificado de CA. Para copiar el certificado de CA cliente, use el programa de transferencia de archivos de su elección para transferir el certificado y el archivo de clave privada al dispositivo Citrix ADC y almacenar los archivos en /nsconfig/ssl.

Para instalar el certificado de CA cliente en el dispositivo Citrix ADC

En el símbolo del sistema, escriba el siguiente comando:

```
1 add ssl certKey <certkeyName> -cert <cert> [(-key <key> [-password]) |
     -fipsKey <fipsKey>][-inform ( DER | PEM )][-expiryMonitor ( ENABLED
     | DISABLED | UNSET ) [-notificationPeriod <positive_integer>]] [-
     bundle ( YES | NO )]
2
3 <!--NeedCopy-->
```

Para las variables, sustituya los siguientes valores:

- **certkeyName**. Un nombre para el certificado de CA de cliente. Debe comenzar con un carácter alfanumérico o de subrayado (_) ASCII y debe constar de uno a treinta y un caracteres. Los caracteres permitidos incluyen caracteres alfanuméricos ASCII, guiones bajos, hash (#), punto (.), espacio, dos puntos (:), arroba (@), igual (=) y guion (-). No se puede cambiar después de crear el par de claves de certificado. Si el nombre incluye uno o más espacios, escríbalo entre comillas dobles o simples (por ejemplo, “mi certificado” o “mi certificado”).
- **certificado**. Nombre de ruta de acceso completo y nombre de archivo del archivo de certificado X509 utilizado para formar el par de claves de certificado. El archivo de certificado debe almacenarse en el dispositivo Citrix ADC, en el directorio /nsconfig/ssl/.

- **clave**. Nombre de ruta de acceso completo y nombre de archivo del archivo que contiene la clave privada del archivo de certificado X509. El archivo de clave debe almacenarse en el dispositivo Citrix ADC en el directorio /nsconfig/ssl/.
- **contraseña**. Si se especifica una clave privada, la frase de contraseña utilizada para cifrar la clave privada. Use esta opción para cargar claves privadas cifradas en formato PEM.
- **fipsKey**. Nombre de la clave FIPS que se creó en el módulo de seguridad de hardware (HSM) de un dispositivo FIPS o una clave que se importó en el HSM.

  > **Nota**
  >
  > Puede especificar una clave o una fipsKey, pero no ambas.

- **inform**. Formato de los archivos de certificado y clave privada, ya sea PEM o DER.
- **passplain**. Frase de contraseña utilizada para cifrar la clave privada. Se requiere cuando se agrega una clave privada cifrada en formato PEM.
- **expiryMonitor**. Configure el dispositivo Citrix ADC para que emita una alerta cuando el certificado esté a punto de caducar. Valores posibles: ENABLED, DISABLED, UNSET.
- **notificationPeriod**. Si `expiryMonitor` está HABILITADO, el número de días antes de que caduque el certificado para emitir una alerta.
- **bundle**. Analice la cadena de certificados como un único archivo después de vincular el certificado del servidor al certificado del emisor dentro del archivo. Valores posibles: SÍ, NO.

Ejemplo

El siguiente ejemplo agrega el certificado de usuario delegado especificado customer-cert.pem a la configuración de Citrix ADC junto con la clave customer-key.pem y establece la contraseña, el formato del certificado, el monitor de caducidad y el período de notificación.

Para agregar el certificado de usuario delegado, debe escribir los siguientes comandos:

```
1 add ssl certKey customer -cert ”/nsconfig/ssl/customer-cert.pem”
2 -key ”/nsconfig/ssl/customer-key.pem” -password ”dontUseDefaultPWs!”
3 -inform PEM -expiryMonitor ENABLED [-notificationPeriod 14]
4
5 <!--NeedCopy-->
```

Creación de la cuenta KCD

Si configura Citrix ADC SSO por delegación, puede configurar la cuenta KCD para que use el nombre de inicio de sesión y la contraseña del usuario, para que use el nombre de inicio de sesión y el keytab

del usuario o para que use el certificado de cliente del usuario. Si configura el SSO con el nombre de usuario y la contraseña, el dispositivo Citrix ADC utiliza la cuenta de usuario delegado para obtener un vale de concesión de tickets (TGT) y, a continuación, utiliza el TGT para obtener tickets de servicio para los servicios específicos que solicita cada usuario. Si configura el SSO con un archivo keytab, el dispositivo Citrix ADC utiliza la información de la cuenta de usuario delegada y de la ficha clave. Si configura el SSO con un certificado de usuario delegado, el dispositivo Citrix ADC usa el certificado de usuario delegado.

> **Nota:**
>
> Para dominios cruzados, el servicePrincipalName del usuario delegado debe tener el formato `host/<name>`. Si no está en este formato, cambie el servicePrincipalName del usuario delegado `<servicePrincipalName>` a `host/<service-account-samaccountname>`. Puede comprobar el atributo de la cuenta de usuario delegada en el controlador de dominio. Un método para cambiar es cambiar el atributo `logonName` del usuario delegado.

Para crear la cuenta KCD para el SSO por delegación con una contraseña

En el símbolo del sistema, escriba los comandos siguientes:

```
add aaa kcdAccount <kcdAccount> {
 -realmStr <string> }
  {
 -delegatedUser <string> }
  {
 -kcdPassword  }
  [-userRealm <string>]
[-enterpriseRealm <string>] [-serviceSPN <string>]
<!--NeedCopy-->
```

Para las variables, sustituya los siguientes valores:

- **kcdAccount**: Nombre para la cuenta KCD. Se trata de un argumento obligatorio. Longitud máxima: 31
- **realmStr**: El territorio de Kerberos. Longitud máxima: 255
- **delegatedUser**: El nombre de usuario que puede realizar la delegación restringida de kerberos. El nombre de usuario delegado se deriva del servicePrincipalName de su controlador de dominio. Para dominios cruzados, el servicePrincipalName del usuario delegado debe tener el formato `host/<name>`. Longitud máxima: 255.
- **kcdPassword**: Contraseña para el usuario delegado. Longitud máxima: 31
- **userRealm**: Dominio del usuario. Longitud máxima: 255

- **enterpriseRealm**: Ámbito empresarial del usuario. Esto solo se da en ciertas implementaciones de KDC en las que KDC espera un nombre de usuario empresarial en lugar de un nombre principal. Longitud máxima: 255
- **serviceSPN**: Servicio SPN. Cuando se especifica, se usa para obtener tickets kerberos. Si no se especifica, Citrix ADC construye el SPN mediante el FQDN del servicio. Longitud máxima: 255

Ejemplo (formato UPN):

Para agregar una cuenta KCD llamada kcdaccount1 a la configuración del dispositivo Citrix ADC con una contraseña de password1 y un dominio de EXAMPLE.COM, especificando la cuenta de usuario delegada en formato UPN (como root), debe escribir los siguientes comandos:

```
1 add aaa kcdaccount kcdaccount1 -delegatedUser root
2 -kcdPassword password1 -realmStr EXAMPLE.COM
3
4 <!--NeedCopy-->
```

Ejemplo (formato SPN):

Para agregar una cuenta KCD llamada kcdaccount1 a la configuración del dispositivo Citrix ADC con una contraseña de contraseña1 y un dominio de EXAMPLE.COM, especificando la cuenta de usuario delegada en formato SPN, debe escribir los siguientes comandos:

```
1 add aaa kcdAccount kcdaccount1 -realmStr EXAMPLE.COM
2 -delegatedUser "host/kcdvserver.example.com" -kcdPassword password1
3
4 <!--NeedCopy-->
```

Crear la cuenta KCD para el SSO por delegación con una ficha de teclas

Si va a utilizar un archivo keytab para la autenticación, primero cree el keytab. Puede crear el archivo keytab manualmente iniciando sesión en el servidor de AD y utilizando la utilidad `ktpass`, o puede usar la utilidad de configuración de Citrix ADC para crear un script por lotes y, a continuación, ejecutar ese script en el servidor de AD para generar el archivo keytab. A continuación, utilice FTP u otro programa de transferencia de archivos para transferir el archivo keytab al dispositivo Citrix ADC y colocarlo en el directorio /nsconfig/krb. Por último, configure la cuenta KCD para Citrix ADC SSO por delegación y proporcione la ruta y el nombre de archivo del archivo keytab al dispositivo Citrix ADC.

> **Nota:**
>
> Para dominios cruzados, si quiere obtener el archivo Keytab como parte de la cuenta de KCD,

> utilice el siguiente comando para el nombre de usuario delegado actualizado.
>
> En el controlador de dominio, cree un archivo Keytab actualizado.
>
> ```
> ktpass /princ <servicePrincipalName-with-prefix<host/>Of-delegateUser
> >@<DC REALM in uppercase> /ptype KRB5_NT_PRINCIPAL /mapuser <DC REALM
>  in uppercase>\<sAMAccountName> /pass <delegatedUserPassword> -out
> filepathfor.keytab
> ```
>
> El archivo `filepathfor.keytab` se puede colocar en el dispositivo Citrix ADC y se puede usar como parte de la configuración de Keytab en la cuenta KCD de ADC.

Para crear el archivo keytab manualmente

Inicie sesión en la línea de comandos del servidor AD y, en el símbolo del sistema, escriba el siguiente comando:

```
1 ktpass princ <SPN> ptype KRB5_NT_PRINCIPAL mapuser <DOMAIN><username>
     pass <password> -out <File_Path>
2 <!--NeedCopy-->
```

Para las variables, sustituya los siguientes valores:

- **SPN**. El nombre principal de servicio de la cuenta de servicio de KCD.
- **DOMINIO**. El dominio del servidor de Active Directory.
- **nombre de usuario**. El nombre de usuario de la cuenta de KSA.
- **contraseña**. La contraseña de la cuenta de KSA.
- **ruta**. El nombre completo de la ruta de acceso del directorio en el que se almacenará el archivo keytab después de generarlo.

Para usar la utilidad de configuración de Citrix ADC para crear un script que genere el archivo keytab

1. Vaya a **Seguridad > AAA - Tráfico de aplicaciones.**
2. En el panel de datos, en **Delegación restringida de Kerberos**, haga clic en Archivo **por lotes** para generar Keytab.
3. En el cuadro de diálogo **Generar script Keytab KCD (delegación restringida de Kerberos)**, defina los siguientes parámetros:
   - Nombre**de usuario del dominio**. El nombre de usuario de la cuenta de KSA.
   - **Contraseña de dominio** La contraseña de la cuenta de KSA.
   - **Director de servicio**. El nombre principal del servicio de la KSA.

- **Nombre del archivo de salida**. La ruta de acceso completa y el nombre de archivo en los que se guardará el archivo keytab en el servidor de AD.

4. Desmarque la casilla **Crear cuenta de usuario de dominio**.
5. Haga clic en **Generar script**.
6. Inicie sesión en el servidor de Active Directory y abra una ventana de línea de comandos.
7. Copie el script de la ventana **Script generado** y péguelo directamente en la ventana de línea de comandos del servidor Active Directory. La keytab se genera y almacena en el directorio bajo el nombre de archivo que especificó como **Nombre de archivo de salida**.
8. Use la utilidad de transferencia de archivos de su elección para copiar el archivo keytab del servidor de Active Directory al dispositivo Citrix ADC y colocarlo en el directorio /nsconfig/krb.

Para crear la cuenta de KCD

En el símbolo del sistema, escriba el siguiente comando:

```
add aaa kcdaccount <accountname>  -keytab <keytab>
<!--NeedCopy-->
```

Ejemplo

Para agregar una cuenta KCD llamada kcdccount1 y usar la keytab llamada kcdvserver.keytab, debe escribir los siguientes comandos:

```
add aaa kcdaccount kcdaccount1  -keytab kcdvserver.keytab
<!--NeedCopy-->
```

Para crear la cuenta KCD para el SSO por delegación con un certificado de usuario delegado

En el símbolo del sistema, escriba el siguiente comando:

```
add aaa kcdaccount <accountname> -realmStr <realm> -delegatedUser <
   user_nameSPN> -usercert <cert> -cacert <cacert>
<!--NeedCopy-->
```

Para las variables, sustituya los siguientes valores:

- **nombre_cuenta**. Nombre de la cuenta de KCD.
- **realmStr**. El dominio de la cuenta KCD, normalmente el dominio para el que está configurado el SSO.

- **delegatedUser**. El nombre de usuario delegado, en formato SPN.
- **usercert**. La ruta de acceso completa y el nombre del archivo de certificado de usuario delegado en el dispositivo Citrix ADC. El certificado de usuario delegado debe contener tanto el certificado de cliente como la clave privada, y debe estar en formato PEM. Si utiliza la autenticación con tarjeta inteligente, debe crear una plantilla de certificado de tarjeta inteligente para permitir que los certificados se importen con la clave privada.
- **cacert**. La ruta de acceso completa y el nombre del archivo de certificado de CA en el dispositivo Citrix ADC.

Ejemplo

Para agregar una cuenta KCD denominada kcdccount1 y utilizar la ficha keytab denominada kcdvserver.keytab, escriba el siguiente comando:

```
add aaa kcdaccount kcdaccount1 -realmStr EXAMPLE.COM
     -delegatedUser ”host/kcdvserver.example.com” -usercert /certs/
        usercert
     -cacert /cacerts/cacert
<!--NeedCopy-->
```

Configuración del SSO de Active Directory para Citrix ADC

Cuando configura el SSO por delegación, además de crear la cuenta KCD en el dispositivo Citrix ADC, también debe crear una cuenta de servicio Kerberos (KSA) coincidente en el servidor de Active Directory LDAP y configurar el servidor para SSO. Para crear el KSA, use el proceso de creación de cuentas en el servidor de Active Directory. Para configurar el SSO en el servidor de Active Directory, abra la ventana de propiedades del KSA. En la ficha **Delegación**, habilite las siguientes opciones: Confiar en este usuario para la delegación solo a los servicios especificados y Usar cualquier protocolo de autenticación. (La opción solo Kerberos no funciona porque no permite la transición de protocolos ni la delegación restringida). Por último, agregue los servicios que administra Citrix ADC SSO.

> **Nota:**
>
> Si la ficha Delegación no está visible en el cuadro de diálogo de propiedades de la cuenta de KSA, antes de poder configurar el KSA como se describe, debe usar la herramienta de línea de comandos
> setspn de Microsoft para configurar el servidor de Active Directory de modo que la ficha esté visible.

Para configurar la delegación de la cuenta de servicio Kerberos

1. En el cuadro de diálogo de configuración de la cuenta LDAP para la cuenta de servicio Kerberos que creó, haga clic en la ficha **Delegación**.
2. Elija **Confiar en este usuario para la delegación solo en los servicios especificados**.
3. En Confiar en este usuario para la delegación solo en los servicios especificados, elija **Usar cualquier protocolo de autenticación**.
4. En Servicios en los que esta cuenta puede presentar credenciales delegadas, haga clic en **Agregar.**
5. En el cuadro de diálogo **Agregar servicios**, haga clic en **Usuarios** o **Equipos**, elija el servidor que aloja los recursos que se asignarán a la cuenta de servicio y, a continuación, haga clic en **Aceptar**.

   > **Nota:**
   >
   > - La delegación restringida no admite los servicios alojados en dominios distintos del dominio asignado a la cuenta, aunque Kerberos pueda tener una relación de confianza con otros dominios.
   > - Use el siguiente comando para crear `setspn` si se crea un usuario en el directorio activo: `setspn -A host/kcdvserver.example.com example\kcdtest`

6. De nuevo en el cuadro de diálogo **Agregar servicios**, en la lista Servicios disponibles, elige los servicios asignados a la cuenta de servicio. Citrix ADC SSO admite los servicios HTTP y MSSQLSVC.
7. Haga clic en **Aceptar.**

Cambios en la configuración para permitir que KCD admita dominios secundarios

Si la cuenta de KCD está configurada con `samAccountName` para `-delegatedUser`, KCD no funciona para los usuarios que acceden a los servicios de los dominios secundarios. En este caso, puede modificar la configuración en el dispositivo Citrix ADC y Active Directory.

- Cambie el nombre de inicio de sesión de la cuenta de servicio `<service-account-samaccountname>` (que está configurada como delegateUser en la cuenta de KCD) en AD en formato `host/<service-account-samaccountname>.<completeUSERDNSDOMAIN>` (por ejemplo, `host/svc_act.child.parent.com`).

  Puede cambiar la cuenta de servicio manualmente o mediante el comando `ktpass`. `ktpass` actualiza automáticamente la cuenta de servicio.

  ```
  ktpass /princ host/svc_act.child.parent.com@CHILD.PARENT.COM /ptype
  KRB5_NT_PRINCIPAL /mapuser CHILD\sv_act /pass serviceaccountpassword -
  out filepathfor.keytab
  ```


- Modifique delegatedUser en la cuenta de KCD en el dispositivo Citrix ADC.
- Modifique el parámetro -delegatedUser en la cuenta de KCD como `host/svc_act.child.parent.com`.

Puntos a tener en cuenta cuando se utilizan cifrados avanzados para configurar la cuenta KCD

> - **Configuración de ejemplo cuando se usa keytab:** `add kcdaccount lbvs_keytab_aes256 -keytab "/nsconfig/krb/kcd2_aes256.keytab"`
> - **Use el siguiente comando cuando keytab tenga varios tipos de cifrado.** El comando también captura los parámetros de usuario del dominio: `add kcdaccount lbvs_keytab_aes256 -keytab "/nsconfig/krb/kcd2_aes256.keytab"-domainUser "HTTP/lbvs.aaa.local"`
> - **Use los siguientes comandos cuando se usen credenciales de usuario:** `add kcdaccount kslb2_user -realmStr AAA.LOCAL -delegatedUser lbvs -kcdPassword <password>`
> - Asegúrese de que se proporciona la información correcta de **domainUser**. Puede buscar el nombre de inicio de sesión del usuario en AD.

Generar el script Keytab KCD

January 12, 2021

El cuadro de diálogo Script de keytab de KCD genera el script keytab, que a su vez genera el archivo keytab necesario para configurar KCD en el dispositivo Citrix ADC.

Para generar el script keytab de KCD mediante la utilidad de configuración

1. Vaya a **Seguridad > AAA: Tráfico de aplicaciones.**
2. En el panel de detalles, en **Delegación restringida de Kerberos**, haga clic en Archivo por lotes para generar keytab.
3. En el cuadro de diálogo Generar KCD (Delegación restringida de Kerberos) **Keytab Script**, rellene los campos como se describe a continuación.
   - **Nombre de usuario del dominio:** nombre del usuario del dominio.
   - **Contraseña de dominio:** contraseña del usuario de dominio.
   - **Principal de servicio:** El principal de servicio.
   - **Nombre de archivo de salida:** Nombre de archivo para el archivo de script KCD.
   - **Crear cuenta de usuario de dominio:** active esta casilla de verificación para crear la cuenta de usuario de dominio especificada.

4. Haga clic en **Generar Script** para generar el script. El script se genera y aparece en el cuadro de texto **Script generado** debajo del botón **Generar Script**.
5. Copie el script y guárdelo como un archivo en el Controller de dominio de AD. Ahora debe ejecutar este script en el Controller de dominio para generar el archivo keytab y, a continuación, copiar el archivo keytab en el directorio /nsconfig/krb/ del dispositivo Citrix ADC.
6. Haga clic en **Aceptar.**

SSO para autenticación básica, resumen y NTLM

August 20, 2021

La configuración de inicio de sesión único (SSO) en Citrix ADC y Citrix Gateway se puede habilitar a nivel global y también por nivel de tráfico. De forma predeterminada, la configuración de SSO está **desactivada** y un administrador puede habilitar el SSO por tráfico o globalmente. Desde el punto de vista de la seguridad, Citrix recomienda a los administradores que **desactiven** el SSO globalmente y habiliten por tráfico. Esta mejora tiene por objeto hacer que la configuración de SSO sea más segura deshonrando cierto tipo de métodos SSO a nivel mundial.

> **Nota:**
>
> Desde la versión 13.0 de la versión 64.35 y superior de la función Citrix ADC, los siguientes tipos de SSO se deshonran en todo el mundo.
>
> - Autentificación básica
> - Autenticación de acceso de resumen
> - NTLM sin negociar la clave NTLM2 o signo de negociación

Tipos de SSO no afectados

Los siguientes tipos de SSO no se ven afectados con esta mejora.

- Autenticación Kerberos
- Autenticación SAML
- Autenticación basada en formularios
- Autenticación al portador de OAuth
- NTLM con Negotiate NTLM2 Clave o Signo de Negociación

Configuraciones de SSO afectadas

A continuación se presentan las configuraciones de SSO afectadas (deshonradas).

Configuraciones globales

```
set tmsessionparam -SSO ON
set vpnparameter -SSO ON
add tmsessionaction tm_act -SSO ON
add vpn sessionaction tm_act -SSO ON
Per traffic configurations
add vpn trafficaction tf_act http -SSO ON
add tm trafficaction tf_act -SSO ON
<!--NeedCopy-->
```

Configuraciones por tráfico

```
add vpn trafficaction tf_act http -SSO ON
add tm trafficaction tf_act -SSO ON
<!--NeedCopy-->
```

> Puede activar o inhabilitar SSO y no puede modificar tipos de SSO individuales.

Medidas de seguridad que deben aplicarse

Como parte de las medidas de seguridad, los tipos de SSO sensibles a la seguridad se deshonran en la configuración global, pero solo se permiten mediante una configuración de acción de tráfico.
Por lo tanto, si un servidor back-end espera Basic, Digest o NTLM sin Negotiate NTLM2 Key o Negotiate Sign, el administrador solo puede permitir el inicio de sesión único mediante la siguiente configuración.

Acción de Tráfico

```
add vpn trafficaction tf_act  http -SSO ON
add tm trafficaction tf_act -SSO ON
<!--NeedCopy-->
```

Directiva de tráfico

```
add tm trafficpolicy <name> <rule> tf_act
add vpn trafficpolicy <name> <rule> tf-act
<!--NeedCopy-->
```


> El administrador debe tener configurada una regla adecuada para la directiva de tráfico para asegurarse de que el SSO esté habilitado solo para el servidor back-end de confianza.

AAA-TM

Casos basados en la configuración global:

```
set tmsessionparam -SSO ON
<!--NeedCopy-->
```

Solución:

```
add tm trafficaction tf_act -SSO ON
add tm trafficpolicy tf_pol true tf_act
<!--NeedCopy-->
```

Enlazar la siguiente directiva de tráfico a todos los servidores virtuales LB donde se espera el SSO:

```
bind lb vserver <LB VS Name> -policy tf_pol -priority 65345
<!--NeedCopy-->
```

Casos basados en la configuración de directiva de sesión:

```
add tmsessionaction tm_act -SSO ON
add tmsession policy <name> <rule> tm_act
add tm trafficaction tf_act -SSO ON
add tm trafficpolicy tf_pol <same rule as session Policy> tf_act
<!--NeedCopy-->
```

Puntos de nota:

- El usuario/grupo AAA de Citrix ADC para la directiva de sesión anterior debe reemplazarse por una directiva de tráfico.
- Enlazar la siguiente directiva a los servidores virtuales de equilibrio de carga para la directiva de sesión anterior,


```
bind lb vserver [LB VS Name] -policy tf_pol -priority 65345
<!--NeedCopy-->
```

- Si se configura una directiva de tráfico con otra prioridad, el comando anterior no funciona correctamente.

La siguiente sección trata de casos basados en conflictos con varias directivas de tráfico asociadas a un tráfico:

Para un tráfico de TM concreto, solo se aplica una directiva de tráfico de TM. Debido a la configuración global de los cambios en las funciones de SSO, la aplicación de una directiva de tráfico de TM adicional con baja prioridad podría no ser aplicable en caso de que ya se haya aplicado una directiva de tráfico de TM con alta prioridad (que no tenga la configuración de SSO necesaria). En la siguiente sección se describe el método para asegurarse de que tales casos se manejan.

Tenga en cuenta que las tres directivas de tráfico siguientes con mayor prioridad se aplican al servidor virtual de equilibrio de carga (LB):

```
add tm trafficaction tf_act1 <Addition config>
add tm trafficaction tf_act2 <Addition config>
add tm trafficaction tf_act3 <Addition config>

add tm trafficpolicy tf_pol1 <rule1> tf_act1
add tm trafficpolicy tf_pol2 <rule2> tf_act2
add tm trafficpolicy tf_pol3 <rule3> tf_act3

bind lb vserver <LB VS Name> -policy tf_pol1 -priority 100
bind lb vserver <LB VS Name> -policy tf_pol2 -priority 200
bind lb vserver <LB VS Name> -policy tf_pol3 -priority 300
<!--NeedCopy-->
```

Método propenso a errores: para resolver la configuración de SSO global, agregue la siguiente configuración:

```
add tm trafficaction tf_act_default -SSO ON
add tm trafficpolicy tf_pol_default true tf_act_default

bind lb vserver <LB VS Name> -policy tf_pol_default -priority 65345
<!--NeedCopy-->
```

Nota: La modificación anterior puede interrumpir el SSO para el tráfico <tf_pol1/tf_pol2/tf_pol3> que afecta a este tráfico, directiva de tráfico <tf_pol_default> no se aplica.

Método correcto: para mitigar esto, la propiedad SSO debe aplicarse individualmente para cada una de las acciones de tráfico correspondientes:

Por ejemplo, en el caso anterior, para que se produzca un SSO para el tráfico que llega a tf_pol1/tf_pol3, se debe aplicar la siguiente configuración junto con <tf_pol_default>.

```
add tm trafficaction tf_act1 <Addition config> -SSO ON
add tm trafficaction tf_act3 <Addition config> -SSO ON
<!--NeedCopy-->
```

Casos de Citrix Gateway

Casos basados en la configuración global:

```
set vpnparameter -SSO ON
<!--NeedCopy-->
```

Solución:

```
add vpn trafficaction vpn_tf_act http  -SSO ON
add vpn trafficpolicy vpn_tf_pol  true vpn_tf_act
bind the following traffic policy to all VPN virtual server where SSO
    is expected:
bind vpn vserver vpn_vs -policy vpn_tf_pol -priority 65345
<!--NeedCopy-->
```

Casos basados en la configuración de directiva de sesión:

```
add vpn sessionaction vpn_sess_act -SSO ON
add vpnsession policy <name> <rule> vpn_sess_act
<!--NeedCopy-->
```

Puntos a tener en cuenta:

- El usuario/grupo AAA de Citrix ADC para la directiva de sesión anterior debe reemplazarse por una directiva de tráfico.
- Enlazar la siguiente directiva a los servidores virtuales LB para la directiva de sesión anterior, `bind lb virtual server [LB VS Name] -policy tf_pol -priority 65345`.

- Si se configura una directiva de tráfico con otra prioridad, el comando anterior no funciona correctamente. En la siguiente sección se tratan los casos basados en conflictos con varias directivas de tráfico asociadas al tráfico.

Casos funcionales basados en conflictos con varias directivas de tráfico asociadas a un tráfico:

Para un tráfico determinado de Citrix Gateway, solo se aplica una directiva de tráfico VPN. Debido a la configuración global de los cambios en las funciones de SSO, es posible que no se aplique una directiva de tráfico VPN adicional con baja prioridad si hay otras directivas de tráfico VPN con alta prioridad que no tienen una configuración de SSO necesaria.

En la siguiente sección se describe el método para asegurarse de que se manejan estos casos:

Tenga en cuenta que hay tres directivas de tráfico con mayor prioridad aplicadas a un servidor virtual VPN:

```
add vpn trafficaction tf_act1 <Addition config>
add vpn trafficaction tf_act2 <Addition config>
add vpn trafficaction tf_act3 <Addition config>

add vpn trafficpolicy tf_pol1 <rule1> tf_act1
add vpn trafficpolicy tf_pol2 <rule2> tf_act2
add vpn trafficpolicy tf_pol3 <rule3> tf_act3

bind vpn vserver <VPN VS Name> -policy tf_pol1 -priority 100
bind vpn vserver <VPN VS Name> -policy tf_pol2 -priority 200
bind vpn vserver <VPN VS Name> -policy tf_pol3 -priority 300
<!--NeedCopy-->
```

Método propenso a errores: para resolver la configuración de SSO global, agregue la siguiente configuración:

```
add vpn trafficaction tf_act_default -SSO ON
add vpn trafficpolicy tf_pol_default true tf_act_default

bind vpn vserver <VPN VS Name> -policy tf_pol_default -priority 65345
<!--NeedCopy-->
```

Nota: La modificación anterior puede interrumpir el SSO para el tráfico que afecta <tf_pol1/tf_pol2/tf_pol3> como para este tráfico, directiva de tráfico <tf_pol_default> no se aplica.

Método correcto: Para mitigar esto, la propiedad SSO debe aplicarse individualmente para cada una de las acciones de tráfico correspondientes.

Por ejemplo, en el caso anterior, para que se produzca un SSO para el tráfico que llega a tf_pol1/tf_pol3, se debe aplicar la siguiente configuración junto con <tf_pol_default>.

```
add vpn trafficaction tf_act1 [Additional config] -SSO ON

add vpn trafficaction tf_act3 [Additional config] -SSO ON
<!--NeedCopy-->
```

Reescritura para las respuestas generadas por Citrix Gateway y el servidor de autenticación

August 20, 2021

Rewrite se refiere a la reescritura de cierta información en las solicitudes o respuestas manejadas por el dispositivo Citrix ADC. La reescritura puede ayudar a proporcionar acceso al contenido solicitado sin exponer detalles innecesarios sobre la configuración real del sitio web. Para obtener información detallada sobre el concepto de reescritura, consulte Reescritura

A partir de la compilación 13.0-76.29 de la versión de Citrix ADC, la compatibilidad con directivas de reescritura se ha ampliado al servidor virtual de Citrix Gateway y a las respuestas generadas por el servidor virtual de autenticación.

> **Nota**
>
> Se introduce un tipo de enlace **AAA_Response** para admitir las directivas de reescritura del servidor virtual Citrix Gateway y las respuestas generadas por el servidor virtual de autenticación.

Ejemplo para utilizar Rewrite

Puede utilizar Rewrite para compartir los recursos disponibles en Citrix ADC local con la implementación de Citrix Cloud. Esto se puede lograr de forma segura implementando el uso compartido de recursos de origen CORS. La reescritura se puede utilizar de la siguiente manera para implementar el encabezado CORS.

Configuración de ejemplo

```
add rewrite action cors_header_action insert_http_header access-control
    -allow-credentials \"true\"

```



```
3 add rewrite policy cors_header_pol true cors_header_action
4
5 add rewrite action non_cors_header_action insert_http_header X-Frame-
    Options \'\"DENY\"\'
6
7 add rewrite policy non_cors_header_pol true non_cors_header_action
8
9 bind authentication vserver av_cors -policy cors_header_pol -priority
    100 -type AAA_RESPONSE
10
11 bind vpn vserver av_cors -policy cors_header_pol -priority 100 -type
    AAA_RESPONSE
```

Compatibilidad del encabezado de respuesta de la directiva de seguridad de contenido para Citrix Gateway y respuestas generadas por servidor virtual de autenticación

July 8, 2022

A partir de la versión 13.0—76.29 de Citrix ADC, se admite el encabezado de respuesta Content-Security-Policy (CSP) para las respuestas generadas por el servidor virtual de autenticación y Citrix Gateway.

El encabezado de respuesta Content-Security-Policy (CSP) es una combinación de directivas que el explorador web utiliza para evitar ataques de scripting entre sitios (CSS).
El encabezado de respuesta HTTP CSP permite a los administradores del sitio web controlar los recursos que el agente de usuario puede cargar para una página determinada. Salvo algunas excepciones, las directivas implican principalmente la especificación de orígenes de servidores y puntos finales de script. Esto ayuda a protegerse contra los ataques de scripts entre sitios.
El encabezado CSP está diseñado para modificar la forma en que los exploradores procesan las páginas y, por lo tanto, para protegerse de varias inyecciones entre sitios, incluido CSS. Es importante establecer el valor del encabezado correctamente, de forma que no impida el correcto funcionamiento del sitio web. Por ejemplo, si el encabezado está configurado para evitar la ejecución de JavaScript en línea, el sitio web no debe utilizar JavaScript en línea en sus páginas.

Estas son las ventajas del encabezado de respuesta del CSP.

- La función principal de un encabezado de respuesta CSP es evitar ataques CSS.
- Además de restringir los dominios desde los que se puede cargar el contenido, el servidor puede especificar qué protocolos se pueden utilizar; por ejemplo (e idealmente, desde el punto de

vista de la seguridad), un servidor puede especificar que todo el contenido debe cargarse mediante HTTPS.

- CSP ayuda a proteger Citrix ADC de ataques de scripts entre sitios protegiendo archivos como “tmindex.html” y “homepage.html. El archivo “tmindex.html” está relacionado con la autenticación y el archivo “homepage.html” está relacionado con los enlaces o aplicaciones publicados.

Configuración del encabezado Content-Security-Policy para las respuestas generadas por el servidor virtual de autenticación y Citrix Gateway

Para habilitar el encabezado CSP, debe configurar su servidor web para que devuelva el encabezado HTTP del CSP.

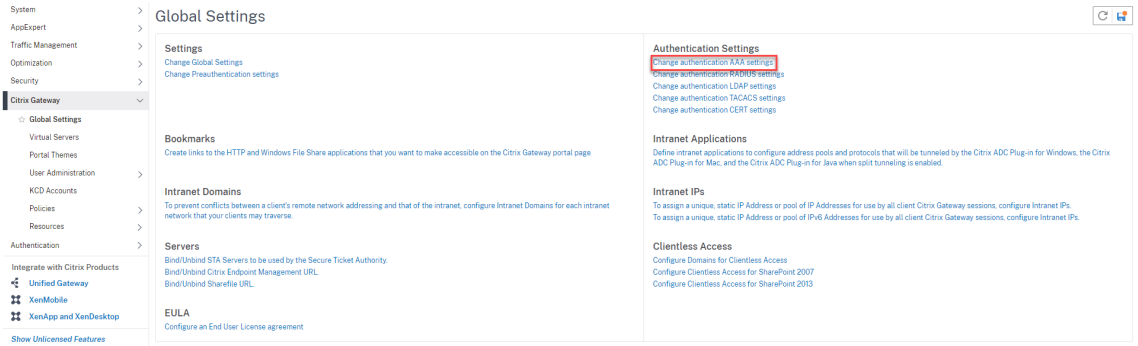
> **Puntos que tener en cuenta**
>
> - De forma predeterminada, el encabezado CSP está inhabilitado.
> - Al habilitar o inhabilitar la directiva CSP predeterminada, se recomienda ejecutar el siguiente comando. `Flush cache contentgroup loginstaticobjects`
> - Para modificar el CSP para /logon/LogonPoint/index.html, modifique el valor “Header set Content-Security-Policy”. según sea necesario en la sección correspondiente al directorio de inicio de sesión que se encuentra en el directorio `/var/netscaler/logon`.

Para configurar CSP para el servidor virtual de autenticación y las respuestas generadas por Citrix Gateway mediante CLI, escriba el siguiente comando en el símbolo del sistema:

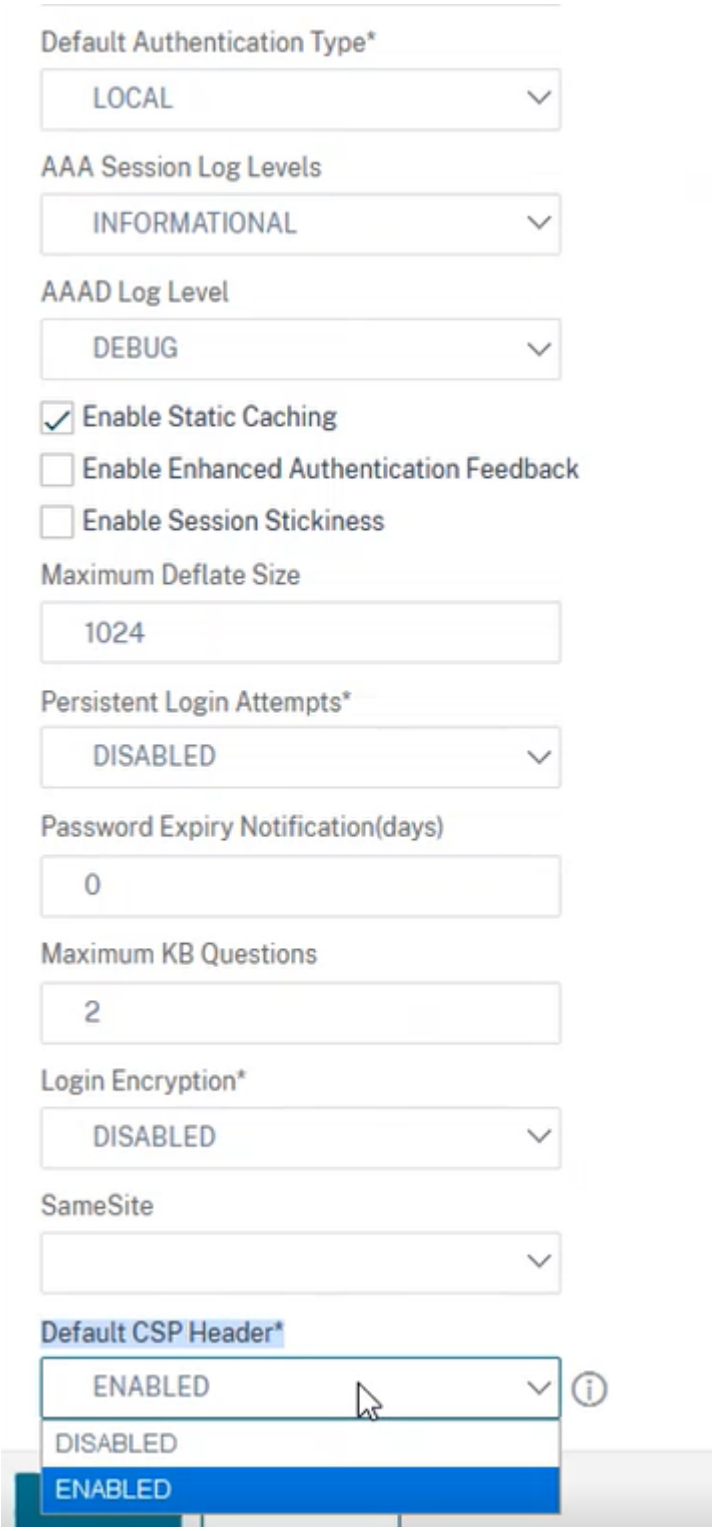
```
1 set aaa parameter -defaultCSPHeader <ENABLE/DISABLE>
```

Para configurar CSP para Citrix Gateway y autenticar las respuestas generadas por el servidor virtual mediante GUI.

1. Vaya a **Citrix Gateway > Configuración global**y haga clic en **Cambiar configuración AAA de autenticación** en Configuración de autenticación.



2. En la página **Configurar parámetros AAA**, seleccione el campo **Habilitado en encabezado CSP predeterminado** .



Ejemplo de personalización del encabezado Content-Security-Policy

A continuación se muestra un ejemplo de personalización del encabezado CSP para incluir imágenes y scripts solo de los dos orígenes especificados siguientes, respectivamente, `https://company.fqdn.com, https://example.com.`

Configuración de ejemplo

```
add rewrite action modify_csp insert_http_header Content-Security-Policy "\"default-src 'self'; script-src 'self' https://company.fqdn.com 'unsafe-inline' 'unsafe-eval'; connect-src 'self'; img-src http://localhost:* https://example.com 'self' data: http: https:; style-src 'self' 'unsafe-inline'; font-src 'self'; frame-src 'self'; child-src 'self' com.citrix.agmacepa://* citrixng://* com.citrix.nsgclient://*; form-action 'self'; object-src 'self'; report-uri /nscsp_violation/report_uri\""

add rewrite policy add_csp true modify_csp

bind authentication vserver auth1 -policy add_csp -priority 1 -gotoPriorityExpression NEXT -type AAA_RESPONSE
```

Restablecimiento personal de contraseñas

May 8, 2022

El restablecimiento de contraseñas de autoservicio es una solución de administración de contraseñas basada en la web. Está disponible tanto en la función de autenticación, autorización y auditoría del dispositivo Citrix ADC como en Citrix Gateway. Elimina la dependencia del usuario de la asistencia del administrador para cambiar la contraseña.

El restablecimiento de contraseña de autoservicio proporciona al usuario final la capacidad de restablecer o crear una contraseña de forma segura en los siguientes casos:

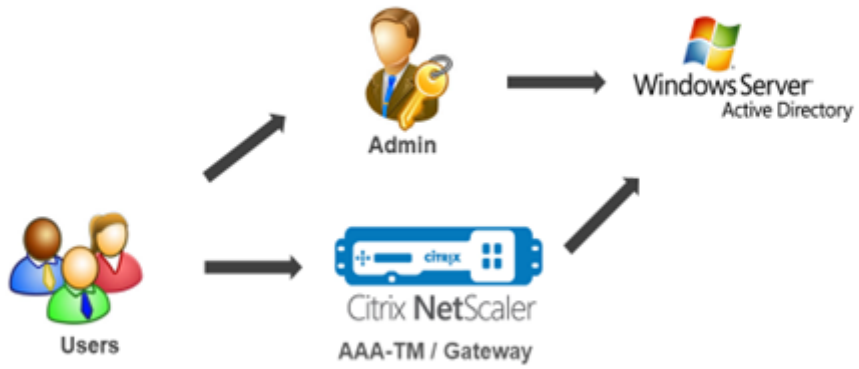
- El usuario ha olvidado la contraseña.
- El usuario no puede iniciar sesión.

Hasta ahora, si un usuario final olvida una contraseña de AD, el usuario final tenía que ponerse en contacto con el administrador de AD para restablecer la contraseña. Con la función de restablecimiento de contraseña de autoservicio, un usuario final puede restablecer la contraseña sin la intervención del administrador.

Los siguientes son algunos de los beneficios de usar el restablecimiento de contraseña de autoservicio:

- Aumento de la productividad mediante el mecanismo de cambio automático de contraseña, que elimina el tiempo de espera para que los usuarios esperen a que se restablezcan las contraseñas.
- Con el mecanismo de cambio automático de contraseña, los administradores pueden concentrarse en otras tareas críticas.

La siguiente ilustración ilustra el flujo de restablecimiento de contraseñas de autoservicio para restablecer la contraseña.



Para usar el restablecimiento automático de contraseñas, un usuario debe estar registrado en la autenticación, autorización y auditoría de Citrix o en el servidor virtual de Citrix Gateway.

El restablecimiento de contraseñas de autoservicio proporciona las siguientes capacidades:

- **Autorregistro de nuevos usuarios.** Puede registrarse como nuevo usuario.
- **Configure las preguntas basadas en el conocimiento.** Como administrador, puede configurar un conjunto de preguntas para los usuarios.
- **Registro de ID de correo electrónico alternativo.** Debe proporcionar una identificación de correo electrónico alternativa durante el registro. La OTP se envía a la ID de correo electrónico alternativa porque el usuario ha olvidado la contraseña de la ID de correo electrónico principal.

> **Nota:**
>
> A partir de la versión 12.1 build 51.xx, el registro de ID de correo electrónico alternativo se puede realizar de forma independiente. Se introduce un nuevo esquema de inicio de

> sesión, **AltEmailRegister.xml**, para realizar solo el registro alternativo de ID de correo electrónico. Anteriormente, el registro de ID de correo electrónico alternativo solo se podía realizar mientras se realizaba el registro de KBA.

- **Restablecer la contraseña olvidada.** El usuario puede restablecer la contraseña respondiendo a las preguntas basadas en el conocimiento. Como administrador, puede configurar y almacenar las preguntas.

El restablecimiento de contraseña de autoservicio proporciona los dos mecanismos de autenticación nuevos siguientes:

- **Preguntas y respuestas basadas en el conocimiento.** Debe registrarse en la autenticación, autorización y auditoría de Citrix o en Citrix Gateway antes de seleccionar el esquema de preguntas y respuestas basado en el conocimiento.
- **Autenticación OTP de correo** Se envía una OTP al ID de correo electrónico alternativo, que el usuario registró durante el registro de restablecimiento de contraseña de autoservicio.

> **Nota**
>
> Estos mecanismos de autenticación se pueden usar para los casos de uso de restablecimiento de contraseña de autoservicio y para cualquier propósito de autenticación similar a cualquiera de los mecanismos de autenticación existentes.

Requisitos previos

Antes de configurar el restablecimiento de contraseña de autoservicio, revise los siguientes requisitos previos:

- Versión 12.1 de la función Citrix ADC, compilación 50.28.
- La versión admitida es el nivel de función de dominio de AD 2016, 2012 y 2008.
- El nombre de usuario ldapBind enlazado a Citrix ADC debe tener acceso de escritura a la ruta de AD del usuario.

  > **Nota**
  >
  > El restablecimiento de contraseña de autoservicio solo se admite en el flujo de autenticación nFactor. Para obtener más información, consulte Autenticación de nFactor mediante Citrix ADC.

Limitaciones

A continuación se presentan algunas de las limitaciones del restablecimiento de contraseñas de autoservicio:

- El restablecimiento de contraseñas de autoservicio se admite en LDAPS. El restablecimiento de contraseñas de autoservicio solo está disponible si el back-end de autenticación es LDAP (protocolo LDAP).
- El usuario no puede ver el ID de correo electrónico alternativo ya registrado.
- Las preguntas y respuestas basadas en el conocimiento, y la autenticación y el registro de OTP por correo electrónico no pueden ser el primer factor en el flujo de autenticación.
- Para el complemento nativo y Receiver, el registro solo se admite a través del explorador.
- El tamaño mínimo de certificado utilizado para el restablecimiento de contraseñas de autoservicio es de 1024 bytes y debe seguir el estándar x.509.

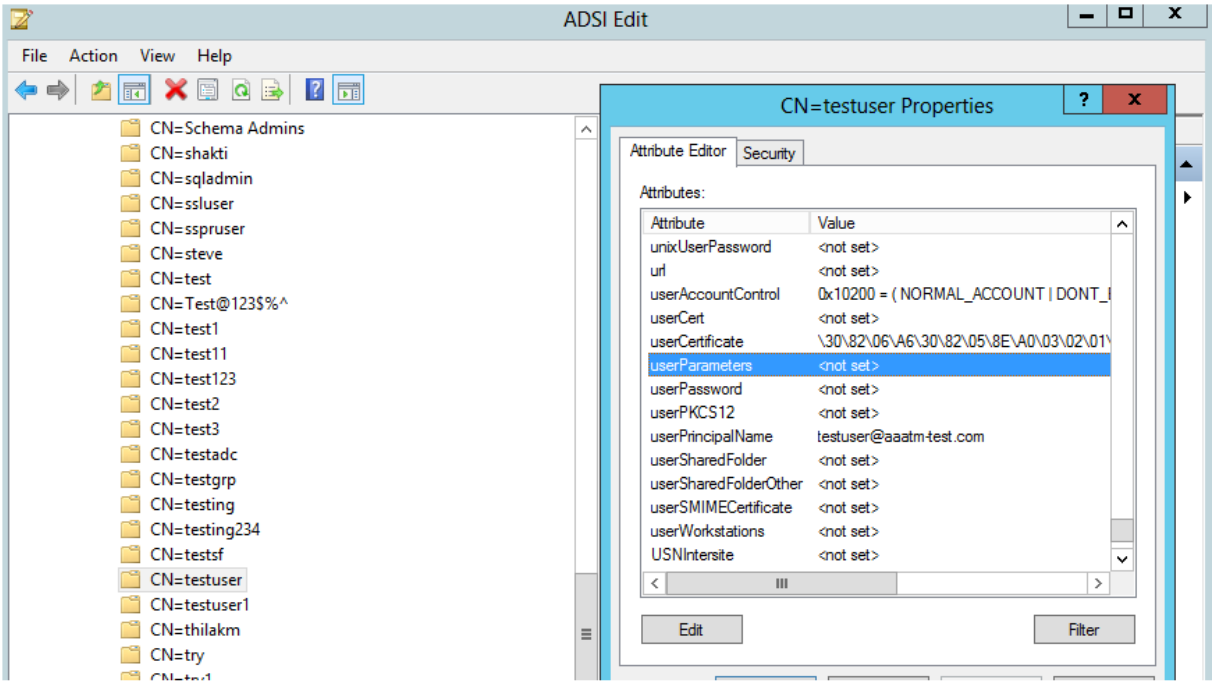
Configuración de Active Directory

Las preguntas y respuestas basadas en el conocimiento de Citrix ADC y la OTP de correo electrónico utilizan un atributo de AD para almacenar los datos de los usuarios. Debe configurar un atributo de AD para almacenar las preguntas y respuestas junto con el ID de correo electrónico alternativo. El dispositivo Citrix ADC lo almacena en el atributo KB configurado en el objeto de usuario de AD. Al configurar un atributo de AD, tenga en cuenta lo siguiente:

- La longitud del atributo debe tener al menos 128 caracteres.
- El atributo de AD debe admitir una longitud máxima de 32 000 valores.
- El tipo de atributo debe ser un “DirectoryString”.
- Se puede utilizar un único atributo de AD para las preguntas y respuestas basadas en el conocimiento y el ID de correo electrónico alternativo.
- No se puede usar un solo atributo de AD para el registro de preguntas y respuestas basadas en el conocimiento y OTP nativo ni en el registro de ID de correo electrónico alternativo
- El administrador LDAP de Citrix ADC debe tener acceso de escritura al atributo AD seleccionado.

También puede usar un atributo de AD existente. Sin embargo, asegúrese de que el atributo que piensa usar no se use en otros casos. Por ejemplo, userParameters es un atributo existente dentro del usuario de AD que puede usar. Para verificar este atributo, lleve a cabo los siguientes pasos:

1. Vaya a **ADSI > seleccione usuario**.
2. Haga clic derecho y desplácese hacia abajo hasta la lista de atributos
3. En el panel de la ventana **CN=TestUser Properties**, puede ver que el atributo **userParameters** no está establecido.



Registro de restablecimiento de contraseña de autoservicio

Para implementar la solución de restablecimiento de contraseñas de autoservicio en un dispositivo Citrix ADC, debe realizar lo siguiente:

- Registro de restablecimiento de contraseña de autoservicio (preguntas y respuestas/ID de correo electrónico basadas en el conocimiento).
- Página de inicio de sesión del usuario (para restablecer la contraseña, que incluye preguntas y respuestas basadas en el conocimiento y validación OTP por correo electrónico y factor de restablecimiento de contraseña final).

Se proporciona un conjunto de catálogos de preguntas predefinidos como un archivo JSON. Como administrador, puede seleccionar las preguntas y crear el esquema de inicio de sesión de registro de restablecimiento de contraseña de autoservicio a través de la GUI de Citrix ADC. Puede elegir cualquiera de las siguientes opciones:

- Seleccione un máximo de cuatro preguntas definidas por el sistema.
- Proporcionar una opción para que los usuarios personalicen dos preguntas y respuestas.

Para ver el archivo JSON de preguntas basadas en el conocimiento predeterminado desde la CLI

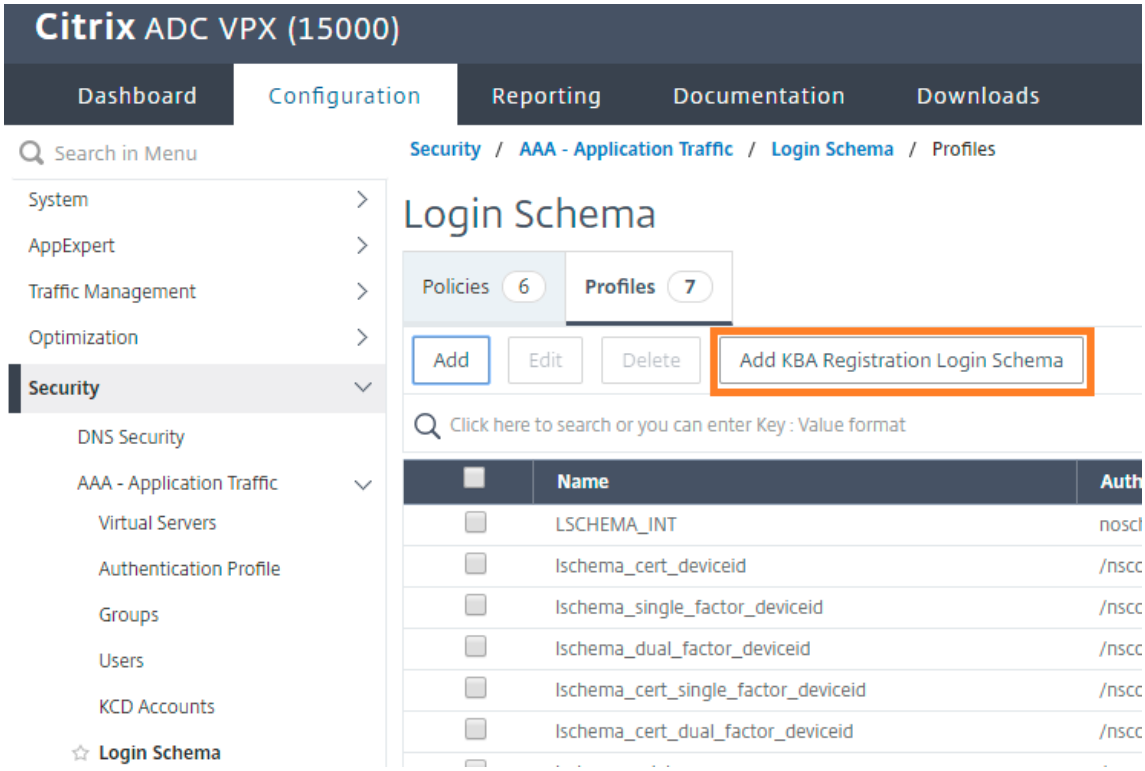
```
root@ns# cd /nsconfig/loginschema/LoginSchema/
root@ns# cat KBQuestions.json
[
    {"question":"What is the last name of the teacher who gave you your first failing
grade?"},
    {"question":"What is the name of your favourite childhood friend?"},
    {"question":"Where were you when you first heard about 9/11?"},
    {"question":"What is the name of a college you applied to but didn't attend?"},
    {"question":"What was the last name of your third grade teacher?"},
    {"question":"What was the name of your first stuffed animal?"},
    {"question":"What is the name of the teacher who gave you your first A?"},
    {"question":"What is the name of the city where you got lost?"},
    {"question":"In what city or town did your mother and father meet?"},
    {"question":"What was your most hated food as a child?"},
    {"question":"What was your most favourite food as a child?"},
    {"question":"What is your favourite website?"},
    {"question":"What is your most disliked website?"},
    {"question":"What is your dream job?"},
    {"question":"Why did the chicken cross the road?"},
    {"question":"Name your first boss."},
    {"question":"What is the name of your favorite school teacher?"},
    {"question":"What is the name of your favorite actor or actress?"},
    {"question":"What is the title of your favorite movie?"},
    {"question":"In what city or town did you spend most of your youth?"}
]
```

Nota

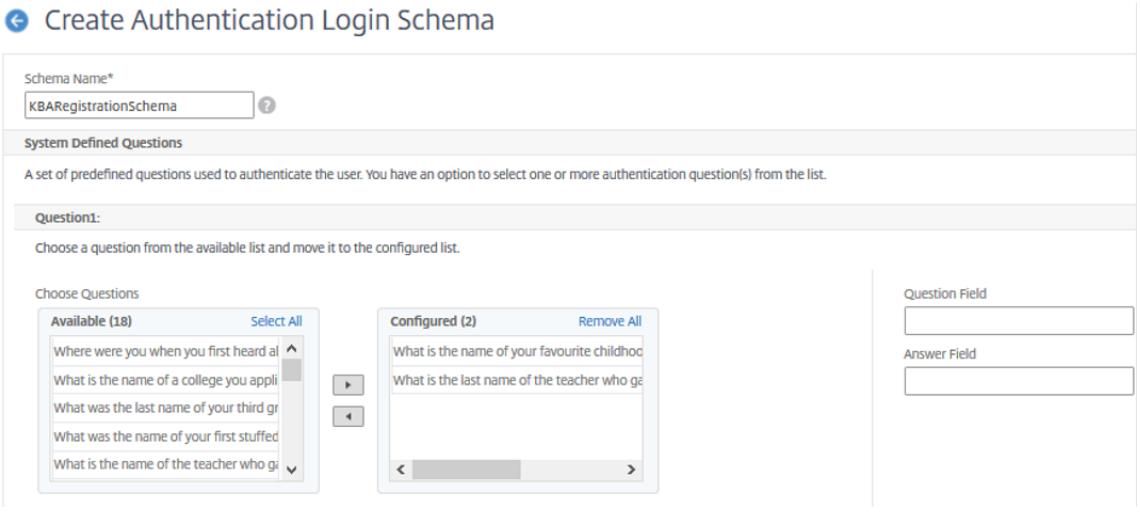
- Citrix Gateway incluye el conjunto de preguntas definidas por el sistema de forma predeterminada. El administrador puede modificar el archivo “KBQuestions.json” para incluir las preguntas de su elección.
- Las preguntas definidas por el sistema solo se muestran en inglés y no están disponibles en otros idiomas.

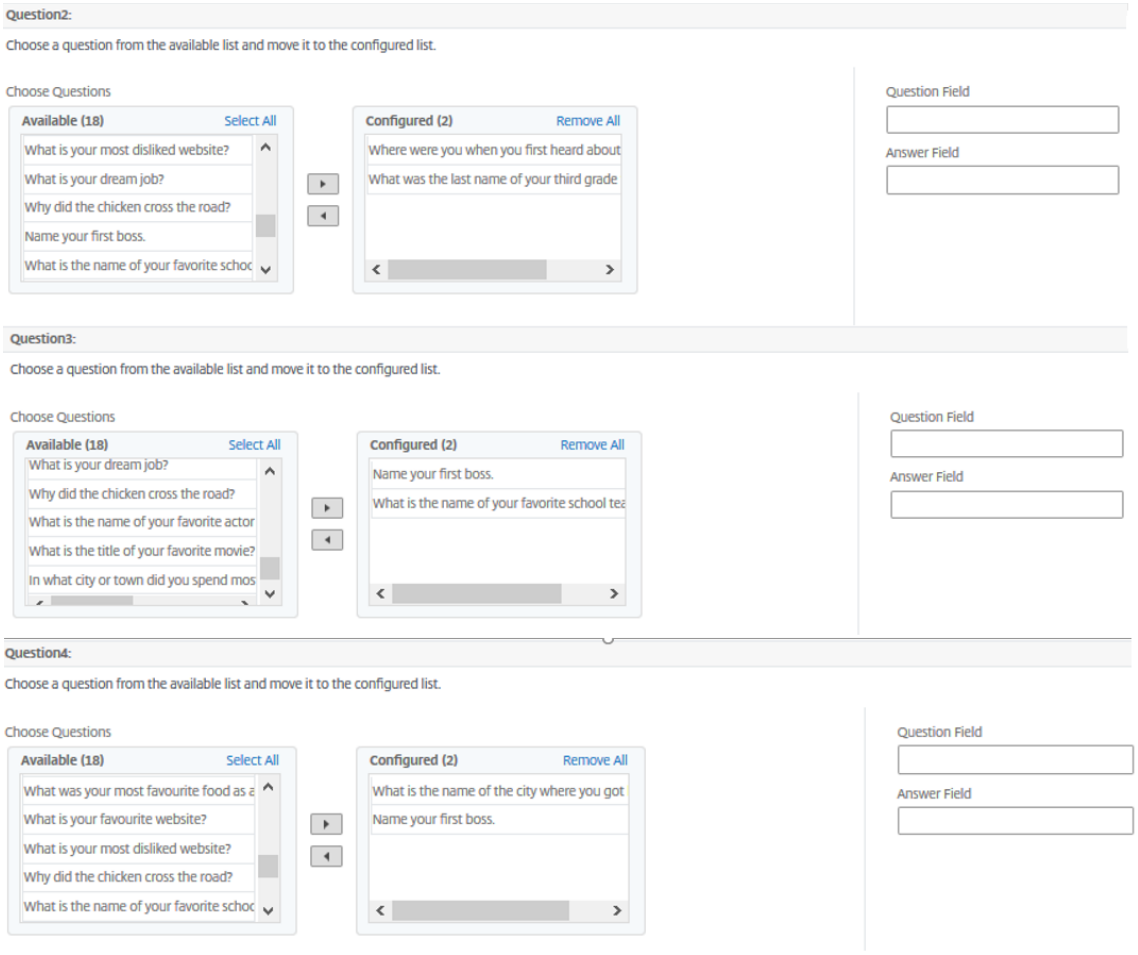
Para completar el esquema de inicio de sesión de registro de preguntas y respuestas basado en el conocimiento

1. Vaya a **Seguridad > AAA — Tráfico de aplicaciones > Esquema de inicio de sesión**.

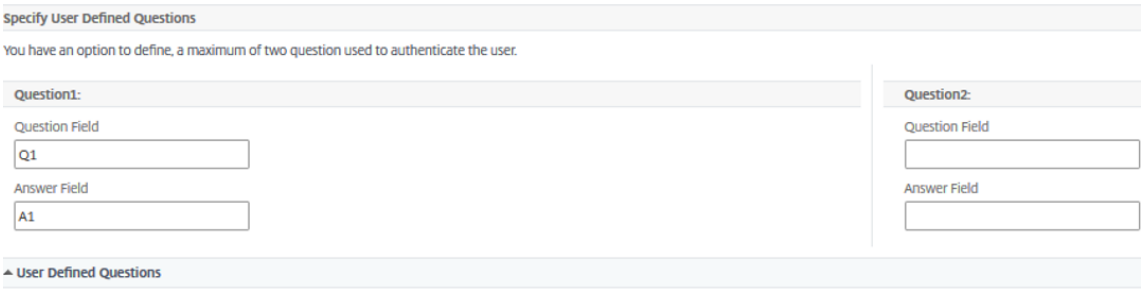


2. En la página **Esquema de inicio** de sesión, haga clic en **Perfiles**.
3. Haga clic en **Agregar esquema de inicio de sesión de registro**de
4. En la página **Crear esquema de inicio de sesión de autenticación**, especifique un nombre en el campo **Nombre del esquema**.

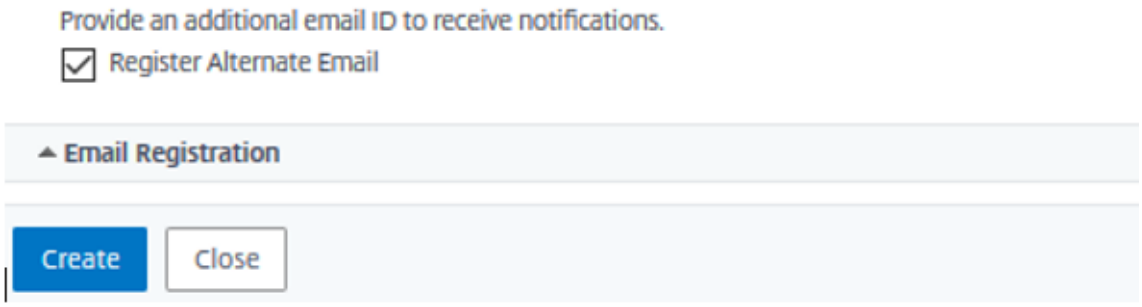




5. Seleccione las preguntas de su elección y muévalas a la lista **Configuradas**.
6. En la sección **Preguntas definidas por el usuario**, puede proporcionar preguntas y respuestas en los campos Q1 y A1.



7. En la sección **Registro de correo electrónico**, marque la opción **Registrar correo electrónico alternativo**. Puede registrar el **ID de correo electrónico alternativo** desde la página de inicio de sesión de registro de usuario para recibir la OTP.



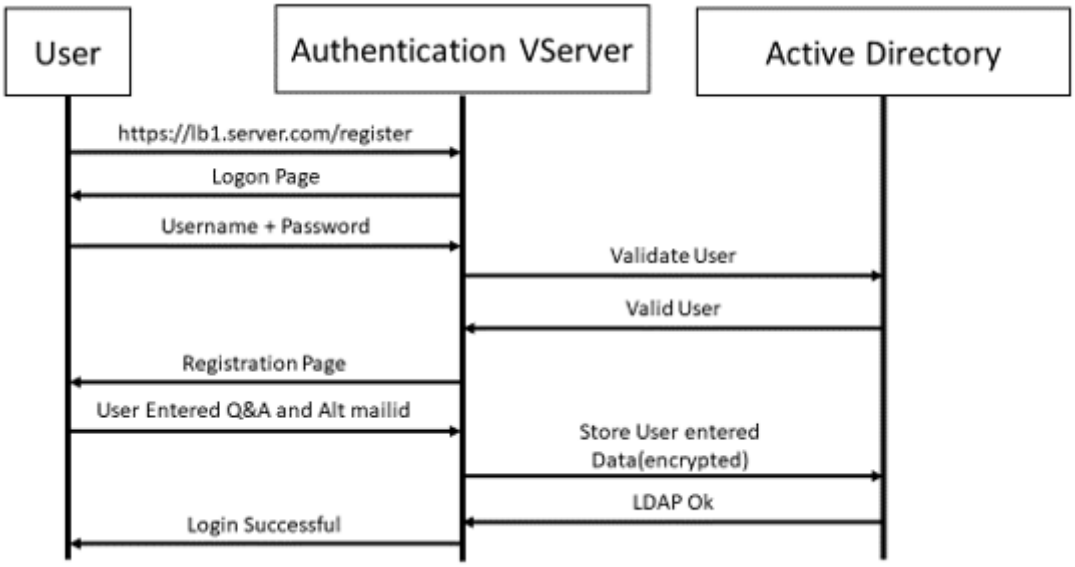
8. Haga clic en **Create**. El esquema de inicio de sesión, una vez generado, muestra todas las preguntas configuradas al usuario final durante el proceso de registro.

Crear un flujo de trabajo de registro y administración de usuarios mediante

Se requiere lo siguiente antes de comenzar la configuración:

- Dirección IP asignada al servidor virtual de autenticación
- FQDN correspondiente a la dirección IP asignada
- Certificado de servidor para servidor virtual de autenticación

Para configurar la página de registro y administración de dispositivos, necesita un servidor virtual de autenticación. La siguiente ilustración ilustra el registro del usuario.



Para crear un servidor virtual de autenticación

1. Configure un servidor virtual de autenticación. Debe ser de tipo SSL y asegúrese de vincular el servidor virtual de autenticación con el tema del portal.


```
> add authentication vserver <vServerName> SSL <ipaddress> <port>
> bind authentication vserver <vServerName> [-portaltheme<string>]
```

2. Vincular el par de certificados y claves de servidor virtual SSL.

```
> bind ssl vserver <vServerName> certkeyName <string>
```

Ejemplo:

```
> add authentication vserver authvs SSL 1.2.3.4 443
> bind authentication vserver authvs -portaltheme RFWebUI
> bind ssl vserver authvs -certkeyname c1
```

Para crear una acción de inicio de sesión LDAP

```
    > add authentication ldapAction <name> {
-serverIP <ipaddr|ipv6_addr|> [-serverPort <port>] [-ldapBase <BASE> ]
     [-ldapBindDn <AD USER>] [-ldapBindDnPassword <PASSWORD>] [-
    ldapLoginName <USER FORMAT>]
```

> **Nota**
>
> Puede configurar cualquier directiva de autenticación como primer factor.

Ejemplo:

```
    > add authentication ldapAction ldap_logon_action -serverIP 1.2.3.4
      -serverPort 636 -ldapBase "OU=Users,DC=server,DC=com" -
     ldapBindDn administrator@ctxnsdev.com -ldapBindDnPassword
     PASSWORD -ldapLoginName samAccountName -serverport 636 -sectype
     SSL -KBAttribute userParameters
```

Para crear una directiva de autenticación para el inicio de sesión LDAP

```
    > add authentication policy <name> <rule> [<reqAction]
```


Ejemplo:

```
> add authentication policy ldap_logon -rule true -action
   ldap_logon_action
```

Para crear una acción de registro de preguntas y respuestas basada en el conocimiento

Se introducen dos nuevos parámetros en `ldapAction`. `KBAttribute` para la autenticación KBA (registro y validación) y `alternateEmailAttr` para el registro del ID de correo electrónico alternativo del usuario.

```
> add authentication ldapAction <name> {
-serverIP  <ipaddr|ipv6_addr|> [-serverPort <port>] [-ldapBase <BASE>
   ] [-ldapBindDn <AD USER>] [-ldapBindDnPassword <PASSWORD>] [-
   ldapLoginName <USER FORMAT>] [-KBAttribute <LDAP ATTRIBUTE>] [-
   alternateEmailAttr <LDAP ATTRIBUTE>]
```

Ejemplo:

```
> add authentication ldapAction ldap1 -serverIP 1.2.3.4 -sectype
   ssl -serverPort 636 -ldapBase "OU=Users,DC=server,DC=com" -
   ldapBindDn administrator@ctxnsdev.com -ldapBindDnPassword
   PASSWORD -ldapLoginName samAccountName -KBAttribute
   userParameters -alternateEmailAttr userParameters
```

Mostrar la pantalla de registro y administración de usuarios

El esquema de inicio de sesión "KBARegistrationSchema.xml" se utiliza para mostrar la página de registro del usuario al usuario final. Utilice la siguiente CLI para mostrar el esquema de inicio de sesión.

```
> add authentication loginSchema <name> -authenticationSchema <string>
```

Ejemplo:

```
> add authentication loginSchema kba_register -authenticationSchema /
   nsconfig/loginschema/LoginSchema/KBARegistrationSchema.xml
```


Citrix recomienda dos formas de mostrar la pantalla de administración y registro de usuarios: URL o atributo LDAP.

Uso de URL

Si la ruta de la URL contiene "/register" (por ejemplo, https://lb1.server.com/register), la página de registro del usuario se muestra con la URL.

Para crear y vincular una directiva de registro

```
1 > add authentication policylabel user_registration -loginSchema
    kba_register
2 > add authentication policy ldap1 -rule true -action ldap1
3 > bind authentication policylabel user_registration -policy ldap1 -
    priority 1
```

Para vincular la directiva de autenticación al servidor virtual de autenticación, autorización y auditoría cuando la dirección URL contiene '/register'

```
1 > add authentication policy ldap_logon -rule "http.req.cookie.value(\"
    NSC_TASS\").contains(\"register\")" -action ldap_logon
2 > bind authentication vserver authvs -policy ldap_logon -nextfactor
    user_registration -priority 1
```

Para enlazar certificado a VPN global

```
1 bind vpn global -userDataEncryptionKey c1
```

> **Nota**
>
> - Debe vincular el certificado para cifrar los datos de usuario (preguntas y respuestas de KB e ID de correo electrónico alternativo registrado) almacenados en el atributo AD.
> - Si el certificado caduca, debe vincular un certificado nuevo y volver a realizar el registro.

Uso de atributo

Puede vincular una directiva de autenticación al servidor virtual de autenticación, autorización y auditoría para comprobar si el usuario ya está registrado o no. En este flujo, cualquiera de las directivas anteriores antes del factor de registro de preguntas y respuestas basado en el conocimiento debe ser LDAP con el atributo KBA configurado. Esto es para comprobar si el usuario de AD está registrado o no utiliza un atributo de AD.

> **Importante**
>
> La regla "AAA.USER.ATTRIBUTE("kba_registered").EQ("0")" obliga a los nuevos usuarios a registrarse para recibir preguntas basadas en conocimientos y respuestas y correo electrónico alternativo.

Para crear una directiva de autenticación para comprobar si el usuario aún no está registrado

```
1 > add authentication policy switch_to_kba_register -rule "AAA.USER.
    ATTRIBUTE(\"kba_registered\").EQ(\"0\")" -action NO_AUTHN
2 > add authentication policy first_time_login_forced_kba_registration -
    rule true -action ldap1
```

Para crear una etiqueta de directiva de registro y vincularla a la directiva de registro LDAP

```
1 > add authentication policylabel auth_or_switch_register -loginSchema
    LSCHEMA_INT
2 > add authentication policylabel kba_registration -loginSchema
    kba_register
3
4 > bind authentication policylabel auth_or_switch_register -policy
    switch_to_kba_register -priority 1 -nextFactor kba_registration
5 > bind authentication policylabel kba_registration -policy
    first_time_login_forced_kba_registration -priority 1
```

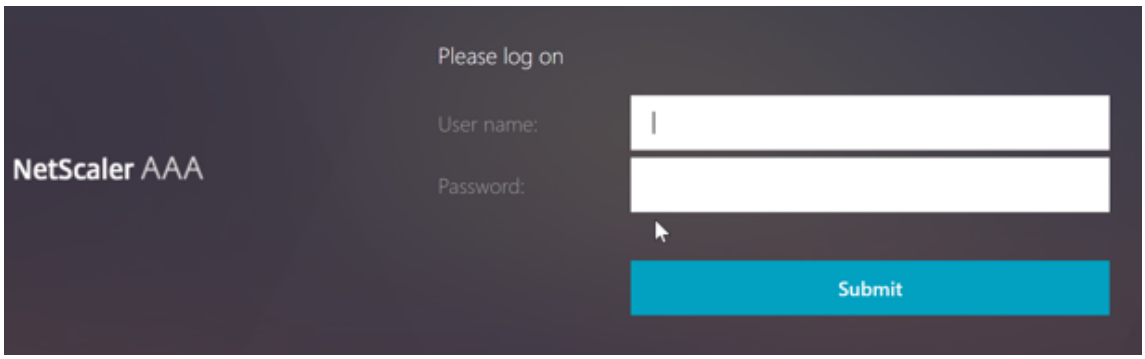
Para vincular la directiva de autenticación al servidor virtual de autenticación, autorización y auditoría

```
1 bind authentication vserver authvs -policy ldap_logon -nextfactor
    auth_or_switch_register -priority 2
```

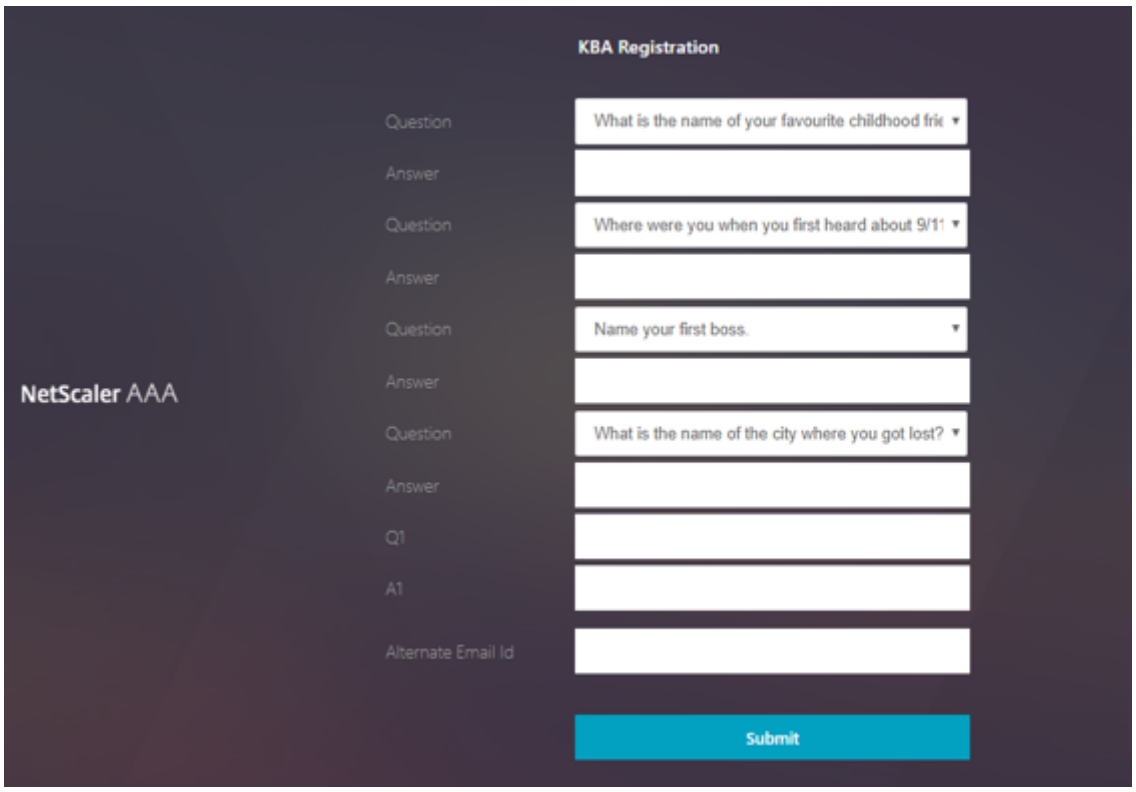

Registro de usuarios y validación de gestión

Una vez que haya configurado todos los pasos mencionados en las secciones anteriores, debe ver la siguiente pantalla de IU.

1. Introduzca la URL del servidor virtual lb; por ejemplo, https://lb1.server.com. Se muestra la pantalla de inicio de sesión.



2. Introduzca el nombre de usuario y la contraseña. Haga clic en **Submit**. Se muestra la pantalla **Registro de usuario**.



3. Seleccione la pregunta preferida en la lista desplegable e introduzca la **respuesta**.
4. Haga clic en **Submit**. Se muestra la pantalla de registro de usuario con éxito.

Configurar página de inicio de sesión de usuario

En este ejemplo, el administrador asume que el primer factor es el inicio de sesión de LDAP (para el que el usuario final ha olvidado la contraseña). A continuación, el usuario sigue el registro de preguntas y respuestas basado en el conocimiento y la validación OTP de ID de correo electrónico y, finalmente, restablece la contraseña mediante el restablecimiento de contraseña de autoservicio.

Puede utilizar cualquiera de los mecanismos de autenticación para el restablecimiento de contraseñas de autoservicio. Citrix recomienda tener una pregunta y una respuesta basadas en el conocimiento, y enviar un correo electrónico OTP o ambos para lograr una privacidad sólida y evitar cualquier restablecimiento ilegítimo de contraseñas de usuario.

Se requiere lo siguiente antes de empezar a configurar la página de inicio de sesión del usuario:

- IP para servidor virtual de equilibrador de carga
- FQDN correspondiente para el servidor virtual del equilibrador de carga
- Certificado de servidor para el equilibrador de carga

Crear un servidor virtual de equilibrador de carga mediante la CLI

Para acceder al sitio web interno, debe crear un servidor virtual LB para hacer frente al servicio back-end y delegar la lógica de autenticación en el servidor virtual de autenticación.

```
1 > add lb vserver lb1 SSL 1.2.3.162 443 -persistenceType NONE -
     cltTimeout 180 -AuthenticationHost otpauth.server.com -
     Authentication ON -authnVsName authvs
2
3 > bind ssl vserver lb1 -certkeyname c1
```

Para representar el servicio de back-end en el equilibrio de carga:

```
1 > add service iis_backendsso_server_com 1.2.3.4 HTTP 80
2
3 > bind lb vserver lb1 iis_backendsso_server_com
```

Crear acción LDAP con autenticación inhabilitada como primera directiva

```
1 > add authentication ldapAction ldap3 -serverIP 1.2.3.4 -serverPort 636
      -ldapBase "OU=Users,DC=server,DC=com" -ldapBindDn
     administrator@ctxnsdev.com -ldapBindDnPassword PASSWORD -
     ldapLoginName samAccountName -authentication disabled
```



```
2
3 > add authentication policy ldap3 -rule aaa.LOGIN.VALUE(”passwdreset”).
     EQ(”1”) -action ldap3
```

Crear una acción de validación de preguntas y respuestas basada en el conocimiento

Para la validación de preguntas y respuestas basada en el conocimiento en el flujo de restablecimiento de contraseñas de autoservicio, debe configurar el servidor LDAP con la autenticación inhabilitada.

```
1 > add authentication ldapAction <LDAP ACTION NAME> -serverIP <SERVER IP
     > -serverPort <SERVER PORT> -ldapBase <BASE> -ldapBindDn <AD USER> -
     ldapBindDnPassword <PASSWORD> -ldapLoginName <USER FORMAT> -
     KBAttribute  <LDAP ATTRIBUTE> - alternateEmailAttr <LDAP ATTRIBUTE>
     -authentication DISABLED
```

Ejemplo:

```
1 > add authentication ldapAction ldap2 -serverIP 1.2.3.4 -serverPort 636
      -ldapBase ”OU=Users,DC=server,DC=com” -ldapBindDn
     administrator@ctxnsdev.com -ldapBindDnPassword PASSWORD -
     ldapLoginName samAccountName -KBAttribute userParameters -
     alternateEmailAttr userParameters -authentication disabled
```

Para crear una directiva de autenticación para la validación de preguntas y respuestas basada en el conocimiento mediante la CLI

```
1 add authentication policy kba_validation -rule true -action ldap2
```

Crear una acción de validación de correo electrónico

LDAP debe ser un factor anterior al factor de validación de correo electrónico porque necesita el ID de correo electrónico del usuario o el ID de correo electrónico alternativo como parte del registro de restablecimiento de contraseña de autoservicio.

> **Nota:**
>
> Para que la solución OTP de correo electrónico funcione, asegúrese de que la autenticación basada en el inicio de sesión esté habilitada en el servidor SMTP.

Para asegurarse de que la autenticación basada en el inicio de sesión esté habilitada, escriba el siguiente comando en el servidor SMTP. Si la autenticación basada en el inicio de sesión está habilitada, observará que el texto **AUTH LOGIN** aparece en negrita en la salida.

```
root@ns# telnet <IP address of the SMTP server><Port number of the
   server>
ehlo
```

Ejemplo:

```
root@ns# telnet 10.106.3.66 25
Trying 10.106.3.66...
Connected to 10.106.3.66.
Escape character is '^]'.
220 E2K13.NSGSanity.com Microsoft ESMTP MAIL Service ready at Fri, 22
   Nov 2019 16:24:17 +0530
ehlo
250-E2K13.NSGSanity.com Hello [10.221.41.151]
250-SIZE 37748736
250-PIPELINING
250-DSN
250-ENHANCEDSTATUSCODES
250-STARTTLS
250-X-ANONYMOUSTLS
250-AUTH LOGIN
250-X-EXPS GSSAPI NTLM
250-8BITMIME
250-BINARYMIME
250-CHUNKING
250 XRDST
```

Para obtener información sobre cómo habilitar la autenticación basada en el inicio de sesión, consulte https://support.microfocus.com/kb/doc.php?id=7020367.

Para configurar la acción de correo electrónico mediante CLI

```
add authentication emailAction emailact -userName sender@example.com -
   password <Password> -serverURL "smtps://smtp.example.com:25" -
   content "OTP is $code"
```

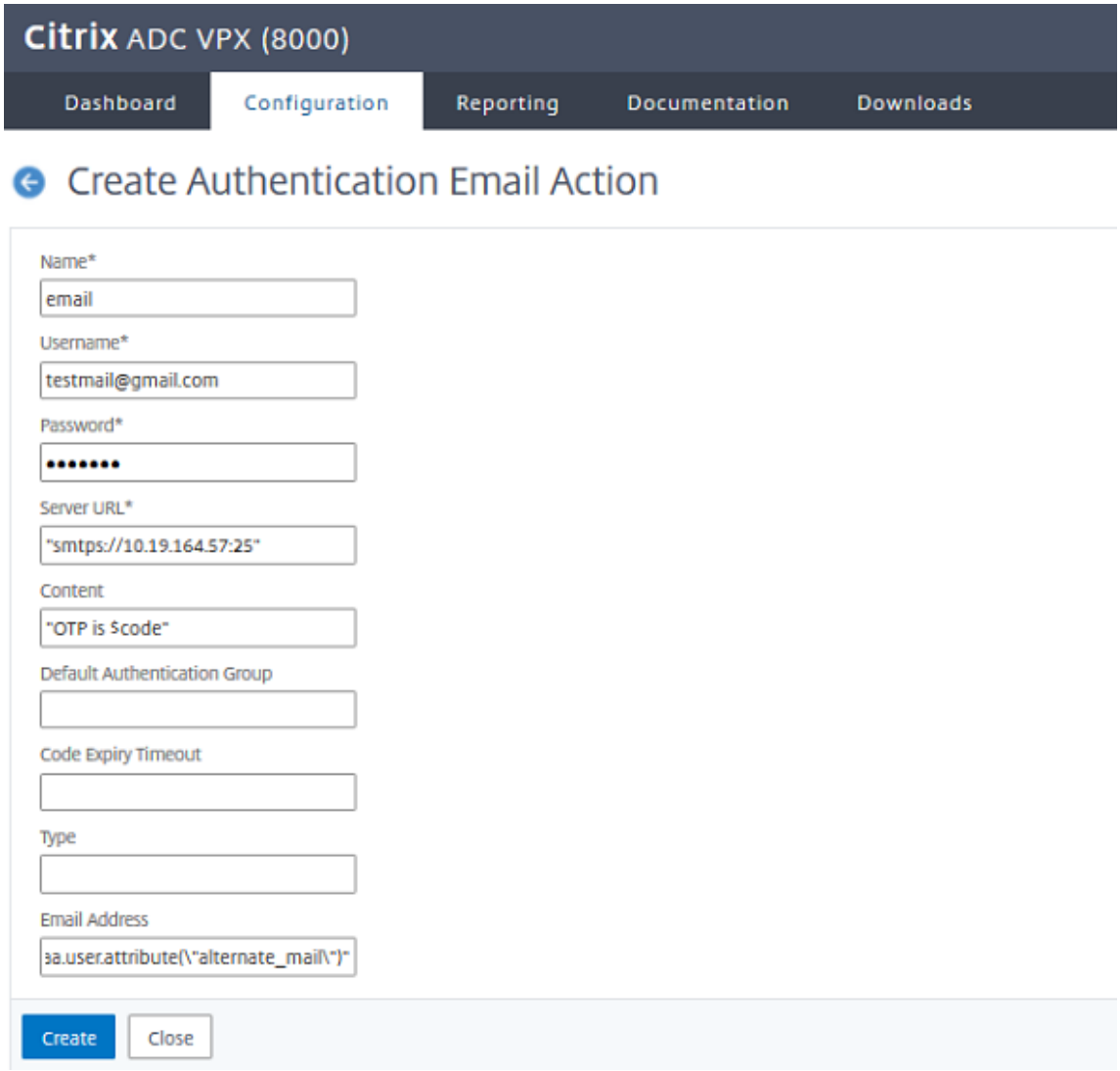

Ejemplo:

```
add authentication emailAction email -userName testmail@gmail.com -
    password 298
    a34b1a1b7626cd5902bbb416d04076e5ac4f357532e949db94c0534832670 -
    encrypted -encryptmethod ENCMTHD_3 -serverURL "smtps
    ://10.19.164.57:25" -content "OTP is $code" -emailAddress "aaa.user.
    attribute(\"alternate_mail\")"
```

> **Nota**
>
> El parámetro "emailAddress" de la configuración es una expresión PI. Por lo tanto, se configura para tomar el ID de correo electrónico de usuario predeterminado de la sesión o el ID de correo electrónico alternativo ya registrado.

Para configurar el ID de correo electrónico mediante la

1. Vaya a **Seguridad > AAA — Tráfico de aplicaciones > directivas > Autenticación > Directivas avanzadas > Acciones > Acción de correo electrónico de autenticación**. Haga clic en **Agregar**.
2. En la página **Crear acción de correo electrónico de autenticación**, rellene los detalles y haga clic en **Crear**.



Para crear una directiva de autenticación para la validación de correo electrónico mediante la CLI

```
1 add authentication policy email_validation -rule true -action email
```

Para crear una directiva de autenticación para el factor de restablecimiento de contraseña

```
1 add authentication policy ldap_pwd -rule true -action ldap_logon_action
```


Presentación de la interfaz de usuario a través del esquema de inicio de sesión

Hay tres loginSchema para restablecer la contraseña de autoservicio para restablecer la contraseña. Utilice los siguientes comandos de CLI para ver los tres esquemas de inicio de sesión:

```
root@ns# cd  /nsconfig/loginschema/LoginSchema/
root@ns# ls -ltr | grep -i password
-r--r--r--  1 nobody  wheel  2088 Nov 13 08:38
   SingleAuthPasswordResetRem.xml
-r--r--r--  1 nobody  wheel  1541 Nov 13 08:38
   OnlyUsernamePasswordReset.xml
-r--r--r--  1 nobody  wheel  1391 Nov 13 08:38 OnlyPassword.xml
```

Para crear un restablecimiento de contraseña de autenticación única mediante CLI

```
> add authentication loginSchema lschema_password_reset -
   authenticationSchema ”/nsconfig/loginschema/LoginSchema/
   SingleAuthPasswordResetRem.xml”

> add authentication loginSchemaPolicy lpol_password_reset -rule true -
   action lschema_password_reset
```

Crear un factor de validación OTP basado en el conocimiento y responder por correo electrónico a través de la etiqueta de directivas

Si el primer factor es el inicio de sesión LDAP, puede crear una pregunta y respuesta basadas en el conocimiento y enviar por correo electrónico etiquetas de directiva OTP para el siguiente factor mediante los siguientes comandos.

```
> add authentication loginSchema lschema_noschema -authenticationSchema
    noschema

> add authentication policylabel kba_validation -loginSchema
   lschema_noschema

> add authentication policylabel email_validation -loginSchema
   lschema_noschema
```


Crear factor de restablecimiento de contraseña a través de la etiqueta de directiva

Puede crear el factor de restablecimiento de contraseña a través de la etiqueta de directiva mediante los siguientes comandos.

```
> add authentication loginSchema lschema_noschema -authenticationSchema
    noschema

> add authentication policylabel password_reset -loginSchema
    lschema_noschema

> bind authentication policylabel password_reset -policyName ldap_pwd -
    priority 10 -gotoPriorityExpression NEXT
```

Enlaza la pregunta y respuesta basadas en el conocimiento y la directiva de correo electrónico a las directivas creadas anteriormente mediante los siguientes comandos.

```
> bind authentication policylabel email_validation -policyName
    email_validation -nextfactor password_reset -priority 10 -
    gotoPriorityExpression NEXT

> bind authentication policylabel kba_validation -policyName
    kba_validation -nextfactor email_validation -priority 10 -
    gotoPriorityExpression NEXT
```

Enlazar el flujo

Debe tener el flujo de inicio de sesión de LDAP creado en la directiva de autenticación para el inicio de sesión de LDAP. En este flujo, el usuario hace clic en el enlace de contraseña olvidada que aparece en la primera página de inicio de sesión de LDAP, luego en la validación KBA seguida de la validación OTP y, finalmente, en la página de restablecimiento de contraseña.

```
bind authentication vserver authvs -policy ldap3 -nextfactor
    kba_validation -priority 10 -gotoPriorityExpression NEXT
```

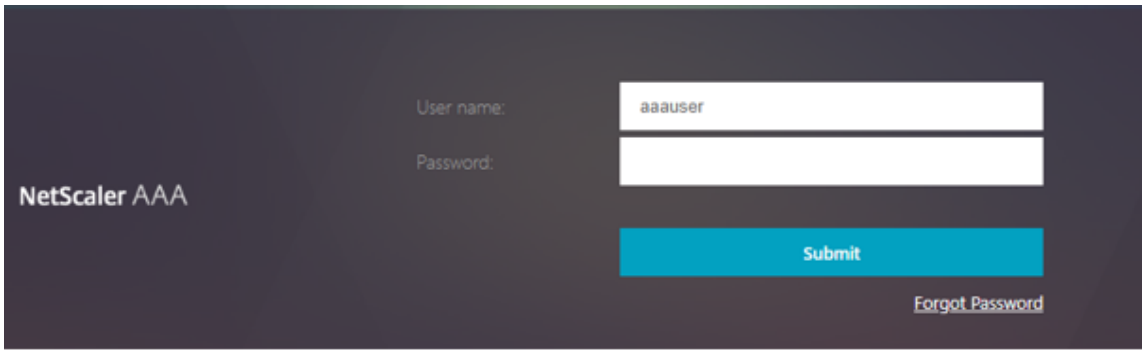
Para enlazar todo el flujo de la interfaz de usuario


```
bind authentication vserver authvs -policy lpol_password_reset -
    priority 20 -gotoPriorityExpression END
```

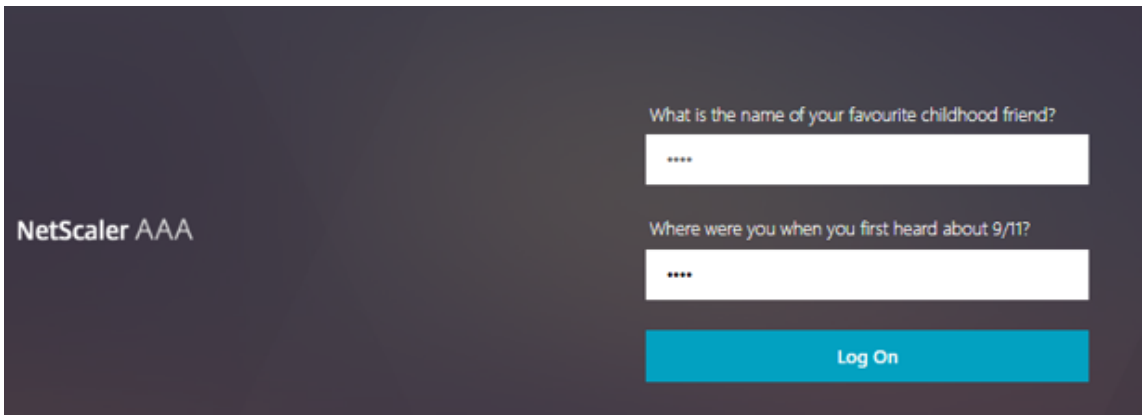
Flujo de trabajo de inicio de sesión para restablecer la contraseña

A continuación se muestra un flujo de trabajo de inicio de sesión de usuario si el usuario necesita restablecer la contraseña:

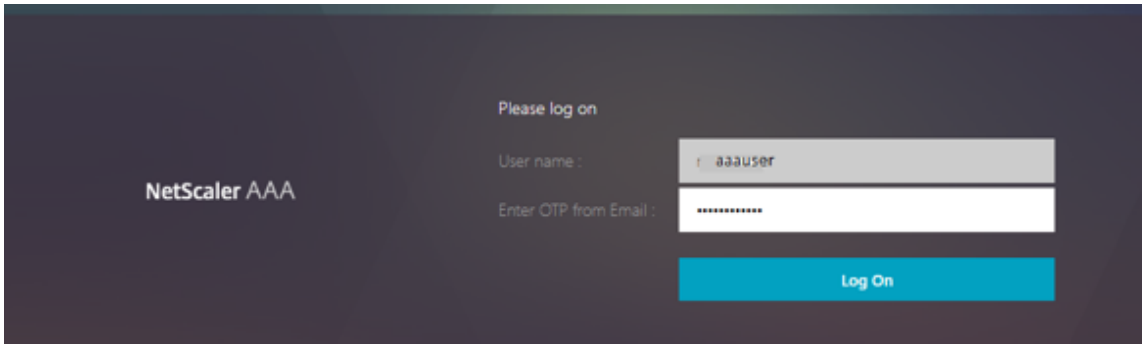
1. Introduzca la URL del servidor virtual lb; por ejemplo, https://lb1.server.com. Se muestra la pantalla de inicio de sesión.



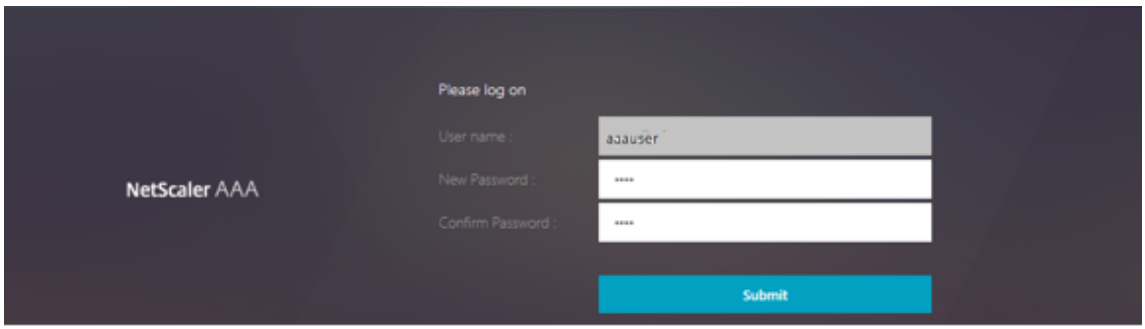
2. Haga clic en **He olvidado mi contraseña**. Una pantalla de validación muestra dos preguntas de un máximo de seis preguntas y respuestas registradas contra un usuario de AD.



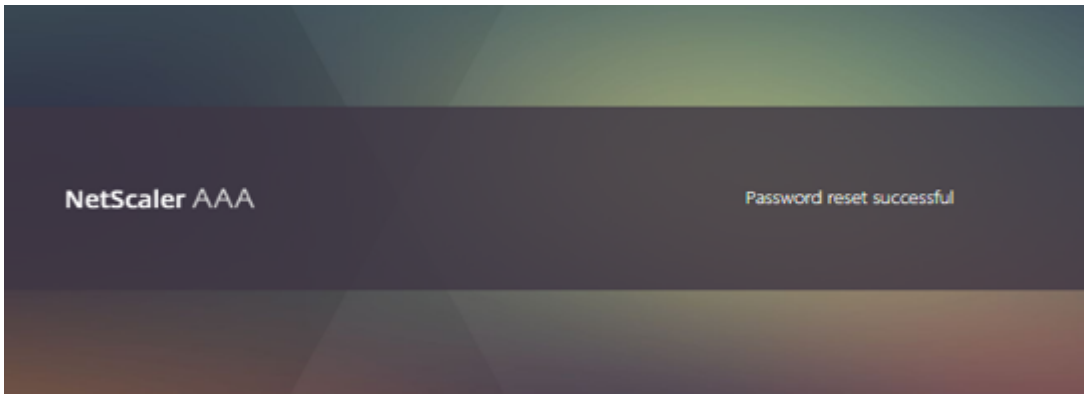
3. Responda a las preguntas y haga clic **en Iniciar sesión**. Se muestra una pantalla de validación de OTP de correo electrónico en la que debe introducir la OTP recibida en el ID de correo electrónico alternativo registrado.



4. Introduzca la OTP de correo electrónico. Una vez que la validación de OTP por correo electrónico se realiza correctamente, se muestra la página de restablecimiento de contraseña.



5. Introduzca una nueva contraseña y confirme la nueva contraseña. Haga clic en **Submit**. Una vez que el restablecimiento de la contraseña se haya realizado correctamente, se mostrará la pantalla de restablecimiento de la contraseña



Ahora puede iniciar sesión con la contraseña de restablecimiento.

Solución de problemas

Citrix ofrece una opción para solucionar algunos de los problemas básicos a los que puede enfrentarse al usar el restablecimiento de contraseña de autoservicio. La siguiente sección le ayuda a solucionar algunos de los problemas que pueden producirse en áreas específicas.

Registro NS

Antes de analizar el registro, se recomienda establecer el nivel de registro para depurar mediante el siguiente comando:

```
> set syslogparams -loglevel DEBUG
```

Registro

El siguiente mensaje indica un registro de usuario correcto.

```
”ns_aaa_insert_hash_keyValue_entry key:kba_registered value:1”
Nov 14 23:35:51 <local0.debug> 10.102.229.76 11/14/2018:18:05:51 GMT
    0-PPE-1 : default SSLVPN Message 1588 0 :  ”
    ns_aaa_insert_hash_keyValue_entry key:alternate_mail value:
    eyJ2ZXJzaW9uIjoiMSIsICJraWQiOiIxbk1oWjN0T2NjLVVvZUx6NDRwZFhxdS01dTA9IiwgImtleS
    ==.oKmvOalaOJ3a9z7BcGCSegNPMw==”
```

Validación de preguntas y respuestas basadas en el conocimiento

El siguiente mensaje indica una validación correcta de preguntas y respuestas basadas en el conocimiento.

```
”NFactor: Successfully completed KBA Validation, nextfactor is email”
```

Validación de ID de correo electrónico

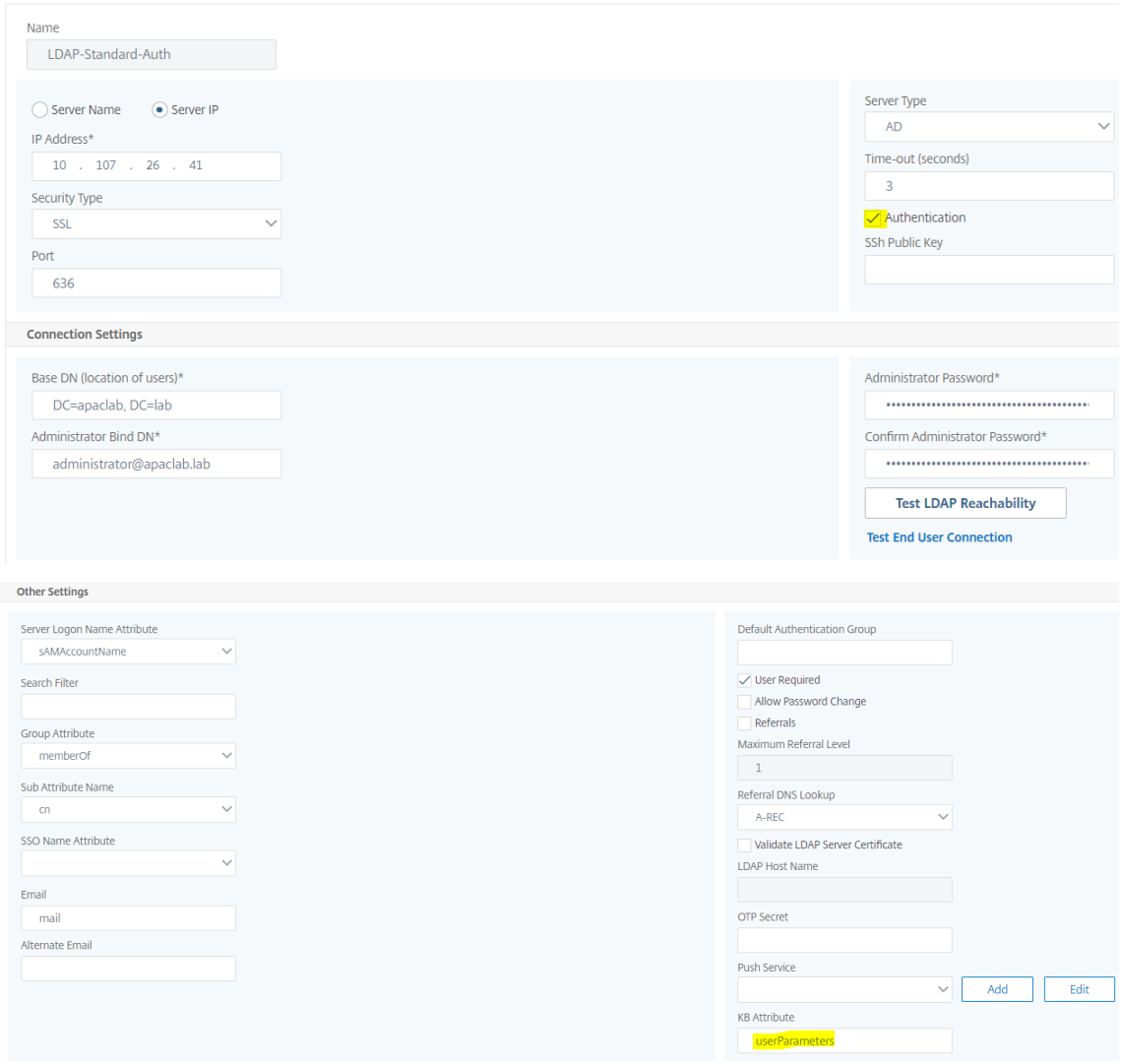
El siguiente mensaje indica que se ha restablecido correctamente la contraseña.

```
”NFactor: Successfully completed email auth, nextfactor is pwd_reset”
```

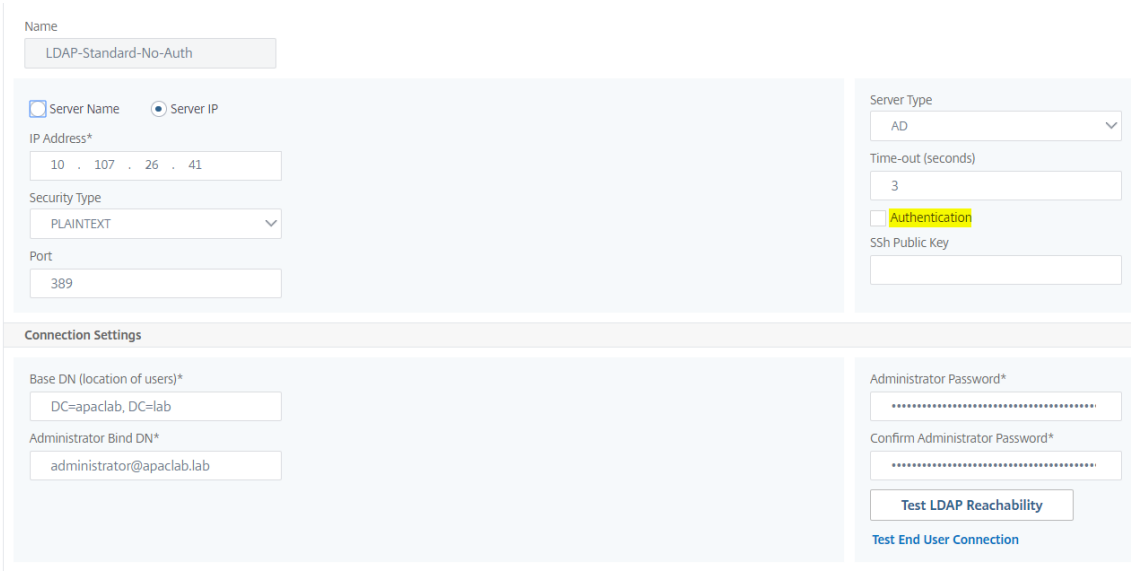
Configurar SSPR mediante el visualizador nFactor

Antes de comenzar la configuración de SSPR, debemos agregar los siguientes servidores LDAP:

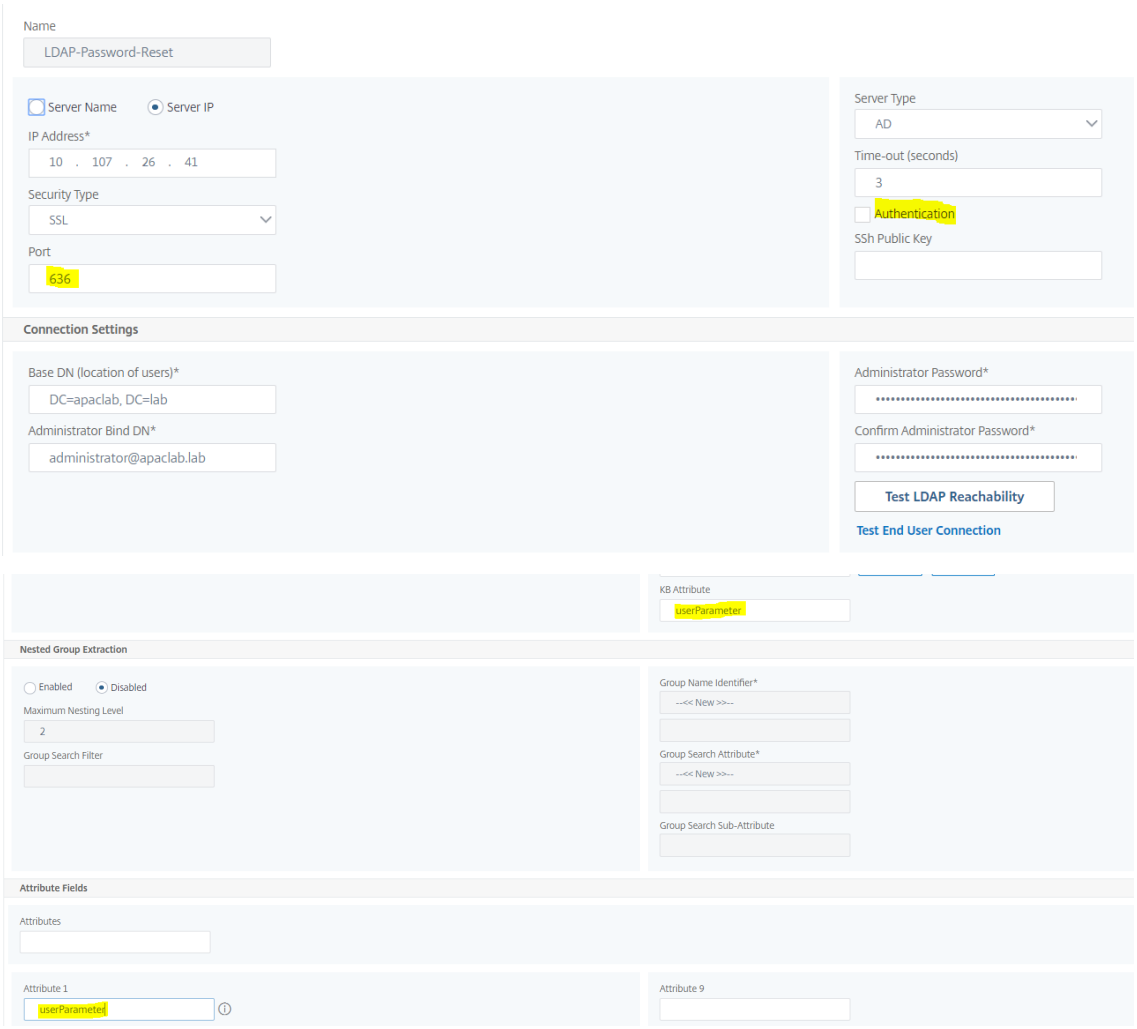
1. Servidor LDAP estándar con la autenticación habilitada para la autenticación de usuarios y el atributo AD especificado.



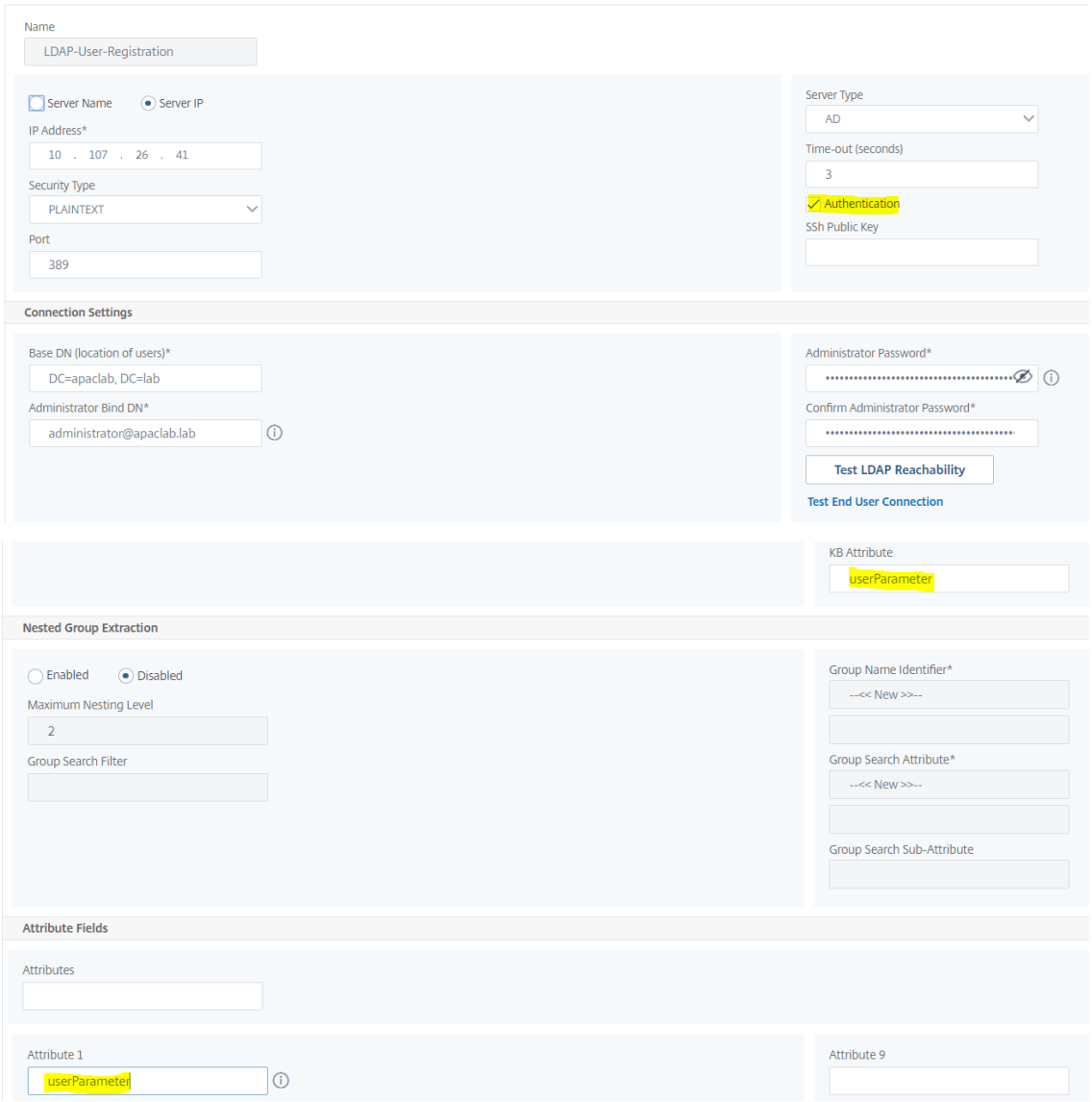
2. Servidor LDAP para la extracción de parámetros de usuario sin autorización.



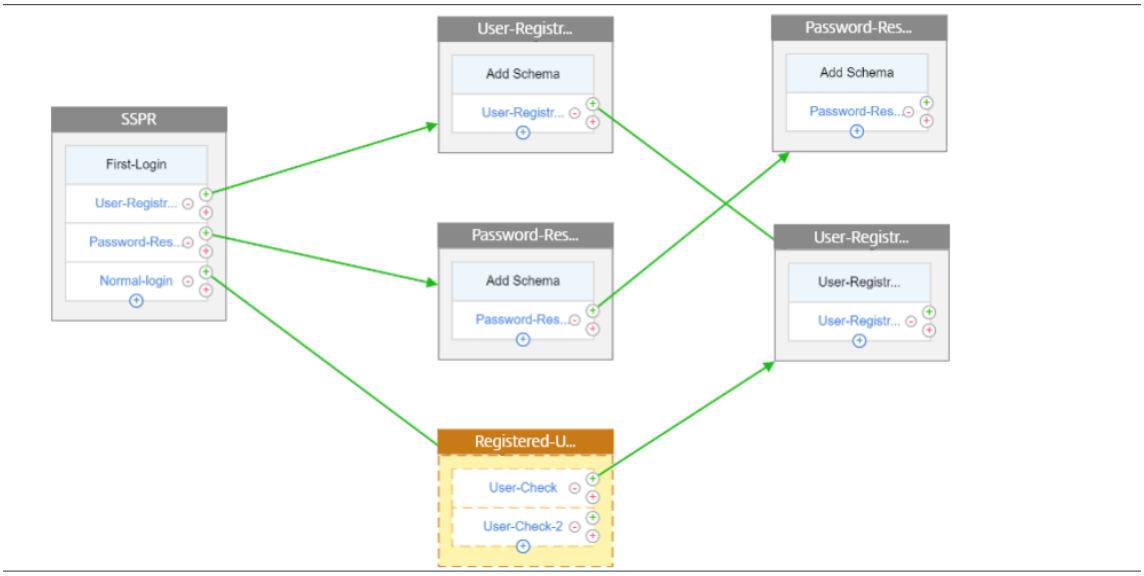
3. Servidor LDAP para restablecer la contraseña en SSL sin autorización. Además, el atributo AD que se utilizará para almacenar los detalles del usuario debe definirse en este servidor.



4. Servidor LDAP para el registro de usuarios, con la autenticación habilitada y el atributo AD especificado



5. En la siguiente ilustración se muestra el flujo completo:



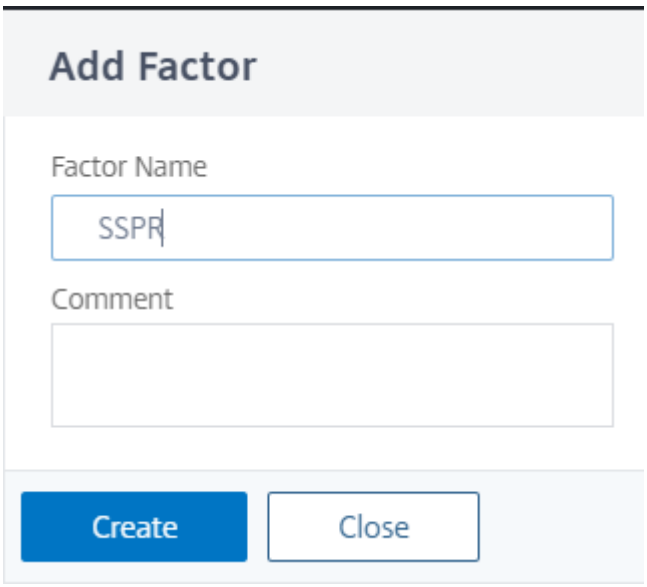
6. Enlazar el certificado globalmente mediante el siguiente comando CLI:

```
1 bind vpn global -userDataEncryptionKey Wildcard
```

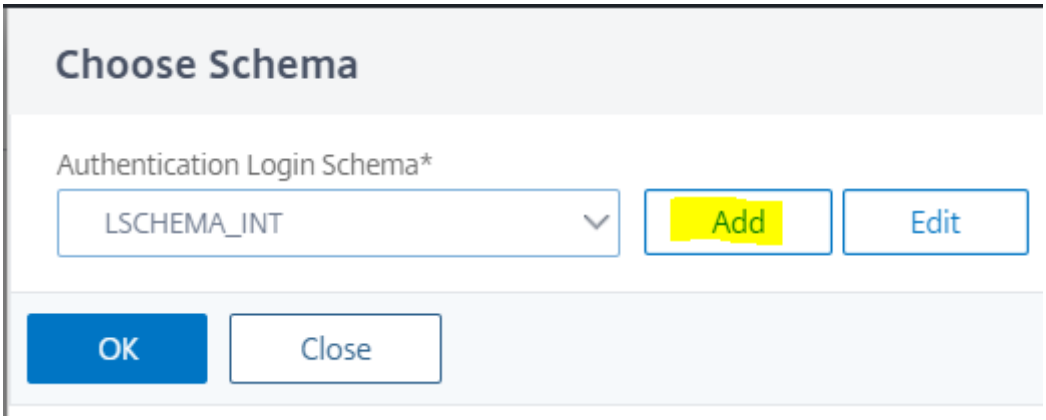
Ahora que se han agregado los servidores LDAP, proceda con la configuración de nFactor mediante el visualizador

1. Vaya a **Seguridad > AAA > Tráfico de aplicaciones > Visualizador nFactor > Flujos nFactor**, haga clic en **Agregar** y haga clic en el icono más dentro del cuadro.

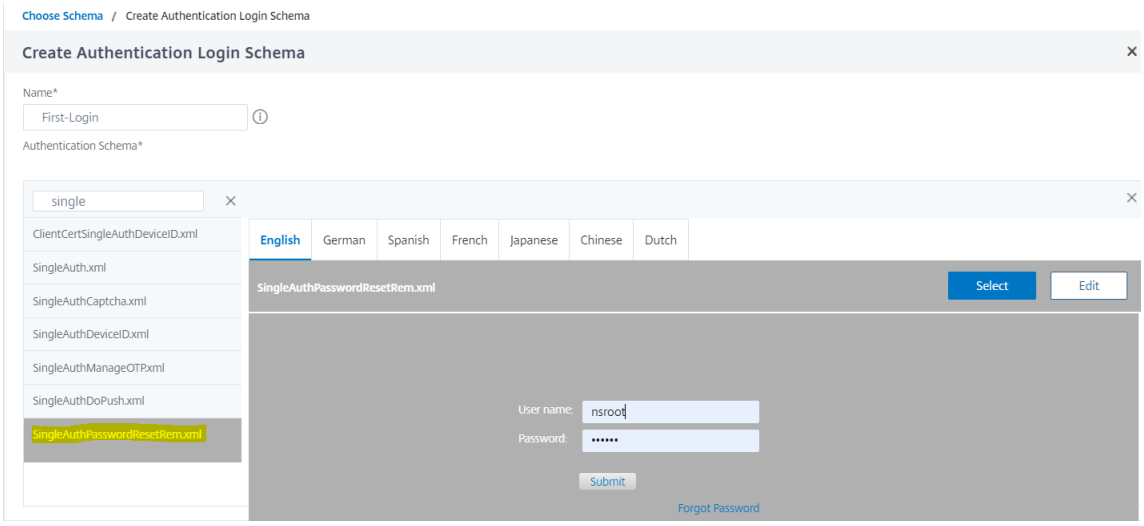
2. Dé un nombre al flujo.



3. Haga clic en **Agregar esquema** que sirva como esquema predeterminado. Haga clic en **Agregar** en la página Esquema de inicio de sesión



4. Después de darle un nombre al esquema, selecciónelo. Haga clic en **Seleccionar** en la esquina superior derecha para seleccionar el esquema.



5. Haga clic en **Crear** y luego en **Aceptar**.

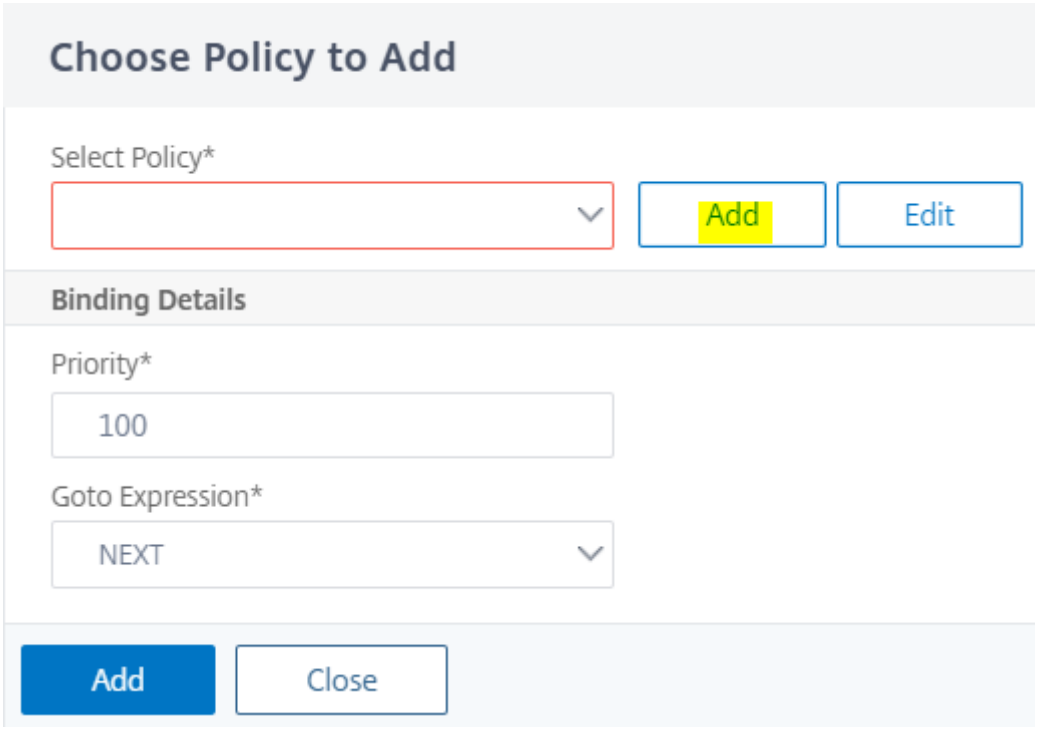
Una vez que se agrega el esquema predeterminado, tenemos que configurar los siguientes tres flujos:

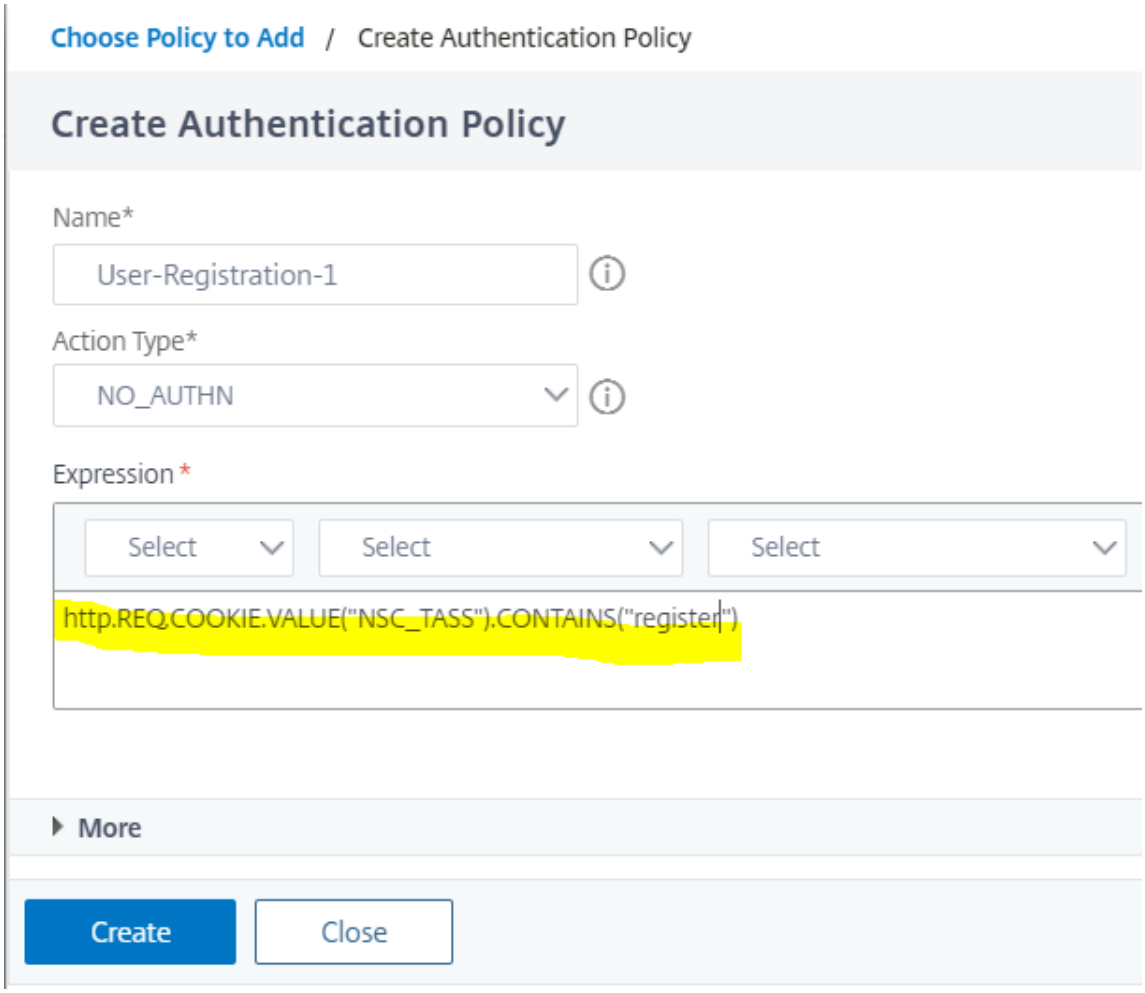
- **Registro de usuarios**: para el registro explícito de usuarios
- **Restablecimiento de contraseña**: para restablecer la contraseña
- Inicio de**sesión normal + Comprobación de usuario registrado**: En caso de que el usuario esté registrado e introduzca la contraseña correcta, el usuario inicia sesión. En caso de que el usuario no esté registrado, lo lleva a la página de registro.

Registro de usuarios

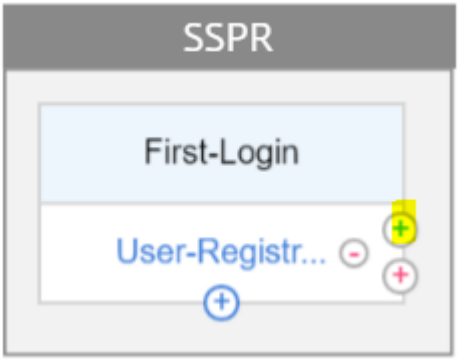
Vamos a continuar desde donde lo dejamos después de agregar el esquema.

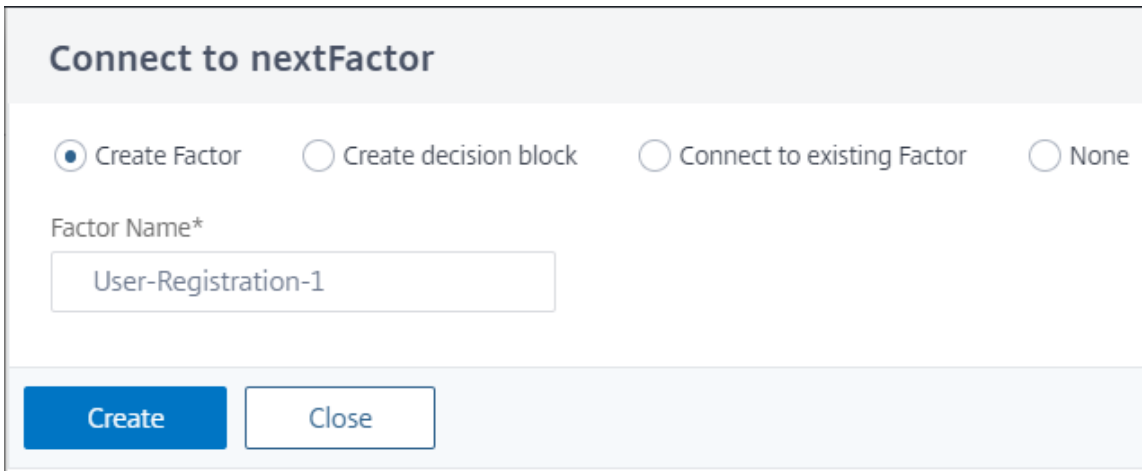
1. Haga clic en **Add Policy**para comprobar si el usuario está intentando registrarse de forma explícita.



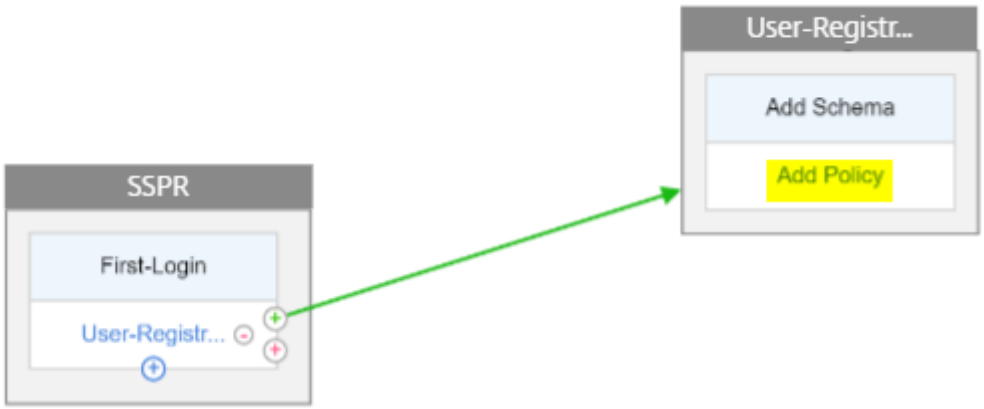


2. Haga clic en **Crear** y, después, en **Agregar**.
3. Haga clic en el icono '+' verde resaltado para agregar el siguiente factor de autenticación al flujo de registro de usuarios.

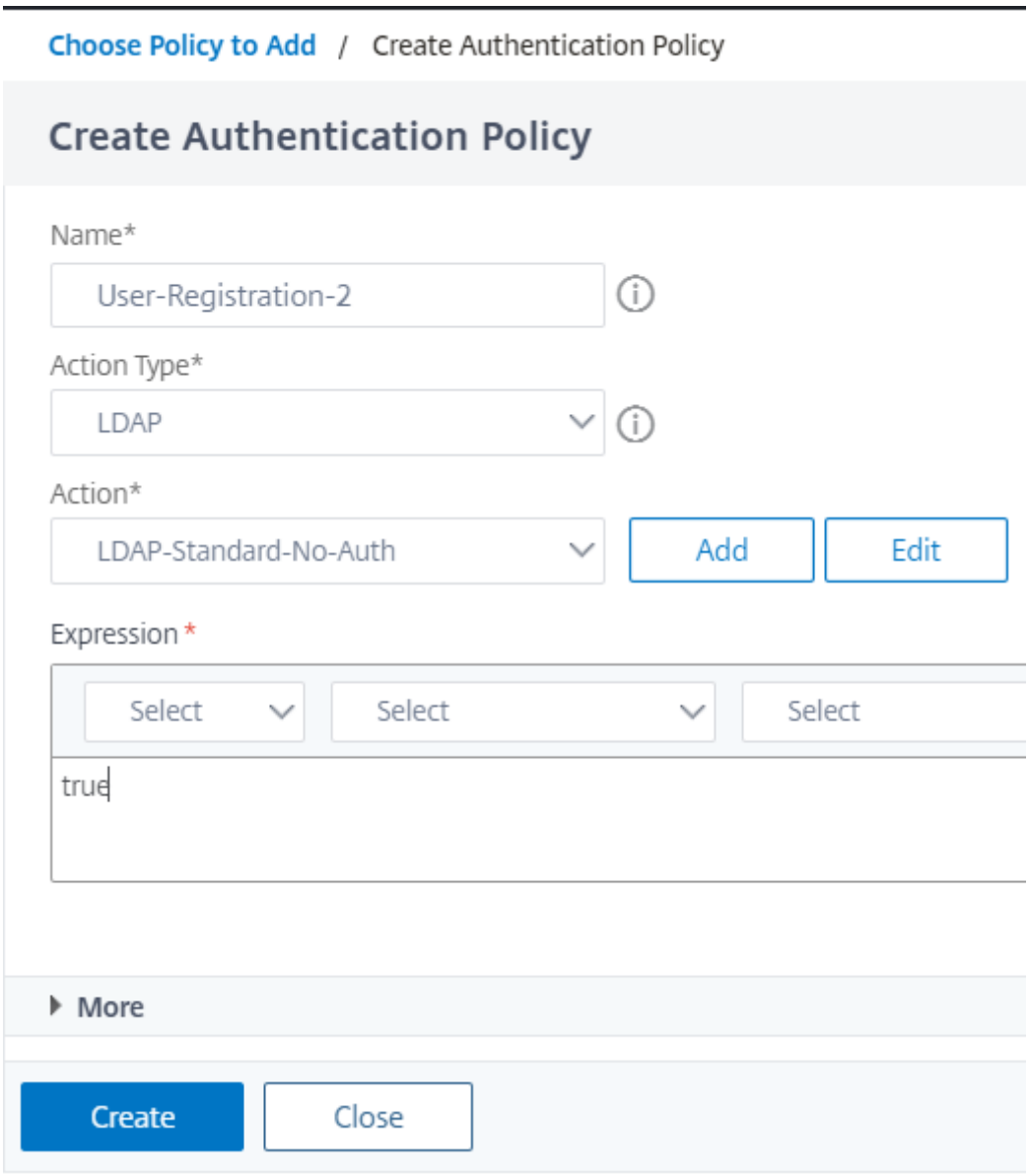




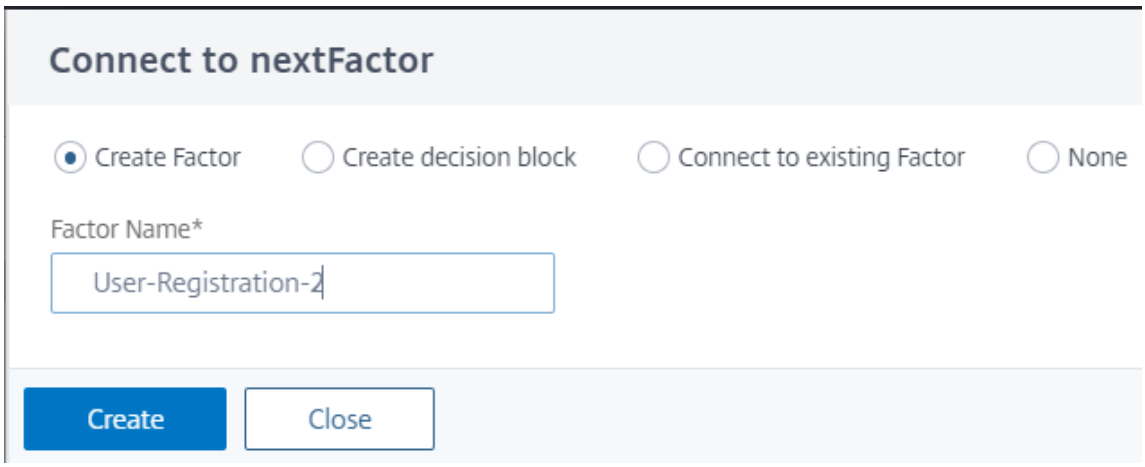
4. Haga clic en **Create**.
5. Haga clic en **Agregar directiva** para el factor Registro de usuarios-1.



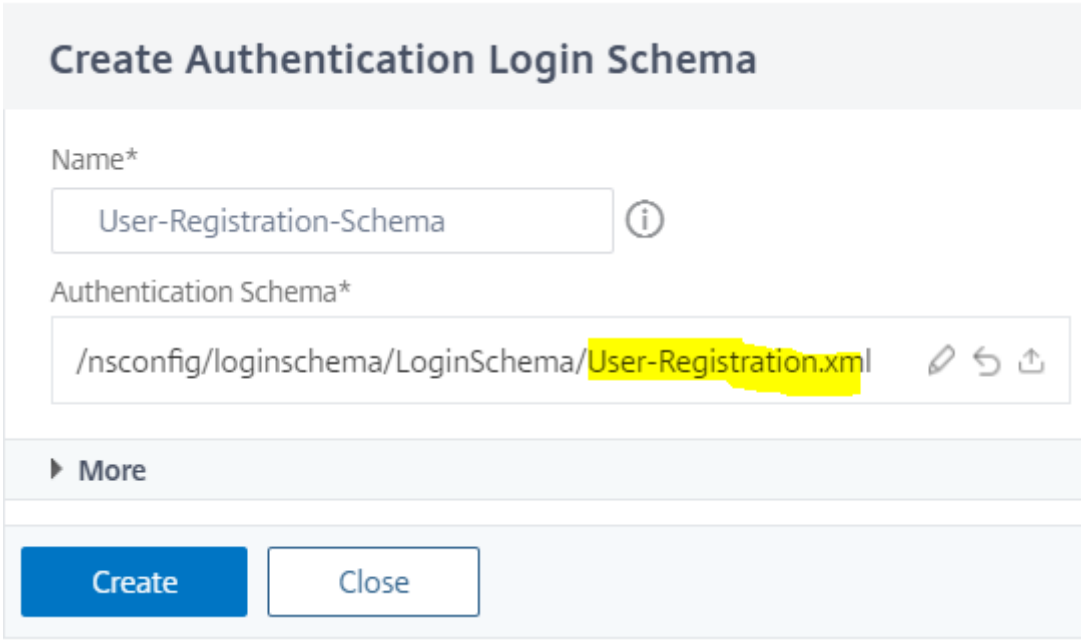
6. Cree la directiva de autenticación. Esta directiva extrae la información del usuario y la valida antes de redirigirla a la página de registro.



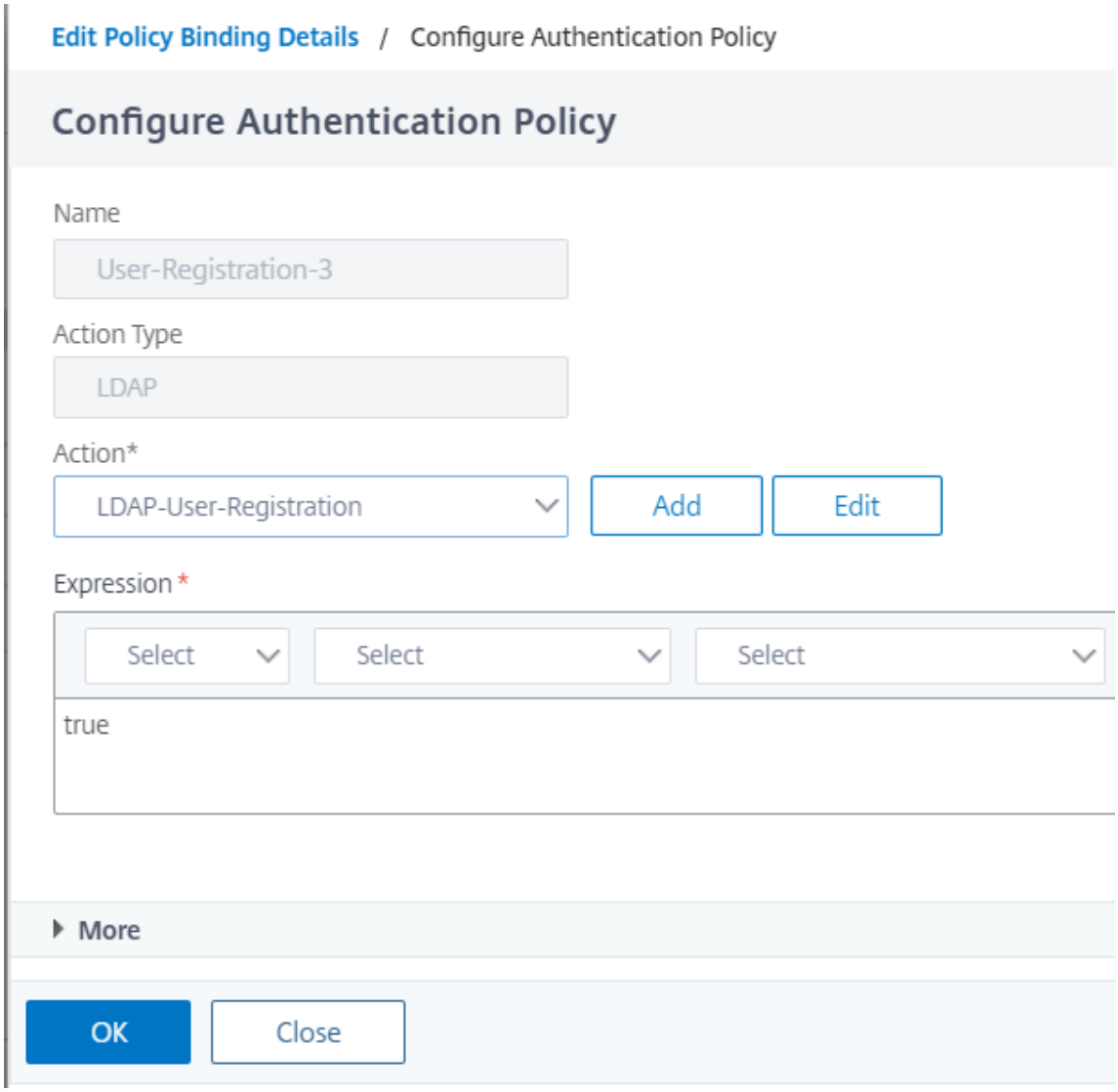
7. Haga clic en **Crear** y, después, en **Agregar**.
8. Ahora haga clic en el icono verde "+" para crear otro factor para el registro de usuario y haga clic en **Crear**. Haga clic en **Agregar esquema**.



9. Crea el siguiente esquema.



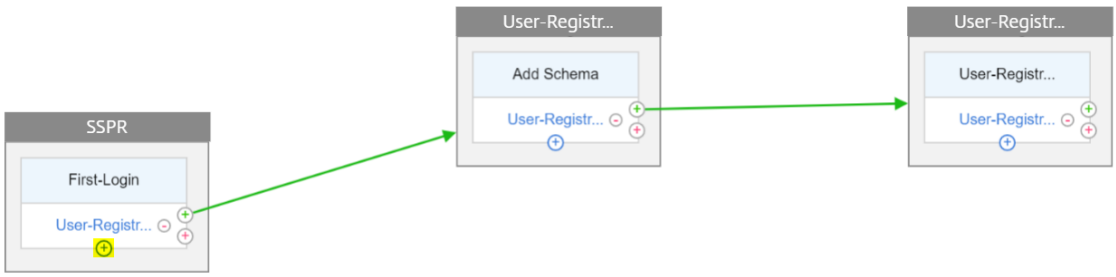
10. Haga clic en **Agregar directiva** y cree la siguiente directiva de autenticación.



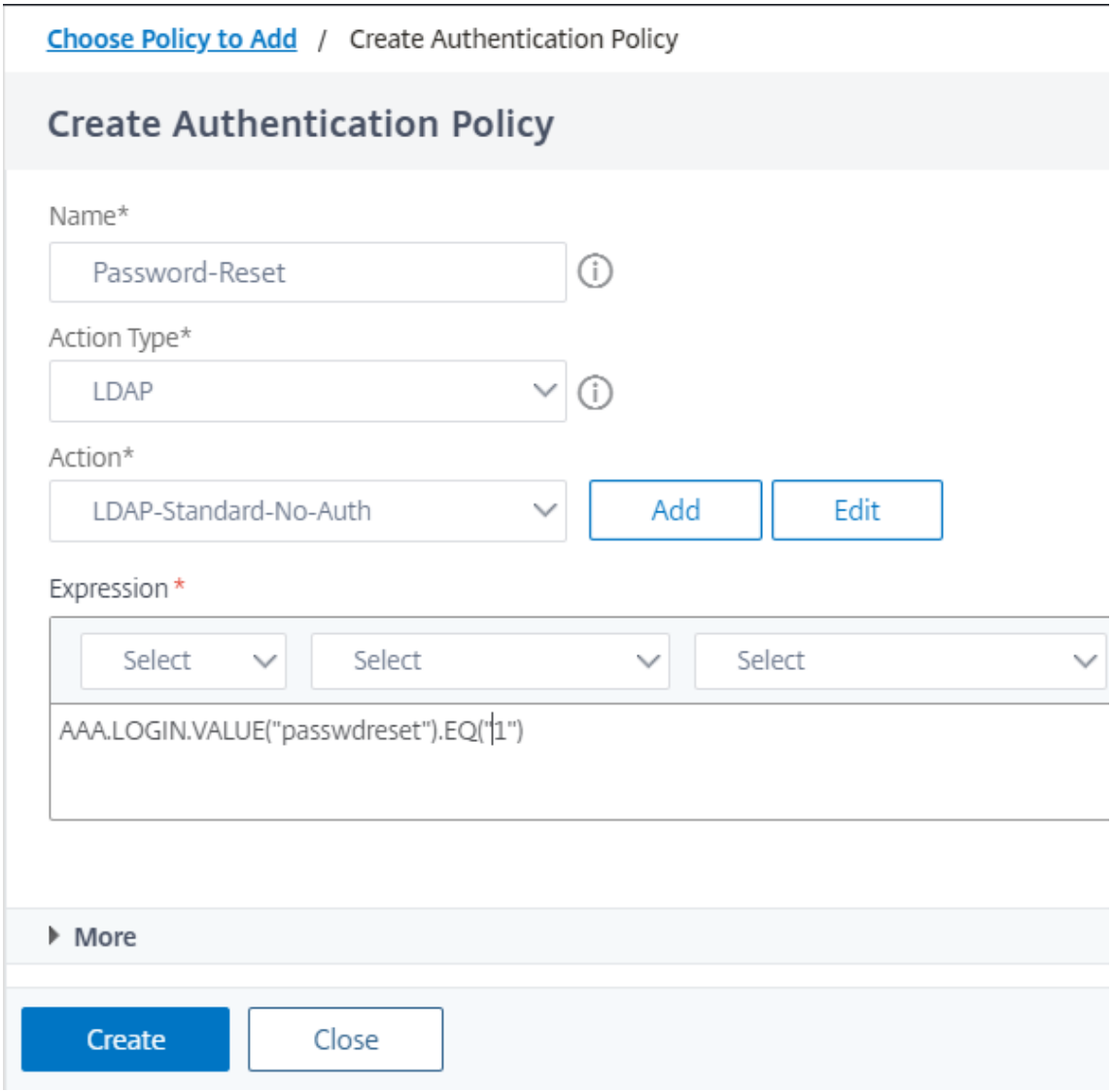
11. Haga clic en **Crear** y haga clic en **Agregar**.

Restablecimiento de contraseña

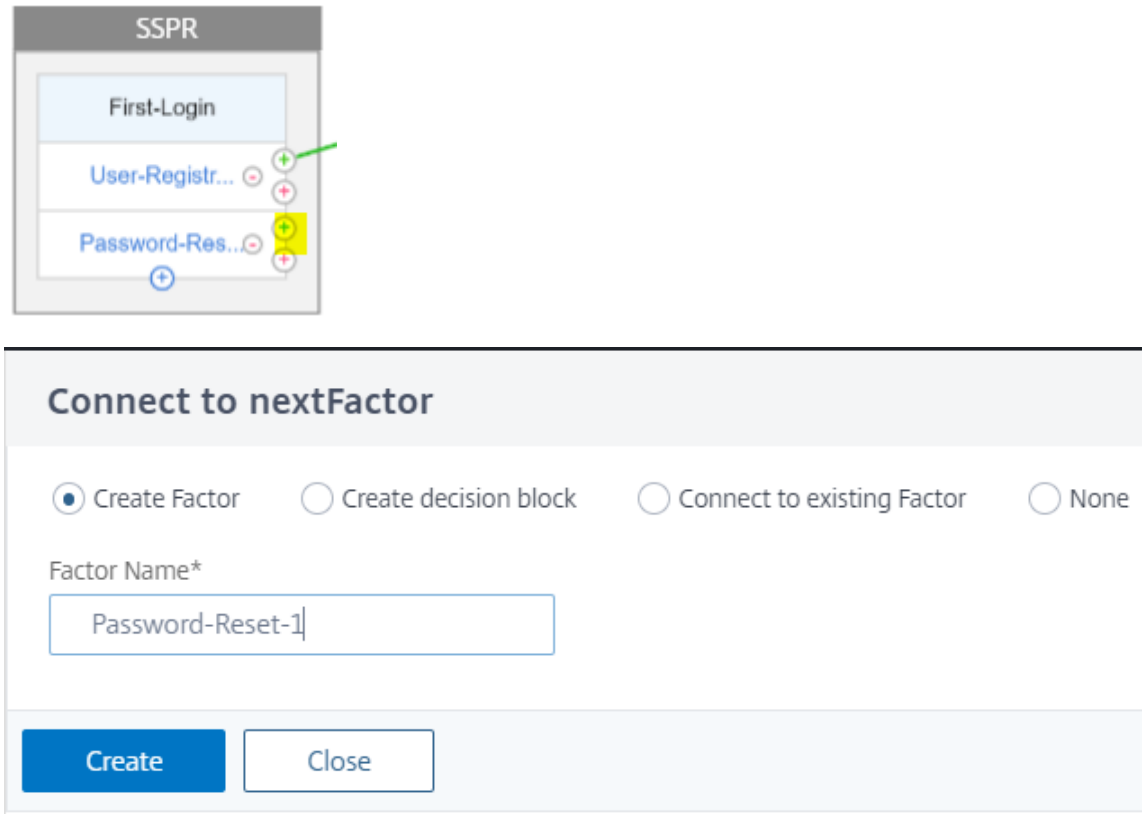
1. Haga clic en el icono azul "+" para agregar otra directiva (flujo de restablecimiento de contraseña) para el factor SSPR principal.



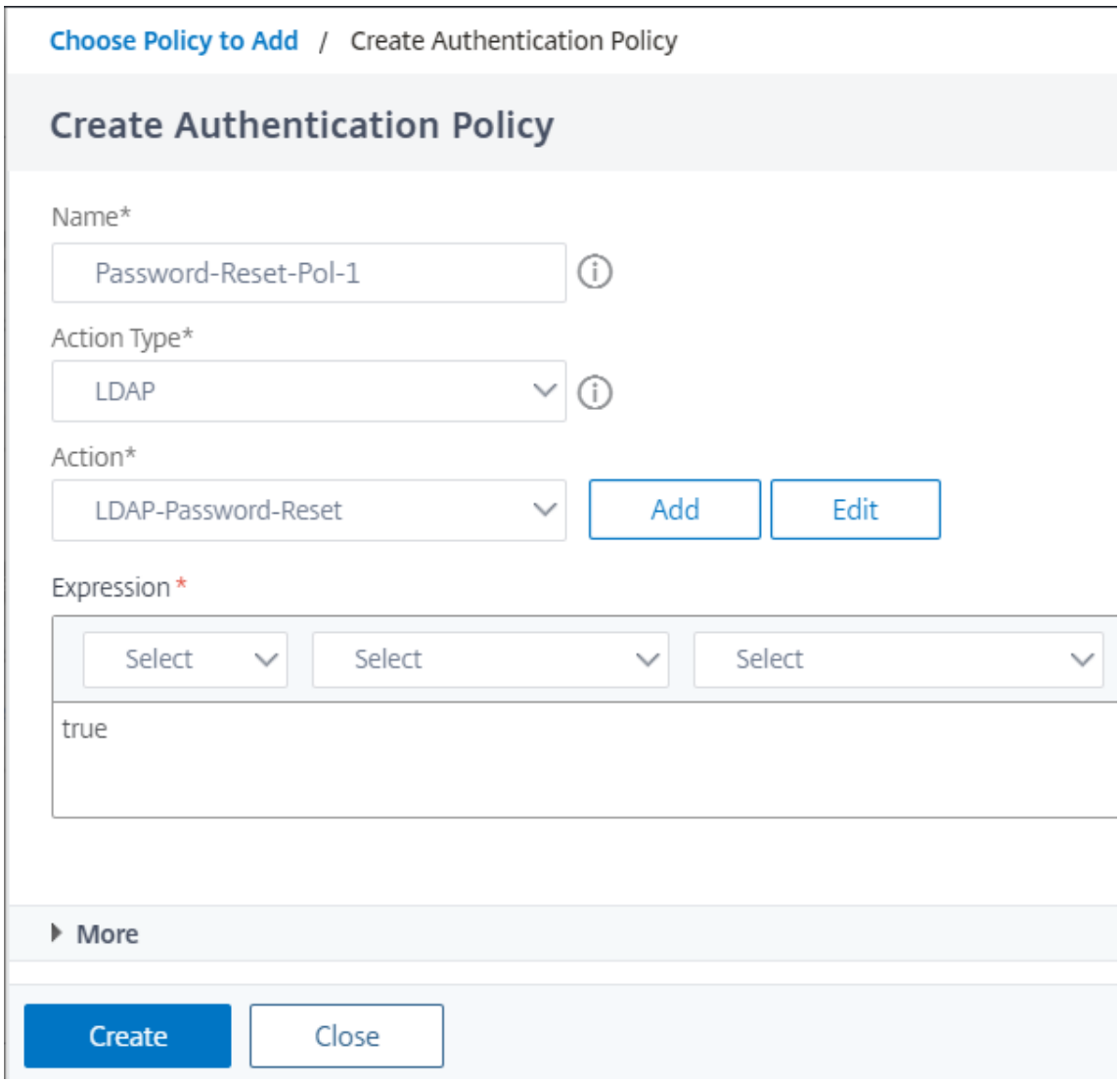
2. Haga clic en **Agregar** y cree una directiva de autenticación. Esta directiva se activa si el usuario hace clic en “Olvidé mi contraseña” en la página de inicio de sesión.



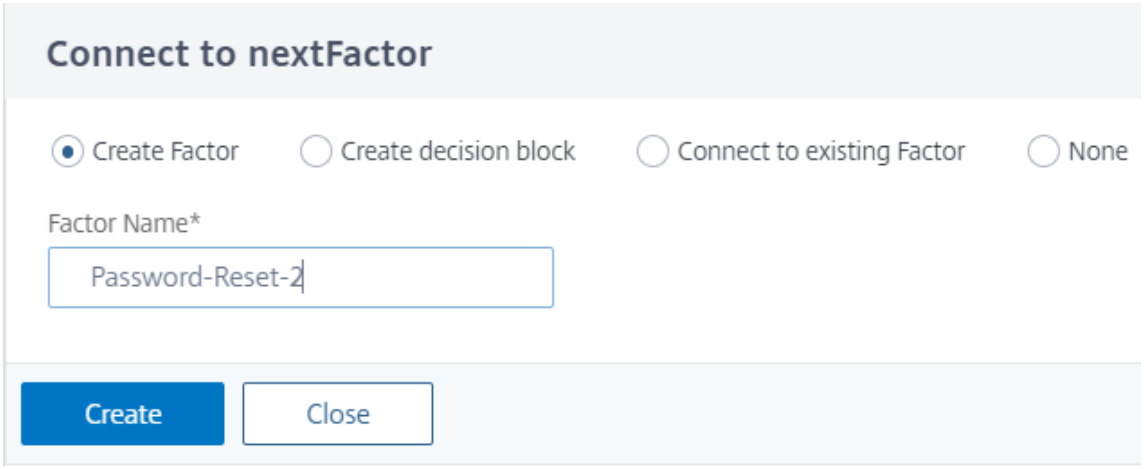
3. Haga clic en **Crear** y haga clic en **Agregar**.
4. Haga clic en el icono verde “+” de la directiva de autenticación de restablecimiento de contraseña para agregar otro factor.



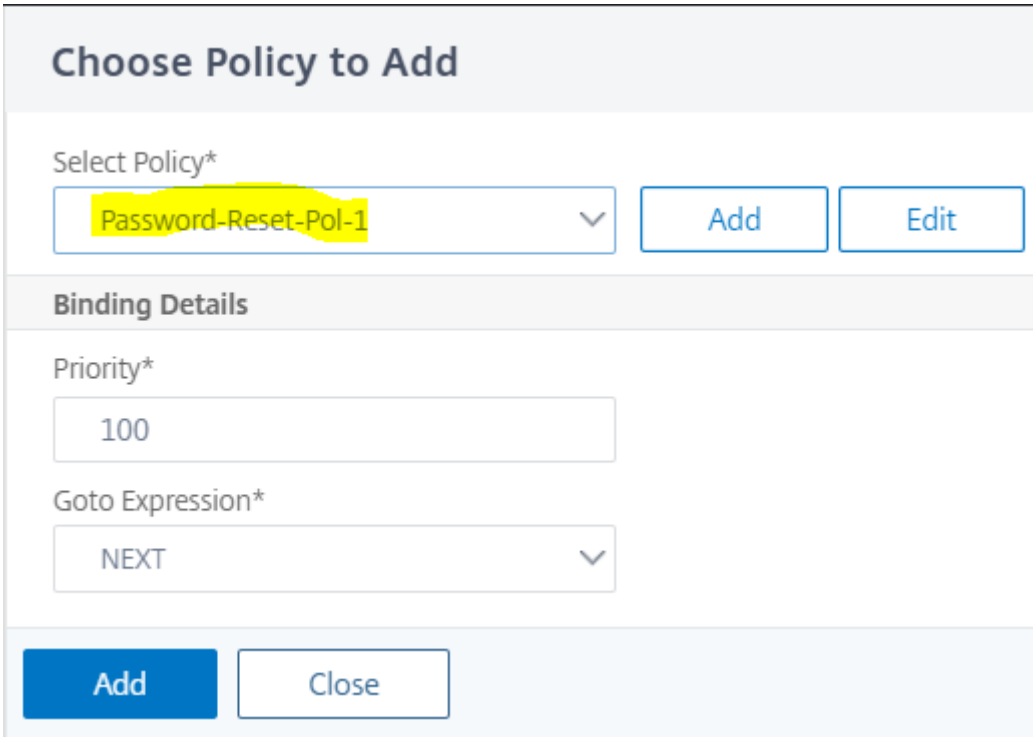
5. Haga clic en **Create**.
6. Haga clic en **Agregar directiva** para crear una directiva de autenticación para el factor creado anteriormente. Este factor sirve para validar al usuario.



7. Haga clic en **Crear** y haga clic en **Agregar**.
8. Haga clic en el icono verde “+” para agregar otro factor para el flujo del factor de contraseña, esto valida las respuestas proporcionadas para restablecer la contraseña. Haga clic en **Create**.

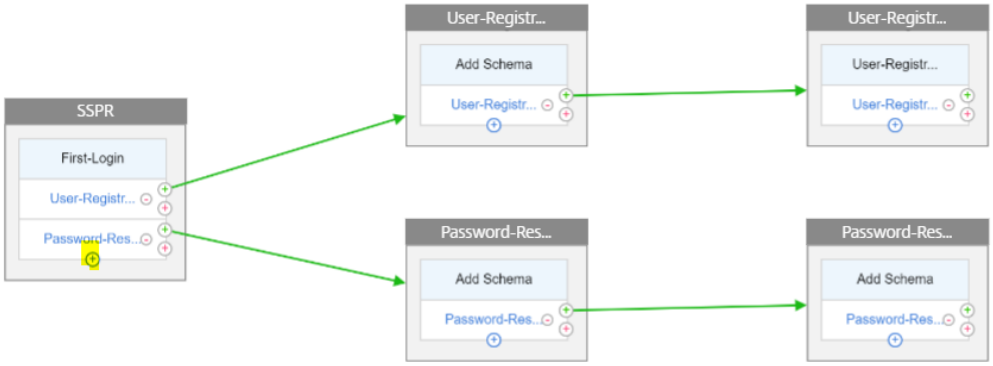


9. Haga clic en **Agregar directiva** para agregar una directiva de autenticación para el factor.
10. Seleccione la misma directiva de autenticación en el menú desplegable que creamos anteriormente y haga clic en **Agregar**.

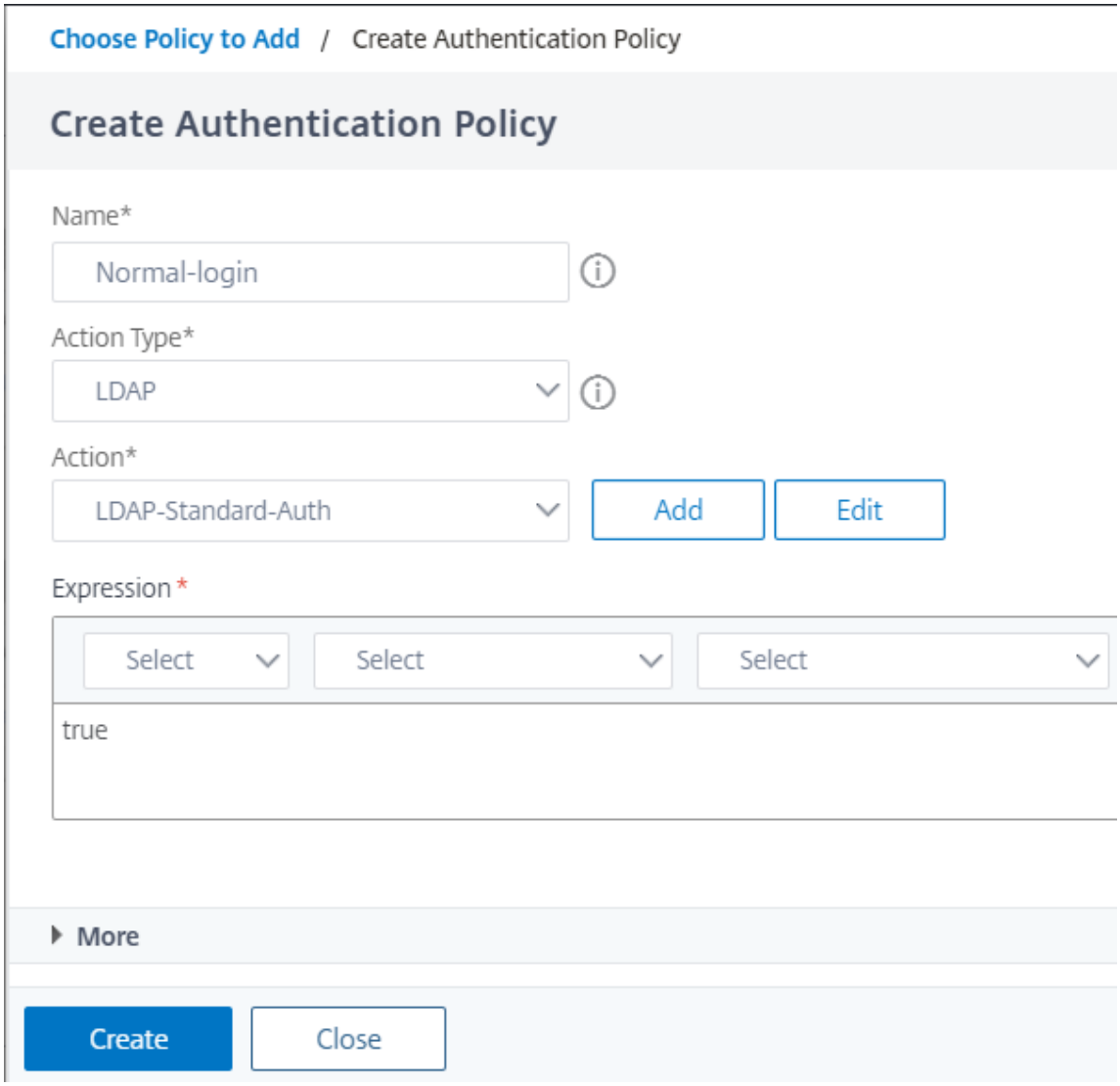


Inicio de sesión normal + Comprobación de usuario registrado

1. Haga clic en el icono azul “+” para agregar otra directiva de autenticación (flujo de inicio de sesión normal) al factor SSPR principal.

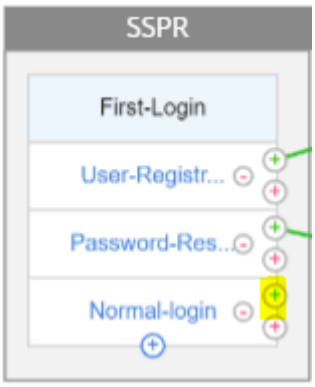


2. Haga clic en **Agregar**para crear una directiva de autenticación para el inicio de sesión normal del usuario.

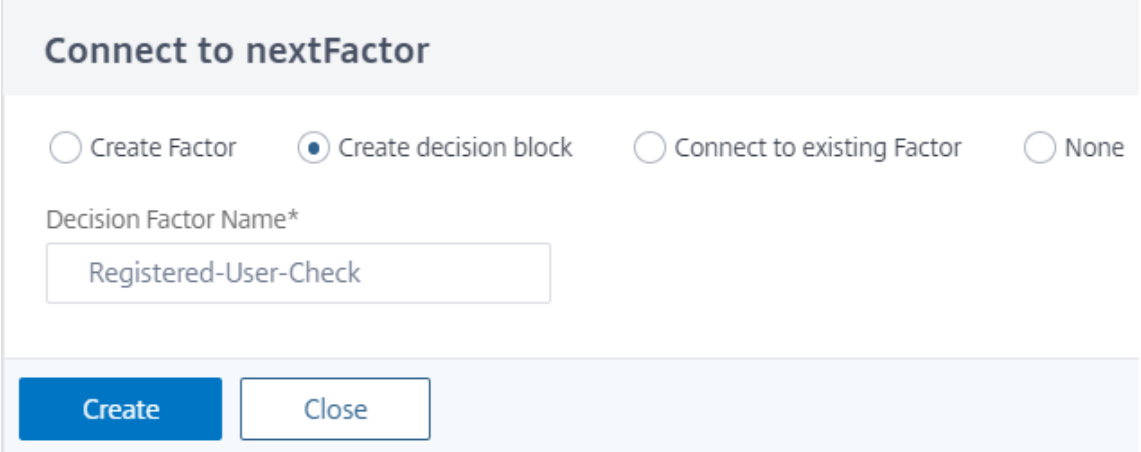


3. Haga clic en **Crear** y haga clic en **Agregar**.

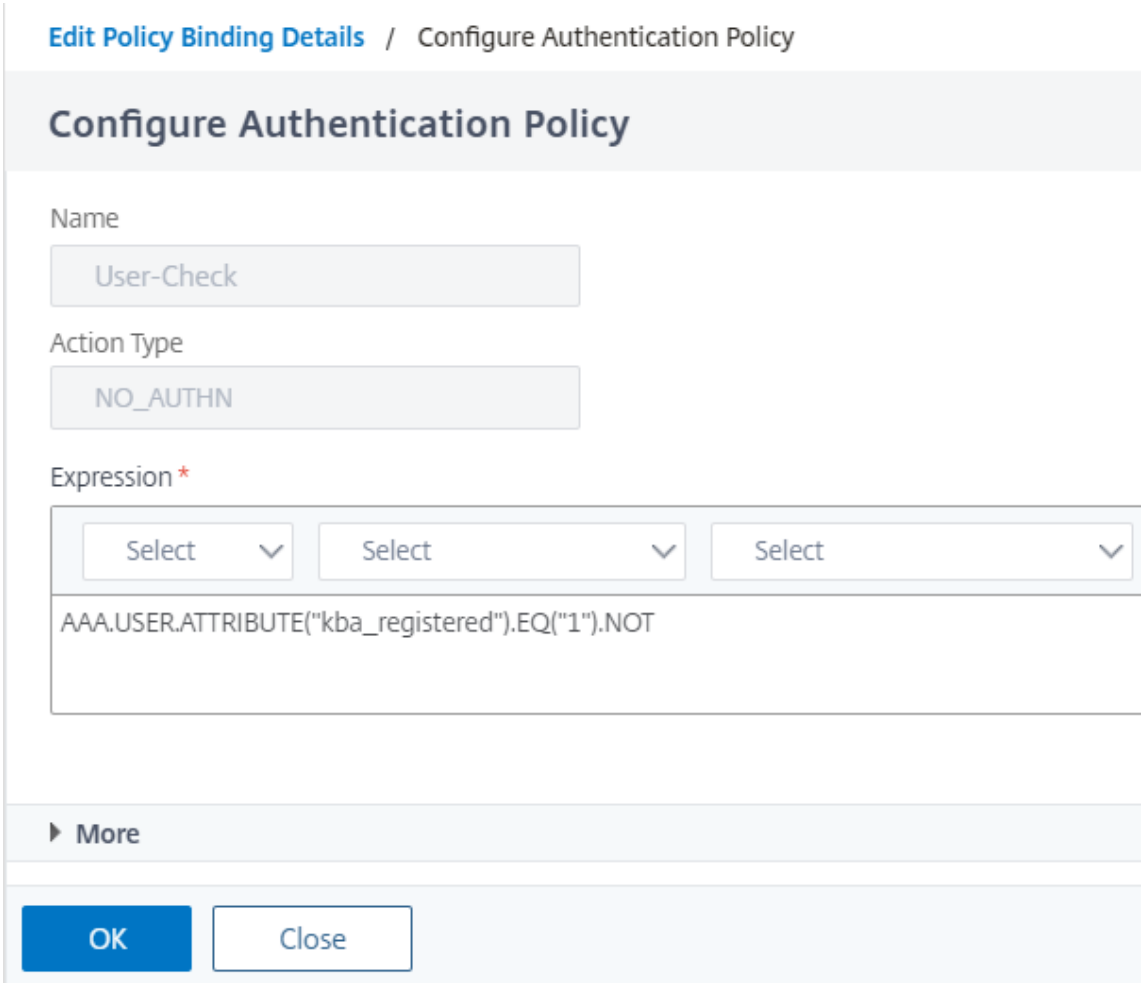
4. Haga clic en el icono verde “+” de la directiva creada anteriormente para agregar otro factor, que es el bloque de decisión. Haga clic en **Create**.



5. Haga clic en **Create**.

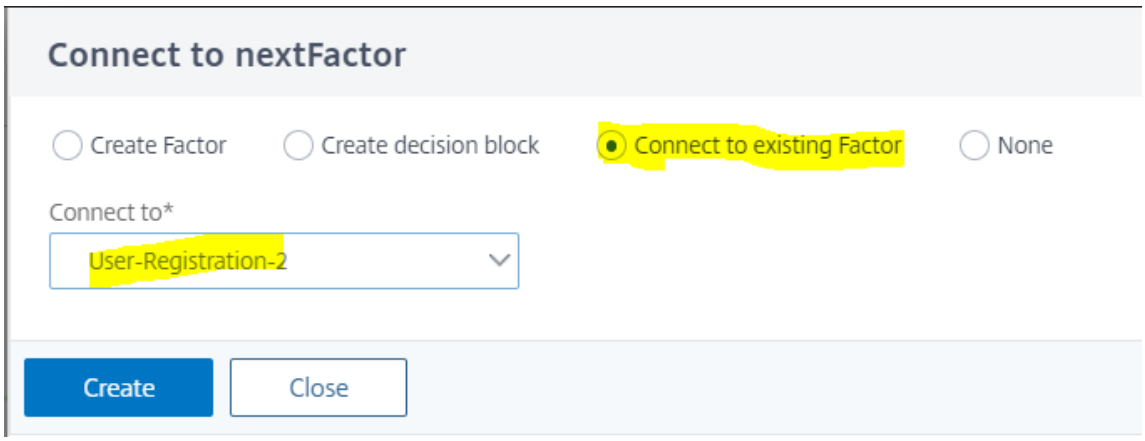


6. Haga clic en **Agregar directiva** para crear una directiva de autenticación para este factor de decisión.

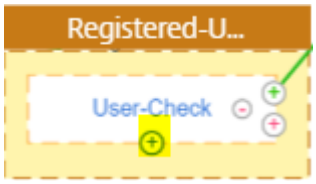


7. Haga clic en **Crear** y luego en **Agregar**. Esto comprueba si el usuario está registrado o no.
8. Haga clic en el icono verde “+” para apuntar al usuario a la directiva de registro.

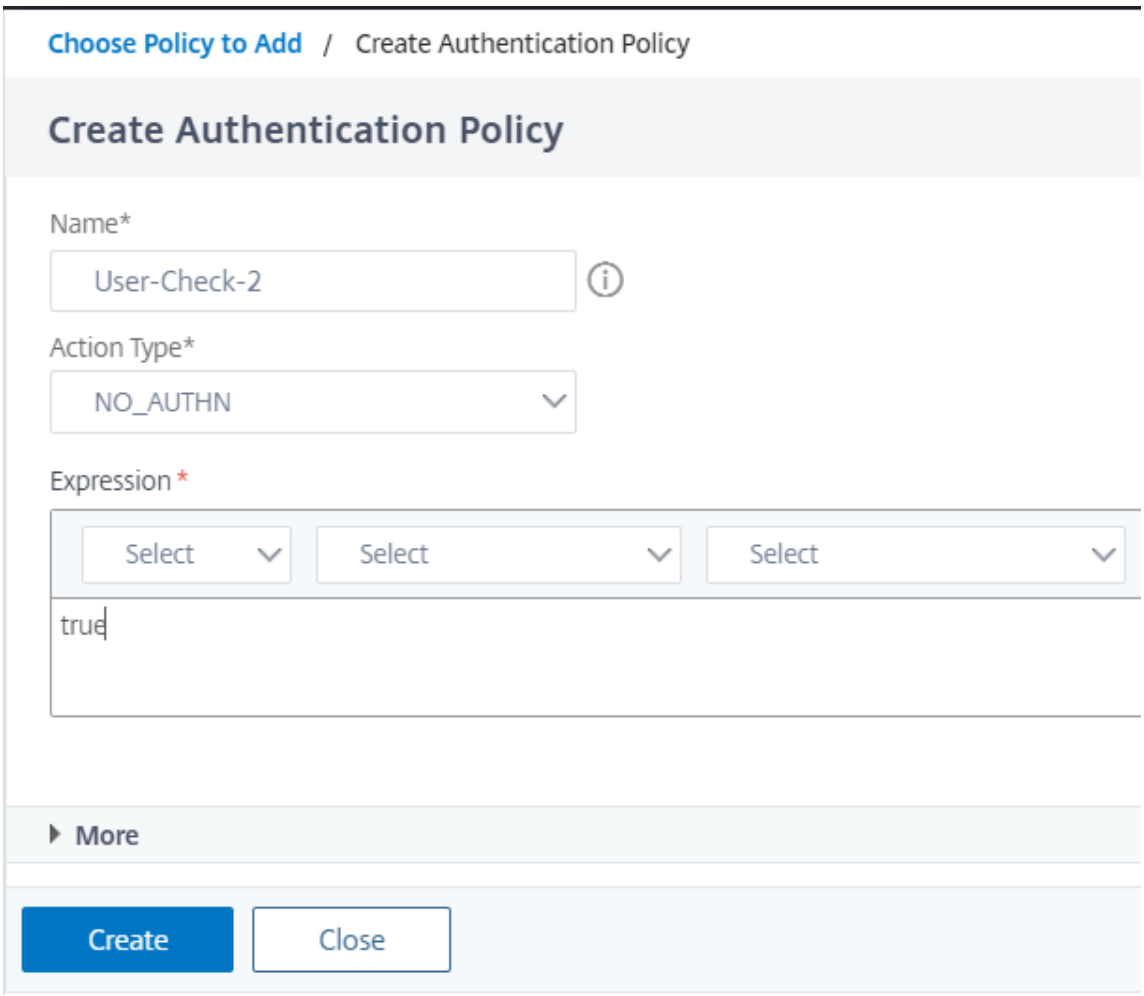
9. Seleccione el factor de registro en el menú desplegable y haga clic en **Crear**.



10. Ahora haga clic en el icono azul "+" para agregar otra directiva al bloque de decisión, esta directiva es para que el usuario registrado finalice la autenticación.



11. Haga clic en **Agregar directiva** para crear una directiva de autenticación.



12. Haga clic en **Crear** y haga clic en **Agregar**.

Sondeo durante la autenticación

August 20, 2021

A partir de la compilación 13.0.79.64 de la versión de Citrix ADC, se puede configurar un dispositivo Citrix ADC para el mecanismo de sondeo durante la autenticación multifactor.

Si el sondeo está configurado en un dispositivo Citrix ADC, los endpoints (como un explorador web o una aplicación) pueden sondear (sondear) el dispositivo durante la autenticación a intervalos configurados para obtener el estado de la solicitud de autenticación enviada.

El sondeo se puede configurar para gestionar las autenticaciones cuando un endpoint deja caer una conexión TCP mientras se autentica con un dispositivo Citrix ADC.

Puntos a tener en cuenta

- La configuración de sondeo es compatible con los métodos de autenticación LDAP, RADIUS y TACACS.
- El cliente puede sondear las solicitudes de autenticación desde el segundo factor en adelante.

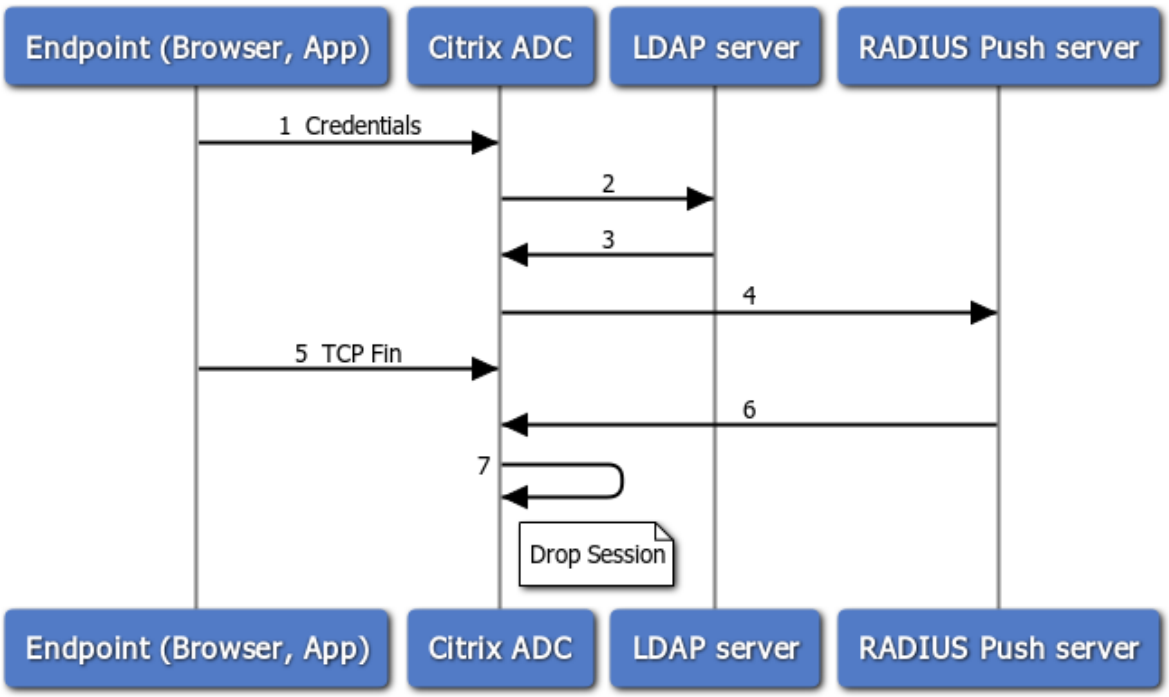
¿Por qué configurar el sondeo?

A veces, al autenticarse, cambiar entre las aplicaciones (por ejemplo, una aplicación de inicio de sesión y una aplicación de autenticación) hace que los endpoints pierdan la conexión con el dispositivo Citrix ADC, lo que provoca una interrupción en el flujo de autenticación. Con el sondeo configurado, se puede evitar esta interrupción en la autenticación.

Descripción del mecanismo de votación

A continuación se muestra un ejemplo del flujo de eventos durante la autenticación sin necesidad de que se haya configurado el sondeo.

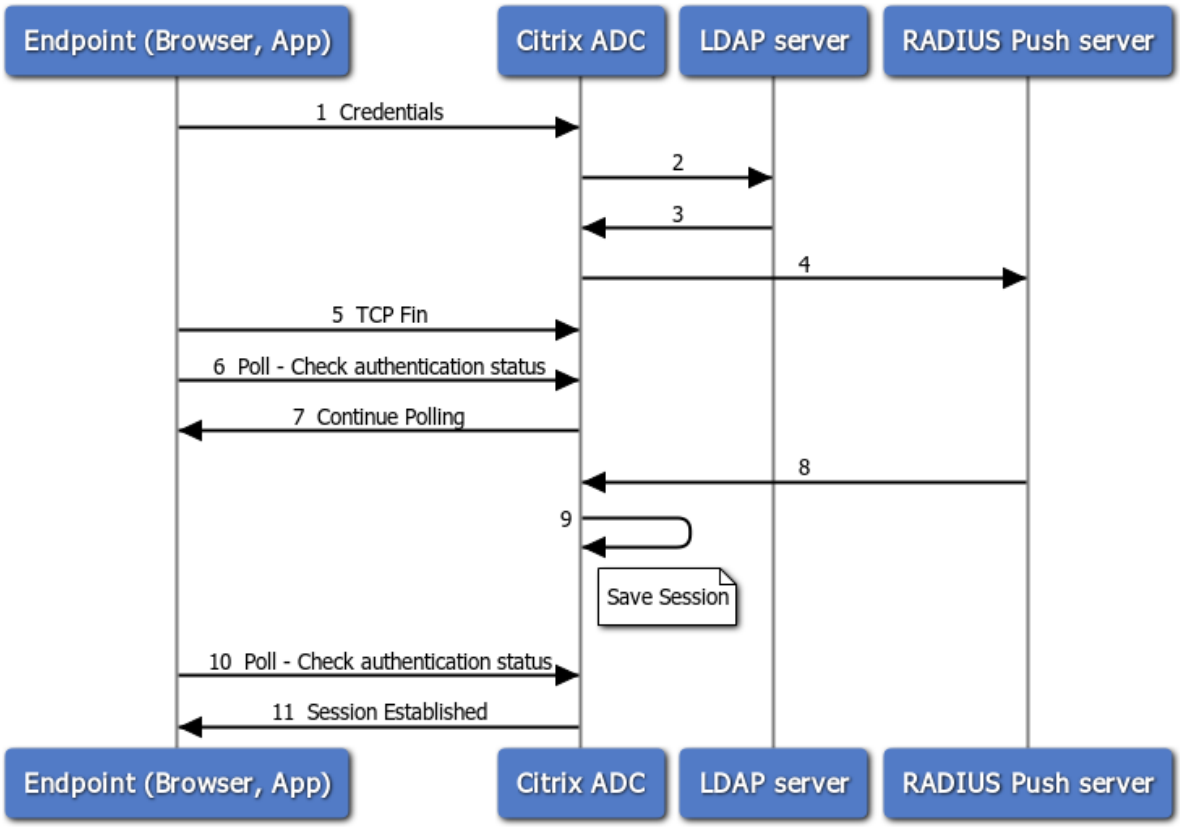
El mecanismo de sondeo permite que un dispositivo Citrix ADC reanude una autenticación continua con el endpoint sin tener que reiniciar el proceso de autenticación en un caso raro de restablecimiento de la conexión TCP en el extremo.



1. Un endpoint (aplicación o explorador web) se autentica con credenciales.

2. El nombre de usuario y la contraseña se verifican con un directorio de primer factor existente (LDAP/Active Directory).
3. Si se proporcionan las credenciales correctas, la autenticación pasa al siguiente factor.
4. En este punto, el dispositivo Citrix ADC envía una solicitud al servidor Push RADIUS.
5. Mientras el dispositivo Citrix ADC espera una respuesta del servidor RADIUS, el punto final deja caer la conexión TCP.
6. Citrix ADC recibe una respuesta del servidor Push RADIUS.
7. Puesto que no se encuentra ninguna conexión TCP de cliente, el dispositivo Citrix ADC interrumpe la sesión y se produce un error en el inicio de sesión.

A continuación se muestra un ejemplo del flujo de eventos durante la autenticación con el sondeo configurado.



1. Un endpoint (aplicación o explorador web) se autentica con credenciales.
2. El nombre de usuario y la contraseña se verifican con un directorio de primer factor existente (LDAP/Active Directory).
3. Si se proporcionan las credenciales correctas, la autenticación pasa al siguiente factor.
4. En este punto, el dispositivo Citrix ADC envía una solicitud al servidor Push RADIUS.
5. Mientras el dispositivo Citrix ADC espera una respuesta del servidor RADIUS, el punto final deja caer la conexión TCP.
6. Endpoint envía una encuesta (sondeo) al dispositivo Citrix ADC para comprobar el estado de

autenticación.

7. Dado que el dispositivo Citrix ADC no escucha información del servidor RADIUS, solicita al endpoint que continúe sondeando.
8. El dispositivo Citrix ADC recibe respuesta del servidor Push RADIUS.
9. Como no se encuentra ninguna conexión TCP de cliente, ADC guarda el estado de la sesión.
10. Endpoint vuelve a sondeos para comprobar el estado de autenticación.
11. El dispositivo Citrix ADC establece la sesión y el inicio de sesión se realiza correctamente.

Configurar sondeos mediante CLI

A continuación se muestra un ejemplo de configuración CLI.

Configurar primer factor

```
add authentication ldapAction ldap-new -serverIP 10.106.40.65 -
    serverPort 636 -ldapBase "dc=aaatm-test,dc=com" -ldapBindDn
    administrator@aaatm-test.com -ldapBindDnPassword 2
    f63d3659103464a4fad0ade65e2ccfd4e8440e36ddff941d29796af03e01139 -
    encrypted -encryptmethod ENCMTHD_3 -ldapLoginName sAMAccountName -
    groupAttrName memberof -subAttributeName CN -secType SSL -
    alternateEmailAttr userParameters

add authentication Policy ldap-new -rule true -action ldap-new

bind authentication vserver avs -policy ldap-new -priority 1 -
    nextFactor rad_factor
<!--NeedCopy-->
```

Configurar segundo factor

```
add authentication radiusAction rad1 -serverIP 10.102.229.120 -radKey 1
    b1613760143ce2371961e9a9eb5392c86a4954a62397f29a01b5d12b42ce232 -
    encrypted -encryptmethod ENCMTHD_3

add authentication Policy rad -rule true -action rad1
<!--NeedCopy-->
```

Configurar esquema de inicio de sesión Poll.xml


```
add authentication loginSchema polling_schema -authenticationSchema
    LoginSchema/Poll.xml

add authentication policylabel rad_factor -loginSchema polling_schema

bind authentication policylabel rad_factor -policyName rad -priority 1
    -gotoPriorityExpression NEXT
<!--NeedCopy-->
```

Configurar sondeos mediante GUI

Para obtener pasos detallados sobre la configuración de la autenticación multifactor mediante la GUI, consulte Configuración de la autenticación nFactor.

A continuación se presentan los pasos de alto nivel de ejemplo necesarios para configurar Citrix ADC for Polling a partir del segundo factor.

1. Cree un primer factor para la autenticación, por ejemplo, LDAP.
2. Cree un segundo factor para la autenticación, por ejemplo RADIUS.
3. Agregue **Poll.xml** presente en Citrix ADC (/nsConfig/loginSchema/LoginSchema/) como esquema de inicio de sesión para el segundo factor.

Gestión de sesiones y tráfico

October 5, 2021

Parámetros de la sesión

Después de configurar los perfiles de autenticación, autorización y auditoría, configure los ajustes de sesión para personalizar las sesiones de usuario. La configuración de la sesión es:

- **El tiempo de espera de la sesión.**

  Controla el período tras el cual el usuario se desconecta automáticamente y debe volver a autenticarse para acceder a la intranet.

- **La configuración de autorización predeterminada.**

  Determina si el dispositivo Citrix ADC permitirá o denegará de forma predeterminada el acceso al contenido para el que no existe una directiva de autorización específica.

- **Configuración de inicio de sesión único.**

  Determina si el dispositivo Citrix ADC iniciará sesión de los usuarios en todas las aplicaciones web automáticamente después de autenticarse o pasará a los usuarios a la página de inicio de sesión de la aplicación web para autenticarse en cada aplicación.

- **Configuración del índice de credenciales.**

  Determina si el dispositivo Citrix ADC utiliza las credenciales de autenticación principal o secundaria para el inicio de sesión único.

Para configurar los ajustes de sesión, puede adoptar uno de los dos enfoques. Si quiere una configuración diferente para distintas cuentas de usuario o grupos, cree un perfil para cada cuenta de usuario o grupo para el que quiera configurar los ajustes de sesiones personalizadas. También crea directivas para seleccionar las conexiones a las que aplicar perfiles concretos y vincular las directivas a usuarios o grupos. También puede enlazar una directiva al servidor virtual de autenticación que gestiona el tráfico al que quiere aplicar el perfil.

Si quiere la misma configuración para todas las sesiones o si quiere personalizar la configuración predeterminada de las sesiones que no tienen configurados perfiles y directivas específicos, puede configurar simplemente la configuración global de la sesión.

Perfiles de sesión

Para personalizar las sesiones de usuario, primero debe crear un perfil de sesión. El perfil de sesión permite anular la configuración global de cualquiera de los parámetros de sesión.

> **Nota**
>
> Los términos “perfil de sesión” y “acción de sesión” significan lo mismo.

Para crear un perfil de sesión mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para crear un perfil de sesión y comprobar la configuración:

```
1 add tm sessionAction <name> [-sessTimeout <mins>] [-
     defaultAuthorizationAction ( ALLOW | DENY )][-SSO ( ON | OFF )][-
     ssoCredential ( PRIMARY | SECONDARY )] [-ssoDomain <string>][-
     httpOnlyCookie ( YES | NO )] [-persistentCookie ( ENABLED | DISABLED
      )] [-persistentCookieValidity <minutes>]
2
3 show tm sessionAction <name>
4 <!--NeedCopy-->
```


Ejemplo

```
> add tm sessionAction session-profile -sessTimeout 30 -
   defaultAuthorization ALLOW
 Done
> show tm sessionAction session-profile
1)      Name: session-profile
        Authorization action : ALLOW
        Session timeout: 30 minutes
 Done
<!--NeedCopy-->
```

Para modificar un perfil de sesión mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para modificar un perfil de sesión y comprobar la configuración:

```
set tm sessionAction <name> [-sessTimeout <mins>] [-
   defaultAuthorizationAction ( ALLOW | DENY )][-SSO ( ON | OFF )][-
   ssoCredential ( PRIMARY | SECONDARY )] [-ssoDomain <string>][-
   httpOnlyCookie ( YES | NO )] [-persistentCookie ( ENABLED | DISABLED
    )] [-persistentCookieValidity <minutes>]

show tm sessionAction
<!--NeedCopy-->
```

Ejemplo

```
> set tm sessionAction session-profile -sessTimeout 30 -
   defaultAuthorization ALLOW
 Done
> show tm sessionAction session-profile
1)      Name: session-profile
        Authorization action : ALLOW
        Session timeout: 30 minutes
 Done
<!--NeedCopy-->
```


Para quitar un perfil de sesión mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba el siguiente comando para quitar un perfil de sesión:

```
rm tm sessionAction <name>
<!--NeedCopy-->
```

Para configurar perfiles de sesión mediante la utilidad de configuración

1. Vaya a **Seguridad > AAA - Tráfico de aplicaciones > Sesión.**
2. Vaya a **Seguridad > AAA - Tráfico de aplicaciones > Directivas > Sesión.**
3. En el panel de detalles, haga clic en la ficha **Perfiles** .
4. En la ficha **Perfiles**, realice una de las siguientes acciones:
   - Para crear un nuevo perfil de sesión, haga clic en **Agregar.**
   - Para modificar un perfil de sesión existente, selecciónelo y, a continuación, haga clic en **Modificar.**
5. En el cuadro de diálogo Crear perfil de sesión de memoria de traducción o Configurar perfil de sesión de memoria de traducción, escriba o seleccione valores para los parámetros.
   - name*: actionName (no se puede cambiar para una acción de sesión configurada previamente).
   - Tiempo de espera de sesión: sessTimeout
   - Inicio de sesión único en aplicaciones web: inicio de sesión único
   - Acción de autorización predeterminada: DefaultAuthorizationAction
   - Índice de credenciales: SSOCredential
   - Dominio de inicio de sesión único: SSOdomain
   - Cookie de solo HTTP: HTTP OnlyCookie
   - Habilitar cookie persistent—Cookie persistente
   - Validez de cookies persistentes: validez de cookies persistentes
6. Haga clic en **Crear** o **Aceptar**. El perfil de sesión que ha creado aparece en el panel Directivas y perfiles de sesión.

Directivas de sesión

Después de crear uno o varios perfiles de sesión, crea directivas de sesión y, a continuación, enlaza las directivas de forma global o a un servidor virtual de autenticación para ponerlas en vigor.

Para crear una directiva de sesión mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para crear una directiva de sesión y comprobar la configuración:

```
-  add tm sessionPolicy <name> <rule> <action>
-  show tm sessionPolicy <name>
<!--NeedCopy-->
```

Ejemplo

```
> add tm sessionPolicy session-pol ”URL == /\*.png” session-profile
Done
> show tm sessionPolicy session-pol
1)      Name: session-pol       Rule: URL == '/\*.png'
        Action: session-profile
 Done
<!--NeedCopy-->
```

Para modificar una directiva de sesión mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para modificar una directiva de sesión y comprobar la configuración:

```
-  set tm sessionPolicy <name> [-rule <expression>] [-action <action>]
-  show tm sessionPolicy <name>
<!--NeedCopy-->
```

Ejemplo

```
> set tm sessionPolicy session-pol ”URL == /\*.png” session-profile
 Done
> show tm sessionPolicy session-pol
1)      Name: session-pol       Rule: URL == '/\*.png'
        Action: session-profile
 Done
<!--NeedCopy-->
```


Para enlazar globalmente una directiva de sesión mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para enlazar globalmente una directiva de sesión y verificar la configuración:

```
bind tm global -policyName <policyname> [-priority <priority>]
<!--NeedCopy-->
```

Ejemplo

```
> bind tm global -policyName session-pol
 Done

> show tm sessionPolicy session-pol
1)      Name: session-pol       Rule: URL == '/*.png'
        Action: session-profile
        Policy is bound to following entities
        1) TM GLOBAL    PRIORITY : 0
 Done

<!--NeedCopy-->
```

Para enlazar una directiva de sesión a un servidor virtual de autenticación mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba el siguiente comando para enlazar una directiva de sesión a un virtual de autenticación y compruebe la configuración:

```
bind authentication vserver <name> -policy <policyname> [-priority <
    priority>]
<!--NeedCopy-->
```

Ejemplo

```
bind authentication vserver auth-vserver-1 -policyName Session-Pol-1 -
    priority 1000
Done
<!--NeedCopy-->
```


Para desenlazar una directiva de sesión de un servidor virtual de autenticación mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para desvincular una directiva de sesión de un servidor virtual de autenticación y compruebe la configuración:

```
unbind authentication vserver <name> -policy <policyname>
<!--NeedCopy-->
```

Ejemplo

```
unbind authentication vserver auth-vserver-1 -policyName Session-Pol-1
Done
<!--NeedCopy-->
```

Para desenlazar una directiva de sesión vinculada globalmente mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para desenlazar una directiva de sesión vinculada globalmente:

```
unbind tm global -policyName <policyname>
<!--NeedCopy-->
```

Ejemplo

```
unbind tm global -policyName Session-Pol-1
Done
<!--NeedCopy-->
```

Para quitar una directiva de sesión mediante la interfaz de línea de comandos

En primer lugar, desvincule la directiva de sesión de global y, a continuación, en el símbolo del sistema, escriba los siguientes comandos para quitar una directiva de sesión y comprobar la configuración:


```
rm tm sessionPolicy <name>
<!--NeedCopy-->
```

Ejemplo

```
rm tm sessionPolicy Session-Pol-1
Done

<!--NeedCopy-->
```

Para configurar y enlazar directivas de sesión mediante la utilidad de configuración

1. Vaya a **Seguridad > AAA - Tráfico de aplicaciones > Sesión**.
2. Vaya a **Seguridad > AAA - Tráfico de aplicaciones > Directivas > Sesión**.
3. En el panel de detalles, en la ficha **Directivas**, realice una de las siguientes acciones:
   - Para crear una nueva directiva de sesión, haga clic en **Agregar**.
   - Para modificar una directiva de sesión existente, selecciónela y, a continuación, haga clic en **Modificar**.
4. En el cuadro de diálogo **Crear directiva** de **sesión o Configurar directiva** de sesión, escriba o seleccione los valores de los parámetros.
   - name*—policyName (no se puede cambiar para una directiva de sesión configurada previamente).
   - Perfil de solicidad*: nombreacción
   - expresión*: regla (se introducen expresiones seleccionando primero el tipo de expresión en la lista desplegable situada más a la izquierda debajo del área de texto Expresión y, a continuación, escribiendo la expresión directamente en el área de texto de la expresión, o haciendo clic en **Agregar** para abrir el cuadro de diálogo Agregar expresión y utilizar el menú desplegable. listas en él para construir su expresión.)
5. Haga clic en **Crear** o **Aceptar**. La directiva que ha creado aparece en el panel de detalles de la página **Directivas** y **perfiles** de sesión.
6. Para enlazar globalmente una directiva de sesión, en el panel de detalles, seleccione **Enlaces globales** en la lista desplegable **Acción** y rellene el cuadro de diálogo.
   - Seleccione el nombre de la directiva de sesión que quiere enlazar globalmente.
   - Haga clic en **OK**.
7. Para enlazar una directiva de sesión a un servidor virtual de autenticación, en el panel de navegación, haga clic en **Servidores virtuales**y agregue esa directiva a la lista de directivas.
   - En el panel de detalles, seleccione el servidor virtual y, a continuación, haga clic en **Modificar**.

- En la **sección Selecciones avanzadas** a la derecha del área de detalles, haga clic en **Directivas**.
- Seleccione una directiva o haga clic en el icono **más** para agregar una directiva.
- En la columna **Prioridad** de la izquierda, modifique la prioridad predeterminada para asegurarse de que la directiva se evalúa en el orden correcto.
- Haga clic en **OK**.
  Aparece un mensaje en la barra de estado que indica que la directiva se ha configurado correctamente.

Configuración de sesión global

Además de crear directivas y perfiles de sesión, o en lugar de crearlas, puede configurar la configuración global de la sesión. Esta configuración controla la configuración de la sesión cuando no hay ninguna directiva explícita que los anule.

Para configurar la configuración de la sesión mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para configurar la configuración global de la sesión y verifique la configuración:

```
set tm sessionParameter [-sessTimeout <mins>][-
    defaultAuthorizationAction ( ALLOW | DENY )][-SSO ( ON | OFF )][-
    ssoCredential ( PRIMARY | SECONDARY )][-ssoDomain <string>][-
    httpOnlyCookie ( YES | NO )][-persistentCookie ( ENABLED | DISABLED
    )] [-persistentCookieValidity <minutes>]
<!--NeedCopy-->
```

Ejemplo

```
> set tm sessionParameter -sessTimeout 30
  Done
> set tm sessionParameter -defaultAuthorizationAction DENY
  Done
> set tm sessionParameter -SSO ON
  Done
> set tm sessionParameter -ssoCredential PRIMARY
  Done
<!--NeedCopy-->
```


Para configurar los ajustes de sesión mediante la utilidad de configuración

1. Vaya a **Seguridad > AAA - Tráfico de aplicaciones**
2. En el panel de detalles, en **Configuración**, haga clic en Cambiar configuración global.
3. En el cuadro de diálogo **Configuración global de la sesión**, escriba o seleccione los valores de los parámetros.
    - Tiempo de espera de sesión: sessTimeout
    - Acción de autorización predeterminada: DefaultAuthorizationAction
    - Inicio de sesión único en aplicaciones web: inicio de sesión único
    - Índice de credenciales: SSOCredential
    - Dominio de inicio de sesión único: SSOdomain
    - Cookie de solo HTTP: HTTP OnlyCookie
    - Habilitar cookie persistent—Cookie persistente
    - Validez de cookie persistente (minutos) — PersistentCookieValidity
    - Página de inicio: página de inicio
4. Haga clic en **OK**.

Configuración de tráfico

Si utiliza el inicio de sesión único (SSO) basado en formularios o SAML para sus aplicaciones protegidas, configure esa función en la configuración de Tráfico. El inicio de sesión único permite a los usuarios iniciar sesión una vez para acceder a todas las aplicaciones protegidas, en lugar de exigirles que inicien sesión por separado para acceder a cada una de ellas.

El inicio de sesión único basado en formularios le permite utilizar un formulario web de su propio diseño como método de inicio de sesión en lugar de una ventana emergente genérica. Por lo tanto, puede incluir el logotipo de su empresa y otra información que quiera que vean sus usuarios en el formulario de inicio de sesión. El inicio de sesión único de SAML le permite configurar un dispositivo Citrix ADC o una instancia de dispositivo virtual para autenticarse en otro dispositivo Citrix ADC en nombre de los usuarios que se han autenticado con el primer dispositivo.

Para configurar cualquier tipo de inicio de sesión único, primero debe crear un formulario o un perfil de inicio de sesión único de SAML. A continuación, crea un perfil de tráfico y lo vincula al perfil de SSO que creó. A continuación, crea una directiva y la vincula al perfil de tráfico. Por último, vincula la directiva de forma global o a un servidor virtual de autenticación para poner en práctica la configuración.

Perfiles de tráfico

Después de crear al menos un formulario o un perfil sso SAML, debe crear un perfil de tráfico.

> **Nota:**
>
> En esta función, los términos “perfil” y “acción” significan lo mismo.

Para crear un perfil de tráfico mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
add tm trafficAction <name> [-appTimeout <mins>][-SSO ( ON | OFF ) [-
    formSSOAction <string>]][-persistentCookie ( ENABLED | DISABLED )][-
    InitiateLogout ( ON | OFF )]
<!--NeedCopy-->
```

Ejemplo

```
add tm trafficAction Traffic-Prof-1  - appTimeout 10 -SSO ON -
    formSSOAction SSO-Prof-1
<!--NeedCopy-->
```

Para modificar un perfil de sesión mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
set tm trafficAction <name> [-appTimeout <mins>] [-SSO ( ON | OFF ) [-
    formSSOAction <string>]] [-persistentCookie ( ENABLED | DISABLED )]
    [-InitiateLogout ( ON | OFF )]
<!--NeedCopy-->
```

Ejemplo

```
set tm trafficAction Traffic-Prof-1  - appTimeout 10 -SSO ON -
    formSSOAction SSO-Prof-1
<!--NeedCopy-->
```

Para quitar un perfil de sesión mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:


```
rm tm trafficAction <name>
<!--NeedCopy-->
```

Ejemplo

```
rm tm trafficAction Traffic-Prof-1
<!--NeedCopy-->
```

Para configurar perfiles de tráfico mediante la utilidad de configuración

1. Vaya a **Seguridad > AAA - Tráfico de aplicaciones > Tráfico.**
2. Vaya a **Seguridad > AAA - Tráfico de aplicaciones > Directivas > Tráfico.**
3. En el panel de detalles, haga clic en la ficha Perfiles.
4. En la ficha Perfiles, realice una de las siguientes acciones:
   - Para crear un nuevo perfil de tráfico, haga clic en **Agregar.**
   - Para modificar un perfil de tráfico existente, selecciónelo y, a continuación, haga clic en **Modificar.**
5. En el cuadro de diálogo **Crear perfil** de **tráfico o Configurar perfil** de tráfico, especifique los valores de los parámetros.
   - nombre*: nombre (no se puede cambiar para una acción de sesión configurada previamente).
   - AppTimeout: AppTimeout
   - Inicio de sesión único: inicio de sesión único
   - Acción de SSO de formulario: acción de formulario SSO
   - Acción de inicio de sesión único de SAML: acción SAMLSSO
   - Habilitar cookie persistent—Cookie persistente
   - Iniciar cierre de sesión: iniciar sesión
6. Haga clic en **Crear** o **Aceptar**. El perfil de tráfico que ha creado aparece en el panel Directivas de tráfico, Perfiles y en el panel Form SSO Profiles o SAML SSO Profiles, según corresponda.

Compatibilidad con expresiones AAA.USER y AAA.LOGIN

La expresión AAA.USER se ha implementado ahora para reemplazar las expresiones HTTP.REQ.USER existentes. La expresión AAA.USER se aplica para controlar el tráfico no HTTP, como Secure Web Gateway (SWG) y el mecanismo de acceso basado en roles (RBA). Las expresiones AAA.USER equivalen a las expresiones HTTP.REQ.USER.

Puede utilizar la expresión en varias acciones o configuraciones de perfiles.

En el símbolo del sistema, escriba:

```
add tm trafficAction <name> [SSO (ON|OFF)] [-userExpression <string>]

add tm trafficAction <name> [SSO (ON|OFF)] [-passwdExpression <string>]

<!--NeedCopy-->
```

Ejemplo

```
add tm trafficAction tm_act -SSO ON -userExpression "AAA.USER.NAME"

add tm trafficAction tm_act -SSO ON -userExpression "AAA.USER.PASSWD"

add tm trafficPolicy tm_pol true tm_act

bind lb vserver lb1 -policyName tm_pol -priority 2
<!--NeedCopy-->
```

> **Nota:**
>
> Si utiliza la expresión HTTP.REQ.USER, el mensaje de advertencia "HTTP.REQ.USER ha quedado obsoleto. Usar AAA.USER en su lugar" aparece en el símbolo del sistema.

- **Expresión AAA.LOGIN.** La expresión LOGIN representa el inicio de sesión previo, también conocido como solicitud de inicio de sesión. La solicitud de inicio de sesión puede proceder de Citrix Gateway, del proveedor de identidades SAML o de la autenticación de OAuth. Citrix ADC extraerá los atributos necesarios de la configuración de directivas. La expresión AAA.LOGIN contiene los atributos, que se pueden obtener según lo siguiente:
  - **AAA.LOGIN.USERNAME.** El nombre de usuario (si se encuentra) se obtiene de la solicitud de inicio de sesión actual. La misma expresión aplicada a una solicitud sin inicio de sesión (determinada por una autenticación, autorización y auditoría) da como resultado una cadena vacía.
  - **AAA.LOGIN.PASSWORD.** La contraseña de usuario (si se encuentra) se obtiene de la solicitud de inicio de sesión actual. La expresión da como resultado una cadena vacía si no se encuentra la contraseña.
  - **AAA.LOGIN.PASSWORD2.** La segunda contraseña (si se encuentra) se obtiene de la solicitud de inicio de sesión.
  - **AAA.LOGIN.DOMAIN.** La información del dominio se obtiene de la solicitud de inicio de sesión.

- **AAA.USER.ATTRIBUTE (“#”).** La expresión se utiliza para almacenar el atributo de usuario. Aquí # puede ser un valor entero (entre 1 y 16) o un valor de cadena. Puede utilizar estos valores de índice mediante la expresión AAA.USER.ATTRIBUTE (“#”). El módulo de autenticación, autorización y auditoría busca el atributo de sesiones de usuario y `AAA.USER.ATTRIBUTE(”##”)` consulta la tabla hash para ese atributo en particular. Por ejemplo, si `Attributes(”samaccountname”)` está configurado, `AAA.USER.ATTRIBUTE(”samaccountname”)` consultaría el mapa hash y obtendría el valor correspondiente a `samaccountname`.

Directivas de tráfico

Después de crear uno o varios perfiles de tráfico y de SSO de formulario, se crean directivas de tráfico y, a continuación, se enlazan las directivas, ya sea de forma global o a un servidor virtual de administración del tráfico, para ponerlas en práctica.

Para crear una directiva de tráfico mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
add tm trafficPolicy <name> <rule> <action>
<!--NeedCopy-->
```

Ejemplo

```
add tm trafficPolicy Traffic-Pol-1 ”HTTP.REQ.HEADER(”Cookie”).CONTAINS(
   ”login=true”)” Traffic-Prof-1
<!--NeedCopy-->
```

Para modificar una directiva de tráfico mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
set tm trafficPolicy <name> <rule> <action>
<!--NeedCopy-->
```

Ejemplo


```
set tm trafficPolicy Traffic-Pol-1 ”HTTP.REQ.HEADER(”Cookie”).CONTAINS(
   ”login=true”)” Traffic-Prof-1
<!--NeedCopy-->
```

Para enlazar globalmente una directiva de tráfico mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
bind tm global -policyName <string> [-priority <priority>]
<!--NeedCopy-->
```

Ejemplo

```
bind tm global -policyName Traffic-Pol-1
<!--NeedCopy-->
```

Para enlazar una directiva de tráfico a un servidor virtual de equilibrio de carga o conmutación de contenido mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba uno de los siguientes comandos:

```
bind lb vserver <name> -policy <policyName> [-priority <priority>]

bind cs vserver <name> -policy <policyName> [-priority <priority>]
<!--NeedCopy-->
```

Ejemplo

```
bind authentication vserver auth-vserver-1 -policyName Traffic-Pol-1 -
   priority 1000
<!--NeedCopy-->
```

Para desvincular una directiva de tráfico enlazado globalmente mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:


```
unbind tm global -policyName <policyname>
<!--NeedCopy-->
```

Ejemplo

```
unbind tm global -policyName Traffic-Pol-1
<!--NeedCopy-->
```

Para desenlazar una directiva de tráfico de un servidor virtual de equilibrio de carga o conmutación de contenido mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba uno de los siguientes comandos:

```
unbind lb vserver <name> -policy <policyname>

unbind cs vserver <name> -policy <policyname>
<!--NeedCopy-->
```

Ejemplo

```
unbind authentication vserver auth-vserver-1 -policyName Traffic-Pol-1
<!--NeedCopy-->
```

Para quitar una directiva de tráfico mediante la interfaz de línea de comandos

En primer lugar, desvincule la directiva de sesión de global y, a continuación, en el símbolo del sistema, escriba:

```
rm tm trafficPolicy <name>
<!--NeedCopy-->
```

Ejemplo


```
rm tm trafficPolicy Traffic-Pol-1
<!--NeedCopy-->
```

Para configurar y enlazar directivas de tráfico mediante la utilidad de configuración

1. Vaya a **Seguridad > AAA - Tráfico de aplicaciones > Tráfico.**
2. Vaya a **Seguridad > AAA - Tráfico de aplicaciones > Directivas > Tráfico.**
3. En el panel de detalles, realice una de las acciones siguientes:
   - Para crear una nueva directiva de sesión, haga clic en **Agregar.**
   - Para modificar una directiva de sesión existente, selecciónela y, a continuación, haga clic en **Modificar.**
4. En el cuadro de diálogo **Crear directiva de tráficoo Configurar directiva de tráfico**, especifique los valores de los parámetros.
   - name*—policyName (no se puede cambiar para una directiva de sesión configurada previamente).
   - profile*: nombreAcción
   - Expresión: regla (se introducen expresiones seleccionando primero el tipo de expresión en la lista desplegable situada más a la izquierda debajo del área de texto Expresión y, a continuación, escribiendo la expresión directamente en el área de texto de la expresión o haciendo clic en Agregar para abrir el cuadro de diálogo Agregar expresión y utilizar las listas desplegables que contiene para construye su expresión).
5. Haga clic en **Crear** o **Aceptar**. La directiva que ha creado aparece en el panel de detalles de la página **Directivas** y **perfiles** de sesión.

Perfiles de SSO de formularios

Para habilitar y configurar el SSO basado en formularios, primero debe crear un perfil de SSO.

> **Nota**
>
> - El inicio de sesión único basado en formularios no funciona si el formulario está personalizado para incluir Javascript.
> - En esta función, los términos “perfil” y “acción” significan lo mismo.

Para crear un perfil de SSO de formulario mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:


```
add tm formSSOAction <name> -actionURL <URL> -userField <string> -
    passwdField <string> -ssoSuccessRule <expression> [-nameValuePair <
    string>] [-responsesize <positive_integer>][-nvtype ( STATIC |
    DYNAMIC )][-submitMethod ( GET | POST )]

show tm formSSOAction [<name>]
<!--NeedCopy-->
```

Ejemplo

```
add tm formSSOAction SSO-Prof-1 -actionURL "/logon.php"
-userField "loginID" -passwdField "passwd"
-nameValuePair "loginID passwd" -responsesize "9096"
-ssoSuccessRule "HTTP.RES.HEADER("Set-Cookie").CONTAINS("LogonID")"
-nvtype STATIC -submitMethod GET
 - sessTimeout 10 -defaultAuthorizationAction ALLOW
<!--NeedCopy-->
```

Para modificar el SSO de un formulario mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
set tm formSSOAction <name> -actionURL <URL> -userField <string> -
    passwdField <string> -ssoSuccessRule <expression> [-nameValuePair <
    string>] [-responsesize <positive_integer>][-nvtype ( STATIC |
    DYNAMIC )][-submitMethod ( GET | POST )]
<!--NeedCopy-->
```

Ejemplo

```
set tm formSSOAction SSO-Prof-1 -actionURL "/logon.php"
-userField "loginID" -passwdField "passwd"
-ssoSuccessRule "HTTP.RES.HEADER("Set-Cookie").CONTAINS("LogonID")"
-nameValuePair "loginID passwd" -responsesize "9096"
-nvtype STATIC -submitMethod GET
 - sessTimeout 10 -defaultAuthorizationAction ALLOW
<!--NeedCopy-->
```


Para quitar un perfil de SSO de formulario mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
rm tm formSSOAction <name>
<!--NeedCopy-->
```

Ejemplo

```
rm tm sessionAction SSO-Prof-1
<!--NeedCopy-->
```

Para configurar perfiles de SSO de formulario mediante la utilidad de configuración

1. Vaya a **Seguridad > AAA - Tráfico de aplicaciones > Directivas > Tráfico**.
2. En el panel de detalles, haga clic en la ficha **Perfiles de SSO de formulario** .
3. En la ficha Perfiles de SSO de formulario, realice una de las siguientes acciones:
   - Para crear un nuevo perfil de SSO de formulario, haga clic en **Agregar**.
   - Para modificar un perfil de SSO de formulario existente, selecciónelo y, a continuación, haga clic en Modificar.
4. En el cuadro de diálogo **Crear perfil de SSO** de **formulario o Configurar perfil de SSO** de formulario, especifique los valores de los parámetros:
   - nombre*: nombre (no se puede cambiar para una acción de sesión configurada previamente).
   - URL de acción*: actionURL
   - Campo Nombre de usuario*: campo de usuario
   - Campo de contraseña*: campo de contraseña
   - expresión* — ssoSuccessRule
   - Pares de valor de nombre: NameValuePair
   - Tamaño de respuesta: tamaño de respuesta
   - Extracción: tipo NV
   - Método de envío: método Submit
5. Haga clic en **Crear** o **Aceptar**y, a continuación, en **Cerrar**. El perfil de SSO de formulario que ha creado aparece en el panel **Directivas de tráfico**, **perfiles**y **perfiles de SSO de formulario** .

Perfiles de inicio de sesión único SAML

Para habilitar y configurar el inicio de sesión único basado en SAML, primero debe crear un perfil de SSO SAML.

Para crear un perfil de inicio de sesión único de SAML mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
add tm samlSSOProfile <name> -samlSigningCertName <string> -
    assertionConsumerServiceURL <URL> -relaystateRule <expression> -
    sendPassword (ON | OFF) [-samlIssuerName <string>]
<!--NeedCopy-->
```

Ejemplo

```
add tm samlSSOProfile saml-SSO-Prof-1 -samlSigningCertName "Example,
    Inc."  -assertionConsumerServiceURL "https://service.example.com" -
    relaystateRule "true"  -sendPassword "ON" -samlIssuerName "Example,
    Inc."
<!--NeedCopy-->
```

Para modificar un inicio de sesión único de SAML mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
set tm samlSSOProfile <name> -samlSigningCertName <string> -
    assertionConsumerServiceURL <URL> -relaystateRule <expression> -
    sendPassword (ON | OFF) [-samlIssuerName <string>]
<!--NeedCopy-->
```

Ejemplo

```
set tm samlSSOProfile saml-SSO-Prof-1 -samlSigningCertName "Example,
    Inc."  -assertionConsumerServiceURL "https://service.example.com" -
    relaystateRule "true"  -sendPassword "ON" -samlIssuerName "Example,
    Inc."
<!--NeedCopy-->
```

Para quitar un perfil de SSO SAML mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:


```
rm tm samlSSOProfile <name>
<!--NeedCopy-->
```

Ejemplo

```
rm tm sessionAction saml-SSO-Prof-1
<!--NeedCopy-->
```

Para configurar un perfil de inicio de sesión único de SAML mediante la utilidad de configuración

1. Vaya a **Seguridad > AAA - Tráfico de aplicaciones > Directivas > Tráfico.**
2. En el panel de detalles, haga clic en la ficha **Perfiles de inicio de sesión único de SAML** .
3. En la ficha **Perfiles de inicio de sesión único de SAML**, realice una de las siguientes acciones:
   - Para crear un nuevo perfil de inicio de sesión único de SAML, haga clic en **Agregar.**
   - Para modificar un perfil de inicio de sesión único de SAML existente, selecciónelo y, a continuación, haga clic en **OpenEdit**.
4. En el cuadro de diálogo **Crear perfiles** de inicio de **sesión único SAML o Configurar perfiles de SSO** SAML, defina los siguientes parámetros:
   - Nombre*
   - Nombre del certificado de firma*
   - URL ACS*
   - Regla de estado de relés*
   - Enviar contraseña
   - Nombre del emisor
5. Haga clic en **Crear** o en **Aceptar**y, a continuación, en **Cerrar.** El perfil de inicio de sesión único de SAML que ha creado aparece en el panel Directivas de tráfico, perfiles y perfiles de inicio de sesión único de SAML.

Tiempo de espera de sesión para OWA 2010

Ahora puede forzar el tiempo de espera de las conexiones de OWA 2010 tras un período de inactividad especificado. OWA envía repetidas solicitudes de mantenimiento al servidor para evitar tiempos de espera. Mantener las conexiones abiertas puede interferir con el inicio de sesión único.

Para forzar el tiempo de espera de OWA 2010 tras un período especificado mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos:


```
add tm trafficAction <actname> [-forcedTimeout <forcedTimeout> -
    forcedTimeoutVal <mins>]
<!--NeedCopy-->
```

Por<actname>, sustituye por un nombre su directiva de tráfico. Por<mins>, sustituya el número de minutos tras los cuales se iniciará un tiempo de espera forzado. Por, sustitúyalo por uno de los valores siguientes:

-**START**: Inicia el temporizador para que se agote el tiempo de espera forzado si aún no se ha iniciado un temporizador. Si existe un temporizador de ejecución, no tiene efecto.
-**STOP** : detiene un temporizador de funcionamiento. Si no se encuentra ningún temporizador de ejecución, no tiene efecto.
-**RESET** : reinicia un temporizador de ejecución. Si no se encuentra ningún temporizador de ejecución, inicia un temporizador como si se hubiera utilizado la opción START.

```
add tm trafficPolicy <polname> <rule> <actname>
<!--NeedCopy-->
```

Por<polname>, sustituye por un nombre su directiva de tráfico. Por<rule>, sustituya una regla en la directiva Citrix ADC Advanced.

```
bind lb vserver <vservername>  - policyName <name> -priority <number>
<!--NeedCopy-->
```

Por<vservername>, sustituya el nombre del servidor virtual de administración del tráfico de autenticación, autorización y auditoría. Por<priority>, sustitúyalo por un entero que designe la prioridad de la directiva.

Ejemplo

```
add tm trafficAction act-owa2010timeout -forcedTimeout RESET -
    forcedTimeoutVal 10
add tm trafficPolicy pol-owa2010timeout true act-owa2010timeout
bind lb vserver vs-owa2010 -policyName pol-owa2010timeout -priority 10
<!--NeedCopy-->
```


Limitación de velocidad para Citrix Gateway

March 9, 2022

La función de limitación de velocidad de Citrix Gateway permite definir la carga máxima para una entidad de red o entidad virtual determinada en el dispositivo Citrix Gateway. Dado que el dispositivo Citrix Gateway consume todo el tráfico no autenticado, el dispositivo suele estar expuesto a solicitudes de proceso a un ritmo elevado. La función de limitación de velocidad le permite configurar el dispositivo Citrix Gateway para supervisar la velocidad de tráfico asociada a una entidad y tomar medidas preventivas, en tiempo real, basadas en el tráfico. Para obtener más información sobre cómo funciona la limitación de velocidad en un dispositivo Citrix ADC, consulte Limitación de velocidad.

Citrix ADC tiene la función de limitación de velocidad que proporciona protección a los servidores back-end para una velocidad imprevista. Dado que la función de Citrix ADC no servía para el tráfico no autenticado que administra Citrix Gateway, Citrix Gateway necesitaba su propia funcionalidad de limitación de velocidad. Esto es necesario para comprobar una tasa imprevista de solicitudes de varias fuentes a las que está expuesto el dispositivo Citrix Gateway. Por ejemplo, solicitudes de control o inicio de sesión no autenticadas y determinadas API expuestas para validaciones de dispositivos o usuarios finales.

Casos de uso comunes para la limitación de velocidad

- Limita el número de solicitudes por segundo de una URL.
- Elimine una conexión en función de las cookies recibidas en la solicitud de un host en particular si la solicitud excede el límite de velocidad.
- Limite el número de solicitudes HTTP que llegan del mismo host (con una máscara de subred concreta) y que tienen la misma dirección IP de destino.

Configurar la limitación de velocidad para Citrix Gateway

Requisitos previos

Servidor virtual de autenticación configurado.

Puntos que tener en cuenta

- En los pasos de configuración, se configura un identificador de límite de muestra. Lo mismo se puede configurar con todos los parámetros admitidos como selector de flujo, modo. Para obtener una descripción exhaustiva de las capacidades de limitación de tarifas, consulte Limitación de tarifas.

- La directiva también se puede enlazar a un servidor virtual VPN de la siguiente manera. Necesita un servidor virtual VPN configurado para enlazar las directivas mediante el siguiente comando.

```
bind vpn vserver  -policy denylogin  - pri 1  - type aaa_request
<!--NeedCopy-->
```

- AAA_REQUEST es un punto de enlace recién introducido para las directivas de respuesta. Las directivas configuradas en este punto de enlace se aplican a todas las solicitudes entrantes del servidor virtual especificado. Las directivas se procesan para el tráfico no autenticado o de control antes de cualquier otro procesamiento.
- La vinculación de la directiva al servidor virtual de Citrix Gateway permite limitar la velocidad en el punto de enlace AAA_REQUEST para todo el tráfico consumido por Citrix Gateway, incluidas las solicitudes no autenticadas.
- La vinculación de la directiva a un servidor virtual de autenticación limita las solicitudes de control o no autenticadas que llegan al servidor virtual de autenticación.

Para configurar la limitación de velocidad mediante la interfaz de línea de comandos, en el símbolo del sistema, escriba los siguientes comandos:

```
add limitIdentifier <limitIdentifier name> -threshold <positive_integer
    > -timeslice <positive_integer> -mode <mode type>
<!--NeedCopy-->
```

Ejemplo:

```
add limitIdentifier limit_one_login -threshold 10 -timeslice 4294967290
    -mode REQUEST_RATE
<!--NeedCopy-->
```

```
add responderaction denylogin respondwith  ' "HTTP/1.1 200 OK\r\n\r\n"
    +  "Request is denied due to unusual rate" '
<!--NeedCopy-->
```

```
add responder policy denylogin 'sys.check_limit("limit_one_login")'
   denylogin
```



```
<!--NeedCopy-->
```

```
bind authentication vserver <vserver name> -policy denylogin -pri 1 -
    type aaa_request
<!--NeedCopy-->
```

Ejemplo:

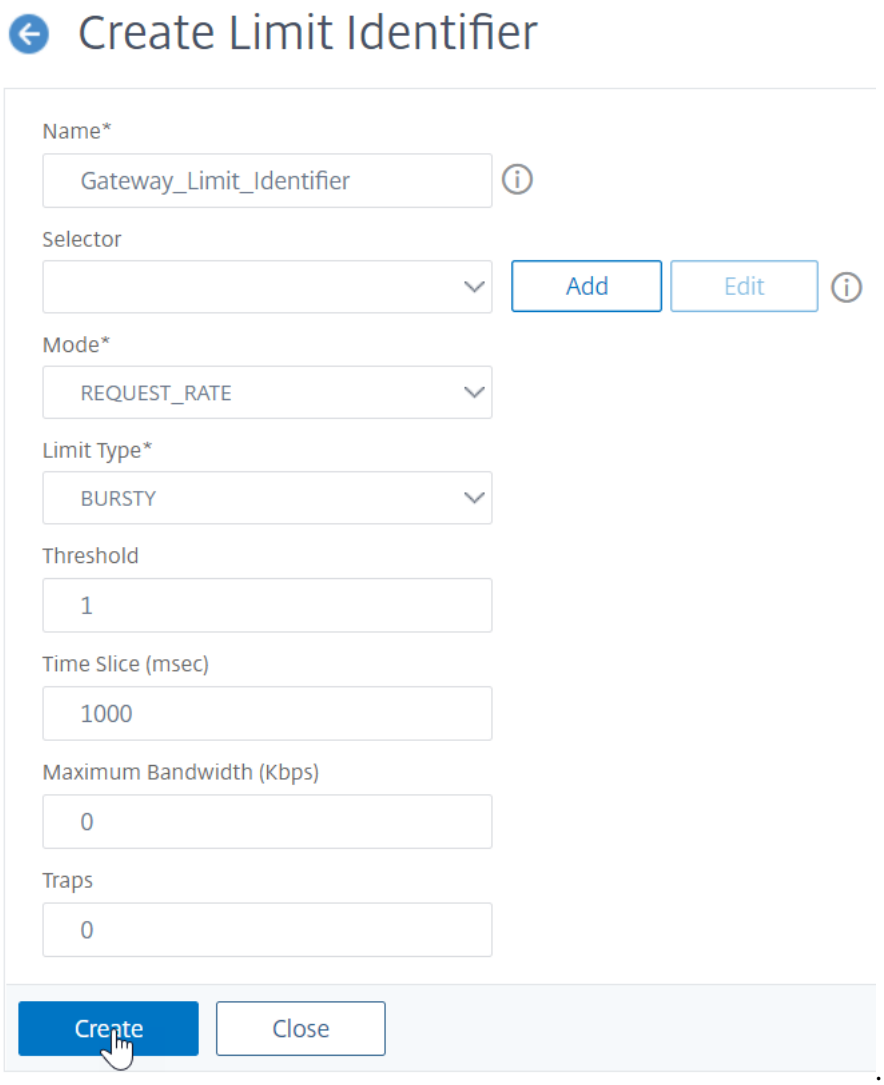
```
bind authentication vserver authvserver -policy denylogin -pri 1 -
    type aaa_request
<!--NeedCopy-->
```

Descripción del parámetro

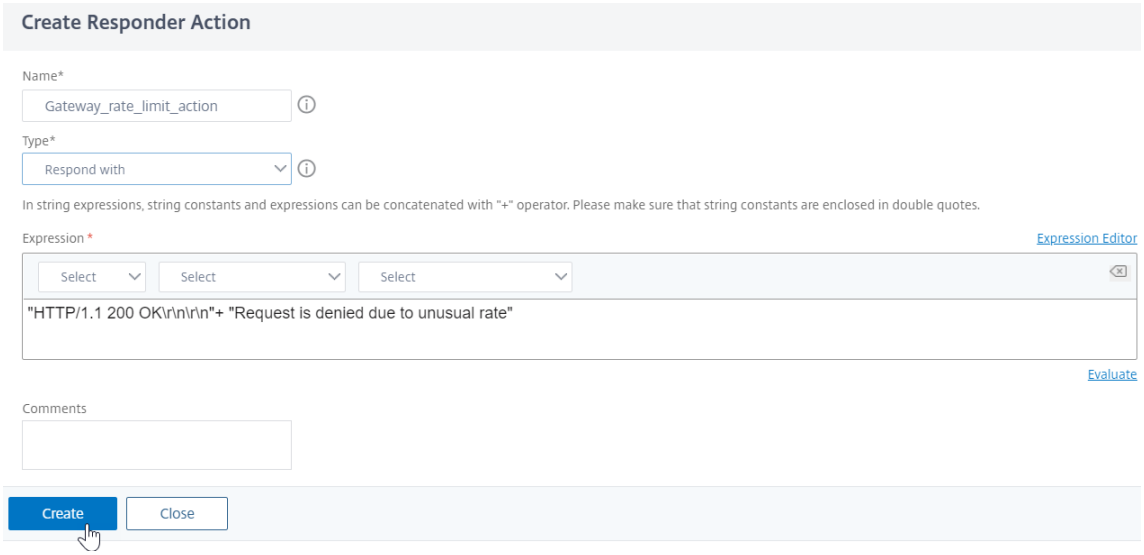
- **LimitIdentifier:** nombre de un identificador de límite de velocidad. Debe comenzar con una letra ASCII o un carácter de guión bajo (_) y debe constar únicamente de caracteres alfanuméricos o de guión bajo ASCII. No se deben utilizar palabras reservadas. Se trata de un argumento obligatorio. Longitud máxima: 31
- **umbral:** número máximo de solicitudes permitidas en el segmento de tiempo determinado cuando se realiza un seguimiento de las solicitudes (el modo se establece como REQUEST_RATE) por segmento de tiempo. Cuando se realiza un seguimiento de las conexiones (el modo se establece como CONNECTION), es el número total de conexiones que se dejarían pasar. Valor por defecto: 1 Valor mínimo: 1 Valor máximo: 4294967295
- **TimeSlice -** Intervalo de tiempo, en milisegundos, especificado en múltiplos de 10, durante el cual se realiza un seguimiento de las solicitudes para comprobar si cruzan el umbral. El argumento solo es necesario cuando el modo se establece en REQUEST_RATE. Valor predeterminado: 1000 Valor mínimo: 10 Valor máximo: 4294967295
- **mode:** define el tipo de tráfico que se va a rastrear.
  - REQUEST_RATE: rastrea las solicitudes/el segmento de tiempo.
  - CONEXIÓN: realiza un seguimiento de las transacciones activas.

Para configurar la limitación de velocidad mediante la GUI de Citrix ADC:

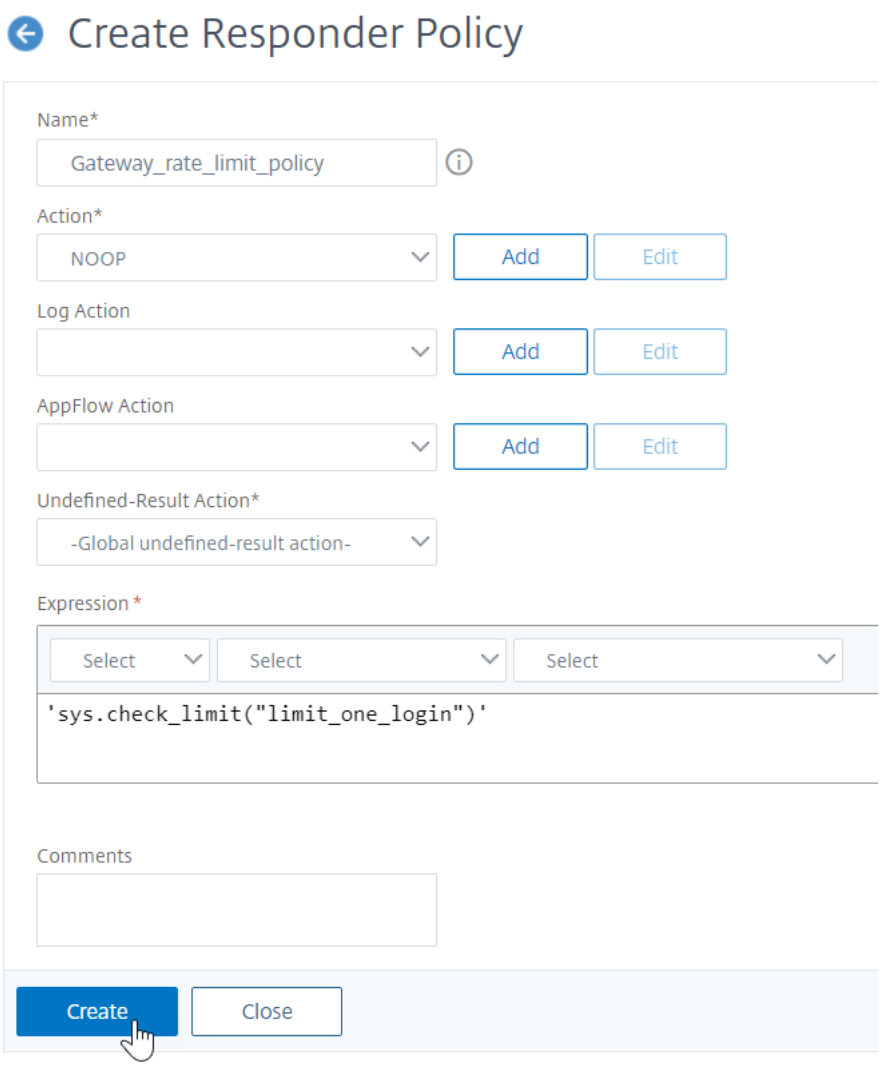
1. Vaya a **AppExpert > Límite de velocidad > Identificadores de límite**, haga clic en **Agregar** y especifique los detalles relevantes como se especifica en la sección CLI.



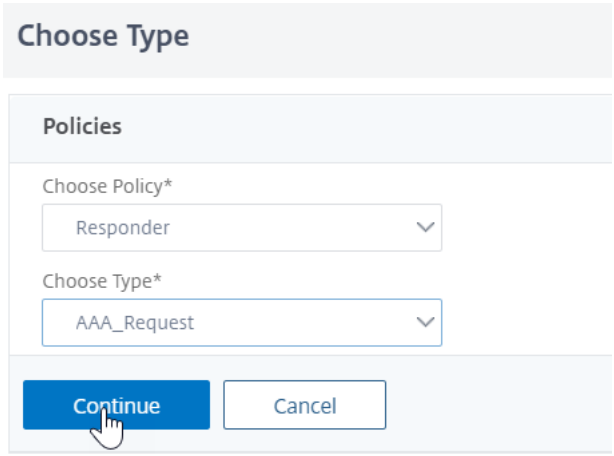
2. Vaya a **AppExpert>Respondedor>Directivas**. En la página **Directivas de respuesta**, haga clic en **Agregar**.
3. En la página **Crear directiva de respuesta**, cree una directiva de respuesta con una acción de respuesta que tenga el identificador de límite.
4. Para crear una acción de respuesta, haga clic en **Agregar** junto a **Acción** e introduzca un nombre para la acción de respuesta.
5. Seleccione escribir como **Responder con** en el menú desplegable, especifique la siguiente expresión, “HTTP/1.1 200 OK\ r\ n\ r\ n”+ “Solicitud denegada debido a una tasa inusual” y haga clic en **Crear**.



6. Para crear una directiva de respuesta, en la página **Crear directiva de respuesta**, introduzca un nombre para la directiva de respuesta, especifique la siguiente expresión, 'sys.check_limit ("limit_one_login") 'y haga clic en **Crear**.



7. Enlazar la directiva de respuesta al servidor virtual de autenticación.
   - Vaya a **Seguridad>Tráfico de aplicaciones AAA>Servidor virtual**.
   - Seleccione el servidor virtual.
   - Agregue una directiva.
   - Elija la directiva de respuesta que quiere vincular al servidor, establezca la prioridad.
   - Elija el tipo como **AAA-REQUEST** y haga clic en **Continuar**.



> **Nota:** También puede habilitar la limitación de velocidad en el punto de enlace AAA_REQUEST para el servidor virtual VPN.

Configuración de los casos de uso habituales para aplicar la limitación de velocidad a Citrix Gateway

A continuación se muestran ejemplos de comandos para configurar casos de uso comunes.

- Limita el número de solicitudes por segundo de una URL.

```
add stream selector ipStreamSelector http.req.url "client.ip.src"

add ns limitIdentifier ipLimitIdentifier -threshold 4 -timeslice 1000 -mode request_rate -limitType smooth -selectorName ip StreamSelector

add responder policy ipLimitResponderPolicy "http.req.url.contains(\" myasp.asp\" ) && sys.check_limit(\" ipLimitIdentifier\" )" myWebSiteRedirectAction

bind authentication virtual server authvserver -policy denylogin -pri 1 -type aaa_request
<!--NeedCopy-->
```

- Desconectar una conexión en función de las cookies recibidas a petición de www.yourcompany.com si la solicitud supera el límite de tarifa.


```
add stream selector cacheStreamSelector  “http.req.cookie.value(\” mycookie\” )”  “client.ip.src.subnet(24)”

add ns limitIdentifier myLimitIdentifier  -Threshold 2  -timeSlice 3000  -selectorName reqCookieStreamSelector

add responder action sendRedirectURL redirect `”http://www.mycompany.com”` + http.req.url'

add responder policy rateLimitCookiePolicy

 “http.req.url.contains(\www.yourcompany.com) && sys.check_limit(\” myLimitIdentifier\” )”  sendRedirectUrl

<!--NeedCopy-->
```

- Limite el número de solicitudes HTTP que llegan del mismo host (con una máscara de subred de 32) y que tienen la misma dirección IP de destino.

```
add stream selector ipv6_sel  “CLIENT.IPv6.src.subnet(32)” CLIENT.IPv6.dst

add ns limitIdentifier ipv6_id  -imeSlice 20000  -selectorName ipv6_sel

add lb vserver ipv6_vip HTTP 3ffe:: 209 80  -persistenceType NONE  -cltTime

add responder action redirect_page redirect  “\” `http://redirectpage.com/\” ”`

add responder policy ipv6_resp_pol  “SYS.CHECK_LIMIT(\” ipv6_id\” )”  redirect_page

bind responder global ipv6_resp_pol 5 END  -type DEFAULT
<!--NeedCopy-->
```

Autorizar el acceso de usuario a los recursos de la aplicación

January 12, 2021

Puede controlar los recursos a los que un usuario autenticado puede acceder dentro de una aplicación.

Para ello, asocie una directiva de autorización a cada uno de los usuarios, ya sea individualmente o asociando la directiva a un grupo de usuarios. La directiva de autorización debe especificar lo siguiente:

- **Regla.** El recurso al que se debe autorizar el acceso. Esto se puede especificar mediante el uso de expresiones básicas o avanzadas.
- **Acción.** Si se debe permitir o denegar el acceso al recurso.

De forma predeterminada, el acceso a todos los recursos de una aplicación es **DENEGADO** a todos los usuarios. Sin embargo, puede cambiar esta acción de autorización predeterminada para **permitir** el acceso a todos los usuarios (estableciendo los parámetros de sesión en el perfil de sesión o estableciendo los parámetros de sesión globales).

> **Advertencia**
>
> Para obtener una seguridad óptima, Citrix recomienda no cambiar la acción de autorización predeterminada de DENEGAR a AUTORIZAR. En su lugar, se recomienda crear directivas de autorización específicas para los usuarios que necesitan acceso a recursos específicos.

Para configurar la autorización mediante la CLI

1. Configure la directiva de autorización.

   ns-cli-prompt<name> <rule> <action> > **agregar directiva de autorización

2. Asocie la directiva con el usuario o grupo apropiado.

   - Enlazar la directiva a un usuario específico.

     ns-cli-prompt<policyname> > **bind aaa user <username> -policy

   - Enlazar la directiva a un grupo específico.

     ns-cli-prompt<policyname> > **bind aaa group <groupName> -policy

Para configurar la autorización mediante la interfaz gráfica de usuario (ficha Configuración)

1. Cree la directiva de autorización.

   Vaya a **Seguridad > AAA: Tráfico de aplicaciones > Directivas > Autorización**, haga clic en **Agregar** y defina la directiva según sea necesario.

2. Asocie la directiva con el usuario o grupo apropiado.

Vaya a **Seguridad > AAA: Tráfico de aplicaciones > Usuarios** o **grupos** y modifique el usuario o grupo correspondiente para asociarlo a la directiva de autorización.

Configuraciones de autorización de ejemplo

A continuación se muestran algunas configuraciones de ejemplo para autorizar el acceso de los usuarios a algunos recursos de la aplicación. Tenga en cuenta que estos son comandos CLI. Puede hacer configuraciones similares mediante la GUI, aunque no debe incluir la expresión entre comillas (“).

- `add authorization policy authzpol1 ”HTTP.REQ.URL.SUFFIX.EQ(\”gif\”)” ALLOW<!--NeedCopy-->`
- `bind aaa user user1 -policy authzpol1<!--NeedCopy-->`
- `add authorization policy authzpol2 ”HTTP.REQ.URL.SUFFIX.EQ(\”png\”)” DENY<!--NeedCopy-->`
- `bind aaa group group1 -policy authzpol2<!--NeedCopy-->`

Auditoría de sesiones autenticadas

January 12, 2021

Puede configurar el dispositivo Citrix ADC para que mantenga un registro de todos los eventos que se desencadenan en una sesión autenticada. Con esta información, puede auditar la información de estado y estado, para ver el historial de los usuarios en orden cronológico.

Para ello, defina una directiva de auditoría que especifique lo siguiente:

- **Tipo de registro.** Los registros se pueden almacenar de forma remota (syslog) o localmente en el dispositivo Citrix ADC (nslog).
- **Regla.** Las condiciones en las que se almacenan los registros.
- **Acción.** Detalles del servidor de registro y otros detalles para crear las entradas de registro.

Esta directiva de auditoría se puede configurar en diferentes niveles: Nivel de usuario, nivel de grupo, autenticación, autorización y auditoría de servidor virtual y nivel de sistema global. Las directivas configuradas en el nivel de usuario tienen la prioridad más alta.

> **Nota**
>
> En este tema se detallan los pasos para usar syslog. Realice los cambios necesarios para usar nslog.

Para configurar la auditoría de syslog mediante la CLI

1. Configure el servidor de auditoría con la configuración de registro correspondiente.

   ns-cli-prompt> **add audit syslogAction <name> <serverIP> ...**

2. Configure la directiva de auditoría asociando el servidor de auditoría.

   ns-cli-prompt<name> <rule> <action> > **agregar auditoría SysLogPolicy

3. Asocie la directiva de auditoría a una de las siguientes entidades:

   - Enlazar la directiva a un usuario específico.

     ns-cli-prompt> **bind aaa user <userName> -policy <policyname>…

   - Enlazar la directiva a un grupo específico.

     ns-cli-prompt> **bind aaa group <groupName> -policy <policyname>…

   - Enlazar la directiva a un servidor virtual de autenticación, autorización y auditoría.

     ns-cli-prompt> **bind authentication vserver <name> -policy <policyname>…

   - Enlazar la directiva globalmente al dispositivo Citrix ADC.

     ns-cli-prompt> **bind tm global -policyName** <policyname>…

Para configurar la auditoría de syslog mediante la interfaz gráfica de usuario (ficha Configuración)

1. Configure el servidor de auditoría y la directiva.

   Vaya a **Seguridad > AAA: Tráfico de aplicaciones > Directivas > Auditoría > Syslog** y configure el servidor y la directiva en las fichas correspondientes.

2. Asocie la directiva a una de las siguientes opciones:

   - Enlazar la directiva a un usuario específico.

     Vaya a **Seguridad > AAA: Tráfico de aplicaciones > Usuarios** y asocie la directiva de autorización con el usuario correspondiente.

   - Enlazar la directiva a un grupo específico.

     Vaya a **Seguridad > AAA: Tráfico de aplicaciones > Grupos** y asocie la directiva de autorización al grupo correspondiente.

   - Enlazar la directiva a un servidor virtual de autenticación, autorización y auditoría.

     Vaya a **Seguridad > AAA: Tráfico de aplicaciones > Servidores virtuales** y asocie la directiva de autorización con el servidor virtual correspondiente.

- Enlazar la directiva globalmente al dispositivo Citrix ADC.

  Vaya a **Seguridad > AAA: Tráfico de aplicaciones > Directivas > Auditoría > Syslog** o **Nslog**, seleccione la directiva de autorización y haga clic en **Acción > Enlaces globales** para enlazar la directiva globalmente.

Citrix ADC como proxy de Servicios de federación de Active Directory

February 19, 2022

Servicios de federación de Active Directory (ADFS) es un servicio de Microsoft que permite la experiencia de inicio de sesión único (SSO) para clientes autenticados de Active Directory a recursos fuera del centro de datos de la empresa. Una comunidad de servidores ADFS permite a los usuarios internos acceder a servicios externos alojados en la nube. Pero en el momento en que los usuarios externos entran en la mezcla, los usuarios externos deben tener una forma de conectarse de forma remota y acceder a servicios basados en la nube a través de la identidad federada. La mayoría de las empresas no prefieren mantener el servidor ADFS expuesto en la DMZ. Por lo tanto, el proxy ADFS desempeña un papel fundamental en la conectividad de usuarios remotos y el acceso a aplicaciones.

Durante más de una década, el dispositivo Citrix ADC desempeña funciones similares de conectividad de usuarios remotos y acceso a aplicaciones. Citrix ADC Appliance se convierte en la solución preferida que se utiliza como proxy ADFS para admitir una nueva implementación de ADFS para habilitar los siguientes servicios:

- Conectividad segura.
- Autenticación y manejo de identidad federada.

Para obtener más información sobre Citrix ADC como proveedor de identidad SAML, consulte Citrix ADC como proveedor de identidad de SAML.

Ventajas del proxy ADFS

- Reduce el espacio en DMZ para satisfacer las necesidades de la mayoría de las empresas.
- Proporciona una experiencia de inicio de SSO para los usuarios finales.
- Admite métodos enriquecidos para la autenticación previa y permite la autenticación multifactor.
- Soporta clientes activos y pasivos.

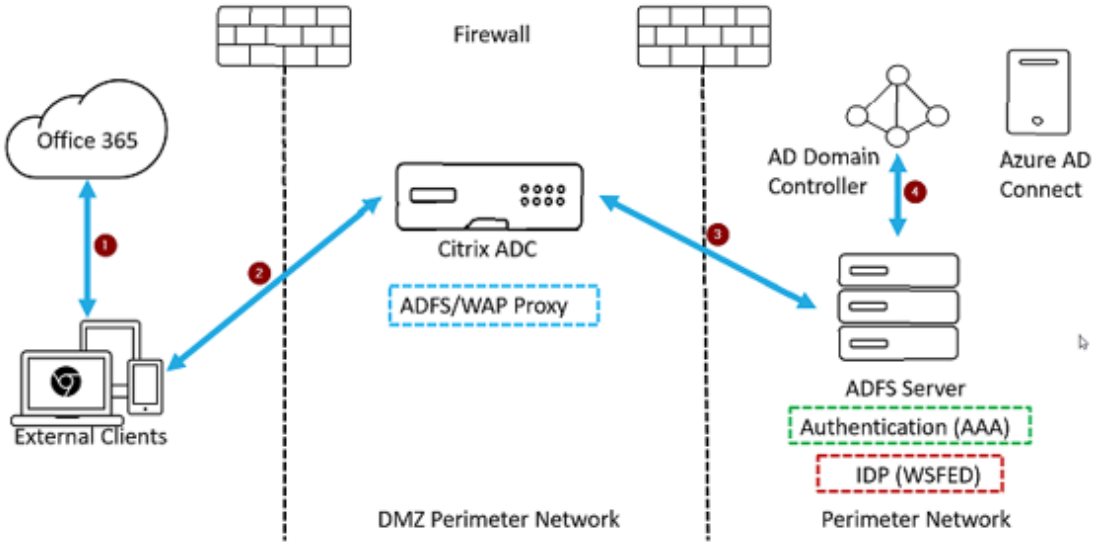
Requisitos previos para usar Citrix ADC como proxy ADFS

Antes de configurar el dispositivo Citrix ADC como proxy ADFS, asegúrese de que se cumplen los siguientes requisitos previos.

- Un dispositivo Citrix ADC con versión 12.1 o posterior.
- Servidor ADFS de dominio.
- Certificado SSL de dominio.
- IP virtual para servidor virtual de conmutación de contenido.
- Habilite las funciones de equilibrio de carga, descarga SSL, conmutación de contenido, reescritura y autenticación, autorización y auditoría de administración de tráfico en el dispositivo Citrix ADC.

Configurar el dispositivo Citrix ADC como proxy ADFS

Para lograr este caso de uso, configure Citrix ADC como proxy ADFS en la zona DMZ. El servidor ADFS se configura junto con el Controller de dominio de AD en el back-end.



1. Una solicitud de cliente para acceder a Microsoft Office365 se redirige a Citrix ADC implementado como proxy ADFS.
2. Las credenciales del usuario se pasan al servidor ADFS.
3. El servidor ADFS autentica las credenciales con AD local del dominio.
4. El servidor ADFS tras la validación de las credenciales con AD, genera un token que se pasa a Microsoft Office365 para el establecimiento de la sesión.

A continuación se describen los pasos de alto nivel que implica configurar el dispositivo Citrix ADC antes de configurarlo como proxy ADFS.

En el símbolo del sistema de Citrix ADC, escriba los siguientes comandos:

1. Cree un perfil SSL para back-end y habilite SNI en el perfil SSL. Inhabilite SSLv3/TLS1.


```
add ssl profile <new SSL profile> -sniEnable ENABLED -ssl3 DISABLED -
tls1 DISABLED -commonName <FQDN of ADFS>
```

2. Inhabilite SSLv3/TLS1 para el servicio.

```
set ssl service <adfs service name> -sslProfile <SSL profile created in
 the above step>
```

3. Habilite la extensión SNI para los apretones de manos del servidor back-end.

   - `set vpn parameter -backendServerSni ENABLED`
   - `set ssl parameter -denySSLReneg NONSECURE`

Configurar el dispositivo Citrix ADC como proxy ADFS mediante la CLI

Las siguientes secciones se clasifican en función del requisito para completar los pasos de configuración.

Para configurar el servicio ADFS

1. Configure el servicio ADFS en Citrix ADC para el servidor ADFS.

```
add service <Domain_ADFS_Service> <ADFS Server IP> SSL 443 -gslb NONE -
maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport YES -sp OFF
-cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO -CMP NO
```

   Ejemplo

   add service CTXTEST_ADFS_Service 1.1.1.1 SSL 443 -gslb NONE -maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport YES -sp OFF -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO -CMP NO

2. Configure FQDN para el servidor virtual de conmutación de contenido y habilite SNI.

```
set ssl service <Domain_ADFS_Service> -SNIEnable ENABLED -commonName <
sts.domain.com>
```

   Ejemplo

   set ssl service CTXTEST_ADFS_Service -SNIEnable ENABLED -commonName sts.ctxtest.com

Para configurar el servidor virtual de equilibrio de carga ADFS

> **Importante**
>
> Se requiere un certificado SSL de dominio (SSL_CERT) para el tráfico seguro.

1. Configurar el servidor virtual de equilibrio de carga ADFS.

   ```
   add lb vserver <Domain_ADFS_LBVS> SSL <IP_address> -persistenceType
   NONE -cltTimeout 180
   ```

   Ejemplo

   ```
   add lb vserver CTXTEST_ADFS_LBVS SSL 192.168.1.0 -persistenceType NONE
   -cltTimeout 180
   ```

2. Enlazar el servidor virtual de equilibrio de carga ADFS al servicio ADFS.

   ```
   bind lb vserver <Domain_ADFS_LBVS> <Domain_ADFS_Service>
   ```

   Ejemplo

   ```
   bind lb vserver CTXTEST_ADFS_LBVS CTXTEST_ADFS_Service
   ```

3. Enlazar un par de certificados de servidor virtual SSL.

   ```
   bind ssl vserver <Domain_ADFS_LBVS> -certkeyName <SSL_CERT>
   ```

   Ejemplo

   ```
   bind ssl vserver CTXTEST_ADFS_LBVS -certkeyName ctxtest_newcert_2019
   ```

Para configurar el servidor virtual de conmutación de contenido para el dominio

> **Nota**
>
> Se requiere una IP virtual libre (por ejemplo, 2.2.2.2) procesada por NAT a IP pública para cambiar el servidor virtual de contenido. Debe ser accesible tanto para tráfico externo como interno.

1. Cree un servidor virtual de conmutación de contenido con VIP gratuito.

   ```
   add cs vserver <Domain_CSVS> SSL <FREE VIP> 443 -cltTimeout 180 -
   persistenceType NONE
   ```

   Ejemplo

   ```
   add cs vserver CTXTEST_CSVS SSL 2.2.2.2 443 -cltTimeout 180 -persistenceType
    NONE
   ```

2. Vincular el servidor virtual de conmutación de contenido al servidor virtual de equilibrio de carga.

   ```
   bind cs vserver <Domain_CSVS> -lbvserver <Domain_ADFS_LBVS>
   ```

   Ejemplo

   - `bind cs vserver CTXTEST_CSVS -lbvserver CTXTEST_ADFS_LBVS`
   - `set ssl vserver CTXTEST_CSVS -sessReuse DISABLED`

3. Enlazar un par de certificados de servidor virtual SSL.

   ```
   bind ssl vserver <Domain_CSVS> -certkeyName <SSL_CERT>
   ```

   Ejemplo

   ```
   bind ssl vserver CTXTEST_CSVS -certkeyName ctxtest_newcert_2019
   ```

Protocolos compatibles

Los protocolos proporcionados por Microsoft desempeñan un papel vital en la integración con el dispositivo Citrix ADC. Citrix ADC como proxy ADFS admite los siguientes protocolos:

- **Federación WS-.** Para obtener más información, consulte Protocolo de federación de servicios web.
- **ADFSPIP**. Para obtener más información, consulte Cumplimiento del protocolo de integración de proxy de Active Directory Federation

> **Nota**
>
> El dispositivo Citrix ADC no admite la autenticación de certificados de dispositivo cuando se implementa como proxy ADFS.

Protocolo de federación de servicios web

May 8, 2022

La federación de servicios web (WS-Federation) es un protocolo de identidad que permite que un servicio de token de seguridad (STS) de un dominio de confianza proporcione información de autenticación a un STS de otro dominio de confianza cuando hay una relación de confianza entre los dos dominios.

Ventajas de WS-Federation

WS-Federation admite clientes activos y pasivos, mientras que el IdP SAML solo admite clientes pasivos.

- Los clientes activos son clientes nativos de Microsoft, como los clientes de Outlook y Office (Word, PowerPoint, Excel y OneNote).
- Los clientes pasivos son clientes basados en explorador, como Google Chrome, Mozilla Firefox e Internet Explorer.

Requisitos previos para usar Citrix ADC como WS-Federation

Antes de configurar el dispositivo Citrix ADC como proxy ADFS, revise lo siguiente:

- Active Directory
- Certificado SSL de dominio.
- El certificado SSL de Citrix ADC y el certificado de firma de token de ADFS en el servidor ADFS deben ser los mismos.

> **Importante**
>
> IdP de SAML ahora es capaz de gestionar el protocolo WS-Federation. Por lo tanto, para configurar el IdP de WS-Federation, debe configurar realmente el IdP de SAML. No ve ninguna interfaz de usuario que mencione explícitamente WS-Federation.

Funciones admitidas por Citrix ADC cuando se configuran como proxy ADFS e IdP de WS-Federation

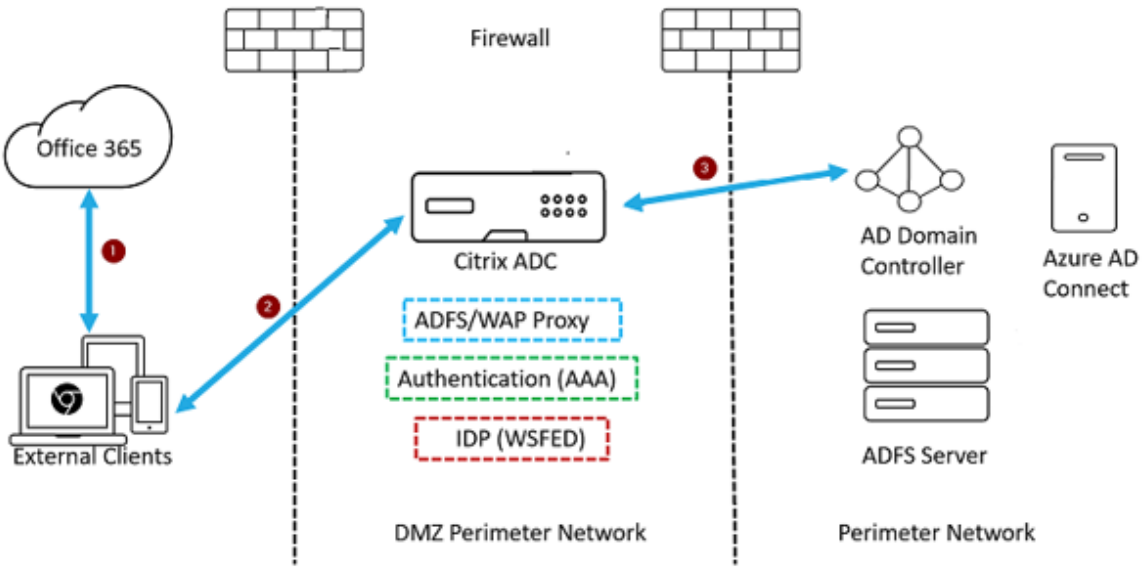
En la siguiente tabla se enumeran las funciones admitidas por el dispositivo Citrix ADC cuando se configura como proxy ADFS e IdP de WS-Federation.

Funciones	Configurar el dispositivo Citrix ADC como proxy ADFS	Citrix ADC como proveedor de identidad de WS-Federation	Citrix ADC como ADFSPIP
Equilibrio de carga	Sí	Sí	Sí
Terminación de SSL	Sí	Sí	Sí
Limitación de tarifas	Sí	Sí	Sí
Consolidación (reduce el espacio del servidor DMZ y ahorra IP pública)	Sí	Sí	Sí
Firewall de aplicaciones web (WAF)	Sí	Sí	Sí
Descarga de autenticación al dispositivo Citrix ADC	Sí	Sí (clientes activos y pasivos)	Sí
Single Sign-On (SSO)	Sí	Sí (clientes activos y pasivos)	Sí

Funciones	Configurar el dispositivo Citrix ADC como proxy ADFS	Citrix ADC como proveedor de identidad de WS-Federation	Citrix ADC como ADFSPIP
Autenticación de varios factores (nFactor)	No	Sí (clientes activos y pasivos)	Sí
Autenticación multifactor Azure	No	Sí (clientes activos y pasivos)	Sí
Se puede evitar la comunidad de servidores ADFS	No	Sí	Sí

Configurar el dispositivo Citrix ADC como proveedor de identidad de WS-Federation

Configure Citrix ADC como IdP de WS-Federation (IdP de SAML) en una zona DMZ. El servidor ADFS se configura junto con el controlador de dominio de AD en el back-end.



1. La solicitud del cliente a Microsoft Office365 se redirige al dispositivo Citrix ADC.
2. El usuario introduce las credenciales para la autenticación multifactor.
3. Citrix ADC valida las credenciales con AD y genera un token de forma nativa en el dispositivo Citrix ADC. Las credenciales se pasan a Office365 para obtener acceso.

> **Nota**
>
> La compatibilidad con el proveedor de identidades de WS-Federation se realiza de forma nativa a través del dispositivo Citrix ADC en comparación con el equilibrador de carga de F5 Networks.

Configurar el dispositivo Citrix ADC como IdP de WS-Federation (IdP de SAML) mediante la CLI

Las siguientes secciones se clasifican según el requisito de completar los pasos de configuración.

Para configurar la autenticación LDAP y agregar una directiva

> **Importante**
>
> Para los usuarios de dominio, para iniciar sesión en el dispositivo Citrix ADC con sus direcciones de correo electrónico corporativas, debe configurar lo siguiente:

- Configure el servidor y la directiva de autenticación LDAP en el dispositivo Citrix ADC.
- Enlácela a la dirección IP virtual de autenticación, autorización y auditoría (también se admite el uso de una configuración LDAP existente).

```
1 add authentication ldapAction <Domain_LDAP_Action> -serverIP <Active
     Directory IP> -serverPort 636 -ldapBase "cn=Users,dc=domain,dc=com"
     -ldapBindDn "cn=administrator,cn=Users,dc=domain,dc=com" -
     ldapBindDnPassword <administrator password> -encrypted -
     encryptmethod ENCMTHD_3 -ldapLoginName sAMAccountName -groupAttrName
      memberOf -subAttributeName cn -secType SSL -ssoNameAttribute
     UserPrincipalName -followReferrals ON -Attribute1 mail -Attribute2
     objectGUID
2
3 add authentication Policy <Domain_LDAP_Policy> -rule true -action <
     Domain_LDAP_Action>
4 <!--NeedCopy-->
```

Ejemplo

```
1 add authentication ldapAction CTXTEST_LDAP_Action -serverIP 3.3.3.3 -
     serverPort 636 -ldapBase "cn=Users,dc=ctxtest,dc=com" -ldapBindDn "
     cn=administrator,cn=Users,dc=ctxtest,dc=com" -ldapBindDnPassword
     xxxxxxxxxxx -encrypted -encryptmethod ENCMTHD_3 -ldapLoginName
     sAMAccountName -groupAttrName memberOf -subAttributeName cn -secType
```



```
    SSL -ssoNameAttribute UserPrincipalName -followReferrals ON -
    Attribute1 mail -Attribute2 objectGUID
2
3 add authentication Policy CTXTEST_LDAP_Policy -rule true -action
    CTXTEST_LDAP_Action
4 <!--NeedCopy-->
```

Para configurar Citrix ADC como IdP de WS-Federation o IdP de SAML

Crear una acción y una directiva de IdP de WS-Federation (IdP SAML) para la generación de tokens. Más adelante, vincúlela al servidor virtual de autenticación, autorización y auditoría.

```
1 add authentication samlIdPProfile <Domain_SAMLIDP_Profile> -
    samlIdPCertName <SSL_CERT> -assertionConsumerServiceURL "https://
    login.microsoftonline.com/login.srf" -samlIssuerName <Issuer Name
    for Office 365 in ADFS Server> -rejectUnsignedRequests OFF -audience
     urn:federation:MicrosoftOnline -NameIDFormat persistent -NameIDExpr
     "HTTP.REQ.USER.ATTRIBUTE(2).B64ENCODE" -Attribute1 IDPEmail -
    Attribute1Expr "HTTP.REQ.USER.ATTRIBUTE(1)"
2
3 add authentication samlIdPPolicy <Domain_SAMLIDP_Policy> -rule "HTTP.
    REQ.HEADER("referer").CONTAINS("microsoft") || true" -action <
    Domain_SAMLIDP_Profile>
4 <!--NeedCopy-->
```

Ejemplo

```
1 add authentication samlIdPProfile CTXTEST_SAMLIDP_Profile -
    samlIdPCertName ctxtest_newcert_2019 -assertionConsumerServiceURL "
    https://login.microsoftonline.com/login.srf" -samlIssuerName "http
    ://ctxtest.com/adfs/services/trust/" -rejectUnsignedRequests OFF -
    audience urn:federation:MicrosoftOnline -NameIDFormat persistent -
    NameIDExpr "HTTP.REQ.USER.ATTRIBUTE(2).B64ENCODE" -Attribute1
    IDPEmail -Attribute1Expr "HTTP.REQ.USER.ATTRIBUTE(1)"
2
3 add authentication samlIdPPolicy CTXTEST_SAMLIDP_Policy -rule "HTTP.REQ
    .HEADER("referer").CONTAINS("microsoft") || true" -action
    CTXTEST_SAMLIDP_Profile
4 <!--NeedCopy-->
```


Para configurar un servidor virtual de autenticación, autorización y auditoría para autenticar a los empleados que inician sesión en Office365 con credenciales corporativas

```
add authentication vserver <Domain_AAA_VS> SSL <IP_address>`
<!--NeedCopy-->
```

Ejemplo

```
add authentication vserver CTXTEST_AAA_VS SSL 192.168.1.0

bind authentication vserver CTXTEST_AAA_VS -portaltheme RfWebUI
<!--NeedCopy-->
```

Para vincular el servidor virtual de autenticación y la directiva

```
bind authentication vserver <Domain_AAA_VS> -policy <
    Domain_SAMLIDP_Policy> -priority 100 -gotoPriorityExpression NEXT

bind authentication vserver <Domain_AAA_VS> -policy <Domain_LDAP_Policy
    > -priority 100 -gotoPriorityExpression NEXT
<!--NeedCopy-->
```

Ejemplo

```
bind authentication vserver CTXTEST_AAA_VS -policy
    CTXTEST_SAMLIDP_Policy -priority 100 -gotoPriorityExpression NEXT

bind authentication vserver CTXTEST_AAA_VS -policy CTXTEST_LDAP_Policy
    -priority 100 -gotoPriorityExpression NEXT

bind ssl vserver CTXTEST_AAA_VS -certkeyName ctxtest_newcert_2019
<!--NeedCopy-->
```

Para configurar el cambio de contenido

```
add cs action <Domain_CS_Action> -targetVserver <Domain_AAA_VS>

```



```
add cs policy <Domain_CS_Policy> -rule "is_vpn_url || http.req.url.
    contains("/adfs/ls") || http.req.url.contains("/adfs/services/trust"
    ) || -action <Domain_CS_Action>
<!--NeedCopy-->
```

Ejemplo

```
add cs action CTXTEST_CS_Action -targetVserver CTXTEST_AAA_VS

add cs policy CTXTEST_CS_Policy -rule "is_vpn_url || http.req.url.
    contains("/adfs/ls") || http.req.url.contains("/adfs/services/trust"
    ) || -action CTXTEST_CS_Action
<!--NeedCopy-->
```

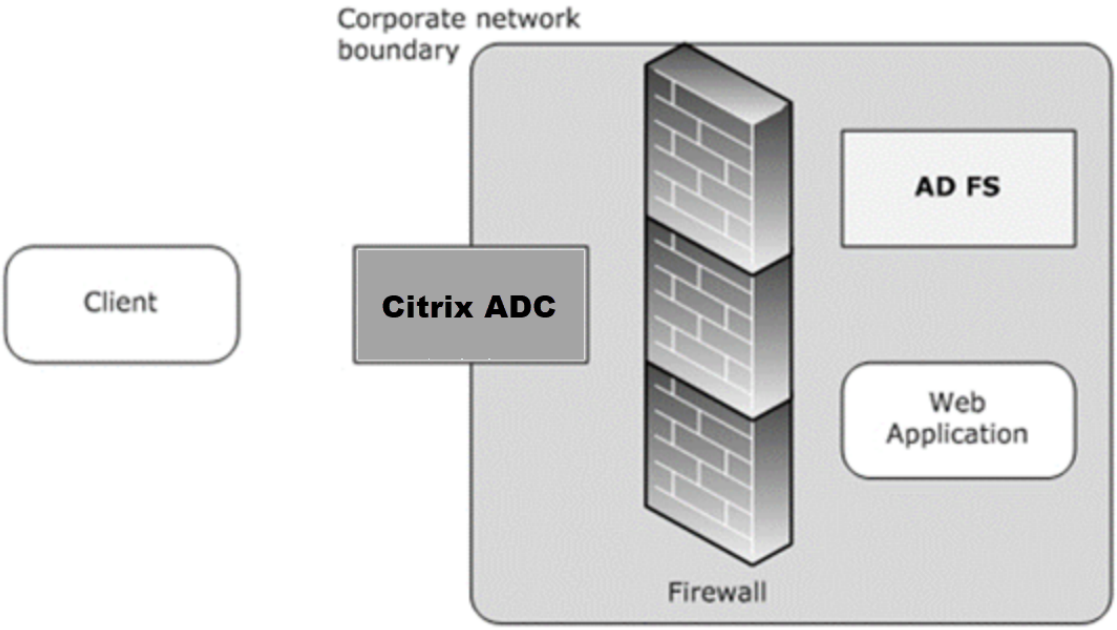
Para enlazar el servidor virtual de conmutación de contenido a la directiva

```
bind cs vserver CTXTEST_CSVS -policyName CTXTEST_CS_Policy -priority
    100
<!--NeedCopy-->
```

Cumplimiento Active Directory protocolo de integración de proxy de servicio de federación

June 22, 2022

Si se van a utilizar proxies de terceros en lugar del proxy de aplicación web, deben admitir el protocolo MS-ADFSPIP, que especifica las reglas de integración de ADFS y WAP. ADFSPIP integra los Servicios de federación de Active Directory con un proxy de autenticación y aplicación para permitir el acceso a los servicios ubicados dentro de los límites de la red corporativa para los clientes que se encuentran fuera de ese límite.



Requisitos previos

Para establecer correctamente la confianza entre el servidor proxy y la comunidad de ADFS, revise la siguiente configuración en el dispositivo Citrix ADC:

- Cree un perfil SSL para el back-end y habilite el SNI en el perfil SSL. Inhabilite SSLv3/TLS1. En el símbolo del sistema, escriba el siguiente comando:

```
1  add ssl profile <new SSL profile> -sniEnable ENABLED -ssl3
      DISABLED -tls1 DISABLED -commonName <FQDN of ADFS>
2  <!--NeedCopy-->
```

- Inhabilite SSLv3/TLS1 para el servicio. En el símbolo del sistema, escriba el siguiente comando:

```
1  set ssl service <adfs service name> -sslProfile
      ns_default_ssl_profile_backend
2  <!--NeedCopy-->
```

- Habilite la extensión SNI para los apretones de manos del servidor back-end. En el símbolo del sistema, escriba el siguiente comando:


```
set vpn parameter  - backendServerSni ENABLED

set ssl parameter -denySSLReneg NONSECURE
<!--NeedCopy-->
```

> **Importante**
>
> Para casos de Home Realm Discovery (HRD) en los que la autenticación debe descargarse en el servidor de ADFS, Citrix recomienda inhabilitar tanto la autenticación como el SSO en el dispositivo Citrix ADC.

Mecanismo de autenticación

A continuación se muestra el flujo de eventos de alto nivel para la autenticación.

1. **Establecer confianza con el servidor de ADFS**: El servidor de Citrix ADC establece confianza con el servidor de ADFS al registrar un certificado de cliente. Una vez que se establece la confianza, el dispositivo Citrix ADC restablece la confianza después del reinicio sin la intervención del usuario.

   Al expirar el certificado, debe restablecer la confianza eliminando y agregando el perfil de proxy ADFS de nuevo.

2. **Dispositivos de punto final publicados**: El dispositivo Citrix ADC obtiene automáticamente la lista de dispositivos de punto final publicados en el establecimiento de confianza posterior al servidor de ADFS. Estos dispositivos de punto final publicados filtran las solicitudes reenviadas al servidor de ADFS.

3. **Insertar encabezados en las solicitudes de los clientes**: Cuando el dispositivo Citrix ADC tuneliza las solicitudes de los clientes, los encabezados HTTP relacionados con ADFSPIP se agregan al paquete mientras se envían al servidor de ADFS. Puede implementar el control de acceso en el servidor de ADFS en función de estos valores de encabezado. Se admiten los siguientes encabezados.

   - X-MS-Proxy
   - X-MS-Endpoint-Absolute-Path
   - X-MS-Forwarded-Client-IP
   - X-MS-Proxy
   - X-MS-Target-Role
   - X-MS-ADFS-Proxy-Client-IP

4. **Administrar el tráfico de los usuarios finales**: El tráfico de los usuarios finales se redirige de forma segura a los recursos deseados.

> **Nota**
>
> El dispositivo Citrix ADC utiliza la autenticación basada en formularios.

Configurar Citrix ADC para que admita el servidor de ADFS

Requisitos previos

- Configure el servidor Context Switching (CS) como front-end con un servidor de autenticación, autorización y auditoría detrás de CS. En el símbolo del sistema, escriba:

```
add cs vserver <cs vserver name> SSL 10.220.xxx.xx 443
-cltTimeout 180 -AuthenticationHost <adfs server hostname> -
   Authentication OFF -persistenceType NONE
<!--NeedCopy-->
```

```
add cs action <action name1> -targetLBVserver <lb vserver name>
<!--NeedCopy-->
```

```
add cs action <action name2> -targetLBVserver <lb vserver name>
<!--NeedCopy-->
```

```
add cs policy <policy name1> -rule " http.req.url.contains("/adfs
   /services/trust") || http.req.url.contains("federationmetadata
   /2007-06/federationmetadata.xml")" -action <action name1>
<!--NeedCopy-->
```

```
add cs policy <policy name2> -rule "HTTP.REQ.URL.CONTAINS("/adfs/
   ls")" -action <action name2>
<!--NeedCopy-->
```

```
bind cs vserver <cs vserver name> -policyName <policy name1> -
   priority 100
<!--NeedCopy-->
```



```
bind cs vserver <cs vserver name> -policyName <policy name2> -
   priority 110
<!--NeedCopy-->
```

```
bind cs vserver <cs vserver name> -lbvserver <lb vserver name>
<!--NeedCopy-->
```

- Agregue un servicio ADFS. En el símbolo del sistema, escriba:

```
add service <adfs service name> <adfs server ip> SSL 443
<!--NeedCopy-->
```

```
set ssl service <adfs service name> -sslProfile
   ns_default_ssl_profile_backend
<!--NeedCopy-->
```

- Agregue un servidor virtual con equilibrio de carga. En el símbolo del sistema, escriba:

```
add lb vserver <lb vserver name> SSL 0.0.0.0 0
<!--NeedCopy-->
```

```
set ssl vserver <lb vserver name> -sslProfile
   ns_default_ssl_profile_frontend
<!--NeedCopy-->
```

- Enlaza el servicio al servidor con equilibrio de carga. En el símbolo del sistema, escriba:

```
bind lb vserver <lb vserver name> <adfs service name>
<!--NeedCopy-->
```

Para configurar Citrix ADC para que funcione con el servidor de ADFS, debe hacer lo siguiente:

1. Crear una clave de perfil SSL CertKey para usarla con el perfil de proxy ADFS

2. Crear un perfil de proxy ADFS
3. Asocie el perfil de proxy ADFS al servidor virtual LB

Cree un certificado SSL con clave privada para usarlo con el perfil de proxy ADFS

En el símbolo del sistema, escriba:

```
1     add ssl certkey <certkeyname>  - cert <certificate path> -key <
         keypath>
2  <!--NeedCopy-->
```

Nota: El archivo de certificado y el archivo de clave deben estar presentes en el dispositivo Citrix ADC. Crear un perfil de proxy ADFS mediante la CLI

En el símbolo del sistema, escriba:

```
1  add authentication adfsProxyProfile  <profile name> -serverUrl <https:
      //<server FQDN or IP address>/> -username <adfs admin user name> -
      password <password for admin user> -certKeyName <name of the CertKey
       profile created above>
2  <!--NeedCopy-->
```

Donde:

Nombre del perfil: nombre del perfil de proxy de AFDS que se va a crear

ServerUrl: nombre de dominio completo del servicio ADFS, incluidos el protocolo y el puerto. Por ejemplo: `https://adfs.citrix.com`

`Username` — Nombre de usuario de una cuenta de administrador que existe en el servidor de ADFS

Contraseña: contraseña de la cuenta de administrador utilizada como nombre de usuario

certKeyName: nombre del perfil SSL CertKey creado anteriormente

Asociar el perfil de proxy ADFS al servidor virtual de equilibrio de carga mediante la CLI

En la implementación de ADFS, se utilizan dos servidores virtuales de equilibrio de carga, uno para el tráfico del cliente y el otro para el intercambio de metadatos. El perfil proxy de ADFS debe estar asociado con el servidor virtual de equilibrio de carga que es el front-end del servidor de ADFS.

En el símbolo del sistema, escriba:


```
set lb vserver <adfs-proxy-lb> -adfsProxyProfile <name of the ADFS
   proxy profile>
<!--NeedCopy-->
```

Función de renovación de confianza para ADFSPIP

Puede renovar la confianza de los certificados existentes que están a punto de caducar o si el certificado existente no es válido. La renovación de confianza de los certificados se realiza solo cuando se establece la confianza entre el dispositivo Citrix ADC y el servidor de ADFS. Para renovar la confianza del certificado, debe proporcionar el nuevo certificado.

> **Importante**
>
> Se requiere intervención manual para la renovación de la confianza de los nuevos certificados.

En el siguiente ejemplo se enumeran los pasos involucrados en la renovación de la confianza del certificado:

1. El dispositivo Citrix ADC envía certificados antiguos (SerializedTrustCertificate) y nuevos (SerializedReplacementCertificate) en la solicitud POST al servidor de ADFS para la renovación de la confianza.
2. El servidor de ADFS responde con un éxito de 200 OK si la confianza se renueva correctamente.
3. El dispositivo Citrix ADC actualiza el estado como “ESTABLISHED_RENEW_SUCCESS” si la renovación de la confianza se realiza correctamente. Si se produce un error en la renovación de la confianza, el estado se actualiza como “ESTABLISHED_RENEW_FAILED” y el dispositivo Citrix ADC sigue utilizando el certificado anterior.

> **Nota**
>
> No puede actualizar la clave de certificado si ya está enlazada a algún perfil de proxy de ADFS.

Para configurar la renovación de confianza de certificados mediante la CLI

En el símbolo del sistema, escriba:

```
set authentication adfsProxyProfile <name> [-CertKeyName <string>]
<!--NeedCopy-->
```

Ejemplo:


```
1 set authentication adfsProxyProfile adfs_2 -CertKeyName ca_cert1
2 <!--NeedCopy-->
```

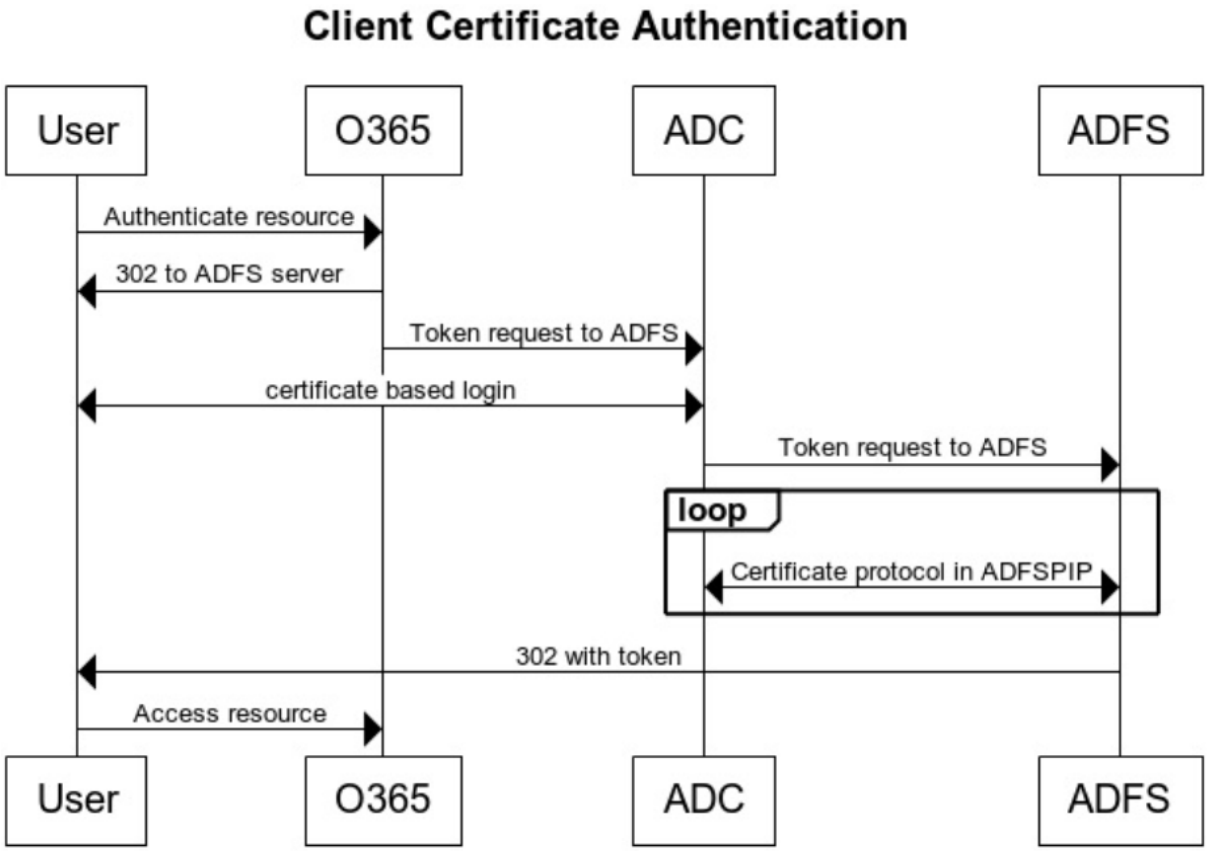
Autenticación basada en certificados de cliente en el servidor de ADFS

A partir de Windows server 2016, Microsoft introdujo una nueva forma de autenticar a los usuarios cuando se accede a ADFS a través de servidores proxy. Ahora, los usuarios finales pueden iniciar sesión con sus certificados, evitando así el uso de una contraseña.

Los usuarios finales a menudo acceden a ADFS a través de un proxy, especialmente cuando no están en las instalaciones. Por lo tanto, los servidores proxy ADFS deben admitir la autenticación de certificados de cliente a través del protocolo ADFSPIP.

Cuando ADFS se equilibra de carga mediante un dispositivo Citrix ADC, para admitir la autenticación basada en certificados en el servidor de ADFS, los usuarios también deben iniciar sesión en el dispositivo Citrix ADC con el certificado. Esto permite que Citrix ADC pase el certificado de usuario a ADFS para proporcionar SSO al servidor de ADFS.

El siguiente diagrama describe el flujo de autenticación de certificados de cliente.



Configurar el SSO para el servidor de ADFS mediante el certificado de cliente

Para configurar el SSO para el servidor de ADFS mediante el certificado de cliente, primero debe configurar la autenticación del certificado de cliente en el dispositivo Citrix ADC. A continuación, debe vincular la directiva de autenticación de certificados al servidor virtual de autenticación, autorización y auditoría.

Además, debe realizar los siguientes pasos.

- Se debe configurar un servidor virtual de conmutación de contexto adicional con el puerto 49443 y este servidor virtual de conmutación de contexto debe apuntar al mismo servidor virtual de equilibrio de carga que está abierto para todos los puertos, que creó anteriormente.
- El puerto 49443 debe abrirse en el dispositivo Citrix ADC para la autenticación.
- La directiva de conmutación de contexto debe vincularse al mismo servidor virtual de equilibrio de carga con el puerto 443 abierto que creó anteriormente.
- Debe vincular el mismo servicio SSL que creó anteriormente al servidor virtual de equilibrio de carga.
- Si ya ha creado un perfil SSL para el back-end, debe usar ese perfil.

En el símbolo del sistema, escriba;

```
1  add cs vserver <name> <serviceType> <port>
2
3  bind cs vserver <name> (-lbvserver <string> | -vServer <string> | [-
       targetLBVserver <string>]
4
5  set ssl vserver <vServerName [-sslProfile <string>]
6
7  bind ssl vserver <vServerName -certkeyName <string>
8
9  add authentication certAction <action name>
10
11 add authentication Policy <policy name> -rule <expression> -action <
       action name>
12
13 add authentication policylable <label Name>
14
15 bind authentication policylabel <label Name> -policyName <name of the
       policy> -priority<integer>
16
17 <!--NeedCopy-->
```


Ejemplo:

```
add cs vserver srv123_adfsproxy_csvs_tls SSL $VIP_1 49443

bind cs vserver srv123_adfsproxy_csvs_tls -lbvserver
   srv123_adfs_lbvserver

set ssl vserver srv123_adfsproxy_csvs_tls -sslProfile
   ns_default_ssl_profile_frontend

bind ssl vserver srv123_adfsproxy_csvs_tls -certkeyName
   srv123_wildcardcert

add authentication certAction adfsproxy-cert

add authentication Policy cert1 -rule TRUE -action adfsproxy-cert

add authentication policylable certfactor

bind authentication policylabel certfactor  - policyName cert1  -
   priority 100

<!--NeedCopy-->
```

Para obtener información sobre la configuración del certificado de cliente en el dispositivo Citrix ADC, consulte Configurar la autenticación de certificados de cliente mediante directivas avanzadas.

Usar un dispositivo Citrix Gateway local como el proveedor de identidades para Citrix Cloud

January 21, 2022

Citrix Cloud admite el uso de dispositivos Citrix Gateway locales como proveedores de identidades para autenticar a los suscriptores que inician sesión en sus espacios de trabajo.

Con la autenticación de Citrix Gateway, puede:

- Siga autenticando a los usuarios a través de su dispositivo Citrix Gateway existente para que puedan acceder a los recursos de la implementación local de Virtual Apps and Desktops a través de Citrix Workspace.

- Use las funciones de autenticación, autorización y auditoría de Citrix Gateway con Citrix Workspace.
- Proporcione a sus usuarios acceso a los recursos que necesitan a través de Citrix Workspace mediante funciones como la autenticación de paso, tarjetas inteligentes, tokens seguros, directivas de acceso condicional y federación.

La autenticación de Citrix Gateway se puede utilizar con las siguientes versiones de producto:

- Citrix Gateway 13.0 41.20 Advanced Edition o posterior
- Citrix Gateway 12.1 54.13 Advanced Edition o posterior

Requisitos previos

- Cloud Connectors: necesita al menos dos servidores en los que instalar el software Citrix Cloud Connector.
- Active Directory: Realice las comprobaciones necesarias.
- Requisitos de Citrix Gateway
  - Utilice directivas avanzadas en la puerta de enlace local debido a la obsolescencia de las directivas clásicas.
  - Al configurar la puerta de enlace para autenticar suscriptores en Citrix Workspace, la puerta de enlace actúa como un proveedor de OpenID Connect. Los mensajes entre Citrix Cloud y Gateway se ajustan al protocolo OIDC, que implica la firma digital de tokens. Por lo tanto, debe configurar un certificado para firmar estos tokens.
  - Sincronización de reloj: la puerta de enlace debe estar sincronizada con la hora NTP.

Para obtener más información, consulte Prerequisites.

Crear una directiva de IdP de OAuth en Citrix Gateway local

> **Importante:**
>
> Debe haber generado el ID de cliente, el secreto y la URL de redireccionamiento en la ficha **Citrix Cloud > Administración de acceso e identidad > Autenticación**. Para obtener más información, consulte Conectar un Citrix Gateway local a Citrix Cloud.

La creación de una directiva de autenticación de IdP de OAuth implica las siguientes tareas:

1. Crea un perfil de IdP de OAuth.
2. Agrega una directiva de IdP de OAuth.
3. Enlazar la directiva de IdP de OAuth a un servidor virtual de autenticación.
4. Enlazar el certificado globalmente.

Creación de un perfil de IdP de OAuth mediante la CLI

En el símbolo del sistema, escriba;

```
add authentication OAuthIDPProfile <name> [-clientID <string>][-
    clientSecret ][-redirectURL <URL>][-issuer <string>][-audience <
    string>][-skewTime <mins>] [-defaultAuthenticationGroup <string>]

add authentication OAuthIdPPolicy <name> -rule <expression> [-action <
    string> [-undefAction <string>] [-comment <string>][-logAction <
    string>]

add authentication ldapAction <name> -serverIP <IP> -ldapBase "dc=aaa,
    dc=local"

ldapBindDn <administrator@aaa.local> -ldapBindDnPassword <password> -
    ldapLoginName sAMAccountName

add authentication policy <name> -rule <expression> -action <string>

bind authentication vserver auth_vs -policy <ldap_policy_name> -
    priority <integer> -gotoPriorityExpression NEXT

bind authentication vserver auth_vs -policy <OAuthIDPPolicyName> -
    priority <integer> -gotoPriorityExpression END

bind vpn global  - certkey <>
<!--NeedCopy-->
```

Creación de un perfil de IdP de OAuth mediante la interfaz gráfica de usuario

1. Vaya a **Seguridad > AAA — Tráfico de aplicaciones > Directivas > Autenticación > Directivas avanzadas > IdP de OAuth**.

   ! [Oauth-IDP-navigation] (/en-us/citrix-adc/media/oauth-navigation-to-idp.png)

2. En la página **IdP de OAuth**, seleccione la ficha **Perfiles** y haga clic en **Agregar**.
3. Configure el perfil de IdP de OAuth.

   > **Nota:**
   >
   > - Copie y pegue los valores de ID de cliente, secreto y URL de redireccionamiento desde la ficha **Citrix Cloud > Administración de acceso e identidad > Autenticación** para

> establecer la conexión con Citrix Cloud.
>
> - Introduzca la URL de la puerta de enlace correctamente en el Ejemplo de **nombre del emisor**: https://GatewayFQDN.com
> - También copie y pegue el ID de cliente en el campo **Audiencia**.
> - **Enviar contraseña**: habilite esta opción para admitir el inicio de sesión único. De forma predeterminada, esta opción está inhabilitada.

4. En la pantalla **Crear perfil de proveedor de identidad de OAuth de autenticación**, defina los valores para los siguientes parámetros y haga clic en **Crear**.

   - **Nombre**: Nombre del perfil de autenticación. Debe empezar por una letra, un número o un guion bajo (_). El nombre debe contener solo letras, números y los caracteres de guion (-), punto (.), almohadilla (#), espacio ( ), arroba (@), igual (=), dos puntos (:) y guiones bajos. No se puede cambiar una vez creado el perfil.
   - **ID de cliente**: Cadena única que identifica al SP. El servidor de autorización defiere la configuración del cliente mediante este ID. Longitud máxima: 127.
   - **Secreto de cliente**: Cadena secreta establecida por el usuario y el servidor de autorización. Longitud máxima: 239.
   - **URL de redirección**: Punto final del SP en el que se debe publicar el código/token.
   - **Nombre del emisor**: Identidad del servidor cuyos tokens se van a aceptar. Longitud máxima: 127. Ejemplo:https://GatewayFQDN.com
   - **Destinatario**: Se dirige al destinatario del token enviado por el IdP. El destinatario comprueba este token.
   - **Tiempo sesgado**: Esta opción especifica el sesgo de reloj permitido (en minutos) que Citrix ADC permite en un token entrante. Por ejemplo, si SkewTime es 10, el token sería válido desde (tiempo actual - 10) min a (tiempo actual+ 10) min, es decir, 20 min en total. Valor por defecto: 5.
   - **Grupo de autenticación predeterminado**: Un grupo que se agrega a la lista de grupos internos de la sesión cuando el IdP elige este perfil y que se puede usar en el flujo nFactor. Se puede usar en la expresión (AAA.USER.IS_MEMBER_OF (“xxx”)) para que las directivas de autenticación identifiquen el flujo de nFactor relacionado con la parte de confianza. Longitud máxima: 63

   Se agrega un grupo a la sesión para este perfil para simplificar la evaluación de directivas y ayudar a personalizar las directivas. Este grupo es el grupo predeterminado que se elige cuando la autenticación se realiza correctamente, además de los grupos extraídos. Longitud máxima: 63.

   ! [Oauth-IDP-profile-parameters] (/en-us/citrix-adc/media/oauth-idp-profile.png)

5. Haga clic en **Directivas** y en **Agregar.**
6. En la pantalla **Crear directiva de IDP de OAuth de autenticación**, defina los valores para los siguientes parámetros y haga clic en **Crear**.
   - **Nombre**: Nombre de la directiva de autenticación.
   - **Acción**: Nombre del perfil creado anteriormente.
   - **Acción de registro**: Nombre de la acción de registro de mensajes que se utilizará cuando una solicitud coincida con esta directiva. No es un archivo obligatorio.
   - Acción de**resultado indefinido: acción** a realizar si el resultado de la evaluación de directivas no está definido (UNDEF). No es un campo obligatorio.
   - **Expresión**: Expresión sintáctica predeterminada que la directiva utiliza para responder a una solicitud específica. Por ejemplo, es cierto.
   - **Comentarios**: Cualquier comentario sobre la directiva.

   ! [Oauth-IDP-policy] (/en-us/citrix-adc/media/oauth-idp-policy.png)

> **Nota:**
>
> Cuando **SendPassword** se establece en ON (OFF de forma predeterminada), las credenciales de usuario se cifran y pasan a través de un canal seguro a Citrix Cloud. Pasar las credenciales de usuario a través de un canal seguro le permite habilitar el SSO en Citrix Virtual Apps and Desktops al iniciarse.

Enlace de la directiva OAuthIDP y la directiva LDAP al servidor virtual de autenticación

1. Vaya a **Configuración > Seguridad > Tráfico de aplicaciones AAA > Directivas > Autenticación > Directivas avanzadas > Acciones > LDAP**.
2. En la pantalla **Acciones de LDAP**, haga clic en **Agregar**.
3. En la pantalla **Crear servidor LDAP de autenticación**, defina los valores de los siguientes parámetros y haga clic en **Crear**.
   - **Nombre:** nombre de la acción LDAP
   - **ServerName/ServerIP:** proporciona FQDN o IP del servidor LDAP
   - Elija los valores adecuados **para Tipo de seguridad, Puerto, Tipo de servidor, Tiempo de espera**
   - Asegúrese de que **la autenticación** esté marcada
   - **DN base:** Base desde la que se inicia la búsqueda LDAP. Por ejemplo, `dc=aaa,dc=local`.
   - **DN de enlace de administrador:** nombre de usuario del enlace al servidor LDAP. Por ejemplo, admin@aaa.local.
   - **Contraseña de administrador/Confirmar contraseña: Contraseña para enlazar LDAP**
   - Haga clic en **Probar conexión** para probar su configuración.
   - **Atributo de nombre de inicio de sesión del servidor:** elija **“sAMAccountName”**

- Otros campos no son obligatorios y, por lo tanto, se pueden configurar según sea necesario.

4. Vaya a **Configuración > Seguridad > Tráfico de aplicaciones AAA > Directivas > Autenticación > Directivas avanzadas > Directiva.**
5. En la pantalla **Directivas de autenticación**, haga clic en **Agregar**.
6. En la página **Crear directiva de autenticación**, defina los valores de los siguientes parámetros y haga clic en **Crear.**
   - **Nombre:** nombre de la directiva de autenticación LDAP.
   - **Tipo de acción:** seleccione **LDAP.**
   - **Acción:** seleccione la acción LDAP.
   - **Expresión: expresión** de sintaxis predeterminada que utiliza la directiva para responder a una solicitud específica. Por ejemplo, cierto**.

Compatibilidad con implementaciones de GSLB activo-activas en Citrix Gateway

January 21, 2022

Citrix Gateway configurado como proveedor de identidad (IdP) mediante el protocolo OIDC puede admitir implementaciones de GSLB activo-activas.

Para obtener más información sobre la configuración de una configuración de GSLB, consulte Ejemplo de una configuración y configuración de GSLB.

> **Importante:**
>
> Citrix Cloud no admite GSLB activo-activo con Citrix Gateway como proveedor de identidades de OAuth.

Compatibilidad activa-activa de GSLB para la autenticación multifactor mediante proxy de conexión

A partir de la versión 13.1 build 12.x de Citrix ADC, se agrega compatibilidad para la implementación activa-activa de GSLB para la autenticación multifactor mediante el proxy de conexión. Esta compatibilidad se aplica a los casos de autenticación, autorización y auditoría de Citrix Gateway y Citrix ADC. El proxy de conexión se utiliza para enrutar solicitudes a los sitios GSLB correctos una vez que la autenticación se realiza correctamente. Para obtener información sobre la persistencia del proxy de conexión, consulte Proxy de conexión.

Funcionamiento

La cookie de persistencia del sitio GSLB se inserta en la respuesta de autenticación. Con esta cookie, Citrix ADC o el dispositivo Citrix Gateway identifican si la solicitud es para un sitio local o un sitio remoto. Las solicitudes se enrutan en consecuencia.

> **Importante:**
>
> - Solo se admite la implementación de tipo activo-activo GSLB.
> - No se admite la topología principal-secundario.
> - El tipo de persistencia en la implementación de GSLB debe configurarse como "ConnectionProxy".

Compatibilidad de configuración para el atributo de cookie SameSite

May 8, 2022

El atributo SameSite indica al explorador si la cookie se puede utilizar para el contexto entre sitios o solo para el contexto del mismo sitio. Además, si se pretende acceder a una aplicación en un contexto entre sitios, solo puede hacerlo a través de la conexión HTTPS. Para obtener más información, consulte RFC6265.

Hasta febrero de 2020, el atributo SameSite no estaba establecido explícitamente en Citrix ADC. El explorador tomó el valor predeterminado (Ninguno). No establecer el atributo SameSite no afectó a las implementaciones de autenticación, autorización y auditoría de Citrix Gateway.

Con la actualización de ciertos exploradores, como Google Chrome 80, se produce un cambio en el comportamiento predeterminado entre dominios de las cookies. El atributo SameSite se puede establecer en uno de los siguientes valores. El valor predeterminado para Google Chrome se establece en Lax. Para determinadas versiones de otros exploradores, es posible que el valor predeterminado del atributo SameSite siga estando establecido en Ninguno.

- **Ninguno**: indica que el explorador utilizará una cookie en el contexto entre sitios solo en conexiones seguras.
- **Lax**: Indica al explorador que utilizará una cookie para solicitudes en el mismo dominio y para sitios cruzados. Para sitios cruzados, solo los métodos HTTP seguros, como la solicitud GET, pueden usar la cookie. Por ejemplo, una solicitud GET de un subdominio abc.example.com puede leer la cookie de otro subdominio xyz.example.com mediante GET.
  Para sitios cruzados, solo se utilizan métodos HTTP seguros porque los métodos HTTP seguros no alteran el estado del servidor. Para obtener más información, consulte https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie/SameSite#lax
- **Estricto**: utiliza la cookie solo en el mismo contexto del sitio.

Si no hay ningún atributo SameSite en la cookie, Google Chrome asume la funcionalidad de SameSite = Lax.
Como resultado, para las implementaciones dentro de un iframe con contexto entre sitios que requieren que el explorador inserte cookies, Google Chrome no comparte cookies entre sitios. Como resultado, es posible que el iframe del sitio web no se cargue.

Configurar el atributo de cookie SameSite

Se agrega un nuevo atributo de cookie llamado SameSite a la VPN y a los servidores virtuales de autenticación, autorización y auditoría. Este atributo se puede establecer a nivel global y a nivel de servidor virtual.

Para configurar el atributo SameSite, debe hacer lo siguiente:

1. Establecer el atributo SameSite para el servidor virtual
2. Enlazar cookies al conjunto de parches (si el explorador deja caer cookies entre sitios)

Configuración del atributo SameSite mediante la CLI

Para establecer el atributo SameSite en el nivel del servidor virtual, utilice los siguientes comandos.

```
set vpn vserver VP1 -SameSite [STRICT | LAX | None]
set authentication vserver AV1 -SameSite [STRICT | LAX | None]
<!--NeedCopy-->
```

Para establecer el atributo SameSite a nivel global, utilice los siguientes comandos.

```
set aaa parameter -SameSite [STRICT | LAX | None]
set vpn parameter -SameSite [STRICT | LAX | None]
<!--NeedCopy-->
```

Nota: La configuración del nivel del servidor virtual tiene preferencia sobre la configuración de nivel global. Citrix recomienda configurar el atributo de cookie SameSite en el nivel del servidor virtual.

Enlazar cookies al patset mediante la CLI

Si el explorador descarta las cookies entre sitios, puede vincular esa cadena de cookie al conjunto de parches NS_Cookies_SameSite existente para que se agregue el atributo SameSite a la cookie.

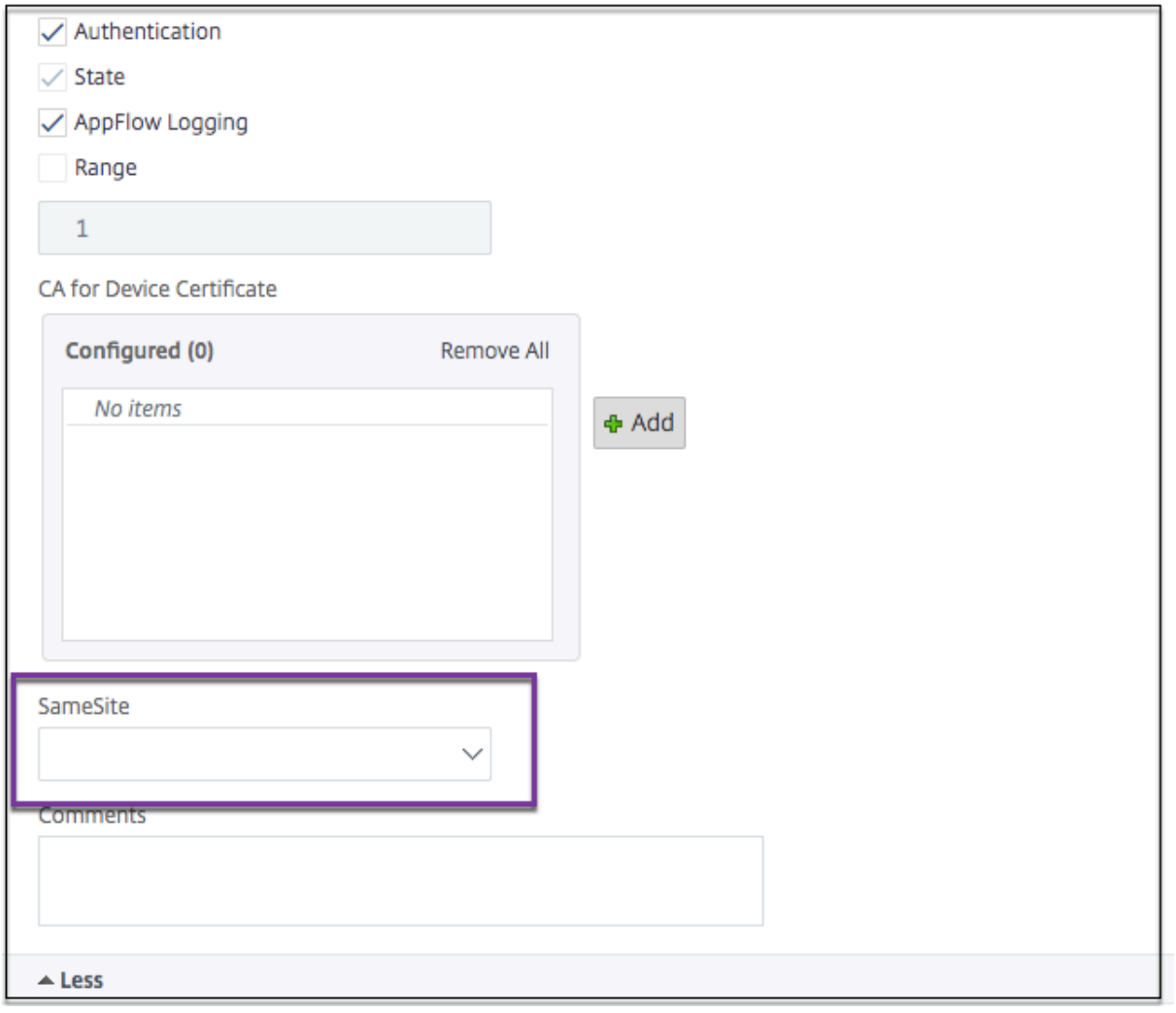
Ejemplo:


```
bind patset ns_cookies_SameSite ”NSC_TASS”
bind patset ns_cookies_SameSite ”NSC_TMAS”
<!--NeedCopy-->
```

Configuración del atributo sameSite mediante la interfaz gráfica de usuario

Para establecer el atributo SameSite en el nivel del servidor virtual:

1. Vaya a **Seguridad > AAA — Tráfico de aplicaciones > Servidores virtuales.**
2. Seleccione un servidor virtual y haga clic en **Modificar**.
3. Haga clic en el icono de edición de la sección **Configuración básica**y haga clic en **Más**.
4. En **SameSite**, seleccione la opción según sea necesario.

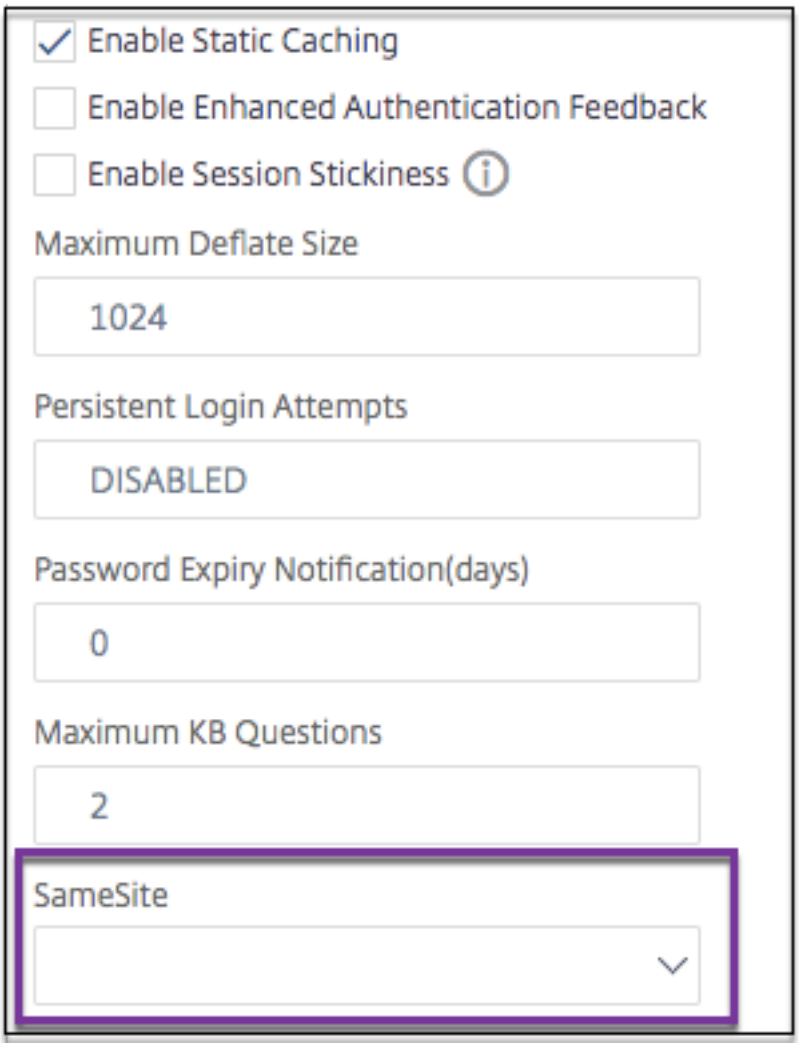


Para establecer el atributo SameSite a nivel global:

1. Vaya a **Seguridad > AAA — Tráfico de aplicaciones > Cambiar configuración de autenti-**

cación.

2. En la página **Configure AAA Parameter**, haga clic en la lista **SameSite** y seleccione la opción según sea necesario.



Configuración de autenticación, autorización y auditoría para protocolos de uso común

February 19, 2022

La configuración del dispositivo Citrix ADC para la autenticación, la autorización y la auditoría requiere una configuración específica en el dispositivo Citrix ADC y en los exploradores de los clientes. La configuración varía según el protocolo utilizado para la autenticación, autorización y auditoría.

Para obtener más información sobre la configuración del dispositivo Citrix ADC para la autenticación Kerberos, consulte Gestión de la autenticación, autorización y auditoría con Kerberos/NTLM.

Gestión de la autenticación, autorización y auditoría con Kerberos/NTLM

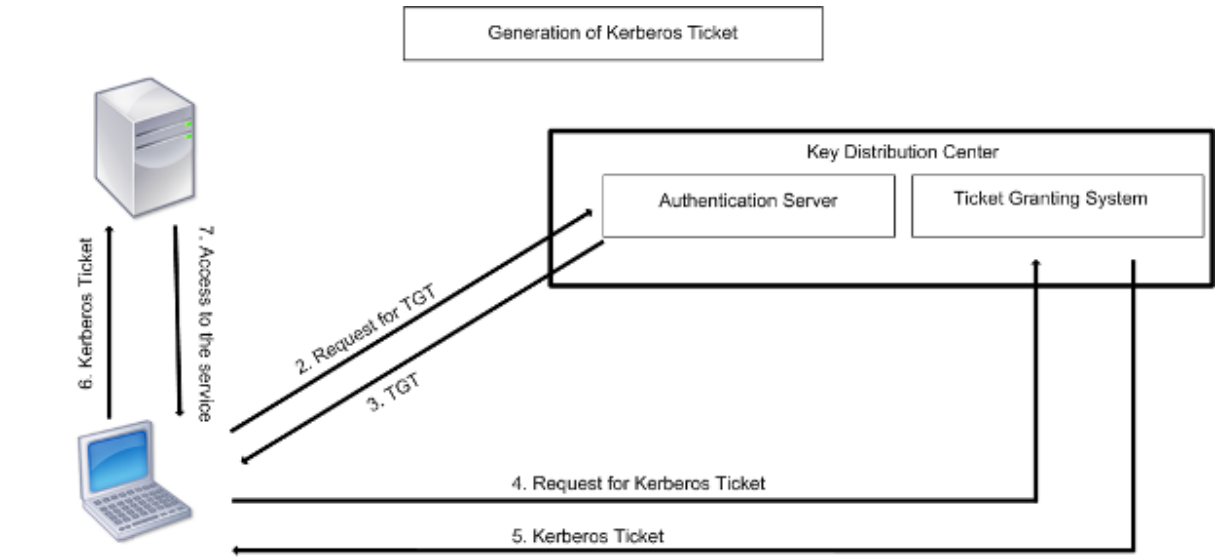
August 20, 2021

Kerberos, un protocolo de autenticación de red de equipos, proporciona una comunicación segura a través de Internet. Diseñado principalmente para aplicaciones cliente-servidor, proporciona una autenticación mutua mediante la cual el cliente y el servidor pueden garantizar la autenticidad del otro. Kerberos utiliza un tercero de confianza, denominado Centro de distribución de claves (KDC). Un KDC consta de un servidor de autenticación (AS), que autentica a un usuario, y un servidor de concesión de tíquets (TGS).

Cada entidad de la red (cliente o servidor) tiene una clave secreta que solo es conocida por sí misma y por el KDC. El conocimiento de esta clave implica la autenticidad de la entidad. Para la comunicación entre dos entidades de la red, el KDC genera una clave de sesión, denominada tíquet Kerberos o tíquet de servicio. El cliente realiza una solicitud al AS para obtener credenciales para un servidor específico. A continuación, el cliente recibe un tíquet, denominado Tíquet de concesión de tíquets (TGT). A continuación, el cliente se pone en contacto con el TGS, mediante el TGT que recibió del AS para demostrar su identidad, y solicita un servicio. Si el cliente puede usar el servicio, el TGS emite un tíquet Kerberos al cliente. A continuación, el cliente se pone en contacto con el servidor que aloja el servicio (denominado servidor de servicio), mediante el tíquet Kerberos para demostrar que está autorizado a recibir el servicio. El tíquet Kerberos tiene una vida útil configurable. El cliente se autentica con el AS solo una vez. Si se pone en contacto con el servidor físico varias veces, reutiliza el tíquet AS.

La siguiente ilustración muestra el funcionamiento básico del protocolo Kerberos.

Ilustración 1. **Funcionamiento de Kerberos**



La autenticación Kerberos tiene las siguientes ventajas:

- Autenticación más rápida. Cuando un servidor físico obtiene un tíquet Kerberos de un cliente, el servidor tiene suficiente información para autenticar el cliente directamente. No tiene que ponerse en contacto con un Controller de dominio para la autenticación del cliente y, por lo tanto, el proceso de autenticación es más rápido.
- Autenticación mutua. Cuando el KDC emite un tíquet Kerberos a un cliente y el cliente utiliza el tíquet para acceder a un servicio, solo los servidores autenticados pueden descifrar el tíquet Kerberos. Si el servidor virtual del dispositivo Citrix ADC puede descifrar el tíquet Kerberos, puede concluir que tanto el servidor virtual como el cliente están autenticados. Por lo tanto, la autenticación del servidor ocurre junto con la autenticación del cliente.
- Inicio de sesión único entre Windows y otros sistemas operativos compatibles con Kerberos.

La autenticación Kerberos puede tener las siguientes desventajas:

- Kerberos tiene requisitos de tiempo estrictos; los relojes de los hosts involucrados deben sincronizarse con el reloj del servidor Kerberos para asegurarse de que la autenticación no falla. Puede mitigar esta desventaja mediante el uso de los daemons del Protocolo de hora de red para mantener sincronizados los relojes del host. Los tíquets Kerberos tienen un período de disponibilidad, que puede configurar.
- Kerberos necesita que el servidor central esté disponible continuamente. Cuando el servidor Kerberos está inactivo, nadie puede iniciar sesión. Puede mitigar este riesgo mediante el uso de varios servidores Kerberos y mecanismos de autenticación de reserva.
- Dado que toda la autenticación está controlada por un KDC centralizado, cualquier compromiso en esta infraestructura, como la contraseña del usuario para una estación de trabajo local que se está robando, puede permitir que un atacante suplante a cualquier usuario. Puede mitigar este riesgo hasta cierto punto mediante solo un equipo de escritorio o portátil en el que confíe,

o aplicando la autenticación previa mediante un token de hardware.

Para utilizar la autenticación Kerberos, debe configurarla en el dispositivo Citrix ADC y en cada cliente.

Optimización de la autenticación Kerberos en la autenticación, autorización y auditoría

El dispositivo Citrix ADC optimiza y mejora el rendimiento del sistema mientras que la autenticación Kerberos. El demonio de autenticación, autorización y auditoría recuerda la solicitud Kerberos pendiente para el mismo usuario para evitar la carga en el Centro de distribución de claves (KDC), lo que evitará solicitudes duplicadas.

Cómo Citrix ADC implementa Kerberos para la autenticación de clientes

August 20, 2021

> **Importante**
>
> La autenticación Kerberos/NTLM solo se admite en la versión NetScaler 9.3 nCore o posterior, y solo se puede utilizar para la autenticación, autorización y auditoría de servidores virtuales de administración de tráfico.

Citrix ADC maneja los componentes involucrados en la autenticación Kerberos de la siguiente manera:

Centro de distribución de claves (KDC)

En Windows 2000 Server o versiones posteriores, el controlador de dominio y el KDC forman parte de Windows Server. Si Windows Server está UP y en ejecución, indica que el controlador de dominio y el KDC están configurados. El KDC es también el servidor de Active Directory.

> **Nota**
>
> Todas las interacciones Kerberos se validan con el controlador de dominio Kerberos de Windows.

Servicio de autenticación y negociación de protocolos

Un dispositivo Citrix ADC admite la autenticación Kerberos en los servidores virtuales de autenticación de administración de tráfico, autorización y auditoría. Si falla la autenticación Kerberos, Citrix ADC utiliza la autenticación NTLM.

De forma predeterminada, Windows 2000 Server y versiones posteriores de Windows Server utilizan Kerberos para la autenticación, la autorización y la auditoría. Si crea una directiva de autenticación con NEGOCIATE como tipo de autenticación, Citrix ADC intenta utilizar el protocolo Kerberos para la

autenticación, autorización y auditoría y, si el explorador del cliente no recibe un tíquet Kerberos, Citrix ADC utiliza la autenticación NTLM. Este proceso se conoce como negociación.

El cliente puede no recibir un tíquet Kerberos en cualquiera de los siguientes casos:

- Kerberos no es compatible con el cliente.
- Kerberos no está habilitado en el cliente.
- El cliente está en un dominio distinto del KDC.
- El directorio de acceso del KDC no es accesible para el cliente.

Para la autenticación Kerberos/NTLM, Citrix ADC no utiliza los datos que están presentes localmente en el dispositivo Citrix ADC.

Autorización

El servidor virtual de administración de tráfico puede ser un servidor virtual de equilibrio de carga o un servidor virtual de conmutación de contenido.

Auditorías

El dispositivo Citrix ADC admite la auditoría de la autenticación Kerberos con el siguiente registro de auditoría:

- Seguimiento completo de auditoría de la actividad de usuario final de administración de tráfico
- Registro de SYSLOG y TCP de alto rendimiento
- Seguimiento completo de auditoría de los administradores del sistema
- Todos los eventos del sistema
- Formato de registro que permite ejecutar scripts

Entorno soportado

La autenticación Kerberos no necesita ningún entorno específico en Citrix ADC. El cliente (explorador) debe proporcionar soporte para la autenticación Kerberos.

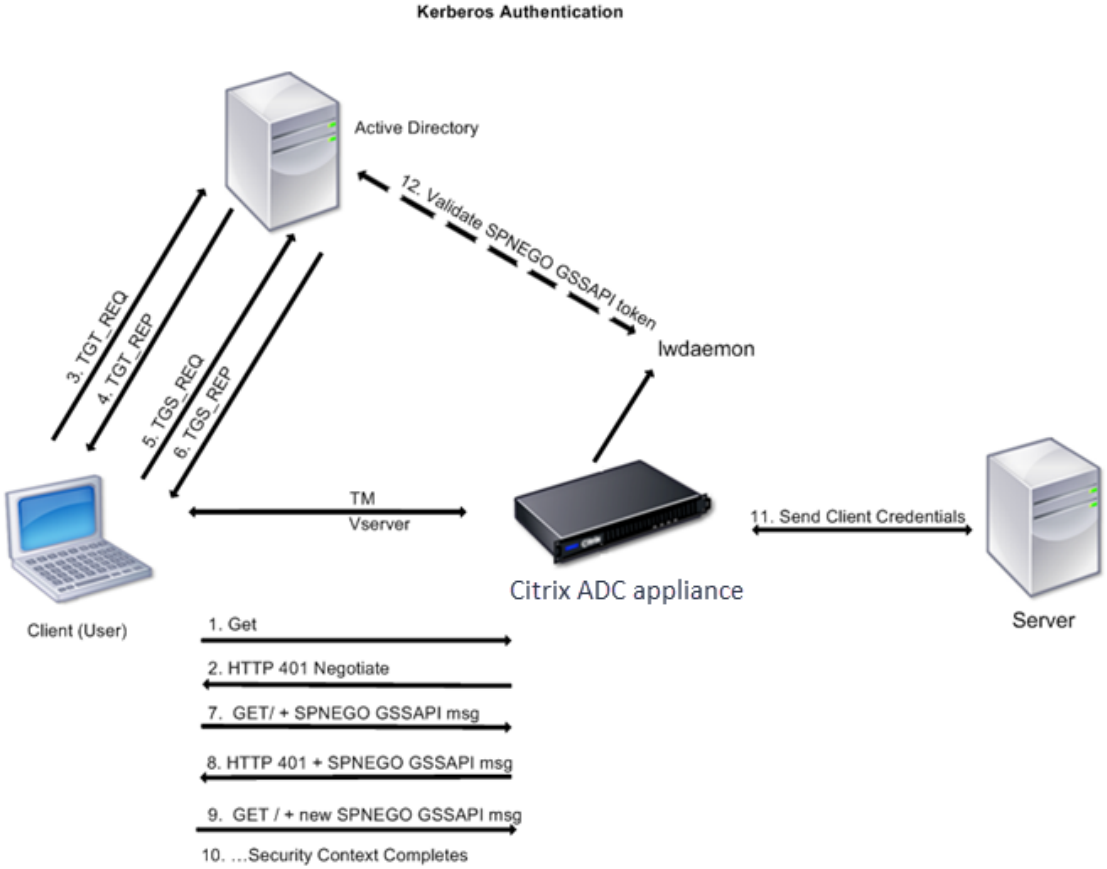
Alta disponibilidad

En una configuración de alta disponibilidad, solo el dispositivo Citrix ADC activo se une al dominio. En caso de una conmutación por error, el demonio Citrix ADC lwagent une el dispositivo Citrix ADC secundario al dominio. No se requiere ninguna configuración específica para esta funcionalidad.

Proceso de autenticación Kerberos

La siguiente ilustración muestra un proceso típico para la autenticación Kerberos en el entorno Citrix ADC.

Ilustración 1. Proceso de autenticación Kerberos en Citrix ADC



La autenticación Kerberos se produce en las etapas siguientes:

El cliente se autentica en el KDC

1. El dispositivo Citrix ADC recibe una solicitud de un cliente.
2. El servidor virtual de administración del tráfico (equilibrio de carga o conmutación de contenido) del dispositivo Citrix ADC envía un desafío al cliente.
3. Para responder al desafío, el cliente obtiene un tíquet Kerberos.
    - El cliente envía al servidor de autenticación del KDC una solicitud de un tíquet de concesión de tíquets (TGT) y recibe el TGT. (Consulte 3, 4 en la ilustración, Proceso de autenticación Kerberos.)
    - El cliente envía el TGT al servidor de concesión de tíquets del KDC y recibe un tíquet Kerberos. (Consulte 5, 6 en la ilustración, Proceso de autenticación Kerberos.)

> **Nota**
>
> El proceso de autenticación anterior no es necesario si el cliente ya tiene un tíquet Kerberos cuya vida útil no ha expirado. Además, los clientes como Servicios web, .NET o J2EE, que admiten SPNEGO, obtienen un tíquet Kerberos para el servidor de destino, crean un token SPNEGO e insertan el token en el encabezado HTTP cuando envían una solicitud HTTP. No pasan por el proceso de autenticación del cliente.

El cliente solicita un servicio.

1. El cliente envía el tíquet Kerberos que contiene el token SPNEGO y la solicitud HTTP al servidor virtual de administración de tráfico en Citrix ADC. El token SPNEGO tiene los datos GSSAPI necesarios.
2. El dispositivo Citrix ADC establece un contexto de seguridad entre el cliente y el dispositivo Citrix ADC. Si Citrix ADC no puede aceptar los datos proporcionados en el tíquet Kerberos, se le pedirá al cliente que obtenga otro tíquet. Este ciclo se repite hasta que los datos GSSAPI sean aceptables y se establezca el contexto de seguridad. El servidor virtual de administración de tráfico en Citrix ADC actúa como un proxy HTTP entre el cliente y el servidor físico.

El**dispositivo Citrix ADC completa la autenticación.**

1. Una vez completado el contexto de seguridad, el servidor virtual de administración de tráfico valida el token SPNEGO.
2. Desde el token SPNEGO válido, el servidor virtual extrae el ID de usuario y las credenciales de GSS, y las pasa al demonio de autenticación.
3. Una autenticación correcta completa la autenticación Kerberos.

Configuración de la autenticación kerberos en el dispositivo Citrix ADC

December 7, 2021

En este tema se proporcionan los pasos detallados para configurar la autenticación Kerberos en el dispositivo Citrix ADC mediante la CLI y la GUI.

Configuración de la autenticación Kerberos en la CLI

1. Habilite la función de autenticación, autorización y auditoría para garantizar la autenticación del tráfico en el dispositivo.

   ns-cli-prompt> **enable ns feature** AAA

2. Agregue el archivo keytab al dispositivo Citrix ADC. Se necesita un archivo keytab para descifrar el secreto recibido del cliente durante la autenticación Kerberos. Un único archivo keytab con-

tiene detalles de autenticación para todos los servicios que están enlazados al servidor virtual de administración de tráfico en el dispositivo Citrix ADC.

Primero genere el archivo keytab en el servidor de Active Directory y, a continuación, transfiéralo al dispositivo Citrix ADC.

- Inicie sesión en el servidor de Active Directory y agregue un usuario para la autenticación Kerberos mediante el siguiente comando.

```
net user <username> <password> /add
```

> **Nota**
>
> En la sección **Propiedades del usuario**, asegúrese de que la opción “Cambiar contraseña en el próximo inicio de sesión” no esté seleccionada y que la opción “La contraseña no caduca” esté seleccionada.

- Asigne el servicio HTTP al usuario anterior y exporte el archivo keytab. Por ejemplo, ejecute el siguiente comando en el servidor de Active Directory:

```
ktpass /out keytabfile /princ HTTP/owa.newacp.com@NEWACP.COM
   /pass <user password> /mapuser newacp\\dummy /ptype KRB5\
   _NT\_PRINCIPAL
```

> **Nota**
>
> Puede asignar más de un servicio si se requiere autenticación para más de un servicio. Si quiere asignar más servicios, repita el comando anterior para cada servicio. Puede dar el mismo nombre o nombres diferentes para el archivo de salida.

- Transfiera el archivo keytab al dispositivo Citrix ADC mediante el comando **ftp** de unix o cualquier otra utilidad de transferencia de archivos de su elección.

3. El dispositivo Citrix ADC debe obtener la dirección IP del controlador de dominio del nombre de dominio completo (FQDN). Por lo tanto, Citrix recomienda configurar Citrix ADC con un servidor DNS.

   ns-cli-prompt> **add dns nameserver** <ip-address>

   > **Nota**
   >
   > Como alternativa, puede agregar entradas de host estáticas o utilizar cualquier otro medio para que el dispositivo Citrix ADC pueda resolver el nombre FQDN del controlador de dominio en una dirección IP.

4. Configure la acción de autenticación y, a continuación, asociarla a una directiva de autenticación.

   - Configure la acción de negociación.

     ns-cli-prompt> **add authentication negotiateAction** <name> -domain <domain name> -domainUser <domain user name> -domainUserPasswd <domain user password> -defaultAuthenticationGroup <default authentication group> -keytab <string> -NTLMPath <string>

     Nota: Para la configuración de usuario de dominio y nombre de dominio, vaya al cliente y utilice el comando klist como se muestra en el siguiente ejemplo:

     Cliente: nombre de usuario @ AAA.LOCAL

     Servidor: http/onPrem_IDP.AAA.local @ AAA.LOCAL

     agregar autenticación NegotiateAction <name>- dominio - Usuario de dominio <HTTP/onprem_idp.aaa.local>

   - Configure la directiva de negociación y asocie la acción de negociación a esta directiva.

     ns-cli-prompt> **add authentication negotiatePolicy** <name> <rule> <reqAction>

5. Cree un servidor virtual de autenticación y asocie la directiva de negociación con él.

   - Cree un servidor virtual de autenticación.

     ns-cli-prompt> **add authentication vserver** <name> SSL <ipAuthVserver> 443 -authenticationDomain <domainName>

   - Enlace la directiva de negociación al servidor virtual de autenticación.

     ns-cli-prompt> **bind authentication vserver** <name> -policy <negotiatePolicyName>

6. Asocie el servidor virtual de autenticación con el servidor virtual de administración del tráfico (equilibrio de carga o conmutación de contenido).

   ns-cli-prompt> **set lb vserver** <name> -authn401 ON -authnVsName <string>

   > **Nota**
   >
   > También se pueden realizar configuraciones similares en el servidor virtual de conmutación de contenido.

7. Verifique las configuraciones haciendo lo siguiente:

   - Acceda al servidor virtual de administración de tráfico mediante el FQDN. Por ejemplo, Sample

   - Ver los detalles de la sesión en la CLI.

     ns-cli-prompt> **show aaa session**

Configuración de la autenticación Kerberos en la GUI

1. Habilite la función de autenticación, autorización y auditoría.

   Vaya a **Sistema** > **Configuración**, haga clic en **Configurar funciones básicas** y habilite la función de autenticación, autorización y auditoría.

2. Agregue el archivo keytab como se detalla en el paso 2 del procedimiento CLI mencionado anteriormente.

3. Agrega un servidor DNS.

   Vaya a **Administración del tráfico > DNS > Servidores**de nombres y especifique la dirección IP del servidor DNS.

4. Configure la acción y la directiva **Negociar**.

   Vaya a **Seguridad > AAA - Tráfico de aplicaciones > Directivas > Autenticación > Directivas avanzadas**> Directiva y cree una directiva con **Negociar** como tipo de acción. Haga clic en **AGREGAR** para crear un nuevo servidor de negociación de autenticación o haga clic en **Modificar** para configurar los detalles existentes.

5. Enlace la directiva de negociación al servidor virtual de autenticación.

   Vaya a **Seguridad > AAA - Tráfico de aplicaciones > Servidores virtuales**y asocie la directiva **Negotiate** con el servidor virtual de autenticación.

6. Asocie el servidor virtual de autenticación con el servidor virtual de administración del tráfico (equilibrio de carga o conmutación de contenido).

   Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**y especifique la configuración de autenticación relevante.

   > **Nota**
   >
   > También se pueden realizar configuraciones similares en el servidor virtual de conmutación de contenido.

7. Verifique las configuraciones como se detalla en el paso 7 del procedimiento CLI mencionado anteriormente.

Configurar la autenticación kerberos en un cliente

January 12, 2021

La compatibilidad con Kerberos debe configurarse en el explorador para usar Kerberos para la autenticación. Puede utilizar cualquier explorador compatible con Kerberos. Siga las instrucciones para

configurar el soporte Kerberos en Internet Explorer y Mozilla Firefox. Para otros exploradores, consulte la documentación del explorador.

Para configurar Internet Explorer para la autenticación Kerberos

1. En el menú **Herramientas**, seleccione **Opciones de Internet**.
2. En la ficha **Seguridad**, haga clic en **Intranet local** y, a continuación, haga clic en **Sitios**.
3. En el cuadro de diálogo **Intranet local**, asegúrese de que la opción Detectar automáticamente la red de intranet está seleccionada y, a continuación, haga clic en **Avanzadas**.
4. En el cuadro de diálogo **Intranet local**, agregue los sitios web de los dominios del servidor virtual de administración de tráfico en el dispositivo Citrix ADC. Los sitios especificados se convierten en sitios de intranet local.
5. Haga clic en **Cerrar** o en **Aceptar** para cerrar los cuadros de diálogo.

Para configurar Mozilla Firefox para la autenticación Kerberos

1. Asegúrese de que tiene Kerberos configurado correctamente en su equipo.
2. Escriba about:config en la barra de URL.
3. En el cuadro de texto del filtro, escriba network.negotiate.
4. Cambie network.negotiate-auth.delegation-uris al dominio que quiere agregar.
5. Cambie network.negotiate-auth.trusted-uris al dominio que quiere agregar.

> **Nota:** Si está ejecutando Windows, también debe introducir sspi en el cuadro de texto del filtro y cambiar la opción network.auth.use-sspi a False.

Descarga de autenticación Kerberos desde servidores físicos

February 19, 2022

El dispositivo Citrix ADC puede descargar las tareas de autenticación de los servidores. En lugar de que los servidores físicos autentiquen las solicitudes de los clientes, Citrix ADC autentica todas las solicitudes de los clientes antes de reenviarlas a cualquiera de los servidores físicos vinculados a él. La autenticación de usuarios se basa en tokens de Active Directory.

No hay autenticación entre Citrix ADC y el servidor físico y la descarga de autenticación es transparente para los usuarios finales. Tras el inicio de sesión inicial en un equipo con Windows, el usuario final no tiene que introducir ninguna información de autenticación adicional en una ventana emergente o en una página de inicio de sesión.

En la versión actual del dispositivo Citrix ADC, la autenticación Kerberos solo está disponible para los servidores virtuales de administración del tráfico de autenticación, autorización y auditoría. La aut-

enticación Kerberos no es compatible con SSL VPN en el dispositivo Citrix Gateway Advanced Edition ni en la administración de dispositivos Citrix ADC.

La autenticación Kerberos requiere configuración en el dispositivo Citrix ADC y en los exploradores cliente.

Para configurar la autenticación Kerberos en el dispositivo Citrix ADC

> **Nota**
>
> Las contraseñas utilizadas en la siguiente configuración de ejemplo son solo ejemplos y no las contraseñas de configuración reales.

1. Cree una cuenta de usuario en Active Directory. Al crear una cuenta de usuario, compruebe las siguientes opciones en la sección Propiedades de usuario:
   - Asegúrese de no seleccionar la opción Cambiar contraseña en el próximo inicio de sesión.
   - Asegúrese de seleccionar la opción La contraseña no caduca.
2. En el servidor de AD, en el símbolo del sistema de la CLI, escriba:
   - ktpass -princ HTTP/kerberos.crete.lab.net@crete.lab.net -ptype KRB5_NT_PRINCIPAL -mapuser kerbuser@crete.lab.net -mapop set -pass <password> -out C:\kerbtabfile.txt

   > **Nota**
   >
   > Asegúrese de escribir el comando anterior en una sola línea. El resultado del comando anterior se escribe en el archivo C:\kerbtabfile.txt.
3. Cargue el archivo kerbtabfile.txt en el directorio /etc del dispositivo Citrix ADC mediante un cliente de Secure Copy (SCP).
4. Ejecute el siguiente comando para agregar un servidor DNS al dispositivo Citrix ADC.
   - agregar servidor de nombres dns 1.2.3.4

   El dispositivo Citrix ADC no puede procesar solicitudes Kerberos sin el servidor DNS. Asegúrese de utilizar el mismo servidor DNS que se utiliza en el dominio de Microsoft Windows.
5. Cambie a la interfaz de línea de comandos de Citrix ADC.
6. Ejecute el siguiente comando para crear un servidor de autenticación Kerberos:
   - add authentication negotiateAction KerberosServer -domain “crete.lab.net” -domainUser kerbuser -domainUserPasswd <password> -keytab /var/mykcd.keytab

   > **Nota**
   >
   > Si keytab no está disponible, puede especificar los parámetros: domain, domainUser y -domainUserPasswd.

7. Ejecute el siguiente comando para crear una directiva de negociación:

   - `add authentication negotiatePolicy Kerberos-Policy "REQ.IP.DESTIP == 192.168.17.200"KerberosServer<!--NeedCopy-->`

8. Ejecute el siguiente comando para crear un servidor virtual de autenticación.

   - `add authentication vserver Kerb-Auth SSL 192.168.17.201 443 -AuthenticationDomain crete.lab.net<!--NeedCopy-->`

9. Ejecute el siguiente comando para enlazar la directiva Kerberos al servidor virtual de autenticación:

   - `bind authentication vserver Kerb-Auth -policy Kerberos-Policy -priority 100<!--NeedCopy-->`

10. Ejecute el siguiente comando para enlazar un certificado SSL al servidor virtual de autenticación. Puede utilizar uno de los certificados de prueba, que puede instalar desde la interfaz gráfica de usuario del dispositivo Citrix ADC. Ejecute el siguiente comando para utilizar el certificado de muestra de ServerTestCert.

    - `bind ssl vserver Kerb-Auth -certkeyName ServerTestCert<!--NeedCopy-->`

11. Cree un servidor virtual de equilibrio de carga HTTP con la dirección IP 192.168.17.200.

    Asegúrese de crear un servidor virtual desde la interfaz de línea de comandos para las versiones de NetScaler 9.3 si son anteriores a la 9.3.47.8.

12. Ejecute el siguiente comando para configurar un servidor virtual de autenticación:

    - `set lb vserver <name>-authn401 ON -authnVsName Kerb-Auth<!--NeedCopy-->`

13. Introduzca el nombre de host Ejemplo en la barra de direcciones del explorador Web.

    El explorador web muestra un cuadro de diálogo de autenticación porque la autenticación Kerberos no está configurada en el explorador.

    > **Nota**
    >
    > La autenticación Kerberos requiere una configuración específica en el cliente. Asegúrese de que el cliente puede resolver el nombre de host, lo que hace que el explorador web se conecte a un servidor virtual HTTP.

14. Configure Kerberos en el explorador web del equipo cliente.

    - Para configurar en Internet Explorer, consulte Configuración de Internet Explorer para la autenticación Kerberos.
    - Para configurar en Mozilla Firefox, consulte Configuración de Internet Explorer para la autenticación Kerberos.

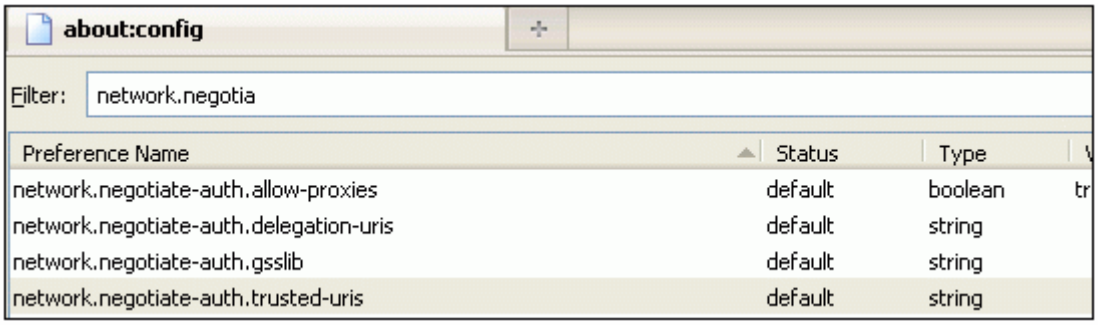
15. Compruebe si puede acceder al servidor físico back-end sin autenticación.

Para configurar Internet Explorer para la autenticación Kerberos

1. Seleccione **Opciones de Internet** en el menú **Herramientas** .
2. Activa la ficha **Seguridad** .
3. Seleccione **Intranet local en** la sección Seleccionar una zona para ver los cambios de configuración de seguridad.
4. Haga clic en **Sitios**.
5. Haga clic en **Avanzadas**.
6. Especifique la URL, el ejemplo y haga clic en **Agregar**.
7. Reinicie **Internet Explorer**.

Para configurar Mozilla Firefox para la autenticación Kerberos

1. Escriba about:config en la barra de direcciones del explorador.
2. Haga clic en la exención de responsabilidad de advertencia.
3. Escriba **network.negotiate-auth.trusted-URIS** en el cuadro **Filtro** .
4. Haga doble clic en **Network.negotiate-auth.trusted-URIS.** A continuación se muestra una pantalla de ejemplo.



5. En el cuadro de diálogo Introducir valor de cadena, especifique www.crete.lab.net.
6. Reinicia Firefox.

Solución de problemas relacionados con la autenticación y la autorización

February 19, 2022

Localizar mensajes de error

Localizar los mensajes de error generados por el sistema Citrix ADC nFactor

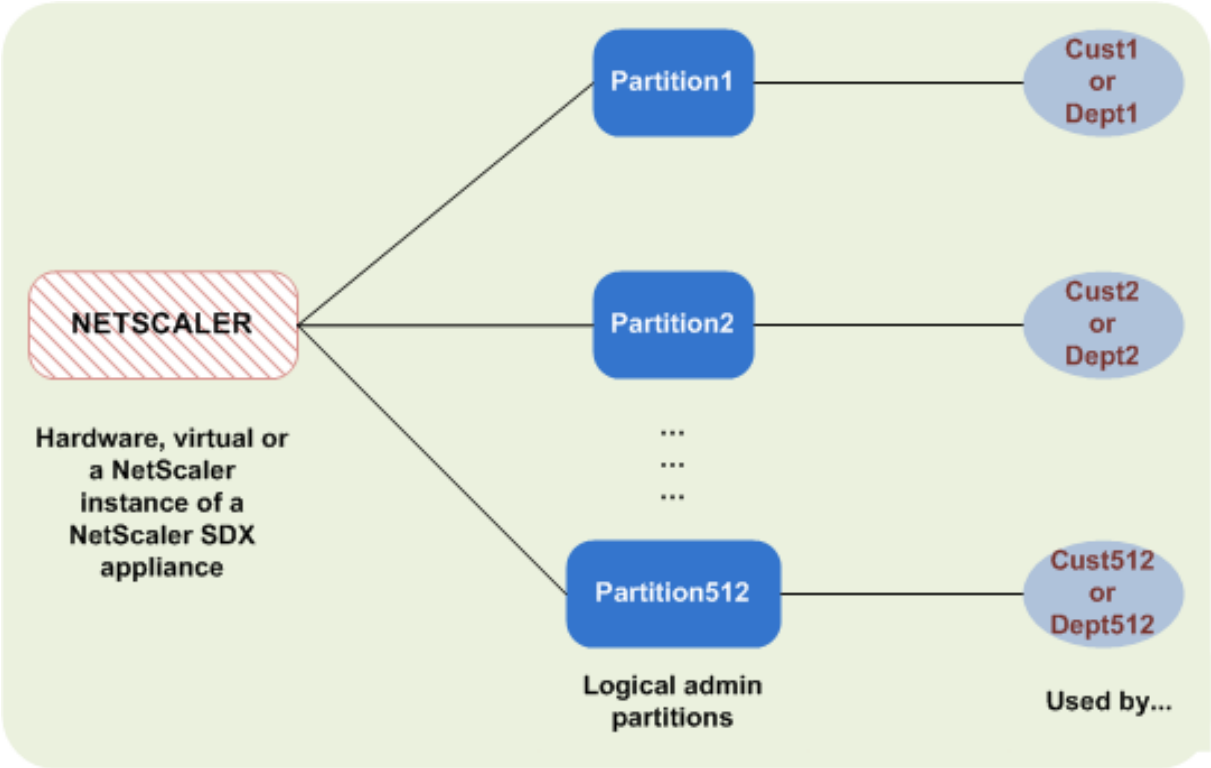
Solucionar problemas de autenticación con el módulo aaad.debug

Solucionar problemas de autenticación en Citrix ADC y Citrix Gateway con el módulo aaad.debug

Partición de administrador

September 8, 2021

Un dispositivo Citrix ADC se puede dividir en entidades lógicas denominadas particiones de administración. Cada partición se puede configurar y utilizar como dispositivo Citrix ADC independiente. En la siguiente ilustración se muestran las particiones de un dispositivo Citrix ADC que utilizan diferentes clientes y departamentos:



Un dispositivo Citrix ADC particionado tiene una única partición predeterminada y una o más particiones de administración. En la siguiente tabla se proporcionan más detalles sobre los dos tipos de particiones:

> **Nota**
>
> En un dispositivo particionado, el modo BridgeBPDU se puede habilitar solo en la partición predeterminada y no en las particiones administrativas.

Disponibilidad:

El dispositivo Citrix ADC se suministra con una única partición, que se denomina partición predeterminada. La partición predeterminada se conserva incluso después de particionar el dispositivo Citrix ADC.

Debe crearse explícitamente como se describe en Configurar particiones de administración.

Número de particiones:

Uno

Un dispositivo Citrix ADC puede tener una o más particiones de administración (un máximo de 512).

Acceso de usuario y roles:

Todos los usuarios de Citrix ADC, que no están asociados a una directiva de comandos *específica de una partición*, pueden acceder a la partición predeterminada y configurarla. Como siempre, la política de comandos asociada restringe las operaciones que un usuario puede realizar.

Los superusuarios de Citrix ADC crean el acceso de usuario y los roles, que también especifican los usuarios de esa partición. Solo los superusuarios y los usuarios asociados de la partición pueden acceder a la partición de administrador y configurarla.

> **Nota**
>
> Los usuarios de particiones no tienen acceso de shell.

Estructura de archivos:

Todos los archivos de una partición predeterminada se almacenan en la estructura de archivos predeterminada de Citrix ADC.

Por ejemplo, el directorio */nsconfig* almacena el archivo de configuración de Citrix ADC y el directorio */var/log/* almacena los registros de Citrix ADC.

Todos los archivos de una partición de administrador se almacenan en rutas de directorio que tienen el nombre de la partición de administrador.

Por ejemplo, el archivo de configuración de Citrix ADC (ns.conf) se almacena en el `/nsconfig/partitions/<partitionName>` directorio. Otros archivos específicos de particiones se almacenan en los `/var/partitions/<partitionName>` directorios.

Otras rutas de una partición de administrador:

- Archivos descargados: `/var/partitions/<partitionName>/download/`
- Archivos de registro: `/var/partitions/<partitionName>/log/`

> **Nota**
>
> En la actualidad, el registro no se admite a nivel de partición. Por lo tanto, este directorio está vacío y todos los registros se almacenan en el `/var/log/` directorio.

- Archivos relacionados con el certificado SSL CRL: `/var/partitions/<partitionName>/netscaler/ssl`

Recursos disponibles:

Todos los recursos de Citrix ADC.

Recursos de Citrix ADC asignados explícitamente a la partición de administración.

Acceso de usuarios y roles

Al autenticar y autorizar un dispositivo Citrix ADC particionado, un administrador raíz puede asignar un administrador de particiones a una o más particiones. El administrador de particiones puede autorizar a los usuarios a esa partición sin afectar a otras particiones. Los usuarios de la partición están autorizados a acceder solo a esa partición utilizando la dirección SNIP. Tanto el administrador raíz como el administrador de particiones pueden configurar el acceso basado en roles (RBA) autorizando a los usuarios a acceder a diferentes aplicaciones.

Los roles de administrador y de usuario se pueden describir de la siguiente manera:

Administrador raíz. Accede al dispositivo particionado a través de su dirección NSIP y puede otorgar acceso al usuario a una o más particiones. El administrador también puede asignar administradores de particiones a una o más particiones. El administrador puede crear un administrador de particiones a partir de la partición predeterminada mediante una dirección NSIP o cambiar a una partición y, a continuación, crear un usuario y asignar acceso de administrador de particiones mediante una dirección SNIP.

Administrador de particiones. Accede a la partición especificada a través de una dirección NSIP asignada por el administrador raíz. El administrador puede asignar acceso basado en roles al acceso de usuario de particiones a esa partición y también configurar la autenticación de servidor externo mediante la configuración específica de la partición.

Usuario del sistema. Accede a las particiones a través de la dirección NSIP. Tiene acceso a las particiones y recursos especificados por el administrador raíz.

Usuario de partición. Accede a una partición a través de una dirección SNIP. El administrador de particiones crea la cuenta de usuario y el usuario tiene acceso a los recursos, solo dentro de la partición.

Puntos que tener en cuenta

A continuación se presentan algunos puntos que debe recordar al proporcionar acceso basado en roles en una partición.

1. Los usuarios de Citrix ADC que acceden a la GUI a través de la dirección NSIP utilizan la configuración de autenticación de partición predeterminada para iniciar sesión en el dispositivo.
2. Los usuarios del sistema de particiones que acceden a la GUI a través de una dirección SNIP de partición utilizan la configuración de autenticación específica de la partición para iniciar sesión en el dispositivo.
3. El usuario de partición creado en una partición no puede iniciar sesión con la dirección NSIP.
4. El usuario de Citrix ADC vinculado a una partición no puede iniciar sesión mediante la dirección SNIP de la partición.
5. Los usuarios del sistema que se autentican a través de un servidor de autenticación externo (por ejemplo, LDAP, RADIUS, TACACS) deben acceder a una partición a través de una dirección SNIP.

Caso de uso para administrar el acceso basado en roles en una configuración particionada

Considere un escenario en el que una organización empresarial, www.example.com tiene varias unidades de negocio y un administrador centralizado que administra todas las instancias de su red. Sin embargo, desean proporcionar privilegios de usuario y entorno exclusivos para cada unidad de negocio.

A continuación se presentan los administradores y usuarios administrados por configuración predeterminada de autenticación de particiones y configuración específica de particiones en un dispositivo particionado.

John: Administrador raíz

George: Administrador de particiones

Adam: Usuario del sistema

Jane: Usuario de particiones

John, es el administrador raíz de un dispositivo Citrix ADC particionado. John administra todas las cuentas de usuario y cuentas de usuario administrativas en todas las particiones (por ejemplo, P1, P2, P3, P4 y P5) dentro del dispositivo. John proporciona acceso detallado basado en roles a las entidades desde la partición predeterminada del dispositivo. John crea cuentas de usuario y asigna acceso a particiones a cada cuenta. George, como ingeniero de redes dentro de la organización, prefiere tener acceso basado en roles a pocas aplicaciones que se ejecutan en la partición P2. Según la administración de usuarios, John crea un rol de administrador de particiones para George y asocia su cuenta de usuario a una política de comandos partition-admin en la partición P2. Adam es otro ingeniero de redes prefiere acceder a una aplicación que se ejecuta en P2. John crea una cuenta de

usuario del sistema para Adam y asocia su cuenta de usuario a una partición P2. Una vez creada la cuenta, Adam puede iniciar sesión en el dispositivo para acceder a la interfaz de administración de Citrix ADC a través de la dirección NSIP y cambiar a la partición P2 según el enlace de usuario/grupo.

Supongamos que Jane, que es otro ingeniero de redes, quiere acceder directamente a una aplicación que se ejecuta solo en la partición P2, George (administrador de particiones) puede crear una cuenta de usuario de partición para ella y asociar su cuenta con políticas de comandos para obtener privilegios de autorización. La cuenta de usuario de Jane creada dentro de la partición ahora está directamente asociada a P2. Ahora Jane puede acceder a la interfaz de administración de Citrix ADC a través de la dirección SNIP y no puede cambiar a ninguna otra partición.

> **Nota**
>
> Si un administrador de particiones crea la cuenta de usuario de Jane en la partición P2, el administrador solo puede acceder a la interfaz de administración de Citrix ADC a través de la dirección SNIP (creada dentro de la partición). El administrador no puede acceder a la interfaz a través de la dirección NSIP. Del mismo modo, si la cuenta de usuario de Adam la crea un administrador raíz en la partición predeterminada y está enlazada a una partición P2. El administrador puede acceder a la interfaz de administración de Citrix ADC solo a través de la dirección NSIP o la dirección SNIP creada en la partición predeterminada (con el acceso de administración habilitado). Y no se permite acceder a la interfaz de partición a través de la dirección SNIP creada en la partición administrativa.

Configurar roles y responsabilidades para los administradores de particiones

A continuación se presentan las configuraciones que realiza un administrador raíz en una partición predeterminada.

Creación de particiones administrativas y usuarios del sistema: un administrador raíz crea particiones administrativas y usuarios del sistema en la partición predeterminada del dispositivo. A continuación, el administrador asocia a los usuarios a distintas particiones. Si está vinculado a una o más particiones, puede cambiar de una partición a otra según los enlaces de usuario. Además, el acceso a una o más particiones enlazadas solo está autorizado por el administrador raíz.

Autorización del usuario del sistema como administrador de particiones para una partición específica: una vez creada una cuenta de usuario, el administrador raíz cambia a una partición específica y autoriza al usuario como administrador de particiones. Se realiza asignando la política de comandos partition-admin a la cuenta de usuario. Ahora, el usuario puede acceder a la partición como administrador de particiones y administrar entidades dentro de la partición.

A continuación se presentan las configuraciones que realiza un administrador de particiones en una partición administrativa.

Configuración de la dirección SNIP en una partición administrativa: el administrador de la partición

inicia sesión en la partición y crea una dirección SNIP y proporciona acceso de administración a la dirección.

Creación y vinculación de un usuario del sistema de particiones con la directiva de comandos de partición: el administrador de particiones crea usuarios de particiones y define el alcance del acceso de los usuarios. Se realiza vinculando la cuenta de usuario a las directivas de comandos de partición.

Creación y vinculación de grupos de usuarios del sistema de particiones con la directiva de comandos de partición: el administrador de particiones crea grupos de usuarios de particiones y define el ámbito del acceso a grupos de usuarios. Se realiza vinculando la cuenta de grupo de usuarios a las directivas de comandos de partición.

Configuración de la autenticación del servidor externo para usuarios externos (opcional): esta configuración se realiza para autenticar a los usuarios TACACS externos que acceden a la partición mediante la dirección SNIP.

A continuación se presentan las tareas que se realizan en la configuración del acceso basado en roles para los usuarios de particiones en una partición administrativa.

1. Creación de una partición administrativa: antes de crear usuarios de particiones en una partición administrativa, primero debe crear la partición. Como administrador raíz, puede crear una partición a partir de la partición predeterminada mediante la utilidad de configuración o una interfaz de línea de comandos.
2. Cambio del acceso de usuario de la partición predeterminada a la partición P2: si es administrador de particiones que accede al dispositivo desde la partición predeterminada, puede cambiar de la partición predeterminada a una partición específica. Por ejemplo, la partición P2 basada en el enlace de usuario.
3. Agregar una dirección SNIP a la cuenta de usuario de partición con acceso de administración habilitado, una vez que haya cambiado el acceso a una partición de administración. Crea una dirección SNIP y proporciona acceso de administración a la dirección.
4. Creación y vinculación de un usuario del sistema de particiones con directiva de comandos de partición: si es administrador de particiones, puede crear usuarios de particiones y definir el alcance del acceso de los usuarios. Se realiza vinculando la cuenta de usuario a las directivas de comandos de partición.
5. Creación y enlace de grupos de usuarios de particiones con la directiva de comandos de partición: si es administrador de particiones, puede crear grupos de usuarios de particiones y definir el ámbito del control de acceso de usuarios. Se realiza vinculando la cuenta de grupo de usuarios a las directivas de comandos de partición.

Configuración de la autenticación del servidor externo para usuarios externos (opcional): esta configuración se realiza para autenticar a los usuarios TACACS externos que acceden a la partición mediante una dirección SNIP.

Beneficios del uso de particiones de administración

Puede aprovechar las siguientes ventajas utilizando particiones de administración para su implementación:

- Permite la delegación de la propiedad administrativa de una aplicación al cliente.
- Reduce el coste de propiedad de ADC sin comprometer el rendimiento y la facilidad de uso.
- Protege contra cambios de configuración injustificados. En un dispositivo Citrix ADC sin particiones, los usuarios autorizados de la otra aplicación pueden cambiar intencionadamente o no intencionalmente las configuraciones necesarias para la aplicación. Puede llevar a comportamientos indeseables. Esta posibilidad se reduce en un dispositivo Citrix ADC particionado.
- Aísla el tráfico entre diferentes aplicaciones mediante el uso de VLAN dedicadas para cada partición.
- Acelera y permite escalar las implementaciones de aplicaciones.
- Permite la administración y la generación de informes a nivel de aplicación o localizadas.

Analicemos un par de casos para comprender los escenarios en los que se pueden utilizar las particiones de administración.

Caso de usuario 1: Cómo se utiliza la partición de administrador en una red empresarial

Consideremos un escenario al que se enfrenta una empresa llamada **Foo.com**.

- **Foo.com** tiene un solo Citrix ADC.
- Hay cinco departamentos y cada departamento tiene una aplicación que requiere implementarse con Citrix ADC.
- Cada aplicación debe ser administrada de forma independiente por un conjunto diferente de usuarios o administradores.
- Debe restringirse a otros usuarios el acceso a las configuraciones.
- La aplicación o el back-end deben poder compartir recursos como direcciones IP.
- El departamento de TI global debe poder controlar la configuración a nivel de Citrix ADC, que debe ser común a todas las particiones.
- Las solicitudes deben ser independientes entre sí. Un error en la configuración de una aplicación no debe afectar a la otra.

Un Citrix ADC sin particiones no podría cumplir estos requisitos. Sin embargo, puede cumplir todos estos requisitos mediante la partición de un Citrix ADC.

Simplemente cree una partición para cada una de las aplicaciones, asigne los usuarios necesarios a las particiones, especifique una VLAN para cada partición y defina la configuración global en la partición predeterminada.

Caso de uso 2: Cómo utiliza un proveedor de servicios una partición de administrador

Consideremos un escenario al que se enfrenta un proveedor de servicios llamado **BigProvider**:

- BigProvider tiene 5 clientes: 3 pequeñas empresas y 2 grandes empresas.
- **SmallBiz**, **SmallerBiz**y **StartupBiz** solo necesitan la funcionalidad más básica de Citrix ADC.
- **BigBiz** y **LargeBiz** son empresas más grandes y tienen aplicaciones que atraen mucho tráfico. Les gustaría utilizar algunas de las funciones más complejas de Citrix ADC.

En un enfoque sin particiones, el administrador de Citrix ADC suele utilizar un dispositivo Citrix ADC SDX y aprovisionar una instancia de Citrix ADC para cada cliente.

La solución se adapta a **BigBizy LargeBiz**porque sus aplicaciones necesitan la potencia sin disminuir de todo el dispositivo Citrix ADC sin particiones. Sin embargo, esta solución podría no ser tan rentable para el mantenimiento de**SmallBiz**,**SmallerBiz**y**StartupBiz**.

Por lo tanto, **BigProvider** decide la siguiente solución:

- Uso de un dispositivo Citrix ADC SDX para abrir instancias Citrix ADC dedicadas para **BigBiz** y **LargeBiz**.
- Utilizando un solo Citrix ADC que se divide en tres particiones, una para **SmallBiz**, **SmallerBiz**y **StartupBiz**.

El administrador de Citrix ADC (superusuario) crea una partición de administración para cada uno de estos clientes y especifica los usuarios de las particiones. También especifica los recursos de Citrix ADC para las particiones y especifica la VLAN que utilizará el tráfico destinado a cada una de las particiones.

Compatibilidad con configuraciones de Citrix ADC en la partición de administración

October 5, 2021

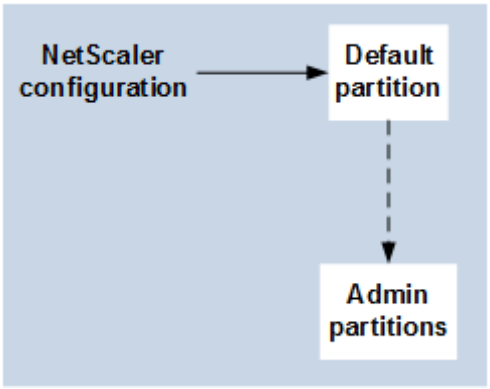
Las configuraciones de Citrix ADC se pueden clasificar en los tres tipos de configuraciones siguientes. Depende de la configuración de Citrix y de la partición en la que se realice la configuración.

> **Nota**
>
> - Las particiones de administración no se pueden configurar en un clúster de Citrix ADC. Significa que un clúster Citrix ADC no se puede particionar.
> - Las particiones de administración no se pueden configurar en un dispositivo FIPS Citrix ADC 14000.
> - Elcaso 3 enumera las funciones de Citrix ADC que no se admiten en las particiones de administración.

- Las plantillas de equilibrio de carga no son compatibles con las particiones administrativas.

Caso 1 (configuraciones globales)

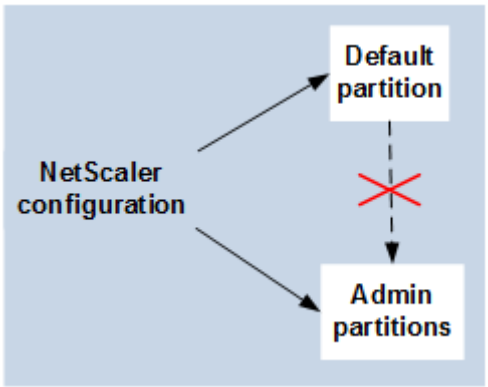
Configuraciones que se pueden realizar SOLO en la partición predeterminada y que están disponibles o afectan a todas las particiones de administración.



- Actualizaciones de entidades integradas para monitores, perfiles TCP, perfiles HTTP, etc.
- Actualizaciones de los parámetros globales para syslog, NSLOG, weblog, conmutación de contenido, IPSEC, SIP, DHCP, protección contra sobretensiones, almacenamiento en búfer TCP y recopilación de sistemas.
- Configuraciones de alta disponibilidad (HA)
- Cambios de interfaz y VLAN
- Configuraciones de usuario

Caso 2 (configuraciones específicas de particiones)

Configuraciones que se pueden realizar de forma independiente en particiones predeterminadas y de administración. Estas configuraciones solo son aplicables a la partición en la que se realizan.

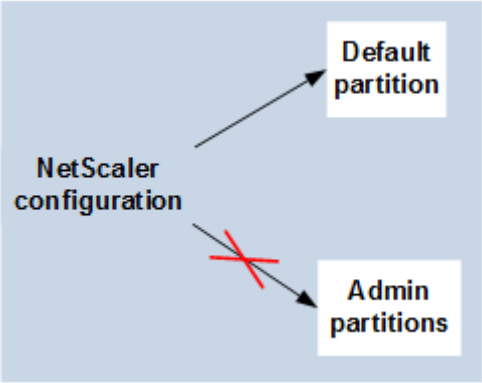


- Obtención de estadísticas de nivel de tráfico de una partición.

- El administrador de particiones puede actualizar los enlaces IP para la VLAN que está enlazada a esa partición. Pero no se pueden actualizar los enlaces de interfaz.
- Borrado de configuraciones de Citrix ADC.
- Parámetros específicos de la función para las siguientes funciones: AppFlow, AppQoe, compresión HTTP, DNS, TCP, HTTP, cifrado, respuesta, reescritura y SSL.
- Configuraciones específicas de funciones como servidores virtuales, servicios y monitores.

Caso 3

Configuraciones que no se pueden realizar en particiones de administración. Estas funciones se pueden configurar en la partición predeterminada, pero no afectan a las particiones de administración.



> **Nota:**
>
> Las configuraciones compatibles con las particiones de administración de una versión concreta se marcan como **Sí**.

Componente de función	Función Citrix ADC	NetScaler 11.1	NetScaler 12.0	Citrix ADC 12.1	Citrix ADC 13.0	Citrix ADC 13.1
Redes	Dominio de tráfico	No (no se admite desde la compilación 60.13 en adelante)	No	No	No	No
Directiva	Extensibilidad	Sí	Sí	Sí	Sí	Sí
Equilibrio de carga	Escala automática de DBS	Sí	Sí	Sí	Sí	Sí

Componente de función	Función Citrix ADC	NetScaler 11.1	NetScaler 12.0	Citrix ADC 12.1	Citrix ADC 13.0	Citrix ADC 13.1
Equilibrio de carga	DNSSEG	No	No	Sí	Sí	Sí
Equilibrio de carga	Diameter	Sí	Sí	Sí	Sí	Sí
Equilibrio de carga	RTSP	No	No	No	No	No
Equilibrio de carga	Conexión segura	Sí	Sí	Elementos retirados	Elementos retirados	Eliminado
Equilibrio de carga	Grupo de servicios de escalabilidad automática	Sí	Sí	Sí	Sí	Sí
Capacidad de administración	Autenticación externa RBA	Sí	Sí	Sí	Sí	Sí
Capacidad de administración	RISE Cisco	No	No	No	Sí	Sí
Capacidad de administración	ACI - Cisco	Sí	Sí	Sí	Sí	Sí
Capacidad de administración	AppExpert	Sí	Sí	Sí	Sí	Sí
Capacidad de administración	HDX Insight	No	No	No	No	No
Capacidad de administración	Insight	No	No	No	No	No

Componente de función	Función Citrix ADC	NetScaler 11.1	NetScaler 12.0	Citrix ADC 12.1	Citrix ADC 13.0	Citrix ADC 13.1
VPN	Conector Citrix Cloud-Bridge	No	No	No	No	No
VPN	VPN de Citrix Gateway o SSL	No	No	No	No	No
VPN	Proxy ICA de SSL VPN	No	No	No	No	No
VPN	Interfaz web en Citrix ADC	No	No	No	No	No
SSL	Perfil SSL	Sí	Sí	Sí	Sí	Sí
SSL	SSL-FIPS	No	No	No	No	No
SSL	HSM externo	No	No	No	No	No
Infra	Redirección de caché	No	No	No	No	No
Infra	Almacenamie en caché integrado	Sí	Sí	Sí	Sí	Sí
Red	VXLAN	Sí	Sí	Sí	Sí	Sí
Red	Cierre con período de gracia	Sí	Sí	Sí	Sí	Sí
Red	LSN	No	No	No	No	No
Red	Logotipo listo para IPv6	Sí	Sí	Sí	Sí	Sí
Red	vPath	Sí	Sí	Sí	Sí	Sí
Equilibrio de carga	Datastream	Sí	Sí	Sí	Sí	Sí

Componente de función	Función Citrix ADC	NetScaler 11.1	NetScaler 12.0	Citrix ADC 12.1	Citrix ADC 13.0	Citrix ADC 13.1
Registros	Registro web	Sí	Sí	Sí	Sí	Sí
Red	L2 Param/L3 Param	Sí	Sí	Sí	Sí	Sí
Red	Túnel GRE	Sí	Sí	Sí	Sí	Sí
Equilibrio de carga	Supervisión con guiones	Sí	Sí	Sí	Sí	Sí
Equilibrio de carga	GSLB	Sí	Sí	Sí	Sí	Sí
Infra	Espejado de conexiones	Sí	Sí	Sí	Sí	Sí
Infra	FEO	Sí	Sí	Sí	Sí	Sí
Infra	Traza ns	Sí	Sí	Sí	Sí	Sí
Equilibrio de carga	Cola por prioridad	Sí	Sí	Elementos retirados	Elementos retirados	Eliminado
Red	HDOSP	Sí	Sí	Elementos retirados	Elementos retirados	Eliminado
Red	Perfil neto	Sí	Sí	Sí	Sí	Sí
Red	Redes (función restringida)	Sí	Sí	Sí	Sí	Sí
Red	VRRP (función restringida)	Sí	Sí	Sí	Sí	Sí

Componente de función	Función Citrix ADC	NetScaler 11.1	NetScaler 12.0	Citrix ADC 12.1	Citrix ADC 13.0	Citrix ADC 13.1
Registros	Registro de auditoría (SYSLOG-TCP, LB de servidores syslog, compatibilidad con SNIP y compatibilidad con FQDN para syslog)	Sí	Sí	Sí	Sí	Sí
VPN	Citrix Gateway	No	No	No	No	No
VPN	AAA-TM	Sí	Sí	Sí	Sí	Sí
AppFlow	AppFlow	No	Sí (solo IPFIX)	Sí (solo IPFIX)	Sí	Sí
AppFW	Firewall de aplicaciones	No	No	No	No	No
Transformación de URL	Transformación de URL	No	No	No	No	No
Equilibrio de carga	Almacenamie en búfer TCP	No	No	No	No	No
Directivas	Respondedor OCSP	Sí	Sí	Sí	Sí	Sí
Registro de auditoría	SYSLOG-TCP	No	Sí	Sí	Sí	Sí
Optimización	Optimización front-end	No	Sí	Sí	Sí	Sí
AppQoE	AppQoE	Sí	Sí	Sí	Sí	Sí

En la tabla anterior se enumeran algunas de las funciones como **Funciones restringidas** en la con-

figuración de la partición de administración. En la siguiente sección se explica el motivo por el que algunas de las funciones se mencionan como **Funciones restringidas**.

- **VRRP**. El VRRP es una función restringida en la partición de administración debido a lo siguiente:
  - La adición o eliminación de VRID solo se puede hacer desde el contexto de partición predeterminado. Sin embargo, una vez creado un VRID, se puede utilizar en particiones no predeterminadas.
  - La funcionalidad VRRP solo se admite en las VLAN dedicadas.
  - La funcionalidad VRRP no se admite en las VLAN compartidas, utilizada por la partición de administración. Está bloqueado internamente. No se muestra ningún mensaje de error durante la configuración. El protocolo está bloqueado en una VLAN compartida (etiquetada o sin etiqueta) enlazada a una partición predeterminada o a cualquier partición administrativa.

> **Importante**
>
> Para admitir la implementación activa-activa mediante VRRP, VIP principal y de reserva deben utilizar el mismo VRID. No se pueden utilizar VRID diferentes.

- **Networking**. Algunas de las configuraciones de red (L2 Param y L3 Param) no son compatibles ni son válidas en el contexto de la partición. Si encuentra alguna de estas configuraciones, aparece el siguiente mensaje de error. “ERROR: Esta opción de configuración no se admite en la partición no predeterminada. “

Configurar particiones de administración

September 8, 2021

> **Importante**
>
> - Solo los superusuarios están autorizados a crear y configurar particiones de administración.
> - A menos que se especifique lo contrario, las configuraciones para configurar una partición de administrador deben realizarse desde la partición predeterminada.

Al particionar un dispositivo Citrix ADC, está creando en efecto varias instancias de un único dispositivo Citrix ADC. Cada instancia tiene sus propias configuraciones y el tráfico de cada una de estas particiones queda aislado de la otra. Se realiza asignando a cada partición una VLAN dedicada o una VLAN compartida.

Un Citrix ADC particionado tiene una partición predeterminada y las particiones de administración que se crean. Para configurar una partición de administrador, primero debe crear una partición con los

recursos pertinentes (memoria, ancho de banda máximo y conexiones). A continuación, especifique los usuarios que pueden acceder a la partición y el nivel de autorización de cada uno de los usuarios de la partición.

El acceso a un Citrix ADC particionado es lo mismo que acceder a un Citrix ADC no particionado: a través de la dirección NSIP o cualquier otra dirección IP de administración. Como usuario, después de proporcionar sus credenciales de inicio de sesión válidas, se le lleva a la partición a la que está vinculado. Cualquier configuración que cree se guarda en esa partición. Si está asociado a más de una partición, se le lleva a la primera partición a la que se asoció. Si desea configurar entidades en una de las otras particiones, debe cambiar explícitamente a esa partición.

Tras acceder a la partición adecuada, las configuraciones que realiza se guardan en esa partición y son específicas de esa partición.

> **Nota**
>
> - Los superusuarios de Citrix ADC y otros usuarios que no son particiones se llevan a la partición predeterminada.
> - Los usuarios de todas las 512 particiones pueden iniciar sesión simultáneamente.

Sugerencia

Para acceder a un dispositivo Citrix ADC particionado a través de HTTPS mediante el SNIP (con el acceso de administración habilitado), asegúrese de que cada partición tenga el certificado de su administrador de particiones. Dentro de la partición, el administrador de particiones debe hacer lo siguiente:

1. Agregue el certificado a Citrix ADC.

   ```
   add ssl certKey ns-server-certificate -cert ns-server.cert-key ns-server.key
   ```

2. Enlazarlo a un servicio denominado `nshttps-<SNIP>-3009`, donde `<SNIP>` debe reemplazarse por la dirección SNIP, en este caso 100.10.10.1.

   ```
   bind ssl service nshttps-100.10.10.1-3009 -certkeyName ns-server-certificate
   ```

Limitación de recursos de particiones

En un dispositivo Citrix ADC con particiones, un administrador de red puede crear una partición con recursos de partición como memoria, ancho de banda y límite de conexión configurados como ilimitados. Se hace especificando Zero como valor de recurso de partición. Donde cero indica que el recurso es ilimitado en la partición y se puede consumir hasta los límites del sistema. La configuración de recursos de partición resulta útil cuando se migra una implementación de dominio de tráfico a una

partición administrativa o si no conoce el límite de asignación de recursos para una partición de una implementación determinada.

El límite de recursos para una partición administrativa es el siguiente:

1. **Memoria de partición**. Es la memoria máxima asignada para una partición. Asegúrese de especificar los valores al crear una partición.

   > **Nota**
   >
   > A partir de NetScaler 12.0, al crear una partición, puede establecer el límite de memoria en Cero. Si ya se ha creado una partición con un límite de memoria específico, puede reducir el límite a cualquier valor o establecer el límite como Cero.

   Parámetro: maxMemLimit

   La memoria máxima se asigna en MB en una partición. Un valor cero indica que la memoria es ilimitada en la partición y puede consumirse hasta los límites del sistema.

   Valor predeterminado: 10

2. Ancho de**banda de particiones**. Ancho de banda máximo asignado para una partición. Si especifica un límite, asegúrese de que se encuentra dentro del rendimiento con licencia del dispositivo. De lo contrario, no limitará el ancho de banda utilizado por la partición. El límite especificado es responsable del ancho de banda que requiere la aplicación. Si el ancho de banda de la aplicación supera el límite especificado, se eliminan los paquetes.

   > **Nota**
   >
   > A partir de NetScaler 12.0, cuando puede crear una partición, puede establecer el límite de ancho de banda de la partición en Cero. Si ya se ha creado una partición con un ancho de banda específico, puede reducir el ancho de banda o establecer el límite como Cero.

   Parámetro: MaxBandwidth

   El ancho de banda máximo se asigna en Kbps en una partición. Un valor cero indica que el ancho de banda no está restringido. Es decir, la partición puede consumir hasta los límites del sistema.

   Valor predeterminado: 10240

   Valor máximo: 42949672,95

3. **Conexión de partición**. Número máximo de conexiones simultáneas que se pueden abrir en una partición. El valor debe acomodar el flujo simultáneo máximo esperado dentro de la partición. Las conexiones de partición se contabilizan desde la memoria de cuota de partición. Anteriormente, las conexiones se contabilizaban desde la memoria de cuota de partición predeterminada. Se configura solo en el lado del cliente, no en las conexiones TCP del servidor back-end. No se pueden establecer nuevas conexiones más allá de este valor configurado.

> **Nota**
>
> A partir de NetScaler 12.0, puede crear una partición con el número de conexiones abiertas establecido en Cero. Si ya ha creado una partición con un número específico de conexiones abiertas, puede reducir el límite de conexión o establecer el límite como Cero.

Parámetro: MaxConnections

Número máximo de conexiones simultáneas que se pueden abrir en la partición. Un valor cero indica que no hay límite en el número de conexiones abiertas.

Valor predeterminado: 1024

Valor mínimo: 0

Valor máximo: 42949672,95

Configurar una partición de administrador

Para configurar una partición de administrador, complete las siguientes tareas.

Para acceder en una partición de administrador mediante la CLI

1. Inicie sesión en el dispositivo Citrix ADC.
2. Comprueba si estás en la partición correcta. El símbolo del sistema muestra el nombre de la partición seleccionada actualmente.
3. En caso afirmativo, vaya al siguiente paso.
4. En caso negativo, obtenga una lista de las particiones con las que está asociado y cambie a la partición adecuada.
   - `show system user <username>`
   - **`switch`** `ns partition <partitionName>`
5. Ahora, puede realizar las configuraciones necesarias al igual que un Citrix ADC no particionado.

Para acceder a una partición de administrador mediante la GUI

1. Inicie sesión en el dispositivo Citrix ADC.
2. Comprueba si estás en la partición correcta. La barra superior de la GUI muestra el nombre de la partición seleccionada actualmente.
   - En caso afirmativo, vaya al siguiente paso.

- En caso negativo, vaya a **Configuración > Sistema > Administración de particiones > Particiones**, haga clic con el botón derecho en la partición a la que desea cambiar y seleccione **Cambiar**.

3. Ahora, puede realizar las configuraciones necesarias al igual que un Citrix ADC no particionado.

Agregar una partición de administrador

El administrador raíz agrega una partición administrativa desde la partición predeterminada y vincula la partición con la VLAN 2.

Para crear una partición administrativa mediante la CLI

En el símbolo del sistema, escriba:

```
1 add partition <partitionname>
```

Cambiar el acceso de usuario de la partición predeterminada a una partición de administrador

Ahora puede cambiar el acceso de usuario de la partición predeterminada a la partición Par1.

Para cambiar una cuenta de usuario de una partición predeterminada a una partición de administrador mediante la CLI:

En el símbolo del sistema, escriba:

```
1 Switch ns partition <pname>
```

Agregar dirección SNIP a una cuenta de usuario de partición con acceso de administración habilitado

En la partición, cree una dirección SNIP con el acceso de administración habilitado.

Para agregar una dirección SNIP a la cuenta de usuario de partición con acceso de administración habilitado mediante la interfaz de línea de comandos:

En el símbolo del sistema, escriba:

```
> add ns ip <ip address> <subnet mask> -mgmtAccess enabled
```


Crear y vincular un usuario de partición con la directiva de comandos de partición

En la partición, cree un usuario del sistema de particiones y vincule al usuario con políticas de comandos partition-admin.

Para crear y enlazar un usuario del sistema de particiones con la directiva de comandos de partición mediante la CLI:

En el símbolo del sistema, escriba:

```
> add system user <username> <password>

Done
```

Creación y vinculación de grupos de usuarios de particiones con directiva de comandos de partición

En Partition Par1, cree un grupo de usuarios del sistema de particiones y vincule el grupo con una política de comandos de partición, como administrador de particiones, solo lectura de particiones, operador de partición o red de particiones.

Para crear y enlazar un grupo de usuarios de partición con la directiva de comandos de partición mediante la interfaz de línea de comandos:

```
1 > add system group <groupName>
2 > bind system group <groupname> (-userName | -policyName <cmdpolicy> <
     priority> | -partitionName)
```

Configuración de la autenticación del servidor externo para usuarios externos

En la partición Par1, puede configurar una autenticación de servidor externo para autenticar a los usuarios TACACS externos que accedan a la partición a través de una dirección SNIP.

Para configurar la autenticación de servidor externo para usuarios externos mediante la interfaz de línea de comandos:

En el símbolo del sistema, escriba:

```
1 > add authentication tacacsaction <name> -serverip <IP> -tacacsSecret <
     secret key> -authorization ON -accounting ON
2 > add authentication policy <policname> -rule true -action <name>
3 > bind system global <policyname> -priority <value>1
```


Configurar una cuenta de usuario del sistema de particiones en una partición mediante la GUI

Para configurar una cuenta de usuario de partición en una partición administrativa, debe crear un usuario de partición o un grupo de usuarios de particiones y vincularlo a las directivas de comandos de partición. Además, puede configurar la autenticación del servidor externo para un usuario externo.

Para crear una cuenta de usuario de partición en una partición mediante la GUI

Vaya a **Sistema > Administración**de **usuarios, haga clic en Usuarios** para agregar un usuario del sistema de particiones y vincular al usuario a las políticas de comandos (partitionadmin/partition-only/partition-operator/partition-network).

Para crear una cuenta de grupo de usuarios de particiones en una partición mediante la GUI

Vaya a **Sistema > Administración de usuarios**, haga clic en **Grupos** para agregar un grupo de usuarios del sistema de particiones y vincular el grupo de usuarios a las políticas de comandos (partitionadmin/partition-only/partition-operator/partition-network).

Para configurar la autenticación de servidor externo para usuarios externos mediante la GUI

Vaya a **Sistema > Autenticación > Acciones básicas** y haga clic en **TACACS** para configurar un servidor TACACS para autenticar a los usuarios externos que acceden a la partición.

Configuración de ejemplo

La siguiente configuración muestra cómo crear un usuario de partición o un grupo de usuarios de particiones y vincularlo a las directivas de comandos de partición. Además, cómo configurar la autenticación del servidor externo para autenticar a un usuario externo.

```
1  > add partition Par1
2  > switch ns partition Par1
3  > add ns ip 10.102.29.203 255.255.255.0 -mgmtAccessenabled
4  > add system user John Password
5  > bind system user Jane partition-read-only -priority 1
6  > add system group Retail
7  > bind system group Retail -policyname partition-network 1 (where 1 is
       the priority number)
8  > bind system group Retail  - username Jane
9  > add authentication tacacssaction tacuser  - serverip 10.102.29.200  -
       tacacsSecret Password  - authorization ON  - accounting ON
10 > add authentication policy polname  - rule true  - action tacacsAction
```



```
11  > bind system global polname  -priority 1
```

Directivas de comandos para usuarios de particiones y grupos de usuarios de particiones en partición administrativa

Comandos para autorizar una cuenta de usuario dentro de una partición administrativa	Directivas de comandos disponibles dentro de una partición administrativa (políticas integradas)	Tipo de acceso a cuenta de usuario
agregar usuario del sistema	Administrador de particiones	SNIP (con acceso de administración habilitado)
agregar grupo de sistemas	Red de particiones	SNIP (con acceso de administración habilitado)
agregar autenticación <action, policy>, enlazar sistema global <policy name>	Partición de sólo lectura	SNIP (con acceso de administración habilitado)
quitar usuario del sistema	Administrador de particiones	SNIP (con acceso de administración habilitado)
quitar grupo de sistemas	Administrador de particiones	SNIP (con acceso de administración habilitado)
bind system cmdpolicy al usuario del sistema; bind system cmdpolicy al grupo de sistemas	Administrador de particiones	SNIP (con acceso de administración habilitado)

Configurar un canal Ethernet LACP en la partición administrativa predeterminada

Con el Protocolo de control de agregación de enlaces (LACP), puede combinar varios puertos en un único enlace de alta velocidad (también denominado canal). Un dispositivo habilitado para LACP intercambia unidades de datos LACP (LACPDU) a través del canal.

Hay tres modos de configuración de LACP que puede habilitar en la partición predeterminada de un dispositivo Citrix ADC:

1. Activo. Un puerto en modo activo envía LACPDU. La agregación de enlaces se forma si el otro extremo del enlace Ethernet está en modo activo o pasivo LACP.
2. pasiva. Un puerto en modo pasivo envía LACPDU solo cuando recibe LACPDU. La agregación de

enlaces se forma si el otro extremo del enlace Ethernet está en modo activo LACP.

3. Inhabilitar: No se forma la agregación de enlaces.

> **Nota**
>
> De forma predeterminada, la agregación de vínculos está deshabilitada en la partición predeterminada del dispositivo.

LACP intercambia LACPDU entre dispositivos conectados mediante un enlace Ethernet. Estos dispositivos suelen denominarse actor o socio.

Una unidad de datos LACPDU contiene los siguientes parámetros:

- Modo LACP. Activo, pasivo o deshabilitado.
- Tiempo de espera de LACP. El período de espera antes de que se agote el tiempo de espera del compañero o actor. Valores posibles: Largo y Corto. Predeterminado: Long.
- Llave de puerto. Distinguir entre los diferentes canales. Cuando la clave es 1, se crea LA/1. Cuando la clave es 2, se crea LA/2. Valores posibles: Entero del 1 al 8. 4 a 8 es para CLAG de clúster.
- Prioridad de puerto. Valor mínimo: 1. Valor máximo: 65535. Predeterminado: 32768.
- Prioridad del sistema. Utiliza esta prioridad junto con el MAC del sistema para formar el ID del sistema para identificar de forma exclusiva el sistema durante la negociación de LACP con el socio. Establece la prioridad del sistema entre 1 y 65535. El valor predeterminado se establece en 32768.
- Interfaz. Admite 8 interfaces por canal en el dispositivo NetScaler 10.1 y admite 16 interfaces por canal en dispositivos NetScaler 10.5 y 11.0.

Después de intercambiar LACPDU, el actor y el socio negocian la configuración y deciden si agregan los puertos a la agregación.

Configurar y verificar LACP

En la siguiente sección se muestra cómo configurar y verificar LACP en la partición de administración.

Para configurar y verificar LACP en un dispositivo Citrix ADC mediante la CLI

1. Habilite LACP en cada interfaz.

   ```
   set interface <Interface_ID> -lacpMode PASSIVE -lacpKey 1<!--NeedCopy
   -->
   ```

   Cuando habilita LACP en una interfaz, los canales se crean dinámicamente. Además, cuando habilita LACP en una interfaz y configura LACPKey en 1, la interfaz se enlaza automáticamente al canal LA/1.

> **Nota**
>
> Cuando vincula una interfaz a un canal, los parámetros del canal tienen prioridad sobre los parámetros de la interfaz, por lo que se ignoran los parámetros de la interfaz. Si LACP crea un canal dinámicamente, no puede realizar las operaciones de adición, enlace, desvinculación o eliminación del canal. Un canal creado dinámicamente por LACP se elimina automáticamente cuando deshabilita LACP en todas las interfaces del canal.

2. Establezca la prioridad del sistema.

   ```
   set lacp -sysPriority <Positive_Integer><!--NeedCopy-->
   ```

3. Compruebe que LACP funciona según lo esperado.

   "'show interface

   ```
   1 ```show channel<!--NeedCopy-->
   ```

   ```
   show LACP<!--NeedCopy-->
   ```

   > **Nota**
   >
   > En algunas versiones del Cisco Internetwork Operating System (iOS), la ejecución del <VLAN_ID>comando switchport trunk native VLAN hace que el switch de Cisco etiquete las PDU LACP. Hace que falle el canal LACP entre el conmutador Cisco y el dispositivo Citrix ADC. Sin embargo, este problema no afecta a los canales de agregación de enlaces estáticos configurados en el procedimiento anterior.

Guardar la configuración de todas las particiones de administrador de la partición predeterminada

Los administradores pueden guardar la configuración de todas las particiones de administrador a la vez desde la partición predeterminada.

Guardar todas las particiones de administrador de la partición predeterminada mediante la CLI

En el símbolo del sistema, escriba:

```
save ns config -all
```

Compatibilidad con informes personalizados basados en particiones y clústeres

La GUI de Citrix ADC muestra solo los informes personalizados creados en la partición de visualización actual o en el clúster.

Anteriormente, la GUI de Citrix ADC se utilizaba para almacenar los nombres de los informes personalizados directamente en el archivo back-end sin mencionar el nombre de la partición o el clúster para diferenciarlo.

Para ver los informes personalizados de la partición o clúster actuales en la GUI

- Vaya a la pestaña **Informes** .
- Haga clic en **Informes personalizados** para ver los informes creados en la partición actual o en el clúster.

Compatibilidad para vincular certificados globales de VPN en una configuración particionada para IdP de OAuth

En una configuración particionada, ahora puede vincular los certificados a VPN global para implementaciones de IdP de OAuth.

Para enlazar los certificados en Configuración particionada mediante la CLI

En el símbolo del sistema, escriba:

```
1 bind vpn global [-certkeyName <string>] [-userDataEncryptionKey <string
     >]
```

Configuración de VLAN para particiones de administración

January 31, 2022

Las VLAN se pueden enlazar a una partición como una VLAN “dedicada” o una VLAN “compartida”. Según su implementación, puede enlazar una VLAN a una partición para aislar su tráfico de red de otras particiones.

VLAN dedicada : una VLAN enlazada solo a una partición con la opción “Compartir” inhabilitada y debe ser una VLAN etiquetada. Por ejemplo, en una implementación cliente-servidor, por razones de seguridad, un administrador del sistema crea una VLAN dedicada para cada partición del lado del servidor.

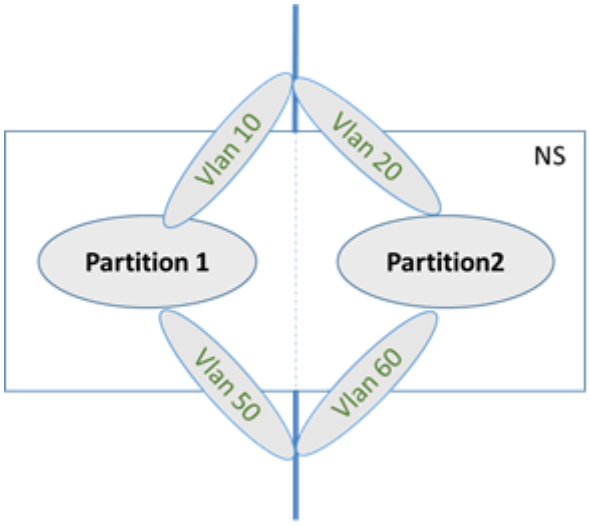
VLAN compartida: VLAN enlazada (compartida en) a varias particiones con la opción “Compartir” habilitada. Por ejemplo, en una implementación cliente-servidor, si el administrador del sistema no tiene control sobre la red del lado del cliente, se crea una VLAN y se comparte en varias particiones.

La VLAN compartida se puede utilizar en varias particiones. Se crea en la partición predeterminada y puede enlazar una VLAN compartida a varias particiones. De forma predeterminada, una VLAN compartida está vinculada implícitamente a la partición predeterminada y, por lo tanto, no se puede enlazar explícitamente.

> **Nota**
>
> - Un dispositivo Citrix ADC implementado en cualquier plataforma de hipervisor (ESX, KVM, Xen e Hyper-V) debe cumplir las condiciones siguientes en una configuración de partición y dominio de tráfico:
>   - Enable the promiscuous mode, MAC changes, MAC spoofing, or forged transmit for shared VLANs with partition.
>   - Enable the VLAN with port group properties of the virtual switch, if the traffic is through a dedicated VLAN.
> - En un dispositivo Citrix ADC con particiones (multiarrendatario), un administrador del sistema puede aislar el tráfico que fluye a una partición o particiones concretas. Se realiza vinculando una o más VLAN a cada partición. Una VLAN se puede dedicar a una partición o Compartida a través de varias particiones.

VLAN dedicadas

Para aislar el tráfico que fluye hacia una partición, cree una VLAN y asócielo a la partición. La VLAN es visible solo para la partición asociada y el tráfico que fluye a través de la VLAN se clasifica y procesa solo en la partición asociada.



Para implementar una VLAN dedicada para una partición concreta, haga lo siguiente.

1. Agregue una VLAN (V1).
2. Enlazar una interfaz de red a la VLAN como interfaz de red etiquetada.

3. Crea una partición (P1).
4. Enlazar partición (P1) a la VLAN dedicada (V1).

Configure lo siguiente mediante la CLI

- Crear una VLAN

  ```
  add vlan <id>
  ```

Ejemplo

```
1     add vlan 100
```

- Vincular una VLAN

  ```
  bind vlan <id> -ifnum <interface> -tagged
  ```

Ejemplo

```
1     bind vlan 100  - ifnum 1/8 -tagged
```

- Crear una partición

  ```
  Add ns partition <partition name> [-maxBandwidth <positive_integer>][-
  maxConn <positive_integer>] [-maxMemLimit <positive_integer>]
  ```

Ejemplo

```
1     Add ns partition P1  - maxBandwidth 200  - maxconn 50  - maxmemlimit
         90
2
3     Done
```

- Enlazar una partición a una VLAN

  ```
  bind partition <partition-id> -vlan <id>
  ```

Ejemplo

```
1     bind partition P1  - vlan 100
```


Configurar una VLAN dedicada mediante la GUI de Citrix ADC

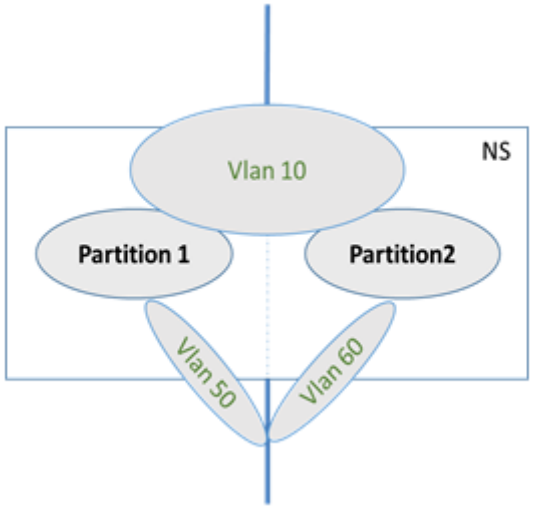
1. Vaya a **Configuración > Sistema > Red > VLAN*** y haga clic en **Agregar** para crear una VLAN.
2. En la página **Crear VLAN**, defina los siguientes parámetros:
   - ID DE VLAN
   - Alias
   - Unidad de transmisión máxima
   - Redirección dinámica
   - Redirección dinámica IPv6
   - Uso compartido de particiones
3. En la sección **Enlaces de interfaz**, seleccione una o más interfaces y enlácelas a la VLAN.
4. En la sección **Enlaces IP**, seleccione una o más direcciones IP y enlácelas a la VLAN.
5. Haga clic en **Aceptar** y **Listo**.

VLAN compartida

En una configuración de VLAN compartida, cada partición tiene una dirección MAC y el tráfico recibido en la VLAN compartida se clasifica por dirección MAC. Solo se recomienda una VLAN de capa 3 porque puede restringir el tráfico de subred. Una dirección MAC de partición es aplicable e importante solo para una implementación de VLAN compartida.

> **Nota**
>
> A partir de Citrix ADC versión 12.1 compilación 51.16, la VLAN compartida en un dispositivo con particiones admite el protocolo de redirección dinámica.

El siguiente diagrama muestra cómo se comparte una VLAN (VLAN 10) en dos particiones.



Para implementar una configuración de VLAN compartida, haga lo siguiente:

1. Cree una VLAN con la opción de compartir “habilitada” o habilite la opción de compartir en una VLAN existente. Por defecto, la opción está “inhabilitada”.
2. Enlazar la interfaz de partición a la VLAN compartida.
3. Crea las particiones, cada una con su propia dirección PartitionMac.
4. Enlazar las particiones a la VLAN compartida.

Configurar una VLAN compartida mediante la CLI

En el símbolo del sistema, escriba uno de los siguientes comandos para agregar VLAN o establezca el parámetro de uso compartido de una VLAN existente:

```
add vlan <id> [-sharing (ENABLED | DISABLED)]

set vlan <id> [-sharing (ENABLED | DISABLED)]

add vlan 100  -sharing ENABLED

set vlan 100  -sharing ENABLED
```

Enlazar una partición a una VLAN compartida mediante la CLI

En el símbolo del sistema, escriba:

```
bind partition <partition-id> -vlan <id>

bind partition P1  -vlan 100

add ns partition P1  -maxBandwidth 200  -maxconn 50    -maxmemlimit 90
    -partitionMAC<mac_addr

Done
```

Configurar una dirección MAC de partición mediante la CLI

```
set ns partition <partition name> [-partitionMAC<mac_addr>]

set ns partition P1  -partitionMAC 22:33:44:55:66:77
```


Vincular particiones a una VLAN compartida mediante la CLI

```
bind partition <partition-id> -vlan <id>

bind partition <partition-id> -vlan <id>

bind partition P1  - vlan 100

bind partition P2  - vlan 100

bind partition P3  - vlan 100

bind partition P4  - vlan 100
```

Configurar VLAN compartida mediante la GUI de Citrix ADC

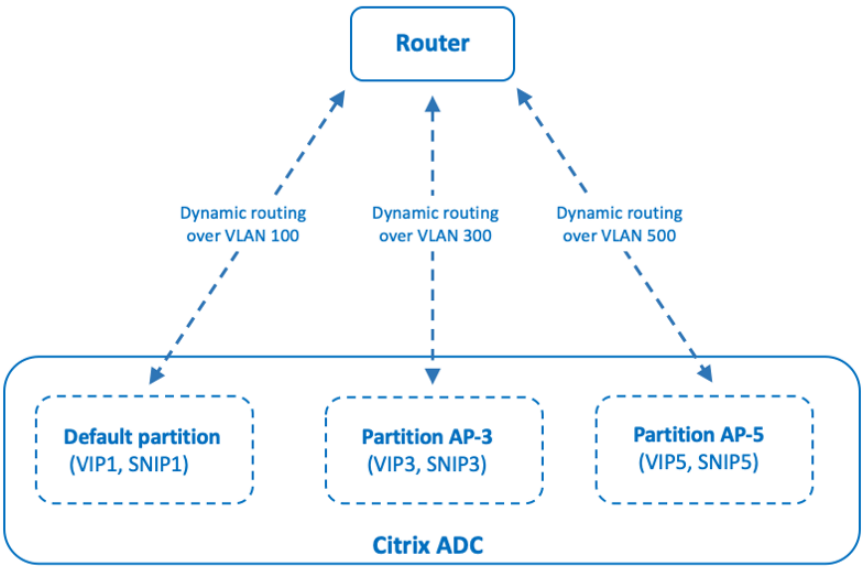
1. Vaya a **Configuración > Sistema > Red > VLAN** y, a continuación, seleccione un perfil de **VLAN** y haga clic en **Modificar** para establecer el parámetro de compartición de particiones.
2. En la página **Crear VLAN**, seleccione la casilla de verificación **Compartir particiones** .
3. Haga clic en **Aceptar** y, a continuación, **Listo**.

Redirección dinámica a través de una VLAN compartida entre particiones de administración

Las particiones de administración de un dispositivo Citrix ADC proporcionan una forma de alojar a varios arrendatarios.

A partir de la versión 12.1 de Citrix ADC, compilación 51.16, una VLAN compartida en un dispositivo con particiones admite el protocolo de redirección dinámica. La redirección se puede configurar en VLAN dedicadas o compartidas asociadas con particiones administrativas.

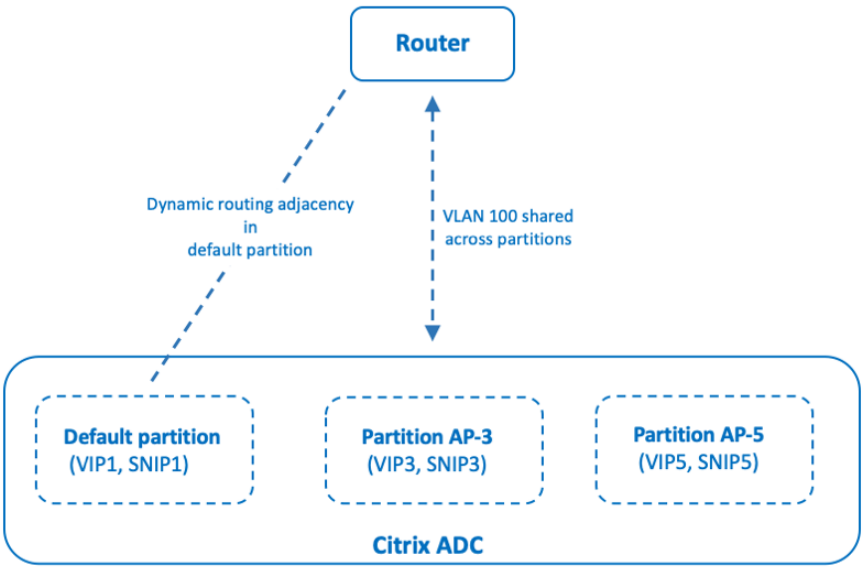
VLAN dedicada de una partición de administración. En una VLAN dedicada, la ruta de datos del arrendatario se identifica mediante una o más VLAN. El resultado es una configuración estricta y un aislamiento de rutas de datos para el arrendatario. Para anunciar el estado de una dirección VIP, la redirección dinámica está habilitado en cada partición y la adyacencia de redirección se establece por partición.



Dynamic routing over a dedicated VLAN per partition

Una VLAN compartida entre particiones de administración. En una VLAN compartida, las direcciones VIP configuradas en una partición no predeterminada se pueden anunciar mediante una única adyacencia o interconexión formada en la partición predeterminada. Se utiliza una dirección SNIP en la partición no predeterminada como siguiente salto para todas las direcciones VIP (configuradas con la opción **AdvertiseOnDefaultPartition**) de esa partición no predeterminada. La dirección SNIP configurada se marca como una dirección IP de salto siguiente en los anuncios de redirección.

Considere un ejemplo de configuración de particiones de administración en un dispositivo Citrix ADC, la VLAN 100 se comparte en la partición predeterminada y en particiones no predeterminadas: AP-3 y AP-5. Las direcciones SNIP SNIP1 se agregan en la partición predeterminada, SNIP3 se agrega en AP-3 y SNIP5 en AP-5. Se puede acceder a SNIP1, SNIP3 y SNIP5 a través de la vlan-100. Las direcciones VIP VIP1 se agregan en la partición predeterminada, VIP3 se agrega en AP-3 y VIP5 en AP-5. VIP3 y VIP5 se anuncian mediante la adyacencia única o el peering formado en la partición predeterminada.



Dynamic routing over a shared VLAN across partitions

Antes de comenzar

Antes de configurar el redirección dinámica a través de una VLAN compartida en una partición de administración no predeterminada, asegúrese de que:

- **El redirección dinámica se configura en la VLAN compartida en la partición predeterminada**. La configuración del redirección dinámica en la VLAN compartida en la partición predeterminada consta de los siguientes pasos:
  1. Habilite el redirección dinámica en la VLAN compartida.
  2. Agregar una dirección IP de SNIP con redirección dinámica habilitado. Esta dirección IP de SNIP se utiliza para redirección dinámica con el flujo ascendente.
  3. Enlazar la subred IP SNIP a la VLAN compartida.
- **Uno o varios protocolos de redirección dinámica se configuran en la partición predeterminada**. Para obtener más información, consulte Configuración de protocolos de redirección dinámica.

Pasos de configuración

La configuración del redirección dinámica a través de una VLAN compartida en una partición de administración no predeterminada consta de los siguientes pasos:

1. **Agregue una dirección IP SNIP en la partición no predeterminada**. Esta dirección IP del SNIP debe estar en la misma subred de la dirección IP del SNIP que se utiliza para el redirección dinámica en la partición predeterminada.

2. **Establezca o habilite los siguientes parámetros para anunciar una dirección VIP, en una partición no predeterminada, mediante redirección dinámica**.
    - Puerta de enlace de ruta de host (HostRTGW). Establezca este parámetro en la dirección SNIP agregada en el paso anterior.
    - Publicidad en la partición predeterminada (AdvertiseOnDefaultPartition). Active este parámetro.

Configuración de ejemplo

Considere un ejemplo de configuración de una partición de administración en un dispositivo Citrix ADC. En este dispositivo se ha configurado una partición de administración no predeterminada AP-3. Una VLAN100 de VLAN compartida está vinculada a AP-3. La siguiente configuración de ejemplo configura el redirección dinámica, a través de VLAN100, en AP-3.

Pasos	Configuración de ejemplo
En la partición de administración predeterminada	-
Habilite el redirección dinámica en la VLAN 100 compartida.	`set vlan 100 -dynamicRouting enabled`
Agregar dirección IP SNIP 192.0.2.10 con redirección dinámica habilitado.Esta dirección IP SNIP se utiliza para la redirección dinámica con la dirección ascendente.	`add ns ip 192.0.2.10 255.255.255.0 -type SNIP -dynamicRouting enabled`
Enlazar la subred de 192.0.2.10 a la VLAN 100 compartida.	`bind vlan 100 -IPAddress 192.0.2.10 255.255.255.0`
En la partición de administración no predeterminada AP-3	-
Agregar la dirección IP del SNIP 192.0.2.30. Esta dirección IP del SNIP se encuentra en la misma subred que la dirección IP del SNIP 192.0.2.10 en la partición predeterminada.	`add ns ip 192.0.2.30 255.255.255.0 -type SNIP`
Para publicidad de la dirección VIP 203.0.113.300 mediante redirección dinámica, habilite el parámetro `advertiseOnDefaultPartition` y establezca el parámetro `hostRtGw` en 192.0.2.30.	`set ns ip 203.0.113.300 255.255.255.255 -hostRoute enabled -advertiseOnDefaultPartition enabled -hostRtGw 192.0.2.30`

Redirección dinámica de IPv6 a través de una VLAN compartida en la partición de administración

Los comandos `enable ns feature IPv6PT` y `set L3Param -ipv6DynamicRouting ENABLED` deben estar habilitados para que una dirección IPv6 se redirija dinámicamente a través de una VLAN compartida en una partición de administración. Las siguientes configuraciones de ejemplo le ayudan a configurar el redirección dinámica de IPv6 a través de VLAN compartida.

Configuración de ejemplo

La siguiente configuración de ejemplo configura el redirección dinámica, a través de VLAN 100, en AP-3.

Pasos	Configuración de ejemplo
En la partición de administración predeterminada	-
Habilite el redirección dinámica en la VLAN 100 compartida.	`set vlan 100 -dynamicRouting enabled`
Agregue la dirección IP SNIP 2001:b:c:d 1/64 con el redirección dinámica habilitado.La dirección IP SNIP se utiliza para el redirección dinámica con el flujo ascendente.	`add ns ip6 2001:b:c:d::1/64 -type SNIP -dynamicRouting enabled`
Enlazar subred de 2001:b:c:d 1/64 a la VLAN 100 compartida.	`bind vlan 100 -IPAddress 2001:b:c:d::1/64`
En la partición de administración no predeterminada AP-3	-
Agregue la dirección IP SNIP 2001:b:c:d 2/64. Esta dirección IP SNIP se encuentra en la misma subred que la dirección IP SNIP 2001:b:c:d 2/64 en la partición predeterminada.	`add ns ip6 2001:b:c:d::2/64 -type SNIP`
Para publicidad de la dirección VIP 2002 1/128 mediante redirección dinámica, habilite el parámetro `advertiseOnDefaultPartition` y establezca el parámetro `ip6hostRtGw` en 2001:b:c:d 2.	`set ns ip6 2002::1/128 -hostRoute enabled -advertiseOnDefaultPartition enabled -ip6hostRtGw 2001:b:c:d::2`

El VIP presente en la partición de administración debe verse en VTYSH de la partición predeterminada

como una ruta del núcleo.

```
> switch partition default
Done

>vtysh
ns#

ns# sh ipv6 route kernel

IPv6 routing table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
   IA - OSPF inter area, E1 - OSPF external type 1,
   E2 - OSPF external type 2, I - IS-IS, B - BGP
Timers: Uptime

K      2002::1/128 via 2001:b:c:d::2, vlan0, 01:24:15
                                >> on Default Partition, VIP : 2002::1
   present in AP known via SNIP6 : 2001:b:c:d::2 is present in AP as a
   Kernel Route
```

Se puede anunciar hacia arriba mediante la opción “redistribuir kernel” en OSPFv3/BGP+ en la partición predeterminada.

```
ns# sh run router ipv6 ospf
!
router ipv6 ospf 1
redistribute kernel
!
```

VLAN compartida con partición de administración en el dispositivo Citrix ADC SDX

En el dispositivo SDX, debe generar y configurar la dirección PMAC mediante la interfaz de usuario de Management Service antes de utilizar las particiones de administración con VLAN compartidas. Management Service le permite generar direcciones MAC de partición mediante:

- Uso de una dirección MAC base
- Especificación de direcciones MAC personalizadas
- Generación aleatoria de direcciones MAC

Nota

- Las direcciones MAC generadas aleatoriamente se utilizan para otras implementaciones distintas de la alta disponibilidad.
- Después de generar las direcciones MAC de la partición, debe reiniciar la instancia de Citrix ADC antes de configurar las particiones admin. Para obtener más información sobre la generación de direcciones MAC de particiones desde el dispositivo SDX, consulte Generación de direcciones MAC de particiones para configurar la partición de administración en una instancia Citrix ADC en el dispositivo SDX.

Compatibilidad con VXLAN para particiones de administración

August 20, 2021

En un dispositivo Citrix ADC con particiones, similar a la configuración de una VLAN, puede configurar una VXLAN en la partición predeterminada. Después de configurar una VXLAN, puede enlazarla a una partición administrativa o, si una VXLAN extiende una VLAN enlazada a una partición, el dispositivo enlaza la VXLAN a la partición en el mismo dominio de difusión. Es aplicable en la desvinculación de una VLAN que desvincula una VXLAN de la partición.

Para obtener más información sobre cómo funciona VXLAN en un dispositivo Citrix ADC, consulte VXLAN.

Además, para obtener más información sobre cómo funciona la VLAN en un dispositivo Citrix ADC con particiones, consulte Partición de administración.

Puntos a recordar antes de configurar una VXLAN

Recuerde los siguientes puntos antes de configurar una VXLAN en un dispositivo Citrix ADC con particiones:

- Cuando extienda una VLAN a través de VXLAN, asegúrese de que VLAN está enlazada a la partición.
- Solo un administrador de particiones debe configurar el IP y el redirección dinámica para VXAN en la partición administrativa.

No se admite una VXLAN compartida en un dispositivo con particiones, por lo que no se puede etiquetar una VXLAN a una VLAN compartida o no se puede convertir una VLAN compartida cuando se etiqueta a una VXLAN.

Configuraciones VXLAN compatibles

A continuación se presentan las configuraciones VXLAN compatibles.

Extender la VLAN a través de una VXLAN en el mismo dominio de difusión

Los siguientes pasos de CLI le ayudan a extender una VLAN a través de una VXLAN y de la manera opuesta dentro del mismo dominio de difusión.

1. Agregar una VLAN en la partición predeterminada

```
1  add vlan <id>
```

2. Exalmacén la VLAN sobre una VXLAN dentro del mismo dominio de difusión.

```
1 add vxlan <vxlan id>  - vlan <id>
```

3. Configure un par `vtep` para transportar todo el tráfico BUM (difusión de multidifusión desconocida).

> **Nota**
>
> La `vtep` dirección puede ser una dirección de multidifusión.

```
1 add bridgetable -mac <mac_addr> -vxlan <positive_integer> -vtep <
     ip_addr> [-vni <positive_integer>][-deviceVlan <
     positive_integer>]
```

4. Enlazar direcciones IP a VXLAN.

```
1 bind vxlan <id> [-srcIP <ip_addr>][-IPAddress <ip_addr|ipv6_addr
     |*> [<netmask>]]
```

5. Enlazar VLAN a una partición administrativa.

```
1 bind partition <partition-id> -vxlan <id>
2
3 add vlan 3000
4
```



```
add vxlan 3000  -vlan 10

add bridgetable  -mac 00:00:00:00:00:00  -vxlan 3000 -vtep
    10.102.58.8  -vni 11

bind vxlan 3000  -  srcIP 10.102.101.15

bind partition p1  -vlan 10
```

Compatibilidad con SNMP para particiones de administración

January 12, 2021

Un dispositivo Citrix ADC con particiones utiliza la infraestructura SNMP para limitar la velocidad de partición y supervisar los detalles de utilización de recursos de partición.

Trampas SNMP para límite de velocidad de partición de administración

En un dispositivo Citrix ADC con particiones, una alarma PARTITION-RATE-LIMIT puede generar nueve capturas SNMP para notificar que un recurso de partición (como ancho de banda, conexión o memoria) ha alcanzado su límite o ha vuelto a la normalidad.

Las nueve capturas SNMP siguientes se generan cuando:

- **partitionCONNThresholdReached**. El número de conexiones activas de una partición supera su porcentaje de umbral alto.
- **partitionCONNThresholdNormal**. El número de conexiones activas es menor o igual que el porcentaje de umbral normal.
- **partitionBWThresholdReached**. El uso de ancho de banda de la partición alcanza su porcentaje de umbral alto.
- **partitionMEMThresholdReached**. El uso actual de memoria de la partición supera su porcentaje de umbral alto.
- **partitionMEMThresholdNormal**. El uso actual de memoria de la partición es menor o igual que el porcentaje de umbral normal.
- **partitionMEMLimitExceeded.** El uso actual de memoria de la partición supera su porcentaje límite de memoria.
- **partitionCONNLimitExceeded**. El número de conexiones activas para una partición supera el límite configurado y se están descartando nuevas conexiones.
- **partitionCONNLimitNormal**. El número de conexiones activas para una partición va por debajo de su límite configurado y la partición ahora puede aceptar una nueva conexión.

- **partitionBWLimitExceeded**. El uso actual de ancho de banda para una partición ha superado el límite configurado.

Los valores de umbral para las capturas SNMP no son configurables y son los siguientes:

- Umbral alto = 80% (aplicable a todas las trampas límite de velocidad de partición)
- Umbral bajo = 60% (aplicable a todas las trampas límite de tasa de partición)
- Límite de memoria = 95% (aplicable solo para capturas de memoria de partición)

Configuración de la alarma PARTITION-RATE-LIMIT

Para configurar la alarma PARTITION-RATE-LIMIT en una partición específica y habilitar la generación de mensajes de captura SNMP.

1. Activar la alarma PARTITION-RATE-LIMIT
2. Configurar la alarma PARTITION-RATE-LIMIT
3. Configurar el destino de captura SNMP

Para habilitar la alarma PARTITION-RATE-LIMIT mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos:

```
enable snmp alarm PARTITION-RATE-LIMIT

show snmp alarm PARTITION-RATE-LIMIT
```

Para configurar la alarma de PARTICIÓN-RATE-LIMIT mediante la CLI

En el símbolo del sistema, escriba el siguiente comando:

```
set snmp alarm PARTITION-RATE-LIMIT [-state ( ENABLED | DISABLED )] [-
    severity <severity>] [-logging ( ENABLED | DISABLED )]
```

Para configurar el destino de captura SNMP mediante la CLI

En el símbolo del sistema, escriba el siguiente comando:


```
add snmp trap <trapClass> <trapDestination> [-version <version>] [-td <
    positive_integer>] [-destPort <port>] [-communityName <string>] [-
    srcIP <ip_addr|ipv6_addr>] [-severity <severity>] [-allPartitions (
    ENABLED | DISABLED )]
```

Para configurar la alarma de límite de índice de partición mediante la interfaz gráfica de usuario

Vaya a **Sistema > SNMP > Alarmas**, seleccione **PARTICIÓN-RATE-LIMIT** alarm y configure los parámetros de alarma.

Para configurar el destino de captura SNMP mediante la GUI

Vaya a **Sistema > SNMP > Trap**, especifique la dirección IP del dispositivo de destino.

Supervisión SNMP para la utilización de recursos de partición

Con SNMP, puede supervisar los detalles de utilización de los recursos de una partición (como ancho de banda, conexión y memoria) en tiempo real en un dispositivo Citrix ADC. Se realiza enviando una solicitud SNMP (como SNMP GET, SNMP GET BULK, SNMP GETNEXT o SNMP WALK) desde el Administrador SNMP.

> **Nota**
>
> Para supervisar los recursos de partición, debe configurar la comunidad SNMP en la partición predeterminada. En este caso, *PartitionTable* se mantiene en la partición predeterminada y la comunicación SNMP se realiza a través de la dirección NSIP del dispositivo.

Considere un caso en el que un administrador de Citrix ADC quiera conocer el uso del ancho de banda de la partición P1 en el dispositivo. SNMP Manager recupera esta información enviando una solicitud SNMP GET en el OID (PartitionCurrentBandwidth) correspondiente a la dirección NSIP del dispositivo. El agente SNMP de la partición predeterminada recupera y envía el uso de ancho de banda actual de P1 al Administrador SNMP a través de la dirección NSIP.

En la siguiente tabla se enumeran los contadores SNMP que forman parte de *PartitionTable* y su descripción:

Parámetro SNMP	SNMP OID	Descripción
partitionName	1.3.6.1.4.1.5951.4.1.1.88.1.1	Nombre de partición
partitionCurrentBandwidth	1.3.6.1.4.1.5951.4.1.1.88.1.2	Uso actual del ancho de banda de la partición.

Parámetro SNMP	SNMP OID	Descripción
partitionCurrentConnections	1.3.6.1.4.1.5951.4.1.1.88.1.3	Número actual de conexiones activas de la partición.
partitionMemoryUsagePcnt	1.3.6.1.4.1.5951.4.1.1.88.1.4	Uso actual de la memoria (en porcentaje) de la partición.

Compatibilidad con registros de auditoría para particiones de administración

August 20, 2021

En un dispositivo Citrix ADC con particiones, para mejorar la seguridad de los datos, puede configurar el registro de auditoría en una partición administrativa mediante directivas avanzadas. Por ejemplo, es posible que quiera ver los registros (estados e información de estado) de una partición específica. Tiene varios usuarios accediendo a diferentes conjuntos de funciones en función de sus niveles de autorización en la partición.

Puntos que tener en cuenta

1. Los registros de auditoría generados a partir de la partición se almacenan como un único archivo de registro (/var/log/ns.log).
2. Configure la dirección de subred del servidor de registro de auditoría (syslog o ns log) como la dirección IP de origen en la partición para enviar los mensajes de registro de auditoría.
3. La partición predeterminada utiliza el NSIP como dirección IP de origen para los mensajes de registro de auditoría de forma predeterminada.
4. Puede mostrar el mensaje audit-log mediante el comando “show audit messages”.

Para obtener información sobre la configuración del registro de auditoría, consulte Configuración de NetScaler Appliance for Audit Logging.

Configurar el registro de auditoría en el dispositivo Citrix ADC con particiones

Complete las siguientes tareas para configurar el registro de auditoría en una partición administrativa.

1. Configurar la dirección IP de la subred de partición. Dirección SNIP IPv4 de una partición administrativa.

2. Configurar la acción de registro de auditoría (registro syslog y ns). Una acción de auditoría es un conjunto de información que especifica los mensajes que se van a registrar y cómo registrar los mensajes en el servidor de registro externo.
3. Configurar directivas de registro de auditoría (registro syslog y ns). Las directivas de registro de auditoría definen mensajes de registro para la partición de origen en el servidor de registro syslog o ns.
4. Vincular la directiva de registro de auditoría a las entidades SysGlobal y NSGlobal. Enlazar una directiva de registro de auditoría a una entidad global del sistema.
5. Revisar las estadísticas del registro de auditoría. Muestra las estadísticas del registro de auditoría y evalúa la configuración.

Configure lo siguiente mediante la CLI

1. Crear la dirección IP de subred de una partición

```
add ns ip <ip address> <subnet mask>
```

2. Crear una acción syslog

```
add audit syslogAction <name> <serverIP> [-serverPort <port>] -logLevel
 <logLevel> [-dateFormat (MMDDYYYY | DDMMYYYY )] [-transport ( TCP |
UDP )]
```

3. Crear una acción de registro ns

```
add audit nslogAction <name> <serverIP> [-serverPort <port>] -logLevel
<logLevel> [-dateFormat (MMDDYYYY | DDMMYYYY )]
```

4. Crear directivas de registro de auditoría syslog

```
add audit syslogpolicy syslog-pol1 true audit-action1
```

5. Crear un registro ns directivas de registro de auditoría

```
add audit nslogpolicy nslog-pol1 true audit-action1
```

6. Enlazar una directiva de registro de auditoría a la entidad SysLogGlobal

```
bind audit sysloggloba -policyName <name> -priority <priority_integer>
 -globalBindType SYSTEM_GLOBAL
```

7. Enlazar una directiva de registro de auditoría a la entidad NSLogGlobal

```
bind audit nsloggloba -policyName <name> -priority <priority_integer>
-globalBindType SYSTEM_GLOBAL
```

8. Mostrar estadísticas de registro de auditoría

```
stat audit -detail
```


Ejemplo

```
add ns ip 10.102.1.1 255.255.255.0
add audit syslogAction syslog_action1 10.102.1.2 -logLevel
    INFORMATIONAL -dateFormat MMDDYYYY -transport UDP
add audit syslogpolicy syslog-pol1 true syslog_action1
bind audit sysloggloba l -policyName syslog-pol1 -priority 1 -
    globalBindType SYSTEM_GLOBAL
```

Almacenamiento de registros

Cuando el servidor SYSLOG o NSLOG recopila información de registro de todas las particiones, se almacena como mensajes de registro en el archivo ns.log. Los mensajes de registro contienen la siguiente información:

- Nombre de partición.
- La dirección IP.
- Una marca de tiempo.
- El tipo de mensaje
- Los niveles de registro predefinidos (Crítico, Error, Aviso, Advertencia, Informativo, Depuración, Alerta y Emergencia)
- La información del mensaje.

Mostrar direcciones PMAC configuradas para la configuración de VLAN compartida

January 31, 2022

Para utilizar una configuración de partición con configuración de VLAN compartida, necesita una dirección MAC virtual denominada dirección MAC de partición (PMAC). La partición utiliza la dirección PMAC para su comunicación en la VLAN compartida. Se configura una dirección PMAC única para cada partición y se utiliza en todas las VLAN compartidas enlazadas a esa partición. En el caso de una plataforma que no es SDX (VPX o MPX), la dirección PMAC puede especificarse por el usuario o generarse internamente mediante un dispositivo Citrix ADC. Si no se especifica la dirección PMAC para una partición, se genera internamente cuando la partición está vinculada a la primera VLAN compartida. En el caso de una plataforma SDX, las direcciones PMAC siempre deben configurarse primero desde la herramienta SVM y, a continuación, asignarse a una partición.

Para mostrar una lista de los PMAC configurados, puede utilizar el comando **Show ns PartitionMac** . El comando permite verificar los PMAC configurados a través de la CLI o GUI de Citrix ADC. El co-

mando muestra todas las direcciones PMAC y las particiones correspondientes (si están asignadas). En el caso de una plataforma que no es SDX, el comando muestra todas las direcciones PMAC y sus particiones correspondientes porque la dirección PMAC se asigna a una partición solo cuando es necesario (cuando una partición está vinculada a una VLAN compartida). Sin embargo, en el caso de una plataforma SDX, es posible que tenga algunos PMAC sin asignar en la lista.

Para obtener información sobre cómo generar PMAC para la plataforma SDX, consulte el tema Generación de direcciones MAC de particiones .

Mostrar PMAC mediante la CLI de Citrix ADC

En el símbolo del sistema, escriba el siguiente comando:

```
show ns partitionMAC
```

```
Partition MAC Partition Name

1) f2:0c:64:da:f6:d7

2) b4:0c:43:da:f6:d2

3) a6:e7:b2:6c:48:e0

Done
```

Mostrar direcciones PMAC mediante la GUI de Citrix ADC

1. Inicie sesión en el dispositivo Citrix ADC y vaya a **Configuración > Sistema > Partición MAC**.
2. La página Partition MAC muestra una lista de los PMAC y sus particiones.

AppExpert

July 8, 2022

En los temas siguientes se proporciona una referencia conceptual e instrucciones de configuración para AppExpert y otras funciones del dispositivo Citrix ADC.

> **Nota**
>
> Para obtener información sobre las extensiones de directivas, consulte Extensiones de directivas.

- Action Analytics: Recopila estadísticas en tiempo de ejecución sobre la base de criterios predefinidos. Cuando se utiliza con directivas, la función también le proporciona la infraestructura para la optimización automática del tráfico en tiempo real.
- Aplicaciones y plantillas de AppExpert: Simplifique los pasos de configuración del dispositivo Citrix® NetScaler® mediante aplicaciones, plantillas de aplicación, aplicaciones Citrix Gateway y plantillas de entidades.
- AppQOE: Calidad de experiencia a nivel de aplicación (AppQOE) integra varias funciones de seguridad basadas en directivas existentes del dispositivo Citrix ADC en una única función integrada que aprovecha un nuevo mecanismo de cola, la colocación en cola justa.
- Plantilla de entidad: describe cómo utilizar plantillas de entidad para configurar y configurar entidades Citrix ADC individuales, como una directiva o un servidor virtual. Una plantilla de entidad proporciona una especificación y un conjunto de valores predeterminados para el objeto.
- Llamadas HTTP: solicitud HTTP que el dispositivo Citrix ADC genera y envía a una aplicación externa cuando se cumplen ciertos criterios durante la evaluación de directivas.
- Conjuntos de patrones: Permite la coincidencia de cadenas durante la evaluación de una directiva avanzada.
- Directivas y expresiones: Reglas que determinan las operaciones que debe realizar el dispositivo Citrix ADC.
- Limitación de velocidad: Define la carga máxima para una entidad de red o entidad virtual determinada en el dispositivo Citrix ADC.
- Respondedor: Basa las respuestas en quién envía la solicitud, desde dónde se envía y otros criterios con implicaciones de seguridad y administración del sistema.
- Reescritura: reescribe la información de las solicitudes o respuestas gestionadas por el dispositivo Citrix ADC.
- Mapas de cadenas: realice la coincidencia de patrones en todas las funciones de Citrix ADC que utilizan la sintaxis de directiva predeterminada.

Análisis de acciones

October 5, 2021

El rendimiento de su sitio web o aplicación depende de qué tan bien optimices la entrega del contenido solicitado con más frecuencia. Técnicas como el almacenamiento en caché y la compresión ayudan a acelerar la prestación de servicios a los clientes, pero debe poder identificar los recursos

que se solicitan con mayor frecuencia y, a continuación, almacenar en caché o comprimir esos recursos. Puede identificar los recursos utilizados con mayor frecuencia agregando estadísticas en tiempo real sobre el tráfico de sitios web o aplicaciones. Estadísticas como la frecuencia con la que se accede a un recurso en relación con otros recursos y cuánto ancho de banda consumen esos recursos ayudan a determinar si esos recursos deben almacenarse en caché o comprimirse para mejorar el rendimiento del servidor y la utilización de la red. Estadísticas como los tiempos de respuesta y el número de conexiones simultáneas a la aplicación le ayudan a determinar si debe mejorar los recursos del servidor.

Si el sitio web o la aplicación no cambian con frecuencia, puede utilizar productos que recopilan datos estadísticos y, a continuación, analizar manualmente las estadísticas y optimizar la entrega de contenido. Sin embargo, si no quiere realizar optimizaciones manuales, o si su sitio web o aplicación es de naturaleza dinámica, necesita una infraestructura que no solo pueda recopilar datos estadísticos sino que también pueda optimizar automáticamente la entrega de recursos sobre la base de las estadísticas. En el dispositivo Citrix ADC, esta funcionalidad la proporciona la función de análisis de acciones. La función funciona en un único dispositivo Citrix ADC y recopila estadísticas de tiempo de ejecución según los criterios que defina. Cuando se utiliza con directivas Citrix ADC, la función también le proporciona la infraestructura que necesita para la optimización automática del tráfico en tiempo real.

Al configurar la función de análisis de acciones, especifique los atributos de solicitud para los que quiere recopilar datos estadísticos, por ejemplo, URL y métodos HTTP mediante la configuración de expresiones de directiva avanzadas en una entidad denominada selector. A continuación, configura un identificador para configurar ajustes como el intervalo de muestreo y el recuento de muestras. También configura una directiva que permite al dispositivo evaluar el tráfico según lo especificado por el par selector-identificador. Por último, vincula la directiva a un punto de enlace para comenzar a recopilar estadísticas.

El dispositivo también le proporciona un conjunto de selectores, identificadores y directivas de respuesta integrados que puede utilizar para empezar a utilizar la función.

El dispositivo agrega las siguientes estadísticas:

- Número de solicitudes.
- Ancho de banda consumido por las solicitudes.
- El tiempo de respuesta.
- Número de conexiones simultáneas.

Puede configurar la función para que realice la ordenación en tiempo de ejecución de los registros de un atributo de su elección. Puede ver los datos estadísticos mediante la interfaz de línea de comandos o la herramienta Stream Sessions de la utilidad de configuración.

Configurar un selector

October 5, 2021

Un selector es un filtro para identificar solicitudes. Consta de hasta cinco expresiones de directivas avanzadas individuales que identifican atributos de solicitud como la dirección IP del cliente y la URL de la solicitud. Cada expresión es una expresión de directiva avanzada no compuesta y se considera que está en una relación AND con las demás expresiones. A continuación se presentan algunos ejemplos de expresiones selectoras:

- `HTTP.REQ.URL`
- `CLIENT.IP.SRC`
- `HTTP.RES.BODY(1000).AFTER_STR("<string>").BEFORE_STR("<string>")"`
- `CLIENT.IP.SRC.SUBNET(24)`

Los selectores se utilizan en configuraciones de limitación de velocidad y análisis de acciones. Un selector es opcional en una configuración de limitación de velocidad, pero es necesario en una configuración de análisis de acciones.

El orden en que se especifican los parámetros es significativo. Por ejemplo, si configura una dirección IP y un dominio (en ese orden) en un selector y, a continuación, especifica el dominio y la dirección IP (en orden inverso) en otro selector, Citrix ADC considera que estos valores son únicos. Esto puede hacer que la misma transacción se cuente dos veces. Además, si varias directivas invocan el mismo selector, Citrix ADC, de nuevo, puede contar la misma transacción más de una vez.

Si modifica una expresión en un selector, puede aparecer un error si alguna directiva que la invoca está vinculada a un nuevo rótulo de directiva o punto de enlace. Por ejemplo, supongamos que crea un selector denominado myLimitSelector1, lo invoca desde myLimitId1 e invoca el identificador desde una directiva DNS denominada DNSrateLimit1. Si cambia la expresión en myLimitSelector1, es posible que reciba un error al vincular DNSrateLimit1 a un nuevo punto de enlace. La solución consiste en modificar estas expresiones antes de crear las directivas que las invocan.

El dispositivo Citrix ADC proporciona selectores integrados pdf para algunos de los casos de uso más comunes. Consulte el pdf.

También puede configurar un selector con expresiones que identifiquen los atributos de solicitud de su elección. Por ejemplo, es posible que quiera crear un registro para una solicitud que llega con un encabezado específico. Para evaluar el encabezado, puede agregarlo `HTTP.REQ.HEADER("<header_name>")` al selector que va a utilizar.

Para configurar un selector mediante la interfaz de línea de comandos:

En el símbolo del sistema, escriba los siguientes comandos para configurar un selector y verificar la configuración:

- add stream selector <name> <rule> ...
- show stream selector

Ejemplo

```
> add stream selector myselector HTTP.REQ.URL CLIENT.IP.SRC
 Done
> show stream selector myselector
    Name: myselector
    Expressions:
        1) HTTP.REQ.URL
        2) CLIENT.IP.SRC
 Done
>
<!--NeedCopy-->
```

Para modificar o quitar un selector mediante la interfaz de línea de comandos:

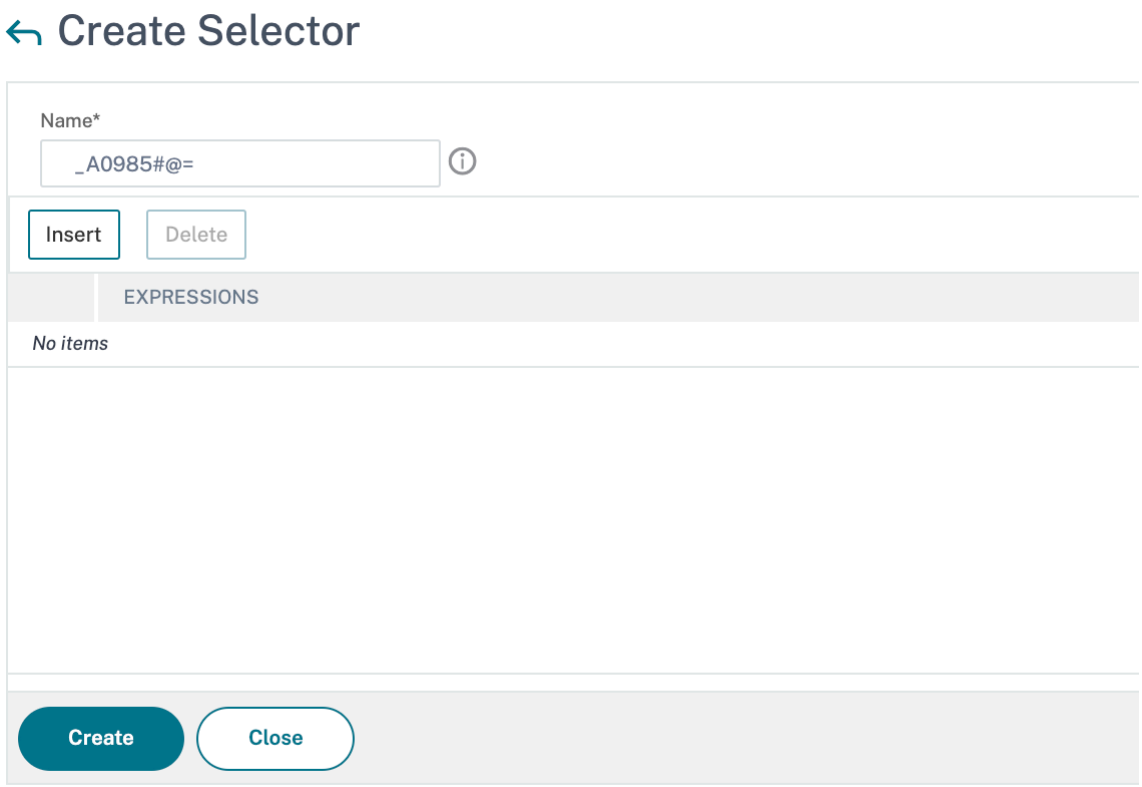
- Para modificar un selector, escriba el comando set stream selector, el nombre del selector y el parámetro rule con las expresiones. Introduzca las expresiones existentes que quiere conservar, junto con las nuevas expresiones que quiera agregar.
- Para quitar un selector, escriba el comando rm stream selector y el nombre del selector.

Para configurar un selector mediante la interfaz gráfica de usuario:

1. Vaya a **AppExpert** > **Análisis de acciones** > **Selectores**.
2. En el panel de detalles, realice una de las acciones siguientes:
   - Para crear un selector, haga clic en **Agregar**.
   - Para modificar un selector, selecciónelo y, a continuación, haga clic en **Modificar**.
3. En la página **Crear Selector** o **Configurar Selector**, defina los siguientes parámetros:
   - Name. Para agregar un nombre para el selector, introduzca el nombre en el archivo **Nombre** . El nombre debe comenzar por un carácter ASCII, alfanumérico o de guión bajo. El nombre debe contener solo caracteres alfanuméricos, guiones bajos, hash, punto, espacio, dos puntos, at, iguales y guiones ASCII.
   - Expresiones. Para agregar la expresión a la configuración del selector, haga clic en **Insertar**. Para quitar una expresión de la configuración del selector, en el cuadro Expresión, seleccione la expresión y, a continuación, haga clic en **Eliminar**. Nota: En el cuadro Expresiones, introduzca un parámetro válido. Por ejemplo, introduzca HTTP. A continuación, introduzca un punto después de este parámetro. Aparecerá un menú desplegable. El contenido de este menú proporciona las palabras clave que pueden seguir a la palabra clave inicial introducida. Para seleccionar la siguiente palabra clave de este prefijo de expresión, haga doble clic en la selección del menú desplegable. El cuadro de texto **Expre-**

siones muestra la primera y la segunda palabra clave del prefijo de expresión, por ejemplo, HTTP.REQ. Continúe agregando componentes de expresión hasta que se forme la expresión completa.

4. Haga clic en **Insertar**.
5. Continúe agregando hasta cinco expresiones no compuestas.
6. Haga clic en **Crear** y luego en **Cerrar**.



Configurar un identificador de flujo

August 20, 2021

Configurar un identificador de flujo para especificar parámetros para recopilar datos estadísticos de las solicitudes identificadas por un selector determinado. Un identificador especifica el selector que se va a utilizar, el intervalo de recopilación de estadísticas, el recuento de muestras y el campo en el que se van a ordenar los registros.

El dispositivo Citrix ADC incluye los siguientes identificadores de flujo integrados para casos de uso habituales. Todos los identificadores integrados especifican un recuento de muestra de 1 y un intervalo de 1 minuto. Además, ordenan los datos en el atributo
Requests. Se diferencian solo en estar asociados con diferentes selectores incorporados. Cada iden-

tificador integrado está asociado con un selector integrado del mismo nombre (por ejemplo, el identificador incorporado
Top_URL está asociado con el selector integrado
Top_URL). Los siguientes son los identificadores incorporados:

- URL superior
- Clients
- Top_URL_Clients_lbvServer
- Top_URL_clients_csvserver
- Top_MSSQL_query_db_lbvserver
- Top_mysql_query_db_lbvserver

Para obtener más información sobre los selectores integrados, consulte Configuración de un selector.

Nota: La longitud máxima para almacenar los resultados de cadena de selectores (por ejemplo, HTTP.REQ.URL) es de 60 caracteres. Si la cadena (por ejemplo, URL) tiene 1000 caracteres de longitud, de los cuales 50 son suficientes para identificar de forma única una cadena, utilice una expresión para extraer solo los 50 caracteres necesarios.

No se puede modificar la configuración de un identificador integrado. Sin embargo, puede crear un identificador con una configuración de su elección.

Para configurar un identificador de flujo mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para configurar un identificador de flujo y verificar la configuración:

- `add stream identifier <name> <selectorName> [-interval <positive_integer>] [-SampleCount <positive_integer>] [-sort <sort>]`
- `show stream identifier <name>`

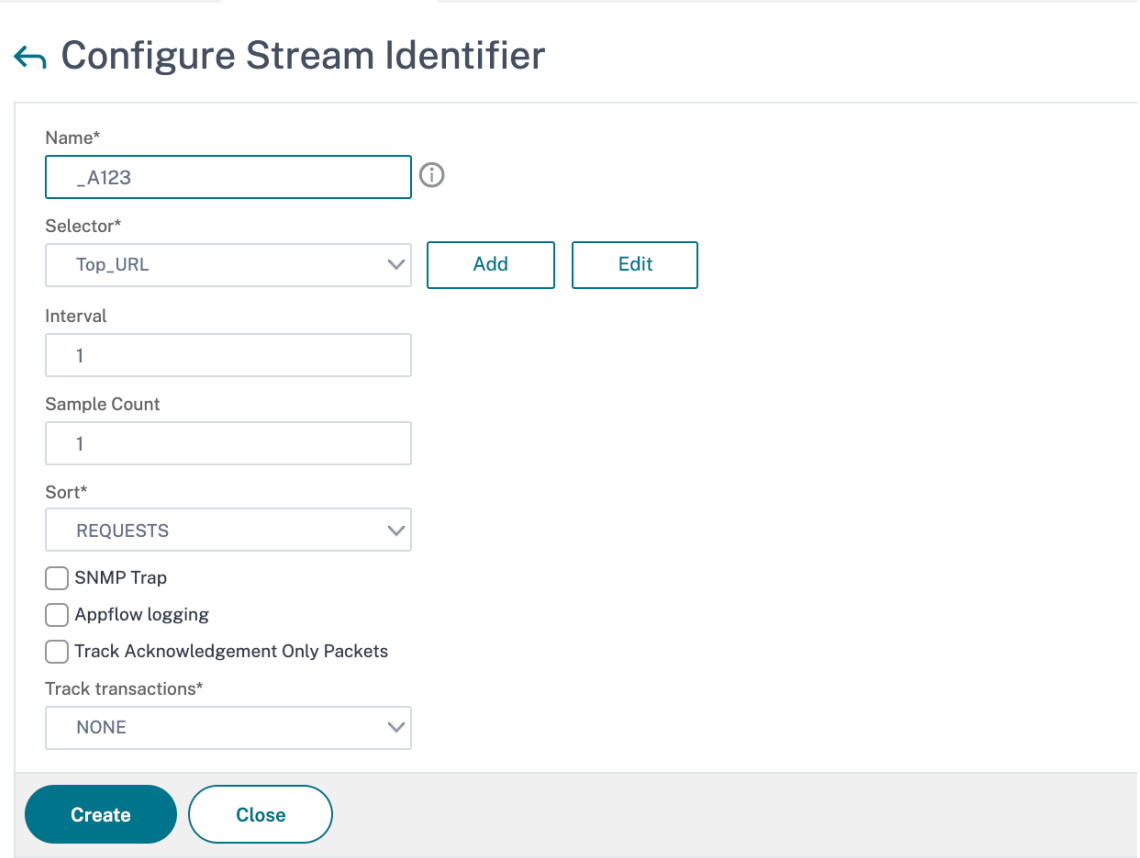
Ejemplo

```
1 > add stream identifier myidentifier Top_URL -interval 10 -sampleCount
     100
2  Done
3 <!--NeedCopy-->
```

Para configurar un identificador de flujo mediante la interfaz gráfica de usuario

1. Vaya a **AppExpert** > **Análisis de acciones** > **Identificadores de secuencias**.
2. En el panel de detalles, realice una de las acciones siguientes:
   - Para crear un identificador de flujo, haga clic en **Agregar**.
   - Para modificar un identificador de flujo, selecciónelo y, a continuación, haga clic en **Modificar**.

3. En la página Configurar Identificador de Stream, defina los siguientes parámetros:
   - Nombre
   - Selector
   - Intervalo
   - Recuento de ejemplos
   - Ordenar
4. Haga clic en **Crear** y, a continuación, en **Cerrar**.



Ver estadísticas

August 20, 2021

Puede ver las estadísticas recopiladas en formato tabular en la interfaz de línea de comandos y en formato gráfico en la utilidad de configuración.

En la siguiente tabla se describen las estadísticas recopiladas:

Estadísticas	Nombre de columna en la salida del comando <identifier name> stat stream identifier	Descripción
Cantidad de solicitudes	**Req**	Número de solicitudes para las que se crearon registros en el último<interval> número de minutos.
Ancho de banda consumido	**BandW**	El ancho de banda total consumido por las solicitudes recibidas en el último<interval> número de minutos. El ancho de banda total de una solicitud es el ancho de banda consumido por la solicitud y su respuesta. El valor se redondea al siguiente valor entero superior o siguiente inferior. Por lo tanto, podría diferir ligeramente del valor esperado. Por ejemplo, si el consumo total de ancho de banda de una solicitud es de 2,2 KB. Es posible que se muestre que una instancia de la solicitud ha consumido 2 KB. Es posible que se muestre que dos instancias han consumido 4 KB, pero tres instancias podrían mostrarse que han consumido 7 KB.
Tiempo de respuesta	**RSPTime**	Tiempo medio de respuesta para todas las solicitudes recibidas en el último<interval> número de minutos.

Estadísticas	Nombre de columna en la salida del comando <identifier name> stat stream identifier	Descripción
Conexiones simultáneas	**Con**	Número total de conexiones simultáneas que están abiertas actualmente.

Para ver los datos estadísticos recopilados para un identificador de flujo mediante la línea de comandos

En el símbolo del sistema, escriba:

```
stat stream identifier <name> [<pattern> ...] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>] [-sortBy <sortBy> [<sortOrder>]
```

Ejemplos

El ejemplo 1 ordena la salida de la columna BandW, en orden descendente. El ejemplo 2 ordena la salida en el ejemplo 1, en la columna **Req** y en orden ascendente.

Ejemplo 1

```
> stat stream identifier myidentifier -sortBy BandW Descending -fullValues
Stream Session statistics
                     Req                  BandW
User1                508                 125924
User2               5020                  12692
User3               2025                   4316

                  RspTime                   Conn
User1                5694                      0
User2                 109                      0
User3                   3                      0
 Done
<!--NeedCopy-->
```

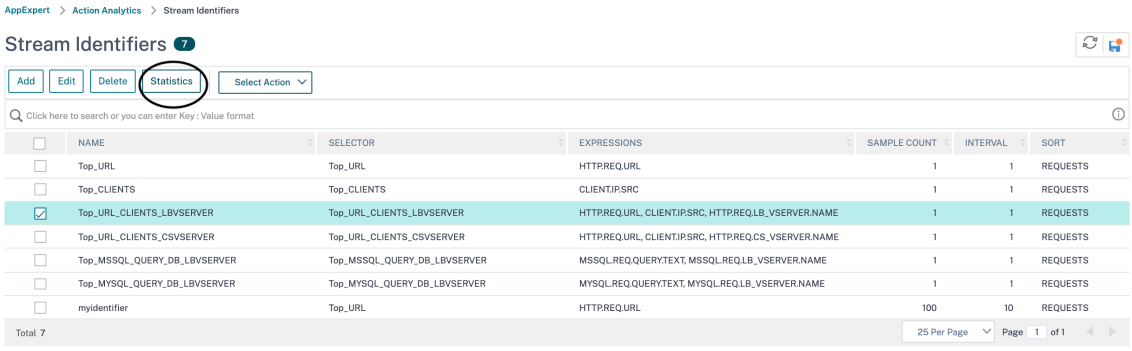
Ejemplo 2


```
> stat stream identifier myidentifier -sortBy Req Ascending -
    fullValues
Stream Session statistics
                     Req                  BandW
User1                508                 125924
User3               2025                   4316
User2               5020                  12692

                 RspTime                   Conn
User1               5694                      0
User3                  3                      0
User2                109                      0
 Done
<!--NeedCopy-->
```

Para ver los datos estadísticos recopilados para un identificador de flujo mediante la interfaz gráfica de usuario

1. Vaya a **AppExpert** > **Análisis de acciones** > **Identificadores de secuencias**.
2. Seleccione el identificador de flujo cuyas sesiones quiere ver y, a continuación, haga clic en Estadísticas Para obtener información sobre cómo agrupar la salida en función de los valores recopilados para varias expresiones de selector.



Agrupación de registros en valores de atributo

January 12, 2021

Información estadística, como el número de veces que se ha accedido a una URL determinada en general y por cliente, y el número total de solicitudes GET y POST por cliente pueden proporcionar información valiosa sobre si alguno de sus recursos necesita ampliarse para satisfacer la demanda u optimizarse para la entrega. Para obtener estas estadísticas, debe utilizar un conjunto apropiado de expresiones selectoras y, a continuación, utilizar el parámetro pattern en el comando stat stream

identifier. La agrupación se basa en el patrón especificado en el comando. La agrupación se puede realizar simultáneamente en los valores de varias expresiones.

En la interfaz de línea de comandos, puede agrupar la salida mediante patrones de su elección. En la utilidad de configuración, el patrón depende de las opciones que realice al obtener detalles a través de los valores de varias expresiones selectoras. Por ejemplo, considere un selector que tenga las expresiones`HTTP.REQ.URL`,`CLIENT.IP.SRC`, y`HTTP.REQ.LB_VSERVER.NAME`, en ese orden. La página principal de estadísticas muestra iconos para cada una de estas expresiones. Si hace clic en el icono de`CLIENT.IP.SRC`, la salida se basa en los patrones *?*. La salida muestra estadísticas para cada dirección IP del cliente. Si hace clic en una dirección IP, la salida se basa en los patrones *`<IP address>` ? y?`<IP address>` * donde`<IP address>` es la dirección IP que ha seleccionado. En la salida resultante, si hace clic en una URL, el patrón utilizado es`<URL> <IP address>` ?.

Para agrupar los registros en los valores de las expresiones selectoras mediante la interfaz de línea de comandos

En la solicitud de comando, escriba el siguiente comando para agrupar los registros sobre la base de una expresión de selector:

```
stat stream identifier <name> [<pattern> ...]
```

Los siguientes ejemplos utilizan un patrón diferente para demostrar el efecto del patrón en la salida del comando stat stream identifier. Las expresiones selectoras son HTTP.REQ.URL y HTTP.REQ.HEADER ("UserHeader"), en ese orden. Las solicitudes contienen un encabezado personalizado cuyo nombre es UserHeader. Tenga en cuenta que en los ejemplos, un valor estadístico dado cambia según lo determinado por la agrupación, pero la suma total de los valores de un campo dado sigue siendo la misma.

Ejemplo 1

En el siguiente comando, el patrón utilizado es ? ?. El dispositivo agrupa la salida en los valores recopilados para ambas expresiones selectoras. Los encabezados de fila consisten en los valores de expresión separados por un signo de interrogación (?). La fila con el encabezado /mysite/mypage1.html?Ed muestra estadísticas de las solicitudes realizadas por el usuario Ed para la URL /misitio/mipágina1.html.

> **Nota:**
>
> Debe asegurarse de escribir el siguiente comando con "?¿"en lugar de "?". Por ejemplo, si selector utiliza una expresión: Client.ip.src y client.tcp.srcport. El comando Stat para agrupar la salida en los valores recopilados para el selector es 'stat stream identifier myidentifier? ? -FullValues' como se indica a continuación.


```
> stat stream identifier myidentifier ? ? -fullValues
Stream Session statistics
                                                Req                  BandW
/mysite/mypage2.html?Grace                        1                   2553
/mysite/mypage1.html?Grace                        2                      4
/mysite/mypage1.html?Ed                           8                     16
/mysite/mypage2.html?Joe                          1                   2554
/mysite/mypage1.html?Joe                          5                     10
/mysite/?Joe                                      1                      4

                                             RspTime                  Conn
/mysite/mypage2.html?Grace                         0                      0
/mysite/mypage1.html?Grace                         0                      0
/mysite/mypage1.html?Ed                            0                      0
/mysite/mypage2.html?Joe                           0                      0
/mysite/mypage1.html?Joe                           0                      0
/mysite/?Joe                                       6                      0
 Done
<!--NeedCopy-->
```

Ejemplo 2

En el siguiente comando, el patrón utilizado es *?. El dispositivo agrupa la salida en los valores acumulados para la segunda expresión HTTP.REQ.HEADER (“UserHeader”). Las filas muestran estadísticas de todas las solicitudes realizadas por los usuarios Grace, Ed y Joe.

> **Nota:**
>
> Asegúrese de escribir el siguiente comando con “?¿”en lugar de “?”.

```
> stat stream identifier myidentifier * ?
Stream Session statistics
                   Req     BandW  RspTime      Conn
Grace                3      2557        0         0
Ed                   8        16        0         0
Joe                  7      2568        6         0
 Done
<!--NeedCopy-->
```

Ejemplo 3

En el siguiente comando, el patrón utilizado es ? *, que es el patrón predeterminado. La salida se agrupa en los valores recopilados para la primera expresión del selector. Cada fila muestra estadísticas para una URL.

> **Nota:**
>
> Asegúrese de escribir el siguiente comando con "?¿"en lugar de "?".

```
> stat stream identifier myidentifier ? * -fullValues
Stream Session statistics

                                        Req                  BandW
/mysite/mypage2.html                      2                   5107
/mysite/mypage1.html                     15                     30
/mysite/                                  1                      4

                                    RspTime                   Conn
/mysite/mypage2.html                      0                      0
/mysite/mypage1.html                      0                      0
/mysite/                                  6                      0
 Done
<!--NeedCopy-->
```

Ejemplo 4

En el siguiente comando, el patrón utilizado es* *. El dispositivo muestra un conjunto de estadísticas colectivas para todas las solicitudes recibidas, sin título de fila.

```
> stat stream identifier myidentifier * *
Stream Session statistics
                  Req    BandW  RspTime     Conn
                   18     5141        6        0
 Done
<!--NeedCopy-->
```

Ejemplo 5

En el siguiente comando, el patrón es /mysite/mypage1.html *. El dispositivo muestra un conjunto de estadísticas colectivas para todas las solicitudes recibidas para la URL /mysite/mypage1.html, sin título de fila.

```
> stat stream identifier myidentifier /mysite/mypage1.html *
Stream Session statistics
                  Req    BandW  RspTime     Conn
                   15       30        0        0
 Done
```



```
<!--NeedCopy-->
```

Borrado de una sesión de flujo

August 20, 2021

Puede vaciar todos los registros que se han acumulado para un identificador de flujo.

Para borrar una sesión de flujo mediante la interfaz de línea de comandos

En la solicitud de comando, escriba los siguientes comandos para borrar una sesión de flujo y verificar los resultados:

- sesión de flujo claro
- identificador de flujo stat

Ejemplo

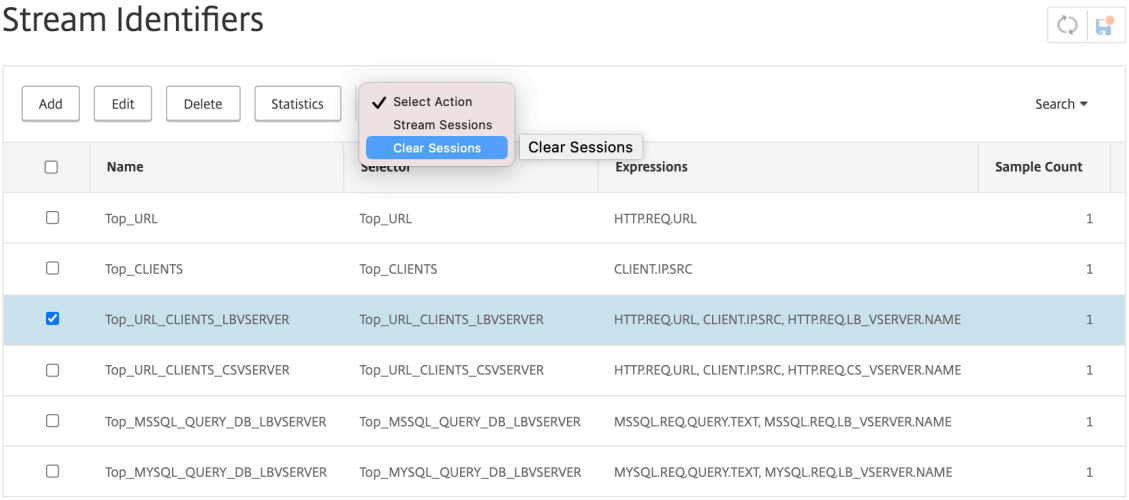
En este ejemplo se utiliza primero el comando stat stream identifier, de modo que se puede hacer una comparación con el comando stat stream identifier que se utiliza para verificar el resultado del comando clear stream session.

```
>stat stream identifier myidentifier
Stream Session statistics
                  Req    BandW  RspTime     Conn
/aed....html        2        0        0        0
/                 636      303       12        0
 Done
>clear stream session myidentifier
 Done
>stat stream identifier myidentifier
 Done
<!--NeedCopy-->
```

Para borrar una sesión de flujo mediante la interfaz gráfica de usuario

1. Vaya a **AppExpert** > **Análisis de acciones** > **Identificadores de secuencias**.

2. Seleccione el identificador de flujo cuyas sesiones quiere borrar y, a continuación, haga clic en **Borrar sesiones**.



Configurar directivas para optimizar el tráfico

October 5, 2021

Para poner en vigor el par selector-identificador de la configuración de análisis de acciones, debe asociar el par con el punto del flujo de tráfico en el que quiere recopilar estadísticas. Puede hacerlo configurando una directiva avanzada y haciendo referencia al identificador de flujo desde la regla de directiva. Puede utilizar directivas de compresión, directivas de almacenamiento en caché, directivas de reescritura, directivas de firewall de aplicaciones, directivas de respuesta y cualquier otra directiva cuya acción se base en una expresión booleana.

La función de análisis de acciones introduce un conjunto de funciones y expresiones de directivas avanzadas para recopilar y evaluar datos. La expresión `ANALYTICS.STREAM(<identifier_name>)` se utiliza para hacer referencia al identificador que quiere utilizar. La expresión COLLECT_STATS se utiliza para recopilar datos estadísticos. Funciones como `IS_TOP(<uint>)` y `IS_TOP_FREQUENTS(<uint>)` se utilizan para tomar decisiones automáticas de optimización del tráfico en tiempo real.

- **ES_TOP (<number>).** Busca si un objeto determinado está en la parte superior <number>de los elementos. Por ejemplo, es el elemento entre los 10 elementos principales. Cuando varios elementos tienen el recuento, se consideran de naturaleza similar. La función sort debe estar activada para evitar una condición undef.
- **IS_TOP_FREQUENTS().** Busca si un objeto determinado está en la parte superior de los elementos que están en los elementos superiores. Por ejemplo, es el elemento entre el 50% superior de todos los elementos superiores mantenidos. Los elementos que tienen los mismos valores se

consideran de naturaleza similar. La función sort debe estar activada para evitar una condición undef.

Es la configuración de su directiva la que determina si el dispositivo Citrix ADC solo debe recopilar datos del tráfico o también realizar una acción. Si el dispositivo solo debe recopilar datos estadísticos, puede configurar una directiva con la regla `ANALYTICS.STREAM(<identifier_name>).COLLECT_STATS` y la acción NOOP. La directiva NOOP debe ser la directiva con mayor prioridad en el punto de enlace. Esta directiva es suficiente si solo está recopilando estadísticas. Las decisiones de optimización del tráfico, como qué comprimir o almacenar en caché, deben basarse en una evaluación manual y periódica de los datos estadísticos.

Si, además de recopilar estadísticas, el dispositivo también debe realizar una acción sobre el tráfico, debe configurar el parámetro GoToPriorityExpression de la directiva NOOP para que se evalúe posteriormente otra directiva que tenga la regla y la acción deseadas. Esta segunda directiva debe tener una regla que empiece por el prefijo `ANALYTICS.STREAM(<identifier_name>)` y una función que evalúe los datos.

A continuación se muestra un ejemplo de dos directivas de respuesta configuradas y enlazadas globalmente. La directiva responder_stat_collection permite al dispositivo recopilar estadísticas basadas en el identificador, myidentifier. La directiva responder_notify evalúa los datos que se recopilan.

Ejemplo

```
> add responder action send_notification respondwith '"You are in the
   Top 10 list for bandwidth consumption"'
 Done
> add responder policy responder_stat_collection' ANALYTICS.STREAM("
   myidentifier").COLLECT_STATS' NOOP
Done
> add responder policy responder_notify 'ANALYTICS.STREAM("myidentifier
   ").BANDWIDTH.IS_TOP(10)' send_notification
 Done
> bind responder global responder_stat_collection 10 NEXT
 Done
> bind responder global responder_notify 20 END
 Done
<!--NeedCopy-->
```


Cómo limitar el consumo de ancho de banda por usuario o dispositivo cliente

August 20, 2021

Su sitio web, aplicación o servicio de alojamiento de archivos tiene recursos finitos de red y servidor disponibles para servir a todos sus usuarios. Uno de los recursos más importantes es el ancho de banda. Un consumo considerable de ancho de banda solo por un subconjunto de la base de usuarios puede provocar congestión de la red y una menor disponibilidad de recursos para otros usuarios. Para evitar la congestión de la red, es posible que tenga que limitar el consumo de ancho de banda de un cliente mediante técnicas de denegación de servicio temporales, como responder a una solicitud de cliente con una página HTML si ha excedido un valor de ancho de banda preconfigurado durante un período de tiempo fijo previo a la solicitud.

En general, puede regular el consumo de ancho de banda por dispositivo cliente o por usuario. Este caso de uso demuestra cómo puede limitar el consumo de ancho de banda por cliente a 100 MB durante un período de tiempo de una hora. El caso de uso también demuestra cómo puede regular el consumo de ancho de banda por usuario a 100 MB durante un período de tiempo de una hora, mediante un encabezado personalizado que proporciona el nombre de usuario. En ambos casos, el seguimiento del consumo de ancho de banda durante un período de tiempo en movimiento de una hora se logra estableciendo el parámetro de intervalo en el identificador de flujo en 60 minutos. Los casos de uso también demuestran cómo puede importar una página HTML para enviarla a un cliente que ha superado el límite. La importación de una página HTML no solo simplifica la configuración de la acción de respuesta en estos casos de uso, sino que también simplifica la configuración de todas las acciones de respuesta que necesitan la misma respuesta.

Para limitar el consumo de ancho de banda por usuario o dispositivo cliente mediante la interfaz de línea de comandos

En la interfaz de línea de comandos, realice las siguientes tareas para configurar el análisis de acciones para limitar el consumo de ancho de banda de un cliente o usuario. Cada paso incluye comandos de ejemplo y su salida.

1. **Configure la configuración de equilibrio de carga.** Configure el servidor virtual de equilibrio de carga mysitevip y, a continuación, configure todos los servicios que necesite. Enlazar los servicios al servidor virtual. El siguiente ejemplo crea diez servicios y los vincula a mysitevip.

```
1 > add lb vserver mysitevip HTTP 192.0.2.17 80
2  Done
3 > add service service[1-10] 192.0.2.[240-249] HTTP 80
4 service ”service1” added
```



```
service "service2" added
service "service3" added
.
.
.
service "service10" added
 Done
> bind lb vserver vserver1 service[1-10]
service "service1" bound
service "service2" bound
service "service3" bound
.
.
.
service "service10" bound
 Done
<!--NeedCopy-->
```

2. **Configure el selector de flujo.** Configure uno de los siguientes selectores de flujo:

   - Para limitar el consumo de ancho de banda por cliente, configure un selector de flujo que identifique la dirección IP del cliente.

     ```
     > add stream selector myselector CLIENT.IP.SRC
      Done
     <!--NeedCopy-->
     ```

   - Para limitar el consumo de ancho de banda por usuario sobre la base del valor de un encabezado de solicitud que proporciona el nombre de usuario, configure un selector de flujo que identifique el encabezado. En el ejemplo siguiente, el nombre del encabezado es UserHeader.

     ```
     > add stream selector myselector HTTP.REQ.HEADER( "UserHeader
         " )
      Done
     <!--NeedCopy-->
     ```

3. **Configure un identificador de flujo.** Configure un identificador de flujo que utilice el selector de flujo. Establezca el parámetro de intervalo en 60 minutos.


```
> add stream identifier myidentifier myselector -interval 60 -
   sampleCount 1 -sort BANDWIDTH
 Done
<!--NeedCopy-->
```

4. **Configure la acción de respondedor.** Importe la página HTML que quiere enviar a los usuarios o clientes que hayan superado el límite de consumo de ancho de banda y, a continuación, utilice la página en respuesta action crossed_limits.

```
> import responder htmlpage http://.1.1.1/stdpages/wait.html
   crossed-limits.html
This operation may take some time, Please wait...

 Done
> add responder action crossed_limits respondwithhtmlpage crossed-
   limits.html
 Done
<!--NeedCopy-->
```

5. **Configure las directivas de Responder.** Configure la directiva de respuesta myrespol1 con la regla ANALYTICS.STREAM (“myidentifier”).COLLECT_STATS y la acción NOOP. A continuación, configure la directiva myrespol2 para determinar si un cliente o usuario ha cruzado el límite de 100 MB. La directiva myrespol2 se configura con la acción de respuesta crossed_limits.

```
> add responder policy myrespol1 'ANALYTICS.STREAM(”myidentifier”)
   .COLLECT_STATS' NOOP
 Done
> add responder policy myrespol2 'ANALYTICS.STREAM(”myidentifier”)
   .BANDWIDTH.GT(104857600)' crossed_limits
 Done
<!--NeedCopy-->
```

6. **Enlazar las directivas de respuesta al servidor virtual de equilibrio de carga.** La directiva myrespol1, que solo recopila datos estadísticos, debe tener la prioridad más alta y una expresión GOTO de NEXT.

```
> bind lb vserver mysitevip -policyName myrespol1 -priority 1 -
   gotoPriorityExpression NEXT
 Done
```



```
> bind lb vserver mysitevip -policyName myrespol2 -priority 2 -
    gotoPriorityExpression END
 Done
<!--NeedCopy-->
```

7. **Pruebe la configuración.** Pruebe la configuración enviando solicitudes HTTP de prueba, desde varios clientes o usuarios, al servidor virtual de equilibrio de carga y mediante el comando stat stream identifier para ver las estadísticas que se recopilan para el identificador especificado. El siguiente resultado muestra las estadísticas de los clientes.

```
> stat stream identifier myidentifier -sortBy BandW  - fullValues
Stream Session statistics
                            Req             BandW
192.0.2.30                  5000            3761
192.0.2.31                  29              2602
192.0.2.32                  25              51

                            RspTime         Conn
192.0.2.30                  2               0
192.0.2.31                  0               0
192.0.2.32                  0               0
 Done
>
<!--NeedCopy-->
```

Aplicaciones AppExpert

June 22, 2022

> **Advertencia**
>
> La funcionalidad de la plantilla de aplicación está obsoleta y, como alternativa, Citrix recomienda utilizar los libros de estilos. Para obtener más información, consulte el tema StyleBooks.

Una aplicación AppExpert es un conjunto de configuraciones que configura en el dispositivo Citrix ADC. La administración de aplicaciones de AppExpert se simplifica mediante una GUI (GUI) que permite especificar subconjuntos de tráfico de aplicaciones y un conjunto distinto de directivas de seguridad y optimización para procesar cada subconjunto de tráfico. Además, consolida los pasos de implementación en una vista, para que pueda configurar rápidamente las direcciones IP de destino para los clientes y especificar servidores host.

Después de configurar la aplicación AppExpert, debe verificar que la aplicación funciona correctamente. Si es necesario, puede personalizar la configuración para que se ajuste a sus necesidades.

Periódicamente, puede verificar y supervisar la configuración mediante la visualización de los contadores de varios componentes de la aplicación, las estadísticas y el Visualizador de aplicaciones. También puede configurar directivas de autenticación, autorización y auditoría (autenticación, autorización y auditoría) para la aplicación.

Terminología de aplicaciones AppExpert

A continuación se indican los términos utilizados en la función de aplicaciones AppExpert y las descripciones de las entidades para las que se utilizan los términos:

Dispositivo de punto final público. La combinación de dirección IP y puerto en la que el dispositivo Citrix ADC recibe las solicitudes de los clientes de la aplicación web asociada. Un dispositivo de punto final público se puede configurar para recibir tráfico HTTP o HTTP seguro (HTTPS). Todas las solicitudes de cliente de la aplicación web deben enviarse a un dispositivo de punto final público. A una aplicación AppExpert se le pueden asignar varios puntos finales.

Unidad de aplicación. Entidad de aplicación AppExpert que procesa un subconjunto del tráfico de aplicaciones web y equilibra la carga de un conjunto de servicios que alojan el contenido asociado. El subconjunto de tráfico que debe administrar una unidad de aplicación se define mediante una regla. Cada unidad de aplicación también define su propio conjunto de directivas de seguridad y optimización del tráfico para las solicitudes y respuestas que administra. Los servicios de Citrix ADC asociados a estas directivas son compresión, almacenamiento en caché, reescritura, respuesta y firewall de aplicaciones.

De forma predeterminada, todas las aplicaciones de AppExpert con al menos una unidad de aplicación incluyen una unidad de aplicación predeterminada que no se puede eliminar. La unidad de aplicación predeterminada no está asociada a una regla para identificar solicitudes y siempre se coloca en último lugar en el orden de unidades de aplicación. Define un conjunto de directivas para procesar cualquier solicitud que no coincida con las reglas configuradas para las demás unidades de aplicación. Garantizando así que se procesan todas las solicitudes de los clientes.

Servicio. Combinación de la dirección IP del servidor que aloja la instancia de la aplicación web y el puerto al que se asigna la aplicación en el servidor, en el formato `\<IP address\>:\<Port\>`. Una aplicación web que atiende muchas solicitudes se aloja en varios servidores. Se dice que cada servidor aloja una instancia de la aplicación web, y cada instancia de la aplicación web está representada por un servicio en el dispositivo Citrix ADC.

Regla de unidad de aplicación. Expresión de directiva avanzada que define las funciones de un subconjunto de tráfico de una unidad de aplicación. La regla de ejemplo siguiente es una expresión de directiva avanzada que identifica un subconjunto de tráfico que consta de cuatro tipos de imágenes:


```
HTTP.REQ.URL.SUFFIX.EQ("bmp")|| HTTP.REQ.URL.SUFFIX.EQ("gif")|| HTTP.REQ.
URL.SUFFIX.EQ("png")|| HTTP.REQ.URL.SUFFIX.EQ("jpg")
```

Para obtener más información sobre las expresiones de directivas avanzadas, consulte Directivas y expresiones.

Subconjunto de tráfico. Conjunto de solicitudes de clientes que requieren un conjunto común de directivas de seguridad y optimización del tráfico. Una unidad de aplicación administra un subconjunto de tráfico y se define mediante una regla.

Cómo funciona la aplicación AppExpert

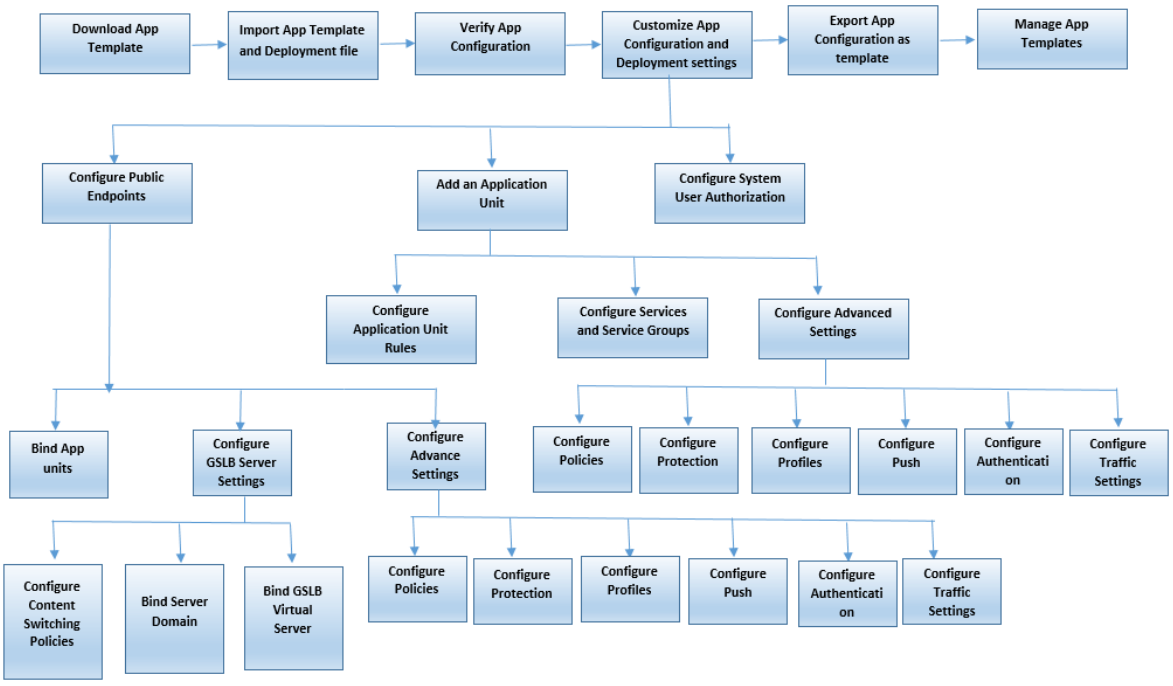
June 22, 2022

Cuando el punto final recibe una solicitud de cliente, el dispositivo Citrix ADC evalúa la solicitud con respecto a la regla que está configurada para la unidad de aplicación más alta. Si la solicitud cumple con esta regla, la solicitud se procesa mediante las directivas configuradas para la unidad de aplicación y, a continuación, se reenvía a un servicio. La elección del servicio depende de los servicios que estén configurados para la aplicación y de parámetros como el algoritmo de equilibrio de carga y el método de persistencia configurados para la unidad de la aplicación.

Si la solicitud no cumple con la regla, la solicitud se evalúa con respecto a la regla para la siguiente unidad de aplicación más alta. En este orden, la solicitud se evalúa con respecto a cada regla de unidad de aplicación hasta que la solicitud cumpla con una regla. Si la solicitud no cumple ninguna de las reglas configuradas, la procesa la unidad de aplicación predeterminada, que siempre es la última unidad de aplicación.

Puede configurar varios puntos finales públicos para una aplicación AppExpert. En una configuración de este tipo, de forma predeterminada, cada unidad de aplicación procesa las solicitudes recibidas por todos los puntos finales públicos y equilibra la carga de todos los servicios que están configurados para la aplicación. Sin embargo, puede especificar que una unidad de aplicación procese el tráfico solo desde un subconjunto de los puntos finales públicos y equilibre la carga solo un subconjunto de los servicios que están configurados para la aplicación AppExpert.

El siguiente diagrama de flujo ilustra la secuencia de flujo de la aplicación AppExpert para usar una plantilla de aplicación integrada.



Si prefiere crear una aplicación personalizada sin usar una plantilla, haga lo siguiente:

1. Cree una aplicación personalizada.
2. Configure los parámetros de aplicación e implementación.
3. Exporte la configuración a nuevos archivos de plantilla (opcional).
4. Importe los archivos de plantilla a otros dispositivos Citrix ADC que requieran una configuración similar de la aplicación AppExpert

Personalización de la configuración

July 8, 2022

Después de comprobar que la aplicación AppExpert funciona correctamente, puede personalizar la configuración para adaptarla a sus requisitos.

Después de comprobar que la configuración de la aplicación AppExpert funciona correctamente, puede configurar la aplicación y los ajustes de implementación para que se ajusten a sus requisitos. Al importar una plantilla de aplicación y un archivo de implementación, el sistema rellena automáticamente la aplicación de destino con los valores de configuración disponibles (como unidades de aplicación, reglas de unidades de aplicación, directivas, configuración de persistencia, métodos de equilibrio de carga, perfiles y configuración de tráfico). En esta aplicación, puede configurar parámetros de implementación, como puntos finales públicos, servicios y grupos de servicios para cada subconjunto de tráfico. Si desea que la aplicación AppExpert administre un subconjunto

de tráfico que no está incluido en la plantilla, puede agregar una unidad de aplicación para un subconjunto de tráfico o modificar la unidad de aplicación existente. Después de personalizar la configuración, también puede especificar el orden de evaluación de cada subconjunto de tráfico que administra la aplicación.

La configuración de una aplicación AppExpert consta de los siguientes pasos:

1. Configuración de puntos finales públicos
2. Configuración de unidades de aplicación
3. Especificación del orden de evaluación
4. Visualización de la configuración de la aplicación mediante el

Además, puede configurar las directivas que proporciona la plantilla. Si la plantilla de aplicación AppExpert no incluye directivas para una función específica de Citrix ADC, como Rewrite o Application Firewall, puede configurar sus propias directivas.

Configurar dispositivos de punto final públicos

June 22, 2022

Si no especificó un punto final público al importar una aplicación de AppExpert, puede especificar puntos de enlace públicos después de crear la aplicación. Puede configurar un punto de enlace público de tipo HTTP y un punto de enlace público de tipo HTTPS para su aplicación AppExpert.

Si los endpoints ya están configurados para la aplicación, puede disociarlos de la aplicación AppExpert y eliminar los dispositivos de punto final que ya no necesite. Tenga en cuenta que al disociar un punto final público de la aplicación AppExpert, el punto final se desvincula automáticamente de la unidad de aplicación asociada, pero no se elimina del sistema.

Para configurar puntos finales públicos para una aplicación AppExpert:

1. Vaya a **AppExpert** > **Aplicaciones**.
2. En el panel de detalles, haga clic con el botón derecho en la aplicación para la que desea configurar puntos de enlace públicos y, a continuación, haga clic en Modificar.
3. En la página **Aplicaciones**, vaya a la sección **Punto final público** y haga clic en el icono del lápiz.
4. En el control deslizante **Dispositivo de punto final público**, defina los siguientes parámetros.
   a) Tipo de punto final público. Seleccione el botón de opción para definir el tipo de punto final.
   b) Nombre. Nombre del punto final público.
   c) Dirección IP. Dirección IP del punto final público.
   d) Puerto. Número de puerto del punto final público.
   e) Protocolo. Seleccione un tipo de protocolo como HTTP o HTTPS.
5. Haga clic en **Continuar.**

6. En la sección **Unidades de aplicación**, seleccione una unidad de aplicación de la lista.
7. Haga clic en **Continuar** para configurar la directiva y los detalles del servidor.
8. Haga clic en **Aceptar** y luego en Listo
9. Haga clic en Cerrar.

Para obtener más información sobre los parámetros del cuadro de diálogo **Configurar punto final público**, consulte Cambio de contenido.

Configurar servicios y grupos de servicios para una unidad de aplicación

June 22, 2022

Al configurar un servicio o grupo de servicios, puede modificar un servicio o grupo de servicios existente o agregar nuevos servicios a la aplicación AppExpert. Agregue servicios o grupos de servicios si no los especificó al importar la plantilla de aplicación. También agrega servicios y grupos de servicios cuando aumenta el número de servidores que alojan instancias de la aplicación. Puede configurar un servicio y un grupo de servicios para una unidad de aplicación solo después de configurar el servicio o el grupo de servicios para la aplicación AppExpert.

Para configurar un servicio o grupo de servicios para la aplicación AppExpert:

1. Vaya a **AppExpert** > **Aplicaciones**.
2. En el panel de detalles, haga clic con el botón secundario del mouse en la aplicación y haga clic en **Modificar**.
3. En la página **Aplicaciones**, seleccione una unidad de aplicación y, a continuación, haga clic en **Continuar**.
4. En la sección **Servicios y grupos de servicios**, haga lo siguiente:
   a) En el control deslizante Enlace de servicio, defina los siguientes parámetros.
      i. Servicio. Seleccione un servicio de equilibrio de carga de la lista o cree uno nuevo.
      ii. Peso Proporcione un valor de peso para el servicio.
   b) Haga clic en **Vincular** y luego en **Listo.**
   c) En el control deslizante ServiceGroup Binding, defina los siguientes parámetros:
      i. Nombre del grupo de servicios. Seleccione un grupo de servicios de equilibrio de carga o cree un grupo de servicios nuevo.
      ii. Haga clic en **Enlazar** y **,**a
   d) Haga clic en **Listo**.
5. Haga clic en **Continuar** para establecer otras configuraciones.

Creación de unidades de aplicación

June 22, 2022

Es posible que necesite agregar unidades de aplicación para subconjuntos de tráfico que sean específicas de la implementación de su aplicación web o que no estén definidas en la plantilla. Al crear una unidad de aplicación, debe configurar una regla para la unidad de aplicación.

Para crear una unidad de aplicación para la aplicación AppExpert:

1. Vaya a **AppExpert** > **Aplicaciones**.
2. En el panel de detalles, haga clic con el botón secundario del mouse en la aplicación a la que quiere agregar una unidad de aplicación y, a continuación, haga clic en **Agregar**.
3. En la página **Aplicaciones**, vaya a la sección **Unidades de aplicación** y haga clic en el icono del **lápiz**.

Para configurar expresiones de directivas para una unidad de aplicación:

1. Vaya a **AppExpert** > **Aplicaciones**.
2. En el panel de detalles, haga clic con el botón secundario del mouse en la aplicación a la que quiere agregar una unidad de aplicación y, a continuación, haga clic en **Agregar**.
3. En la página **Aplicaciones**, vaya a la sección **Unidades de aplicación** y haga clic en el icono **+** para crear una unidad y agregar expresiones de directiva.
4. Para especificar el formato de la nueva expresión, realice una de las siguientes acciones:
    a) Para especificar que quiere configurar una expresión de directiva en el cuadro Regla, haga clic en Sintaxis clásica.
    b) Para especificar que quiere configurar una expresión avanzada en el cuadro Regla, haga clic en Directiva avanzada.
    c) En el cuadro Regla, configure la expresión.
5. Haga clic en **Aceptar**.

Configuración de reglas de unidades de aplicación

June 22, 2022

Es posible que quiera configurar una regla de unidad de aplicación para incluir o excluir determinados tipos de tráfico. Al configurar la regla, también puede definir la sintaxis de la expresión.

Para configurar una regla de unidad de aplicación:

1. En el panel de navegación de la GUI, expanda AppExpert y, a continuación, haga clic en **Aplicaciones**.

2. En el panel de detalles, haga clic con el botón secundario del mouse en la unidad de aplicación para la que quiere modificar la regla y, a continuación, haga clic en **Abrir**.
3. En el cuadro de diálogo Configurar unidad de aplicación, haga lo siguiente:
   a) Para especificar el formato de la nueva expresión, realice una de las siguientes acciones:
      - Para especificar que quiere configurar una expresión de directiva avanzada en el cuadro Regla, haga clic en **Sintaxis clásica**.
      - Para especificar que desea configurar una expresión avanzada en el cuadro Regla, haga clic en **Directiva avanzada**.
   b) En el cuadro Regla, configure la expresión.
4. Haga clic en **Aceptar**.

Configuración de directivas para unidades de aplicación

June 22, 2022

Para una aplicación AppExpert, puede configurar directivas de compresión, almacenamiento en caché, reescritura, respuesta y firewall de aplicaciones. Las plantillas que descarga del sitio web de Citrix Community le proporcionan un conjunto de directivas que cumplen los requisitos de administración de aplicaciones más comunes. Es posible que quiera ajustar o personalizar estas directivas. Si el conjunto de directivas proporcionado para una unidad de aplicación determinada no incluye directivas para una función concreta, puede crear y enlazar sus propias directivas para esa función.

Si crea una aplicación AppExpert sin utilizar una plantilla, debe configurar todas las directivas que necesita la aplicación web.

La GUI utiliza varios iconos para indicar si las directivas están configuradas o no para una función. En el caso de una unidad de aplicación, si se configura una directiva para una función determinada, se muestra un icono que representa la función. Por ejemplo, si se configura una directiva de compresión para una unidad de aplicación, se muestra un icono de compresión en la columna Compresión de la unidad de aplicación. Para las funciones para las que no se ha configurado ninguna directiva, se muestra un icono que muestra un signo más (+).

Nota: Al configurar directivas para unidades de aplicación, es posible que deba configurar directivas y expresiones que estén en la directiva clásica o avanzada. Además, al configurar directivas de directivas avanzadas, es posible que necesite especificar parámetros como expresiones Goto e invocar bancos de directivas.

Para obtener información sobre cómo configurar directivas y expresiones en ambos formatos, consulte Directivas y expresiones.

Configuración de directivas de compresión

Puede utilizar directivas clásicas o avanzadas para configurar la compresión, pero no puede vincular directivas de compresión de ambos tipos a la misma unidad de aplicación.

Para configurar una directiva de compresión para una unidad de aplicación:

1. Vaya a **AppExpert** > **Aplicaciones**.
2. En el panel de detalles, en la fila de la unidad de aplicación que quiere configurar, haga clic en el icono proporcionado en la columna Compresión.
3. En el cuadro de diálogo Configurar directivas de compresión, realice una o varias de las acciones siguientes, según las tareas de configuración que quiera realizar:
   - Haga clic en Cambiar a directiva avanzada si quiere configurar una directiva de compresión avanzada de directivas. Si quiere enlazar o configurar directivas de compresión clásicas y si se encuentra en la vista de directivas avanzadas, puede hacer clic en Cambiar a sintaxis clásica para volver a la vista de directivas clásica y empezar a modificar directivas clásicas vinculadas o crear y enlazar nuevas directivas de compresión clásicas.
     Importante: Esta configuración también determina qué directivas se muestran cuando se desea insertar una directiva. Por ejemplo, si se encuentra en la vista de directivas avanzada, al hacer clic en Insertar directiva, la lista que aparece en la columna Nombre de la directiva incluirá únicamente directivas avanzadas. No se pueden enlazar directivas de ambos tipos a una unidad de aplicación.
   - Si quiere configurar directivas clásicas, haga clic en Solicitud o Respuesta, en función de si quiere que la directiva se evalúe en el momento de la solicitud o en el momento de la respuesta.
     Puede configurar directivas de compresión clásicas tanto en tiempo de solicitud como en tiempo de respuesta para una unidad de aplicación. Después de evaluar todas las directivas de tiempo de solicitud, si no se encuentra ninguna coincidencia, el dispositivo evalúa las directivas de tiempo de respuesta.
   - Para modificar una directiva de compresión que ya está vinculada a la unidad de aplicación, haga clic en el nombre de la directiva y, a continuación, haga clic en Modificar directiva. A continuación, en el cuadro de diálogo Configurar directiva de compresión, modifique la directiva y, a continuación, haga clic en Aceptar.
     Para obtener información sobre cómo modificar una directiva de compresión, consulte Compresión.
   - Para desvincular una directiva, haga clic en el nombre de la directiva y, a continuación, haga clic en Desvincular directiva.
   - Para modificar la prioridad asignada a una directiva, haga doble clic en el valor de prioridad y, a continuación, introduzca un nuevo valor.
   - Para regenerar prioridades asignadas, haga clic en Regenerar prioridades.
   - Para insertar una nueva directiva, haga clic en **Insertar directiva** y, en la lista que se mues-

tra en la columna Nombre de directiva, haga clic en **Nueva directiva**. A continuación, en el cuadro de diálogo Crear directiva de compresión, configure la directiva y, a continuación, haga clic en **Crear**.
Para obtener información sobre cómo modificar una directiva de compresión, consulte Compresión.

- Si va a configurar una expresión de directiva avanzada, haga lo siguiente:
  - En la columna Expresión GoTo, seleccione una expresión GoTo.
  - En la columna Invocar, especifique el banco de directivas que quiere invocar si la directiva actual se evalúa como TRUE.

4. Haga clic en **Aplicar cambios**y, a continuación, en **Cerrar**.

Configuración de directivas de almacenamiento en caché

Solo puede utilizar expresiones y directivas avanzadas para configurar directivas de almacenamiento en caché.

Para configurar directivas de almacenamiento en caché para una unidad de aplicación:

1. Vaya a **AppExpert** > **Aplicaciones**.
2. En el panel de detalles, en la fila de la unidad de aplicación que quiere configurar, haga clic en el icono proporcionado en la columna Almacenamiento en caché.
3. En el cuadro de diálogo Configurar directivas de caché, realice una o varias de las acciones siguientes, según las tareas de configuración que quiera realizar:
   - Haga clic en Solicitud o Respuesta, en función de si quiere que la directiva se evalúe en el momento de la solicitud o en el momento de la respuesta.
     Puede configurar directivas de almacenamiento en caché tanto de tiempo de solicitud como de tiempo de respuesta para una unidad de aplicación. Después de evaluar todas las directivas de tiempo de solicitud, si no se encuentra ninguna coincidencia, el dispositivo evalúa las directivas de tiempo de respuesta.
   - Para modificar una directiva de almacenamiento en caché que ya está vinculada a la unidad de aplicación, haga clic en el nombre de la directiva y, a continuación, haga clic en Modificar directiva. A continuación, en el cuadro de diálogo **Configurar directiva de caché**, modifique la directiva y, a continuación, haga clic en **Aceptar**.
     Para obtener información sobre cómo modificar una directiva de almacenamiento en caché, consulte Almacenamiento en caché integrado.
   - Para desvincular una directiva, haga clic en el nombre de la directiva y, a continuación, haga clic en **Desvincular directiva**.
   - Para modificar la prioridad asignada a una directiva, haga doble clic en el valor de prioridad y, a continuación, introduzca un nuevo valor.
   - Para volver a generar las prioridades asignadas, haga clic en **Regenerar prioridades**.
   - Para insertar una nueva directiva, haga clic en **Insertar directiva** y, en la lista que se mues-

tra en la columna Nombre de directiva, haga clic en **Nueva directiva**. A continuación, en el cuadro de diálogo **Crear directiva de caché**, configure la directiva y, a continuación, haga clic en **Crear**.
Para obtener información sobre cómo modificar una directiva de almacenamiento en caché, consulte Almacenamiento en caché integrado.

- En la columna Expresión GoTo, seleccione una expresión GoTo.
- En la columna Invocar, especifique el banco de directivas que quiere invocar si la directiva actual se evalúa como TRUE.

4. Haga clic en **Aplicar cambios**y, a continuación, en **Cerrar**.

Configuración de directivas de reescritura

Solo puede usar expresiones y directivas avanzadas para configurar directivas de reescritura.

Para configurar directivas de reescritura para una unidad de aplicación:

1. Vaya a **AppExpert** > **Aplicaciones**.
2. En el panel de detalles, en la fila de la unidad de aplicación que quiere configurar, haga clic en el icono proporcionado en la columna Reescritura.
3. En el cuadro de diálogo **Configurar directivas de reescritura**, realice una o varias de las acciones siguientes, según las tareas de configuración que quiera realizar:
   - Haga clic en Solicitud o Respuesta, en función de si quiere que la directiva se evalúe en el momento de la solicitud o en el momento de la respuesta.
     Puede configurar directivas de reescritura tanto en tiempo de solicitud como en tiempo de respuesta para una unidad de aplicación. Después de evaluar todas las directivas de tiempo de solicitud, si no se encuentra ninguna coincidencia, el dispositivo evalúa las directivas de tiempo de respuesta.
   - Para modificar una directiva de reescritura que ya está vinculada a la unidad de aplicación, haga clic en el nombre de la directiva y, a continuación, haga clic en **Modificar directiva**.
     A continuación, en el cuadro de diálogo Configurar directiva de reescritura, modifique la directiva y, a continuación, haga clic en **Aceptar**.
     Para obtener información sobre cómo modificar una directiva de reescritura, consulte Reescritura.
   - Para desvincular una directiva, haga clic en el nombre de la directiva y, a continuación, haga clic en **Desvincular directiva**.
   - Para modificar la prioridad asignada a una directiva, haga doble clic en el valor de prioridad y, a continuación, introduzca un nuevo valor.
   - Para volver a generar las prioridades asignadas, haga clic en **Regenerar prioridades**.
   - Para insertar una nueva directiva, haga clic en **Insertar directiva** y, en la lista que se muestra en la columna **Nombre de directiva**, haga clic en **Nueva directiva.** A continuación, en el cuadro de diálogo **Crear directiva de reescritura**, configure la directiva y, a contin-

uación, haga clic en **Crear**.
Para obtener información sobre cómo modificar una directiva de reescritura, consulte Reescritura.
- En la columna Expresión GoTo, seleccione una expresión GoTo.
- En la columna Invocar, especifique el banco de directivas que quiere invocar si la directiva actual se evalúa como TRUE.

4. Haga clic en **Aplicar cambios**y, a continuación, en **Cerrar**.

Configuración de directivas de respuesta

Solo puede usar expresiones y directivas avanzadas para configurar las directivas de Responder.

Para configurar directivas de Responder para una unidad de aplicación:

1. Vaya a **AppExpert** > **Aplicaciones**.
2. En el panel de detalles, en la fila de la unidad de aplicación que quiere configurar, haga clic en el icono proporcionado en la columna Respondedor.
3. En el cuadro de diálogo **Configurar directivas de respuesta**, realice una o varias de las acciones siguientes, según las tareas de configuración que quiera realizar:
   - Para modificar una directiva de filtro que ya está vinculada a la unidad de aplicación, haga clic en el nombre de la directiva y, a continuación, haga clic en **Modificar directiva**. A continuación, en el cuadro de diálogo Configurar directiva de Responder, modifique la directiva y, a continuación, haga clic en **Aceptar**.
     Para obtener información sobre cómo modificar una directiva de Respondedor, consulte Respondedor.
   - Para desvincular una directiva, haga clic en el nombre de la directiva y, a continuación, haga clic en **Desvincular directiva**.
   - Para modificar la prioridad asignada a una directiva, haga doble clic en el valor de prioridad y, a continuación, introduzca un nuevo valor.
   - Para volver a generar las prioridades asignadas, haga clic en **Regenerar prioridades**.
   - Para insertar una nueva directiva, haga clic en Insertar directiva y, en la lista que aparece en la columna Nombre de la directiva, haga clic en Nueva directiva. A continuación, en el cuadro de diálogo Crear directiva de Responder, configure la directiva y, a continuación, haga clic en Crear.
     Para obtener información sobre cómo modificar una directiva de Respondedor, consulte Respondedor.
   - En la columna Expresión GoTo, seleccione una expresión GoTo.
   - En la columna Invocar, especifique el banco de directivas que quiere invocar si la directiva actual se evalúa como TRUE.
4. Haga clic en **Aplicar cambios**y, a continuación, en **Cerrar**.

Configuración de directivas de firewall de aplicaciones

Puede configurar directivas y expresiones tanto clásicas como avanzadas para Application Firewall. Sin embargo, si una directiva de un tipo ya está enlazada globalmente o a un servidor virtual configurado en el dispositivo, no se puede enlazar una directiva del otro tipo a una unidad de aplicación. Por ejemplo, si una directiva avanzada ya está enlazada de forma global o a un servidor virtual, no se puede enlazar una directiva clásica a una unidad de aplicación.

Para configurar las directivas de Application Firewall para una unidad de aplicación:

1. Vaya a **AppExpert** > **Aplicaciones**.
2. En el panel de detalles, en la fila de la unidad de aplicación que quiere configurar, haga clic en el icono proporcionado en la columna **Firewall de aplicaciones**.
3. En el cuadro de diálogo **Configurar directivas de firewall de aplicaciones**, realice una o varias de las acciones siguientes, en función de las tareas de configuración que quiera realizar:
   - Haga clic en Expresión clásica o Expresión avanzada según el tipo de expresión que quiera configurar para la directiva Application Firewall.
     Importante: Esta configuración también determina qué directivas se muestran cuando se quiere insertar una directiva. Por ejemplo, si selecciona Expresión avanzada, al hacer clic en **Insertar directiva**, la lista que aparece en la columna **Nombre de la directiva** incluirá únicamente las directivas de directivas avanzadas. No se pueden enlazar directivas de ambos tipos a una unidad de aplicación. Esta opción no está disponible si una directiva de cualquiera de los dos tipos ya está vinculada de forma global o a un servidor virtual.
   - Para modificar una directiva de firewall de aplicaciones que ya está vinculada a la unidad de aplicación, haga clic en el nombre de la directiva y, a continuación, haga clic en Modificar directiva. A continuación, en el cuadro de diálogo Configurar directiva de firewall de aplicaciones, modifique la directiva y, a continuación, haga clic en Aceptar.
     Para obtener información sobre cómo modificar una directiva de firewall de aplicaciones, consulte Directivas.
   - Para desvincular una directiva, haga clic en el nombre de la directiva y, a continuación, haga clic en Desvincular directiva.
   - Para modificar la prioridad asignada a una directiva, haga doble clic en el valor de prioridad y, a continuación, introduzca un nuevo valor.
   - Para regenerar prioridades asignadas, haga clic en Regenerar prioridades.
   - Para insertar una nueva directiva, haga clic en **Insertar directiva** y, en la lista que aparece en la columna **Nombre de la directiva**, haga clic en Nueva directiva. A continuación, en el cuadro de diálogo **Crear directiva de firewall de aplicaciones**, configure la directiva y, a continuación, haga clic en **Crear**.
     Para obtener información sobre cómo modificar una directiva de firewall de aplicaciones, consulte Directivas.
4. Haga clic en **Aplicar cambios**y, a continuación, en **Cerrar**.

Configuración de unidades de aplicación

June 22, 2022

Para configurar una unidad de aplicación mediante la GUI:

1. Vaya a la sección **AppExpert** > **Aplicaciones** > **Unidad de aplicación** y, a continuación, haga clic en el icono más para agregar una nueva unidad de aplicación para un subconjunto de tráfico.
2. En el control deslizante **Unidad de aplicación**, defina los siguientes parámetros:

   - Nombre
   - Expresión

   Puede insertar una expresión agregando los componentes de la expresión manualmente o mediante el enlace Editor de expresiones. Para agregar una expresión manualmente, introduzca un componente selector y, a continuación, escriba un punto (.) para mostrar una lista en la que pueda seleccionar el siguiente componente. Por ejemplo, escriba HTTP y, a continuación, escriba un punto. Aparecerá un menú desplegable. El contenido de este menú proporciona las palabras clave que pueden seguir a la palabra clave inicial introducida. Seleccione un componente en el menú desplegable. El cuadro de texto Expresión* ahora muestra los componentes que ha agregado a la expresión (por ejemplo, HTTP.REQ). Siga agregando componentes hasta que se forme la expresión completa.

   Si prefiere ayuda para formar la expresión, puede usar el enlace Editor de expresiones. En la página Editor de expresiones, puede crear una expresión seleccionando componentes en los cuadros desplegables. Seleccione los componentes y haga clic en Listo para insertar la expresión en la página Unidad de aplicación.
3. Haga clic en **Continuar** para vincular servicios y grupos de servicios.
4. Haga clic en la sección **Servicio** para seleccionar o agregar un servicio virtual y vincularlo a la unidad de aplicación.
5. Haga clic en **Continuar** y haga clic en la sección **Grupo de servicios** para seleccionar o agregar un grupo de servicios virtual y vincularlo a la unidad de aplicación.
6. Haga clic en **Vincular** y **continuar** para configurar la configuración avanzada (como directivas, método, persistencia, protección, perfiles, inserción, autenticación y configuración de tráfico) para la unidad de aplicación.
7. Haga clic en el icono **más** de cada sección para establecer los parámetros de configuración.
8. Haga clic en **Aceptar** y luego en **Listo**.

Para modificar una unidad de aplicación de una aplicación mediante la GUI:

Vaya a **AppExpert** > **Aplicaciones**, seleccione una aplicación y haga clic en **Modificar**. En la sección **Unidad de aplicación**, seleccione una entidad, haga clic en el icono de edición y modifique la configuración de la unidad de aplicación.

Nota: No puede modificar el nombre y la expresión de regla de una unidad de aplicación existente.

Los tutoriales en vídeo de Citrix ADC le permiten comprender las funciones de Citrix ADC de una manera fácil y sencilla. Consulte el vídeo https://www.youtube.com/watch?v=bJ5_i8fV2hc para aprender a configurar una unidad de aplicación.

Configuración de puntos finales públicos para una aplicación

June 22, 2022

Para configurar puntos finales públicos para una aplicación mediante la GUI:

1. Vaya a **AppExpert** > **Aplicaciones**, seleccione una entidad de aplicación y, a continuación, haga clic en **Modificar**.
2. En la sección **Punto final público**, haga clic en **+** para configurar un nuevo punto final público.
3. En el control deslizante **Dispositivo de punto final público**, realice una de las siguientes acciones:
   a) Haga clic en **Nuevo** para crear un nuevo punto final.
   b) Haga clic en **Punto final público existente** para seleccionar un punto final de la lista desplegable.
4. Defina los siguientes parámetros de punto final:
   a) Nombre
   b) Dirección IP
   c) Protocolo
   d) Port
5. Haga clic en **Continuar** para configurar opciones adicionales, como unidades de aplicación, enlaces de servidor GSLB, directivas, perfiles, inserción, configuración de tráfico y autenticación.
6. Haga clic en **Aceptar** y luego en **Listo**.
7. Haga clic en **Continuar** y, a continuación, en **Listo**.

Para modificar un punto final público de una aplicación mediante la GUI:

Vaya a **AppExpert** > **Aplicaciones**, seleccione una aplicación y haga clic en **Modificar**. En la sección **Punto final público**, seleccione un punto final, haga clic en el icono del lápiz y modifique la configuración del punto final.

Para eliminar un punto final público de una aplicación mediante la GUI:

Vaya a **AppExpert** > **Aplicaciones** > **Punto final público,** haga clic en el icono del lápiz para ver el icono de eliminación junto a la entidad.

Los tutoriales en vídeo de Citrix ADC le permiten comprender las funciones de Citrix ADC de una manera fácil y sencilla. Consulte el vídeo https://www.youtube.com/watch?v=z4v-edQiVpw para aprender a configurar un dispositivo de punto final público.

Especificación del orden de evaluación de las unidades de aplicación

June 22, 2022

Las reglas de la unidad de aplicación se evalúan en el orden en que se colocan en la GUI. La regla que se configura para la unidad de aplicación superior siempre se configura primero, seguida de la regla que se configura para la segunda unidad de aplicación superior, y así sucesivamente. La unidad de aplicación predeterminada siempre se evalúa en último lugar.

Cuando una solicitud coincide con la regla que está configurada para una unidad de aplicación, la solicitud es procesada por la unidad de aplicación y no se realiza ninguna otra coincidencia. Por lo tanto, el orden de evaluación de las unidades de aplicación se convierte en un factor importante si los subconjuntos de tráfico para dos o más unidades de aplicación se superponen. Si los subconjuntos de tráfico de dos o más unidades de aplicación se superponen, debe especificar el orden en el que una solicitud entrante se compara con las reglas de la unidad de aplicación.

Para especificar el orden de evaluación de las unidades de aplicación:

1. Vaya a **AppExpert** > **Aplicaciones**, seleccione una aplicación y haga clic en **Modificar**. En la sección **Unidad de aplicación**, haga clic en el icono de **lápiz** y, a continuación, sitúe el cursor sobre la casilla de verificación situada a la izquierda del nombre de la unidad de aplicación. Haga clic en el icono que aparece junto a la casilla de verificación y mantenga pulsado el mouse para arrastrar la aplicación hacia arriba o hacia abajo a una nueva ubicación en la lista de prioridades.

Configuración de grupos de persistencia para unidades de aplicaciones

June 22, 2022

Puede configurar un grupo de persistencia para las unidades de aplicación en una aplicación AppExpert. En el contexto de una aplicación AppExpert, un grupo de persistencia es un grupo de unidades de aplicación que puede tratar como una sola entidad con el fin de aplicar una configuración de persistencia común. Cuando la aplicación se exporta a un archivo de plantilla de aplicación, se incluye la configuración del grupo de persistencia y se aplica automáticamente a las unidades de la aplicación al importar la aplicación AppExpert.

Para configurar un grupo de persistencia para una aplicación mediante la GUI:

1. Vaya a **AppExpert** > **Aplicaciones**.
2. En el cuadro de diálogo **Vista de aplicaciones**, haga clic en el nombre de la aplicación para cuyas unidades de aplicación desea configurar un grupo de persistencia y, a continuación, haga clic en Configurar **grupos de persistencia**.
3. En el cuadro de diálogo **Configurar grupos de persistencia**, realice una de las siguientes acciones:
   - Para agregar un grupo de persistencia, haga clic en **Agregar**.
   - Para modificar un grupo de persistencia, haga clic en **Abrir**.
4. En el cuadro de diálogo **Crear grupo** de **persistencia o Configurar grupo** de persistencia, defina los siguientes parámetros:
   - Nombre del grupo: nombre del grupo de persistencia. Para que el dispositivo Citrix ADC reconozca el grupo de persistencia como parte de la configuración de la aplicación, el nombre de la aplicación AppExpert debe incluirse en el nombre del grupo de persistencia, como prefijo. Por lo tanto, de forma predeterminada, el dispositivo muestra el prefijo en el cuadro Nombre de grupo y no se puede eliminar ese prefijo. Introduzca un nombre de su elección después del prefijo.
   - Persistencia: tipo de persistencia del servidor virtual. Si selecciona SOURCEIP, en el cuadro Máscara de red IPv4, introduzca una máscara de red que especifique el número de bits que el dispositivo debe tener en cuenta al crear sesiones de persistencia. Si selecciona COOKIEINSERT, en los cuadros Dominio de cookie y Nombre de cookie, especifique un atributo de dominio para enviar en la directiva Set-Cookie y un nombre para la cookie, respectivamente.
   - Tiempo de espera: período de tiempo durante el que está en vigor una sesión de persistencia.
   - Persistencia de backup: tipo de persistencia de backup para el grupo.
   - Tiempo de espera de respaldo: período, en minutos, durante el cual la persistencia del respaldo está en vigor.
   - Unidades de aplicación: para agregar una unidad de aplicación al grupo de persistencia, en el cuadro Unidades de aplicación disponibles, haga clic en la unidad de aplicación y, a continuación, haga clic en Agregar. Para eliminar una unidad de aplicación del grupo de persistencia, en el cuadro Unidades de aplicación configuradas, haga clic en la unidad de aplicación y, a continuación, haga clic en **Eliminar**.
5. Haga clic en **Aceptar**.

Visualización de aplicaciones de AppExpert y configuración de entidades mediante el visualizador de aplicaciones

June 22, 2022

La función Visualizador muestra una representación gráfica de la configuración de una aplicación. Incluye el nombre del punto final público, las unidades de aplicación asignadas al punto final público y el número de directivas y servicios vinculados a la aplicación. Puede usar el visualizador para obtener una descripción general visual de la configuración de una aplicación AppExpert y configurar algunas de las entidades que se muestran. De forma predeterminada, el visualizador muestra las unidades de aplicación, los servicios y los monitores de la aplicación seleccionada.

Para ver una aplicación AppExpert mediante el visualizador de aplicaciones:

1. Vaya a **AppExpert** > **Aplicaciones**, seleccione una entidad de aplicación y haga clic en **Visualizador**.

Configuración de la autenticación, autorización y auditoría de usuarios

June 22, 2022

Puede configurar la autorización de los usuarios y grupos para permitirles acceder a una aplicación AppExpert. Si el usuario o grupo AAA para el que desea configurar permisos aún no se ha creado, puede crearlo desde AppExpert y, a continuación, configurar los permisos para el acceso a la aplicación.

Para configurar usuarios AAA y grupos de usuarios AAA para una aplicación mediante la utilidad de configuración

1. Vaya a **AppExpert** > **Aplicaciones**, seleccione una entidad de aplicación y, a continuación, haga clic en **Modificar**.
2. En la sección **Configuración avanzada**, haga clic en **Autorización**y configure los usuarios y grupos de usuarios autorizados.
3. Haga clic en la sección Usuario **AAA** para vincular a los usuarios autorizados a la aplicación.
4. En el control deslizante **Usuario de AAA**, defina los parámetros.
5. Haga clic en **Continuar** y, a continuación, haga clic en **Directivas de autorización** en la sección **Configuración avanzada**.
6. En el control deslizante **Directiva de autorización**, enlace una directiva de autorización a la aplicación.
7. Haga clic en **Continuar**y, a continuación, haga clic en la sección **Grupo de autorización** de la sección **Configuración avanzada**.
8. En el control deslizante Enlace de **grupo AAA**, enlace un grupo de usuarios de autorización a la aplicación.
9. Haga clic en **Continuar** y, a continuación, haga clic en **Directivas** en la sección **Configuración avanzada**.

10. En el control deslizante **Directivas**, enlace una directiva **Audit Syslog** o **Audit NSLog** a la aplicación.
11. Haga clic en **Continuar** y, a continuación, en **Listo**.

Para modificar los usuarios de AAA y los grupos de usuarios de AAA de una aplicación mediante la GUI:

Vaya a **AppExpert** > **Aplicaciones** > **Configuración avanzada** y haga clic en **Autorización**. A continuación, haga clic en el icono de edición y especifique valores para la configuración de autorización de usuarios o grupos de usuarios

Para eliminar usuarios de AAA y grupos de usuarios de AAA mediante la interfaz gráfica de usuario:

Vaya a **AppExpert** > **Aplicaciones**, seleccione una aplicación y haga clic en **Modificar**. En la página **Aplicaciones**, haga clic en **Configuración avanzada** y haga clic en **Autorización**. Haga clic en el icono de eliminar situado junto a la entidad.

Supervisión de una aplicación Citrix ADC

July 8, 2022

Después de personalizar la aplicación AppExpert, puede ver las estadísticas de la aplicación para asegurarse de que la aplicación y todas sus entidades funcionan correctamente. También puede usar el Visualizador de aplicaciones para supervisar las estadísticas asociadas con ciertas entidades, como directivas y servidores virtuales.

También puede ver los contadores de visitas de varias entidades a intervalos regulares para asegurarse de que los contadores se están actualizando.

Ver estadísticas de aplicaciones

En el nodo **Aplicaciones**, puede seleccionar una aplicación y ver la página Estadísticas de la aplicación. En la página Estadísticas, puede supervisar el estado y los estados de los puntos finales públicos y las unidades de aplicación, y ver la siguiente información estadística:

- Solicitudes y respuestas por segundo para cada uno de los puntos finales públicos y unidades de aplicación.
- Bytes por segundo, en cada punto final, para el tráfico entrante y saliente.
- Los contadores de visitas de la unidad de aplicación y el número de conexiones de cliente y servidor para cada unidad de aplicación.
- Estadísticas de los servicios que están vinculados a las unidades de aplicación.

En la página Estadísticas, también puede ver el uso de la CPU, el uso de la memoria y los registros del sistema.

Para ver las estadísticas de una aplicación:

1. Vaya a **AppExpert** > **Aplicaciones**.
2. En el panel de detalles, haga clic en la aplicación de la que desea ver las estadísticas y, a continuación, haga clic en **Estadísticas**.

Supervisión de una aplicación mediante el visualizador de aplicaciones

Puede usar el Visualizador de aplicaciones para supervisar la cantidad de solicitudes recibidas por segundo en un momento dado por los servidores virtuales y la cantidad de visitas por segundo en un momento dado para las directivas de reescritura, respuesta y caché.

Para ver la información estadística de los servidores virtuales, las directivas de reescritura, las directivas de respuesta y las directivas de caché en el visualizador:

1. Vaya a **AppExpert** > **Aplicaciones**.
2. En el panel de detalles, seleccione la aplicación de la que desea ver la información estadística y, a continuación, haga clic en **Visualizador**.
3. En la ventana **Visualizador de aplicaciones**, haga lo siguiente:
   - Para ver las estadísticas, haga clic en **Mostrar estadísticas**.
     La información estadística se muestra en los nodos respectivos del visualizador. Esta información no se actualiza en tiempo real y debe actualizarse manualmente.
   - Para actualizar la información estadística, haga clic en **Actualizar estadísticas**.

Visualización de aciertos

Los contadores de visitas que se proporcionan para varias entidades de aplicaciones de AppExpert le permiten supervisar el funcionamiento de los puntos finales públicos y las unidades de aplicación. Para una aplicación, el cuadro de diálogo Hits muestra el número total de solicitudes recibidas por cada punto final público configurado. Para una unidad de aplicación, el cuadro de diálogo Hits muestra el número de solicitudes que la unidad de aplicación procesó desde cada uno de los extremos públicos y el recuento total de aciertos. Para obtener instrucciones sobre cómo ver contadores de visitas, consulte Verificación y prueba de la configuración.

Eliminar una aplicación

June 22, 2022

Si ya no necesita una aplicación y sus unidades de aplicación, puede eliminarla. Cuando elimina una aplicación AppExpert, los servicios de backend no se eliminan y cualquier punto final público que la aplicación haya utilizado estará disponible para que lo usen otras aplicaciones.

Al eliminar una aplicación, también se le pide que especifique si desea eliminar las directivas y acciones enlazadas que no se utilizan en ningún otro lugar.

Para eliminar una unidad de aplicación de una aplicación mediante la GUI:

Vaya a **AppExpert** > **Aplicaciones**, seleccione una aplicación y haga clic en **Modificar**. En la sección **Unidad de aplicación**, haga clic en el icono de eliminar junto a la entidad

Configurar la autenticación, la autorización y la auditoría de aplicaciones

June 22, 2022

Puede configurar Autenticación, Autorización y Auditoría (AAA) para las aplicaciones que configure en el dispositivo. Una directiva de autenticación que se configura para una aplicación define el tipo de autenticación que se debe aplicar cuando un usuario o un grupo intenta acceder a la aplicación. Si se utiliza la autenticación externa, la directiva también especifica el servidor de autenticación externo. Las directivas de autorización configuradas para una aplicación especifican si un usuario o grupo en particular puede acceder a la aplicación. Las directivas de auditoría definen el tipo de registro de auditoría, el nivel en el que se realiza el registro y otras configuraciones del servidor de auditoría. Las directivas de autenticación y auditoría utilizan el formato de directiva clásico.

Las directivas de autenticación, autorización y auditoría se pueden configurar en cualquier orden. Sin embargo, antes de configurar AAA para una aplicación, debe configurar un punto final público para la aplicación.

La configuración de la autenticación para una aplicación implica especificar un FQDN de autenticación, un servidor virtual de autenticación, un certificado de servidor y directivas de autenticación y sesión. Las directivas de autenticación se enlazan automáticamente al servidor virtual de autenticación especificado para la aplicación.

Para configurar la autenticación de una aplicación AppExpert:

1. Vaya a **AppExpert** > **Aplicaciones**.
2. En el panel de detalles, realice una de las acciones siguientes:
    a) Haga clic en Agregar para agregar una autenticación para una nueva aplicación.
    b) Haga clic en Modificar para modificar una aplicación existente.
3. En la página **Aplicaciones**, seleccione una unidad de aplicación.
4. En la página deslizante **Unidad de aplicación**, haga clic en Autenticación en la sección **Configuración avanzada**.
5. En la sección **Autenticación**, seleccione el tipo de autenticación de la siguiente manera:
    a) Autenticación basada

b) Autentificación basada en 401
c) Nada

6. Haga clic en **Aceptar** y, a continuación, haga clic en **Listo**.

Configurar la autorización de aplicaciones

Puede configurar la autorización de los usuarios y grupos para permitirles acceder a una aplicación AppExpert. Si el usuario o grupo AAA para el que desea configurar permisos aún no se ha creado, puede crearlo desde AppExpert y, a continuación, configurar los permisos para el acceso a la aplicación.

Para configurar los permisos para que un usuario o grupo AAA acceda a una aplicación AppExpert:

1. Vaya a **AppExpert** > **Aplicaciones**.
2. En el panel de detalles, haga clic en la aplicación AppExpert para la que desea configurar un acceso de usuario o grupo.
3. En la página **Aplicaciones** y, a continuación, haga clic en Autorización en la sección **Configuración avanzada**.
4. Lleve a cabo una de las siguientes acciones:
   - Si el usuario o grupo AAA para el que desea configurar permisos ya está en el árbol Grupos/Usuarios, arrastre el usuario o el grupo desde el árbol Grupos/Usuarios al nodo Usuarios o Grupos del árbol de aplicaciones. A continuación, haga clic con el botón derecho en el usuario o grupo y, a
   - Si el usuario o grupo AAA para el que desea configurar permisos no está configurado en el dispositivo, en el árbol de aplicaciones, haga clic con el botón secundario en Usuarios o grupos y, a continuación, haga clic en Agregar. En el cuadro de diálogo Crear grupo AAA o Crear usuario AAA, rellene los valores, haga clic en Crear y, a continuación, haga clic en Cerrar.
     El usuario o el grupo se crean con el permiso establecido en Permitir. Para cambiar la configuración de permisos, haga clic con el botón secundario en el grupo o usuario y, a continuación, haga clic en la configuración
5. Haga clic en **Listo** y luego en **Cerrar**.

Configurar la auditoría de aplicaciones

Al configurar directivas de auditoría para una aplicación, debe especificar el servidor al que deben dirigirse los mensajes de registro, el formato de los mensajes registrados y el nivel de registro. Si lo desea, puede configurar otros parámetros, como la función de registro y el formato de fecha. Las directivas de auditoría se vinculan automáticamente a todos los puntos finales públicos de la aplicación AppExpert.

Para configurar las directivas de auditoría de una aplicación:

1. Vaya a **AppExpert** > **Aplicaciones**.
2. En el panel de detalles, haga clic en la aplicación para la que desea configurar las directivas de auditoría.
3. En la página del control deslizante Unidad de aplicación, haga clic en el icono + en la sección **Directivas** para configurar las directivas de auditoría.
4. En la página del control deslizante **Directivas**, seleccione el tipo de directiva como Auditoría de Syslog o Auditoría de Nslog y haga clic en **Continuar**.
5. En la sección Vinculación de directivas, defina los siguientes parámetros.
   a) Seleccione una directiva para la vinculación. Si no tiene una directiva de vinculación, haga clic en + para crear una nueva directiva.
   b) Para crear una nueva directiva de auditoría, en Nombre de directiva, haga clic en **Nueva directiva** y, a continuación, en la página **Directiva**, haga lo siguiente:
      i. En el cuadro Nombre, escriba un nombre para la directiva.
      ii. El cuadro Nombre ya contiene la cadena que se requiere al principio del nombre del servidor. No puede modificar la cadena.
      iii. En la lista Tipo de auditoría, seleccione el tipo de auditoría (SYSLOG o NSLOG).
      iv. Si el servidor de auditoría que desea especificar ya aparece en la lista de servidores, seleccione el servidor de la lista y, a continuación, si desea modificar la configuración del servidor, haga clic en Modificar. En el cuadro de diálogo Configurar servidor de auditoría, modifique la configuración según corresponda y, a continuación, haga clic en Aceptar. Para obtener más información sobre la configuración del cuadro de diálogo Configurar servidor de auditoría, consulte Auditoría de sesiones autenticadas.
      v. Si quiere configurar un nuevo servidor de auditoría, haga clic en Nuevo y, a continuación, en el cuadro de diálogo Crear servidor de auditoría, escriba un nombre para el servidor, especifique la dirección IP del servidor, el número de puerto y otras opciones, según corresponda. Cuando haya terminado, haga clic en **Aceptar**.
      vi. Haga clic en **Create**.
   c) Para cambiar las prioridades de las nuevas directivas de auditoría que creó, en Prioridad, para cada directiva para la que desea cambiar la prioridad, haga doble clic en el valor de prioridad y escriba el nuevo valor de prioridad.
   d) Para regenerar las prioridades, haga clic en **Regenerar prioridades**.
   e) Para desvincular una directiva, haga clic en la directiva y, a continuación, haga clic en **Desvincular directiva**.
   f) Para modificar una directiva, haga clic en la directiva y, a continuación, haga clic en **Modificar directiva.**
6. Haga clic en **Aplicar cambios y,** a continuación, en **Cerrar**.

Desactivación de AAA para una aplicación

Después de configurar AAA para una aplicación, puede inhabilitar la configuración de AAA para esa aplicación. Al inhabilitar AAA para una aplicación, la configuración no se pierde. Puede habilitar AAA para la aplicación cuando quiera volver a aplicar la configuración.

Para habilitar o inhabilitar AAA para una aplicación:

1. Vaya a **AppExpert** > **Aplicaciones**.
2. En el panel de detalles, haga clic en la aplicación para la que desea habilitar o inhabilitar AAA y, a continuación, realice una de las siguientes acciones:
3. Para inhabilitar AAA en la aplicación, haga clic en **Desactivar AAA.**
4. Para habilitar AAA en la aplicación, haga clic **en Activar AAA**.

Configuración de una aplicación Citrix ADC personalizada

July 8, 2022

Si una plantilla de aplicación de AppExpert no está disponible para la aplicación web que desea administrar a través del dispositivo Citrix ADC, o si las plantillas de aplicación de AppExpert disponibles no se ajustan a sus requisitos, puede crear una aplicación de AppExpert sin una plantilla.

Para crear una aplicación AppExpert sin plantilla, primero debe crear una aplicación y unidades de aplicación. A continuación, se configuran los puntos finales públicos, los servicios y los grupos de servicios. Por último, configura las directivas que determinan cómo se evalúa y procesa el tráfico de las aplicaciones.

Después de crear la aplicación y las unidades de aplicación y configurar las directivas, debe verificar la configuración y probarla para asegurarse de que funciona correctamente, tal como lo haría cuando configura una aplicación mediante una plantilla de aplicación AppExpert prediseñada. A continuación, debe supervisar la aplicación para asegurarse de que la aplicación y sus entidades funcionan correctamente.

Creación de una aplicación

Al crear una aplicación AppExpert, el dispositivo crea un contenedor al que puede agregar unidades de aplicación. La unidad de aplicación predeterminada no se crea hasta que se crea la primera unidad de aplicación.

Para crear una aplicación AppExpert mediante la GUI:

1. Vaya a **AppExpert** > **Aplicaciones**.
2. En el panel de detalles, haga clic con el botón secundario en **Aplicaciones**y, **a**continuación,

3. En el cuadro de diálogo **Crear aplicación**, en Nombre, escriba un nombre para la aplicación y, a continuación, haga clic en **Aceptar**.

Creación de unidades de aplicación

Para cada subconjunto de tráfico asociado a la aplicación web, debe crear una unidad de aplicación.

Para crear una unidad de aplicación para la aplicación AppExpert mediante la GUI:

1. Vaya a **AppExpert** > **Aplicaciones**.
2. En el panel de detalles, haga clic con el botón secundario del mouse en la aplicación a la que quiere agregar una unidad de aplicación y, a continuación, haga clic en **Agregar**.
3. Haga clic en **Create**.

Configuración de puntos finales públicos para una aplicación AppExpert

Después de crear todas las unidades de aplicación que necesita, debe configurar uno o más puntos de enlace públicos para permitir que los clientes accedan a la aplicación web a través del dispositivo Citrix ADC.

Para configurar puntos finales públicos para una aplicación AppExpert mediante la GUI:

1. Vaya a **AppExpert** > **Aplicaciones**.
2. En el panel de detalles, haga clic con el botón secundario en la aplicación para la que desea configurar puntos de enlace públicos y, a continuación, haga clic en **Configurar puntos de enlace públicos**.
3. En el cuadro de diálogo Elegir puntos finales públicos de la aplicación, realice una de las siguientes acciones:
   - Si los puntos finales que desea aparecen en el cuadro de diálogo, haga clic en las casillas de verificación correspondientes.
   - Si desea especificar todos los puntos finales públicos, haga clic en **Activar todo**.
   - Si desea disociar los puntos finales de la aplicación AppExpert, desactive las casillas de verificación correspondientes.
   - Si desea crear un nuevo punto final público, haga clic en **Agregar**. A continuación, en el cuadro de diálogo Crear punto final público, configure los parámetros de punto final y haga clic en **Aceptar**.

     En el cuadro de diálogo **Crear punto final público**, solo puede especificar el nombre, la dirección IP, el puerto y el protocolo del punto final. Puede especificar la configuración de punto final adicional después de crear el punto final público. Para especificar parámetros de punto final adicionales, después de crear el punto final, en el cuadro de diálogo Elegir puntos finales públicos, haga clic en el punto final y, a continuación, haga clic en **Abrir**. A continuación, en el cuadro de diálogo **Configurar dispositivo de punto final público**, proporcione opciones adicionales y, a continuación, haga clic en **Aceptar**.

Para obtener más información sobre los parámetros de los cuadros de diálogo **Crear dispositivo de punto final público** y **Configurar dispositivo de punto final público**, consulte Cambio de contenido.

- Si quiere modificar un dispositivo de punto final público, haga clic en el extremo y, a continuación, haga clic en **Abrir**. A continuación, en el cuadro de diálogo **Configurar dispositivo de punto final público**, modifique la configuración del dispositivo de punto final y, a continuación, haga clic en **Aceptar**.
  Para obtener más información sobre los parámetros del cuadro de diálogo Configurar dispositivo de punto final público, consulte Cambio de contenido.

4. Haga clic en **Cerrar**.

Configuración de puntos finales públicos para una unidad de aplicación

Para una unidad de aplicación, especifique extremos públicos de la misma manera que especificaría extremos públicos para una aplicación creada a partir de una plantilla de aplicación AppExpert. Para obtener más información sobre cómo especificar un subconjunto de dispositivos de punto final de una unidad de aplicación, consulte Configuración de dispositivos de punto final para una unidad de aplicación.

Para configurar dispositivos de punto final para una unidad de aplicación mediante la GUI:

1. Vaya a **AppExpert** > **Aplicaciones**.
2. En el panel de detalles, haga clic con el botón derecho en la unidad de aplicación para la que desea especificar puntos finales públicos y, a continuación, haga clic en **Configurar puntos finales públicos**.
3. En el cuadro de diálogo **Elegir puntos finales públicos** de la unidad de aplicación, realice una de las siguientes acciones:
   - Si especifica puntos de enlace para la unidad de aplicación por primera vez, desactive las casillas de verificación correspondientes a los puntos de enlace que no desea que estén enlazados a la unidad de aplicación.
   - Si desea especificar puntos finales que aparecen en el cuadro de diálogo pero que no están enlazados actualmente a la unidad de la aplicación, haga clic en las casillas de verificación correspondientes.
4. Haga clic en **Aceptar**.

Configuración de servicios y grupos de servicios para una aplicación AppExpert

Los servicios y los grupos de servicios están disponibles para las unidades de aplicación solo después de configurar los servicios y los grupos de servicios para la aplicación AppExpert. Por lo tanto, debe configurar los servicios y los grupos de servicios para la aplicación AppExpert antes de configurar los servicios para las unidades de la aplicación. Todos los servicios y grupos de servicios que configure

para una aplicación AppExpert deben usar el mismo protocolo (HTTP o HTTPS). El procedimiento para configurar servicios y grupos de servicios para una aplicación AppExpert que no se crea a partir de una plantilla es el mismo que para una aplicación creada a partir de una plantilla.

Para configurar un servicio o grupo de servicios para la aplicación AppExpert mediante la GUI:

1. Vaya a **AppExpert** > **Aplicaciones**.
2. En el panel de detalles, haga clic con el botón secundario en la aplicación para la que quiere configurar servicios o grupos de servicios y, a continuación, haga clic en **Configurar servicios de backend**.
3. En el cuadro de diálogo Configurar servicios de backend, realiza una de las siguientes acciones:
   - Para configurar los servicios, haga clic en la ficha **Servicios**.
   - Para configurar grupos de servicios, haga clic en la ficha **Grupos de servicios**.
4. En la ficha **Servicio** o **Grupos** de servicios, realice una de las siguientes acciones:
   - Si los servicios o grupos de servicios que desea aparecen en la ficha, haga clic en las casillas de verificación correspondientes.
   - Si desea especificar todos los servicios o grupos de servicios, haga clic en **Activar todos**.
   - Si desea crear un servicio o grupo de servicios nuevo, haga clic en **Agregar**. A continuación, en el cuadro de diálogo **Crear servicio** o en el cuadro de diálogo **Crear grupo de servicios**, configure los parámetros del servicio o grupo de servicios, respectivamente, y, a continuación, haga clic en **Crear**.
   - Si desea modificar un servicio, haga clic en el servicio y, a continuación, en Abrir. A continuación, en el cuadro de diálogo **Configurar servicio** o **Crear grupo de servicios**, configure la configuración del servicio o grupo de servicios respectivamente y, a continuación, haga clic en **Aceptar**.

Para obtener información sobre la configuración de los cuadros de diálogo Crear servicio, Configurar **servicio y Crear grupo** de servicios, consulte Equilibrio de carga.

Configuración de servicios y grupos de servicios para una unidad de aplicación

Después de configurar los servicios y los grupos de servicios, debe configurar los servicios y los grupos de servicios para cada unidad de aplicación. Sin embargo, este paso no es necesario si cada servicio de backend aloja todo el contenido asociado a la aplicación web. Los servicios y grupos de servicios se configuran para una unidad de aplicación si el contenido asociado a la unidad de aplicación está alojado solo en un subconjunto de los servidores backend.

Para configurar servicios o grupos de servicios para una unidad de aplicación mediante la GUI:

1. Vaya a **AppExpert** > **Aplicaciones**.
2. En el panel de detalles, haga clic con el botón secundario en la unidad de aplicación para la que quiere configurar un servicio o grupo de servicios y, a continuación, haga clic en **Configurar servicios de backend**.

3. En el cuadro de diálogo **Configurar servicios de backend**, realiza una de las siguientes acciones:
   - Para configurar los servicios, haga clic en la ficha **Servicios**.
   - Para configurar grupos de servicios, haga clic en la ficha **Grupos de servicios**.
4. En la ficha **Servicios** o **Grupos de servicios**, siga uno de estos procedimientos:
   - Desactive las casillas de verificación correspondientes a los servicios o grupos de servicios que no desea configurar para la unidad de aplicación. Asegúrese de que están activadas las casillas de verificación que corresponden a los servicios o grupos de servicios que desea configurar para la unidad de aplicación. A continuación, en la columna Peso, especifique el peso que desea asignar a cada servicio configurado.
   - Para especificar todos los servicios o grupos de servicios, haga clic en **Activar todos**.
5. En las fichas **Método** y **Persistencia** y **Avanzado**, especifique los parámetros deseados.
6. Haga clic en **Aceptar**.

Configuración de directivas

Los procedimientos para configurar directivas para una aplicación AppExpert que se crea sin utilizar una plantilla son los mismos que para una aplicación AppExpert creada a partir de una plantilla. Para obtener más información, consulte Configuración de directivas para unidades de aplicación.

Aplicaciones gateway de Citrix

June 22, 2022

Cuando configura una aplicación AppExpert para administrar una aplicación web a través del dispositivo Citrix® Citrix ADC®, también crea un conjunto de unidades de aplicación y configura un conjunto de directivas de seguridad y optimización del tráfico para cada unidad. Las directivas que configura para cada unidad de aplicación (directivas para funciones como Compresión, Almacenamiento en caché y Reescritura) evalúan el tráfico destinado únicamente a esa unidad. Además de estas directivas, es posible que desee configurar directivas de Access Gateway para la aplicación en su conjunto a fin de optimizar el tráfico de la aplicación cuando se accede a través de Access Gateway. La función Aplicaciones de Access Gateway le permite configurar las directivas de Access Gateway (autorización, tráfico, acceso sin cliente y compresión TCP) para una aplicación AppExpert. Después de configurar las directivas de Citrix Gateway para las aplicaciones de AppExpert, puede incluir la configuración de directivas en las plantillas de aplicaciones de AppExpert que cree.

También puede configurar directivas de Citrix Gateway para subredes de intranet, recursos compartidos de archivos y otros recursos de red. Por último, puede crear marcadores para las aplicaciones de AppExpert y ciertos recursos si desea que los usuarios puedan acceder a ellos desde la página de inicio de Citrix Gateway.

Puede configurar las entidades en la función Aplicaciones de Citrix Gateway solo mediante la GUI.

Cómo funciona una aplicación Citrix Gateway

Al crear una aplicación AppExpert en el nodo Aplicaciones de la GUI, se crea automáticamente una aplicación Access Gateway correspondiente en el nodo Aplicaciones de Access Gateway. Además, se crea automáticamente una regla que utiliza el punto final público configurado de la aplicación AppExpert para la entrada de la aplicación Access Gateway. Si se configuran varios puntos de enlace para la aplicación AppExpert, la regla incluye todos los puntos de enlace públicos configurados. El dispositivo Citrix ADC usa esta regla para aplicar cualquier directiva de Access Gateway configurada al tráfico recibido en el punto final público de la aplicación AppExpert. El tráfico recibido en el punto final público de la aplicación AppExpert se evalúa primero con las directivas de Citrix Gateway y, a continuación, con las directivas configuradas para las unidades de aplicación de la aplicación AppExpert.

La regla que se crea para las directivas de acceso sin cliente para una aplicación de Access Gateway es una expresión avanzada que también utiliza el punto final público que está configurado para la aplicación AppExpert. Por lo tanto, antes de configurar las directivas de Citrix Gateway para una aplicación AppExpert, debe configurar puntos de enlace públicos para la aplicación AppExpert.

Cuando se incluye la configuración de Citrix Gateway en una plantilla de aplicación, la información específica de la implementación, como la información de la dirección IP y el puerto, y la regla que se crea a partir de esta información no se incluyen en la plantilla.

Cómo funciona una configuración de Citrix ADC para un recurso compartido de archivos

En el dispositivo Citrix ADC, puede configurar directivas de autorización para un recurso compartido de archivos alojado en la red de su organización.

Cuando crea un recurso compartido de archivos, especifica un nombre para el recurso compartido de archivos y la ruta de red al recurso compartido de archivos. En la ruta de red, puede especificar el nombre del servidor o la dirección IP del servidor. Se crea automáticamente una regla que utiliza los componentes de la ruta del recurso compartido de archivos para el recurso compartido de archivos. Esta regla permite que el dispositivo identifique las solicitudes de archivos alojados en el servidor de archivos compartidos. Cualquier directiva de autorización que esté configurada para el recurso compartido de archivos se aplica a las solicitudes entrantes.

La configuración de Citrix ADC para un recurso compartido de archivos no se puede guardar en las plantillas de la aplicación AppExpert.

Cómo funciona una configuración de Citrix ADC para una subred de intranet

Para las subredes de intranet que forman parte de la red, puede configurar directivas de autorización, tráfico y compresión TCP en el dispositivo Citrix ADC. Al agregar una subred de intranet, debe especificar la dirección IP y la máscara de red de la subred de intranet. Se crea automáticamente una regla que utiliza estos dos parámetros para la subred de la intranet. El dispositivo aplica las directivas configuradas a cualquier solicitud que tenga una dirección IP de destino y una máscara de red configuradas en la dirección IP y la máscara de red de la subred, respectivamente.

La configuración de Citrix ADC para una subred de intranet no se puede guardar en las plantillas de la aplicación AppExpert.

Cómo funciona la categoría de otros recursos

La categoría Otros recursos le permite configurar las directivas de Access Gateway para cualquier recurso de red mediante una regla de su elección. Cuando configura el dispositivo Citrix ADC para procesar las solicitudes del recurso de red, configura una expresión clásica para identificar las solicitudes que están asociadas con el recurso de red. Puede configurar directivas de autorización, tráfico, acceso sin cliente y compresión TCP para un recurso de red en Otros recursos. El dispositivo Citrix ADC aplica las directivas de Citrix Gateway configuradas a cualquier solicitud que coincida con la regla configurada.

La configuración de Citrix ADC para un recurso de red en Otros recursos no se puede guardar en las plantillas de la aplicación AppExpert.

Convenciones de denominación de entidades

La función Aplicaciones de Citrix Gateway aplica una convención de nomenclatura para algunas de las entidades que se crean en esta función. Por ejemplo, los nombres de los perfiles que crea para las directivas de tráfico de una subred de intranet siempre comienzan con una cadena que consiste en el nombre de la subred de intranet seguido de un guión bajo (_). El nombre que proporciona para la entidad se anexa a esta cadena. Si el nombre de una subred es “subnet1”, el nombre del perfil comienza por “subnet1_. “ Cuando se requiere una convención de nomenclatura de este tipo (en el cuadro de texto en el que se escribe el nombre de una entidad, por ejemplo), la interfaz de usuario inserta automáticamente la cadena con la que debe comenzar el nombre de la entidad y no le permite modificarlo.

Agregar subredes de intranet

June 22, 2022

Puede especificar las directivas de autorización y tráfico para el tráfico que se dirige a las subredes de intranet que están configuradas en la red. Las reglas para estas directivas se crean automáticamente mediante los parámetros que especifique para la subred.

Para configurar una subred de intranet mediante la GUI:

1. En el panel de navegación de la GUI, expanda **AppExpert**y, a continuación, haga clic en Aplicaciones de Access Gateway.
2. En el panel de detalles, realice una de las acciones siguientes:
   - Para agregar una subred de intranet, haga clic en **Subredes de intranet**y, a continuación, haga clic en **Agregar**.
   - Para modificar una subred de intranet, haga clic en una subred de intranet y, a continuación, en **Abrir**.
3. En el cuadro de diálogo **Crear subred** de **intranet o Configurar subred** de intranet, haga lo siguiente:
   a) En el cuadro Nombre, escriba un nombre para la subred de intranet que va a agregar. Este parámetro no se puede cambiar para una subred de intranet existente.
   b) En el cuadro Dirección IP, escriba la dirección IP de la subred de la intranet.
   c) En el cuadro Máscara de red, escriba la máscara de red que se utilizará para la subred de la intranet.
   d) Haga clic en **Crear** o **Aceptar**y, a continuación, en **Cerrar**.

Agregar otros recursos

June 22, 2022

Para un recurso de red que agregue a Otros recursos, debe configurar la expresión de directiva avanzada que identifique el subconjunto de tráfico asociado al recurso.

Para configurar un recurso en otros recursos mediante la interfaz gráfica de usuario:

1. En el panel de navegación de la GUI, expanda AppExpert y, a continuación, haga clic en **Aplicaciones de Access Gateway**.
2. En el panel de detalles, realice una de las acciones siguientes:
   - Para agregar un recurso, haga clic en **Otros recursos**y, a continuación, haga clic en **Agregar**.
   - Para modificar un recurso, haga clic en un recurso y, a continuación, haga clic en **Abrir**.
3. En el cuadro de diálogo **Crear recursoo Configurar recurso**, haga lo siguiente:
   a) En el cuadro Nombre, escriba el nombre del recurso que va a agregar. Este parámetro no se puede cambiar para un recurso existente.

b) En el cuadro Regla, escriba la regla que identificará el subconjunto de tráfico asociado al recurso que va a agregar.
También puede hacer clic en **Configurar**y, a continuación, crear la regla en el cuadro de diálogo **Crear expresión**.
c) Haga clic en **Crear** o **Aceptar**y, a continuación, en **Cerrar**.

Configuración de directivas de autorización

June 22, 2022

Puede configurar las directivas de autorización de Citrix Gateway para que los usuarios y grupos AAA accedan a un recurso.

Para configurar los permisos para que un usuario o grupo AAA acceda a un recurso mediante la GUI:

1. En el panel de navegación de la GUI, expanda AppExpert y, a continuación, haga clic en **Aplicaciones de Access Gateway**.
2. En el panel de detalles, en la columna Autorización, haga clic en el icono de la aplicación, el recurso compartido de archivos, la subred de la intranet o el recurso para el que desea configurar las directivas de autorización para los usuarios y grupos de AAA.
3. Lleve a cabo una de las siguientes acciones:
   - Si el usuario o grupo AAA para el que desea configurar permisos ya está en el árbol Grupos/Usuarios, arrastre el usuario o el grupo desde el árbol Grupos/Usuarios al nodo Usuarios o Grupos del árbol <application name>. A continuación, haga clic con el botón secundario en el usuario o grupo y haga clic en **Permitir**.
   - Si el usuario o grupo AAA para el que desea configurar permisos no está configurado en el dispositivo, en el árbol <application name>, haga clic con el botón secundario en Usuarios o grupos y, a continuación, haga clic en **Agregar**. En el cuadro de diálogo Crear **grupo AAA** o **Crear usuario AAA**, rellene los valores, haga clic en **Crear**y, a continuación, haga clic en **Cerrar**.
     El usuario o el grupo se crean con el permiso establecido en Permitir. Para cambiar la configuración de permisos, haga clic con el botón secundario en el grupo o usuario y, a continuación, haga clic en la configuración
4. Haga clic en **Cerrar**.

Configuración de directivas de tráfico

June 22, 2022

Las directivas de tráfico que configura para los recursos del nodo Aplicaciones de Citrix Gateway controlan las conexiones de los clientes a la aplicación. No es necesario configurar una regla para el recurso. Regla que se crea automáticamente al crear el recurso. Solo necesitas asociar un perfil de solicitud a la directiva de tráfico. En el perfil de tráfico, se especifican parámetros como el protocolo, el tiempo de espera de la aplicación y la asociación de tipos de archivo.

Para configurar las directivas de tráfico de un recurso

1. En el panel de navegación de la GUI, expanda AppExperty, a continuación, haga clic en Aplicaciones de Access Gateway.
2. En el panel de detalles, en la columna Tráfico, haga clic en el icono proporcionado para la aplicación, el recurso compartido de archivos, la subred de la intranet o el recurso para el que quiere configurar las directivas de tráfico.
3. En el cuadro de diálogo **Configurar directivas de tráfico**, haga lo siguiente:
   - Para especificar una directiva de tráfico existente, haga clic en **Insertar directiva**y, a continuación, en la columna Nombre de la directiva, haga clic en el nombre de la directiva.
   - Para configurar una nueva directiva, haga clic en Insertar directiva y, a continuación, en la columna Nombre de la directiva, haga clic en Nueva directiva. En el cuadro de diálogo Crear directiva de tráfico, en el cuadro Nombre, después del guión bajo (_), escriba un nombre para la directiva. A continuación, en Perfil de solicitud, seleccione un perfil de solicitud existente o haga clic en Nuevo para configurar un nuevo perfil de solicitud. También puede seleccionar un perfil existente y, a continuación, hacer clic en Modificar para modificar el perfil.
     Para obtener más información sobre la configuración de una directiva o un perfil de tráfico, consulte Citrix Gateway.
   - Para modificar una directiva que ha insertado, en la columna Nombre de la directiva, haga clic en el nombre de la directiva y, a continuación, haga clic en Modificar directiva. Para modificar solo el perfil asociado, en la columna Perfil, haga clic en el nombre del perfil y, a continuación, haga clic en **Modificar perfil**.
   - Para regenerar las prioridades asignadas a las directivas, haga clic en **Regenerar prioridades**.
   - Para especificar un nuevo valor de prioridad para una directiva, en la columna Prioridad, haga doble clic en la prioridad asignada y, a continuación, introduzca el valor que quiera.
   - Para desvincular una directiva, haga clic en la directiva y, a continuación, haga clic en **Desvincular directiva**.
4. Haga clic en **Aplicar cambios**y, a continuación, en **Cerrar**.

Configuración de directivas de acceso sin cliente

June 22, 2022

El acceso sin cliente, cuando se configura para un recurso en el dispositivo Citrix ADC, permite a los usuarios finales acceder al recurso sin utilizar el software cliente de Citrix Gateway. Los usuarios pueden utilizar exploradores web para acceder a recursos como Outlook Web Access. Para configurar el acceso sin cliente para un recurso, configure una directiva de acceso sin cliente asociada a un perfil de acceso sin cliente.

Para configurar una directiva de acceso sin cliente para un recurso del nodo Aplicaciones de Citrix Gateway:

1. En el panel de navegación de la GUI, expanda **AppExpert**y, a continuación, haga clic en **Aplicaciones de Access Gateway**.
2. En el panel de detalles, en la columna **Acceso sin cliente**, haga clic en el icono de la aplicación, recurso compartido de archivos, subred de intranet o recurso para el que quiere configurar una directiva de acceso sin cliente.
3. En el cuadro de diálogo **Configurar directivas de acceso sin cliente**, haga lo siguiente:
   - Para especificar una directiva de acceso sin cliente existente, haga clic en **Insertar directiva**y, a continuación, en la columna **Nombre de la directiva**, haga clic en el nombre de la directiva.
   - Para configurar una nueva directiva de acceso sin cliente, haga clic en **Insertar directiva**y, a continuación, en la columna **Nombre de la directiva**, haga clic en **Nueva directiva**. En el cuadro de diálogo **Crear directiva de acceso sin cliente**, en el cuadro Nombre, después del guión bajo (_), escriba un nombre para la directiva. A continuación, en Perfil, seleccione un perfil existente o haga clic en Nuevo para configurar un nuevo perfil. También puede seleccionar un perfil existente y, a continuación, hacer clic en **Modificar** para modificar el perfil.
     Para obtener más información sobre cómo configurar un perfil o directiva de acceso sin cliente, consulte Citrix Gateway.
   - Para modificar una directiva que ha insertado, en la columna Nombre de la directiva, haga clic en el nombre de la directiva y, a continuación, haga clic en **Modificar directiva**. Para modificar solo el perfil asociado, en la columna Perfil, haga clic en el nombre del perfil y, a continuación, haga clic en Modificar perfil.
   - Para especificar un nuevo valor de prioridad para una directiva, en la columna Prioridad, haga doble clic en la prioridad asignada y, a continuación, introduzca el valor que quiera.
   - Para desvincular una directiva, haga clic en la directiva y, a continuación, haga clic en **Desvincular directiva**.
4. Haga clic en **Aplicar cambios**y, a continuación, en **Cerrar**.

Configuración de directivas de compresión TCP

June 22, 2022

Puede configurar directivas de compresión TCP para una aplicación a fin de aumentar el rendimiento de la aplicación. La compresión TCP reduce la latencia de la red, reduce los requisitos de ancho de banda y aumenta la velocidad de transmisión. Al configurar una directiva de compresión TCP, asocia una acción de compresión a la directiva. La acción de compresión especifica Compress, GZIP, Deflate o NoCompress como el tipo de compresión. Para obtener más información sobre las directivas de compresión y las acciones de compresión, consulte Citrix Gateway.

Para configurar una directiva de compresión TCP para un recurso en el nodo Aplicaciones de Citrix Gateway

1. En el panel de navegación de la GUI, expanda **AppExpert**y, a continuación, haga clic en **Aplicaciones de Access Gateway**.
2. En el panel de detalles, en la columna Compresión TCP, haga clic en el icono de la aplicación, recurso compartido de archivos, subred de intranet o recurso para el que quiere configurar una directiva de compresión TCP.
3. En el cuadro de diálogo **Configurar directivas de compresión TCP**, haga lo siguiente:
   - Para especificar una directiva de compresión TCP existente, haga clic en **Insertar directiva**y, a continuación, en la columna **Nombre de la directiva**, haga clic en el nombre de la directiva.
   - Para crear una nueva directiva de compresión TCP, haga clic en Insertar directiva y, a continuación, en la columna Nombre de la directiva, haga clic en Nueva directiva. En el cuadro de diálogo Crear directiva de compresión TCP, en el cuadro Nombre de la directiva, después del guión bajo ("_"), escriba un nombre para la directiva. A continuación, en Acción, seleccione una acción existente o haga clic en Nueva y configure una nueva acción. También puede hacer clic en Ver para ver el tipo de compresión configurado.
     Para obtener más información sobre cómo configurar una directiva o acción de compresión TCP, consulte Citrix Gateway, Advanced Edition en Citrix Gateway.
   - Para modificar una directiva que ha insertado, en la columna Nombre de la directiva, haga clic en el nombre de la directiva y, a continuación, haga clic en **Modificar directiva**.
   - Para regenerar las prioridades asignadas a las directivas, haga clic en **Regenerar prioridades**.
   - Para especificar un nuevo valor de prioridad para una directiva, en la columna Prioridad, haga doble clic en la prioridad asignada y, a continuación, introduzca el valor que quiera.
   - Para desvincular una directiva, haga clic en la directiva y, a continuación, haga clic en **Desvincular directiva**.
4. Haga clic en **Aplicar cambios y,** a continuación, en **Cerrar**.

Configurar marcadores

June 22, 2022

Puede configurar marcadores para aplicaciones o recursos internos que estén disponibles para un usuario autorizado. A continuación, puede vincular el marcador a un usuario, grupo de usuarios o servidor virtual de forma global y habilitarlo para el usuario en la interfaz de acceso. Los vínculos de marcadores que cree aparecen en los paneles de sitios web bajo sitios web de empresa.

Para obtener más información, consulte el tema Creación y aplicación de vínculos web.

AppQoE

October 5, 2021

Calidad de experiencia a nivel de aplicación (AppQoE) integra varias funciones de seguridad basadas en directivas existentes del dispositivo Citrix ADC en una única función integrada que aprovecha un nuevo mecanismo de cola, la cola justa. La cola justa administra las solicitudes a servidores web y aplicaciones con equilibrio de carga a nivel de servidor virtual en lugar de en el nivel de servicio, lo que le permite gestionar la cola de todas las solicitudes a un sitio web o aplicación como un grupo antes del equilibrio de carga, en lugar de como secuencias separadas después del equilibrio de carga.

- **Sobrecarga simple.** Cualquier servidor, por robusto que sea, puede aceptar solo un número limitado de conexiones a la vez. Cuando un sitio web o aplicación protegidos recibe demasiadas solicitudes a la vez, la función Protección contra sobretensiones detecta la sobrecarga y pone en cola el exceso de conexiones hasta que el servidor pueda aceptarlas. La función AppQoe muestra una página web alternativa que notifica a los usuarios de que el recurso que solicitaron no está disponible.
- **Ataques de denegación de servicio (DOS).** Cualquier recurso público es vulnerable a ataques cuyo propósito es derribar ese servicio y denegar a los usuarios legítimos el acceso a él. La función de protección contra sobretensiones ayuda a gestionar los ataques DOS además de otros tipos de cargas elevadas. Además, la función de protección contra denegación de servicio HTTP se dirige a los ataques DOS contra sus sitios web, envía desafíos a los sospechosos de atacantes y descarta las conexiones si los clientes no envían una respuesta adecuada.

Hasta la versión actual del sistema operativo Citrix ADC, estas funciones se implementaban en el nivel de servicio, lo que significa que cada servicio tenía asignadas sus propias colas. Aunque las colas de nivel de servicio funcionan, también tienen algunas desventajas, la mayoría de las cuales se deben a que el dispositivo Citrix ADC tiene que equilibrar la carga de las solicitudes antes de implementar cualquiera de las funciones de protección que dependen de la puesta en cola. La implementación de

funciones de protección antes de hacer cola tiene varias ventajas, algunas de las cuales se enumeran a continuación:

- Las conexiones no se vacían si un servicio cambia de estado, ya que están en una cola de nivel de servicio.
- Durante períodos de alta carga, como un ataque de denegación de servicio, y los DoS HTTP entran en juego antes del equilibrio de carga, lo que permite que estas funciones detecten y desvíen el tráfico no deseado o de menor prioridad del equilibrador de carga antes de que el equilibrador de carga tenga que soportarlo.

Además de implementar la cola justa, AppQoE integra un conjunto de funciones que proporcionan un conjunto diferente de herramientas para lograr un objetivo común: Proteger sus recursos en red de demandas excesivas o inapropiadas. La colocación de estas funciones en un marco común le permite configurarlas e implementarlas con mayor facilidad.

Activación de AppQoE

January 12, 2021

Para configurar AppQoE, primero debe habilitar la función.

Para habilitar AppQoE mediante la línea de comandos

En el símbolo del sistema, escriba los siguientes comandos:

- habilitar la función ns appqoe
- show ns feature

Ejemplo:

```
> enable ns feature appqoe
 Done
> show ns feature

        Feature                         Acronym             Status
        -------                         -------             ------
 1)     Web Logging                     WL                  ON
 2)     Surge Protection                SP                  ON
 3)     Load Balancing                  LB                  ON
 ...
 1)     AppQoE                          AppQoE              ON
 Done
```



```
<!--NeedCopy-->
```

Para habilitar AppQoE mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **Configuración**.
2. En el panel de detalles, haga clic en **Configurar funciones avanzadas**.
3. En el cuadro de diálogo **Configurar funciones avanzadas**, active la casilla de verificación **AppQoE**.
4. Haga clic en **Aceptar**.

Acciones de AppQoE

January 12, 2021

Después de habilitar la función AppQoE, debe configurar una o más acciones para gestionar solicitudes.

> **Importante:**
>
> No se requieren parámetros individuales específicos para crear una acción, pero debe incluir al menos un parámetro o no puede crear la acción.

Para configurar una acción AppQoE mediante la línea de comandos

En el símbolo del sistema, escriba los siguientes comandos:

- `add appqoe action <name> [-priority <priority>] [-respondWith (ACS|NS)[<customfile>] [-altContentSvcName <string>] [-altContentPath <string>] [-maxConn <positive_integer>] [-delay <usecs>] [-polqDepth <positive_integer>] [-priqDepth <positive_integer>] [-dosTrigExpression <expression>] [-dosAction (**SimpleResponse** | **HICResponse**)]`
- `show appqoe action`

Ejemplo

Para configurar la cola de prioridad con profundidades de cola de directivas de 10 y 1000 para colas de prioridad media y baja, respectivamente:

```
> add appqoe action appqoe-act-basic-prhigh -priority HIGH
 Done

```



```
> add appqoe action appqoe-act-basic-prmedium -priority MEDIUM -
   polqDepth 10
 Done

> add appqoe action appqoe-act-basic-prlow -priority LOW -polqDepth
   1000
 Done

> show appqoe action

1.       Name: appqoe-act-basic-prhigh
        ActionType: PRIORITY_QUEUING
        Priority: HIGH
        PolicyQdepth: 0
        Qdepth: 0

1.      Name: appqoe-act-basic-prmedium
        ActionType: PRIORITY_QUEUING
        Priority: MEDIUM
        PolicyQdepth: 10
        Qdepth: 0

1.      Name: appqoe-act-basic-prlow
        ActionType: PRIORITY_QUEUING
        Priority: LOW
        PolicyQdepth: 1000
        Qdepth: 0
Done
<!--NeedCopy-->
```

Para modificar una acción AppQoE existente mediante la línea de comandos

En el símbolo del sistema, escriba los siguientes comandos:

- `set appqoe action <name> [-priority <priority>] [-altContentSvcName <string>] [-altContentPath <string>] [-polqDepth <positive_integer>] [-priqDepth <positive_integer>] [-maxConn <positive_integer>] [-delay <usecs>] [-dosTrigExpression <expression>] [-dosAction ( SimpleResponse | HICResponse )]`
- `show appqoe action`

Para eliminar una acción AppQoE mediante la línea de comandos

En el símbolo del sistema, escriba los siguientes comandos:

- `rm appqoe action <name>`
- `show appqoe action`

Parámetros para configurar una acción AppQoE

- name. Un nombre para la nueva acción o el nombre de la acción existente que quiere modificar. El nombre puede comenzar con una letra, un número o un símbolo de subrayado, y puede consistir de uno a letras, números y los símbolos de guión (-), punto (.) libra (#), espacio (), signo (@), igual (=), dos puntos (:) y guión bajo (_).
- prioridad. Cola de prioridad a la que se asigna la solicitud. Cuando un servidor web protegido o una aplicación está muy cargado y no puede aceptar solicitudes adicionales, especifica el orden en el que se deben cumplir las solicitudes en espera cuando los recursos están disponibles. Las opciones son:

1. **HIGH.** Cumple la solicitud tan pronto como los recursos estén disponibles.
2. **MEDIUM.** Cumple la solicitud después de haber cumplido todas las solicitudes en la cola de prioridad ALTA.
3. **LOW.** Cumple la solicitud después de haber cumplido todas las solicitudes en las colas de prioridad HIGH y MEDIUM.
4. **LOWEST.** Cumple la solicitud solo después de que haya completado todas las solicitudes en colas de mayor prioridad.

Si la prioridad no está configurada, el dispositivo Citrix ADC asigna la solicitud a la cola de prioridad más baja de forma predeterminada.

- respondWith. Configura el dispositivo Citrix ADC para que realice la acción Respondedor especificada cuando se alcance el umbral especificado. Debe utilizarse con una de las siguientes configuraciones:
  - **ACS:** sirve contenido de un servicio de contenido alternativo. Umbral: MaxConn (conexiones máximas) o retraso.
  - **NS:** sirve una respuesta integrada del dispositivo Citrix ADC. Umbral: MaxConn (conexiones máximas) o retraso.
  - **NO ACTION:** No sirve contenido alternativo. Asigna conexiones a la cola de prioridad más baja si se alcanza el umbral MaxConn (conexiones máximas) o de retraso.
- AltContentSvcName. Si se especifica -ResponseWith ACS, el nombre del servicio de contenido alternativo, normalmente una dirección URL absoluta del servidor web que aloja el contenido alternativo.

- AltContentPath. Si se especifica -responseWith (ACS | NS), la ruta de acceso al contenido alternativo.
- OlqDepth. Valor de umbral de profundidad de cola de directivas para la cola de directivas asociada a esta acción. Cuando el número de conexiones en la cola de directivas asociada a esta acción aumenta al número especificado, las solicitudes posteriores se asignan a la cola de directivas más baja. Valor mínimo: 1 Valor máximo: 4,294,967,294
- PriqDepth. Valor de umbral de profundidad de cola de directivas para la cola de prioridad especificada. Si el número de solicitudes en la cola especificada en el servidor virtual al que está enlazada la directiva asociada a la acción actual aumenta al número especificado, las solicitudes posteriores se asignan a la cola de prioridad MÁS BAJO. Valor mínimo: 1 Valor máximo: 4,294,967,294
- MaxConn. Número máximo de conexiones que se pueden abrir para las solicitudes que coinciden con la regla de directiva. Valor mínimo: 1 Valor máximo: 4,294,967,294
- retraso. Umbral de retraso, en microsegundos, para las solicitudes que coinciden con la regla de directiva. Si una solicitud coincidente se ha retrasado durante más tiempo que el umbral, el dispositivo
  Citrix ADC realiza la acción especificada. Si se especifica NO ACCIÓN, el dispositivo asigna solicitudes a la cola de prioridad MÁS BAJO. Valor mínimo: 1 Valor máximo: 599999,999
- dosTrigExpression. Agrega una comprobación opcional de segundo nivel para activar acciones DoS.
- dosAction. Acción que se debe realizar cuando el dispositivo determine que él o un servidor protegido están bajo ataque DoS. Valores posibles: SimpleResponse, HiCResponse.

Estos valores especifican métodos de respuesta desafío HTTP para validar la autenticidad de las solicitudes entrantes para mitigar un ataque HTTP-DDoS.

En el proceso de generación y validación de respuesta desafío HTTP, AppQoE utiliza cookies para validar la respuesta del cliente y verificar que el cliente parece ser genuino. Al enviar un desafío, un dispositivo Citrix ADC genera dos cookies:

Cookie de encabezado (_DOSQ). Contiene información específica del cliente para que el dispositivo Citrix ADC pueda verificar la respuesta.

Cookie de cuerpo (_DOSH). Información utilizada para validar el equipo cliente. El explorador del cliente (o el usuario, en el caso de HIC) calcula un valor para esta cookie. El dispositivo Citrix ADC compara ese valor con el valor esperado para verificar el cliente.

La información que el dispositivo envía al cliente para calcular el valor _DOSH se basa en la configuración de Acción de DoS.

1. SimpleResponse: En este caso, un dispositivo Citrix ADC divide el valor y genera un código

JavaScript para combinar el valor final. Una máquina cliente capaz de calcular el valor original se considera genuina.

2. HiCResponse: En este caso, un dispositivo Citrix ADC genera dos números de un solo dígito y genera imágenes para esos números. A continuación, mediante un marco de revisión posterior, el dispositivo inserta esas imágenes como cadenas base64.

Limitaciones

1. Esta no es una implementación trivial CAPTCHA, por lo que no se utiliza ese término.
2. El número de validación se basa en un número generado por Citrix ADC que no cambia en 120 segundos. Este número debe ser dinámico o específico del cliente.

Para configurar una acción AppQoE mediante la utilidad de configuración

1. Vaya a **App-Expert** > **AppQoE** > **Acciones**.
2. En el panel de detalles, realice una de las acciones siguientes:
   - Para crear una nueva acción, haga clic en **Agregar**.
   - Para modificar una acción existente, selecciónela y, a continuación, haga clic en **Modificar**.
3. En la pantalla **Crear acción AppQoE** o **Configurar acción AppQoE**, escriba o seleccione valores para los parámetros. El contenido del cuadro de diálogo corresponde a los parámetros descritos en “Parámetros para configurar la acción AppQoE” de la siguiente manera (asterisco indica un parámetro obligatorio):
   - Nombre: Name
   - Tipo de acción: RespondWith
   - Prioridad: Priority
   - Profundidad de cola de directivas: PolqDepth
   - Profundidad de la cola: PriqDepth
   - Acción de DOS: DosAction
4. Haga clic en **Crear** o **Aceptar**.

Parámetros de AppQoE

January 12, 2021

En los parámetros de AppQoE, se configura la duración de la sesión de una sesión de AppQoE, el nombre de archivo del archivo que contiene la respuesta personalizada y el número de conexiones de cliente que se pueden colocar en una cola.

Para configurar los parámetros de AppQoE mediante la línea de comandos

En el símbolo del sistema, escriba los siguientes comandos:

- `set appqoe parameter [-sessionLife <secs>] [-avgwaitingclient <positive_integer>] [-MaxAltRespBandWidth <positive_integer>] [-dosAttackThresh <positive_integer>]`
- `show appqoe parameter`

Parámetros para configurar los parámetros de AppQoE

- sessionLife

  Número de segundos que deben esperar después de mostrar contenido alternativo antes de que el dispositivo vuelva a mostrar el mismo contenido. Valor predeterminado: 300 Máximo Valor mínimo: 1 Valor máximo: 4.294.967.294

- avgwaitingclient

  El número medio de solicitudes de cliente que pueden estar en la cola de espera de servicio. Valor predeterminado: 1000000 Valor máximo: 4.294.967.294

- MaxAltrespbandwidth

  El ancho de banda máximo que se consume al enviar respuestas alternativas. Si se alcanza el máximo, el dispositivo deja de enviar el contenido alternativo hasta que disminuya el consumo de ancho de banda. Valor predeterminado: 100 Valor mínimo: 1 Valor máximo: 4.294.967.294

- Dosatckthrsh

  Umbral de ataque de denegación de servicio. Número de conexiones que deben estar esperando en colas antes de que el dispositivo responda con medidas de protección DoS. Valor predeterminado: 2000 Valor mínimo: 0 Valor máximo: 4.294.967.294

Para configurar la configuración del parámetro AppQoE mediante la interfaz gráfica de usuario

1. Vaya a **AppExpert** > **AppQoE**.
2. En el panel de detalles, haga clic en **Configurar parámetros de AppQoE**.
3. En la pantalla **Configurar parámetros AppQoE**, escriba o seleccione valores para los parámetros. El contenido del cuadro de diálogo corresponde a los parámetros descritos en “Parámetros para configurar los parámetros de AppQoE” de la siguiente manera (asterisco indica un parámetro obligatorio):
   - Duración de la sesión (secs)
   - sessionLife

- Cliente promedio de espera: Avgwaitingclient
- Límite de ancho de banda de respuesta alternativa (Mbps): MaxAltrespbandwidth
- Umbral de ataque DOS —DOSATTackThresh

4. Haga clic en **Aceptar**.

Directivas de AppQoE

January 12, 2021

Para implementar AppQoE, debe configurar al menos una directiva para indicar a su Citrix ADC cómo distinguir las conexiones que se van a poner en cola en una cola específica.

Para configurar una directiva AppQoE mediante la línea de comandos

En el símbolo del sistema, escriba el siguiente comando:

```
add appqoe policy <name> -rule <expression> -action <string>
```

Ejemplo:

En el ejemplo siguiente se seleccionan las solicitudes con un encabezado User-Agent que contiene “Android” y las asigna a la cola de prioridad media. Estas solicitudes provienen de smartphones y tabletas que ejecutan el sistema operativo Google Android.

```
1  > add appqoe action appqoe-act-primd -priority MEDIUM
2  Done
3  > add appqoe policy appqoe-pol-primd -rule ”HTTP.REQ.HEADER(”User-Agent
       ”).CONTAINS(”Android”)” -action appqoe-act-primd
4  Done
5  > sh appqoe policy appqoe-pol-primd
6          Name: appqoe-pol-primd
7          Rule: HTTP.REQ.HEADER(”User-Agent”).CONTAINS(”Android”)
8          Action: appqoe-act-primd
9          Hits: 0
10
11 Done
12 <!--NeedCopy-->
```


Parámetros para configurar una directiva de AppQoE

- name. Un nombre para la directiva AppQoE. El nombre puede comenzar con una letra, un número o un símbolo de subrayado, y puede constar de una a 127 letras, números y los símbolos de guión (-), punto (.) libra (#), espacio (), signo (@), igual (=), dos puntos (:) y guión bajo (_). Debe elegir un nombre que ayude a identificar el tipo de acción.
- regla. Expresión Citrix ADC que indica al dispositivo qué conexiones debe manejar.
- acción. La acción AppQoE que se debe realizar cuando una conexión coincide con la directiva.

Para configurar una directiva de AppQoE mediante la utilidad de configuración

1. Vaya a **App-Expert** > **AppQoE** > **Directivas**.
2. En el panel de detalles, realice una de las acciones siguientes:
   - Para crear una directiva, haga clic en **Agregar**.
   - Para modificar una directiva existente, selecciónela y, a continuación, haga clic en **Modificar**.
3. Si va a crear una directiva, en el cuadro de diálogo **Crear directiva de AppQoE**, en el cuadro de texto Nombre, escriba un nombre para la nueva directiva.

   El nombre puede comenzar con una letra, un número o un símbolo de subrayado, y puede constar de una a 127 letras, números y los símbolos de guión (-), punto (.) libra (#), espacio (), signo (@), igual (=), dos puntos (:) y guión bajo (_). Debe elegir un nombre que ayude a identificar el propósito y el efecto de esta directiva.

   Si está modificando una directiva existente, omita este paso. No se puede cambiar el nombre de una directiva existente.
4. En la lista desplegable **Acción**, elija la acción AppQoE que quiere realizar cuando la directiva coincida con una conexión. Haga clic en el signo más (+) para abrir el cuadro de diálogo **Agregar acción AppQoE** y agregar una nueva acción.
5. En el cuadro de texto **Regla**, escriba la expresión de directiva directamente o haga clic en Nuevo para crear una expresión de directiva. Si hace clic en Nuevo, lleve a cabo los siguientes pasos:
   a) En el cuadro de diálogo **Crear expresión**, haga clic en **Agregar**.
   1 En el cuadro de diálogo **Agregar expresión**, seleccione una expresión común de la lista desplegable **Expresiones de uso frecuente** o utilice las listas desplegables **Construct Expression** para crear la expresión que define el tráfico que se va a filtrar.
   Si elige crear su propia expresión, comience seleccionando el primer término de la primera lista desplegable del lado izquierdo del área Expresión de construcción. Las opciones de esa lista son:
   - HTTP

- SYS
- CLIENTE
- SERVER
- ANALÍTICA
- TEXTO

La opción predeterminada es HTTP. Después de realizar una elección en la primera lista desplegable (o aceptar el valor predeterminado), puede elegir el siguiente término de la expresión en la lista desplegable situada a la derecha de la misma. Los términos de esa lista y otras listas que siguen cambian según sus opciones anteriores. Las listas solo ofrecen términos que son opciones válidas. Continúe seleccionando términos hasta que haya terminado la expresión.

a) Cuando haya creado la expresión que quiere, haga clic en **Aceptar**. La expresión se agrega en el cuadro de texto **Expresión**.

6. Haga clic en **Crear**. La expresión aparece en el cuadro de texto **Regla**.

Plantilla de entidad para el servidor virtual de equilibrio de carga

August 20, 2021

> **Advertencia**
>
> La funcionalidad de la plantilla de entidad queda obsoleta desde Citrix ADC 13.0 compilación 82.x en adelante y Citrix recomienda utilizar los libros de estilo como alternativa. Para obtener más información, consulte el tema Libros de estilo .

Una plantilla de entidad es una recopilación de información para crear una plantilla de servidor virtual de equilibrio de carga en un dispositivo Citrix ADC. Proporciona una especificación y un conjunto de valores predeterminados que se configurarán para un servidor virtual de equilibrio de carga. Mediante una plantilla que define un conjunto de valores predeterminados, puede configurar rápidamente varios servidores virtuales que requieren una configuración similar y eliminar varios pasos de configuración.

Puede crear una plantilla de entidad exportando los detalles del servidor virtual de equilibrio de carga a un archivo de plantilla. Esto solo se puede hacer a través de la GUI de Citrix ADC. La GUI de Citrix ADC se utiliza para exportar, importar y administrar plantillas de entidad. Puede compartir plantillas de entidad con otros administradores y administrar plantillas guardadas localmente en su dispositivo o equipo. También puede importar plantillas de entidad desde el dispositivo o el equipo local.

Antes de crear una plantilla, debe estar familiarizado con la configuración del servidor virtual de equilibrio de carga.

Plantilla de servidor virtual de equilibrio de carga

Las plantillas de entidad de equilibrio de carga se crean de la misma manera que se crean las plantillas de aplicación Citrix ADC. Al exportar un servidor virtual de equilibrio de carga a un archivo de plantilla, se crean automáticamente los dos archivos siguientes:

- Archivo de plantilla de servidor virtual de equilibrio de carga. Contiene elementos XML que almacenan los valores de los parámetros configurados para el servidor virtual de equilibrio de carga. El archivo también contiene elementos XML para almacenar información sobre directivas enlazadas.
- Archivo de implementación. Contiene elementos XML que almacenan información específica de la implementación, como servicios, grupos de servicios y variables configuradas.
  En los archivos de plantilla y de implementación, cada unidad de información de configuración se encapsula en un elemento XML específico destinado a ese tipo de unidad. Por ejemplo, el parámetro del método de equilibrio de carga, lbMethod, se encapsula dentro de las<lbmethod> etiquetas</lbmethod> y.

> **Nota:**
>
> Después de exportar un servidor virtual de equilibrio de carga, puede agregar elementos, quitar elementos y modificar elementos existentes antes de importar la información de configuración a un dispositivo Citrix ADC.

Cómo funciona una plantilla de servidor virtual de equilibrio de carga

Cuando se crea una plantilla para un servidor virtual de equilibrio de carga, se especifican los valores predeterminados para el servidor. Especifique qué valores deben ser de solo lectura, qué valores no deben mostrarse y qué valores pueden configurar los usuarios. También puede configurar las páginas que componen el asistente de importación de plantillas. Toda la información y la configuración que proporcione se almacenan en el archivo de plantilla.
Cuando un usuario importa la plantilla a un dispositivo Citrix ADC, la GUI lo guía a través de las distintas páginas que configuró para la plantilla. La GUI muestra los valores de los parámetros de solo lectura y solicita al usuario que especifique los valores para los parámetros configurables. Después de que el usuario siga las instrucciones, el dispositivo crea la entidad con los valores configurados.
Puede crear o modificar una plantilla de entidad para un servidor virtual de equilibrio de carga desde el nodo Administración del tráfico.
Para exportar los detalles del servidor virtual a una plantilla, debe especificar las siguientes opciones y configuraciones para la plantilla:

- El valor predeterminado de un parámetro.
- Si los valores predeterminados son visibles para los usuarios.
- Si los usuarios pueden cambiar los valores predeterminados.

- El número de páginas del asistente de importación de entidades, incluidos los nombres de página, el texto y los parámetros disponibles.
- Entidades que deben estar enlazadas a la entidad para la que se crea la plantilla.

Por ejemplo, al crear una plantilla de servidor virtual de equilibrio de carga, puede especificar las directivas que quiere vincular al servidor virtual que cree a partir de la plantilla. Sin embargo, solo se incluye información de enlace en la plantilla. Las entidades enlazadas no están incluidas. Si la plantilla de entidad se importa a otro dispositivo Citrix ADC, las entidades enlazadas deben existir en el dispositivo en el momento de la importación para que el enlace se realice correctamente. Si no existe ninguna de las entidades enlazadas en el dispositivo de destino, la entidad (para la que se configuró la plantilla) se crea sin ningún enlace. Si solo existe un subconjunto de las entidades enlazadas en el dispositivo de destino, están enlazadas a la entidad que se crea a partir de la plantilla.
Al exportar una plantilla para el servidor virtual de equilibrio de carga, los parámetros de configuración de la entidad aparecen en la plantilla. Todas las entidades enlazadas se seleccionan de forma predeterminada, pero se pueden modificar los enlaces según sea necesario. Al igual que en el caso de una plantilla que no se basa en una entidad existente, solo se incluye información vinculante y no las entidades. Puede guardar la plantilla con los valores de configuración existentes o utilizar los parámetros como base para crear una nueva configuración para una plantilla.

Configurar variables en la plantilla de servidor virtual de equilibrio de carga

Las plantillas de servidor virtual de equilibrio de carga admiten la declaración de variables en los parámetros de equilibrio de carga configurados y en las directivas y acciones vinculadas. La capacidad de declarar variables le permite reemplazar valores preconfigurados por valores que se adapten al entorno en el que va a importar la plantilla.

Como ejemplo, considere la siguiente expresión configurada para una directiva enlazada a un servidor virtual de equilibrio de carga para el que está creando una plantilla. La expresión evalúa el valor del encabezado accept-language en una solicitud HTTP.

```
HTTP.REQ.HEADER("Accept-Language").CONTAINS("en-us")
```

Si quiere que el valor del encabezado sea configurable en el momento de la importación, puede especificar la cadena en-us como variable.

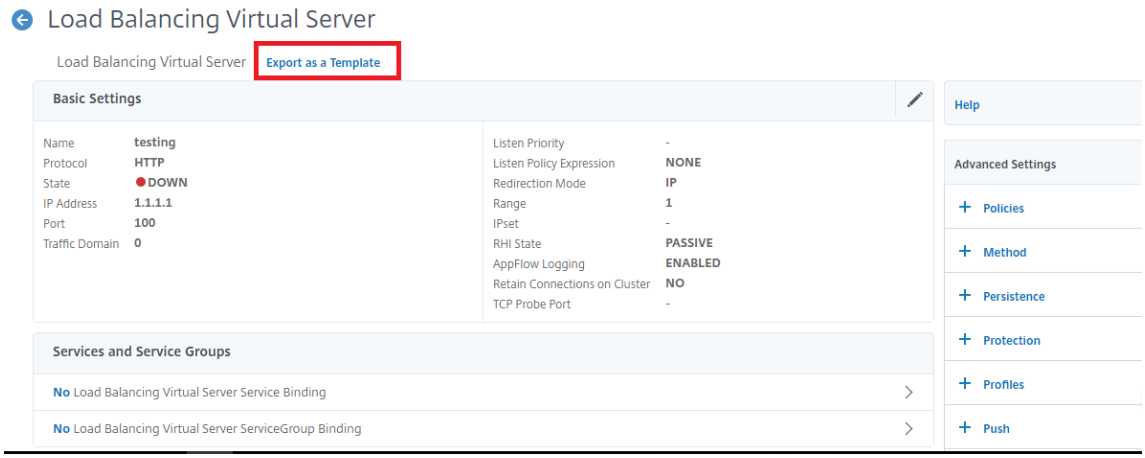
Después de crear una variable, puede hacer lo siguiente:

- Asigne más cadenas a una variable existente. Después de crear una variable para una cadena, puede seleccionar y asignar otras partes de la misma o diferente expresión a la variable. Las cadenas que asigna a una variable no necesitan ser las mismas. En el momento de la importación, todas las cadenas asignadas a la variable se reemplazan con el valor que proporcione.
- Ver la cadena o cadenas asignadas a la variable.
- Ver una lista de todas las entidades y parámetros que utilizan la variable

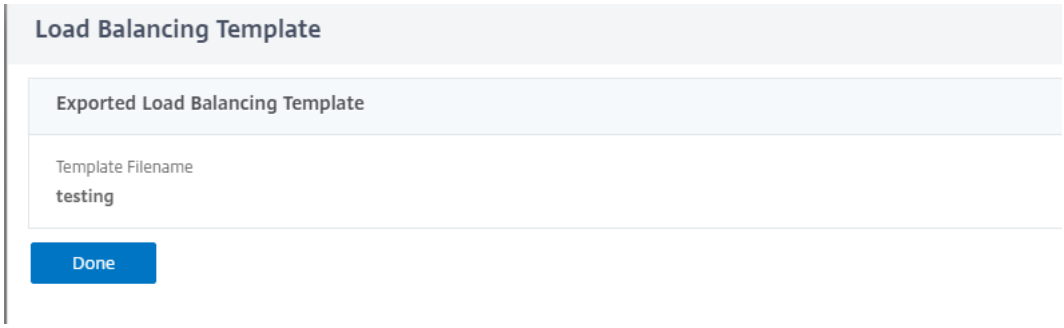
Para configurar variables en una plantilla de servidor virtual de equilibrio de carga

Complete el siguiente procedimiento para configurar variables para una plantilla de servidor virtual de equilibrio de carga mediante la GUI de Citrix ADC

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**
2. En el panel de detalles, haga clic con el botón secundario en el servidor virtual que quiere exportar a un archivo de plantilla y, a continuación, haga clic en **Agregar**.
3. En la página **Crear servidor virtual de equilibrio de carga**, establezca los parámetros del servidor virtual. Para obtener más información sobre la configuración de un servidor virtual de equilibrio de carga, consulte Cómo funciona el equilibrio de carga
4. Una vez que haya establecido los parámetros para el servidor virtual de equilibrio de carga, haga clic en **Listo**.



5. Haga clic en el vínculo **Exportar como plantilla** en la parte superior para exportar los detalles del servidor como archivo de plantilla.
6. En la página **Crear Plantilla de Equilibrio de Carga**, introduzca la configuración de la plantilla.
7. Haga clic en **Done**.



Modificar una plantilla de servidor virtual de equilibrio de carga

Solo se pueden modificar los parámetros, enlaces y páginas configurados para una plantilla. El nombre y la ubicación de la plantilla especificados cuando se creó la plantilla no se pueden cambiar. El dispositivo Citrix ADC no ofrece la opción de modificar una plantilla de servidor virtual de equilibrio de carga.

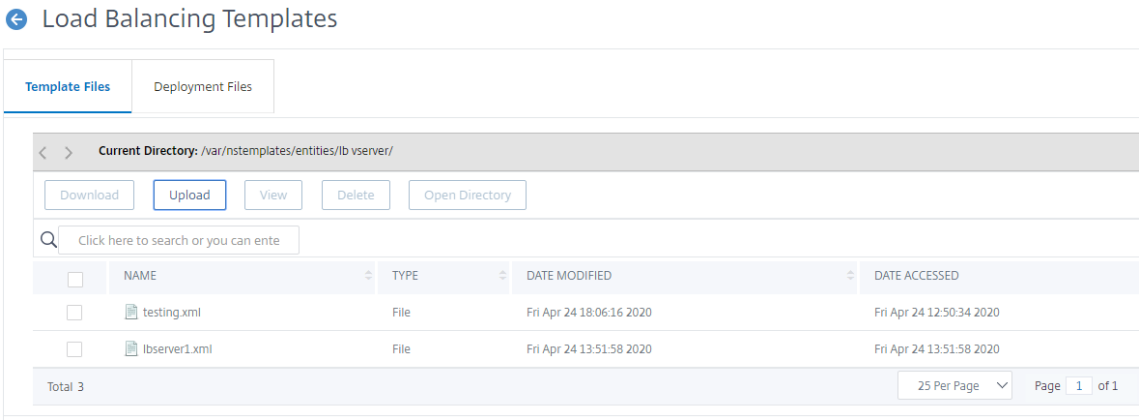
Para modificar un servidor virtual de equilibrio de carga mediante la GUI de Citrix ADC

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**.
2. En la página **Servidor virtual de equilibrio de carga**, modifique los parámetros de entidad.
3. Haga clic en Done.
4. Haga clic en **Exportar como vínculo de plantilla**.
5. Los cambios modificados ahora están disponibles en el archivo de plantilla de servidor virtual de equilibrio de carga.
6. En la página **Plantilla de equilibrio de carga exportada**, haga clic en **Listo**.

Administrar plantillas de servidor virtual de equilibrio de carga

Puede organizar los archivos de plantilla de servidor virtual de equilibrio de carga y los archivos de implementación mediante la GUI de Citrix ADC.

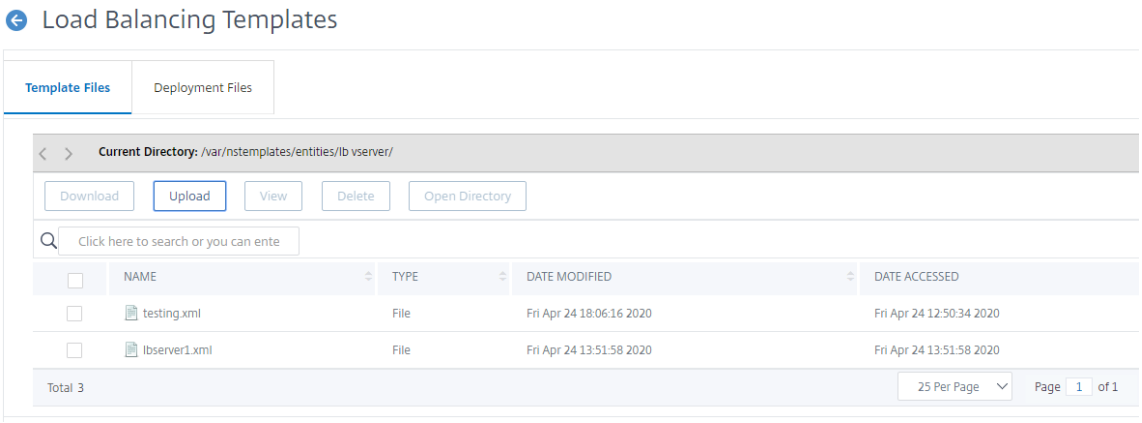
1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**.
2. En la página **Servidores virtuales**, seleccione la **acción Administrar plantilla**.
3. En la página **Plantillas de equilibrio de carga**, haga clic en la ficha **Archivo de plantilla**.
4. En la página de ficha **Archivos de plantilla**, puede cargar o descargar una plantilla desde y hacia la carpeta de plantillas del dispositivo.



5. Haga clic en **Cerrar**.

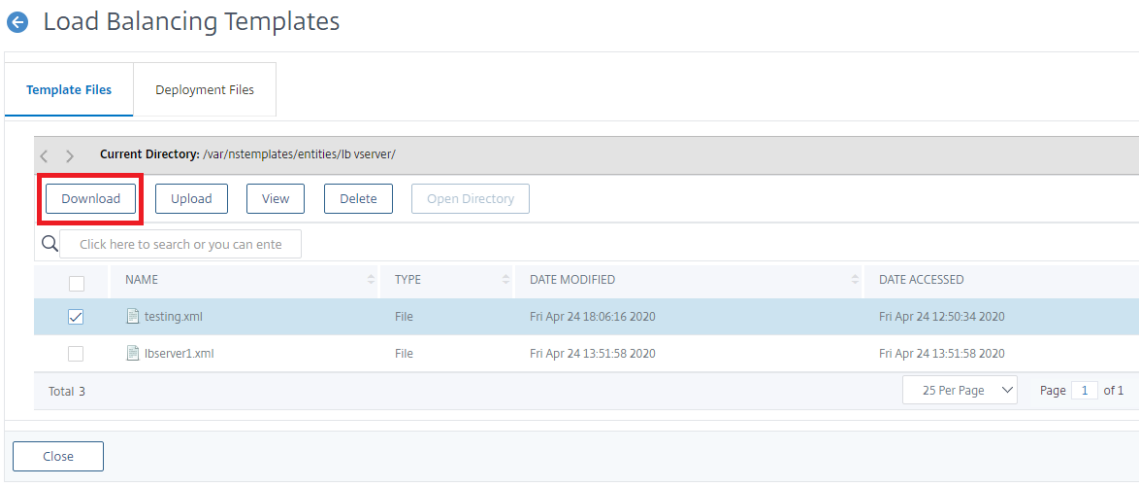
Para cargar la plantilla de entidad de servidor virtual de equilibrio de carga mediante la GUI de Citrix ADC

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**.
2. En la página **Servidores virtuales**, haga clic en **Seleccionar acción** y, a continuación, seleccione **Administrar plantilla**.
3. En la página Plantillas de equilibrio de carga, haga clic en la ficha **Archivos de plantilla**.
4. En la página de ficha **Archivos de plantilla**, haga clic en **Cargar** para cargar una plantilla.
5. Haga clic en **Cerrar**.



Para descargar la plantilla de entidad de servidor virtual de equilibrio de carga mediante la GUI de Citrix ADC

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**.
2. En la página **Servidores virtuales**, haga clic en **Seleccionar acción** y, a continuación, seleccione **Administrar plantilla**.
3. En la página **Plantillas de equilibrio de carga**, haga clic en la ficha **Archivos de plantilla** .
4. En la página de ficha Archivos de plantilla, seleccione un archivo de plantilla y haga clic en Descargar.
5. Haga clic en Cerrar.



Ejemplo de plantilla de servidor virtual de equilibrio de carga y plantilla de implementación

A continuación se muestra un ejemplo de un archivo de plantilla que se creó a partir de un servidor virtual de equilibrio de carga llamado “Lbvip”:

```
COPY

<?xml version=”1.0” encoding=”UTF-8” ?>
  <template>
    <template_info>
      <entity_name>Lbvip</entity_name>
      <version_major>10</version_major>
      <version_minor>0</version_minor>
      <build_number>40.406</build_number>
    </template_info>
    <entitytemplate>
      <lbvserver_list>
        <lbvserver>
          <name>Lbvip</name>
          <servicetype>HTTP</servicetype>
          <ipv46>0.0.0.0</ipv46>
          <ipmask>*</ipmask>
          <port>0</port>
          <range>1</range>
          <persistencetype>NONE</persistencetype>
          <timeout>2</timeout>
          <persistencebackup>NONE</persistencebackup>
          <backuppersistencetimeout>2</backuppersistencetimeout>
          <lbmethod>LEASTCONNECTION</lbmethod>
```



```
            <persistmask>255.255.255.255</persistmask>
            <v6persistmasklen>128</v6persistmasklen>
            <pq>OFF</pq>
            <sc>OFF</sc>
            <m>IP</m>
            <datalength>0</datalength>
            <dataoffset>0</dataoffset>
            <sessionless>DISABLED</sessionless>
            <state>ENABLED</state>
            <connfailover>DISABLED</connfailover>
            <clttimeout>180</clttimeout>
            <somethod>NONE</somethod>
            <sopersistence>DISABLED</sopersistence>
            <sopersistencetimeout>2</sopersistencetimeout>
            <redirectportrewrite>DISABLED</redirectportrewrite>
            <downstateflush>DISABLED</downstateflush>
            <gt2gb>DISABLED</gt2gb>
            <ipmapping>0.0.0.0</ipmapping>
            <disableprimaryondown>DISABLED</disableprimaryondown>
            <insertvserveripport>OFF</insertvserveripport>
            <authentication>OFF</authentication>
            <authn401>OFF</authn401>
            <push>DISABLED</push>
            <pushlabel>none</pushlabel>
            <l2conn>OFF</l2conn>
            <appflowlog>DISABLED</appflowlog>
            <icmpvsrresponse>PASSIVE</icmpvsrresponse>
            <lbvserver_cmppolicy_binding_list>
              <lbvserver_cmppolicy_binding>
                <name>Lbvip</name>
                <policyname>NOPOLICY-COMPRESSION</policyname>
                <priority>100</priority>
                <gotopriorityexpression>END</gotopriorityexpression>
                <bindpoint>REQUEST</bindpoint>
              </lbvserver_cmppolicy_binding>
            </lbvserver_cmppolicy_binding_list>
          </lbvserver>
        </lbvserver_list>
      </entitytemplate>
    </template>
<!--NeedCopy-->
```

Ejemplo de un archivo de implementación

A continuación se muestra el archivo de implementación asociado con el servidor virtual en el ejemplo anterior:
COPY

```
<?xml version=”1.0” encoding=”UTF-8” ?>
  <template_deployment>
    <template_info>
      <entity_name>Lbvip</entity_name>
      <version_major>10</version_major>
      <version_minor>0</version_minor>
      <build_number>40.406</build_number>
    </template_info>
    <service_list>
      <service>
      <ip>1.2.3.4</ip>
      <port>80</port>
      <servicetype>HTTP</servicetype>
      </service>
    </service_list>
    <servicegroup_list>
      <servicegroup>
        <name>svcgrp</name>
        <servicetype>HTTP</servicetype>
        <servicegroup_servicegroupmember_binding_list>
          <servicegroup_servicegroupmember_binding>
            <ip>1.2.3.90</ip>
            <port>80</port>
          </servicegroup_servicegroupmember_binding>
        <servicegroup_servicegroupmember_binding>
          <ip>1.2.8.0</ip>
          <port>80</port>
        </servicegroup_servicegroupmember_binding>
        <servicegroup_servicegroupmember_binding>
          <ip>1.2.8.1</ip>
          <port>80</port>
        </servicegroup_servicegroupmember_binding>
        <servicegroup_servicegroupmember_binding>
          <ip>1.2.9.0</ip>
          <port>80</port>
        </servicegroup_servicegroupmember_binding>
      </servicegroup_servicegroupmember_binding_list>
    </servicegroup>
  </servicegroup_list>
```



```
</template_deployment>

<!--NeedCopy-->
```

Llamadas HTTP

October 5, 2021

Para determinados tipos de solicitudes, o cuando se cumplen determinados criterios durante la evaluación de directivas, es posible que quiera paralizar brevemente la evaluación de directivas, recuperar información de un servidor y, a continuación, realizar una acción específica que depende de la información que se recupere. En otras ocasiones, cuando recibe determinados tipos de solicitudes, es posible que quiera actualizar una base de datos o el contenido alojado en un servidor web. Las llamadas HTTP permiten realizar todas estas tareas.

Una llamada HTTP es una solicitud HTTP o HTTPS que el dispositivo Citrix ADC genera y envía a una aplicación externa cuando se cumplen determinados criterios durante la evaluación de directivas. La información que se recupera del servidor se puede analizar mediante expresiones de directivas avanzadas y se puede realizar una acción adecuada. Puede configurar llamadas HTTP para conmutación de contenido HTTP, conmutación de contenido TCP, reescritura, respuesta y para el método de equilibrio de carga basado en tokens.

Antes de configurar una llamada HTTP, debe configurar una aplicación en el servidor al que se enviará la llamada. La aplicación, denominada *agente de llamada HTTP*, debe configurarse para responder a la solicitud de llamada HTTP con la información necesaria. El agente de llamada HTTP también puede ser un servidor web que sirve los datos para los que el dispositivo Citrix ADC envía la llamada. Debe asegurarse de que el formato de la respuesta a una llamada HTTP no cambia de una invocación a otra.

Después de configurar el agente de llamada HTTP, configure la llamada HTTP en el dispositivo Citrix ADC. Por último, para invocar la llamada, incluya la llamada en una directiva avanzada en la función Citrix ADC adecuada y, a continuación, vincule la directiva al punto de enlace en el que quiere que se evalúe la directiva.

Después de configurar la llamada HTTP, debe verificar la configuración para asegurarse de que la llamada funciona correctamente.

Cómo funciona una llamada HTTP

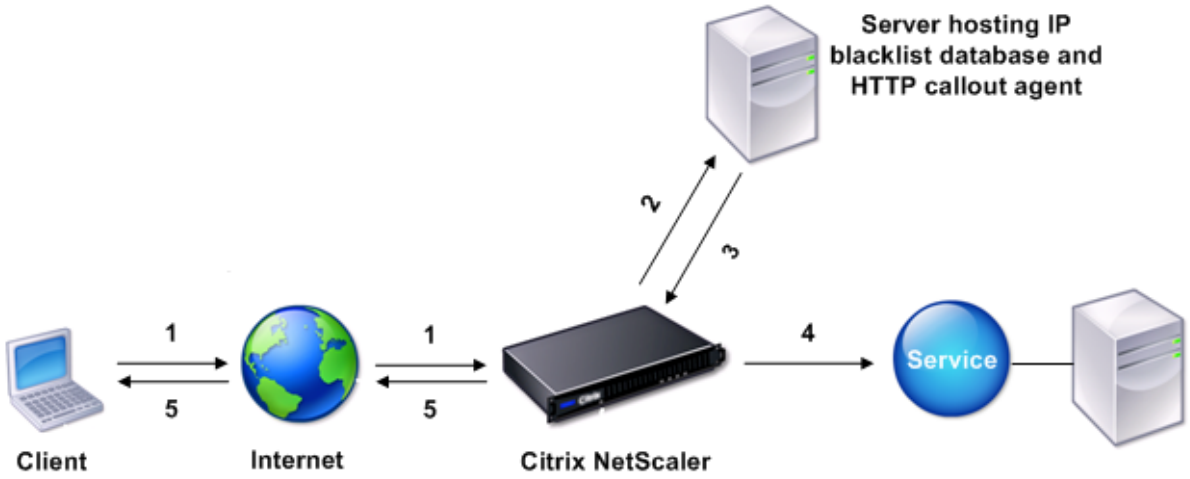
August 20, 2021

Cuando el dispositivo Citrix ADC recibe una solicitud de cliente, el dispositivo evalúa la solicitud en función de las directivas vinculadas a varios puntos de enlace. Durante esta evaluación, si el dispositivo encuentra la expresión de llamada HTTP`SYS.HTTP_CALLOUT(<name>)`, detiene brevemente la evaluación de directivas y envía una solicitud al agente de llamada HTTP mediante los parámetros configurados para la llamada HTTP especificada. Al recibir la respuesta, el dispositivo inspecciona la parte especificada de la respuesta y, a continuación, realiza una acción o evalúa la siguiente directiva, en función de si la evaluación de la respuesta del agente de llamada HTTP se evalúa como TRUE o FALSE, respectivamente. Por ejemplo, si la llamada HTTP se incluye en una directiva de respuesta, si la evaluación de la respuesta se evalúa como TRUE, el dispositivo realiza la acción asociada a la directiva de respuesta.

Si la configuración de llamada HTTP es incorrecta o incompleta, o si la llamada se invoca recursivamente, el dispositivo genera una condición UNDEF y actualiza el contador de visitas indefinido.

La siguiente ilustración ilustra el funcionamiento de una llamada HTTP que se invoca desde una directiva de respuesta enlazada globalmente. La llamada HTTP está configurada para incluir la dirección IP del cliente asociada a una solicitud entrante. Cuando el dispositivo Citrix ADC recibe una solicitud de un cliente, el dispositivo genera la solicitud de llamada y la envía al servidor de llamada, que aloja una base de datos de direcciones IP en la lista de prohibidos y un agente de llamada HTTP que comprueba si la dirección IP del cliente aparece en la base de datos. El agente de llamada HTTP recibe la solicitud de llamada, comprueba si aparece la dirección IP del cliente y envía una respuesta que evalúa el dispositivo Citrix ADC. Si la respuesta indica que la dirección IP del cliente no está en la lista de prohibidos, el dispositivo reenvía la respuesta al servicio configurado. Si la dirección IP del cliente está en la lista de prohibidos, el dispositivo restablece la conexión del cliente

Ilustración 1. Modelo de entidad de llamada HTTP



1: Client request
2: HTTP callout request to check whether the client is blacklisted
3: Response from HTTP callout agent
4: Request forwarded to service if 3 indicates a safe IP address
5: Connection RESET if 3 indicates a bad IP address

Notas sobre el formato de las solicitudes y respuestas HTTP

January 12, 2021

El dispositivo Citrix ADC no comprueba la validez de la solicitud de llamada HTTP. Por lo tanto, antes de configurar llamadas HTTP, debe conocer el formato de una solicitud HTTP. También debe conocer el formato de una respuesta HTTP, ya que la configuración de una llamada HTTP implica la configuración de expresiones que evalúan la respuesta del agente de llamada HTTP.

Esta sección incluye las siguientes secciones:

- Formato de una solicitud HTTP
- Formato de una respuesta HTTP

Formato de una solicitud HTTP

Una solicitud HTTP contiene una serie de líneas que terminan con un retorno de carro y un avance de línea, representado como cualquiera`<CR><LF> or \r\n`.

La primera línea de una solicitud (la *línea de mensaje*) contiene el método HTTP y el destino. Por ejemplo, una línea de mensaje para una solicitud GET contiene la palabra clave GET y una cadena que representa el objeto que se va a obtener, como se muestra en el ejemplo siguiente:


```
GET /mysite/mydirectory/index.html HTTP/1.1\r\n
<!--NeedCopy-->
```

El resto de la solicitud contiene encabezados HTTP, incluido un encabezado Host requerido y, si corresponde, un cuerpo del mensaje.

La solicitud termina con una línea bancaria (un extra<CR><LF> or \r\n).

A continuación se muestra un ejemplo de una solicitud:

```
Get /mysite/index.html HTTP/1.1\r\n
Host: 10.101.101.10\r\n
Accept: \*/\*\r\n
\r\n
<!--NeedCopy-->
```

Formato de una respuesta HTTP

Una respuesta HTTP contiene un mensaje de estado, encabezados HTTP de respuesta y el objeto solicitado o, si no se puede servir el objeto solicitado, un mensaje de error.

A continuación se presenta un ejemplo de una respuesta:

```
HTTP/1.1 200 OK\r\n
Content-Length: 55\r\n
Content-Type: text/html\r\n
Last-Modified: Wed, 12 Aug 1998 15:03:50 GMT\r\n
Accept-Ranges: bytes\r\n
ETag:  “04f97692cbd1:377” \r\n
Date: Thu, 19 Jun 2008 19:29:07 GMT\r\n
\r\n
<55-character response>
<!--NeedCopy-->
```

Configuración de una llamada HTTP

October 5, 2021

Al configurar una llamada HTTP, especifica el tipo de solicitud (HTTP o HTTPS), el destino y el formato de la solicitud. El formato esperado de la respuesta y, por último, la parte de la respuesta que quiere analizar.

Para el destino, debe especificar la dirección IP y el puerto del agente de llamada HTTP. O bien, utilice un servidor virtual de equilibrio de carga, conmutación de contenido o redirección de caché para administrar las solicitudes de llamada HTTP.

En el primer caso, las solicitudes de llamada HTTP se envían directamente al agente de llamada HTTP. En el segundo caso, las solicitudes de llamada HTTP se envían a la dirección IP virtual (VIP) del servidor virtual especificado. El servidor virtual procesa la solicitud de la misma manera que procesa una solicitud de cliente. Por ejemplo, si espera que se generen muchas llamadas, puede configurar instancias del agente de llamadas HTTP en varios servidores, vincular estas instancias (como servicios) a un servidor virtual de equilibrio de carga y, a continuación, especificar el servidor virtual de equilibrio de carga en la configuración de llamada HTTP. A continuación, el servidor virtual de equilibrio de carga equilibra la carga en las instancias configuradas según lo determinado por el algoritmo de equilibrio de carga.

Para el formato de la solicitud de llamada HTTP, puede especificar los atributos individuales de la solicitud de llamada HTTP (una llamada HTTP basada en atributos) o bien especificar toda la solicitud de llamada HTTP como expresión de directiva avanzada (una llamada HTTP basada en expresiones).

Para el formato de la solicitud de llamada HTTP, puede especificar los atributos individuales de la solicitud de llamada HTTP (una llamada HTTP basada en atributos) o puede especificar toda la solicitud de llamada HTTP como expresión de directiva avanzada (llamada HTTP basada en expresiones).

Para obtener más información, consulte Policy-httpCallout

Parámetro	Descripción
Nombre	Nombre de la llamada, máximo de 127 caracteres
Dirección IP y puerto (dirección IP/ *puerto*) o nombre del servidor virtual (vserver)	Dirección IPv4 o IPv6 del servidor al que se envía la llamada, o un comodín y el puerto del servidor al que se envía la llamada o un comodín. O bien, el nombre de un servidor virtual de equilibrio de carga, cambio de contenido o redirección de caché con un tipo de servicio HTTP.
Método HTTP (método HttpTp)	Método HTTP (HttpMethod). Método utilizado en la solicitud HTTP que envía esta llamada. Valores válidos: GET o POST. Predeterminado: GET.

Parámetro	Descripción
Expresión de host (HostExpr)	Expresión de host (HostExpr). Expresión de texto avanzada para configurar el encabezado Host. Longitud máxima: 255. La expresión puede ser un valor literal o puede ser una expresión avanzada que deriva el valor. Ejemplos: “10.101.10.11”, “http.req.header (“Host”)”
Expresión de raíz de URL (URLStemExpr)	Expresión de raíz de URL (URLStemExpr) Expresión de cadena avanzada para generar el sistema URL. Longitud máxima: 8191. La expresión puede ser una cadena literal o una expresión que deriva el valor. Ejemplos: “” /mysite/index.html “” “http.req.url”
Encabezados HTTP (encabezados)	Encabezados HTTP (encabezados). Expresión de texto avanzada para insertar encabezados HTTP y sus valores en la solicitud de llamada HTTP. Especifique un valor para cada encabezado. El nombre del encabezado se especifica como cadena y el valor del encabezado como expresión avanzada. Especifique los encabezados separados por espacio. Como -headers cip (client.ip.src) hdr (http.req.header (“HDR”)). El número de encabezados puede ser de 8
Solicitud basada en expresiones para enviar al servidor (FullReqExpr)	Solicitud HTTP exacta que Citrix ADC debe enviar como expresión avanzada a 8191 caracteres. Si especifica este parámetro, debe omitir los argumentos HttpMethod, HostExpr, URLStemExpr, encabezados y parámetros. La expresión de solicitud está restringida por la entidad en la que se utiliza la llamada. Por ejemplo, una expresión HTTP.RES no se puede utilizar en un banco de directivas de tiempo de solicitud ni en un banco de directivas de conmutación de contenido TCP.

Parámetro	Descripción
Solicitud basada en expresiones para enviar al servidor (BodyExpr)	Expresión de cadena avanzada para generar el cuerpo de la solicitud. La expresión puede contener una cadena literal o una expresión que deriva el valor (por ejemplo, client.ip.src). Exclusiva mutuamente con -FullReqExpr.
Parámetros	Expresión avanzada para insertar parámetros de consulta en la solicitud HTTP que envía la llamada. Especifique un valor para cada parámetro que configure. Si la solicitud de llamada utiliza el método GET, estos parámetros se insertan en la URL. Si la solicitud de llamada utiliza el método POST, estos parámetros se insertan en el cuerpo POST. El nombre del parámetro de consulta se configura como cadena y el valor como expresión avanzada. Los valores de los parámetros están codificados por URL. Especifique los parámetros separados por espacios como parámetros name1 (“name1”) name2 (http.req.header (“hdr”)). Se pueden configurar 8 parámetros como máximo.
Tipo de devolución (ReturnType)	Tipo de datos que devuelve la aplicación de destino en la respuesta a la llamada. Valores válidos: TEXTO: trata el valor devuelto como una cadena de texto. NUM: trata el valor devuelto como un número. BOOL: trata el valor devuelto como un valor booleano. Nota: No se puede cambiar el tipo de devolución después de configurarlo.

Parámetro	Descripción
Expresión para extraer datos de la respuesta (ResultExpr)	Expresión avanzada que extrae objetos HTTP.RES de la respuesta a la llamada HTTP. La longitud máxima es de 8191. Las operaciones de esta expresión deben coincidir con el tipo de devolución. Por ejemplo, si configura un tipo de texto de retorno, la expresión de resultado debe ser una expresión basada en texto. Si el tipo de devolución es num, la expresión de resultado (ResultExpr) debe devolver un valor numérico similar al siguiente: “http.res.body (10000) .length” Nota: A veces, si establece un tipo de devolución de TEXTO y el resultado enviado desde el servidor supera los 16 KB, la expresión de resultado puede devolver NULL. Por ejemplo, cuando el resultado es una cadena concatenada que supera los 16 KB.
Esquema	Tipo de esquema del servidor de llamadas. Ejemplo: HTTP, https
Caché para Secs	Duración, en segundos, durante la que se almacena en caché la respuesta de la llamada. Las respuestas almacenadas en caché se almacenan en un grupo de contenido de almacenamiento en caché integrado denominado “CalloutContentGroup”. Si no se configura ninguna duración, las respuestas de llamada no se almacenan en caché a menos que se utilice una configuración normal de almacenamiento en caché para almacenarlas en caché. Este parámetro tiene prioridad sobre cualquier configuración normal de almacenamiento en caché que de otro modo se aplicaría a estas respuestas.

Nota: El dispositivo no comprueba la validez de la solicitud. Debes asegurarte de que la solicitud sea válida y no contiene ninguna información confidencial. Una configuración de llamada HTTP incorrecta o incompleta da como resultado una condición UNDEF en tiempo de ejecución que no está asociada a una acción. La condición UNDEF simplemente actualiza el contador de visitas indefinidas,

lo que permite solucionar problemas de una llamada HTTP configurada incorrectamente. Sin embargo, el dispositivo analiza la solicitud de llamada HTTP para permitirle configurar determinadas funciones de Citrix ADC para la llamada. Esto puede conducir a una llamada HTTP que se invoca a sí misma. Para obtener información sobre la recursión de llamadas y cómo puede evitarla, consulte Evitar la recursión de llamadas HTTP.

Por último, independientemente de si utiliza atributos de solicitud HTTP o una expresión para definir el formato de la solicitud de llamada HTTP, debe especificar el formato de la respuesta del agente de llamada HTTP y la parte de la respuesta que quiere evaluar. El tipo de respuesta puede ser un valor booleano, un número o un texto. Basándose únicamente en este tipo de devolución, puede utilizar los métodos de expresión adicionales en la respuesta de llamada. Si el tipo de devolución es un número, puede utilizar la expresión basada en números en la respuesta de llamada. La parte de la respuesta que quiere evaluar se especifica mediante una expresión. Por ejemplo, si especifica que la respuesta contiene texto, se puede utilizar `HTTP.RES.BODY(<unit>)` para especificar que el dispositivo debe evaluar solo los primeros <unit>bytes de la respuesta del agente de llamada.

En la línea de comandos, primero se crea una llamada HTTP mediante el comando add. Cuando se agrega una llamada, todos los parámetros se establecen en un valor predeterminado de NONE, excepto el método HTTP, que se establece en un valor predeterminado de GET. A continuación, configure los parámetros de la llamada mediante el comando set. El comando set se utiliza para configurar ambos tipos de llamadas (basadas en atributos y basadas en expresiones). La diferencia radica en los parámetros que se utilizan para configurar los dos tipos de llamadas. Por lo tanto, las instrucciones de línea de comandos siguientes incluyen un comando set para configurar una llamada basada en atributos y un comando set para configurar una llamada basada en expresiones. En la utilidad de configuración, todas estas tareas de configuración se realizan en un solo cuadro de diálogo.

Nota: Antes de colocar una llamada HTTP en una directiva, puede modificar todos los parámetros configurados excepto el tipo de devolución. Una vez que una llamada HTTP está en una directiva, no se puede modificar por completo una expresión configurada en la llamada. Por ejemplo, no puede cambiar HTTP.REQ.HEADER (“myval”) a CLIENT.IP.SRC. Puede modificar los operadores y argumentos que se pasan a la expresión. Por ejemplo, puede cambiar`HTTP.REQ.HEADER(”myVal1”)` a`HTTP.REQ.HEADER(”myVal2”)` o`HTTP.REQ.HEADER(”myVal”)` a`HTTP.REQ.HEADER(”myVal”).AFTER_STR(<string>)`. Si el comando set falla, cree una llamada HTTP.

La configuración de llamadas HTTP implica la configuración de expresiones de directivas avanzadas. Para obtener más información sobre cómo configurar expresiones de directivas avanzadas, consulte Configuración de expresiones de directivas avanzadas: Introducción.

Para configurar una llamada HTTP mediante la interfaz de línea de comandos

En el símbolo del sistema, haga lo siguiente:

Cree una llamada HTTP.


```
add policy httpCallout <name> [-IPAddress <ip_addr|ipv6_addr>] [-port<
    port>] [-vServer <string>] [-returnType <returnType>] [-httpMethod (
    GET | POST )] [-hostExpr <expression>]  [-urlStemExpr <expression>]
    [-headers <name(value)> ...] [-parameters <name(value)> ...] [-
    bodyExpr <expression>] [-fullReqExpr <expression>] [-scheme ( http |
     https )] [-resultExpr <expression>] [-cacheForSecs <secs>] [-
    comment <string>]

<!--NeedCopy-->
```

Ejemplo:

```
add policy httpCallout mycallout -vserver lbv1 -returnType num -
    httpMethod GET -hostExpr 'http.req.header("Host")'-urlStemExpr "http
    .req.url" -parameters Name("My Name") -headers Name("MyHeader")-
    resultExpr "http.res.body(10000).length"

<!--NeedCopy-->
```

Modifique la configuración de la llamada HTTP.

```
set policy httpCallout <name> [-IPAddress <ip_addr|ipv6_addr|\*>] [-
    port <port|\*>] [-vServer <string>] [-returnType <returnType>] [-
    httpMethod ( GET | POST )] [-hostExpr <string>] [-urlStemExpr <
    string>] [-headers <name(value)> ...] [-parameters <name(value)>
    ...] [-resultExpr <string>]

<!--NeedCopy-->
```

Ejemplo:

```
> set policy httpCallout mycallout -vserver lbv1 -returnType num -
    httpMethod GET -hostExpr 'http.req.header("Host")'-urlStemExpr "http
    .req.url" -parameters Name("My Name") -headers Name("MyHeader") -
    resultExpr "http.res.body(10000).length"
<!--NeedCopy-->
```

Configure la llamada HTTP mediante el parámetro FullReqExpr.


```
set policy httpCallout <name> [-vServer <string>] [-returnType <
    returnType>] [-fullReqExpr <string>] [-resultExpr <string>]
<!--NeedCopy-->
```

Ejemplo:

```
> set policy httpCallout mycallout1 -vserver lbv1 -returnType num
    fullReqExpr q{
 "GET " + http.req.url + "HTTP/" + http.req.version.major + "." + http.
    req.version.minor.sub(1) + "r\nHost:10.101.10.10\r\nAccept: \*/\*\r
    \n\r\n" }


<!--NeedCopy-->
```

Verifique las configuraciones de la llamada HTTP.

```
show policy httpCallout `<name>`

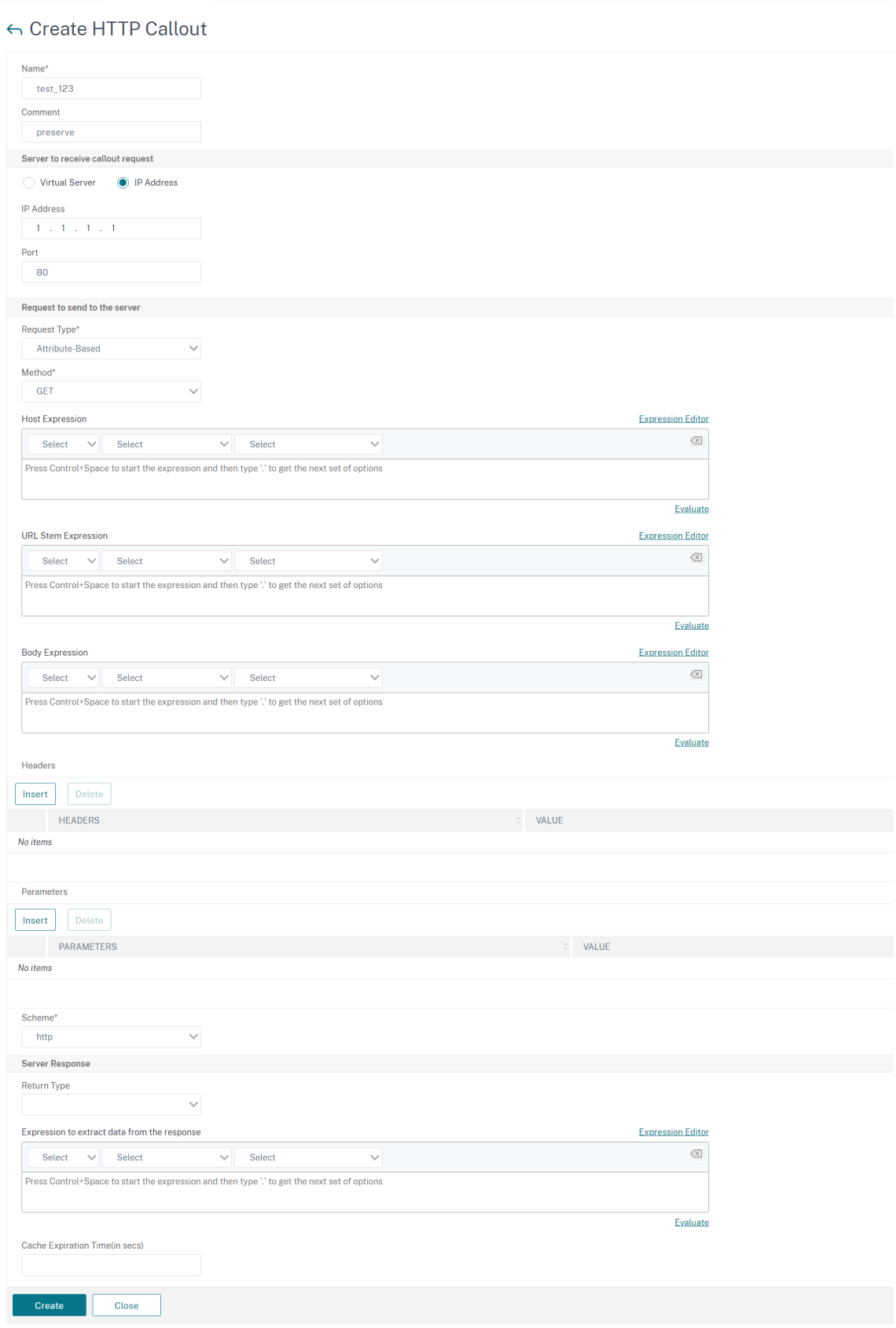
sh policy httpCallout mycallout1
> Name: mycallout1
>Vserver: lbv1 (UP)
Effective Vserver state: UP
Return type: TEXT
Scheme: HTTP
Full REQ expr: "GET " + http.req.url + "HTTP/" + http.req.version.major
    + "." + http.req.version.minor.sub(1)+ "r\nHost:10.101.10.10\r\
    nAccept: \*/\*\r\n\r\n"
Result expr: http.res.body(100)
Hits: 0
Undef Hits: 0
Done
>

<!--NeedCopy-->
```

Para configurar una llamada HTTP mediante la utilidad de configuración

1. Vaya a **AppExpert** > **Llamadas HTTP**.
2. En el panel de detalles, haga clic en **Agregar**.

3. En el cuadro de diálogo **Crear llamada HTTP**, configure los parámetros de la llamada HTTP. Para obtener una descripción del parámetro, pase el cursor del ratón sobre la casilla de verificación.
4. Haga clic en **Create** y, luego, en **Close**.



Verificación de la configuración

August 20, 2021

Para que una llamada HTTP funcione correctamente, todos los parámetros de llamada HTTP y las entidades asociadas a la llamada deben configurarse correctamente. Aunque el dispositivo Citrix ADC no comprueba la validez de los parámetros de llamada HTTP, indica el estado de las entidades enlazadas, es decir, el servidor o el servidor virtual al que se envía la llamada HTTP. En la siguiente tabla se enumeran los iconos y se describen las condiciones en las que se muestran los iconos.

Icono	Indica que
	El estado del servidor que aloja el agente de llamada HTTP, o el servidor virtual de equilibrio de carga, cambio de contenido o redirección de caché al que se envía la llamada HTTP es UP.
	El estado del servidor que aloja el agente de llamada HTTP, o el servidor virtual de equilibrio de carga, cambio de contenido o redirección de caché al que se envía la llamada HTTP es OUT OF SERVICE.
	El estado del servidor que aloja el agente de llamada HTTP, o el servidor virtual de equilibrio de carga, cambio de contenido o redirección de caché al que se envía la llamada HTTP es DOWN.

Cuadro 1 Iconos que indican los estados de entidades enlazadas a una llamada HTTP

Para que una llamada HTTP funcione correctamente, el icono debe ser verde en todo momento. Si el icono no es verde, compruebe el estado del servidor de llamadas o del servidor virtual al que se envía la llamada HTTP. Si la llamada HTTP no funciona como se esperaba aunque el icono sea verde, compruebe los parámetros configurados para la llamada.

También puede verificar la configuración enviando solicitudes de prueba que coincidan con la directiva desde la que se invoca la llamada HTTP, comprobando el contador de visitas para la directiva y la llamada HTTP y comprobando las respuestas que el dispositivo Citrix ADC envía al cliente.

Nota: Una llamada HTTP a veces puede invocarse recursivamente por segunda vez. Si esto sucede, el contador de visitas se incrementa en dos recuentos para cada llamada generada por el dispositivo.

Para que el contador de visitas muestre el valor correcto, debe configurar la llamada HTTP de tal manera que no se invoque por segunda vez. Para obtener más información sobre cómo evitar la recursión de llamadas HTTP, consulte Evitar la recursión de llamadas HTTP.

Para ver el contador de visitas de una llamada HTTP

1. Vaya a **AppExpert** > **Llamadas HTTP**.
2. En el panel de detalles, haga clic en la llamada HTTP para la que quiere ver el contador de visitas y, a continuación, vea las visitas en el área **Detalles**.

Invocación de una llamada HTTP

October 5, 2021

Después de configurar una llamada HTTP, se invoca la llamada mediante la inclusión de la expresión `SYS.HTTP_CALLOUT(<name>)` en una regla de directiva avanzada. En esta expresión, `<name>` es el nombre de la llamada HTTP que quiere invocar.

Puede utilizar operadores de expresión de directiva avanzada con la expresión de llamada para procesar la respuesta y, a continuación, realizar una acción adecuada. El tipo de devolución de la respuesta del agente de llamada HTTP determina el conjunto de operadores que se pueden utilizar en la respuesta. Si la parte de la respuesta que quiere analizar es texto, puede utilizar un operador de texto para analizar la respuesta. Por ejemplo, puede usar el <string>operador CONTAINS() para comprobar si la parte especificada de la respuesta contiene una cadena concreta, como en el ejemplo siguiente:

```
SYS.HTTP_CALLOUT(mycallout).contains("Good IP address")
<!--NeedCopy-->
```

Si utiliza la expresión anterior en una directiva de respuesta, puede configurar una acción de respuesta adecuada.

Del mismo modo, si la parte de la respuesta que quieres evaluar es un número, puede usar un operador numérico como GT (int). Si la respuesta contiene un valor booleano, puede usar un operador booleano.

Nota: Una llamada HTTP puede invocarse a sí misma de forma recursiva. Se puede evitar la recursividad de llamadas HTTP combinando la expresión de llamada HTTP con una expresión de directiva avanzada que impide la recursividad. Para obtener información sobre cómo evitar la recursión de llamadas HTTP, consulte Evitar la recursión de llamadas HTTP.

También puede hacer llamadas HTTP en cascada configurando directivas que invocan cada una de ellas una llamada después de evaluar las llamadas generadas previamente. En este caso, después de que una directiva invoca una llamada, cuando el dispositivo Citrix ADC analiza la llamada antes de enviarla al servidor de llamadas, un segundo conjunto de directivas puede evaluar la llamada e invocar llamadas adicionales, que a su vez pueden evaluarse mediante un tercer conjunto de directivas, etc. Esta implementación se describe en el siguiente ejemplo.

En primer lugar, puede configurar una llamada HTTP denominada myCallout1 y, a continuación, configurar una directiva de respuesta, Pol1, para invocar myCallout1. A continuación, podría configurar una segunda llamada HTTP, MyCallout2, y una directiva de respuesta, Pol2. Configurar Pol2 para evaluar myCallout1 e invocar myCallout2. Enlaza ambas directivas de respuesta globalmente.

Para evitar la recursividad de llamadas HTTP, myCallout1 se configura con un encabezado HTTP personalizado único denominado “Request1”. “ Pol1 está configurado para evitar la recursividad de llamadas HTTP mediante la expresión de directiva avanzada,

```
1 HTTP.REQ.HEADER(”Request1”).EQ(”Callout Request”).NOT.
2 <!--NeedCopy-->
```

Pol2 utiliza la misma expresión de directiva avanzada, pero excluye el operador .NOT para que la directiva evalúe MyCallout1 cuando el dispositivo Citrix ADC lo está analizando. Tenga en cuenta que myCallout2 identifica su propio encabezado único denominado “Request2” y Pol2 incluye una expresión de directiva avanzada para evitar que MyCallout2 se invoque de forma recursiva.

Ejemplo:

```
1  > add policy httpCallout myCallout1
2
3  Done
4
5  > set policy httpCallout myCallout1 -IPAddress 10.102.3.95 -port 80 -
       returnType TEXT -hostExpr
6   ””10.102.3.95”” -urlStemExpr ””/cgi-bin/check_clnt_from_database.pl””
        -headers Request1
7  (”Callout Request”) -parameters cip(CLIENT.IP.SRC) -resultExpr ”HTTP.
       RES.BODY(100)”
8
9  Done
10
11 > add responder policy Pol1 ”HTTP.REQ.HEADER(”Request1”).EQ(”Callout
       Request”).NOT &&
12 SYS.HTTP_CALLOUT(myCallout1).CONTAINS(”IP Matched”)” RESET
```



```
13
14 Done
15
16 > bind responder global Pol1 100 END -type OVERRIDE
17
18 Done
19
20 > add policy httpCallout myCallout2
21
22 Done
23
24 > set policy httpCallout myCallout2 -IPAddress 10.102.3.96 -port 80 -
      returnType TEXT -hostExpr
25 ””10.102.3.96”” -urlStemExpr ””/cgi-bin/
      check_clnt_location_from_database.pl”” -headers Request2
26 (”Callout Request”) -parameters cip(CLIENT.IP.SRC) -resultExpr ”HTTP.
      RES.BODY(200)”
27
28  Done
29
30 > add responder policy Pol2 ”HTTP.REQ.HEADER(”Request2”).EQ(”Callout
      Request”).NOT &&
31  HTTP.REQ.HEADER(”Request1”).EQ(”Callout Request”) && SYS.HTTP_CALLOUT(
       myCallout2).CONTAINS
32 (”APAC”)” RESET
33
34  Done
35
36 > bind responder global Pol2 110 END -type OVERRIDE
37
38 Done
39 <!--NeedCopy-->
```

Evitar la recursividad de llamadas HTTP

October 5, 2021

Aunque el dispositivo Citrix ADC no comprueba la validez de la solicitud de llamada HTTP, la analiza una vez antes de enviarla al agente de llamada HTTP. Este análisis permite que el dispositivo trate la solicitud de llamada como cualquier otra solicitud entrante, lo que a su vez le permite configurar varias funciones útiles de Citrix ADC (como el almacenamiento en caché integrado) para que funcionen en la solicitud de llamada.

Sin embargo, durante este análisis, la solicitud de llamada HTTP puede seleccionar la misma directiva y, por lo tanto, invocarse a sí misma de forma recursiva. El dispositivo detecta la invocación recursiva y genera una condición indefinida (UNDEF). Sin embargo, la invocación recursiva hace que los contadores de selección de llamadas HTTP y de directiva aumenten en dos recuentos cada uno en lugar de un recuento cada uno.

Para evitar que una llamada se invoque por sí misma, debe identificar al menos una función única de la solicitud de llamada HTTP y, a continuación, excluir todas las solicitudes con esta función de ser procesadas por la regla de directiva que invoca la llamada. Puede hacerlo si incluye otra expresión de directiva avanzada en la regla de directivas. La expresión debe preceder a la expresión `SYS.HTTP_CALLOUT(<name>)` para que se evalúe antes de evaluar la expresión de llamada. Por ejemplo:

```
<Expression that prevents callout recursion> OR SYS.HTTP_CALLOUT(<name
    >)
<!--NeedCopy-->
```

Al configurar una regla de directivas de esta manera, cuando el dispositivo genera la solicitud y la analiza, la regla compuesta se evalúa como FALSE, la llamada no se genera por segunda vez y los contadores de selección se incrementan correctamente.

Una forma de asignar una función única a una solicitud de llamada HTTP es incluir un encabezado HTTP personalizado único al configurar la llamada. A continuación se muestra un ejemplo de una llamada HTTP llamada “myCallout”. “ La llamada genera una solicitud HTTP que comprueba si la dirección IP de un cliente está presente en una base de datos de direcciones IP en la lista de prohibidos. La llamada incluye un encabezado personalizado llamado “Solicitud”, que se establece en el valor “Solicitud de llamada”. “ Una directiva de respuesta enlazada globalmente, “Pol1”, invoca la llamada HTTP pero excluye todas las solicitudes cuyo encabezado de solicitud esté configurado con este valor, lo que impide una segunda invocación de myCallout. La expresión que impide una segunda invocación es HTTP.REQ.HEADER (“Solicitud”) .EQ (“Solicitud de llamada”) .NOT.

Ejemplo:

```
> add policy httpCallout myCallout
 Done

> set policy httpCallout myCallout -IPAddress 10.102.3.95 -port 80 -
    returnType TEXT -hostExpr ””10.102.3.95”” -urlStemExpr ””/cgi-bin/
    check_clnt_from_database.pl”” -headers Request(”Callout Request”) -
    parameters cip(CLIENT.IP.SRC) -resultExpr ”HTTP.RES.BODY(100)”
Done

```



```
> add responder policy Pol1 ”HTTP.REQ.HEADER(”Request”).EQ(”Callout
    Request”).NOT && SYS.HTTP_CALLOUT(myCallout).CONTAINS(”IP Matched”)”
     RESET
Done

> bind responder global Pol1 100 END -type OVERRIDE
Done
<!--NeedCopy-->
```

Nota:
También puede configurar una expresión para comprobar si la URL de solicitud incluye la expresión raíz configurada para la llamada HTTP. Para implementar la solución, asegúrese de que el agente de llamada HTTP solo puede responder a las llamadas HTTP y no a otras solicitudes dirigidas a través del dispositivo. Si el agente de llamada HTTP es una aplicación o un servidor web que atiende otras solicitudes de cliente, dicha expresión impide que el dispositivo procese esas solicitudes de cliente. En su lugar, utilice un encabezado personalizado único como se describió anteriormente.

Almacenamiento en caché de respuestas de llamada HTTP

January 12, 2021

Para mejorar el rendimiento durante el uso de llamadas, puede utilizar la función de almacenamiento en caché integrada para almacenar en caché las respuestas de llamada. Las respuestas se almacenan en un grupo de contenido de almacenamiento en caché integrado denominado CalloutContentGroup durante un período de tiempo especificado.

Nota: Para almacenar en caché las respuestas de llamada, asegúrese de que la función de almacenamiento en caché integrada esté habilitada.

Para establecer la duración de la caché mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
set policy httpCallout <name> -cacheForSecs <secs>
```

Ejemplo:

```
> set httpcallout httpcallout1 -cacheForSecs 120
<!--NeedCopy-->
```


Para establecer la duración de la caché mediante la utilidad de configuración

1. Vaya a **AppExpert > Llamadas HTTP**.
2. En el panel de detalles, seleccione la llamada HTTP para la que quiere establecer la duración de la caché y haga clic en **Abrir**.
3. En el cuadro de diálogo **Configurar llamada HTTP**, especifique el **tiempo de caducidad de la caché**.
4. Compruebe que ha especificado la duración de tiempo correcta y, a continuación, haga clic en **Aceptar**.

Caso de uso: Filtrar clientes mediante una lista de prohibidos de IP

October 5, 2021

Las llamadas HTTP se pueden utilizar para bloquear solicitudes de clientes que están en la lista de prohibidos por el administrador. La lista de clientes puede ser una lista de prohibidos públicamente conocida, una lista de prohibidos que mantenga para su organización o una combinación de ambas.

El dispositivo Citrix ADC comprueba la dirección IP del cliente con la lista de prohibidos preconfigurada y bloquea la transacción si la dirección IP se ha incluido en la lista de prohibidos. Si la dirección IP no está en la lista, el dispositivo procesa la transacción.

Para implementar esta configuración, debe realizar las siguientes tareas:

1. Habilite el respondedor en el dispositivo Citrix ADC.
2. Cree una llamada HTTP en el dispositivo Citrix ADC y configúrela con detalles sobre el servidor externo y otros parámetros necesarios.
3. Configure una directiva de respuesta para analizar la respuesta a la llamada HTTP y, a continuación, vincular la directiva de forma global.
4. Cree un agente de llamada HTTP en el servidor remoto.

Activación del respondedor

Debe habilitar el respondedor antes de poder usarlo.

Para habilitar el respondedor mediante la interfaz gráfica de usuario

1. Asegúrese de haber instalado la licencia de respuesta.
2. En la utilidad de configuración, expanda AppExpert, haga clic con el botón secundario en **Respondery**, a continuación, haga clic en **Activar función Responder**

Creación de una llamada HTTP en el dispositivo Citrix ADC

Cree una llamada HTTP, Http_callout, con la configuración de parámetros que se muestra en la tabla siguiente. Para obtener más información sobre cómo crear una llamada HTTP, consulte Configuración de una llamada HTTP pdf.

Configurar una directiva de respuesta y vincularla globalmente

Después de configurar la llamada HTTP, compruebe la configuración de llamada y, a continuación, configure una directiva de respuesta para invocar la llamada. Aunque puede crear una directiva de respuesta en el subnodo
Directivas y, a continuación, enlazarla globalmente mediante
Responder Policy Manager, esta demostración utiliza
Responder Policy Manager para crear la directiva de respuesta y enlazar la directiva de forma global.

Para crear una directiva de respuesta y vincularla globalmente mediante

1. Vaya a **AppExpert** > **Responder**.
2. En el panel de detalles, en **Policy Manager**, haga clic en **Policy Manager**.
3. En el cuadro de diálogo **Responder Policy Manager**, haga clic en **Anular global**.
4. Haga clic en **Insertar directiva**y, a continuación, en **Nombre de la directiva**, haga clic en **Nueva directiva**.
5. En el cuadro de diálogo **Crear directiva de respuesta**, haga lo siguiente:
   a) En Nombre, escriba **PolicyResponder1**.
   b) En **Acción**, seleccione **RESTABLECER**.
   c) En Acción de **resultado no definido, seleccione Acciónglobal de resultado indefinido** .
   d) En **Expresión**, escriba la siguiente expresión de directiva avanzada:

```
1 ”HTTP.REQ.HEADER(”Request”).EQ(”Callout Request”).NOT && SYS.
     HTTP_CALLOUT(HTTP_Callout).CONTAINS(”IP Matched”)”
2 <!--NeedCopy-->
```

   e) Haga clic en **Crear**y, a continuación, en **Cerrar**.
6. Haga clic en **Aplicar cambios**y, a continuación, en **Cerrar**.

Creación de un agente de llamada HTTP en el servidor remoto

Ahora debe crear un agente de llamada HTTP en el servidor de llamadas remoto que recibirá las solicitudes de llamada del dispositivo Citrix ADC y responderá de forma adecuada. El agente de llamada HTTP es un script diferente para cada implementación y debe escribirse teniendo en cuenta las especificaciones del servidor, como el tipo de base de datos y el lenguaje de scripts admitido.

A continuación se muestra un agente de llamada de ejemplo que verifica si la dirección IP dada es parte de una lista de prohibidos IP. El agente se ha escrito en el lenguaje de scripting Perl y utiliza una base de datos MYSQL.

El siguiente script CGI comprueba si hay una dirección IP determinada en el servidor de llamadas.

```
#!/usr/bin/perl -w
print ”Content-type: text/html\n\n”;
        use DBI();
        use CGI qw(:standard);
#Take the Client IP address from the request query
        my $ip_to_check = param('cip');
# Where a MYSQL database is running
        my $dsn = 'DBI:mysql:BAD_CLIENT:localhost';
# Database username to connect with
        my $db_user_name =  ‘dbuser’ ;
# Database password to connect with
        my $db_password = 'dbpassword';
        my ($id, $password);
# Connecting to the database
        my $dbh = DBI->connect($dsn, $db_user_name, $db_password);
        my $sth = $dbh->prepare(qq{
  select * from bad_clnt  }
 );
        $sth->execute();
        while (my ($ip_in_database) = $sth->fetchrow_array()) {

        chomp($ip_in_database);
# Check for IP match
        if ($ip_in_database eq $ip_to_check) {

              print ”\n IP Matched\n”;
                                                    $sth->finish();
                                              exit;
                 }

        }
```



```
32
33         print ”\n IP Failed\n”;
34         $sth->finish();
35         exit;
36 <!--NeedCopy-->
```

Caso de uso: compatibilidad con ESI para obtener y actualizar contenido de forma dinámica

October 5, 2021

Edge Side Includes (ESI) es un lenguaje de marcado para el ensamblaje de contenido web dinámico de nivel perimetral. Ayuda a acelerar las aplicaciones dinámicas basadas en Web mediante la definición de un lenguaje de marcado sencillo para describir los componentes de páginas web que se pueden almacenar en caché y no se pueden almacenar en caché que se pueden agregar, ensamblar y entregar en el perímetro de la red. Mediante el uso de llamadas HTTP en el dispositivo Citrix ADC, puede leer las construcciones ESI y agregar o ensamblar contenido de forma dinámica.

Para implementar esta configuración, debe realizar las siguientes tareas:

1. Habilite la reescritura en el dispositivo Citrix ADC.
2. Cree una llamada HTTP en el dispositivo y configúrela con detalles sobre el servidor externo y otros parámetros necesarios.
3. Configure una acción de reescritura para reemplazar el contenido ESI por el cuerpo de respuesta de llamada.
4. Configure una directiva de reescritura para especificar las condiciones en las que se realiza la acción y, a continuación, vincule la directiva de reescritura de forma global.

Habilitar la reescritura

La reescritura debe estar habilitada antes de utilizarla en el dispositivo Citrix ADC. En el procedimiento siguiente se describen los pasos para habilitar la función de reescritura.

Para habilitar la reescritura mediante la interfaz gráfica de usuario

1. Asegúrese de haber instalado la licencia de reescritura.
2. En la utilidad de configuración, expanda AppExpert, haga clic con el botón secundario en Reescribir y, a continuación, haga clic en Habilitar función de reescritura.

Crear una llamada HTTP en el dispositivo Citrix ADC

Para obtener más información sobre cómo crear una llamada HTTP, consulte Configuración de una llamada HTTP.
Para obtener más información sobre los valores de los parámetros, consulte Parámetros y valores para HTTP-Callout-2 pdf.

Configuración de la acción de reescritura

Cree una acción de reescritura, Action-Rewrite-1, para reemplazar el contenido ESI por el cuerpo de respuesta de la llamada. Utilice la configuración de parámetros que se muestra en la tabla siguiente.

Cuadro 2. Parámetros y valores de Action-Rewrite-1

Parámetro	Valor
Nombre	Action-Rewrite-1
Tipo	Reemplazar
Expresión para elegir la referencia de texto de destino	“HTTP.RES.BODY(500).AFTER_STR (\” <ejemplo>\”).BEFORE_STR (\”</ejemplo>\”)”
Expresión de cadena para texto de sustitución	“SYS.HTTP_CALLOUT(HTTP-Callout-2)”

Para configurar la acción de reescritura mediante la utilidad de configuración

1. Vaya a **AppExpert** > **Reescribir** > **Acciones**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En el cuadro de diálogo **Crear acción de reescritura**, en Nombre, escriba **Action-Rewrite-1**.
4. En Tipo, seleccione **REEMPLAZAR**.
5. En **Expresión** para elegir la referencia de texto de destino, escriba la siguiente expresión de directiva avanzada:

```
1 ”HTTP.RES.BODY(500).AFTER_STR(”<example>”).BEFORE_STR(”<example>”)
    ”
2 <!--NeedCopy-->
```

6. En la expresión de cadena del texto de sustitución, escriba la siguiente expresión de cadena:


```
”SYS.HTTP_CALLOUT(HTTP-Callout-2)”
<!--NeedCopy-->
```

7. Haga clic en **Crear**y, a continuación, en **Cerrar**.

Creación de la directiva de reescritura y vinculación global

Cree una directiva de reescritura, Policy-Rewrite-1, con la configuración de parámetros que se muestra en la tabla siguiente. Puede crear una directiva de reescritura en el subnodo Directivas y, a continuación, enlazarla globalmente mediante el Administrador de directivas de reescritura. Alternativamente, puede utilizar el Administrador de directivas de reescritura para realizar ambas tareas simultáneamente. En esta demostración se utiliza el Administrador de directivas de reescritura para realizar ambas tareas.

Tabla 3. Parámetros y valores de Policy-Rewrite-1

Parámetro	Valor
Nombre	Policy-Rewrite-1
Acción	Action_Rewrite-1
Acción de resultado indefinido	-Acción global de resultados indefinidos-
Expresión	“HTTP.REQ.HEADER(“Name”).CONTAINS (“Callout”).NOT”

Para configurar una directiva de reescritura y vincularla de forma global mediante la utilidad de configuración

1. Vaya a **AppExpert** > **Reescribir**.
2. En el panel de detalles, en **Policy Manager**, haga clic en **Reescribir Policy Manager**.
3. En el cuadro de diálogo **Reescribir Policy Manager**, haga clic en **Anular global**.
4. Haga clic en **Insertar directiva**y, a continuación, en la columna **Nombre de la directiva**, haga clic en **Nueva directiva**.
5. En el cuadro de diálogo **Crear directiva de reescritura**, haga lo siguiente:
   1.En Nombre, escriba Policy-Rewrite-1.
   a) En Acción, seleccione Action-Rewrite-1.
   b) En Acción de resultado no definido, seleccione Acción global de resultado indefinido.
   c) En Expresión, escriba la siguiente expresión de directiva avanzada:


```
"HTTP.REQ.HEADER("Name").CONTAINS("Callout").NOT"
<!--NeedCopy-->
```

a) Haga clic en **Crear**y, a continuación, en **Cerrar**.

6. Haga clic en **Aplicar cambios**y, a continuación, en **Cerrar**.

Caso de uso: Control de acceso y autenticación

August 20, 2021

En zonas de alta seguridad, es obligatorio autenticar externamente al usuario antes de que los clientes accedan a un recurso. En el dispositivo Citrix ADC, puede utilizar llamadas HTTP para autenticar externamente al usuario evaluando las credenciales proporcionadas. En este ejemplo, se supone que el cliente envía el nombre de usuario y la contraseña a través de encabezados HTTP en la solicitud. Sin embargo, se podría obtener la misma información de la URL o del cuerpo HTTP.

Para implementar esta configuración, debe realizar las siguientes tareas:

1. Habilite la función de respuesta en el dispositivo Citrix ADC.
2. Cree una llamada HTTP en el dispositivo y configúrela con detalles sobre el servidor externo y otros parámetros necesarios.
3. Configure una directiva de Responder para analizar la respuesta y, a continuación, enlazar la directiva globalmente.
4. Cree un agente de llamada en el servidor remoto.

Habilitar Respondedor

La función de respuesta debe estar habilitada antes de usarla en el dispositivo Citrix ADC.

Para habilitar Respondedor mediante la utilidad de configuración

1. Asegúrese de que la licencia de respondedor está instalada.
2. En la utilidad de configuración, expanda AppExpert, haga clic con el botón derecho en Responder y, a continuación, haga clic en **Habilitar función**

Crear una llamada HTTP en el dispositivo Citrix ADC

Cree una llamada HTTP, HTTP-Callout-3, con la configuración de parámetros que se muestra en la tabla siguiente. Para obtener más información sobre cómo crear una llamada HTTP, consulte Configuración de una llamada HTTP.

Cuadro 1 Parámetros y valores para HTTP-Callout-3

Parámetro	Valor	Nombre
Nombre	Policy-Responder-3	

Parámetro

Valor

Nombre

HTTP-Callout-3

Servidor para recibir la solicitud de llamada:

Dirección IP

10.103.9.95

Port

80

Solicitud de envío al servidor:

Método

GET

Expresión de host

10.102.3.95

Expresión del tallo de URL

“/cgi-bin/authenticate.pl”

Encabezados:

Nombre

Solicitar

Value-expression

Solicitud de llamada

Parámetros:

Nombre

Nombre de usuario

Value-expression

HTTP.REQ.HEADER (“Nombre de usuario”).VALUE (0)

Nombre

Password

Value-expression

HTTP.REQ.HEADER (“Contraseña”).VALUE (0)

Respuesta del servidor:

Tipo de devolución

TEXTO

Expresión para extraer datos de la respuesta

HTTP.RES.BODY (100)

Creación de una directiva de Responder para analizar la respuesta

Cree una directiva de respondedor, Policy-Responder-3, que comprobará la respuesta del servidor de llamadas y RESTAURE la conexión si la dirección IP de origen se ha incluido en la lista de prohibidos. Cree la directiva con la configuración de parámetros que se muestra en la tabla siguiente. Aunque puede crear una directiva de respondedor en el subnodo
Directivas y, a continuación, vincularla globalmente mediante el Administrador de directivas de Respondedor, esta demostración utiliza el Administrador de directivas de
Respondedor para crear la directiva de respondedor y enlazar la directiva globalmente.

Tabla 2. Parámetros y valores para Policy-Responder-3

Parámetro	Valor
Nombre	Policy-Responder-3
Action	RESTABLECER
Undefined-Result-Action	-Global undefined-result action-
Expresión	“HTTP.REQ.HEADER(\“Solicitud\”).EQ(\“Solicitud de llamada\”).NOT && SYS.HTTP_CALLOUT(HTTP-Callout-3).CONTAINS(\“Error de autenticación\”)”

Para crear una directiva de respuesta y vincularla globalmente mediante la utilidad de configuración

1. Vaya a **AppExpert** > **Respondedor**.
2. En el panel de detalles, en **Administrador de directivas**, haga clic en **Administrador de directivas de Responder**.
3. En el cuadro de diálogo **Administrador de directivas de respondedor**, haga clic en **Sustituir global**.
4. Haga clic en **Insertar directiva** y, a continuación, en la columna **Nombre de directiva**, haga clic en **Nueva directiva**.
5. En el cuadro de diálogo **Crear directiva de respondedor**, haga lo siguiente:
   a) En Nombre, escriba Policy-Responder-3.
   b) En Acción, selecciona **RESTABLECER**.
   c) En Acción de resultado no definido, seleccione Acción global de resultado no definido.
   d) En el cuadro de texto Expresión, escriba:

```
1 ”HTTP.REQ.HEADER(”Request”).EQ(”Callout Request”).NOT && SYS.
     HTTP_CALLOUT(HTTP-Callout-3).CONTAINS(”Authentication Failed”)”
2 <!--NeedCopy-->
```

   a) Haga clic en **Crear** y, a continuación, en **Cerrar**.
6. Haga clic en **Aplicar cambios** y, a continuación, en **Cerrar**.

Crear un agente de llamada HTTP en el servidor remoto

Ahora necesita crear un agente de llamada HTTP en el servidor de llamadas remoto. El agente de llamada HTTP recibe solicitudes de llamada del dispositivo Citrix ADC y responde adecuadamente. El agente de llamada es un script diferente para cada implementación y debe escribirse teniendo en cuenta las especificaciones del servidor, como el tipo de base de datos y el lenguaje de scripting admitido.

Lo que sigue es ejemplo de pseudo-código agente de llamada que verifica si el nombre de usuario y la contraseña proporcionados son válidos. El agente se puede implementar en cualquier lenguaje de programación de su elección. El pseudo-código debe usarse solo como guía para desarrollar el agente de llamada. Puede crear funciones adicionales en el programa.

Para verificar el nombre de usuario y la contraseña proporcionados mediante pseudo-código

1. Acepte el nombre de usuario y la contraseña proporcionados en la solicitud y formatéelos adecuadamente.
2. Conéctese a la base de datos que contiene todos los nombres de usuario y contraseñas válidos.
3. Compruebe las credenciales proporcionadas en la base de datos.
4. Dar formato a la respuesta según lo requiera la llamada HTTP.
5. Envíe la respuesta al dispositivo Citrix ADC.

Caso de uso: Filtrado de spam basado en OWA

August 20, 2021

El filtrado de spam es la capacidad de bloquear dinámicamente correos electrónicos que no provienen de una fuente conocida o de confianza o que tienen contenido inapropiado. El filtrado de spam requiere una lógica empresarial asociada que indique que un tipo concreto de mensaje es spam. Cuando el dispositivo Citrix ADC procesa mensajes de Outlook Web Access (OWA) basados en el protocolo HTTP, las llamadas HTTP se pueden utilizar para filtrar el correo no deseado.

Puede utilizar llamadas HTTP para extraer cualquier parte del mensaje entrante y comprobar con un servidor de llamadas externo configurado con reglas destinadas a determinar si un mensaje es legítimo o spam. En caso de correo electrónico no deseado, por razones de seguridad, el dispositivo Citrix ADC no notifica al remitente que el correo electrónico está marcado como spam.

El siguiente ejemplo lleva a cabo una comprobación muy básica de varias palabras clave enumeradas en el asunto del correo electrónico. Estas comprobaciones pueden ser más complejas en un entorno de producción.

Para implementar esta configuración, debe realizar las siguientes tareas:

1. Habilite la función de respuesta en el dispositivo Citrix ADC.
2. Cree una llamada HTTP en el dispositivo Citrix ADC y configúrela con detalles sobre el servidor externo y otros parámetros necesarios.
3. Cree una directiva de respuesta para analizar la respuesta y, a continuación, enlazar la directiva globalmente.
4. Cree un agente de llamada en el servidor remoto.

Habilitar Respondedor

La función de respuesta debe estar habilitada para poder utilizarla en el dispositivo Citrix ADC.

Para habilitar Respondedor mediante la interfaz gráfica de usuario

1. Asegúrese de que la licencia de respondedor está instalada.
2. En la utilidad de configuración, expanda AppExpert, haga clic con el botón secundario del mouse en **Respondedor** y, a continuación, haga clic en **Habilitar la función Respondedor**.

Crear una llamada HTTP en el dispositivo Citrix ADC

Cree una llamada HTTP, HTTP-Callout-4, con la configuración de parámetros que se muestra en la tabla siguiente. Para obtener más información sobre cómo crear una llamada HTTP, consulte Configuración de una llamada HTTP.

Para obtener más información, consulte Parámetros y valores para HTTP-Callout-4 pdf.

Crear una acción de respuesta

Crea una acción de respuesta, Action-Responder-4. Cree la acción con los parámetros que se muestran en la tabla siguiente.

Parámetro	Valor
Nombre	Action-Responder-4
Tipo	Responda con
Dispositivo de destino	””HTTP/1.1 200 OK\r\nServer: Microsoft-IIS/6.0\r\nX-Powered-By: ASP.NET\r\nContent-Length: 0\r\nMS-WebStorage: 6.5.6944\r\nCache-Control: No-cache\r\n\r\n””

Tabla 2. Parámetros y valores para Action-Responder-4

Para crear una acción de respuesta mediante la utilidad de configuración

1. Vaya a **AppExpert** > **Responder** > **Acciones**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En el cuadro de diálogo **Crear acción de respuesta**, en Nombre, escriba **Action-Responder-4**.
4. En Tipo, haga clic en **Responder con**.
5. En Destino, escriba:


```
1 ""HTTP/1.1 200 OK\r\nServer: Microsoft-IIS/6.0\r\nX-Powered-By:
     ASP.NET\r\nContent-Length: 0\r\nMS-WebStorage: 6.5.6944\r\
     nCache-Control: no-cache\r\n\r\n""
2 <!--NeedCopy-->
```

6. Haga clic en **Crear** y, a continuación, en **Cerrar**.

Creación de una directiva de Responder para invocar la llamada HTTP

Cree una directiva de respuesta, Policy-Responder-4, que comprobará el cuerpo de la solicitud y, si el cuerpo contiene la palabra "
asunto", invoque la llamada HTTP para verificar el correo electrónico. Cree la directiva con la configuración de parámetros que se muestra en la tabla siguiente. Aunque puede crear una directiva de Responder en el subnodo
Directivas y, a continuación, vincularla globalmente mediante el Administrador de directivas de Responder, esta demostración utiliza el Administrador de directivas de
Responder para crear la directiva de Responder y vincularla globalmente.

Parámetro	Valor
Nombre	Policy-Responder-4
Action	Action-Responder-4
Undefined-Result-Action	-Global undefined-result action-
Expresión	"HTTP.REQ.BODY (1000).CONTAINS ("urn:schemas:httpmail:subject") && SYS.HTTP_CALLOUT (HTTP-Callout-4)"

Para crear una directiva de respuesta mediante la utilidad de configuración

1. Vaya a **AppExpert** > **Respondedor**.
2. En el panel de detalles, en **Administrador de directivas**, haga clic en **Administrador de directivas de respondedor**.
3. En el cuadro de diálogo **Administrador de directivas de respondedor**, haga clic en **Sustituir global**.
4. Haga clic en **Insertar directiva** y, a continuación, en la columna **Nombre de directiva**, haga clic en **Nueva directiva**.
5. En el cuadro de diálogo **Crear directiva de respondedor**, haga lo siguiente:

a) En Nombre, escriba **Policy-Responder-4**.
b) En Acción, haga clic en **Action-Responder-4**.
c) En Acción de resultado no definido, haga clic en Acción **global de resultado no definido**.
d) En el cuadro de texto **Expresión**, escriba:

```
"HTTP.REQ.BODY(1000).CONTAINS("urn:schemas:httpmail:subject")
   && SYS.HTTP_CALLOUT(HTTP-Callout-4)"
<!--NeedCopy-->
```

e) Haga clic en **Crear** y, a continuación, en **Cerrar**.

6. Haga clic en **Aplicar cambios** y, a continuación, en **Cerrar**.

Crear un agente de llamada HTTP en el servidor remoto

Ahora tendrá que crear un agente de llamada HTTP en el servidor de llamada remoto. El agente de llamada HTTP recibe solicitudes de llamada del dispositivo Citrix ADC y responde en consecuencia. El agente de llamada es un script diferente para cada implementación y debe escribirse teniendo en cuenta las especificaciones del servidor, como el tipo de base de datos y el lenguaje de scripting admitido.

El siguiente pseudocódigo proporciona instrucciones para crear un agente de llamada que comprueba una lista de palabras que generalmente se entiende que indican correos spam. El agente se puede implementar en cualquier lenguaje de programación de su elección. El pseudo-código debe usarse solo como guía para desarrollar el agente de llamada. Puede crear funciones adicionales en el programa.

Para identificar el correo no deseado mediante pseudo-código

1. Acepte el asunto del correo electrónico proporcionado por el dispositivo Citrix ADC.
2. Conéctese a la base de datos que contiene todos los términos con los que se comprueba el asunto del correo electrónico.
3. Compruebe las palabras del asunto del correo electrónico con la lista de palabras de spam.
4. Dar formato a la respuesta según lo requiera la llamada HTTP.
5. Envíe la respuesta al dispositivo Citrix ADC.

Caso de uso: Dynamic content switching

January 12, 2021

Este caso de uso proporciona conmutación dinámica de contenido mediante una llamada HTTP para obtener el nombre del servidor virtual de equilibrio de carga al que se reenvía la solicitud.

1. Agregue un servidor virtual de conmutación de contenido.

```
add cs vserver cs_vserver1 HTTP 10.102.29.196 80
<!--NeedCopy-->
```

2. Cree una llamada HTTP.

```
add policy httpCallout http_callout1
<!--NeedCopy-->
```

3. Configure la llamada HTTP para que responda con el nombre del servidor virtual de equilibrio de carga desde una solicitud que contiene la dirección IP del cliente en el encabezado HTTP “X-CLIENT-IP”.

```
> set policy httpCallout http_callout1 -IPAddress 10.217.14.23 -
    port 80 -returnType TEXT -hostExpr ””www.get-lbvip.com”” -
    urlStemExpr ””/index.html”” -headers X-CLIENT-IP(CLIENT.IP.SRC)
     -resultExpr ”HTTP.RES.BODY(1000).AFTER_STR(”<lbvip>”).
    BEFORE_STR(”<lbvip”)”
<!--NeedCopy-->
```

4. Configure la acción de cambio de contenido para recuperar la respuesta de llamada.

```
add cs action cs_action1 -targetVserverExpr 'SYS.HTTP_CALLOUT(
    http_callout1)'
<!--NeedCopy-->
```

> Nota:
>
> Debe vincular un servidor virtual de equilibrio de carga al servidor virtual de conmutación de contenido para tener en cuenta:

- La no disponibilidad del servidor virtual de equilibrio de carga en el que se resuelve la llamada.
- Condición UNDEF que resulta de la ejecución de la llamada.


```
> bind cs vserver cs_vserver1 -lbvserver default_lbvip
<!--NeedCopy-->
```

5. Configure la directiva de conmutación de contenido.

```
add cs policy cs_policy1 -rule true -action cs_action1
<!--NeedCopy-->
```

6. Vinculación de la directiva de conmutación de contenido al servidor virtual de conmutación de contenido.

```
bind cs vserver cs_vserver1 -policyName cs_policy1 -priority 10
<!--NeedCopy-->
```

Conjuntos de patrones y conjuntos de datos

January 21, 2022

Las expresiones de directiva para operaciones de coincidencia de cadenas en un amplio conjunto de patrones de cadenas tienden a ser largas y complejas. Los recursos consumidos por la evaluación de expresiones tan complejas son significativos en términos de ciclos de procesamiento, memoria y tamaño de configuración. Puede crear expresiones más sencillas y que consumen menos recursos mediante la coincidencia de patrones.

Según el tipo de patrones que quiera hacer coincidir, puede utilizar una de las siguientes funciones para implementar la coincidencia de patrones:

- Un conjunto de patrones es una matriz de patrones indexados que se utilizan para la comparación de cadenas durante la evaluación de la directiva de sintaxis predeterminada. Ejemplo de conjunto de patrones: tipos de imagen {svg, bmp, PNG, GIF, tiff, jpg}.
- Un conjunto de datos es una forma especializada de conjunto de patrones. Es una matriz de patrones de tipos número (entero), dirección IPv4 o dirección IPv6.

La diferencia entre `patset` y `dataset` es que en `dataset` comparamos la condición límite. Por ejemplo, si la cadena de entrada es 1.1.1.11 y supone que el patrón 1.1.1.1 está enlazado a `patset` y a `dataset` de tipo IPv4, se configura un conjunto de datos `patset` y para comprobar si la dirección IP está presente en la solicitud. Después de la evaluación, `patset` devuelve que 1.1.1.1 está presente en la entrada, pero la evaluación `dataset` es falsa. Esto se debe a una verificación de límites en la que la

dirección IP no forma parte de ninguna otra dirección IP. Esto significa que, después del patrón enlazado, no debe haber ningún número entero.

A menudo, puede utilizar conjuntos de patrones o conjuntos de datos. Sin embargo, en los casos en que quiera coincidencias específicas para datos numéricos o direcciones IPv4 e IPv6, debe utilizar conjuntos de datos.

> **Nota:**
>
> Los conjuntos de patrones y los conjuntos de datos solo se pueden usar en directivas de sintaxis predeterminadas.

Para utilizar conjuntos de patrones o conjuntos de datos, cree primero el conjunto de patrones o el conjunto de datos y enlaza los patrones a él. A continuación, cuando configure una directiva para comparar una cadena en un paquete, utilice un operador apropiado y pase el nombre del conjunto de patrones o del conjunto de datos como argumento.

Cómo funciona la coincidencia de cadenas con conjuntos de patrones y conjuntos de datos

August 20, 2021

Un conjunto de patrones o un conjunto de datos contiene un conjunto de patrones, y a cada patrón se le asigna un índice único. Cuando se aplica una directiva a un paquete, una expresión identifica una cadena que se va a evaluar y el operador compara la cadena con los patrones definidos en el conjunto de patrones o conjunto de datos hasta que se encuentre una coincidencia o se hayan comparado todos los patrones. Luego, en función de su función, el operador devuelve un valor booleano que indica si se encontró o no un patrón coincidente o el índice del patrón que coincide con la cadena.

Nota: En este tema se explica el funcionamiento de un conjunto de patrones. Los conjuntos de datos funcionan de la misma manera. La única diferencia entre los conjuntos de patrones y los conjuntos de datos es el tipo de patrones definidos en el conjunto.

Considere el siguiente caso de uso para entender cómo los patrones se pueden usar para la coincidencia de cadenas.

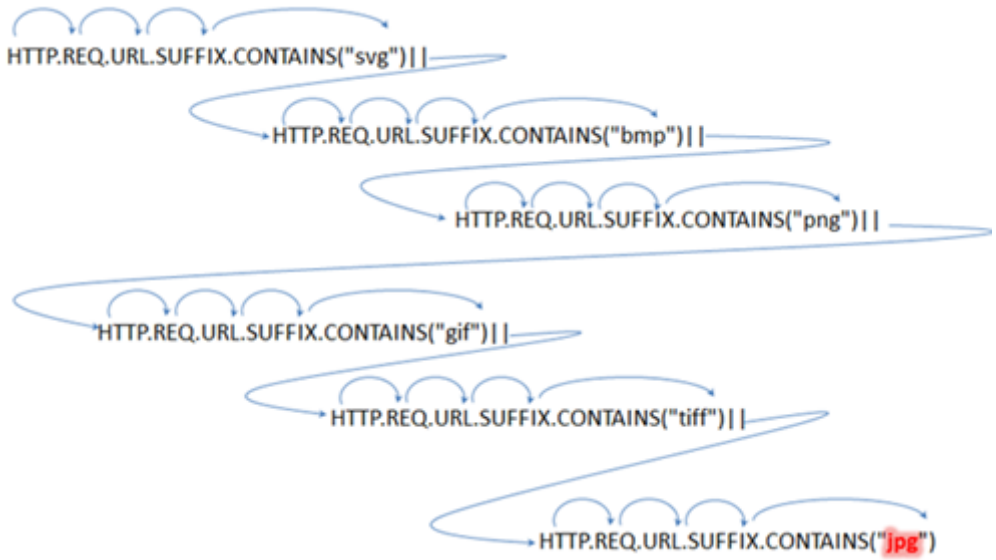
Quiere determinar si el sufijo URL (texto de destino) contiene alguna de las extensiones de archivo de imagen. Sin usar conjuntos de patrones, tendría que definir una expresión compleja, de la siguiente manera:

```
1 HTTP.REQ.URL.SUFFIX.CONTAINS("svg") ¦¦ HTTP.REQ.URL.SUFFIX.CONTAINS("
    bmp") ¦¦ HTTP.REQ.URL.SUFFIX.CONTAINS("png") ¦¦
```

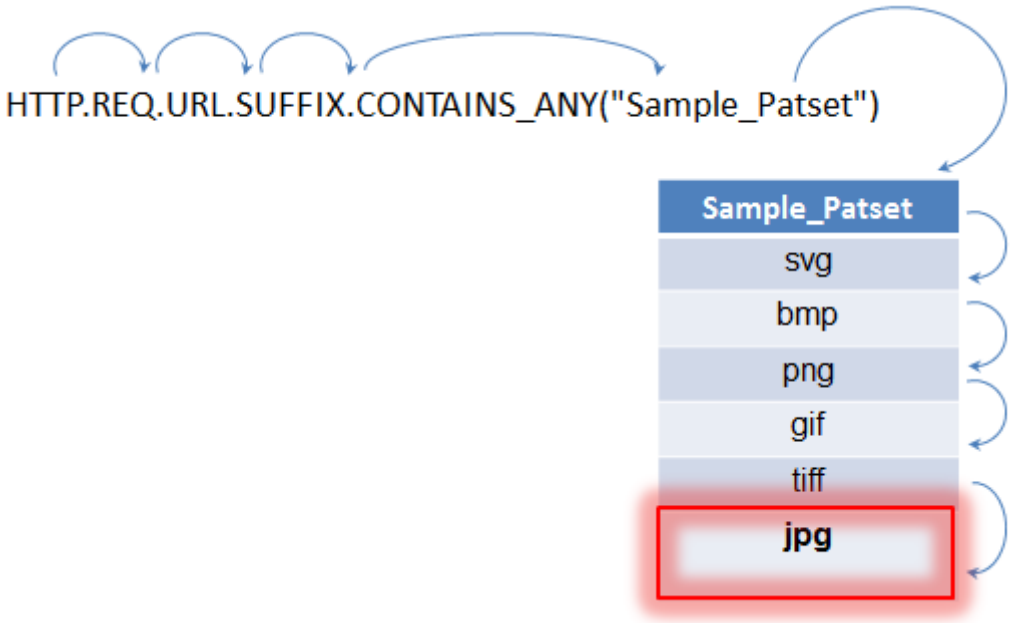


```
2 HTTP.REQ.URL.SUFFIX.CONTAINS(”gif”) ¦¦ HTTP.REQ.URL.SUFFIX.CONTAINS(”
    tiff”) ¦¦ HTTP.REQ.URL.SUFFIX.CONTAINS(”jpg”)
3 <!--NeedCopy-->
```

Si la URL tiene un sufijo de “jpg” con la expresión compuesta anterior, el dispositivo Citrix ADC debe iterar secuencialmente toda la expresión compuesta, de una subexpresión a la siguiente, para determinar que la solicitud se refiere a una imagen jpg. La siguiente ilustración muestra los pasos del proceso.



Cuando una expresión compuesta incluye cientos de subexpresiones, el proceso anterior requiere un uso intensivo de recursos. Una mejor alternativa es una expresión que invoca un conjunto de patrones, como se muestra en la siguiente ilustración.



Durante la evaluación de directivas como se muestra anteriormente, el operador (CONTAINS_ANY) compara la cadena identificada en la solicitud con los patrones definidos en el conjunto de patrones hasta que se encuentre una coincidencia. Con la expresión Sample_Patset, las múltiples iteraciones a través de seis subexpresiones se reducen a una sola.

Al eliminar la necesidad de configurar expresiones compuestas que realizan la coincidencia de cadenas con varias operaciones OR, los conjuntos de patrones o conjuntos de datos simplifican la configuración y aceleran el procesamiento de solicitudes y respuestas.

Configuración de un conjunto de patrones

August 20, 2021

Para configurar un conjunto de patrones, debe especificar las cadenas que van a servir como patrones. Puede asignar manualmente un valor de índice único a cada uno de estos patrones, o puede permitir que los valores de índice se asignen automáticamente.

Nota: Los conjuntos de patrones distinguen entre mayúsculas y minúsculas (a menos que especifique la expresión para ignorar mayúsculas y minúsculas). Por lo tanto, el patrón de cadena “producto1”, por ejemplo, no es el mismo que el patrón de cadena “Producto1.”

Puntos para recordar acerca de los valores de índice:

- No se puede enlazar el mismo valor de índice a más de un patrón.
- Un valor de índice asignado automáticamente es un número mayor que el valor de índice más alto de los patrones existentes dentro del conjunto de patrones. Por ejemplo, si el valor de

índice más alto de los patrones existentes en un conjunto de patrones es 104, el siguiente valor de índice asignado automáticamente es 105.
- Si no especifica un índice para el primer patrón, el valor de índice 1 se asigna automáticamente a ese patrón.
- Los valores de índice no se regeneran automáticamente si se eliminan o modifican uno o varios patrones. Por ejemplo, si el conjunto contiene cinco patrones, con índices de 1 a 5, y si se elimina el patrón con un índice de 3, los demás valores de índice del conjunto de patrones no se regeneran automáticamente para producir valores de 1 a 4.
- El valor máximo de índice que se puede asignar a un patrón es 4294967290. Si ese valor ya está asignado a un patrón del conjunto, debe asignar manualmente valores de índice a los patrones recién agregados. Un valor de índice no utilizado que sea inferior a un valor utilizado actualmente no se puede asignar automáticamente.

Para configurar un conjunto de patrones mediante la interfaz de línea de comandos

En el símbolo del sistema, haga lo siguiente:

1. Cree un conjunto de patrones.

```
add policy patset <name>
```

Ejemplo:

```
add policy patset samplepatset
```

1. Enlazar patrones al conjunto de patrones.

```
bind policy patset <name> <string> [-index <positive_integer>][-charset
 ( ASCII | UTF_8 )] [-comment <string>]
```

Ejemplo:

```
bind policy patset samplepatset product1 -index 1 -comment short description
 about the pattern bound to the pattern set
```

Nota: Repita este paso para todos los patrones que quiera enlazar al conjunto de patrones.

1. Verifique la configuración.

```
show policy patset <name>
```

Para configurar un conjunto de patrones mediante la utilidad de configuración

1. Vaya a **AppExpert** > **Conjuntos de patrones**.
2. En el panel de detalles, haga clic en **Agregar** para abrir el cuadro de diálogo **Crear conjunto de patrones**.
3. Especifique un nombre para el conjunto de patrones en el cuadro de texto Nombre.

4. En Especificar patrón, escriba el primer patrón y, opcionalmente, especifique valores para los siguientes parámetros:
   - Tratar barra diagonal inversa como carácter de escape: Active esta casilla de verificación para especificar que los caracteres de barra diagonal inversa que pueda incluir en el patrón se tratarán como caracteres de escape.
   - Índice: Valor de índice asignado por el usuario, desde 1 hasta 4294967290.
5. Compruebe que ha introducido los caracteres correctos y, a continuación, haga clic en **Agregar**.
6. Repita los pasos 4 y 5 para agregar más patrones y, a continuación, haga clic en **Crear**.

Configurar conjuntos de patrones basados en archivos

El dispositivo Citrix ADC admite conjuntos de patrones basados en archivos.

Para configurar conjuntos de patrones basados en archivos mediante CLI

En el símbolo del sistema, escriba los siguientes comandos:

- Importe un nuevo archivo de conjunto de patrones en el dispositivo Citrix ADC.

```
import policy patsetfile <src> <name> -delimiter <char> -charset
   <ASCII | UTF_8>
<!--NeedCopy-->
```

Ejemplo:

```
import policy patsetfile local:test.csv clientids_list -
   delimiter ,
<!--NeedCopy-->
```

Puede importar un archivo desde un dispositivo local, un servidor HTTP o un servidor FTP. Para agregar el archivo desde su dispositivo local, el archivo debe estar disponible en la `/var/tmp` ubicación.

- Actualice un archivo de conjunto de patrones existente en el dispositivo Citrix ADC.

```
update policy -patsetfile <patset filename>
<!--NeedCopy-->
```

Ejemplo:


```
update policy -patsetfile clientids_list
<!--NeedCopy-->
```

- Agregue un archivo de conjunto de patrones al motor de paquetes.

```
add policy -patsetfile <patset filename>
<!--NeedCopy-->
```

Ejemplo:

```
add policy -patsetfile clientids_list
<!--NeedCopy-->
```

- Enlazar patrones al conjunto de patrones.

```
add policy patset <patset name> -patsetfile <patset filename>
<!--NeedCopy-->
```

Ejemplo:

```
add policy patset clientid_patset -patsetfile clientids_list
<!--NeedCopy-->
```

- Verifique la configuración.

```
show policy patsetfile clientids_list

Name: clientids_list
Patset Name: clientid_patset
Number of Imported Patterns: 8
Number of Bound Patterns: 8
(All the patterns bound successfully)

Done
<!--NeedCopy-->
```


Para configurar conjuntos de patrones basados en archivos mediante GUI

1. Vaya a **AppExpert-> Archivos de conjuntos de patrones**.
2. En el panel **Importado**, haga clic en **Importar**.
3. En la página **Configurar archivo de patset de directivas**, seleccione el archivo que quiere importar y haga clic en **Aceptar**.
4. Seleccione el archivo importado y haga clic en **Agregar**.
5. En la página **Crear Archivo de Patset de Directivas**, introduzca los detalles y haga clic en **Crear** para agregar un conjunto de patrones de directivas.

Configuración de un conjunto de datos

March 9, 2022

Para configurar un conjunto de datos, debe especificar las cadenas que sirven como patrón, asignar un tipo (número, dirección IPv4 o dirección IPv6) y configurar el rango del conjunto de datos. Puede asignar manualmente un valor de índice único al patrón o puede permitir que los valores de índice se asignen automáticamente. El conjunto de datos no está relacionado con HTTP ni con ningún protocolo de 7 capas. Solo funciona en texto o cadena. Hay diferentes tipos de conjuntos de datos, como NUM, ULONG, IPv4, IPv6, MAC, DOUBLE. Puede seleccionar un tipo y definir el rango del conjunto de datos en función del tipo especificado.

> **Nota:**
>
> Los conjuntos de datos de directivas distinguen entre mayúsculas y minúsculas (a menos que especifique la expresión para ignorar las mayúsculas Por lo tanto, la dirección MAC ff:ff:ff:ff:ff:ff, por ejemplo, no es la misma que la dirección MAC FF:FF:FF:FF:FF:FF.

Las reglas aplicadas para los valores de índice de los conjuntos de datos son similares a los conjuntos de patrones. Para obtener información sobre los valores de índice, consulte Configuración de un conjunto de patrones.

Configurar un conjunto de datos

Complete los siguientes pasos para configurar un conjunto de datos:

1. Agregar un conjunto de datos de directivas
2. Enlazar patrón a un conjunto de datos
3. Agregar una expresión de directiva
4. Comprobar la configuración de la directiva

Agregar un conjunto de datos de directivas

En el símbolo del sistema, haga lo siguiente:

```
add policy dataset <name> <type>
```

Ejemplo:

```
add policy dataset ds1 ipv4 -comment numbers
```

Enlazar un patrón al conjunto de datos

En el símbolo del sistema, escriba:

```
bind policy dataset <name> <value> [-index <positive_integer>] [-endRange <
string>] [-comment <string>]
```

Ejemplo:

```
bind policy dataset ds1 1.1.1.1 -endRange 1.1.1.10 -comment short description
 about the pattern bound to the data set
```

> **Nota:**
>
> Debe repetir este paso para todos los patrones que quiere vincular al conjunto de datos. Solo puede enlazar hasta 5000 patrones a un conjunto de datos.
>
> Además, un rango de conjunto de datos no debe superponerse con otros rangos enlazados a un conjunto de datos y no puede incluir valores únicos enlazados al conjunto de datos. Si vincula un conjunto de datos con un rango superpuesto, se produce un error.

Ejemplo:

```
1 add policy dataset ip_set ipv4
2  Done
3 bind policy dataset ip_set 2.2.2.25
4  Done
5 bind policy dataset ip_set 2.2.2.20 -endRange 2.2.2.30
6 ERROR: The range overlaps an existing range or includes a value bound
     to the dataset.
7 <!--NeedCopy-->
```

Se considera que un valor está en el conjunto de datos si es igual a un solo valor enlazado al conjunto de datos o se encuentra entre el valor inferior y el valor superior (valor inferior <= valor && valor <- valor superior), para un rango enlazado al conjunto de datos.

Usar la expresión de directiva en un conjunto de datos de directivas

En el símbolo del sistema, escriba:

```
add policy expression exp1 http.req.body(100).contains_any(”ds1”)
```

Donde:
La expresión comprueba si hay algún patrón (o patrón dentro del rango) enlazado al conjunto de datos ds1 está presente en los primeros 100 bytes del cuerpo de la solicitud HTTP.

Verificar la configuración del conjunto

En el símbolo del sistema, escriba:

```
show policy dataset ds1
> show policy dataset ds1
```

Ejemplo:

```
        Dataset:        ds1
         Type:   IPV4
1)       Bound Dataset Range from: 1.1.1.1       through: 1.1.1.10
          Index:  1
<!--NeedCopy-->
```

Configurar un conjunto de datos mediante la utilidad de configuración

Siga los pasos que se indican a continuación para configurar un conjunto de datos de directivas:

1. Vaya a **AppExpert > Conjuntos de datos**.
2. En el panel de detalles, en Conjuntos de datos, haga clic en **Agregar**.
3. En la página **Configurar conjunto de datos**, defina los siguientes parámetros.
   a) Nombre. Nombre del conjunto de datos de directivas.
   b) Tipo. Tipo de valor que se va a vincular al conjunto de datos.

   Configuración del conjunto de datos
4. Haga clic en **Insertar** para vincular el valor del conjunto de datos del tipo específico.
   a) Valor. Valor del tipo especificado asociado al conjunto de datos.
   b) Índice. El valor de índice del conjunto de datos.
   c) Gama final. La entrada del conjunto de datos. Este es un intervalo de <value> a <end_range>.

d) Observaciones. Breve descripción del conjunto de datos.

enlace conjunto de datos

5. Haga clic en **Insertar** y **cerrar**.
6. Ingrese los comentarios.
7. Haga clic en **Crear** y **cerrar**.

Notación de subred de CIDR en direcciones IPv4 e IPv6 para el conjunto de datos de directivas

Los conjuntos de datos de directivas para direcciones IPv4 e IPv6 permiten que el valor enlazado sea subredes mediante la notación CIDR. La notación CIDR especifica la dirección y el rango de la subred. Notación CIDR <address>/<n>, donde <address> es la primera dirección de la subred y <n> es un número entero que especifica el número de bits situados más a la izquierda en la máscara de subred, que define el intervalo de la subred.

Por ejemplo, 192.128.0.0/10 representa una subred IPv4 que comienza en la dirección 192.129.0.0 con una máscara 0xFFC0000 (255.192.0.0).

Ejemplo:

```
add policy dataset ds1 ipv4
bind policy dataset ds1 192.128.0.0/10
show policy dataset ds1
    Dataset: ds1
    Type: IPV4
Bound Dataset Value: 192.128.0.0/10 Index: 1 Comment: Subnet range from
    192.128.0.0 through 192.191.255.255

<!--NeedCopy-->
```

Ejemplo de subred IPv6:

Un ejemplo de subred IPv6 sería 2001:db8:123::/56, que comienza en la dirección 2001:db8:123:: con una máscara FFFF:FFFF:FFFF:FF00::

```
add policy dataset ds2 ipv6
bind policy dataset ds2 2001:db8:123::/56
show policy dataset ds2
    Dataset: ds2
    Type: IPV61
```



```
6 Bound Dataset Value: 2001:db8:123::/56 Index: 1 Comment: Subnet range
     from 2001:db8:123:: through 2001:db8:123:ff:ffff:ffff:ffff:ffff
7
8 <!--NeedCopy-->
```

La dirección inicial de la subred vendrá determinada por la dirección especificada enmascarada por la máscara de subred. Se emite una advertencia si la dirección especificada no coincide con la dirección inicial resultante.

Por ejemplo:

```
1 bind policy dataset ds1 192.168.0.0/10
2 Warning: Starting subnet address masked using subnet mask to create new
      starting address [192.128.0.0]
3 show policy dataset ds1
4     Dataset: ds1
5     Type: IPV4
6 Bound Dataset Value:192.168.0.0/10 Index: 1 Comment: Subnet range from
     192.128.0.0 through 192.191.255.255
7
8 <!--NeedCopy-->
```

Uso de conjuntos de patrones y conjuntos de datos

October 5, 2021

Las expresiones de directiva avanzadas que toman conjuntos de patrones o conjuntos de datos como argumento se pueden utilizar para realizar operaciones de coincidencia de cadenas.

El uso es el siguiente:

```
1 <text>.<operator>(”<name>”)
2 <!--NeedCopy-->
```

donde:

- <text> es la expresión que identifica una cadena de un paquete. Ejemplo: HTTP.REQ.HEADER (“Host”).
- <operator> es uno de los operadores descritos en la tabla Tipos de conjuntos de patrones pdf.

Para ver el uso de muestra, consulte Uso de muestra.

Ejemplo de uso

August 20, 2021

Para comprender el uso de conjuntos de patrones en expresiones, considere el ejemplo de un conjunto de patrones denominado “tipos de imagen”.

Patrones	Valor del índice
SVG	1
BMP	2
png	3
gif	4
tiff	5
jpg	6

Cuadro 1 Conjunto de patrones “tipos de imagen”

Ejemplo 1: Determine si el sufijo de una solicitud HTTP es una de las extensiones de archivo definidas en el conjunto de patrones “tipos de imagen”.

- **expresión.** HTTP.REQ.URL.SUFFIX.EQUALS_ANY (“tipos de imagen”)
- **URL de ejemplo.** `http://www.example.com/homepageicon.jpg`
- **Resultado.** TRUE

Ejemplo 2: Determine si el sufijo de una solicitud HTTP es una de las extensiones de archivo definidas en el conjunto de patrones “imagetypes” y devuelva el índice de ese patrón.

- **expresión.** HTTP.REQ.URL.SUFFIX.EQUALS_INDEX (“tipos de imagen”)
- **URL de ejemplo.** `http://www.example.com/mylogo.png`
- **Resultado.** 4 (El valor de índice del patrón “gif”).

Ejemplo 3: Utilice el valor de índice de un patrón para determinar si el sufijo de URL se encuentra dentro de un rango de valores de índice especificado.

- **expresión.** HTTP.REQ.URL.SUFFIX.EQUALS_INDEX (“tipos de imagen”).GE (3) && HTTP.REQ.URL.SUFFIX.EQU
  (“tipos de imagen”).LE (5)
- **URL de ejemplo.** `http://www.example.com/mylogo.png`
- **Resultado.** TRUE (El valor de índice de los tipos de archivo gif es 4.)

Ejemplo 4: Implemente un conjunto de directivas para las extensiones de archivo bmp, jpg y png, y un conjunto diferente de directivas para los archivos gif, tiff y svg.

Una expresión que devuelve el índice de un patrón coincidente se puede utilizar para definir subconjuntos de tráfico para una aplicación web. Las dos expresiones siguientes se pueden utilizar en las directivas de conmutación de contenido para un servidor virtual de conmutación de contenido:

- HTTP.REQ.URL.SUFFIX.EQUALS_INDEX ("tipos de imagen").LE (3)
- HTTP.REQ.URL.SUFFIX.EQUALS_INDEX ("tipos de imagen").GE (4)

Variables

August 20, 2021

Las variables son objetos nombrados que almacenan información en forma de tokens. Estos tokens se utilizan dentro y entre diferentes transacciones en Citrix ADC Appliance para computación interna y procesamiento de directivas.

El dispositivo Citrix ADC admite la creación de variables de los siguientes tipos:

- **Variables Singleton.** Puede tener un solo valor de uno de los siguientes tipos: Ulong y text (tamaño máximo). El tipo ulong es un entero de 64 bits sin signo, el tipo de texto es una secuencia de bytes y el tamaño máximo es el número máximo de bytes en la secuencia.
- **Asignar variables.** Los mapas contienen valores asociados con las claves: Cada par clave-valor se denomina entrada de mapa. La clave de cada entrada es única dentro del mapa. Los mapas se especifican de la siguiente manera:

  map (key_type, value_type, max-values).

  donde

  - *key_type* es el tipo de datos de la clave. Es de tipo texto (tamaño máximo).
  - *value_type* es el tipo de datos de los valores del mapa. Puede ser de tipo ulong o texto (tamaño máximo).
  - *max-values* es el número máximo de entradas que puede contener el mapa. Es de tipo ulong.

Los valores de estas variables se establecen mediante asignaciones que deben invocarse en acciones de directiva.

> **Nota**: Las variables aún no se admiten en una configuración de alta disponibilidad o en un clúster.

Ámbito de variables

Una variable de mapa o una variable singleton pueden tener un ámbito global. Alternativamente, el alcance de una variable singleton puede limitarse a una sola transacción.

- **Variable de ámbito global**: Una variable con ámbito global (el valor predeterminado) solo tiene una instancia y esa instancia tiene el mismo valor en todos los núcleos de un dispositivo Citrix ADC y en todos los nodos de una configuración de clúster o HA. Los valores de variables globales existen hasta que se eliminan explícitamente, hasta que caducan o hasta que se reinicie un dispositivo independiente o se reinicien todos los nodos de una configuración de clúster o HA.
- **Variable de ámbito de transacción**: Una variable con ámbito de transacción tiene una instancia independiente, con su propio valor, para cada transacción procesada por el dispositivo Citrix ADC. Cuando se completa el procesamiento de la transacción, se elimina el valor de la variable de transacción.

> **Nota**: Las variables de ámbito de transacción están disponibles en Citrix ADC versión 10.5.e o posterior.

Configuración y Uso de Variables

August 20, 2021

Primero debe crear una variable y, a continuación, asignar un valor o especificar la operación que debe realizarse en la variable. Después de realizar estas operaciones, puede utilizar la asignación como acción de directiva.

Nota: Una vez configurada, la configuración de una variable no se puede modificar ni restablecer. Si es necesario cambiar la variable, se deben eliminar la variable y todas las referencias a la variable (expresiones y asignaciones). La variable se puede volver a agregar con nuevos ajustes, y las referencias (expresiones y asignaciones) se pueden volver a agregar.

Para configurar variables mediante la interfaz de línea de comandos

1. Cree una variable.

```
1 add ns variable <name> -type <string> [-scope global] [-ifFull ( undef
     | lru )] [-ifValueTooBig ( undef | truncate )] [-ifNoValue ( undef |
      init )] [-init <string>] [-expires <positive_integer>] [-comment <
     string>]
2 <!--NeedCopy-->
```


Nota: Consulte la página man “man add ns variable” para la descripción de los parámetros del comando.

Ejemplo 1: Crear una variable ulong llamada “my_counter” e inicializarla en 1.

```
add ns variable my_counter  - type ulong -init 1
<!--NeedCopy-->
```

Ejemplo 2: Cree un mapa denominado “user_privilege_map”. El mapa contendrá claves de longitud máxima 15 caracteres y valores de texto de longitud máxima 10 caracteres, con un máximo de 10000 entradas.

```
add ns variable user_privilege_map -type map(text(15),text(10),10000)
<!--NeedCopy-->
```

Nota: Si el mapa contiene 10000 entradas sin caducar, las asignaciones para claves nuevas reutilizan una de las entradas utilizadas menos recientemente. De forma predeterminada, una expresión que intenta obtener un valor para una clave inexistente inicializará un valor de texto vacío.

Asigne el valor o especifique la operación que se realizará en la variable. Esto se hace mediante la creación de una asignación.

```
add ns assignment <name> -variable <expression> [-set <expression> | -
    add <expression> | -sub <expression> | -append <expression> | -clear
    ] [-comment <string>]
<!--NeedCopy-->
```

Nota: Se hace referencia a una variable mediante el selector de variables ($). Por lo tanto, **$variable1** se utiliza para hacer referencia a variables de texto o ulong. Del mismo modo, **$variable2[clave-expresión]**se utiliza para hacer referencia a variables de mapa.

Ejemplo 1: Defina una asignación denominada “inc_my_counter” que agrega automáticamente 1 a la variable “my_counter”.

```
add ns assignment inc_my_counter -variable $my_counter -add 1
<!--NeedCopy-->
```

Ejemplo 2: Defina una asignación denominada “set_user_privilege” que agregue a la variable “user_privilege_map” una entrada para la dirección IP del cliente con el valor devuelto por la llamada HTTP “get_user_privilege”.


```
add ns assignment set_user_privilege -variable $user_privilege_map[
    client.ip.src.typecast_text_t] -set sys.http.callout(
    get_user_privilege)
<!--NeedCopy-->
```

Nota: Si ya existe una entrada para esa clave, se reemplazará el valor. De lo contrario, se agregará una nueva entrada para la clave y el valor. Según la declaración anterior para user_privilege_map, si el mapa ya tiene 10000 entradas, una de las entradas utilizadas menos recientemente se reutilizará para la nueva clave y valor.

1. Invocar la asignación de variable en una directiva.

   Hay dos funciones que pueden operar en variables de mapa.

   - **$name.valueExists(key-expression).** Devuelve true si hay un valor en el mapa seleccionado por la clave-expresión. De lo contrario, devuelve false. Esta función actualizará la información de caducidad y LRU si existe la entrada de mapa, pero no creará una nueva entrada de mapa si el valor no existe.
   - **$name.valueCount.** Devuelve el número de valores actualmente retenidos por la variable. Este es el número de entradas en un mapa. Para una variable singleton, esto es 0 si la variable no está inicializada o 1 de lo contrario.

   Ejemplo: invoque la asignación denominada “set_user_privilege” con una directiva de compresión.

```
add cmp policy set_user_privilege_pol -rule $user_privilege_map.
    valueExists(client.ip.src.typecast_text_t).not -resAction
    set_user_privilege
<!--NeedCopy-->
```

Use Case para insertar encabezado HTTP en el lado de respuesta

El siguiente ejemplo muestra un ejemplo de una variable singleton.

Agregue una variable singleton de texto de tipo. Esta variable puede contener un máximo de 100 bytes de datos.

```
add ns variable http_req_data -type text(100) -scope transaction
<!--NeedCopy-->
```


Agregue una acción de asignación, que se usará para almacenar los datos de solicitud HTTP en la variable.

```
1 add ns assignment set_http_req_data -variable $http_req_data -set http.
     req.body(100)
2 <!--NeedCopy-->
```

Agregue una acción de reescritura para insertar encabezado HTTP, cuyo valor se obtendrá de la variable.

```
1 add rewrite action act_ins_header insert_http_header user_name
     $http_req_data.after_str("user_name").before_str("password")
2 <!--NeedCopy-->
```

Agregue una directiva de reescritura que evaluará en el tiempo de solicitud y lleve a cabo una acción de asignación para almacenar datos. Cuando llegamos a esta directiva, tomaremos una acción de asignación y almacenaremos los datos en la variable ns (http_req_data)

```
1 add rewrite policy pol_set_variable true set_http_req_data
2
3 bind rewrite global pol_set_variable 10 -type req_dEFAULT
4 <!--NeedCopy-->
```

Agregue una directiva de reescritura que evaluará en el tiempo de respuesta y agregue un encabezado HTTP en la respuesta.

```
1 add rewrite policy pol_ins_header true act_ins_header
2
3 bind rewrite global pol_ins_header 10 -type res_dEFAULT
4 <!--NeedCopy-->
```

Acción de asignación

En un dispositivo Citrix ADC, una acción de asignación vinculada a la directiva se activa cuando la regla de directiva se evalúa como verdadera. La acción actualiza el valor de la variable que se puede utilizar en evaluaciones posteriores de reglas de directiva. De esta forma, la misma variable se puede actualizar y utilizar para las evaluaciones posteriores de directivas en la misma función. Anteriormente,

el dispositivo ejecutaba acciones de asignación solo después de evaluar todas las directivas de la función cuando las directivas de las acciones de asignación asociadas se evaluaban como verdaderas. Por lo tanto, el valor de variable establecido por la acción de asignación no se puede utilizar en las evaluaciones posteriores de reglas de directiva dentro de la entidad.

Esta funcionalidad se puede entender mejor con un caso de uso que controla la lista de acceso de los clientes en un dispositivo Citrix ADC. La decisión de acceso es proporcionada por un servicio web separado, con la solicitud`GET /client-access?<client-IP-address>` que devuelve una respuesta con "BLOCK" o "Permitir" en el cuerpo. La llamada HTTP está configurada para incluir la dirección IP del cliente asociada a una solicitud entrante. Cuando el dispositivo Citrix ADC recibe una solicitud de un cliente, el dispositivo genera la solicitud de llamada y la envía al servidor de llamada, que aloja una base de datos de direcciones IP en la lista de prohibidos y un agente de llamada HTTP que comprueba si la dirección IP del cliente aparece en la base de datos. El agente de llamada HTTP recibe la solicitud de llamada, comprueba si aparece la dirección IP del cliente y envía una respuesta. La respuesta es un código de estado, 200, 302 junto con "BLOCK" o "Permitir" en el cuerpo. En función del código de estado, el dispositivo realiza la evaluación de directivas. Si la evaluación de la directiva es verdadera, la acción de asignación se activa inmediatamente y la acción establece el valor en la variable. El dispositivo utiliza y establece este valor de variable para la posterior evaluación de directivas en el mismo módulo.

Caso práctico para configurar la acción de asignación

Siga los pasos que se indican a continuación para configurar la acción de asignación y utilizar la variable para las directivas siguientes:

1. La decisión de acceso es proporcionada por un servicio web separado, con la solicitud que devuelve una respuesta con BLOCK o Allow en el cuerpo.

   ```
   GET /url-service>/url-allowed?<URL path>
   ```

2. Configure una variable de mapa para contener las decisiones de acceso de las URL.

   ```
   add ns variable url_list_map -type 'map(text(1000),text(10),10000)'
   ```

3. Configure una llamada HTTP para enviar la solicitud de acceso al servicio web.

   ```
   add policy httpCallout url_list_callout -vserver url_vs -returnType
   TEXT -urlStemExpr '"/url-allowed?" + HTTP.REQ.URL.PATH'-resultExpr '
   HTTP.RES.BODY(10)'
   ```

4. Configure una acción de asignación para invocar la llamada para obtener la decisión de acceso y asignarla a la entrada de mapa para la URL.

   ```
   add ns assignment client_access_assn -variable '$client_access_map[
   CLIENT.IP.SRC.TYPECAST_TEXT_T]'-set SYS.HTTP_CALLOUT(client_access_callout
   )
   ```


5. Configure una acción de respuesta para enviar una respuesta 403 si se bloquea una solicitud de URL.

   ```
   add responder action url_list_block_act respondwith '"HTTP/1.1 403
   Forbidden\\r\\n\\r\\n"'
   ```

6. Configure una directiva de respuesta para establecer la entrada de mapa para la dirección URL si aún no está establecida. Con la mejora inmediata de la acción, el valor de entrada de mapa se establece cuando se evalúa esta directiva. Antes de la mejora, la asignación no se hizo hasta que todas las directivas de respuesta habían sido evaluadas decisión es proporcionada por un servicio web separado.

   ```
   add responder policy url_list_assn_pol '!$url_list_map.VALUEEXISTS(HTTP
   .REQ.URL.PATH)'url_list_assn
   ```

7. Configure una directiva de respuesta para bloquear el acceso a una URL si su valor de entrada de mapa es BLOCK. Con la mejora inmediata de la acción, la entrada de mapa establecida por la directiva anterior está disponible para su uso en esta directiva. Antes de la mejora, la entrada del mapa todavía se desconfiguraría en este punto.

   ```
   add responder policy client_access_block_pol '$client_access_map[CLIENT
   .IP.SRC.TYPECAST_TEXT_T] == "BLOCK"'client_access_block_act
   ```

8. Enlazar las directivas de Responder al servidor virtual. **Nota**: No podemos vincular globalmente las directivas porque no queremos ejecutarlas para la llamada HTTP en un servidor virtual independiente.

   ```
   bind lb vserver vs -policyName client_access_assn_pol -priority 10 -
   gotoPriorityExpression NEXT -type REQUEST
   bind lb vserver vs -policyName client_access_block_pol -priority 20 -
   gotoPriorityExpression END -type REQUEST
   ```

Para configurar variables mediante la utilidad de configuración

1. Vaya a **AppExpert > Variables NS**, para crear una variable.
2. Vaya a **AppExpert > Asignaciones NS**, para asignar valores a la variable.
3. Desplácese hasta el área de entidad adecuada en la que quiera configurar la asignación como una acción.

Caso de uso: Privilegios de usuario de almacenamiento en caché

January 12, 2021

En este caso de uso, los privilegios de usuario (“GOLD”, “SILVER”, etc.) deben recuperarse de un servicio web externo.

Para lograr este caso de uso, realice las siguientes operaciones

Cree una llamada HTTP para obtener los privilegios de usuario del servicio web externo.

```
add policy httpcallout <name> [-IPAddress <ip_addr|ipv6_addr>] [-port <port>] [-vServer <string>] [-returnType <returnType>] [-httpMethod ( GET | POST )] [-hostExpr <string>] [-urlStemExpr <string>] [-headers <name(value)> ...] [-parameters <name(value)> ...] [-bodyExpr <string>][-fullReqExpr <string>] [-scheme ( http | https )] [-resultExpr <string>] [-cacheForSecs <secs>] [-comment <string>]

add policy httpcallout get_user_privilege -ipaddress 10.217.193.84 -port 80 -returnType text -httpMethod GET -hostExpr '”/get_user_privilege”' -resultExpr 'http.res.body(5)'
<!--NeedCopy-->
```

Almacene los privilegios en una variable.

```
add ns variable <name> -type <string> [-scope ( global | transaction )][-ifFull ( undef | lru )] [-ifValueTooBig ( undef | truncate )][-ifNoValue ( undef | init )] [-init <string>] [-expires <positive_integer>] [-comment <string>]

add ns variable user_privilege_map -type map(text(15),text(10),10000) -expires 1200

add ns assignment set_user_privilege -variable $user_privilege_map[client.ip.src] -set sys.http_callout(get_user_privilege)
<!--NeedCopy-->
```

Cree una directiva para comprobar si ya hay una entrada en caché para la dirección IP del cliente; de lo contrario, llama a la llamada HTTP para establecer una entrada de mapa para el cliente.

```
add cmp policy <name> -rule <expression> -resAction <string>

add cmp policy set_user_privilege_pol -rule $user_privilege_map.valueExists(client.ip.src).not -resAction set_user_privilege>
```



```
<!--NeedCopy-->
```

Cree una directiva que se comprime si la entrada de privilegios en caché para el cliente es “GOLD”.

```
add cmp policy <name> -rule <expression> -resAction <string>

add cmp policy compress_if_gold_privilege_pol -rule '
    $user_privilege_map[client.ip.src].eq(”GOLD”)' -resAction compress
<!--NeedCopy-->
```

Enlazar las directivas de compresión globalmente.

```
bind cmp global <policyName> [-priority <positive_integer>] [-state (
    ENABLED | DISABLED )] [-gotoPriorityExpression <expression>] [-type
    <type>] [-invoke (<labelType> <labelName>) ]

bind cmp global set_user_privilege_pol -priority 10 NEXT

bind cmp global compress_if_gold_privilege_pol -priority 20 END
<!--NeedCopy-->
```

Caso de uso: Limitar la cantidad de sesiones

June 2, 2022

En este caso de uso, el requisito es limitar el número de sesiones de back-end activas. En la implementación, cada inicio de sesión tiene “login” en la URL y cada cierre de sesión tiene “logout” en la URL. Al iniciar sesión correctamente, el back-end establece una cookie de identificación de sesión con un valor único de diez caracteres.

Para lograr este caso de uso, realice las siguientes operaciones:

1. Cree una variable de asignación que pueda almacenar cada sesión activa. La clave del mapa es el sessionid. El tiempo de caducidad de la variable se establece en 600 segundos (10 minutos).

```
> add ns variable session_map -type map(text(10),ulong,100) -
    expires 600
<!--NeedCopy-->
```


2. Cree las siguientes asignaciones para la variable de asignación:

   - Cree una entrada para el ID de sesión y establezca ese valor en 1 (este valor no se utiliza).

```
1 > add ns assignment add_session -variable '$session_map[http.
     req.cookie.value(”sessionid”)]' -set 1
2 <!--NeedCopy-->
```

   - Desasignar la entrada de un ID de sesión, lo que disminuye implícitamente el recuento de valores de session_map.

```
1 > add ns assignment delete_session -variable '$session_map[
     http.req.cookie.value(”sessionid”)]' -clear
2 <!--NeedCopy-->
```

3. Cree directivas de respuesta para lo siguiente:

   - Para comprobar si existe una entrada de mapa para ese sessionid en la solicitud HTTP. La asignación add_session se ejecuta si la entrada del mapa no existe.

```
1 > add responder policy add_session_pol 'http.req.url.contains
     (”example”) || $session_map.valueExists(http.req.cookie.
     value(”abc”))' add_session
2 <!--NeedCopy-->
```

     Nota: La función
     valueExists() de la directiva
     add_session_pol cuenta como referencia a la entrada de mapa de la sesión, por lo que cada solicitud restablece el tiempo de expiración de su sesión. Si no se reciben solicitudes para una sesión después de 10 minutos, se desasignará la entrada de la sesión.

   - Para comprobar cuándo se cierra la sesión. Se ejecuta la asignación delete_session.

```
1 add responder policy delete_session_pol ”http.req.url.
     contains(”Logout”)” delete_session
2 <!--NeedCopy-->
```


- Para comprobar si hay solicitudes de inicio de sesión y si el número de sesiones activas supera las 100. Si se cumplen estas condiciones, para limitar el número de sesiones, se redirige al usuario a una página que indica que el servidor está ocupado.

```
add responder action redirect_too_busy redirect "/too_busy.
   html"
add responder policy check_login_pol "http.req.url.contains("
   example") && $session_map.valueCount > 100"
   redirect_too_busy
<!--NeedCopy-->
```

4. Vincular las directivas de respuesta de forma global

```
bind responder global add_session_pol 30 next
bind responder global delete_session_pol 10
bind responder global check_login_pol 20
<!--NeedCopy-->
```

Directivas y expresiones

October 5, 2021

Los temas siguientes proporcionan la información conceptual y de referencia que necesita para configurar directivas avanzadas en el dispositivo Citrix® Citrix ADC®.

Para conocer todas las expresiones de directivas avanzadas compatibles con el dispositivo Citrix ADC, consulte Expresiones de directiva.

Introducción a las directivas y expresiones	Describe el propósito de las expresiones, directivas y acciones, y cómo las utilizan las distintas aplicaciones Citrix ADC.
Configuración de directivas avanzadas	Describe la estructura de las directivas avanzadas y cómo configurarlas individualmente y como bancos de directivas.
Configuración de expresiones avanzadas: Introducción	Describe la sintaxis y la semántica de las expresiones y presenta brevemente cómo configurar expresiones y directivas.

Expresiones avanzadas: evaluación de texto	Describe las expresiones que configura cuando quiere operar con texto (por ejemplo, el cuerpo de una solicitud HTTP POST o el contenido de un certificado de usuario).

Expresiones avanzadas: trabajo con fechas, horas y números	Describe las expresiones que configura cuando quiere operar con cualquier tipo de datos numéricos (por ejemplo, la longitud de una URL, la dirección IP de un cliente o la fecha y hora en que se envió una solicitud HTTP).
Expresiones avanzadas: análisis de datos HTTP, TCP y UDP	Describe expresiones para analizar direcciones IP e IPv6, direcciones MAC y datos específicos del tráfico HTTP y TCP.

Expresiones avanzadas: análisis de certificados SSL	Describe cómo configurar expresiones para el tráfico SSL y los certificados de cliente; por ejemplo, cómo recuperar la fecha de caducidad de un certificado o del emisor del certificado.					
Expresiones avanzadas: direcciones IP y MAC, rendimiento, ID de VLAN	Describe expresiones que puede utilizar para trabajar con cualquier otro dato relacionado con el cliente o servidor que no se haya tratado en otros capítulos.	Datos encasillados	Describe expresiones para transformar datos de un tipo a otro.	Expresiones regulares	Describe cómo pasar expresiones regulares como argumentos a operadores en expresiones avanzadas.	Referencia de

expresiones	Referencia para argumentos de expresiones avanzadas.	Resumen Ejemplos de directivas y expresiones avanzadas	Ejemplos de directivas y expresiones avanzadas, tanto en formato de referencia rápida como de aprendizaje, que puede personalizar para su propio uso.
Tutorial Ejemplos de directivas avanzadas para reescritura	Ejemplos de directivas avanzadas para su uso en la función de reescritura.		
Tutorial Examples of Directivas	Ejemplos de directivas para funciones de Citrix ADC como firewall de aplicaciones y SSL.		

Migración de reglas mod_rewrite de Apache a directivas avanzadas	Ejemplos de funciones escritas con el motor mod_rewrite del servidor HTTP Apache, con ejemplos de estas funciones después de traducirlas a directivas Rewrite y Responder en Citrix ADC.

Introducción a directivas y expresiones

October 5, 2021

En muchas funciones de Citrix ADC, las directivas controlan la forma en que una función evalúa los datos. Una directiva utiliza una expresión lógica, denominada regla, para evaluar los datos y aplica una o varias acciones según la evaluación. De forma alternativa, una directiva puede aplicar un perfil, que define una acción compleja.

Algunas funciones de Citrix ADC utilizan directivas avanzadas, que ofrecen mayores capacidades que las directivas clásicas anteriores. Si ha migrado a una versión más reciente del software Citrix ADC y ha configurado directivas clásicas para funciones que utilizan directivas avanzadas, debe migrar manualmente las directivas a una infraestructura de directivas avanzada.

Directiva avanzada Infraestructura

October 5, 2021

> **Advertencia**
>
> Las expresiones de directiva clásicas están obsoletas desde Citrix ADC 12.0 compilación 56.20 en adelante y, como alternativa, Citrix recomienda utilizar directivas avanzadas. Para obtener más información, consulte Directivas avanzadas

La infraestructura avanzada de directivas (PI) permite analizar más datos (por ejemplo, el cuerpo de una solicitud HTTP) y configurar más operaciones en la regla de directivas (por ejemplo, transformar los datos del cuerpo de una solicitud en un encabezado HTTP).

Además de asignar una directiva una acción o un perfil, la vincula a un punto concreto del procesamiento asociado con las funciones de Citrix ADC. El punto de enlace es un factor que determina cuándo se evaluará la directiva.

Beneficios del uso de directivas avanzadas

Las directivas de directivas avanzadas utilizan un potente lenguaje de expresión basado en un modelo de objetos de clase y ofrecen varias opciones que mejoran la capacidad de configurar el comportamiento de varias funciones de Citrix ADC. Con la infraestructura de directivas avanzadas (PI), puede hacer lo siguiente:

- Realice análisis detallados del tráfico de red de las capas 2 a 7.
- Evalúe cualquier parte del encabezado o cuerpo de una solicitud o respuesta HTTP o HTTPS.
- Vincular directivas a los múltiples puntos de enlace que admite la infraestructura de directivas avanzadas (PI) en los niveles de servidor virtual, de anulación y de anulación por defecto.
- Utilice expresiones goto para transferir el control a otras directivas y puntos de enlace, según lo determinado por el resultado de la evaluación de expresiones.
- Utilice herramientas especiales como conjuntos de patrones, etiquetas de directivas, identificadores de límite de velocidad y llamadas HTTP, que le permiten configurar directivas de manera eficaz para casos de uso complejos.

Además, la utilidad de configuración amplía un sólido soporte de interfaz gráfica de usuario para la infraestructura de directivas avanzadas (PI) y expresiones y permite a los usuarios que tienen un conocimiento limitado de los protocolos de red configurar directivas de forma rápida y sencilla. La utilidad de configuración también incluye una función de evaluación de directivas para directivas avanzadas. Puede utilizar esta función para evaluar una directiva avanzada y probar su comportamiento antes de comprobarla, lo que reduce el riesgo de errores de configuración.

Componentes básicos de una directiva avanzada

A continuación se presentan algunas funciones de una directiva avanzada:

- Name. Cada directiva tiene un nombre exclusivo.
- Regla. La regla es una expresión lógica que permite a la función Citrix ADC evaluar un fragmento de tráfico u otro objeto. Por ejemplo, una regla puede permitir que Citrix ADC determine si una solicitud HTTP se originó desde una dirección IP concreta o si un encabezado Cache-Control de una solicitud HTTP tiene el valor “No-Cache”.

Las directivas avanzadas pueden utilizar todas las expresiones disponibles en una directiva clásica, a excepción de las expresiones clásicas para el cliente VPN SSL. Además, las directivas avanzadas permiten configurar expresiones más complejas.

- Fijaciones. Para asegurarse de que Citrix ADC pueda invocar una directiva cuando sea necesaria, debe asociarla o vincularla a uno o más puntos de enlace.

Puede enlazar una directiva globalmente o a un servidor virtual. Para obtener más información, consulte Acerca de los enlaces de directivas.

- Una acción asociada. Una acción es una entidad independiente de una directiva. En última instancia, la evaluación de directivas da lugar a que Citrix ADC realice una acción.

Por ejemplo, una directiva de la caché integrada puede identificar solicitudes HTTP de archivos.png o.jpeg. Una acción asociada a esta directiva determina que las respuestas a este tipo de solicitudes se sirven desde la caché.

Para algunas funciones, las acciones se configuran como parte de un conjunto de instrucciones más complejo conocido como perfil.

Cómo utilizan las directivas las distintas funciones de Citrix ADC

Citrix ADC admite varias funciones que dependen de las directivas para su funcionamiento. En la tabla siguiente se resume el modo en que las funciones de Citrix ADC utilizan las directivas.

Nombre de función	Tipo de directiva	Cómo utilizar las directivas en la función
Sistema	Clásico	Para la función Autenticación, las directivas contienen esquemas de autenticación para distintos métodos de autenticación. Por ejemplo, puede configurar esquemas de autenticación basados en certificados y LDAP. También se configuran las directivas en la función Auditoría.
DNS	Avanzado	Determinar cómo llevar a cabo la resolución DNS de las solicitudes.
SSL	Clásico y avanzado	Para determinar cuándo aplicar una función de cifrado y agregar información de certificado al texto sin cifrar. Para proporcionar seguridad de extremo a extremo, después de descifrar un mensaje, la función SSL vuelve a cifrar el texto sin cifrar y utiliza SSL para comunicarse con los servidores web.
Compresión	Clásico y avanzado	Determinar qué tipo de tráfico se comprime.
Almacenamiento en caché integrado	Avanzado	Para determinar si las respuestas HTTP se pueden almacenar en caché.
Responder	Avanzado	Configurar el comportamiento de la función Responder.

Nombre de función	Tipo de directiva	Cómo utilizar las directivas en la función
Funciones de protección	Clásico	Configurar el comportamiento de las funciones Filter, SureConnect y Priority Queue Server.
Conmutación de contenido	Clásico y avanzado	Determinar qué servidor o grupo de servidores es responsable de atender las respuestas, en función de las funciones de una solicitud entrante. Las funciones de solicitud incluyen el tipo de dispositivo, el idioma, las cookies, el método HTTP, el tipo de contenido y el servidor de caché asociado.
AAA - Gestión del tráfico	Clásico. Excepciones: Las directivas de tráfico solo admiten infraestructuras de directivas (PI) avanzadas y las directivas de autorización admiten la infraestructura de directivas (PI) avanzada.	Para comprobar la seguridad del lado del cliente antes de que los usuarios inicien sesión y establezcan una sesión. Las directivas de tráfico, que determinan si se requiere el inicio de sesión único (SSO), utilizan únicamente la directiva Avanzada. Las directivas de autorización autorizan a los usuarios y grupos que tienen acceso a los recursos de la intranet a través del dispositivo.
Redirección de caché	Clásico	Para determinar si las respuestas se entregan desde una caché o desde un servidor de origen.

Nombre de función	Tipo de directiva	Cómo utilizar las directivas en la función
Reescribe	Avanzado	Identificar los datos HTTP que quiere modificar antes de servir. Las directivas proporcionan reglas para modificar los datos. Por ejemplo, puede modificar los datos HTTP para redirigir una solicitud a una nueva página principal, a un nuevo servidor o a un servidor seleccionado en función de la dirección de la solicitud entrante, o puede modificar los datos para enmascarar la información del servidor en una respuesta por motivos de seguridad. La función URL Transformer identifica las URL de las transacciones HTTP y los archivos de texto con el fin de evaluar si se debe transformar una URL.
Firewall de aplicaciones	Clásico y avanzado	Identificar las funciones del tráfico y los datos que deben o no admitirse a través del firewall.
Citrix Gateway, función Acceso sin cliente	Avanzado	Para definir reglas de reescritura para el acceso web general mediante Citrix Gateway.
Citrix Gateway	Clásico	Determinar cómo Citrix Gateway realiza la autenticación, autorización, auditoría y otras funciones.

Acerca de las acciones y los perfiles

Las directivas no toman medidas por sí mismas sobre los datos. Las directivas proporcionan una lógica de solo lectura para evaluar el tráfico. Para permitir que una función realice una operación basada en una evaluación de directivas, debe configurar acciones o perfiles y asociarlos a directivas.

Nota: Las acciones y los perfiles son específicos de determinadas funciones. Para obtener información sobre la asignación de acciones y perfiles a entidades, consulte la documentación de las funciones individuales.

Acerca de las acciones

Las acciones son pasos que realiza Citrix ADC, según la evaluación de la expresión de la directiva. Por ejemplo, si una expresión de una directiva coincide con una dirección IP de origen concreta de una solicitud, la acción asociada a esta directiva determina si se permite la conexión.

Los tipos de acciones que Citrix ADC puede llevar a cabo son específicos de cada función. Por ejemplo, en Reescritura, las acciones pueden reemplazar el texto de una solicitud, cambiar la URL de destino de una solicitud, etc. En el almacenamiento en caché integrado, las acciones determinan si las respuestas HTTP se entregan desde la caché o desde un servidor de origen.

En algunas funciones de Citrix ADC, las acciones están predefinidas y en otras son configurables. En algunos casos, (por ejemplo, Reescritura), se configuran las acciones con los mismos tipos de expresiones que se utilizan para configurar la regla de directiva asociada.

Acerca de los perfiles

Algunas funciones de Citrix ADC permiten asociar perfiles, o tanto acciones como perfiles, a una directiva. Un perfil es un conjunto de ajustes que permiten a la función realizar una función compleja. Por ejemplo, en el firewall de la aplicación, un perfil de datos XML puede realizar varias operaciones de filtrado, como examinar los datos en busca de sintaxis XML ilegal o pruebas de inyección de SQL.

Uso de acciones y perfiles en determinadas funciones

En la tabla siguiente se resume el uso de acciones y perfiles en distintas funciones de Citrix ADC. La tabla no es exhaustiva. Para obtener más información sobre los usos específicos de las acciones y los perfiles de una función, consulte la documentación de la función.

Función	Uso de una acción	Uso de un perfil
Firewall de aplicaciones	Sinónimo de perfil	Todas las funciones de firewall de aplicaciones utilizan perfiles para definir comportamientos complejos, incluido el aprendizaje basado en patrones. Estos perfiles se agregan a las directivas.
Citrix Gateway	Las siguientes funciones de las acciones de uso de Citrix Gateway: Autenticación previa. Utiliza las acciones Permitir y Denegar. Estas acciones se agregan a un perfil., Autorización. Utiliza las acciones Permitir y Denegar. Estas acciones se agregan a una directiva. Compresión TCP. Utiliza varias acciones. Estas acciones se agregan a una directiva.	Las siguientes funciones utilizan un perfil: Autenticación previa, Sesión, Tráfico y Acceso sin cliente. Después de configurar los perfiles, los agregará a las directivas.
Reescribe	Las acciones de reescritura de URL se configuran y se agregan a una directiva.	No se usa.
Almacenamiento en caché integrado	Configurar acciones de almacenamiento en caché e invalidación dentro de una directiva	No se usa.
AAA - Gestión del tráfico	Se selecciona un tipo de autenticación, se establece una acción de autorización de ALLOW o DENY, o se establece la auditoría en SYSLOG o NSLOG.	Puede configurar los perfiles de sesión con una acción de autorización y tiempo de espera predeterminados.

Función	Uso de una acción	Uso de un perfil
Funciones de protección	Las acciones se configuran dentro de las directivas para las siguientes funciones: Filtro, Compresión, Responder y SureConnect.	No se usa.
SSL	Las acciones se configuran dentro de las directivas SSL	No se usa.
Sistema	La acción está implícita. Para la función Autenticación, es Permitir o Denegar. En el caso de la auditoría, está activada o desactivada la auditoría.	No se usa.
DNS	La acción está implícita. Se trata de Drop Packets o la ubicación de un servidor DNS.	No se usa.
Descarga de SSL	La acción está implícita. Se basa en una directiva que se asocia a un servidor virtual SSL o a un servicio.	No se usa.
Compresión	Determinar el tipo de compresión que se aplicará a los datos	No se usa.
Conmutación de contenido	La acción está implícita. Si una solicitud coincide con la directiva, la solicitud se dirige al servidor virtual asociado a la directiva.	No se usa.
Redirección de caché	La acción está implícita. Si una solicitud coincide con la directiva, la solicitud se dirige al servidor de origen.	No se usa.

Acerca de las vinculaciones de directivas

Una directiva está asociada o vinculada a una entidad que permite invocar la directiva. Por ejemplo, puede vincular una directiva a la evaluación de tiempo de solicitud que se aplica a todos los servidores virtuales. Un conjunto de directivas vinculadas a un punto de enlace determinado constituye un banco de directivas.

A continuación se presenta un resumen de los diferentes tipos de puntos de enlace de una directiva:

- Tiempo de solicitud global. Una directiva puede estar disponible para todos los componentes de una función en el momento de la solicitud.
- Tiempo de respuesta global. Una directiva puede estar disponible para todos los componentes de una función en el momento de respuesta.
- Tiempo de solicitud, específico del servidor virtual.

Una directiva se puede enlazar al procesamiento en tiempo de solicitud de un servidor virtual concreto. Por ejemplo, puede enlazar una directiva de tiempo de solicitud a un servidor virtual de redirección de caché para garantizar que determinadas solicitudes se reenvíen a un servidor virtual de equilibrio de carga para la caché y que otras solicitudes se envíen a un servidor virtual de equilibrio de carga para el origen.

- Tiempo de respuesta específico del servidor virtual. Una directiva también se puede enlazar al procesamiento del tiempo de respuesta de un servidor virtual concreto.
- Etiqueta de directiva definida por el usuario. Para la infraestructura de directivas avanzada (PI), puede configurar agrupaciones personalizadas de directivas (bancos de directivas) definiendo una etiqueta de directiva y recopilando un conjunto de directivas relacionadas bajo el rótulo de directiva.
- Otros puntos de enlace. La disponibilidad de puntos de enlace adicionales depende del tipo de directiva avanzada y de las funciones específicas de la función Citrix ADC pertinente.

Para obtener información adicional sobre los enlaces de directivas avanzadas, consulte Vincular directivas que utilizan el tema Directivas avanzadas .

Acerca del orden de evaluación de las directivas

Los grupos de directivas y las directivas de un grupo se evalúan en un orden determinado, en función de lo siguiente:

- El punto de enlace de la directiva, por ejemplo, si la directiva está vinculada al procesamiento en tiempo de solicitud de un servidor virtual o al procesamiento de tiempo de respuesta global. Por ejemplo, en el momento de la solicitud, Citrix ADC evalúa todas las directivas de tiempo de solicitud antes de evaluar cualquier directiva específica del servidor virtual.
- El nivel de prioridad de la directiva. Para cada punto del proceso de evaluación, un nivel de prioridad asignado a una directiva determina el orden de evaluación en relación con otras di-

rectivas que comparten el mismo punto de enlace. Por ejemplo, cuando Citrix ADC evalúa un banco de directivas específicas del servidor virtual en el momento de la solicitud, comienza con la directiva asignada al valor de prioridad más bajo. En las directivas, los niveles de prioridad deben ser únicos en todos los puntos de enlace.

En el caso de las directivas avanzadas, Citrix ADC selecciona una agrupación o un banco de directivas en un punto concreto del procesamiento general. El siguiente es el orden de evaluación de las agrupaciones básicas, o bancos, de las directivas avanzadas:

1. Anulación global en el momento de la solicitud
2. En el momento de la solicitud, específico del servidor virtual (un punto de enlace por servidor virtual)
3. Valor predeterminado global en el tiempo de solicitud
4. Anulación global del tiempo de respuesta
5. Tiempo de respuesta específico del servidor virtual
6. Valor predeterminado global de tiempo de respuesta

Sin embargo, dentro de cualquiera de los bancos de directivas anteriores, el orden de evaluación es más flexible que en las directivas. Dentro de un banco de directivas, puede apuntar a la siguiente directiva que se evaluará independientemente del nivel de prioridad, y puede invocar bancos de directivas que pertenezcan a otros puntos de enlace y bancos de directivas definidos por el usuario.

Orden de evaluación basado en el flujo de tráfico

A medida que el tráfico fluye a través de Citrix ADC y se procesa mediante diversas funciones, cada función realiza una evaluación de directivas. Cuando una directiva coincide con el tráfico, Citrix ADC almacena la acción y continúa procesando hasta que los datos están a punto de salir de Citrix ADC. En ese momento, Citrix ADC suele aplicar todas las acciones coincidentes. El almacenamiento en caché integrado, que solo aplica una acción final de caché o nocache, es una excepción.

Algunas directivas afectan el resultado de otras directivas. A continuación se presentan algunos ejemplos:

- Si se proporciona una respuesta desde la memoria caché integrada, otras funciones de Citrix ADC no procesan la respuesta ni la solicitud que la inició.
- Si la función de filtrado de contenido impide que se publique una respuesta, ninguna función posterior evalúa la respuesta.

Si el firewall de la aplicación rechaza una solicitud entrante, ninguna otra función puede procesarla.

Expresiones directivas avanzadas

October 5, 2021

Uno de los componentes más fundamentales de una directiva es su regla. Una regla de directiva es una expresión lógica que permite a la directiva analizar el tráfico. La mayor parte de la funcionalidad de la directiva se deriva de su expresión.

Una expresión hace coincidir las funciones del tráfico u otros datos con uno o varios parámetros y valores. Por ejemplo, una expresión puede permitir que Citrix ADC logre lo siguiente:

- Determina si una solicitud contiene un certificado.
- Determine la dirección IP de un cliente que envió una solicitud TCP.
- Identificar los datos que contiene una solicitud HTTP (por ejemplo, una hoja de cálculo o una aplicación de procesamiento de textos popular).
- Calcula la longitud de una solicitud HTTP.

Acerca de las expresiones directivas avanzadas

Cualquier función que utilice una infraestructura de directivas avanzada también utiliza expresiones avanzadas. Para obtener información sobre qué funciones utilizan directivas avanzadas, consulte la tabla Función, Tipo de directiva y Uso de directivas de Citrix ADC.

Las expresiones de directiva avanzadas tienen otros usos. Además de configurar expresiones avanzadas en las reglas de directivas, las
expresiones avanzadas se configuran en las siguientes situaciones:

- Almacenamiento en caché integrado:

  Las expresiones de directivas avanzadas se utilizan para configurar un selector para un grupo de contenido en la memoria caché integrada.

- Equilibrio de carga:

  Las expresiones de directivas avanzadas se utilizan para configurar la extracción de tokens de un servidor virtual de equilibrio de carga que utiliza el método TOKEN para el equilibrio de carga.

- Reescritura:

  Las expresiones de directivas avanzadas se utilizan para configurar acciones de reescritura.

- Directivas basadas en tarifas:

  Las expresiones de directivas avanzadas se utilizan para configurar selectores de límites al configurar una directiva para controlar la velocidad del tráfico a varios servidores.

A continuación se presentan algunos ejemplos sencillos de expresiones de directivas avanzadas:

- Una URL de solicitud HTTP no contiene más de 500 caracteres.

```
http.req.url.length \<= 500
```

- Una solicitud HTTP contiene una cookie de menos de 500 caracteres.

```
http.req.cookie.length \< 500
```

- Una URL de solicitud HTTP contiene una cadena de texto concreta.

```
http.req.url.contains(".html")
```

Conversión de expresiones de directiva mediante la herramienta NSPEPI

January 21, 2022

> **Nota:**
>
> Puede descargar la herramienta de comprobación de preconfiguración y NSPEPI desde el GitHub público. Para obtener más información, consulta la página NEPEPI de GitHub y la página README para obtener instrucciones detalladas para descargar, instalar y usar las herramientas. Recomendamos a los clientes que utilicen las herramientas disponibles en GitHub para obtener la versión más completa y actualizada.

Las funciones y funcionalidades clásicas basadas en directivas han sido obsoletas a partir de NetScaler 12.0 build 56.20. Como alternativa, Citrix recomienda utilizar la infraestructura de directivas avanzada. Como parte de este esfuerzo, al actualizar a Citrix ADC 12.1 compilación 56.20 o posterior, debe reemplazar las funciones y funcionalidades clásicas basadas en directivas por sus funciones y funcionalidades no obsoletas correspondientes. Además, debe convertir las directivas y expresiones clásicas en directivas y expresiones avanzadas. Además, todas las nuevas funciones de Citrix ADC solo admiten la infraestructura de directivas avanzada.

La herramienta `nspepi` puede realizar lo siguiente:

1. Convertir expresiones de directiva clásicas en expresiones de directiva avanzadas.
2. Convierta determinadas directivas clásicas y sus vinculaciones de entidad en directivas y enlaces avanzados.
3. Convierta algunas funciones obsoletas más en sus correspondientes funciones no obsoletas.
4. Convierta los comandos de filtro clásicos en comandos de filtro avanzados.

> **Nota:**
>
> Una vez que la herramienta `nspepi` convierte correctamente el archivo de configuración ns.conf, la herramienta muestra el archivo convertido como un archivo nuevo con el prefijo "new_". Si el archivo de configuración convertido contiene errores o advertencias, debe corregirlos manual-

> mente como parte del proceso de conversión. Una vez convertido, debe probar el archivo en el entorno de prueba y utilizarlo para reemplazar el archivo de configuración ns.conf real. Después de realizar la prueba, debe reiniciar el dispositivo para el archivo de configuración ns.conf recién convertido o corregido.

Las funciones que solo admiten directivas o expresiones clásicas quedan obsoletas y se pueden sustituir por las funciones no obsoletas correspondientes.

> **Nota:**
>
> La información relativa a la versión anterior de la herramienta `nspepi` está disponible en formato PDF. Para obtener más información, consulte Conversión de directivas clásica con la herramienta nspepi anterior a la versión 12.1-51.16 PDF.

Advertencias de conversión y archivos de error

Antes de utilizar la herramienta para la conversión, hay algunas advertencias que debes tener en cuenta:

1. Todas las advertencias y errores se envían a la consola. Se ha creado un archivo de advertencia en el que se almacenan los archivos de configuración.
2. El archivo de advertencias y errores tiene el mismo nombre que el archivo de entrada pero con el prefijo “warn_” agregado al nombre del archivo. Durante la conversión de expresiones (cuando se utiliza -e), las advertencias aparecen en el directorio actual con el nombre “warn_expr”.

> **Nota:**
>
> Este archivo tiene un formato de archivo de registros estándar, con sello de fecha/hora y nivel de registro. Las instancias anteriores del archivo se conservan con sufijos como “.1”, “.2”, etc., ya que la herramienta se ejecuta varias veces. Se conservarán como máximo 10 instancias.

Formato de archivo convertido

Al convertir un fichero de configuración (mediante “-f”), el fichero convertido se coloca en el mismo directorio donde existe el fichero de configuración de entrada con el mismo nombre pero con el prefijo “new_”.

Comandos o funciones gestionados por la herramienta de conversión nspepi

A continuación se indican los comandos que se manejan durante el proceso de conversión automática.

- Las siguientes directivas clásicas y sus expresiones se convierten en directivas y expresiones avanzadas. La conversión incluye vinculaciones de entidades y vinculaciones globales.

1. add appfw policy
2. add cmp policy
3. add cr policy
4. add cs policy
5. add tm sessionPolicy
6. add filter action
7. add filter policy
8. filter policy binding a load balancing, content switching, cache redirection y global.

> **Nota:**
>
> Sin embargo, para “add tm sessionPolicy”, no se puede vincular a la anulación global en las directivas avanzadas.

- El parámetro de regla configurado en “add lb virtual server” se convierte de expresión clásica a expresión avanzada.
- El parámetro SPDY configurado en el comando “add ns httpProfile” o “set ns httpProfile” se cambia a “-http2 ENABLED”.
- Expresiones con nombre (comandos “add policy expression”). Cada expresión de directiva clásica con nombre se convierte en su expresión denominada avanzada correspondiente con “nspepi_adv_” establecido como prefijo. Además, el uso de expresiones con nombre para las expresiones clásicas convertidas se cambia a las expresiones con nombre avanzadas correspondientes. Además, cada expresión con nombre tiene dos expresiones con nombre, una es Clásica y la otra Avanzada (como se muestra a continuación).
- Se admite la conversión Tunnel TrafficPolicy
- Manejo de las vinculaciones de directivas clásicas integradas en CMP, CR y Tunnel.
- La función Patclass se convierte en una función de conjunto de Pat.
- El parámetro “-pattern” del comando “agregar acción de reescritura” se convierte para usar el parámetro “-search”.
- SYS.EVAL_CLASSIC_EXPR se convierte en la expresión avanzada equivalente no obsoleta. Estas expresiones se pueden ver en cualquier comando en el que se permitan expresiones avanzadas.
- Los prefijos Q y S de las expresiones avanzadas se convierten en expresiones avanzadas equivalentes no obsoletas. Estas expresiones se pueden ver en cualquier comando en el que se permitan expresiones avanzadas.

Por ejemplo:

```
add policy expression classic_expr ns_true
Converts to:
add policy expression classic_expr ns_true
add policy expression nspepi_adv_classic_expr TRUE
<!--NeedCopy-->
```


- Se elimina el parámetro PolicyType configurado en el comando “set cmp parameter”. De forma predeterminada, el tipo de directiva es “Avanzada”.

Convertir comandos de filtro clásicos en comandos de filtro avanzados

La herramienta `nspepi` puede convertir comandos basados en acciones de filtro clásicas como agregar, enlazar, etc. en comandos de filtro avanzados.

Sin embargo, la herramienta nepepi no admite los siguientes comandos de filtro.

1. add filter action <`action Name`> FORWARD <`service name`>
2. add filter action <`action name`> ADD prebody
3. add filter action <`action name`> ADD postbody

> **Nota:**
>
> 1. Si existen entidades de reescritura o respuesta en ns.conf y sus directivas están enlazadas globalmente con la expresión `GOTO` como `END` o `USER_INVOCATION_RESULT` y el tipo de enlace es `REQ_X` o `RES_X`, la herramienta convierte parcialmente los comandos de filtro de enlace y los comenta. Se muestra una advertencia para realizar un esfuerzo manual.
> 2. Si existen funciones de reescritura o respuesta existentes y sus directivas están enlazadas a servidores virtuales (por ejemplo, equilibrio de carga, cambio de contenido o redirección de caché) de tipo HTTPS con `GOTO - END` o `USER_INVOCATION_RESULT`, la herramienta convierte parcialmente los comandos de filtro de enlace y, a continuación, comenta. Se muestra una advertencia para realizar un esfuerzo manual.

Ejemplo

A continuación se muestra un ejemplo de entrada:

```
1  add lb vserver v1 http 1.1.1.1 80 -persistenceType NONE -cltTimeout
       9000
2  add cs vserver csv1 HTTP 1.1.1.2 80 -cltTimeout 180 -persistenceType
       NONE
3  add cr vserver crv1 HTTP 1.1.1.3 80 -cacheType FORWARD
4  add service svc1 1.1.1.4 http 80
5  add filter action fact_add add 'header:value'
6  add filter action fact_variable add 'H1:%%HTTP.TRANSID%%'
7  add filter action fact_prebody add prebody
8  add filter action fact_error_act1 ERRORCODE 200 ”<HTML>Good URL</HTML>”
9  add filter action fact_forward_act1 FORWARD svc1
10 add filter policy fpol_add_res -rule ns_true -resAction fact_add
```



```
add filter policy fpol_error_res -rule ns_true -resAction
    fact_error_act1
add filter policy fpol_error_req -rule ns_true -reqAction
    fact_error_act1
add filter policy fpol_add_req -rule ns_true -reqAction fact_add
add filter policy fpol_variable_req -rule ns_true -reqAction
    fact_variable
add filter policy fpol_variable_res -rule ns_true -resAction
    fact_variable
add filter policy fpol_prebody_req -rule ns_true -reqAction
    fact_prebody
add filter policy fpol_prebody_res -rule ns_true -resAction
    fact_prebody
add filter policy fpol_forward_req -rule ns_true -reqAction
    fact_forward_act1
bind lb vserver v1 -policyName fpol_add_res
bind lb vserver v1 -policyName fpol_add_req
bind lb vserver v1 -policyName fpol_error_res
bind lb vserver v1 -policyName fpol_error_req
bind lb vserver v1 -policyName fpol_variable_res
bind lb vserver v1 -policyName fpol_variable_req
bind lb vserver v1 -policyName fpol_forward_req
bind cs vserver csv1 -policyName fpol_add_req
bind cs vserver csv1 -policyName fpol_add_res
bind cs vserver csv1 -policyName fpol_error_res
bind cs vserver csv1 -policyName fpol_error_req
bind cr vserver crv1 -policyName fpol_add_req
bind cr vserver crv1 -policyName fpol_add_res
bind cr vserver crv1 -policyName fpol_error_res
bind cr vserver crv1 -policyName fpol_error_req
bind cr vserver crv1 -policyName fpol_forward_req
bind filter global fpol_add_req
bind filter global fpol_add_res
bind filter global fpol_error_req
bind filter global fpol_error_res
bind filter global fpol_variable_req
bind filter global fpol_variable_res
bind filter global fpol_variable_res -state DISABLED
bind filter global fpol_prebody_req
bind filter global fpol_forward_req
After conversion, warning/error messages will be displayed for manual
    effort.
Warning files:
cat warn_<input file name>:
2019-11-07 17:13:34,724: ERROR - Conversion of [add filter action
```



```
    fact_prebody add prebody] not supported in this tool.
48  2019-11-07 17:13:34,739: ERROR - Conversion of [add filter action
    fact_forward_act1 FORWARD svc1] not supported in this tool.
49  2019-11-07 17:13:38,042: ERROR - Conversion of [add filter policy
    fpol_prebody_req -rule ns_true -reqAction fact_prebody] not
    supported in this tool.
50  2019-11-07 17:13:38,497: ERROR - Conversion of [add filter policy
    fpol_prebody_res -rule ns_true -resAction fact_prebody] not
    supported in this tool.
51  2019-11-07 17:13:39,035: ERROR - Conversion of [add filter policy
    fpol_forward_req -rule ns_true -reqAction fact_forward_act1] not
    supported in this tool.
52  2019-11-07 17:13:39,060: WARNING - Following bind command is commented
    out because state is disabled. Advanced expressions only have a
    fixed ordering of the types of bindings without interleaving, except
     that global bindings are allowed before all other bindings and
    after all bindings. If you have global bindings in the middle of non
    -global bindings or any other interleaving then you will need to
    reorder all your bindings for that feature and direction. Refer to
    nspepi documentation. If command is required please take a backup
    because comments will not be saved in ns.conf after triggering 'save
     ns config': bind filter global fpol_variable_res -state DISABLED
53
54
55  <!--NeedCopy-->
```

A continuación se presenta un ejemplo de salida. Todos los comandos convertidos se comentan.

```
1  cat new_<input file name>
2  add rewrite action fact_add insert_http_header header ””value””
3  add filter action fact_prebody add prebody
4  add filter action fact_forward_act1 FORWARD svc1
5  add filter policy fpol_prebody_req -rule ns_true -reqAction
    fact_prebody
6  add filter policy fpol_prebody_res -rule ns_true -resAction
    fact_prebody
7  add filter policy fpol_forward_req -rule ns_true -reqAction
    fact_forward_act1
8  bind lb vserver v1 -policyName fpol_forward_req
9  bind cr vserver crv1 -policyName fpol_forward_req
10 #bind filter global fpol_variable_res -state DISABLED
11 bind filter global fpol_prebody_req
12 bind filter global fpol_forward_req
```



```
13 add rewrite action nspepi_adv_fact_variable insert_http_header H1 HTTP.
   RES.TXID
14 add rewrite action fact_variable insert_http_header H1 HTTP.REQ.TXID
15 add responder action fact_error_act1 respondwith "HTTP.REQ.VERSION.
   APPEND(" 200 OK\r
16 nConnection: close\r
17 nContent-Length: 21\r\n\r
18 n<HTML>Good URL</HTML>")"
19 add rewrite action nspepi_adv_fact_error_act1 replace_http_res "HTTP.
   REQ.VERSION.APPEND(" 200 OK\r
20 nConnection: close\r
21 nContent-Length: 21\r\n\r
22 n<HTML>Good URL</HTML>")"
23 add rewrite policy fpol_add_res TRUE fact_add
24 add rewrite policy fpol_error_res TRUE nspepi_adv_fact_error_act1
25 add responder policy fpol_error_req TRUE fact_error_act1
26 add rewrite policy fpol_add_req TRUE fact_add
27 add rewrite policy fpol_variable_req TRUE fact_variable
28 add rewrite policy fpol_variable_res TRUE nspepi_adv_fact_variable
29 set cmp parameter -policyType ADVANCED
30 bind rewrite global fpol_add_req 100 NEXT -type REQ_DEFAULT
31 bind rewrite global fpol_variable_req 200 NEXT -type REQ_DEFAULT
32 bind rewrite global fpol_add_res 100 NEXT -type RES_DEFAULT
33 bind rewrite global fpol_error_res 200 NEXT -type RES_DEFAULT
34 bind rewrite global fpol_variable_res 300 NEXT -type RES_DEFAULT
35 bind responder global fpol_error_req 100 END -type REQ_DEFAULT
36 bind lb vserver v1 -policyName fpol_add_res -type RESPONSE -priority
   100 -gotoPriorityExpression NEXT
37 bind lb vserver v1 -policyName fpol_error_res -type RESPONSE -priority
   200 -gotoPriorityExpression NEXT
38 bind lb vserver v1 -policyName fpol_variable_res -type RESPONSE -
   priority 300 -gotoPriorityExpression NEXT
39 bind lb vserver v1 -policyName fpol_add_req -type REQUEST -priority 100
    -gotoPriorityExpression NEXT
40 bind lb vserver v1 -policyName fpol_variable_req -type REQUEST -
   priority 200 -gotoPriorityExpression NEXT
41 bind lb vserver v1 -policyName fpol_error_req -type REQUEST -priority
   100 -gotoPriorityExpression END
42 bind cs vserver csv1 -policyName fpol_add_req -type REQUEST -priority
   100 -gotoPriorityExpression NEXT
43 bind cs vserver csv1 -policyName fpol_add_res -type RESPONSE -priority
   100 -gotoPriorityExpression NEXT
44 bind cs vserver csv1 -policyName fpol_error_res -type RESPONSE -
   priority 200 -gotoPriorityExpression NEXT
45 bind cs vserver csv1 -policyName fpol_error_req -type REQUEST -priority
```



```
        100 -gotoPriorityExpression END
46 bind cr vserver crv1 -policyName fpol_add_req -type REQUEST -priority
       100 -gotoPriorityExpression NEXT
47 bind cr vserver crv1 -policyName fpol_add_res -type RESPONSE -priority
       100 -gotoPriorityExpression NEXT
48 bind cr vserver crv1 -policyName fpol_error_res -type RESPONSE -
       priority 200 -gotoPriorityExpression NEXT
49 bind cr vserver crv1 -policyName fpol_error_req -type REQUEST -priority
        100 -gotoPriorityExpression END
50
51 <!--NeedCopy-->
```

Convierta los comandos de filtro clásicos en comandos de funciones avanzadas si los enlaces de directivas de reescritura o respuesta existentes tienen la expresión goto END o USE_INNVOCATION

En esta conversión, si una directiva de reescritura vinculada a uno o más servidores virtuales y si el servidor tiene END o USE_INVOCATION_RESULT, la herramienta comenta los comandos.

Ejemplo

A continuación se muestra un comando de entrada de ejemplo:

```
1  COPY
2  add filter policy fpol1 -rule ns_true -resAction reset
3  add filter policy fpol2 -rule ns_true -reqAction reset
4  add rewrite policy pol1 true NOREWRITE
5  add rewrite policylabel pl http_res
6  bind rewrite policylabel pl pol1 1
7  bind rewrite global NOPOLICY 1 USE_INVOCATION_RESULT -type RES_DEFAULT
       -invoke policylabel pl
8  add responder policy pol2 true NOOP
9  add responder policylabel pl -policylabeltype HTTP
10 bind responder policylabel pl pol2 1
11 bind responder global NOPOLICY 1 USE_INVOCATION_RESULT -type
       REQ_DEFAULT -invoke policylabel pl
12 bind lb vserver v1_tcp -policyName pol1 -priority 100 -
       gotoPriorityExpression USE_INVOCATION_RESULT -type RESPONSE
13 bind cs vserver csv1_tcp -policyName pol1 -priority 100 -
       gotoPriorityExpression USE_INVOCATION_RESULT -type RESPONSE
14 bind lb vserver v1_tcp -policyName pol2 -priority 100 -
       gotoPriorityExpression USE_INVOCATION_RESULT -type REQUEST
```



```
bind cs vserver csv1_tcp -policyName pol2 -priority 100 -
    gotoPriorityExpression USE_INVOCATION_RESULT -type REQUEST
bind cr vserver crv1_tcp -policyName pol2 -priority 100 -
    gotoPriorityExpression USE_INVOCATION_RESULT -type REQUEST
bind lb vserver v1_http -policyName fpol1
bind cs vserver csv1_http -policyName fpol1
bind lb vserver v2_http -policyName fpol2
bind cs vserver csv2_http -policyName fpol2
bind cr vserver crv2_http -policyName fpol2
bind filter global fpol1 -priority 100
bind filter global fpol2 -priority 100
<!--NeedCopy-->
```

A continuación se muestra un ejemplo de comando de salida:

```
COPY
add rewrite policy pol1 true NOREWRITE
add rewrite policylabel pl http_res
bind rewrite policylabel pl pol1 1
add responder policy pol2 true NOOP
add responder policylabel pl -policylabeltype HTTP
bind responder policylabel pl pol2 1
add rewrite policy fpol1 TRUE RESET
add responder policy fpol2 TRUE RESET
#bind lb vserver v1_http -policyName fpol1 -type RESPONSE
#bind cs vserver csv1_http -policyName fpol1 -type RESPONSE
#bind rewrite global fpol1 100 -type RES_DEFAULT
#bind lb vserver v2_http -policyName fpol2 -type REQUEST
#bind cs vserver csv2_http -policyName fpol2 -type REQUEST
#bind cr vserver crv2_http -policyName fpol2 -type REQUEST
#bind responder global fpol2 100 -type REQ_DEFAULT
bind rewrite global NOPOLICY 1 USE_INVOCATION_RESULT -type RES_DEFAULT
    -invoke policylabel pl
bind responder global NOPOLICY 1 USE_INVOCATION_RESULT -type
    REQ_DEFAULT -invoke policylabel pl
bind lb vserver v1_tcp -policyName pol1 -priority 100 -
    gotoPriorityExpression USE_INVOCATION_RESULT -type RESPONSE
bind lb vserver v1_tcp -policyName pol2 -priority 100 -
    gotoPriorityExpression USE_INVOCATION_RESULT -type REQUEST
bind cs vserver csv1_tcp -policyName pol1 -priority 100 -
    gotoPriorityExpression USE_INVOCATION_RESULT -type RESPONSE
bind cs vserver csv1_tcp -policyName pol2 -priority 100 -
    gotoPriorityExpression USE_INVOCATION_RESULT -type REQUEST
```



```
23 bind cr vserver crv1_tcp -policyName pol2 -priority 100 -
      gotoPriorityExpression USE_INVOCATION_RESULT -type REQUEST-
24
25 <!--NeedCopy-->
```

Comandos o funciones no gestionados por la herramienta de conversión nspepi

A continuación se presentan algunos comandos que no se manejan como parte del proceso de conversión automática.

- Algunos enlaces no se pueden convertir si hay cierto entrelazado de prioridades entre puntos de enlace globales y no globales, entre usuarios y grupos, y también entre enlaces a diferentes entidades. Estos tienen la configuración afectada comentada y se produce un error. Dichas configuraciones se deben convertir manualmente.
- Tanto las directivas clásicas como las avanzadas pueden vincularse a cmp global. Hay muchos casos en los que la funcionalidad cambia una vez que las directivas clásicas se convierten en directivas avanzadas. Hemos convertido comandos que se pueden resolver comentando algunas directivas. Sin embargo, hay algunos comandos que no se pueden convertir. En tales casos, se producirá un error y la conversión debe realizarse manualmente.
- No todos los usos de las expresiones con nombre integradas clásicas se convierten en expresiones con nombre avanzadas equivalentes.
- Las expresiones de seguridad del cliente no se gestionan.
- La opción “-precedence” para los servidores virtuales de conmutación de contenido y redirección de caché no se gestiona.
- Conexión segura (SC)
- Cola prioritaria (PQ)
- Denegación de servicio HTTP (HDOS)
- Inyección HTML
- Autenticación
- Autorización
- VPN
- Syslog
- Nslog
- Las expresiones clásicas basadas en archivos no se gestionan.

> **Nota:**
>
> Para algunas funciones como Patclass/filter, se cambia la sintaxis del comando. Si hay directivas cmd, es posible que sea necesario cambiar las directivas de cmd según los requisitos del cliente.

Problemas conocidos

La herramienta `nspepi` puede producir los siguientes errores:

- Si hay algún problema al convertir una expresión.
- Si una expresión de directiva con nombre utiliza el parámetro -ClientSecurityMessage porque este parámetro no se admite en la expresión de directiva avanzada.

> **Nota:**
>
> Todas las vinculaciones de directivas clásicas con la opción -state inhabilitada se comentan. La opción -state no está disponible para las vinculaciones de directivas avanzadas.

Ejecución de la herramienta nspepi

A continuación se muestra un ejemplo de línea de comandos para ejecutar la herramienta `nspepi`. Esta herramienta se ejecuta desde la línea de comandos del shell (debe escribir el comando "shell" en la "CLI" de NetScaler para llegar a eso). Se debe especificar "-f" o "-e" para realizar una conversión. El uso de "-d" está pensado para que el personal de Citrix lo analice con fines de asistencia técnica.

```
usage: nspepi [-h] (-e <classic policy expression> | -f <path to ns
    config file>)[-d] [-v] [-V

Convert classic policy expressions to advanced policy expressions and
    deprecated commands to non-deprecated
commands.

optional arguments:
-h, --help show this help message and exit
-e <classic policy expression>, --expression <classic policy expression
    >
convert classic policy expression to advanced policy
expression (maximum length of 8191 allowed)
-f <path to ns config file>, --infile <path to ns config file>
convert netscaler config file
-d, --debug log debug output
-v, --verbose show verbose output
-V, --version show program's version number and exit
<!--NeedCopy-->
```

Ejemplos de uso:

1. `nspepi -e "req.tcp.destport == 80"`
2. `nspepi -f ns.conf`

A continuación se presentan algunos ejemplos de ejecución de la herramienta `nspepi` mediante la CLI

Salida de ejemplo para el parámetro —e:

```
root@ns# nspepi -e ”req.http.header foo == ”bar””
”HTTP.REQ.HEADER(”foo”).EQ(”bar”)”
<!--NeedCopy-->
```

Salida de ejemplo para el parámetro -f:

```
root@ns# cat sample.conf
add c\*\*Input\*\*r vserver cr_vs HTTP -cacheType TRANSPARENT -
   cltTimeout 180 -originUSIP OFF
add cr policy cr_pol1 -rule ns_true
bind cr vserver cr_vs -policyName cr_pol1
<!--NeedCopy-->
```

Ejecutar nspepi con el parámetro -f:

```
nspepi -f sample.conf
<!--NeedCopy-->
```

La configuración convertida está disponible en un nuevo archivo `new_sample.conf`.
Compruebe si hay advertencias o errores que se hayan generado en el archivo `warn_sample.conf`.

Ejemplo de salida del parámetro -f junto con el parámetro -v

```
nspepi -f sample.conf -v
INFO - add cr vserver cr_vs HTTP -cacheType TRANSPARENT -cltTimeout 180
    -originUSIP OFF
INFO - add cr policy cr_pol1 -rule TRUE -action ORIGIN
INFO - bind cr vserver cr_vs -policyName cr_pol1 -priority 100 -
   gotoPriorityExpression END -type REQUEST
<!--NeedCopy-->
```

La configuración convertida está disponible en un nuevo archivo `new_sample.conf`.
Compruebe si hay advertencias o errores que se hayan generado en el archivo `warn_sample.conf`.

Archivo de configuración convertido:


```
root@ns# cat new_sample.conf
add cr vserver cr_vs HTTP -cacheType TRANSPARENT -cltTimeout 180 -
    originUSIP OFF
add cr policy cr_pol1 -rule TRUE -action ORIGIN
set cmp parameter -policyType ADVANCED
bind cr vserver cr_vs -policyName cr_pol1 -priority 100 -
    gotoPriorityExpression END -type REQUEST

<!--NeedCopy-->
```

Ejemplo de salida de una configuración de ejemplo sin errores ni advertencias:

```
nspepi -f sample_2.conf
<!--NeedCopy-->
```

La configuración convertida está disponible en un nuevo archivo `new_sample_2.conf`. Compruebe si hay advertencias o errores que se hayan generado en el archivo `warn_sample_2.conf` .

Ejemplo de salida de una configuración de ejemplo con advertencias:

```
root@ns# cat sample_2.conf
add policy expression security_expr "req.tcp.destport == 80" -
    clientSecurityMessage "Not allowed"
set cmp parameter -policyType CLASSIC
add cmp policy cmp_pol1 -rule ns_true -resAction COMPRESS
add cmp policy cmp_pol2 -rule ns_true -resAction COMPRESS
add cmp policy cmp_pol3 -rule TRUE -resAction COMPRESS
bind cmp global cmp_pol1
bind cmp global cmp_pol2 -state DISABLED
bind cmp global cmp_pol3 -priority 1 -gotoPriorityExpression END -type
    RES_DEFAULT
bind lb vserver lb_vs -policyName cmp_pol2
root@ns#
<!--NeedCopy-->
```

Ejemplo de ejecución de nspepi con el parámetro -f:

```
root@ns# nspepi -f sample_2.conf
```



```
2 ERROR - Error in converting expression security_expr : conversion of
    clientSecurityMessage based expression is not supported.
3 WARNING - Following bind command is commented out because state is
    disabled. Advanced expressions only have a fixed ordering of the
    types of bindings without interleaving, except that global bindings
    are allowed before all other bindings and after all bindings. If you
     have global bindings in the middle of non-global bindings or any
    other interleaving then you will need to reorder all your bindings
    for that feature and direction. Refer to nspepi documentation. If
    command is required please take a backup because comments will not
    be saved in ns.conf after triggering 'save ns config': bind cmp
    global cmp_pol2 -state DISABLED
4 Warning - Bindings of advanced CMP policies to cmp global are commented
     out, because initial global cmp parameter is classic but advanced
    policies are bound. Now global cmp parameter policy type is set to
    advanced. If commands are required please take a backup because
    comments will not be saved in ns.conf after triggering 'save ns
    config'. Advanced expressions only have a fixed ordering of the
    types of bindings without interleaving, except that global bindings
    are allowed before all other bindings and after all bindings. If you
     have global bindings in the middle of non-global bindings or any
    other interleaving then you will need to reorder all your bindings
    for that feature and direction. Refer to nspepi documentation.
5 root@ns#
6 <!--NeedCopy-->
```

Archivo convertido:

```
1 root@ns# cat new_sample_2.conf
2 add policy expression security_expr ”req.tcp.destport == 80” -
    clientSecurityMessage ”Not allowed”
3 set cmp parameter -policyType ADVANCED
4 add cmp policy cmp_pol1 -rule TRUE -resAction COMPRESS
5 add cmp policy cmp_pol2 -rule TRUE -resAction COMPRESS
6 add cmp policy cmp_pol3 -rule TRUE -resAction COMPRESS
7 #bind cmp global cmp_pol2 -state DISABLED
8 #bind cmp global cmp_pol3 -priority 1 -gotoPriorityExpression END -type
     RES_DEFAULT
9 bind cmp global cmp_pol1 -priority 100 -gotoPriorityExpression END -
    type RES_DEFAULT
10 bind lb vserver lb_vs -policyName cmp_pol2 -priority 100 -
    gotoPriorityExpression END -type RESPONSE
11 root@ns#
```



```
<!--NeedCopy-->
```

Archivo de advertencias:

```
root@ns# cat warn_sample_2.conf
2019-02-28 06:20:10,590: ERROR - Error in converting expression
    security_expr : conversion of clientSecurityMessage based expression
     is not supported.
2019-02-28 06:20:12,187: WARNING - Following bind command is commented
    out because state is disabled. Advanced expressions only have a
    fixed ordering of the types of bindings without interleaving, except
     that global bindings are allowed before all other bindings and
    after all bindings. If you have global bindings in the middle of non
    -global bindings or any other interleaving then you will need to
    reorder all your bindings for that feature and direction. Refer to
    nspepi documentation. If command is required please take a backup
    because comments will not be saved in ns.conf after triggering 'save
     ns config': bind cmp global cmp_pol2 -state DISABLED
2019-02-28 06:20:12,191: WARNING - Bindings of advanced CMP policies to
     cmp global are commented out, because initial global cmp parameter
    is classic but advanced policies are bound. Now global cmp parameter
     policy type is set to advanced. If commands are required please
    take a backup because comments will not be saved in ns.conf after
    triggering 'save ns config'. Advanced expressions only have a fixed
    ordering of the types of bindings without interleaving, except that
    global bindings are allowed before all other bindings and after all
    bindings. If you have global bindings in the middle of non-global
    bindings or any other interleaving then you will need to reorder all
     your bindings for that feature and direction. Refer to nspepi
    documentation.
root@ns#
<!--NeedCopy-->
```

Vincular prioridades

Las directivas avanzadas no permiten el entrelazado arbitrario por prioridad entre globales y no globales ni entre distintos tipos de enlace. Si confía en este tipo de intercalado de prioridades de directivas clásicas, deberá ajustar las prioridades para que se ajusten a las reglas de directivas avanzadas y para obtener el comportamiento deseado.

Las prioridades de las directivas avanzadas son locales hasta un punto de enlace. Un punto de enlace es una combinación única de protocolo, función, dirección y entidad (las entidades son servidores

virtuales específicos, usuarios, grupos, servicios y anulación global o predeterminada global). Las prioridades directivas no se siguen a través de los puntos vinculantes.

Para un protocolo, función y dirección determinados, el orden de evaluación de las directivas avanzadas se indica a continuación:

- Anulación global.
- Usuario de autenticación, autorización y auditoría (actual).
- Grupos de autenticación, autorización y auditoría (de los que el usuario es miembro) por orden de peso: el orden no está definido si dos o más grupos tienen el mismo peso.
- Servidor virtual LB en el que se recibió la solicitud o que ha seleccionado Content Switching.
- Servidor virtual de conmutación de contenido, servidor virtual de redirección de caché en el que se recibió la solicitud.
- Servicio seleccionado por equilibrio de carga.
- Valor predeterminado global.

Para la evaluación de la directiva de autorización, el pedido es:

- Anulación de sistemas.
- Servidor virtual de equilibrio de carga en el que se recibió la solicitud o que CS seleccionó.
- Servidor virtual de conmutación de contenido en el que se recibió la solicitud.
- Valor predeterminado del sistema.

Dentro de cada punto de enlace, las directivas se evalúan en orden de prioridad, desde el número más bajo hasta el número más alto. Las directivas solo se evalúan para el protocolo utilizado y la dirección desde la que se recibió el mensaje.

Vinculación de directivas clásicas que requieren una nueva priorización manual

Estos son algunos tipos de vinculaciones de directivas clásicas que requieren una nueva priorización manual para satisfacer sus necesidades. Todo esto es para una función determinada y la dirección.

- Prioridades clásicas que aumentan en número de prioridad opuesto a la dirección de las listas de tipos de entidad anteriores. Por ejemplo, un enlace de servidor virtual de conmutación de contenido inferior a un enlace de servidor virtual de equilibrio de carga.
- Prioridades clásicas que intercalan grupos de autenticación, autorización y auditoría. Una parte de un grupo está antes que otro grupo y otra parte va detrás de ese otro grupo.
- Prioridades clásicas que aumentan en número distinto del orden de ponderación de los grupos de autenticación, autorización y auditoría.
- Las prioridades mundiales clásicas que son menos que algunas prioridades no mundiales y las mismas prioridades mundiales son mayores que otras prioridades no mundiales (en otras palabras, cualquier segmento de prioridades que sean no globales, seguido de uno o más globales, seguido de uno o más globales, seguido de uno no global).

Herramienta de comprobación de preconfiguración

April 5, 2022

> **Nota:**
>
> Puede descargar la herramienta de verificación de preconfiguración y NSPEPI desde GitHub público. Para obtener más información, consulta la página NEPEPI de GitHub y la página de preconfiguración de GitHub para obtener instrucciones detalladas sobre cómo descargar las herramientas. Recomendamos a los clientes que utilicen las herramientas disponibles en GitHub para obtener la versión más completa y actualizada.

Hay una herramienta de validación previa disponible en las versiones de Citrix ADC 12.1, 13.0 y 13.1 para comprobar si se sigue utilizando alguna funcionalidad no válida o eliminada en cualquier configuración de funciones. Las herramientas validan el archivo `nsconfig` si contiene comandos o parámetros en un comando que se ha eliminado en la versión Citrix ADC 13.1. Si el resultado de la validación muestra el uso de comandos eliminados o no válidos, antes de actualizar el dispositivo, debe modificar la configuración por la alternativa recomendada por Citrix.

La herramienta también valida el uso de expresiones de directiva clásicas utilizadas en la configuración de entidades que no admiten directivas clásicas. Puede modificar manualmente o utilizar la herramienta `nspepi`.

La herramienta valida el siguiente uso:

1. Expresiones de directiva clásicas en las funciones Content Switching, Cache Redirection, AppFW, SSL y CMP.
2. Función de filtro (también conocida como filtrado de contenido): acciones, directivas y vinculación
3. SPDY en perfil HTTP, conexión segura (SC), cola prioritaria (PQ), denegación de servicio HTTP (DoS) e inyección HTML.
4. Expresiones clásicas en reglas de persistencia de equilibrio de cargas.
5. Parámetros “Pattern” y “BypassSafetyCheck” en las acciones de reescritura.
6. “SYS.EVAL_CLASSIC_EXPR” en expresiones avanzadas.
7. entidad de configuración “patclass”.
8. “HTTP.REQ.BODY” sin ningún argumento en las expresiones avanzadas.
9. Prefijos Q y S en expresiones avanzadas.
10. Parámetro “policyType” para la configuración del parámetro cmp.

Ejecutar herramienta de revalidación previa en UNIX Shell

En el símbolo del sistema, escriba:


```
check_invalid_config <config_file>
<!--NeedCopy-->
```

Ejemplo:

```
root@ns## check_invalid_config/nsconfig/ns.conf
```

Donde, el archivo de configuración es el archivo de configuración de Citrix ADC. El archivo debe ser de una configuración guardada como `ns.conf`.

Salida de ejemplo con errores de validación

A continuación se muestra un ejemplo de resultado del archivo de configuración con errores en la versión 13.1 de Citrix ADC:

```
add policy expression x "sys.eval_classic_expr("ns_true")"
add cmp policy cmp_pol -rule ns_true -resAction GZIP
add cs policy cs_pol_2 -rule ns_true
add cs policy cs_pol_3 -domain www.abc.com
add cs policy cs_pol_4 -url "/abc"
add rewrite action act_1 replace_all "http.req.body(1000)" http.req.url
    -pattern abcd
add rewrite action act_123 replace_all http.req.url ""aaaa"" -pattern
   abcd
add responder action ract respondwith "Q.URL + Q.HEADER("abcd")"
add responder policy rsp_pol "sys.eval_classic_expr("ns_true")" DROP
add appfw policy aff_pol_1 "http.req.body.length.gt(10)" APPFW_BYPASS
add appfw policy aff_pol ns_true APPFW_BYPASS

<!--NeedCopy-->
```

Al recibir estos errores, puede utilizar la herramienta de actualización `nspepi` para convertir su configuración o convertirla manualmente. Para obtener más información, consulte el tema de la herramienta nspepi.

> **Nota:**
>
> Puede ejecutar la herramienta `nspepi` solo en Citrix ADC versión 12.1, 13.0 y versiones posteriores.

Salida de ejemplo sin errores de validación

A continuación se muestra un ejemplo de salida del archivo de configuración sin configuración eliminada o no válida:

```
root@ns# check_invalid_config /var/tmp/new_ns.conf
No issue detected with the configuration.
root@ns#
<!--NeedCopy-->
```

Preguntas frecuentes sobre la depreciación de directivas clásicas

December 2, 2021

- **¿ Cuáles son las directivas clásicas obsoletas a partir de la versión 12.0 de Citrix ADC?**

  Todas las funciones y funcionalidades mencionadas en la tabla Directivas obsoletas están obsoletas de Citrix ADC versión 12.0 compilación 56.20. Citrix recomienda que vea las siguientes tablas (en formato PDF) para obtener detalles de las funciones y las directivas obsoletas.

  - Tabla 1 para directivas obsoletas y su alternativa.
  - Tabla 2 para las funcionalidades obsoletas de Citrix ADC y su alternativa con detalles de configuración.

- **¿Cómo puedo convertir funciones y funcionalidades basadas en directivas clásicas en directivas avanzadas?**

  Puede utilizar la herramienta `nspepi` propietaria de Citrix ADC para convertir comandos, expresiones y configuraciones. `nspepi` ayuda a convertir todas las expresiones clásicas de la configuración de Citrix ADC en expresiones directivas avanzadas. Para obtener más información sobre la herramienta `nspepi`, consulte Conversión de expresiones de directivas mediante la herramienta NSPEPI.

- **¿De qué versión están obsoletas las funciones y funcionalidades basadas en directivas clásicas?**

  Citrix ADC 12.0 compilación 56.20 y posterior.

- **¿De qué versión se quitan las funciones y funcionalidades clásicas basadas en directivas obsoletas del dispositivo Citrix ADC?**

  Citrix ADC versión 13.1 en adelante. Para obtener más información, consulte la tabla Directivas obsoletas.

- **¿Qué pasos debo seguir cuando actualizo mi dispositivo a una compilación que no admite las funciones clásicas basadas en directivas?**

  Citrix recomienda utilizar directivas avanzadas antes de actualizar el dispositivo a versiones posteriores a Citrix ADC versión 13.0. Para obtener más información, consulte Directivas avanzadas.

- **¿Durante cuánto tiempo se admitirán las funciones obsoletas en un dispositivo Citrix ADC?**

  Citrix no admitirá la directiva clásica y su uso en versiones posteriores a la versión 13.0 de Citrix ADC.

  La directiva y las expresiones clásicas están en desuso (se desaconseja su uso y NO se eliminan) a partir de 12.0 build 56.20. La directiva y las expresiones siguen funcionando en todos los lugares de la misma manera que solían funcionar en todas las compilaciones de la versión 13.0. Sin embargo, desde la versión 13.1 de Citrix ADC en adelante, se han eliminado ciertas funciones y funcionalidades basadas en directivas de Classic.

- **¿Tengo que reiniciar el dispositivo después de convertir el archivo de configuración?**

  Sí, debe reiniciar la instancia de Citrix ADC después de la conversión correcta del archivo `ns.config`.

Antes de proceder

October 5, 2021

Antes de configurar expresiones y directivas, asegúrese de comprender la función relevante de Citrix ADC y la estructura de los datos, de la siguiente manera:

- Lea la documentación sobre la función correspondiente.
- Busque en el flujo de datos el tipo de datos que quiere configurar.

Es posible que quiera realizar un seguimiento del tipo de tráfico o contenido que quiere configurar. Esto le dará una idea de los parámetros y valores, y las operaciones con estos parámetros y valores, que debe especificar en una expresión.

Nota: Citrix ADC admite la directiva Avanzada dentro de una función. No se pueden tener ambos tipos en la misma función. En las últimas versiones, algunas funciones de Citrix ADC han migrado del uso de directivas y expresiones a directivas y expresiones avanzadas. Si una función de su interés ha cambiado al formato de directiva avanzada, es posible que tenga que migrar manualmente la información anterior. A continuación se presentan las pautas para decidir si necesitas migrar tus directivas:

- Si configuró directivas clásicas en una versión de la función Almacenamiento en caché integrado anterior a la versión 9.0 y luego actualizó a la versión 9.0 o posterior, no habrá ningún impacto. Todas las directivas heredadas se migran al formato de directiva avanzada.

- Para otras funciones, debe migrar manualmente las directivas y expresiones clásicas a la sintaxis avanzada si la función ha migrado a la directiva Avanzada.

Configurar la infraestructura de directivas avanzada

January 12, 2021

Puede crear directivas avanzadas para varias funciones de Citrix ADC, como DNS, Reescritura, Responder y Almacenamiento en caché integrado, y la función de acceso sin cliente en Citrix Gateway. Las directivas controlan el comportamiento de estas funciones.

Cuando crea una directiva, le asigna un nombre, una regla (una expresión), atributos específicos de entidad y una acción que se realiza cuando los datos coinciden con la directiva. Después de crear la directiva, se determina cuándo se invoca vinculándola globalmente o bien al procesamiento de tiempo de solicitud o tiempo de respuesta para un servidor virtual.

Las directivas que comparten el mismo punto de enlace se conocen como *banco de directivas*. Por ejemplo, todas las directivas enlazadas a un servidor virtual constituyen el banco de directivas del servidor virtual. Al vincular la directiva, se le asigna un nivel de prioridad para especificar cuándo se invoca en relación con otras directivas del banco. Además de asignar un nivel de prioridad, puede configurar un orden de evaluación arbitrario para las directivas de un banco especificando expresiones GoTo.

Además de bancos de directivas asociados a un punto de enlace integrado o a un servidor virtual, puede configurar *etiquetas de directivas*. Una etiqueta de directiva es un banco de directivas identificado por un nombre arbitrario. Se invoca una etiqueta de directiva y las directivas que contiene desde un banco de directivas global o específico del servidor virtual. Se puede invocar una etiqueta de directiva o un banco de directivas de servidor virtual desde varios bancos de directivas.

Para algunas funciones, puede utilizar el administrador de directivas para configurar y enlazar directivas.

Reglas para nombres en identificadores utilizados en directivas

August 20, 2021

Los nombres de los identificadores de las entidades de expresión con nombre asignado, llamada HTTP, conjunto de patrones y limitación de velocidad deben comenzar con un alfabeto ASCII o un guión bajo (_). Los caracteres restantes pueden ser caracteres alfanuméricos ASCII o guiones bajos (_).

Los nombres de estos identificadores no deben comenzar con las siguientes palabras reservadas:

- Las palabras ALT, TRUE o FALSE o el identificador de un carácter Q o S.
- Indicador de sintaxis especial RE (para expresiones regulares) o XP (para expresiones XPath).
- Prefijos de expresión, que actualmente son los siguientes:
  - CLIENTE
  - EXTEND
  - HTTP
  - SERVER
  - SYS
  - TARGET
  - TEXTO
  - URL
  - MYSQL
  - MS SQL

Además, los nombres de estos identificadores no pueden ser los mismos que los nombres de las constantes de enumeración utilizadas en la infraestructura de directivas. Por ejemplo, el nombre de un identificador no puede ser IGNORECASE, YEAR o LATIN2_CZECH_CS (un conjunto de caracteres MySQL).

Nota: El dispositivo Citrix ADC realiza una comparación de identificadores sin distinción entre mayúsculas y minúsculas con estas palabras y constantes de enumeración. Por ejemplo, los nombres de los identificadores no pueden comenzar con TRUE, True o true.

Crear o modificar una directiva

August 20, 2021

Todas las directivas tienen algunos elementos comunes. La creación de una directiva consiste, como mínimo, en asignar un nombre a la directiva y configurar una regla. Las herramientas de configuración de directivas para las distintas entidades tienen áreas de superposición, pero también diferencias. Para obtener información detallada sobre la configuración de una directiva para una función concreta, incluida la asociación de una acción con la directiva, consulte la documentación de la función.

Para crear una directiva, comience por determinar el propósito de la directiva. Por ejemplo, puede que quiera definir una directiva que identifique las solicitudes HTTP para archivos de imagen o las solicitudes de cliente que contengan un certificado SSL. Además de conocer el tipo de información con la que quiere que funcione la directiva, necesita conocer el formato de los datos que está analizando la directiva.

A continuación, determine si la directiva es aplicable globalmente o si pertenece a un servidor virtual concreto. Considere también el efecto que tendrá en la directiva que está a punto de configurar el orden en el que se evalúan las directivas (que se determinará por la forma en que se vinculen las directivas).

Crear una directiva mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para crear una directiva y verificar la configuración:

```
- add responder|dns|cs|rewrite|cache policy <policyName> -rule <
   expression> [<feature-specific information>]

- show rewrite policy <name>
<!--NeedCopy-->
```

Ejemplo 1:

```
add rewrite policy "pol_remove-ae" true "act_remove-ae"
Done
> show rewrite policy pol_remove-ae
            Name: pol_remove-ae
            Rule: true
            RewriteAction: act_remove-ae
            UndefAction: Use Global
            Hits: 0
            Undef Hits: 0
            Bound to: GLOBAL RES_OVERRIDE
            Priority: 90
            GotoPriorityExpression: END
Done
<!--NeedCopy-->
```

Ejemplo 2:

```
add cache policy BranchReportsCachePolicy -rule q{
 http.req.url.query.value("actionoverride").contains("branchReport s")
    }
  -action cache
Done
```



```
show cache policy BranchReportsCachePolicy
            Name: BranchReportsCachePolicy
            Rule: http.req.url.query.value(”actionoverride”).contains(”
               branchReports”)
            CacheAction: CACHE
            Stored in group: DEFAULT
            UndefAction: Use Global
            Hits: 0
            Undef Hits: 0
Done
<!--NeedCopy-->
```

Nota: En la línea de comandos, las comillas dentro de una regla de directiva (la expresión) deben ser escapadas o delimitadas con el delimitador q. Para obtener más información, consulte Configurar expresiones de directivas avanzadas: Introducción.

Crear o modificar una directiva mediante la interfaz gráfica de usuario

1. En el panel de exploración, expanda el nombre de la función para la que quiere configurar una directiva y, a continuación, haga clic en **Directivas**. Por ejemplo, puede seleccionar **Cambio de contenido, Almacenamiento en caché integrado, DNS, Reescritura o Responder**.
2. En el panel de detalles, haga clic en **Agregar**o seleccione una directiva existente y haga clic en **Abrir**. Aparecerá un cuadro de diálogo de configuración de directivas.
3. Especifique valores para los siguientes parámetros. (Un asterisco indica un parámetro obligatorio. Para un término entre paréntesis, consulte el parámetro correspondiente en “Parámetros para crear o modificar una directiva.”)
4. Haga clic en **Crear** y, a continuación, en **Cerrar**.
5. Haga clic en **Guardar**. Se agrega una directiva.
   Nota: Después de crear una directiva, puede ver los detalles de la directiva haciendo clic en la entrada de directiva en el panel de configuración. Los detalles resaltados y subrayados son vínculos a la entidad correspondiente (por ejemplo, una expresión con nombre).

Ejemplos de configuración de directivas

August 20, 2021

Estos ejemplos muestran cómo se introducen las directivas y sus acciones asociadas en la interfaz de línea de comandos. En la utilidad de configuración, las expresiones aparecerían en la ventana Expresión del cuadro de diálogo de configuración de entidad para la función de almacenamiento en caché integrada o reescritura.

A continuación se muestra un ejemplo de creación de una directiva de almacenamiento en caché. Tenga en cuenta que las acciones para las directivas de almacenamiento en caché están integradas, por lo que no es necesario configurarlas por separado de la directiva.

```
1   add cache policy BranchReportsCachePolicy -rule q{
2  http.req.url.query.value("actionoverride").contains("branchReports") }
3   -action cache
4 <!--NeedCopy-->
```

A continuación se muestra un ejemplo de una directiva y acción de reescritura:

```
1  add rewrite action myAction1 INSERT_HTTP_HEADER "myHeader" "
      valueForMyHeader"
2  add rewrite policy myPolicy1 "http.req.url.contains("myURLstring")"
      myAction1
3 <!--NeedCopy-->
```

Nota: En la línea de comandos, las comillas dentro de una regla de directiva (la expresión) deben ser escapadas o delimitadas con el delimitador q. Para obtener más información, consulte Configurar expresiones de directivas avanzadas: Introducción.

Configurar y vincular directivas con el gestor de directivas

October 5, 2021

> **Advertencia:**
>
> Las expresiones de directiva clásicas ya no son compatibles con Citrix ADC 12.0, compilación 56.20 en adelante y, como alternativa, Citrix recomienda utilizar directivas avanzadas. Para obtener más información, consulte Directivas avanzadas.

Algunas aplicaciones proporcionan un Policy Manager especializado en la utilidad de configuración de Citrix ADC para simplificar la configuración de bancos de directivas. También le permite buscar y eliminar directivas y acciones que no se están usando.

Policy Manager está disponible actualmente para las funciones de reescritura, almacenamiento en caché integrado, respuesta y compresión.

Los siguientes son equivalentes de teclado para los procedimientos de esta sección:

- Para modificar una celda en el Administrador de directivas, puede utilizar el tabulador hasta la celda y hacer clic en F2 o pulsar la barra espaciadora del teclado.
- Para seleccionar una entrada en un menú desplegable, puede utilizar el tabulador hasta la entrada, pulsar la barra espaciadora para ver el menú desplegable, utilizar las teclas FLECHA ARRIBA y ABAJO para desplazarse hasta la entrada que quiera y volver a pulsar la barra espaciadora para seleccionarla.
- Para cancelar una selección en un menú desplegable, pulse la tecla Escape.
- Para insertar una directiva, vaya a la fila situada encima del punto de inserción y pulse Control + Insertar o haga clic en Insertar directiva.
- Para quitar una directiva, vaya a la fila que contiene la directiva y pulse Eliminar.

Nota: Tenga en cuenta que al eliminar la directiva, Citrix ADC busca los valores de Goto Expression de otras directivas del banco. Si alguno de estos valores de Goto Expression coincide con el nivel de prioridad de la directiva eliminada, se quitará.

Configurar enlaces de directivas mediante el gestor de directivas

1. En el panel de navegación, haga clic en la función para la que quiere configurar directivas. Las opciones son Responder, Almacenamiento en caché integrado, Reescritura o Compresión.
2. En el panel de detalles, haga clic en **Administrador de directivas**.
3. En cualquier momento antes de completar la configuración de los enlaces de directivas, si quiere configurar enlaces para directivas que utilizan la directiva avanzada, haga clic en el botón Cambiar a directiva avanzada.
4. Para funciones distintas de Responder, para especificar el punto de enlace, haga clic en Solicitud o Respuesta y, a continuación, haga clic en uno de los puntos de enlace de tiempo de solicitud o tiempo de respuesta. Las opciones son Sobrescribir global, Servidor virtual LB, Servidor virtual CS, Global predeterminado o Etiqueta de directiva. Si está configurando el Respondedor, los tipos de flujo Solicitud y Respuesta no están disponibles.
5. Para enlazar una directiva a este punto de enlace, haga clic en Insertar directiva y seleccione una directiva configurada previamente, una etiqueta NOPOLICY o la opción Nueva directiva. Dependiendo de la opción que seleccione, tiene las siguientes opciones:
   - **Nueva directiva:** cree la directiva como se describe en "Crear o modificar una directiva" y, a continuación, configure el nivel de prioridad, la expresión GoTo y la invocación de directivas como se describe en la tabla, "Formato de cada entrada de un banco de directivas. "
   - **Directiva existente**, **NOPOLICY** o `NOPOLICY\<feature name\>`: Configure el nivel de prioridad, la expresión GoTo y la invocación de directivas tal y como se describe en la tabla, "Formato de cada entrada de un banco de directivas". Las opciones **NOPOLICY** o

NOPOLICY\<feature name\> solo están disponibles para las directivas que utilizan directivas avanzadas.

6. Repita los pasos anteriores para agregar entradas a este banco de directivas.
7. Para modificar el nivel de prioridad de una entrada, puede realizar cualquiera de las siguientes acciones:

   - Haga doble clic en el campo Prioridad de una entrada y modifique el valor.
   - Haga clic y arrastre una directiva a otra fila de la tabla.
   - Haga clic en Regenerar prioridades.

   En los tres casos, los niveles de prioridad de todas las demás directivas se modifican según sea necesario para acomodar el nuevo valor. Las expresiones Goto con valores enteros también se actualizan automáticamente. Por ejemplo, si cambia un valor de prioridad de 10 a 100, todas las directivas con un valor Goto Expression de 10 se actualizan al valor 100.
8. Para cambiar la directiva, la acción o la invocación del banco de directivas de una fila de la tabla, haga clic en la flecha hacia abajo situada a la derecha de la entrada y realice una de las acciones siguientes:

   - Para cambiar la directiva, seleccione otro nombre de directiva o seleccione Nueva directiva y siga los pasos de Crear o modificar una directiva.
   - Para cambiar la expresión Ir a, seleccione Siguiente, Fin, USE_INVLATION_RESULT o seleccione más e introduzca una expresión cuyo resultado devuelva el nivel de prioridad de otra entrada en este banco de directivas.
   - Para modificar una invocación, seleccione un banco de directivas existente o haga clic en Nueva etiqueta de directiva y siga los pasos descritos en Vincular una directiva a una etiqueta de directiva.
9. Para desvincular una directiva o una invocación de etiqueta de directiva de este banco, haga clic en cualquier campo de la fila que contenga la directiva o etiqueta de directiva y, a continuación, haga clic en Desenlazar directiva.
10. Cuando hayas terminado, haga clic en Aplicar cambios. Un mensaje en la barra de estado indica que la directiva está enlazada correctamente.

Eliminar directivas no utilizadas mediante el gestor de directivas

1. En el panel de navegación, haga clic en la función para la que quiere configurar el banco de directivas. Las opciones son Responder, Almacenamiento en caché integrado o Reescritura.
2. En el panel de detalles, haga clic en administrador de directivas <Feature Name>.
3. En el cuadro de diálogo **Nombre de función** > **Administrador de directivas**r, haga clic en **Configuración de limpieza**.

4. En el cuadro de diálogo **Configuración de limpieza**, seleccione los elementos que quiera eliminar y, a continuación, haga clic en **Quitar**.
5. En el cuadro de diálogo Quitar, haga clic en **Sí**.
6. Haga clic en **Cerrar**. Un mensaje en la barra de estado indica que la directiva se ha quitado correctamente.

Desenlazar una directiva

August 20, 2021

Si quiere volver a asignar una directiva o eliminarla, primero debe eliminar su enlace.

Desenlazar globalmente una directiva avanzada integrada de almacenamiento en caché, reescritura o compresión mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para desenlazar una directiva avanzada integrada de almacenamiento en caché, reescritura o compresión globalmente y verificar la configuración:

```
- unbind cache|rewrite|cmp global <policyName> [-type req_override|
   req_default|res_override|res_default] [-priority <positiveInteger>]

- show cache|rewrite|cmp global
<!--NeedCopy-->
```

Ejemplo:

```
> unbind cache global_nonPostReq
Done
> show cache global
    1)      Global bindpoint: REQ_DEFAULT
            Number of bound policies: 1

    2)      Global bindpoint: RES_DEFAULT
            Number of bound policies: 1

Done
<!--NeedCopy-->
```


La prioridad solo es necesaria para la directiva “dummy” denominada NOPOLICY.

Desvincular una directiva de Responder globalmente mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para desvincular globalmente una directiva de respuesta y verificar la configuración:

```
1 - unbind responder global <policyName> [-type override|default] [-
    priority <positiveInteger>]
2
3 - show responder global
4 <!--NeedCopy-->
```

Ejemplo:

```
1 > unbind responder global pol404Error
2 Done
3 > show responder global
4     1)      Global bindpoint: REQ_DEFAULT
5             Number of bound policies: 1
6 Done
7 <!--NeedCopy-->
```

La prioridad solo es necesaria para la directiva “dummy” denominada NOPOLICY.

Desenlazar una directiva DNS globalmente mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para desvincular globalmente una directiva DNS y verificar la configuración:

```
1 - unbind responder global <policyName>
2
3 - unbind responder global
4 <!--NeedCopy-->
```

Ejemplo:


```
unbind dns global dfgdfg
Done
show dns global
    Policy name : dfgdfggfhg
            Priority : 100
            Goto expression : END
Done
<!--NeedCopy-->
```

Desenlazar una directiva avanzada de un servidor virtual mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para desenlazar una directiva avanzada de un servidor virtual y compruebe la configuración:

```
-  unbind cs vserver <name> -policyName <policyName> [-priority <
   positiveInteger>] [-type REQUEST|RESPONSE]

-  show lb vserver <name>
<!--NeedCopy-->
```

Ejemplo:

```
unbind cs vserver vs-cont-switch  -policyName pol1
Done
> show cs vserver vs-cont-switch
            vs-cont-switch (10.102.29.10:80) - HTTP Type: CONTENT
            State: UP
            Last state change was at Wed Aug 19 08:56:55 2009 (+18 ms)
            Time since last state change: 0 days, 02:47:55.750
            Client Idle Timeout: 180 sec
            Down state flush: ENABLED
            Disable Primary Vserver On Down : DISABLED
            Port Rewrite : DISABLED
            State Update: DISABLED
            Default:        Content Precedence: RULE
            Vserver IP and Port insertion: OFF
            Case Sensitivity: ON
            Push: DISABLED  Push VServer:
            Push Label Rule: none
Done
```



```
19 <!--NeedCopy-->
```

La prioridad solo es necesaria para la directiva “dummy” denominada NOPOLICY.

Desenlazar una directiva avanzada integrada de almacenamiento en caché, respuesta, reescritura o compresión mediante la interfaz gráfica de usuario

1. En el panel de navegación, haga clic en la función con la directiva que quiere desvincular (por ejemplo, Almacenamiento en caché integrado).
2. En el panel de detalles, haga clic en Administrador de directivas de <Feature Name>.
3. En el cuadro de diálogo **Administrador de directivas**, seleccione el punto de enlace con la directiva que quiere desenlazar, por ejemplo, Global avanzada.
4. Haga clic en el nombre de directiva que quiere desenlazar y, a continuación, haga clic en Desenlazar directiva.
5. Haga clic en **Aplicar cambios**.
6. Haga clic en **Cerrar**. Un mensaje en la barra de estado indica que la directiva no está enlazada correctamente.

Desenlazar una directiva DNS globalmente mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico** > **DNS** > **Directivas**.
2. En el panel de detalles, haga clic en **Vinculaciones globales**.
3. En el cuadro de diálogo **Enlaces globales**, seleccione directiva y haga clic en **Desvincular directiva**.
4. Haga clic en **Aceptar**. Un mensaje en la barra de estado indica que la directiva se ha desenlazado correctamente.

Desenlazar una directiva avanzada de un servidor virtual de equilibrio de carga o cambio de contenido mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico,** expanda Equilibrio de carga o Cambio de contenido y, a continuación, haga clic en **Servidores virtuales**.
2. En el panel de detalles, haga doble clic en el servidor virtual del que quiere desenlazar la directiva.
3. En la ficha **Directivas**, en la columna **Activo**, desactive la casilla de verificación situada junto a la directiva que quiere desvincular.
4. Haga clic en **Aceptar**. Un mensaje en la barra de estado indica que la directiva se ha desenlazado correctamente.

Crear etiquetas de directiva

August 20, 2021

Además de los puntos de enlace integrados en los que se configuran bancos de directivas, también puede configurar etiquetas de directivas definidas por el usuario y asociarlas.

Dentro de una etiqueta de directiva, se vinculan directivas y se especifica el orden de evaluación de cada directiva en relación con otras en el banco de directivas para la etiqueta de directiva. El dispositivo Citrix ADC también le permite definir un orden de evaluación arbitrario de la siguiente manera:

- Puede utilizar expresiones "goto" para apuntar a la siguiente entrada del banco que se evaluará después de la actual.
- Puede utilizar una entrada en un banco de directivas para invocar a otro banco.

Cada función determina el tipo de directiva que puede enlazar a una etiqueta de directiva, el tipo de servidor virtual de equilibrio de carga al que puede enlazar la etiqueta y el tipo de servidor virtual de conmutación de contenido desde el que se puede invocar la etiqueta. Por ejemplo, una etiqueta de directiva TCP solo puede enlazarse a un servidor virtual de equilibrio de carga TCP. No puede enlazar directivas HTTP a una etiqueta de directiva de este tipo. Y puede invocar una etiqueta de directiva TCP solo desde un servidor virtual de conmutación de contenido TCP.

Después de configurar una nueva etiqueta de directiva, puede invocarla desde uno o más bancos para los puntos de enlace integrados.

Crear una etiqueta de directiva de almacenamiento en caché mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para crear una etiqueta de directiva de almacenamiento en caché y compruebe la configuración:

```
1 -  add cache policylabel <labelName> -evaluates req|res
2
3 -  show cache policylabel<labelName>
4 <!--NeedCopy-->
```

Ejemplo:

```
1 > add cache policylabel lbl-cache-pol -evaluates req
2 Done
3
4 > show cache policylabel lbl-cache-pol
```



```
            Label Name: lbl-cache-pol
            Evaluates: REQ
            Number of bound policies: 0
            Number of times invoked: 0
Done
<!--NeedCopy-->
```

Crear una etiqueta de directiva de conmutación de contenido mediante la CLI

En el símbolo del sistema, escriba los comandos siguientes para crear una etiqueta de directiva Content Switching y compruebe la configuración:

```
-  add cs policylabel <labelName> http|tcp|rtsp|ssl

-  show cs policylabel <labelName>
<!--NeedCopy-->
```

Ejemplo:

```
> add cs policylabel lbl-cs-pol http
Done
> show cs policylabel lbl-cs-pol
            Label Name: lbl-cs-pol
            Label Type: HTTP
            Number of bound policies: 0
            Number of times invoked: 0
Done
<!--NeedCopy-->
```

Crear una etiqueta de directiva de reescritura mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para crear una etiqueta de directiva de reescritura y verificar la configuración:

```
-  add rewrite policylabel <labelName> http_req|http_res|url|text|
   clientless_vpn_req|clientless_vpn_res

-  show rewrite policylabel <labelName>
<!--NeedCopy-->
```


Ejemplo:

```
> add rewrite policylabel lbl-rewrt-pol http_req
Done

> show rewrite policylabel lbl-rewrt-pol
            Label Name: lbl-rewrt-pol
            Transform Name: http_req
            Number of bound policies: 0
            Number of times invoked: 0
Done
<!--NeedCopy-->
```

Crear una etiqueta de directiva de Responder mediante la CLI

En el símbolo del sistema, escriba los comandos siguientes para crear una etiqueta de directiva de Responder y compruebe la configuración:

```
-  add responder policylabel <labelName>

-  show responder policylabel <labelName>
<!--NeedCopy-->
```

Ejemplo:

```
> add responder policylabel lbl-respndr-pol
Done

> show responder policylabel lbl-respndr-pol
            Label Name: lbl-respndr-pol
            Number of bound policies: 0
            Number of times invoked: 0
Done
<!--NeedCopy-->
```

Nota: Invocar esta etiqueta de directiva desde un banco de directivas. Para obtener más información, consulte la sección “Vinculación de una directiva a una etiqueta de directiva”.

Crear una etiqueta de directiva mediante la interfaz gráfica de usuario

1. En el panel de exploración, expanda la función para la que quiere crear una etiqueta de directiva y, a continuación, haga clic en **Etiquetas de directiva**. Las opciones son Almacenamiento en caché integrado, Reescritura, Content Switching o Responder.
2. En el panel de detalles, haga clic en **Agregar**.
3. En el cuadro Nombre, escriba un nombre único para esta etiqueta de directiva.
4. Introduzca información específica de entidad para la etiqueta de directiva. Por ejemplo, para Almacenamiento en caché integrado, en el menú desplegable Evaluados, seleccione REQ si quiere que esta etiqueta de directiva contenga directivas de tiempo de solicitud, o seleccione RES si quiere que esta etiqueta de directiva contenga directivas de tiempo de respuesta. Para Reescribir, debe seleccionar un nombre de transformación.
5. Haga clic en **Crear**.
6. Configure uno de los bancos de directivas integrados para invocar esta etiqueta de directiva. Para obtener más información, consulte la sección "Vinculación de una directiva a una etiqueta de directiva". Un mensaje en la barra de estado indica que la etiqueta de directiva se ha creado correctamente.

Enlazar una directiva a una etiqueta de directiva

Al igual que con los bancos de directivas que están enlazados a los puntos de enlace integrados, cada entrada de una etiqueta de directiva es una directiva vinculada a la etiqueta de directiva. Al igual que con las directivas que están enlazadas globalmente o a un servidor virtual, cada directiva vinculada a la etiqueta de directiva también puede invocar un banco de directivas o una etiqueta de directiva que se evalúa después de procesar la entrada actual. En la tabla siguiente se resumen las entradas de una etiqueta de directiva.

- **Name**. El nombre de una directiva o, para invocar a otro banco de directivas sin evaluar una directiva, el nombre de directiva "ficticio" NOPOLICY.

  Puede especificar NOPOLICY más de una vez en un banco de directivas, pero solo puede especificar una directiva con nombre una vez.

- **Priority**. Un número entero. Esta configuración puede funcionar con la expresión GoTo.

- **Expresión GoTo**. Determina la siguiente directiva que se va a evaluar en este banco. Puede proporcionar uno de los siguientes valores:

  - **SIGUIENTE**. Vaya a la directiva con la siguiente prioridad más alta.
  - **FIN**. Detener la evaluación.
  - **USE_INVOCATION_RESULT**. Aplicable si esta entrada invoca otro banco de directivas. Si el GoTo final en el banco invocado tiene un valor de END, la evaluación se detiene. Si el GoTo final es algo distinto de END, el banco de directivas actual realiza un NEXT.

  - **Número positivo:** Número de prioridad de la próxima directiva que se va a evaluar.
  - **Expresión numérica**. Expresión que produce el número de prioridad de la siguiente directiva que se va a evaluar.

  El GoTo solo puede avanzar en un banco de directivas.

  Si omite la expresión GoTo, es lo mismo que especificar END.

- **Tipo de invocación**. Designa un tipo de banco de directivas. El valor puede ser uno de los siguientes:
  - **Solicitar Vserver**. Invoca las directivas de tiempo de solicitud asociadas a un servidor virtual.
  - **Servidor de respuesta**. Invoca directivas de tiempo de respuesta asociadas a un servidor virtual.
  - **Etiqueta de directiva**. Invoca otro banco de directivas, identificado por la etiqueta de directiva del banco.
- **Nombre de invocación**. Nombre de un servidor virtual o una etiqueta de directiva, según el valor especificado para el tipo de invocación.

Configurar una etiqueta de directiva o banco de directivas de servidor virtual

August 20, 2021

Después de crear directivas y crear bancos de directivas vinculando las directivas, puede realizar una configuración adicional de directivas dentro de una etiqueta o banco de directivas. Por ejemplo, antes de configurar la invocación de un banco de directivas externo, es posible que quiera esperar hasta que haya configurado ese banco de directivas.

Este tema incluye las siguientes secciones:

- Configurar una etiqueta de directiva
- Configurar un banco de directivas para un servidor virtual

Configurar una etiqueta de directiva

Una etiqueta de directiva consiste en un conjunto de directivas e invocaciones de otras etiquetas de directiva y bancos de directivas específicos de servidor virtual. Un parámetro Invoke permite invocar una etiqueta de directiva o un banco de directivas específico del servidor virtual desde cualquier otro banco de directivas. Una entrada NoPolicy de propósito especial le permite invocar un banco externo

sin procesar una expresión (una regla). La entrada NoPolicy es una directiva "ficticia" que no contiene una regla.

Para configurar etiquetas de directivas desde la línea de comandos de Citrix ADC, tenga en cuenta las siguientes elaboraciones de la sintaxis de comandos:

- GoToTriorityExpression se configura como se describe en la Tabla 2. Formato de cada entrada en un banco de directivas de la sección "Inscripciones en un banco de directivas" de directivas vinculadas mediante directivas avanzadas.
- El argumento type es obligatorio. Esto es a diferencia de vincular una directiva convencional, donde este argumento es opcional.
- Puede invocar el banco de directivas enlazadas a un servidor virtual mediante el mismo método que utiliza para invocar una etiqueta de directiva.

Configurar una etiqueta de directiva mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para configurar una etiqueta de directiva y verificar la configuración:

```
1 - bind cache|rewrite|responder policylabel <policylabelName> -
    policyName <policyName> -priority <priority> [-
    gotoPriorityExpression <gotoprioritыExpression>] [-invoke reqvserver
    |resvserver|policylabel <policyLabelName>|<vserverName>]
2
3 - show cache|rewrite|responder policylabel <policylabelName>
4 <!--NeedCopy-->
```

Ejemplo:

```
1  bind cache policylabel _reqBuiltinDefaults -policyName  _nonGetReq -
       priority 100
2  Done
3  show cache policylabel _reqBuiltinDefaults
4              Label Name: _reqBuiltinDefaults
5              Evaluates: REQ
6              Number of bound policies: 3
7              Number of times invoked: 0
8      1)      Policy Name: _nonGetReq
9              Priority: 100
10             GotoPriorityExpression: END
11     2)      Policy Name: _advancedConditionalReq
```



```
12              Priority: 200
13              GotoPriorityExpression: END
14
15      3)      Policy Name: _personalizedReq
16              Priority: 300
17              GotoPriorityExpression: END
18  Done
19  <!--NeedCopy-->
```

Invocar una etiqueta de directiva desde un banco de directivas de reescritura con una entrada NOPOLICY mediante la CLI

En el símbolo del sistema, escriba los comandos siguientes para invocar una etiqueta de directiva desde un banco de directivas de Rewrite con una entrada NOPOLICY y compruebe la configuración:

```
1  -  bind rewrite global <policyName> <priority> <gotoPriorityExpression>
       -type REQ_OVERRIDE|REQ_DEFAULT|RES_OVERRIDE|RES_DEFAULT -invoke
      reqvserver|resvserver|policylabel <policyLabelName>|<vserverName>
2
3  -  show rewrite global
4  <!--NeedCopy-->
```

Ejemplo:

```
1  > bind rewrite global NOPOLICY 100 -type REQ_DEFAULT -invoke
      policylabel lbl-rewrt-pol
2  Done
3  > show rewrite global
4      1)      Global bindpoint: REQ_DEFAULT
5              Number of bound policies: 1
6
7      2)      Global bindpoint: REQ_OVERRIDE
8              Number of bound policies: 1
9  Done
10 <!--NeedCopy-->
```


Invocar una etiqueta de directiva desde un banco de directivas de almacenamiento en caché integrado mediante la CLI

En el símbolo del sistema, escriba los comandos siguientes para invocar una etiqueta de directiva desde un banco de directivas de Almacenamiento en caché integrado y compruebe la configuración:

```
1 - bind cache global NOPOLICY -priority <priority> -
    gotoPriorityExpression <gotoprioritыExpression> -type REQ_OVERRIDE|
    REQ_DEFAULT|RES_OVERRIDE|RES_DEFAULT -invoke reqvserver|resvserver|
    policylabel <policyLabelName>|<vserverName>
2
3 - show cache global
4 <!--NeedCopy-->
```

Ejemplo:

```
1 bind cache global NOPOLICY -priority 100 -gotoPriorityExpression END -
    type REQ_DEFAULT -invoke policylabel lbl-cache-pol
2 Done
3 > show cache global
4     1)      Global bindpoint: REQ_DEFAULT
5             Number of bound policies: 2
6
7     2)      Global bindpoint: RES_DEFAULT
8             Number of bound policies: 1
9
10 Done
11 <!--NeedCopy-->
```

Invocar una etiqueta de directiva desde un banco de directivas de Responder mediante la CLI

En el símbolo del sistema, escriba los comandos siguientes para invocar una etiqueta de directiva desde un banco de directivas de respondedor y compruebe la configuración:

```
1 - bind responder global NOPOLICY <priority> <gotoprioritыExpression> -
    type OVERRIDE|DEFAULT -invoke vserver|policylabel <policyLabelName
    >|<vserverName>
2
3 - show responder global
4 <!--NeedCopy-->
```


Ejemplo:

```
> bind responder global NOPOLICY 100 NEXT -type DEFAULT -invoke
   policylabel lbl-respndr-pol
Done
> show responder global
    1)      Global bindpoint: REQ_DEFAULT
            Number of bound policies: 2

Done
<!--NeedCopy-->
```

Configurar una etiqueta de directiva mediante la interfaz gráfica de usuario

1. En el panel de exploración, expanda la función para la que quiere configurar una etiqueta de directiva y, a continuación, haga clic en Etiquetas de directiva. Las opciones son Almacenamiento en caché integrado, Reescritura o Responder.
2. En el panel de detalles, haga doble clic en la etiqueta que quiere configurar.
3. Si va a agregar una nueva directiva a esta etiqueta de directiva, haga clic en Insertar directiva y, en el campo Nombre de directiva, seleccione Nueva directiva. Para obtener más información sobre cómo agregar una directiva, consulte Crear o modificar una directiva. Tenga en cuenta que si está invocando un banco de directivas y no quiere que se evalúe una regla antes de la invocación, haga clic en Insertar directiva y, en el campo Nombre de directiva, seleccione NOPOLICY.
4. Para cada entrada de esta etiqueta de directiva, configure lo siguiente:
   - **Nombre de directiva:**

     Esto ya está determinado por el nombre de la directiva, la nueva directiva o la entrada NOPOLICY que insertó en este banco.
   - **Prioridad:**

     Valor numérico que determina un orden absoluto de evaluación dentro del banco o se utiliza junto con una expresión GoTo.
   - **Expresión:**

     La regla de directiva. Las expresiones de directiva se describen en detalle en los siguientes capítulos. Para obtener una introducción, consulte Configurar expresiones de directivas avanzadas: Introducción.

- **Acción:**

  La acción que se debe realizar si esta directiva se evalúa como TRUE.

- **Expresión GoTo:**

  Opcional. Se utiliza para aumentar el nivel de prioridad para determinar la siguiente directiva o banco de directivas que se va a evaluar. Para obtener más información sobre los posibles valores de una expresión GoTo, consulte la Tabla 2. Formato de cada entrada en un banco de directivas de la sección "Inscripciones en un banco de directivas" de directivas vinculadas mediante directivas avanzadas.

- **Invocar:**

  Opcional. Invoca otro banco de directivas.

5. Haga clic en **Aceptar**. Un mensaje en la barra de estado indica que la etiqueta de directiva se ha configurado correctamente.

Configurar un banco de directivas para un servidor virtual

Puede configurar un banco de directivas para un servidor virtual. El banco de directivas puede contener directivas individuales y cada entrada del banco de directivas puede invocar opcionalmente una etiqueta de directiva o un banco de directivas que haya configurado para otro servidor virtual. Si invoca una etiqueta de directiva o banco de directivas, puede hacerlo sin activar una expresión (una regla) seleccionando una entrada "ficticia" de NOPOLICY en lugar de un nombre de directiva.

Agregar directivas a un banco de directivas de servidor virtual mediante la CLI

En el símbolo del sistema, escriba los comandos siguientes para agregar directivas a un banco de directivas de servidor virtual y compruebe la configuración:

```
1 - bind lb|cs vserver <virtualServerName> <serviceType> [-policyName <
    policyName>] [-priority <positiveInteger>] [-gotoPriorityExpression
    <expression>] [-type REQUEST|RESPONSE]
2
3 - show lb|cs vserver <virtualServerName>
4 <!--NeedCopy-->
```

Ejemplo:

```
1 add lb vserver vs-cont-sw TCP
2 Done
```



```
show lb vserver vs-cont-sw
            vs-cont-sw (0.0.0.0:0) - TCP    Type: ADDRESS
            State: DOWN
            Last state change was at Wed Aug 19 10:04:02 2009 (+279 ms)
            Time since last state change: 0 days, 00:02:14.420
            Effective State: DOWN
            Client Idle Timeout: 9000 sec
            Down state flush: ENABLED
            Disable Primary Vserver On Down : DISABLED
            No. of Bound Services :  0 (Total)       0 (Active)
            Configured Method: LEASTCONNECTION
            Mode: IP
            Persistence: NONE
            Connection Failover: DISABLED
Done
<!--NeedCopy-->
```

Invocar una etiqueta de directiva desde un banco de directivas de servidor virtual con una entrada NOPOLICY mediante la CLI

En el símbolo del sistema, escriba los comandos siguientes para invocar una etiqueta de directiva desde un banco de directivas de servidor virtual con una entrada NOPOLICY y compruebe la configuración:

```
-  bind lb|cs vserver <virtualServerName> -policyName NOPOLICY-REWRITE|
   NOPOLICY-CACHE|NOPOLICY-RESPONDER -priority <integer> -type REQUEST|
   RESPONSE -gotoPriorityExpression <gotoprioritыExpression> -invoke
   reqVserver|resVserver|policyLabel <vserverName>|<labelName>

-  show lb vserver
<!--NeedCopy-->
```

Ejemplo:

```
> bind lb vserver vs-cont-sw -policyname NOPOLICY-REWRITE -priority 200
    -type REQUEST -gotoPriorityExpression NEXT -invoke policyLabel lbl-
   rewrt-pol
Done
<!--NeedCopy-->
```


Configurar un banco de directivas de servidor virtual mediante la interfaz gráfica de usuario

1. En el panel de navegación izquierdo, expanda ** **Traffic Management** > **Load Balancing, Traffic Management** > **Cambio de contenido, Traffic Management** > **SSL Offload, Security** > **AAA: Tráfico de aplicaciones**o **Citrix Gateway**, según corresponda y, a continuación, haga clic en **Servidores virtuales.**
2. En el panel de detalles, seleccione el servidor virtual que quiere configurar y, a continuación, haga clic en **Abrir**.
3. En el cuadro de diálogo **Configurar servidor virtual**, haga clic en la ficha **Directivas**.
4. Para crear una nueva directiva en este banco, haga clic en el icono correspondiente al tipo de directiva o etiqueta de directiva que quiere agregar al banco de directivas del servidor virtual, haga clic en **Insertar directiva**. Tenga en cuenta que si quiere invocar una etiqueta de directiva sin evaluar una regla de directiva, seleccione la directiva "ficticia" de NOPOLICY.
5. Para configurar una entrada existente en este banco de directivas, escriba lo siguiente:
   - **Prioridad:**

     Valor numérico que determina un orden absoluto de evaluación dentro del banco o se utiliza junto con una expresión GoTo.
   - **Expresión:**

     La regla de directiva. Las expresiones de directiva se describen en detalle en los siguientes capítulos. Para obtener una introducción, consulte Configuración de expresiones de directivas avanzadas: Introducción.
   - **Acción:**

     La acción que se debe realizar si esta directiva se evalúa como TRUE.
   - **Expresión GoTo:**

     Opcional. Determina la siguiente evaluación de directiva o banco de directivas. Para obtener más información sobre los valores posibles para una expresión Goto, consulte la sección "Entradas en un banco de directivas" en Vincular directivas mediante directivas avanzadas.
   - **Invocar:**

     Opcional. Para invocar a otro banco de directivas, seleccione el nombre de la etiqueta de directiva o banco de directivas del servidor virtual que quiere invocar.
6. Haga clic en **Aceptar**. Un mensaje en la barra de estado indica que la directiva se ha configurado correctamente.

Invocar o quitar una etiqueta de directiva o banco de directivas de servidor virtual

August 20, 2021

A diferencia de una directiva, que solo puede vincularse una vez, puede utilizar una etiqueta de directiva o un banco de directivas de un servidor virtual varias veces invocándola. La invocación se puede realizar desde dos lugares:

- Desde el enlace de una directiva con nombre en un banco de directivas.
- Desde el enlace para una entrada “ficticia” de NOPOLICY en un banco de directivas.

Normalmente, la etiqueta de directiva debe ser del mismo tipo que la directiva desde la que se invoca. Por ejemplo, podría invocar una etiqueta de directiva de Responder desde una directiva de Responder.

Nota: Al enlazar o desvincular una entrada NOPOLICY global en un banco de directivas en la línea de comandos, especifique una prioridad para distinguir una entrada NOPOLICY de otra.

Invocar una etiqueta de directiva de reescritura o almacenamiento en caché integrada mediante la CLI

En el símbolo del sistema, escriba uno de los siguientes comandos para invocar una etiqueta de directiva de reescritura o almacenamiento en caché integrada y verificar la configuración:

```
1 - bind cache global <policy> -priority <positive_integer> [-
    gotoPriorityExpression <expression>] -type REQ_OVERRIDE|REQ_DEFAULT|
    RES_OVERRIDE|RES_DEFAULT] -invoke reqvserver|resvserver|policylabel
    <label_name>
2
3 - bind rewrite global<policy> -priority <positive_integer> [-
    gotoPriorityExpression <expression>] -type REQ_OVERRIDE|REQ_DEFAULT|
    RES_OVERRIDE|RES_DEFAULT] -invoke reqvserver|resvserver|policylabel
    <label_name>
4
5 - show cache global|show rewrite global
6 <!--NeedCopy-->
```

Ejemplo:


```
> bind cache global _nonPostReq2 -priority 100 -type req_override -
    invoke
     policylabel lbl-cache-pol
Done
> show cache global
     1)      Global bindpoint: REQ_DEFAULT
             Number of bound policies: 2

     2)      Global bindpoint: RES_DEFAULT
             Number of bound policies: 1

     3)      Global bindpoint: REQ_OVERRIDE
             Number of bound policies: 1

Done
<!--NeedCopy-->
```

Invocar una etiqueta de directiva de Responder mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para invocar una etiqueta de directiva de respuesta y verificar la configuración:

```
-  bind responder global <policy_Name> <priority_as_positive_integer>
    [<gotoPriorityExpression>] -type REQ_OVERRIDE|REQ_DEFAULT|OVERRIDE|
    DEFAULT -invoke vserver|policylabel <label_name>

-  show responder global
<!--NeedCopy-->
```

Ejemplo:

```
> bind responder global pol404Error1 300 -invoke policylabel lbl-
    respndr-pol
Done
> show responder global
     1)      Global bindpoint: REQ_DEFAULT
             Number of bound policies: 2

Done
<!--NeedCopy-->
```


Invocar un banco de directivas de servidor virtual mediante la CLI

En el símbolo del sistema, escriba los comandos siguientes para invocar un banco de directivas de servidor virtual y compruebe la configuración:

```
-  bind lb vserver <vserver_name> -policyName <policy_Name> -priority <
   positive_integer> [-gotoPriorityExpression <expression>] -type
   REQUEST|RESPONSE -invoke reqvserver|resvserver|policylabel <
   policy_Label_Name>

-  bind lb vserver <vserver_name>
<!--NeedCopy-->
```

Ejemplo:

```
> bind lb vserver lbvip -policyName ns_cmp_msapp -priority 100
Done

> show lb vserver lbvip
            lbvip (8.7.6.6:80) - HTTP       Type: ADDRESS
            State: DOWN
            Last state change was at Wed Jul 15 05:54:24 2009 (+166 ms)
            Time since last state change: 28 days, 06:37:49.250
            Effective State: DOWN
            Client Idle Timeout: 180 sec
            Down state flush: ENABLED
            Disable Primary Vserver On Down : DISABLED
            Port Rewrite : DISABLED
            No. of Bound Services :  0 (Total)       0 (Active)
            Configured Method: LEASTCONNECTION
            Mode: IP
            Persistence: NONE
            Vserver IP and Port insertion: OFF
            Push: DISABLED  Push VServer:
            Push Multi Clients: NO
            Push Label Rule: none

    1)      CSPolicy: pol-cont-sw   CSVserver: vs-cont-sw   Priority:
        100   Hits: 0

    2)      Policy : pol-ssl Priority:0
    3)      Policy : ns_cmp_msapp Priority:100
```



```
27      4)      Policy : cf-pol Priority:1      Inherited
28  Done
29  <!--NeedCopy-->
```

Quitar una etiqueta de directiva de reescritura o almacenamiento en caché integrada mediante la CLI

En el símbolo del sistema, escriba uno de los siguientes comandos para quitar una etiqueta de directiva de reescritura o almacenamiento en caché integrada y verificar la configuración:

```
1  -  unbind rewrite global <policyName> -priority <positiveInteger> -type
       REQ_OVERRIDE|REQ_DEFAULT|RES_OVERRIDE|RES_DEFAULT
2
3  -  unbind cache global <policyName> -priority <positiveInteger> -type
      REQ_OVERRIDE|REQ_DEFAULT|RES_OVERRIDE|RES_DEFAULT
4
5  -  show rewrite global|show cache global
6  <!--NeedCopy-->
```

Ejemplo:

```
1  > unbind rewrite global NOPOLICY -priority 100 -type REQ_OVERRIDE
2  > show rewrite global
3  Done
4      1)      Global bindpoint: REQ_DEFAULT
5              Number of bound policies: 1
6
7  Done
8  <!--NeedCopy-->
```

Quitar una etiqueta de directiva de Responder mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para quitar una etiqueta de directiva de respuesta y verificar la configuración:

```
1  -  unbind responder global <policyName> -priority <positiveInteger> -
      type OVERRIDE|DEFAULT
2
```



```
3 -  show responder global
4 <!--NeedCopy-->
```

Ejemplo:

```
1 > unbind responder global NOPOLICY -priority 100 -type REQ_DEFAULT
2 Done
3 > show responder global
4     1)      Global bindpoint: REQ_DEFAULT
5             Number of bound policies: 1
6
7 Done
8 <!--NeedCopy-->
```

Quitar una etiqueta de directiva de servidor virtual mediante la CLI

En el símbolo del sistema, escriba uno de los siguientes comandos para quitar una etiqueta de directiva de servidor virtual y comprobar la configuración:

```
1 -  unbind lb vserver <virtualServerName> -policyName NOPOLICY-REWRITE|
     NOPOLICY-RESPONDER|NOPOLICY-CACHE -type REQUEST|RESPONSE -priority <
     positiveInteger>
2
3 -  unbind cs vserver <virtualServerName> -policyName NOPOLICY-REWRITE|
     NOPOLICY-RESPONDER|NOPOLICY-CACHE -type REQUEST|RESPONSE -priority <
     positiveInteger>
4
5 -  show lb vserver|show cs vserver
6 <!--NeedCopy-->
```

Ejemplo:

```
1 > unbind lb vserver lbvip -policyName ns_cmp_msapp -priority 200
2 Done
3 > show lb vserver lbvip
4             lbvip (8.7.6.6:80) - HTTP       Type: ADDRESS
5             State: DOWN
6             Last state change was at Wed Jul 15 05:54:24 2009 (+161 ms)
7             Time since last state change: 28 days, 06:47:54.600
```



```
8               Effective State: DOWN
9               Client Idle Timeout: 180 sec
10              Down state flush: ENABLED
11              Disable Primary Vserver On Down : DISABLED
12              Port Rewrite : DISABLED
13              No. of Bound Services :  0 (Total)       0 (Active)
14              Configured Method: LEASTCONNECTION
15              Mode: IP
16              Persistence: NONE
17              Vserver IP and Port insertion: OFF
18              Push: DISABLED  Push VServer:
19              Push Multi Clients: NO
20              Push Label Rule: none
21
22      1)      CSPolicy: pol-cont-sw   CSVserver: vs-cont-sw   Priority:
            100   Hits: 0
23
24      1)      Policy : pol-ssl Priority:0
25      2)      Policy : cf-pol Priority:1      Inherited
26  Done
27  <!--NeedCopy-->
```

Invocar una etiqueta de directiva o banco de directivas de servidor virtual mediante la interfaz gráfica de usuario

1. Vincular una directiva, como se describe en Vincular una directiva globalmente, Vincular una directiva a un servidor virtualo Vincular una directiva a una etiqueta de directiva. Alternativamente, puede introducir una entrada “dummy” de NOPOLICY en lugar de un nombre de directiva. Puede hacerlo si no quiere evaluar una directiva antes de evaluar el banco de directivas.
2. En el campo Invocar, seleccione el nombre de la etiqueta de directiva o del banco de directivas del servidor virtual que quiere evaluar si el tráfico coincide con la directiva enlazada. Un mensaje en la barra de estado indica que la etiqueta de directiva o el banco de directivas del servidor virtual se invoca correctamente.

Quitar una invocación de etiqueta de directiva mediante la interfaz gráfica de usuario

1. Abra la directiva y desactive el campo Invocar. Al desvincular la directiva también se elimina la invocación de la etiqueta. Un mensaje en la barra de estado indica que la etiqueta de directiva se ha quitado correctamente.

Configuración de la expresión de directiva avanzada: Introducción

January 12, 2021

Las directivas avanzadas evalúan los datos en función de la información proporcionada en Expresiones de directivas avanzadas. Una expresión de directiva avanzada analiza los elementos de datos (por ejemplo, encabezados HTTP, direcciones IP de origen, la hora del sistema Citrix ADC y los datos del cuerpo POST). Además de configurar una expresión de directiva avanzada en una directiva, en algunas funciones de Citrix ADC, puede configurar la expresión de directiva avanzada fuera del contexto de una directiva.

Para crear una expresión de directiva avanzada, seleccione un prefijo que identifique una parte de datos que quiere analizar y, a continuación, especifique una operación para realizar en los datos. Por ejemplo, una operación puede hacer coincidir un fragmento de datos con una cadena de texto que especifique, o puede transformar una cadena de texto en un encabezado HTTP. Otras operaciones coinciden con una cadena devuelta con un conjunto de cadenas o un patrón de cadenas. Las expresiones compuestas se configuran especificando operadores booleanos y aritméticos y mediante paréntesis para controlar el orden de evaluación.

La expresión de directiva avanzada también puede contener expresiones clásicas. Puede asignar un nombre a una expresión utilizada con frecuencia para evitar tener que crear la expresión repetidamente.

Las directivas y algunas otras entidades incluyen reglas que el dispositivo Citrix ADC utiliza para evaluar un paquete en el tráfico que fluye a través de él, extraer datos del propio sistema Citrix ADC, enviar una solicitud (una "llamada") a una aplicación externa o analizar otro dato. Una regla adopta la forma de una expresión lógica que se compara con el tráfico y, en última instancia, devuelve valores de TRUE o FALSE.

Los elementos de la regla pueden devolver valores TRUE o FALSE, cadena o numéricos.

Antes de configurar una expresión de directiva avanzada, debe comprender las funciones de los datos que la directiva u otra entidad debe evaluar. Por ejemplo, cuando se trabaja con la función Almacenamiento en caché integrado, una directiva determina qué datos se pueden almacenar en la caché. Con el Almacenamiento en caché integrado, necesita conocer las direcciones URL, encabezados y otros datos en las solicitudes y respuestas HTTP que recibe Citrix ADC. Con este conocimiento, puede configurar directivas que coincidan con los datos reales y habilitar Citrix ADC para administrar el almacenamiento en caché para el tráfico HTTP. Esta información le ayuda a determinar el tipo de expresión que necesita configurar en la directiva.

Elementos básicos de una expresión de directiva avanzada

August 20, 2021

Una expresión de directiva avanzada consiste, como mínimo, en un prefijo (o un único elemento utilizado en lugar de un prefijo). La mayoría de las expresiones también especifican una operación que se realizará en los datos que identifica el prefijo. Dar formato a una expresión de hasta 1.499 caracteres de la siguiente manera:

```
<prefix>.<operation> [<compound-operator> <prefix>.<operation>. . .]
```

donde

- <prefix>

  es un punto de anclaje para iniciar una expresión.

  El prefijo es una clave delimitada por períodos que identifica una unidad de datos. Por ejemplo, el prefijo siguiente examina las solicitudes HTTP para la presencia de un encabezado denominado Content-Type:

  http.req.header (“Tipo de contenido”)

  Los prefijos también se pueden usar por sí mismos para devolver el valor del objeto que el prefijo identifica.

- <operation>

  identifica una evaluación que se va a realizar en los datos identificados por el prefijo.

  Por ejemplo, considere la siguiente expresión:

  http.req.header (“Tipo de contenido”).eq (“text/html”)

  En esta expresión, el siguiente es el componente del operador:

  eq (“texto/html”)

  Este operador hace que Citrix ADC evalúe cualquier solicitud HTTP que contenga un encabezado Content-Type y, en particular, determine si el valor de este encabezado es igual a la cadena “text/html”. Para obtener más información, consulte “Operaciones. “

- <compound-operator>

  es un operador booleano o aritmético que forma una expresión compuesta a partir de varios elementos de prefijo o prefijo.operation.

  Por ejemplo, considere la siguiente expresión:

  http.req.header(“Content-Type”).eq(“text/html”) && http.req.url.contains(“.html”)

Prefijos

Un prefijo de expresión representa una parte discreta de datos. Por ejemplo, un prefijo de expresión puede representar una dirección URL HTTP, un encabezado HTTP Cookie o una cadena en el cuerpo de una solicitud HTTP POST. Un prefijo de expresión puede identificar y devolver una amplia variedad de tipos de datos, incluidos los siguientes:

- Una dirección IP de cliente en un paquete TCP/IP
- Hora del sistema Citrix ADC
- Una llamada externa sobre HTTP
- Un tipo de registro TCP o UDP

En la mayoría de los casos, un prefijo de expresión comienza con una de las siguientes palabras clave:

- CLIENTE:
  - Identifica una función del cliente que está enviando una solicitud o recibiendo una respuesta, como en los siguientes ejemplos:
  - El prefijo client.ip.dst designa la dirección IP de destino en la solicitud o respuesta.
  - El prefijo client.ip.src designa la dirección IP de origen.
- HTTP:
  - Identifica un elemento en una solicitud HTTP o una respuesta, como en los siguientes ejemplos:
  - El prefijo http.req.body (integer) designa el cuerpo de la solicitud HTTP como un objeto de texto de líneas múltiples, hasta la posición de carácter designada en entero.
  - El prefijo http.req.header (“header_name”) designa un encabezado HTTP, como se especifica en header_name.
  - El prefijo http.req.url designa una URL HTTP en formato codificado en URL.
- SERVIDOR:

  Identifica un elemento del servidor que está procesando una solicitud o enviando una respuesta.
- SYS:

  Identifica una función del dispositivo Citrix ADC que está procesando el tráfico.

  Nota: Tenga en cuenta que las directivas DNS solo admiten objetos SYS, CLIENT y SERVER.

  Además, en Citrix Gateway, la función VPN sin cliente puede usar los siguientes tipos de prefijos:
- TEXTO:

  Identifica cualquier elemento de texto en una solicitud o respuesta.
- OBJETIVO:

  Identifica el destino de una conexión.

- URL:

  Identifica un elemento en la parte URL de una solicitud o respuesta HTTP.

Como regla general, cualquier prefijo de expresión puede ser una expresión autónoma. Por ejemplo, el prefijo siguiente es una expresión completa que devuelve el contenido del encabezado HTTP especificado en el argumento de cadena (entre comillas):

```
http.res.header.("myheader")
```

O puede combinar prefijos con operaciones simples para determinar los valores TRUE y FALSE. Por ejemplo, lo siguiente devuelve un valor TRUE o FALSE:

```
http.res.header.("myheader").exists
```

También puede utilizar operaciones complejas en prefijos individuales y varios prefijos dentro de una expresión, como en el ejemplo siguiente:

```
http.req.url.length + http.req.cookie.length <= 500
```

Los prefijos de expresión que se pueden especificar dependen de la función Citrix ADC. En la tabla siguiente se describen los prefijos de expresión que son de interés por entidad

Función	Tipos de prefijo de expresión utilizados en la entidad
DNS	SYS, CLIENTE, SERVIDOR
Responder en funciones de protección	HTTP, SYS, CLIENT
Conmutación de contenido	HTTP, SYS, CLIENT
Reescribe	HTTP, SYS, CLIENT, SERVER, URL, TEXT, TARGET, VPN
Almacenamiento en caché integrado	HTTP, SYS, CLIENTE, SERVIDOR
Citrix Gateway, acceso sin cliente	HTTP, SYS, CLIENT, SERVER, URL, TEXT, TARGET, VPN

Cuadro 1 Tipos permitidos de prefijos de expresión en varias funciones de Citrix ADC

Nota: Para obtener más información sobre los prefijos de expresión permitidos en una función, consulte la documentación de esa función.

Expresiones de un solo elemento

El tipo más simple de expresión de directiva avanzada contiene un único elemento. Este elemento puede ser uno de los siguientes:

- Es true. Una expresión de directiva avanzada puede consistir simplemente en el valor verdadero. Este tipo de expresión siempre devuelve un valor TRUE. Es útil para encadenar acciones de directiva y activar expresiones GoTo.
- Falsa. Una expresión de directiva avanzada puede consistir simplemente en el valor false. Este tipo de expresión siempre devuelve un valor de FALSE.
- Prefijo para una expresión compuesta. Por ejemplo, el prefijo HTTP.REQ.HOSTNAME es una expresión completa que devuelve un nombre de host y HTTP.REQ.URL es una expresión completa que devuelve una dirección URL. El prefijo también se puede utilizar junto con operaciones y prefijos adicionales para formar una expresión compuesta.

Operaciones

En la mayoría de las expresiones, también se especifica una operación en los datos que identifica el prefijo. Por ejemplo, supongamos que especifica el prefijo siguiente:

```
http.req.url
```

Este prefijo extrae las URL en las solicitudes HTTP. Este prefijo de expresión no requiere que se utilice ningún operador en una expresión. Sin embargo, al configurar una expresión que procesa direcciones URL de solicitud HTTP, puede especificar operaciones que analicen funciones particulares de la dirección URL. A continuación se presentan algunas posibilidades:

- Busque un nombre de host concreto en la URL.
- Busque una ruta en particular en la URL.
- Evalúe la longitud de la URL.
- Busque una cadena en la URL que indique una marca de tiempo y conviértala a GMT.

A continuación se muestra un ejemplo de un prefijo que identifica un encabezado HTTP denominado Servidor y una operación que busca la cadena IIS en el valor del encabezado:

```
http.res.header("Server").contains("IIS")
```

A continuación se muestra un ejemplo de un prefijo que identifica nombres de host y una operación que busca la cadena “www.mycompany.com” como el valor del nombre:

```
http.req.hostname.eq("www.mycompany.com")
```

Operaciones básicas en prefijos de expresión

En la tabla siguiente se describen algunas de las operaciones básicas que se pueden realizar en prefijos de expresión.

Operación	Determina si o no
CONTIENE (<string>)	El objeto coincide <string>. A continuación se presenta un ejemplo: Http.req.header (“Cache-Control”).contains (“no-cache”)
EXISTE	Un elemento en particular está presente en un objeto. Lo que sigue es un ejemplo: Http.res.header (“MyHDR”).exists
EQ (<text>)	Un valor no numérico determinado está presente en un objeto. Lo que sigue es un ejemplo: Http.req.method.eq (post)
EQ (<integer>)	Un valor numérico determinado está presente en un objeto. A continuación se presenta un ejemplo: Client.ip.dst.eq (10.100.10.100)
LT (<integer>)	El valor de un objeto es menor que un valor determinado. A continuación se presenta un ejemplo: Http.req.content_length.lt (5000)
GT (<integer>)	El valor de un objeto es mayor que un valor determinado. Lo que sigue es un ejemplo: Http.req.content_length.gt (5)

En la siguiente tabla se resumen algunos de los tipos de operaciones disponibles.

Tipo de operación	Descripción
Operaciones de texto	Coincide cadenas individuales y conjuntos de cadenas con cualquier parte de un destino. El destino puede ser una cadena completa, el inicio de una cadena o cualquier parte de texto entre el inicio y el final de la cadena. Por ejemplo, puede extraer la cadena “XYZ” de “XYZSOMEText”. O bien, puede comparar un valor de encabezado HTTP con una matriz de cadenas diferentes. También puede transformar texto en otro tipo de datos. Los siguientes son ejemplos: Transformar una cadena en un valor entero, crear una lista a partir de las cadenas de consulta en una URL, y transformar una cadena en un valor de tiempo.
Operaciones numéricas	Las operaciones numéricas incluyen la aplicación de operadores aritméticos, la evaluación de la longitud del contenido, el número de elementos de una lista, fechas, horas y direcciones IP.

Expresiones de directiva avanzadas compuestas

October 5, 2021

Puede configurar una expresión de directiva avanzada con operadores booleanos o aritméticos y operaciones atómicas. La siguiente expresión compuesta tiene AND booleano:

```
http.req.hostname.eq(”mycompany.com”)&& http.req.method.eq(post)
```

La siguiente expresión agrega el valor de dos destinos y compara el resultado con un tercer valor:

```
http.req.url.length + http.req.cookie.length \<= 500
```

Una expresión compuesta puede tener cualquier número de operadores lógicos y aritméticos.

La siguiente expresión evalúa la duración de una solicitud HTTP. Esta expresión se basa en la URL y la cookie.
Esta expresión evalúa el texto del encabezado. Además, hace un AND booleano en estos dos resultados:


```
http.req.url.length + http.req.cookie.length \<= 500 && http.req.header.
contains("some text")
```

Puede utilizar paréntesis para controlar el orden de evaluación en una expresión compuesta.

Booleanos en expresiones compuestas

Las expresiones compuestas se configuran con los siguientes operadores:

- &&.

  Este operador es un AND lógico. Para que la expresión se evalúe como TRUE, todos los componentes deben evaluarse como TRUE.

  Ejemplo:

  http.req.url.hostname.eq ("MiHost") && http.req.header ("MiHeader").existe

.

- Este operador es un OR lógico. Si algún componente de la expresión se evalúa como TRUE, toda la expresión es TRUE.
- !.

  P No es lógico en la expresión.

A veces, la utilidad de configuración Citrix ADC ofrece operadores AND, NOT y OR en el cuadro de diálogo **Agregar expresión** . Sin embargo, estas expresiones compuestas son de uso limitado. Citrix recomienda utilizar los operadores &&,	y! Para configurar expresiones compuestas que utilizan lógica booleana.

Paréntesis en expresiones compuestas

Puede utilizar paréntesis para controlar el orden de evaluación de una expresión. A continuación, se muestra un ejemplo:

```
http.req.url.contains("myCompany.com")|| (http.req.url.hostname.eq("myHost"
```



```
)&& http.req.header("myHeader").exists)
```

El siguiente es otro ejemplo:

```
(http.req.header("Content-Type").exists && http.req.header("Content-Type").
eq("text/html"))|| (http.req.header("Transfer-Encoding").exists || http.req
.header("Content-Length").exists)
```

Operaciones compuestas para cuerdas

En la tabla siguiente se describen los operadores que se pueden utilizar para configurar operaciones compuestas en datos de cadena.

Operaciones que producen un valor de cadena	Descripción
str + str	Concatena el valor de la expresión a la izquierda del operador con el valor a la derecha. Ejemplo: http.req.hostname + http.req.url.protocol
str + núm	Concatena el valor de la expresión a la izquierda del operador con un valor numérico a la derecha. Ejemplo: http.req.hostname + http.req.url.content_length
núm + str	Concatena el valor numérico de la expresión en el lado izquierdo del operador con un valor de cadena a la derecha. Ejemplo: http.req.url.content_length + http.req.url.hostname
str + ip	Concatena el valor de cadena de la expresión en el lado izquierdo del operador con un valor de dirección IP a la derecha. Ejemplo: http.req.hostname + 10.00.000.00
IP + str	Concatena el valor de la dirección IP de la expresión de la izquierda del operador con un valor de cadena a la derecha. Ejemplo: client.ip.dst + http.req.url.hostname

Operaciones que producen un valor de cadena	Descripción
str1 ALT str2	Utiliza cadena2 si la evaluación de cadena1 da como resultado una excepción undef o el resultado es una cadena nula. De lo contrario, usa cadena1 y nunca evalúa cadena2. Ejemplo: http.req.hostname alt client.ip.src

Operaciones en cadenas que producen un resultado de TRUE o FALSE	Descripción
str == str	Evalúa si las cadenas de ambos lados del operador son las mismas. A continuación se muestra un ejemplo: http.req.header (“myheader”) == http.res.header (“myheader”)
str <= str	Evalúa si la cadena del lado izquierdo del operador es la misma que la cadena de la derecha o la precede alfabéticamente.
str >= str	Evalúa si la cadena del lado izquierdo del operador es la misma que la cadena de la derecha o la sigue alfabéticamente.
str < str	Evalúa si la cadena del lado izquierdo del operador precede alfabéticamente a la cadena de la derecha.
str > str	Evalúa si la cadena del lado izquierdo del operador sigue alfabéticamente a la cadena de la derecha.
str!! = str	Evalúa si las cadenas a ambos lados del operador son diferentes.

Operaciones lógicas en cadenas	Descripción
libro y libro	Este operador es un AND lógico. Al evaluar los componentes de la expresión compuesta, todos los componentes que están unidos por AND deben evaluarse como VERDADERO. A continuación se muestra un ejemplo: http.req.method.e (GET) && http.req.url.query. (“viewReport && my_pagelabel”)

Operaciones lógicas en cadenas	Descripción		
bool	bool	Este operador es un OR lógico. Al evaluar los componentes de la expresión compuesta, si algún componente de la expresión perteneciente a OR se evalúa como TRUE, toda la expresión es TRUE. A continuación se muestra un ejemplo: http.req.url.contains (“.js”)	http.res.header. (“Tipo de contenido”). Contiene (“javascript”)
Bool	Realiza un NO lógico en la expresión.		

Operaciones compuestas para números

Puede configurar expresiones numéricas compuestas. Por ejemplo, la siguiente expresión devuelve un valor numérico que es la suma de una longitud de encabezado HTTP y una longitud de URL:

```
http.req.header.length + http.req.url.length
```

En las tablas siguientes se describen los operadores que se pueden utilizar para configurar expresiones compuestas para datos numéricos.

Operaciones aritméticas en números	Descripción
núm_+ núm	Agregue el valor de la expresión de la izquierda del operador al valor de la expresión de la derecha. A continuación se muestra un ejemplo: http.req.content_l + http.req.url.length
num: Num	Reste el valor de la expresión de la derecha del operador del valor de la expresión de la izquierda.
num*num	Multiplica el valor de la expresión de la izquierda del operador por el valor de la expresión de la derecha. A continuación se muestra un ejemplo: client.interface.rxt 9

Operaciones aritméticas en números	Descripción
núm/núm	Divida el valor de la expresión de la izquierda del operador por el valor de la expresión de la derecha.
número% núm	Calcule el módulo, o el resto numérico en una división del valor de la expresión a la izquierda del operador por el valor de la expresión a la derecha. Por ejemplo, los valores “15 mod 4” son iguales a 3 y “12 mod 4” equivalen a 0.

Operaciones aritméticas en números	Descripción
~número	Devuelve un número después de aplicar una negación lógica bit a bit del número. En el siguiente ejemplo se supone que numeric.expression devuelve 12 (binario 1100): ~numeric.expression. El resultado de aplicar el operador ~ es -11 (un binario 1110011, 32 bits totales con todos a la izquierda). Tenga en cuenta que todos los valores devueltos de menos de 32 bits antes de aplicar el operador tienen ceros implícitamente a la izquierda para que tengan 32 bits de ancho.

Operaciones aritméticas en números	Descripción
número ^ número	Compara dos patrones de bits de igual longitud y realiza una operación XOR en cada par de bits correspondientes en cada argumento numérico, devolviendo 1 si los bits son diferentes y 0 si son iguales. Devuelve un número después de aplicar una XOR bit a bit al argumento entero y al valor numérico actual. Si los valores de la comparación bit a bit son los mismos, el valor devuelto es 0. En el ejemplo siguiente se supone que numeric.expression1 devuelve 12 (binario 1100) y numeric.expression2 devuelve 10 (binario 1010): Numeric.expression1 ^ numeric.expresión2E resultado de aplicar el

Operaciones aritméticas en números	Descripción			
número	número	Devuelve un número después de aplicar un OR bit a bit a los valores numéricos. Si cualquiera de los valores de la comparación bit a bit es 1, el valor devuelto es 1. En el ejemplo siguiente se supone que numeric.expression1 devuelve 12 (binario 1100) y numeric.expression2 devuelve 10 (binario 1010): Numeric.expression1	numeric.expression2 El resultado de aplicar el operador	a toda la expresión es 14 (binario 1110). Tenga en cuenta que todos los valores devueltos de menos de 32 bits antes de aplicar el operador tienen ceros implícitamente a la izquierda para que tengan 32 bits de ancho.

Operaciones aritméticas en números	Descripción
número & número	Compara dos patrones de bits de igual longitud y realiza una operación AND a bit en cada par de bits correspondientes, devolviendo 1 si ambos bits contienen un valor de 1 y 0 si cualquiera de los bits es 0. En el ejemplo siguiente se supone que numeric.expression1 devuelve 12 (binario 1100) y numeric.expression2 devuelve 10 (binario 1010): Numeric.expression1 & numeric.expression2 La expresión completa se evalúa como 8 (binario 1000). Tenga en cuenta que todos los valores devueltos de menos de 32 bits antes de aplicar el operador tienen ceros implícitamente a la izquierda para

Operaciones aritméticas en números	Descripción
núm « núm	Devuelve un número después de un desplazamiento a la izquierda bit a bit del valor numérico por el número de argumento de bits del lado derecho. Tenga en cuenta que el número de bits desplazados es el módulo entero 32. En el siguiente ejemplo se supone que numeric.expression1 devuelve 12 (binario 1100) y numeric.expression2 devuelve 3: numeric.expression1 « numeric.expression2 El resultado de aplicar el operador LSHIFT es 96 (un binario 1100000) .Tenga en cuenta que todos los valores devueltos de menos de 32 bits antes de aplicar el operador tienen ceros implícitamente a la izquierda para

Operaciones aritméticas en números	Descripción
núm » núm	Devuelve un número después de un desplazamiento a la derecha a bit del valor numérico por el número de argumento entero de bits. Tenga en cuenta que el número de bits desplazados es el módulo entero 32. En el ejemplo siguiente se supone que numeric.expression1 devuelve 12 (binario 1100) y numeric.expression2 devuelve 3: Numeric.expression1 numeric.expression2 El resultado de aplicar el operador RSHIFT es 1 (un binario 0001). Tenga en cuenta que todos los valores devueltos de menos de 32 bits antes de aplicar el operador tienen ceros implícitamente a

Operaciones aritméticas en números	Descripción

Operadores numéricos que producen un resultado de TRUE o FALSE	Descripción
num == num	Determine si el valor de la expresión a la izquierda del operador es igual al valor de la expresión a la derecha.
num! = num	Determina si el valor de la expresión de la izquierda del operador no es igual al valor de la expresión de la derecha.
num > num	Determina si el valor de la expresión de la izquierda del operador es mayor que el valor de la expresión de la derecha.
num < num	Determina si el valor de la expresión de la izquierda del operador es inferior al valor de la expresión de la derecha.
num >= num	Determina si el valor de la expresión de la izquierda del operador es mayor o igual que el valor de la expresión de la derecha.
num <= num	Determina si el valor de la expresión de la izquierda del operador es menor o igual que el valor de la expresión de la derecha

Funciones para tipos de datos en la infraestructura de directivas

La infraestructura de directivas de Citrix ADC admite los siguientes tipos de datos numéricos:

- Entero (32 bits)
- Largo sin firmar (64 bits)
- Doble (64 bits)

Las expresiones simples pueden devolver todos estos tipos de datos. Además, puede crear expresiones compuestas que utilicen operadores aritméticos y operadores lógicos para evaluar o devolver los valores de estos tipos de datos. Además, puede utilizar todos estos valores en expresiones de directiva. Constantes literales de tipo unsigned long se pueden especificar agregando la cadena ul al número. Las constantes literales de tipo double contienen un punto (.), un exponente o ambos.

Operadores aritméticos, operadores lógicos y promoción de tipos

En las expresiones compuestas, se pueden utilizar los siguientes operadores aritméticos y lógicos estándar para los tipos de datos largos dobles y sin signo:

- +, -, * y/

%, ~, ^, &,	, «, y » (no se aplica al doble)

-

- ==,! =, >, <, >= y <=

Todos estos operadores tienen el mismo significado que en el lenguaje de programación C.

En todos los casos de operaciones mixtas entre operandos de tipo entero, largo sin signo y doble. La promoción de tipo se realiza para realizar la operación en los operandos del mismo tipo. La operación promueve un tipo de prioridad inferior al operando con el tipo de prioridad más alta. El orden de precedencia (superior a inferior) es el siguiente:

- Doble
- Largo sin firmar
- Número entero

Por lo tanto, una operación que devuelve un resultado numérico devuelve un resultado del tipo más alto involucrado en la operación.

Por ejemplo, si los operandos son de tipo integer y sin signo long, el operando entero se convierte automáticamente en tipo unsigned long. Esta conversión de tipo se realiza en expresiones simples. El tipo de datos identificado por el prefijo de expresión no coincide con el tipo de datos que se transfieren como argumento a la función. En la operación HTTP.REQ.CONTENT_LENGTH.DIV (3ul), el prefijo HTTP.REQ.CONTENT_LENGTH devuelve un entero que se convierte en un largo sin firmar. Long

sin signo: el tipo de datos que se pasa como argumento a la función DIV(), se realiza una división larga sin firmar. Del mismo modo, el argumento se puede promover en una expresión. Por ejemplo, HTTP.REQ.HEADER ("MyHeader") .TYPECAST_DOUBLE_AT.DIV (5) promueve el entero 5 para escribir doble y realiza una división de doble precisión.

Para obtener información sobre las expresiones para convertir datos de un tipo en datos de otro tipo, consulte Datos de fundición por tipografía.

Especificar el juego de caracteres en expresiones

January 12, 2021

La infraestructura de directivas del dispositivo Citrix ADC admite conjuntos de caracteres ASCII y UTF-8. El juego de caracteres predeterminado es ASCII. Si el tráfico para el que está configurando una expresión consta solo de caracteres ASCII, no es necesario especificar el juego de caracteres en la expresión. El dispositivo permite todos los literales de cadena y caracteres que incluyen caracteres binarios. Sin embargo, los conjuntos de caracteres UTF-8 todavía requieren que la cadena y los literales de caracteres sean un UTF-8 válido.

```
CLIENT.TCP.PAYLOAD(100).CONTAINS("\xff\x02")
```

En una expresión, la función SET_CHAR_SET () debe introducirse en el punto de la expresión después del cual el procesamiento de datos debe llevarse a cabo en el juego de caracteres especificado. Por ejemplo, en la expresión HTTP.REQ.BODY (1000).AFTER_REGEX (re/siguiente ejemplo/).BEFORE_REGEX (RE/en el ejemplo anterior/).CONTAINS_ANY ("alfabeto griego"), si las cadenas almacenadas en el conjunto de patrones "Greek_Alphabet" están en UTF-8, debe incluir la función SET_CHAR_SET(UTF_8) inmediatamente antes de la función CONTAINS_ANY ("<string>"), de la siguiente manera:

```
HTTP.REQ.BODY(1000).AFTER_REGEX(re/following example/).BEFORE_REGEX(re/In
the preceding example/).SET_CHAR_SET(UTF_8).CONTAINS_ANY("Greek_ alphabet")
```

La función SET_CHAR_SET() establece el juego de caracteres para todo el procesamiento posterior (es decir, para todas las funciones posteriores) de la expresión, a menos que sea reemplazado posteriormente en la expresión por otra función SET_CHAR_SET() que cambia el juego de caracteres. Por lo tanto, si todas las funciones de una expresión simple determinada están destinadas a UTF-8, puede incluir la función SET_CHAR_SET(UTF_8) inmediatamente después de las funciones que identifican texto (por ejemplo, las funciones HEADER("<name>") o BODY(<int>) functions). En el segundo ejemplo que sigue al primer párrafo anterior, si los argumentos ASCII pasados a las funciones AFTER_REGEX () y BEFORE_REGEX() se cambian a cadenas UTF-8, puede incluir la función SET_CHAR_SET(UTF_8) inmediatamente después de la función BODY (1000), de la siguiente manera:


```
HTTP.REQ.BODY(1000).SET_CHAR_SET(UTF_8).AFTER_REGEX(re/Bücher/).BEFORE_REGEX
(re/Wörterbuch/).CONTAINS_ANY("Greek_alphabet")
```

El juego de caracteres UTF-8 es un superconjunto del juego de caracteres ASCII, por lo que las expresiones configuradas para el juego de caracteres ASCII continúan funcionando como se esperaba si cambia el conjunto de caracteres a UTF-8.

Expresiones compuestas con diferentes conjuntos de caracteres

En una expresión compuesta, si un subconjunto de expresiones está configurado para trabajar con datos en el conjunto de caracteres ASCII y el resto de las expresiones están configuradas para trabajar con datos en el conjunto de caracteres UTF-8, el conjunto de caracteres especificado para cada expresión individual se considera cuando se evalúan las expresiones individualmente. Sin embargo, al procesar la expresión compuesta, justo antes de procesar los operadores, el dispositivo promueve el conjunto de caracteres de los valores ASCII devueltos a UTF-8. Por ejemplo, en la siguiente expresión compuesta, la primera expresión simple evalúa los datos del juego de caracteres ASCII mientras que la segunda expresión simple evalúa los datos del juego de caracteres UTF-8:

```
HTTP.REQ.HEADER("MyHeader")== HTTP.REQ.BODY(10).SET_CHAR_SET(UTF_8)
```

Sin embargo, al procesar la expresión compuesta, justo antes de evaluar el operador booleano "es igual a", el dispositivo Citrix ADC promueve el conjunto de caracteres del valor devuelto por HTTP.REQ.HEADER ("MyHeader") a UTF-8.

La primera expresión simple del siguiente ejemplo evalúa los datos del juego de caracteres ASCII. Sin embargo, cuando el dispositivo Citrix ADC procesa la expresión compuesta, justo antes de concatenar los resultados de las dos expresiones simples, el dispositivo promueve el conjunto de caracteres del valor devuelto por HTTP.REQ.BODY(10) a UTF-8.

```
HTTP.REQ.BODY(10)+ HTTP.REQ.HEADER("MyHeader").SET_CHAR_SET(UTF_8)
```

Por lo tanto, la expresión compuesta devuelve datos en el conjunto de caracteres UTF-8.

Especificar el juego de caracteres basado en el juego de caracteres del tráfico

Puede establecer el conjunto de caracteres en UTF-8 en función de las funciones del tráfico. Si no está seguro de si el juego de caracteres del tráfico que se está evaluando es UTF-8, puede configurar una expresión compuesta en la que la primera expresión compruebe el tráfico UTF-8 y las expresiones posteriores establezcan el conjunto de caracteres en UTF-8. A continuación se muestra un ejemplo de una expresión compuesta que primero comprueba el valor de "charset" en el encabezado Content-Type de la solicitud para "UTF-8" antes de comprobar si los primeros 1000 bytes en la solicitud contienen la cadena UTF-8 Bücher:


```
HTTP.REQ.HEADER("Content-Type").SET_TEXT_MODE(IGNORECASE).TYPECAST_NVLIST_T
('=', '; ', '"').VALUE("charset").EQ("UTF-8")&& HTTP.REQ.BODY(1000).SET_CHAR_SET
(UTF_8).CONTAINS("Bücher")
```

Si está seguro de que el conjunto de caracteres del tráfico que se está evaluando es UTF-8, la segunda expresión del ejemplo es suficiente.

Literales de caracteres y cadenas en expresiones

Durante la evaluación de expresiones, incluso si el conjunto de caracteres actual es ASCII, los literales de caracteres y los literales de cadena, que están entre comillas simples (‘’) y comillas (“”), respectivamente, se consideran literales en el conjunto de caracteres UTF-8. En una expresión dada, si una función está operando en literales de caracteres o cadenas en el conjunto de caracteres ASCII e incluye un carácter no ASCII en el literal, se devuelve un error.

> **Nota**:
>
> Los literales de cadena en expresiones de directiva avanzadas son ahora tan largos como la expresión de directiva. Se permite que la expresión tenga 1499 bytes u 8191 bytes de longitud.

Valores en formatos hexadecimales y octales

Al configurar una expresión, puede introducir valores en formatos octal y hexadecimal. Sin embargo, cada byte hexadecimal u octal se considera un byte UTF-8. Los bytes UTF-8 no válidos generan errores independientemente de si el valor se introduce manualmente o se pega desde el portapapeles. Por ejemplo, “xcex20” es un carácter UTF-8 no válido porque “c8” no puede ir seguido de “20” (cada byte en una cadena UTF-8 multibyte debe tener el bit alto establecido). Otro ejemplo de un carácter UTF-8 no válido es “xce xa9”, ya que los caracteres hexadecimales están separados por un carácter de espacio en blanco.

Funciones que devuelven cadenas UTF-8

Solo las`text`>`.XPATH` funciones`<text>.XPATH_JSON` y siempre devuelven cadenas UTF-8. Las siguientes rutinas MYSQL determinan en tiempo de ejecución qué juego de caracteres devolver, en función de los datos del protocolo:

- `MYSQL_CLIENT_T.USER`
- `MYSQL_CLIENT_T.DATABASE`
- `MYSQL_REQ_QUERY_T.COMMAND`
- `MYSQL_REQ_QUERY_T.TEXT`
- `MYSQL_REQ_QUERY_T.TEXT(<unsigned int>)`
- `MYSQL_RES_ERROR_T.SQLSTATE`

- MYSQL_RES_ERROR_T.MESSAGE
- MYSQL_RES_FIELD_T.CATALOG
- MYSQL_RES_FIELD_T.DB
- MYSQL_RES_FIELD_T.TABLE
- MSQL_RES_FIELD_T.ORIGINAL_TABLE
- MYSQL_RES_FIELD_T.NAME
- MYSQL_RES_FIELD_T.ORIGINAL_NAME
- MYSQL_RES_OK_T.MESSAGE
- MYSQL_RES_ROW_T.TEXT_ELEM(<unsigned **int**>)

Configuración de conexión de terminal para UTF-8

Al configurar una conexión con el dispositivo Citrix ADC mediante una conexión de terminal (por ejemplo, mediante PuTTY), debe establecer el juego de caracteres para la transmisión de datos en UTF-8.

Funciones mínimas y máximas en una expresión de directiva avanzada

Las expresiones de directiva avanzadas admiten las funciones mínimas y máximas siguientes.

1. (<expression1>.max(<expression2>): Devuelve el máximo de los dos valores.
2. (<expression1>.min(<expression2>): Devuelve el mínimo de los dos valores.

Expresiones clásicas en expresiones de directiva avanzadas

August 20, 2021

> **Advertencia:**
>
> Las expresiones de directiva clásicas ya no son compatibles con Citrix ADC 12.0, compilación 56.20 en adelante y, como alternativa, Citrix recomienda utilizar directivas avanzadas. Para obtener más información, consulte Configurar expresiones de directivas avanzadas: Introducción.

Las expresiones clásicas describen las funciones básicas del tráfico. A veces, es posible que quiera utilizar una expresión clásica en una expresión de directiva avanzada.

A continuación se muestra la sintaxis de todas las expresiones de directiva avanzadas que utilizan una expresión clásica:

SYS.EVAL_CLASSIC_EXPR (“expresión”)

> **Nota:**
>
> La sintaxis y los metadatos de la expresión SYS.EVAL_CLASSIC_EXPR se están quedando en desuso. Puede convertir manualmente o utilizar la herramienta nspepi para convertir la expresión clásica en la expresión avanzada.

A continuación se presentan ejemplos de la expresión SYS.EVAL_CLASSIC_EXPR (“expresión”):

```
1 sys.eval_classic_expr(”req.ssl.client.cipher.bits > 1000”)
2 sys.eval_classic_expr(”url contains abc”)
3 sys.eval_classic_expr(”req.ip.sourceip == 10.102.1.61 -netmask
     255.255.255.255”)
4 sys.eval_classic_expr(”time >= *:30:00GMT”)
5 sys.eval_classic_expr(”e1 || e2”)
6 sys.eval_classic_expr(”req.http.urllen > 50”)
7 sys.eval_classic_expr(”dayofweek == wedGMT”)
8 <!--NeedCopy-->
```

> **Nota:**
>
> Al actualizar Citrix ADC a la versión 9.0 o superior, las directivas de almacenamiento en caché integrado se actualizan automáticamente a directivas avanzadas y las expresiones de estas directivas se actualizan a las directivas avanzadas.

Configurar expresiones de directivas avanzadas en una directiva

October 5, 2021

Puede configurar una expresión de directiva avanzada de hasta 1.499 caracteres en una directiva. La interfaz de usuario de las expresiones de directivas avanzadas depende en cierta medida de la función para la que está configurando la expresión y de si está configurando una expresión para una directiva o para otro uso.

Al configurar expresiones en la línea de comandos, la delimita mediante comillas (“…” o “…”). Dentro de una expresión, se escapan las comillas adicionales mediante una barra diagonal inversa(). Por ejemplo, los siguientes son métodos estándar para escapar las comillas en una expresión:

```
”\”abc\””
```

```
‘\”abc\”’
```

También debe utilizar una barra diagonal inversa para escapar de los signos de interrogación y otras barras invertidas en la línea de comandos. Por ejemplo, la expresión http.req.url.contains (“?”) re-

quiere una barra diagonal inversa para que se analiza el signo de interrogación. Tenga en cuenta que el carácter de barra diagonal inversa no aparecerá en la línea de comandos después de escribir el signo de interrogación. Por otro lado, si escapa una barra diagonal inversa (por ejemplo, en la expresión 'http.req.url.contains ("\\ http") '), los caracteres de escape se repiten en la línea de comandos.

Para que una entrada sea más legible, puede evitar las comillas de toda una expresión. Al principio de la expresión, introduce la secuencia de escape "q" más uno de los siguientes caracteres especiales:/{<	~$^+=&%@'?.

Introduzca solo el carácter especial al final de la expresión, de la siguiente manera:

```
q@http.req.url.contains(”sometext”) && http.req.cookie.exists@

q~http.req.url.contains(”sometext”) && http.req.cookie.exists~
<!--NeedCopy-->
```

Tenga en cuenta que una expresión que utiliza {delimiter se cierra con}.

Para algunas funciones (por ejemplo, Almacenamiento en caché y respuesta integrados), el cuadro de diálogo de configuración de directivas proporciona un cuadro de diálogo secundario para configurar expresiones. Este cuadro de diálogo le permite elegir entre listas desplegables que muestran las opciones disponibles en cada punto durante la configuración de la expresión. No se pueden utilizar operadores aritméticos al utilizar estos cuadros de diálogo de configuración, pero la mayoría de las demás funciones avanzadas de expresión de directivas están disponibles. Para usar operadores aritméticos, escribe tus expresiones en formato libre.

Configurar una regla de sintaxis de directivas avanzada mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para configurar una regla de directiva avanzada y compruebe la configuración:

1. `add cache|dns|rewrite|cs policyName **-rule** expression featureSpecificParameter **-action**`
2. `show cache|dns|rewrite|cs policyName`
   A continuación se muestra un ejemplo de configuración de una directiva de almacenamiento en caché:

   Ejemplo:


```
> add cache policy pol-cache -rule http.req.content_length.le(5) -
   action INVAL
 Done

> show cache policy pol-cache
        Name: pol-cache
        Rule: http.req.content_length.le(5)
        CacheAction: INVAL
        Invalidate groups: DEFAULT
        UndefAction: Use Global
        Hits: 0
        Undef Hits: 0

 Done
<!--NeedCopy-->
```

Configurar una expresión de directiva avanzada mediante la interfaz gráfica de usuario

1. En el panel de navegación, haga clic en el nombre de la función en la que quiere configurar una directiva; por ejemplo, puede seleccionar Almacenamiento en caché integrado, Respondedor, DNS, Reescritura o Cambio de contenido y, a continuación, hacer clic en **Directivas**.
2. Haga clic en Add.
3. Para la mayoría de las entidades, haga clic en el campo **Expresión** . Para cambiar contenido, haga clic en **Configurar**.
4. Haga clic en el icono **Prefijo** (la casa) y seleccione el primer prefijo de expresión de la lista desplegable. Por ejemplo, en Responder, las opciones son HTTP, SYS y CLIENT. El siguiente conjunto de opciones aplicables aparece en una lista desplegable.
5. Haga doble clic en la siguiente opción para seleccionarla y, a continuación, escriba un punto (.). De nuevo, aparece un conjunto de opciones aplicables en otra lista desplegable.
6. Continúe seleccionando opciones hasta que aparezca un campo de entrada (señalado entre paréntesis). Cuando aparezca un campo de entrada, introduzca un valor apropiado entre paréntesis. Por ejemplo, si selecciona GT (int) (formato mayor que, entero), especifica un entero entre paréntesis. Las cadenas de texto se delimitan entre comillas. A continuación se presenta un ejemplo:

   ```
   HTTP.REQ.BODY(1000).BETWEEN("this","that")
   ```

7. Para insertar un operador entre dos partes de una expresión compuesta, haga clic en el icono Operadores (sigma) y seleccione el tipo de operador. A continuación se muestra un ejemplo de

una expresión configurada con OR booleana (señalada por barras verticales dobles, ||):

```
HTTP.REQ.URL.EQ("www.mycompany.com")||HTTP.REQ.BODY(1000).BETWEEN("this
","that")
```

8. Para insertar una expresión con nombre, haga clic en la flecha hacia abajo junto al icono Agregar (el signo más) y seleccione una expresión con nombre.
9. Para configurar una expresión mediante menús desplegables e insertar expresiones integradas, haga clic en el icono Agregar (el signo más). El cuadro de diálogo **Agregar expresión** funciona de forma similar al cuadro de diálogo principal, pero proporciona listas desplegables para seleccionar opciones y proporciona campos de texto para introducir datos en lugar de paréntesis. Este cuadro de diálogo también proporciona una lista desplegable Expresiones usadas con frecuencia que inserta expresiones de uso común. Cuando haya terminado de agregar la expresión, haga clic en **Aceptar**.
10. Cuando haya terminado, haga clic en **Crear**. Un mensaje en la barra de estado indica que la expresión de directiva se ha configurado correctamente.

Pruebe una expresión de directiva avanzada mediante la interfaz gráfica de usuario

1. En el panel de navegación, haga clic en el nombre de la función para la que quiere configurar una directiva (por ejemplo, puede seleccionar Almacenamiento en caché integrado, Respondedor, DNS, Reescritura o Cambio de contenido) y, a continuación, haga clic en Directivas.
2. Seleccione una directiva y haga clic en **Abrir**.
3. Para probar la expresión, haga clic en el icono Evaluar (la marca de verificación).
4. En el cuadro de diálogo evaluador de expresiones, seleccione el tipo de flujo que coincida con la expresión.
5. En el campo **Datos de solicitud HTTP**o **Datos de respuesta HTTP**, pegue la solicitud o respuesta HTTP que quiere analizar con la expresión y haga clic en **Evaluar**. Tenga en cuenta que debe proporcionar una solicitud o respuesta HTTP completa y que el encabezado y el cuerpo deben estar separados por una línea en blanco. Algunos programas que atrapan encabezados HTTP no atrapan también la respuesta. Si va a copiar y pegar solo el encabezado, inserte una línea en blanco al final del encabezado para formar una solicitud o respuesta HTTP completa.
6. Haga clic en **Cerrar** para cerrar este cuadro de diálogo.

Configurar expresiones de directivas avanzadas con nombre

October 5, 2021

En lugar de volver a escribir la misma expresión varias veces en varias directivas, puede configurar

una expresión con nombre y hacer referencia al nombre cada vez que quiera utilizar la expresión en una directiva. Por ejemplo, podría crear las siguientes expresiones con nombre:

- Esta expresión:

  ```
  http.req.body(100).contains("this")
  ```

- Esa expresión:

  ```
  http.req.body(100).contains("that")
  ```

A continuación, puede utilizar estas expresiones con nombre en una expresión de directiva. Por ejemplo, la siguiente es una expresión jurídica basada en los ejemplos anteriores:

Esta expresión	Esa expresión

Puede utilizar el nombre de una expresión de directiva avanzada como prefijo de una función. La expresión nombrada puede ser una expresión simple o una expresión compuesta. La función debe ser una función que pueda funcionar con el tipo de datos que devuelve la expresión nombrada.

Ejemplo 1: Expresión con nombre simple como prefijo

La siguiente expresión con nombre simple, que identifica una cadena de texto, se puede utilizar como prefijo de la <string>función AFTER_STR (" "), que funciona con datos de texto:

```
HTTP.REQ.BODY(1000)
```

Si el nombre de la expresión es top1KB, puede usar top1KB.AFTER_STR ("nombre de usuario") en lugar de HTTP.REQ.BODY (1000) .AFTER_STR ("nombre de usuario").

Ejemplo 2: expresión denominada compuesta como prefijo

Puede crear una expresión compuesta denominada basic_header_value para concatenar el nombre de usuario de una solicitud, dos puntos (:) y la contraseña del usuario, de la siguiente manera:

```
add policy expression basic_header_value "HTTP.REQ.USER.NAME + \":\" + HTTP
.REQ.USER.PASSWD"
```

A continuación, puede utilizar el nombre de la expresión en una acción de reescritura, como se muestra en el siguiente ejemplo:

```
add rewrite action insert_b64encoded_authorization insert_http_header
authorization '"Basic " + basic_header_value.b64encode'
```

En el ejemplo, en la expresión que se utiliza para construir el valor del encabezado personalizado, el algoritmo de codificación B64 se aplica a la cadena devuelta por el compuesto denominado expression.

También puede utilizar una expresión con nombre (ya sea sola o como prefijo de una función) para crear la expresión de texto para el destino de reemplazo en una reescritura.

Configurar una expresión de directiva avanzada con nombre mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para configurar una expresión con nombre y comprobar la configuración:

```
1 -  add policy expression <name><value>
2
3 -  show policy expression <name>
4 <!--NeedCopy-->
```

Ejemplo:

```
1 > add policy expression myExp "http.req.body(100).contains("the other")
     "
2 Done
3
4 > show policy expression myExp
5     1)      Name: myExp  Expr: "http.req.body(100).contains("the other"
         )"  Hits: 0 Type : ADVANCED
6 Done
7 <!--NeedCopy-->
```

La expresión puede tener un máximo de 1.499 caracteres.

Configurar una expresión con nombre mediante la interfaz gráfica de usuario

1. En el panel de navegación, expanda **AppExpert**y, a continuación, haga clic en **Expresiones**.
2. Haga clic en **Expresiones avanzadas**.
3. Haga clic en **Add**.
4. Introduzca un nombre y una descripción para la expresión.
5. Configure la expresión mediante el proceso descrito en Configurar expresión de directiva avanzada. Un mensaje en la barra de estado indica que la expresión de directiva se ha configurado correctamente.

Configurar expresiones de directiva avanzadas fuera del contexto de una directiva

August 20, 2021

Varias funciones, incluidas las siguientes, pueden requerir una expresión de directiva avanzada que no forme parte de una directiva:

- Selectores de almacenamiento en caché integrados:

  Defina varias expresiones no compuestas (selectlets) en la definición del selector. Cada selectlet está en una relación lógica Y implícita con los demás.

- Equilibrio de carga:

  Configurar una expresión para el método TOKEN de equilibrio de carga para un servidor virtual de equilibrio de carga.

- Acciones de reescritura:

  Las expresiones definen la ubicación de la acción de reescritura y el tipo de reescritura que se va a realizar, dependiendo del tipo de acción de reescritura que esté configurando. Por ejemplo, una acción SUPR solo utiliza una expresión de destino. Una acción REPLACE utiliza una expresión de destino y una expresión para configurar el texto de reemplazo.

- Directivas basadas en tasas:

  Utilice expresiones de directiva avanzadas para configurar selectores de límite. Puede utilizar estos selectores al configurar directivas para reducir la velocidad de tráfico a varios servidores. Puede definir hasta cinco expresiones no compuestas (selectlets) en la definición del selector. Cada selectlet está en un AND lógico implícito con los demás.

Configurar una expresión de directiva avanzada fuera de una directiva mediante la CLI (ejemplo del selector de caché)

En el símbolo del sistema, escriba los siguientes comandos para configurar una expresión de directiva avanzada fuera de una directiva y compruebe la configuración:

```
1 -  add cache selector <selectorName> <rule>
2 -  show cache selector <selectorName>
3 <!--NeedCopy-->
```

Ejemplo:


```
> add cache selector mainpageSelector ”http.req.cookie.value(”ABC_def”)
    ”
    ”http.req.url.query.value(”_ghi”)”selector ”mainpageSelector” added
Done
> show cache selector mainpageSelector
            Name: mainpageSelector
            Expressions:
                    1) http.req.cookie.value(”ABC_def”)
                    2) http.req.url.query.value(”_ghi”)
Done
<!--NeedCopy-->
```

A continuación se presenta un comando equivalente que utiliza el delimitador q más legible, tal y como se describe en Configurar expresiones de directiva avanzadas de una directiva:

```
> add cache selector mainpageSelector2 q~http.req.cookie.value(”ABC_def
    ”)~
    q~http.req.url.query.value(”_ghi”)~selector ”mainpageSelector2”
        added
Done
> show cache selector mainpageSelector2
            Name: mainpageSelector2
            Expressions:
                    1) http.req.cookie.value(”ABC_def”)
                    2) http.req.url.query.value(”_ghi”)
Done
<!--NeedCopy-->
```

Expresiones de directiva avanzadas: Evaluar texto

January 12, 2021

Puede configurar una directiva con una expresión de directiva avanzada que evalúe el texto de una solicitud o respuesta. Las expresiones de texto de directivas avanzadas pueden ir desde expresiones simples que realizan la coincidencia de cadenas en encabezados HTTP hasta expresiones complejas que codifican y decodifican texto. Puede configurar expresiones de texto para que distingan entre mayúsculas y minúsculas o para que utilicen o ignoren espacios. También puede configurar expresiones de texto complejas combinando expresiones de texto con operadores booleanos

Puede utilizar prefijos de expresión y operadores para evaluar solicitudes HTTP, respuestas HTTP y

datos VPN y VPN sin cliente. Sin embargo, los prefijos de expresiones de texto no se limitan a evaluar estos elementos del tráfico.

Acerca de expresiones de texto

October 5, 2021

Puede configurar varias expresiones para trabajar con texto que fluye a través del dispositivo Citrix ADC. A continuación se muestran algunos ejemplos de cómo analizar texto mediante una expresión de directiva avanzada:

- Determina que existe un encabezado HTTP concreto.

  Por ejemplo, es posible que quiera identificar las solicitudes HTTP que contienen un encabezado Accept-Language concreto con el fin de dirigir la solicitud a un servidor concreto.

- Determina que una URL HTTP concreta contiene una cadena concreta.

  Por ejemplo, es posible que quiera bloquear las solicitudes de URL específicas. Tenga en cuenta que la cadena puede aparecer al principio, al medio o al final de otra cadena.

- Identificar una solicitud POST dirigida a una aplicación concreta.

  Por ejemplo, es posible que quiera identificar todas las solicitudes POST dirigidas a una aplicación de base de datos con el fin de actualizar los datos de la aplicación almacenados en caché.

Tenga en cuenta que existen herramientas especializadas para ver el flujo de datos de solicitudes y respuestas HTTP. Puede utilizar las herramientas para ver el flujo de datos.

Acerca de las operaciones en el texto

Una expresión basada en texto consta de al menos un prefijo para identificar un elemento de datos y, por lo general, (aunque no siempre) una operación en ese prefijo. Las operaciones basadas en texto pueden aplicarse a cualquier parte de una solicitud o respuesta. Las operaciones básicas sobre el texto incluyen varios tipos de coincidencias de cadenas.

Por ejemplo, la siguiente expresión compara un valor de encabezado con una cadena:

```
http.req.header("myHeader").contains("some-text")
```

Las siguientes expresiones son ejemplos de coincidencia de un tipo de archivo en una solicitud:

```
http.req.url.suffix.contains("jpeg")
```

```
http.req.url.suffix.eq("jpeg")
```


En los ejemplos anteriores, el operador contains permite una coincidencia parcial y el operador eq busca una coincidencia exacta.

Hay otras operaciones disponibles para dar formato a la cadena antes de evaluarla. Por ejemplo, puede utilizar operaciones de texto para eliminar las comillas y los espacios en blanco, convertir la cadena a minúsculas o concatenar cadenas.

> **Nota**: Las operaciones
>
> complejas están disponibles para realizar coincidencias basadas en patrones o para convertir un tipo de formato de texto a otro tipo.

Para obtener más información, consulte estos temas:

- Conjuntos de patrones y conjuntos de datos.
- Expresiones regulares.
- Datos de fundición de tipografía.

Compuestos y precedencia en expresiones de texto

Puede aplicar varios operadores para combinar prefijos o expresiones de texto. Por ejemplo, la siguiente expresión concatena los valores devueltos de cada prefijo:

```
http.req.hostname + http.req.url
```

A continuación se muestra un ejemplo de una expresión de texto compuesto que utiliza un AND lógico. Ambos componentes de esta expresión deben ser TRUE para que una solicitud coincida con la expresión:

```
http.req.method.eq(post)&& http.req.body(1024).startswith(”destination=”)
```

> **Nota:**
>
> Para obtener más información sobre los operadores de composición, consulte Expresiones avanzadas compuestas.

Categorías de expresiones de texto

Las categorías principales de expresiones de texto que se pueden configurar son:

- Información en encabezados HTTP, URL HTTP y el cuerpo POST en solicitudes HTTP.

  Para obtener más información, consulte Prefijos de expresión para texto en solicitudes y respuestas HTTP.

- Información sobre una VPN o una VPN sin cliente.

  Para obtener más información, consulte Prefijos de expresión para VPN y VPN sin cliente.

- Información de carga TCP.

  Para obtener más información sobre las expresiones de carga útil TCP, consulte Expresiones de directiva avanzadas: análisis de datos HTTP, TCP y UDP.

- Texto en un certificado de Secure Sockets Layer (SSL).

  Para obtener información sobre expresiones de texto para datos de certificados SSL y SSL, consulte Expresiones de directiva avanzadas: análisis de certificados SSL y Expresiones para fechas de certificados SSL.

> **Nota: El**
>
> análisis de un cuerpo de documento, como el cuerpo de una solicitud POST, puede afectar al rendimiento. Es posible que quiera probar el impacto en el rendimiento de las directivas que evalúan el cuerpo de un documento.

Directrices para expresiones de texto

Desde el punto de vista del rendimiento, normalmente es mejor utilizar funciones con reconocimiento de protocolo en una expresión. Por ejemplo, la siguiente expresión utiliza una función con reconocimiento de protocolo:

```
HTTP.REQ.URL.QUERY
```

La expresión anterior tiene un mejor rendimiento que la siguiente expresión equivalente, que se basa en el análisis de cadenas:

```
HTTP.REQ.URL.AFTER_STR("?")
```

En el primer caso, la expresión examina específicamente la consulta de URL. En el segundo caso, la expresión explora los datos en busca de la primera aparición de un signo de interrogación.

También hay un beneficio de rendimiento del análisis estructurado del texto, como en la siguiente expresión:

```
HTTP.REQ.HEADER("Example").TYPECAST_LIST_T(',').GET(1)
```

(Para obtener más información sobre la fundición de tipos, consulte Datos de fundición por tipografía. La expresión de conversión de tipos, que recopila datos delimitados por comas y los estructura en una lista, normalmente tendría un mejor rendimiento que el siguiente equivalente no estructurado:

```
HTTP.REQ.HEADER("Example").AFTER_STR(",").BEFORE_STR(",")
```

Por último, las expresiones de texto no estructuradas suelen tener un mejor rendimiento que las expresiones regulares. Por ejemplo, lo siguiente es una expresión de texto no estructurada:

```
HTTP.REQ.HEADER("Example").AFTER_STR("more")
```


La expresión anterior generalmente proporcionaría un mejor rendimiento que el siguiente equivalente, que usa una expresión regular:

```
HTTP.REQ.HEADER("Example").AFTER_REGEX(re/more/)
```

Para obtener más información sobre las expresiones regulares, consulte Expresiones regulares.

Prefijos de expresión para texto en solicitudes y respuestas HTTP

June 22, 2022

Una solicitud o respuesta HTTP normalmente contiene texto, por ejemplo, en forma de encabezados, valores de encabezado, URL y texto del cuerpo de POST. Puede configurar expresiones para que funcionen en uno o más de estos elementos basados en texto en una solicitud o respuesta HTTP.

Para obtener más información sobre los parámetros, consulte Referencia de expresiones de directivas avanzadas de Citrix ADC.

Consulte los temas siguientes para obtener más información sobre cómo configurar el uso de expresiones avanzadas.

- Expresiones de directiva avanzadas compuestas
- Expresiones de directivas avanzadas: direcciones IP y MAC, rendimiento, ID de VLAN
- Expresiones de directivas avanzadas: análisis de SSL
- Expresiones de directiva avanzadas: trabajar con fechas, horas y números
- Elementos básicos de una expresión de directiva avanzada
- Expresiones de directiva avanzadas: evaluación de texto
- Expresiones de directiva avanzadas: análisis de datos HTTP, TCP y UDP
- Ejemplos resumidos de directivas y expresiones de sintaxis predeterminadas

Prefijos de expresión para VPN y VPN sin cliente

August 20, 2021

El motor de directivas avanzado proporciona prefijos específicos para analizar datos VPN o VPN sin cliente. Estos datos incluyen lo siguiente:

- Nombres de host, dominios y direcciones URL en el tráfico VPN.
- Protocolos en el tráfico VPN.
- Consultas en el tráfico VPN.

Estos elementos de texto suelen ser URL y componentes de URL. Además de aplicar las operaciones basadas en texto en estos elementos, puede analizar estos elementos mediante operaciones específicas para analizar direcciones URL. Para obtener más información, consulte Expresiones para extraer segmentos de URL.

Para obtener información sobre los prefijos de expresión VPN, consulte Tabla de expresiones VPN.

Operaciones básicas sobre texto

October 5, 2021

Las operaciones básicas en el texto incluyen operaciones para hacer coincidir cadenas, calcular la longitud de una cadena y controlar la distinción entre mayúsculas y minúsculas. Puede incluir espacios en blanco en una cadena que se pasa como argumento a una expresión, pero la cadena no puede superar los 255 caracteres.

Funciones de comparación de cadenas

En la tabla siguiente se enumeran las operaciones básicas de coincidencia de cadenas en las que las funciones devuelven un valor booleano TRUE o FALSE.

Función	Descripción
`<text>.CONTAINS(<string>)`	Devuelve un valor booleano TRUE si el objetivo contiene `<string>`. Ejemplo:`http.req.url.contains(".jpeg")`
`<text>.EQ(<string>)`	Devuelve un valor booleano TRUE si el objetivo coincide exactamente con `<string>`. Por ejemplo, la siguiente expresión devuelve un valor booleano TRUE para una URL con el nombre de host "myhostabc": `http.req.url.hostname.eq("myhostabc")`
`<text>.STARTSWITH(<string>)`	Devuelve un valor booleano TRUE si el objetivo empieza por `<string>`. Por ejemplo, la siguiente expresión devuelve un valor booleano TRUE para una URL con el nombre de host "myhostabc": `http.req.url.hostname.startswith("myhost")`

Función	Descripción
`<text>.ENDSWITH(<string>)`	Devuelve un valor booleano TRUE si el objetivo termina en<string>. Por ejemplo, la siguiente expresión devuelve un valor booleano TRUE para una URL con el nombre de host "myhostabc": `http.req.url.hostname.endswith("abc")`
`<text>.NE(<string>)`	Devuelve un valor booleano TRUE si el prefijo no es igual al argumento de cadena. Si el prefijo devuelve un valor que no es cadena, el argumento de la función se compara con la representación de cadena del valor devuelto por el prefijo. Puede utilizar las funciones con `SET_TEXT_MODE(IGNORECASE)or SET_TEXT_MODE(NOIGNORECASE)`y con conjuntos de caracteres ASCII y UTF-8.
`<text>.GT(<string>)`	Devuelve un valor booleano TRUE si el prefijo es alfabéticamente mayor que el argumento de cadena. Si el prefijo devuelve un valor que no es cadena, el argumento de la función se compara con la representación de cadena del valor devuelto por el prefijo. Puede utilizar las funciones con `SET_TEXT_MODE(IGNORECASE)` o `SET_TEXT_MODE(NOIGNORECASE)`, y con conjuntos de caracteres ASCII y UTF-8.
`<text>.GE(<string>)`	Devuelve un valor booleano TRUE si el prefijo es alfabéticamente mayor o igual que el argumento de cadena. Si el prefijo devuelve un valor que no es cadena, el argumento de la función se compara con la representación de cadena del valor devuelto por el prefijo. Puede utilizar las funciones con `SET_TEXT_MODE(IGNORECASE)` o `SET_TEXT_MODE(NOIGNORECASE)`, y con conjuntos de caracteres ASCII y UTF-8.

Función	Descripción
`<text>.LT(<string>)`	Devuelve un valor booleano TRUE si el prefijo es alfabéticamente menor que el argumento de cadena. Si el prefijo devuelve un valor que no es cadena, el argumento de la función se compara con la representación de cadena del valor devuelto por el prefijo. Puede utilizar las funciones con `SET_TEXT_MODE(IGNORECASE)` o `SET_TEXT_MODE(NOIGNORECASE)`, y con conjuntos de caracteres ASCII y UTF-8.
`<text>.LE(<string>)`	Devuelve un valor booleano TRUE si el prefijo es alfabéticamente menor o igual que el argumento de cadena. Si el prefijo devuelve un valor que no es cadena, el argumento de la función se compara con la representación de cadena del valor devuelto por el prefijo. Puede utilizar las funciones con `SET_TEXT_MODE(IGNORECASE)` o `SET_TEXT_MODE(NOIGNORECASE)`, y con conjuntos de caracteres ASCII y UTF-8.

Calcula la longitud de una cadena

La operación `<text>.LENGTH` devuelve un valor numérico igual al número de caracteres (no bytes) de una cadena:

```
<text>.LENGTH
```

Por ejemplo, es posible que quiera identificar las URL de solicitud que superan una longitud determinada. A continuación se muestra una expresión que implementa este ejemplo:

```
HTTP.REQ.URL.LENGTH < 500
```

Después de contar los caracteres o elementos de una cadena, puede aplicarles operaciones numéricas. Para obtener más información, consulte Expresiones de directiva avanzadas: trabajo con fechas, horas y números.

Considerar, ignorar y cambiar mayúsculas y minúsculas de texto

Las siguientes funciones funcionan en mayúsculas o minúsculas de los caracteres de la cadena.

Función	Descripción	
<text>.SET_TEXT_MODE (IGNORECASE	NOIGNORECASE)	Esta función activa o desactiva la sensibilidad de mayúsculas y minúsculas en todas las operaciones de texto.
<text>.TO_LOWER	Convierte el destino a minúsculas para un bloque de texto de hasta 2 kilobytes (KB). Devuelve UNDEF si el objetivo supera los 2 KB. Por ejemplo, la cadena “abCD:” se convierte en “abcd:” .	
<text>.TO_UPPER	Convierte el destino a mayúsculas. Devuelve UNDEF si el objetivo supera los 2 KB. Por ejemplo, la cadena “abCD:” se convierte en “ABCD:” .	

Elimina caracteres específicos de una cadena

Puede utilizar la función STRIP_CHARS(<string>) para quitar caracteres específicos del texto devuelto por un prefijo de expresión de directiva avanzada (la cadena de entrada). Todas las instancias de los caracteres especificados en el argumento se quitan de la cadena de entrada. Puede utilizar cualquier método de texto en la cadena resultante, incluidos los métodos utilizados para hacer coincidir la cadena con un conjunto de patrones.

Por ejemplo, en la expresión `CLIENT.UDP.DNS.DOMAIN.STRIP\\_CHARS(".-\\_")`, la función `STRIP\\_CHARS(<string>)` elimina todos los puntos (.), guiones (-) y guiones bajos (_) del nombre de dominio devuelto por el prefijo CLIENT.UDP.DNS.DOMAIN. Si el nombre de dominio que se devuelve es “a.dom_ai_n-name”, la función devuelve la cadena “adomainname”.

En el siguiente ejemplo, la cadena resultante se compara con un conjunto de patrones denominado “listofdomains”:

```
CLIENT.UDP.DNS.DOMAIN.STRIP_CHARS(".-_").CONTAINS_ANY("listofdomains")
```

Nota: No se puede reescribir la cadena devuelta por la función `STRIP_CHARS(<string>)`.

Las siguientes funciones quitan los caracteres coincidentes del principio y el final de una entrada de cadena determinada.

Función	Descripción
`<text>.STRIP_START_CHARS(s)`	Elimina los caracteres coincidentes desde el principio de la cadena de entrada hasta que se encuentra el primer carácter no coincidente y devuelve el resto de la cadena. Debe especificar los caracteres que quiere quitar como una cadena sencilla entre comillas. Por ejemplo, si el nombre de un encabezado es testLang y:*/en_us:es su valor, HTTP.RES.HEADER (“testLang”) .STRIP_START_CHARS (“:”)* elimina los caracteres especificados desde el principio del valor del encabezado hasta que se encuentra el primer carácter no coincidente e y devuelve sen_us: como cadena.
`<text>`.STRIP_END_CHARS	Elimina los caracteres coincidentes desde el final de la cadena de entrada hasta el primer carácter no coincidente y devuelve el resto de la cadena. Debe especificar los caracteres que quiere quitar como una cadena sencilla entre comillas. Por ejemplo, si el nombre de un encabezado es testLang y:*/en_us:es su valor, HTTP.RES.HEADER (“testLang”) .STRIP_START_CHARS (“:”)* elimina los caracteres especificados desde el final del valor del encabezado hasta que se encuentra el primer carácter s no coincidente y devuelve: /_en_us como cadena.

Agregar una cadena a otra cadena

Puede utilizar la función APPEND() para agregar la representación de cadena del argumento a la representación de cadena del valor devuelto por la función anterior. La función anterior puede ser una que devuelva un número, long sin signo, doble, valor de tiempo, dirección IPv4 o dirección IPv6. El argumento puede ser una cadena de texto, número, long sin signo, doble, valor temporal, dirección IPv4 o dirección IPv6. El valor de cadena resultante es el mismo valor de cadena que se obtiene mediante

el operador +.

Operaciones complejas sobre texto

July 15, 2022

Además de una simple coincidencia de cadenas, puede configurar expresiones que examinan la longitud de la cadena y el bloque de texto en busca de patrones en lugar de cadenas específicas.

Tenga en cuenta lo siguiente para cualquier operación basada en texto:

- Para cualquier operación que tome un argumento de cadena, la cadena no puede superar los 255 caracteres.
- Puede incluir espacios en blanco al especificar una cadena en una expresión.

Operaciones sobre la longitud de una cadena

Las siguientes operaciones extraen cadenas mediante un recuento de caracteres.

Operación Conteo de personajes	Descripción
`<text>.TRUNCATE(<count>)`	Devuelve una cadena tras truncar el final del destino por el número de caracteres de `<count>`. Si toda la cadena es más corta que `<count>`, no se devuelve nada.
`<text>.TRUNCATE(<character>,<count>)`	Devuelve una cadena tras truncar el texto después de `<character>` por el número de caracteres especificado en `<count>`.
`<text>.PREFIX(<character>,<count>)`	Selecciona el prefijo más largo del destino que tiene como máximo `<count>` apariciones de `<character>`.

Operación Conteo de personajes	Descripción
<text>.SUFFIX(<character>, <count>)	Selecciona el sufijo más largo del objetivo que tiene como máximo <count> apariciones de <character>. Por ejemplo, considere el siguiente cuerpo de respuesta: peninsula. La siguiente expresión devuelve un valor de sula : http.res.body(100).suffix('n',0). La siguiente expresión devuelve insula: http.res.body(100).suffix('n',1). La siguiente expresión devuelve un valor de peninsula: http.res.body(100). suffix('n',2). La siguiente expresión devuelve un valor de peninsula: http.res .body(100).suffix('n',3).
<text>.SUBSTR(<starting_offset>, < length>)	Seleccione una cadena con el <length>número de caracteres del objeto de destino. Comience a extraer la cadena después de la <starting_offset>. Si el número de caracteres tras el desplazamiento es inferior al valor del argumento <length>, seleccione todos los caracteres restantes.
<text>.SKIP(<character>, <count>)	Seleccione una cadena del objetivo después de omitir el prefijo más largo que tenga como máximo <count> casos de <character>.

Operaciones en una parte de una cadena

Consulte la tabla Operaciones de cadena para saber cómo extraer un subconjunto de una cadena más grande mediante una de las operaciones.

Operaciones para comparar el orden alfanumérico de dos cadenas

La operación COMPARE examina el primer carácter no coincidente de dos cadenas distintas. Esta operación se basa en el orden lexicográfico, que es el método utilizado para ordenar los términos en los diccionarios.

Esta operación devuelve la diferencia aritmética entre los valores ASCII de los primeros caracteres no coincidentes de las cadenas comparadas. Las siguientes diferencias son ejemplos:

- La diferencia entre “abc” y “and” es -1 (basada en la comparación de caracteres del tercer par).
- La diferencia entre “@” y “abc” es -33.
- La diferencia entre “1” y “abc” es -47.

A continuación se presenta la sintaxis de la operación COMPARE.

```
<text>.COMPARE(<string>)
```

Extraer un entero de una cadena de bytes que representan texto

Consulte la tabla Extracción de enteros para saber cómo tratar una cadena de bytes que representa el texto como una secuencia de bytes, extraer 8 bits, 16 bits o 32 bits de la secuencia y, a continuación, convertir los bits extraídos en un entero.

Convertir texto en un valor hash

Puede convertir una cadena de texto en un valor hash mediante la función HASH. Esta función devuelve un entero positivo de 31 bits como resultado de la operación. A continuación se presenta el formato de la expresión:

```
<text>.HASH
```

Esta función ignora las mayúsculas y los espacios en blanco. Por ejemplo, después de la operación, las dos cadenas Ab c y a bc producirían el mismo valor hash.

Codificar y decodificar texto aplicando el algoritmo de codificación Base64

Las dos funciones siguientes codifican y decodifican una cadena de texto aplicando el algoritmo de codificación Base64

Función	Descripción
text.B64ENCODE	Codifica la cadena de texto (designada por texto) aplicando el algoritmo de codificación Base64.
text.B64DECODE	Decodifica la cadena codificada en Base64 (designada por texto) aplicando el algoritmo de decodificación Base64. La operación genera un UNDEF si el texto no está en formato codificado B64.

Refinar la búsqueda en una acción de reescritura mediante la función EXTEND

La función EXTEND se utiliza en acciones de reescritura que especifican patrones o conjuntos de patrones y se dirigen a los cuerpos de los paquetes HTTP. Cuando se encuentra una coincidencia de patrón, la función EXTEND amplía el alcance de la búsqueda mediante un número predefinido de bytes a ambos lados de la cadena coincidente. A continuación, se puede utilizar una expresión regular para reescribir las coincidencias de esta región extendida. Las acciones de reescritura configuradas con la función EXTEND realizan reescrituras más rápidamente que las acciones de reescritura que evalúan cuerpos HTTP enteros utilizando únicamente expresiones regulares.

El formato de la función EXTEND es EXTEND (m, n), donde m y n son el número de bytes por los que se amplía el alcance de la búsqueda antes y después del patrón coincidente, respectivamente. Cuando se encuentra una coincidencia, el nuevo ámbito de búsqueda incluye m bytes que preceden inmediatamente a la cadena coincidente, a la propia cadena y a los n bytes que siguen a la cadena. Una expresión regular se puede utilizar para reescribir una parte de esta nueva cadena.

La función EXTEND solo se puede utilizar si la acción de reescritura en la que se utiliza cumple los siguientes requisitos:

- La búsqueda se realiza utilizando patrones o conjuntos de patrones (no expresiones regulares)
- La acción de reescritura evalúa solo los cuerpos de los paquetes HTTP.

Además, la función EXTEND solo se puede utilizar con los siguientes tipos de acciones de reescritura:

- replace_all
- insert_after_all
- delete_all
- insert_before_all

Por ejemplo, es posible que quiera eliminar todas las instancias dehttp://exampleurl.com/"" yhttp://exampleurl.au/"" de los primeros 1000 bytes del cuerpo. Para ello, puede configurar una acción de reescritura para buscar todas las instancias de la cadena exampleurl, ampliar el alcance de la búsqueda en ambos lados de la cadena cuando se encuentra una coincidencia y, a continuación, utilizar una expresión regular para reescribir en la región extendida. En el ejemplo siguiente se amplía el alcance de la búsqueda 20 bytes a la izquierda y 50 bytes a la derecha de la cadena coincidente:

```
add rewrite action delurl_example delete_all 'HTTP.REQ.BODY(1000)'-search
exampleurl -refineSearch 'extend(20,50).regex_select(re##http://exampleurl
.(com|au)##)'
```

Convertir texto a formato hexadecimal

La siguiente función convierte el texto a formato hexadecimal y extrae la cadena resultante:

```
<text>.BLOB_TO_HEX(<string>)
```


Por ejemplo, esta función convierte la cadena de bytes “abc” a “61:62:63”.

Cifrar y descifrar texto

En las expresiones de directivas avanzadas, puede utilizar las funciones ENCRYPT y DECRYPT para cifrar y descifrar texto. Los datos cifrados por la función ENCRYPT en un dispositivo Citrix ADC o en un par de alta disponibilidad (HA) determinados están diseñados para que la función DECRYPT los descifre en el mismo dispositivo Citrix ADC o par HA. El dispositivo admite los métodos de cifrado RC4, DES3, AES128, AES192 y AES256. El valor de clave necesario para el cifrado no es especificable por el usuario. Cuando se establece un método de cifrado, el dispositivo genera automáticamente un valor de clave aleatorio adecuado para el método especificado. El método predeterminado es el cifrado AES256, que es el método de cifrado más seguro y el que recomienda Citrix.

No es necesario configurar el cifrado a menos que quiera cambiar el método de cifrado o que el dispositivo genere un nuevo valor de clave para el método de cifrado actual.

Nota: También puede cifrar y descifrar cargas XML. Para obtener información sobre las funciones de cifrado y descifrado de cargas útiles XML, consulte Cifrar y descifrar cargas útiles XML.

Configurar cifrado

Durante el inicio, el dispositivo ejecuta el comando set ns encryptionParams con, de forma predeterminada, el método de cifrado AES256 y utiliza un valor de clave generado aleatoriamente adecuado para el cifrado AES256. El dispositivo también cifra el valor de la clave y guarda el comando, con el valor de clave cifrada, en el archivo de configuración de Citrix ADC. Por lo tanto, el método de cifrado AES256 está habilitado para las funciones ENCRYPT y DECRYPT de forma predeterminada. El valor clave que se guarda en el archivo de configuración persiste tras los reinicios, aunque el dispositivo ejecute el comando cada vez que lo reinicie.

Puede ejecutar el comando set ns encryptionParams manualmente o utilizar la utilidad de configuración si quiere cambiar el método de cifrado o si quiere que el dispositivo genere un nuevo valor de clave para el método de cifrado actual. Para utilizar la CLI para cambiar el método de cifrado, establezca solo el parámetro method, como se muestra en “**Ejemplo 1: Cambio del método de cifrado**. “ Si quiere que el dispositivo genere un nuevo valor de clave para el método de cifrado actual, establezca el parámetro method en el método de cifrado actual y el parámetro keyValue en una cadena vacía (“”), como se muestra en “**Ejemplo 2: Generación de un nuevo valor de clave para el método de cifrado actual**. “ Después de generar un nuevo valor de clave, debe guardar la configuración. Si no guarda la configuración, el dispositivo utiliza el valor de clave recién generado solo hasta el próximo reinicio, tras lo cual vuelve al valor clave de la configuración guardada.

Configurar el cifrado mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **Configuración**.
2. En el área **Configuración**, haga clic en **Cambiar parámetros de cifrado**.
3. En el cuadro de diálogo **Cambiar parámetros de cifrado**, realice una de las siguientes acciones:
   - Para cambiar el método de cifrado, en la lista Método, seleccione el método de cifrado que quiera.
   - Para generar un nuevo valor de clave para el método de cifrado actual, haga clic en Generar una nueva clave para el método seleccionado.
4. Haga clic en **Aceptar**.

Utilizar las funciones ENCRYPT y DECRYPT

Puede utilizar las funciones ENCRYPT y DECRYPT con cualquier prefijo de expresión que devuelva texto. Por ejemplo, puede utilizar las funciones ENCRYPT y DECRYPT en las directivas de reescritura para el cifrado de cookie. En el siguiente ejemplo, las acciones de reescritura cifran una cookie denominada MyCookie, que establece un servicio back-end, y descifran la misma cookie cuando un cliente la devuelve:

```
1 add rewrite action my-cookie-encrypt-action replace "HTTP.RES.
    SET_COOKIE.COOKIE("MyCookie").VALUE(0)" "HTTP.RES.SET_COOKIE.COOKIE(
    "MyCookie").VALUE(0).ENCRYPT"
2
3 add rewrite action my-cookie-decrypt-action replace "HTTP.REQ.COOKIE.
    VALUE("MyCookie")" "HTTP.REQ.COOKIE.VALUE("MyCookie").DECRYPT"
4 <!--NeedCopy-->
```

Después de configurar las directivas de cifrado y descifrado, guarde la configuración para que las directivas entren en vigor.

Configurar clave de cifrado para el cifrado de terceros

En las expresiones de directivas avanzadas, puede utilizar las funciones ENCRYPT y DECRYPT para cifrar y descifrar texto en una solicitud o respuesta. Los datos cifrados por la función ENCRYPT en un dispositivo (autónomo, de alta disponibilidad o clúster) están diseñados para que la función DECRYPT los descifre el mismo dispositivo. El dispositivo admite los métodos de cifrado RC4, DES, Triple-DES, AES92 y AES256 y cada uno de estos métodos utiliza una clave secreta tanto para el cifrado como para el descifrado de datos. Puede utilizar cualquiera de estos métodos para cifrar y descifrar datos de dos maneras: autocifrado y cifrado de terceros.

La función de autocifrado de un dispositivo (independiente, de alta disponibilidad o clúster) cifra y, a continuación, descifra los datos mediante la evaluación del valor del encabezado. Un ejemplo para

entender esto es el cifrado HTTP Cookie. La expresión evalúa el encabezado, cifra el valor de la cookie HTTP en el encabezado Set-Cookie de la respuesta saliente y, a continuación, descifra el valor de la cookie cuando se devuelve en el encabezado de cookie de una solicitud entrante posterior del cliente. El valor de clave no es configurable por el usuario; en cambio, cuando se configura un método de cifrado en el comando set ns encryptionParams, el dispositivo genera automáticamente un valor de clave aleatorio para el método configurado. De forma predeterminada, el comando utiliza el método de cifrado AES256, que es el método de alta seguridad y Citrix recomienda este método.

La función de cifrado de terceros cifra o descifra los datos con una aplicación de terceros. Por ejemplo, un cliente puede cifrar los datos de una solicitud y el dispositivo los descifra antes de enviarlos al servidor back-end o viceversa. Para ello, el dispositivo y la aplicación de terceros deben compartir una clave secreta. En el dispositivo, puede configurar directamente la clave secreta mediante un objeto de clave de cifrado y el dispositivo genera automáticamente el valor de la clave para un cifrado más seguro. La misma clave se configura manualmente en el dispositivo de terceros para que tanto el dispositivo como la aplicación de terceros puedan utilizar la misma clave para cifrar y descifrar datos.

Nota: Con el cifrado de terceros, también puede cifrar y descifrar cargas útiles XML. Para obtener información sobre las funciones de cifrado y descifrado de cargas útiles XML, consulte “Cifrado y descifrado de cargas útiles XML.

Métodos de cifrado

Un método de cifrado proporciona dos funciones: una función de cifrado que transforma una secuencia de bytes de texto sin formato en una secuencia de bytes de texto cifrado y una función de descifrado que transforma el texto cifrado en texto sin formato. Los métodos de cifrado utilizan secuencias de bytes denominadas claves para realizar el cifrado y el descifrado. Los métodos de cifrado que utilizan la misma clave para el cifrado y el descifrado se denominan simétricos. Los métodos de cifrado que utilizan claves diferentes para el cifrado y el descifrado son asimétricos. Los ejemplos más notables de cifrados asimétricos se encuentran en la criptografía de clave pública, que utiliza una clave pública disponible para cualquier persona para el cifrado y una clave privada conocida solo por el descifrador.

Un buen método de cifrado hace inviable descifrar (“descifrar”) el texto cifrado si no posee la clave. “No factible” significa realmente que descifrar el texto cifrado tomaría más tiempo y recursos informáticos de lo que vale la pena. A medida que las computadoras se vuelven más potentes y baratas, los cifrados que antes eran inviables de descifrar se vuelven más factibles. Además, con el tiempo, se encuentran fallas en los métodos de cifrado (o en sus implementaciones), lo que facilita el descifrado. Por lo tanto, se prefieren los métodos de cifrado más nuevos a los más antiguos. En general, las claves de mayor longitud proporcionan una mayor seguridad que las claves más cortas, a costa de tiempos de cifrado y descifrado más largos.

Un método de cifrado puede utilizar cifrados de flujo o de bloques. RC4 es el cifrado de flujo más

seguro y solo se utiliza para aplicaciones heredadas. Los cifrados de bloques pueden incluir relleno.

Cifrados Stream

Un método de cifrado de flujo funciona en bytes individuales. Solo hay un cifrado de flujo disponible en los dispositivos Citrix ADC: RC4, que utiliza una longitud de clave de 128 bits (16 bytes). Para una clave dada, RC4 genera una secuencia pseudoaleatoria de bytes, llama a un flujo de claves, que está en X o con el texto sin formato para producir el texto cifrado. RC4 ya no se considera seguro y solo debe utilizarse si lo requieren las aplicaciones heredadas.

Cifrados por bloques

Un método de cifrado por bloques funciona en un bloque fijo de bytes. Un dispositivo Citrix ADC proporciona dos cifrados por bloques: Estándar de cifrado de datos (DES) y Estándar de cifrado avanzado (AES). DES utiliza un tamaño de bloque de 8 bytes y (en un dispositivo Citrix ADC) dos opciones de longitud de clave: 64 bits (8 bytes), de los cuales 56 bits son datos y 8 bits son paridad, y Triple-DES, una longitud de clave de 192 bits (24 bytes). AES tiene un tamaño de bloque de 16 bytes y (en Citrix ADC) tres opciones de longitud de clave: 128 bits (16 bytes), 192 bits (24 bytes) y 256 bits (32 bytes).

Acolchado

Si el texto sin formato de un cifrado de bloque no es un número integral de bloques, puede ser necesario rellenar con más bytes. Por ejemplo, supongamos que el texto sin formato es “xyzzy” (hex 78797a7a79). Para un bloque Triple-DES de 8 bytes, este valor tendría que rellenarse para crear 8 bytes. El esquema de relleno debe permitir que la función de descifrado determine la longitud del texto sin formato original después del descifrado. A continuación se presentan algunos esquemas de relleno actualmente en uso (n es el número de bytes agregados):

- PKCS7: Suma n bytes de valor n cada uno. Por ejemplo, 78797a7a79030303. Este es el esquema de relleno utilizado por OpenSSL y la función de directiva ENCRYPT(). El esquema de relleno PKCS5 es el mismo que el de PKCS7.
- ANSI X.923: Agrega n-1 cero bytes y un byte final de valor n. Por ejemplo, 78797a7a79000003.
- ISO 10126: Agrega n-1 bytes aleatorios y un byte final de valor n. Por ejemplo, 78797a7a79xxxx03, donde xx puede ser cualquier valor de byte. La función de directiva DECRYPT() acepta este esquema de relleno, lo que también le permite aceptar los esquemas PKCS7 y ANSI X.923.
- ISO/IEC 7816-4: agrega un byte 0x80 y n-1 cero bytes. Por ejemplo, 78797a7a79800000. Esto también se llama relleno OneAndZeros.
- Cero: agrega n cero bytes. Ejemplo: 78797a7a79000000. Solo se puede utilizar con texto sin formato que no incluya bytes NUL.

Si se utiliza relleno y el texto sin formato es un número integral de bloques, normalmente se agrega un bloque adicional para que la función de descifrado pueda determinar sin ambigüedades la longitud original del texto sin formato. Para PCKS7 y bloque de 8 bytes, sería 0808080808080808.

Modos de operación

Hay varios modos de operación diferentes para los cifrados por bloques, que especifican cómo se cifran varios bloques de texto sin formato. Algunos modos utilizan un vector de inicialización (VI), un bloque de datos aparte del texto sin formato que se utiliza para iniciar el proceso de cifrado. Es una buena práctica utilizar un VI diferente para cada cifrado, de modo que el mismo texto sin formato produzca un texto cifrado diferente. El VI no necesita ser secreto, por lo que se antecede al texto cifrado. Los modos incluyen:

- Libro de códigos electrónico (ECB): Cada bloque de texto sin formato se cifra de forma independiente. No se utiliza una vía intravenosa. El relleno es necesario si el texto sin formato no es un múltiplo del tamaño del bloque de cifrado. El mismo texto sin formato y la misma clave siempre producen el mismo texto cifrado. Por este motivo, el ECB se considera menos seguro que otros modos y solo debe utilizarse para aplicaciones heredadas.
- Encadenamiento de bloques de cifrado (CBC): Cada bloque de texto sin formato se somete a XOR con el bloque de texto cifrado anterior, o el VI del primer bloque, antes de cifrarse. El relleno es necesario si el texto sin formato no es un múltiplo del tamaño del bloque de cifrado. Este es el modo que se utiliza con el método Citrix ADC encryptionParams.
- Retroalimentación de cifrado (CFB): El bloque de texto cifrado anterior, o el VI del primer bloque, se cifra y la salida se realiza con XOR con el bloque de texto sin formato actual para crear el bloque de texto cifrado actual. La retroalimentación puede ser de 1 bit, 8 bits o 128 bits. Puesto que el texto sin formato se somete a XOR con el texto cifrado, no es necesario rellenar.
- Retroalimentación de salida (OFB): Se genera una secuencia de claves aplicando el cifrado sucesivamente al VI y XORing los bloques keystream con el texto sin formato. No es necesario acolchado.

Configurar claves de cifrado para el cifrado de terceros

A continuación se presentan las tareas de configuración que se realizan en la configuración de la clave de cifrado.

1. Agregar una clave de cifrado. Configura una clave de cifrado para un método de cifrado especificado con un valor de clave especificado.
2. Modificación de una clave de cifrado. Puede modificar los parámetros de una clave de cifrado configurada.
3. Desconfiguración de una clave de cifrado. Establece los parámetros de una clave de cifrado configurada en sus valores predeterminados. Debe existir un valor de encryptionKey con el

nombre. Establece el relleno en DEFAULT (determinado por el método), elimina un VI existente, lo que hace que ENCRYPT() genere un VI aleatorio. Elimina un comentario existente. El método y el valor de la clave no se pueden restablecer.

4. Eliminación de una clave de cifrado. Elimina una clave de cifrado configurada. La clave no puede tener ninguna referencia.
5. Muestra una clave de encriptación. Muestra los parámetros de la clave de cifrado configurada o de todas las claves configuradas. Si se omite el nombre, el valor clave no se muestra.

Agregar una clave de cifrado mediante la CLI

En el símbolo del sistema, escriba:

```
add ns encryptionKey <name> -method <method> [-keyValue <keyvalue>][-
padding (OFF | ON)] [-iv <hexstring>] -keyValue <keyvalue> [-comment <
string>]
```

Donde:

```
1 <method> = ( NONE | RC4 | DES3 | AES128 | AES192 | AES256 | DES | DES-
     CBC | DES-CFB | DES-OFB | DES-ECB | DES3-CBC | DES3-CFB | DES3-OFB |
      DES3-ECB | AES128-CBC | AES128-CFB | AES128-OFB | AES128-ECB |
     AES192-CBC | AES192-CFB | AES192-OFB | AES192-ECB | AES256-CBC |
     AES256-CFB | AES256-OFB | AES256-ECB ) <hexstring> = hex-encoded
     byte sequence
2 <!--NeedCopy-->
```

Los métodos de cifrado anteriores especifican el modo de operación con CBC como modo de operación predeterminado. Por lo tanto, los métodos DES, DES2, AES128, AES192 y AES256 son equivalentes a los métodos DES-CBC, DES3-CBC, AES128-CBC, AES192-CBC y AES256-CBC.

Modificar una clave de cifrado mediante la CLI

En el símbolo del sistema, escriba:

```
set ns encryptionKey <name> [-method <method>] [-keyValue <keyvalue>] [-
padding ( OFF | ON )] [-iv <string>] [-comment <string>]
```

Desestablecer una clave de cifrado mediante la CLI

En el símbolo del sistema, escriba:

```
unset ns encryptionKey <name> [-padding] [-iv] [-comment]
```


Quitar una clave de cifrado mediante la CLI

En el símbolo del sistema, escriba:

```
rm ns encryptionKey <name>
```

Mostrar una clave de cifrado mediante la CLI

En el símbolo del sistema, escriba:

Ejemplo:

```
show ns encryptionKey [<name>]

add ns encryptionKey my_key -method aes256 -keyValue 26
    ea5537b7e0746089476e5658f9327c0b10c3b4778c673a5b38cee182874711 -iv
    c2bf0b2e15c15004d6b14bcdc7e5e365
set ns encryptionKey my_key -keyValue
    b8742b163abcf62d639837bbee3cef9fb5842d82d00dfe6548831d2bd1d93476
unset ns encryptionKey my_key -iv
rm ns encryptionKey my_key
show ns encryptionKey my_key
Name: my_key
Method: AES256
Padding: DEFAULT
Key Value: (not disclosed)
<!--NeedCopy-->
```

Agregar una clave de cifrado mediante la interfaz gráfica de usuario

Vaya a **Sistema** > **Claves de cifrado** y haga clic en **Agregar** para crear una clave de cifrado.

Modificar una clave de cifrado mediante la interfaz gráfica de usuario

Vaya a **Sistema** > **Claves de cifrado** y haga clic en **Modificar** para modificar los parámetros de una clave de cifrado configurada.

Quitar una clave de cifrado mediante la interfaz gráfica de usuario

Vaya a **Sistema** > **Claves de cifrado** y haga clic en **Eliminar**.

Funciones ENCRYPT y DECRYPT para cifrado de terceros

A continuación se presenta la función ENCRYPT utilizada para el cifrado de terceros.

```
ENCRYPT (encryptionKey, out_encoding)
```

Donde:

Los datos de entrada del dispositivo son el texto que se va a cifrar

encryptionKey: Parámetro de cadena opcional que especifica el objeto de clave de cifrado configurado para proporcionar el método de cifrado, el valor de la clave secreta y otros parámetros de cifrado. Si se omite, el método utiliza el valor de clave generado automáticamente asociado al comando set ns encryptionParamS.

out_encoding: Este valor especifica cómo se codifica la salida. Si se omite, se utiliza la codificación BASE64.

Entrada:

```
BASE64: original PEM base64-encoding: 6 bits (0..63) encoded as one
    ASCII character:
                  0..23 = 'A'..'Z', 24..51 = 'a'..'z', 52..61 = '0'..'9
                     ', 62 = '+', 63 = '/', '=' = pad byte.
       BASE64URL:  URL and Filename safe base64-encoding: same as BASE64
            except 62 = '-', 63 = '_'
       HEX_UPPER:  Hexadecimal with 0..9 = '0'..'9' and 10..15 = 'A'..'F
          '.
       HEX_LOWER:  Hexadecimal with 0..9 = '0'..'9' and 10..15 = 'a'..'f
          '.
       HEX_COLONS: Hexadecimal with 0..9 = '0'..'9' and 10..15 = 'A'..'F
          '; ':' between each hex byte. Matches BLOB_TO_HEX() output
          format
       HEX:  For input, accepts HEX_UPPER, HEX_LOWER, and HEX_COLONS
          format. For output, produces HEX_LOWER format
<!--NeedCopy-->
```

Salida: El resultado es un texto cifrado mediante el método y la clave especificados y codificado mediante una codificación de salida especificada. Inserta un VI generado antes del texto cifrado para los métodos y modos de bloque que requieren una VI, y no se especifica ninguna VI para la EncryptionKey o se omite la EncryptionKey.

A continuación se presenta la función DECRYPT utilizada para el descifrado de terceros.

```
DECRYPT(encryptionKey, in_encoding)
```

Donde:

Los datos de entrada son un texto cifrado que utiliza el método especificado y la clave codificados mediante la codificación de entrada especificada. Se espera que este texto incluya un VI generado antes del texto cifrado para los métodos y modos de bloque que requieren una VI, y no se especifica ninguna VI para la EncryptionKey o se omite la EncryptionKey.

encryptionKey: parámetro de cadena opcional que especifica el objeto EncryptionKey configurado para proporcionar el método de cifrado, la clave secreta y otros parámetros de cifrado. Si se omite, se utilizará el método y la clave generada automáticamente asociada a la configuración encryption-Params

in_encoding: parámetro de enumeración opcional que especifica cómo se espera que se codifique la entrada. Los valores son los mismos que los out_encoding de ENCRYPT. Si se omite, se espera la codificación BASE64.

Los datos de salida son un texto descifrado sin codificar.

Variantes y parámetros opcionales

A continuación se presentan las variantes de estas funciones con los parámetros opcionales:

Variante	Descripción
ENCRYPT	Utilice el comando encryptionParams y el parámetro de codificación de salida BASE64.
ENCRYPT(out_encoding)	Utilice encryptionParams y el parámetro de codificación de salida especificado.
ENCRYPT(encryptionKey)	Utilice el parámetro de codificación de salida encryptionKey y BASE64 especificado.
ENCRYPT(encryptionKey, out_encoding)	Utilice el parámetro encryptionKey y el parámetro de codificación de salida especificados.
DECRYPT	Utilice el comando encryptionParams y el parámetro de codificación de entrada BASE64.
DECRYPT(out_encoding)	Utilice el comando encryptionParams y el parámetro de codificación de entrada especificado.
DECRYPT(encryptionKey)	Utilice el parámetro de codificación de entrada encryptionKey y BASE64 especificado.
DECRYPT(encryptionKey, out_encoding)	Utilice el parámetro encryptionKey y de codificación de entrada especificados.

Configurar claves HMAC

Los dispositivos Citrix ADC admiten una función de código de autenticación de mensajes con hash (HMAC) que calcula un método de resumen o un hash del texto de entrada mediante una clave secreta compartida entre el remitente del mensaje y el receptor del mensaje. El método de resumen (derivado de una técnica RFC 2104) autentica al remitente y verifica que el contenido del mensaje no se haya alterado. Por ejemplo, cuando un cliente envía un mensaje con la clave HMAC compartida a un dispositivo Citrix ADC, las expresiones de directiva avanzadas (PI) utilizan la función HMAC para calcular el código basado en hash del texto seleccionado. Luego, cuando el receptor recibe el mensaje con la clave secreta, vuelve a calcular el HMAC comparándolo con el HMAC original para determinar si el mensaje ha sido alterado. La función HMAC es compatible con dispositivos independientes y dispositivos en una configuración de alta disponibilidad o en un clúster. Su uso es similar a configurar una clave de cifrado.

Los comandos add ns hmackey y set ns hmackey incluyen un parámetro que especifica el método de resumen y la clave secreta compartida que se utilizará para el cálculo de HMAC.

Para configurar una clave HMAC, debe realizar lo siguiente:

1. Agregar una clave HMAC. Configura una clave HMAC con un valor de clave especificado.
2. Modificación de una clave HMAC. Modifica los parámetros de una clave HMAC configurada. El método de resumen se puede cambiar sin cambiar el valor clave, ya que el resumen no determina la longitud del valor clave. Sin embargo, es aconsejable especificar una nueva clave al cambiar el resumen.
3. Desajuste de una clave HMAC. Establece los parámetros de una clave HMAC configurada en sus valores predeterminados. Debe existir un objeto hmacKey con el nombre. El único parámetro que se puede anular es el comentario, que se elimina.
4. Extracción de una clave HMAC. Elimina una clave configurada. La clave no puede tener ninguna referencia.
5. Muestra una clave HMAC. Muestra los parámetros de la clave ac HMAC configurada o de todas las claves configuradas. Si se omite el nombre, el valor clave no se muestra.

Configurar una clave HMAC única y aleatoria

Puede generar automáticamente una clave HMAC única. Si el dispositivo es una configuración de clúster, la clave HMAC se genera al inicio del proceso y se distribuye a todos los nodos y motores de paquetes. Esto garantiza que la clave HMAC sea la misma para todos los motores de paquetes y todos los nodos del clúster.

En el símbolo del sistema, escriba:

```
add ns hmacKey <your_key> -digest <digest> -keyValue <keyvalue>
```

Ejemplo:


```
add ns hmacKey <name> -digest sha1 -keyValue AUTO
```

Donde:

- La sintaxis del nombre es correcta y no duplica el nombre de una clave existente.
- El valor de clave “AUTO” se puede utilizar en los comandos set para generar nuevas claves para los objetos EncrytionKey y hmacKey existentes.

> **Nota:**
>
> La generación automática de claves resulta útil si el dispositivo Citrix ADC cifra y descifra datos con la clave o genera y verifica una clave HMAC. Dado que el valor de la clave en sí ya está cifrado cuando se muestra, no puede recuperar el valor de clave generado para que lo utilice ninguna otra parte.

Ejemplo:

```
add ns hmacKey my_hmac_key -digest sha1 -keyValue 0c753c6c5ef859189cacdf95b506d02c179
```

Los métodos de cifrado anteriores especifican el modo de operación con CBC como modo de operación predeterminado. Por lo tanto, los métodos DES, DES2, AES128, AES192 y AES256 son equivalentes a los métodos DES-CBC, DES3-CBC, AES128-CBC, AES192-CBC y AES256-CBC.

Modificar una clave HMAC mediante la CLI

Este comando modifica los parámetros configurados para una clave HMAC. Puede cambiar el resumen sin cambiar el valor clave, ya que el resumen no determina la longitud del valor clave. Sin embargo, es aconsejable especificar una nueva clave al cambiar el resumen. En el símbolo del sistema, escriba:

```
1 set ns hmacKey <name> [-digst <digest>] [-keyValue <keyvalue>]
2 [-comment <string>]
3
4 <!--NeedCopy-->
```

Desconfigurar una clave HMAC mediante la CLI

Este comando establece los parámetros configurados para una clave HMAC con sus valores predeterminados. Debe existir un objeto hmacKey con el nombre. El único parámetro que se puede desactivar es la opción de comentario, que se elimina. En el símbolo del sistema, escriba:

```
unset ns hmacKey <name> -comment
```


Eliminar una clave HMAC mediante la CLI

Este comando elimina la clave hmac configurada. La clave no puede tener referencias. En el símbolo del sistema, escriba:

```
rm ns hmacKey <name>
```

Mostrar una clave HMAC mediante la CLI

En el símbolo del sistema, escriba:

```
show ns encryptionKey [<name>]

add ns hmacKey my_hmac_key -digest sha1 -keyValue 0
    c753c6c5ef859189cacdf95b506d02c1797407d
set ns hmacKey my_hmac_key -keyValue
    f348c594341a840a1f641a1cf24aa24c15eb1317
rm ns hmacKey my_hmac_key
show ns hmacKey my_hmac_key
           Name: my_hmac_key
     Digest: SHA1
     Key Value: (not disclosed)
<!--NeedCopy-->
```

Expresiones de directiva avanzadas: Trabajar con fechas, horas y números

January 12, 2021

La mayoría de los datos numéricos que procesa el dispositivo Citrix ADC consta de fechas y horas. Además de trabajar con fechas y horas, el dispositivo procesa otros datos numéricos, como la longitud de las solicitudes y respuestas HTTP. Para procesar estos datos, puede configurar expresiones de directiva avanzadas que procesen números.

Una expresión numérica consiste en un prefijo de expresión que devuelve un número y, a veces, pero no siempre, un operador que puede realizar una operación en el número. Ejemplos de prefijos de expresión que devuelven números son `SYS.TIME.DAY`, `HTTP.REQ.CONTENT_LENGTH` y `HTTP.RES.BODY.LENGTH`. `Numeric` los operadores pueden trabajar con cualquier expresión de prefijo que devuelva datos en formato numérico. El operador, `GT(<int>)` por ejemplo, se puede utilizar con cualquier expresión de prefijo, como HTTP.REQ.CONTENT_LENGTH, que devuelve un entero.

Formato de fechas y horas en una expresión

August 20, 2021

Al configurar una expresión de directiva avanzada en una directiva que funcione con fechas y horas (por ejemplo, la hora del sistema Citrix ADC o una fecha en un certificado SSL), especifique un formato de hora como se indica a continuación:

```
GMT|LOCAL [<yyyy>] [<month>] [<d>] [<h>] [<m>] [<s>]
```

Donde:

- <yyyy>es un año de cuatro dígitos después de GMT o LOCAL.
- <month>es una abreviatura de tres caracteres para el mes, por ejemplo, Jan, Dic.
- <d>es un día de la semana o un entero para la fecha.

  No puede especificar el día como lunes, martes, etc. Especifique un entero para un día específico del mes o especifique una fecha como el primer, segundo, tercer día de la semana del mes, etc. A continuación se presentan ejemplos de especificar un día de la semana:

  - Sun_1 es el primer domingo del mes.
  - Sun_3 es el tercer domingo del mes.
  - Wed_3 es el tercer miércoles del mes.
  - 30 es un ejemplo de una fecha exacta en un mes.
- <h>es la hora, por ejemplo, 10h.
- <s> es el número de segundos, por ejemplo, 30s.

La expresión de ejemplo siguiente es true si la fecha está entre 2008 Jan y 2009 Jan, basada en GMT.

```
http.req.date.between(GMT 2008 Jan, GMT 2009 Jan)
```

La expresión de ejemplo siguiente es verdadera para marzo y todos los meses que siguen a marzo del año calendario, según GMT:

```
sys.time.ge(GMT 2008 Mar)
```

Cuando especifique una fecha y hora, tenga en cuenta que el formato distingue entre mayúsculas y minúsculas y debe conservar el número exacto de espacios en blanco entre las entradas.

```
1 **Note:**
2
3 In an expression that requires two time values, both must use GMT or
     both must use LOCAL. You cannot mix the two in an expression.
4
```



```
Unlike when you use the SYS.TIME prefix in an advanced policy
    expression, if you specify SYS.TIME in a rewrite action, the Citrix
    ADC returns a string in conventional date format (for example, Sun,
    06 Nov 1994 08:49:37 GMT). For example, the following rewrite action
     replaces the http.res.date header with the Citrix ADC system time
    in a conventional date format:

add rewrite action sync_date replace http.res.date sys.time
```

Expresiones para la hora del sistema Citrix ADC

August 20, 2021

El prefijo de expresión SYS.TIME extrae la hora del sistema Citrix ADC. Puede configurar expresiones que determinen si un evento concreto se produjo en un momento determinado o dentro de un intervalo de tiempo determinado de acuerdo con la hora del sistema Citrix ADC.

En la tabla siguiente se describen las expresiones que puede crear mediante el prefijo SYS.TIME.

- **SYS.TIME.BETWEEN(<time1>, <time2>):**

  Devuelve un valor booleano TRUE si el valor devuelto es posterior <time1> y anterior a <time2>.

  Dar formato a los <time1> <time2> argumentos, de la siguiente manera:

  - Ambos deben ser GMT o ambos LOCAL.
  - <time2>debe ser más tarde que <time1>.

  Por ejemplo, si la hora actual es GMT 2005 May 1 10h 15m 30s, y es el primer domingo del mes, puede especificar lo siguiente:

  - sys.time.between (GMT 2004, GMT 2006)
  - sys.time.between (GMT 2004 Jan, GMT 2006 Nov)
  - sys.time.between (GMT 2004 Jan, GMT 2006)
  - sys.time.between(GMT 2005 May Sun_1, GMT 2005 May Sun_3)
  - sys.time.between(GMT 2005 May 1, GMT May 2005 1)
  - sys.time.between(LOCAL 2005 May 1, LOCAL May 2005 1)

- **SYS.TIEM.DÍA:**

  Devuelve el día actual del mes como un número del 1 al 31.

- **SYS.TIME.EQ(<time>):**

  Devuelve un valor booleano TRUE si la hora actual es igual al <time> argumento.

Por ejemplo, si la hora actual es GMT 2005 May 1 10h 15m 30s, y es el primer domingo del mes, puede especificar lo siguiente (los resultados de la evaluación se muestran entre paréntesis):

- sys.time.eq (GMT 2005) (TRUE en este ejemplo).
- sys.time.eq (GMT 2005 Dec) (FALSE en este ejemplo).
- sys.time.eq (LOCAL 2005 May) (Se evalúa como TRUE o FALSE en este ejemplo, en función de la zona horaria actual).
- sys.time.eq (GMT 10h) (TRUE en este ejemplo).
- sys.time.eq (GMT 10h 30s) (TRUE en este ejemplo).
- sys.time.eq (GMT 10 de mayo) (TRUE en este ejemplo).
- sys.time.eq (GMT Sun) (TRUE en este ejemplo).
- sys.time.eq (GMT May Sun_1) (TRUE en este ejemplo).

- **SYS.TIME.NE(<time>):**

  Devuelve un valor booleano TRUE si la hora actual no es igual al <time> argumento.

- **SYS.TIME.GE(<time>):**

  Devuelve un valor booleano TRUE si la hora actual es posterior o igual a <time>.

  Por ejemplo, si la hora actual es GMT 2005 May 1 10h 15m 30s, y es el primer domingo del mes, puede especificar lo siguiente (los resultados de la evaluación se muestran entre paréntesis):

  - sys.time.ge (GMT 2004) (TRUE en este ejemplo).
  - sys.time.ge (GMT 2005 Jan) (TRUE en este ejemplo).
  - sys.time.ge (LOCAL 2005 May) (TRUE o FALSE en este ejemplo, en función de la zona horaria actual).
  - sys.time.ge (GMT 8h) (TRUE en este ejemplo).
  - sys.time.ge (GMT 30m) (FALSE en este ejemplo).
  - sys.time.ge (GMT 10 de mayo) (TRUE en este ejemplo).
  - sys.time.ge (GMT May 10h 0m) (TRUE en este ejemplo).
  - sys.time.ge (GMT Sun) (TRUE en este ejemplo).
  - sys.time.ge (GMT May Sun_1) (TRUE en este ejemplo).

- **SYS.TIME.GT(<time>):**

  Devuelve un valor booleano TRUE si el valor de tiempo es posterior al <time> argumento.

  Por ejemplo, si la hora actual es GMT 2005 May 1 10h 15m 30s, y es el primer domingo del mes, puede especificar lo siguiente (los resultados de la evaluación se muestran entre paréntesis):

  - sys.time.gt (GMT 2004) (TRUE en este ejemplo).
  - sys.time.gt (GMT 2005 Jan) (TRUE en este ejemplo).
  - sys.time.gt (LOCAL 2005 May) (VERDADERO o FALSE, en función de la zona horaria actual).
  - sys.time.gt (GMT 8h) (TRUE en este ejemplo).
  - sys.time.gt (GMT 30m) (FALSE en este ejemplo).

- sys.time.gt (GMT May 10h) (FALSE en este ejemplo).
- sys.time.gt (GMT May 10h 0m) (TRUE en este ejemplo).
- sys.time.gt (GMT Sun) (FALSE en este ejemplo).
- sys.time.gt (GMT May Sun_1) (FALSE en este ejemplo).

- **SYS.TIME.HOURS:**

  Devuelve la hora actual como un entero de 0 a 23.

- **SYS.TIME.LE(<time>):**

  Devuelve un valor booleano TRUE si el valor de tiempo actual precede o es igual al <time> argumento.

  Por ejemplo, si la hora actual es GMT 2005 May 1 10h 15m 30s, y es el primer domingo del mes, puede especificar lo siguiente (los resultados de la evaluación se muestran entre paréntesis):

  - sys.time.le (GMT 2006) (TRUE en este ejemplo).
  - sys.time.le (GMT 2005 Dec) (TRUE en este ejemplo).
  - sys.time.le (LOCAL 2005 May) (TRUE o FALSE en función de la zona horaria actual).
  - sys.time.le (GMT 8h) (FALSE en este ejemplo).
  - sys.time.le (GMT 30m) (TRUE en este ejemplo).
  - sys.time.le (GMT May 10h) (TRUE en este ejemplo).
  - sys.time.le (GMT Jun 11h) (TRUE en este ejemplo).
  - sys.time.le (GMT Wed) (TRUE en este ejemplo).
  - sys.time.le (GMT May Sun_1) (TRUE en este ejemplo).

- **SYS.TIME.LT(<time>):**

  Devuelve un valor booleano TRUE si el valor de hora actual precede al <time> argumento.

  Por ejemplo, si la hora actual es GMT 2005 May 1 10h 15m 30s, y es el primer domingo del mes, puede especificar lo siguiente (los resultados de la evaluación se muestran entre paréntesis):

  - sys.time.lt (GMT 2006) (TRUE en este ejemplo).
  - sys.time.lt.time.lt (GMT 2005 Dec) (TRUE en este ejemplo).
  - sys.time.lt (LOCAL 2005 mayo) (TRUE o FALSE en función de la zona horaria actual).
  - sys.time.lt (GMT 8h) (FALSE en este ejemplo).
  - sys.time.lt (GMT 30m) (TRUE en este ejemplo).
  - sys.time.lt (GMT May 10h) (FALSE en este ejemplo).
  - sys.time.lt (GMT Jun 11h) (TRUE en este ejemplo).
  - sys.time.lt (GMT Wed) (TRUE en este ejemplo).
  - sys.time.lt (GMT May Sun_1) (FALSE en este ejemplo).

- **SYS.TIME.MINUTES:**

  Devuelve el minuto actual como un entero de 0 a 59.

- **SYS.TIEM.MONES:**

  Extrae el mes actual y devuelve un entero del 1 (enero) al 12 (diciembre).

- **SYS.TIME.RELATIVE_BOOT:**

  Calcula el número de segundos para el reinicio anterior o programado más cercano y devuelve un entero.

  Si el tiempo de arranque más cercano está en el pasado, el entero es negativo. Si está en el futuro, el entero es positivo.

- **SYS.TIME.RELATIVE_NOW:**

  Calcula el número de segundos entre la hora actual del sistema Citrix ADC y la hora especificada, y devuelve un entero que muestra la diferencia.

  Si la hora designada está en el pasado, el entero es negativo; si está en el futuro, el entero es positivo.

- **SYS.TIME.SECONDS:**

  Extrae los segundos de la hora actual del sistema Citrix ADC y devuelve ese valor como un entero de 0 a 59.

- **SYS.TIME.WEEKDAY:**

  Devuelve el día de la semana actual como un valor comprendido entre 0 (domingo) y 6 (sábado).

- **SYS.TIME.WITHIN (<time1>, <time2>):**

  Si omite un elemento de tiempo en <time1>, por ejemplo, el día o la hora, se supone que tiene el valor más bajo en su rango. Si omite un elemento en <time2>, se supone que tiene el valor más alto de su rango.

  Los rangos de los elementos de tiempo son los siguientes: Mes 1-12, día 1-31, días laborables 0-6, hora 0-23, minutos 0-59 y segundos 0-59. Si especifica el año, debe hacerlo en ambos <time1> y <time2>.

  Por ejemplo, si la hora es GMT 2005 10 de mayo 10h 15m 30s, y es el segundo martes del mes, puede especificar lo siguiente (los resultados de la evaluación se muestran entre paréntesis):

  - sys.time.within (GMT 2004, GMT 2006) (TRUE en este ejemplo).
  - sys.time.within (GMT 2004 Jan, GMT 2006 Mar) (FALSE, mayo no está en el rango de enero a marzo).
  - sys.time.within (GMT Feb, GMT) (TRUE, mayo está en el rango de febrero a diciembre).
  - sys.time.within (GMT Sun_1, GMT Sun_3) (TRUE, el segundo martes es entre el primer domingo y el tercer domingo).
  - sys.time.within (GMT 2005 May 1 10h, GMT May 2005 1 17h) (TRUE en este ejemplo).

  - sys.time.within (LOCAL 2005 1 de mayo, LOCAL 1 de mayo de 2005) (TRUE o FALSE, en función de la zona horaria del sistema Citrix ADC).

- **SYS.TIEM.AÑO:**

  Extrae el año de la hora actual del sistema y devuelve ese valor como un entero de cuatro dígitos.

Expresiones para fechas de certificado SSL

August 20, 2021

Puede determinar el período de validez de los certificados SSL configurando una expresión que contenga el prefijo siguiente:

```
CLIENT.SSL.CLIENT_CERT
```

La expresión de ejemplo siguiente coincide con un tiempo concreto de caducidad con la información del certificado:

```
client.ssl.client_cert.valid_not_after.eq(GMT 2009)
```

En la tabla siguiente se describen las operaciones basadas en el tiempo en certificados SSL. Para obtener la expresión que quiera, reemplace el *certificado* de la expresión de la primera columna con la expresión de prefijo “CLIENT.SSL.CLIENT_CERT”.

- `<certificate>.VALID_NOT_AFTER`:

  Devuelve el último día antes de la expiración del certificado. El formato devuelto es el número de segundos desde el 1 de enero de 1970 GMT (0 horas, 0 minutos, 0 segundos).

- **<certificate>.VALID_NOT_AFTER.BREANT (<time1>, <time2>):**

  Devuelve un valor booleano TRUE si la validez del certificado está entre los <time1> <time2> argumentos y. Ambos <time1> y <time2> deben especificarse completamente. A continuación se presentan ejemplos:

  GMT 1995 Jan está completamente especificado.

  GMT Jan no está completamente especificado

  GMT 1995 20 no está totalmente especificado.

  GMT Jan Mon_2 no está completamente especificado.

  <time1> <time2>Los argumentos y deben ser tanto GMT como LOCAL, y <time2> deben ser mayores que <time1>.

  Por ejemplo, si es GMT 2005 May 1 10h 15m 30s, y el primer domingo del mes, puede especificar lo siguiente (los resultados de la evaluación están entre paréntesis).

- …between(GMT 2004, GMT 2006) (TRUE)
- …between(GMT 2004 Jan, GMT 2006 Nov) (TRUE)
- …between(GMT 2004 Jan, GMT 2006) (TRUE)
- …between(GMT 2005 May Sun_1, GMT 2005 May Sun_3) (TRUE)
- …between(GMT 2005 May 1, GMT May 2005 1) (TRUE)
- …between(LOCAL 2005 May 1, LOCAL May 2005 1) (TRUE or FALSE, en función de la zona horaria del sistema Citrix ADC).

- **<certificate>.VALID_NOT_AFTER.DAY:**

  Extrae el último día del mes en que el certificado es válido y devuelve un número del 1 al 31, según corresponda para la fecha.

- **<certificate>.VALID_NOT_AFTER.EQ (<time>):**

  Devuelve un valor booleano TRUE si el tiempo es igual al <time> argumento.

  Por ejemplo, si la hora actual es GMT 2005 May 1 10h 15m 30s, y es el primer domingo del mes, puede especificar lo siguiente (los resultados de la evaluación de este ejemplo están entre paréntesis):

  - …eq(GMT 2005) (TRUE)
  - …eq(GMT 2005 Dec) (FALSE)
  - ..eq (LOCAL 2005 May) (VERDADERO o FALSO, en función de la zona horaria actual)
  - …eq(GMT 10h) (TRUE)
  - …eq(GMT 10h 30s) (TRUE)
  - …eq(GMT May 10h) (TRUE)
  - …eq(GMT Sun) (TRUE)
  - …eq(GMT May Sun_1) (TRUE)

- **<certificate>.VALID_NOT_AFTER.GE (<time>):**

  Devuelve un valor booleano TRUE si el valor de tiempo es mayor o igual que el argumento <time>.

  Por ejemplo, si el valor de hora es GMT 2005 May 1 10h 15m 30s y es el primer domingo del mes de mayo de 2005, puede especificar lo siguiente (los resultados de la evaluación de este ejemplo están entre paréntesis):

  - …ge(GMT 2004) (TRUE)
  - …ge(GMT 2005 Jan) (TRUE)
  - …ge(LOCAL 2005 May) (TRUE or FALSE, en función de la zona horaria actual.)
  - …ge(GMT 8h) (TRUE)
  - …ge(GMT 30m) (FALSE)
  - …ge(GMT May 10h) (TRUE)
  - …ge(GMT May 10h 0m) (TRUE)

- …ge(GMT Sun) (TRUE)
- …ge(GMT May Sun_1) (TRUE)

- **<certificate>.VALID_NOT_AFTER.GT (<time>):**

  Devuelve un valor booleano TRUE si el valor de tiempo es mayor que el argumento <time>.

  Por ejemplo, si el valor de hora es GMT 2005 May 1 10h 15m 30s y es el primer domingo del mes de mayo de 2005, puede especificar lo siguiente (los resultados de la evaluación de este ejemplo están entre paréntesis):

  - …gt(GMT 2004) (TRUE)
  - …gt(GMT 2005 Jan) (TRUE)
  - …gt(LOCAL 2005 May) (TRUE or FALSE, depending on the current time zone.)
  - …gt(GMT 8h) (TRUE)
  - …gt(GMT 30m) (FALSE)
  - …gt(GMT May 10h) (FALSE)
  - …gt(GMT Sun) (FALSE)
  - …gt(GMT May Sun_1) (FALSE)

- **<certificate>.VALID_NOT_AFTER.HORS:**

  Extrae la última hora en que el certificado es válido y devuelve ese valor como un entero de 0 a 23.

- **<certificate>.VALID_NOT_AFTER.LE (<time>):**

  Devuelve un valor booleano TRUE si el tiempo precede o es igual al <time> argumento.

  Por ejemplo, si el valor de hora es GMT 2005 May 1 10h 15m 30s y es el primer domingo del mes de mayo de 2005, puede especificar lo siguiente (los resultados de la evaluación de este ejemplo están entre paréntesis):

  - …le(GMT 2006) (TRUE)
  - …le(GMT 2005 Dec) (TRUE)
  - ..le (LOCAL 2005 May) (VERDADERO o FALSO, en función de la zona horaria actual.)
  - ..le (GMT 8h) (FALSO)
  - ..le (GMT 30m) (TRUE)
  - …le(GMT May 10h) (TRUE)
  - …le(GMT Jun 11h) (TRUE)
  - …le(GMT Wed) (TRUE)
  - …le(GMT May Sun_1) (TRUE)

- **<certificate>.VALID_NOT_AFTER.LT (<time>):**

  Devuelve un valor booleano TRUE si el tiempo precede al <time> argumento.

Por ejemplo, si la hora actual es GMT 2005 May 1 10h 15m 30s, y es el primer domingo del mes, puede especificar lo siguiente:

- …lt(GMT 2006) (TRUE)
- …lt(GMT 2005 Dec) (TRUE)
- …lt(LOCAL 2005 May) (TRUE or FALSE, en función de la zona horaria actual.)
- …lt(GMT 8h) (FALSE)
- …lt(GMT 30m) (TRUE)
- …lt(GMT May 10h) (FALSE)
- …lt(GMT Jun 11h) (TRUE)
- …lt(GMT Wed) (TRUE)
- …lt(GMT May Sun_1) (FALSE)

- **<certificate>.VALID_NOT_AFTER.MINUTS:**

  Extrae el último minuto en que el certificado es válido y devuelve ese valor como un entero de 0 a 59.

- **<certificate>.VALID_NOT_AFTER.MONTH:**

  Extrae el último mes en que el certificado es válido y devuelve ese valor como un entero del 1 (enero) al 12 (diciembre).

- **<certificate>.VALID_NOT_AFTER.RELATIVE_BOOT:**

  Calcula el número de segundos para el reinicio anterior o programado más cercano y devuelve un entero. Si el tiempo de arranque más cercano está en el pasado, el entero es negativo. Si está en el futuro, el entero es positivo.

- **<certificate>.VALID_NOT_AFTER.RELATIVE_NOW;**

  Calcula el número de segundos entre la hora actual del sistema y la hora especificada y devuelve un entero. Si el tiempo está en el pasado, el entero es negativo; si es en el futuro, el entero es positivo.

- **<certificate>.VALID_NOT_AFTER.SECONS:**

  Extrae el último segundo en que el certificado es válido y devuelve ese valor como un entero de 0 a 59.

- **<certificate>.VALID_NOT_AFTER.WEED:**

  Extrae el último día de la semana en que el certificado es válido. Devuelve un número entre 0 (domingo) y 6 (sábado) para indicar el día de la semana en el valor de tiempo.

- **<certificate>.VALID_NOT_AFTER.WSIN (<time1>, <time2>):**

  Devuelve un valor booleano TRUE si el tiempo se encuentra dentro de todos los rangos definidos por los elementos de <time1> y <time2>.

Si omite un elemento de tiempo desde <time1>, se supone que tiene el valor más bajo en su rango. Si omite un elemento de <time2>, se supone que tiene el valor más alto de su rango. Si especifica un año en <time1>, debe especificarlo en <time2>.

Los intervalos de los elementos de tiempo son los siguientes: Mes 1-12, día 1-31, días laborables 0-6, hora 0-23, minutos 0-59 y segundos 0-59. Para que el resultado sea TRUE, cada elemento del tiempo debe existir en el rango correspondiente que especifique en <time1>, <time2>.

Por ejemplo, si la hora es GMT 2005 10 de mayo 10h 15m 30s, y es el segundo martes del mes, puede especificar lo siguiente (los resultados de la evaluación están entre paréntesis):

- …within(GMT 2004, GMT 2006) (TRUE)
- …within(GMT 2004 Jan, GMT 2006 Mar) (FALSE, mayo no está en el rango de enero a marzo.)
- ..within (GMT Feb, GMT) (TRUE, mayo está en el rango de febrero a diciembre)
- ..within (GMT Sun_1, GMT Sun_3) (TRUE, el segundo martes se encuentra dentro del rango del primer domingo al tercer domingo)
- …within(GMT 2005 May 1 10h, GMT May 2005 1 17h) (TRUE)
- …within(LOCAL 2005 May 1, LOCAL May 2005 1) (TRUE or FALSE, en función de la zona horaria del sistema Citrix ADC)

- **<certificate>.VALID_NOT_AFTER.YEAR:**

  Extrae el último año en que el certificado es válido y devuelve un entero de cuatro dígitos.

- **<certificate>.VALID_NOT_ANTES:**

  Devuelve la fecha en que el certificado de cliente pasa a ser válido.

  El formato devuelto es el número de segundos desde el 1 de enero de 1970 GMT (0 horas, 0 minutos, 0 segundos).

- **<certificate>.VALID_NOT_BEANTER.BREANTERE (<time1>, <time2>):**

  Devuelve un valor booleano TRUE si el valor de tiempo está entre los dos argumentos de tiempo. Ambos <time1> <time2> argumentos y deben especificarse completamente.

  A continuación se presentan ejemplos:

  GMT 1995 Jan está completamente especificado.
  GMT Jan no está completamente especificado.
  GMT 1995 20 no está totalmente especificado.
  GMT Jan Mon_2 no está completamente especificado.
  Los argumentos de tiempo deben ser GMT o ambos LOCAL, y <time2> deben ser mayores que <time1>.

  Por ejemplo, si el valor de hora es GMT 2005 May 1 10h 15m 30s y es el primer domingo del mes de mayo de 2005, puede especificar lo siguiente (los resultados de la evaluación de este ejemplo

están entre paréntesis):

- …between(GMT 2004, GMT 2006) (TRUE)
- …between(GMT 2004 Jan, GMT 2006 Nov) (TRUE)
- …between(GMT 2004 Jan, GMT 2006) (TRUE)
- …between(GMT 2005 May Sun_1, GMT 2005 May Sun_3) (TRUE)
- …between(GMT 2005 May 1, GMT May 2005 1) (TRUE)
- …between(LOCAL 2005 May 1, LOCAL May 2005 1) (TRUE or FALSE, en función de la zona horaria del sistema Citrix ADC).

- **<certificate>.VALID_NOT_BEANTER.DAY:**

  Extrae el último día del mes en el que el certificado es válido y devuelve ese valor como un número del 1 al 31 que representa ese día.

- **<certificate>.VALID_NOT_BEFORE.EQ (<time>):**

  Devuelve un valor booleano TRUE si el tiempo es igual al <time> argumento.

  Por ejemplo, si el valor de hora es GMT 2005 May 1 10h 15m 30s y es el primer domingo del mes de mayo de 2005, puede especificar lo siguiente (los resultados de la evaluación de este ejemplo están entre paréntesis):

  - …eq(GMT 2005) (TRUE)
  - …eq(GMT 2005 Dec) (FALSE)
  - ..eq (LOCAL 2005 May) (VERDADERO o FALSO, en función de la zona horaria actual).
  - …eq(GMT 10h) (TRUE)
  - …eq(GMT 10h 30s) (TRUE)
  - …eq(GMT May 10h) (TRUE)
  - …eq(GMT Sun) (TRUE)
  - …eq(GMT May Sun_1) (TRUE)

- **<certificate>.VALID_NOT_BEFORE.GE (<time>):**

  Devuelve un valor booleano TRUE si el tiempo es mayor que (después) o igual al <time> argumento.

  Por ejemplo, si el valor de hora es GMT 2005 May 1 10h 15m 30s, y es el primer domingo del mes de mayo de 2005, puede especificar lo siguiente (los resultados de la evaluación están entre paréntesis):

  - …ge(GMT 2004) (TRUE)
  - …ge(GMT 2005 Jan) (TRUE)
  - …ge(LOCAL 2005 May) (TRUE or FALSE, en función de la zona horaria actual.)
  - …ge(GMT 8h) (TRUE)
  - …ge(GMT 30m) (FALSE)
  - …ge(GMT May 10h) (TRUE)

- …ge(GMT May 10h 0m) (TRUE)
- …ge(GMT Sun) (TRUE)
- …ge(GMT May Sun_1) (TRUE)

- **<certificate>.VALID_NOT_BEFORE.GT (<time>):**

  Devuelve un valor booleano TRUE si se produce el tiempo después del <time> argumento.

  Por ejemplo, si el valor de hora es GMT 2005 May 1 10h 15m 30s, y es el primer domingo del mes de mayo de 2005, puede especificar lo siguiente (los resultados de la evaluación están entre paréntesis):

  - …gt(GMT 2004) (TRUE)
  - …gt(GMT 2005 Jan) (TRUE)
  - …gt(LOCAL 2005 May) (TRUE or FALSE, depending on the current time zone.)
  - …gt(GMT 8h) (TRUE)
  - …gt(GMT 30m) (FALSE)
  - …gt(GMT May 10h) (FALSE)
  - …gt(GMT May 10h 0m) (TRUE)
  - …gt(GMT Sun) (FALSE)
  - …gt(GMT May Sun_1) (FALSE)

- **<certificate>.VALID_NOT_BEANTER.HOURS:**

  Extrae la última hora en que el certificado es válido y devuelve ese valor como un entero de 0 a 23.

- **<certificate>.VALID_NOT_BEFORE.LE (<time>)

  Devuelve un valor booleano TRUE si el tiempo precede o es igual al <time> argumento.

  Por ejemplo, si el valor de hora es GMT 2005 May 1 10h 15m 30s y es el primer domingo del mes de mayo de 2005, puede especificar lo siguiente (los resultados de la evaluación de este ejemplo están entre paréntesis):

  - …le(GMT 2006) (TRUE)
  - …le(GMT 2005 Dec) (TRUE)
  - …le(LOCAL 2005 May) (TRUE or FALSE,depending on the current time zone.)
  - …le(GMT 8h) (FALSE)
    . -. .le(GMT 30m) (TRUE)
  - …le(GMT May 10h) (TRUE)
  - …le(GMT Jun 11h) (TRUE)
  - …le(GMT Wed) (TRUE)
  - …le(GMT May Sun_1) (TRUE)

- **<certificate>.VALID_NOT_BEFORE.LT(<time>):**

Devuelve un valor booleano TRUE si el tiempo precede al <time> argumento.

Por ejemplo, si el valor de hora es GMT 2005 May 1 10h 15m 30s y es el primer domingo del mes de mayo de 2005, puede especificar lo siguiente (los resultados de la evaluación de este ejemplo están entre paréntesis):

- …lt(GMT 2006) (TRUE)
- …lt(GMT 2005 Dec) (TRUE)
- …lt(LOCAL 2005 May) (TRUE or FALSE, en función de la zona horaria actual.)
- …lt(GMT 8h) (FALSE)
- …lt(GMT 30m) (TRUE)
- …lt(GMT May 10h) (FALSE)
- …lt(GMT Jun 11h) (TRUE)
- …lt(GMT Wed) (TRUE)
- …lt(GMT May Sun_1) (FALSE)

- **<certificate>.VALID_NOT_BEFORE.MINUTES:**

  Extrae el último minuto en que el certificado es válido. Devuelve el minuto actual como un entero de 0 a 59.

- **<certificate>.VALID_NOT_BEFORE.MONTH:**

  Extrae el último mes en que el certificado es válido. Devuelve el mes actual como un entero del 1 (enero) al 12 (diciembre).

- **<certificate>.VALID_NOT_BEFORE.RELATIVE_BOOT:**

  Calcula el número de segundos para el reinicio anterior o programado de Citrix ADC más cercano y devuelve un entero. Si el tiempo de arranque más cercano está en el pasado, el entero es negativo; si está en el futuro, el entero es positivo.

- **<certificate>.VALID_NOT_BEFORE.RELATIVE_NOW:**

  Devuelve el número de segundos entre la hora actual del sistema Citrix ADC y la hora especificada como un entero. Si la hora designada está en el pasado, el entero es negativo. Si está en el futuro, el entero es positivo.

- **<certificate>.VALID_NOT_BEFORE.SECONDS:**

  Extrae el último segundo en que el certificado es válido. Devuelve el segundo actual como un entero de 0 a 59.

- **<certificate>.VALID_NOT_BEFORE.WEEKDAY:**

  Extrae el último día de la semana en que el certificado es válido. Devuelve el día de la semana como un número entre 0 (domingo) y 6 (sábado).

- **<certificate>.VALID_NOT_BEFORE.WITHIN(<time1>, <time2>):**

Devuelve un valor booleano TRUE si cada elemento de tiempo existe dentro del intervalo definido en los <time1> <time2> argumentos,.

Si omite un elemento de tiempo desde <time1>, se supone que tiene el valor más bajo en su rango. Si omite un elemento de tiempo desde <time2>, se supone que tiene el valor más alto en su rango. Si especifica un año en <time1>, debe especificarse en <time2>. Los intervalos de los elementos de tiempo son los siguientes: Mes 1-12, día 1-31, días laborables 0-6, hora 0-23, minutos 0-59 y segundos 0-59.

Por ejemplo, si la hora es GMT 2005 10 de mayo 10h 15m 30s, y es el segundo martes del mes, puede especificar lo siguiente (los resultados de la evaluación están entre paréntesis):

- …within(GMT 2004, GMT 2006) (TRUE)
- …within(GMT 2004 Jan, GMT 2006 Mar) (FALSE, mayo no está en el rango de enero a marzo.)
- ..within (GMT Feb, GMT) (TRUE, mayo está en el rango de febrero a diciembre.)
- ..within (GMT Sun_1, GMT Sun_3) (TRUE, el segundo martes es entre el primer domingo y el tercer domingo).
- …within(GMT 2005 May 1 10h, GMT May 2005 1 17h) (TRUE)
- …within(LOCAL 2005 May 1, LOCAL May 2005 1) (TRUE or FALSE, en función de la zona horaria del sistema Citrix ADC)

- **<certificate>.VALID_NOT_BEFORE.YEAR:**

  Extrae el último año en que el certificado es válido. Devuelve el año actual como un entero de cuatro dígitos.

Expresiones para fechas de solicitud y respuesta HTTP

October 5, 2021

Los prefijos de expresión siguientes devuelven el contenido del encabezado HTTP Date como texto o como objeto de fecha. Estos valores se pueden evaluar de la siguiente manera:

- Como número. El valor numérico de un encabezado HTTP Date se devuelve en forma del número de segundos transcurridos desde el 1 de enero de 1970.

  Por ejemplo, la expresión http.req.date.mod (86400) devuelve el número de segundos transcurridos desde el comienzo del día. Estos valores se pueden evaluar mediante las mismas operaciones que otros datos numéricos no relacionados con la fecha. Para obtener más información, consulte Prefijos de expresión para datos numéricos distintos de la fecha y la hora.

- Como encabezado HTTP. Los encabezados de fecha se pueden evaluar mediante las mismas operaciones que otros encabezados HTTP.

Para obtener más información, consulte Expresiones de directivas avanzadas: análisis de datos HTTP, TCP y UDP.

- Como texto. Los encabezados de fecha se pueden evaluar mediante las mismas operaciones que otras cadenas.

Para obtener más información, consulte Expresiones de directivas avanzadas: evaluación de texto.

Prefix	Descripción
HTTP.REQ.DATE	Devuelve el contenido del encabezado HTTP Date como texto o como objeto de fecha. Los formatos de fecha reconocidos son: RFC822. Dom, 06 Jan 1980 08:49:37 GMT, RFC850. Domingo 06-Ene-80 09:49:37 GMT y ASCTIME. Dom Ene 6 08:49:37 1980.
HTTP.RES.DATE	Devuelve el contenido del encabezado HTTP Date como texto o como objeto de fecha. Los formatos de fecha reconocidos son: RFC822. Dom, 06 Jan 1980 8:49:37 GMT, RFC850. Domingo, 06-enero-80 9:49:37 GMT, y ASCTIME. Dom Ene 6 08:49:37 1980.

Generar el día de la semana, como una cadena, en formatos cortos y largos

January 12, 2021

Las funciones `WEEKDAY_STRING_SHORT` y, `WEEKDAY_STRING`generan el día de la semana, como una cadena, en formatos cortos y largos, respectivamente. Las cadenas que se devuelven siempre están en inglés. El prefijo utilizado con estas funciones debe devolver el día de la semana en formato entero y el rango aceptable para el valor devuelto por el prefijo es 0-6. Por lo tanto, puede utilizar cualquier prefijo que devuelva un entero en el rango aceptable. Se genera una condición UNDEF si el valor devuelto no está en este rango o si falla la asignación de memoria.

A continuación se presentan las descripciones de las funciones:

Función	Descripción
<prefix>.WEEKDAY_STRING_SHORT	Devuelve el día de la semana en formato corto. La forma corta siempre tiene 3 caracteres de largo con una mayúscula inicial y los caracteres restantes en minúsculas. Por ejemplo, SYS.TIME.WEEKDAY.WEEKDAY_STRING_SHORT devuelve Sun si el valor devuelto por la función WEEKDAY es 0 y Sat si el valor devuelto por el prefijo es 6.
<prefix>.WEEKDAY_STRING	Devuelve el día de la semana en formato largo. La forma larga siempre tiene un mayúscula inicial, con los caracteres restantes en minúsculas. Por ejemplo,SYS.TIME.WEEKDAY.WEEKDAY_STRING devuelve domingo si el valor devuelto por la función WEEDY es 0 y sábado si el valor devuelto por el prefijo es 6.

Prefijos de expresión para datos numéricos distintos de fecha y hora

August 20, 2021

Además de configurar expresiones que funcionan a tiempo, puede configurar expresiones para los siguientes tipos de datos numéricos:

- La longitud de las solicitudes HTTP, el número de encabezados HTTP en una solicitud, etc.

  Para obtener más información, consulte Expresiones para datos de carga útil HTTP numéricos distintos de las fechas.

- Direcciones IP y MAC.

  Para obtener más información, consulte Expresiones para direcciones IP y subredesIP.

- Datos de cliente y servidor en relación con los ID de interfaz y la tasa de rendimiento de transacciones.

  Para obtener más información, consulte Expresiones para datos numéricos de clientes y servidores.

- Datos numéricos en certificados de cliente distintos de fechas.

Para obtener información sobre estos prefijos, incluido el número de días que transcurren hasta la expiración del certificado y el tamaño de la clave de cifrado, consulte Prefijos de datos numéricos en certificados SSL.

Conversión de números en texto

August 20, 2021

Las siguientes funciones producen cadenas binarias a partir de un número devuelto por un prefijo de expresión. Estas funciones son particularmente útiles en la función de reescritura TCP como cadenas de reemplazo para datos binarios. Para obtener más información sobre la función de reescritura TCP, consulte Reescritura.

Todas las funciones devuelven un valor de texto de tipo. La codificación Endianness que algunas de las funciones aceptan como parámetro es LITTLE_ENDIAN o BIG_ENDIAN.

Función	Descripción
<number>.SIGNED8_STRING	Produce una cadena binaria con signo de 8 bits que representa el número. Si el valor está fuera del rango, se genera una condición undef. Ejemplo: HTTP.REQ.BODY (100).GET_SIGNED8 (16).SUB (3).SIGNED8_STRING
<number>.UNSIGNED8_STRING	Produce una cadena binaria sin signo de 8 bits que representa el número. Si el valor está fuera del rango, se genera una condición undef. Ejemplo: HTTP.REQ.BODY (100).GET_UNSIGNED8 (31).ADD (3).UNSIGNED8_STRING
<number>.SIGNED16_STRING (<endianness>)	Produce una cadena binaria con signo de 16 bits que representa el número. Si el valor está fuera del rango, se genera una condición undef. Ejemplo: HTTP.REQ.BODY (100).SKIP (12).GET_SIGNED16 (0, BIG_ENDIAN).SUB (4).SIGNED16_STRING (BIG_ENDIAN)

Función	Descripción
<number>.UNSIGNED16_STRING (<endianness>)	Produce una cadena binaria sin signo de 16 bits que representa el número. Si el valor está fuera del rango, se genera una condición undef. Ejemplo: HTTP.REQ.BODY (100).GET_UNSIGNED16 (47, LITTLE_ENDIAN).ADD (7).UNSIGNED16_STRING (LITTLE_ENDIAN)
<number>.SIGNED32_STRING (<endianness>)	Produce una cadena binaria con signo de 32 bits que representa el número. Ejemplo: HTTP.REQ.BODY (100).AFTER_STR (“delim”).GET_SIGNED32 (0, BIG_ENDIAN).SUB (1).SIGNED32_STRING (BIG_ENDIAN)
<unsigned_long_number>.UNSIGNED8_STRING	Produce una cadena binaria sin signo de 8 bits que representa el número. Si el valor está fuera del rango, se genera una condición undef. Ejemplo: HTTP.REQ.BODY(100).GET_UNSIGNED8(24).TYPECAST_UNSIG
<unsigned_long_number>.UNSIGNED16_STRING (<endianness>)	Produce una cadena binaria sin signo de 16 bits que representa el número. Si el valor está fuera del rango, se genera una condición undef. Ejemplo: HTTP.REQ.BODY(100).GET_UNSIGNED16(23, LITTLE_ENDIAN).TYPECAST_UNSIGNED_LONG_AT.ADD(10).UNSIG
<unsigned_long_number>.UNSIGNED32_STRING (<endianness>)	Produce una cadena binaria sin signo de 32 bits que representa el número. Si el valor está fuera del rango, se genera una condición undef. Ejemplo: HTTP.REQ.BODY (100).AFTER_STR (“delim2”).GET_UNSIGNED32 (0, BIG_ENDIAN).ADD (2).UNSIGNED32_STRING (BIG_ENDIAN)

Expresiones basadas en servidor virtual

October 5, 2021

El prefijo de expresión `SYS.VSERVER("<vserver-name>")` permite identificar un servidor virtual. Puede utilizar las siguientes funciones con este prefijo para recuperar información relacionada con el servidor virtual especificado:

- **RENDIMIENTO.** Devuelve el rendimiento del servidor virtual en Mbps (megabits por segundo). El valor devuelto es un número largo sin signo.

  Uso: SYS.VSERVER("vserver").THROUGHPUT

- **CONEXIONES.** Devuelve el número de conexiones administradas por el servidor virtual. El valor devuelto es un número largo sin signo.

  Uso: SYS.VSERVER("vserver").CONNECTIONS

- **ESTADO.** Devuelve el estado del servidor virtual. El valor devuelto es UP, DOWN u OUT_OF_SERVICE. Por lo tanto, uno de estos valores se puede pasar como argumento al operador EQ() para realizar una comparación que da como resultado un valor booleano TRUE o FALSE.

  Uso: SYS.VSERVER("vserver").STATE

- **SALUD.** Devuelve el porcentaje de servicios en estado activo del servidor virtual especificado. El valor devuelto es un número entero.

  Uso: SYS.VSERVER("vserver").HEALTH

- **TIEMPO DE RESPIRO.** Devuelve el tiempo de respuesta como un número entero que representa el número de microsegundos. El tiempo de respuesta es el TTFB (tiempo hasta el primer byte) promedio de todos los servicios enlazados al servidor virtual.

  Uso: SYS.VSERVER("vserver").RESPTIME

- **SURGECOUNT.** Devuelve el número de solicitudes de la cola de sobretensión del servidor virtual. El valor devuelto es un número entero.

  Uso: SYS.VSERVER("vserver").SURGECOUNT

Ejemplo 1:

La siguiente directiva de reescritura anula el procesamiento de reescritura si el número de conexiones en el servidor virtual de equilibrio de carga LbvServer supera las 10000:

```
add rewrite policy norewrite_pol sys.vserver("LBvserver").connections.gt
(10000)norewrite
```

Ejemplo 2:

La siguiente acción de reescritura inserta un encabezado personalizado, TP, cuyo valor es la totalidad en el servidor virtual LbvServer:

```
add rewrite action tp_header insert_http_header TP SYS.VSERVER("LBvserver")
.THROUGHPUT
```

Ejemplo 3:

La siguiente acción de mensaje de registro de auditoría escribe el TTFB promedio de los servicios enlazados a un servidor virtual, en el archivo de registro newnslog:

```
add audit messageaction log_vserver_resptime_act INFORMATIONAL "\"NS
Response Time to Servers:\" + sys.vserver(\"ssllb\").resptime + \" millisec
\""-logtoNewnslog YES
```

Expresiones de directiva avanzadas: Análisis de datos HTTP, TCP y UDP

February 19, 2022

Puede configurar expresiones de directivas avanzadas para evaluar la carga útil de una solicitud o respuesta HTTP. La carga asociada a una conexión HTTP incluye encabezados HTTP (encabezados estándar o personalizados), cuerpo y URL de conexión. Además, puede evaluar y procesar la carga útil en un paquete TCP o UDP. Para conexiones HTTP, por ejemplo, puede comprobar si existe un encabezado HTTP determinado o si la dirección URL incluye un parámetro de consulta concreto.

Puede configurar expresiones para transformar la codificación URL y aplicar la codificación "segura" HTML o XML para su posterior evaluación. También puede utilizar los prefijos XPATH y JSON para evaluar la fecha en archivos XML y JSON, respectivamente.

Para obtener más información sobre las expresiones de autenticación como AAA.USER, AAA.LOGIN, consulte Autenticación, autorización y auditoría de inicio de sesión y para la expresión AAA.AUTHENTICATION, consulte los temas de autenticación de usuario Citrix ADC AAA .

También puede utilizar expresiones de directiva avanzadas numéricas y basadas en texto para evaluar los datos de solicitud y respuesta HTTP. Para obtener más información, consulte Expresiones de directiva avanzadas: evaluación de texto y expresiones de directivas avanzadas: trabajo con fechas, horas y números.

Expresiones para identificar el protocolo en un paquete IP entrante

August 20, 2021

En la tabla siguiente se enumeran las expresiones que puede utilizar para identificar el protocolo en un paquete entrante.

Expresión	Descripción
CLIENT.IP.PROTOCOL	Identifica el protocolo en los paquetes IPv4 enviados por los clientes.
CLIENT.IPV6.PROTOCOL	Identifica el protocolo en los paquetes IPv6 enviados por los clientes.
SERVIDOR.IP.PROTOCOL	Identifica el protocolo en los paquetes IPv4 enviados por los servidores.
SERVER.IPV6.PROTOCOL	Identifica el protocolo en los paquetes IPv6 enviados por los servidores.

Argumentos para la función PROTOCOLO

Puede pasar el número de protocolo de Internet Assigned Numbers Authority (IANA) a la función PROTOCOLO. Por ejemplo, si quiere determinar si el protocolo de un paquete entrante es TCP, puede utilizar CLIENT.IP.PROTOCOL.EQ (6), donde 6 es el número de protocolo asignado por IANA para TCP. Para algunos protocolos, puede pasar un valor de enumeración en lugar del número de protocolo. Por ejemplo, en lugar de CLIENT.IP.PROTOCOL.EQ (6), puede utilizar CLIENT.IP.PROTOCOL.EQ (TCP). En la tabla siguiente se enumeran los protocolos para los que se pueden utilizar valores de enumeración y los valores de enumeración correspondientes para su uso con la función PROTOCOLO.

Protocolo	Valor de enumeración
Protocolo de control de transmisión (TCP)	TCP
Protocolo de datagramas de usuario (UDP)	UDP
Protocolo de mensajes de control de Internet (ICMP)	ICMP
Encabezado de autenticación IP (AH), para proporcionar servicios de autenticación en IPv4 e IPv6	AH, SÍ
Protocolo de carga útil de seguridad encapsulada (ESP)	ESP
Encapsulación de redirección general (GRE)	GRE
Protocolo de encapsulación IP dentro de IP	IPIP

Protocolo	Valor de enumeración
Protocolo de mensajes de control de Internet para IPv6 (ICMPv6)	ICMPv6
Cabecera de fragmento para IPv6	FRAGMENTO

Casos de casos de uso

Las expresiones de protocolo se pueden utilizar tanto en directivas basadas en solicitudes como en respuestas. Puede utilizar las expresiones en varias funciones de Citrix ADC, como el equilibrio de carga, la optimización de WAN, la conmutación de contenido, la reescritura y las directivas de escucha. Puede utilizar las expresiones con funciones como EQ () y NE (), para identificar el protocolo en una directiva y realizar una acción.

A continuación se presentan algunos casos de uso para las expresiones:

- En las configuraciones de equilibrio de carga del repetidor de rama, puede utilizar las expresiones de una directiva de escucha para el servidor virtual comodín. Por ejemplo, puede configurar el servidor virtual comodín con la directiva de escucha CLIENT.IP.PROTOCOL.EQ (TCP) para que el servidor virtual procese solo el tráfico TCP y simplemente pule todo el tráfico no TCP. Aunque puede utilizar una lista de control de acceso en lugar de la directiva de escucha, la directiva de escucha proporciona un mejor control sobre el tráfico que se procesa.
- Para servidores virtuales de conmutación de contenido de tipo CUALQUIER, puede configurar directivas de conmutación de contenido que conmutan solicitudes en función del protocolo en los paquetes entrantes. Por ejemplo, puede configurar directivas de conmutación de contenido para dirigir todo el tráfico TCP a un servidor virtual de equilibrio de carga y todo el tráfico no TCP a otro servidor virtual de equilibrio de carga.
- Puede utilizar las expresiones basadas en el cliente para configurar la persistencia basada en el protocolo. Por ejemplo, puede utilizar CLIENT.IP.PROTOCOLO para configurar la persistencia sobre la base de los protocolos en los paquetes IPv4 entrantes.

Expresiones para encabezados HTTP y control de caché

August 20, 2021

Un método común para evaluar el tráfico HTTP es examinar los encabezados en una solicitud o una respuesta. Un encabezado puede realizar una serie de funciones, incluidas las siguientes:

- Proporcionar cookies que contengan datos sobre el remitente.
- Identifique el tipo de datos que se están transmitiendo.

- Identifique la ruta por la que han viajado los datos (el encabezado Via).

> **Nota**
>
> Si se utiliza una operación para evaluar los datos de encabezado y texto, la operación basada en encabezado siempre anula la operación basada en texto. Por ejemplo, la operación AFTER_STR, cuando se aplica a un encabezado, reemplaza las operaciones AFTER_STR basadas en texto para todas las instancias del tipo de encabezado actual.

Prefijos para encabezados HTTP

La tabla Prefijos para encabezados HTTP para prefijos de expresión que extraen encabezados HTTP.

Operaciones para encabezados HTTP

La tabla de encabezados Operations for HTTP para las operaciones que se pueden especificar con los prefijos de los encabezados HTTP.

Prefijos para encabezados de control de caché

Los siguientes prefijos se aplican específicamente a los encabezados Cache-Control.

Prefijo de encabezado HTTP	Descripción
HTTP.REQ.CACHE_CONTROL	Devuelve un encabezado Cache-Control en una solicitud HTTP.
HTTP.RES.CACHE_CONTROL	Devuelve un encabezado Cache-Control en una respuesta HTTP.

Operaciones para encabezados de control de caché

Puede aplicar cualquiera de las operaciones para encabezados HTTP a encabezados Cache-Control.

Además, las siguientes operaciones identifican tipos específicos de encabezados Cache-Control. Consulte RFC 2616 para obtener información sobre estos tipos de encabezado.

Operación de encabezado HTTP	Descripción
`Cache-Control header.NAME(<integer>)`	Devuelve como valor de texto el nombre del encabezado Cache-Control que corresponde al componente enésimo de una lista nombre-valor, como se especifica en `<integer>`. El índice del componente nombre-valor se basa en 0. Si el `<integer>` especificado por el argumento integer es mayor que el número de componentes de la lista, se devuelve un objeto de texto de longitud cero. A continuación se muestra un ejemplo: `http.req.cache_control.name(3).contains("some_text")`
Cache-Control header.is_inválido	Devuelve un valor booleano TRUE si el encabezado Cache-Control no está presente en la solicitud o respuesta. A continuación se muestra un ejemplo: `http.req.cache_control.is_invalid`
`Cache-Control header.IS_PRIVATE`	Devuelve un valor booleano TRUE si el encabezado Cache-Control tiene el valor Private. A continuación se muestra un ejemplo: `http.req.cache_control.is_private`
Cache-Control header.is_public	Devuelve un valor booleano TRUE si el encabezado Cache-Control tiene el valor Private. Lo que sigue es un ejemplo: Http.req.cache_control.is_public
Cache-Control Header.is_no_store	Devuelve un valor booleano TRUE si el encabezado Cache-Control tiene el valor No-Store. Lo que sigue es un ejemplo: Http.req.cache_control.is_no_store
Encabezado de control de cache.is_no_cache	Devuelve un valor booleano TRUE si el encabezado Cache-Control tiene el valor No-Cache. Lo que sigue es un ejemplo: Http.req.cache_control.is_no_cache

Operación de encabezado HTTP	Descripción
Cache-Control Header.is_MAX_Age	Devuelve un valor booleano TRUE si el encabezado Cache-Control tiene el valor Max-Age. A continuación se presenta un ejemplo: Http.req.cache_control.is_max_age
Cache-Control header.is_min_fresh	Devuelve un valor booleano TRUE si el encabezado Cache-Control tiene el valor Min-Fresh. Lo que sigue es un ejemplo: Http.req.cache_control.is_min_fresh
Cache-Control Header.is_MAX_obsoleto	Devuelve un valor booleano TRUE si el encabezado Cache-Control tiene el valor Max-Stale. A continuación se presenta un ejemplo: Http.req.cache_control.is_max_stale
Cache-Control header.is_must_revalidate	Devuelve un valor booleano TRUE si el encabezado Cache-Control tiene el valor Dest-Revalidate. A continuación se presenta un ejemplo: Http.req.cache_control.is_must_revalidate
Encabezado de control de cache.is_no_transform	Devuelve un valor booleano TRUE si el encabezado Cache-Control tiene el valor No-Transform. A continuación se presenta un ejemplo: Http.req.cache_control.is_no_transform
Cache-Control header.is_only_if_cache	Devuelve un valor booleano TRUE si el encabezado Cache-Control tiene el valor Only-If-Cached. A continuación se presenta un ejemplo: Http.req.cache_control.is_only_if_cached
Cache-Control Header.is_proxy_revalidate	Devuelve un valor booleano TRUE si el encabezado Cache-Control tiene el valor Proxy-Revalidate. A continuación se presenta un ejemplo: Http.req.cache_control.is_proxy_revalidate
Cache-Control Header.is_s_maxage	Devuelve un valor booleano TRUE si el encabezado Cache-Control tiene el valor S-Maxage. A continuación se presenta un ejemplo: Http.req.cache_control.is_s_maxage

Operación de encabezado HTTP	Descripción
Cache-Control header.is_unknown	Devuelve un valor booleano TRUE si el encabezado Cache-Control es de un tipo desconocido. Lo que sigue es un ejemplo: Http.req.cache_control.is_unknown
Cache-Control Header.MAX_Age	Devuelve el valor del encabezado Cache-Control Max-Age. Si este encabezado está ausente o no es válido, se devuelve 0. A continuación se presenta un ejemplo: Http.req.cache_control.max_age.le (3)
Cache-Control Header.MAX_Stale	Devuelve el valor del encabezado Cache-Control Max-Stale. Si este encabezado está ausente o no es válido, se devuelve 0. A continuación se presenta un ejemplo: Http.req.cache_control.max_stale.le (3)
Cache-Control Header.MIN_FRESH	Devuelve el valor del encabezado Cache-Control Min-Fresh. Si este encabezado está ausente o no es válido, se devuelve 0. Lo que sigue es un ejemplo: Http.req.cache_control.min_fresh.le (3)
Cache-Control Header.s_maxAge	Devuelve el valor del encabezado Cache-Control S-Maxage. Si este encabezado está ausente o no es válido, se devuelve 0. Following es un ejemplo: Http.req.cache_control.s_maxage.eq (2)

Expresiones para extraer segmentos de URL

August 20, 2021

Puede extraer direcciones URL y partes de direcciones URL, como el nombre de host, o un segmento de la ruta de URL. Por ejemplo, la siguiente expresión identifica las solicitudes HTTP para archivos de imagen extrayendo sufijos de archivo de imagen de la dirección URL:

```
http.req.url.suffix.eq("jpeg")|| http.req.url.suffix.eq("gif")
```

La mayoría de las expresiones de las URL funcionan en texto y se describen en Prefijos de expresión

para texto en solicitudes y respuestas HTTP. En esta sección se describe la operación GETE. La operación GET extrae texto cuando se utiliza con los prefijos siguientes:

- HTTP.REQ.URL.PATH
- VPN.BASEURL.PATH
- VPN.CLIENTLESS_BASEURL.PATH

En la tabla siguiente se describen los prefijos de las direcciones URL HTTP.

Prefijo de la URL	Descripción
HTTP.REQ.URL.PATH.GET (<n>)	Devuelve una lista separada slash- (“/”) de la ruta URL. Por ejemplo, considere la siguiente dirección URL:<http://www.mycompany.com/dir1/dir2/dir3/index.html?a=1>. La siguiente expresión devuelve dir1 de esta URL:<http.req.url.path.get(1)>. La siguiente expresión devuelve dir2: Http.req.url.path.get (2)
HTTP.REQ.URL.PATH.GET_REVERSE (<n>)	Devuelve una lista separada slash- (“/”) de la ruta URL, comenzando desde el final de la ruta. Por ejemplo, considere la siguiente dirección URL: <http://www.mycompany.com/dir1/dir2/dir3/index.html?a=1>. La siguiente expresión devuelve index.html de esta URL: <http.req.url.path.get_reverse(0)>. La siguiente expresión devuelve dir3: Http.req.url.path.get_reverse (1)

Expresiones para códigos de estado HTTP y datos numéricos de carga HTTP distintos de fechas

January 12, 2021

En la tabla siguiente se describen los prefijos de valores numéricos en datos HTTP distintos de las fechas.

Prefix	Descripción
HTTP.REQ.CONTENT_LENGTH	Devuelve la longitud de una solicitud HTTP como un número. A continuación se presenta un ejemplo: Http.req.content_length < 500
HTTP.RES.CONTENT_LENGTH	Devuelve la longitud de la respuesta HTTP como un número. A continuación se presenta un ejemplo: Http.res.content_length <= 1000
HTTP.RES.STATUS	Devuelve el código de estado de la respuesta
HTTP.RES.IS_REDIRECT	Devuelve un valor booleano TRUE si el código de respuesta está asociado a una redirección. Los siguientes son los códigos de respuesta de redirección: 300 (opciones múltiples), 301 (movido permanentemente), 302 (Encontrado), 303 (Ver otro), 305 (Usar proxy) y 307 (Redirigir temporal). Nota: El código de estado 304 no se considera un código de estado de respuesta HTTP de redirección. El código de estado 306 no se usa.

Expresiones SIP

August 20, 2021

El lenguaje de expresiones de directivas avanzadas de Citrix ADC contiene varias expresiones que operan en conexiones SIP (Protocolo de inicio de sesión). Estas expresiones están pensadas para ser utilizadas en directivas para cualquier protocolo compatible que funcione sobre una base de solicitud/respuesta. Estas expresiones se pueden utilizar en directivas de conmutación de contenido, limitación de velocidad, respuesta y reescritura.

Ciertas limitaciones se aplican a las expresiones SIP utilizadas con las directivas de respuesta. Solo se permiten las acciones DROP, NOOP o RESPONDWITH en un servidor virtual de equilibrio de carga SIP. Las directivas de respuesta pueden vincularse a un servidor virtual de equilibrio de carga, a un punto de enlace global de anulación, a un punto de enlace global predeterminado o a una etiqueta de directiva sip_udp.

El formato de encabezado utilizado por el protocolo SIP es similar al utilizado por el protocolo HTTP, por lo que muchas de las nuevas expresiones se ven y funcionan muy parecido a sus análogos HTTP.

Cada encabezado SIP consta de una línea que incluye el método SIP, la URL y la versión, seguido de una serie de pares nombre-valor que parecen encabezados HTTP.

A continuación se presenta un encabezado SIP de ejemplo que se hace referencia en las tablas de expresiones debajo de él:

```
INVITE sip:16@www.sip.com:5060;transport=udp SIP/2.0
Record-Route: <sip:200.200.100.22;lr=on>
Via: SIP/2.0/UDP 200.200.100.22;branch=z9hG4bK444b.c8e103d1.0;rport
   =5060;
    received=10.102.84.18
Via: SIP/2.0/UDP 10.102.84.180:5060;branch=z9hG4bK03e76d0b;rport=5060;
    received=10.102.84.160
From: "12" <sip:12@sip_example.com>;tag=00127f54ec85a6d90cc14f45-53
   cc0185
To: "16" <sip:16@sip_example.com>;tag=00127f54ec85a6d90cc14f45-53cc0185
Call-ID: 00127f54-ec850017-0e46f5b9-5ec149c2@10.102.84.180
Max-Forwards: 69CSeq: 101 INVITE
User-Agent: Cisco-CP7940G/8.0
Contact: <sip:12@10.102.84.180:5060;transport=udp>
Expires: 180
Accept: application/sdp
Allow: ACK,BYE,CANCEL,INVITE,NOTIFY,OPTIONS,REFER,REGISTER,UPDATE
Supported: replaces,join,norefersub
Content-Length: 277
Content-Type: application/sdp
Content-Disposition: session;handling=optiona
<!--NeedCopy-->
```

Tablas de referencia SIP

Las tablas siguientes contienen listas de expresiones que operan en encabezados SIP. La primera tabla contiene expresiones que se aplican a los encabezados de solicitud. La mayoría de las expresiones basadas en respuesta son casi las mismas que las expresiones basadas en solicitudes correspondientes. Para crear una expresión de respuesta a partir de la expresión de solicitud correspondiente, cambie las dos primeras secciones de la expresión de SIP.REQ a SIP.RES y realice otros ajustes obvios. La segunda tabla contiene aquellas expresiones de respuesta que son exclusivas de las respuestas y no tienen equivalentes de solicitud. Puede utilizar cualquier elemento de las tablas siguientes como expresión completa por sí mismo, o puede utilizar varios operadores para combinar estos elementos de expresión con otros para formar expresiones más complejas.

Expresiones de solicitud SIP

Expresión	Descripción
SIP.REQ.METHOD	Funciona en el método de la solicitud SIP. Los métodos de solicitud SIP admitidos son ACK, BYE, CANCEL, INFO, INVITE, MESSAGE, NOTIFY, OPTIONS, PRACK, PUBLISH, REFER, REGISTER, SUBSCRIBE y UPDATE. Esta expresión es una derivada de la clase de texto, por lo que todas las operaciones que son aplicables al texto son aplicables a este método. Por ejemplo, para una solicitud SIP de INVITE sip:16@10.102.84.181:5060;transport=udp SIP/2.0, esta expresión devuelve INVITE.
SIP.REQ.URL	Funciona en la URL de solicitud SIP. Esta expresión es una derivada de la clase de texto, por lo que todas las operaciones que son aplicables al texto son aplicables a este método. Por ejemplo, para una solicitud SIP de INVITE sip:16@10.102.84.181:5060;transport=udp SIP/2.0, esta expresión devuelve: 16@10.102.84.181:5060;transport=udp.
SIP.REQ.URL.PROTOCOL	Devuelve el protocolo URL. Por ejemplo, para una URL SIP ofsip:16@www.sip.com:5060;transport=udp, esta expresión devuelve sip.
SIP.REQ.URL.HOSTNAME	Devuelve la parte del nombre de host de la URL SIP. Por ejemplo, para una URL SIP ofsip:16@www.sip.com:5060;transport=udp, esta expresión devuelve www.sip.com:5060.
SIP.REQ.URL.HOSTNAME.PORT	Devuelve la parte del puerto del nombre de host de la URL SIP. Si no se especifica ningún puerto, esta expresión devuelve el puerto SIP predeterminado, 5060. Por ejemplo, para un nombre de host SIP de www.sip.com:5060, esta expresión devuelve 5060.

Expresión	Descripción
SIP.REQ.URL.HOSTNAME.DOMAIN	Devuelve la parte del nombre de dominio del nombre de host de la URL SIP. Si el host es una dirección IP, esta expresión devuelve un resultado incorrecto. Por ejemplo, para un nombre de host SIP de www.sip.com:5060, esta expresión devuelve sip.com. Para un nombre de host SIP 192.168.43.15:5060, esta expresión devuelve un error.
SIP.REQ.URL.HOSTNAME.SERVER	Devuelve la parte del servidor del host. Por ejemplo, para un nombre de host SIP de www.sip.com:5060, esta expresión devuelve www.
SIP.REQ.URL.USERNAME	Devuelve el nombre de usuario que precede al carácter @. Por ejemplo, para una URL SIP de sip:16@www.sip.com:5060;transport=udp, esta expresión devuelve 16.
SIP.REQ.VERSION	Devuelve el número de versión SIP en la solicitud. Por ejemplo, para una solicitud SIP de INVITE sip:16@10.102.84.181:5060;transport=udp SIP/2.0, esta expresión devuelve SIP/2.0.
SIP.REQ.VERSION.MAJOR	Devuelve el número de versión principal (el número a la izquierda del punto). Por ejemplo, para un número de versión SIP de SIP/2.0, esta expresión devuelve 2.
SIP.REQ.VERSION.MINOR	Devuelve el número de versión secundaria (el número a la derecha del punto). Por ejemplo, para un número de versión SIP de SIP/2.0, esta expresión devuelve 0.

Expresión	Descripción
SIP.REQ.CONTENT_LENGTH	Devuelve el contenido del encabezado Content-Length. Esta expresión es una derivada de la clase sip_header_t, por lo que se pueden utilizar todas las operaciones disponibles para encabezados SIP. Por ejemplo, para un encabezado SIP Content-Length de Content-Length: 277, esta expresión devuelve 277.
SIP.REQ.TO	Devuelve el contenido del encabezado To. Por ejemplo, para un encabezado SIP To de A: “16” <sip:16@sip_example.com>;tag=00127f54ec85a6d90cc14f45-53cc0185, esta expresión devuelve “16” <sip:16@sip_example.com>;tag=00127f54ec85a6d90cc14f45-53cc0185.
SIP.REQ.TO.DIRECCIÓN	Devuelve el URI SIP, que se encuentra en el objeto sip_url. Se pueden utilizar todas las operaciones disponibles para los URI SIP. Por ejemplo, para un encabezado SIP To de: “16” <sip:16@sip_example.com>;tag=00127f54ec85a6d90cc14f45-53cc0185, esta expresión devuelve sip:16@sip_example.com.
SIP.REQ.A.DISPLAY_NAME	Devuelve la parte del nombre para mostrar del encabezado To. Por ejemplo, para un encabezado SIP To de: “16” <sip:16@sip_example.com>;tag=00127f54ec85a6d90cc14f45-53cc0185, esta expresión devuelve 16.
SIP.REQ.TO.TAG	Devuelve el valor “tag” del par de valores de nombre “tag” en el encabezado TO. Por ejemplo, para un encabezado SIP To: “16” <sip:16@sip_example.com>;tag=00127f54ec85a6d90cc14f45-53cc0185, esta expresión devuelve 00127f54ec85a6d90cc14f45-53cc0185.

Expresión	Descripción
SIP.REQ.DE	Devuelve el contenido del encabezado From. Por ejemplo, para un encabezado SIP From de: “12” <sip: 12@sip_example.com >; tag=00127f54ec85a6d90cc14f45-53cc0185, esta expresión devuelve sip: 12@sip_example.com.
SIP.REQ.FROM.ADDRESS	Devuelve el URI SIP, que se encuentra en el objeto sip_url. Se pueden utilizar todas las operaciones disponibles para los URI SIP. Por ejemplo, para un encabezado SIP From de: “12” <sip: 12@sip_example.com >; tag=00127f54ec85a6d90cc14f45-53cc0185, esta expresión devuelve sip: 12@sip_example.com.
SIP.REQ.FROM.DISPLAY_NAME	Devuelve la parte del nombre para mostrar del encabezado To. Por ejemplo, para un encabezado SIP From de: “12” <sip: 12@sip_example.com >; tag=00127f54ec85a6d90cc14f45-53cc0185, esta expresión devuelve 12.
SIP.REQ.FROM.TAG	Devuelve el valor “tag” del par nombre/valor “tag” en el encabezado To. Por ejemplo, para un encabezado SIP From de: “12”<sip:12@sip_example.com>; tag=00127f54ec85a6d90cc14f45-53cc0185, esta expresión devuelve 00127f54ec85a6d90cc14f45-53cc0185.
SIP.REQ.VIA	Devuelve el encabezado Via completo. Si hay varios encabezados Via en la solicitud, devuelve el último encabezado Via. Por ejemplo, para los dos encabezados Via del encabezado SIP de ejemplo, esta expresión devuelve Via: SIP/2.0/UDP 10.102.84.180:5060;branch=z9hG4bK03e76d0b;rport=5060;re

Expresión	Descripción
SIP.REQ.VIA.SENTBY_ADDRESS	Devuelve la dirección que envió la solicitud. Por ejemplo, para el encabezado Via a través de: SIP/2.0/UDP 10.102.84.180:5060;branch=z9hG4bK03e76d0b;rport=5060;re esta expresión devuelve 10.102.84.180.
SIP.REQ.VIA.SENTBY_PORT	Devuelve el puerto que envió la solicitud. Por ejemplo, para el encabezado Via a través de: SIP/2.0/UDP 10.102.84.180:5060;branch=z9hG4bK03e76d0b;rport=5060;re esta expresión devuelve 5060.
SIP.REQ.VIA.RPORT	Devuelve el valor del par nombre/valor rport. Por ejemplo, para el encabezado Via a través de: SIP/2.0/UDP 10.102.84.180:5060;branch=z9hG4bK03e76d0b;rport=5060;re esta expresión devuelve 5060.
SIP.REQ.VIA.BRANCH	Devuelve el valor del par nombre/valor de la rama. Por ejemplo, para el encabezado Via a través de: SIP/2.0/UDP 10.102.84.180:5060;branch=z9hG4bK03e76d0b;rport=5060;re esta expresión devuelve z9hG4bK03e76d0b.
SIP.REQ.VIA.RECEIVED	Devuelve el valor del par nombre/valor recibido. Por ejemplo, para el encabezado Via a través de: SIP/2.0/UDP 10.102.84.180:5060;branch=z9hG4bK03e76d0b;rport=5060;re esta expresión devuelve 10.102.84.160.
SIP.REQ.CALLID	Devuelve el contenido del encabezado Callid. Esta expresión es una derivada de la clase sip_header_t, por lo que se pueden utilizar todas las operaciones disponibles para encabezados SIP. Por ejemplo, para un encabezado SIP Callid Ofcall-ID: 00127f54-ec850017-0e46f5b9-5ec149c2@10.102.84.180, esta expresión devuelve 00127f54-ec850017-0e46f5b9-5ec149c2@10.102.84.180.

Expresión	Descripción
SIP.REQ.CSEQ	Devuelve el número CSEQ del CSEQ, como un entero. Por ejemplo, para un encabezado CSEQ SIP de CSeq: 101 INVITE, esta expresión devuelve 101.
SIP.REQ.HEADER(<header_name>)	Devuelve el encabezado SIP especificado. Para <header_name>, sustituya el nombre del encabezado que quiera. Por ejemplo, para devolver el encabezado SIP From, escriba SIP.REQ.HEADER(“From”).
SIP.REQ.HEADER(<header_name>).INSTANCE(<line_number>)	Devuelve la instancia especificada del encabezado SIP especificado. Pueden producirse varias instancias del mismo encabezado SIP. Si quiere una instancia específica de dicho encabezado SIP (por ejemplo, un encabezado Via específico), puede especificar ese encabezado escribiendo un número como <line_number>. Las instancias de encabezado se emparejan desde el último (0) hasta el primero. En otras palabras, SIP.REQ.HEADER (“Via”).INSTANCE (0) devuelve la última instancia del encabezado Via, mientras que SIP.REQ.HEADER (“Via”).INSTANCE (1) devuelve la última instancia pero una de la cabecera Via, y así sucesivamente. Por ejemplo, si se utiliza en el encabezado SIP de ejemplo, SIP.REQ.HEADER (“Via”).INSTANCE (1) ReturnsVia: SIP/2.0/UDP 10.102.84. 180:5060; branch=z9hG4bK03e76d0b;rport=5060.
SIP.REQ.HEADER(<header_name>).VALUE(<line_	Devuelve el contenido de la instancia especificada del encabezado SIP especificado. El uso es casi el mismo que la expresión anterior. Por ejemplo, si se utiliza en el ejemplo de encabezado SIP de la entrada de tabla anterior, SIP.REQ.HEADER (“Via”).VALUE (1) devuelve SIP/2.0/UDP 10.102.84. 180:5060; branch=z9hG4bK03e76d0b;rport=5060.

Expresión	Descripción
SIP.REQ.HEADER(<header_name>).COUNT	Devuelve el número de instancias de un encabezado particular como un entero. Por ejemplo, si se utiliza en el ejemplo de encabezado SIP anterior, SIP.REQ.HEADER (“Via”).COUNT devuelve 2.
SIP.REQ.HEADER (<header_name>).EXISTS	Devuelve un valor booleano de true o false, en función de si el encabezado especificado existe o no. Por ejemplo, si se utiliza en el ejemplo de encabezado SIP anterior, SIP.REQ.HEADER (“Expira”).ExistsReturns true, mientras que SIP.REQ.HEADER (“Caller-ID”).EXISTS devuelve false.
SIP.REQ.HEADER (<header_name>).LIST	Devuelve la lista de parámetros separados por comas en el encabezado especificado. Por ejemplo, si se utiliza en el ejemplo de encabezado SIP anterior, SIP.REQ.HEADER (“Permitir”).LIST devuelve ACK, BYE, CANCEL, INVITE, NOTIFICAR, OPTIONS, REFER, REGISTRAR, UPDATE. Puede anexar la cadena.GET (<list_item_number>) para seleccionar un elemento de lista específico. Por ejemplo, para obtener el primer elemento (ACK) de la lista anterior, escriba SIP.REQ.HEADER (“Permitir”).LIST.GET (0). Para extraer el segundo elemento (BYE), escriba SIP.REQ.HEADER (“Permitir”).LIST.GET (1). Nota: Si el encabezado especificado contiene una lista de pares nombre/valor, se devuelve el par nombre/valor completo.

Expresión	Descripción
SIP.REQ.HEADER (<header_name>).TYPECAST_SIP_HEADER_T (“ <in_header_name> “)	Convierte el tipo <header_name> en <in_header_name>. Cualquier texto se puede convertir en la clase sip_header_t, después de lo cual se pueden usar todas las operaciones basadas en encabezado. Después de realizar esta operación, puede aplicar todas las operaciones que se pueden utilizar con <in_header_name>. Por ejemplo, la expresión SIP.REQ.CONTENT_LENGTH.TYPECAST_SIP_HEADER_T escribe todas las instancias del encabezado Content-Length. Después de realizar esta operación, puede aplicar todas las operaciones de encabezado a todas las instancias del encabezado especificado.
SIP.REQ.HEADER(<header_name>).CONTAINS(<string>)	Devuelve booleano true si la cadena de texto especificada está presente en cualquier instancia del encabezado especificado. Funciona en todas las instancias del encabezado especificado. Las instancias de encabezado se emparejan desde el último (0) hasta el primero.
SIP.REQ.HEADER(<header_name>).EQUALS_ANY	Devuelve un booleano true si cualquier patrón asociado con <patset> coincide con cualquier contenido en cualquier instancia del encabezado especificado. Funciona en todas las instancias del encabezado especificado. Las instancias de encabezado se emparejan desde el último (0) hasta el primero.
SIP.REQ.HEADER(<header_name>).CONTAINS_ANY(<patset>)	Devuelve un booleano true si cualquier patrón asociado con <patset> coincide con cualquier contenido en cualquier instancia del encabezado especificado. Funciona en todas las instancias del encabezado especificado. Las instancias de encabezado se emparejan desde el último (0) hasta el primero.

Expresión	Descripción
SIP.REQ.HEADER(<header_name>).CONTAINS_IN	Devuelve el índice del patrón coincidente asociado con <patset> si ese patrón coincide con cualquier contenido en cualquier instancia del encabezado especificado. Funciona en todas las instancias del encabezado especificado. Las instancias de encabezado se emparejan desde el último (0) hasta el primero.
SIP.REQ.HEADER(<header_name>).EQUALS_INDEX(<patset>)	Devuelve el índice del patrón coincidente asociado con <patset> si ese patrón coincide con cualquier instancia del encabezado especificado. Funciona en todas las instancias del encabezado especificado. Las instancias de encabezado se emparejan desde el último (0) hasta el primero.
SIP.REQ.HEADER(<header_name>).SUBSTR(<stri	Si la cadena especificada está presente en cualquier instancia del encabezado especificado, esta expresión devuelve esa cadena. Por ejemplo, para el encabezado SIP Via: SIP/2.0/UDP 10.102.84. 180:5060; branch=z9hG4bK03e76d0b;rport=5060; recibido=10.102.84.160", SIP.REQ.HEADER ("Via").SUBSTR ("rSUBport=5060") devuelve "rport=5060".sip.req.header ("Vía").header ("Via").header R ("rport=5061") devuelve una cadena vacía.
SIP.REQ.HEADER(<header_name>).AFTER_STR(<string>)	Si la cadena especificada está presente en cualquier instancia del encabezado especificado, esta expresión devuelve la cadena inmediatamente después de esa cadena. Por ejemplo, para el encabezado SIP Via: SIP/2.0/UDP 10.102.84. 180:5060; branch=z9hG4bK03e76d0b;rport=5060; recibido=10.102.84.160, la expresión SIP.REQ.HEADER ("Via").AFTER_STR ("rport=") devuelve 5060.

Expresión	Descripción
SIP.REQ.HEADER(<header_name>).REGEX_MATC	Devuelve booleano verdadero si la expresión regular especificada (expresión regular) coincide con cualquier instancia del encabezado especificado. Debe especificar la expresión regular en el siguiente formato: Re <delimiter> expresión regular <same delimiter>. La expresión regular no puede tener más de 1499 caracteres de longitud. Debe ajustarse a la biblioteca de expresiones regulares PCRE. Consulte http://www.pcre.org/pcre.txt para obtener documentación sobre la sintaxis de expresiones regulares PCRE. La página de comando man pcrepattern también tiene información útil sobre la especificación de patrones mediante expresiones regulares PCRE. La sintaxis de expresión regular admitida en esta expresión tiene algunas diferencias con respecto a PCRE. No se permiten referencias anteriores. Debe evitar las expresiones regulares recursivas; aunque algunas funcionan, muchas no lo hacen. El metacaractero punto (.) coincide con las líneas nuevas. No se admite Unicode. SET_TEXT_MODE (IGNORECASE) anula el (? i) opción interna especificada en la expresión regular.

Expresión	Descripción
SIP.REQ.HEADER(<header_name>).REGEX_SELECT(<regexp>)	Si la expresión regular especificada coincide con cualquier texto de cualquier instancia del encabezado especificado, esta expresión devuelve el texto. Por ejemplo, para el encabezado SIP Via: SIP/2.0/UDP 10.102.84. 180:5060; branch=Z9HG4BK03E76D0b; rport=5060; recived=10.102.84.160, la expresión SIP.REQ.HEADER (“Via”) .REGEX_SELECT (“recived=[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}”) devuelve recibida=10.102.84.160.
SIP.REQ.HEADER(<header_name>).AFTER_REGE	Si la expresión regular especificada coincide con cualquier texto de cualquier instancia del encabezado especificado, esta expresión devuelve la cadena inmediatamente después de ese texto. Por ejemplo, para el encabezado SIP Via: SIP/2.0/UDP 10.102.84. 180:5060; branch=z9hG4bK03e76d0b;rport=5060; recibido=10.102.84.160, la expresión SIP.REQ.HEADER (“Via”).AFTER_REGEX (“recibido=”) devuelve 10.102.84.160.
SIP.REQ.HEADER(<header_name>).BEFORE_REGEX(<regexp>)	Si la expresión regular especificada coincide con cualquier texto de cualquier instancia del encabezado especificado, esta expresión devuelve la cadena inmediatamente antes de ese texto. Por ejemplo, para el encabezado SIP Via: SIP/2.0/UDP 10.102.84. 180:5060; branch=z9hG4bK03e76d0b;rport=5060; recibido=10.102.84.160, la expresión SIP.REQ.HEADER (“Via”).BEEFER_REGEX (“[0-9]{1,3}. [0-9]{ 1,3}. [0-9]{ 1,3}. [0-9]{ 1,3}”) devuelve recibido=.
SIP.REQ.FULL_HEADER	Devuelve todo el encabezado SIP, incluido el CR/LF de terminación.
SIP.REQ.IS_VALID	Devuelve booleano true si el formato de solicitud es válido.

Expresión	Descripción
SIP.REQ.BODY (<length>)	Devuelve el cuerpo de la solicitud, hasta la longitud especificada. Si la longitud especificada es mayor que la longitud del cuerpo de la solicitud, esta expresión devuelve todo el cuerpo de la solicitud.
SIP.REQ.LB_VSERVER	Devuelve el nombre del servidor virtual de equilibrio de carga (LB vserver) que está sirviendo la solicitud actual.
SIP.REQ.CS_VSERVER	Devuelve el nombre del servidor virtual de conmutación de contenido (CS vserver) que está sirviendo la solicitud actual.

Expresiones de respuesta SIP

Expresión	Descripción
SIP.RES.STATUS	Devuelve el código de estado de respuesta SIP. Por ejemplo, si la primera línea de la respuesta es SIP/2.0 100 Tratando, esta expresión devuelve 100.
SIP.RES.STATUS_MSG	Devuelve el mensaje de estado de respuesta SIP. Por ejemplo, si la primera línea de la respuesta es SIP/2.0 100 Intentar, esta expresión devuelve Intentar.
SIP.RES.IS_REDIRECT	Devuelve booleano verdadero si el código de respuesta es una redirección.
SIP.RES.METHOD	Devuelve el método de respuesta extraído de la cadena del método de solicitud en el encabezado CSeQ.

Operaciones para codificación HTTP, HTML y XML y caracteres “seguros”

August 20, 2021

Las siguientes operaciones funcionan con la codificación de datos HTML en una solicitud o respuesta

y datos XML en un cuerpo POST.

- **<text>.HTML_XML_SAFE:**
  Transforma caracteres especiales en formato seguro XML, como en los ejemplos siguientes:

  Un corchete angular que apunta hacia la izquierda (<) se convierte en < Un corchete angular que apunta a la derecha (
) se convierte a > Un símbolo (&) se convierte en & Esta operación protege contra
  los ataques de scripts entre sitios
  . La longitud máxima del texto transformado es de 2048 bytes. Se trata de una operación de solo lectura.

  Después de aplicar la transformación, los operadores adicionales que especifique en la expresión se aplican al texto seleccionado. A continuación se presenta un ejemplo:

  http.req.url.query.html_xml_safe. contiene (“MyQueryString”)

- **<text>.HTTP_HEADER_SAFE:**
  Convierte todos los nuevos caracteres de línea (‘n’) en el texto de entrada a ‘%0A’ para permitir que la entrada se utilice de forma segura en encabezados HTTP.

  Esta operación protege contra ataques de división de respuesta.

  La longitud máxima del texto transformado es de 2048 bytes. Se trata de una operación de solo lectura.

- **<texto>.HTTP_URL_SAFE:**
  Convierte caracteres URL no seguros en valores ‘%xx’, donde “xx” es una representación basada en hexágono del carácter de entrada. Por ejemplo, el signo y comercial (&) se representa como%26 en codificación segura de URL. La longitud máxima del texto transformado es de 2048 bytes. Se trata de una operación de solo lectura.

  Los siguientes son los caracteres seguros de URL. Todos los demás son inseguros:

  - Caracteres alfanuméricos: A-z, A-Z, 0-9
  - Asterix: “*”
  - Y comercial: “&”
  - At-Signo: “@”
  - Dos puntos: “:”
  - Comma: “,”
  - Dólar: “$”
  - Punto: “.”
  - Es igual a: “=”
  - Signo de exclamación: “! “
  - Guión: “-“
  - Abrir y cerrar paréntesis: “(“, “)”

  - Porcentaje: “%”
  - Más: “+”
  - Punto y coma: “;”
  - Comilla simple: “”’
  - Barra: “/”
  - Signo de interrogación: “?”
  - Tilde: “~”
  - Subrayado: “_”

- **<text>MARK_SAFE:**

  Marca el texto como seguro sin aplicar ningún tipo de transformación de datos.

- **<text>.SET_TEXT_MODE (URLENCODED|NOURLENCODED)**

  Transforma toda la codificación%hh en la secuencia de bytes. Esta operación funciona con caracteres (no bytes). De forma predeterminada, un solo byte representa un carácter en codificación ASCII. Sin embargo, si especifica el modo URLENCODED, tres bytes pueden representar un carácter.

  En el ejemplo siguiente, una operación PREFIX (3) selecciona los 3 primeros caracteres de un destino.

  ```
  http.req.url.hostname.prefix(3)
  ```

  En el ejemplo siguiente, Citrix ADC puede seleccionar hasta 9 bytes del destino:

  ```
  http.req.url.hostname.set_text_mode(urlencoded).prefix(3)
  ```

- **<text>.SET_TEXT_MODE (PLUS_AS_SPACE|NO_PLUS_AS_SPACE):**

  Especifica cómo tratar el carácter más (+). La opción PLUS_AS_SPACE reemplaza un carácter más por espacio en blanco. Por ejemplo, el texto “Hola+mundo” se convierte en “hola mundo”. La opción NO_PLUS_AS_SPACE deja caracteres más tal como están.

- **<text>.SET_TEXT_MODE (BACKSLASH_ENCODED|NO_BACKSLASH_ENCODED):**

  Especifica si la decodificación de barras inversas se realiza o no en el objeto de texto representado por <text>.

  Si se especifica BACKSLASH_ENDIED, el operador SET_TEXT_MODE realiza las siguientes operaciones en el objeto de texto:

  - Todas las apariciones de “XXX” se reemplazarán con el carácter “Y” (donde XXX representa un número en el sistema octal y Y representa el equivalente ASCII de XXX). El rango válido de valores octales para este tipo de codificación es de 0 a 377. Por ejemplo, el texto codificado “http72//” y http072//” se decodificarán a <http://>, donde el colon (:) es el equivalente ASCII del valor octal “72”.

- Todas las apariciones de “xHH” se reemplazarán con el carácter “Y” (HH representa un número en el sistema hexadecimal e Y denota el equivalente ASCII de HH. Por ejemplo, el texto codificado “http\x3a//” se decodificará a <http://>, donde los dos puntos (:) es el equivalente ASCII del valor hexadecimal “3a”.
- Todas las apariciones de “\uWWXX” serán reemplazadas por la secuencia de caracteres “YZ” (donde WW y XX representan dos valores hexadecimales distintos y Y y Z representan sus equivalentes ASCII de WW y XX respectivamente. Por ejemplo, el texto codificado “http%u3a2f/” y “http%u003a//” se decodificarán a <http://>, donde “3a” y “2f” son dos valores hexadecimales y los dos puntos (:) y la barra diagonal (“/”) representan sus equivalentes ASCII respectivamente.
- Todas las apariciones de “b”, “n”, “t”, “f” y “r” se reemplazan con los caracteres ASCII correspondientes.

Si se especifica NO_BACKSLASH_ENCODED, la decodificación de barras invertidas no se realiza en el objeto de texto.

- **<text>.SET_TEXT_MODE(BAD_ENCODE_RAISE_UNDEF|NO_BAD_ENCODE_RAISE_UNDEF):**

  Realiza la acción indefinida asociada si se establece el modo URLENCODED o BACKSLASH_ENCODED y se encuentra una codificación incorrecta correspondiente al modo de codificación especificado en el objeto de texto representado por <text>.

  Si se especifica NO_BAD_ENCODE_RAISE_UNDEF, la acción indefinida asociada no se realizará cuando se encuentre una codificación incorrecta en el objeto de texto representado por <text>.

Expresiones para datos TCP, UDP y VLAN

August 20, 2021

Los datos TCP y UDP toman la forma de una cadena o un número. Para prefijos de expresión que devuelven valores de cadena para datos TCP y UDP, puede aplicar cualquier operación basada en texto. Para obtener más información, consulte Expresiones de directivas avanzadas: evaluación de texto.

Para prefijos de expresión que devuelven un valor numérico, como un puerto de origen, puede aplicar una operación aritmética. Para obtener más información, consulte Operaciones básicas sobre prefijos de expresión y Operaciones compuestas para números.

En la tabla siguiente se describen los prefijos que extraen datos TCP y UDP.

Operación GET	Descripción
CLIENT.TCP.PAYLOAD(<integer>)	Devuelve los datos de carga TCP como una cadena, comenzando por el primer carácter de la carga útil y continuando por el número de caracteres del argumento <integer>. Puede aplicar cualquier operación basada en texto a este prefijo.
CLIENT.TCP.SRCPORT	Devuelve el ID del puerto de origen del paquete actual como un número.
CLIENT.TCP.DSTPORT	Devuelve el ID del puerto de destino del paquete actual como un número.
CLIENT.TCP.OPTIONS	Devuelve las opciones TCP establecidas por el cliente. Ejemplos de opciones TCP son Tamaño máximo de segmento (MSS), Escala de ventana, Reconocimiento selectivo (SACK) y Opción de sello de tiempo. Los <type> <m> operadores COUNT, TYPE () y TYPE_NAME () se pueden utilizar con este prefijo. Para ver las opciones TCP establecidas por el servidor, vea el prefijo SERVER.TCP.OPTIONS.
CLIENT.TCP.OPTIONS.COUNT	Devuelve el número de opciones TCP que el cliente ha establecido.
CLIENT.TCP.OPTIONS.TYPE (<type>)	Devuelve el valor de la opción TCP cuyo tipo (o tipo de opción) se especifica como argumento. El valor se devuelve como una cadena de bytes en formato big endian (o orden de bytes de red). Parámetros: Type: Type value

Operación GET	Descripción
CLIENT.TCP.OPTIONS.TYPE_NAME (<m>)	Devuelve el valor de la opción TCP cuya constante de enumeración se especifica como argumento. Las constantes de enumeración que puede pasar como argumento son REPEATER, TIMESTAMP, SACK_PERMITTED, WINDOW y MAXSEG. Para especificar el tipo de opción TCP en lugar de estas constantes de enumeración, utilice CLIENT.TCP.OPTIONS.TYPE (<type>). Para otras opciones TCP, debe usar CLIENT.TCP.OPTIONS.TYPE (<type>). Parámetros: M: Constante de enumeración de opciones TCP
CLIENT.TCP.REPEATER_OPTION.EXISTS	Devuelve un valor booleano TRUE si existen opciones TCP del repetidor.
CLIENT.TCP.REPEATER_OPTION.IP	Devuelve la dirección IPv4 del repetidor de rama desde las opciones TCP del repetidor.
CLIENT.TCP.REPEATER_OPTION.MAC	Devuelve la dirección MAC del repetidor de rama desde las opciones TCP del repetidor.
CLIENT.UDP.DNS.DOMAIN	Devuelve el nombre de dominio DNS.
CLIENT.UDP.DNS.DOMAIN.EQ (“ <hostname> “)	Devuelve un valor booleano TRUE si el nombre de dominio coincide con el <hostname> argumento. La comparación no distingue entre mayúsculas y minúsculas. A continuación se presenta un ejemplo: Client.udp.dns.domain.eq (“www.mycompany.com”)
CLIENT.UDP.DNS.IS_AAAAREC	Devuelve un valor booleano TRUE si el tipo de registro es AAAA. Estos tipos de registros indican una dirección IPv6 en las búsquedas futuras.
CLIENT.UDP.DNS.IS_ANYREC	Devuelve un valor booleano TRUE si es de cualquier tipo de registro.
CLIENT.UDP.DNS.IS_AREC	Devuelve un valor booleano TRUE si el registro es de tipo A. Los registros de tipo A proporcionan la dirección del host.

Operación GET	Descripción
CLIENT.UDP.DNS.IS_CNAMEREC	Devuelve un valor booleano TRUE si el registro es de tipo CNAME. En sistemas que utilizan varios nombres para identificar un recurso, hay un nombre canónico y varios alias. El CNAME proporciona el nombre canónico.
CLIENT.UDP.DNS.IS_MXREC	Devuelve un valor booleano TRUE si el registro es de tipo MX (intercambiador de correo). Este registro DNS describe una prioridad y un nombre de host. Los registros MX del mismo nombre de dominio especifican los servidores de correo electrónico del dominio y la prioridad de cada servidor.
CLIENT.UDP.DNS.IS_NSREC	Devuelve un valor booleano TRUE si el registro es de tipo NS. Se trata de un registro de servidor de nombres que incluye un nombre de host con un registro A asociado. Esto permite localizar el nombre de dominio asociado con el registro NS.
CLIENT.UDP.DNS.IS_PTRREC	Devuelve un valor booleano TRUE si el registro es de tipo PTR. Este es un puntero de nombre de dominio y se utiliza a menudo para asociar un nombre de dominio con una dirección IPv4.
CLIENT.UDP.DNS.IS_SOAREC	Devuelve un valor booleano TRUE si el registro es de tipo SOA. Este es un registro de inicio de autoridad.
CLIENT.UDP.DNS.IS_SRVREC	Devuelve un valor booleano TRUE si el registro es de tipo SRV. Esta es una versión más general del registro MX.
CLIENT.UDP.DSTPORT	Devuelve el ID numérico del puerto de destino UDP del paquete actual.
CLIENT.UDP.SRCPORT	Devuelve el ID numérico del puerto de origen UDP del paquete actual.
CLIENT.UDP.RADIO	Devuelve datos RADIUS para el paquete actual.
CLIENT.UDP.RADIUS.ATTR_TYPE (<type>)	Devuelve el valor del tipo de atributo especificado como argumento.

Operación GET	Descripción
CLIENT.UDP.RADIUS.NOMBRE DE USUARIO	Devuelve el nombre de usuario RADIUS.
CLIENT.TCP.MSS	Devuelve el tamaño máximo del segmento (MSS) de la conexión actual como un número.
CLIENT.VLAN.ID	Devuelve el ID numérico de la VLAN a través de la cual el paquete actual introdujo el dispositivo Citrix ADC.
SERVER.TCP.DSTPORT	Devuelve el ID numérico del puerto de destino del paquete actual.
SERVER.TCP.SRCPORT	Devuelve el ID numérico del puerto de origen del paquete actual.
SERVER.TCP.OPTIONS	Devuelve las opciones TCP establecidas por el servidor. Ejemplos de opciones TCP son Tamaño máximo de segmento (MSS), Escala de ventana, Reconocimiento selectivo (SACK) y Opción de sello de tiempo. Los <type> <m> operadores COUNT, TYPE () y TYPE_NAME () se pueden utilizar con este prefijo. Para ver las opciones TCP establecidas por el cliente, vea el prefijo CLIENT.TCP.OPTIONS.
SERVER.TCP.OPTIONS.COUNT	Devuelve el número de opciones TCP que el servidor ha establecido.
SERVER.TCP.OPTIONS.TYPE (<type>)	Devuelve el valor de la opción TCP cuyo tipo (o tipo de opción) se especifica como argumento. El valor se devuelve como una cadena de bytes en formato big endian (o orden de bytes de red). Parámetros: Type: Type value

Operación GET	Descripción
SERVER.TCP.OPTIONS.TYPE_NAME (<m>)	Devuelve el valor de la opción TCP cuya constante de enumeración se especifica como argumento. Las constantes de enumeración que puede pasar como argumento son REPEATER, TIMESTAMP, SACK_PERMITTED, WINDOW y MAXSEG. Para especificar el tipo de opción TCP en lugar de estas constantes de enumeración, utilice CLIENT.TCP.OPTIONS.TYPE (<type>). Para otras opciones TCP, debe usar CLIENT.TCP.OPTIONS.TYPE (<type>). Parámetros: M: Constante de enumeración de opciones TCP
SERVER.VLAN	Funciona en la VLAN a través de la cual el paquete actual introdujo el dispositivo Citrix ADC.
SERVER.VLAN.ID	Devuelve el ID numérico de la VLAN a través de la cual el paquete actual introdujo el dispositivo Citrix ADC.

Expresiones para evaluar un mensaje DNS e identificar su protocolo de portadora

January 21, 2022

Puede evaluar las solicitudes y respuestas de DNS mediante expresiones que comiencen por DNS.REQ y DNS.RES, respectivamente. También puede identificar el protocolo de capa de transporte que se está usando para enviar los mensajes DNS.

Las siguientes funciones devuelven el contenido de una consulta DNS.

Función	Descripción
DNS.REQ.QUESTION.DOMAIN	Devuelve el nombre de dominio (el valor del campo QNAME) en la sección de preguntas de la consulta DNS. El nombre de dominio se devuelve como una cadena de texto, que se puede pasar a EQ (), NE () y a cualquier otra función que funcione con texto.
DNS.REQ.QUESTION.TYPE	Devuelve el tipo de consulta (el valor del campo QTYPE) en la consulta DNS. El campo indica el tipo de registro de recursos (por ejemplo, A, NS o CNAME) para el que se consulta el servidor de nombres. El valor devuelto se puede comparar con uno de los siguientes valores mediante las funciones EQ () y NE (): A, AAAA, NS, SRV, PTR, CNAME, SOA, MX y ANY. Nota: Solo puede utilizar las funciones EQ () y NE () con la función TYPE. Ejemplo: DNS.REQ.QUESTION.TYPE.EQ (MX)

Las siguientes funciones devuelven el contenido de una respuesta DNS.

Función	Descripción
DNS.RES.HEADER.RCODE	Devuelve el código de respuesta (el valor del campo RCODE) en la sección de encabezado de la respuesta DNS. Solo puede usar las funciones EQ () y NE () con la función RCODE. A continuación se presentan los valores posibles: NOERROR, FORMERR, SERVFAIL, NXDOMAIN, NOTIMP y REFUSED.
DNS.RES.QUESTION.DOMAIN	Devuelve el nombre de dominio (el valor del campo QNAME) en la sección de preguntas de la respuesta DNS. El nombre de dominio se devuelve como una cadena de texto, que se puede pasar a EQ (), NE () y a cualquier otra función que funcione con texto.

Función	Descripción
DNS.RES.QUESTION.TYPE	Devuelve el tipo de consulta (el valor del campo QTYPE) en la sección de preguntas de la respuesta DNS. El campo indica el tipo de registro de recursos (por ejemplo, A, NS o CNAME) que se incluye en la respuesta. El valor devuelto se puede comparar con uno de los siguientes valores mediante las funciones EQ () y NE (): A, AAAA, NS, SRV, PTR, CNAME, SOA, MX y ANY. Solo puede usar las funciones EQ () y NE () con la función TYPE. Ejemplo: DNS.RES.QUESTION.TYPE.EQ (SOA)

Las siguientes funciones devuelven el nombre del protocolo de la capa de transporte.

Función	Descripción
DNS.REQ.TRANSPORT	Devuelve el nombre del protocolo de capa de transporte que se usó para enviar la consulta DNS. Los valores posibles devueltos son TCP y UDP. Solo puede utilizar las funciones EQ () y NE () con la función TRANSPORT. Ejemplo: DNS.REQ.TRANSPORT.EQ (TCP)
DNS.RES.TRANSPORT	Devuelve el nombre del protocolo de capa de transporte que se usó para la respuesta DNS. Los valores posibles devueltos son TCP y UDP. Solo puede utilizar las funciones EQ () y NE () con la función TRANSPORT. Ejemplo: DNS.RES.TRANSPORT.EQ (TCP)

Las siguientes funciones devuelven el nombre de la ubicación coincidente cuando la consulta contiene o no la opción DNS ECS.

Función	Descripción
DNS.REQ.OPT.ECS.IP.MATCHES_LOCATION	Devuelve el nombre de la ubicación coincidente que se usó en la consulta con la opción DNS ECS. Ejemplo:(DNS.REQ.OPT.ECS.IP.MATCHES_LOCATION(“.CH…..”)
client.ip.src.matches_location	Devuelve el nombre de la ubicación coincidente que se usó en la consulta sin la opción DNS ECS. Ejemplo: (client.ip.src.matches_location (“.CH… “)
DNS.REQ.OPT.ECS.IP.MATCHES_LOCATION O client.ip.src.matches_location	Expresión común que se utilizará en la directiva cuando el tráfico DNS pueda tener o no la opción ECS en la consulta. Ejemplo: “(((DNS.REQ.OPT.ECS.IP.MATCHES_LOCATION(“.CH…..”).typec ALT (client.IP.SRC.MATCHES_LOCATION(“.CH…..”).typecast_text_t

XPath y expresiones HTML, XML o JSON

August 20, 2021

La infraestructura de directivas avanzada admite expresiones para evaluar y recuperar datos de archivos HTML, XML y JavaScript Object Notation (JSON). Esto le permite encontrar nodos específicos en un documento HTML, XML o JSON, determinar si existe un nodo en el archivo, localizar nodos en contextos XML (por ejemplo, nodos que tienen elementos principales específicos o un atributo específico con un valor determinado) y devolver el contenido de dichos nodos. Además, puede utilizar expresiones XPath en expresiones de reescritura.

La implementación de expresión de directiva avanzada para XPath incluye un prefijo de expresión de directiva avanzada (como “HTTP.REQ.BODY”) que designa texto HTML o XML, y el operador XPATH que toma la expresión XPath como argumento.

Los archivos HTML son una colección en gran medida libre de etiquetas y elementos de texto. Puede utilizar el operador XPATH_HTML, que toma como argumento una expresión XPath, para procesar archivos HTML. Los archivos JSON son una colección de pares de nombre/valor o una lista ordenada de valores. Puede utilizar el operador XPATH_JSON, que toma como argumento una expresión XPath, para procesar archivos JSON.

- **<text>.XPATH (xpathex):**

Opere en un archivo XML y devuelva un valor booleano.

Por ejemplo, la siguiente expresión devuelve un valor booleano TRUE si existe un nodo llamado "creador" bajo el nodo "Libro" dentro de los primeros 1000 bytes del archivo XML.

```
HTTP.REQ.BODY(1000).XPATH(xp%boolean(//Book/creator)%)
```

Parámetros:

xpathex: Expresión booleana XPath

- **<text>.XPATH (xpathex):**

  Operar en un archivo XML y devolver un valor de tipo de datos "doble".

  Por ejemplo, la siguiente expresión convierte la cadena "36" (un valor de precio) en un valor de tipo de datos "double" si la cadena está en los primeros 1000 bytes del archivo XML:

  ```
  HTTP.REQ.BODY(1000).XPATH(xp%number(/Book/price)%)
  ```

  Parámetros:

  xpathex: Expresión numérica XPath

Ejemplo:

```
    <Book>
    <creator>
        <Person>
            <name>Milton</name>
        </Person>
    </creator>
    <title>Paradise Lost</title>
    </Book>
<!--NeedCopy-->
```

- **<text>.XPATH (xpathex):**

  Opere en un archivo XML y devuelva un conjunto de nodos o una cadena. Los conjuntos de nodos se convierten en cadenas correspondientes mediante el uso de la rutina de conversión de cadenas XPath estándar.

  Por ejemplo, la siguiente expresión selecciona todos los nodos que están encerrados por "/Book/Creator" (un conjunto de nodos) en los primeros 1000 bytes del cuerpo:

  ```
  HTTP.REQ.BODY(1000).XPATH(xp%/Book/creator%)
  ```

  Parámetros:

  xpathex: Expresión XPath

- **<text>.XPATH_HTML (xpathex)**

  Operar en un archivo HTML y devolver un valor de texto.

  Por ejemplo, la siguiente expresión funciona en un archivo HTML y devuelve el texto incluido en `<title\></title\>` las etiquetas si el elemento HTML de título se encuentra en los primeros 1000 bytes:

  ```
  HTTP.REQ.BODY(1000).XPATH_HTML(xp%/html/head/title%)
  ```

  Parámetros:

  xpathex: Expresión de texto XPath

- **<text>.XPATH_HTML_WITH_MARKUP (xpathex)**

  Opere en un archivo HTML y devuelva una cadena que contenga toda la parte seleccionada del documento, incluido el marcado, como incluir las etiquetas de elemento adjunto.

  La siguiente expresión funciona en el archivo HTML y selecciona todo el contenido de la <\ title> etiqueta, incluido el marcado.

  ```
  HTTP.REQ.BODY(1000).XPATH_HTML_WITH_MARKUP( xp%/html/head/title%)
  ```

  La parte del cuerpo HTML seleccionada por la expresión se marca para su posterior procesamiento.

  Parámetros:

  xpathex: Expresión XPath

- **<text>.XPATH_JSON (xpathex)**

  Opere en un archivo JSON y devuelva un valor booleano.

  Por ejemplo, considere el siguiente archivo JSON:

  {”Libro”: {”creator”: {”persona”: {”name”<name>:’}}, ”title” :’<title>’ } }

  La siguiente expresión opera en el archivo JSON y devuelve un valor booleano TRUE si el archivo JSON contiene un nodo llamado “creator”, cuyo nodo principal es “Book”, en los primeros 1000 bytes:

  ```
  HTTP.REQ.BODY(1000).XPATH_JSON(xp%boolean(/Book/creator)%)
  ```

  Parámetros:

  xpathex: Expresión booleana XPath

- **<text>.XPATH_JSON (xpathex)**

  Operar en un archivo JSON y devolver un valor de tipo de datos “doble”.

  Por ejemplo, considere el siguiente archivo JSON:

{”Libro”: {”creator”: {”persona”: {”name”<name>:’}}, ”title” :’<title>’, ”price” :”36”}}

La siguiente expresión opera en el archivo JSON y convierte la cadena “36” en un valor de tipo de datos “double” si la cadena está presente en los primeros 1000 bytes del archivo JSON.

```
HTTP.REQ.BODY(1000).XPATH_JSON(xp%number(/Book/price)%)
```

Parámetros:

xpathex: Expresión numérica XPath

- **<text>.XPATH_JSON (xpathex)**

  Opere en un archivo JSON y devuelva un conjunto de nodos o una cadena. Los conjuntos de nodos se convierten en cadenas correspondientes mediante el uso de la rutina de conversión de cadenas XPath estándar.

  Por ejemplo, considere el siguiente archivo JSON:

  {”Libro”: {”creator”: {”persona”: {”name”<name>:’}}, ”title” :’<title>’ } }

  La siguiente expresión selecciona todos los nodos que están encerrados por ”/Book” (un conjunto de nodos) en los primeros 1000 bytes del cuerpo del archivo JSON y devuelve el valor de cadena correspondiente, que es”<name><title>”:

  ```
  HTTP.REQ.BODY(1000).XPATH_JSON(xp%/Book%)
  ```

  Parámetros:

  xpathex: Expresión XPath

- **<text>.XPATH_JSON_WITH_MARKUP (xpathex)**

  Opere en un archivo XML y devuelva una cadena que contenga toda la parte del documento para el nodo de resultado, incluido el marcado, como incluir las etiquetas de elemento adjunto.

  Por ejemplo, considere el siguiente archivo JSON:

  {”Libro”: {”creator”: {”persona”: {”name”<name>:’}}, ”title” :’<title>’ } }

  La siguiente expresión opera en el archivo JSON y selecciona todos los nodos que están encerrados por “/book/creator” en los primeros 1000 bytes del cuerpo, que es “creator:{ person:{ name:’<name>’ } }.”

  ```
  HTTP.REQ.BODY(1000).XPATH_JSON_WITH_MARKUP(xp%/Book/creator%)
  ```

  La parte del cuerpo JSON seleccionada por la expresión se marca para su posterior procesamiento.

  Parámetros:

  xpathex: Expresión XPath

- **<text>.XPATH_WITH_MARKUP (xpathex):**

  Opere en un archivo XML y devuelva una cadena que contenga toda la parte del documento para el nodo de resultado, incluido el marcado, como incluir las etiquetas de elemento adjunto.

  Por ejemplo, la siguiente expresión opera en un archivo XML y selecciona todos los nodos incluidos por "/Book/Creator" en los primeros 1000 bytes del cuerpo.

  `HTTP.REQ.BODY(1000).XPATH_WITH_MARKUP(xp%/Book/creator%)`

  La parte del cuerpo JSON seleccionada por la expresión se marca para su posterior procesamiento.

  Parámetros:

  xpathex: Expresión XPath

Cifrar y descifrar cargas útiles XML

October 5, 2021

Puede utilizar las funciones XML_ENCRYPT() y XML_DECRYPT() de las expresiones de directiva avanzadas para cifrar y descifrar, respectivamente, datos XML. Estas funciones cumplen con el estándar de cifrado XML del W3C definido en "http://www.w3.org/TR/2001/PR-xmldsig-core-20010820/. " XML_ENCRYPT() y XML_DECRYPT() admiten un subconjunto de la especificación Cifrado XML. En el subconjunto, el cifrado de datos utiliza un método de cifrado masivo (RC4, DES3, AES128, AES192 o AES256) y se utiliza una clave pública RSA para cifrar la clave de cifrado masivo.

Nota: Si quiere cifrar y descifrar texto en una carga útil, debe utilizar las funciones ENCRYPT y DECRYPT. Para obtener más información sobre estas funciones, consulte Cifrar y descifrar texto.

Las funciones XML_ENCRYPT() y XML_DECRYPT() no dependen del servicio de cifrado/descifrado utilizado por los comandos ENCRYPT y DECRYPT para el texto. El método cipher se especifica explícitamente como argumento de la función XML_ENCRYPT(). La función `XML_DECRYPT()` obtiene la información sobre el método de cifrado especificado del elemento `<xenc:EncryptedData>`. A continuación se presentan sinopsis de las funciones de cifrado y descifrado XML:

- Elemento `XML_ENCRYPT(<certKeyName>, <method> [, <flags>])**. Returns an <xenc:EncryptedData>` que contiene el texto de entrada cifrado y la clave de cifrado, que a su vez se cifra mediante RSA.
- `XML_DECRYPT(<certKeyName>)`. Devuelve el texto descifrado del elemento `<xenc:EncryptedData>` de entrada, que incluye el método de cifrado y la clave cifrada con RSA.

Nota: El elemento `<xenc:EncryptedData>` se define en la especificación de cifrado XML del W3C.

A continuación se presentan las descripciones de los argumentos:

- **certKeyName:** selecciona un certificado X.509 con una clave pública RSA para XML_ENCRYPT() o una clave privada RSA para XML_DECRYPT(). La clave de certificado debe haberse creado previamente mediante un comando `add ssl certKey`.
- **method:** Especifica qué método de cifrado se utilizará para cifrar los datos XML. Valores posibles: RC4, DES3, AES128, AES192, AES256.
- **flags:** Máscara de bits que especifica la siguiente información clave opcional (<ds:KeyInfo>) que se incluirá en el elemento <xenc:EncryptedData> generado por `XML_ENCRYPT()`:
  - **1** : incluye un elemento keyName con certKeyName. El elemento es <ds:KeyName>.
  - **2** - Incluya un elemento keyValue con la clave pública RSA del certificado. El elemento es <ds:KeyValue>.
  - **4** - Incluya un elemento x509IssuerSerial con el número de serie del certificado y el DN del emisor. El elemento es <ds:X509IssuserSerial>.
  - **8** - Incluya un elemento x509SubjectName con el nombre distintivo del sujeto del certificado. El elemento es <ds:X509SubjectName>.
  - **16** - Incluye un elemento X509Certificate con el certificado completo. El elemento es <ds:X509Certificate>.

Utilizar las funciones XML_ENCRYPT() y XML_DECRYPT() en expresiones

La función de cifrado XML utiliza pares de claves de certificado SSL para proporcionar certificados X.509 (con claves públicas RSA) para el cifrado de claves y claves privadas RSA para el descifrado de claves. Por lo tanto, antes de utilizar la función XML_ENCRYPT() en una expresión, debe crear un par de claves de certificado SSL. El siguiente comando crea un par de claves de certificado SSL, my-certkey, con el certificado X.509, my-cert.pem, y el archivo de clave privada, my-key.pem.

```
add ssl certKey my-certkey -cert my-cert.pem -key my-key.pem -passcrypt
kxPeMRYnitY=
```

Los siguientes comandos de CLI crean directivas y acciones de reescritura para cifrar y descifrar contenido XML.

```
1 add rewrite action my-xml-encrypt-action replace "HTTP.RES.BODY(10000).
    XPATH_WITH_MARKUP(xp%/%)" "HTTP.RES.BODY(10000).XPATH_WITH_MARKUP(xp
    %/%).XML_ENCRYPT("my-certkey", AES256, 31)"
2
3 add rewrite action my-xml-decrypt-action replace "HTTP.REQ.BODY(10000).
    XPATH_WITH_MARKUP(xp%//xenc:EncryptedData%)" "HTTP.REQ.BODY(10000).
    XPATH_WITH_MARKUP(xp%//xenc:EncryptedData%).XML_DECRYPT("my-certkey"
    )"
4
```



```
5 add rewrite policy my-xml-encrypt-policy "HTTP.REQ.URL.CONTAINS("xml-
    encrypt")" my-xml-encrypt-action
6
7 add rewrite policy my-xml-decrypt-policy "HTTP.REQ.BODY(10000).XPATH(xp
    %boolean(//xenc:EncryptedData)%)" my-xml-decrypt-action
8
9 bind rewrite global my-xml-encrypt-policy 30
10
11 bind rewrite global my-xml-decrypt-policy 30
12 <!--NeedCopy-->
```

En el ejemplo anterior, la acción de reescritura my-xml-encrypt-action cifra todo el documento XML (XPATH_WITH_MARKUP (xp%/%)) de la solicitud mediante el método de cifrado masivo AES-256 y la clave pública RSA de my-certkey para cifrar la clave de cifrado masivo. La acción sustituye el documento por un elemento <xenc:EncryptedData> que contiene los datos cifrados y una clave cifrada. Las banderas representadas por 31 incluyen todos los elementos <ds:KeyInfo> opcionales.

La acción my-xml-decrypt-action descifra el primer elemento <xenc:EncryptedData> de la respuesta (XPATH_WITH_MARKUP(xp%//xenc:EncryptedData%)). Esto requiere la adición previa del espacio de nombres XML de xenc mediante el uso del siguiente comando de CLI:

```
add ns xmlnamespace xenc http://www.w3.org/2001/04/xmlenc##
```

La acción my-xml-decrypt-action utiliza la clave privada RSA de my-certkey para descifrar la clave cifrada y, a continuación, utiliza el método de cifrado masivo especificado en el elemento para descifrar el contenido cifrado. Por último, la acción reemplaza el elemento de datos cifrados por el contenido descifrado.

La directiva de reescritura my-xml-encrypt-policy aplica my-xml-encrypt-action a las solicitudes de URL que contienen xml-encrypt. La acción cifra toda la respuesta de un servicio configurado en el dispositivo Citrix ADC.

La directiva de reescritura my-xml-decrypt-policy aplica my-xml-decrypt-action a las solicitudes que contienen un elemento <xenc:EncryptedData> ((XPATH(xp%//xenc:EncryptedData%) devuelve una cadena no vacía). La acción descifra los datos cifrados en las solicitudes enlazadas para un servicio configurado en el dispositivo Citrix ADC.

Expresiones de directivas avanzadas: análisis de SSL

January 21, 2022

Existen expresiones de directivas avanzadas para analizar los certificados SSL y los mensajes de saludo del cliente SSL.

Analizar certificados SSL

Puede utilizar expresiones de directivas avanzadas para evaluar los certificados de cliente de capa de sockets seguros (SSL) X.509. Un certificado de cliente es un documento electrónico que se puede utilizar para autenticar la identidad de un usuario. Un certificado de cliente contiene (como mínimo) información de versión, un número de serie, un identificador de algoritmo de firma, un nombre de emisor, un período de validez, un nombre de sujeto (usuario), una clave pública y firmas.

Puede examinar tanto las conexiones SSL como los datos en los certificados de cliente. Por ejemplo, es posible que quiera enviar solicitudes SSL que usen cifrados de baja intensidad a una comunidad de servidores virtuales de equilibrio de carga en particular. El siguiente comando es un ejemplo de una directiva de Content Switching que analiza la fuerza de cifrado en una solicitud y hace coincidir las fortalezas de cifrado que son menores o iguales a 40:

```
1 add cs policy p1 -rule "client.ssl.cipher_bits.le(40)"
2 <!--NeedCopy-->
```

Como otro ejemplo, puede configurar una directiva que determine si una solicitud contiene un certificado de cliente:

```
1 add cs policy p2 -rule "client.ssl.client_cert exists"
2 <!--NeedCopy-->
```

O bien, puede configurar una directiva que examine información concreta en un certificado de cliente. Por ejemplo, la siguiente directiva verifica que el certificado tenga uno o más días antes del vencimiento:

```
1 add cs policy p2 -rule "client.ssl.client_cert exists && client.ssl.
     client_cert.days_to_expire.ge(1)"
2 <!--NeedCopy-->
```

> **Nota**
>
> Para obtener información sobre el análisis de fechas y horas de un certificado, consulte Formato de fechas y horas de una expresión y expresiones para fechas de certificado SSL.

Prefijos para datos SSL y certificados basados en texto

En la siguiente tabla se describen los prefijos de expresión que identifican los elementos basados en texto en las transacciones SSL y los certificados de cliente.

Tabla 1. Prefijos que devuelven texto o valores booleanos para datos de certificados de cliente y SSL

Prefix	Descripción
CLIENT.SSL.CLIENT_CERT	Devuelve el certificado de cliente SSL en la transacción SSL actual.
CLIENT.SSL.CLIENT_CERT.TO_PEM	Devuelve el certificado de cliente SSL en formato binario.
CLIENT.SSL.CIPHER_EXPORTABLE	Devuelve un valor booleano TRUE si el cifrado criptográfico SSL es exportable.
CLIENT.SSL.CIPHER_NAME	Devuelve el nombre del cifrado SSL si se invoca desde una conexión SSL y una cadena NULL si se invoca desde una conexión no SSL.
CLIENT.SSL.IS_SSL	Devuelve un valor booleano TRUE si la conexión actual se basa en SSL.
CLIENT.SSL.JA3_FINGERPRINT	Devuelve un valor booleano TRUE si la huella digital JA3 configurada coincide con la huella digital JA3 en el mensaje de saludo del cliente. **Nota:** Esta expresión está disponible en la versión 13.1 compilación 12.x y posteriores.

Prefijos para datos numéricos en certificados SSL

En la tabla siguiente se describen los prefijos que evalúan datos numéricos distintos de las fechas de los certificados SSL. Estos prefijos se pueden utilizar con las operaciones que se describen en Operaciones básicas sobre prefijos de expresión y Operaciones compuestas para números.

Tabla 2. Prefijos que evalúan los datos numéricos distintos de las fechas en los certificados SSL

Prefix	Descripción
CLIENT.SSL.CLIENT_CERT.DAYS_TO_EXPIRE	Devuelve el número de días en que el certificado es válido o devuelve -1 para certificados caducados.
CLIENT.SSL.CLIENT_CERT.PK_SIZE	Devuelve el tamaño de la clave pública utilizada en el certificado.
CLIENT.SSL.CLIENT_CERT.VERSION	Devuelve el número de versión del certificado. Si la conexión no se basa en SSL, devuelve cero (0).

Prefix	Descripción
CLIENT.SSL.CIPHER_BITS	Devuelve el número de bits de la clave criptográfica. Devuelve 0 si la conexión no se basa en SSL.
CLIENT.SSL.VERSION	Devuelve un número que representa la versión del protocolo SSL, de la siguiente manera: 0. La transacción no está basada en SSL: 0x002. La transacción es SSLv2: 0x300. La transacción es SSLv3: 0x301. La transacción es TLSv1: 0x302. La transacción es TLS 1.1: 0x303. La transacción es TLS 1.2: 0x304. La transacción es TLS 1.3.

> **Nota**
>
> Para ver las expresiones relacionadas con las fechas de caducidad de un certificado, consulte Expresiones para fechas de certificado SSL.

Expresiones para certificados SSL

Puede analizar certificados SSL configurando expresiones que usen el siguiente prefijo:

CLIENT.SSL.CLIENT_CERT

En esta sección se describen las expresiones que puede configurar para certificados, excepto las que examinan la caducidad del certificado. Las operaciones basadas en tiempo se describen en Expresiones de directivas avanzadas: trabajo con fechas, horas y números.

En la siguiente tabla se describen las operaciones que puede especificar para el prefijo CLIENT.SSL.CLIENT_CERT.

Tabla 3. Operaciones que se pueden especificar con el prefijo CLIENT.SSL.CLIENT_CERT

Operación de certificado SSL	Descripción
`<certificate>.EXISTS`	Devuelve un valor booleano TRUE si el cliente tiene un certificado SSL.

Operación de certificado SSL	Descripción
`<certificate>.ISSUER`	Devuelve el nombre distintivo (DN) del emisor en el certificado como una lista de nombre-valor. Un signo igual (“=”) es el delimitador del nombre y el valor, y la barra (“/”) es el delimitador que separa los pares nombre-valor. A continuación se muestra un ejemplo del DN devuelto: `/C=US/O=myCompany/OU=www.mycompany.com/CN=www.mycompany.com/emailAddress=myuserid@mycompany.com`
`<certificate>.ISSUER.IGNORE_EMPTY_ELEMENTS`	Devuelve el emisor e ignora los elementos vacíos en una lista de nombre-valor. Por ejemplo, considere lo siguiente: `Cert-Issuer: /c=in/st=kar//l=bangelore //o=mycompany/ou=sales/ /emailAddress=myuserid@mycompany.com`. La siguiente acción Reescritura devuelve un recuento de 6 basado en la definición de emisor anterior: `sh rewrite action insert_ssl_header Name: insert_ssl Operation: insert_http_header Target:Cert-Issuer Value:CLIENT.SSL.CLIENT_CERT.ISSUER.COUNT`. Sin embargo, si cambia el valor al siguiente, el recuento devuelto es 9: `CLIENT.SSL.CLIENT_CERT.ISSUER.IGNORE_EMPTY_ELEMENTS.COUNT`

Hola del cliente SSL de Parse

Puede analizar el mensaje de saludo del cliente SSL configurando expresiones que usen el siguiente prefijo:

Prefix	Descripción
CLIENT.SSL.CLIENT_HELLO.CIPHERS.HAS_CÓDIC HEXADECIMAL	Hace coincidir el código hexadecimal proporcionado en la expresión con los códigos hexadecimales de los conjuntos de cifrado recibidos en el mensaje de saludo del cliente.
CLIENT.SSL.CLIENT_HELLO.CLIENT_VERSION	Versión recibida en el encabezado del mensaje de saludo del cliente.
CLIENT.SSL.CLIENT_HELLO.IS_RENEGOCIAR	Devuelve true si un cliente o un servidor inicia la renegociación de la sesión.
CLIENT.SSL.CLIENT_HELLO.IS_REUSE	Devuelve true si el dispositivo reutiliza la sesión SSL en función del ID de sesión distinto de cero recibido en el mensaje de saludo del cliente.
CLIENT.SSL.CLIENT_HELLO.IS_SCSV	Devuelve true si la capacidad Signaling Cipher Suite Value (SCSV) se anuncia en el mensaje de saludo del cliente. El código hexadecimal para el SCSV de reserva es 0x5600.
CLIENT.SSL.CLIENT_HELLO.IS_SESSION_TICKET	Devuelve true si la extensión del tíquet de sesión con una longitud distinta de cero se anuncia en el mensaje de saludo del cliente.
CLIENT.SSL.CLIENT_HELLO.LENGTH	Longitud recibida en el encabezado del mensaje de saludo del cliente.
CLIENT.SSL.CLIENT_HELLO.SNI	Devuelve el nombre del servidor recibido en la extensión del nombre del servidor del mensaje de saludo del cliente.
CLIENT.SSL.CLIENT_HELLO.ALPN.HAS_NEXTPRC	Devuelve true si el protocolo de aplicación en la extensión ALPN recibido en el mensaje de saludo del cliente coincide con el protocolo proporcionado en la expresión.

Estas expresiones se pueden utilizar en el punto de enlace CLIENTHELLO_REQ. Para obtener más información, consulte Vinculación de directivas SSL.

Expresiones de directivas avanzadas: direcciones IP y MAC, rendimiento, ID de VLAN

October 5, 2021

Puede utilizar prefijos de expresión de directivas avanzadas que devuelven direcciones IPv4 e IPv6, direcciones MAC, subredes IP, datos útiles del cliente y del servidor, como las velocidades de rendimiento en los puertos de interfaz (Rx, Tx y RxTx) y los ID de las VLAN a través de las que se reciben los paquetes. A continuación, puede utilizar varios operadores para evaluar los datos que devuelven estos prefijos de expresión.

Expresiones para direcciones IP y subredes IP

Puede utilizar expresiones de directivas avanzadas para evaluar direcciones y subredes que tienen el formato Protocolo de Internet versión 4 (IPv4) o Protocolo de Internet versión 6 (IPv6). Los prefijos de expresión para direcciones y subredes IPv6 incluyen IPv6 en el prefijo. Los prefijos de expresión para direcciones y subredes IPv4 incluyen IP en el prefijo. A continuación se muestra un ejemplo de expresión que identifica si una solicitud se ha originado en una subred IPv4 concreta.

```
client.ip.src.in_subnet(147.1.0.0/16)
<!--NeedCopy-->
```

A continuación se presentan dos ejemplos de directivas de reescritura que examinan la subred desde la que se recibe el paquete y realizan una acción de reescritura en el encabezado Host. Con estas dos directivas configuradas, la acción de reescritura que se realiza depende de la subred de la solicitud. Estas dos directivas evalúan las direcciones IP que tienen el formato de dirección IPv4.

```
- add rewrite action URL1-rewrite-action replace "http.req.header("Host
   ")" ""www.mycompany1.com""
- add rewrite policy URL1-rewrite-policy "http.req.header("Host").
   contains("www.test1.com") && client.ip.src.in_subnet(147.1.0.0/16)"
   URL1-rewrite-action
- add rewrite action URL2-rewrite-action replace "http.req.header("Host
   ")" ""www.mycompany2.com""
- add rewrite policy URL2-rewrite-policy "http.req.header("Host").
   contains("www.test2.com") && client.ip.src.in_subnet(10.202.0.0/16)"
    URL2-rewrite-action
<!--NeedCopy-->
```


> **Nota**
>
> Los ejemplos anteriores son comandos que escribe en la interfaz de línea de comandos (CLI) de Citrix ADC y, por lo tanto, cada comilla debe ir precedida de una barra diagonal inversa (\). Para obtener más información, consulte Configuración de expresiones de directivas avanzadas en una directiva. “

Prefijos para direcciones IPv4 y subredes IP

En la tabla siguiente se describen los prefijos que devuelven direcciones y subredes IPv4 y segmentos de direcciones IPv4. Puede utilizar operadores numéricos y operadores específicos de direcciones IPv4 con estos prefijos. Para obtener más información sobre las operaciones numéricas, consulte “Operaciones básicas con prefijos de expresión” y “Operaciones compuestas para números. “

Tabla 1. Prefijos que evalúan direcciones IP y MAC

Prefix	Descripción
CLIENT.IP.SRC	Devuelve la IP de origen del paquete actual como dirección IP o como número.
CLIENT.IP.DST	Devuelve la IP de destino del paquete actual como dirección IP o como número.
SERVER.IP.SRC	Devuelve la IP de origen del paquete actual como dirección IP o como número.
SERVER.IP.DST	Devuelve la IP de destino del paquete actual como dirección IP o como número.

Operaciones para direcciones IPv4

La tabla Prefijo para operaciones IPV4 describe los operadores que se pueden utilizar con prefijos que devuelven una dirección IPv4.

Acerca de las expresiones IPv6

El formato de dirección IPv6 ofrece más flexibilidad que el formato IPv4 anterior. Las direcciones IPv6 están en formato hexadecimal (RFC 2373). En los ejemplos siguientes, el ejemplo 1 es una dirección IPv6, el ejemplo 2 es una dirección URL que incluye la dirección IPv6 y el ejemplo 3 incluye la dirección IPv6 y un número de puerto.

Ejemplo 1:


```
9901:0ab1:22a2:88a3:3333:4a4b:5555:6666
<!--NeedCopy-->
```

Ejemplo 2:

```
http://[9901:0ab1:22a2:88a3:3333:4a4b:5555:6666]/
<!--NeedCopy-->
```

Ejemplo 3:

```
https://[9901:0ab1:22a2:88a3:3333:4a4b:5555:6666]:8080/
<!--NeedCopy-->
```

En el ejemplo 3, los corchetes separan la dirección IP del número de puerto (8080).

Tenga en cuenta que solo puede usar el operador '+' para combinar expresiones IPv6 con otras expresiones. El resultado es una concatenación de los valores de cadena devueltos por las expresiones individuales. No se puede utilizar ningún otro operador aritmético con una expresión IPv6. La sintaxis siguiente es un ejemplo:

```
client.ipv6.src + server.ip.dst
<!--NeedCopy-->
```

Por ejemplo, si la dirección IPv6 de origen del cliente es `ABCD:1234::ABCD`y la dirección IPv4 de destino del servidor es `10.100.10.100`, se devuelve la expresión anterior `"ABCD:1234::ABCD10.100.10.100"`.

Tenga en cuenta que cuando el dispositivo Citrix ADC recibe un paquete IPv6, asigna una dirección IPv4 temporal de un intervalo de direcciones IPv4 no utilizado y cambia la dirección de origen del paquete a esta dirección temporal. En el momento de respuesta, la dirección de origen del paquete saliente se sustituye por la dirección IPv6 original.

> **Nota**
>
> Puede combinar una expresión IPv6 con cualquier otra expresión, excepto una expresión que produce un resultado booleano.

Prefijos de expresión para direcciones IPv6

Las direcciones IPv6 devueltas por los prefijos de expresión de la tabla siguiente se pueden tratar como datos de texto. Por ejemplo, el prefijo client.ipv6.dst devuelve la dirección IPv6 de destino en forma de cadena que se puede evaluar como texto.

En la tabla siguiente se describen los prefijos de expresión que devuelven una dirección IPv6.

Tabla 3. Prefijos de expresión IPv6 que devuelven texto

Prefix	Descripción
CLIENT.IPV6	Funciona en la dirección IPv6 del paquete actual.
CLIENT.IPV6.DST	Devuelve la dirección IPv6 del campo de destino del encabezado IP.
CLIENT.IPV6.SRC	Devuelve la dirección IPv6 del campo de origen del encabezado IP. A continuación se presentan ejemplos: `client.ipv6.src.in_subnet(2007::2008/64)` `client.ipv6.src.get1.le(2008)`
SERVER.IPV6	Funciona en la dirección IPv6 del paquete actual.
SERVER.IPV6.DST	Devuelve la dirección IPv6 del campo de destino del encabezado IP.
SERVER.IPV6.SRC	Devuelve la dirección IPv6 del campo de origen del encabezado IP. A continuación se presentan ejemplos: `server.ipv6.src.in_subnet(2007::2008/64)` `server.ipv6.src.get1.le(2008)`

Operaciones para prefijos IPv6

En la tabla siguiente se describen los operadores que se pueden utilizar con prefijos que devuelven una dirección IPv6:

Tabla 4. Operaciones que evalúan direcciones IPv6

Funcionamiento IPv6	Descripción
<ipv6>.EQ(<IPv6_address>	Devuelve un valor booleano TRUE si el valor de la dirección IP es el mismo que el argumento <IPv6_address>. A continuación se muestra un ejemplo: client.ipv6.dst.eq(ABCD:1234::ABCD)
<ipv6>.GET1. . .GET8	Devuelve un segmento de una dirección IPv6 en forma de número. Las expresiones de ejemplo siguientes recuperan segmentos de la dirección ipv6 1000:1001:CD10:0000:0000:89AB:4567:CDEF: client.ipv6.dst.get5 extracts 0000, que es el quinto conjunto de bits de la dirección. client.ipv6.dst.get6 extracts 89AB. client.ipv6.dst.get7 extracts 4567. Puede realizar operaciones numéricas en estos segmentos. Tenga en cuenta que no puede realizar operaciones numéricas cuando recupera una dirección IPv6 completa. Esto se debe a que las expresiones que devuelven una dirección IPv6 completa, como CLIENT.IPV6.SRC, devuelven la dirección en formato de texto.
<ipv6>.IN_SUBNET(<subnet>)	Devuelve un valor booleano TRUE si el valor de la dirección IPv6 se encuentra en la subred especificada por el argumento <subnet>. A continuación se muestra un ejemplo: client.ipv6.dst.eq(1000:1001:CD10 :0000:0000:89AB:4567:CDEF/60)
<ipv6>.IS_IPV4	Devuelve un valor booleano TRUE si se trata de un cliente IPv4 y devuelve un valor booleano FALSE si no lo es.

Funcionamiento IPv6	Descripción
`<ipv6>.SUBNET(<n>)`	Devuelve la dirección IPv6 tras aplicar la máscara de subred especificada como argumento. La máscara de subred puede tomar valores entre 0 y 128. Por ejemplo: `CLIENT.IPV6.SRC.SUBNET(24)`

Expresiones para direcciones MAC

Una dirección MAC consta de valores hexadecimales delimitados por dos puntos en el formato ##:##:##:##:##:##, donde cada "#" representa un número del 0 al 9 o una letra de la A a la F. Los prefijos y operadores de expresión de directivas avanzadas están disponibles para evaluar las direcciones MAC de origen y destino.

Prefijos para direcciones MAC

En la tabla siguiente se describen los prefijos que devuelven direcciones MAC.

Tabla 5. Prefijos que evalúan direcciones MAC

Prefix	Descripción
`client.ether.dstmac`	Devuelve la dirección MAC en el campo de destino del encabezado Ethernet.
`client.ether.srcmac`	Devuelve la dirección MAC del campo de origen del encabezado Ethernet.

Operaciones para direcciones MAC

En la tabla siguiente se describen los operadores que se pueden utilizar con prefijos que devuelven una dirección MAC.

Tabla 6. Operaciones en direcciones MAC

Prefix	Descripción
`<mac address>.EQ(<address>)`	Devuelve un valor booleano TRUE si el valor de la dirección MAC es el mismo que el argumento `<address>`.

Prefix	Descripción
`<mac address>.GET1. . .GET4`	Devuelve un valor numérico extraído del segmento de la dirección MAC especificada en la operación GET. Por ejemplo, si la dirección MAC es 12:34:56:78:9 a:bc, lo siguiente devuelve 34: `client.ether.dstmac.get2`

Expresiones para datos numéricos de clientes y servidores

En la tabla siguiente se describen los prefijos para trabajar con datos numéricos de cliente y servidor, incluidos el rendimiento, los números de puerto y los ID de VLAN.

Tabla 7. Prefijos que evalúan datos numéricos de clientes y servidores

Prefix	**Descripción**
rendimiento client.interface.rx	Devuelve un entero que representa el rendimiento del tráfico recibido sin procesar en kilobytes por segundo (KBps) durante los siete segundos anteriores.
rendimiento client.interface.tx	Devuelve un entero que representa el rendimiento del tráfico transmitido sin procesar en KBps durante los siete segundos anteriores.
rendimiento client.interface.rxtx	Devuelve un entero que representa el rendimiento del tráfico recibido y transmitido sin procesar en KBps durante los siete segundos anteriores.
rendimiento server.interface.rx	Devuelve un entero que representa el rendimiento del tráfico recibido sin procesar en KBps durante los siete segundos anteriores.
rendimiento server.interface.tx	Devuelve un entero que representa el rendimiento del tráfico transmitido sin procesar en KBps durante los siete segundos anteriores.

Prefix	Descripción
rendimiento server.interface.rxtx	Devuelve un entero que representa el rendimiento del tráfico recibido y transmitido sin procesar en KBps durante los siete segundos anteriores.
server.vlan.id	Devuelve un ID numérico de la VLAN a través de la cual el paquete actual se introdujo en Citrix ADC.
client.vlan.id	Devuelve un ID numérico de la VLAN a través de la cual el paquete actual se introdujo en Citrix ADC.

Expresiones de directiva avanzadas: Funciones de análisis de flujo

January 12, 2021

Las expresiones de Stream Analytics comienzan con el <identifier_name> prefijo ANALYTICS.STREAM (). La siguiente lista describe las funciones que se pueden utilizar con este prefijo.

- **COLECT_STATS**

  Recopilar datos estadísticos de las solicitudes que se evalúan con arreglo a la directiva y crear un registro para cada solicitud.

- **SOLICITUDES**

  Devuelve el número de solicitudes que existen para la agrupación de registros especificada. El valor devuelto es de tipo unsigned long.

- **ANCHO DE BANDA**

  Devuelve la estadística de ancho de banda para la agrupación de registros especificada. El valor devuelto es de tipo unsigned long.

- **RESPTIME**

  Devuelve la estadística de tiempo de respuesta para la agrupación de registros especificada. El valor devuelto es de tipo unsigned long.

- **CONEXIONES**

  Devuelve el número de conexiones simultáneas que existen para la agrupación de registros especificada. El valor devuelto es de tipo unsigned long.

- **IS_TOP (n)**

  Devuelve un valor booleano TRUE si el valor estadístico de la agrupación de registros especificada es uno de los n primeros grupos. De lo contrario, devuelve un FALSE booleano.

- **CHECK_LIMIT**

  Devuelve un valor booleano TRUE si la estadística de la agrupación de registros especificada ha alcanzado el límite preconfigurado. De lo contrario, devuelve un FALSE booleano.

Expresiones de directiva avanzadas: DataStream

August 20, 2021

La infraestructura de directivas del dispositivo Citrix ADC incluye expresiones que puede utilizar para evaluar y procesar el tráfico del servidor de bases de datos cuando el dispositivo se implementa entre una comunidad de servidores de aplicaciones y sus servidores de base de datos asociados.

Este tema incluye las siguientes secciones:

- Expresiones para el protocolo MySQL
- Expresiones para evaluar conexiones de Microsoft SQL Server

Expresiones para el protocolo MySQL

Las siguientes expresiones evalúan el tráfico asociado con los servidores de bases de datos MySQL. Puede utilizar las expresiones basadas en solicitudes (expresiones que comienzan con MYSQL.CLIENT y MYSQL.REQ) en directivas para tomar decisiones de conmutación de solicitudes en el punto de enlace del servidor virtual de conmutación de contenido y las expresiones basadas en respuesta (expresiones que comienzan con MYSQL.RES) para evaluar las respuestas del servidor al usuario: Monitores de estado configurados.

- **MYSQL.CLIENT.** Funciona en las propiedades del cliente de una conexión MySQL.
- **MYSQL.CLIENT.CAPABILITIES.** Devuelve el conjunto de indicadores que el cliente ha establecido en el campo de capacidades del paquete de inicialización del protocolo de enlace durante la autenticación. Algunos ejemplos de los indicadores establecidos son CLIENT_FOUND_ROWS, CLIENT_COMPRESS y CLIENT_SSL.
- **MYSQL.CLIENT.CHAR_SET.** Devuelve la constante de enumeración asignada al juego de caracteres que utiliza el cliente. Los operadores EQ(<m>) y NE(<m>), que devuelven valores booleanos para indicar el resultado de una comparación, se utilizan con este prefijo. A continuación se presentan las constantes de enumeración del conjunto de caracteres:
  - LATIN2_CZECH_CS

- DEC8_SWEDISH_CI
- CP850_GENERAL_CI
- GREEK_GENERAL_CI
- LATIN1_GERMAN1_CI
- HP8_ENGLISH_CI
- KOI8R_GENERAL_CI
- LATIN1_SWEDISH_CI
- LATIN2_GENERAL_CI
- SWE7_SWEDISH_CI
- ASCII_GENERAL_CI
- CP1251_BULGARIAN_CI
- LATIN1_DANISH_CI
- HEBREO GENERAL_CI
- LATIN7_ESTONIAN_CS
- LATIN2_HUNGARIAN_CI
- KOI8U_GENERAL_CI
- CP1251_UKRAINIAN_CI
- CP1250_GENERAL_CI
- LATIN2_CROATIAN_CI
- CP1257_LITHUANIAN_CI
- LATIN5_TURKISH_CI
- LATIN1_GERMAN2_CI
- ARMSCII8_GENERAL_CI
- UTF8_GENERAL_CI
- CP1250_CZECH_CS
- CP866_GENERAL_CI
- KEYBCS2_GENERAL_CI
- MACCE_GENERAL_CI
- MACROMAN_GENERAL_CI
- CP852_GENERAL_CI
- LATIN7_GENERAL_CI
- LATIN7_GENERAL_CS
- MACCE_BIN
- CP1250_CROATIAN_CI
- LATIN1_BIN
- LATIN1_GENERAL_CI
- LATIN1_GENERAL_CS
- CP1251_BIN
- CP1251_GENERAL_CI

- CP1251_GENERAL_CS
- MACROMAN_BIN
- CP1256_GENERAL_CI
- CP1257_BIN
- CP1257_GENERAL_CI
- ARMSCII8_BIN
- ASCII_BIN
- CP1250_BIN
- CP1256_BIN
- CP866_BIN
- DEC8_BIN
- GREEK_BIN
- HEBREO
- HP8_BIN
- KEYBCS2_BIN
- KOI8R_BIN
- KOI8U_BIN
- LATIN2_BIN
- LATIN5_BIN
- LATIN7_BIN
- CP850_BIN
- CP852_BIN
- SWE7_BIN
- UTF8_BIN
- GEOSTD8_GENERAL_CI
- GEOSTD8_BIN
- LATIN1_SPANISH_CI
- UTF8_UNICODE_CI
- UTF8_ICELANDIC_CI
- UTF8_LATVIAN_CI
- UTF8_ROMANIAN_CI
- UTF8_SLOVENIAN_CI
- UTF8_POLISH_CI
- UTF8_ESTONIAN_CI
- UTF8_SPANISH_CI
- UTF8_SWEDISH_CI
- UTF8_TURKISH_CI
- UTF8_CZECH_CI
- UTF8_DANISH_CI

  - UTF8_LITHUANIAN_CI
  - UTF8_SLOVAK_CI
  - UTF8_SPANISH2_CI
  - UTF8_ROMAN_CI
  - UTF8_PERSIAN_CI
  - UTF8_ESPERANTO_CI
  - UTF8_HUNGARIAN_CI
  - CONJUNTO DE CARACTERES INVAL_CARACTERES

- **MYSQL.CLIENT.DATABASE.** Devuelve el nombre de la base de datos especificada en el paquete de autenticación que el cliente envía al servidor de base de datos. Este es el atributo databasename.
- MYSQL.CLIENT.USER. Devuelve el nombre de usuario (en el paquete de autenticación) con el que el cliente intenta conectarse a la base de datos. Este es el atributo de usuario.
- **MYSQL.REQ.** Funciona en una solicitud MySQL.
- **MYSQL.REQ.COMMAND.** Identifica la constante de enumeración asignada al tipo de comando en la solicitud. Los operadores EQ(<m>) y NE(<m>), que devuelven valores booleanos para indicar el resultado de una comparación, se utilizan con este prefijo. A continuación se presentan los valores constantes de enumeración:
  - SLEEP
  - QUIT
  - INIT_DB
  - QUERY
  - FIELD_LIST
  - CREATE_DB
  - DROP_DB
  - REFRESH
  - SHUTDOWN
  - STATISTICS
  - PROCESS_INFO
  - CONNECT
  - PROCESS_KILL
  - DEBUG
  - PING
  - HORA
  - DELAYED_INSERT
  - CHANGE_USER
  - BINLOG_DUMP
  - TABLE_DUMP

  - CONNECT_OUT
  - REGISTER_SLAVE
  - STMT_PREPARE
  - STMT_EXECUTE
  - STMT_SEND_LONG_DATA
  - STMT_CLOSE
  - STMT_RESTABLECER
  - SET_OPTION
  - STMT_FETCH

- **MYSQL.REQ.QUERY.** Identifica la consulta en la solicitud MySQL.
- **MYSQL.REQ.QUERY.COMMAND.** Devuelve la primera palabra clave en la consulta MySQL.
- **MYSQL.REQ.QUERY.TALLA.** Devuelve el tamaño de la consulta de solicitud en formato entero. El método SIZE es similar al método CONTENT_LENGTH que devuelve la longitud de una solicitud o respuesta HTTP.
- **MYSQL.REQ.QUERY.TEXT.** Devuelve una cadena que cubre toda la consulta.
- **MYSQL.REQ.QUERY.TEXT(<n>).** Devuelve los primeros n bytes de la consulta MySQL como una cadena. Esto es similar a HTTP.BODY (<n>).

  Parámetros:

  n: Número de bytes a devolver

- **MYSQL.RES.** Funciona en una respuesta MySQL.
- **MYSQL.RES.ATLEAST_ROWS_COUNT(<i>).** Comprueba si la respuesta tiene al menos i número de filas y devuelve un valor booleano VERDADERO o FALSE para indicar el resultado.

  Parámetros:

  i: Número de filas

- **MYSQL.RES.ERROR.** Identifica el objeto de error MySQL. El objeto de error incluye el número de error y el mensaje de error.
- **MYSQL.RES.ERROR.MESSAGE.** Devuelve el mensaje de error que se recupera de la respuesta de error del servidor.
- **MYSQL.RES.ERROR.NUM.** Devuelve el número de error que se recupera de la respuesta de error del servidor.
- **MYSQL.RES.ERROR.SQLSTATE.** Devuelve el valor del campo SQLSTATE en la respuesta de error del servidor. El servidor MySQL traduce valores de número de error a valores SQLSTATE.
- **MYSQL.RES.FIELD(<i>).** Identifica el paquete que corresponde al ith campo individual en la respuesta del servidor. Cada paquete de campo describe las propiedades de la columna asociada. El recuento de paquetes (i) comienza en 0.

Parámetros:

i: Número de paquete

- **MYSQL.RES.FIELD(<i>).CATALOG.** Devuelve la propiedad de catálogo del paquete de campo.
- **MYSQL.RES.FIELD(<i>).CHAR_SET.** Devuelve el conjunto de caracteres de la columna. Los operadores EQ(<m>) y NE(<m>), que devuelven valores booleanos para indicar el resultado de una comparación, se utilizan con este prefijo.
- **MYSQL.RES.FIELD(<i>).DATATYPE.** Devuelve una constante de enumeración que representa el tipo de datos de la columna. Este es el atributo type (también llamado enum_field_type) de la columna. Los operadores EQ(<m>) y NE(<m>), que devuelven valores booleanos para indicar el resultado de una comparación, se utilizan con este prefijo. Los valores posibles para los distintos tipos de datos son:
  - DECIMAL
  - TINY
  - SHORT
  - LONG
  - FLOAT
  - DOUBLE
  - NULL
  - TIMESTAMP
  - LONGLONG
  - INT24
  - FECHA
  - HORA
  - DATETIME
  - YEAR
  - NEWDATE
  - VARCHAR (nuevo en MySQL 5.0)
  - BIT (nuevo en MySQL 5.0)
  - NEWDECIMAL (nuevo en MySQL 5.0)
  - ENUMERACIÓN
  - SET
  - TINY_BLOB
  - MEDIUM_BLOB
  - LONG_BLOB
  - BLOB
  - VAR_STRING
  - STRING
  - GEOMETRY

- **MYSQL.RES.FIELD(<i>).DB.** Devuelve el atributo identificador de base de datos (db) del paquete de campo.
- **MYSQL.RES.FIELD(<i>).DECIMALS.** Devuelve el número de posiciones después del punto decimal si el tipo es DECIMAL o NUMERIC. Este es el atributo decimales del paquete de campo.
- **MYSQL.RES.FIELD(<i>).FLAGS.** Devuelve la propiedad flags del paquete de campo. A continuación se presentan los posibles valores de indicador hexadecimal:
  - 0001: NOT_NULL_FLAG
  - 0002: PRI_KEY_FLAG
  - 0004: UNIQUE_KEY_FLAG
  - 0008: MULTIPLE_KEY_FLAG
  - 0010: BLOB_FLAG
  - 0020: UNSIGNED_FLAG
  - 0040: ZEROFILL_FLAG
  - 0080: BINARY_FLAG
  - 0100: ENUM_FLAG
  - 0200: AUTO_INCREMENT_FLAG
  - 0400: TIMESTAMP_FLAG
  - 0800: SET_FLAG
- **MYSQL.RES.FIELD(<i>).LENGTH.** Devuelve la longitud de la columna. Este es el valor del atributo length del paquete de campo. El valor devuelto puede ser mayor que el valor real. Por ejemplo, una instancia de una columna VARCHAR (2) podría devolver un valor de 2 incluso cuando contenga un solo carácter.
- **MYSQL.RES.FIELD(<i>).NAME.** Devuelve el identificador de columna (el nombre después de la cláusula AS, si existe). Este es el atributo name del paquete de campo.
- **MYSQL.RES.FIELD(<i>).ORIGINAL_NAME.** Devuelve el identificador de columna original (antes de la cláusula AS, si existe). Este es el atributo org_name del paquete de campo.
- **MYSQL.RES.FIELD(<i>).ORIGINAL_TABLE.** Devuelve el identificador de tabla original de la columna (antes de la cláusula AS, si existe). Este es el atributo org_table del paquete de campo.
- **MYSQL.RES.FIELD(<i>).TABLE.** Devuelve el identificador de tabla de la columna (después de la cláusula AS, si existe). Este es el atributo de tabla del paquete de campo.
- **MYSQL.RES.FIELDS_COUNT.** Devuelve el número de paquetes de campo en la respuesta (el atributo field_count del paquete OK).
- **MYSQL.RES.OK.** Identifica el paquete OK enviado por el servidor de base de datos.
- **MYSQL.RES.OK.AFFECTED_ROWS.** Devuelve el número de filas afectadas por una consulta INSERT, UPDATE o DELETE. Este es el valor del atributo affected_rows del paquete OK.

- **MYSQL.RES.OK.INSERT_ID.** Identifica el atributo unique_id del paquete OK. Si la instrucción o consulta de MySQL actual no genera una identidad de incremento automático, el valor de unique_id, y por lo tanto el valor devuelto por la expresión, es 0.
- **MYSQL.RES.OK.MESSAGE.** Devuelve la propiedad message del paquete OK.
- **MYSQL.RES.OK.STATUS.** Identifica la cadena de bits en el atributo server_status del paquete OK. Los clientes pueden utilizar el estado del servidor para comprobar si el comando actual forma parte de una transacción en ejecución. Los bits de la cadena de bits server_status corresponden a los siguientes campos (en el orden dado):
  - IN TRANSACTION
  - AUTO_COMMIT
  - MORE RESULTS
  - MULTI QUERY
  - BAD INDEX USED
  - NO INDEX USED
  - CURSOR EXISTS
  - LAST ROW SEEN
  - DATABASE DROPPED
  - NO BACKSLASH ESCAPES
- **MYSQL.RES.OK.WARNING_COUNT.** Devuelve el atributo warning_count del paquete OK.
- **MYSQL.RES.ROW(<i>).** Identifica el paquete que corresponde al ith fila individual de la respuesta del servidor de base de datos.

  Parámetros:

  i: Número de fila
- **MYSQL.RES.ROW(<i>).DOUBLE_ELEM(<j>).** Comprueba si el jth columna de la i^a fila de la tabla es NULL. Siguiendo las convenciones C, ambos índices i y j comienzan desde 0. Por lo tanto, la fila i y la columna j son en realidad el (i+1)th fila y el (j+1)th columna, respectivamente.

  Parámetros:

  i: Número de fila

  j: Número de columna
- **MYSQL.RES.ROW(<i>).IS_NULL_ELEM(j).** Comprueba si el jth columna de la i^a fila de la tabla es NULL. Siguiendo las convenciones C, ambos índices i y j comienzan desde 0. Por lo tanto, la fila i y la columna j son en realidad el (i+1)th fila y el (j+1)th columna, respectivamente.

  Parámetros:

i: Número de fila

j: Número de columna

- **MYSQL.RES.ROW(<i>).NUM_ELEM(<j>).** Devuelve un valor entero de la jth columna de la i^[a] fila de la mesa. Siguiendo las convenciones C, ambos índices i y j comienzan desde 0. Por lo tanto, la fila i y la columna j son en realidad el (i+1)th fila y el (j+1)th columna, respectivamente.

  Parámetros:

  i: Número de fila

  j: Número de columna

- **MYSQL.RES.ROW(<i>).TEXT_ELEM(j).** Devuelve una cadena de la jth columna de la i^[a] fila de la mesa. Siguiendo las convenciones C, ambos índices i y j comienzan desde 0. Por lo tanto, la fila i y la columna j son en realidad el (i+1)th fila y el (j+1)th columna, respectivamente.

  Parámetros:

  i: Número de fila

  j: Número de columna

- **MYSQL.RES.TIPO.** Devuelve una constante de enumeración para el tipo de respuesta. Sus valores pueden ser ERROR, OK y RESULT_SET. Los operadores EQ(<m>) y NE(<m>), que devuelven valores booleanos para indicar el resultado de una comparación, se utilizan con este prefijo.

Expresiones para evaluar conexiones de Microsoft SQL Server

Las siguientes expresiones evalúan el tráfico asociado con los servidores de base de datos de Microsoft SQL Server. Puede utilizar las expresiones basadas en solicitudes (expresiones que comienzan con MSSQL.CLIENT y MSSQL.REQ) en directivas para tomar decisiones de conmutación de solicitudes en el punto de enlace del servidor virtual de conmutación de contenido y las expresiones basadas en respuesta (expresiones que comienzan con MSSQL.RES) para evaluar las respuestas del servidor al usuario: Monitores de estado configurados.

Expresión	Descripción
MSSQL.CLIENT.CAPABILITIES	Devuelve los campos OptionFlags1, OptionFlags2, OptionFlags3 y TypeFlags del paquete Login7Authentication, en ese orden, como un entero de 4 bytes. Cada campo tiene una longitud de 1 byte y especifica un conjunto de capacidades del cliente.

Expresión	Descripción
MSSQL.CLIENT.DATABASE	Devuelve el nombre de la base de datos cliente. El valor devuelto es de tipo text.
MSSQL.CLIENT.USER	Devuelve el nombre de usuario con el que se autenticó el cliente. El valor devuelto es de tipo text.
MSSQL.REQ.COMMAND	Devuelve una constante de enumeración que identifica el tipo de comando de la solicitud enviada a un servidor de base de datos de Microsoft SQL Server. El valor devuelto es de tipo text. Ejemplos de los valores de la constante de enumeración son QUERY, RESPONSE, RPC y ATENCIÓN. Los operadores EQ(<m>) y NE(<m>), que devuelven valores booleanos para indicar el resultado de una comparación, se utilizan con esta expresión.
MSSQL.REQ.QUERY.COMMAND	Devuelve la primera palabra clave de la consulta SQL. El valor devuelto es de tipo text.
MSSQL.REQ.QUERY.SIZE	Devuelve el tamaño de la consulta SQL en la solicitud. El valor devuelto es un número.
MSSQL.REQ.QUERY.TEXT	Devuelve toda la consulta SQL como una cadena. El valor devuelto es de tipo text.
MSSQL.REQ.QUERY.TEXT(<n>)	Devuelve los primeros n bytes de la consulta SQL. El valor devuelto es de tipo text. Parámetros: N: Número de bytes
MSSQL.REQ.RPC.NAME	Devuelve el nombre del procedimiento al que se llama en una solicitud de llamada a procedimiento remoto (RPC). El nombre se devuelve como una cadena.
MSSQL.REQ.RPC.IS_PROCID	Devuelve un valor Boolean que indica si la solicitud de llamada a procedimiento remoto (RPC) contiene un identificador de procedimiento o un nombre RPC. Un valor devuelto de trueIndica que la solicitud contiene un identificador de procedimiento y un valor devuelto de FALSE indica que la solicitud contiene un nombre RPC.

Expresión	Descripción
MSSQL.REQ.RPC.PROCID	Devuelve el identificador de procedimiento de la solicitud de llamada a procedimiento remoto (RPC) como un entero.
MSSQL.REQ.RPC.BODY **Nota:** No disponible para versiones anteriores a la 10.1.	Devuelve el cuerpo de la solicitud SQL como una cadena en forma de parámetros representados como cláusulas “a=b” separadas por comas, donde “a” es el nombre del parámetro RPC y “b” es su valor.
MSSQL.REQ.RPC.BODY (n) **Nota:** No disponible para versiones anteriores a la 10.1.	Devuelve parte del cuerpo de la solicitud SQL como una cadena en forma de parámetros representados como cláusulas “a=b” separadas por comas, donde “a” es el nombre del parámetro RPC y “b” es su valor. Los parámetros se devuelven solo desde los primeros “n” bytes de la solicitud, omitiendo el encabezado SQL. Solo se devuelven pares nombre-valor completos.
MSSQL.RES.ATLEAST_ROWS_COUNT (i)	Comprueba si la respuesta tiene al menos i número de filas. El valor devuelto es un valor booleano VERDADERO o FalseValue. Parámetros: I: Número de filas
MSSQL.RES.DONE.ROWCOUNT	Devuelve un recuento del número de filas afectadas por una consulta INSERT, UPDATE o DELETE. El valor devuelto es de tipo unsigned long.
MSSQL.RES.DONE.STATUS	Devuelve el campo de estado del token DONE enviado por un servidor de base de datos de Microsoft SQL Server. El valor devuelto es un número.
MSSQL.RES.ERROR.MESSAGE	Devuelve el mensaje de error del token ERROR enviado por un servidor de base de datos de Microsoft SQL Server. Este es el valor del campo MsgText en el token ERROR. El valor devuelto es de tipo text.

Expresión	Descripción
MSSQL.RES.ERROR.NUM	Devuelve el número de error del token ERROR enviado por un servidor de base de datos de Microsoft SQL Server. Este es el valor del campo Número en el token ERROR. El valor devuelto es un número.
MSSQL.RES.ERROR.STATE	Devuelve el estado de error del token ERROR enviado por un servidor de base de datos de Microsoft SQL Server. Este es el valor del campo Estado en el token ERROR. El valor devuelto es un número.
MSSQL.RES.FIELD (<i>) .TIPO DE DATOS	Devuelve el tipo de datos del campo ith en la respuesta del servidor. Las operadores EQ(<m>) y NE(<m>), que devuelven valores booleanos para indicar el resultado de una comparación, se utilizan con este prefijo. Por ejemplo, la siguiente expresión devuelve un valor booleano TRUE si la función DATATYPE devuelve un valor de fecha y hora para el tercer campo de la respuesta: MSSQL.RES.FIELD (<2>).DATATYPE.EQ (datetime) Parámetros: I: Número de fila
MSSQL.RES.FIELD (<i>) .LONGITUD	Devuelve la longitud máxima posible del campo ith en la respuesta del servidor. El valor devuelto es un número. Parámetros: I: Número de fila
MSSQL.RES.FIELD (<i>) .NOMBRE	Devuelve el nombre del campo ith en la respuesta del servidor. El valor devuelto es de tipo text. Parámetros: I: Número de fila

Expresión	Descripción
MSSQL.RES.ROW (<i>) .DOUBLE_ELEMM (<j>)	Devuelve un valor de tipo double de la columna jth de la primera fila de la tabla. Si el valor no es un valor doble, se genera una condición UNDEF. Siguiendo las convenciones C, ambos índices i y j comienzan desde 0 (cero). Por lo tanto, la fila i y la columna j son en realidad la (i + 1) ª fila y la (j + 1) ª columna, respectivamente. Parámetros: I: Número de fila j: Número de columna
MSSQL.RES.ROW (<i>) .NUM_ELEM (j)	Devuelve un valor entero de la columna jth de la fila ith de la tabla. Si el valor no es un valor entero, se genera una condición UNDEF. Siguiendo las convenciones C, ambos índices i y j comienzan desde 0 (cero). Por lo tanto, la fila i y la columna j son en realidad la (i + 1) ª fila y la (j + 1) ª columna, respectivamente. Parámetros: I: Número de fila j: Número de columna
MSSQL.RES.ROW (<i>) .IS_NULL_ELEMM (j)	Comprueba si la columna jth de la ith fila de la tabla es NULL y devuelve un valor booleano TRUE o FALSE para indicar el resultado. Siguiendo las convenciones C, ambos índices i y j comienzan desde 0 (cero). Por lo tanto, la fila i y la columna j son en realidad la (i + 1) ª fila y la (j + 1) ª columna, respectivamente. Parámetros: I: Número de fila j: Número de columna
MSSQL.RES.ROW (<i>) .TEXT_ELEM (j)	Devuelve una cadena de texto de la columna jth de la primera fila de la tabla. Siguiendo las convenciones C, ambos índices i y j comienzan desde 0 (cero). Por lo tanto, la fila i y la columna j son en realidad la (i + 1) ª fila y la (j + 1) ª columna, respectivamente. Parámetros: I: Número de fila j: Número de columna

Expresión	Descripción
MSSQL.RES.TYPE	Devuelve una constante de enumeración que identifica el tipo de respuesta. Los siguientes son los posibles valores devueltos: ERROR, OK y RESULT_SET. Los operadores EQ(<m>) y NE(<m>), que devuelven valores booleanos para indicar el resultado de una comparación, se utilizan con esta expresión.

Datos de conversión de tipos

August 20, 2021

Puede extraer datos de un tipo (por ejemplo, texto o un entero) de solicitudes y respuestas y transformarlos en datos de otro tipo. Por ejemplo, puede extraer una cadena y transformar la cadena en formato de tiempo. También puede extraer una cadena de un cuerpo de solicitud HTTP y tratarla como un encabezado HTTP o extraer un valor de un tipo de encabezado de solicitud e insertarlo en un encabezado de respuesta de un tipo diferente.

Después de convertir el tipo de datos, puede aplicar cualquier operación que sea apropiada para el nuevo tipo de datos. Por ejemplo, si convierte el texto en un encabezado HTTP, puede aplicar cualquier operación que sea aplicable a encabezados HTTP al valor devuelto.

Para obtener más información sobre los datos de fundición por tipos, consulte el pdf Operaciones de fundición por tipografía .

Expresiones regulares

October 5, 2021

Cuando quiere realizar operaciones de coincidencia de cadenas más complejas que las operaciones que realiza con los operadores CONTAINS(”<string>”) o EQ(”<string>”), utiliza expresiones regulares. La infraestructura de directivas del dispositivo Citrix® Citrix ADC® incluye operadores a los que se pueden pasar expresiones regulares como argumentos para la coincidencia de texto. Los nombres de los operadores que trabajan con expresiones regulares incluyen la cadena REGEX. Las expresiones regulares que se pasan como argumentos deben ajustarse a la sintaxis de expresiones regulares que se describe en ”<http://www.pcre.org/pcre.txt>.” Puede obtener más información sobre las

expresiones regulares en "<http://www.regular-expressions.info/quickstart.html>" y en "<http://www.silverstones.com/thebat/Regex.html>."

El texto de destino de un operador que funciona con expresiones regulares puede ser texto o el valor de un encabezado HTTP. A continuación se muestra el formato de una expresión de directiva avanzada que utiliza un operador de expresión regular para operar con texto:

```
<text>.<regex_operator>(re<delimiter><regex_pattern><delimiter>)
```

La cadena <text> representa el prefijo de expresión de directiva avanzada que identifica una cadena de texto de un paquete (por ejemplo, HTTP.REQ.URL). La cadena <regex_operator> representa el operador de expresión regular. La expresión regular siempre comienza con la cadena re. Un par de delimitadores coincidentes, representados por <delimiter>, encierran la cadena <regex_pattern>, que representa la expresión regular.

La siguiente expresión de ejemplo comprueba si la URL de un paquete HTTP contiene la cadena *.jpeg (donde * es un comodín) y devuelve un valor booleano TRUE o FALSE para indicar el resultado. La expresión regular está encerrada entre un par de barras diagonal (/), que actúan como delimitadores.

```
http.req.url.regex_match(re/.<asterisk>\.jpeg/)
```

Los operadores de expresiones regulares se pueden combinar para definir o refinar el alcance de una búsqueda. Por ejemplo, <text>.AFTER_REGEX(reregex_pattern1).BEFORE_REGEX(reregex_pattern2) especifica que el objetivo de la coincidencia de cadenas es el texto entre los patrones regex_pattern1 y regex_pattern2. Puede utilizar un operador de texto en el ámbito definido por los operadores de expresiones regulares. Por ejemplo, puede utilizar el operador CONTAINS("<string>") para comprobar si el ámbito definido contiene la cadena abc:

```
<text>.AFTER_REGEX(re/regex_pattern1).BEFORE_REGEX(re/regex_pattern2/).
CONTAINS("abc")
```

> **Nota**
>
> El proceso de evaluación de una expresión regular lleva intrínsecamente más tiempo que el de un operador como CONTAINS("<string>") o EQ("<string>"), que funcionan con argumentos de cadena simples. Debe usar expresiones regulares solo si su requisito está fuera del alcance de otros operadores.

Funciones básicas de las expresiones regulares

January 12, 2021

A continuación se presentan funciones notables de las expresiones regulares definidas en el dispositivo Citrix ADC:

- Una expresión regular siempre comienza con la cadena “re” seguida de un par de caracteres delimitadores (llamados delimitadores) que encierran la expresión regular que quiere utilizar.

Por ejemplo, re# <regex_pattern> # utiliza el signo numérico (#) como delimitador.

- Una expresión regular no puede superar los 1499 caracteres.
- La coincidencia de dígitos se puede hacer mediante la cadena d (una barra invertida seguida de d).
- El espacio en blanco se puede representar mediante s (una barra invertida seguida de s).
- Una expresión regular puede contener espacios en blanco.

A continuación se presentan las diferencias entre la sintaxis de Citrix ADC y la sintaxis PCRE:

- Citrix ADC no permite referencias anteriores en expresiones regulares.
- No debe usar expresiones regulares recursivas.
- El meta-carácter de punto también coincide con el carácter de nueva línea.
- Unicode no es compatible.
- La operación SET_TEXT_MODE (IGNORECASE) anula el (?i) opción interna en la expresión regular.

Operaciones para expresiones regulares

October 5, 2021

En la tabla siguiente se describen los operadores que funcionan con expresiones regulares. La operación realizada por un operador de expresión regular en una expresión de directiva avanzada determinada depende de si el prefijo de expresión identifica encabezados de texto o HTTP. Las operaciones que evalúan encabezados anulan cualquier operación basada en texto para todas las instancias del tipo de encabezado especificado. Cuando utilice un operador, <text>sustitúyalo por el prefijo de expresión de directiva avanzada que quiera configurar para identificar texto.

Operación de expresión regular	Descripción
<text>.BEFORE_REGEX (<regular expression>)	Selecciona el texto que precede a la cadena que coincide con el <regular expression>argumento. Si la expresión regular no coincide con ningún dato del destino, la expresión devuelve un objeto de texto de longitud 0. La siguiente expresión selecciona la cadena “text” de “text/plain”. http.res.header (“content-type”) .before_regex (re#/#)

Operación de expresión regular	Descripción
<text>.AFTER_REGEX (<regular expression>)	Selecciona el texto que sigue a la cadena que coincide con el <regular expression>argumento. Si la expresión regular no coincide con ningún texto del destino, la expresión devuelve un objeto de texto de longitud 0. La siguiente expresión extrae “Example” de “MyExample”: http.req.header (“etag”) .after_regex (re/my/)
<text>.REGEX_SELECT (<regular expression>)	Selecciona una cadena que coincide con el <regular expression>argumento. Si la expresión regular no coincide con el objetivo, se devuelve un objeto de texto de longitud 0. El siguiente ejemplo extrae la cadena “NS-CACHE-9.0:90” de un encabezado Via: http.req.header (“via”) .regex_select (re! NS-CACHE-\ d.\ d:\ s*\ d {1,3}!)

Operación de expresión regular	Descripción
<text>.REGEX_MATCH (<regular expression>)	Devuelve TRUE si el objetivo <regular expression>coincide con un argumento de hasta 1499 caracteres. La expresión regular debe tener el siguiente formato: re <delimiter>expresión regular< delimiter> Ambos delimitadores deben ser iguales. Además, la expresión regular debe ajustarse a la sintaxis de la biblioteca de expresiones regulares compatible con Perl (PCRE). Para obtener más información, vaya a http://www.pcre.org/pcre.txt. En particular, consulte la página de manual pcrepattern. Sin embargo, tenga en cuenta lo siguiente: No se permiten referencias anteriores. No se recomiendan las expresiones regulares recursivas. El metacarácter de punto también coincide con el carácter de nueva línea. El juego de caracteres Unicode no es compatible. SET_TEXT_MODE (IGNORECASE) anula el (? i) opción interna especificada en la expresión regular. Los siguientes son ejemplos: http.req.hostname.regex_match (re/[[:alpha:]] + (abc) {2,3}/) y http.req.url.set_text_mode (codificado por urlencoded) .regex_match (re# (a b+c) #) El siguiente ejemplo coincide con ab y ab: http.req.url.regex_match (a*b*+c) #) El siguiente ejemplo coincide con ab y aB: http.req.url.regex_match (re/) _match (req.match (req.match (req.match (req. i) b/) El siguiente ejemplo coincide con ab, aB, Ab y AB: http.req.url.set_text_mode (ignorecase) .regex_match (re/ab/) El siguiente ejemplo realiza una coincidencia multilínea sin distinción de mayúsculas y minúsculas en la que el metacarácter de punto también coincide con un carácter de nueva línea: http.req.body.regex_match (re/ (? ixm) (^ab (.*) cd$)/)

Operación de expresión regular	Descripción

Ejemplos resumidos de directivas y expresiones de directivas avanzadas

October 5, 2021

En la tabla siguiente se proporcionan ejemplos de expresiones de directivas avanzadas que puede utilizar como base para sus propias expresiones de directiva avanzadas.

Tabla 1. Ejemplos de expresiones de directivas avanzadas

Tipo de expresión	Expresiones de ejemplo
Observe el método utilizado en la solicitud HTTP.	`http.req.method.eq(post)http.req.method.eq(get)`

Compruebe el valor del encabezado Cache-Control o Pragma en una solicitud HTTP (req) o respuesta (res).	`http.req.header("Cache-Control").contains("no-store")`
	`http.req.header("Cache-Control").contains("no-cache")`
	`http.req.header("Pragma").contains("no-cache")`
	`http.res.header("Cache-Control").contains("private")`
	`http.res.header("Cache-Control").contains("public")`
	`http.res.header("Cache-Control").contains("must-revalidate")http.res.header("Cache-Control").contains ("proxy-revalidate")`
	`http.res.header("Cache-Control").contains("max-age")`

Compruebe la presencia de un encabezado en una solicitud (req) o respuesta (res).	`http.req.header("myHeader").exists` `http.res.header("myHeader").exists`

Tipo de expresión	Expresiones de ejemplo
Busque un tipo de archivo concreto en una solicitud HTTP basada en la extensión del archivo.	`http.req.url.contains(".html")http.req.url.contains(".cgi")http.req.url.contains(".asp")http.req.url.contains(".exe")http.req.url.contains(".cfm")http.req.url.contains(".ex")http.req.url.contains(".shtml")http.req.url.contains(".htx")http.req.url.contains("/cgi-bin/")http.req.url.contains("/exec/")http.req.url.contains("/bin/")`
Busque cualquier cosa que no sea un tipo de archivo concreto en una solicitud HTTP.	`http.req.url.contains(".png").not; http.req.url.contains(".jpeg").not`
Compruebe el tipo de archivo que se envía en una respuesta HTTP según el encabezado Content-Type.	`http.res.header("Content-Type").contains("text")http.res.header("Content-Type").contains "application/msword")http.res.header("Content-Type").contains("vnd.ms-excel")http.res.header("Content-Type").contains("application/vnd.ms-powerpoint"); http.res.header("Content-Type").contains("text/css"); http.res.header("Content-Type").contains("text/xml"); http.res.header("Content-Type").contains("image/")`
Compruebe si esta respuesta contiene un encabezado de caducidad.	`http.res.header("Expires").exists`
Compruebe si hay un encabezado Set-Cookie en una respuesta.	`http.res.header("Set-Cookie").exists`
Compruebe el agente que envió la respuesta.	`http.res.header("User-Agent").contains("Mozilla/4.7")http.res.header("User-Agent").contains("MSIE")`

Tipo de expresión	Expresiones de ejemplo
Compruebe si los primeros 1024 bytes del cuerpo de una solicitud comienzan con la cadena “algún texto”.	`http.req.body(1024).contains(”some text”)`

En la tabla siguiente se muestran ejemplos de configuraciones de directivas y enlaces para funciones de uso común.

Cuadro 2. Ejemplos de directivas avanzadas, expresiones y directivas

Propósito	Ejemplo
Utilice la función de reescritura para reemplazar las apariciones de `http://with https://` en el cuerpo de una respuesta HTTP.	`add rewrite action httpRewriteAction replace_all http.res.body(50000)”\”https://\””-search http://add rewrite policy demo_rep34312 ”http.res.body(50000).contains(\”http://\”)” httpRewriteAction`
Reemplace todas las apariciones de “abcd” por “1234” en los primeros 1000 bytes del cuerpo HTTP.	`add rewrite action abcdTo1234Action replace_all ”http.req.body(1000)”” \”1234\””-search abcd add rewrite policy abcdTo1234Policy ”http.req.body(1000).contains(\”abcd\”)” abcdTo1234Action bind rewrite global abcdTo1234Policy 100 END -type REQ_OVERRIDE`
Rebaja la versión HTTP a 1.0 para evitar que el servidor separe las respuestas HTTP.	`add rewrite action downgradeTo1.0Action replace http.req.version.minor ”\”0\””add rewrite policy downgradeTo1.0Policy ”http.req.version.minor.eq(1)”downgradeTo1.0Action bind lb vserver myLBVserver -policyName downgradeTo1.0Policy -priority 100 -gotoPriorityExpression NEXT -type REQUEST`

Propósito	Ejemplo
Elimine las referencias al protocolo HTTP o HTTPS en todas las respuestas, de modo que si la conexión del usuario es HTTP, el enlace se abra mediante HTTP y, si la conexión del usuario es HTTPS, el enlace se abra mediante HTTPS.	`add rewrite action remove_http_https replace_all "http.res.body(1000000).set_text_mode(ignorecase)""\"//\""-search "re~https?://|HTTPS?://~"add rewrite policy remove_http_https true remove_http_https bind lb vserver test_vsvr -policyName remove_http_https -priority 20 -gotoPriorityExpression NEXT -type RESPONSE`
Reescribe instancias de http: a https: en todas las URL.	`add responder action httpToHttpsAction redirect "\"https://\" + http.req.hostname + http.req.url"add responder policy httpToHttpsPolicy "!CLIENT.SSL.IS_SSL"httpToHttpsAction bind responder global httpToHttpsPolicy 1 END -type OVERRIDE`
Modifique una URL para redirigir de la URL A a la URL B. En este ejemplo, se anexa “file5.html” a la ruta de acceso.	`add responder action appendFile5Action redirect \"http://\" + http.req.hostname + http.req.url + \"/file5.html\""add responder policy appendFile5Policy "http.req.url.eq(\"/testsite\")" appendFile5Action bind responder global appendFile5Policy 1 END -type OVERRIDE`

Propósito	Ejemplo
Redirige una URL externa a una URL interna.	`add rewrite action act_external_to_internal REPLACE 'http.req.hostname.server''”www.my.host.com”'add rewrite policy pol_external_to_internal 'http.req.hostname.server.eq(”www.external.host.com”)'act_external_to_internal bind rewrite global pol_external_to_internal 100 END -type REQ_OVERRIDE`
Redirigir las solicitudes a www.example.com que tengan una cadena de consulta a www.webn.example.com. El valor n se deriva de un parámetro de servidor de la cadena de consulta, por ejemplo, server=5.	`add rewrite action act_redirect_query REPLACE q##http.req.header(”Host”).before_str(”.example.com”)''”Web”+ http.req.url.query.value(”server”)## add rewrite policy pol_redirect_query q##http.req.header(”Host”).eq(”www.example.com”)&& http.req.url.contains(”?”)'act_redirect_query##`
Limita el número de solicitudes por segundo de una URL.	`add ns limitSelector ip_limit_selector http.req.url ”client.ip.src”add ns limitIdentifier ip_limit_identifier -threshold 4 -timeSlice 3600 -mode request_rate -limitType smooth -selectorName ip_limit_selector add responder action my_Web_site_redirect_action redirect ”\”http://www.mycompany.com/\””add responder policy ip_limit_responder_policy ”http.req.url.contains(\”myasp.asp\”)&& sys.check_limit (\”ip_limit_identifier\”)”my_Web_site_redirect_action bind responder global ip_limit_responder_policy 100 END -type default`

Propósito	Ejemplo
Compruebe la dirección IP del cliente pero pase la solicitud sin modificar la solicitud.	`add rewrite policy check_client_ip_policy 'HTTP.REQ.HEADER ("x-forwarded-for").EXISTS HTTP.REQ.HEADER ("client-ip").EXISTS'NOREWRITE bind rewrite global check_client_ip_policy 100 END`
Elimina los encabezados antiguos de una solicitud e inserta un encabezado NS-Client.	`add rewrite action del_x_forwarded_for delete_http_header x-forwarded-for add rewrite action del_client_ip delete_http_header client-ip add rewrite policy check_x_forwarded_for_policy 'HTTP.REQ.HEADER("x-forwarded-for").EXISTS'del_x_forwarded_for add rewrite policy check_client_ip_policy 'HTTP.REQ.HEADER("client-ip").EXISTS' del_client_ip add rewrite action insert_ns_client_header insert_http_header NS-Client 'CLIENT.IP.SRC'add rewrite policy insert_ns_client_policy 'HTTP.REQ.HEADER("x-forwarded-for").EXISTS HTTP.REQ.HEADER("client-ip").EXISTS 'insert_ns_client_header bind rewrite global check_x_forwarded_for_policy 100 200 bind rewrite global check_client_ip_policy 200 300 bind rewrite global insert_ns_client_policy 300 END`

Propósito	Ejemplo
Quite los encabezados antiguos de una solicitud, inserte un encabezado NS-Client y, a continuación, modifique la acción “insertar encabezado” para que el valor del encabezado insertado contenga los valores IP del cliente de los encabezados antiguos y la dirección IP de conexión del dispositivo Citrix ADC. Tenga en cuenta que este ejemplo repite el ejemplo anterior, con la excepción de la acción de reescritura final del conjunto.	‘add rewrite action del_x_forwarded_for delete_http_header x-forwarded-for add rewrite action del_client_ip delete_http_header client-ip add rewrite policy check_x_forwarded_for_policy ‘HTTP.REQ.HEADER(“x-forwarded-for”).EXISTS’ del_x_forwarded_for add rewrite policy check_client_ip_policy ‘HTTP.REQ.HEADER(“client-ip”).EXISTS’ del_client_ip add rewrite action insert_ns_client_header insert_http_header NS-Client ‘CLIENT.IP.SRC’ add rewrite policy insert_ns_client_policy ‘HTTP.REQ.HEADER(“x-forwarded-for”).EXISTS HTTP.REQ.HEADER(“client-ip”).EXISTS’ insert_ns_client_header bind rewrite global check_x_forwarded_for_policy 100 200 bind rewrite global check_client_ip_policy 200 300 bind rewrite global insert_ns_client_policy 300 END set rewrite action insert_ns_client_header -stringBuilderExpr ‘HTTP.REQ.HEADER(“x-forwarded-for”).VALUE(0) + “ “ + HTTP.REQ.HEADER(“client-ip”).VALUE(0) + “ “ + CLIENT.IP.SRC’

Ejemplos de tutoriales de directivas avanzadas para reescritura

October 5, 2021

Con la función de reescritura, puede modificar cualquier parte de un encabezado HTTP y, para las respuestas, puede modificar el cuerpo HTTP. Puede utilizar esta función para llevar a cabo varias tareas útiles, como eliminar encabezados HTTP innecesarios, enmascarar URL internas, redirigir páginas web y redirigir consultas o palabras clave.

En los ejemplos siguientes, primero debe crear una acción de reescritura y una directiva de reescritura. A continuación, vincula la directiva globalmente.

Este documento incluye los siguientes detalles:

- Redirigir una URL externa a una URL interna
- Redirección de una consulta
- Reescribir HTTP a HTTPS
- Eliminación de encabezados no deseados
- Reducción de redireccionamientos de servidores web
- Enmascarar el encabezado del servidor
- Conversión de texto sin formato en cadena codificada en URL y de la forma opuesta

Para obtener más información sobre los comandos y las descripciones de sintaxis, consulte la página Reescritura de Referencia de Comandos .

Redirigir una URL externa a una URL interna

En este ejemplo se describe cómo crear una acción de reescritura y una directiva de reescritura que redirige una URL externa a una URL interna. Se crea una acción, denominada act_external_to_internal, que realiza la reescritura. A continuación, crea una directiva llamada pol_external_to_internal.

Para redirigir una URL externa a una URL interna mediante la CLI

- Para crear la acción de reescritura, en el símbolo del sistema, escriba:

```
add rewrite action act_external_to_internal REPLACE “http.req.hostname.
server” “\” host_name_of_internal_Web_server\” ”
```

- Para crear la directiva de reescritura, en el símbolo del sistema de Citrix ADC, escriba:

```
add rewrite policy pol_external_to_internal ”http.req.hostname.server.eq(\”
host_name_of_external_Web_server\”)”act_external_to_internal
```

- Vincular la directiva de forma global.

Para redirigir una URL externa a una URL interna mediante la utilidad de configuración

1. Vaya a **AppExpert** > **Reescribir** > **Acciones**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En el cuadro de diálogo **Crear acción de reescritura**, escriba el nombre act_external_to_internal.
4. Para reemplazar el nombre de host del servidor HTTP por el nombre del servidor interno, seleccione **Reemplazar** en el cuadro de lista Tipo.
5. En el campo Nombre de encabezado, escriba **Host**.
6. En la expresión de cadena de un campo de texto de reemplazo, escriba el nombre de host interno del servidor Web.

7. Haga clic en **Create** y, luego, en **Close**.
8. En el panel de navegación, haga clic en **Directivas**.
9. En el panel de detalles, haga clic en **Agregar**.
10. En el campo Nombre, escriba pol_external_to_internal. Esta directiva detecta las conexiones al servidor web.
11. En el menú desplegable **Acción**, elija la acción act_external_to_internal.
12. En el editor de expresiones, construya la siguiente expresión:

```
HTTP.REQ.HOSTNAME.SERVER.EQ("www.example.com")
<!--NeedCopy-->
```

1. Enlazar su nueva directiva globalmente.

Redirección de una consulta

En este ejemplo se describe cómo crear una acción de reescritura y una directiva de reescritura que redirija una consulta a la URL adecuada. En el ejemplo se supone que la solicitud contiene un encabezado Host establecido en **www.example.com** y un método GET con la **cadena /query.cgi?server=5**. La redirección extrae el nombre de dominio del encabezado del host y el número de la cadena de consulta, y redirige la consulta del usuario al servidor **Web5.example.com**, donde se procesa el resto de la consulta del usuario.

> **Nota:**
>
> Aunque los siguientes comandos aparecen en varias líneas, debe introducirlos en una sola línea sin saltos de línea.

Para redirigir una consulta a la URL adecuada mediante la CLI

- Para crear una acción de reescritura denominada act_redirect_query que reemplace el nombre de host del servidor HTTP por el nombre del servidor interno, escriba:

```
add rewrite action act_redirect_query REPLACE http.req.header("Host").
before_str(".example.com")'"Web" + http.req.url.query.value("server")'
```

- Para crear una directiva de reescritura denominada pol_redirect_query, escriba los siguientes comandos en el símbolo del sistema de Citrix ADC. Esta directiva detecta conexiones al servidor web que contienen una cadena de consulta. No aplique esta directiva a conexiones que no contengan una cadena de consulta:

```
add rewrite policy pol_redirect_query 'http.req.header("Host").eq(www.
example.com)&& http.req.url.contains("?")'act_redirect_query
```


- Enlazar su nueva directiva globalmente.

Dado que esta directiva de reescritura es muy específica y debe ejecutarse antes de cualquier otra directiva de reescritura, es recomendable asignarle una prioridad alta. Si le asigna una prioridad de 1, se evalúa primero.

Reescribir HTTP a HTTPS

En este ejemplo se describe cómo reescribir las respuestas del servidor Web para buscar todas las URL que empiezan por la cadena "HTTP" y reemplazar esa cadena por "https". Puede usarlo para evitar tener que actualizar páginas web después de mover un servidor de HTTP a HTTPS.

Para redirigir las URL HTTP a HTTPS mediante la CLI

- Para crear una acción de reescritura llamada act_replace_http_with_https que reemplaza todas las instancias de la cadena "HTTP" por la cadena "https", introduzca el siguiente comando:

```
add rewrite action act_replace_http_with_https replace_all 'http.res.body
(100)''"https"'-search http
```

- Para crear una directiva de reescritura denominada pol_replace_http_with_https que detecte conexiones con el servidor web, escriba el siguiente comando:

```
add rewrite policy pol_replace_http_with_https TRUE act_replace_http_with_https
 NOREWRITE
```

- Enlazar su nueva directiva globalmente.

Para solucionar problemas con esta operación de reescritura, consulte "Caso práctico: La directiva de reescritura para convertir enlaces HTTP a HTTPS no funciona. "

Eliminación de encabezados no deseados

En este ejemplo se explica cómo utilizar una directiva de reescritura para quitar encabezados no deseados. En concreto, en el ejemplo se muestra cómo quitar los siguientes encabezados:

- **Aceptar encabezado de codificación.** La eliminación del encabezado Accept Encoding de las respuestas HTTP impide la compresión de la respuesta.
- **Encabezado Ubicación del contenido.** Eliminar el encabezado Ubicación de contenido de las respuestas HTTP impide que el servidor proporcione a un hacker información que podría permitir una infracción de seguridad.

Para eliminar encabezados de las respuestas HTTP, debe crear una acción de reescritura y una directiva de reescritura, y vincular la directiva globalmente.

Para crear la acción Reescritura adecuada mediante la CLI

En el símbolo del sistema, escriba uno de los comandos siguientes para quitar el encabezado Aceptar codificación y evitar la compresión de la respuesta o quitar el encabezado Ubicación de contenido:

- `add rewrite action "act_remove-ae"delete_http_header "Accept-Encoding"`
- `add rewrite action "act_remove-cl"delete_http_header "Content-Location"`

Para crear la directiva de reescritura adecuada mediante la CLI

En el símbolo del sistema, escriba uno de los comandos siguientes para quitar el encabezado Aceptar codificación o el encabezado Ubicación de contenido:

- `add rewrite policy "pol_remove-ae"true "act_remove-ae"`
- `add rewrite policy "pol_remove-cl"true "act_remove-cl"`

Para vincular la directiva globalmente mediante la CLI

En el símbolo del sistema, escriba uno de los comandos siguientes, según corresponda, para vincular globalmente la directiva que ha creado:

- `bind rewrite global pol_remove_ae 100`
- `bind rewrite global pol_remove_cl 200`

Reducción de redireccionamientos de servidores web

En este ejemplo se explica cómo utilizar una directiva de reescritura para modificar las conexiones a la página principal y a otras direcciones URL que terminan con una barra diagonal (/) a la página de índice predeterminada del servidor, evitando redirecciones y reduciendo la carga en el servidor.

Para modificar las solicitudes HTTP a nivel de directorio para incluir la página de inicio predeterminada mediante la CLI

- Para crear una acción de reescritura denominada acción-default-homepage que modifique las direcciones URL que terminan en una barra diagonal para incluir la página principal predeterminada index.html, escriba:

```
add rewrite action "action-default-homepage"replace http.req.url.path "\"/
index.html\""
```

- Para crear una directiva de reescritura denominada policy-default-homepage que detecte conexiones a su página de inicio y aplique su nueva acción, escribe:

```
add rewrite policy "policy-default-homepage"q\##http.req.url.path.EQ("/")"
action-default-homepage"\##
```


- Enlazar globalmente su nueva directiva para ponerla en vigor.

Enmascarar el encabezado del servidor

En este ejemplo se explica cómo utilizar una directiva Rewrite para enmascarar la información del encabezado Server en las respuestas HTTP del servidor web. Ese encabezado contiene información que los piratas informáticos pueden utilizar para poner en peligro su sitio web. Si bien enmascarar el encabezado no impedirá que un hacker experto encuentre información sobre su servidor, dificulta el hackeo de su servidor web y alienta a los hackers a elegir objetivos menos protegidos.

Para enmascarar el encabezado del servidor en las respuestas de la CLI

1. Para crear una acción de reescritura denominada act_mask-server que reemplace el contenido del encabezado Servidor por una cadena no informativa, escriba:

```
add rewrite action ”act_mask-server”replace ”http.RES.HEADER(\”Server\”)””
\”Web Server 1.0\””
```

1. Para crear una directiva de reescritura denominada pol_mask-server que detecte todas las conexiones, escriba:

```
add rewrite policy ”pol_mask-server”true ”act_mask-server”
```

1. Enlazar globalmente su nueva directiva para ponerla en vigor.

Cómo convertir texto sin formato a cadena codificada en URL y de la manera opuesta

Las siguientes expresiones convierten texto sin formato en cadena codificada en URL y de la forma opuesta:

1. URL_RESERVED_CHARS_SAFE (cadena a URL ENCODED).

Ejemplo:

```
(”abc def&123”).URL_RESERVED_CHARS_SAFE
Output will be
 “abc%20def%26123”  which is url encoded.
<!--NeedCopy-->
```

1. SET_TEXT_MODE (URLENCODED) .DECODE_USING_TEXT_MODE. (URL CODIFICADA a cadena)

Ejemplo:


```
("abc%20def%26123").SET_TEXT_MODE(URLENCODED).DECODE_USING_TEXT_MODE
Output will be
 "abc def&123"
<!--NeedCopy-->
```

Ejemplos de directivas de reescritura y respuesta

October 5, 2021

A continuación se presentan algunos ejemplos de directivas de reescritura y respuesta:

Ejemplo 1: Para agregar un encabezado IP de cliente local mediante la interfaz de línea de comandos

```
add rewrite action act_ins_client insert_http_header NS-Client 'CLIENT.
   IP.SRC'
add rewrite policy pol_ins_client http.req.is_valid act_ins_client
bind rewrite global pol_ins_client 300 END

namem@obelix:~$ curl -v http://10.10.10.10/testsite/file5.html
* Hostname was NOT found in DNS cache
*   Trying 10.10.10.10...
* Connected to 10.10.10.10 (10.10.10.10) port 80 (#0)
> GET /testsite/file5.html HTTP/1.1
> User-Agent: curl/7.35.0
> Host: 10.10.10.10
> Accept: \*/\*
>
< HTTP/1.1 200 OK
< Date: Tue, 10 Nov 2020 10:06:48 GMT
* Server Apache/2.2.15 (CentOS) is not blacklisted
< Server: Apache/2.2.15 (CentOS)
< Last-Modified: Thu, 20 Jun 2019 07:16:04 GMT
< ETag: "816c5-5-58bbc1e73cdd3"
< Accept-Ranges: bytes
< Content-Length: 5
< Content-Type: text/html; charset=UTF-8
< NS-Client: 10.102.1.98
<
* Connection #0 to host 10.10.10.10 left intact
```



```
JLEwxt_namem@obelix:~$

<!--NeedCopy-->
```

Ejemplo 2: enmascarar el tipo de servidor HTTP

```
add rewrite action Action-Rewrite-Server_Mask REPLACE HTTP.RES.HEADER("Server") ""Web Server 1.0""
add rewrite policy-Rewrite-Server_Mask HTTP.RES.IS_VALID Action-Rewrite-Server_Mask NOREWRITE
namem@obelix:~$ curl -v http://10.10.10.10/testsite/file5.html
* Hostname was NOT found in DNS cache
*   Trying 10.10.10.10...
* Connected to 10.10.10.10 (10.10.10.10) port 80 (#0)
> GET /testsite/file5.html HTTP/1.1
> User-Agent: curl/7.35.0
> Host: 10.10.10.10
> Accept: \*/\*
>
< HTTP/1.1 200 OK
< Date: Tue, 10 Nov 2020 10:15:42 GMT
* Server Web Server 1.0 is not blacklisted
< Server: Web Server 1.0
< Last-Modified: Thu, 20 Jun 2019 07:16:04 GMT
< ETag: "816c5-5-58bbc1e73cdd3"
< Accept-Ranges: bytes
< Content-Length: 5
< Content-Type: text/html; charset=UTF-8
<
* Connection #0 to host 10.10.10.10 left intact
JLEwxt_namem@obelix:~$
<!--NeedCopy-->
```

Ejemplo 3: Responder redirigiendo a una URL diferente cuando se recibe una url

```
> add responder action act1 redirect ""www.google.com""
 Done
> add responder policy pol1 'HTTP.REQ.URL.CONTAINS("file")' act1
 Done
> bind responder global pol1 1
 Done
```



```
>

name:~$ curl -v http://10.10.10.10/testsite/file5.html
* Hostname was NOT found in DNS cache
*   Trying 10.10.10.10...
* Connected to 10.10.10.10 (10.10.10.10) port 80 (#0)
> GET /testsite/file5.html HTTP/1.1
> User-Agent: curl/7.35.0
> Host: 10.10.10.10
> Accept: \*/\*
>
< HTTP/1.1 302 Found : Moved Temporarily
< Location: www.google.com
< Connection: close
< Cache-Control: no-cache
< Pragma: no-cache
<
* Closing connection 0
name@obelix:~$
<!--NeedCopy-->
```

Ejemplo 4: Responder con un mensaje que puede ser cualquier expresión o texto

```
add responder action act123 respondwith ""Please reach out to
   administrator""
add responder policy pol1 "HTTP.REQ.URL.CONTAINS("file")" act123
bind responder global pol1 100 END

name@obelix:~$ curl -v http://10.10.10.10/testsite/file5.html
* Hostname was NOT found in DNS cache
*   Trying 10.10.10.10..Responder Action and Policy:

>add responder action Redirect-Action redirect ""https://xyz.abc.com/
   dispatcher/SAML2AuthService?siteurl=wmav"" -responseStatusCode 302

>add responder policy Redirect-Policy "HTTP.REQ.HOSTNAME.CONTAINS("abc"
   )" Redirect-Action

Binding to LB Virtual Server:

>bind lb vserver Test1_SF -policyName Redirect-Policy -priority 100 -
   gotoPriorityExpression END -type REQUEST.
* Connected to 10.10.10.10 (10.10.10.10) port 80 (#0)
```



```
> GET /testsite/file5.html HTTP/1.1
> User-Agent: curl/7.35.0
> Host: 10.10.10.10
> Accept: \*/\*
>
* Connection #0 to host 10.10.10.10 left intact
Please reach out to administratort_name@obelix:~$
<!--NeedCopy-->
```

Ejemplo 5: Responder con una página HTML importada

```
import responder htmlpage http://10.10.10.10)/testsite/file5.html
   page112
add responder action act1 respondwithHtmlpage page1
add responder policy pol1 true act1
bind responder global pol1 100

name@obelix:~$ curl -v http://10.10.10.10)/testsite/file5.html
* Hostname was NOT found in DNS cache
*   Trying 10.10.10.10...
* Connected to 10.10.10.10 (10.10.10.10)) port 80 (#0)
> GET /testsite/file5.html HTTP/1.1
> User-Agent: curl/7.35.0
> Host: 10.102.58.140
> Accept: \*/\*
>
< HTTP/1.1 200 OK
< Content-Length: 5
< Content-Type: text/html
<
* Connection #0 to host 10.10.10.10 left intact
JLEwxt_name@obelix:~$
<!--NeedCopy-->
```

Ejemplo 6: URL de redirección basada en HOSTNAME mediante la directiva de respuesta

```
Responder Action and Policy:

>add responder action Redirect-Action redirect ""https://xyz.abc.com/
   dispatcher/SAML2AuthService?siteurl=wmav"" -responseStatusCode 302
```



```
4
5 >add responder policy Redirect-Policy "HTTP.REQ.HOSTNAME.CONTAINS("abc")" Redirect-Action
6
7 Binding to LB Virtual Server:
8
9 >bind lb vserver Test1_SF -policyName Redirect-Policy -priority 100 -gotoPriorityExpression END -type REQUEST
10 <!--NeedCopy-->
```

Limitación de velocidad

October 5, 2021

La función de limitación de velocidad permite definir la carga máxima para una entidad de red o entidad virtual determinada en el dispositivo Citrix ADC. Esta función permite configurar el dispositivo para supervisar la velocidad de tráfico asociada a la entidad y tomar medidas preventivas, en tiempo real, en función de la tasa de tráfico. Esta función resulta especialmente útil cuando la red está siendo atacada por un cliente hostil que envía al dispositivo una gran cantidad de solicitudes. Puede mitigar los riesgos que afectan a la disponibilidad de los recursos para los clientes y mejorar la fiabilidad de la red y los recursos que administra el dispositivo.

Puede supervisar y controlar la tasa de tráfico asociada a las entidades virtuales y definidas por el usuario, incluidos servidores virtuales, URL, dominios y combinaciones de URL y dominios. Puede limitar la velocidad del tráfico si es demasiado alta, basar la información en caché en la velocidad de tráfico y redirigir el tráfico a un servidor virtual de equilibrio de carga determinado si la velocidad de tráfico supera un límite predefinido. Puede aplicar la supervisión basada en tarifas a solicitudes HTTP, TCP y DNS.

Para supervisar la velocidad de tráfico de un caso determinado, configure un *identificador de límite de velocidad*. Un identificador de límite de velocidad especifica umbrales numéricos como el número máximo de solicitudes o conexiones (de un tipo concreto) permitidas en un período de tiempo específico denominado intervalo de *tiempo*.

De forma opcional, puede configurar filtros, conocidos como *selectores de secuencias*, y asociarlos a identificadores de límite de velocidad al configurar los identificadores. Después de configurar el selector de transmisión opcional y el identificador de límite, debe invocar el identificador de límite desde una directiva avanzada. Puede invocar identificadores desde cualquier función en la que el identificador pueda ser útil, como la reescritura, el respondedor, el DNS y el almacenamiento en caché integrado.

Puede habilitar y inhabilitar de forma global las capturas SNMP para los identificadores de límite de velocidad. Cada captura contiene datos acumulativos para el intervalo de recopilación de datos configurado del identificador de límite de velocidad (segmento de tiempo), a menos que haya especificado varias capturas que se generarán por segmento de tiempo. Para obtener más información sobre la configuración de capturas y administradores SNMP, consulte SNMP.

Configuración de un selector de transmisión

October 5, 2021

Un selector de flujo de tráfico es un filtro opcional para identificar una entidad para la que quiere restrinGIR el acceso. El selector se aplica a una solicitud o respuesta y selecciona puntos de datos (claves) que se pueden analizar mediante un identificador de flujo de velocidad. Estos puntos de datos se pueden basar en casi cualquier función del tráfico, incluidas direcciones IP, subredes, nombres de dominio, identificadores TCP o UDP y cadenas o extensiones específicas de las URL.

Un selector de secuencias consta de expresiones de directiva avanzada individuales denominadas selectlets. Cada selectlet es una expresión de directiva avanzada no compuesta. Un selector de flujo de tráfico puede contener hasta cinco expresiones no compuestas denominadas selectlets. Se considera que cada selectlet está en una relación AND con las demás expresiones. A continuación se presentan algunos ejemplos de selectlets:

```
1 http.req.url
2 http.res.body(1000>after_str(”car_model”).before_str(”made_in”)”
3 ”client.ip.src.subnet(24)”
4 <!--NeedCopy-->
```

El orden en que se especifican los parámetros es significativo. Por ejemplo, si configura una dirección IP y un dominio (en ese orden) en un selector y, a continuación, especifica el dominio y la dirección IP (en orden inverso) en otro selector, Citrix ADC considera que estos valores son únicos. Esto puede hacer que la misma transacción se cuente dos veces. Además, si varias directivas invocan el mismo selector, Citrix ADC, de nuevo, puede contar la misma transacción más de una vez.

Nota: Si modifica una expresión en un selector de secuencias, puede aparecer un error si cualquier directiva que la invoque está vinculada a una nueva etiqueta de directiva o punto de enlace. Por ejemplo, supongamos que crea un selector de secuencias denominado myStreamSelector1, lo invoca desde myLimitId1 e invoca el identificador desde una directiva DNS denominada DNSrateLimit1. Si cambia la expresión en myStreamSelector1, es posible que reciba un error al vincular DNSRateLimit1 a un nuevo punto de enlace. La solución consiste en modificar estas expresiones antes de crear las directivas que las invocan.

Para configurar un selector de flujo de tráfico mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
add stream selector <name> <rule> ...
<!--NeedCopy-->
```

Ejemplo:

```
add stream selector myStreamSel HTTP.REQ.URL CLIENT.IP.SRC
<!--NeedCopy-->
```

Para configurar un selector de secuencias mediante la utilidad de configuración

Vaya a AppExpert > Limitación de velocidad > Selectores, haga clic en Agregar y especifique los detalles pertinentes.

Configuración de un identificador de límite de velocidad de tráfico

October 5, 2021

Un identificador de límite de velocidad comprueba si la cantidad de tráfico supera un valor especificado en un intervalo de tiempo determinado. El identificador devuelve un “booleano TRUE” si la cantidad de tráfico supera un límite dentro de un intervalo de tiempo determinado. Al incluir un identificador de límite en la expresión de directiva compuesta DAdvanced de una regla de directiva, debe incluir un selector de flujo. Si no lo especifica, el identificador de límite se aplica a todas las solicitudes o respuestas identificadas por las expresiones compuestas.

> **Nota:**
>
> La longitud máxima para almacenar los resultados de cadena (por ejemplo, HTTP.REQ.URL) es de 60 caracteres. Si la cadena (por ejemplo, URL) tiene 1000 caracteres, de los cuales 50 caracteres son suficientes para identificar de forma exclusiva una cadena, puede utilizar una expresión para extraer los 50 caracteres necesarios.

Para configurar un identificador de límite de tráfico desde la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
add ns limitIdentifier <limitIdentifier> -threshold <positive_integer>
    -timeSlice <positive_integer> -mode <mode> -limitType ( BURSTY |
    SMOOTH ) -selectorName <string> -maxBandwidth <positive_integer> -
    trapsInTimeSlice <positive_integer>
<!--NeedCopy-->
```

Descripción del argumento

Identificador de límite. Nombre de un identificador de límite de tasa. Debe comenzar con una letra ASCII o un carácter de guión bajo (_) y debe constar únicamente de caracteres alfanuméricos o de guión bajo ASCII. No se deben utilizar palabras reservadas. Este es un argumento obligatorio. Longitud máxima: 31

umbral. Número máximo de solicitudes permitidas en el período de tiempo determinado cuando se realiza un seguimiento de las solicitudes (el modo se establece como REQUEST_RATE) por segmento de tiempo. Cuando se realiza un seguimiento de las conexiones (el modo se establece como CONNECTION), es el número total de conexiones que se dejarían pasar. Valor por defecto: 1 Valor mínimo: 1 Valor máximo: 4294967295

TimeSlice. Intervalo de tiempo, en milisegundos, especificado en múltiplos de 10, durante el cual se realiza un seguimiento de las solicitudes para comprobar si cruzan el umbral. Este argumento solo es necesario cuando el modo se establece en REQUEST_RATE. Valor predeterminado: 1000 Valor mínimo: 10 Valor máximo: 4294967295

modo. Define el tipo de tráfico que se va a rastrear.

1. REQUEST_RATE. Realiza un seguimiento de las solicitudes/período de tiempo.
2. CONEXIÓN. Rastrea las transacciones activas.

Tipo límite. Tipo de solicitud suave o con ráfagas.

Nombre del selector. Nombre del selector de límite de tarifa. Si este argumento es NULL, la limitación de velocidad se aplicará a todo el tráfico recibido por el servidor virtual o Citrix ADC (dependiendo de si el identificador de límite está vinculado a un servidor virtual o globalmente) sin ningún **filtro. Longitud máxima: 31**

Ancho de**banda máximo**. Ancho de banda máximo permitido, en kbps. Valor mínimo: 0 Valor máximo: 4294967287

Ejemplo:

Configuración del identificador de límite de velocidad de tráfico en modo BURSTY:

```
add ns limitIdentifier 100_request_limit -threshold 100 -timeSlice 1000
     -mode REQUEST_RATE -limitType BURSTY -selectorName
    limit_100_requests_selector -trapsInTimeSlice 30
<!--NeedCopy-->
```

Configuración del identificador de límite de velocidad de tráfico en modo SMOOTH:

```
add ns limitidentifier limit_req -mode request_rate -limitType smooth -
    timeslice 1000 -Threshold 2000 -trapsInTimeSlice 200
<!--NeedCopy-->
```

Para configurar un identificador de límite de tráfico mediante la utilidad de configuración

Vaya a AppExpert > Limitación de velocidad > Identificadores de límite, haga clic en Agregar y especifique los detalles pertinentes.

Configuración y vinculación de una directiva de velocidad de tráfico

October 5, 2021

Implementar el comportamiento de las aplicaciones basadas en tarifas configurando una directiva en una función adecuada de Citrix ADC. La función debe admitir directivas avanzadas. La expresión de directiva debe contener el siguiente prefijo de expresión para permitir que la función analice la tasa de tráfico:

```
sys.check_limit(<limit_identifier>)
<!--NeedCopy-->
```

Donde limit_identifier es el nombre de un identificador de límite.

La expresión de directiva debe ser una expresión compuesta que contenga al menos dos componentes:

- Expresión que identifica el tráfico al que se aplica el identificador de límite de velocidad. Por ejemplo:

```
1     http.req.url.contains(”my_aspx.aspx”).
2 <!--NeedCopy-->
```

- Expresión que identifica un identificador de límite de velocidad, por ejemplo, sys.check_limit (“my_limit_identifier”). Esta debe ser la última expresión de la expresión de directiva.

Para configurar una directiva basada en tarifas mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba el siguiente comando para configurar una directiva basada en tarifas y verificar la configuración:

```
1 add cache|dns|rewrite|responder policy <policy_name> -rule expression
     && sys.check_limit(”<LimitIdentifierName>”) [<feature-specific
     information>]
2 <!--NeedCopy-->
```

A continuación se muestra un ejemplo completo de una regla de directiva basada en tasas. Tenga en cuenta que en este ejemplo se supone que ha configurado la acción de respuesta, send_direct_url, asociada a la directiva. Tenga en cuenta que el parámetro sys.check_limit debe ser el último elemento de la expresión de directiva:

```
1 add responder policy responder_threshold_policy ”http.req.url.contains(
     ”myindex.html”) && sys.check_limit(”my_limit_identifier”)”
     send_direct_url
2 <!--NeedCopy-->
```

Para obtener información sobre cómo vincular una directiva de forma global o a un servidor virtual, consulte “Vinculación de directivas avanzadas de directivas. “

Para configurar una directiva basada en tasas mediante la utilidad de configuración

1. En el panel de navegación, expanda la función en la que quiere configurar una directiva (por ejemplo, Almacenamiento en caché integrado, Reescritura o Respondedor) y, a continuación, haga clic en Directivas.

2. En el panel de detalles, haga clic en Agregar. En Nombre, introduzca un nombre exclusivo para la directiva.
3. En Expresión, introduzca la regla de directiva y asegúrese de incluir el parámetro sys.check_limit como componente final de la expresión. Por ejemplo:

```
1 http.req.url.contains(”my_aspx.aspx”) && sys.check_limit(”
     my_limit_identifier”)
2 <!--NeedCopy-->
```

4. Introduzca información específica de la función sobre la directiva.

   Por ejemplo, es posible que se le solicite asociar la directiva a una acción o a un perfil. Para obtener más información, consulte la documentación específica de las funciones.
5. Haga clic en Creary, a continuación, en Cerrar.
6. Haga clic en Guardar.

Visualización de la tasa de tráfico

January 12, 2021

Si el tráfico a través de uno o más servidores virtuales coincide con una directiva basada en tasas, puede ver la velocidad de este tráfico. Las estadísticas de tasa se mantienen en el identificador de límite que nombró en la regla de la directiva basada en tasas. Si más de una directiva utiliza el mismo identificador de límite, puede ver la velocidad de tráfico definida por las visitas a todas las directivas que utilizan el identificador de límite concreto.

Para ver la velocidad de tráfico mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba el comando siguiente para ver la velocidad de tráfico:

```
1 show ns limitSessions <limitIdentifier>
2 <!--NeedCopy-->
```

Ejemplo:

```
1 sh limitsession myLimitSession
2 <!--NeedCopy-->
```


Para ver la velocidad de tráfico mediante la utilidad de configuración

1. Vaya a AppExpert > Limitación de velocidad > Identificadores de límite.
2. Seleccione un identificador de límite cuya velocidad de tráfico quiera ver.
3. Haga clic en el botón Mostrar sesiones. Si el tráfico a través de uno o más servidores virtuales coincide con una directiva de limitación de velocidad que utiliza este identificador de límite (y las visitas se encuentran dentro del segmento de tiempo configurado para este identificador), aparece el cuadro de diálogo Detalles de la sesión. De lo contrario, recibirá un mensaje "No hay sesión".

Prueba de una directiva basada en tasas

January 12, 2021

Para probar una directiva basada en tasas, puede enviar tráfico a cualquier servidor virtual al que esté enlazada una directiva basada en tasas.

Descripción general de la tarea: Probar una directiva basada en tasas

1. Configure un selector de flujo (opcional) y un identificador de límite de velocidad (obligatorio). Por ejemplo:

```
add stream selector sel_subnet Q.URL "CLIENT.IP.SRC.SUBNET(24)"
add ns limitIdentifier k_subnet -Threshold 4 -timeSlice 3600 -mode
    REQUEST_RATE  -limittype smooth  -selectorName sel_subnet  -
   trapsInTimeSlice 8
<!--NeedCopy-->
```

2. Configure la acción que quiere asociar a la directiva que utiliza el identificador de límite de velocidad. Por ejemplo:

```
add responder action resp_redirect redirect ""http://response_site
    .com/""
<!--NeedCopy-->
```

3. Configure una directiva que utilice el prefijo de expresión sys.check_limit para llamar al identificador de límite de velocidad. Por ejemplo, la directiva puede aplicar un identificador de límite de velocidad a todas las solicitudes procedentes de una subred concreta, como se indica a continuación:


```
add responder policy resp_subnet "SYS.CHECK_LIMIT("k_subnet")"
   resp_redirect
<!--NeedCopy-->
```

4. Enlazar la directiva globalmente o a un servidor virtual. Por ejemplo:

```
bind responder global resp_subnet 6 END -type DEFAULT
<!--NeedCopy-->
```

5. En una barra de direcciones del explorador, envíe una consulta HTTP de prueba a un servidor virtual. Por ejemplo:

```
http://<IP of a vserver>/testsite/test.txt
<!--NeedCopy-->
```

6. En el símbolo del sistema de Citrix ADC, escriba:

```
show ns limitSessions <limitIdentifier>
<!--NeedCopy-->
```

Ejemplo

```
> sh limitsession k_subnet
1)      Time Remaining:       98 secs  Hits: 2
                            Action Taken: 0
        Total Hash:    1718618  Hash String: /test.txt
        IPs gathered:
                1) 10.217.253.0
        Active Transactions: 0
 Done
>
<!--NeedCopy-->
```

7. Repita la consulta y compruebe de nuevo las estadísticas del identificador de límite para comprobar que las estadísticas se están actualizando correctamente.

Ejemplos de directivas basadas en tarifas

October 5, 2021

En la tabla siguiente se muestran ejemplos de directivas basadas en tarifas.

Table 1. Examples of Rate-Based Policies

Purpose	Example

Limit the number of requests per second from a URL	`add stream selector ipStreamSelector http.req.url "client.ip.src"`
	`add ns limitIdentifier ipLimitIdentifier -threshold 4 -timeSlice 1000`
	`-mode request_rate -limitType smooth -selectorName ipStreamSelector`
	
	`add responder action myWebSiteRedirectAction redirect`
	`"\"http://www.mycompany.com/\""`
	
	`add responder policy ipLimitResponderPolicy "http.req.url.contains(\"myasp.asp\")`
	`&& sys.check_limit(\"ipLimitIdentifier\")" myWebSiteRedirectAction`
	
	`bind responder global ipLimitResponderPolicy 100 END -type default`

Cache a response if the request URL rate exceeds 5 per 20000 milliseconds	`add stream selector cacheStreamSelector http.req.url`
	`add ns limitidentifier cacheRateLimitIdentifier -threshold 5 -timeSlice 2000`
	`-selectorName cacheStreamSelector`
	
	`add cache policy cacheRateLimitPolicy -rule "http.req.method.eq(get)`
	`&& sys.check_limit(\"cacheRateLimitIdentifier\")" -action cache`
	
	`bind cache global cacheRateLimitPolicy -priority 10`

Drop a connection on the basis of cookies received in requests from www.yourcompany.com if the requests exceed the rate limit	`add stream selector reqCookieStreamSelector "http.req.cookie`
	`.value(\"mycookie\")" "client.ip.src.subnet(24)"`
	
	`add ns limitIdentifier myLimitIdentifier -Threshold 2 -timeSlice 3000`
	`-selectorName reqCookieStreamSelector`
	
	`add responder action sendRedirectUrl redirect '\"http://www.mycompany.com\"`
	`+ http.req.url' -bypassSafetyCheck YES`
	
	`add responder policy rateLimitCookiePolicy`
	`"http.req.url.contains(\"www.yourcompany.com\")`
	`&& sys.check_limit(\"myLimitIdentifier\")" sendRedirectUrl`

Drop a DNS packet if the requests from a particular client IP address and DNS domain exceed the rate limit	`add stream selector dropDNSStreamSelector client.udp.dns.domain client.ip.src`
	`add ns limitIdentifier dropDNSRateIdentifier -timeslice 20000 -mode request_rate`
	`-selectorName dropDNSStreamSelector -maxBandwidth 1 -trapsintimeslice 20`
	
	`add dns policy dnsDropOnClientRatePolicy "sys.check_limit`
	`(\"dropDNSRateIdentifier\")" -drop yes`

Limit the number of HTTP requests that arrive from the same host (with a subnet mask of 32) and that have the same destination IP address.	`add stream selector ipv6_sel "CLIENT.IPv6.src.subnet(32)" CLIENT.IPv6.dst Q.URL`
	`add ns limitIdentifier ipv6_id -imeSlice 20000 -selectorName ipv6_sel`
	`add lb vserver ipv6_vip HTTP 3ffe::209 80 -persistenceType NONE -cltTimeout 180`
	`add responder action redirect_page redirect "\"http://redirectpage.com/\""`
	`add responder policy ipv6_resp_pol "SYS.CHECK_LIMIT(\"ipv6_id\")" redirect_page`
	`bind responder global ipv6_resp_pol 5 END -type DEFAULT`

Ejemplos de casos de uso para directivas basadas en tasas

January 12, 2021

Los siguientes casos describen dos usos de directivas basadas en velocidad en el equilibrio de carga global de servidores (GSLB):

- El primer caso describe el uso de una directiva basada en velocidad que envía tráfico a un nuevo centro de datos si la velocidad de solicitudes DNS supera 1000 por segundo.
- En el segundo caso, si llegan más de cinco solicitudes DNS para un cliente DNS local (LDNS) dentro de un período determinado, se eliminan las solicitudes adicionales.

Redirigir el tráfico sobre la base de la tasa de tráfico

En este caso, configurar un método de equilibrio de carga basado en proximidad y una directiva de limitación de velocidad que identifica las solicitudes DNS para una región determinada. En la directiva de limitación de velocidad, especifique un umbral de 1000 solicitudes DNS por segundo. Una directiva DNS aplica la directiva de limitación de velocidad a las solicitudes DNS para la región "Europe.gb.17.London.uk-East.isp-uk." En la directiva DNS, las solicitudes DNS que superen el umbral de limitación de velocidad, comenzando con la solicitud 1001 y continuando hasta el final del intervalo de un segundo, se reenviarán a las direcciones IP asociadas con la región "North America.us.tx.dallas.us-East.isp-US."

La siguiente configuración demuestra este caso:

```
1 add stream selector DNSSelector1 client.udp.dns.domain
2
3 add ns limitIdentifier DNSLimitIdentifier1 -threshold 5 -timeSlice 1000
      -selectorName DNSSelector1
4
5 add dns policy DNSLimitPolicy1 "client.ip.src.matches_location("Europe.
    GB.17.London.\*.\*") &&
6 sys.check_limit("DNSLimitIdentifier1")" -preferredLocation "North
    America.US.TX.Dallas.\*.\*"
7
8 bind dns global DNSLimitPolicy1 5
9 <!--NeedCopy-->
```


Desconexión de solicitudes DNS sobre la base de la tasa de tráfico

En el siguiente ejemplo de equilibrio de carga global del servidor, se configura una directiva de limitación de velocidad que permite dirigir un máximo de cinco solicitudes DNS en un intervalo determinado, por dominio, a un cliente LDNS para su resolución. Se eliminan todas las solicitudes que superen esta tasa. Este tipo de directiva puede ayudar a proteger Citrix ADC contra la explotación de recursos. Por ejemplo, en este caso, si el tiempo de vida (TTL) para una conexión es de cinco segundos, esta directiva impide que el LDNS exija un dominio. En su lugar, utiliza datos almacenados en caché en Citrix ADC.

```
add stream selector LDNSSelector1 client.udp.dns.domain client.ip.src

add ns limitIdentifier LDNSLimitIdentifier1 -threshold 5 -timeSlice
    1000 -selectorName LDNSSelector1

add dns policy LDNSPolicy1 "client.udp.dns.domain.contains(".") && sys.
    check_limit("LDNSLimitIdentifier1")" -drop YES

bind dns global LDNSPolicy1 6

show gslb vserver gvip

gvip - HTTP     State: UP
Last state change was at Mon Sep  8 11:50:48 2008 (+711 ms)
Time since last state change: 1 days, 02:55:08.830
Configured Method: STATICPROXIMITY
BackupMethod: ROUNDROBIN
No. of Bound Services :  3 (Total)       3 (Active)
Persistence: NONE       Persistence ID: 100
Disable Primary Vserver on Down: DISABLED       Site Persistence: NONE
Backup Session Timeout: 0
Empty Down Response: DISABLED
Multi IP Response: DISABLED Dynamic Weights: DISABLED
Cname Flag: DISABLED
Effective State Considered: NONE
1.     site11_svc(10.100.00.00: 80)- HTTP State: UP    Weight: 1
Dynamic Weight: 0       Cumulative Weight: 1
Effective State: UP
Threshold : BELOW
Location: Europe.GB.17.London.UK-East.ISP-UK
2.      site12_svc(10.101.00.100: 80)- HTTP State: UP   Weight: 1
Dynamic Weight: 0       Cumulative Weight: 1
Effective State: UP
```



```
32 Threshold : BELOW
33 Location: North America.US.TX.Dallas.US-East.ISP-US
34 3.      site13_svc(10.102.00.200: 80)- HTTP State: UP   Weight: 1
35 Dynamic Weight: 0       Cumulative Weight: 1
36 Effective State: UP
37 Threshold : BELOW
38 Location: North America.US.NJ.Salem.US-Mid.ISP-US
39 4.      www.gslbindia.com        TTL: 5 secn
40 Cookie Timeout: 0 min   Site domain TTL: 3600 sec
41 Done
42 <!--NeedCopy-->
```

Limitación de velocidad para dominios de tráfico

January 12, 2021

Puede configurar la limitación de velocidad para los dominios de tráfico. La siguiente expresión en el lenguaje de expresiones Citrix ADC para identifica el tráfico asociado con dominios de tráfico.

- client.traffic_domain.id

Puede configurar la limitación de velocidad para el tráfico asociado a un dominio de tráfico determinado, a un conjunto de dominios de tráfico o a todos los dominios de tráfico.

Para configurar la limitación de velocidad para dominios de tráfico, realice los siguientes pasos en un dispositivo Citrix ADC mediante la utilidad de configuración o la línea de comandos Citrix ADC:

1. Configure un selector de flujo que utilice la expresión client.traffic_domain.id para identificar el tráfico asociado a los dominios de tráfico que se va a limitar la velocidad.
2. Configure un identificador de límite de velocidad que especifique parámetros como el umbral máximo para limitar la velocidad del tráfico. También asocia un selector de flujo al limitador de velocidad en este paso.
3. Configure una acción que quiera asociar a la directiva que utiliza el identificador de límite de velocidad.
4. Configure una directiva que utilice el prefijo de expresión sys.check_limit para llamar al identificador de límite de velocidad y asocie la acción a esta directiva.
5. Vincule la directiva globalmente.

Considere un ejemplo en el que dos dominios de tráfico, con identificadores 10 y 20, están configurados en Citrix ADC NS1. En el dominio de tráfico 10, LB1-TD-1 está configurado para equilibrar la carga de los servidores S1 y S2; LB2-TD1 está configurado para equilibrar la carga de los servidores S3 y S4.

En el dominio de tráfico 20, LB1-TD-2 está configurado para equilibrar la carga de los servidores S5 y S6; LB2-TD2 está configurado para equilibrar la carga de los servidores S7 y S8.

En la tabla siguiente se enumeran algunos ejemplos de directivas de limitación de velocidad para dominios de tráfico en la configuración de ejemplo.

Propósito	Comandos CLI
Limite el número de solicitudes a 10 por segundo para cada uno de los dominios de tráfico.	add stream selector tdratelimit-1 CLIENT.TRAFIC_DOMAIN.ID add ns limitidf-1 -threshold 10 -SelectorName tdratelimit-1 -TrapsIntimeslice 0 agregar directiva de respuesta ratelimit-pol “sys.check_limit (“limitidf-1”)” DROP bind responder global ratelimit-pol 1
Limite el número de solicitudes a 5 por cliente por segundo para cada uno de los dominios de tráfico.	add stream selector tdandclientip CLIENT.IP.SRC,CLIENT.TRAFFIC_DOMAIN.ID add ns limitIdentifier td_limitidf -threshold 5 -selectorName tdandclientip -trapsInTimeSlice 5 add responder policy tdratelimit-pol “sys.check_limit(\“td_limitidf\”)” DROP bind responder global tdratelimit-pol 2
Limite el número de solicitudes enviadas para un dominio de tráfico determinado (por ejemplo, dominio de tráfico 10) a 30 solicitudes cada 3 segundos.	add stream selector tdratelimit CLIENT.TRAFFIC_DOMAIN.ID add ns limitIdentifier td10_limitidf -threshold 30 -timeSlice 3000 -selectorName tdratelimit -trapsInTimeSlice 5 add responder policy td10ratelimit “client.traffic_domain.id==10 && sys.check_limit(\“td10_limitidf\”)” DROP bind responder global td10ratelimit 3
Limite el número de conexiones a 5 por cliente por segundo para un dominio de tráfico determinado (por ejemplo, dominio de tráfico 20).	add stream selector tdandclientip CLIENT.IP.SRC CLIENT.TRAFFIC_DOMAIN.ID add ns limitIdentifier td20_limitidf -threshold 5 -mode CONNECTION -selectorName tdandclientip -trapsInTimeSlice 5 add responder policy td20_ratelimit “client.traffic_domain.id==20 && sys.check_limit(\“td20_limitidf\”)” DROP bind responder global td20_ratelimit 4

Configurar límite de velocidad a nivel de paquete

January 21, 2022

Puede configurar un selector de flujo y una directiva de respuesta para recopilar estadísticas a nivel de paquete que fluyen a través de todas las conexiones identificadas por el selector. Si el número de paquetes por segundo supera el umbral configurado, la directiva aplica la acción configurada (RESET o DROP). Puede configurar estas directivas para todos los tipos de servidores virtuales. Se consideran paquetes de todos los tamaños.

Para configurar la limitación de velocidad a nivel de paquetes, lleve a cabo las siguientes tareas

1. Habilitar equilibrio de carga
2. Agregar selector de transmisiones
3. Agregar identificador de transmisión
4. Agregar directiva de Responder
5. Agregar un servidor virtual de equilibrio de carga
6. Directiva de respuesta de enlace

Para habilitar la función de equilibrio de carga

En el símbolo del sistema, escriba:

```
enable ns feature lb
<!--NeedCopy-->
```

Para agregar un selector de transmisiones

En el símbolo del sistema, escriba:

```
add stream selector packetlimitselector client.ip.src client.tcp.
   srcport client.ip.dst client.tcp.dstport
<!--NeedCopy-->
```


Para agregar un identificador de transmisión

En el símbolo del sistema, escriba:

```
add stream identifier packetlimitidentifier packetlimitselector -
   interval 1
<!--NeedCopy-->
```

Para habilitar el seguimiento de paquetes solo ACK

En el símbolo del sistema, escriba:

```
set stream identifier packetlimitidentifier  - trackAckOnlyPackets
   ENABLED
<!--NeedCopy-->
```

Para agregar una directiva de respuesta

En el símbolo del sistema, escriba:

```
add responder policy packet_rate_sessionpolicy "ANALYTICS.STREAM("
   packetlimitidentifier").COLLECT_STATS("PACKET_LIMIT", <
   max_threshold_PPS>, ACTION, 0/1)" NOOP
<!--NeedCopy-->
```

Donde:

- <max_threshold_PPS>es el número máximo de paquetes permitidos a través de la conexión por segundo.
- ACTION puede ser DROP o RESET.
- 0 o 1 representa el tipo de límite; 0 representa el tipo de límite BURSTY y 1 representa el tipo de límite SMOOTH.

Ejemplo:

```
add responder policy packet_rate_sessionpolicy "ANALYTICS.STREAM("
   packetlimitidentifier").COLLECT_STATS("PACKET_LIMIT", 40, RESET, 0)"
    NOOP
```



```
<!--NeedCopy-->
```

Para agregar un servidor virtual de equilibrio de carga

En el símbolo del sistema, escriba:

```
add lb vserver <name> <serviceType> <ip> <port>

add lb vserver Vserver-lb-1 HTTP 10.102.20.200 80
<!--NeedCopy-->
```

Para vincular una directiva de respuesta

Después de configurar el selector y la directiva de respuesta, la directiva se puede vincular de forma global o al servidor virtual específico.

En el símbolo del sistema, escriba uno de los siguientes comandos:

```
bind responder global <policyName> <priority> [<gotoPriorityExpression
   >] [-type <type>] [-invoke  (<labelType>  <labelName>) ]
<!--NeedCopy-->
```

O BIEN:

```
bind lb vserver <name>@  (-policyName <string>@ [-priority <
   positive_integer>]
<!--NeedCopy-->
```

Ejemplos:

```
bind responder global packet_rate_sessionpolicy 101 END -type
   REQ_DEFAULT

bind responder global packet_rate_sessionpolicy 102 END -type

bind lb vserver v1 -policyname packet_rate_sessionpolicy -priority 10
<!--NeedCopy-->
```


Respondedor

February 16, 2021

> **Advertencia**
>
> Las funciones de filtrado que utilizan directivas clásicas están obsoletas y, como alternativa, Citrix recomienda utilizar las funciones de reescritura y respuesta con infraestructura de directivas avanzada.

Las complejas configuraciones web actuales a menudo requieren respuestas diferentes a las solicitudes HTTP que, en la superficie, parecen ser similares. Cuando los usuarios solicitan una página web, es posible que desee proporcionar una página diferente en función de la ubicación geográfica del usuario, especificación del explorador o idiomas que acepte el explorador y el orden de preferencia. Es posible que quiera eliminar la conexión si la solicitud proviene de un rango de IP que ha estado generando ataques DDoS o iniciando intentos de piratería.

Responder admite protocolos como TCP, DNS (UDP) y HTTP. Con el respondedor habilitado en el dispositivo, las respuestas del servidor pueden basarse en quién envía la solicitud, desde dónde se envía y otros criterios con implicaciones de seguridad y administración del sistema. La función es simple y rápida de usar. Al evitar la invocación de funciones más complejas, reduce los ciclos de CPU y el tiempo dedicado al manejo de solicitudes que no requieren procesamiento complejo.

Para gestionar datos confidenciales como información financiera, si quiere asegurarse de que el cliente utiliza una conexión segura para explorar un sitio, puede redirigir la solicitud a una conexión segura mediante el uso`https://` en lugar de`http://`.

Para utilizar un respondedor, haga lo siguiente:

- Habilite una función de respuesta en el dispositivo.
- Configurar una acción de respuesta. La acción puede ser generar una respuesta personalizada, redirigir una solicitud a una página web diferente o restablecer una conexión.
- Configurar una directiva de respuesta. La directiva determina las solicitudes (tráfico) en las que se debe realizar una acción.
- Enlazar cada directiva a un punto de enlace ponerla en vigor. Un punto de enlace hace referencia a una entidad en la que el dispositivo Citrix ADC examina el tráfico para ver si coincide con una directiva. Por ejemplo, un punto de enlace puede ser un servidor virtual de equilibrio de carga.

Puede especificar una acción predeterminada para las solicitudes que no coincidan con ninguna directiva y puede omitir la comprobación de seguridad para las acciones que de otro modo generarían mensajes de error.

La función de reescritura de Citrix ADC ayuda a reescribir cierta información en las solicitudes o respuestas manejadas por Citrix ADC. La siguiente sección muestra algunas diferencias entre las dos

entidades.

Comparación entre las opciones de Reescritura y Responder

La principal diferencia entre la función de reescritura y la función de respondedor es la siguiente:

Responder no se puede utilizar para expresiones basadas en servidor o respuesta. Responder solo se puede utilizar para los siguientes casos en función de los parámetros del cliente:

- Redirigir una solicitud HTTP a nuevos sitios web o páginas web
- Responder con alguna respuesta personalizada
- Desechar o restablecer una conexión a nivel de solicitud

Si existe una directiva de respuesta, Citrix ADC examina la solicitud del cliente, realiza acciones de acuerdo con las directivas aplicables, envía la respuesta al cliente y cierra la conexión con el cliente.

Si existe una directiva de reescritura, Citrix ADC examina la solicitud del cliente o la respuesta del servidor, realiza acciones de acuerdo con las directivas aplicables y reenvía el tráfico al cliente o al servidor.

En general, se recomienda utilizar un respondedor si quiere que el dispositivo restablezca o elimine una conexión basada en un parámetro basado en solicitudes. Utilice un respondedor para redirigir el tráfico o responda con mensajes personalizados. Utilice la reescritura para manipular datos en solicitudes y respuestas HTTP.

Activación de la función Respondedor

October 5, 2021

Para utilizar la función Responder, primero debe habilitarla.

Para habilitar la función de respuesta mediante la CLI de Citrix ADC:

En el símbolo del sistema, escriba los siguientes comandos para habilitar la función de respuesta y verificar la configuración:

- `enable ns feature <feature>`
- `show ns feature`

Ejemplo:

```
1 enable ns feature Responder
2  Done
```



```
> show ns feature

        Feature                         Acronym             Status
        -------                         -------             ------
 1)     Web Logging                     WL                  ON
 2)     Surge Protection                SP                  ON
 .
 .
 .
 19)     Responder                       RESPONDER           ON
 20)     Citrix ADC Push                 push                OFF
 Done
>
<!--NeedCopy-->
```

Para habilitar la función de respuesta mediante la interfaz gráfica de usuario:

1. En el panel de navegación, expanda **Sistema**y, a continuación, haga clic en **Configuración**.
2. En el panel de detalles, en **Modos** y **funciones**, haga clic en **Cambiar funciones avanzadas**.
3. En el cuadro de diálogo **Configurar funciones avanzadas**, active la casilla **Responder** y, a continuación, haga clic en **Aceptar**.
4. ¿En la (s) **función (s) activar/desactivar (s)?** cuadro de diálogo, haga clic en **SÍ**. Aparece un mensaje en la barra de estado que indica que la función se ha habilitado.

Configurar acción de respuesta

October 5, 2021

Después de habilitar la función de respuesta, debe configurar una o varias acciones para gestionar las solicitudes. El respondedor admite los siguientes tipos de acciones:

- **Responda con**. Envía la respuesta definida por la expresión de Target sin reenviar la solicitud a un servidor web. (El dispositivo Citrix ADC sustituye y actúa como servidor web). Utilice este tipo de acción para definir manualmente una respuesta sencilla basada en HTML. Normalmente, el texto de una acción Responder con consiste en un código de error del servidor web y una breve página HTML.
- **Responda con SQL OK**. Envía la respuesta SQL OK designada definida por la expresión Target. Utilice este tipo de acción para enviar una respuesta SQL OK a una consulta SQL.
- **Responda con un error SQL**. Envía la respuesta de error SQL designada definida por la expresión Target. Utilice este tipo de acción para enviar una respuesta de error SQL a una consulta SQL.

- **Responda con la página HTML**. Envía la página HTML designada como respuesta. Puede elegir entre una lista desplegable de páginas HTML que se han cargado anteriormente o cargar una nueva página HTML. Utilice este tipo de acción para enviar una página HTML importada como respuesta. El dispositivo responde con un encabezado personalizado en la acción respondwithhtmlpage responder. Puede configurar hasta ocho encabezados personalizados.
- **Redireccionamiento**. Redirige la solicitud a una página web o servidor web diferente. Una acción de redireccionamiento puede redirigir las solicitudes enviadas originalmente a un sitio web "ficticio" que existe en DNS, pero para el que no existe un servidor web real, a un sitio web real. También puede redirigir las solicitudes de búsqueda a una URL adecuada. Normalmente, el destino de redirección de una acción de redireccionamiento consiste en una URL completa.

Para configurar una acción de respuesta mediante la línea de comandos de Citrix ADC:

Muestra la configuración actual de la acción de respuesta especificada. Si no se proporciona ningún nombre de acción, muestre una lista de todas las acciones de respuesta configuradas actualmente en el dispositivo Citrix ADC, con la configuración abreviada.

En el símbolo del sistema, escriba los siguientes comandos para configurar una acción de respuesta y verificar la configuración:

- `add responder action <name> <type> <target>`
- `show responder action`

Parámetros:

- **Name**. Nombre de la acción de respuesta. Longitud máxima: 127
- **tipo**. Tipo de acción de respuesta. Puede ser: (respondwith).
- **objetivo**. Expresión que especifica con qué responder
- **htmlpage**. Opción que especifica responder con html page
- **éxitos**. Número de veces que se ha realizado la acción.
- **ReferenceCount**. Número de referencias a la acción.
- **UndefHits**. El número de veces que la acción dio lugar al FNUD.
- **comentario**. Cualquier tipo de información sobre esta acción de respuesta.
- **incorporado**. Marcar para determinar si la acción de respuesta está integrada o no

Ejemplo:

```
1 To create a responder action that displays a "Not Found" error page
     for URLs that do not exist:
2
```



```
> add responder action act404Error respondWith '"HTTP/1.1 404 Not Found \r\n\r\n"+ HTTP.REQ.URL.HTTP_URL_SAFE + " does not exist on the web server."'
Done

> show responder action

1) Name: act404Error
Operation: respondwith
Target: "HTTP/1.1 404 Not Found" + HTTP.REQ.URL.HTTP_URL_SAFE + " does not exist on the web server."
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

To create a responder action that displays a "Not Found" error page for URLs that do not exist:

add responder action act404Error respondWith '"HTTP/1.1 404 Not Found\r\n\r\n"+ HTTP.REQ.URL.HTTP_URL_SAFE + " does not exist on the web server."'
Done
> show responder action

1) Name: act404Error
Operation: respondwith
Target: "HTTP/1.1 404 Not Found" + HTTP.REQ.URL.HTTP_URL_SAFE + " does not exist on the web server."
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done
<!--NeedCopy-->
```

Para modificar una acción de respuesta existente mediante la línea de comandos de Citrix ADC:

En el símbolo del sistema, escriba el siguiente comando para modificar una acción de respuesta existente y verificar la configuración:

- `set responder action <name> -target <string>`
- `show responder action`

Ejemplo:


```
set responder action act404Error  -target '"HTTP/1.1 404 Not Found\r\n\
    r\n"+ HTTP.REQ.URL.HTTP_URL_SAFE + " does not exist on the web
    server."'
 Done
> show responder action

1)      Name: act404Error
        Operation: respondwith
        Target: "HTTP/1.1 404 Not Found" + HTTP.REQ.URL.HTTP_URL_SAFE +
            " does not exist on the web server."
        Hits: 0
        Undef Hits: 0
        Action Reference Count: 0
 Done
<!--NeedCopy-->
```

Para quitar una acción de respuesta mediante la línea de comandos de Citrix ADC:

En el símbolo del sistema, escriba el siguiente comando para quitar una acción de respuesta y verificar la configuración:

- `rm responder action <name>`
- `show responder action`

Ejemplo:

```
rm responder action act404Error
 Done

> show responder action
 Done
<!--NeedCopy-->
```

Para agregar encabezados personalizados en la acción responsewithhtmlpage responder mediante la línea de comandos de Citrix ADC:

Un dispositivo Citrix ADC ahora puede responder con encabezados personalizados en la acción responsewithhtmlpage responder. Puede configurar hasta ocho encabezados personalizados. Anteriormente, el dispositivo solo respondía con encabezados estáticos `Content-type:text/html` y `Content-Length:<value>`.

> **Nota:**
>
> En la configuración de encabezados personalizados, también puede sobrescribir el valor del en-

> cabezado “Content-Type”.

En el símbolo del sistema, escriba el siguiente comando:

```
add responder action <name> <type> (<target> | <htmlpage>)[-comment <string
>] [-responseStatusCode <positive_integer>] [-reasonPhrase <expression>] [-
headers <name(value)> ...]
```

Donde:

nombre. Nombre de la acción de respuesta. Debe comenzar con una letra, un número o un carácter de guión bajo (_) y debe contener solo letras, números y guión (-), punto (.), guión (.), espacio(), at (@), igual a (=), dos puntos (:) y guión bajo. Se puede cambiar después de agregar la directiva de respuesta.

Tipo. Tipo de acción de respuesta. Los ajustes disponibles funcionan de la siguiente manera:

1. respondwith <target>: Responde a la solicitud con la expresión especificada como destino.
2. respondwithhtmlpage: responde a la solicitud con el objeto de página HTML cargado especificado como destino.
3. redirect: redirige la solicitud a la URL especificada como destino.
4. sqlresponse_ok - Envía una respuesta SQL OK.
5. sqlresponse_error - Envía una respuesta SQL ERROR. Este es un argumento obligatorio. Valores posibles: noop, respondwith, redirigir, responder con htmlpage, sqlresponse_ok, sqlresponse_error

Objetivo. Expresión que especifica con qué responder. Normalmente es una URL para directivas de redireccionamiento o una expresión de sintaxis predeterminada. Además de las expresiones de sintaxis predeterminada de Citrix ADC que hacen referencia a la información de la solicitud, una expresión de generador de cadenas puede contener texto y HTML, y códigos de escape simples que definen líneas y párrafos nuevos. Coloque cada elemento de expresión de stringbuilder (ya sea una expresión de sintaxis predeterminada de Citrix ADC o una cadena) entre comillas dobles. Usa el signo más (+) para unir los elementos.

htmlpage. En el caso de las directivas respondwithhtmlpage, nombre del objeto de página HTML que se va a utilizar como respuesta. En primer lugar, debe importar el objeto de página. Longitud máxima: 31

Comentario. Cualquier tipo de información sobre esta acción de respuesta. Longitud máxima: 255

Código de estado de respuesta. Código de estado de respuesta HTTP, por ejemplo 200, 302, 404, etc. El valor
predeterminado para el tipo de acción de redirección es 302 y para respondwithhtmlpage es 200 Valor mínimo: 100 Valor máximo: 599

reasonPhrase. Expresión que especifica la frase del motivo de la respuesta HTTP. La frase del motivo puede ser un literal de cadena con comillas o una expresión PI. Por ejemplo: “URL no válida:” + HTTP.REQ.URL Longitud máxima: 8191

Encabezados. Uno o más encabezados para insertar en la respuesta HTTP. Cada encabezado se especifica como "name (expr)", donde expr es una expresión que se evalúa en tiempo de ejecución para proporcionar el valor del encabezado con nombre. Puede configurar un máximo de ocho encabezados para una acción de respuesta.

Para configurar una acción de respuesta mediante la interfaz gráfica de usuario:

1. Vaya a **AppExpert > Responder > Acciones**.
2. En el panel de detalles, realice una de las acciones siguientes:
   - Para crear una acción, haga clic en **Agregar**.
   - Para modificar una acción existente, selecciónela y, a continuación, haga clic en **Abrir**.
3. Haga clic en **Crear** o en **Aceptar**, en función de si va a crear una acción o modificar una acción existente.
4. Haga clic en **Cerrar**. Aparece un mensaje en la barra de estado que indica que la función se ha habilitado.
5. Para eliminar una acción de respuesta, selecciónela y, a continuación, haga clic en **Quitar**. Aparece un mensaje en la barra de estado que indica que la función se ha inhabilitado.

Para agregar una expresión mediante el cuadro de diálogo **Agregar expresión**

1. En el cuadro de diálogo **Crear acción** de **respuesta o Configurar acción** de respuesta, haga clic en **Agregar**.
2. En el cuadro de diálogo **Agregar expresión**, en el primer cuadro de lista, elija el primer término de la expresión.
   - HTTP. El protocolo HTTP. Elija esta opción si quiere examinar algún aspecto de la solicitud que pertenece al protocolo HTTP.
   - DICE. Uno o varios sitios web protegidos. Elija esta opción si quiere examinar algún aspecto de la solicitud que pertenece al destinatario de la solicitud.
   - CLIENTE. El equipo que envió la solicitud. Elija esta opción si quiere examinar algún aspecto del remitente de la solicitud.
   - ANALÍTICA. Los datos analíticos asociados a la solicitud. Elija esta opción si quiere examinar los metadatos de la solicitud.
   - SORBO. Solicitud SIP. Elija esta opción si quiere examinar algún aspecto de una solicitud SIP. Al elegir, el cuadro de lista situado más a la derecha muestra los términos apropiados para la siguiente parte de la expresión.
3. En el segundo cuadro de lista, elige el segundo término para su expresión. Las elecciones dependen de la elección que haya realizado en el paso anterior y son apropiadas para el contexto. Después de hacer la segunda elección, la ventana de Ayuda situada debajo de la ventana Construir expresión (que estaba en blanco) muestra ayuda para describir el propósito y el uso del término que acaba de elegir.
4. Siga eligiendo términos en los cuadros de lista que aparecen a la derecha del cuadro de lista

anterior o escribiendo cadenas o números en los cuadros de texto que aparecen para pedirle que escriba un valor hasta que finalice la expresión.

Configuración de la acción HTTP global

Puede configurar la acción HTTP global para que invoque una acción de respuesta cuando se agote el tiempo de espera de una solicitud HTTP. Para configurar esta función, primero debe crear la acción de respuesta que quiere invocar. A continuación, configura la acción de tiempo de espera HTTP global para responder a un tiempo de espera con esa acción de respuesta.

Para configurar la acción HTTP global mediante la línea de comandos de Citrix ADC:

En el símbolo del sistema, escriba el siguiente comando:

- `set ns httpProfile -reqTimeoutAction <responder action name>`
- `save ns config`

Por `<responder action name>`, sustituya el nombre de la acción de respuesta.

Configurar importación de páginas HTML

Cuando un dispositivo Citrix ADC responde con un mensaje personalizado, podemos responder con un archivo HTML. Puede importar el archivo mediante el comando **`import`** `responder htmlpage` y, a continuación, utilizar este archivo en el comando `add responder action <act name> respondwithhtmlpage <file name>`. También puede importar el archivo a través de la GUI de Citrix ADC. Puede importar la página HTML deseada en la carpeta del dispositivo y cargarla durante el tiempo de ejecución del respondedor.

Importar página HTML mediante la CLI

En el símbolo del sistema, escriba:

```
import responder htmlpage [<src>] <name> [-comment <string>] [-overwrite][-CAcertFile <string>]
```

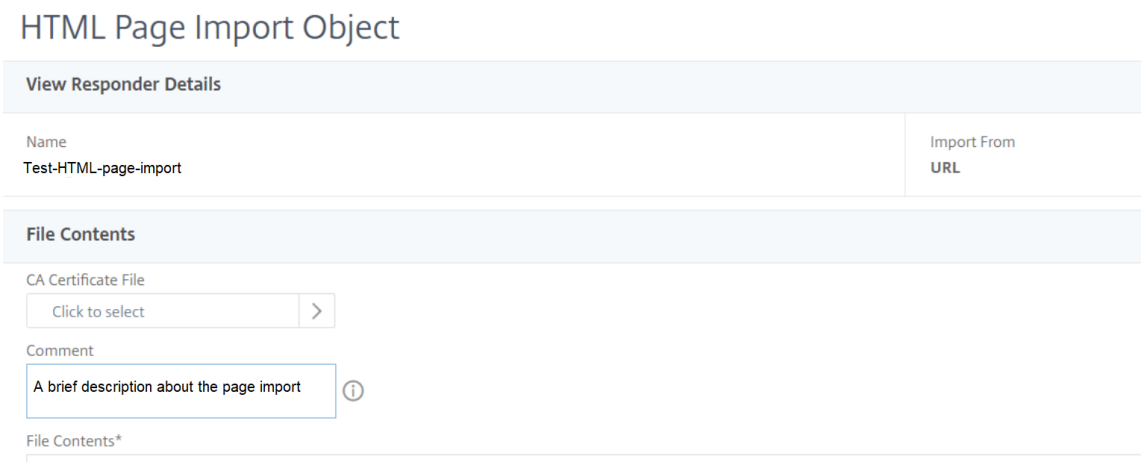
Ejemplo:

```
import responder htmlpage http://www.example.com/page.html my-responder-page -CAcertFile my_root_ca_cert
```

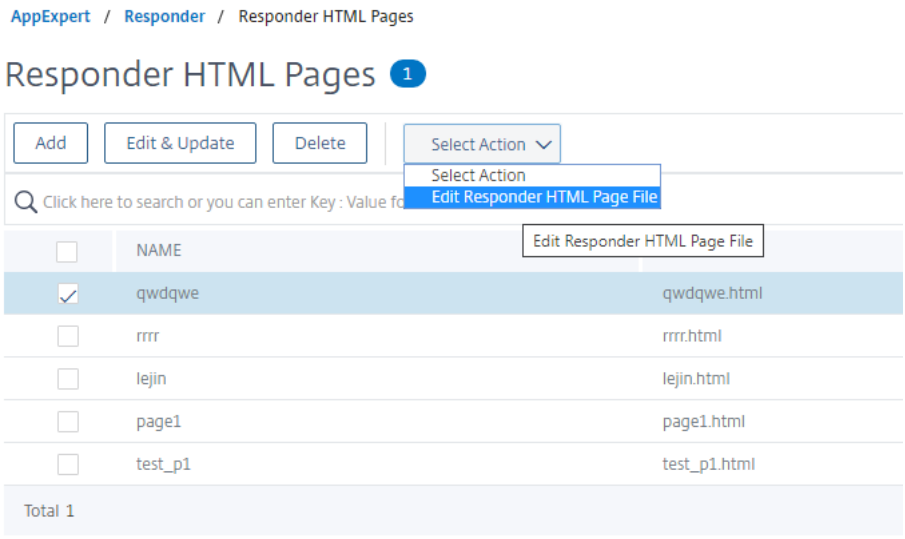
Donde:
certificado de CA se utiliza para verificar el certificado de cliente. El certificado debe importarse mediante el comando de CLI “import ssl certfile” o su equivalente a través de API o GUI. Si el nombre del certificado no está configurado, se utilizan los certificados de CA raíz predeterminados para la verificación del certificado.

Importar página HTML mediante la GUI de Citrix ADC

1. Vaya a **AppExpert** > **Responder** > **Importación de páginas HTML**.
2. En el panel de detalles de **Responder HTML Imports**, haga clic en **Agregar**.
3. En la **página Objeto de importación de página HTML**, defina los siguientes parámetros:
   a) Name. Nombre de la página HTML.
   b) Importar desde. Importado de un archivo, texto o texto.
   c) URL. Seleccione esta opción para introducir la ubicación URL del archivo HTML.
   d) archivo. Seleccione el archivo HTML del directorio del dispositivo.
   e) Texto. Seleccione el archivo HTML como texto.
4. Haga clic en **Continue**.
5. Compruebe los detalles de la página HTML del respondedor
6. Haga clic en **Done**.



Para modificar una página HTML, puede seleccionar un archivo y hacer clic en **Modificar archivo de página HTML de Responder** en la lista desplegable **Seleccionar acción** .



Configuración de una directiva de respuesta

October 5, 2021

Después de configurar una acción de respuesta, debe configurar una directiva de respuesta para seleccionar las solicitudes a las que debe responder el dispositivo Citrix ADC. Una directiva de respuesta se basa en una regla, que consiste en una o más expresiones. La regla está asociada a una acción, que se realiza si una solicitud coincide con la regla.

Nota: Para crear y administrar directivas de respuesta, la GUI proporciona asistencia que no está disponible en el símbolo del sistema de Citrix ADC.

Para configurar una directiva de respuesta mediante la línea de comandos de Citrix ADC:

En el símbolo del sistema, escriba:

- `add responder policy <name> <expression> <action> [<undefaction>]-appFlowaction <actionName>`
- `show responder policy <name>`

Ejemplo:

```
1 > add responder policyThree ”CLIENT.IP.SRC.IN_SUBNET(222.222.0.0/16)”
     RESET
2  Done
3 > show responder policyThree
4
```



```
5          Name: policyThree
6          Rule: CLIENT.IP.SRC.IN_SUBNET(222.222.0.0/16)
7          Responder Action: RESET
8          UndefAction: Use Global
9          Hits: 0
10         Undef Hits: 0
11  Done
12 <!--NeedCopy-->
```

Para modificar una directiva de respuesta existente mediante la línea de comandos de Citrix ADC:

En el símbolo del sistema, escriba:

- `set responder policy <name> [-rule <expression>] [-action <string>] [-undefAction <string>]`
- `show responder policy <name>`

Para quitar una directiva de respuesta mediante la línea de comandos de Citrix ADC:

En el símbolo del sistema, escriba:

- `rm responder policy <name>`
- `show responder policy`

Ejemplo:

```
1 >rm responder policy pol404Error
2  Done
3
4 > show responder policy
5  Done
6 <!--NeedCopy-->
```

Para configurar una directiva de respuesta mediante la interfaz gráfica de usuario:

1. Vaya a **AppExpert > Responder > Directivas**.
2. En el panel de detalles, realice una de las acciones siguientes:
   - Para crear una nueva directiva, haga clic en **Agregar**.
   - Para modificar una directiva existente, selecciónela y, a continuación, haga clic en **Abrir**.
3. Haga clic en **Crear** o en **Aceptar**, en función de si va a crear una nueva directiva o modificar una directiva existente.
4. Haga clic en **Cerrar**. Aparece un mensaje en la barra de estado que indica que la función se ha configurado.

Vincular una directiva de respuesta

February 19, 2022

Para poner en práctica una directiva, debe vincularla globalmente, de modo que se aplique a todo el tráfico que fluye a través del dispositivo Citrix ADC, o a un servidor virtual específico, de modo que la directiva se aplique únicamente a las solicitudes cuya dirección IP de destino sea el VIP de ese servidor virtual.

Cuando vincula una directiva, le asigna una prioridad. La prioridad determina el orden en que se evalúan las directivas que defina. Puede establecer la prioridad en cualquier número entero positivo.

En el sistema operativo Citrix ADC, las prioridades de directivas funcionan en orden inverso: Mayor sea el número, menor será la prioridad. Por ejemplo, si tiene tres directivas con prioridades de 10, 100 y 1000, la directiva asignada a una prioridad de 10 se ejecuta primero, luego a la directiva se le asigna una prioridad de 100 y, por último, a la directiva se le asigna un orden de 1000. La función de respuesta implementa solo la primera directiva que coincide con una solicitud, no las directivas adicionales que también podría coincidir, por lo que la prioridad de la directiva es importante para obtener los resultados que pretende.

Puede dejar mucho espacio para agregar otras directivas en cualquier orden y configurarlas para evaluarlas en el orden que quiera, estableciendo prioridades con intervalos de 50 o 100 entre cada directiva cuando la vincule globalmente. A continuación, puede agregar más directivas en cualquier momento sin tener que reasignar la prioridad de una directiva existente.

Para obtener información adicional sobre las directivas de enlace en Citrix ADC, consulte Directivas y expresiones.

> **Nota:**
>
> Las directivas de respuesta están vinculadas a servidores virtuales basados en TCP.

Para enlazar globalmente una directiva de Responder mediante la línea de comandos de Citrix ADC:

En el símbolo del sistema, escriba el siguiente comando para enlazar globalmente una directiva de respuesta y verificar la configuración:

- `bind responder global <policyName> <priority> [<gotoPriorityExpression> [-type <type>] [-invoke (<labelType> <labelName>)]`
- `show responder global`

Ejemplo:

```
1 > bind responder global poliError 100
2  Done
```



```
> show responder global
1)      Global bindpoint: REQ_DEFAULT
        Number of bound policies: 1

 Done
<!--NeedCopy-->
```

Para enlazar la directiva de Responder a un servidor virtual específico mediante la línea de comandos de Citrix ADC:

En el símbolo del sistema, escriba:

- `bind lb vserver <name> -policyname <policy_name> -priority <priority>`
- `show lb vserver vs-loadbal <name>`

Ejemplo:

```
> bind lb vserver vs-loadbal -policyName policyTwo -priority 100
 Done
> show lb vserver
1)      vs-loadbal (10.102.29.20:80) - HTTP     Type: ADDRESS
        State: OUT OF SERVICE
        Last state change was at Wed Aug 19 09:05:47 2009 (+211 ms)
        Time since last state change: 2 days, 00:58:03.260
        Effective State: DOWN
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Port Rewrite : DISABLED
        No. of Bound Services :  0 (Total)       0 (Active)
        Configured Method: LEASTCONNECTION
        Mode: IP
        Persistence: NONE
        Vserver IP and Port insertion: OFF
        Push: DISABLED  Push VServer:
        Push Multi Clients: NO
        Push Label Rule: none
2)      vs-cont-sw (0.0.0.0:0) - TCP    Type: ADDRESS
        State: DOWN
        Last state change was at Wed Aug 19 10:03:46 2009 (+213 ms)
        Time since last state change: 2 days, 00:00:04.260
        Effective State: DOWN
        Client Idle Timeout: 9000 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
```



```
29          No. of Bound Services :  0 (Total)       0 (Active)
30          Configured Method: LEASTCONNECTION
31          Mode: IP
32          Persistence: NONE
33          Connection Failover: DISABLED
34  Done
35 <!--NeedCopy-->
```

Para enlazar globalmente una directiva de respuesta mediante la interfaz gráfica de usuario:

1. Vaya a **AppExpert** > **Respondedor** > **Directivas**.
2. En la página **Directivas de Responder**, seleccione una directiva de Responder y, a continuación, haga clic en **Administrador de directivas**.
3. En el cuadro de diálogo **Administrador de directivas de Responder** menú Puntos de enlace, seleccione Global predeterminada.
4. Haga clic en **Insertar directiva** para insertar una nueva fila y mostrar una lista desplegable de todas las directivas de respuesta independientes.
5. Haga clic en una de las directivas de la lista. Esa directiva se inserta en la lista de directivas de respuesta enlazadas globalmente.
6. Haga clic en **Aplicar cambios**.
7. Haga clic en **Cerrar**. Aparece un mensaje en la barra de estado que indica que la configuración se ha completado correctamente.

Para enlazar una directiva de respuesta a un servidor virtual específico mediante la interfaz gráfica de usuario:

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**.
2. En la página **Servidores virtuales de equilibrio de carga**, seleccione el servidor virtual al que quiere enlazar la directiva de respuesta y, a continuación, haga clic en **Abrir**.
3. En el cuadro de diálogo **Configurar servidor virtual** (equilibrio de carga), seleccione la ficha **Directivas**, que muestra una lista de todas las directivas configuradas en el dispositivo Citrix ADC.
4. Seleccione la casilla de verificación situada junto al nombre de la directiva que quiere enlazar a este servidor virtual.
5. Haga clic en **OK**. Aparece un mensaje en la barra de estado que indica que la configuración se ha completado correctamente.

Configuración de la acción predeterminada para una directiva de respondedor

August 20, 2021

El dispositivo Citrix ADC genera un evento no definido (evento UNDEF) cuando una solicitud no coincide con una directiva de respuesta. A continuación, el dispositivo realiza la acción predeterminada asignada a eventos no definidos. De forma predeterminada, la acción reenvía la solicitud a la siguiente función, como equilibrio de carga, filtrado de contenido, etc. Este comportamiento predeterminado garantiza que las solicitudes no requieren ninguna acción de respuesta específica para enviarse a los servidores web. Además, los clientes reciben acceso al contenido que han solicitado.

Sin embargo, si uno o varios sitios web que protege el dispositivo Citrix ADC reciben un número significativo de solicitudes no válidas o malintencionadas, es posible que quiera cambiar la acción predeterminada para restablecer la conexión del cliente o eliminar la solicitud. En este tipo de configuración, escribiría una o más directivas de respuesta que coincidieran con cualquier solicitud legítima y simplemente redirigirlas a sus destinos originales. A continuación, su dispositivo Citrix ADC bloquearía cualquier otra solicitud según lo especificado por la acción predeterminada que haya configurado.

Puede asignar cualquiera de las siguientes acciones a un evento indefinido:

- **NOOP**. La acción NOOP aborta el procesamiento de respondedor pero no altera el flujo del paquete. De modo que el dispositivo continúe procesando solicitudes que no coinciden con ninguna directiva de respuesta y, finalmente, las reenvía a la dirección URL solicitada a menos que interviene otra función y bloquee o redirija la solicitud. Esta acción es apropiada para las solicitudes normales a los servidores web y es la configuración predeterminada.
- **RESTABLECER**. Si la acción indefinida se establece en RESTABLECER, el dispositivo restablece la conexión del cliente e informa al cliente de que debe restablecer su sesión con el servidor web. La acción es adecuada para solicitudes repetidas de páginas web que no existen, o para conexiones que podrían ser intentos de hackear o sondear sus sitios web protegidos.
- **DROP**. Si la acción indefinida se establece en DROP, el dispositivo descarta la solicitud de forma silenciosa sin responder al cliente de ninguna manera. Esta acción es apropiada para las solicitudes que parecen formar parte de un ataque DDoS u otro ataque sostenido en los servidores.

Nota: Los eventos UNDEF se activan solo para las solicitudes de los clientes. No se activan eventos del UNDEF para las respuestas.

Para establecer la acción indefinida mediante la línea de comandos de Citrix ADC:

En el símbolo del sistema, escriba el siguiente comando para establecer la acción indefinida y verificar la configuración:

- `set responder param -undefAction (RESET|DROP|NOOP)[-timeout <msecs>]`
- `show responder param`

Donde:

timeout: Tiempo máximo en milisegundos para permitir el procesamiento de todas las directivas y sus acciones seleccionadas sin interrupción. Si se alcanza el tiempo de espera, la evaluación hace que se

eleve un Fondo de las Naciones Unidas para el Medio Entorno y no se realiza ningún procesamiento posterior.

Valor mínimo: 1

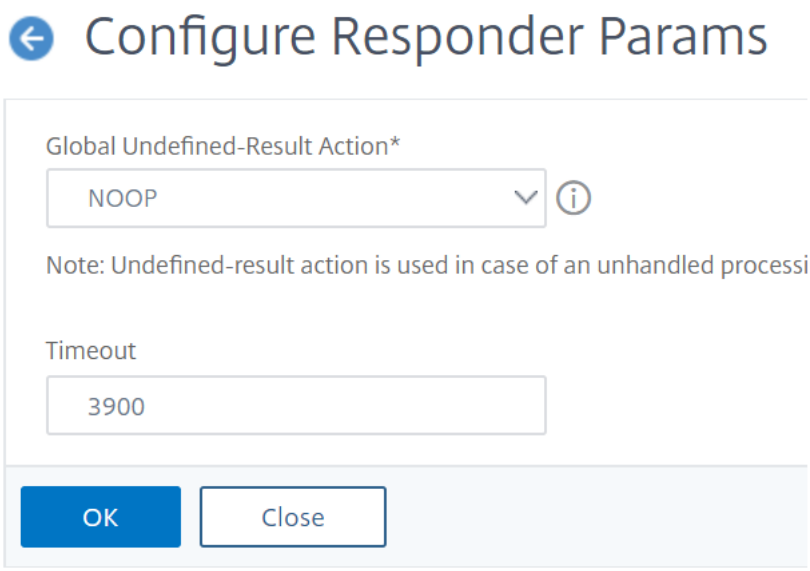
Valor máximo: 5000

Ejemplo:

```
>set responder param -undefAction RESET -timeout 3900
 Done
> show responder param
Action Name: RESET
Timeout: 3900
 Done
>
<!--NeedCopy-->
```

Establecer la acción indefinida mediante la GUI

1. Vaya a **AppExpert** > **Responder** y, a continuación, en **Configuración**, haga clic en el vínculo **Cambiar configuración de respondedor**.
2. En la página **Definir Parámetros de Respondedor**, establezca los siguientes parámetros:
   a) Acción global de resultados indefinidos. La acción de resultado no definido se prefiere en una excepción de procesamiento no controlado en las directivas y acciones de respuesta. Seleccione **NOOP**, **RESET**o **DROP**.
   b) Tiempo de espera. Tiempo máximo en milisegundos para permitir el procesamiento de todas las directivas y sus acciones seleccionadas sin interrupción. Si se alcanza el tiempo de espera, la evaluación hace que se eleve un Fondo de las Naciones Unidas para el Medio Entorno y no se realiza ningún procesamiento posterior.
3. Haga clic en **Aceptar**.



Ejemplos de directivas y acciones de respuesta

January 21, 2022

Las acciones y directivas de respuesta son poderosas y complejas, pero puede comenzar con aplicaciones relativamente simples.

Ejemplo: bloqueo del acceso desde direcciones IP especificadas

Los siguientes procedimientos bloquean el acceso a su (s) sitio (s) web protegido (s) por parte de los clientes originados en el CIDR 222.222.0.0/16. El respondedor envía un mensaje de error que indica que el cliente no está autorizado a acceder a la URL solicitada.

Para bloquear el acceso mediante la línea de comandos de Citrix ADC:

En el símbolo del sistema, escriba los siguientes comandos para bloquear el acceso:

- add responder action act_unauthorized responder con “HTTP/1.1 403 Forbidden\ r\ n\ r\ n” + “Cliente:” + CLIENT.IP.SRC + “no está autorizado para acceder a la URL:” + “HTTP.REQ.URL.HTTP_URL_SAFE”’
- agregar directiva de respuesta pol_un “CLIENT.IP.SRC.IN_SUBNET (222.222.0.0/16)” act_unauthorized
- bind respondedor global pol_un 10

Para bloquear el acceso mediante la interfaz gráfica de usuario:

1. En el panel de navegación, expanda **Responder**y, después, haga clic en **Acciones**.

2. En el panel de detalles, haga clic en **Agregar**.
3. En el cuadro de diálogo **Crear acción de respuesta**, haga lo siguiente:
   a) En el cuadro de texto **Nombre**, escriba act_unauthorized.
   b) En Tipo, selecciona Responder con.
   c) En el área de texto Target, escriba la siguiente cadena: "HTTP/1.1 403 Forbidden\ r\ n\ r\ n" + "Cliente:" + CLIENT.IP.SRC + "no está autorizado a acceder a la URL:" + HTTP.REQ.URL.HTTP_URL_SAFE
   d) Haga clic en **Crear** y, a continuación, en **Cerrar**.
   La acción de respuesta que configuró, denominada act_unauthorized, ahora aparece en la página **Acciones de respuesta**.
4. En el panel de navegación, haga clic en **Directivas**.
5. En el panel de detalles, haga clic en **Agregar**.
6. En el cuadro de diálogo **Crear directiva de respuesta**, haga lo siguiente:
   a) En el cuadro de texto Nombre, escriba pol_unauthorized.
   b) En **Acción**, selecciona act_unauthorized.
   c) En la ventana **Expresión**, escriba la siguiente regla: CLIENT.IP.SRC.IN_SUBNET (222.222.0.0/16)
   d) Haga clic en **Crear** y, luego, en **Cerrar**.
   La directiva de Responder configurada, denominada pol_unauthorized, aparece ahora en la página **Directivas de Responder**.
7. Vincule globalmente su nueva directiva, pol_unauthorized, como se describe en Vincular una directiva de respuesta.

Ejemplo: Redirigir un cliente a una nueva dirección URL

Los siguientes procedimientos redirigen a los clientes que acceden a su (s) sitio (s) Web protegido (s) desde el CIDR 222.222.0.0/16 a una URL especificada.

Para redirigir a los clientes mediante la línea de comandos de Citrix ADC:

En el símbolo del sistema, escriba los siguientes comandos para redirigir a los clientes y verificar la configuración:

- agregar acción de respuesta redirección act_redirect "<http://www.example.com/404.html>"
- mostrar acción de respuesta act_redirect
- agregar directiva de respuesta pol_redirect "CLIENT.IP.SRC.IN_SUBNET (222.222.0.0/16)" act_redirect
- mostrar directiva de respuesta pol_redirect
- respuesta de enlace global pol_redirect 10

Ejemplo:


```
> add responder action act_redirect redirect `" http ://www.example.com
    /404.html "`
Done

> add responder policy pol_redirect "CLIENT.IP.SRC.IN_SUBNET
    (222.222.0.0/16)" act_redirect
Done
<!--NeedCopy-->
```

Para redirigir a los clientes mediante la GUI:

1. Vaya a **AppExpert** > **Responder** > **Acciones**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En el cuadro de diálogo **Crear acción de respuesta**, haga lo siguiente:
   a) En el cuadro de texto **Nombre**, escriba act_redirect.
   b) En Tipo, selecciona **Redirigir**.
   c) En el área de texto **Target**, escriba la siguiente cadena: "<http://www.example.com/404.html>"
   d) Haga clic en **Crear** y, luego, en **Cerrar**.
   La acción de respuesta que configuró, denominada act_redirect, ahora aparece en la página **Acciones de respuesta**.
4. En el panel de navegación, haga clic en **Directivas**.
5. En el panel de detalles, haga clic en **Agregar**.
6. En el cuadro de diálogo **Crear directiva de respuesta**, haga lo siguiente:
   a) En el cuadro de texto **Nombre**, escriba pol_redirect.
   b) En **Acción**, selecciona act_redirect.
   c) En la ventana **Expresión**, escriba la siguiente regla: CLIENT.IP.SRC.IN_SUBNET (222.222.0.0/16)
   d) Haga clic en **Crear** y, luego, en **Cerrar**.
   La directiva de Responder configurada, denominada pol_redirect, aparece ahora en la página **Directivas de Responder**.
7. Vincule globalmente su nueva directiva, pol_redirect, como se describe en Vinculación de una directiva de respuesta.

Funcionalidad de Diameter para Responder

January 12, 2021

La función Responder ahora es compatible con el protocolo Diameter. Puede configurar Responder

para que responda a las solicitudes de Diameter como lo hace las solicitudes HTTP y TCP. Por ejemplo, puede configurar Responder para que responda a las solicitudes de un origen de Diameter específico con una redirección a una página web mejorada para dispositivos móviles. Se han agregado varias expresiones Citrix ADC que admiten el examen del encabezado Diameter y los pares atributo-valor (AVP). Estas expresiones admiten la búsqueda de AVP específicos por índice, ID o nombre, examinan la información de cada AVP y envían una respuesta adecuada.

Para configurar Responder para que responda a una solicitud de Diameter:

En el símbolo del sistema, escriba los siguientes comandos:

- `add responder action <actname> RESPONDWITH "DIAMETER.NEW_REDIRECT(\"aaa://host.example.com\")"`

  Para, <actname>sustituya un nombre para la nueva acción. El nombre puede constar de entre uno y 127 caracteres de longitud y puede contener letras, números y símbolos de guión (-) y guión bajo (_). Para aaa://host.example.com, sustituya la dirección URL del anfitrión de Diameter al que quiere redirigir las conexiones.

- add responder policy <polname> "diameter.req.avp(264).value.eq("host1.example.net")" <actname>

  Para <polname>, sustituya un nombre para la nueva directiva. Al igual que en el caso de <actname>, el nombre puede constar de entre uno y 127 caracteres de longitud, y puede contener letras, números y los símbolos de guión (-) y guión bajo (_). Para host1.example.net, sustituya el nombre del host de origen de las solicitudes que quiere redirigir. Para <actname>, sustituya el nombre de la acción que acaba de crear.

- `bind lb vserver <vservername> -policyName <polname> -priority <priority> -type REQUEST`

  Para <vservername>, sustituya el nombre del servidor virtual de equilibrio de carga al que quiere enlazar la directiva. Para <polname>, sustituya el nombre de la directiva que acaba de crear. Para <priority>, sustituya la directiva por una prioridad.

Ejemplo:

Para crear una acción Responder y una directiva para responder a las solicitudes de Diameter que se originan en "host1.example.net" con una redirección a "host.example.com", puede agregar la siguiente acción y directiva y enlazar la directiva como se muestra.

```
1 > add responder action act_resp-dm-redirect RESPONDWITH "DIAMETER.
     NEW_REDIRECT("aaa://host.example.com")"
2 Done
3
```



```
> add responder pol_resp-dm-redirect "diameter.req.avp(264).value.eq("
    host1.example.net")" act_resp-dm-redirect
Done

> bind lb vserver vs1 -policyName pol_resp-dm-redirect -priority 10 -
    type REQUEST
Done
<!--NeedCopy-->
```

Soporte RADIUS para Respondedor

August 20, 2021

El lenguaje de expresiones Citrix ADC contiene expresiones que pueden extraer información de solicitudes RADIUS y manipularlas. Estas expresiones permiten utilizar la función Responder para responder a las solicitudes RADIUS. Las directivas y acciones de respuesta pueden utilizar cualquier expresión que sea apropiada o relevante para una solicitud RADIUS. Las expresiones disponibles permiten identificar el tipo de mensaje RADIUS, extraer cualquier par atributo-valor (AVP) de la conexión y enviar respuestas diferentes sobre la base de esa información. También puede crear etiquetas de directiva que invoquen todas las directivas de Responder para conexiones RADIUS.

Puede utilizar expresiones RADIUS para crear respuestas simples que no requieran comunicación con el servidor RADIUS al que se envió la solicitud. Cuando una directiva de Responder coincide con una conexión, Citrix ADC construye y envía la respuesta RADIUS apropiada sin ponerse en contacto con el servidor de autenticación RADIUS. Por ejemplo, si la dirección IP de origen de una solicitud RADIUS proviene de una subred especificada en la directiva de respuesta, Citrix ADC puede responder a esa solicitud con un mensaje de rechazo de acceso o simplemente eliminar la solicitud.

También puede crear etiquetas de directiva para enrutar tipos específicos de solicitudes RADIUS a través de una serie de directivas adecuadas para dichas solicitudes.

Nota: Las expresiones RADIUS actuales no funcionan con atributos RADIUS IPv6.

La documentación de Citrix ADC para expresiones compatibles con RADIUS asume la familiaridad con la estructura básica y el propósito de las comunicaciones RADIUS. Si necesita más información sobre RADIUS, consulte la documentación del servidor RADIUS o busque en línea una introducción al protocolo RADIUS.

Configuración de directivas de Responder para RADIUS

En el siguiente procedimiento se utiliza la línea de comandos de Citrix ADC para configurar una acción y una directiva de respuesta y enlazar la directiva a un punto de enlace global específico de RADIUS.

Para configurar una acción y una directiva Responder y enlazar la directiva:

En el símbolo del sistema, escriba los siguientes comandos:

- `add responder action <actName> <actType>`
- `add responder policy <polName> <rule> <actName>`
- `bind responder policy <polName> <priority> <nextExpr> -type <bindPoint>` donde `<bindPoint>` representa uno de los puntos de enlace globales específicos de RADIUS.

Expresiones RADIUS para Responder

En una configuración de Responder, puede utilizar las siguientes expresiones Citrix ADC para hacer referencia a varias partes de una solicitud RADIUS.

Identificación del tipo de conexión:

- RADIUS.IS_CLIENT. Devuelve TRUE si la conexión es un mensaje de cliente (solicitud) RADIUS.
- RADIUS.IS_SERVER. Devuelve TRUE si la conexión es un mensaje de servidor RADIUS (respuesta).

Expresiones de solicitud:

- `RADIUS.REQ.CODE`. Devuelve el número que corresponde al tipo de solicitud RADIUS. Una derivada de la clase num_at. Por ejemplo, una solicitud de acceso RADIUS devolvería 1 (uno). Una solicitud de contabilidad RADIUS devolvería 4.
- `RADIUS.REQ.LENGTH`. Devuelve la longitud de la solicitud RADIUS, incluido el encabezado. Una derivada de la clase num_at.
- `RADIUS.REQ.IDENTIFIER`. Devuelve el identificador de solicitud RADIUS, un número asignado a cada solicitud que permite que la solicitud coincida con la respuesta correspondiente. Una derivada de la clase num_at.
- `RADIUS.REQ.AVP(<AVP Code No>).VALUE`. Devuelve el valor de la primera aparición de este AVP como una cadena de tipo text_t.
- `RADIUS.REQ.AVP(<AVP code no>).INSTANCE(instance number)`. Devuelve la instancia especificada del AVP como una cadena de tipo RAVP_T. Un AVP RADIUS específico puede aparecer varias veces en un mensaje RADIUS. INSTANCE (0) devuelve la primera instancia, INSTANCE (1) devuelve la segunda instancia, y así sucesivamente, hasta dieciséis instancias.
- `RADIUS.REQ.AVP(<AVP code no>).VALUE(instance number)`. Devuelve el valor de la instancia especificada del AVP como una cadena de tipo text_t.
- `RADIUS.REQ.AVP(<AVP code no>).COUNT`. Devuelve el número de instancias de un AVP específico en una conexión RADIUS, como un entero.
- `RADIUS.REQ.AVP(<AVP code no>).EXISTS`. Devuelve TRUE si el tipo especificado de AVP existe en el mensaje, o FALSE si no lo hace.

Expresiones de respuesta:

Las expresiones de respuesta RADIUS son idénticas a las expresiones de solicitud RADIUS, excepto que RES reemplaza a REQ.

Cast tipografía de los valores AVP:

El ADC admite expresiones para convertir valores AVP RADIUS en los tipos de datos de texto, entero, entero sin signo, largo, sin signo, dirección IPv4, dirección ipv6, prefijo ipv6 y tiempo. La sintaxis es la misma que para otras expresiones de conversión de tipos de Citrix ADC.

Ejemplo:

El ADC admite expresiones para convertir valores AVP RADIUS en los tipos de datos de texto, entero, entero sin signo, largo, sin signo, dirección IPv4, dirección ipv6, prefijo ipv6 y tiempo. La sintaxis es la misma que para otras expresiones de conversión de tipos de Citrix ADC.

```
RADIUS.REQ.AVP(8).VALUE(0).typecast_ip_address_at
<!--NeedCopy-->
```

Expresiones de tipo AVP:

Citrix ADC admite expresiones para extraer valores AVP de RADIUS mediante los códigos enteros asignados descritos en RFC2865 y RFC2866. También puede utilizar alias de texto para realizar la misma tarea. A continuación se presentan algunos ejemplos.

- RADIUS.REQ.AVP (1).VALUE o Radius.REQ.UserName.Value. Extrae el valor de nombre de usuario RADIUS.
- RADIUS.REQ.AVP (4). VALUE o RADIUS.REQ. acct_session_id.value. Extrae el AVP ACCT-session-ID (código 44) del mensaje.
- RADIUS.REQ.AVP (26). VALUE o RADIUS.REQ.VENDOR_SPECCI.VALUE. Extrae el valor específico del proveedor.

Los valores de los AVP RADIUS más utilizados se pueden extraer de la misma manera.

Puntos de enlace RADIUS:

Hay cuatro puntos de enlace globales disponibles para las directivas que contienen expresiones RADIUS.

- RADIUS_REQ_OVERRIDE. Prioridad o anulación de la cola de directivas de solicitud.
- RADIUS_REQ_DEFAULT. Cola de directivas de solicitudes estándar.
- RADIUS_RES_OVERRIDE. Prioridad o anulación de la cola de directivas de respuesta.
- RADIUS_RES_DEFAULT. Cola de directivas de respuesta estándar.

Expresiones específicas de la respuesta RADIUS:

- RADIUS_RESPONDWITH. Responda con la respuesta RADIUS especificada. La respuesta se crea con expresiones Citrix ADC, tanto expresiones RADIUS como cualquier otra que sea aplicable.

- RADIUS.NUEVO_RESPUESTA. Envía una nueva respuesta RADIUS al usuario.
- RADIUS.NEW_ACCESSREJECT. Rechaza la solicitud RADIUS.
- RADIUS.NEW_AVP. Agrega el nuevo AVP especificado a la respuesta.

Casos de uso

Los siguientes son los casos de uso para RADIUS con Responder.

Bloqueo de solicitudes RADIUS desde una red específica

Para configurar la función de respuesta para bloquear las solicitudes de autenticación de una red específica, comience por crear una acción de respuesta que rechace las solicitudes. Utilice la acción en una directiva que seleccione las solicitudes de las redes que quiere bloquear. Enlazar la directiva de respuesta a un punto de enlace global específico de RADIUS, especificando:

- La prioridad
- FIN como valor NextExpr, para asegurarse de que la evaluación de directivas se detiene cuando se coincide con esta directiva
- RADIUS_REQ_OVERRIDE como la cola a la que se asigna la directiva, de modo que se evalúe antes que las directivas asignadas a la cola predeterminada

Para configurar Responder para bloquear los inicios de sesión de una red específica**

- `add responder action <actName> <actType>`
- `add responder policy <polName> <rule> <actName>`
- `bind responder global <polName> <priority> <nextExpr> -type <bindPoint>`

Ejemplo:

```
1 > add responder action rspActRadiusReject respondwith radius.
     new_accessreject
2 Done
3
4 > add responder policy rspPolRadiusReject client.ip.src.in_subnet
     (10.224.85.0/24) rspActRadiusReject
5 Done
6
7 > bind responder global rspPolRadiusReject 1 END -type
     RADIUS_REQ_OVERRIDE
8 <!--NeedCopy-->
```


Compatibilidad con DNS para la función Respondedor

January 12, 2021

Puede configurar la función de respuesta para responder a las solicitudes DNS como lo hace a las solicitudes HTTP y TCP. Por ejemplo, podría configurarlo para enviar respuestas DNS a través de UDP y asegurarse de que las solicitudes DNS del cliente se envían a través de TCP. Varias expresiones Citrix ADC admiten el examen del encabezado DNS en la solicitud. Estas expresiones examinan campos de encabezado específicos y envían una respuesta adecuada.

- **Expresiones DNS**. En una configuración de Responder, puede utilizar las siguientes expresiones Citrix ADC para hacer referencia a varias partes de una solicitud DNS:

Expresiones	Descripciones
DNS.NEW_RESPONSE	Crea una nueva respuesta DNS vacía basada en la solicitud.
DNS.NEW_RESPONSE <AA, TC, rcode>	Crea una nueva respuesta DNS basada en los parámetros especificados.

- **Puntos de enlace DNS**. Los siguientes puntos de enlace globales están disponibles para las directivas que contienen expresiones DNS.

Puntos de enlace	Descripciones
DNS_REQ_OVERRIDE	Prioridad o anulación de la cola de directivas de solicitud.
DNS_REQ_DEFAULT	Cola de directivas de solicitudes estándar.

  Además de los puntos de enlace predeterminados, puede crear etiquetas de directiva de tipo DNS y enlazar directivas de DNS a ellos.

Configuración de directivas de Responder para DNS

En el procedimiento siguiente se utiliza la línea de comandos de Citrix ADC para configurar una acción y una directiva de respuesta y enlazar la directiva a un punto de enlace global específico de la respuesta.

Para configurar Responder para que responda a una solicitud DNS:

En el símbolo del sistema, escriba los siguientes comandos:

1. `add responder action <actName> <actType>`

   Para, `<actname>`sustituya un nombre para la nueva acción. El nombre puede tener entre 1 y 127 caracteres y puede contener letras, números, guiones (-) y símbolos de subrayado (_). Para`<actType>`, sustituya un tipo de acción de *respuesta, RespondWith*.

2. `add responder policy <polName> <rule> <actName>`

   Para `<polname>`, sustituya un nombre para la nueva directiva. Para`<actname>`, el nombre puede tener entre 1 y 127 caracteres y puede contener símbolos de letras, números, guión (-) y guión bajo (_). Para `<actname>`, sustituya el nombre de la acción que acaba de crear.

3. `bind responder policy <polName> <priority> <nextExpr> -type <bindPoint>`

   Para`<bindPoint>`, especifique uno de los puntos de enlace globales específicos de la respuesta. Para`<polName>`, sustituya el nombre de la directiva que acaba de crear. Para`<priority>`, especifique la prioridad de la directiva.

Configuración de ejemplo: Aplique todas las solicitudes DNS a través de TCP:

Para aplicar todas las solicitudes DNS a través de TCP, cree una acción de respuesta que establezca el bit TC y rcode como NOERROR.

```
> add responder action resp_act_set_tc_bit respondwith DNS.NEW_RESPONSE
    (true, true, NOERROR)
Done

> add responder policy enforce_tcp  dns.REQ.TRANSPORT.EQ(udp)
    resp_act_set_tc_bit
Done

>bind lb vserver dns_udp  - policyName  enforce_tcp   -type request  -
    priority 100
Done
<!--NeedCopy-->
```

Soporte MQTT para el respondedor

January 12, 2021

La función Respondedor admite el protocolo MQTT. Puede configurar directivas de respuesta para realizar una acción basada en los parámetros del mensaje MQTT entrante.

La acción responde con cualquiera de las siguientes opciones a una nueva conexión:

- DROP
- RESTABLECER
- NOOP
- Una acción de respuesta para iniciar una nueva respuesta MQTT CONNACK.

Configuración de directivas de respuesta para MQTT

Después de habilitar la función respondedor, debe configurar una o más acciones para gestionar las solicitudes MQTT. A continuación, configure una directiva de respuesta. Puede enlazar las directivas de respuesta globalmente, o a un servidor virtual de equilibrio de carga específico o servidor virtual de conmutación de contenido.

Los siguientes puntos de enlace están disponibles para enlazar las directivas de respuesta globalmente:

- MQTT_REQ_DEFAULT
- MQTT_REQ_OVERRIDE
- MQTT_JUMBO_REQ_DEFAULT
- MQTT_JUMBO_REQ_OVERRIDE

Los siguientes puntos de enlace están disponibles para enlazar las directivas de respuesta a un servidor virtual de conmutación de contenido o equilibrio de carga:

- PETICIÓN
- MQTT_JUMBO_REQ (este punto de enlace se utiliza solo para paquetes Jumbo)

Para configurar el respondedor para responder a una solicitud MQTT mediante CLI

En el símbolo del sistema, escriba los siguientes comandos:

Configurar una acción de respuesta.

```
1 add responder action <actName> <actType>
2 <!--NeedCopy-->
```

- Para, `actname`sustituya un nombre para la nueva acción. El nombre puede tener de 1 a 127 caracteres de longitud y puede contener letras, números, guiones (-) y guión bajo (_).
- Por `actType`, sustituya un tipo de acción respondedor, respondwith.

Ejemplo:


```
1 add responder action mqtt_connack_unsup_ver respondwith MQTT.
     NEW_CONNACK(132)
2 <!--NeedCopy-->
```

Configurar una directiva de respuesta. El dispositivo Citrix ADC responde a las solicitudes MQTT seleccionadas por esta directiva de respuesta.

```
1 add responder policy <polName> <rule> <actname>
2 <!--NeedCopy-->
```

- Para `polname`, sustituya un nombre para la nueva directiva.
- Por `actname`, sustituya el nombre de la acción que ha creado.

Ejemplo:

```
1 add responder policy reject_lower_version "MQTT.HEADER.COMMAND.EQ(
     CONNECT) && MQTT.VERSION.LT(3)" mqtt_connack_unsup_ver
2 <!--NeedCopy-->
```

Enlazar la directiva de respuesta a un servidor virtual de equilibrio de carga específico o a un servidor virtual de conmutación de contenido específico. La directiva solo se aplica a las solicitudes MQTT cuya dirección IP de destino es el VIP de ese servidor virtual.

```
1 bind lb vserver <name> -policyName <policy_name> -priority <priority>
2
3 bind cs vserver <name> -policyName <policy_name> -priority <priority>
4 <!--NeedCopy-->
```

- Por `policy_name`, sustituya el nombre de la directiva que ha creado.
- Para`priority`, especifique la prioridad de la directiva.

Ejemplo:

```
1 bind lb vserver lb1 -policyName reject_lower_version -priority 50
2
3 bind cs vserver mqtt_frontend_cs -policyName reject_lower_version -
     priority 5
4 <!--NeedCopy-->
```


Caso de uso 1: Filtrar clientes en función del nombre de usuario o ID de cliente

El administrador puede configurar una directiva de respuesta de MQTT para rechazar la conexión basándose en el nombre de usuario o Id. de cliente en el mensaje MQTT CONNECT.

Ejemplo de configuración para filtrar clientes en función del ID de cliente

```
add policy patset filter_clients
bind policy patset filter_clients client1

add responder action mqtt_connack_invalid_client respondwith MQTT.
    NEW_CONNACK(2)

add responder policy reject_clients "MQTT.HEADER.COMMAND.EQ(CONNECT) &&
     mqtt.connect.clientid.equals_any("filter_clients")"
    mqtt_connack_invalid_client

bind cs vserver mqtt_frontend_cs -policyName reject_clients -priority 5
<!--NeedCopy-->
```

Caso de uso 2: Limite la longitud máxima de mensajes MQTT para manejar paquetes jumbo

El administrador puede configurar una directiva de respuesta de MQTT para eliminar la conexión del cliente si la longitud del mensaje excede un determinado umbral, o tomar las medidas necesarias en función del requisito.

Para manejar paquetes jumbo, las directivas de respuesta con cualquiera de los siguientes patrones de regla están enlazadas al punto de enlace jumbo:

- MQTT.MESSAGE_LENGTH
- MQTT.COMANDO
- MQTT.FROM_CLIENT
- MQTT.FROM_SERVER

Las directivas vinculadas a puntos de enlace jumbo se evalúan solo para paquetes jumbo.

Configuración de ejemplo para limitar la longitud máxima de mensajes MQTT

```
set lb parameter -dropmqttjumbomessage no

add responder policy drop_large_message MQTT.MESSAGE_LENGTH.GT(100000)
    reset
```



```
4
5 bind cs vserver mqtt_frontend_cs -policyName drop_large_message -
     priority 10
6 <!--NeedCopy-->
```

En este ejemplo, el `dropmqttjumbomessage` parámetro se establece en NO. Por lo tanto, el dispositivo ADC procesa los mensajes con una longitud superior a 64.000 bytes y menos de 1.00,000 bytes. Los mensajes con una longitud superior a 1.00,000 bytes se restablecen.

Cómo redirigir la solicitud HTTP a HTTPS mediante Responder

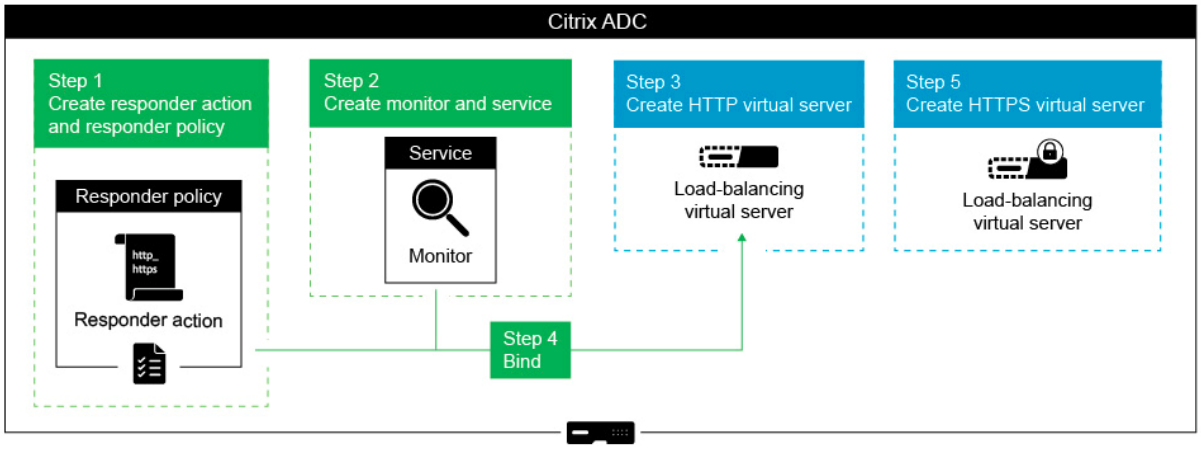
January 12, 2021

En este artículo se explica cómo configurar la función de respuesta con un equilibrio de carga direcciones IP del servidor virtual y redirigir las solicitudes de cliente de HTTP a HTTPS.

Considere un caso en el que un usuario podría intentar acceder a un sitio web seguro mediante el envío de una solicitud HTTP. En lugar de descartar la solicitud, es posible que quiera redirigir la solicitud a un sitio web seguro. Puede utilizar la función de respuesta para redirigir la solicitud al sitio web seguro sin cambiar la ruta y la consulta de URL a la que el usuario intenta acceder.

Cómo Responder Citrix ADC redirige una solicitud de HTTP a HTTPS

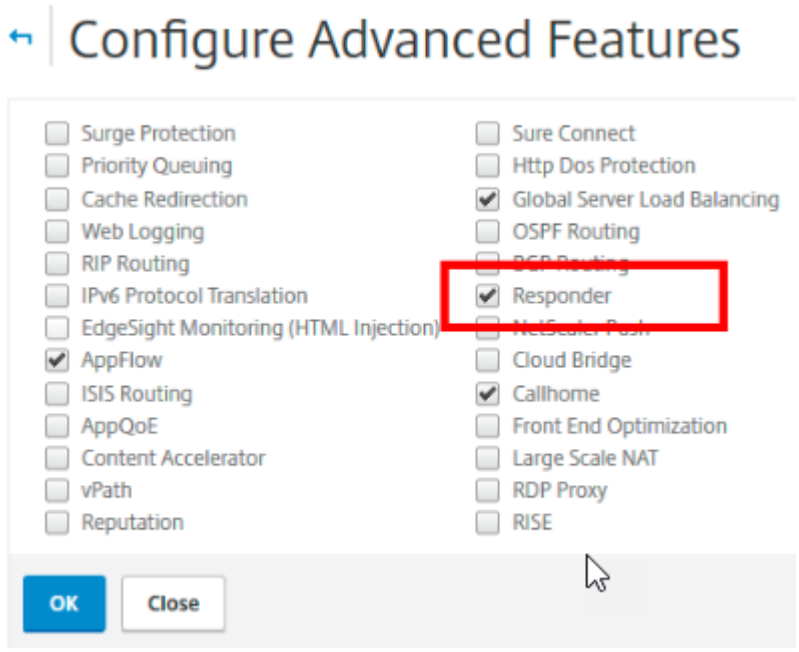
En la siguiente ilustración se muestra un flujo paso a paso de cómo el dispositivo redirige una solicitud.



> **Nota**: Las rutas de navegación y las capturas de pantalla se derivan de NetScaler 11.0.

Para configurar la función Responder junto con las direcciones VIP de equilibrio de carga de un dispositivo NetScaler para redirigir las solicitudes de cliente de HTTP a HTTPS, siga el procedimiento siguiente.

1. Habilite la función de respuesta en el dispositivo. Vaya a **Sistema** > **Configuración** > **Configurar funciones avanzadas** > **Responder**.



2. Cree una acción de respuesta y especifique un nombre adecuado, como http_to_https_actn, en el campo Nombre.
3. Para crear una acción de respuesta, en el panel de navegación, expanda **AppExpert** > **Responder**, haga clic en **Acciones** y, a continuación, haga clic en **Agregar**.
4. Seleccione Redirigir como tipo.
5. En el campo **Expresión**, escriba la siguiente expresión:

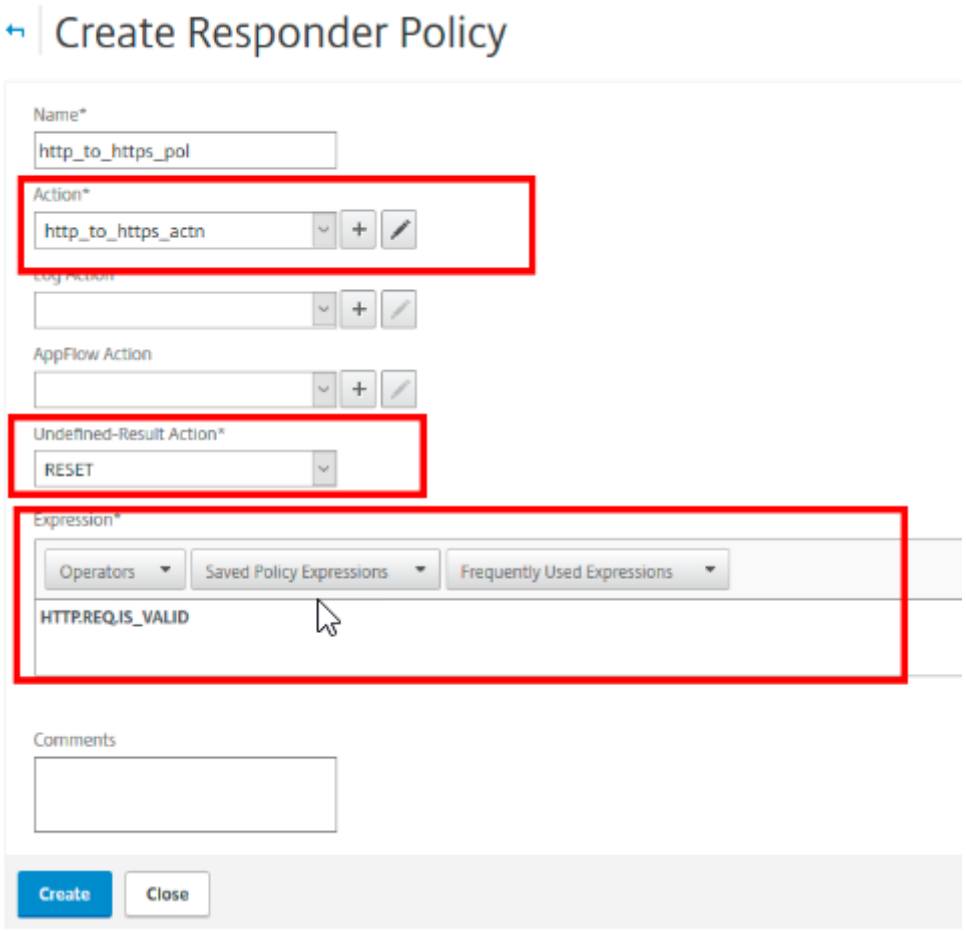
   ```
   "https://"+ HTTP.REQ.HOSTNAME.HTTP_URL_SAFE + HTTP.REQ.URL.PATH_AND_QUERY
   .HTTP_URL_SAFE.
   ```

6. En NetScaler versión 9.0 y 10.0, asegúrese de que la opción **Evitar comprobación de seguridad** esté desactivada.

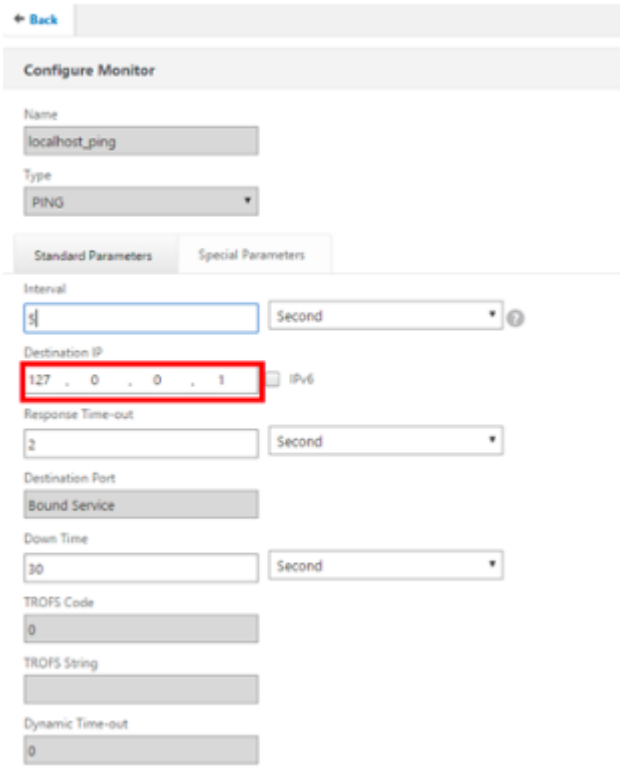
   Nota: Esta opción no está presente desde NetScaler 11.0 en adelante.

7. Cree una **directiva de respuesta** y especifique un nombre adecuado, como http_to_https_pol, en el campo Nombre.
8. Para crear una directiva de Responder, en el panel de navegación, expanda **AppExpert** > **Responder**, haga clic en **Directivas** y, a continuación, haga clic en **Agregar**.
9. En la lista Acción, seleccione el nombre de acción que ha creado.
10. En la lista Acción no definida, seleccione RESTABLECER.

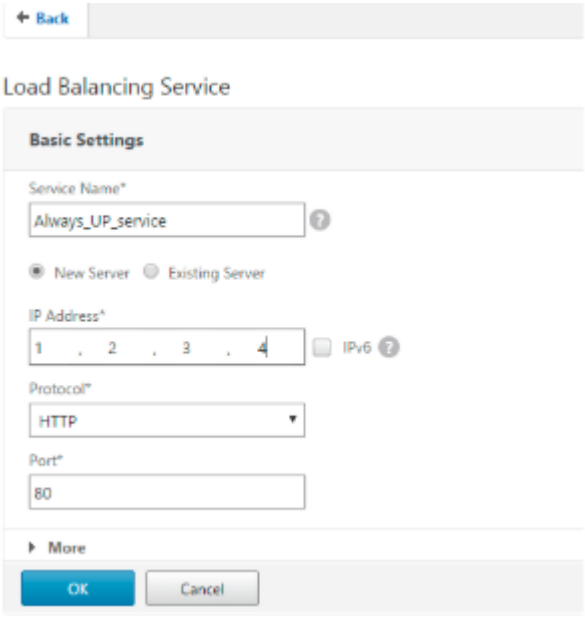
11. Escriba la expresión **HTTP.REQ.IS_VALID** en el campo **Expresión** como se muestra en la siguiente captura de pantalla.



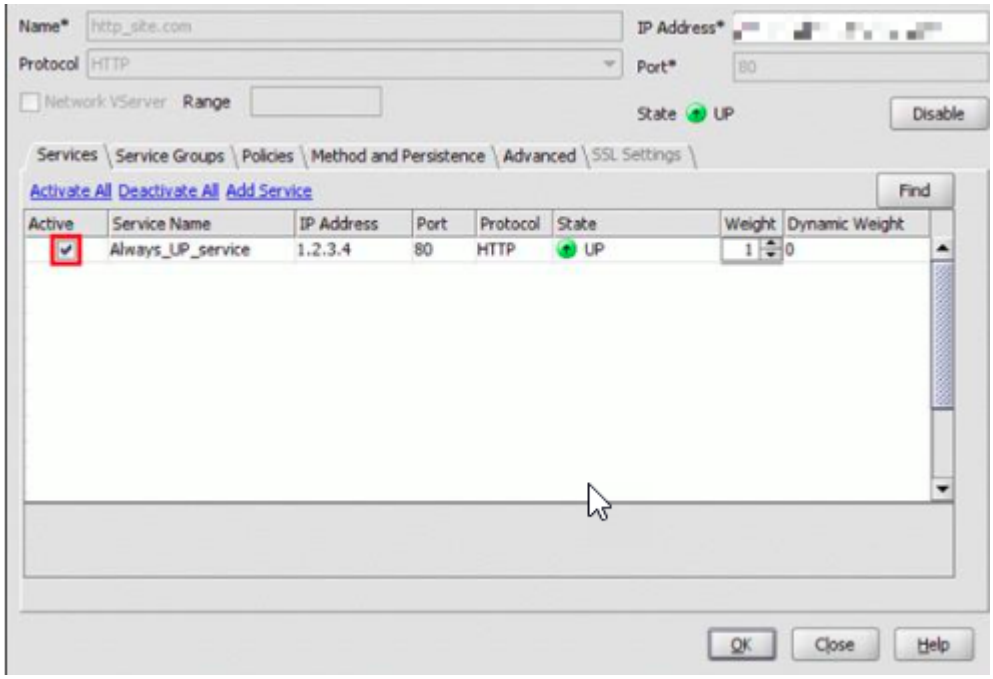
1. Cree un monitor para el que el estado siempre esté marcado como UP y especifique un nombre adecuado, como localhost_ping, en el campo Nombre.
2. Para crear un monitor, en el panel de navegación expanda **Equilibrio de carga**, haga clic en **Monitores** y, a continuación, haga clic en **Agregar**.
3. En el campo **IP de destino**, especifique la dirección IP 127.0.0.1, como se muestra en la siguiente captura de pantalla.



4. Cree un servicio y especifique un nombre adecuado, como Always_up_Service, en el campo **Nombre**.
5. Para crear un servicio, en el panel de navegación, expanda **Equilibrio de carga**, haga clic en **Servicios** y, a continuación, haga clic en **Agregar**.
6. Especifique una dirección IP no existente en el campo **Servidor**.



7. Especifique 80 en el campo **Puerto**.
8. Agregue el monitor creado de la lista **Monitores disponibles**.
9. Cree un servidor virtual de equilibrio de carga y especifique un nombre apropiado en el campo **Nombre**.
10. Para crear un servidor virtual de equilibrio de carga, en el panel de navegación, expanda **Equilibrio de carga**, haga clic en **Servicios** y, a continuación, haga clic en **Agregar**.
11. Especifique la dirección IP del sitio web en el campo Dirección IP.
12. Seleccione HTTP en la lista Protocolo.
13. Escriba 80 en el campo Puerto.
14. En NetScaler versión 9.0 y 10.0, seleccione la opción Active para el servicio que ha creado en la ficha Servicios como se muestra en la siguiente captura de pantalla. Esta opción está obsoleta en NetScaler versión 11.0.



15. Haga clic en la ficha **Directivas**.
16. Enlazar la directiva Responder que creó a la dirección VIP de Equilibrio de carga HTTP del sitio web.
17. Cree un servidor virtual de equilibrio de carga seguro que tenga la dirección IP del sitio web y el puerto como 443.

Para crear una configuración similar al procedimiento anterior desde la interfaz de línea de comandos del dispositivo, ejecute los siguientes comandos:

```
enable ns feature responder
add responder action http_to_https_actn redirect ""https://" + http.req
    .hostname.HTTP_URL_SAFE + http.REQ.URL.PATH_AND_QUERY.HTTP_URL_SAFE"
add responder policy http_to_https_pol HTTP.REQ.IS_VALID
    http_to_https_actn RESET
add lb monitor localhost_ping PING -LRTM ENABLED -destIP 127.0.0.1
add service Always_UP_service 1.2.3.4 HTTP 80 -gslb NONE -maxClient 0 -
    maxReq 0 -cip ENABLED dummy -usip NO -sp OFF -cltTimeout 180 -
    svrTimeout 360 -CKA NO -TCPB NO -CMP YES
bind lb monitor localhost_ping Always_UP_service
add lb vserver http_site.com HTTP 10.217.96.238 80 -persistenceType
    COOKIEINSERT -timeout 0 -cltTimeout 180
bind lb vserver http_site.com Always_UP_service
bind lb vserver http_site.com -policyName http_to_https_pol -priority 1
     -gotoPriorityExpression END
```



```
<!--NeedCopy-->
```

Notas:

- El estado del puerto 80 Load Balancing Redirect servidor virtual debe estar UP para que funcione la redirección.
- Es posible que los exploradores web no redireccionen correctamente si el servidor virtual HTTPS no está activo.
- Esta configuración de redireccionamiento permite situaciones en las que varios dominios están enlazados a la misma dirección IP.
- Si el cliente envía una solicitud HTTP no válida al servidor virtual de redirección, el dispositivo envía un código de mensaje RESTABLECER.

Solucionar problemas

August 20, 2021

Si la función de respuesta no funciona como se esperaba después de configurarla, puede utilizar algunas herramientas comunes para acceder a los recursos de Citrix ADC y diagnosticar el problema.

Recursos para la solución de problemas

Para obtener los mejores resultados, utilice los siguientes recursos para solucionar un problema de caché integrada en un dispositivo Citrix ADC:

- El archivo ns.conf
- Los archivos de seguimiento relevantes del cliente y del dispositivo Citrix ADC

Además de los recursos anteriores, las siguientes herramientas aceleran la solución de problemas:

- El iehttpheaders o una utilidad similar
- La aplicación Wireshark personalizada para los archivos de seguimiento Citrix ADC

Solución de problemas de respuesta

- **Problema**

  La función Responder está configurada, pero la acción Responder no funciona.

  Solución:

  - Compruebe que la función está habilitada.

- Compruebe los contadores de visitas de cualquiera de las directivas para ver si los contadores se están incrementando.
- Compruebe que las directivas y acciones están configuradas correctamente.
- Compruebe que las acciones y directivas están enlazadas correctamente.
- Registre los trazados de paquetes en el cliente y en el dispositivo Citrix ADC, y analícelos para obtener algún puntero al problema.
- Registre los rastros de paquetes iehttpHeaters en el cliente y verifique las solicitudes y respuestas HTTP para obtener algún puntero al problema.

- **Problema**

  Necesita crear una página de mantenimiento.

  Solución:

1. Configure los servicios y el servidor virtual.
2. Configure un servidor virtual de copia de seguridad con un servicio vinculado a él. Esto garantiza que el estado del sitio web siempre se muestre como UP.
3. Configure el servidor virtual principal para que use el servidor virtual de copia de seguridad como una copia de seguridad.
4. Cree una acción de respuesta con un destino apropiado. A continuación se muestra un ejemplo para su referencia:

   ```
   add responder action sorry_page respondwith q{ ”HTTP/1.0 200 OK”+”\r\n\
   r\n”+ ”<html><body>Sorry, this page is not available\</body>\</html>”+
   ”\r\n”}
   ```

5. Cree una directiva de respuesta y vincule la acción a ella.
6. Enlazar la directiva de respondedor al servidor virtual de copia de seguridad.

Reescribe

February 19, 2022

> **Advertencia:**
>
> Las funciones de filtro que utilizan directivas clásicas están obsoletas y, como alternativa, Citrix recomienda utilizar las funciones de reescritura y respuesta con una infraestructura de directivas avanzada.

Rewrite se refiere a la reescritura de cierta información en las solicitudes o respuestas manejadas por el dispositivo Citrix ADC. La reescritura puede ayudar a proporcionar acceso al contenido solicitado

sin exponer detalles innecesarios sobre la configuración real del sitio web. Algunas situaciones en las que la función de reescritura resulta útil son las siguientes:

- Para mejorar la seguridad, Citrix ADC puede reescribir todos los `http://links` como `https://` en el cuerpo de respuesta.
- En la implementación de descarga de SSL, los enlaces inseguros de la respuesta deben convertirse en enlaces seguros. Con la opción de reescritura, reescribir todos los `http://links` como `https://` para asegurarse de que las respuestas salientes de Citrix ADC al cliente tengan los vínculos protegidos.
- Si un sitio web tiene que mostrar una página de error, puede mostrar una página de error personalizada en lugar de la página de error 404 predeterminada. Por ejemplo, si muestra la página principal o el mapa del sitio web en lugar de una página de error, el visitante permanece en el sitio en lugar de alejarse del sitio web.
- Si quieres lanzar un nuevo sitio web, pero usas la URL anterior, puede usar la opción Reescribir.
- Cuando un tema de un sitio tiene una URL complicada, puede reescribirlo con una URL sencilla y fácil de recordar (también conocida como “URL interesante”).
- Puede agregar el nombre de página predeterminado a la URL de un sitio web. Por ejemplo, si la página predeterminada del sitio web de una empresa es `http://www.abc.com/index.php`, cuando el usuario escribe “abc.com” en la barra de direcciones del explorador, puede volver a escribir la URL en “abc.com/index.php”.

Al habilitar la función de reescritura, Citrix ADC puede modificar los encabezados y el cuerpo de las solicitudes y respuestas HTTP.

Para reescribir solicitudes y respuestas HTTP, puede utilizar expresiones de directivas Citrix ADC con reconocimiento de protocolo en las directivas de reescritura que configure. Los servidores virtuales que administran las solicitudes y respuestas HTTP deben ser de tipo
HTTP o
SSL. En el tráfico HTTP, puede realizar las siguientes acciones:

- Modificar la URL de una solicitud
- Agregar, modificar o eliminar encabezados
- Agrega, reemplaza o elimina cualquier cadena específica del cuerpo o de los encabezados.

Para reescribir las cargas útiles TCP, considere la carga útil como un flujo de bytes sin procesar. Cada uno de los servidores virtuales que administran las conexiones TCP debe ser de tipo TCP o SSL_TCP. El término reescritura TCP se utiliza para referirse a la reescritura de cargas útiles TCP que no son datos HTTP. En el tráfico TCP, puede agregar, modificar o eliminar cualquier parte de la carga útil TCP.

Para ver ejemplos para utilizar la función de reescritura, consulte Ejemplos de directivas y acciones de reescritura.

Comparación entre las opciones de Reescritura y Responder

La principal diferencia entre la función de reescritura y la función de respuesta es la siguiente:

Responder no se puede utilizar para expresiones de respuesta o basadas en servidor. Responder solo se puede utilizar en los siguientes casos según los parámetros del cliente:

- Redirigir una solicitud HTTP a nuevos sitios web o páginas web
- Responder con alguna respuesta personalizada
- Dejar o restablecer una conexión en el nivel de solicitud

Si hay una directiva de respuesta, Citrix ADC examina la solicitud del cliente, actúa de acuerdo con las directivas aplicables, envía la respuesta al cliente y cierra la conexión con el cliente.

Si hay una directiva de reescritura, Citrix ADC examina la solicitud del cliente o la respuesta del servidor, actúa de acuerdo con las directivas aplicables y reenvía el tráfico al cliente o al servidor.

En general, se recomienda utilizar un respondedor si quiere que Citrix ADC restablezca o interrumpe una conexión en función de un cliente o un parámetro basado en solicitudes. Usa el respondedor para redirigir el tráfico o responder con mensajes personalizados. Utilice la reescritura para manipular datos en solicitudes y respuestas HTTP.

Cómo funciona la reescritura

Una directiva de reescritura consiste en una regla y una acción. La regla determina el tráfico en el que se aplica la reescritura y la acción determina la acción que debe realizar el dispositivo Citrix ADC. Puede definir varias directivas de reescritura. Para cada directiva, especifique el punto de enlace y la prioridad.

Un punto de enlace hace referencia a un punto del flujo de tráfico en el que Citrix ADC examina el tráfico para comprobar si se le puede aplicar alguna directiva de reescritura. Puede enlazar una directiva a un servidor virtual de equilibrio de carga o conmutación de contenido específico, o hacer que la directiva sea global si quiere que la directiva se aplique a todo el tráfico que gestiona Citrix ADC. Estas directivas se denominan directivas globales.

Además de las directivas definidas por el usuario, Citrix ADC tiene algunas directivas predeterminadas. No se puede modificar ni eliminar una directiva predeterminada.

Para evaluar las directivas, Citrix ADC sigue el siguiente orden:

- Directivas globales
- Directivas vinculadas a servidores virtuales específicos
- Directivas predeterminadas

> **Nota:**

> Citrix ADC solo puede aplicar una directiva de reescritura cuando está vinculada a un punto.

Citrix ADC implementa la función de reescritura en los siguientes pasos:

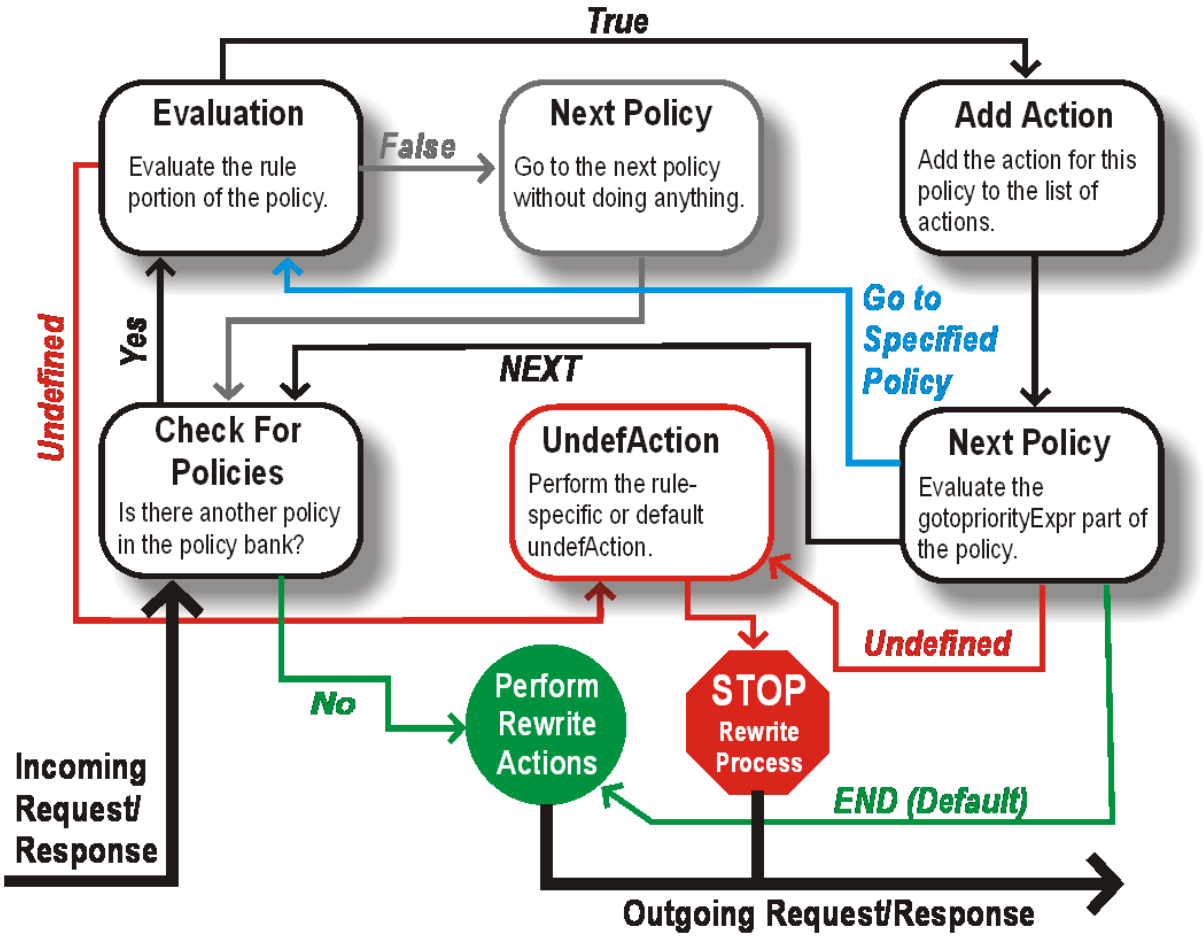
- El dispositivo Citrix ADC comprueba si hay directivas globales y, a continuación, busca directivas en puntos de enlace individuales.
- Si hay varias directivas enlazadas a un punto de enlace, Citrix ADC evalúa las directivas en el orden de prioridad. La directiva con mayor prioridad se evalúa en primer lugar. Después de evaluar cada directiva, si la directiva se evalúa como TRUE, agrega la acción asociada a la directiva en la que se realiza la acción asociada. Se produce una coincidencia cuando las funciones especificadas en la regla de directiva coinciden con las funciones de la solicitud o respuesta que se está evaluando.
- Para cualquier directiva, además de la acción, puede especificar la directiva que debe evaluarse después de evaluar la directiva actual. Esta directiva se conoce como “Ir a la expresión”. Para cualquier directiva, si se especifica Ir a expresión (GoToPriorityExtr), Citrix ADC evalúa la directiva Ir a expresión. Ignora la directiva con la siguiente prioridad máxima.

  Puede especificar la prioridad de la directiva para indicar la directiva Ir a expresión; no puede usar el nombre de la directiva. Si quiere que Citrix ADC deje de evaluar otras directivas después de evaluar una directiva concreta, puede establecer la expresión Ir a la expresión en “FIN”.
- Una vez evaluadas todas las directivas o cuando una directiva tiene la opción Ir a expresión establecida como END, Citrix ADC comienza a realizar las acciones de acuerdo con la lista de acciones.

Para obtener más información sobre la configuración de directivas de reescritura, consulte Configuración de una directiva de reescritura y acerca de las directivas de reescritura vinculantes, consulte Vinculación de una directiva de reescritura.

La siguiente ilustración ilustra cómo Citrix ADC procesa una solicitud o respuesta cuando se utiliza la función de reescritura.

Ilustración 1. El proceso de reescritura



Evaluación de directivas

La directiva con mayor prioridad se evalúa en primer lugar. Citrix ADC no detiene la evaluación de las directivas de reescritura cuando encuentra una coincidencia. Evalúa todas las directivas de reescritura configuradas en Citrix ADC.

- Si una directiva se evalúa como TRUE, Citrix ADC sigue el procedimiento que se indica a continuación:
  - Si la directiva tiene la opción Ir a expresión establecida en END, Citrix ADC deja de evaluar todas las demás directivas y comienza a reescribir.
  - GoToPriorityExpression se puede establecer en 'NEXT', 'END', algún entero o 'INVOCATION_LIST'. El valor determina la directiva con la siguiente prioridad. En la tabla siguiente se muestra la acción realizada por Citrix ADC para cada valor de la expresión.

Valor de la expresión	Acción
PRÓXIMO	Se evalúa la directiva con la siguiente prioridad.

Valor de la expresión	Acción
FIN	Se detiene la evaluación de las directivas.
<an integer>	Se evalúa la directiva con prioridad especificada.
INVOCATION_LIST	Goto NEXT o END se aplica en función del resultado de la lista de invocación.

- Si una directiva se evalúa como FALSE, Citrix ADC continúa la evaluación por orden de prioridad.
- Si una directiva se evalúa como UNDEFINED (no se puede evaluar en el tráfico recibido debido a un error), Citrix ADC realiza la acción asignada a la condición UNDEFINED (denominada UnDefaction) y detiene la evaluación adicional de las directivas.

Citrix ADC inicia la reescritura real solo una vez finalizada la evaluación. Hace referencia a la lista de acciones identificadas por las directivas que se evalúan como TRUE e inicia la reescritura. Después de implementar todas las acciones de la lista, Citrix ADC reenvía el tráfico según sea necesario.

> **Nota:**
>
> Asegúrese de que las directivas no especifican acciones conflictivas o superpuestas en la misma parte del encabezado o cuerpo HTTP, ni en la carga útil TCP. Cuando se produce un conflicto de este tipo, Citrix ADC encuentra una situación indefinida y anula la reescritura.

Acciones de reescritura

En el dispositivo Citrix ADC, especifique las acciones que se deben llevar a cabo, como agregar, reemplazar o eliminar texto dentro del cuerpo, agregar, modificar o eliminar encabezados o cualquier cambio en la carga útil TCP como acciones de reescritura. Para obtener más información sobre las acciones de reescritura, consulte Configuración de una acción de reescritura.

En la siguiente tabla se describen los pasos que puede realizar Citrix ADC cuando una directiva se evalúa como TRUE.

Acción	Resultado
Insertar	Se lleva a cabo la acción de reescritura especificada para la directiva.
NOREWRITE	La solicitud o respuesta no se vuelve a escribir. Citrix ADC reenvía el tráfico sin volver a escribir ninguna parte del mensaje.
RESTABLECER	La conexión se anula en el nivel TCP.

Acción	Resultado
GOTA	Se descarta el mensaje.

> **Nota**:
>
> Para cualquier directiva, puede configurar la acción inferior (acción que se realizará cuando la directiva se evalúe como UNDEFINED) como NOREWRITE, RESET o DROP.

Para utilizar la función de
reescritura, realice los siguientes pasos:

- Habilite la función en Citrix ADC.
- Defina acciones de reescritura.
- Defina directivas de reescritura.
- Enlazar las directivas a un punto de enlace para que la directiva entre en vigor.

Habilitar reescritura

Habilite la función de reescritura en el dispositivo Citrix ADC si quiere volver a escribir las solicitudes o respuestas HTTP o TCP. Si la función está habilitada, Citrix ADC realiza una acción de reescritura de acuerdo con las directivas especificadas. Para obtener más información, consulte Cómo funciona la reescritura.

Para habilitar la entidad de reescritura mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para habilitar la función de reescritura y verificar la configuración:

- habilitar función ns REESCRIBIR
- función show ns

Ejemplo:

```
> enable ns feature REWRITE
 Done
> show ns feature

        Feature                         Acronym             Status
        -------                         -------             ------
 1)     Web Logging                     WL                  OFF
 2)     Surge Protection                SP                  ON
 .
 .
```



```
11   .
12   1)     Rewrite                          REWRITE              ON
13   .
14   .
15   1)     Citrix ADC Push                   push                 OFF
16   Done
17 <!--NeedCopy-->
```

Para habilitar la función de reescritura mediante la interfaz gráfica de usuario

1. En el panel de navegación, haga clic en **Sistema**y, a continuación, en **Configuración**.
2. En el panel de detalles, en Modos y funciones, haga clic en **Configurar funciones básicas**.
3. En el cuadro de diálogo **Configurar funciones básicas**, active la casilla de verificación Reescritura y, a continuación, haga clic en **Aceptar**.
4. En el cuadro de diálogo **Habilitar/inhabilitar funciones**, haga clic en **Sí**. Aparece un mensaje en la barra de estado que indica que la función seleccionada se ha habilitado.

Configurar una acción de reescritura

> **Advertencia**
>
> La función Patrón de una acción de reescritura está obsoleta a partir de Citrix ADC 12.0 compilación 56.20 y, como alternativa, Citrix recomienda utilizar el parámetro Acción de reescritura de búsqueda.

Una acción de reescritura indica los cambios realizados en una solicitud o respuesta antes de enviarla a un servidor o cliente.

Las expresiones definen lo siguiente:

- Tipo de acción de reescritura.
- Ubicación de la acción de reescritura.
- Tipo de configuración de acción de reescritura.

Por ejemplo, una acción DELETE solo utiliza una expresión de destino. Una acción REEMPLAZAR utiliza una expresión de destino y una expresión para configurar el texto de sustitución.

Después de habilitar la función de reescritura, debe configurar una o varias acciones a menos que sea suficiente con una acción de reescritura integrada. Todas las acciones integradas tienen nombres que comienzan por la cadena ns_cvpn, seguidos de una cadena de letras y caracteres de guión bajo. Las acciones integradas realizan tareas útiles y complejas, como decodificar partes de una solicitud o respuesta de VPN sin cliente o modificar datos JavaScript o XML. Las acciones integradas se pueden ver, habilitar y inhabilitar, pero no se pueden modificar ni eliminar.

> Nota:
>
> Los tipos de acción que solo se pueden utilizar para la reescritura HTTP se identifican en la columna **Tipo de acción de reescritura**.

Para obtener más información, consulte **Parámetro Type**.

Crear una acción de reescritura mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para crear una acción de reescritura y comprobar la configuración:

- `add rewrite action <name> <type> <target> [<stringBuilderExpr>] [-search <expression>] [refineSearch <expression>] [-comment<string>]`
- `show rewrite action <name>`

Para obtener más información, consulte la tabla Tipos de acción de reescritura y sus argumentos .

La función de reescritura tiene las siguientes acciones integradas:

- Norewrite-envía la solicitud o respuesta al usuario sin volver a escribirla.
- RESET: restablece la conexión y notifica al explorador del usuario para que el usuario pueda reenviar la solicitud.
- DROP: interrumpe la conexión sin enviar una respuesta al usuario.

Uno de los siguientes tipos de flujo está asociado implícitamente a cada acción:

- Solicitud: la acción se aplica a la solicitud.
- Respuesta: la acción se aplica a la respuesta.
- Neutral: la acción se aplica tanto a las solicitudes como a las respuestas.

Nombre

Nombre de la acción de reescritura definida por el usuario. Debe comenzar con una letra, un número o un carácter de guión bajo (_) y debe contener solo letras, números y guión (-), punto (.), guión (.), espacio(), at (@), igual a (=), dos puntos (:) y guión bajo. Se puede cambiar después de agregar la directiva de reescritura.

parámetro Type

El parámetro **Type** muestra el tipo de acción de reescritura definida por el usuario.

A continuación se indican los valores del parámetro **Type** :

- REPLACE <target> <string_builder_expr>. Reemplaza la cadena por la expresión del generador de cadenas.

Ejemplo:

```
> add rewrite action replace_http_act replace http.res.body(100) '"
    new_replaced_data"'
Done
> sh rewrite action replace_http_act
Name: replace_http_act
Operation: replace
Target:http.res.body(100)
Value:"new_replaced_data"
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- REPLACE_ALL <target> <string_builder_expr1> -(search)<string_builder_expr2>. En la solicitud o respuesta especificada por <target>, reemplaza todas las apariciones de la cadena definida por <string_builder_expr1> con la cadena definida por <string_builder_expr2>. Puede utilizar la función de búsqueda para buscar las cadenas que se van a reemplazar.

Ejemplo:

```
> add policy patset pat_list_2
Done
> bind policy patset pat_list_2 "www.abc.com"
Done
> bind policy patset pat_list_2 "www.def.com"
Done
> add rewrite action refineSearch_act_31 replace_all "HTTP.RES.BODY
    (100000)" ""https://""-search "patset("pat_list_2")" -refineSearch "
    EXTEND(7,0).REGEX_SELECT(re#http://#)"
Done

> sh rewrite action refineSearch_act_31
Name: refineSearch_act_31
Operation: replace_all
```



```
Target:HTTP.RES.BODY(100000)
Refine Search:EXTEND(7,0).REGEX_SELECT(re#http://#)
Value:”https://”
Search: patset(”pat_list_2”)
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- REPLACE_HTTP_RES <string_builder_expr>. Reemplaza la respuesta HTTP completa por la cadena definida por la expresión del generador de cadenas.

Ejemplo:

```
> add rewrite action replace_http_res_act replace_http_res '”HTTP/1.1
   200 OK\r\n\r\nSending from ADC”'
 Done
> sh rewrite action replace_http_res_act
Name: replace_http_res_act
Operation: replace_http_res
Target:”HTTP/1.1 200 OK
Sending from ADC”
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- REPLACE_SIP_RES <target>. Reemplaza la respuesta SIP completa por la cadena especificada por <target>.

Ejemplo:

```
> add rewrite action replace_sip_res_act replace_sip_res '”HTTP/1.1 200
    OK\r\n\r\nSending from ADC”'
Done
> sh rewrite action replace_sip_res_act
Name: replace_sip_res_act
Operation: replace_sip_res
Target:”HTTP/1.1 200 OK
```



```
7  Sending from ADC”
8  Hits: 0
9  Undef Hits: 0
10 Action Reference Count: 0
11 Done
12
13 <!--NeedCopy-->
```

- INSERT_HTTP_HEADER <header_string_builder_expr> <contents_string_builder_expr>. Inserta el encabezado HTTP especificado por <header_string_builder_expr> y el contenido del encabezado especificado por <contents_string_builder_expr>.

Ejemplo:

```
1  > add rewrite action ins_cip_header insert_http_header ”CIP” ”CLIENT.IP
       .SRC”
2  Done
3  > sh rewrite action ins_cip_header
4  Name: ins_cip_header
5  Operation: insert_http_header
6  Target:CIP
7  Value:CLIENT.IP.SRC
8  Hits: 0
9  Undef Hits: 0
10 Action Reference Count: 0
11 Done
12
13 <!--NeedCopy-->
```

- DELETE_HTTP_HEADER <target>. Elimina el encabezado HTTP especificado por <target>

Ejemplo:

```
1  > add rewrite action del_true_client_ip_header delete_http_header ”True
       -Client-IP”
2  Done
3  > sh rewrite action del_true_client_ip_header
4  Name: del_true_client_ip_header
5  Operation: delete_http_header
6  Target:True-Client-IP
7  Hits: 0
8  Undef Hits: 0
9  Action Reference Count: 0
```



```
10 Done
11
12 <!--NeedCopy-->
```

- CORRUPT_HTTP_HEADER <target>. Reemplaza el nombre del encabezado de todas las apariciones del encabezado HTTP especificado por <target> un nombre dañado, de modo que el receptor no lo reconozca. Ejemplo: MY_HEADER se cambia a MHEY_ADER.

Ejemplo:

```
1 > add rewrite action corrupt_content_length_hdr corrupt_http_header ”
     Content-Length”
2 Done
3 > sh rewrite action corrupt_content_length_hdr
4 Name: corrupt_content_length_hdr
5 Operation: corrupt_http_header
6 Target:Content-Length
7 Hits: 0
8 Undef Hits: 0
9 Action Reference Count: 0
10 Done
11
12 <!--NeedCopy-->
```

- INSERT_BEFORE <string_builder_expr1> <string_builder_expr1>. Busca la cadena especificada en <string_builder_expr1> e inserta la cadena <string_builder_expr2 > delante de ella.

```
1 > add rewrite action insert_before_ex_act insert_before http.res.body
     (100) '”Add this string in the starting”'
2 Done
3 > sh rewrite action insert_before_ex_act
4 Name: insert_before_ex_act
5 Operation: insert_before
6 Target:http.res.body(100)
7 Value:”Add this string in the starting”
8 Hits: 0
9 Undef Hits: 0
10 Action Reference Count: 0
11 Done
12
13 <!--NeedCopy-->
```


- INSERT_BEFORE_ALL <target> <string_builder_expr1> -(search)<string_builder_expr2>. En la solicitud o respuesta especificada por <target>, localiza todas las apariciones de la cadena especificada en <string_builder_expr1> e inserta la cadena especificada en <string_builder_expr2> antes de ella. Puede usar la función de búsqueda para encontrar las cadenas.

Ejemplo:

```
> add policy patset pat
 Done
> bind policy patset pat abcd
 Done
> add rewrite action refineSearch_act_1 insert_before_all http.res.body
    (10) 'target.prefix(10) + ”refineSearch_testing”' -search patset(”
    pat”) -refineSearch extend(10,10)
 Done
> sh rewrite action refineSearch_act_1
Name: refineSearch_act_1
Operation: insert_before_all
Target:http.res.body(10)
Refine Search:extend(10,10)
Value:target.prefix(10) + ”refineSearch_testing”
Search: patset(”pat”)
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- INSERT_AFTER <string_builder_expr1> <string_builder_expr2>. Busca la cadena especificada en <string_builder_expr1>e inserta la cadena especificada en <string_builder_expr2> después de eso.
  Ejemplo:

```
> add rewrite action insert_after_act insert_after http.req.body(100) '
    ”add this string after 100 bytes”'
Done
> sh rewrite action insert_after_act
Name: insert_after_act
Operation: insert_after
Target:http.req.body(100)
```



```
Value:”add this string after 100 bytes”
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- INSERT_AFTER_ALL <target> <string_builder_expr1> -(search)<string_builder_expr>. En la solicitud o respuesta especificada por <target>, localiza todas las apariciones de la cadena especificada por <string_builder_expr1> e inserta la cadena especificada por <string_builder_expr2> después de cada una. Puede usar la función de búsqueda para encontrar las cadenas.

Ejemplo:

```
> add rewrite action refineSearch_act_2 insert_after_all http.res.body
   (100) '”refineSearch_testing”' -search text(”abc”) -refineSearch
   extend(0, 10)
Done
> sh rewrite action refineSearch_act_2
Name: refineSearch_act_2
Operation: insert_after_all
Target:http.res.body(100)
Refine Search:extend(0, 10)
Value:”refineSearch_testing”
Search: text(”abc”)
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- DELETE <target>. Busca y elimina el objetivo especificado.

Ejemplo:

```
> add rewrite action delete_ex_act delete http.req.header(”HDR”)
Done
> sh rewrite action delete_ex_act
Name: delete_ex_act
```



```
Operation: delete
Target:http.req.header(”HDR”)
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- DELETE_ALL <target> -(search)<string_builder_expr>. En la solicitud o respuesta especificada por <target>, localiza y elimina todas las apariciones de la cadena especificada por <string_builder_expr>. Puede usar la función de búsqueda para encontrar las cadenas.

Ejemplo:

```
>add rewrite action refineSearch_act_4 delete_all ”HTTP.RES.BODY(50000)
   ” -search text(”Windows Desktops”) -refineSearch ”EXTEND(40,40).
   REGEX_SELECT(re#\s`\*`<AppData>.`\*`\s`\*`<\\/AppData>#)”
Done
> show REWRITE action refineSearch_act_4
Name: refineSearch_act_4
Operation: delete_all
Target:HTTP.RES.BODY(50000)
Refine Search:EXTEND(40,40).REGEX_SELECT(re#\s`\*`<AppData>.`\*`\s
   `\*`</AppData>#)
Search: text(”Windows Desktops”)
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- REPLACE_DIAMETER_HEADER_FIELD <target> <field value>. En la solicitud o respuestas, modifique el campo de encabezado especificado por <target>. Use Diameter.req.flags.SET(<flag>) o Diameter.req.flags.UNSET<flag> como stringbuilderexpression para configurar o desconfigurar banderas.

Ejemplo:


```
> add rewrite action replace_diameter_field_ex_act
    replace_diameter_header_field diameter.req.flags diameter.req.flags.
    set(PROXIABLE)
Done
> sh rewrite action replace_diameter_field_ex_act
Name: replace_diameter_field_ex_act
Operation: replace_diameter_header_field
Target:diameter.req.flags
Value:diameter.req.flags.set(PROXIABLE)
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- REPLACE_DNS_HEADER_FIELD <target>. En la solicitud o respuesta modifica el campo de encabezado especificado por <target>.

Ejemplo:

```
> add rewrite action replace_dns_hdr_act replace_dns_header_field dns.
    req.header.flags.set(AA)
Done
> sh rewrite action replace_dns_hdr_act
Name: replace_dns_hdr_act
Operation: replace_dns_header_field
Target:dns.req.header.flags.set(AA)
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- REPLACE_DNS_ANSWER_SECTION <target>. Reemplaza la sección de respuestas DNS en la respuesta. Esto se aplica únicamente a los registros A y AAAA. Use expresiones DNS.NEW_RRSET_A y NS.NEW_RRSET_AAAA para configurar la nueva sección de respuestas.

Ejemplo:

```
> add rewrite action replace_dns_ans_act replace_dns_answer_section
    DNS.NEW_RRSET_A("1.1.1.1", 10)
```



```
Done
> sh rewrite action replace_dns_ans_act
Name: replace_dns_ans_act
Operation: replace_dns_answer_section
Target:DNS.NEW_RRSET_A("1.1.1.1", 10)
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- CLIENTLESS_VPN_DECODE<target>. Decodifica el patrón especificado por el destino en formato VPN sin cliente.

Ejemplo:

```
> add rewrite action cvpn_decode_act_1 clientless_vpn_decode http.req.
   body(100)
Done
> sh rewrite action cvpn_decode_act_1
Name: cvpn_decode_act_1
Operation: clientless_vpn_decode
Target:http.req.body(100)
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- CLIENTLESS_VPN_DECODE_ALL<target>-search<expression>. Decodifica TODOS los patrones especificados por el parámetro de búsqueda en formato VPN sin cliente.

Ejemplo:

```
> add rewrite action act1 clientless_vpn_decode_all http.req.body(100)
   -search text("abcd")
Done
> sh rewrite action act1
Name: act1
Operation: clientless_vpn_decode_all
Target:http.req.body(100)
```



```
7  Search: text(”abcd”)
8  Hits: 0
9  Undef Hits: 0
10 Action Reference Count: 0
11 Done
12
13 <!--NeedCopy-->
```

- CLIENTLESS_VPN_ENCODE<target>. Codifica el patrón especificado por target en formato VPN sin cliente.

Ejemplo:

```
1  > add rewrite action cvpn_encode_act_1 clientless_vpn_encode http.req.
      body(100)
2  Done
3  > sh rewrite action cvpn_encode_act_1
4  Name: cvpn_encode_act_1
5  Operation: clientless_vpn_encode
6  Target:http.req.body(100)
7  Hits: 0
8  Undef Hits: 0
9  Action Reference Count: 0
10 Done
11
12 <!--NeedCopy-->
```

- CLIENTLESS_VPN_ENCODE_ALL<target>-search<expression>. Codifica TODOS los patrones especificados en el parámetro de búsqueda en formato VPN sin cliente.

Ejemplo:

```
1  > add rewrite action act2 clientless_vpn_encode_all http.req.body(100)
      -search text(”abcd”)
2  Done
3  > sh rewrite action act2
4  Name: act1
5  Operation: clientless_vpn_encode_all
6  Target:http.req.body(100)
7  Search: text(”abcd”)
8  Hits: 0
9  Undef Hits: 0
10 Action Reference Count: 0
```



```
11 Done
12
13 <!--NeedCopy-->
```

- CORRUPT_SIP_HEADER<target>. Reemplaza el nombre del encabezado de todas las apariciones del encabezado SIP especificado por <target> con un nombre dañado, de modo que el receptor no lo reconozca.

Ejemplo:

```
1 > add rewrite action corrupt_sip_hdr_act corrupt_sip_header SIP_HDR
2 Done
3 > sh rewrite action corrupt_sip_hdr_act
4 Name: corrupt_sip_hdr_act
5 Operation: corrupt_sip_header
6 Target:SIP_HDR
7 Hits: 0
8 Undef Hits: 0
9 Action Reference Count: 0
10 Done
11
12 <!--NeedCopy-->
```

- INSERT_SIP_HEADER <header_string_builder_expr> <contents_string_builder_expr>. Inserta el encabezado SIP especificado por <header_string_builder_expr> y el contenido del encabezado especificado por <contents_string_builder_expr>.

Ejemplo:

```
1 > add rewrite action insert_sip_hdr_act insert_sip_header SIP_HDR '"
    inserting_sip_header"'
2  Done
3 >sh rewrite action insert_sip_hdr_act
4 Name: insert_sip_hdr_act
5 Operation: insert_sip_header
6 Target:SIP_HDR
7 Value:"inserting_sip_header"
8 Hits: 0
9 Undef Hits: 0
10 Action Reference Count: 0
11 Done
12
```



```
<!--NeedCopy-->
```

- DELETE_SIP_HEADER<target>. Elimina el encabezado SIP especificado por <target>

Ejemplo:

```
> add rewrite action delete_sip_hdr delete_sip_header  SIP_HDR
Done
> sh rewrite action delete_sip_hdr
Name: delete_sip_hdr
Operation: delete_sip_header
Target:SIP_HDR
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

Parámetro objetivo

El parámetro Target es una expresión que especifica qué parte de la solicitud o respuesta se va a reescribir.

StringBuilderExpr

StringBuilderExpr es una expresión que especifica el contenido que se va a insertar en la solicitud o respuesta en la ubicación especificada. Esta expresión sustituye a una cadena especificada.

Ejemplo 1. Inserción de un encabezado HTTP con la IP del cliente:

```
> add rewrite action insertact INSERT_HTTP_HEADER "client-IP" CLIENT.IP
    .SRC
Done
> show rewrite action insertact
Name: insertact
Operation: insert_http_header
Target:Client-IP
Value:CLIENT.IP.SRC
BypassSafetyCheck : NO
Hits: 0
```



```
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

Ejemplo 2. Reemplazo de cadenas en una carga útil TCP (reescritura TCP):

```
> add rewrite action client_tcp_payload_replace_all REPLACE_ALL
  'client.tcp.payload(1000)' '"new-string"' -search text("old-string")
Done
> show rewrite action client_tcp_payload_replace_all
Name: client_tcp_payload_replace_all
Operation: replace_all
Target:client.tcp.payload(1000)
Value:"new-string"
Search: text("old-string")
BypassSafetyCheck : NO
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done
>
<!--NeedCopy-->
```

Buscar una parte de la solicitud o respuesta para volver a escribirla

La funcionalidad de búsqueda ayuda a encontrar todas las instancias del patrón requerido en la solicitud o respuesta.

La funcionalidad de búsqueda se debe utilizar en los siguientes tipos de acción:

- INSERT_BEFORE_ALL
- INSERT_AFTER_ALL
- REPLACE_ALL
- DELETE_ALL
- CLIENTLESS_VPN_ENCODE_ALL
- CLIENTLESS_VPN_DECODE_ALL

La funcionalidad de búsqueda no se puede utilizar con los siguientes tipos de acción:

- INSERT_HTTP_HEADER
- INSERT_BEFORE

- INSERT_AFTER
- REEMPLAZAR
- SUPRIMIR
- DELETE_HTTP_HEADER
- CORRUPT_HTTP_HEADER
- REPLACE_HTTP_RES
- CLIENTLESS_VPN_ENCODE
- CLIENTLESS_VPN_DECODE
- INSERT_SIP_HEADER
- DELETE_SIP_HEADER
- CORRUPT_SIP_HEADER
- REPLACE_DIAMETER_HEADER_FIELD
- REPLACE_DNS_ANSWER_SECTION
- REPLACE_DNS_HEADER_FIELD
- REPLACE_SIP_RES

Se admiten los siguientes tipos de búsqueda:

- Text - Una cadena literal
  Ejemplo: -search text (“hola”)
- Expresión regular: patrón que se utiliza para hacer coincidir varias cadenas en la solicitud o respuesta
  Ejemplo ⊠expresión regular de búsqueda (re~^hello*~)
- XPATH: expresión XPATH para buscar XML.
  Ejemplo ⊠buscar xpath (xp%/a/b%)
- JSON: expresión XPATH para buscar en JSON.
  Ejemplo ⊠search xpath_json (xp%/a/b%)
  HTML - Expresión XPATH para buscar HTML
  Ejemplo ⊠search xpath_html (xp%/html/body%)
  Patset - Busca todos los patrones enlazados a la entidad patset.
  Ejemplo: -search patset(“patset1”)
- Datset: busca todos los patrones enlazados a la entidad de conjunto de datos.
  Ejemplo: -search dataset(“dataset1”)
- AVP: número AVP que se utiliza para hacer coincidir varios AVP en un mensaje de diámetro/radio
  Ejemplo ⊠search avp (999)

Afinar los resultados de la búsqueda

Puede utilizar la funcionalidad Perfeccionar búsqueda para especificar los criterios adicionales para refinar los resultados de la búsqueda. La funcionalidad Perfeccionar búsqueda solo se puede utilizar si se utiliza la funcionalidad de búsqueda.

El parámetro Refine search siempre comienza con la operación “extend (m, n)”, donde ‘m’ especifica algunos bytes a la izquierda del resultado de la búsqueda y ‘n’ especifica varios bytes a la derecha del resultado de la búsqueda para ampliar el área seleccionada.

Si la acción de reescritura configurada es:

```
> add rewrite action test_refine_search replace_all http.res.body(10) '
    ” testing_refine_search” ' -search text(”abc”) -refineSearch extend
    (1,1)
And the HTTP response body is abcxxxx456.

<!--NeedCopy-->
```

A continuación, el parámetro search encuentra el patrón “abc” y, dado que el parámetro RefineSearch también está configurado para comprobar un byte adicional a la izquierda y un byte adicional a la derecha del patrón coincidente. El texto sustituido resultante es: abcx. Por lo tanto, el resultado de esta acción es `testing_refine_searchxxx456`.

Ejemplo 1:Uso de la funcionalidad Perfeccionar búsqueda en el tipo de acción INSERT_BEFORE_ALL.

```
> add policy patset pat
Done
> bind policy patset pat abcd
Done
> add rewrite action refineSearch_act_1 insert_before_all http.res.body
    (10) 'target.prefix(10) + ”refineSearch_testing”' -search patset(”
    pat”) -refineSearch extend(10,10)
Done
> sh rewrite action refineSearch_act_1
Name: refineSearch_act_1
Operation: insert_before_all
Target:http.res.body(10)
Refine Search:extend(10,10)
Value:target.prefix(10) + ”refineSearch_testing”
Search: patset(”pat”)
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```


Ejemplo 2: Uso de la funcionalidad Perfeccionar búsqueda en el tipo de acción INSERT_AFTER_ALL.

```
> add rewrite action refineSearch_act_2 insert_after_all http.res.body
   (100) '"refineSearch_testing"' -search text("abc") -refineSearch
   extend(0, 10)
Done
> sh rewrite action refineSearch_act_2
Name: refineSearch_act_2
Operation: insert_after_all
Target:http.res.body(100)
Refine Search:extend(0, 10)
Value:"refineSearch_testing"
Search: text("abc")
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

Ejemplo 3: Uso de la funcionalidad Perfeccionar búsqueda en el tipo de acción REPLACE_ALL.

```
> add policy patset pat_list_2
Done
> bind policy patset pat_list_2 "www.abc.com"
Done
> bind policy patset pat_list_2 "www.def.com"
Done
> add rewrite action refineSearch_act_31 replace_all "HTTP.RES.BODY
   (100000)" ""https://"" -search "patset("pat_list_2")" -refineSearch
   "EXTEND(7,0).REGEX_SELECT(re#http://#)"
Done
> sh rewrite action refineSearch_act_31
Name: refineSearch_act_31
Operation: replace_all
Target:HTTP.RES.BODY(100000)
Refine Search:EXTEND(7,0).REGEX_SELECT(re#http://#)
Value:"https://"
Search: patset("pat_list_2")
Hits: 0
Undef Hits: 0
Action Reference Count: 0
```



```
19 Done
20
21 <!--NeedCopy-->
```

Ejemplo 4: Uso de la funcionalidad Perfeccionar búsqueda en el tipo de acción DELETE_ALL.

```
1 >add rewrite action refineSearch_act_4 delete_all ”HTTP.RES.BODY(50000)
     ” -search text(”Windows Desktops”) -refineSearch ”EXTEND(40,40).
     REGEX_SELECT(re#\s*<AppData>.\*\s\*<\\/AppData>#)”
2 > show REWRITE action refineSearch_act_4
3 Name: refineSearch_act_4
4 Operation: delete_all
5 Target:HTTP.RES.BODY(50000)
6 Refine Search:EXTEND(40,40).REGEX_SELECT(re#\s*<AppData>.\*\s\*</
     AppData>#)
7 Search: text(”Windows Desktops”)
8 Hits: 0
9 Undef Hits: 0
10 Action Reference Count: 0
11 Done
12 >
13 <!--NeedCopy-->
```

Ejemplo 5: Uso de la funcionalidad Refinar búsqueda en el tipo de acción CLIENTLESS_VPN_ENCODE_ALL.

”’

```
add rewrite action act2 clientless_vpn_encode_all http.req.body(100) -search text(“abcd”)
Done
sh rewrite action act2
Name: act1
Operation: clientless_vpn_encode_all
Target:http.req.body(100)
Search: text(“abcd”)
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done
```

”’

Ejemplo 6: Uso de la funcionalidad Refinar búsqueda en el tipo de acción CLIENTLESS_VPN_DECODE_ALL.


```
> add rewrite action act1 clientless_vpn_decode_all http.req.body(100)
   -search text(”abcd”)
Done
> sh rewrite action act1
Name: act1
Operation: clientless_vpn_decode_all
Target:http.req.body(100)
Search: text(”abcd”)
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done
>
<!--NeedCopy-->
```

Modificar una acción de reescritura existente mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para modificar una acción de reescritura existente y compruebe la configuración:

- `set rewrite action <name> [-target <expression>] [-stringBuilderExpr <expression>] [-search <expression>] [-refineSearch <expression>] [-comment <string>]`

En el símbolo del sistema, escriba los siguientes comandos para verificar la configuración modificada

- `show rewrite action <name>`

Ejemplo:

```
> set rewrite action insertact -target ”Client-IP”
 Done
> show rewrite action insertact

Name: insertact
Operation: insert_http_header   Target:Client-IP
Value:CLIENT.IP.SRC
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

```



```
<!--NeedCopy-->
```

Eliminar una acción de reescritura mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para quitar una acción de reescritura:

```
rm rewrite action <name>
```

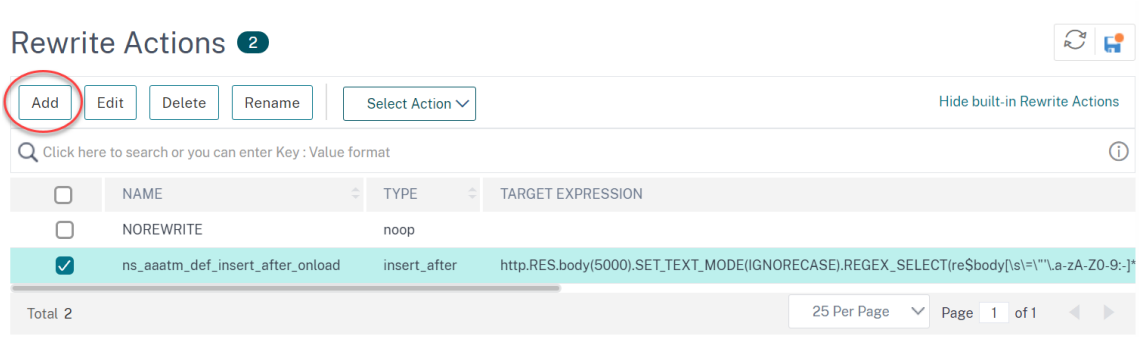
Ejemplo:

```
> rm rewrite action insertact
Done

<!--NeedCopy-->
```

Configurar una acción de reescritura mediante la utilidad de configuración

1. Vaya a **AppExpert > Rewrite > Actions**.
2. En el panel de detalles, realice una de las acciones siguientes:
   - Para crear una acción, haga clic en **Agregar**.
   - Para modificar una acción existente, selecciónela y, a continuación, haga clic en **Modificar**.
3. Haga clic en **Crear** o **Aceptar**. Aparece un mensaje en la barra de estado que indica que la acción se ha configurado correctamente.
4. Repita los pasos 2 a 4 para crear o modificar tantas acciones de reescritura como quiera.
5. Haga clic en **Cerrar**.



Agregar una expresión mediante el cuadro de diálogo Agregar expresión

1. En el cuadro de diálogo **Crear acción** de **reescritura o Configurar acción** de reescritura, en el área de texto del argumento de tipo que quiera introducir, haga clic en **Agregar**.
2. En el cuadro de diálogo **Agregar expresión**, en el primer cuadro de lista, elija el primer término de la expresión.
   - HTTP. El protocolo HTTP. Elija esta opción si quiere examinar algún aspecto de la solicitud que pertenece al protocolo HTTP.
   - DICE. Los sitios web protegidos. Elija esta opción si quiere examinar algún aspecto de la solicitud que pertenece al destinatario de la solicitud.
   - CLIENTE. El equipo que envió la solicitud. Elija esta opción si quiere examinar algún aspecto del remitente de la solicitud.

Al elegir, el cuadro de lista situado más a la derecha muestra los términos apropiados para la siguiente parte de la expresión.

1. En el segundo cuadro de lista, elige el segundo término para su expresión. Las elecciones dependen de la elección que haya realizado en el paso anterior y son apropiadas para el contexto. Después de hacer la segunda elección, la ventana de Ayuda situada debajo de la ventana Construir expresión (que estaba en blanco) muestra ayuda para describir el propósito y el uso del término que acaba de elegir.
2. Siga eligiendo términos en los cuadros de lista que aparecen a la derecha del cuadro de lista anterior o escribiendo cadenas o números en los cuadros de texto que aparecen para pedirle que escriba un valor hasta que finalice la expresión.
   Para obtener más información sobre el lenguaje de expresiones PI y la creación de expresiones para directivas de respuesta, consulte “Directivas y expresiones. “

Si quiere probar el efecto de una acción de reescritura cuando se utiliza en datos HTTP de ejemplo, puede utilizar el Evaluador de expresiones de reescritura.

Reescritura de cargas útiles TCP

Las expresiones de destino de las acciones de reescritura de TCP deben comenzar con uno de los prefijos de expresión siguientes:

- **CLIENT.TCP.PAYLOAD.** Para reescribir cargas útiles TCP en solicitudes de clientes. Por ejemplo, CLIENT.TCP.PAYLOAD(10000).AFTER_STR(“string1”).
- **SERVIDOR.TCP.PAYLOAD.** Para reescribir cargas útiles TCP en las respuestas del servidor. Por ejemplo, SERVER.TCP.PAYLOAD(1000).B64DECODE.BETWEEN(“string1”,”string2”).

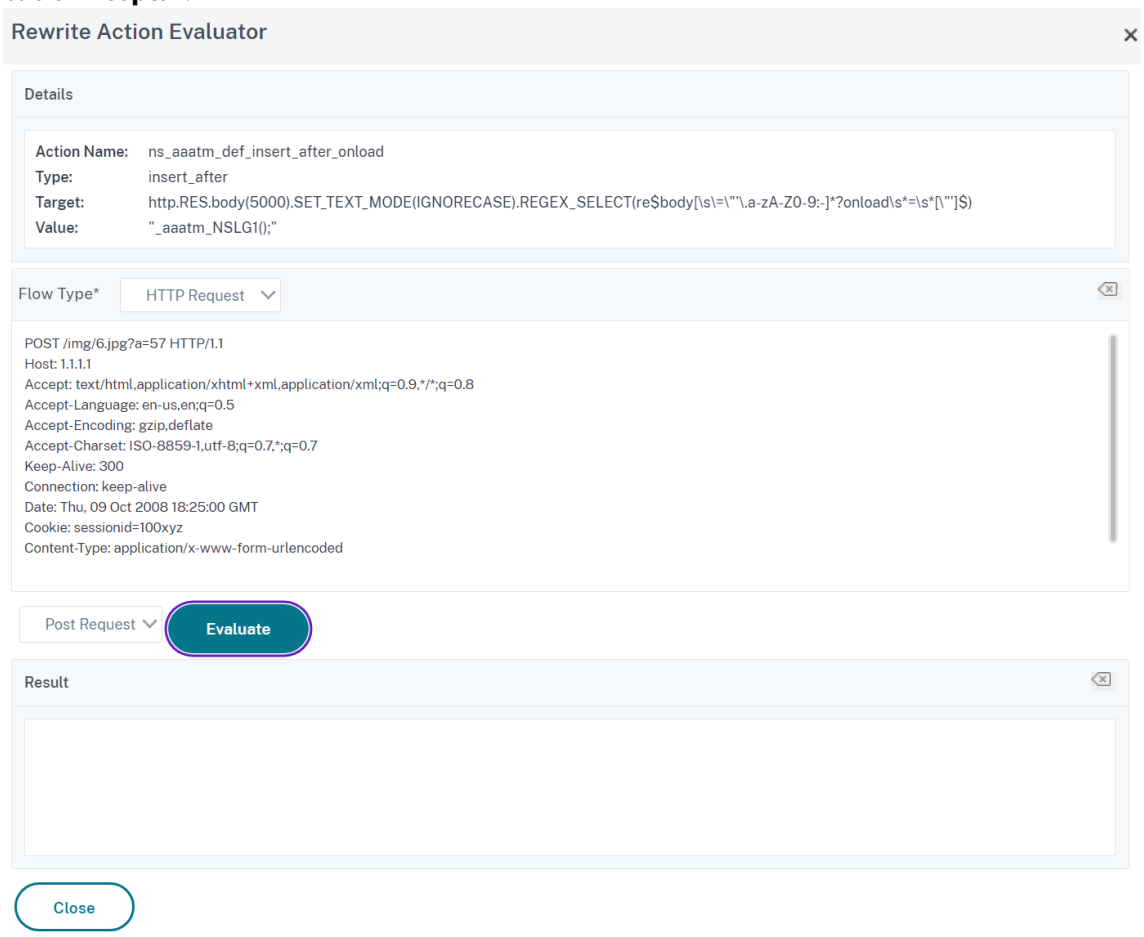
Evaluar una acción de reescritura mediante el cuadro de diálogo Rewrite Action Evaluator

1. En el panel de detalles **Acciones de reescritura**, seleccione la acción de reescritura que quiere evaluar y, a continuación, haga clic en **Evaluar**.
2. En el cuadro de diálogo Reescribir evaluador de expresiones, especifique los valores de los siguientes parámetros. (Un asterisco indica un parámetro obligatorio).

   Acción de reescritura: si la acción de reescritura que quiere evaluar no está seleccionada, selecciónela en la lista desplegable. Tras seleccionar una acción de reescritura, en la sección Detalles se muestran los detalles de la acción de reescritura seleccionada.
   Nuevo: seleccione Nuevo para abrir el cuadro de diálogo Crear acción de reescritura y crear una acción de reescritura.
   Modificar (Modify): seleccione Modificar para abrir el cuadro de diálogo Configurar acción de reescritura y modificar la acción de reescritura seleccionada.
   Tipo de flujo: especifica si se debe probar la acción de reescritura seleccionada con datos de solicitud HTTP o datos de respuesta HTTP. El valor predeterminado es Solicitud. Si quieres probar con datos de respuesta, seleccione Respuesta.
   Datos de solicitud o respuesta HTTP*: proporciona espacio para proporcionar los datos HTTP que el evaluador de acciones de reescritura utiliza para las pruebas. Puede pegar los datos directamente en la ventana o hacer clic en Muestra para insertar algunos encabezados HTTP de ejemplo.
   Mostrar fin de línea: especifica si se deben mostrar caracteres de final de línea de estilo UNIX (\n) al final de cada línea de datos HTTP de muestra.
   Ejemplo: inserta datos HTTP de ejemplo en la ventana Datos de solicitud/respuesta HTTP. Puede elegir datos GET o POST.
   Examinar: abre una ventana de exploración local para que pueda elegir un archivo que contenga datos HTTP de ejemplo de una ubicación local o de red.
   Borrar: borra los datos HTTP de muestra actuales de la ventana Datos de solicitud/respuesta HTTP.
3. Haga clic en Evaluar. El **evaluador de acciones de reescritura** evalúa el efecto de la acción Reescribir en los datos de ejemplo elegidos y muestra los resultados modificados por la acción **Reescritura** seleccionada en la ventana **Resultados** . Las adiciones y eliminaciones se resaltan como se indica en la leyenda de la esquina inferior izquierda del cuadro de diálogo.
4. Continúa evaluando las acciones de reescritura hasta que hayas determinado que todas tus acciones tienen el efecto que querías.
   - Puede modificar la acción de reescritura seleccionada y probar la versión modificada haciendo clic en **Modificar** para abrir el cuadro de diálogo **Configurar acción de reescritura**, realizar y guardar los cambios y, a continuación, volver a hacer clic en Evaluar.

- Puede evaluar una acción de reescritura diferente con los mismos datos de solicitud o respuesta seleccionándola en la lista desplegable **Acción de reescritura** y, a continuación, haciendo clic en **Evaluar** de nuevo.

5. Haga clic en **Cerrar** para cerrar el **evaluador de reescritura de expresiones** y volver al panel **Acciones de reescritura** .
6. Para eliminar una acción de reescritura, seleccione la acción de reescritura que quiera eliminar y, a continuación, haga clic en **Eliminar** y, cuando se le solicite, confirme su elección haciendo clic en **Aceptar**.



Configurar la directiva de reescritura

Después de crear las acciones de reescritura necesarias, debe crear al menos una directiva de reescritura para seleccionar las solicitudes que quiere que reescriba el dispositivo Citrix ADC.

Una directiva de reescritura consiste en una regla, que a su vez consta de una o más expresiones, y una acción asociada que se lleva a cabo si una solicitud o respuesta coincide con la regla. Las reglas de directiva para evaluar las solicitudes y respuestas HTTP se pueden basar en casi cualquier parte de una solicitud o respuesta.

Aunque no se pueden utilizar acciones de reescritura de TCP para reescribir datos que no sean la carga útil TCP, puede basar las reglas de directiva para las directivas de reescritura de TCP en la información de la capa de transporte y en las capas situadas debajo de la capa de transporte.

Si una regla configurada coincide con una solicitud o respuesta, se desencadena la directiva correspondiente y se lleva a cabo la acción asociada a ella.

> **Nota:**
>
> Puede utilizar la interfaz de línea de comandos o la GUI para crear y configurar directivas de reescritura. Los usuarios que no están completamente familiarizados con la interfaz de línea de comandos y el lenguaje de expresión de directivas de Citrix ADC normalmente encontrarán mucho más fácil utilizar la interfaz gráfica de usuario.

Para agregar una nueva directiva de reescritura mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para agregar una nueva directiva de reescritura y compruebe la configuración:

- `<add rewrite policy <name> <expression> <action> [<undefaction>]`
- `<show rewrite policy <name>`

Ejemplo 1. Reescritura de contenido HTTP

```
> add rewrite policyNew ”HTTP.RES.IS_VALID” insertact NOREWRITE
 Done
> show rewrite policyNew
        Name: policyNew
        Rule: HTTP.RES.IS_VALID
        RewriteAction: insertact
        UndefAction: NOREWRITE
        Hits: 0
        Undef Hits: 0

 Done
<!--NeedCopy-->
```

Ejemplo 2. Reescritura de una carga útil TCP (reescritura TCP):

```
> add rewrite policy client_tcp_payload_policy CLIENT.IP.SRC.EQ
   (172.168.12.232) client_tcp_payload_replace_all
 Done
> show rewrite policy client_tcp_payload_policy
        Name: client_tcp_payload_policy
```



```
5          Rule: CLIENT.IP.SRC.EQ(172.168.12.232)
6          RewriteAction: client_tcp_payload_replace_all
7          UndefAction: Use Global
8          LogAction: Use Global
9          Hits: 0
10         Undef Hits: 0
11
12  Done
13 >
14 <!--NeedCopy-->
```

Para modificar una directiva de reescritura existente mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para modificar una directiva de reescritura existente y compruebe la configuración:

- `<set rewrite policy <name> -rule <expression> -action <action> [<undefaction>]`
- `<show rewrite policy <name>`

Ejemplo:

```
1  > set rewrite policyNew -rule ”HTTP.RES.IS_VALID” -action insertaction
2   Done
3
4  > show rewrite policyNew
5          Name: policyNew
6          Rule: HTTP.RES.IS_VALID
7          RewriteAction: insertaction
8          UndefAction: NOREWRITE
9          Hits: 0
10         Undef Hits: 0
11
12  Done
13 <!--NeedCopy-->
```

Para quitar una directiva de reescritura mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba el siguiente comando para quitar una directiva de reescritura:

`rm rewrite policy <name>`

Ejemplo:


```
> rm rewrite policyNew
Done
<!--NeedCopy-->
```

Para configurar una directiva de reescritura mediante la interfaz gráfica de usuario

1. Vaya a **AppExpert > Rewrite > Policies**.
2. En el panel de detalles, realice una de las acciones siguientes:
   - Para crear una directiva, haga clic en Agregar.
   - Para modificar una directiva existente, selecciónela y, a continuación, haga clic en Abrir.
3. Haga clic en **Crear** o **Aceptar**. Aparece un mensaje en la barra de estado que indica que la directiva se ha configurado correctamente.
4. Repita los pasos 2 a 4 para crear o modificar tantas acciones de reescritura como quiera.
5. Haga clic en **Cerrar**. Para eliminar una directiva de reescritura, seleccione la directiva de reescritura que quiera eliminar, haga clic en **Quitar** y, cuando se le solicite, confirme su elección haciendo clic en **Aceptar**.

Directiva de reescritura de enlaces

Después de crear una directiva de reescritura, debe vincularla para que se aplique. Puede enlazar su directiva a Global si quiere aplicarla a todo el tráfico que pasa por su Citrix ADC, o puede enlazar su directiva a un servidor virtual o punto de enlace específico para dirigir únicamente ese servidor virtual o enlazar el tráfico entrante del punto a esa directiva. Si una solicitud entrante coincide con una directiva de reescritura, se lleva a cabo la acción asociada a esa directiva.

Las directivas de reescritura para evaluar las solicitudes y respuestas HTTP se pueden enlazar a servidores virtuales de tipo HTTP o SSL, o a los puntos de enlace REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE y RES_DEFAULT. Las directivas de reescritura para la reescritura de TCP solo pueden enlazarse a servidores virtuales de tipo TCP o SSL_TCP, o a los puntos de enlace OTHERTCP_REQ_OVERRIDE, OTHERTCP_REQ_DEFAULT, OTHERTCP_RES_OVERRIDE y OTHERTCP_RES_DEFAULT.

> **Nota:**
>
> El término OTHERTCP se utiliza en el contexto del dispositivo Citrix ADC para referirse a todas las solicitudes y respuestas TCP o SSL_TCP que quiere tratar como un flujo de bytes sin procesar, independientemente de los protocolos que encapsulen los paquetes TCP.

Cuando vincula una directiva, le asigna una prioridad. La prioridad determina el orden en que se evalúan las directivas que defina. Puede establecer la prioridad en cualquier número entero positivo.

En el sistema operativo Citrix ADC, las prioridades de las directivas funcionan en orden inverso: cuanto mayor sea el número, menor será la prioridad. Por ejemplo, si tiene tres directivas con prioridades de

10, 100 y 1000, la directiva asignada con una prioridad de 10 se aplica primero, luego a la directiva se le asigna una prioridad de 100 y, por último, a la directiva se le asigna un orden de 1000.

A diferencia de la mayoría de las demás funciones del sistema operativo Citrix ADC, la función de reescritura continúa evaluando e implementando directivas después de que una solicitud coincida con una directiva. Sin embargo, el efecto de una directiva de acción concreta en una solicitud o respuesta suele ser diferente en función de si se realiza antes o después de otra acción. La prioridad es importante para obtener los resultados deseados.

Puede dejar suficiente espacio para agregar otras directivas en cualquier orden y configurarlas para que se evalúen en el orden que quiera, estableciendo prioridades con intervalos de 50 o 100 entre cada directiva cuando la vincule. Si lo hace, puede agregar más directivas en cualquier momento sin tener que reasignar la prioridad de una directiva existente.

Al enlazar una directiva de reescritura, también tiene la opción de asignar una expresión goto (goToPriorityExpression) a la directiva. Una expresión goto puede ser cualquier entero positivo que coincida con la prioridad asignada a una directiva diferente que tenga una prioridad superior a la directiva que contiene la expresión goto. Si asigna una expresión goto a una directiva y una solicitud o respuesta coincide con la directiva, Citrix ADC irá inmediatamente a la directiva cuya prioridad coincida con la expresión goto. Omitirá todas las directivas con números de prioridad inferiores a los de la directiva actual, pero superiores al número de prioridad de la expresión goto, y no las evalúa.

Para enlazar globalmente una directiva de reescritura mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para enlazar globalmente una directiva de reescritura y compruebe la configuración:

- `bind rewrite global <policyName> <priority> [<gotoPriorityExpression>] [-type <type>] [-invoke (<labelType> <labelName>)]`
- `show rewrite global`

Ejemplo:

```
>bind rewrite global policyNew 10
 Done

> show rewrite global
1)      Global bindpoint: RES_DEFAULT
        Number of bound policies: 1

2)      Global bindpoint: REQ_OVERRIDE
        Number of bound policies: 1

 Done
<!--NeedCopy-->
```


Para enlazar la directiva de reescritura a un servidor virtual específico mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para enlazar la directiva de reescritura a un servidor virtual específico y compruebe la configuración:

- `bind lb vserver <name>@ (<serviceName>@ [-weight <positive_integer>])| <serviceGroupName>@ | (-policyName <string>@ [-priority <positive_integer>] [-gotoPriorityExpression <expression>] [-type ( REQUEST | RESPONSE )] [-invoke (<labelType> <labelName>)] )`
- `show lb vserver <name>`

Ejemplo:

```
> bind lb vserver lbvip -policyName ns_cmp_msapp -priority 50
 Done
>
> show lb vserver lbvip
        lbvip (8.7.6.6:80) - HTTP       Type: ADDRESS
        State: DOWN
        Last state change was at Wed Jul 15 05:54:24 2009 (+226 ms)
        Time since last state change: 28 days, 01:57:26.350
        Effective State: DOWN
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Port Rewrite : DISABLED
        No. of Bound Services :  0 (Total)       0 (Active)
        Configured Method: LEASTCONNECTION
        Mode: IP
        Persistence: NONE
        Vserver IP and Port insertion: OFF
        Push: DISABLED  Push VServer:
        Push Multi Clients: NO
        Push Label Rule: none

1)      Policy : ns_cmp_msapp Priority:50
2)      Policy : cf-pol Priority:1      Inherited
 Done
<!--NeedCopy-->
```

Para enlazar una directiva de reescritura a un punto de enlace mediante la interfaz gráfica de usuario

1. Vaya a **AppExpert** >**Reescribir** > **Directivas**.
2. En el panel de detalles, seleccione la directiva de reescritura que quiere enlazar globalmente y, a continuación, haga clic en **Administrador de directivas**.
3. En el cuadro de diálogo **Reescribir el Administrador de directivas**, en el menú **Enlazar puntos**, realice una de las siguientes acciones:
   a) Si quiere configurar enlaces para directivas de reescritura HTTP, haga clic en **HTTP**y, a continuación, en **Solicitud** o **Respuesta**, en función de si quiere configurar directivas de reescritura basadas en solicitudes o directivas de reescritura basadas en respuestas.
   b) Si quiere configurar enlaces para directivas de reescritura TCP, haga clic en **TCP**y, a continuación, haga clic en **Cliente** o **Servidor**, en función de si quiere configurar directivas de reescritura TCP del lado del cliente o directivas de reescritura TCP del lado del servidor.
4. Haga clic en el punto de enlace al que quiere enlazar la directiva de reescritura. El cuadro de diálogo **Rewrite Policy Manager** muestra todas las directivas de reescritura enlazadas al punto de enlace seleccionado.
5. Haga clic en **Insertar directiva** para insertar una nueva fila y mostrar una lista desplegable con todas las directivas de reescritura independientes disponibles.
6. Haga clic en la directiva que quiera enlazar al punto de enlace. La directiva se inserta en la lista de directivas de reescritura vinculadas al punto de enlace.
7. En la columna **Prioridad**, puede cambiar la prioridad a cualquier entero positivo. Para obtener más información sobre este parámetro, consulte prioridad en “Parámetros para vincular una directiva de reescritura”. “
8. Si quiere omitir directivas e ir directamente a una directiva específica si la directiva actual coincide, cambie el valor de la columna Goto Expression para que sea igual a la prioridad de la siguiente directiva que se aplicará. Para obtener más información sobre este parámetro, consulte GoToPriorityExpression en “Parámetros para vincular una directiva de reescritura. “
9. Para modificar una directiva, haga clic en la directiva y, a continuación, haga clic en **Modificar directiva**.
10. Para desvincular una directiva, haga clic en la directiva y, a continuación, haga clic en **Desvincular directiva**.
11. Para modificar una acción, en la columna Acción, haga clic en la acción que quiera modificar y, a continuación, haga clic en **Modificar acción**.
12. Para modificar una etiqueta de invocación, en la columna **Invocar**, haga clic en la etiqueta de invocación que quiera modificar y, a continuación, haga clic en **Modificar etiqueta de invocación**.
13. Para regenerar las prioridades de todas las directivas enlazadas al punto de enlace que está configurando actualmente, haga clic en **Regenerar prioridades**. Las directivas mantienen sus prioridades existentes en relación con las demás directivas, pero las prioridades se renumeran en múltiplos de 10.
14. Haga clic en **Aplicar cambios**.

15. Haga clic en **Cerrar**. Aparece un mensaje en la barra de estado que indica que la directiva se ha configurado correctamente.

Para enlazar una directiva de reescritura a un servidor virtual específico mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**.
2. En la lista de servidores virtuales del panel de detalles, seleccione el servidor virtual al que quiere enlazar la directiva de reescritura y, a continuación, haga clic en **Abrir**.
3. En el cuadro de diálogo **Configurar servidor virtual (equilibrio de carga)**, seleccione la ficha **Directivas** . Todas las directivas configuradas en su Citrix ADC aparecen en la lista.
4. Seleccione la casilla de verificación situada junto al nombre de la directiva que quiere enlazar a este servidor virtual.
5. Haga clic en **OK**. Aparece un mensaje en la barra de estado que indica que la directiva se ha configurado correctamente.

Configurar etiquetas de directivas de reescritura

Si quiere crear una estructura de directivas más compleja que la admitida por directivas individuales, puede crear rótulos de directiva y, a continuación, enlazarlos como lo haría con directivas. Una etiqueta de directiva es un punto definido por el usuario al que están vinculadas las directivas. Cuando se invoca una etiqueta de directiva, todas las directivas vinculadas a ella se evalúan en el orden de prioridad configurado. Una etiqueta de directiva puede incluir una o varias directivas, a cada una de las cuales se le puede asignar su propio resultado. Una coincidencia en una directiva del rótulo de directiva puede dar lugar a pasar a la siguiente directiva, invocar una etiqueta de directiva diferente o un recurso apropiado, o poner fin inmediatamente a la evaluación de la directiva y devolver el control a la directiva que invocó la etiqueta de directiva.

Una etiqueta de directiva de reescritura consta de un nombre, un nombre de transformación que describe el tipo de directiva incluida en la etiqueta de directiva y una lista de directivas enlazadas a la etiqueta de directiva. Cada directiva enlazada a la etiqueta de directiva contiene todos los elementos descritos en Configuración de una directiva de reescritura.

Nota: Puede utilizar la interfaz de línea de comandos o la GUI para crear y configurar etiquetas de directivas de reescritura. Los usuarios que no están completamente familiarizados con la interfaz de línea de comandos y el lenguaje de infraestructura de directivas (PI) de Citrix ADC suelen encontrar mucho más fácil utilizar la interfaz gráfica de usuario.

Para configurar una etiqueta de directiva de reescritura mediante la interfaz de línea de comandos

Para agregar una etiqueta de directiva de reescritura, en el símbolo del sistema, escriba el siguiente comando:

```
add rewrite policylabel <labelName> <transform>
```


Por ejemplo, para agregar una etiqueta de directiva de reescritura denominada PollabelHttpResponses para agrupar todas las directivas que funcionan con respuestas HTTP, debe escribir lo siguiente:

```
add rewrite policy label polLabelHTTPResponses http_res
```

Para modificar una etiqueta de directiva de reescritura existente, en el símbolo del sistema de **Citrix ADC**, escriba el siguiente comando:

```
set rewrite policy <name> <transform>
```

> **Nota:**
>
> El comando set rewrite policy utiliza las mismas opciones que el comando add rewrite policy.

Para quitar una etiqueta de directiva de reescritura, en el símbolo del sistema de **Citrix ADC**, escriba el siguiente comando:

```
rm rewrite policy<name>
```

Por ejemplo, para quitar una etiqueta de directiva de reescritura denominada PollabelHttpResponses, escribiría lo siguiente:

```
rm rewrite policy polLabelHTTPResponses
```

Para configurar una etiqueta de directiva de reescritura mediante la interfaz gráfica de usuario

1. Vaya a **AppExpert** > **Reescribir** > **Etiquetas de directivas**.
2. En el panel de detalles, realice una de las acciones siguientes:
   - Para crear una etiqueta de directiva, haga clic en **Agregar**.
   - Para modificar una etiqueta de directiva existente, selecciónela y, a continuación, haga clic en **Abrir**.
3. Agregar o quitar directivas de la lista vinculada a la etiqueta de directiva.
   - Para agregar una directiva a la lista, haga clic en **Insertar directiva** y elija una directiva en la lista desplegable. Puede crear una directiva y agregarla a la lista si selecciona Nueva directiva en la lista y sigue las instrucciones de Configuración de una directiva de reescritura.
   - Para quitar una directiva de la lista, selecciónela y, a continuación, haga clic en Desenlazar directiva.
4. Modifique la prioridad de cada directiva editando el número de la columna Prioridad.
   También puede volver a numerar las directivas automáticamente haciendo clic en Regenerar prioridades.
5. Haga clic en **Crear** o **Aceptar**y, a continuación, en **Cerrar**.
   Para quitar una etiqueta de directiva, selecciónela y, a continuación, haga clic en **Quitar**. Para cambiar el nombre de una etiqueta de directiva, selecciónela y haga clic en **Cambiar nombre**. Modifique el nombre de la directiva y, a continuación, haga clic en **Aceptar** para guardar los cambios.

Ejemplos de directivas y acciones de reescritura

January 19, 2021

Los ejemplos de esta sección muestran cómo configurar la reescritura para realizar varias tareas útiles. Los ejemplos se dan en la sala de servidores de Example Manufacturing Inc., una empresa de fabricación de tamaño mediano que utiliza su sitio web para administrar una parte considerable de sus ventas, entregas y asistencia al cliente.

Ejemplo de fabricación tiene dos dominios: Example.com para su sitio web y correo electrónico a los clientes, y example.net para su intranet. Los clientes utilizan el sitio web de ejemplo para realizar pedidos, solicitar presupuestos, investigar productos y ponerse en contacto con el servicio al cliente y el soporte técnico.

Como parte importante del flujo de ingresos de ejemplo, el sitio web debe responder rápidamente y mantener la confidencialidad de los datos del cliente. Ejemplo, por lo tanto, tiene varios servidores web y utiliza dispositivos Citrix ADC para equilibrar la carga del sitio web y administrar el tráfico hacia y desde sus servidores web.

Los administradores de sistema de ejemplo utilizan las funciones de reescritura para realizar las siguientes tareas:

Ejemplo 1: Eliminar antiguos encabezados de IP de cliente y X-Forwarded-For

Example Inc. elimina los encabezados HTTP X-Forwarded-For y Client-IP HTTP de las solicitudes entrantes.

Ejemplo 2: Agregar un encabezado IP de cliente local

Example Inc. agrega un nuevo encabezado IP de cliente local a las solicitudes entrantes.

Ejemplo 3: Etiquetado de conexiones seguras e inseguras

Example Inc. etiqueta las solicitudes entrantes con un encabezado que indica si la conexión es una conexión segura.

Ejemplo 4: Enmascarar el tipo de servidor HTTP

Example Inc. modifica el encabezado HTTP Server: Para que los usuarios no autorizados y el código malintencionado no puedan utilizar ese encabezado para determinar el software del servidor HTTP que utiliza.

Ejemplo 5: Redirigir una URL externa a una URL interna

Example Inc. oculta información sobre los nombres reales de sus servidores web y la configuración de su sala de servidores a los usuarios, para hacer que las URL de su sitio web sean más cortas y fáciles de recordar y para mejorar la seguridad de su sitio.

Ejemplo 6: Migración de reglas del módulo de reescritura de Apache

Example Inc. movió sus reglas de reescritura de Apache a un dispositivo Citrix ADC, traduciendo la sintaxis de script basada en Apache Perl a la sintaxis de regla de reescritura de Citrix ADC.

Ejemplo 7: Redirección de palabras clave de marketing

El departamento de marketing de Example Inc. establece URL simplificadas para ciertas búsquedas de palabras clave predefinidas en el sitio web de la empresa.

Ejemplo 8: Redirigir las consultas al servidor consultado.

Example Inc. redirige ciertas solicitudes de consulta al servidor apropiado.

Ejemplo 9: Redirección de la página principal

Example Inc. adquirió recientemente un competidor más pequeño, y ahora redirige las solicitudes a la página principal de la empresa adquirida a una página en su propio sitio web.

Ejemplo 10: Cifrado RSA basado en directivas

Example Inc. encripta el contenido de encabezado o cuerpo HTTP predefinido y definido por el usuario mediante la clave pública PEM RSA.

Cada una de estas tareas requiere que los administradores del sistema creen acciones y directivas de reescritura y las vinculen a un punto de enlace válido en Citrix ADC.

Ejemplo 1: Eliminar encabezados antiguos X-Forwarded-For y Client-IP

February 19, 2022

Example Inc. quiere eliminar los encabezados HTTP X-Forwarded-For y Client-IP de las solicitudes entrantes, de modo que los únicos encabezados X-Forwarded-For que aparecen sean los agregados por el servidor local. Esta configuración se puede realizar a través de la línea de comandos de Citrix ADC o de la utilidad de configuración. El administrador del sistema de Example Inc. es un ingeniero de redes de la antigua escuela y prefiere usar una CLI siempre que sea posible, pero quiere asegurarse de que entiende la interfaz de la utilidad de configuración para que pueda mostrar a los nuevos administradores del sistema en el equipo cómo usarla.

Los ejemplos siguientes muestran cómo realizar cada configuración con la CLI y la utilidad de configuración. Los procedimientos se abrevian en el supuesto de que los usuarios ya conocerán los conceptos básicos de crear acciones de reescritura, crear directivas de reescritura y directivas de enlace.

- Para obtener información más detallada sobre la creación de acciones de reescritura, consulte Configuración de una acción de reescritura.
- Para obtener información más detallada sobre la creación de directivas de reescritura, consulte Configuración de una directiva de reescritura.

- Para obtener información más detallada sobre las directivas de reescritura de enlaces, consulte Vinculación de una directiva de reescritura.

Para eliminar los encabezados X-Rewarded y Client-IP antiguos de una solicitud mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos en el orden mostrado:

```
add rewrite action act_del_xfor delete_http_header x-forwarded-for
add rewrite action act_del_cip delete_http_header client-ip
add rewrite policy pol_check_xfor 'HTTP.REQ.HEADER(”x-forwarded-for”).
    EXISTS' act_del_xfor
add rewrite policy pol_check_cip 'HTTP.REQ.HEADER(”client-ip”).EXISTS'
    act_del_cip
bind rewrite global pol_check_xfor 100 200
bind rewrite global pol_check_cip 200 300
<!--NeedCopy-->
```

Para eliminar los encabezados X-Rewarded y Client-IP antiguos de una solicitud mediante la utilidad de configuración

En el cuadro de diálogo Crear acción de reescritura, cree dos acciones de reescritura con las siguientes descripciones.

Nombre	Tipo	Argumentos
act_del_xfor	delete_http_header	x-forwarded-para
act_del_cip	delete_http_header	cliente-ip

En el cuadro de diálogo Crear directiva de reescritura, cree dos directivas de reescritura con las siguientes descripciones.

Nombre	Expresión	Action
pol_check_xfor	‘HTTP.REQ.HEADER (“x-forwarded-for”).EXIST’	act_del_xfor
pol_check_cip	‘HTTP.REQ.HEADER (“cliente-ip”).EXIST’	act_del_cip

Enlazar ambas directivas a global, asignando las prioridades y goto valores de expresión que se muestran a continuación.

Nombre	Prioridad	Expresión de GoTo
pol_check_xfor	100	200
pol_check_cip	200	300

Todos los antiguos encabezados HTTP X-Forwarded-For y Client-IP HTTP ahora se eliminan de las solicitudes entrantes.

Ejemplo 2: Agregar un encabezado IP de cliente local

August 20, 2021

Example Inc. quiere agregar un encabezado HTTP de IP cliente local a las solicitudes entrantes. Este ejemplo contiene dos versiones ligeramente diferentes de la misma tarea básica.

Para agregar un encabezado IP de cliente local mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos en el orden mostrado:

```
1 add rewrite action act_ins_client insert_http_header NS-Client 'CLIENT.
     IP.SRC'
2 add rewrite policy pol_ins_client 'HTTP.REQ.HEADER(”x-forwarded-for”).
     EXISTS || HTTP.REQ.HEADER(”client-ip”).EXISTS' act_ins_client
3 bind rewrite global pol_ins_client 300 END
4 <!--NeedCopy-->
```

Para agregar un encabezado IP de cliente local mediante la utilidad de configuración

En el cuadro de diálogo Crear acción de reescritura, cree una acción de reescritura con la siguiente descripción.

Nombre	Tipo	Argumentos
act_ins_client	insert_http_header	Cliente NS-‘ CLIENT.IP.SRC ‘

En el cuadro de diálogo Crear directiva de reescritura, cree una directiva de reescritura con la siguiente descripción.

Nombre	Expresión	Action
pol_ins_client	‘HTTP.REQ.HEADER (“x-forwarded-for”).EXISTS || HTTP.REQ.HEADER (“cliente-ip”).EXIST’	act_ins_client

Vincular la directiva a global, asignando las prioridades y goto valores de expresión que se muestran a continuación.

Nombre	Prioridad	Expresión de GoTo
pol_ins_client	100	Siguiente

Ejemplo 3: Etiquetado de conexiones seguras e inseguras

January 12, 2021

Example Inc. quiere etiquetar las solicitudes entrantes con un encabezado que indica si la conexión es o no una conexión segura. Esto ayuda al servidor a realizar un seguimiento de las conexiones seguras después de que Citrix ADC haya descifrado las conexiones.

Para implementar esta configuración, comenzaría creando acciones de reescritura con los valores mostrados en las tablas siguientes. Estas acciones etiquetan las conexiones al puerto 80 como conexiones inseguras y las conexiones al puerto 443 como conexiones seguras.

Nombre de la acción	Tipo de acción de reescritura	Nombre de encabezado	Valor
Action-Rewrite-SSL_YES	INSERT_HTTP_HEADER	SSL	SÍ

Nombre de la acción	Tipo de acción de reescritura	Nombre de encabezado	Valor
Action-Rewrite-SSL_NO	INSERT_HTTP_HEADER	SSL	NO

A continuación, creará una directiva de reescritura con los valores que se muestran en las tablas siguientes. Estas directivas comprueban las solicitudes entrantes para determinar qué solicitudes se dirigen al puerto 80 y cuáles al puerto 443. A continuación, las directivas agregan el encabezado SSL correcto.

Nombre de la directiva	Nombre de la acción	Acción indefinida	Expresión
Policy-Rewrite-SSL_YES	Action-Rewrite-SSL_YES	NOREWRITE	CLIENT.TCP.DSTPORT.EQ (443)
Policy-Rewrite-SSL_NO	Action-Rewrite-SSL_NO	NOREWRITE	CLIENT.TCP.DSTPORT.EQ (80)

Por último, vinculará las directivas de reescritura a Citrix ADC, asignando a la primera directiva una prioridad de 200 y a la segunda una prioridad de 300, y estableciendo la expresión goto de ambas directivas en END.

Cada conexión entrante al puerto 80 ahora tiene un encabezado HTTP SSL:NO agregado y cada conexión entrante al puerto 443 tiene un encabezado HTTP SSL:YES agregado.

Ejemplo 4: enmascarar el tipo de servidor HTTP

October 5, 2021

Example Inc. quiere modificar el encabezado HTTP Server: para que los usuarios no autorizados y el código malintencionado no puedan usar el encabezado para identificar el software que utiliza el servidor HTTP.

Para modificar el encabezado HTTP Server:, crearía una acción de reescritura y una directiva de reescritura con los valores de las tablas siguientes.

Nombre de la acción	Tipo de acción de reescritura	Expresión para elegir la referencia objetivo	Expresión de cadena para texto de sustitución
Server_Mask de reescritura de acción	REEMPLAZAR	HTTP.RES.HEADER(“Se	“Web Server 1.0”

Nombre de la directiva	Nombre de la acción	Acción indefinida	Expresión
Server_Mask de reescritura de directivas	Server_Mask de reescritura de acción	NOREWRITE	HTTP.RES.IS_VALID

Comandos de ejemplo:

```
> add rewrite action Action-Rewrite-Server_Mask REPLACE HTTP.RES.HEADER(”Server”)”\”Web Server 1.0\””
```

```
> add rewrite policy-Rewrite-Server_Mask HTTP.RES.IS_VALID Action-Rewrite-Server_Mask NOREWRITE
```

A continuación, enlazaría globalmente la directiva de reescritura, asignaría una prioridad de 100 y establecería la expresión de prioridad Goto de la directiva en END.

El encabezado HTTP Server: ahora se modifica para que diga “Web Server 1.0”, enmascarando el software de servidor HTTP real utilizado por el sitio web de Example Inc.

Ejemplo 5: Redirigir una URL externa a una URL interna

January 31, 2022

Example Inc. quiere ocultar la configuración real de su sala de servidores a los usuarios para mejorar la seguridad de sus servidores web.

Para mejorar la seguridad, debe crear una acción de reescritura con los valores que se muestran en las tablas siguientes. Para los encabezados de solicitud, la acción de la tabla se modifica `www.example.com` a web.hq.example.net. En el caso de los encabezados de respuesta, la acción hace lo contrario, traduciendo `web.hq.example.net` en `www.example.com`.

Nombre de acción	Tipo de acción de reescritura	Expresión para elegir la referencia objetivo	Expresión de cadena para texto de sustitución
Reescritura de acción Solici-tud_Server_Replace	REEMPLAZAR	HTTP.REQ.HOSTNAME.S	“Web.hq.example.net”
Reescritura de acción Re-sponse_Server_Replace	REEMPLAZAR	HTTP.RES.HEADER(“Server”)	“www.ejemplo.com”

La primera directiva verifica las solicitudes entrantes para ver si son válidas. Si son válidos, lleva a cabo la acción Action-Rewrite-Request_Server_Replace. La segunda directiva comprueba las respuestas para ver si se originan en el servidor `web.hq.example.net`. Si lo hacen, realiza la acción Action-Rewrite-Response_Server_Replace.

Ejemplos de acción y directiva de reescritura para redirigir una URL externa.

```
add rewrite action Action-Rewrite-Request_Server_Replace REPLACE HTTP.REQ.
HOSTNAME.SERVER '”Web.hq.example.net”'
```

```
add rewrite action Action-Rewrite-Response_Server_Replace REPLACE HTTP.RES.
HEADER(”Server”)'”www.example.com”'
```

```
add rewrite policy Rewrite-Request_Server_Replace HTTP.REQ.HOSTNAME.SERVER.
EQ(”www.example.com”)Action-Rewrite-Request_Server_Replace NOREWRITE
```

```
add rewrite policy Rewrite-Response_Server_Replace HTTP.REQ.HEADER(”Server”
).EQ(”Web.hq.example.net”)Action-Rewrite-Response_Server_Replace
```

Por último, debe vincular las directivas de reescritura, asignando a cada una una prioridad de 500 porque están en bancos de directivas diferentes y no entran en conflicto. Establece la expresión goto en SIGUIENTE para ambos enlaces.

```
bind rewrite global Policy-Rewrite-Request_Server_Replace 500 END -type
REQ_DEFAULT
```

```
bind rewrite global Policy-Rewrite-Response_Server_Replace 500 END -type
RES_DEFAULT
```

Todas las instancias de `www.example.com` en los encabezados de solicitud ahora se cambian a `web.hq.example.net`, y todas las instancias de `web.hq.example.net` de encabezados de respuesta ahora se cambian a `www.example.com`.

Ejemplo 6: Migración de reglas del módulo de reescritura de Apache

August 20, 2021

Example Inc., actualmente está usando el módulo de reescritura de Apache para procesar las solicitudes de búsqueda enviadas a sus servidores web y redirigir esas solicitudes al servidor apropiado sobre la base de la información en la URL de solicitud. Example Inc. quiere simplificar su configuración migrando estas reglas a la plataforma Citrix ADC.

A continuación se muestran varias reglas de reescritura de Apache que Ejemplo utiliza actualmente. Estas reglas redirigen las solicitudes de búsqueda a una página de resultados especial si no tienen una cadena SiteID o si tienen una cadena SiteID igual a cero (0), o a la página de resultados estándar si no se aplican estas condiciones.

Las siguientes son las reglas actuales de reescritura de Apache:

- RewriteCond% {REQUEST_FILENAME} ^/search$ [NC]
- RewriteCond% {QUERY_STRING}. siteId= [OR]
- RewriteCond %{QUERY_STRING} SiteId=0
- RewriteCond %{QUERY_STRING} CallName=DisplayResults [NC]
- Reescritura de la regla ^.*$ results2.html [, IP]
- RewriteCond% {REQUEST_FILAME} ^/search$[NC]
- RewriteCond %{QUERY_STRING} CallName=DisplayResults [NC]
- RewriteRule ^.*$ /results.html [, IP]

Para implementar estas reglas de reescritura de Apache en Citrix ADC, debe crear acciones de reescritura con los valores de las tablas siguientes.

Nombre de la acción	Tipo de acción de reescritura	Expresión para elegir la referencia de destino	Expresión de cadena para texto de reemplazo
Action-Rewrite-Display_Results_NulSit	REPLACE	HTTP.REQ.URL	“/results2.html”
Action-Rewrite-Display_Results	REPLACE	HTTP.REQ.URL	“/results2.html”

A continuación, crear directivas de reescritura con los valores como se muestra en las tablas siguientes.

Nombre de la directiva	Nombre de la acción	Acción indefinida	Expresión
Reescritura de directiva-display_resultados_nul	Action-Rewrite-Display_Results_NulSit	NOREWRITE	HTTP.REQ.URL.PATH.SET_TEXT_MOD (IGNORECASE).EQ (“/search”) && (! HTTP.REQ.URL.QUERY.CONTAINS (“siteId=”) || HTTP.REQ.URL.QUERY.CONTAINS (“siteId=0”) || HTTP.REQ.URL.QUERY.SET_TEXT_MO (IGNORE-CASE).CONTAINS (“call-Name=displayResults”))
Reescritura de directiva-Display_Results	Action-Rewrite-Display_Results	NOREWRITE	HTTP.REQ.URL.PATH.SET_TEXT_MOD (IGNORECASE).EQ (“/search”) || HTTP.REQ.URL.QUERY.SET_TEXT_MO (IGNORE-CASE).CONTAINS (“call-Name=displayResults”))

Finalmente, vincularía las directivas de reescritura, asignando a la primera una prioridad de 600 y a la segunda una prioridad de 700, y luego establecería la expresión goto en NEXT para ambos enlaces.

El dispositivo Citrix ADC ahora maneja estas solicitudes de búsqueda exactamente como lo hacía el servidor web antes de migrar las reglas del módulo de reescritura de Apache.

Ejemplo 7: Redirección de palabras clave de marketing

January 12, 2021

El departamento de marketing de Example Inc. quiere configurar direcciones URL simplificadas para determinadas búsquedas de palabras clave predefinidas en el sitio web de la empresa. Para estas palabras clave, quiere redefinir la URL como se muestra a continuación.

- URL externa:

http://www.example.com/\<marketingkeyword\>

- URL interna:

http://www.example.com/go/kwsearch.asp?keyword=\<marketingkeyword\>

Para configurar la redirección de palabras clave de marketing, debe crear una acción de reescritura con los valores de la tabla siguiente.

Nombre de la acción	Tipo de acción de reescritura	Expresión para elegir la ubicación de destino	Expresión de cadena para texto de reemplazo
Action-Rewrite-Modify_URL	INSERT_ANTES	HTTP.REQ.URL.PATH.GE (1)	"" go/k-wsearch.aspkeyword="l"

A continuación, creará una directiva de reescritura con los valores de la tabla siguiente.

Nombre de la directiva	Nombre de la acción	Acción indefinida	Expresión
Reescritura de directivas-modificación_URL	Action-Rewrite-Modify_URL	NOREWRITE	HTTP.REQ.HOSTNAME.SERVER.EQ ("www.example.com")

Finalmente, vincularía la directiva de reescritura, asignándole una prioridad de 800. A diferencia de las directivas de reescritura anteriores, esta directiva debe ser la última en aplicarse a una solicitud que coincida con sus criterios. Por este motivo, el administrador de Citrix ADC establece su Expresión de prioridad GoTo en END.

Cualquier solicitud que utilice una palabra clave de marketing se redirige a la página CGI de búsqueda de palabras clave, después de lo cual se realiza una búsqueda y se omiten todas las directivas restantes.

Ejemplo 8: Redirigir consultas al servidor de consulta

October 5, 2021

Example Inc. quiere redirigir las solicitudes de consulta al servidor apropiado, como se muestra a continuación.

- <Request: GET /query.cgi?server=5HOST: www.example.com

- <Redirect URL: <http://web-5.example.com/>

Para implementar esta redirección, primero debe crear una acción de reescritura con los valores de la tabla siguiente.

Nombre de la acción	Tipo de acción de reescritura	Expresión para elegir la referencia objetivo	Expresión de cadena para texto de sustitución
Acción-Reescritura-Replace_Hostheader	REEMPLAZAR	HTTP.REQ.HEADER(“Ho	“server-“ + plo.com”) HTTP.REQ.URL.QUERY.VALUE(“web”)

A continuación, crearía una directiva de reescritura con los valores de la tabla siguiente.

Nombre de la directiva	Nombre de la acción	Acción indefinida	Expresión
Policy-Rewrite-Replace_Hostheader	Action-Rewrite-Replace_Hostheader	NOREWRITE	HTTP.REQ.HEADER(”Host”).EQ(”www.example.com”)

Comandos de ejemplo:

```
> add rewrite action Action-Rewrite-Server_Mask REPLACE HTTP.RES.HEADER(”Server”)”\”Web Server 1.0\””
Done

> add rewrite policy-Rewrite-Server_Mask HTTP.RES.IS_VALID Action-Rewrite-Server_Mask NOREWRITE
Done
```

Por último, enlazaría la directiva de reescritura, asignándole una prioridad de 900. Dado que esta directiva debe ser la última directiva aplicada a una solicitud que coincida con sus criterios, debe establecer la expresión goto en END.

Las solicitudes entrantes a cualquier URL que comience por <http://www.example.com/query.cgi?server>= se redirigen al número de servidor de la consulta.

Ejemplo 9: Redirección de la página principal

January 12, 2021

New Company, Inc. adquirió recientemente un competidor más pequeño, Empresa comprada, y quiere redirigir la página principal de Empresa comprada a una nueva página en su propio sitio web, como se muestra aquí.

- URL anterior:http://www.purchasedcompany.com/*
- Nueva URL:http://www.newcompany.com/products/page.htm

Para redirigir las solicitudes a la página principal de la empresa comprada, debe crear acciones de reescritura con los valores de la tabla siguiente.

Nombre de la acción	Tipo de acción de reescritura	Expresión para elegir la referencia de destino	Expresión de cadena para texto de reemplazo
Acción-reescritura-reemplazar_URLR	REPLACE	HTTP.REQ.URL.PATH_A	“/products/page.htm”
Action-Rewrite-Replace_Host	REPLACE	HTTP.REQ.HOSTNAME	“www.newcompany.com”

A continuación, creará directivas de reescritura con los valores de la tabla siguiente.

Nombre de la directiva	Nombre de la acción	Acción indefinida	Expresión
Reescritura de directivas: Sustitución de ninguno	Reescritura de acción-Reemplace-Ninguno	NOREWRITE	!HTTP.REQ.HOSTNAME.SERVER.EQ (“www.purchasedcompany.com”)
Reescritura de directivas, reemplazo de host	Action-Rewrite-Replace_Host	NOREWRITE	HTTP.REQ.HOSTNAME.SERVER.EQ (“www.purchasedcompany.com”)
Reescritura de dirección-Reemplazar-URL	Acción-reescritura-reemplazar_URL	NOREWRITE	HTTP.REQ.IS_VALID

Finalmente, vincularía las directivas de reescritura globalmente, asignando a la primera una prioridad de 100, la segunda una prioridad de 200 y la tercera una prioridad de 300. Estas directivas deben ser las últimas directivas aplicadas a una solicitud que coincida con los criterios. Por este motivo, establezca la expresión goto en END para la primera y tercera directiva, y en 300 para la segunda directiva. Esto garantiza que todas las solicitudes restantes se procesen correctamente.

Las solicitudes al antiguo sitio web de la empresa adquirida ahora se redirigen a la página correcta en la página principal de Nueva Empresa.

Ejemplo 10: Cifrado RSA basado en directivas

August 20, 2021

El algoritmo RSA utiliza la función PKEY_ENCRYPT_PEM () para cifrar el contenido de encabezado o cuerpo HTTP predefinido y definido por el usuario. La función solo acepta claves públicas RSA (no claves privadas) y los datos cifrados no pueden ser mayores que la longitud de la clave pública. Cuando los datos que se cifran son más cortos que la longitud de la clave, el algoritmo utiliza el método de relleno RSA_PKCS1.

En un caso de ejemplo, la función se puede utilizar con la función B64ENCODE () en una acción de reescritura para reemplazar un valor de encabezado HTTP con un valor cifrado por una clave pública RSA. A continuación, el destinatario descifra los datos que se están cifrando mediante la clave privada RSA.

Puede implementar la función mediante una directiva de reescritura. Para ello, debe completar las siguientes tareas:

1. Agregar clave pública RSA como expresión de directiva.
2. Crear acción de reescritura.
3. Crear directiva de reescritura.
4. Vincular directiva de reescritura como global.
5. Verificar el cifrado RSA

Cifrado RSA basado en directivas mediante la interfaz de comandos de Citrix ADC

Complete las siguientes tareas para configurar el cifrado RSA basado en directivas mediante la interfaz de comandos de Citrix ADC.

Para agregar clave pública RSA como expresión de directiva mediante la interfaz de comandos de Citrix ADC:

```
1 add policy expression pubkey '"-----BEGIN RSA PUBLIC KEY-----
     MIGJAoGBAKl5vgQEj73Kxp+9
     yn1v5gPR1pnc4oLM2a0kaWwBOsB6rzCIy6znwnvwCY1xRvQhRlJSAyJbloL7wZFIJ2FOR8Cz
     +8ZQWXU2syG+udi4EnWqLgFYowF9zK+o79az597eNPAjsHZ/C2oL/+6qY5a/
     f1z8bQPrHC4GpFfAEJhh/+NnAgMBAAE=-----END RSA PUBLIC KEY-----"'
2 <!--NeedCopy-->
```


Para agregar reescribir una acción para cifrar una solicitud de encabezado HTTP mediante la interfaz de comandos Citrix ADC:

```
add rewrite action encrypt_act insert_http_header encrypted_data
HTTP.REQ.HEADER(”data_to_encrypt”).PKEY_ENCRYPT_PEM(pubkey).B64ENCODE
```

Para agregar una directiva de reescritura mediante la interfaz de comandos de Citrix ADC:

```
1 add rewrite policy encrypt_pol 'HTTP.REQ.HEADER(”data_to_encrypt”).
     EXISTS' encrypt_act
2 <!--NeedCopy-->
```

Para enlazar la directiva de reescritura global mediante la interfaz de comandos de Citrix ADC:

```
bind rewrite global encrypt_pol 10 -type RES_DEFAULT
```

Para verificar el cifrado RSA mediante la interfaz de comandos de Citrix ADC:

```
1  >curl -v -H ”data_to_encrypt: Now is the time that tries men's souls”
      http://10.217.24.7/`
2
3  * About to connect() to 10.217.24.7 port 80 (#0)
4
5  *  Trying 10.217.24.7...
6
7  *  connected
8
9  *  Connected to 10.217.24.7 (10.217.24.7) port 80 (#0)
10
11 > GET / HTTP/1.1
12 > User-Agent: curl/7.24.0 (amd64-portbld-freebsd8.4) libcurl/7.24.0
      OpenSSL/0.9.8y zlib/1.2.3
13 > Host: 10.217.24.7
14 > Accept: \*/\*
15 > data_to_encrypt: Now is the time that tries men's souls
16 >
17 < HTTP/1.1 200 OK
18 < Date: Mon, 09 Oct 2017 05:22:37 GMT
19 < Server: Apache/2.2.24 (FreeBSD) mod_ssl/2.2.24 OpenSSL/0.9.8y DAV/2
20 < Last-Modified: Thu, 20 Feb 2014 20:29:06 GMT
21 < ETag: ”6bd9f2-2c-4f2dc5b570880”
22 < Accept-Ranges: bytes
23 < Content-Length: 44
```



```
< Content-Type: text/html
< encrypted_data: UliegKBJqZd7JdaC49XMLEK1+eQN2rEfevypW91gKvBVlaKM9N9/
   C2BKuztS99SE0xQaisidzN5IgeIcpQMn+
   CiKYVlLzPG1RuhGaqHYzIt6C8A842da7xE4OlV5SHwScqkqZ5aVrXc3EwtUksna7jOLr40aLeXnnB
   /DB11pUAE=
<
* Connection #0 to host 10.217.24.7 left intact
<html><body><h1>It works!</h1></body></html>* Closing connection #0

<!--NeedCopy-->
```

La ejecución posterior de este comando curl con los mismos datos para cifrar muestra que los datos cifrados son diferentes en cada ejecución. Esto se debe a que el relleno inserta bytes aleatorios al comienzo de los datos para cifrar, haciendo que los datos cifrados sean diferentes cada vez.

```
>curl -v -H "data_to_encrypt: Now is the time that tries men's souls"
   http://10.217.24.7/`

< encrypted_data:
   DaOjtl1Pl4DlQKf58MMeL4cFwFvZwhjMqv5aUYM5Iyzk4UpwIYhpRvgTNu2lXEVc1H0tcR1EGC
   /ViQncLc4EbTurCWLbzjce3+fknnMmzF0lRT6ZZXWbMvsNFOxDA1SnuAgwxWXy/
   ooe9Wy6SYsL2oi1sr5wTG+RihDd9zP+P14=

>curl -v -H "data_to_encrypt: Now is the time that tries men's souls"
   http://10.217.24.7/

. . .

< encrypted_data: eej6YbGP68yHn48qFUvi+fkG+OiO8j3yYLScrRBU+
   TPQ8WeDVaWnDNAVLvL0ZYHHAU1W2YDRYb+8
   cdKHLpW36QbI6Q5FfBuWKZSI2hSyUvypTpCoAYcHXFv0ns+tRtg0EPNNj+
   lyGjKQWtFi6K8IXXISoDy42FblKIlaA7gEriY=
<!--NeedCopy-->
```

Cifrado RSA basado en directivas mediante la interfaz gráfica de usuario

La interfaz gráfica de usuario le permite realizar las siguientes tareas:

Para agregar clave pública RSA como expresión de directiva mediante la GUI:

1. Inicie sesión en el dispositivo Citrix ADC y vaya a **Configuraciones** > **AppExpert** > **Expresiones avanzadas**.

2. En el panel de detalles, haga clic en **Agregar** para definir una clave pública RSA como expresión de directiva avanzada.
3. En la página Crear expresión, defina los siguientes parámetros:
   a) Nombre de expresión. Nombre de la expresión avanzada.
   b) Expresión. Defina la clave pública RSA como una expresión avanzada mediante el Editor de expresiones.
   c) Comentarios. Una breve descripción de la expresión.
4. Haga clic en **Crear**.

Para agregar reescribir una acción para cifrar una solicitud de encabezado HTTP mediante la GUI:

1. Inicie sesión en el dispositivo Citrix ADC y vaya a **Configuraciones** > **AppExpert** > **Reescritura** > **Acciones**.
2. En el panel de detalles, haga clic en **Agregar** para agregar una acción de reescritura.
3. En la pantalla **Crear acción de reescritura**, defina los siguientes parámetros:
   a) Name. Nombre de la acción de reescritura.
   b) Tipo. Seleccione el tipo de acción como INSERT_HTTP_HEADER.
   c) Utilice el tipo de acción para insertar un encabezado. Introduzca el nombre del encabezado HTTP que debe reescribirse.
   d) Expresión. Nombre de la expresión de directiva avanzada asociada a la acción.
   e) Comentarios. Breve descripción de la acción de reescritura.
4. Haga clic en **Crear**.

Para agregar una directiva avanzada de reescritura mediante la interfaz gráfica de usuario:

1. Inicie sesión en el dispositivo Citrix ADC y vaya a **Configuraciones** > **AppExpert** > **Reescribir** > **Directivas**.
2. En la página **Volver a escribir directivas**, haga clic en **Agregar** para agregar una directiva de reescritura.
3. En la página **Crear Directiva de Reescritura**, establezca los siguientes parámetros:
   a) Name. Nombre de la directiva de reescritura.
   b) Acción. Nombre de la acción de reescritura que se va a realizar si la solicitud o respuesta coincide con esta directiva de reescritura.
   c) Acción de registro. Nombre de la acción de registro de mensajes que se va a utilizar cuando una solicitud coincide con esta directiva.
   d) Acción de resultado no definido. Acción que se debe realizar si el resultado de la evaluación de directivas no está definido.
   e) Expresión. Nombre de la expresión de directiva avanzada que desencadena la acción.
   f) Comentarios. Breve descripción de la acción de reescritura.
4. Haga clic en **Crear**.

Para vincular la directiva de reescritura global mediante la GUI:

1. Inicie sesión en el dispositivo Citrix ADC y vaya a **Configuraciones** > **AppExpert** > **Reescribir** >

Directivas.

2. En la pantalla **Volver a escribir directivas**, seleccione una directiva de reescritura que quiera enlazar y haga clic en **Administrador de directivas**.
3. En la página Reescribir Policy Manager, en la sección Puntos de enlace, establezca los siguientes parámetros:
   a) Punto de enlace. Seleccione el punto de enlace como Global por defecto.
   b) Protocolo. Seleccione el tipo de protocolo como HTTP.
   c) Tipo de conexión. Seleccione el tipo de conexión como Solicitud.
   d) Haga clic en **Continuar** para ver la sección **Enlace de directivas**.
   e) En la sección **Enlace de directivas**, seleccione la directiva de reescritura y establezca los parámetros de enlace.
4. Haga clic en **Vincular**.

Ejemplo 11: Cifrado RSA basado en directivas sin operación de relleno

August 20, 2021

La función de directiva PKEY_ENCRYPT_PEM_NO_PADDING () utiliza el algoritmo RSA sin operación de relleno antes de realizar el cifrado RSA. La función de directiva funciona igual que la función PKEY_ENCRYPT_PEM (), excepto que utiliza el método RSA_NO_PADDING en lugar de RSA_PKCS1_PADDING. El parámetro pkey es una cadena de texto con una clave pública RSA codificada por PME. Al igual que PKEY_ENCRYPT_PEM (), puede utilizar una expresión de directiva para la clave.

Puede implementar la función mediante una directiva de reescritura. Para ello, debe completar las siguientes tareas:

1. Agregar clave pública RSA como expresión de directiva.
2. Crear acción de reescritura.

Cifrado RSA basado en directivas mediante la interfaz de comandos de Citrix ADC

Complete las siguientes tareas para configurar el cifrado RSA basado en directivas mediante la interfaz de comandos de Citrix ADC.

Para agregar clave pública RSA sin expresión de directiva de relleno mediante la interfaz de comandos Citrix ADC:

```
1 add expression rsa_pub_key_4096 '"-----BEGIN RSA PUBLIC KEY-----" + "
     MIICCgKCAgEArrwBldKd48xrpOSRPMrg+eNAO0ODU6t5b/WYQLdElqNv7WpefBrA" +
```



```
      ”nwI2s619gEU1r4zoLqL7l5ALtt5Z+F0JBYfOzBzOky0GtEJ5iX5GP4QxT65J3nHH” +
       ”4MTF3acmjvXxclmaKXEFlaVIzW7FTr3Luw/CnOjflAB403Q6F9VBVvQmOVYWnqoI”
      + ”+0q1VIg6Q1pAcvdKBiOf85BBofE5EIbZ/1Jt0CdbsV568l+8ve7BnSUncFHoRR3O”
       + ”/VfSsDuNWZf7n3RNMzxEuIA72UGPzNYFQzvcPOdzd0aN7jAXw0mgC/NSvKzGKHlo
      ” + ”mUYYBzlVQdDMZWnd6jSzsBRXSXxsNEy/
      RuXwplrA5epo7JdCoMkfeI4vUXm6MNr8” + ”
      TQdFqIc1pdnOsbRf9ec62XbcfR7P8CDTsmLSaagx3rjenPdB+LTWKw2VUF+YONIg” +
      ”jM3fyFef9ovVhLhS5HvMqFGs8P75W+d7BOIbIu3EngACiEJOpYSsETD4WgPK6Iyv” +
       ”j6cxsLeYMtElTb0fBIIqysCHdmjF3M1lqdqp4dKs3+W798GJZYM5MxZKUzrBi0Xu”
      + ”e7GtSh2aimsfQureUD+0z0RN2umeDsYcA1ghXMclDP+jLS1lnrv0Yvo+TKcm9b8G”
       + ”uR/drbCrCsGyWFW+bsAu3AWz9S6TePurP5unRmNNvXpH5DRgsYl3d50CAwEAAQ
      ==” + ”-----END RSA PUBLIC KEY-----”
<!--NeedCopy-->
```

Para agregar una acción de reescritura para ninguna expresión de directiva de relleno mediante la interfaz de comandos de Citrix ADC:

```
add rewrite action rsa_encrypt_act insertHttpHeader encrypted 'HTTP.REQ.
HEADER(”plaintext”).PKEY_ENCRYPT_PEM_NO_PADDING(rsa_pub_key_4096)
```

Cifrado RSA basado en directivas sin opción de relleno mediante el uso de la interfaz gráfica de usuario

La interfaz gráfica de usuario le permite realizar las siguientes tareas:

Para agregar clave pública RSA para ninguna operación de relleno como expresión de directiva mediante la GUI:

1. Inicie sesión en el dispositivo Citrix ADC y vaya a **Configuraciones** > **AppExpert** > **Expresiones avanzadas**.
2. En el panel de detalles, haga clic en **Agregar** para definir una clave pública RSA como expresión de directiva avanzada.
3. En la página Crear expresión, defina los siguientes parámetros:
   a) Nombre de expresión. Nombre de la expresión avanzada.
   b) Expresión. Defina la clave pública RSA como una expresión avanzada mediante el Editor de expresiones.
      Nota: La longitud máxima de cadena es de 255 caracteres en una expresión de directiva. Para cualquier llave de más de 1024 bits, tienes que romper la llave en trozos más pequeños y concatenar los trozos juntos como “chunk1” + “chunk2” +…
   c) Comentarios. Una breve descripción de la expresión.
4. Haga clic en **Crear**.

Para agregar reescribir una acción mediante la GUI:

1. Inicie sesión en el dispositivo Citrix ADC y vaya a **Configuraciones** > **AppExpert** > **Reescritura** > **Acciones**.
2. En el panel de detalles, haga clic en **Agregar** para agregar una acción de reescritura.
3. En la pantalla **Crear acción de reescritura**, defina los siguientes parámetros:
   a) Name. Nombre de la acción de reescritura.
   b) Tipo. Seleccione el tipo de acción como INSERT_HTTP_HEADER.
   c) Utilice el tipo de acción para insertar un encabezado. Introduzca el nombre del encabezado HTTP que debe reescribirse.
   d) Expresión. Nombre de la expresión de directiva avanzada asociada a la acción.
   e) Comentarios. Breve descripción de la acción de reescritura.
4. Haga clic en **Crear**.

Ejemplo 12: Configure la reescritura para cambiar el nombre de host y la dirección URL en la solicitud del cliente en el dispositivo Citrix ADC

January 12, 2021

La función de reescritura en un dispositivo Citrix ADC se utiliza para convertir la URL disponible en la solicitud del cliente en otra URL que el servidor back-end pueda comprender. Puede obtener los siguientes beneficios mediante la función de reescritura:

- Mejora la seguridad ocultando la URL real en el recurso, que es solicitado por el cliente.
- Impide que el acceso de usuarios no autorizados obtenga acceso a los recursos de red.

Considere un ejemplo en el que otra organización adquiere su organización actual. Se convierte en un trabajo difícil para los administradores informar sobre la nueva dirección web a cada usuario de la organización adquirida. En este caso, el uso de la función de reescritura resulta conveniente cambiar el nombre de host y la URL en las solicitudes de cliente para el sitio web de la organización adquirida. Puede utilizar rewrite para cambiar temporalmente las URL en la solicitud del cliente cuando el sitio web está bajo mantenimiento.

En la siguiente sección se describe el procedimiento para cambiar el nombre de host y la dirección URL en una solicitud de cliente mediante la función de reescritura.

Considere un ejemplo en el que el usuario introduce una`http://www.example.com` URL en el explorador web. El administrador del sitio web quiere que el dispositivo Citrix ADC convierta la dirección URL anterior en la solicitud del cliente como`http://myexample.example.net.in/resource/inventory/s?t=112`.

En el ejemplo anterior, el administrador del sitio web quiere que el dispositivo Citrix ADC reemplace el nombre de dominio “example.com” por “myexample.example.net.in” y la URL por “resource/inven-

tory/s?t=112”.

Realice lo siguiente mediante la CLI

1. Inicie sesión en el dispositivo Citrix ADC con SSH.
2. Agregue acciones de reescritura.
   - `add rewrite action rewrite_host_hdr_act replace ”HTTP.REQ.HEADER(\”Host\”)””\”myexample.example.net.in\””`
   - `add rewrite action rewrite_url_act replace HTTP.REQ.URL.PATH_AND_QUERY ”\”/resource/inventory/s?t=112\””`
3. Agregue directivas de reescritura para las acciones de reescritura.
   - `add rewrite policy rewrite_host_hdr_pol ”HTTP.REQ.HEADER(\”Host\”).CONTAINS(\”www.example.com\”)”rewrite_host_hdr_act`
   - `add rewrite policy rewrite_url_pol ”HTTP.REQ.HEADER(\”Host\”).CONTAINS(\”www.example.com\”)”rewrite_url_act`
4. Enlazar las directivas de reescritura a un servidor virtual.
   - `bind lb vserver rewrite_LB -policyName rewrite_host_hdr_pol -priority 10 -gotoPriorityExpression 20 -type REQUEST`
   - `bind lb vserver rewrite_LB -policyName rewrite_url_pol -priority 20 -gotoPriorityExpression END -type REQUEST`

Transformación de URL

February 19, 2022

La función de transformación de URL proporciona un método para modificar todas las direcciones URL de las solicitudes designadas desde una versión externa vista por usuarios externos a una dirección URL interna vista solo por los servidores web y el personal de TI. Puede redirigir las solicitudes de los usuarios sin problemas, sin exponer su estructura de red a los usuarios. También puede modificar direcciones URL internas complejas que a los usuarios les resulte difícil recordar en direcciones URL externas más simples y fáciles de recordar.

> **Nota**
>
> Antes de poder utilizar la función de transformación de URL, debe habilitar la función de reescritura. Para habilitar la función Reescritura, consulte Habilitación de la función de reescritura.

> La función de transformación de URL reescribe las URL en el cuerpo de respuesta HTML y no se aplica a JavaScript y otras variables.

Para comenzar a configurar la transformación de URL, cree perfiles, cada uno describiendo una transformación específica. Dentro de cada perfil, creará una o varias acciones que describan la transformación en detalle. A continuación, crea directivas, cada una de las cuales identifica un tipo de solicitud HTTP para transformar y asocia cada directiva con un perfil adecuado. Finalmente, vincula globalmente cada directiva para ponerla en vigor.

Configuración de Perfiles de Transformación de URL

January 12, 2021

Un perfil describe una transformación de URL específica como una serie de acciones. El perfil funciona principalmente como contenedor para las acciones, determinando el orden en que se realizan las acciones. La mayoría de las transformaciones transforman un nombre de host externo y una ruta opcional en un nombre de host interno y una ruta de acceso diferente. Las transformaciones más útiles son simples y requieren una sola acción, pero puede utilizar varias acciones para realizar transformaciones complejas.

No puede crear acciones y, a continuación, agregarlas a un perfil. Primero debe crear el perfil y, a continuación, agregarle acciones. En la CLI, crear una acción y configurar la acción son pasos independientes. Crear un perfil y configurar el perfil son pasos independientes tanto en la CLI como en la utilidad de configuración.

Para crear un perfil de transformación de URL mediante la línea de comandos de Citrix ADC

En el símbolo del sistema de Citrix ADC, escriba los siguientes comandos, en el orden mostrado, para crear un perfil de transformación de URL y verificar la configuración. A continuación, puede repetir los comandos segundo y tercero para configurar acciones adicionales:

- `add transform profile <profileName> -type URL [-onlyTransformAbsURLinBody (ON|OFF)] \[-comment <comment>]`
- `add transform action <name> <profileName> <priority>`
- `set transform action <name> [-priority <priority>] [-reqUrlFrom <expression>] [-reqUrlInto <expression>] [-resUrlFrom <expression>] [-resUrlInto <expression>] [-cookieDomainFrom <expression>] [-cookieDomainInto <expression>] [-state (ENABLED|DISABLED)] [-comment "<string>"]`
- `show transform profile <name>`

Ejemplo:

```
> add transform profile shoppingcart -type URL
 Done
> add transform action actshopping shoppingcart 1000
 Done
> set transform action actshopping -priority 1000 -reqUrlFrom 'shopping
   .example.com' -reqUrlInto 'www.example.net/shopping' -resUrlFrom '
   www.example.net/shopping' -resUrlInto 'shopping.example.com' -
   cookieDomainFrom 'example.com' -cookieDomainInto 'example.net' -
   state ENABLED -comment 'URL transformation for shopping cart.'
 Done
> show transform profile shoppingcart
        Name: shoppingcart
                Type: URL       onlyTransformAbsURLinBody: OFF
        Comment:
        Actions:

1)              Priority 1000   Name: actshopping       ENABLED
 Done
<!--NeedCopy-->
```

Para modificar un perfil o una acción de transformación de URL existente mediante la línea de comandos de Citrix ADC

En el símbolo del sistema de Citrix ADC, escriba los siguientes comandos para modificar un perfil o acción de transformación de URL existente y verificar la configuración:

Nota: Utilice un comando set transform profile o set transform action, respectivamente. El comando set transform profile toma los mismos argumentos que el comando add transform profile, y set transform action es el mismo comando que se utilizó para la configuración inicial.

- `set transform action <name> [-priority <priority>] [-reqUrlFrom <expression>] [-reqUrlInto <expression>] [-resUrlFrom <expression>] [-resUrlInto <expression>] [-cookieDomainInto <expression>] [-state (ENABLED|DISABLED)] [-comment ”<string>”]`
- `show transform profile <name>`

Ejemplo:


```
> set transform action actshopping -priority 1000 -reqUrlFrom '
   searching.example.net' -reqUrlInto 'www.example.net/searching' -
   resUrlFrom 'www.example.net/searching' -resUrlInto 'searching.
   example.com' -cookieDomainInto 'example.net' -state ENABLED -comment
    'URL transformation for searching cart.'
 Done
> show transform profile shoppingcart
        Name: shoppingcart
                Type: URL       onlyTransformAbsURLinBody: OFF
        Comment:
        Actions:

1)              Priority 1000   Name: actshopping       ENABLED
 Done
<!--NeedCopy-->
```

Para quitar un perfil de transformación de URL y acciones mediante la línea de comandos de Citrix ADC

Primero elimine todas las acciones asociadas a ese perfil escribiendo el siguiente comando una vez para cada acción:

- rm transform action <name> Una vez que haya eliminado todas las acciones asociadas a un perfil, elimine el perfil como se muestra a continuación.
- perfil de transformación derm<name>

Para crear un perfil de transformación de URL mediante la utilidad de configuración

1. En el panel de navegación, expanda **Reescribir**, expanda Transformación de URL y, a continuación, haga clic en **Perfiles**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En el cuadro de diálogo **Crear perfil de transformación de URL**, escriba o seleccione valores para los parámetros. El contenido del cuadro de diálogo corresponde a los parámetros descritos en “Parámetros para configurar perfiles de transformación de URL” de la siguiente manera (asterisco indica un parámetro requerido):
   - Nombre*: Nombre
   - Comentario—comentario
   - Solo transforma las URL absolutas en el cuerpo de respuesta: OnlyTransformabsurlinBody
4. Haga clic en **Crear** y, a continuación, en **Cerrar**. Aparece un mensaje en la barra de estado que indica que el perfil se ha configurado correctamente.

Para configurar un perfil de transformación de URL y acciones mediante la utilidad de configuración

1. En el panel de navegación, expanda **Reescribir**, expanda Transformación de URL y, a continuación, haga clic en **Perfiles**.
2. En el panel de detalles, seleccione el perfil que quiere configurar y, a continuación, haga clic en **Abrir**.
3. En el cuadro de diálogo **Configurar perfil de transformación de URL**, realice una de las acciones siguientes.
   - Para crear una nueva acción, haga clic en **Agregar**.
   - Para modificar una acción existente, selecciónela y, a continuación, haga clic en **Abrir**.
4. Rellene el cuadro de diálogo **Crear acción** de **transformación de URL o Modificar acción** de transformación de URL escribiendo o seleccionando valores para los parámetros. El contenido del cuadro de diálogo corresponde a los parámetros descritos en "Parámetros para configurar perfiles de transformación de URL" de la siguiente manera (asterisco indica un parámetro requerido):
   - Nombre de acción*: Nombre
   - Comentarios: Comentario
   - Prioridad*: Prioridad
   - Solicitar URL de—RequrlFrom
   - Solicitar URL en: RequrlinTo
   - URL de respuesta de—resUrlFrom
   - URL de respuesta en—resUrlInto
   - Dominio de cookies de—cookieDomainFrom
   - Dominio de cookies en—cookieDomainInto
   - Habilitado—estado
5. Guarde los cambios.
   - Si va a crear una nueva acción, haga clic en **Crear** y, a continuación, en **Cerrar**.
   - Si está modificando una acción existente, haga clic en **Aceptar**.
     Aparece un mensaje en la barra de estado que indica que el perfil se ha configurado correctamente.
6. Repita los pasos 3 a 5 para crear o modificar acciones adicionales.
7. Para eliminar una acción, selecciónela y, a continuación, haga clic en Quitar. Cuando se le solicite, haga clic en Aceptar para confirmar la eliminación.
8. Haga clic en **Aceptar** para guardar los cambios y cerrar el cuadro de diálogo Modificar perfil de transformación de URL.
9. Para eliminar un perfil, seleccione el perfil en el panel de detalles y, a continuación, haga clic en **Quitar**. Cuando se le solicite, haga clic en **Aceptar** para confirmar la eliminación.

Configuración de directivas de transformación de URL

August 20, 2021

Después de crear un perfil de transformación de URL, creará una directiva de transformación de URL para seleccionar las solicitudes y respuestas que el dispositivo Citrix ADC debe transformar mediante el perfil. La transformación de URL considera cada solicitud y la respuesta a ella como una sola unidad, por lo que las directivas de transformación de URL solo se evalúan cuando se recibe una solicitud. Si una directiva coincide, Citrix ADC transforma tanto la solicitud como la respuesta.

Nota: Las funciones de transformación de URL y reescritura no pueden funcionar en el mismo encabezado HTTP durante el procesamiento de solicitudes. Debido a esto, si quiere aplicar una transformación de URL a una solicitud, debe asegurarse de que ninguna de las cabeceras HTTP que modificará esté manipulada por ninguna acción de reescritura.

Para configurar una directiva de transformación de URL mediante la línea de comandos de Citrix ADC

Debe crear una nueva directiva. En la línea de comandos, solo se puede quitar una directiva existente. En el símbolo del sistema de Citrix ADC, escriba los siguientes comandos para configurar una directiva de transformación de URL y verificar la configuración:

- `<add transform policy <name> <rule> <profileName>`
- `<show transform policy <name>`

Ejemplo:

```
1  > add transform policy polsearch  HTTP.REQ.URL.SUFFIX.EQ(”Searching”)
       prosearching
2   Done
3  > show transform policy polsearch
4  1)      Name: polsearch
5          Rule: HTTP.REQ.URL.SUFFIX.EQ(”Searching”)
6          Profile: prosearching
7          Priority: 0
8          Hits: 0
9   Done
10 <!--NeedCopy-->
```


Para quitar una directiva de transformación de URL mediante la línea de comandos de Citrix ADC

En el símbolo del sistema de Citrix ADC, escriba el comando siguiente para quitar una directiva de transformación de URL:

```
rm transform policy <name>
```

Ejemplo:

```
1 > rm transform policy polsearch
2 Done
3 <!--NeedCopy-->
```

Para configurar una directiva de transformación de URL mediante la utilidad de configuración

1. En el panel de navegación, expanda **Volver a escribir**, expanda Transformación de URL y, a continuación, haga clic en **Directivas**.
2. En el panel de detalles, realice una de las acciones siguientes:
   - Para crear una nueva directiva, haga clic en **Agregar**.
   - Para modificar una directiva existente, selecciónela y, a continuación, haga clic en **Abrir**.
3. En el cuadro de diálogo **Crear directiva de transformación** de **URL o Configurar directiva de transformación** de URL, escriba o seleccione valores para los parámetros. El contenido del cuadro de diálogo corresponde a los parámetros descritos en "Parámetros para configurar directivas de transformación de URL" de la siguiente manera (el asterisco indica un parámetro obligatorio):
   - nombre*: Nombre (no se puede cambiar para una directiva configurada previamente).
   - Perfil*: NombreDePerfil
   - expresión—regla

   Si quiere ayuda para crear una expresión para una nueva directiva, puede mantener presionada la tecla Control y presionar la barra espaciadora mientras el cursor se encuentra en el cuadro de texto Expresión. Para crear la expresión, puede escribirla directamente como se describe a continuación, o puede utilizar el cuadro de diálogo Agregar expresión.
4. Haga clic en **Prefijo** y elija el prefijo de la expresión.

   Las opciones disponibles son:
   - HTTP: Protocolo HTTP. Elija esto si quiere examinar algún aspecto de la solicitud que pertenece al protocolo HTTP.

- SYS: Los sitios web protegidos. Elija esta opción si quiere examinar algún aspecto de la solicitud que pertenece al destinatario de la solicitud.
- Cliente: Equipo que envió la solicitud. Elija esto si quiere examinar algún aspecto del remitente de la solicitud.
- Servidor: Equipo al que se envió la solicitud. Elija esto si quiere examinar algún aspecto del destinatario de la solicitud.
- URL: URL de la solicitud. Elija esta opción si quiere examinar algún aspecto de la URL a la que se envió la solicitud.
- Texto: Cualquier cadena de texto de la solicitud. Elija esta opción si quiere examinar una cadena de texto en la solicitud.
- target: Destino de la solicitud. Elija esto si quiere examinar algún aspecto del destino de solicitud.

Después de elegir un prefijo, Citrix ADC muestra una ventana de solicitud de dos partes que muestra las posibles opciones siguientes en la parte superior y una breve explicación de lo que significa la opción seleccionada en la parte inferior. Las opciones dependen del prefijo que haya elegido.

5. Seleccione su próximo período.

Si eligió HTTP como prefijo, sus opciones son REQ, que especifica las solicitudes HTTP, y RES, que especifica las respuestas HTTP. Si elige otro prefijo, sus opciones son más variadas. Para obtener ayuda sobre una opción específica, haga clic en esa opción una vez para mostrar información sobre ella en la ventana de solicitud inferior.

Cuando esté seguro de qué opción quiere, haga doble clic en ella para insertarla en la ventana Expresión.

1. Escriba un punto y, a continuación, continúe seleccionando términos en los cuadros de lista que aparecen a la derecha del cuadro de lista anterior. Escriba las cadenas de texto o los números adecuados en los cuadros de texto que aparecen para solicitarle que introduzca un valor, hasta que finalice la expresión.
2. Haga clic en **Crear** o en **Aceptar**, en función de si está creando una nueva directiva o modificando una existente.
3. Haga clic en **Cerrar**. Aparece un mensaje en la barra de estado que indica que la directiva se ha configurado correctamente.

Para agregar una expresión mediante el cuadro de diálogo Agregar expresión

1. En el cuadro de diálogo **Crear acción de respondedor** o **Configurar acción de respondedor**, haga clic en **Agregar**.

2. En el cuadro de diálogo **Agregar expresión**, en el primer cuadro de lista elija el primer término para la expresión.

    - HTTP. El protocolo HTTP. Elija esto si quiere examinar algún aspecto de la solicitud que pertenece al protocolo HTTP.
    - SYS. Los sitios web protegidos. Elija esta opción si quiere examinar algún aspecto de la solicitud que pertenece al destinatario de la solicitud.
    - CLIENT. El equipo que envió la solicitud. Elija esto si quiere examinar algún aspecto del remitente de la solicitud.
    - SERVER. El equipo al que se envió la solicitud. Elija esto si quiere examinar algún aspecto del destinatario de la solicitud.
    - URL. La URL de la solicitud. Elija esta opción si quiere examinar algún aspecto de la URL a la que se envió la solicitud.
    - TEXT. Cualquier cadena de texto en la solicitud. Elija esta opción si quiere examinar una cadena de texto en la solicitud.
    - TARGET. El destino de la solicitud. Elija esto si quiere examinar algún aspecto del destino de solicitud.
      Cuando elija, el cuadro de lista situado más a la derecha muestra los términos apropiados para la siguiente parte de la expresión.

3. En el segundo cuadro de lista, elija el segundo término para su expresión. Las opciones dependen de la elección que haya realizado en el paso anterior y son apropiadas para el contexto. Después de realizar su segunda elección, la ventana Ayuda situada debajo de la ventana Construir expresión (que estaba en blanco) muestra ayuda que describe el propósito y el uso del término que acaba de elegir.

4. Siga eligiendo términos en los cuadros de lista que aparecen a la derecha del cuadro de lista anterior o escribiendo cadenas o números en los cuadros de texto que aparecen para pedirle que escriba un valor hasta que finalice la expresión.

Directivas de transformación de URL de enlace global

January 12, 2021

Después de configurar las directivas de transformación de URL, las vincula a Global o a un punto de enlace para ponerlas en vigor. Después del enlace, cualquier solicitud o respuesta que coincida con una directiva de transformación de URL se transforma mediante el perfil asociado a dicha directiva.

Cuando vincula una directiva, le asigna una prioridad. La prioridad determina el orden en que se evalúan las directivas definidas. Puede establecer la prioridad en cualquier entero positivo. En el sistema operativo Citrix ADC, las prioridades de directivas funcionan en orden inverso: Cuanto mayor

sea el número, menor será la prioridad.

Dado que la función de transformación de URL implementa solo la primera directiva que coincide con una solicitud, no las directivas adicionales que también podría coincidir, la prioridad de directiva es importante para lograr los resultados deseados. Si asigna a su primera directiva una prioridad baja (como 1000), indica al Citrix ADC que la ejecute solo si otras directivas con una prioridad mayor no coinciden con una solicitud. Si asigna a su primera directiva una prioridad alta (por ejemplo, 1), dígale al Citrix ADC que la ejecute primero y omita cualquier otra directiva que también pueda coincidir. Puede dejar mucho espacio para agregar otras directivas en cualquier orden, sin tener que reasignar prioridades, estableciendo prioridades con intervalos de 50 o 100 entre cada directiva cuando vincule sus directivas globalmente.

Nota: Las directivas de transformación de URL no se pueden vincular a servidores virtuales basados en TCP.

Para enlazar una directiva de transformación de URL mediante la línea de comandos de Citrix ADC

En el símbolo del sistema de Citrix ADC, escriba los siguientes comandos para enlazar globalmente una directiva de transformación de URL y verificar la configuración:

- `bind transform global <policyName> <priority>`
- `show transform global`

Ejemplo:

```
1 > bind transform global polisearching 100
2  Done
3 > show transform global
4 1)      Policy Name: polisearching
5         Priority: 100
6
7  Done
8 <!--NeedCopy-->
```

Para enlazar una directiva de transformación de URL mediante la utilidad de configuración

1. En el panel de navegación, expanda Volver a escribir, Transformación de URL y, a continuación, haga clic en **Directivas.
2. En el panel de detalles, haga clic en **Administrador de directivas**.

3. En el cuadro de diálogo **Transformar Policy Manager**, elija el punto de enlace al que quiere enlazar la directiva**. Las opciones son:
    - **Anular Global.** Las directivas enlazadas a este punto de enlace procesan todo el tráfico de todas las interfaces del dispositivo Citrix ADC y se aplican antes que cualquier otra directiva.
    - **Servidor virtual LB.** Las directivas enlazadas a un servidor virtual de equilibrio de carga se aplican solo al tráfico procesado por ese servidor virtual de equilibrio de carga y se aplican antes de cualquier directiva global predeterminada. Después de seleccionar LB Virtual Server, también debe seleccionar el servidor virtual de equilibrio de carga específico al que quiere enlazar esta directiva.
    - **Servidor virtual CS.** Las directivas enlazadas a un servidor virtual de conmutación de contenido se aplican solo al tráfico procesado por ese servidor virtual de conmutación de contenido y se aplican antes de cualquier directiva global predeterminada. Después de seleccionar CS Virtual Server, también debe seleccionar el servidor virtual de conmutación de contenido específico al que quiere enlazar esta directiva.
    - **Global predeterminada.** Las directivas vinculadas a este punto de enlace procesan todo el tráfico de todas las interfaces del dispositivo Citrix ADC.
    - **Etiqueta de directiva.** Las directivas enlazadas a una etiqueta de directiva procesan el tráfico que la etiqueta de directiva les enruta. La etiqueta de directiva controla el orden en que se aplican las directivas a este tráfico.
4. Seleccione Insertar directiva para insertar una nueva fila y mostrar una lista desplegable con todas las directivas de transformación de URL independientes disponibles.
5. Seleccione la directiva que quiere enlazar o seleccione Nueva directiva para crear una nueva directiva. La directiva que ha seleccionado o creado se inserta en la lista de directivas de transformación de URL enlazadas globalmente.
6. Realice ajustes adicionales en el enlace.
    - Para modificar la prioridad de directiva, haga clic en el campo para habilitarla y, a continuación, escriba una nueva prioridad. También puede seleccionar Regenerar Prioridades para volver a numerar las prioridades de manera uniforme.
    - Para modificar la expresión de directiva, haga doble clic en ese campo para abrir el cuadro de diálogo Configurar directiva de transformación, donde puede modificar la expresión de directiva.
    - Para establecer la expresión Goto, haga doble clic en el campo del encabezado de columna Goto Expression para mostrar la lista desplegable, donde puede elegir una expresión.
    - Para establecer la opción Invocar, haga doble clic en el campo del encabezado de columna Invocar para mostrar la lista desplegable, donde puede elegir una expresión.
7. Repita los pasos 3 a 6 para agregar cualquier directiva de transformación de URL adicional que quiera enlazar globalmente.
8. Haga clic en **Aceptar** para guardar los cambios. Aparece un mensaje en la barra de estado que

indica que la directiva se ha configurado correctamente.

Compatibilidad con RADIUS para la función de reescritura

August 20, 2021

El lenguaje de expresiones Citrix ADC incluye expresiones que pueden extraer información y manipular mensajes RADIUS en solicitudes y respuestas. Estas expresiones permiten utilizar la función de reescritura para modificar partes de un mensaje RADIUS antes de enviarlo a su destino. Las directivas y acciones de reescritura pueden utilizar cualquier expresión que sea apropiada o relevante para un mensaje RADIUS. Las expresiones disponibles permiten identificar el tipo de mensaje RADIUS, extraer cualquier par atributo-valor (AVP) de la conexión y modificar AVP RADIUS. También puede crear etiquetas de directiva para conexiones RADIUS.

Puede utilizar las nuevas expresiones RADIUS en Reglas de reescritura para varios propósitos. Por ejemplo, podría:

- Elimine la parte de dominio del nombre de usuario AVP de RADIUS para simplificar el inicio de sesión único (SSO).
- Inserte un AVP específico del proveedor, como el campo MSISDN utilizado en las operaciones de la compañía telefónica para contener información del suscriptor.

También puede crear etiquetas de directiva para enrutar tipos específicos de solicitudes RADIUS a través de una serie de directivas adecuadas para dichas solicitudes.

> **Nota**:
>
> RADIUS for Rewrite tiene las siguientes limitaciones:

- Citrix ADC no vuelve a firmar solicitudes o respuestas RADIUS reescritas. Si el servidor de autenticación RADIUS requiere mensajes RADIUS firmados, la autenticación fallará.
- Las expresiones RADIUS disponibles actualmente no funcionan con atributos RADIUS IPv6.

La documentación de Citrix ADC para expresiones compatibles con RADIUS asume la familiaridad con la estructura básica y el propósito de las comunicaciones RADIUS. Si necesita más información sobre RADIUS, consulte la documentación del servidor RADIUS o busque en línea una introducción al protocolo RADIUS.

Configuración de directivas de reescritura para RADIUS

El procedimiento siguiente utiliza la línea de comandos de Citrix ADC para configurar una acción y una directiva de reescritura y enlazar la directiva a un punto de enlace global específico de reescritura.

Para configurar una acción y una directiva de reescritura y enlazar la directiva:

En el símbolo del sistema, escriba los siguientes comandos:

- `add rewrite action <actName> <actType>`
- `add rewrite policy <polName> <rule> <actName>`
- `bind rewrite policy <polName> <priority> <nextExpr> -type <bindPoint>` donde `<bindPoint>` representa uno de los puntos de enlace globales específicos de reescritura.

Expresiones RADIUS para reescritura

En una configuración de reescritura, puede utilizar las siguientes expresiones Citrix ADC para hacer referencia a varias partes de una solicitud o respuesta RADIUS.

Identificación del tipo de conexión:

- `RADIUS.IS_CLIENT`

  Devuelve TRUE si la conexión es un mensaje de cliente (solicitud) RADIUS.

- `RADIUS.IS_SERVER`

  Devuelve TRUE si la conexión es un mensaje de servidor RADIUS (respuesta).

Expresiones de solicitud:

- `RADIUS.REQ.CODE`

  Devuelve el número que corresponde al tipo de solicitud RADIUS. Una derivada de la clase num_at. Por ejemplo, una solicitud de acceso RADIUS devolvería 1 (uno). Una solicitud de contabilidad RADIUS devolvería 4.

- `RADIUS.REQ.LENGTH`

  Devuelve la longitud de la solicitud RADIUS, incluido el encabezado. Una derivada de la clase num_at.

- `RADIUS.REQ.IDENTIFIER`

  Devuelve el identificador de solicitud RADIUS, un número asignado a cada solicitud que permite que la solicitud coincida con la respuesta correspondiente. Una derivada de la clase num_at.

- `RADIUS.REQ.AVP(<AVP Code No>).VALUE`

  Devuelve el valor de la primera aparición de este AVP como una cadena de tipo text_t.

- `RADIUS.REQ.AVP(<AVP code no>).INSTANCE(instance number)`

  Devuelve la instancia especificada del AVP como una cadena de tipo RAVP_T. Un AVP RADIUS específico puede aparecer varias veces en un mensaje RADIUS. INSTANCE (0) devuelve la primera

instancia, INSTANCE (1) devuelve la segunda instancia, y así sucesivamente, hasta dieciséis instancias.

- `RADIUS.REQ.AVP(<AVP code no>).VALUE(instance number)`

  Devuelve el valor de la instancia especificada del AVP como una cadena de tipo text_t.

- `RADIUS.REQ.AVP(<AVP code no>).COUNT`

  Devuelve el número de instancias de un AVP específico en una conexión RADIUS, como un entero.

- `RADIUS.REQ.AVP(<AVP code no>).EXISTS`

  Devuelve TRUE si el tipo especificado de AVP existe en el mensaje, o FALSE si no lo hace.

Expresiones de respuesta:

Las expresiones de respuesta RADIUS son idénticas a las expresiones de solicitud RADIUS, excepto que RES reemplaza a REQ.

Conversión de tipos de valores AVP:

El ADC admite expresiones para convertir valores AVP RADIUS en los tipos de datos de texto, entero, entero sin signo, largo, sin signo, dirección IPv4, dirección ipv6, prefijo ipv6 y tiempo. La sintaxis es la misma que para otras expresiones de conversión de tipos de Citrix ADC.

Ejemplo:

El ADC admite expresiones para convertir valores AVP RADIUS en los tipos de datos de texto, entero, entero sin signo, largo, sin signo, dirección IPv4, dirección ipv6, prefijo ipv6 y tiempo. La sintaxis es la misma que para otras expresiones de conversión de tipos de Citrix ADC.

```
1 RADIUS.REQ.AVP(8).VALUE(0).typecast_ip_address_at
2 <!--NeedCopy-->
```

Expresiones de tipo AVP:

Citrix ADC admite expresiones para extraer valores AVP de RADIUS mediante los códigos enteros asignados descritos en RFC2865 y RFC2866. También puede utilizar alias de texto para realizar la misma tarea. A continuación se presentan algunos ejemplos.

- `RADIUS.REQ.AVP (1).VALUE or RADIUS.REQ.USERNAME.value`

  Extrae el valor de nombre de usuario RADIUS.

- `RADIUS.REQ.AVP (4). VALUE or RADIUS.REQ. ACCT\\_SESSION\\_ID.value`

  Extrae el AVP ACCT-session-ID (código 44) del mensaje.

- `RADIUS.REQ.AVP (26). VALUE or RADIUS.REQ.VENDOR\\_SPECIFIC.VALUE`

  Extrae el valor específico del proveedor.

Los valores de los AVP RADIUS más utilizados se pueden extraer de la misma manera.

Puntos de enlace RADIUS:

Hay cuatro puntos de enlace globales disponibles para las directivas que contienen expresiones RADIUS.

- `RADIUS_REQ_OVERRIDE`

  Prioridad o anulación de la cola de directivas de solicitud.

- `RADIUS_REQ_DEFAULT`

  Cola de directivas de solicitudes estándar.

- `RADIUS_RES_OVERRIDE`

  Prioridad o anulación de la cola de directivas de respuesta.

- `RADIUS_RES_DEFAULT`

  Cola de directivas de respuesta estándar.

Expresiones específicas de reescritura de RADIUS:

- `RADIUS.NEW_AVP`

  Devuelve el AVP RADIUS especificado como una cadena.

- `RADIUS.NEW_AVP_INTEGER32`

  Devuelve el AVP RADIUS especificado como un entero.

- `RADIUS.NEW_AVP_UNSIGNED32`

  Devuelve el AVP RADIUS especificado como un entero sin signo.

- `RADIUS.NEW_VENDOR_SPEC_AVP(<ID>, <definition>)`

  Agrega los AVP específicos de proveedor extendido especificados a la conexión. Para, `<ID>` sustituya un número largo. Para, `<definition>`sustituya una cadena que contenga los datos para el AVP.

- `RADIUS.REQ.AVP_START`

  Devuelve la ubicación entre el final del encabezado RADIUS y el inicio de los AVP. Se utiliza en acciones de reescritura.

  Ejemplo:


```
1     add rewrite action insert1 insert_after radius.req.avp_start radius
          .new_avp(33, ”NEW AVP”)
2 <!--NeedCopy-->
```

- `RADIUS.REQ.AVP_END`

  Devuelve la ubicación al final del mensaje de radio (o, en otras palabras, al final de todos los AVP) en el mensaje de radio. Se utiliza al realizar acciones de reescritura.

  Ejemplo:

```
1     add rewrite action insert2 insert_before radius.req.avp_end ”radius
          .new_avp(33, ”NEW AVP”)”
2 <!--NeedCopy-->
```

- `RADIUS.REQ.AVP_LIST`

  Devuelve la ubicación al inicio de los AVP en un mensaje RADIUS y la longitud del mensaje RADIUS, excluyendo el encabezado. En otras palabras, devuelve todos los AVP de un mensaje RADIUS. Se utiliza para realizar acciones de reescritura.

  Ejemplo:

```
1     add rewrite action insert3 insert_before_all radius.req.avp_list ”
          radius.new_avp(33, ”NEW AVP”)” -search ”avp(33)”
2 <!--NeedCopy-->
```

Tipos de acción de reescritura válidos para RADIUS:

Los tipos de acción Rewrite que se pueden utilizar con expresiones RADIUS son:

- INSERT_AFTER
- INSERT_ANTES
- INSERT_AFTER_ALL
- INSERT_BEFORE_ALL
- SUPRIMIR
- DELETE_ALL
- REPLACE
- REPLACE_ALL

Todos `INSERT_ actions` se pueden utilizar para insertar un AVP RADIUS en una conexión RADIUS.

Casos de uso

Los siguientes son casos de uso para RADIUS con reescritura.

Reescritura del nombre de usuario AVP

Para configurar la función de reescritura para eliminar la cadena Dominio del nombre de usuario AVP de RADIUS, comience por crear una acción de reescritura REEMPLAZAR como se muestra en el ejemplo siguiente. Utilice la acción en una directiva de reescritura que seleccione todas las solicitudes RADIUS. Enlazar la directiva a un punto de enlace global. Al hacerlo, establezca la prioridad en el nivel adecuado para permitir que cualquier directiva de bloqueo o rechazo surta efecto primero, pero asegúrese de que todas las solicitudes que no estén bloqueadas o rechazadas se vuelvan a escribir. Establezca la Expresión GoTo (gotoPriorityExpr) en NEXT para continuar la evaluación de directivas y adjunte la directiva a la cola RADIUS_REQ_DEFAULT.

Ejemplo:

```
1 add rewrite action rwActRadiusDomainDel replace radius.req.user_name q/
     RADIUS.NEW_AVP(1,RADIUS.REQ.USER_NAME.VALUE.AFTER_STR(" "))/
2 add rewrite policy RadiusRemoveDomainPol true rwActRadiusDomainDel
3 <!--NeedCopy-->
```

> **Nota**:
>
> La directiva de reescritura para RADIUS no es aplicable a un servidor virtual de Gateway. Si un servidor virtual de Gateway se utiliza un equilibrio de carga, entonces RADIUS debe configurarse y la directiva de reescritura debe vincularse a un servidor virtual de equilibrio de carga RADIUS.

Inserción de un AVP específico del proveedor

Para configurar la acción de reescritura para insertar un AVP específico del proveedor que contenga el contenido del campo MSISDN, comience por crear una acción INSERT de reescritura que inserte el campo MSISDN en la solicitud. Utilice la acción en una directiva Rewrite que selecciona todas las solicitudes RADIUS. vincule la directiva a global, estableciendo la prioridad en un nivel adecuado y los demás parámetros, como se muestra en el ejemplo siguiente.

Ejemplo:

```
1 add rewrite action rwActRadiusInsMSISDN insert_after radius.req.
     avp_start RADIUS.NEW_VENDOR_SPEC_AVP(<VENDOR ID>, "RADIUS.NEW_AVP(<
     Attribute Code>, <MSISDN>)")
```



```
add rewrite policy rwPolRadiusInsMSISDN true rwActRadiusInsMSISDN
bind rewrite global rwPolRadiusInsMSISDN 100 NEXT -type
   RADIUS_REQ_DEFAULT
<!--NeedCopy-->
```

Funcionalidad de Diameter para Rewrite

January 12, 2021

La función Rewrite ahora admite el protocolo Diameter. Puede configurar Rewrite para modificar las solicitudes de Diameter y la respuesta como lo haría con las solicitudes y respuestas HTTP o TCP, lo que le permite utilizar Rewrite para administrar el flujo de solicitudes de Diameter y realizar las modificaciones necesarias. Por ejemplo, si el valor "Origen-Host" en una solicitud de Diameter no es apropiado, puede usar Rewrite para reemplazarlo por un valor que sea aceptable para el servidor de Diameter.

Para configurar Rewrite para modificar una solicitud de Diameter

Para configurar la función Rewrite para reemplazar el Origen-Host en una solicitud de Diameter por un valor diferente, en el símbolo del sistema, escriba los comandos siguientes:

- <agregar acción de reescritura <actname> reemplazar "DIAMETER.REQ.AVP (264,\" Citrix ADC.Example.NET\")"
  Para <actname>, sustituya un nombre para la nueva acción. El nombre puede constar de entre uno y 127 caracteres de longitud y puede contener letras, números y símbolos de guión (-) y guión bajo (_). Para Citrix ADC.example.net, sustituya el Origen de host que quiere utilizar en lugar del Nombre de host original.
- add rewrite policy <polname> "Diameter.req.avp (264).value.eq ("host.example.com")"
  <actname> Para <polname>, sustituya un nombre para la nueva directiva. Al igual que en el caso de <actname>, el nombre puede constar de entre uno y 127 caracteres de longitud, y puede contener letras, números y los símbolos de guión (-) y guión bajo (_). Para host.example.com, sustituya el nombre del origen de host que quiera cambiar. Para <actname>, sustituya el nombre de la acción que acaba de crear.
- bind lb vserver <vservername> -PolicyName <polname> -priority <priority> -type <vservername> REQUEST
  Para, sustituya el nombre del servidor virtual de equilibrio de carga al que quiere enlazar la directiva. Para <polname>, sustituya el nombre de la directiva que acaba de crear. Para <priority>, sustituya la directiva por una prioridad.

Ejemplo:

Para crear una acción y una directiva de reescritura para modificar todos los orígenes de host de Diameter de “host.example.com” a “Citrix ADC.example.net”, puede agregar la siguiente acción y directiva y enlazar la directiva como se muestra.

```
> add rewrite action rw_act_replace_avp replace ”diameter.req.avp(264)” ”diameter.new.avp(264,”Citrix ADC.example.net”)”
> add rewrite policy rw_diam_pol ”diameter.req.avp(264).value.eq(”client.realm2.net”)” rw_act_replace_avp
> bind lb vserver vs1 -policyName rw_diam_pol -priority 10 -type REQUEST

Done
<!--NeedCopy-->
```

Compatibilidad con DNS para la función de reescritura

August 20, 2021

Puede configurar la función de reescritura para modificar las solicitudes y respuestas DNS, como lo haría para las solicitudes y respuestas HTTP o TCP. Puede usar rewrite para administrar el flujo de solicitudes DNS y realizar las modificaciones necesarias en el encabezado o en la sección de respuestas. Por ejemplo, si la respuesta DNS no tiene el bit AA establecido en el indicador de encabezado, puede usar rewrite para establecer el bit AA en la respuesta DNS y enviarlo al cliente.

Expresiones DNS

En una configuración de reescritura, puede utilizar las siguientes expresiones Citrix ADC para hacer referencia a varias partes de una solicitud o respuesta DNS:

Consulte Expresiones y descripciones

Puntos de enlace DNS

Los siguientes puntos de enlace globales están disponibles para las directivas que contienen expresiones DNS.

Puntos de enlace	Descripción
DNS_REQ_OVERRIDE	Anular la cola de directivas de solicitudes.

Puntos de enlace	Descripción
DNS_REQ_DEFAULT	Cola de directivas de solicitudes estándar.
DNS_RES_OVERRIDE	Anular la cola de directivas de respuesta.
DNS_RES_DEFAULT	Cola de directivas de respuesta estándar.

Además de los puntos de enlace predeterminados, puede crear etiquetas de directiva de tipo DNS_REQ o DNS_RES y enlazar directivas DNS a ellos.

Reescribir tipos de acción para DNS

- **replace_dns_answer_section**—Esta acción reemplaza la sección de respuestas DNS con la expresión definida en la directiva DNS.
- **replace_dns_header_field**—Comprueba el tipo de código de operación en la solicitud DNS. Devuelve True o False, que indica si el tipo de código de operación de la solicitud DNS coincide con el tipo de código de operación especificado. Esta acción reemplaza la sección de encabezado DNS con la expresión definida en la directiva DNS.

Configuración de directivas de reescritura para DNS

El procedimiento siguiente utiliza la línea de comandos de Citrix ADC para configurar una acción y una directiva de reescritura y enlazar la directiva a un punto de enlace global específico de reescritura.

Configurar la acción y la directiva de reescritura y enlazar la directiva para DNS

En el símbolo del sistema, escriba los siguientes comandos:

1. `add rewrite action <actName> <actType>`

   Para, <actname>sustituya un nombre para la nueva acción. El nombre puede tener entre 1 y 127 caracteres y puede contener letras, números, guiones (-) y símbolos de subrayado (_). Para<actType>, especifique los tipos de acción de reescritura proporcionados para las expresiones DNS.

2. `add rewrite policy <polName> <rule> <actName>`

   Para <polname>, sustituya un nombre para la nueva directiva. Para<actname>, el nombre puede tener entre 1 y 127 caracteres y puede contener símbolos de letras, números, guión (-) y guión bajo (_). Para <actname>, sustituya el nombre de la acción que acaba de crear.

3. `bind rewrite global <polName> <priority> <gotoPriorityExpression> -type <bindPoint>`

Para<polName>, sustituya el nombre de la directiva que acaba de crear. Para<priority>, especifique la prioridad de la directiva. Para<bindPoint>, sustituya uno de los puntos de enlace globales específicos de reescritura.

Ejemplo:

Establezca el bit AA de la solicitud DNS para equilibrar la carga del servidor virtual.

Los siguientes comandos configuran el dispositivo Citrix ADC para que actúe como un servidor DNS autorizado para todas las consultas a las que sirve.

```
1 add rewrite action set_aa replace_dns_header_field dns.req.header.flags
     .set(aa)
2 add rewrite policy pol !dns.req.header.flags.is_set(aa)  set_aa
3 bind rewrite global  pol  100  -type dns_res_override
4 <!--NeedCopy-->
```

Modifique la respuesta y la sección de encabezado.

Si el servidor responde con un dominio NX, puede establecer la acción de reescritura para reemplazar la respuesta con la dirección IP especificada. Una NOPOLICY-REWRITE le permite invocar un banco externo sin procesar una expresión (una regla). Esta entrada es una directiva ficticia que no contiene una regla pero dirige la entrada a una etiqueta de directiva o bancos de directivas específicos de un servidor virtual.

```
1 add rewrite action set_aa_res replace_dns_header_field "dns.res.header.
     flags.set(aa)"
2 add rewrite action modify_nxdomain_res replace_dns_answer_section "dns.
     new_rrset_a("10.102.218.160",300)"
3 add rewrite policy set_res_aa true set_aa_res
4 add add rewrite policy modify_answer "dns.RES.HEADER.RCODE.EQ(nxdomain)
      && dns.RES.QUESTION.TYPE.EQ(A)"
5 modify_nxdomain_res
6 add rewrite policylabel MODIFY_NODATA dns_res
7 bind rewrite policylabel MODIFY_NODATA modify_answer 10 END
8 bind rewrite policylabel MODIFY_NODATA set_res_aa 11 END
9 bind lb vserver v1 -policyName NOPOLICY-REWRITE -priority 11 -
     gotoPriorityExpression END -type
10 RESPONSE -invoke policylabel MODIFY_NODATA
11 <!--NeedCopy-->
```

Limitaciones:

- Las directivas de reescritura solo se evalúan si el dispositivo Citrix ADC está configurado como un servidor proxy DNS y se produce una pérdida de caché.
- Si el indicador Recursion Available (RA) del encabezado está establecido en YES, el indicador RA no se modificará en las reescrituras.
- Si el indicador RA en el encabezado está establecido en YES, el indicador de CD en el encabezado se modifica independientemente de cualquier acción de reescritura.

Compatibilidad con MQTT para reescritura

January 21, 2022

La función de reescritura admite el protocolo MQTT. Puede configurar directivas de reescritura para que tomen medidas en función de los parámetros de las solicitudes del cliente MQTT y las respuestas del servidor.

Acción de reescritura para MQTT

La acción de reescritura de MQTT indica los cambios realizados en la solicitud o respuesta de MQTT antes de enviarla a un servidor o cliente.

Expresión:

```
add rewrite action <name> <rewrite_type> <target> <rewrite_action>
```

Tipo de reescritura para MQTT

Según el tipo de regla de expresión de reescritura que se utilice, se admiten los siguientes tipos de reescritura de MQTT:

- `replace_mqtt`
- `insert_before_mqtt`
- `insert_after_mqtt`
- `delete_mqtt`
- `insert_mqtt`

Reescribir el objetivo para MQTT

En los siguientes ejemplos de ejemplo, la función de reescritura de MQTT utiliza expresiones de directiva para indicar la parte de la solicitud que se va a modificar (destino) y la modificación que se va a realizar (expresión de cadena):

- Reescriba un identificador de cliente en el paquete de conexión mediante el tipo de acción `replace_mqtt`.

  ```
  add rewrite action rwact1 replace_mqtt MQTT.CONNECT.CLIENTID "\"xyz\""
  ```

- Reescribir un tema en la solicitud de publicación mediante el tipo de acción `replace_mqtt`.

  ```
  add rewrite action rwact1 replace_mqtt MQTT.PUBLISH.TOPIC "\"testing/
  test123\""
  ```

- Reescribe para insertar una propiedad con el tipo de acción insert_mqtt.

  ```
  add rewrite action rwact1 insert_mqtt MQTT.NEW_PROPERTY("prop1", "test"
  )
  ```

- Elimina un tema con el tipo de acción delete_mqtt.

  ```
  add rewrite action rwact2 delete_mqtt MQTT.SUBSCRIBE.TOPIC_FILTERS.
  TOPIC(1)
  ```

Acción de reescritura para MQTT

Las siguientes son las acciones de reescritura predefinidas para MQTT:

- `MQTT.NEW_KEEPALIVE(interval)`
- `MQTT.NEW_PACKET_IDENTIFIER(packetID)`
- `MQTT.NEW_REASON_CODE(retCode)`
- `MQTT.NEW_PUBLISH(topic_name, payload)`
- `MQTT.NEW_CONNECT_USERNAME(username)`
- `MQTT.NEW_CONNECT_WILL_MESSAGE(will_topic, will_payload, will_Qos, will_retain)`
- `MQTT.NEW_TOPIC(topic, qos)`
- `MQTT.NEW_TOPIC(topic)`
- `MQTT.NEW_PROPERTY(key, value)`

Ejemplo de la acción de reescritura predefinida:

```
add rewrite action rwact1 replace_mqtt MQTT.CONNECT.KEEPALIVE MQTT.NEW_KEEPALIVE
(90)
```

Ejemplo de la acción de reescritura definida por el usuario:

```
add rewrite action rwact1 replace_mqtt MQTT.CONNECT.USERNAME "\"user1\""
```

Directiva de reescritura para MQTT

Una directiva de reescritura para MQTT consiste en una regla y una acción. La regla determina el tráfico de MQTT en el que se aplica la reescritura y la acción determina la acción que debe realizar el

dispositivo Citrix ADC.

Expresión:

```
add rewrite policy <name> <rewrite_rule> <rewrite_action>
```

Ejemplo:

```
add rewrite action insert_mqtt_username insert_mqtt MQTT.NEW_CONNECT_USERNAME
("user1")

add rewrite policy rewrite_mqtt_username "MQTT.COMMAND.EQ(CONNECT)&& MQTT.
CONNECT.USERNAME.LENGTH.EQUALS(0)insert_mqtt_username
```

Puntos de enlace para MQTT

Puede vincular una directiva de reescritura de forma global o a un servidor virtual de equilibrio de carga específico o a un servidor virtual de conmutación de contenido.
Los siguientes son los puntos de enlace globales:

- MQTT_REQ_DEFAULT
- MQTT_REQ_OVERRIDE
- MQTT_RES_DEFAULT
- MQTT_RES_OVERRIDE

Expresión:

- `bind rewrite global <policyName> <priority> [-type MQTT_REQ_OVERRIDE | MQTT_REQ_DEFAULT | MQTT_RES_OVERRIDE | MQTT_RES_DEFAULT]`
- `bind lb|cs vserver <virtualServerName> -policyName <policyName> -priority <positiveInteger> -type REQUEST|RESPONSE`

Ejemplo:

- `bind rewrite global pol1 10 -type MQTT_REQ_DEFAULT`
- `add/bind lb vserver v1 -policyName pol1 -type reqUEST -priority 10`

Configurar una directiva de reescritura para MQTT

Para configurar una directiva de reescritura, siga los pasos y escriba los comandos en el símbolo del sistema:

1. Habilite la función de reescritura en el dispositivo Citrix ADC.

   ```
   enable ns feature REWRITE
   ```


2. Agregue una acción de reescritura.

   ```
   add rewrite action rwact1 replace_mqtt MQTT.CONNECT.KEEPALIVE MQTT.
   NEW_KEEPALIVE(10)
   ```

3. Agregue una directiva de reescritura.

   ```
   add rewrite policy pol1 MQTT.COMMAND.EQ(CONNECT)rwact1
   ```

4. Configure un servidor virtual de equilibrio de carga MQTT.

   ```
   add lb vserver v1 MQTT 1.1.1.1 1883
   ```

5. Enlazar la directiva de reescritura de forma global o a un servidor virtual de equilibrio de carga específico.

   ```
   bind rewrite global pol1 10 -type MQTT_REQ_DEFAULT
   ```

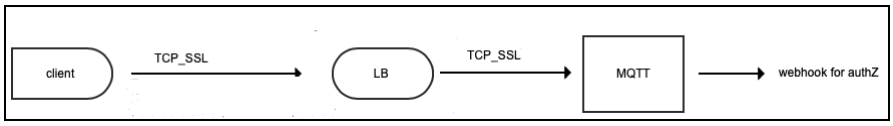
   ```
   add/bind lb vserver v1 -policyName pol1 -type REQUEST -priority 10
   ```

Caso de uso 1: Reemplace el nombre de usuario en el mensaje MQTT CONNECT por el nombre del certificado

El administrador puede configurar una directiva de reescritura de MQTT para reemplazar el nombre de usuario por el nombre del certificado del cliente.

Vamos a considerar un ejemplo. La solicitud del cliente tiene un mensaje `MQTT CONNECT` que contiene el nombre de usuario como “admin”. Este nombre de usuario debe reemplazarse por el número de serie (16 dígitos) que se extrae del certificado de cliente (nombre del certificado).

En la siguiente ilustración se muestra el flujo de trabajo:



1. Se envía una solicitud de Protocolo de control de transporte (TCP) al equilibrador de carga.
2. En el equilibrador de carga, el nombre de usuario se reemplaza por el nombre del certificado.
3. La solicitud se reenvía al intermediario de MQTT.
4. Este nuevo nombre de usuario se usa para la autorización a través de la carga útil de webhook.

Configuración de ejemplo:

```
add rewrite action mqtt_rw_unameact1 replace_mqtt MQTT.CONNECT.USERNAME
CLIENT.SSL.CLIENT_CERT.SERIALNUMBER
```

```
add rewrite policy mqtt_rw_uname_pol1 ”MQTT.COMMAND.EQ(CONNECT)”mqtt_rw_unameact1
```



```
bind cs vserver mqtt_frontend_cs -policyName mqtt_rw_uname_pol1 -priority
10 -gotoPriorityExpression END -type REQUEST
```

Caso de uso 2: Proporcionar una suscripción a un nuevo TEMA

El administrador puede proporcionar una suscripción a un TEMA nuevo. Vamos a considerar un ejemplo. La solicitud de un cliente tiene una suscripción al TEMA 1. El administrador puede configurar una directiva de reescritura para proporcionar suscripción a un nuevo TEMA 2. La suscripción se puede insertar antes o después.

Configuración de ejemplo:

- `add rewrite action act2 insert_before_mqtt MQTT.TOPIC_FILTERS.TOPIC(1) MQTT.NEW_TOPIC(topic2, 2)`
- `add rewrite policy policy2 “MQTT.COMMAND.EQ(SUBSCRIBE)&& MQTT.SUBSCRIBE. TOPIC_FILTERS.TOPIC.CONTAINS(\”test\”)”act2`

Mapas de cuerdas

October 5, 2021

Puede utilizar los mapas de cadenas para realizar coincidencias de patrones en todas las funciones de Citrix ADC que utilizan la sintaxis de directivas predeterminada. Un mapa de cadenas es una entidad de Citrix ADC que consta de pares clave-valor. Las claves y los valores son cadenas en formato ASCII o UTF-8. La comparación de cadenas utiliza dos nuevas funciones, `MAP_STRING(<string_map_name>)` y `IS_STRINGMAP_KEY(<string_map_name>)`.

Una configuración de directivas que utiliza mapas de cadenas funciona mejor que una que hace coincidencias de cadenas mediante expresiones de directiva, y se necesitan menos directivas para realizar la coincidencia de cadenas con un gran número de pares clave-valor. Los mapas de cadenas también son intuitivos, fáciles de configurar y dan como resultado una configuración más pequeña.

Cómo funcionan los mapas de cadenas

Los mapas de cadenas son similares en estructura a los conjuntos de patrones (un conjunto de patrones define una asignación de valores de índice a cadenas; un mapa de cadenas define una asignación de cadenas a cadenas) y los comandos de configuración para los mapas de cadenas (comandos como add, bind, unbind, remove y show) son sintácticamente similares a la configuración comandos para conjuntos de patrones. Además, al igual que con los valores de índice de un conjunto de patrones, cada clave de un mapa de cadenas debe ser única en todo el mapa. En la tabla siguiente se muestra un mapa de cadenas denominado url_string_map, que contiene URL como claves y valores.

Tecla	Valor
/url_1.html	http://www.redirect_url_1.com/url_1.html
/url_2.html	http://www.redirect_url_2.com/url_2.html
/url_3.html	http://www.redirect_url_1.com/url_1.html

Tabla 1. String Map “url_string_map”

En la tabla siguiente se describen las dos funciones que se han introducido para habilitar la coincidencia de cadenas con claves en un mapa de cadenas. La coincidencia de cadenas siempre se realiza con las teclas. Además, las siguientes funciones realizan una comparación entre las claves del mapa de cadenas y la cadena completa que devuelve el prefijo de expresión. Los ejemplos de las descripciones hacen referencia al ejemplo anterior.

Para obtener información completa sobre las dos funciones introducidas para habilitar la coincidencia de cadenas con las claves de un mapa de cadenas, consulte Tabla de funciones de mapa de cadenas pdf.

Configuración de un mapa de cadenas

Primero crea un mapa de cadenas y, a continuación, enlaza pares clave-valor a él. Puede crear un mapa de cadenas desde la interfaz de línea de comandos (CLI) o la utilidad de configuración.

Para configurar un mapa de cadenas mediante la interfaz de línea de comandos

En el símbolo del sistema, haga lo siguiente:

1. Crea un mapa de cadenas.

```
add policy stringmap <name> -comment <string>
```

1. Enlaza un par clave-valor al mapa de cadenas.

```
bind policy stringmap <name> <key> <value> [-comment <string>]
```

Ejemplo:

```
1 bind policy stringmap url_string_map1 ”/url_1.html” ”http://www.
     redirect_url_1.com/url_1.html”
2 <!--NeedCopy-->
```


Para configurar un mapa de cadenas mediante la GUI de Citrix ADC

Vaya a **AppExpert** > **String Maps**, haga clic en **Agregar** y especifique los detalles pertinentes.

Ejemplo: directiva de respuesta con una acción de redirección

En el siguiente caso de uso se trata de una directiva de respuesta con una acción de redirección. En el ejemplo siguiente, los cuatro primeros comandos crean el mapa de cadenas url_string_map y enlazan los tres pares clave-valor utilizados en el ejemplo anterior. Después de crear el mapa y vincular los pares clave-valor, crea una acción de respuesta (act_url_redirects) que redirige al cliente a la URL correspondiente del mapa de cadenas o a www.default.com. También configura una directiva de respuesta (pol_url_redirects) que comprueba si las URL solicitadas coinciden con alguna de las claves de url_string_map y, a continuación, realiza la acción configurada. Por último, vincula la directiva de respuesta al servidor virtual de conmutación de contenido que recibe las solicitudes de cliente que se van a evaluar.

```
add stringmap url_string_map

bind stringmap url_string_map /url_1.html http://www.redirect_url_1.com/
url_1.html

bind stringmap url_string_map /url_2.html http://www.redirect_url_2.com/
url_2.html

bind stringmap url_string_map /url_3.html http://www.redirect_url_1.com/
url_1.html
```

‘add responder action act_url_redirects redirect ‘HTTP.REQ.URL.MAP_STRING(“url_string_map”) ALT “www.default.com”’

```
add responder policy pol_url_redirects TRUE act_url_redirects

bind cs vserver csw_redirect -policyname pol_url_redirects -priority 1 -
type request
```

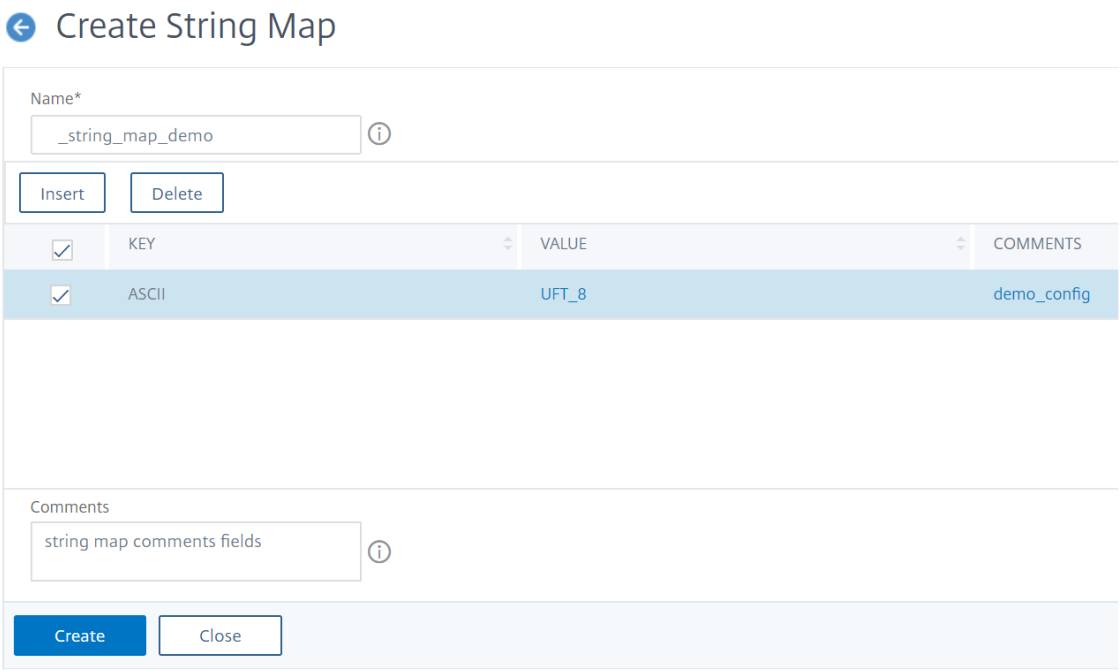
Para configurar un mapa de cadenas mediante la GUI de Citrix ADC

Siga el procedimiento que se indica a continuación para configurar un mapa de cadenas.

1. En el panel de navegación, expanda **AppExpert** y haga clic en **String Maps**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En la página **Crear mapa de cadenas**, defina los siguientes parámetros:
   - Name. Nombre del mapa de cadenas.
   - Configure el valor clave. Entrada de valores clave basada en ASCII vinculada al mapa de cadenas

- Comentarios. Breve descripción de los valores clave enlazados al mapa de cadenas.

4. Haga clic en **Crear** y **cerrar**.



Conjuntos de URL

August 20, 2021

Esta función le permite poner en la lista de prohibidos un millón de URL. La sección incluye los siguientes temas:

- Introducción
- Uso de expresiones avanzadas de directiva para la evaluación de URL
- Configuración de un conjunto de direcciones URL
- Semántica de patrones de URL
- Categorías de URL en la lista de prohibidos

Introducción

August 20, 2021

Para evitar el acceso a sitios web restringidos, un dispositivo Citrix ADC utiliza un algoritmo de coincidencia de URL especializado. El algoritmo utiliza un conjunto de direcciones URL que puede con-

tener una lista de direcciones URL de hasta 1 millón (1.000.000) entradas en la lista de prohibidos. Cada entrada puede incluir metadatos que definen categorías de URL y grupos de categorías como patrones indexados. El dispositivo también puede descargar periódicamente URL de conjuntos de URL altamente sensibles administrados por agencias de aplicación de Internet (con sitios web gubernamentales) u organizaciones de Internet. Una vez que el conjunto de direcciones URL se descarga de un sitio web e importa en el dispositivo, el dispositivo cifra los conjuntos de direcciones URL (según lo requieran estas agencias) y se mantienen confidenciales y las entradas no se manipulan.

El dispositivo Citrix ADC utiliza directivas avanzadas para determinar si se debe bloquear, permitir o redirigir una dirección URL entrante. Estas directivas utilizan expresiones avanzadas para evaluar las direcciones URL entrantes contra las entradas incluidas en la lista de prohibidos. Una entrada puede incluir metadatos. Para las entradas que no tienen metadatos, es posible que quiera utilizar una expresión que evalúe la dirección URL en función de una coincidencia exacta de cadena. Para otras direcciones URL, es posible que quiera utilizar una expresión que evalúe los metadatos de la dirección URL, además de una expresión que compruebe la coincidencia exacta de una cadena.

Caso de uso para directivas de acceso seguro a Internet para ISP/Telcos

Un conjunto de URL permite a un ISP (ISP) o a un cliente de Telco aplicar las directivas de acceso seguro a Internet exigidas por el gobierno, tales como:

1. Bloquear el acceso a sitios ilegales de Internet (abuso infantil, drogas, etc.)
2. Navegación segura para niños

Un dispositivo Citrix ADC le permite descargar periódicamente conjuntos de URL administrados por agencias de aplicación de Internet u organizaciones independientes de Internet. El dispositivo descarga periódicamente la lista y la actualiza de forma segura. La lista se almacena como conjuntos de URL confidenciales para que no sea manipulada ni legible por humanos. El conjunto de URL descargado periódicamente funciona como un conjunto en la lista de prohibidos para fines de evaluación de URL.

Si tiene una dirección URL privada establecida y el contenido de la lista se mantiene confidencial y el administrador de la red no conoce las direcciones URL de la lista de prohibidos presentes en la lista. Para asegurarse de que la directiva está configurada correctamente y se hace referencia a la lista correcta, debe configurar la URL Canary y agregarla al conjunto de URL. Mediante la URL Canary, el administrador puede solicitar a través del dispositivo que utiliza la URL privada establecida para asegurarse de que se busca para cada solicitud de URL.

Expresiones de directivas avanzadas para la evaluación de URL

January 12, 2021

En la tabla siguiente se describen las expresiones que puede utilizar para evaluar direcciones URL entrantes con entradas en un conjunto de direcciones URL.

Nota: HTTP.REQ.URL está generalizado para ser utilizado como <URL expression>

Expresión	Operación
<URL expression>.URLSET_MATCHES_ANY	Evalúa como TRUE si la URL coincide exactamente con cualquier entrada del conjunto de URL.
<URL expression>.GET_URLSET_METADATA (<URLSET>)	La expresión GET_URLSET_METADATA() devuelve los metadatos asociados si la URL coincide exactamente con cualquier patrón dentro del conjunto de URL. Se devuelve una cadena vacía si no hubo coincidencia.
<URL expression>.GET_URLSET_METADATA (<URLSET>).EQ (<METADATA>	Evalúa como TRUE si los metadatos coincidentes son iguales a <METADATA>.
<URL expression> .GET_URLSET_METADATA(<URLSET>).TYPECAST_LIST_T(‘,’).GET(0).EQ(<CATEGORY>)	Evalúa como TRUE si los metadatos coincidentes están al principio de la categoría. Este patrón se puede utilizar para codificar campos separados dentro de los metadatos, pero solo coincide con el primer campo.
HTTP.REQ.HOSTNAME.APPEND (HTTP.REQ.URL)	Se une a los parámetros host y URL, que luego se pueden utilizar como un <URL expression> para la coincidencia.

Configuración del conjunto de URL

October 5, 2021

Puede realizar las siguientes tareas para configurar un conjunto de URL y restringir las URL en una plataforma Citrix ADC:

1. Importa un conjunto de URL (descárgalo y cifrítalo). La importación de un conjunto de URL en un dispositivo Citrix ADC le permite:

- Para descargar el archivo URL.
- Para agregar el archivo al dispositivo.
- Para cifrar el archivo.
  Hasta que no agregue el conjunto de URL al sistema, no será visible para el usuario.

Puede descargar un conjunto de las siguientes formas:

- Descargue un conjunto de URL una vez desde un servidor remoto y especifíquelo como `http://myserver.com/file_with_urlset.csv`
- agregue un archivo bajo la `/var/tmp/` ruta dentro de ADC y utilice el comando, como en el ejemplo:

```
> shell cat /var/tmp/test_urlset.csv
example.com
google.com
> import policy urlset top10
k -url local:test_urlset.csv -delimiter ”,” -rowSeparator ”n” -interval
    10 -privateSet -canaryUrl http://www.in.gr
Done

<!--NeedCopy-->
```

El conjunto de URL importado se clasifica en diferentes categorías y grupos de categorías de la base de datos. Esto es válido solo si existen categorías en los metadatos del archivo de conjunto de URL.

Nota: Es posible que tengas patrones de URL sin metadatos.

Una vez importado el archivo, podrá actualizar, eliminar o mostrar las propiedades del archivo. Una vez insertado el archivo en el dispositivo, puede modificar las entradas añadiendo más filas.

El conjunto importado se almacena en formato de archivo cifrado en el directorio Citrix ADC. La lista importada contiene millones de entradas URL. A continuación, «La lista importada puede contener hasta 1 millón de entradas URL. De lo contrario, el dispositivo devuelve un mensaje de error que indica que el valor supera el límite. Si el conjunto de direcciones URL importado tiene entradas en la lista de prohibidos con metadatos, el dispositivo detecta los metadatos al importarlos.

Una vez que haya importado un conjunto de URL y lo agregue al dispositivo, el conjunto de URL está disponible para directivas avanzadas para identificar el conjunto de URL correcto durante la evaluación de URL entrante. `HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URLSET_MATCHES_ANY (<URL set name>)`

1. Actualización de un conjunto de URL en el dispositivo Citrix ADC. Una vez que haya insertado el archivo en el dispositivo, en este intervalo puede actualizar manualmente un archivo URL mediante la interfaz de línea de comandos.
2. Exportación de un conjunto de URL. Si prefieres una copia de seguridad del conjunto de URL, puedes exportar la lista de patrones de URL y guardar una copia del mismo en una URL de destino. Antes de exportar, compruebe si el conjunto de URL está marcado como privado. Si está marcado como privado, el conjunto de URL no se puede exportar. La funcionalidad de

exportación no funciona con un conjunto privado. Por lo tanto, un nuevo conjunto de URL se `myurl` importaría sin definir un conjunto privado, y luego se exportaría a otro archivo en una ruta local, como se indica a continuación:

```
> shell touch /var/tmp/test_urlset_export.csv
Done
> shell cat /var/tmp/test_urlset_export.csv
Done
> shell cat /var/tmp/test_urlset.csv
example.com
google.com
Done
> export urlset myurl -url local:test_urlset_export.csv

> import urlset myurl -url local:test_urlset.csv
Done
(a non-private urlset is imported)

<!--NeedCopy-->
```

1. Eliminación de un conjunto de URL. Si quiere eliminar un conjunto de direcciones URL de entradas en la lista de prohibidos, puede utilizar el comando remove para eliminar el conjunto de direcciones URL del dispositivo Citrix ADC.
2. Mostrar un conjunto de URL. Puede mostrar las propiedades de un conjunto de URL mediante el comando show.

> **Nota:** Las URL con parte de consulta se eliminan durante la importación.

Ejemplo:

```
show urlset
Name: top100 PatternCount: 100 Delimiter:  RowSeparator: Interval: 0
Done
<!--NeedCopy-->
```

Importar un conjunto de URL con meta mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:


```
import urlset <name> [-overwrite] [ - delimiter <character>] [-
    rowSeparator <character>] [-url] <url> [-interval <seconds>] [-
    privateSet] [-canaryUrl <URL>]
<!--NeedCopy-->
```

Donde:

Delimitador es un registro de archivo CSV con el valor predeterminado establecido como 44.

RowSeparator es un separador de filas de archivos CSV con el valor predeterminado establecido como 10.

El intervalo es el intervalo de tiempo en segundos, redondeado a los 15 minutos más próximos en los que se produce la actualización del conjunto de URL.

CanaryURL es una URL que se utiliza para realizar pruebas cuando el contenido del conjunto de URL se mantiene confidencial.

Ejemplo

```
import policy urlset -url local:test_urlset.csv -delimiter ”,”-rowSeparator
 ”n”-interval 10 -privateSet -canaryUrl http://www.in.gr
```

Realizar coincidencia explícita de subdominio para un conjunto de URL importado

Ahora puede realizar una coincidencia explícita de subdominio para un conjunto de URL importado. Se añade un nuevo parámetro, «SubdomainExactMatch» al comando «Import Policy URLSet». Cuando habilita el parámetro, el algoritmo de filtrado de URL realiza una coincidencia explícita de subdominios. Por ejemplo, si la URL entrante es «news.example.com» y si la entrada del conjunto de URL es «ejemplo.com», el algoritmo no coincide con las URL.

En el símbolo del sistema, escriba:

```
import policy urlset <name> [-overwrite] [-delimiter <character>][-rowSeparator
 <character>] -url [-interval <secs>] [-privateSet][-subdomainExactMatch]
[-canaryUrl <URL>]
```

Ejemplo:

```
import policy urlset forth_urlset -url local:test_urlset.csv -interval 3600
 -subdomainExactMatch
```

Para mostrar el conjunto de URL mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
show urlset <name>
```


Ejemplo:

En el símbolo del sistema, escriba:

```
1          URLset     Count
2          ------     -----
3 1)       top1k      100
4  Done
5
6 > show urlset top1k
7          Count      Delimiter  Interval   RowSeparator
8          -----      ---------  --------   ------------
9          100              ,        0         0x0a
10  Done
11 >
12
13 <!--NeedCopy-->
```

Para mostrar el conjunto de URL importado mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
show urlset -imported
```

Ejemplo:

En el símbolo del sistema, escriba:

```
1          URLset
2          ------
3 1)       top1k
4  Done
5 <!--NeedCopy-->
```

Para mostrar el conjunto de URL <urlset_name> mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
show urlset <name>
```


Para exportar un conjunto de URL mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
export urlset <name> <url>
```

Para agregar un conjunto de URL mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
add urlset <urlset_name>
```

Para actualizar un conjunto de URL mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
update urlset <name>
```

Para quitar un comando de conjunto de URL mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
remove urlset <name>
```

Ejemplo:

> Nota:
>
> Antes de importar o exportar un conjunto de URL, debe asegurarse de que los `test_urlset.csv` archivos `test_urlset_export.csv` y se crean y están disponibles en el `/var/tmp` directorio.

```
1  import policy urlset -url local:test_urlset.csv -delimiter ”,” -
       rowSeparator ”n” -interval 10 -privateSet -overwrite  - canaryUrl
       http://www.in.gr
2
3  add policy urlset top10k
4
5  update policy urlset top10k
6
7  sh policy urlset
8
9  sh policy urlset top10k
10
11 export policy urlset urlset1 -url local:test_urlset_export.csv
```



```
12
13 import policy urlset top10k -url local:test_urlset.csv  - privateSet
14
15 add policy urlset top10k
16
17 update policy urlset top10k
18
19 show policy urlset top10k
20 <!--NeedCopy-->
```

Mostrar conjuntos de URL importados

Ahora puede mostrar conjuntos de URL importados además de los conjuntos de URL añadidos. Para ello, se añade un nuevo parámetro «importado» al comando «show url set». Si habilita esta opción, el dispositivo muestra todos los conjuntos de URL importados y distingue los conjuntos de URL importados de los conjuntos de URL añadidos.

En el símbolo del sistema, escriba:

```
show policy urlset [<name>] [-imported]
```

Ejemplo:

```
show policy urlset -imported
```

Para importar un conjunto de URL mediante la GUI

Vaya a **AppExpert** > **Conjuntos de URL**y haga clic en **Importar** para descargar el conjunto de URL.

Para agregar un conjunto de URL mediante la GUI

Vaya a **AppExpert** > **Conjuntos de URL**, haga clic en **Agregar** para crear un archivo de conjunto de URL para el conjunto de URL descargado.

Para editar un conjunto de URL mediante la GUI

Vaya a **AppExpert** > **Conjuntos de URL**, seleccione un conjunto de URL y haga clic en **Editar** para modificarlo.

Para actualizar un conjunto de URL mediante la GUI

Vaya a **AppExpert** > **Conjuntos de URL,** seleccione un conjunto de **URL y haga clic en Actualizar conjunto** de URL para actualizar el conjunto de URL con las últimas modificaciones introducidas en el archivo.

Para exportar un conjunto de URL mediante la GUI

Vaya a **AppExpert > Conjuntos**de URL, seleccione un conjunto de URL y haga clic en **Exportar conjunto** de URL para exportar los patrones de URL de un conjunto a una URL de destino y guardarlo en esa ubicación.

Semántica de patrones de URL

August 20, 2021

En la tabla siguiente se muestran los patrones de URL utilizados para especificar la lista de páginas que quiere filtrar. Por ejemplo, el patrón de URL `http://www.example.com/bar` coincide con una sola página `http://www.example.com/bar`. Para cubrir todas las páginas en las que la URL empieza por www.example.com/bar, debes añadir explícitamente un "*" al final.

Para obtener más información, consulte Tabla de asignación de metadatos de patrones de URL .

Categorías de URL

August 20, 2021

A continuación se muestra una lista de categorías en la lista de prohibidos.

S.No	Categorías en la lista de prohibidos
1	Actividades ilegales
2	Drogas ilegales
3	Medicación
4	Marihuana
5	Terrorismo/Extremistas
6	Armas
7	Odio/calumnias
8	Violencia/Suicidio
9	Promoción/Defensa en general
10	Adultos/Pornografía
11	Desnudez

S.No	Categorías en la lista de prohibidos
12	Servicios sexuales
13	Enlaces/Búsqueda de adultos
14	Hacking/Cracking
15	Malware
16	Proxies remotos
17	Cachés de motor de búsqueda
18	Traductores
19	Citas
20	Bodas/Matrimonios
21	Valores de mercado
22	Comercio online
23	Seguros
24	Productos financieros
25	Apuestas en general
26	Lotería
27	Juegos online
28	Juegos
29	Subastas
30	Compras/Venta al por menor
31	Bienes raíces
32	Compras por Internet
33	Chat basado en web
34	Mensajes instantáneos
35	Correo basado en web
36	Suscripciones de correo electrónico
37	Tablones de anuncios
38	Tablones de anuncios TI
39	Páginas Web/Blogs personales
40	Descargas

S.No	Categorías en la lista de prohibidos
41	Descargas de programas
42	Servicios de almacenamiento
43	Medios streaming
44	Empleo
45	Desarrollo profesional
46	Negocio secundario
47	Grotesco
48	Eventos especiales
49	Temas populares
50	Noticias/Revista para adultos
51	Fumar
52	Bebida
53	Alcohol
54	Fetiche
55	Expresión sexual (texto)
56	Juegos de disfraces
57	Ocultismo
58	Hogar y familia
59	Deporte profesional
60	Deportes en general
61	Eventos de la vida
62	Viajes y turismo
63	Organismo público de turismo
64	Transporte público
65	Alojamiento
66	Música
67	Horóscopo/Astrología/Adivinación
68	Artista/Personaje famoso
69	Gastronomía

S.No	Categorías en la lista de prohibidos
70	Entretenimiento/Lugares/Actividades
71	Religiones tradicionales
72	Religiones
73	Directiva
74	Anuncios/Publicidad
75	Sorteos/Premios
76	SPAM
77	Noticias
78	Automoción
79	Negocios y comercio
80	Informática e Internet
81	Educación
82	Gobierno
83	Estado
84	Telefonía por Internet
85	Ejército
86	Peer to Peer/Torrents
87	Ocio y pasatiempos
88	Referencia
89	Portales y motores de búsqueda
90	Educación sexual
91	Servicios de telefonía móvil y SMS
92	Publicación y aplicaciones móviles
93	Spyware
94	Infraestructura y redes de entrega de contenido
95	Sitios para niños
96	Trajes de baño y lencería
97	Eventos artísticos y culturales

S.No	Categorías en la lista de prohibidos
98	Sitios de alojamiento
99	Filantropía y organizaciones sin ánimo de lucro
100	Sitios para compartir y buscar fotos
101	Tonos de llamada
102	Belleza y moda
103	Almacenes de aplicaciones móviles
104	Dominios aparcados
105	Emoticonos
106	Operadores móviles
107	Botnets
108	Sitios infectados
109	Sitios de phishing
110	Keyloggers
111	Malware móvil
112	Sin contenido
113	Agricultura
114	Arquitectura
115	Asociaciones/Gremios/Sindicatos
116	Libros/eBooks
117	BOT Phone Home
118	DDNS
119	URL no admitida
120	Derecho legal
121	Comunidades locales
122	Otros
123	Revistas online
124	Mascotas/Veterinaria
125	Piratería y robo de copyright
126	Direcciones IP privadas

S.No	Categorías en la lista de prohibidos
127	Reciclaje/Medio ambiente
128	Ciencia
129	Sociedad y cultura
130	Servicios de transporte y flete
131	Fotografía y cine
132	Museos e Historia
133	eLearning
134	Redes sociales en general
135	Facebook
136	Facebook: Publicación
137	Facebook: Comentarios
138	Facebook: Amigos
139	Facebook: Carga de fotos
140	Facebook: Eventos
141	Facebook: Aplicaciones
142	Facebook: Chat
143	Facebook: Preguntas
144	Facebook: Carga de vídeos
145	Facebook: Grupos
146	Facebook: Juegos
147	LinkedIn
148	LinkedIn: Actualizaciones
149	LinkedIn: Correo
150	LinkedIn: Conexiones
151	LinkedIn: Empleo
152	Twitter
153	Twitter: Publicación
154	Twitter: Correo
155	Twitter: Seguir

S.No	Categorías en la lista de prohibidos
156	YouTube
157	YouTube: Comentarios
158	YouTube: Carga de vídeo
159	YouTube: Compartir
160	Instagram
161	Instagram: Carga
162	Instagram: Comentarios
163	Instagram: Mensaje privado
164	Tumblr
165	Tumblr: Publicación
166	Tumblr: Comentarios
167	Tumblr: Carga de fotos o vídeos
168	Google+
169	Google+: Publicación
170	Google+: Comentarios
171	Google+: Carga de fotos
172	Google+: Carga de vídeos
173	Google+: Chat de vídeo
174	Pinterest
175	Pinterest: Pin
176	Vine: Carga
177	Vine: Comentarios
178	Vine: Mensaje
179	Ask.fm
180	Ask.fm: Pregunta
181	Ask.fm: Respuesta
182	YikYak
183	YikYak: Publicación
184	YikYak: Comentarios

S.No	Categorías en la lista de prohibidos
185	Wordpress
186	Wordpress: Publicación
187	Wordpress: Carga

AppFlow

October 5, 2021

El dispositivo Citrix ADC es un punto de control central para todo el tráfico de aplicaciones en el centro de datos. Recopila información valiosa a nivel de flujo y sesión de usuario para aplicaciones de supervisión del rendimiento de las aplicaciones, análisis e inteligencia empresarial. También recopila datos de rendimiento de páginas web e información de base de datos. AppFlow transmite la información mediante el formato Internet Protocol Flow Information Export (IPFIX), que es un estándar abierto del Grupo de trabajo de ingeniería de Internet (IETF) definido en RFC 5101. IPFIX (la versión estandarizada de NetFlow de Cisco) se utiliza ampliamente para supervisar la información de flujo de red. AppFlow define nuevos elementos de información para representar información a nivel de aplicación, datos de rendimiento de páginas web e información de base de datos.

Mediante UDP como protocolo de transporte, AppFlow transmite los datos recopilados, denominados *registros de flujo*, a uno o más recopiladores IPv4. Los recopiladores agregan los registros de flujo y generan informes históricos o en tiempo real.

AppFlow proporciona visibilidad a nivel de transacción para flujos HTTP, SSL, TCP, SSL_TCP y HDX Insight. Puede muestrear y filtrar los tipos de flujo que quiere supervisar.

> **Nota**
>
> Para obtener más información sobre HDX Insight, consulte HDX Insight.

AppFlow utiliza acciones y directivas para enviar registros de un flujo seleccionado a un conjunto específico de recopiladores. Una acción de AppFlow especifica qué conjunto de recopiladores reciben los registros de AppFlow. Las directivas, basadas en expresiones avanzadas, se pueden configurar para seleccionar flujos para los que se envían registros de flujo a los recopiladores especificados por la acción de AppFlow asociada.

Para limitar los tipos de flujos, puede habilitar AppFlow para un servidor virtual. AppFlow también puede proporcionar estadísticas para el servidor virtual.

También puede habilitar AppFlow para un servicio específico, que represente un servidor de aplicaciones, y supervisar el tráfico a ese servidor de aplicaciones.

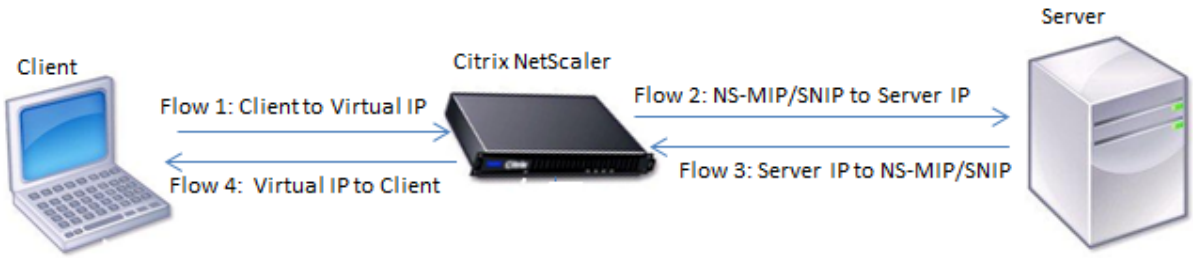
Nota: Esta función solo se admite en las compilaciones nCore de Citrix ADC.

Cómo funciona AppFlow

En el caso de implementación más común, el tráfico entrante fluye hacia una dirección IP virtual (VIP) del dispositivo Citrix ADC y se equilibra la carga en un servidor. El tráfico saliente fluye desde el servidor a una dirección IP asignada o de subred en Citrix ADC y del VIP al cliente. Un flujo es una colección unidireccional de paquetes IP identificados por las cinco tuplas siguientes: SourceIP, SourcePort, DesTip, DestPort y protocol.

La siguiente ilustración describe cómo funciona la función AppFlow.

Ilustración 1. Secuencia de flujo de Citrix ADC



Como se muestra en la ilustración, los identificadores de flujo de red para cada tramo de una transacción dependen de la dirección del tráfico.

Los diferentes flujos que forman un registro de flujo son:

Flujo 1: <Client-IP, Client-Port, VIP-IP, VIP-port, Protocol>

Flujo 2: <NS-MIP/SNIP, NS-port, Server-IP, Server-Port, Protocol>

Flujo 3: <Server-IP, Server-Port, NS-MIP/SNIP, NS-Port, Protocol>

Flujo 4: <VIP-IP, VIP-port, Client-IP, Client-Port, Protocol>

Para ayudar al recopilador a vincular los cuatro flujos de una transacción, AppFlow agrega un elemento transactionID personalizado a cada flujo. Para la conmutación de contenido a nivel de aplicación, como HTTP, es posible equilibrar la carga de una conexión TCP de un solo cliente para distintas conexiones TCP de back-end para cada solicitud. AppFlow proporciona un conjunto de registros para cada transacción.

Registros de flujo

Los registros de AppFlow contienen información estándar de NetFlow o IPFIX, como marcas de tiempo para el inicio y el final de un flujo, recuento de paquetes y recuento de bytes. Los registros de AppFlow también contienen información a nivel de aplicación (como URL HTTP, métodos de solicitud HTTP y

códigos de estado de respuesta, tiempo de respuesta del servidor y latencia). Datos de rendimiento de la página web (como el tiempo de carga de la página, el tiempo de procesamiento de la página y el tiempo dedicado a la página). Y la información de la base de datos (como el protocolo de base de datos, el estado de respuesta de la base de datos y el tamaño de respuesta Los registros de flujo IPFIX se basan en plantillas que deben enviarse antes de enviar registros de flujo.

Plantillas

AppFlow define un conjunto de plantillas, una para cada tipo de flujo. Cada plantilla contiene un conjunto de elementos de información (IE) estándar y elementos de información específicos de la empresa (EIE). Las plantillas IPFIX definen el orden y el tamaño de los elementos de información (Internet Explorer) en el registro de flujo. Las plantillas se envían a los recopiladores a intervalos regulares, como se describe en RFC 5101.

Una plantilla puede incluir las siguientes EIE:

- transactionID

  Número de 32 bits sin firmar que identifica una transacción a nivel de aplicación. Para HTTP, corresponde a un par de solicitud y respuesta. Todos los registros de flujo que corresponden a este par de solicitudes y respuestas tienen el mismo identificador de transacción. En el caso más común, hay cuatro `uniflow` registros que corresponden a esta transacción. Si Citrix ADC genera la respuesta por sí mismo (servida desde la caché integrada o mediante una directiva de seguridad), es posible que solo haya dos registros de flujo para esta transacción.

- connectionID

  Número de 32 bits sin firmar que identifica una conexión de capa 4 (TCP o UDP). Los flujos de Citrix ADC son bidireccionales, con dos registros de flujo independientes para cada dirección del flujo. Este elemento de información se puede utilizar para vincular los dos flujos.

  Para Citrix ADC, un ConnectionId es un identificador de la estructura de datos de conexión para realizar un seguimiento del progreso de una conexión. En una transacción HTTP, por ejemplo, un connectionID determinado puede tener varios elementos transactionID correspondientes a varias solicitudes realizadas en esa conexión.

- tcpRTT

  Tiempo de ida y vuelta, en milisegundos, medido en la conexión TCP. Se puede utilizar como métrica para determinar la latencia del cliente o del servidor en la red.

- httpRequestMethod

  Número de 8 bits que indica el método HTTP utilizado en la transacción. Junto con la plantilla se envía una plantilla de opciones con la asignación de número a método.

- httpRequestSize

  Número de 32 bits sin firmar que indica el tamaño de la carga útil de la solicitud.

- httpRequestURL

  La URL HTTP solicitada por el cliente.

- httpUserAgent

  Origen de las solicitudes entrantes al servidor web.

- httpResponseStatus

  Número de 32 bits sin firmar que indica el código de estado de respuesta.

- httpResponseSize

  Número de 32 bits sin firmar que indica el tamaño de la respuesta.

- httpResponseTimeToFirstByte

  Número de 32 bits sin firmar que indica el tiempo que tarda en recibir el primer byte de la respuesta.

- httpResponseTimeToLastByte

  Número de 32 bits sin firmar que indica el tiempo que se tarda en recibir el último byte de la respuesta.

- flowFlags

  Indicador de 64 bits sin firmar que se utiliza para indicar diferentes condiciones de flujo.

EIE para datos de rendimiento de páginas web

- clientInteractionStartTime

  Hora en la que el explorador recibe el primer byte de la respuesta para cargar cualquier objeto de la página, como imágenes, guiones y hojas de estilo.

- clientInteractionEndTime

  Hora en la que el explorador recibió el último byte de respuesta para cargar todos los objetos de la página, como imágenes, scripts y hojas de estilo.

- clientRenderStartTime

  Hora en la que el explorador empieza a renderizar la página.

- clientRenderEndTime

  Hora en la que un explorador terminó de renderizar toda la página, incluidos los objetos incrustados.

EIE para información de bases de datos

- dbProtocolName

  Número de 8 bits sin firmar que indica el protocolo de base de datos. Los valores válidos son 1 para MS SQL y 2 para MySQL.

- dbReqType

  Número de 8 bits sin firmar que indica el método de solicitud de base de datos utilizado en la transacción. Para MS SQL, los valores válidos son 1 para QUERY, 2 para TRANSACTION y 3 para RPC. Para obtener valores válidos para MySQL, consulte la documentación de MySQL.

- dbReqString

  Indica la cadena de solicitud de base de datos sin el encabezado.

- dbRespStatus

  Número de 64 bits sin firmar que indica el estado de la respuesta de la base de datos recibida del servidor web.

- dbRespLength

  Número de 64 bits sin firmar que indica el tamaño de la respuesta.

- dbRespStatString

  Cadena de estado de respuesta recibida del servidor web.

Configuración de la función AppFlow

June 22, 2022

Puede configurar AppFlow de la misma manera que la mayoría de las demás funciones basadas en directivas. En primer lugar, habilite la función AppFlow. A continuación, especifique los recopiladores a los que se envían los registros de flujo. Después de eso, defina acciones, que son conjuntos de recopiladores configurados. A continuación, configure una o varias directivas y asocie una acción a cada directiva. La directiva indica al dispositivo Citrix ADC que seleccione las solicitudes cuyos registros de flujo se envían a la acción asociada. Por último, vincula cada directiva globalmente o al servidor virtual específico para ponerla en práctica.

Puede configurar aún más los parámetros de AppFlow para especificar el intervalo de actualización de la plantilla y permitir la exportación de la información de HttpURL, HttpCookie y HttPreferer. En cada recopilador, debe especificar la dirección IP de Citrix ADC como dirección del exportador.

> **Nota**
>
> Para obtener información sobre cómo configurar Citrix ADC como exportador en el recopilador, consulte la documentación del recopilador específico.

La utilidad de configuración proporciona herramientas que ayudan a los usuarios a definir las directivas y acciones. Determina exactamente cómo el dispositivo Citrix ADC exporta los registros de un flujo en particular a un conjunto de recopiladores (acción). La interfaz de línea de comandos proporciona un conjunto correspondiente de comandos basados en CLI para los usuarios experimentados que prefieren una línea de comandos.

Activación de AppFlow

Para poder usar la función AppFlow, primero debe habilitarla.

> **Nota**
>
> AppFlow solo se puede habilitar en dispositivos Citrix ADC de nCore.

Habilitar la función AppFlow mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba uno de los siguientes comandos:

```
enable ns feature AppFlow
<!--NeedCopy-->
```

Habilitar la función AppFlow mediante la utilidad de configuración

Vaya a **Sistema > Configuración**, haga clic en **Configurar funciones avanzadas** y seleccione la opción **AppFlow**.

Especificación de un recopilador

Un recopilador recibe los registros de AppFlow generados por el dispositivo Citrix ADC. Para enviar los registros de AppFlow, debe especificar al menos un recopilador. De forma predeterminada, el recopilador escucha los mensajes IPFIX en el puerto UDP 4739. Puede cambiar el puerto predeterminado al configurar el selector. Del mismo modo, de forma predeterminada, NSIP se utiliza como IP de origen para el tráfico de AppFlow. Puede cambiar esta IP de origen predeterminada a una dirección SNIP al configurar un recopilador. También puede eliminar los recolectores no utilizados.

Especificar un recopilador mediante la interfaz de línea de comandos

> **Importante**
>
> A partir de la versión 12.1 de Citrix ADC, compilación 55.13, puede especificar el tipo de recopilador que quiere utilizar. Se introduce un nuevo parámetro "Transport" en el comando `add appflow collector`. De forma predeterminada, el recopilador escucha los mensajes IPFIX. Puede cambiar el tipo de recopilador a `logstream` o `ipfix` o descansar mediante el parámetro "Transporte". Para obtener más información sobre la configuración, consulte el ejemplo.

En el símbolo del sistema, escriba los siguientes comandos para agregar un recopilador y verificar la configuración:

```
1 -  add appflow collector <name> -IPAddress <ipaddress> -port <
     port_number> -netprofile <netprofile_name> -Transport <Transport>
2
3 -  show appflow collector <name>
4 <!--NeedCopy-->
```

Ejemplo

```
1 add appflow collector col1 -IPaddress 10.102.29.251 -port 8000 -
     netprofile n2 -Transport ipfix
2 <!--NeedCopy-->
```

Especificar varios recopiladores mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para agregar y enviar los mismos datos a varios recopiladores:

```
1 add appflow collector <collector1> -IPAddress <IP>
2
3 add appflow collector <collector2> -IPAddress <IP>
4
5 add appflow action <action> -collectors <collector1> <collector2>
6
7 add appflow policy <policy> true <action>
8
9 bind lbvserver <lbvserver> -policy <policy> -priority <priority>
```



```
<!--NeedCopy-->
```

Especificar uno o más recopiladores mediante la utilidad de configuración

Vaya a **Sistema > AppFlow > Recopiladores**y cree el recopilador de AppFlow.

Configurar una acción de AppFlow

Una acción AppFlow es un recopilador de conjuntos, al que se envían los registros de flujo si coincide la directiva AppFlow asociada.

Configurar una acción de AppFlow mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para configurar una acción de AppFlow y verificar la configuración:

```
add appflow action <name> --collectors <string> ... [-
   clientSideMeasurements (Enabled|Disabled) ] [-comment <string>]

show appflow action
<!--NeedCopy-->
```

Ejemplo

```
add appflow action apfl-act-collector-1-and-3 -collectors collector-1
   collecter-3
<!--NeedCopy-->
```

Configurar una acción de AppFlow mediante la utilidad de configuración

Vaya a **Sistema > AppFlow > Acciones**y cree la acción AppFlow.

Configurar una directiva de AppFlow

Después de configurar una acción de AppFlow, debe configurar una directiva de AppFlow. Una directiva de AppFlow se basa en una regla, que consta de una o más expresiones.

> **Nota**
>
> Para crear y administrar directivas de AppFlow, la utilidad de configuración proporciona asistencia que no está disponible en la interfaz de línea de comandos.

Configurar una directiva de AppFlow mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba el siguiente comando para agregar una directiva de AppFlow y verificar la configuración:

```
add appflow policy <name> <rule> <action>

show appflow policy <name>
<!--NeedCopy-->
```

Ejemplo

```
add appflow policy apfl-pol-tcp-dsprt client.TCP.DSTPORT.EQ(22) apfl-
   act-collector-1-and-3
<!--NeedCopy-->
```

Configurar una directiva de AppFlow mediante la utilidad de configuración

Vaya a **Sistema > AppFlow > Directivas** y cree la directiva de AppFlow.

Agregar una expresión mediante el cuadro de diálogo Agregar expresión

1. En el cuadro de diálogo Agregar expresión, en el primer cuadro de lista, elija el primer término de la expresión.

   -
   HTTP
   El protocolo HTTP. Elija la opción si desea examinar algún aspecto de la solicitud que pertenece al protocolo HTTP.
   -
   SSL


```
Los sitios web protegidos. Elija la opción si desea examinar algún
     aspecto de la solicitud que pertenezca al destinatario de la
    solicitud. -
CLIENT

The computer that sent the request. Choose the option if you want
    to examine some aspect of the sender of the request. Al elegir,
     el cuadro de lista situado más a la derecha muestra los té
    rminos apropiados para la siguiente parte de la expresión.
```

2. En el segundo cuadro de lista, elige el segundo término para su expresión. Las elecciones dependen de la elección que haya realizado en el paso anterior y son apropiadas para el contexto. Después de hacer la segunda elección, la ventana de Ayuda situada debajo de la ventana Construir expresión (que estaba en blanco) muestra ayuda para describir el propósito y el uso del término que acaba de elegir.
3. Siga eligiendo términos en los cuadros de lista que aparecen a la derecha del cuadro de lista anterior o escribiendo cadenas o números en los cuadros de texto que aparecen para pedirle que escriba un valor hasta que finalice la expresión.

Vincular una directiva de AppFlow

Para poner en práctica una directiva, debe vincularla de forma global, de modo que se aplique a todo el tráfico que fluye a través de Citrix ADC, o a un servidor virtual específico, de modo que la directiva se aplique solo al tráfico relacionado con ese servidor virtual.

Cuando vincula una directiva, le asigna una prioridad. La prioridad determina el orden en que se evalúan las directivas que defina. Puede establecer la prioridad en cualquier número entero positivo.

En el sistema operativo Citrix ADC, las prioridades de las directivas funcionan en orden inverso: cuanto mayor sea el número, menor será la prioridad. Por ejemplo, si tiene tres directivas con prioridades de 10, 100 y 1000, la directiva a la que se le ha asignado una prioridad de 10 se ejecuta primero. Posteriormente, la directiva se asignó con una prioridad de 100, y finalmente la directiva asignó un orden de 1000.

Puede dejar espacio suficiente para agregar otras directivas en cualquier orden y, aun así, configurarlas para que se evalúen en el orden que desee. Puede lograrlo estableciendo prioridades con intervalos de 50 o 100 entre cada directiva cuando la vincula globalmente. A continuación, puede agregar más directivas en cualquier momento sin tener que cambiar la prioridad de una directiva existente.

Enlazar globalmente una directiva de AppFlow mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba el siguiente comando para vincular globalmente una directiva de AppFlow y verificar la configuración:

```
bind appflow global <policyName> <priority> [<gotoPriorityExpression [-
    type <type>] [-invoke (<labelType> <labelName>)]

show appflow global
<!--NeedCopy-->
```

Ejemplo

```
bind appflow global af_policy_lb1_10.102.71.190 1 NEXT -type
    REQ_OVERRIDE -invoke vserver google
<!--NeedCopy-->
```

Enlazar una directiva de AppFlow a un servidor virtual específico mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba el siguiente comando para vincular una directiva de AppFlow a un servidor virtual específico y verificar la configuración:

```
bind lb vserver <name> -policyname <policy_name> -priority <priority>
<!--NeedCopy-->
```

Ejemplo

```
bind lb vserver google -policyname af_policy_google_10.102.19.179 -
    priority 251
<!--NeedCopy-->
```


Enlazar globalmente una directiva de AppFlow mediante la utilidad de configuración

Vaya a **Sistema > AppFlow**, haga clic en **Administrador de directivas de AppFlow** y seleccione el punto de enlace (predeterminado global) y el tipo de conexión pertinentes y, a continuación, enlace la directiva de AppFlow.

Enlazar una directiva de AppFlow a un servidor virtual específico mediante la utilidad de configuración

Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**, seleccione el servidor virtual y haga clic en **Directivas** y vincule la directiva de AppFlow.

Habilitar AppFlow para servidores virtuales

Si desea supervisar solo el tráfico a través de ciertos servidores virtuales, habilite AppFlow específicamente para esos servidores virtuales. Puede habilitar AppFlow para el equilibrio de carga, el cambio de contenido, la redirección de caché, la VPN con SSL, GSLB y servidores virtuales de autenticación.

Habilitar AppFlow para un servidor virtual mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
set cs vserver <name> <protocol> <IPAddress> <port> -appflowLog ENABLED
<!--NeedCopy-->
```

Ejemplo

```
set cs vserver Vserver-CS-1 HTTP 10.102.29.161 80 -appflowLog ENABLED
<!--NeedCopy-->
```

Habilitar AppFlow para un servidor virtual mediante la utilidad de configuración

Vaya a **Administración del tráfico > Cambio de contenido > Servidores virtuales**, seleccione el servidor virtual y habilite la opción Registro de AppFlow.

Habilitar AppFlow para un servicio

Puede habilitar AppFlow para los servicios que se van a vincular a los servidores virtuales de equilibrio de carga.

Habilitar AppFlow para un servicio mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
set service <name> -appflowLog ENABLED
<!--NeedCopy-->
```

Ejemplo

```
set service ser -appflowLog ENABLED
<!--NeedCopy-->
```

Habilitar AppFlow para un servicio mediante la utilidad de configuración

Vaya a **Administración del tráfico > Equilibrio de carga > Servicios**, seleccione el servicio y habilite la opción Registro de AppFlow.

Establecer los parámetros de AppFlow

Puede configurar los parámetros de AppFlow para personalizar la exportación de datos a los recopiladores.

Establezca los parámetros de AppFlow mediante la interfaz de línea de comandos

> **Importante**
>
> - A partir de Citrix ADC versión 12.1 compilación 55.13, puede utilizar el NSIP para enviar registros `Logstream` en lugar del SNIP. Se introduce un nuevo parámetro "logstreamOverNSIP" en el comando `set appflow param`. De forma predeterminada, el parámetro "LogStreamOvernSIP" es DISABLED, debe "ENABLE". Para obtener más información sobre la configuración, consulte el ejemplo.
> - A partir de la versión 13.0 build 58.x de Citrix ADC, puede habilitar la opción de aplicación Web SaaS en la función AppFlow. Se puede habilitar para recibir el uso de datos de apli-

> caciones web o SaaS del servicio Citrix Gateway. Para obtener más información sobre la configuración, consulte el ejemplo.

En el símbolo del sistema, escriba los siguientes comandos para establecer los parámetros de AppFlow y verificar la configuración:

```
- set appflow param [-templateRefresh <secs>] [-appnameRefresh <secs>]
   [-flowRecordInterval <secs>] [-udpPmtu <positive_integer>] [-
  httpUrl ( \*\*ENABLED\*\* | \*\*DISABLED\*\* )] [-httpCookie ( \*\*
  ENABLED\*\* | \*\*DISABLED\*\* )] [-httpReferer ( \*\*ENABLED\*\* |
  \*\*DISABLED\*\* )] [-httpMethod ( \*\*ENABLED\*\* | \*\*DISABLED
  \*\* )] [-httpHost ( \*\*ENABLED\*\* | \*\*DISABLED\*\* )] [-
  httpUserAgent ( \*\*ENABLED\*\* | \*\*DISABLED\*\* )] [-
  httpXForwardedFor ( \*\*ENABLED\*\* | \*\*DISABLED\*\* )][-
  clientTrafficOnly ( \*\*YES\*\* | \*\*NO\*\*)] [-
  webSaaSAppUsageReporting ( \*\*ENABLED\*\* | \*\*DISABLED\*\* )] [-
  logstreamOverNSIP ( \*\*ENABLED\*\* | \*\*DISABLED\*\* )]

- show appflow Param
<!--NeedCopy-->
```

Ejemplo

```
set appflow Param -templateRefresh 240 -udpPmtu 128 -httpUrl enabled -
   webSaaSAppUsageReporting ENABLED -logstreamOverNSIP ENABLED
<!--NeedCopy-->
```

Establezca los parámetros de AppFlow mediante la utilidad de configuración

Vaya a **Sistema > AppFlow**, haga clic en **Cambiar configuración de AppFlow**y especifique los parámetros de AppFlow relevantes.

Soporte para ofuscación de ID de suscriptor

A partir de la versión 13.0 build 35.xx de Citrix ADC, la configuración de AppFlow se ha mejorado para admitir el algoritmo “SubscriberidOfuscation” para ofuscar MSISDN en los registros de AppFlow de capa 4 o capa 7. Sin embargo, antes de configurar el algoritmo como MD5 o SHA256, primero debe habilitarlo como un parámetro de AppFlow. El parámetro está inhabilitado de forma predeterminada.

Configurar el algoritmo de ofuscación de ID de suscriptor mediante la CLI

En el símbolo del sistema, escriba:

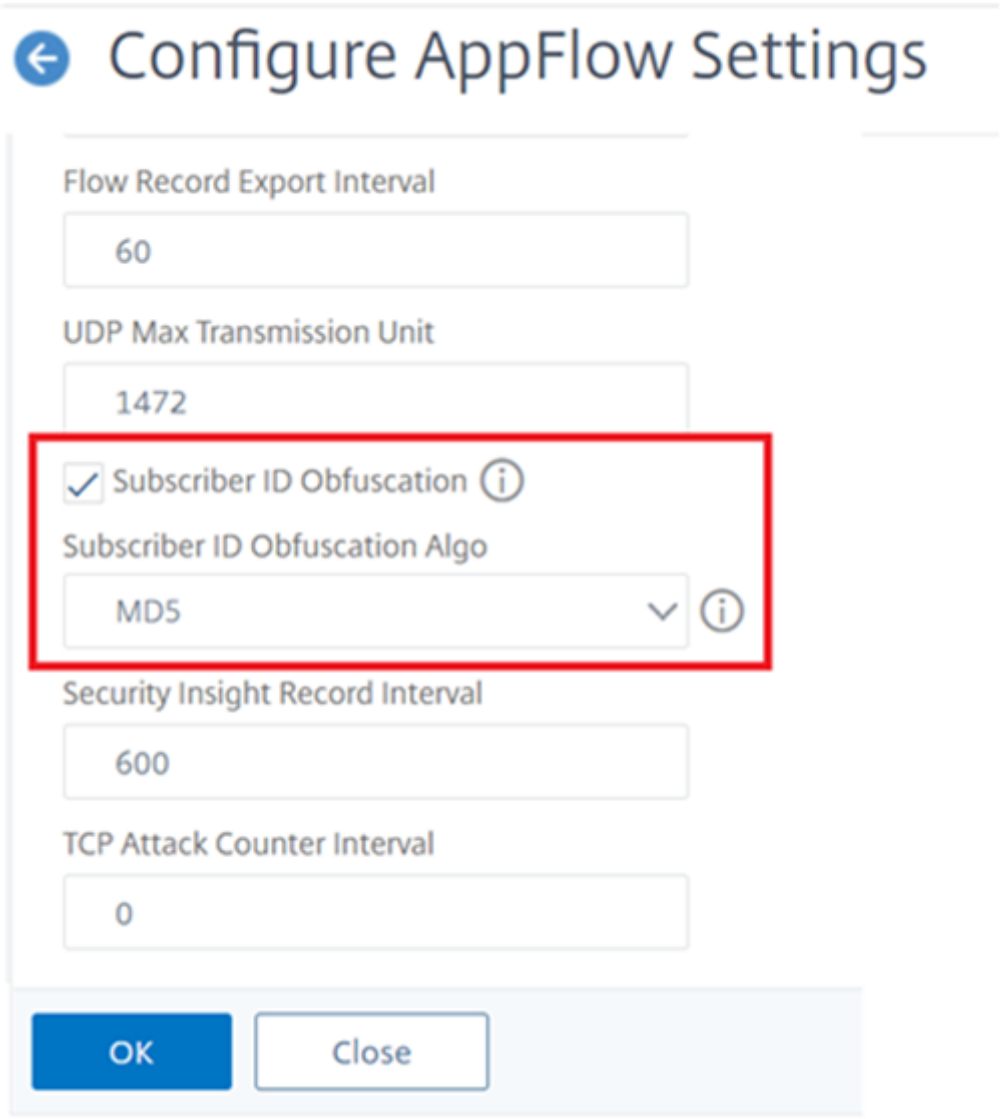
```
set appflow param [-subscriberIdObfuscation ( ENABLED | DISABLED )  [-
    subscriberIdObfuscationAlgo ( MD5 | SHA256 )]]
<!--NeedCopy-->
```

Ejemplo

```
set appflow param  - subscriberIdObfuscation ENABLED  -
    subscriberIdObfuscationAlgo SHA256
<!--NeedCopy-->
```

Configurar el algoritmo de ofuscación de ID de suscriptor mediante la GUI

1. Vaya a **Sistema > AppFlow**.
2. En el panel detallado de AppFlow, haga clic en **Cambiar configuración de AppFlow** en **Configuración**.
3. En la página Configure AppFlow Settings, defina los siguientes parámetros:
   - **Ofuscación de ID de suscriptor** Habilite la opción de ofuscación de MSISDN en los registros de AppFlow L4/L7.
   - **Algo de ofuscación de ID de abonado.** Seleccione el tipo de algoritmo como MD5 o SHA256.
4. Haga clic en **Aceptar** y **cerrar**.



Ejemplo: configurar AppFlow para DataStream

El siguiente ejemplo ilustra el procedimiento para configurar AppFlow para DataStream mediante la interfaz de línea de comandos.

```
enable feature appflow

add db user sa password freebsd

add lbvserver lb0 MSSQL 10.102.147.97 1433 -appflowLog ENABLED

add service sv0 10.103.24.132 MSSQL 1433 -appflowLog ENABLED
```



```
8
9  bind lbvserver lb0 sv0
10
11 add appflow collector col0 -IPAddress 10.102.147.90
12
13 add appflow action act0 -collectors col0
14
15 add appflow policy pol0 "mssql.req.query.text.contains("select")" act0
16
17 bind lbvserver lb0 -policyName pol0 -priority 10
18 <!--NeedCopy-->
```

Cuando el dispositivo Citrix ADC recibe una solicitud de base de datos, el dispositivo evalúa la solicitud en función de una directiva configurada. Si se encuentra una coincidencia, los detalles se envían al recopilador AppFlow configurado en la directiva.

Suscribir contadores en el recopilador de métricas

El recopilador de métricas admite la exportación de datos de análisis de series temporales cada 30 segundos en diferentes formatos, como AVRO, formato Prometheus y formato Influx DB. El recopilador de métricas admite la actualización dinámica de contadores, lo que le permite agregar los contadores necesarios a un archivo de esquema. Puede configurar el nombre del archivo de esquema mediante la interfaz CLI. El recopilador de métricas lee los nombres de los contadores del archivo de esquema y los exporta. El archivo de esquema predeterminado `schema.json` está presente en `/var/metrics_conf/`.

Configurar el recopilador de métricas para suscribir contadores mediante la CLI

Inicie la exportación de métricas configurando un servicio de recopilador.

En el símbolo del sistema, escriba:

"'

set analytics profile ns_analytics_time_series_profile -metrics ENABLED -collectors <collector name> -schemaFile <schema file name> schema.json -outputMode <avro | influx | prometheus>

"'

> **Nota:** `schema.json` Es la configuración predeterminada de schemaFile.

Se puede configurar un nuevo archivo de esquema con un conjunto de contadores necesario mediante el comando CLI para que el recopilador de métricas lo exporte. El archivo de esquema debe estar presente en la ubicación `/var/metrics_conf/`.

El archivo de esquema que contiene toda la lista de contadores (reference_schema.json) admitidos por stats infra está presente en la ubicación `/var/metrics_conf/`. Este archivo se puede usar como referencia para crear una lista personalizada de contadores.

Compruebe el resultado de la configuración de CLI en el símbolo del sistema:

”’

show analytics profile ns_analytics_time_series_profile
Name: ns_analytics_time_series_profile
Collector: <collector name>
Profile-type: timeseries
Output Mode: avro
Metrics: ENABLED
Schema File: schema.json
Events: ENABLED
Auditlog: DISABLED
Serve mode: Push
Reference Count: 0

”’

Exportación de datos de rendimiento de páginas web al recopilador de AppFlow

August 20, 2021

La aplicación EdgeSight Monitoring proporciona datos de supervisión de páginas web con los que puede supervisar el rendimiento de varias aplicaciones web servidas en un entorno Citrix ADC. Ahora puede exportar estos datos a recopiladores de AppFlow para obtener un análisis exhaustivo de las aplicaciones de la página web. AppFlow, que se basa en el estándar IPFIX, proporciona información más específica sobre el rendimiento de las aplicaciones web que la supervisión de EdgeSight por sí sola.

Puede configurar servidores virtuales de equilibrio de carga y conmutación de contenido para exportar datos de supervisión de EdgeSight a recopiladores de AppFlow. Antes de configurar un servidor virtual para la exportación de AppFlow, asocie una acción de AppFlow a la directiva de respuesta de EdgeSight Monitoring.

Los siguientes datos de rendimiento de páginas web se exportan a AppFlow:

- **Tiempo de carga de página**. Tiempo transcurrido, en milisegundos, desde que el explorador comienza a recibir el primer byte de una respuesta hasta que el usuario comienza a interactuar

con la página. En esta etapa, es posible que no se cargue todo el contenido de la página.
- **Tiempo de procesamiento de página**. Tiempo transcurrido, en milisegundos, desde que el explorador recibe el primer byte de respuesta hasta que se ha renderizado todo el contenido de la página o se ha agotado el tiempo de espera de la acción de carga de la página.
- **Tiempo empleado en la página**. Tiempo empleado por los usuarios en una página. Representa el tiempo transcurrido entre la solicitud de una página y la siguiente.

AppFlow transmite los datos de rendimiento mediante el formato de Internet Protocol Flow Information Export (IPFIX), que es un estándar abierto de Internet Engineering Task Force (IETF) definido en RFC 5101. Las plantillas de AppFlow utilizan los siguientes elementos de información específicos de la empresa (EIE) para exportar la información:

- **Hora de finalización de carga del cliente**. Hora en que el explorador recibió el último byte de una respuesta para cargar todos los objetos de la página, como imágenes, scripts y hojas de estilo.
- **Hora de inicio de carga del cliente**. Hora en que el explorador recibe el primer byte de la respuesta para cargar cualquier objeto de la página, como imágenes, scripts y hojas de estilo.
- **Hora de finalización del procesamiento del cliente**. Hora en la que un explorador terminó de renderizar toda la página, incluidos los objetos incrustados.
- **Hora de inicio del modelizado del cliente**. Hora en la que el explorador comenzó a representar la página.

Requisitos previos para exportar datos de rendimiento de páginas web a recopiladores de AppFlow

Antes de asociar la acción AppFlow con la directiva AppFlow, compruebe que se han cumplido los siguientes requisitos previos:

- La función AppFlow se ha habilitado y configurado.
- Se ha habilitado la función Respondedor.
- Se ha habilitado la función de supervisión de EdgeSight.
- La supervisión de EdgeSight se ha habilitado en los servidores virtuales de equilibrio de carga o conmutación de contenido enlazados a los servicios de las aplicaciones para las que quiere recopilar los datos de rendimiento.

Asociación de una acción de AppFlow a la directiva de respuesta de supervisión de EdgeSight

Para exportar los datos de rendimiento de la página web al recopilador de AppFlow, debe asociar una acción de AppFlow a la directiva de respuesta de EdgeSight Monitoring. Una acción AppFlow especifica qué conjunto de recopiladores reciben el tráfico.

Para asociar una acción de AppFlow a la directiva EdgeSight Monitoring Responder mediante la CLI

En el símbolo del sistema, escriba:

```
set responder policy <name> -appflowAction <action_Name>
<!--NeedCopy-->
```

Ejemplo

```
set responder policy pol -appflowAction actn
<!--NeedCopy-->
```

Para asociar una acción de AppFlow a la directiva EdgeSight Monitoring Responder mediante la GUI

1. Vaya a **AppExpert** > **Respondedor** > **Directivas**.
2. En el panel de detalles, seleccione una directiva de respuesta de supervisión de EdgeSight y, a continuación, haga clic en **Abrir**.
3. En el cuadro de diálogo **Configurar directiva de respuesta**, en la lista desplegable **Acción de AppFlow**, seleccione la acción AppFlow asociada a los recopiladores a los que desea enviar los datos de rendimiento de la página web.
4. Haga clic en **Aceptar**.

Configuración de un servidor virtual para exportar estadísticas de EdgeSight a recopiladores de AppFlow

Para exportar información de estadísticas de EdgeSight desde un servidor virtual al recopilador AppFlow, debe asociar una acción AppFlow con el servidor virtual.

Para asociar una acción de AppFlow a un servidor virtual de equilibrio de carga o conmutación de contenido mediante la GUI

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**. También puede navegar a **Administración del tráfico** > **Cambio de contenido** > **Servidores virtuales**.
2. En el panel de detalles, seleccione un servidor virtual o varios servidores virtuales y, a continuación, haga clic en **Habilitar supervisión de EdgeSight**.

3. En el cuadro de diálogo Habilitar supervisión de EdgeSight, active la casilla de verificación **Exportar estadísticas de EdgeSight a Appflow**.
4. En la lista desplegable Acción de AppFlow, seleccione la acción **AppFlow** . La acción AppFlow define la lista de recopiladores AppFlow a los que exporta las estadísticas de EdgeSight Monitoring. Si ha seleccionado varios servidores virtuales de equilibrio de carga, la misma acción de AppFlow se asocia a las directivas de respuesta vinculadas a ellos. Posteriormente, puede cambiar la acción AppFlow configurada para cada servidor virtual de equilibrio de carga seleccionado individualmente, si es necesario.
5. Haga clic en **Aceptar**.

Fiabilidad de sesión en el par de alta disponibilidad de Citrix ADC

July 27, 2022

Cuando se produce una interrupción de la red o una conmutación por error del dispositivo durante una sesión ICA, la reconexión de la sesión puede utilizar uno de estos dos mecanismos: fiabilidad de la sesión o Reconexión automática de clientes.

Fiabilidad de sesión. El modo preferido es una experiencia fluida para el usuario. La interrupción apenas se nota en caso de interrupciones breves de la red.

Reconexión automática de clientes. La alternativa implica reiniciar el cliente. Este mecanismo es perjudicial para el usuario y no siempre se admite.

Los receptores pueden volver a conectar sus sesiones ICA sin problemas mediante la función de fiabilidad de sesiones ICA, cuando HDX Insight está habilitado.
Esta función funciona tanto de forma independiente como en una configuración de par de alta disponibilidad de Citrix ADC, e incluso cuando se produce una conmutación por error de Citrix ADC.

> **Nota:**
>
> - Los dispositivos Citrix ADC deben ejecutarse en la versión de software 11.1, compilación 49.16, o una posterior.
> - No debe habilitar ni inhabilitar el modo de fiabilidad de la sesión cuando los dispositivos Citrix ADC tengan conexiones activas.
> - La activación o desactivación de la función cuando las conexiones siguen activas hace que HDX Insight deje de analizar esas sesiones después de que se produzca una conmutación por error. Esto provoca la pérdida de información sobre las sesiones.
> - La fiabilidad de la sesión en una configuración de alta disponibilidad está inhabilitada de forma predeterminada para la versión 11.1 49.16 o una posterior del software Citrix ADC. La fiabilidad de la sesión se admite en una configuración de alta disponibilidad solo si ambos

> nodos de la configuración ejecutan la misma compilación (por ejemplo, la versión 11.1, compilación 53). En otras palabras, la fiabilidad de la sesión no se admite en una configuración de alta disponibilidad si ambos nodos ejecutan compilaciones diferentes (por ejemplo, un nodo tiene la versión 11.1, compilación 53, mientras que el otro tiene la versión 11.1, compilación 56). La fiabilidad de la sesión para SSL VDA se admite si se cumplen las siguientes condiciones:
>
>   - The "EnableSRonHAFailover" parameter in the `set ica parameter` command must be YES.
>   - The HTTPS must be used instead of HTTP while configuring the virtual server.
>
> - Cuando HDX Insight está habilitado, las aplicaciones de cifrado y los escritorios básicos se vuelven a conectar después de una conmutación por error de alta disponibilidad incluso si el parámetro EnableSRonHAFailover está inhabilitado.

Para configurar la fiabilidad de la sesión mediante CLI:

1. En la línea de comandos, utilice las credenciales de administrador del sistema predeterminadas para iniciar sesión en el sistema.
2. Para habilitar la fiabilidad de la sesión en la conmutación por error de alta disponibilidad, en la solicitud, escriba: `set ica parameter EnableSRonHAFailover YES`
3. Para inhabilitar la fiabilidad de la sesión en la conmutación por error de alta disponibilidad, en la solicitud, escriba: `set ica parameter EnableSRonHAFailover NO`

Para habilitar la fiabilidad de la sesión en la conmutación por error de alta disponibilidad mediante GUI:

1. En un explorador web, escriba la dirección IP de la instancia principal de Citrix ADC en el par HA (por ejemplo, http://192.168.100.1).
2. En **Nombre de usuario** y **Contraseña**, introduzca las credenciales de administrador.
3. En la ficha **Configuración**, vaya a **Sistema** > **Configuración** y haga clic en **Cambiar parámetros ICA**.
4. En la sección **Cambiar parámetros ICA**, seleccione **Fiabilidad de la sesión en la conmutación por error de alta disponibilidad**.
5. Haga clic en **Aceptar**.

Limitaciones

- Al habilitar esta función, se aumenta el consumo de ancho de banda, lo que se debe a que la función desactiva la compresión ICA. Y el tráfico adicional entre los nodos principal y secundario para mantenerlos sincronizados.
- Esta función solo se admite en el modo Activo-Pasivo. El modo Activo-Activo no se admite actualmente.
- Cuando HDX Insight está habilitado y la fiabilidad de la sesión en el botón de alta disponibili-

dad se establece en NO, solo se admite el modo de reconexión ACR en el caso de conmutación por error de alta disponibilidad de Citrix ADC. El botón de alta disponibilidad no inhabilita la fiabilidad de la sesión si HDX Insight está inhabilitado.

La tabla **Semántica de reconexión de sesión** es la siguiente:

La sesión vuelve a conectar la semántica

Estado	EnableSRonHAFailover Sí	EnableSRonHAFailover No (valor predeterminado)
Compatible con HDX Insight	La reconexión de sesiones ICA funciona	La reconexión de sesiones ICA no funciona
HDX Insight inhabilitado	La reconexión de sesiones ICA funciona	La reconexión de sesiones ICA funciona

Puntos que tener en cuenta

- La fiabilidad de las sesiones ICA funciona de forma inmediata con Citrix Gateway.
- La fiabilidad de la sesión para las sesiones ICA no funciona cuando se cumplen las dos condiciones siguientes:
  - HDX Insight está habilitado
  - EnableSRonHAFailover está establecido en NO
- Establecer el botón EnableSRonHAFailover en SÍ o NO no supone ninguna diferencia cuando HDX Insight está inhabilitado.

Citrix Web App Firewall

August 20, 2021

Los siguientes temas tratan los detalles de instalación y configuración de la función Citrix Web App Firewall.

Introducción	Información general sobre la seguridad web y cómo funciona el Web App Firewall.
Configuración	Cómo configurar el Web App Firewall para proteger un sitio web, un servicio web o un sitio web 2.0.

Firmas	Una descripción detallada sobre las firmas y cómo configurarlas desde una herramienta de análisis de vulnerabilidades admitida, y defina sus propias firmas, con ejemplos.
Introducción a las comprobaciones de seguridad	Una descripción detallada de las comprobaciones de seguridad de Web App Firewall, con información de configuración y ejemplos.
Perfiles	Descripción de cómo se configuran y utilizan los perfiles en Web App Firewall.
Directivas	Descripción de cómo se utilizan las directivas al configurar Web App Firewall, con ejemplos de directivas útiles.
Importaciones	Descripción de cómo el Web App Firewall utiliza diferentes tipos de archivos importados y cómo importar y exportar archivos.
Configuración global	Descripción de las funciones de Web App Firewall que se aplican a todos los perfiles y cómo configurarlos.
Casos de uso	Ejemplos extendidos que demuestran cómo configurar el Web App Firewall para proteger mejor tipos específicos de sitios web y servicios web más complejos.
Registros, estadísticas e informes	Cómo acceder y utilizar los registros del Web App Firewall, las estadísticas y los informes para ayudar a configurar el Web App Firewall.

Citrix Web App Firewall ofrece opciones fáciles de configurar para cumplir con una amplia gama de requisitos de seguridad de aplicaciones. Los perfiles de Web App Firewall, que consisten en conjuntos de comprobaciones de seguridad, se pueden utilizar para proteger tanto las solicitudes como las respuestas, proporcionando inspecciones profundas a nivel de paquete. Cada perfil incluye una opción para seleccionar protecciones básicas o protecciones avanzadas. Algunas protecciones pueden requerir el uso de otros archivos. Por ejemplo, las comprobaciones de validación xml pueden requerir archivos WSDL o esquema. Los perfiles también pueden utilizar otros archivos, como firmas u objetos de error. Estos archivos se pueden agregar localmente o pueden importarse con anticipación y

guardarse en el dispositivo para su uso futuro.

Cada directiva identifica un tipo de tráfico y ese tráfico se inspecciona para detectar las infracciones de comprobación de seguridad especificadas en el perfil asociado a la directiva. Las directivas pueden tener diferentes puntos de enlace, que determinan el alcance de la directiva. Por ejemplo, una directiva enlazada a un servidor virtual específico se invoca y evalúa solo para el tráfico que fluye a través de ese servidor virtual. Las directivas se evalúan en el orden de sus prioridades designadas y se aplica la primera que coincide con la solicitud o respuesta.

- Implementación rápida de la protección de Web App Firewall

  Puede utilizar el siguiente procedimiento para la implementación rápida de la seguridad de Web App Firewall:

  1. Agregue un perfil de Web App Firewall y seleccione el tipo apropiado (html, xml, JSON) para los requisitos de seguridad de la aplicación.
  2. Seleccione el nivel de seguridad requerido (básico o avanzado).
  3. Agregue o importe los archivos necesarios, como firmas o WSDL.
  4. Configure el perfil para utilizar los archivos y realice los cambios necesarios en la configuración predeterminada.
  5. Agregar una directiva de Web App Firewall para este perfil.
  6. Enlazar la directiva al punto de enlace de destino y especificar la prioridad.

- Entidades de Web App Firewall

  Perfil: un perfil de Web App Firewall especifica qué buscar y qué hacer. Inspecciona tanto la solicitud como la respuesta para determinar qué posibles violaciones de seguridad deben verificarse y qué acciones deben tomarse al procesar una transacción. Un perfil puede proteger una carga HTML, XML o HTML y XML. Dependiendo de los requisitos de seguridad de la aplicación, puede crear un perfil básico o avanzado. Un perfil básico puede proteger contra ataques conocidos. Si se requiere mayor seguridad, puede implementar un perfil avanzado para permitir el acceso controlado a los recursos de la aplicación, bloqueando ataques de día cero. Sin embargo, un perfil básico se puede modificar para ofrecer protecciones avanzadas, y a la inversa. Hay disponibles varias opciones de acción (por ejemplo, bloquear, registrar, aprender y transformar). Las comprobaciones de seguridad avanzadas pueden utilizar cookies de sesión y etiquetas de formulario ocultas para controlar y supervisar las conexiones del cliente. Los perfiles de Web App Firewall pueden aprender las infracciones desencadenadas y sugerir las reglas de relajación.

  Protecciones básicas: un perfil básico incluye un conjunto preconfigurado de reglas de relajación de URL de inicio y denegación de URL. Estas reglas de relajación determinan qué solicitudes deben permitirse y cuáles deben denegarse. Las solicitudes entrantes se comparan con estas listas y se aplican las acciones configuradas. Esto permite al usuario ser capaz de proteger aplicaciones con una configuración mínima para reglas de relajación. Las reglas de URL de

inicio protegen contra la navegación forzada. Las vulnerabilidades conocidas del servidor web que explotan los hackers pueden detectarse y bloquearse habilitando un conjunto de reglas predeterminadas Denegar URL. Los ataques lanzados comúnmente, como desbordamiento de búfer, SQL o scripts entre sitios también se pueden detectar fácilmente.

Protecciones avanzadas: como su nombre indica, se utilizan protecciones avanzadas para aplicaciones que tienen requisitos de seguridad más altos. Las reglas de relajación se configuran para permitir el acceso solo a datos específicos y bloquear el resto. Este modelo de seguridad positiva mitiga los ataques desconocidos, que podrían no ser detectados por las comprobaciones de seguridad básicas. Además de todas las protecciones básicas, un perfil avanzado realiza un seguimiento de una sesión de usuario mediante el control de la navegación, la comprobación de cookies, la especificación de los requisitos de entrada para varios campos de formulario y la protección contra la manipulación de formularios o ataques de falsificación de solicitudes entre sitios. El aprendizaje, que observa el tráfico e implementa las relajaciones adecuadas, está habilitado de forma predeterminada para muchas comprobaciones de seguridad. Aunque son fáciles de usar, las protecciones avanzadas requieren la debida consideración, ya que ofrecen una seguridad más estricta, pero también requieren más procesamiento y no permiten el uso del almacenamiento en caché, lo que puede afectar el rendimiento.

Importar: la funcionalidad de importación resulta útil cuando los perfiles de Web App Firewall deben utilizar archivos externos, es decir, archivos alojados en un servidor web externo o interno, o que deben copiarse desde un equipo local. Importar un archivo y almacenarlo en el dispositivo es útil, especialmente en situaciones en las que tiene que controlar el acceso a sitios web externos o cuando la compilación lleva mucho tiempo, los archivos grandes se deben sincronizar entre implementaciones de alta disponibilidad o puede reutilizar un archivo copiándolo en varios dispositivos. Por ejemplo:

- Los WSDL alojados en servidores web externos se pueden importar localmente antes de bloquear el acceso a sitios web externos.
- Los archivos de firma grandes generados por una herramienta de análisis externa como Cenzic se pueden importar y precompilar, mediante el esquema del dispositivo Citrix.
- Una página de error HTML o XML personalizada se puede importar desde un servidor web externo o copiar desde un archivo local.

Firmas: las firmas son potentes porque utilizan la coincidencia de patrones para detectar ataques maliciosos y se pueden configurar para comprobar tanto la solicitud como la respuesta de una transacción. Son una opción preferida cuando se necesita una solución de seguridad personalizable. Hay varias opciones (por ejemplo, bloquear, registrar, aprender y transformar) disponibles para la acción que se debe realizar cuando se detecta una coincidencia de firma. El Web App Firewall tiene un objeto de firma predeterminado integrado que consta de más de 1.300 reglas de firma, con una opción para obtener las reglas más recientes mediante la función de actualización automática. Las reglas creadas por otras herramientas de análisis

también se pueden importar. El objeto de firma se puede personalizar agregando nuevas reglas, que pueden funcionar con las demás comprobaciones de seguridad especificadas en el perfil de Web App Firewall. Una regla de firma puede tener varios patrones y puede marcar una infracción solo cuando todos los patrones coinciden, evitando así falsos positivos. La selección cuidadosa de un `fastmatch` patrón literal para una regla puede optimizar significativamente el tiempo de procesamiento.

Directivas: las directivasde Web App Firewall se utilizan para filtrar y separar el tráfico en diferentes tipos. Esto proporciona la flexibilidad necesaria para implementar diferentes niveles de protección de seguridad para los datos de la aplicación. El acceso a datos altamente confidenciales puede dirigirse a inspecciones avanzadas de comprobación de seguridad, mientras que los datos menos sensibles están protegidos por inspecciones de seguridad básicas. Las directivas también se pueden configurar para omitir la inspección de comprobación de seguridad para el tráfico inofensivo. Una mayor seguridad requiere más procesamiento, por lo que el diseño cuidadoso de las directivas puede proporcionar la seguridad deseada junto con un rendimiento optimizado. La prioridad de la directiva determina el orden en que se evalúa y su punto de enlace determina el alcance de su aplicación.

Resumen

1. Capacidad para proteger una amplia gama de aplicaciones protegiendo diferentes tipos de datos, implementando el nivel adecuado de seguridad para diferentes recursos y obteniendo el máximo rendimiento.
2. Flexibilidad para agregar o modificar una configuración de seguridad. Puede ajustar o relajar las comprobaciones de seguridad activando o desactivando las protecciones básicas y avanzadas.
3. Opción para convertir un perfil HTML a un perfil XML o Web2.0 (HTML+XML) y a la inversa, proporcionando la flexibilidad necesaria para agregar seguridad para diferentes tipos de carga útil.
4. Acciones fáciles de implementar para bloquear ataques, supervisarlos en registros, recopilar estadísticas o incluso transformar algunas cadenas de ataque para hacerlos inofensivos.
5. Capacidad para detectar ataques inspeccionando las solicitudes entrantes y para evitar fugas de datos confidenciales mediante la inspección de las respuestas enviadas por los servidores.
6. Capacidad para aprender del patrón de tráfico para obtener recomendaciones para reglas de relajación fácilmente modificables que se pueden implementar para permitir excepciones.
7. Modelo de seguridad híbrido que aplica la potencia de las firmas personalizables para bloquear los ataques que coincidan con los patrones especificados y proporciona la flexibilidad para utilizar las comprobaciones del modelo de seguridad positiva para protecciones de seguridad básicas o avanzadas.
8. Disponibilidad de informes de configuración completos, incluida información sobre el cumplimiento de PCI-DSS.

Preguntas frecuentes y guía de implementación

July 8, 2022

P: ¿Por qué Citrix Web App Firewall es la opción preferida para proteger las aplicaciones?

Con las siguientes funciones, Citrix Web App Firewall ofrece una solución de seguridad completa:

- **Modelo de seguridad híbrida:** el modelo de seguridad híbrida de Citrix ADC le permite aprovechar tanto un modelo de seguridad positivo como un modelo de seguridad negativo para crear una configuración idónea para sus aplicaciones.
  - El**modelo de seguridad positiva** protege contra desbordamiento de búfer, manipulación de parámetros CGI-BIN, manipulación de formularios y campos ocultos, exploración forzada, envenenamiento de cookies o sesiones, ACL rotas, scripts entre sitios (scripts entre sitios), inyección de comandos, inyección SQL, activación de errores sensible Fuga de información, uso inseguro de la criptografía, configuración incorrecta del servidor, puertas traseras y opciones de depuración, aplicación de directivas basadas en tarifas, vulnerabilidades de plataforma bien conocidas, vulnerabilidades de día cero, falsificación de solicitudes entre sitios (CSRF) y filtración de tarjetas de crédito y otros datos confidenciales.
  - El**modelo de seguridad negativa** utiliza firmas de conjunto enriquecido para protegerse contra vulnerabilidades de aplicaciones HTTP y L7. Web App Firewall está integrado con varias herramientas de análisis de terceros, como las que ofrecen Cenzic, Qualys, Whitehat e IBM. Los archivos XSLT integrados permiten importar reglas fácilmente, que se pueden utilizar junto con las reglas basadas en Snort de formato nativo. Una función de actualización automática obtiene las últimas actualizaciones de las nuevas vulnerabilidades.

El modelo de seguridad positiva podría ser la opción preferida para proteger aplicaciones que tienen una gran necesidad de seguridad, ya que le ofrece la opción de controlar por completo quién puede acceder a qué datos. Permites solo lo que quieres y bloquea el resto. Este modelo incluye una configuración de comprobación de seguridad integrada, que se puede implementar con unos pocos clics. Sin embargo, tenga en cuenta que cuanto más estricta sea la seguridad, mayor será la sobrecarga de procesamiento.

El modelo de seguridad negativa podría ser preferible para aplicaciones personalizadas. Las firmas permiten combinar varias condiciones y una coincidencia y la acción especificada solo se activan cuando se cumplen todas las condiciones. Bloqueas solo lo que no quieres y permites el resto. Un patrón de coincidencia rápida específico en una ubicación específica puede reducir significativamente la sobrecarga de procesamiento para optimizar el rendimiento. La opción de agregar sus propias reglas de firma, en función de las necesidades de seguridad específicas de sus aplicaciones, le da la

flexibilidad de diseñar sus propias soluciones de seguridad personalizadas.

- **Detección y protección de solicitudes y respuestas: puede inspeccionar las solicitudes entrantes para detectar cualquier comportamiento sospechoso y tomar las medidas adecuadas, así como** comprobar las respuestas para detectar y proteger contra la fuga de datos confidenciales.
- **Conjunto completo de protecciones integradas para cargas útiles HTML, XML y JSON:** Web App Firewall ofrece 19 comprobaciones de seguridad diferentes. Seis de ellos (como URL de inicio y Denegar URL) se aplican tanto a datos HTML como XML. Cinco comprobaciones (como la coherencia de campo y el formato de campo) son específicas de HTML y ocho (como el formato XML y la interoperabilidad de servicios web) son específicas de las cargas útiles XML. Esta función incluye un amplio conjunto de acciones y opciones. Por ejemplo, el cierre de URL le permite controlar y optimizar la navegación a través de su sitio web para protegerte contra la navegación forzosa sin tener que configurar reglas de relajación para permitir todas y cada una de las URL legítimas. Tiene la opción de eliminar o eliminar los datos confidenciales, como los números de tarjetas de crédito, de la respuesta. Ya sea protección contra ataques de matriz SOAP, denegación de servicio XML (xDoS), prevención de análisis WSDL, comprobación de archivos adjuntos o cualquier otro tipo de ataques XML, tiene la tranquilidad de saber que tiene un escudo sólido que protege sus datos cuando sus aplicaciones están protegidas por Web App Firewall. Las firmas permiten configurar reglas mediante expresiones XPATH-para detectar infracciones en el cuerpo y en el encabezado de una carga útil JSON.
- **GWT:** Compatibilidad con la protección de las aplicaciones de Google Web Toolkit para protegerlas contra SQL, scripts entre sitios y violaciones de comprobación de coherencia de campos de formulario.
- Interfaz**gráfica de usuario (GUI) sin Java y fácil de usar: una interfaz gráfica de usuario** intuitiva y comprobaciones de seguridad preconfiguradas facilitan la implementación de la seguridad haciendo clic en unos pocos botones. Un asistente le pide y le guía para crear los elementos necesarios, como perfiles, directivas, firmas y enlaces. La GUI basada en HTML5 no tiene ninguna dependencia de Java. Su rendimiento es significativamente mejor que el de las versiones anteriores basadas en Java.
- **CLI fácil de usar y automatizable:** La mayoría de las opciones de configuración disponibles en la GUI también están disponibles en la interfaz de línea de comandos (CLI). Los comandos CLI se pueden ejecutar mediante un archivo por lotes y son fáciles de automatizar.
- **Compatibilidad con API REST:** El protocolo Citrix ADC NITRO admite un amplio conjunto de API REST para automatizar la configuración de Web App Firewall y recopilar estadísticas pertinentes para la supervisión continua de las infracciones de seguridad.
- **Aprendizaje:** La capacidad del Web App Firewall para aprender mediante la supervisión del tráfico para ajustar la seguridad es muy fácil de usar. El motor de aprendizaje recomienda re-

glas, lo que facilita la implementación de relajaciones sin tener competencia en las expresiones regulares.

- **Compatibilidad con el editor de RegEx:** Las expresiones regulares ofrecen una solución elegante al dilema de querer consolidar reglas y, al mismo tiempo, optimizar la búsqueda. Puede aprovechar el poder de las expresiones regulares para configurar direcciones URL, nombres de campo, patrones de firma, etc. El editor de RegEx integrado en la interfaz gráfica de usuario le ofrece una referencia rápida para las expresiones y proporciona una forma cómoda de validar y probar la precisión de su RegEx.
- **Página de error personalizada:** las solicitudes bloqueadas se pueden redirigir a una URL de error. También tiene la opción de mostrar un objeto de error personalizado que utiliza variables compatibles y la directiva Citrix Advanced (expresiones PI avanzadas) para incrustar información de solución de problemas para el cliente.
- Informes de**PCI-DSS, estadísticas y otros informes de infracciones:** El amplio conjunto de informes facilita el cumplimiento de los requisitos de cumplimiento de PCI-DSS, la recopilación de estadísticas sobre los contadores de tráfico y la visualización de informes de infracciones de todos los perfiles o solo de un perfil.
- **Registro y click-to-rule desde el registro:** se admite el registro detallado tanto para el formato nativo como para el formato CEF. Web App Firewall le ofrece la posibilidad de filtrar los mensajes de registro de destino en el visor de syslog. Puede seleccionar un mensaje de registro e implementar una regla de relajación correspondiente con solo hacer clic en un botón. Tiene la flexibilidad de personalizar los mensajes de registro y también es compatible con la generación de registros web. Para obtener más información, consulte el tema Registros de Web App Firewall.
- **Incluir registros de infracciones en registros de seguimiento:** la capacidad de incluir mensajes de registro en los registros de seguimiento facilita la depuración de comportamientos inesperados, como restablecer y bloquear.
- **Clonación:** La útil opción de perfil Importar/Exportar le permite clonar la configuración de seguridad de un dispositivo Citrix ADC a otros. Las opciones de exportación de datos aprendidos facilitan la exportación de las reglas aprendidas a un archivo Excel. A continuación, puede hacer que el propietario de la aplicación las revise y apruebe antes de aplicarlas.
- Se puede diseñar**una plantilla de AppExpert** (un conjunto de opciones de configuración) para proporcionar la protección adecuada a sus sitios web. Puede simplificar y acelerar el proceso de implementación de una protección similar en otros dispositivos exportando estas plantillas de cortador de cookies a una plantilla.

Para obtener más información, consulte el tema de plantilla de AppExpert.

- **Comprobaciones de seguridad sin sesión:** la implementación de comprobaciones de seguridad sin sesión puede ayudarle a reducir el espacio de memoria y acelerar el procesamiento.

- **Interoperabilidad con otras funciones de Citrix ADC:** Web App Firewall funciona a la perfección con otras funciones de Citrix ADC, como reescritura, transformación de URL, almacenamiento en caché integrado, CVPN y limitación de velocidad.
- **Compatibilidad con expresiones de PI en las directivas:** puede aprovechar el poder de las expresiones de PI avanzadas para diseñar directivas que implementen diferentes niveles de seguridad para distintas partes de su aplicación.
- **Compatibilidad con IPv6:** El Web App Firewall admite los protocolos IPv4 e IPv6.
- **Protección de seguridad basada en geolocalización:** tiene la flexibilidad de utilizar la directiva Citrix Advanced (PI Expressions) para configurar directivas basadas en la ubicación, que se puede utilizar junto con una base de datos de ubicaciones integrada para personalizar la protección del firewall. Puede identificar las ubicaciones desde las que se originan las solicitudes malintencionadas y aplicar el nivel deseado de inspecciones de comprobación de seguridad para las solicitudes que se originan en una ubicación geográfica específica.
- **Rendimiento:** el **streaming** del lado de la solicitud mejora significativamente el rendimiento. En cuanto se procesa un campo, los datos resultantes se reenvían al backend mientras continúa la evaluación de los campos restantes. La mejora del tiempo de procesamiento es especialmente significativa cuando se manejan puestos de gran tamaño.
- **Otras funciones de seguridad:** Web App Firewall tiene otras configuraciones de seguridad que pueden ayudar a garantizar la seguridad de sus datos. Por ejemplo, el **campo Confidencial permite bloquear la filtración de información confidencial** en los mensajes de registro y Eliminar **comentario HTML** permite eliminar los comentarios HTML de la respuesta antes de reenviarlos al cliente. **Los tipos de campo** se pueden utilizar para especificar qué entradas están permitidas en los formularios enviados a la solicitud.

P: ¿Qué debo hacer para configurar Web App Firewall?

Haga lo siguiente:

- Agregue un perfil de Web App Firewall y seleccione el tipo adecuado (html, xml, web2.0) para los requisitos de seguridad de la aplicación.
- Seleccione el nivel de seguridad necesario (básico o avanzado).
- Agregue o importe los archivos necesarios, como firmas o WSDL.
- Configure el perfil para que utilice los archivos y realice cualquier otro cambio necesario en la configuración predeterminada.
- Agregue una directiva de Web App Firewall para este perfil.
- Enlace la directiva al punto de enlace de destino y especifique la prioridad.

P: ¿Cómo sé qué tipo de perfil elegir?

El perfil Web App Firewall ofrece protección para cargas útiles HTML y XML. En función de las necesidades de la aplicación, puede elegir un perfil HTML o un perfil XML. Si su aplicación admite datos HTML y XML, puede elegir un perfil Web2.0.

P: ¿Cuál es la diferencia entre los perfiles básicos y avanzados? ¿Cómo decido cuál necesito?

La decisión de utilizar un perfil básico o avanzado depende de la necesidad de seguridad de su aplicación. Un perfil básico incluye un conjunto preconfigurado de reglas de relajación de URL de inicio y denegar URL. Estas reglas de relajación determinan qué solicitudes están permitidas y cuáles denegadas. Las solicitudes entrantes coinciden con las reglas preconfiguradas y se aplican las acciones configuradas. El usuario puede proteger las aplicaciones con una configuración mínima de reglas de relajación. Las reglas de URL de inicio protegen contra la navegación forzosa. Las vulnerabilidades conocidas del servidor web que explotan los piratas informáticos se pueden detectar y bloquear activando un conjunto de reglas predeterminadas de denegar URL. Los ataques lanzados con frecuencia, como desbordamiento de búfer, SQL o scripts entre sitios, también se pueden detectar fácilmente.

Como su nombre indica, las protecciones avanzadas son para aplicaciones que tienen requisitos de seguridad más altos. Las reglas de relajación se configuran para permitir el acceso solo a datos específicos y bloquear el resto. Este modelo de seguridad positiva mitiga los ataques desconocidos, que podrían no detectarse mediante comprobaciones de seguridad básicas. Además de todas las protecciones básicas, un perfil avanzado realiza un seguimiento de la sesión de un usuario mediante el control de la navegación, la comprobación de cookies, la especificación de los requisitos de entrada para varios campos de formulario y la protección contra la manipulación de formularios o los ataques de falsificación de solicitudes entre sitios. El aprendizaje, que observa el tráfico y recomienda las relajaciones adecuadas, está habilitado de forma predeterminada para muchas comprobaciones de seguridad. Aunque son fáciles de usar, las protecciones avanzadas requieren la debida consideración, ya que ofrecen una seguridad más estricta pero también requieren más procesamiento. Algunas comprobaciones de seguridad anticipadas no permiten el uso del almacenamiento en caché, lo que puede afectar al rendimiento.

Tenga en cuenta los siguientes puntos a la hora de decidir si quiere utilizar perfiles básicos o avanzados:

- Los perfiles básicos y avanzados son solo plantillas iniciales. Siempre puede modificar el perfil básico para implementar funciones de seguridad avanzadas y viceversa.
- Las comprobaciones de seguridad avanzadas requieren más procesamiento y pueden afectar al rendimiento. A menos que su aplicación necesite seguridad avanzada, es posible que quiera comenzar con un perfil básico y reforzar la seguridad según sea necesario para su aplicación.

- No quiere habilitar todas las comprobaciones de seguridad a menos que su aplicación lo necesite.

P: ¿Qué es una directiva? ¿Cómo selecciono el punto de enlace y establezco la prioridad?

Las directivas de Web App Firewall pueden ayudarle a ordenar el tráfico en grupos lógicos para configurar distintos niveles de implementación de seguridad. Seleccione cuidadosamente los puntos de enlace de las directivas para determinar qué tráfico coincide con cada directiva. Por ejemplo, si quiere que todas las solicitudes entrantes se comprueben en busca de ataques de scripts SQL/cross-site, puede crear una directiva genérica y vincularla globalmente. O bien, si quiere aplicar comprobaciones de seguridad más estrictas al tráfico de un servidor virtual que aloja aplicaciones que contienen datos confidenciales, puede vincular una directiva a ese servidor virtual.

La asignación cuidadosa de prioridades puede mejorar el procesamiento del tráfico. Desea asignar prioridades más altas a directivas más específicas y prioridades más bajas a directivas genéricas. Tenga en cuenta que cuanto mayor sea el número, menor será la prioridad. Una directiva con una prioridad de 10 se evalúa antes que una directiva que tiene una prioridad de 15.

Puede aplicar diferentes niveles de seguridad a distintos tipos de contenido, por ejemplo, las solicitudes de objetos estáticos como imágenes y texto se pueden omitir utilizando una directiva y las solicitudes de otros contenidos confidenciales pueden someterse a una comprobación muy estricta mediante una segunda directiva.

P: ¿Cómo configuro las reglas para proteger mi aplicación?

El Web App Firewall hace que sea muy fácil diseñar el nivel de seguridad adecuado para su sitio web. Puede tener varias directivas de Web App Firewall, enlazadas a diferentes perfiles de Web App Firewall, para implementar diferentes niveles de inspecciones de comprobación de seguridad para sus aplicaciones. Puede supervisar inicialmente los registros para observar qué amenazas de seguridad se están detectando y qué infracciones se están desencadenando. Puede agregar manualmente las reglas de relajación o aprovechar las reglas aprendidas recomendadas de Web App Firewall para implementar las relajaciones necesarias y evitar falsos positivos.

Citrix Web App Firewall ofrece compatibilidad con **visualizadores** en la GUI, lo que facilita mucho la administración de reglas. Puede ver fácilmente todos los datos en una pantalla y tomar medidas sobre varias reglas con un solo clic. La mayor ventaja del visualizador es que recomienda expresiones regulares para consolidar varias reglas. Puede seleccionar un subconjunto de reglas basando su selección en el delimitador y en la URL de acción. El soporte del visualizador está disponible para ver 1) reglas aprendidas y 2) reglas de relajación.

1. El visualizador de reglas aprendidas ofrece la opción de modificar las reglas e implementarlas como relajaciones. También puede omitir (ignorar) reglas.

2. El visualizador de relajaciones implementadas le ofrece la opción de agregar una nueva regla o modificar una existente. También puede habilitar o inhabilitar un grupo de reglas seleccionando un nodo y haciendo clic en el botón **Activar** o **Desactivar** del visualizador de relajación.

P: ¿Qué son las firmas? ¿Cómo sé qué firmas debo usar?

Una firma es un objeto que puede tener varias reglas. Cada regla consta de uno o varios patrones que se pueden asociar a un conjunto de acciones especificado. Web App Firewall tiene un objeto de firma predeterminado integrado que consta de más de 1300 reglas de firma, con la opción de obtener las reglas más recientes mediante la función de **actualización automática** para obtener protección contra nuevas vulnerabilidades. Las reglas creadas por otras herramientas de análisis también se pueden importar.

Las firmas son muy potentes porque utilizan la coincidencia de patrones para detectar ataques maliciosos y se pueden configurar para comprobar tanto la solicitud como la respuesta de una transacción. Son una opción preferida cuando se necesita una solución de seguridad personalizable. Hay varias opciones de acción disponibles (por ejemplo, bloquear, registrar, aprender y transformar) cuando se detecta una coincidencia de firma. Las firmas predeterminadas cubren reglas para proteger diferentes tipos de aplicaciones, como web-cgi, web-coldfusion, web-frontpage, web-iis, web-php, web-client, web-activex, web-shell-shock y web-struts. Para satisfacer las necesidades de su aplicación, puede seleccionar e implementar las reglas pertenecientes a una categoría específica.

Sugerencias para el uso de firmas:

- Puede hacer una copia del objeto de firma predeterminado y modificarlo para habilitar las reglas que necesitas y configurar las acciones que quieras.
- El objeto de firma se puede personalizar agregando nuevas reglas, que pueden funcionar junto con otras reglas de firma.
- Las reglas de firma también se pueden configurar para que funcionen junto con las comprobaciones de seguridad especificadas en el perfil de Web App Firewall. Si una firma y una comprobación de seguridad detectan una coincidencia que indica una infracción, la acción más restrictiva es la que se aplica.
- Una regla de firma puede tener varios patrones y configurarse para marcar una infracción solo cuando todos los patrones coinciden, evitando así falsos positivos.
- La selección cuidadosa de un patrón de coincidencia rápida literal para una regla puede optimizar significativamente el tiempo de procesamiento.

P: ¿Funciona Web App Firewall con otras funciones de Citrix ADC?

Web App Firewall está totalmente integrado en el dispositivo Citrix ADC y funciona a la perfección con otras funciones. Puede configurar la máxima seguridad para su aplicación mediante otras funciones de seguridad de Citrix ADC junto con Web App Firewall. Por ejemplo, **AAA-TM** se puede utilizar para

autenticar al usuario, comprobar la autorización del usuario para acceder al contenido y registrar los accesos, incluidos los intentos de inicio de sesión no válidos. La**reescritura se** puede utilizar para modificar la URL o para agregar, modificar o eliminar encabezados, y **Responder** se puede utilizar para entregar contenido personalizado a distintos usuarios. Puede definir la carga máxima de su sitio web utilizando la **limitación de velocidad** para supervisar el tráfico y reducir la velocidad si es demasiado alta. La protección**de denegación de servicio (DoS) HTTP** puede ayudar a distinguir entre clientes HTTP reales y clientes DoS maliciosos. Puede reducir el alcance de la inspección de comprobación de seguridad vinculando las directivas de Web App Firewall a los servidores virtuales y, al mismo tiempo, optimizar la experiencia del usuario mediante la función **Equilibrio de carga** para administrar las aplicaciones más utilizadas. Las solicitudes de objetos estáticos, como imágenes o texto, pueden eludir la inspección de las comprobaciones de seguridad, aprovechando el almacenamiento en **caché** o la **compresión** integrados para optimizar el uso del ancho de banda de dicho contenido.

P: ¿Cómo procesa la carga útil el Web App Firewall y las demás funciones de Citrix ADC?

Hay disponible un diagrama que muestra los detalles del flujo de paquetes L7 en un dispositivo Citrix ADC en la sección Orden de procesamiento de funciones .

P: ¿Cuál es el flujo de trabajo recomendado para la implementación de Web App Firewall?

Ahora que conoce las ventajas de utilizar las protecciones de seguridad de última generación de Citrix Web App Firewall, es posible que quiera recopilar información adicional que le ayude a diseñar la solución óptima para sus necesidades de seguridad. Citrix recomienda hacer lo siguiente:

- **Conozca su entorno:** Conocer su entorno le ayudará a identificar la mejor solución de protección de seguridad (firmas, controles de seguridad o ambas) para sus necesidades. Antes de comenzar la configuración, debe recopilar la siguiente información.
  - **SO:** ¿Qué tipo de sistema operativo (MS Windows, Linux, BSD, Unix, otros) tienes?
  - **Servidor web:** ¿Qué servidor web (IIS, Apache o Citrix ADC Enterprise Server) está ejecutando?
  - **Aplicación:** ¿Qué tipo de aplicaciones se ejecutan en el servidor de aplicaciones (por ejemplo, ASP.NET, PHP, Cold Fusion, ActiveX, FrontPage, Struts, CGI, Apache Tomcat, Domino y WebLogic)?
  - ¿Tiene aplicaciones personalizadas o aplicaciones listas para usar (por ejemplo, Oracle, SAP)? ¿Qué versión está usando?
  - **SSL:** ¿Necesitas SSL? Si es así, ¿qué tamaño de clave (512, 1024, 2048, 4096) se utiliza para firmar certificados?
  - **Volumen de tráfico:** ¿Cuál es la tasa media de tráfico a través de sus aplicaciones? ¿Tienes picos estacionales o específicos en el tráfico?

  - **Server Farm:** ¿Cuántos servidores tiene? ¿Necesitas usar el equilibrio de cargas?
  - **Base de datos:** ¿Qué tipo de base de datos (MS-SQL, MySQL, Oracle, Postgres, SQLite, nosql, Sybase, Informix, etc.) utiliza?
  - **Conectividad de base de datos:** ¿Qué tipo de conectividad de base de datos tiene (DSN, cadena de conexión por archivo, cadena de conexión de archivo único) y qué controladores se utilizan?
- **Identifique sus necesidades de seguridad:** es posible que quiera evaluar qué aplicaciones o datos específicos necesitan la máxima protección de seguridad, cuáles son menos vulnerables y cuáles son los que pueden eludirse de forma segura la inspección de seguridad. Esto le ayudará a encontrar una configuración óptima y a diseñar directivas y puntos de enlace adecuados para segregar el tráfico. Por ejemplo, es posible que quiera configurar una directiva para omitir la inspección de seguridad de las solicitudes de contenido web estático, como imágenes, archivos MP3 y películas, y configurar otra directiva para aplicar comprobaciones de seguridad avanzadas a las solicitudes de contenido dinámico. Puede utilizar varias directivas y perfiles para proteger distintos contenidos de la misma aplicación.
- **Requisito de licencia:** Citrix ofrece una solución unificada para optimizar el rendimiento de su aplicación aprovechando un amplio conjunto de funciones como equilibrio de carga, cambio de contenido, almacenamiento en caché, compresión, respuesta, reescritura y filtrado de contenido, por nombrar algunas. Identificar las funciones que quieres puede ayudarte a decidir qué licencia necesitas.
- **Instalación y referencia de un dispositivo Citrix ADC:** cree un servidor virtual y ejecute tráfico de prueba a través de él para tener una idea de la velocidad y la cantidad de tráfico que circula por el sistema. Esta información le ayudará a identificar sus necesidades de capacidad y a seleccionar el dispositivo adecuado (VPX, MPX o SDX).
- **Implementar Web App Firewall:** Utilice el asistente Web App Firewall para proceder con una configuración de seguridad sencilla. El asistente le guiará por varias pantallas y le pedirá que agregue un perfil, una directiva, una firma y comprobaciones de seguridad.
  - **Perfil:** seleccione un nombre significativo y el tipo adecuado (HTML, XML o WEB 2.0) para su perfil. La directiva y las firmas se generarán automáticamente con el mismo nombre.
  - **Directiva:** La directiva generada automáticamente tiene la expresión predeterminada (true), que selecciona todo el tráfico y está enlazada globalmente. Este es un buen punto de partida a menos que tengas en mente una directiva específica que quieras usar.
  - **Protecciones:** El asistente le ayuda a aprovechar el modelo de seguridad híbrida, en el que puede utilizar las firmas predeterminadas que ofrecen un amplio conjunto de reglas para proteger distintos tipos de aplicaciones. El modo de edición**simple** permite ver las distintas categorías (CGI, Cold Fusion, PHP, etc.). Puede seleccionar una o varias categorías para identificar un conjunto específico de reglas aplicables a su aplicación. Utilice la opción **Acción** para habilitar todas las reglas de firma de las categorías seleccionadas. Asegúrese de que el bloqueo está desactivado para poder supervisar el tráfico antes de re-

forzar la seguridad. Haga clic en **Continuar**. En el panel **Especificar protecciones profundas**, puede realizar los cambios necesarios para implementar las protecciones de comprobación de seguridad. En la mayoría de los casos, las protecciones básicas son suficientes para la configuración de seguridad inicial. Ejecute el tráfico durante un tiempo para recopilar una muestra representativa de los datos de inspección de seguridad.

- **ReFUERZO DE LA SEGURIDAD:** Después de implementar Web App Firewall y observar el tráfico durante un tiempo, puede empezar a reforzar la seguridad de sus aplicaciones implementando relajaciones y, a continuación, habilitando el bloqueo. Las reglas de **aprendizaje**, **visualizador** y **clic para implementar** son funciones útiles que hacen que sea muy fácil ajustar la configuración para obtener el nivel adecuado de relajación. En este punto, también puede cambiar la expresión de la directiva y/o configurar directivas y perfiles adicionales para implementar los niveles de seguridad deseados para diferentes tipos de contenido.
- **Depuración:** si observa un comportamiento inesperado de la aplicación, Web App Firewall ofrece varias opciones para una depuración sencilla:
  * **Registro**. Si se bloquean solicitudes legítimas, el primer paso es comprobar el archivo ns.log para ver si se está desencadenando alguna infracción inesperada de comprobación de seguridad.
  * **Inhabilitar función.** Si no vaya ninguna infracción pero sigue observando un comportamiento inesperado, como el restablecimiento de una aplicación o el envío de respuestas parciales, puede inhabilitar la función Web App Firewall para la depuración. Si el problema persiste, descarta el Web App Firewall como sospechoso.
  * **Seguimiento de registros con mensajes de registro.** Si el problema parece estar relacionado con Web App Firewall y necesita una inspección más detallada, tiene la opción de incluir mensajes de infracción de seguridad en un nstrace. Puede usar "Seguir secuencia TCP" en el seguimiento para ver los detalles de la transacción individual, incluidos los encabezados, la carga útil y el mensaje de registro correspondiente, juntos en la misma pantalla. Los detalles sobre cómo utilizar esta funcionalidad están disponibles en los Apéndices.

Introducción a Citrix Web Application Firewall

August 20, 2021

Citrix Web App Firewall evita infracciones de seguridad, pérdida de datos y posibles modificaciones no autorizadas en sitios web que acceden a información confidencial de negocios o clientes. Lo hace filtrando tanto las solicitudes como las respuestas, examinándolas en busca de pruebas de actividad maliciosa y bloqueando las solicitudes que exhiben dicha actividad. Su sitio está protegido no solo de tipos comunes de ataques, sino también de ataques nuevos, aún desconocidos. Además de proteger

los servidores web y sitios web del acceso no autorizado, Web App Firewall protege contra vulnerabilidades en códigos o scripts CGI heredados, marcos web, software de servidor web y otros sistemas operativos subyacentes.

Citrix Web App Firewall está disponible como dispositivo independiente o como función en un dispositivo virtual Citrix ADC (VPX). En la documentación de Web App Firewall, el término Citrix ADC hace referencia a la plataforma en la que se ejecuta Web App Firewall, independientemente de si esa plataforma es un dispositivo de firewall dedicado, un ADC de Citrix en el que también se han configurado otras funciones o un dispositivo Citrix ADC VPX.

Para utilizar el Web App Firewall, debe crear al menos una configuración de seguridad para bloquear las conexiones que infrinjan las reglas establecidas para los sitios web protegidos. El número de configuraciones de seguridad que puede desear crear depende de la complejidad de su sitio web. A veces, una sola configuración es suficiente. En otros casos, especialmente aquellos que incluyen sitios web interactivos, sitios web que acceden a servidores de bases de datos, almacéns en línea con carritos de compra, es posible que necesite varias configuraciones diferentes para proteger mejor los datos confidenciales sin desperdiciar un esfuerzo significativo en contenido que no es vulnerable a ciertos tipos de ataques. A menudo, puede dejar sin cambios los valores predeterminados de la configuración global, que afectan a todas las configuraciones de seguridad. Sin embargo, puede cambiar la configuración global si entran en conflicto con otras partes de la configuración o si prefiere personalizarla.

Seguridad de aplicaciones web

La seguridad de aplicaciones web es la seguridad de red para equipos y programas que se comunican mediante los protocolos HTTP y HTTPS. Se trata de un ámbito amplio en el que abundan los defectos y debilidades de seguridad. Los sistemas operativos tanto en servidores como en clientes tienen problemas de seguridad y son vulnerables a ataques. El software de servidor web y las tecnologías habilitadoras de sitios web como CGI, Java, JavaScript, PERL y PHP tienen vulnerabilidades subyacentes. Los exploradores y otras aplicaciones cliente que se comunican con aplicaciones habilitadas para Web también tienen vulnerabilidades. Los sitios web que utilizan cualquier tecnología pero la más simple de HTML, incluyendo cualquier sitio que permite la interacción con los visitantes, a menudo tienen vulnerabilidades propias.

En el pasado, una violación de la seguridad era a menudo solo una molestia, pero hoy en día no es así. Por ejemplo, los ataques en los que un hacker obtuvo acceso a un servidor web e hizo modificaciones no autorizadas (desfiguradas) en un sitio web solían ser comunes. Por lo general, eran lanzados por hackers que no tenían más motivación que demostrar sus habilidades a compañeros hackers o avergonzar a la persona o empresa objetivo. Sin embargo, la mayoría de las infracciones de seguridad actuales están motivadas por el deseo de dinero. La mayoría trata de lograr uno o ambos de los siguientes objetivos: obtener información privada sensible y potencialmente valiosa, u obtener acceso no autorizado y control de un sitio web o servidor web.

Ciertas formas de ataques web se centran en obtener información privada. Estos ataques a menudo son posibles incluso contra sitios web que son lo suficientemente seguros como para evitar que un atacante tome el control total. La información que un atacante puede obtener de un sitio web puede incluir nombres de clientes, direcciones, números de teléfono, números de seguridad social, números de tarjetas de crédito, registros médicos y otra información privada. El atacante puede utilizar esta información o venderla a otros. Gran parte de la información obtenida por tales ataques está protegida por la ley, y toda por la costumbre y la expectativa. Una infracción de este tipo puede tener graves consecuencias para los clientes cuya información privada se vea comprometida. En el mejor de los casos, estos clientes tienen que ejercer vigilancia para evitar que otros abusen de sus tarjetas de crédito, abran cuentas de crédito no autorizadas a su nombre o se apropien de sus identidades (robo de identidad). En el peor de los casos, los clientes pueden enfrentar calificaciones crediticias arruinadas o incluso ser culpados por actividades delictivas en las que no tenían parte.

Otros ataques web tienen como objetivo obtener el control (o *comprometer*) un sitio web o el servidor en el que opera, o ambos. Un hacker que obtenga el control de un sitio web o servidor puede usarlo para alojar contenido no autorizado, actuar como proxy para contenido alojado en otro servidor web, proporcionar servicios SMTP para enviar correo electrónico masivo no solicitado o proporcionar servicios DNS para apoyar tales actividades en otros servidores web comprometidos. La mayoría de los sitios web alojados en servidores web comprometidos promueven negocios cuestionables o completamente fraudulentos. Por ejemplo, la mayoría de los sitios web de phishing y los sitios web de explotación infantil se alojan en servidores web comprometidos.

Proteger sus sitios web y servicios web contra estos ataques requiere una defensa multicapa capaz de bloquear ataques conocidos con funciones identificables y protegerse contra ataques desconocidos, que a menudo se pueden detectar porque se ven diferentes del tráfico normal a sus sitios web y sitios web servicios.

Ataques web conocidos

La primera línea de defensa para sus sitios web es la protección contra el gran número de ataques que se sabe que existen y que han sido observados y analizados por expertos en seguridad web. Los tipos comunes de ataques contra sitios web basados en HTML incluyen:

- **Ataques de desbordamiento de búfer.** El envío de una URL larga, una cookie larga o información larga a un servidor web hace que el sistema se bloquee, bloquee o proporcione acceso no autorizado al sistema operativo subyacente. Se puede utilizar un ataque de desbordamiento de búfer para obtener acceso a información no autorizada, poner en peligro un servidor web o ambos.
- **Ataques de seguridad de cookies.** Enviar una cookie modificada a un servidor web, generalmente con la esperanza de obtener acceso a contenido no autorizado mediante el uso de credenciales falsificadas.

- **Exploración forzada.** Acceder directamente a las URL de un sitio web, sin navegar a las URL con hipervínculos en la página principal u otras URL de inicio comunes en el sitio web. Las instancias individuales de navegación forzosa pueden indicar un usuario que marcó una página en su sitio web, pero los intentos repetidos de acceder a contenido inexistente o contenido al que los usuarios nunca deben acceder directamente, suelen representar un ataque a la seguridad del sitio web. La navegación forzada se utiliza normalmente para obtener acceso a información no autorizada, pero también se puede combinar con un ataque de desbordamiento de búfer en un intento de comprometer su servidor.
- **Ataques de seguridad de formularios web.** Enviar contenido inapropiado a su sitio web en un formulario web. El contenido inapropiado puede incluir campos ocultos modificados, HTML o código en un campo destinado únicamente a datos alfanuméricos, una cadena demasiado larga en un campo que acepta solo una cadena corta, una cadena alfanumérica en un campo que acepta solo un entero y una amplia variedad de otros datos que su sitio web no espera recibir en ese formulario web. Un ataque de seguridad de formularios web se puede utilizar para obtener información no autorizada de su sitio web o para comprometer el sitio web directamente, generalmente cuando se combina con un ataque de desbordamiento de búfer.

Dos tipos especializados de ataques a la seguridad de formularios web merecen una mención especial:

- **Ataques de inyección SQL.** Enviar un comando SQL activo o comandos en un formulario web o como parte de una dirección URL, con el objetivo de hacer que una base de datos SQL ejecute el comando o comandos. Los ataques de inyección SQL se utilizan normalmente para obtener información no autorizada.
- **Ataques de scripts entre sitios.** Usar una URL o un script en una página web para infringir la directiva del mismo origen, que prohíbe que cualquier script obtenga propiedades o modifique cualquier contenido de un sitio web diferente. Dado que los scripts pueden obtener información y modificar archivos en su sitio web, permitir que un script acceda al contenido de un sitio web diferente puede proporcionar al atacante los medios para obtener información no autorizada, poner en peligro un servidor web o ambos.

Los ataques contra servicios web basados en XML normalmente se clasifican en al menos una de las dos categorías siguientes: Intentos de enviar contenido inapropiado a un servicio web o intentos de violar la seguridad de un servicio web. Los tipos comunes de ataques contra servicios web basados en XML incluyen:

- **Código u objetos malintencionados.** Solicitudes XML que contienen código u objetos que pueden obtener directamente información confidencial o que pueden proporcionar a un atacante el control del servicio web o del servidor subyacente.
- **Solicitudes XML mal formadas.** Solicitudes XML que no se ajustan a la especificación XML de W3C y que, por lo tanto, pueden violar la seguridad en un servicio web inseguro
- **Ataques de denegación de servicio (DoS).** Solicitudes XML que se envían repetidamente y en

gran volumen, con la intención de abrumar el servicio web de destino y denegar a los usuarios legítimos el acceso al servicio web.

Además de los ataques basados en XML estándar, los servicios web XML y los sitios web 2.0 también son vulnerables a ataques de inyección SQL y scripts entre sitios, como se describe a continuación:

- **Ataques de inyección SQL.** Envío de un comando SQL activo o comandos en una solicitud basada en XML, con el objetivo de hacer que una base de datos SQL ejecute ese comando o comandos. Al igual que con los ataques de inyección HTML SQL, los ataques de inyección XML SQL se utilizan normalmente para obtener información no autorizada.
- **Ataques de scripts entre sitios.** Usar un script incluido en una aplicación basada en XML para infringir la directiva del mismo origen, que no permite que ningún script obtenga propiedades de ni modifique ningún contenido de una aplicación diferente. Dado que los scripts pueden obtener información y modificar archivos mediante la aplicación XML, permitir que un script acceda al contenido que pertenece a una aplicación diferente puede proporcionar a un atacante los medios para obtener información no autorizada, poner en peligro la aplicación o ambos

Los ataques web conocidos generalmente se pueden detener filtrando el tráfico del sitio web para obtener funciones específicas (firmas) que siempre aparecen para un ataque específico y nunca deben aparecer en el tráfico legítimo. Este enfoque tiene las ventajas de requerir relativamente pocos recursos y presentar relativamente poco riesgo de falsos positivos. Por lo tanto, es una herramienta valiosa para combatir ataques a sitios web y servicios web, y configurar la protección básica de firmas.

Ataques web desconocidos

La mayor amenaza contra sitios web y aplicaciones no proviene de ataques conocidos, sino de ataques desconocidos. La mayoría de los ataques desconocidos se clasifican en una de dos categorías: los ataques lanzados recientemente para los cuales las empresas de seguridad aún no han desarrollado una defensa efectiva (ataques de día cero), y ataques dirigidos cuidadosamente a un sitio web o servicio web específico en lugar de muchos sitios web o servicios web (ataques con lanza). Estos ataques, al igual que los ataques conocidos, están destinados a obtener información privada confidencial, comprometer el sitio web o servicio web y permitir que se utilice para ataques posteriores, o ambos objetivos.

Los ataques de día cero son una amenaza importante para todos los usuarios. Estos ataques suelen ser de los mismos tipos que los ataques conocidos; los ataques de día cero suelen involucrar SQL inyectado, un script entre sitios, una falsificación de solicitud entre sitios u otro tipo de ataque similar a los ataques conocidos. Por lo general, se dirigen a vulnerabilidades que los desarrolladores del software, sitio web o servicio web de destino no conocen o que han aprendido. Por lo tanto, las empresas de seguridad no han desarrollado defensas contra estos ataques, e incluso si lo han hecho, los usuarios no han obtenido e instalado los parches ni han realizado las soluciones necesarias para protegerse contra estos ataques. El tiempo transcurrido entre el descubrimiento de un ataque de día cero y la

disponibilidad de una defensa (la ventana de vulnerabilidad) se está reduciendo, pero los autores aún pueden contar con horas o incluso días en los que muchos sitios web y servicios web carecen de protección específica contra el ataque.

Los ataques con lanza son una amenaza importante, pero para un grupo de usuarios más selectos. Un tipo común de ataque con lanza, un phishes de lanza, está dirigido a clientes de un banco o institución financiera específico, o (menos comúnmente) a empleados de una empresa u organización específica. A diferencia de otros phishes, que a menudo son falsificaciones crudamente escritas que un usuario con alguna familiaridad con las comunicaciones reales de ese banco o institución financiera puede reconocer, los phishes lanza son letras perfectas y convincentes. Pueden contener información específica del individuo que, a primera vista, ningún extraño debe conocer o ser capaz de obtener. Por lo tanto, el phisher de lanza es capaz de convencer al objetivo de que proporcione la información solicitada, que el phisher puede utilizar para saquear cuentas, procesar dinero obtenido ilegalmente de otras fuentes, o para obtener acceso a otra información, incluso más sensible.

Ambos tipos de ataques tienen ciertas funciones que normalmente se pueden detectar, aunque no mediante el uso de patrones estáticos que buscan funciones específicas, al igual que las firmas estándar. La detección de estos tipos de ataques requiere enfoques más sofisticados e intensivos en recursos, como el filtrado heurístico y sistemas de modelos de seguridad positivos. El filtrado heurístico se ve, no para patrones específicos, sino para patrones de comportamientos. Los sistemas de modelos de seguridad positivos modelan el comportamiento normal del sitio web o servicio web que protegen y, a continuación, bloquean las conexiones que no encajan en ese modelo de uso normal. Las comprobaciones de seguridad basadas en URL y en formularios web perfilan el uso normal de sus sitios web y, a continuación, controlan cómo interactúan los usuarios con sus sitios web, mediante tanto heurística como seguridad positiva para bloquear el tráfico anómalo o inesperado. Tanto la seguridad heurística como la positiva, diseñada e implementada correctamente, pueden capturar la mayoría de los ataques que las firmas pierden. Sin embargo, requieren mucho más recursos que las firmas, y debe pasar algún tiempo configurándolas correctamente para evitar falsos positivos. Por lo tanto, se utilizan, no como la línea principal de defensa, sino como copias de seguridad de firmas u otros enfoques menos intensivos en recursos.

Al configurar estas protecciones avanzadas además de las firmas, se crea un modelo de seguridad híbrido, que permite al Web App Firewall proporcionar una protección completa contra ataques conocidos y desconocidos.

Cómo funciona Citrix Web Application Firewall

Al instalar Web App Firewall, se crea una configuración de seguridad inicial, que consta de una directiva, un perfil y un objeto de firmas. La directiva es una regla que identifica el tráfico que se va a filtrar y el perfil identifica los patrones y tipos de comportamiento que se deben permitir o bloquear cuando se filtra el tráfico. Los patrones más simples, que se denominan firmas, no se especifican dentro del perfil, sino en un objeto signatures asociado al perfil.

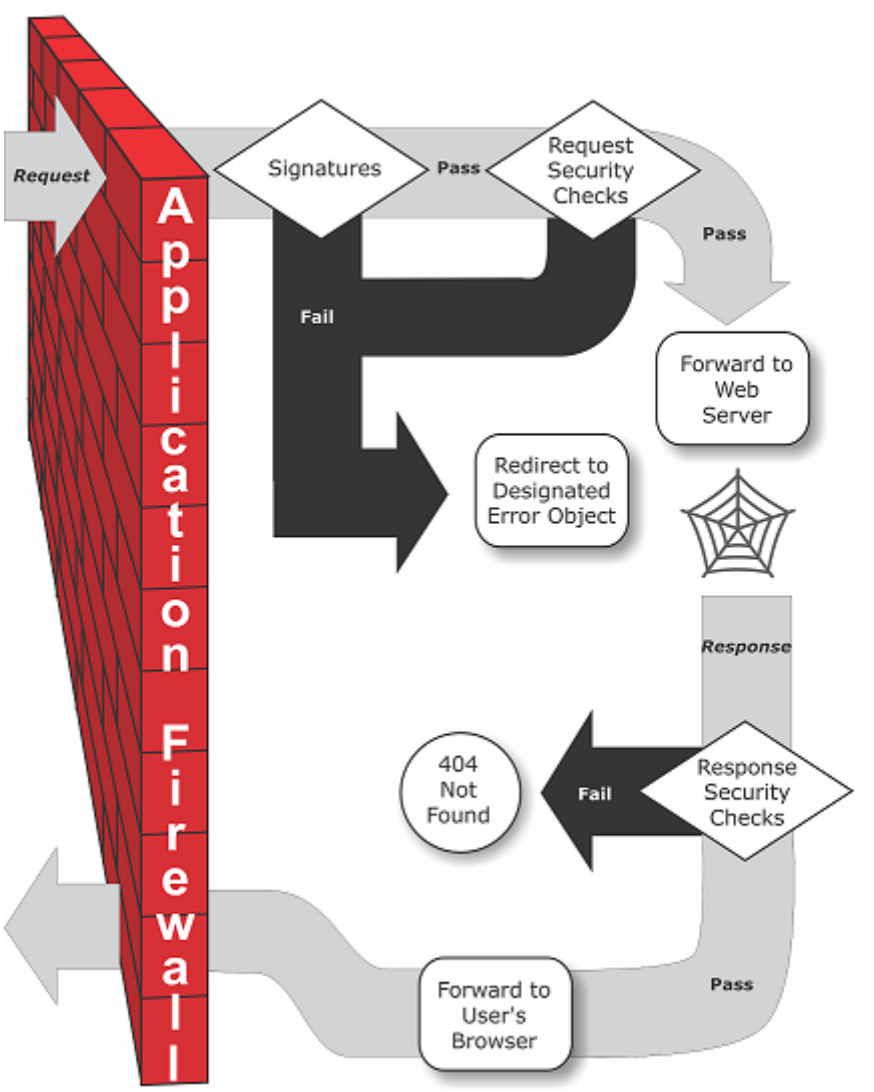
Una firma es una cadena o patrón que coincide con un tipo de ataque conocido. El Web App Firewall contiene más de mil firmas en siete categorías, cada una dirigida a ataques contra tipos específicos de servidores web y contenido web. Citrix actualiza la lista con nuevas firmas a medida que se identifican nuevas amenazas. Durante la configuración, especifique las categorías de firmas adecuadas para los servidores web y el contenido que necesita proteger. Las firmas proporcionan una buena protección básica con una baja sobrecarga de procesamiento. Si sus aplicaciones tienen vulnerabilidades especiales o detecta un ataque contra ellas para el que no existe ninguna firma, puede agregar sus propias firmas.

Las protecciones más avanzadas se denominan comprobaciones de seguridad. Una comprobación de seguridad es una inspección algorítmica más rigurosa de una solicitud de patrones o tipos de comportamiento específicos que podrían indicar un ataque o constituir una amenaza para sus sitios web y servicios web protegidos. Puede, por ejemplo, identificar una solicitud que intente realizar un determinado tipo de operación que podría infringir la seguridad, o una respuesta que incluya información privada confidencial, como un número de seguridad social o un número de tarjeta de crédito. Durante la configuración, especifique las comprobaciones de seguridad adecuadas para los servidores web y el contenido que necesita proteger. Los controles de seguridad son restrictivos. Muchos de ellos pueden bloquear solicitudes y respuestas legítimas si no agrega las excepciones apropiadas (relajaciones) al configurarlas. Identificar las excepciones necesarias no es difícil si utiliza la función de aprendizaje adaptativo, que observa el uso normal de su sitio web y crea excepciones recomendadas.

El Web App Firewall se puede instalar como un dispositivo de red de capa 3 o como un puente de red de capa 2 entre sus servidores y sus usuarios, generalmente detrás del enrutador o firewall de su empresa. Debe instalarse en una ubicación donde pueda interceptar el tráfico entre los servidores web que quiere proteger y el concentrador o conmutador a través del cual los usuarios acceden a esos servidores web. A continuación, configure la red para enviar solicitudes al Web App Firewall en lugar de directamente a los servidores web, y las respuestas al Web App Firewall en lugar de directamente a los usuarios. El Web App Firewall filtra ese tráfico antes de reenviarlo a su destino final, mediante tanto su conjunto de reglas internas como sus adiciones y modificaciones. Bloquea o hace inofensiva cualquier actividad que detecte como dañina y, a continuación, reenvía el tráfico restante al servidor web. La siguiente ilustración proporciona una descripción general del proceso de filtrado.

> **Nota:**
>
> La ilustración omite la aplicación de una directiva al tráfico entrante. Ilustra una configuración de seguridad en la que la directiva es procesar todas las solicitudes. Además, en esta configuración, se ha configurado y asociado un objeto de firmas con el perfil, y se han configurado comprobaciones de seguridad en el perfil.

Ilustración 1. Un diagrama de flujo de filtrado de Web App Firewall



Como se muestra en la ilustración, cuando un usuario solicita una dirección URL en un sitio web protegido, el Web App Firewall examina primero la solicitud para asegurarse de que no coincide con una firma. Si la solicitud coincide con una firma, Citrix Web Application Firewall muestra el objeto de error (una página web ubicada en el dispositivo Web App Firewall y que puede configurar mediante la función de importación) o reenvía la solicitud a la dirección URL de error designada (la página de error). Las firmas no requieren tantos recursos como las comprobaciones de seguridad, por lo que detectar y detener los ataques detectados por una firma antes de ejecutar cualquiera de las comprobaciones de seguridad reduce la carga en el servidor.

Si una solicitud pasa la inspección de firma, Web App Firewall aplica las comprobaciones de seguridad de solicitud que se han habilitado. Las comprobaciones de seguridad de la solicitud verifican que la solicitud es adecuada para su sitio web o servicio web y no contiene material que pueda representar una amenaza. Por ejemplo, las comprobaciones de seguridad examinan la solicitud de signos que indican que puede ser de un tipo inesperado, solicitar contenido inesperado o contener datos de for-

mularios web inesperados y posiblemente malintencionados, comandos SQL o scripts. Si la solicitud falla en una comprobación de seguridad, Web App Firewall desinfecta la solicitud y, a continuación, la envía al dispositivo Citrix ADC (o al dispositivo virtual Citrix ADC) o muestra el objeto de error. Si la solicitud supera las comprobaciones de seguridad, se envía de nuevo al dispositivo Citrix ADC, que completa cualquier otro procesamiento y reenvía la solicitud al servidor web protegido.

Cuando el sitio web o el servicio web envían una respuesta al usuario, el Web App Firewall aplica las comprobaciones de seguridad de respuesta que se han habilitado. Las comprobaciones de seguridad de respuesta examinan la respuesta en busca de fugas de información privada confidencial, signos de defacción del sitio web u otro contenido que no debe estar presente. Si la respuesta falla una comprobación de seguridad, Web App Firewall elimina el contenido que no debe estar presente o bloquea la respuesta. Si la respuesta pasa las comprobaciones de seguridad, se envía de nuevo al dispositivo Citrix ADC, que la reenvía al usuario.

Funciones de Citrix Web Application Firewall

Las funciones básicas de Web App Firewall son directivas, perfiles y firmas, que proporcionan un modelo de seguridad híbrido tal como se describe en Ataques web conocidos, Ataques web desconocidosy Cómo funciona Web App Firewall. Cabe destacar la función de aprendizaje, que observa el tráfico de las aplicaciones protegidas y recomienda los ajustes de configuración adecuados para determinadas comprobaciones de seguridad.

La función de importación administra los archivos que se cargan en Web App Firewall. A continuación, el Web App Firewall utiliza estos archivos en varias comprobaciones de seguridad o cuando responde a una conexión que coincide con una comprobación de seguridad.

Puede utilizar las funciones de registros, estadísticas e informes para evaluar el rendimiento del Web App Firewall e identificar posibles necesidades de más protecciones.

Cómo Citrix Web Application Firewall modifica el tráfico de aplicaciones

Citrix Web Application Firewall afecta al comportamiento de una aplicación web que protege al modificar lo siguiente:

- Cookies
- Encabezados de HTTP
- Formularios/Datos

Cookie de sesión de Citrix Web Application Firewall

Para mantener el estado de la sesión, Citrix ADC Web App Firewall genera su propia cookie de sesión. Esta cookie se transfiere únicamente entre el explorador web y el Firewall de aplicaciones web de

Citrix ADC y no al servidor web. Si algún pirata informático intenta modificar la cookie de sesión, Application Firewall descarta la cookie antes de reenviar la solicitud al servidor y trata la solicitud como una nueva sesión de usuario. La cookie de sesión está presente mientras el explorador web esté abierto. Cuando se cierra el explorador web, la cookie de sesión de Application Firewall pasa a ser válida. El estado de la sesión mantiene la información de las URL y formularios visitados por el cliente.

La cookie de sesión configurable de Web App Firewall es`citrix_ns_id`.

A partir de la compilación 12.1 54 y 13.0 de Citrix ADC, la consistencia de las cookies no tiene sesión y no impone la adición de cookies de sesión `citrix_ns_id` generada por el dispositivo.

Cookies de Citrix Web App Firewall

Muchas aplicaciones web generan cookies para realizar un seguimiento de la información específica del usuario o de la sesión. Esta información puede ser preferencias del usuario o artículos del carrito de compras. Una cookie de aplicación web puede ser uno de los dos tipos siguientes:

- **Cookies persistentes**: Estas cookies se almacenan localmente en el equipo y se utilizan de nuevo la próxima vez que visite el sitio. Este tipo de cookie generalmente contiene información sobre el usuario, como inicio de sesión, contraseña o preferencias.
- **Cookies de sesión o transitorias** - Estas cookies se utilizan solo durante la sesión y se destruyen después de que finalice la sesión. Este tipo de cookie contiene información sobre el estado de la aplicación, como elementos del carrito de compras o credenciales de sesión.

Los hackers pueden intentar modificar o robar cookies de aplicaciones para secuestrar una sesión de usuario o hacerse pasar por un usuario. El Firewall de aplicaciones evita tales intentos con la ayuda del hash de las cookies de aplicación y al agregar más cookies con las firmas digitales. Mediante el seguimiento de las cookies, Application Firewall garantiza que las cookies no se modifiquen o comprometan entre el explorador del cliente y el Application Firewall. El firewall de aplicaciones no modifica las cookies de la aplicación.

Citrix Web Application Firewall genera las siguientes cookies predeterminadas para realizar un seguimiento de las cookies de la aplicación:

- **Cookies persistentes**:`citrix_ns_id_wlf`. Nota: Wlf significa que vivirá para siempre.
- **Cookies de sesión o transitorias**:`citrix_ns_id_wat`. Nota: Wat significa actuará de forma transitoria.
  Para realizar un seguimiento de las cookies de aplicación, Application Firewall agrupa las cookies de aplicación persistentes o de sesión juntas y, a continuación, hash y firmar todas las cookies juntas. Por lo tanto, Application Firewall genera una`wlf` cookie para rastrear todas las cookies de aplicación persistentes y una`wat` cookie para rastrear todas las cookies de sesión de aplicaciones.

La siguiente tabla muestra el número y los tipos de cookies generadas por el Firewall de aplicaciones en función de las cookies generadas por la aplicación web:

Antes de Citrix ADC Web App Firewall	Para
Una cookie persistente	Cookie persistente: `citix_ns_id_wlf`
Una cookie transitoria	Cookie transitoria: `citix_ns_id_wat`
Múltiples cookies persistentes, múltiples cookies transitorias	Una cookie persistente: `citrix_ns_id_wlf`, una cookie transitoria: `citix_ns_id_wat`

Citrix Web App Firewall permite cifrar la cookie de la aplicación. Application Firewall también proporciona una opción para proxy de la cookie de sesión enviada por la aplicación, almacenándola con el resto de los datos de sesión de Application Firewall y no enviándola al cliente. Cuando un cliente envía una solicitud a la aplicación que incluye una cookie de sesión de Application Firewall, Application Firewall inserta la cookie enviada de nuevo en la solicitud antes de enviar la solicitud a la aplicación de origen. Application Firewall también permite agregar las banderas HttpOnly y/o Secure a las cookies.

Cómo afecta el firewall de la aplicación a los encabezados HTTP

Tanto las solicitudes HTTPS como las respuestas HTTPS utilizan encabezados para enviar información sobre uno o más mensajes de HTTPs. Un encabezado es una serie de líneas con cada línea que contiene un nombre seguido de dos puntos y un espacio, y un valor. Por ejemplo, el encabezado Host tiene el siguiente formato:

```
Host: www.citrix.com
```

Algunos campos de encabezado se utilizan tanto en los encabezados de solicitud como en los encabezados de respuesta, mientras que otros son apropiados solo para una solicitud o una respuesta. El Firewall de aplicaciones puede agregar, modificar o eliminar algunos encabezados en una o más solicitudes o respuestas HTTPS para mantener la seguridad de la aplicación.

Encabezados de solicitud eliminados por Citrix Web Application Firewall

Muchos de los encabezados de solicitud relacionados con el almacenamiento en caché se eliminan para ver cada solicitud dentro del contexto de una sesión. Del mismo modo, si la solicitud incluye un encabezado de codificación para permitir que el servidor web envíe respuestas comprimidas, el Firewall de aplicaciones elimina este encabezado para que el Web App Firewall inspeccione el contenido de la respuesta del servidor no comprimido para evitar cualquier fuga de datos confidenciales al cliente.

Application Firewall elimina los siguientes encabezados de solicitud:

- Rango: Se utiliza para recuperarse de transferencias parciales o fallidas de archivos.
- If-Range: Permite a un cliente recuperar un objeto parcial cuando ya contiene una parte de ese objeto en su caché (GET condicional).
- If-Modified-Since: Si el objeto solicitado no se modifica desde el tiempo especificado en este campo, no se devuelve una entidad desde el servidor. Obtiene un error HTTP 304 no modificado.
- If-None-Match: Permite actualizaciones eficientes de la información almacenada en caché con una cantidad mínima de sobrecarga.
- Accept-Encoding: Qué métodos de codificación están permitidos para un objeto concreto, como gzip.

Encabezado de solicitud modificado por Citrix Web Application Firewall

Si un explorador web utiliza los protocolos HTTP/1.0 o anteriores, el explorador abre y cierra continuamente la conexión de socket TCP después de recibir cada respuesta. Esto agrega sobrecarga al servidor web e impide mantener el estado de la sesión. El protocolo HTTP/1.1 permite que la conexión permanezca abierta durante la sesión. Application Firewall modifica el siguiente encabezado de solicitud para utilizar HTTP/1.1 entre Application Firewall y el servidor web, independientemente del protocolo utilizado por el explorador web:
Connection: Keep-alive

Encabezados de solicitud agregados por Citrix Web Application Firewall

Application Firewall actúa como un proxy inverso y reemplaza la dirección IP de origen original de la sesión por la dirección IP del Application Firewall. Por lo tanto, todas las solicitudes registradas en el registro del servidor web indican que las solicitudes se envían desde el Firewall de aplicaciones.

Encabezado de respuesta eliminado por Citrix Web Application Firewall

El firewall de aplicaciones puede bloquear o modificar contenido, como eliminar números de tarjetas de crédito o eliminar comentarios, lo que puede dar lugar a una discordancia de tamaño. Para evitar tal caso, Application Firewall descarta el siguiente encabezado:

Content-Length: Indica el tamaño del mensaje enviado al destinatario.
Encabezados de respuesta modificados por el firewall de aplicaciones

Muchos de los encabezados de respuesta modificados por Application Firewall están relacionados con el almacenamiento en caché. Los encabezados de almacenamiento en caché en las respuestas HTTP (S) deben modificarse para forzar al explorador web a enviar siempre una solicitud al servidor web para obtener los datos más recientes y no utilizar la caché local. Sin embargo, algunas aplicaciones ASP utilizan complementos independientes para mostrar contenido dinámico y pueden requerir la capacidad de almacenar en caché los datos temporalmente en el explorador. Para permitir

el almacenamiento en caché temporal de datos cuando se habilitan protecciones de seguridad avanzada, como FFC, cierre de URL o comprobaciones CSRF, Application Firewall agrega o modifica los encabezados de control de caché en la respuesta del servidor mediante la siguiente lógica:

- Si el servidor envía Pragma: sin caché, entonces Application Firewall no realiza ninguna modificación.
- Si Solicitud de cliente es HTTP 1.0, el Firewall de aplicaciones inserta Pragma: no-cache.
- Si Solicitud de cliente es HTTP 1.1 y tiene Caché Control: No-store, entonces Application Firewall no realiza ninguna modificación.
- Si Solicitud de cliente es HTTP 1.1 y Respuesta del servidor tiene encabezado Cache-Control sin almacén o sin directiva de caché, entonces Application Firewall no realiza ninguna modificación.
- Si la solicitud de cliente es HTTP 1.1 y la respuesta del servidor no tiene encabezado de control de caché o el encabezado Cache-Control no tiene ninguna directiva de almacén o no-caché, el firewall de aplicación completa las siguientes tareas:

1. Inserta cache-control: Max-age=3, debe revalidar, privado.
2. Inserta X-cache-control-ORIG = valor original del encabezado Cache-Control.
3. Elimina el encabezado Last-Modified.
4. Sustituye a Etag.
5. Inserta X-Expires-Orig=Valor original del encabezado de caducidad enviado por el servidor.
6. Modifica el encabezado de caducidad y establece la fecha de caducidad de la página web en el pasado, de modo que siempre se recoja de nuevo.
7. Modifica Accept-Ranges y lo establece en ninguno.

Para reemplazar los datos almacenados temporalmente en caché en el explorador del cliente cuando Application Firewall cambia la respuesta como, por ejemplo, para StripComments, X-out/Remove SafeObject, xout o quitar tarjeta de crédito o transformación de URL, Application Firewall realiza las siguientes acciones:

1. Elimina Last-Modified del servidor antes de reenviarlo al cliente.
2. Reemplaza a Etag por un valor determinado por Application Firewall.

Encabezados de respuesta agregados por Citrix Web App Firewall

- `Transfer-Encoding`: En trozos. Este encabezado transmite información a un cliente sin tener que conocer la longitud total de la respuesta antes de enviar la respuesta. Este encabezado es obligatorio porque se elimina el encabezado de longitud de contenido.
- `Set-Cookie`: Las cookies agregadas por el firewall de aplicaciones.
- `Xet-Cookie`: si la sesión es válida y si la respuesta no ha caducado en caché, puede servir desde caché y no es necesario enviar una nueva cookie porque la sesión sigue siendo válida. En

tal caso, el Set-Cookie se cambia a Xet-Cookie. Para el explorador web.

Cómo se ven afectados los datos del formulario

El firewall de aplicaciones protege contra ataques que intentan modificar el contenido del formulario original enviado por el servidor. También puede proteger contra ataques de falsificación de solicitudes entre sitios. El Firewall de aplicaciones se logra insertando la etiqueta de formulario oculta as_fid en la página.

Ejemplo:<input type=”hidden”name=”as_fid”value=”VRgWq0I196Jmg/+LOY7C”/>

El campo oculto as_fid se utiliza para la consistencia del campo. Application Firewall utiliza este campo para realizar un seguimiento de todos los campos del formulario, incluidos los pares de nombre/valor de campo oculto y para garantizar que ninguno de los campos del formulario enviado por el servidor se cambie en el lado del cliente. La comprobación CSRF también utiliza esta etiqueta de formulario única as_fid para asegurarse de que los formularios enviados por el usuario fueron servidos al usuario en esta sesión y ningún pirata informático está intentando secuestrar la sesión del usuario.

Comprobación de formularios sin sesión

Application Firewall también ofrece una opción para proteger los datos del formulario mediante la consistencia de campos sin sesión. Esto resulta útil para aplicaciones en las que los formularios pueden tener un gran número de campos ocultos dinámicos que conducen a una asignación alta de memoria por sesión por parte del firewall de aplicaciones. La comprobación de consistencia de campos sin sesión se logra insertando otro campo oculto as_ffc_field solo para solicitudes POST o para solicitudes GET y POST en función de la configuración configurada. El firewall de aplicaciones cambia el método GET a POST cuando reenvía el formulario al cliente. A continuación, el dispositivo revierte el método a GET al enviarlo de vuelta al servidor. El valor as_ffc_field puede ser grande porque contiene el resumen cifrado del formulario que se sirve. El siguiente es un ejemplo de la comprobación de formulario sin sesión:

```
1 <input type=”hidden” name=”as_ffc_field” value=”CwAAAAVIGLD/
     luRRi1Wu1rbYrFYargEDcO5xVAxsEnMP1megXuQfiDTGbwk0fpgndMHqfMbzfAFdjwR+
     TOm1oT
2 +u+Svo9+NuloPhtnbkxGtNe7gB/o8GlxEcK9ZkIIVv3oIL/
     nIPSRWJljgpWgafzVx7wtugNwnn8/
     GdnhneLCJTaYU7ScnC6LexJDLisI1xsEeONWt8Zm
3 +vJTa3mTebDY6LVyhDpDQfBgI1XLgfLTexAUzSNWHYyloqPruGYfnRPw+
     DIGf6gGwn1BYLEsRHKNbjJBrKpOJo9JzhEqdtZ1g3bMzEF9PocPvM1Hpvi5T6VB
4 /YFunUFM4f+bD7EAVcugdhovzb71CsSQX5+qcC1B8WjQ==” />
5 <!--NeedCopy-->
```


Despojado de comentarios HTML

Application Firewall también ofrece la opción de quitar todos los comentarios HTML en las respuestas antes de enviarlos al cliente. Esto afecta no solo a los formularios, sino a todas las páginas de respuesta. Application Firewall localiza y elimina cualquier texto incrustado entre "<!-" y "->" etiquetas de comentario. Las etiquetas permanecen para indicar que existía un comentario en esa ubicación del código fuente HTML. Cualquier texto incrustado en cualquier otra etiqueta HTML o JavaScript se ignora.
Es posible que algunas aplicaciones no funcionen correctamente si tienen JavaScript incorrectamente incrustado en las etiquetas de comentario. Una comparación del código fuente de la página antes y después de que Application Firewall eliminara los comentarios puede ayudar a identificar si alguno de los comentarios eliminados tenía el JavaScript requerido incrustado en ellos.

Protección de tarjetas de crédito

El Firewall de aplicaciones ofrece una opción para inspeccionar los encabezados y el cuerpo de la respuesta y elimina o elimina los números de la tarjeta de crédito antes de reenviar la respuesta al cliente. Actualmente Application Firewall ofrece protección para las siguientes tarjetas de crédito principales: American Express, Diners Club, Discover, JCB, MasterCard y Visa. La acción de salida x funciona independientemente de la acción Bloquear.

Protección segura de objetos

Al igual que los números de tarjetas de crédito, también se puede evitar la fuga de otros datos confidenciales mediante la comprobación de seguridad de Application Firewall Safe Object para eliminar o eliminar el contenido confidencial de la respuesta.

La acción de scripts entre sitios transforma

Cuando la transformación está habilitada para scripts entre sitios, Web App Firewall cambia `"<"into "%26lt;"and ">"into "%26gt;"` en las solicitudes. Si la configuración CheckRequestTheaders en el Web App Firewall está habilitada, el Web App Firewall inspecciona los encabezados de solicitud y transforma estos caracteres en Encabezado y cookies también. La acción de transformación no bloquea ni transforma los valores enviados originalmente por el servidor. Hay un conjunto de atributos y etiquetas predeterminados para scripts entre sitios que permite Web App Firewall. También se proporciona una lista predeterminada de patrones de scripts entre sitios denegados. Estos se pueden personalizar seleccionando el objeto de firmas y haciendo clic en el cuadro de **diálogo Administrar patrones de scripting SQL/Cross Site** en la GUI.

Transformación de caracteres especiales SQL

Application Firewall tiene las siguientes reglas de transformación predeterminadas para caracteres especiales de SQL:

De	Para	Transformación
‘(comillas simples, es decir, %27)	”	Otra cita sencilla
\ (barra invertida que es%5C)	|Se agregó otra barra invertida	
; (punto y coma que es%3B)		Se cayó

Cuando la transformación de caracteres especiales está habilitada y CheckRequestTheaders se establece en ON, entonces la transformación de caracteres especiales ocurre en Encabezados y cookies también.
Nota: Algunos encabezados de solicitud como User-Agent, Accept-Encoding generalmente contienen punto y coma y pueden verse afectados por la transformación SQL.

Comportamiento de Citrix Web Application Firewall en el que corrompe el encabezado ESPERE

1. Siempre que NetScaler recibe una solicitud HTTP con el encabezado EXPECT en ella, NetScaler envía la respuesta EXPECT: 100 -continue al cliente en nombre del servidor back-end.
2. Este comportamiento se debe a que las protecciones de Application Firewall deben ejecutarse en toda la solicitud antes de reenviar la solicitud al servidor, NetScaler debe obtener la solicitud completa del cliente.
3. Al recibir una `100 continue` respuesta, el cliente envía la parte restante de la solicitud que completa la solicitud.
4. NetScaler ejecuta todas las protecciones y, a continuación, reenvía la solicitud al servidor.
5. Ahora, como NetScaler está reenviando la solicitud completa, el encabezado EXPECT que vino en la solicitud inicial se vuelve obsoleto, como resultado NetScaler corrompe este encabezado y lo envía al servidor.
6. El servidor al recibir la solicitud ignora cualquier encabezado que esté dañado.

Configuración del Web App Firewall

July 8, 2022

Puede configurar Citrix Web App Firewall (Web App Firewall) mediante cualquiera de los métodos siguientes:

- **Asistente para Web App Firewall.** Un cuadro de diálogo que consta de una serie de pantallas que le guían a través del proceso de configuración.
- **Plantilla de AppExpert de Citrix Web Interface.** Plantilla de AppExpert (un conjunto de opciones de configuración) diseñada para proporcionar la protección adecuada a los sitios web. Esta plantilla de AppExpert contiene las opciones de configuración de Web App Firewall adecuadas para proteger muchos sitios web.
- **GUI de Citrix ADC.** La interfaz de configuración basada en web.
- **Interfaz de línea de comandos de Citrix ADC.** Interfaz de configuración de línea de comandos.

Citrix recomienda utilizar el Asistente para Web App Firewall. La mayoría de los usuarios encontrarán que es el método más fácil para configurar Web App Firewall, y está diseñado para evitar errores. Si tiene un nuevo Citrix ADC o VPX que utilizará principalmente para proteger sitios web, puede que la plantilla AppExpert de Interfaz Web sea una mejor opción, ya que proporciona una buena configuración predeterminada, no solo para Web App Firewall, sino para todo el dispositivo. Tanto la GUI como la interfaz de línea de comandos están pensados para usuarios experimentados, principalmente para modificar una configuración existente o utilizar opciones avanzadas.

Asistente para Web App Firewall

El Asistente para Web App Firewall es un cuadro de diálogo que consta de varias pantallas que le piden que configure cada parte de una configuración simple. A continuación, el Web App Firewall crea los elementos de configuración adecuados a partir de la información que le proporciona. Esta es la forma más simple y, para la mayoría de los propósitos, la mejor manera de configurar el Web App Firewall.

Para utilizar el asistente, conéctese a la GUI con el explorador de su elección. Cuando se establezca la conexión, compruebe que el Web App Firewall está habilitado y, a continuación, ejecute el Asistente para Web App Firewall, que le pedirá información de configuración. No es necesario que proporcione toda la información solicitada la primera vez que utilice el asistente. En su lugar, puede aceptar la configuración predeterminada, realizar algunas tareas de configuración relativamente sencillas para habilitar funciones importantes y, a continuación, permitir que el Web App Firewall recopile información importante para ayudarle a completar la configuración.

Por ejemplo, cuando el asistente le pide que especifique una regla para seleccionar el tráfico que se va a procesar, puede aceptar el valor predeterminado, que selecciona todo el tráfico. Cuando le presente una lista de firmas, puede habilitar las categorías de firmas adecuadas y activar la recopilación de estadísticas para esas firmas. Para esta configuración inicial, puede omitir las protecciones avanzadas (comprobaciones de seguridad). El asistente crea automáticamente la directiva, el objeto de firmas y el perfil adecuados (colectivamente, la configuración de seguridad) y vincula la directiva a global. A continuación, el Web App Firewall comienza a filtrar las conexiones a los sitios web protegidos, registrando las conexiones que coincidan con una o varias de las firmas habilitadas y recopilando estadísticas sobre las conexiones con las que coincide cada firma. Después de que el Web App Firewall procese parte del tráfico, puede volver a ejecutar el asistente y examinar los registros y las estadísticas

para ver si alguna de las firmas que ha habilitado coincide con el tráfico legítimo. Después de determinar qué firmas están identificando el tráfico que quiere bloquear, puede habilitar el bloqueo para esas firmas. Si su sitio web o servicio web no es complejo, no utiliza SQL y no tiene acceso a información privada confidencial, esta configuración de seguridad básica probablemente proporcionará una protección adecuada.

Es posible que necesite protección adicional si, por ejemplo, su sitio web es dinámico. El contenido que utiliza scripts puede necesitar protección contra ataques de scripts entre sitios. El contenido web que utiliza SQL, como carritos de compra, muchos blogs y la mayoría de los sistemas de administración de contenido, puede necesitar protección contra ataques de inyección SQL. Los sitios web y los servicios web que recopilan información privada confidencial, como números de seguridad social o números de tarjetas de crédito, pueden requerir protección contra la exposición involuntaria de dicha información. Ciertos tipos de software de servidor web o servidor XML pueden requerir protección contra tipos de ataques adaptados a ese software. Otra consideración es que elementos específicos de sus sitios web o servicios web pueden requerir una protección diferente a la de otros elementos. El examen de los registros y las estadísticas de Web App Firewall puede ayudarle a identificar las protecciones adicionales que puede necesitar.

Después de decidir qué protecciones avanzadas se necesitan para los sitios web y los servicios web, puede volver a ejecutar el asistente para configurar esas protecciones. Algunas comprobaciones de seguridad requieren que se introduzcan excepciones (relajación) para evitar que la comprobación bloquee el tráfico legítimo. Puede hacerlo manualmente, pero generalmente es más fácil habilitar la función de aprendizaje adaptativo y permitirle recomendar la relajación necesaria. Puede utilizar el asistente tantas veces como sea necesario para mejorar la configuración de seguridad básica y/o crear configuraciones de seguridad adicionales.

El asistente automatiza algunas tareas que tendría que realizar manualmente si no lo utiliza. Crea automáticamente una directiva, un objeto de firmas y un perfil, y les asigna el nombre que proporcionó cuando se le pidió el nombre de la configuración. El asistente también agrega la configuración de protección avanzada al perfil, vincula el objeto de firmas al perfil, asocia el perfil a la directiva y la aplica vinculándolo a Global.

No se pueden realizar algunas tareas en el asistente. No se puede utilizar el asistente para enlazar una directiva a un punto de enlace distinto de Global. Si quiere que el perfil se aplique solo a una parte específica de la configuración, debe configurar manualmente el enlace. No puede configurar los parámetros del motor ni algunas otras opciones de configuración global en el asistente. Aunque puede configurar cualquiera de las opciones de protección avanzadas en el asistente, si quiere modificar una configuración específica en una única comprobación de seguridad, puede ser más fácil hacerlo en las pantallas de configuración manual de la GUI.

Para obtener más información sobre el uso del Asistente para Web App Firewall, consulte Asistente para Web App Firewall.

La plantilla de AppExpert de Citrix Web Interface

Las plantillas AppExpert son un enfoque diferente y más sencillo para configurar y administrar aplicaciones empresariales complejas. La pantalla de AppExpert en la GUI consta de una tabla. Las aplicaciones se enumeran en la columna situada más a la izquierda, y las funciones de Citrix ADC aplicables a esa aplicación aparecen cada una en su propia columna a la derecha. (En la interfaz de AppExpert, las funciones asociadas a una aplicación se denominan *unidades de aplicación*). En la interfaz de AppExpert, configura el tráfico interesante para cada aplicación y activa las reglas de compresión, almacenamiento en caché, reescritura, filtrado, respuesta y Web App Firewall, en lugar de tener que configurar cada función individualmente.

La plantilla AppExpert de interfaz web contiene reglas para las siguientes firmas de Web App Firewall y comprobaciones de seguridad:

- **Denegar la comprobación de URL.** Detecta conexiones con contenido que se sabe que representa un riesgo para la seguridad o con cualquier otra URL que designe.
- **Comprobación de desbordamiento de búfer.** Detecta los intentos de provocar un desbordamiento de búfer en un servidor web protegido.
- **Comprobación de coherencia de cookies.** Detecta modificaciones maliciosas en las cookies establecidas por un sitio web protegido.
- **Comprobación de coherencia de campos de formulario.** Detecta modificaciones en la estructura de un formulario web en un sitio web protegido.
- **Comprobación de etiquetado de formularios CSRF.** Detecta ataques de falsificación de solicitudes entre sitios.
- **Comprobación Formatos de campo.** Detecta información inapropiada cargada en formularios web en un sitio web protegido.
- **Comprobación de inyección HTML SQL.** Detecta intentos de inyectar código SQL no autorizado.
- **Comprobación de scripts HTML entre sitios.** Detecta ataques de scripts entre sitios.

Para obtener información sobre la instalación y el uso de una plantilla de AppExpert, consulte Aplicaciones y plantillas de AppExpert.

La GUI de Citrix

La GUI es una interfaz basada en web que proporciona acceso a todas las opciones de configuración para la función Web App Firewall, incluidas las opciones avanzadas de configuración y administración que no están disponibles desde ninguna otra herramienta de configuración o interfaz. Específicamente, muchas opciones avanzadas de Firmas solo se pueden configurar en la GUI. Solo puede revisar las recomendaciones generadas por la función de aprendizaje en la GUI. Puede enlazar directivas a un punto de enlace distinto de Global solo en la GUI.

Para obtener una descripción de la GUI, consulte Interfaces de configuración de Web App Firewall.

Para obtener más información sobre el uso de la GUI para configurar Web App Firewall, consulte Configuración manual mediante la GUI.

Para obtener instrucciones sobre cómo configurar Web App Firewall mediante la GUI, consulte Configuración manual mediante la GUI. Para obtener información sobre la GUI de citrix-adc, consulte Interfaces de configuración de Web App Firewall.

La interfaz de línea de comandos de Citrix ADC

La interfaz de línea de comandos Citrix ADC es un shell UNIX modificado basado en el shell bash de FreeBSD. Para configurar Web App Firewall desde la interfaz de línea de comandos, escriba comandos en el símbolo del sistema y presione la tecla Intro, tal como lo hace con cualquier otro shell Unix. Puede configurar la mayoría de los parámetros y opciones para Web App Firewall mediante la línea de comandos de NetScaler. Las excepciones son la función de firmas, muchas de cuyas opciones solo se pueden configurar mediante la interfaz gráfica de usuario o el asistente de Web App Firewall, y la función de aprendizaje, cuyas recomendaciones solo se pueden revisar en la interfaz de usuario.

Para obtener instrucciones sobre cómo configurar Web App Firewall mediante la línea de comandos de Citrix ADC, consulte Configuración manual mediante la interfaz de línea de comandos.

Habilitar Citrix Web App Firewall

January 12, 2021

Para poder crear una configuración de seguridad, debe habilitar la función Citrix Web App Firewall en el dispositivo.

Puntos que tener en cuenta

- Si está configurando un dispositivo Citrix Web App Firewall dedicado o actualizando un dispositivo existente, la función ya está habilitada. No es necesario realizar ninguno de los procedimientos descritos aquí.
- Si tiene un nuevo Citrix ADC o VPX, debe habilitar la función Citrix Web App Firewall antes de configurarla.
- Si está actualizando un dispositivo Citrix ADC o VPX desde una versión anterior, primero debe habilitar la función Citrix Web App Firewall antes de configurarla.

> **Nota:**
>
> Si va a actualizar un dispositivo Citrix ADC o VPX desde una versión anterior, es posible que tenga que actualizar las licencias del dispositivo antes de habilitar Citrix Web App Firewall. Consulte

> con su representante o distribuidor de Citrix para obtener la licencia correcta.

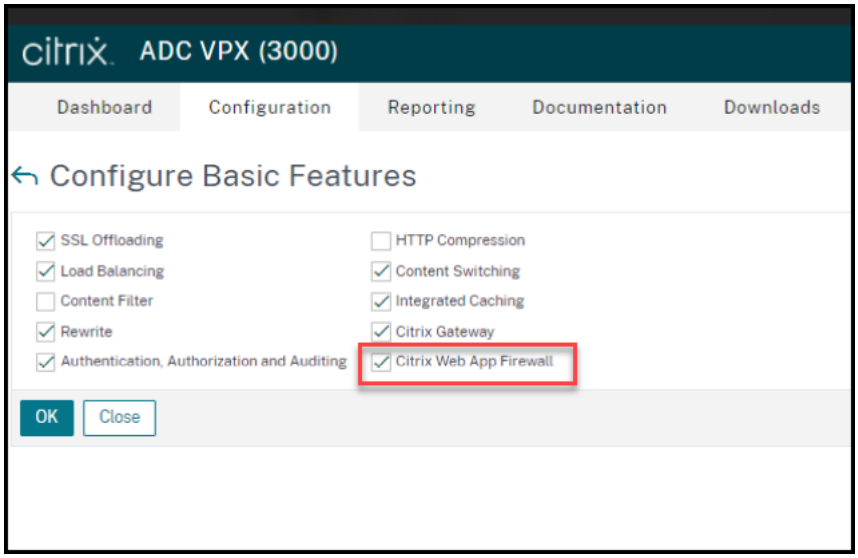
Habilitar Citrix Web App Firewall mediante la interfaz de comandos

En el símbolo del sistema, escriba el siguiente comando:

```
enable ns feature AppFW
```

Habilitar el Web App Firewall mediante la GUI

1. Vaya a **Sistema** > **Configuración**.
2. En el panel de detalles, haga clic en **Configurar funciones avanzadas**.
3. En la página **Configurar funciones avanzadas**, seleccione **Citrix Web App Firewall**.
4. Haga clic en **Aceptar**.



Asistente para Web App Firewall

August 20, 2021

A diferencia de la mayoría de los asistentes, Citrix Web App Firewall Wizard está diseñado no solo para simplificar el proceso de configuración inicial, sino también para modificar las configuraciones creadas anteriormente y mantener la configuración de Web App Firewall. Un usuario típico ejecuta el asistente varias veces, omitiendo algunas de las pantallas cada vez.

El Asistente para Web App Firewall crea automáticamente perfiles, directivas y firmas.

Abrir el asistente

Para ejecutar el Asistente para Web App Firewall, abra la GUI y siga estos pasos:

1. Vaya a **Seguridad** > **Firewall de aplicaciones**.
2. En el panel de detalles, en **Introducción**, haga clic en **Asistente para firewall de aplicaciones**. Se abrirá el asistente.

Para obtener más información sobre la GUI, consulte "Interfaces de configuración de Web App Firewall. "

Pantallas del asistente

El Asistente para Web App Firewall muestra las siguientes pantallas en una página tabular:

1. Especificar nombre: en esta pantalla, al crear una nueva configuración de seguridad, especifique un nombre significativo y el tipo apropiado (HTML, XML o WEB 2.0) para su perfil. La directiva y las firmas predeterminadas se generan automáticamente mediante el mismo nombre.

Nombre de perfil

El nombre puede comenzar con una letra, un número o un símbolo de subrayado, y puede constar de 1 a 31 letras, números y los símbolos de guión (-), punto (.) libra (#), espacio (), en (@), igual (=), dos puntos (:) y guión bajo (_). Elija un nombre que le resulte más fácil a los demás saber qué contenido protege su nueva configuración de seguridad.

> **Nota:**
>
> Dado que el asistente utiliza este nombre tanto para la directiva como para el perfil, está limitado a 31 caracteres. Las directivas creadas manualmente pueden tener nombres de hasta 127 caracteres de longitud.

Al modificar una configuración existente, seleccione Modificar configuración existente y, a continuación, en la lista desplegable Nombre, seleccione el nombre de la configuración existente que quiere modificar.

> **Nota:**
>
> Solo las directivas enlazadas a global o a un punto de enlace aparecen en esta lista; no se puede modificar una directiva independiente mediante el asistente Firewall de aplicaciones. Debe vincularlo manualmente a Global o a un punto de enlace, o modificarlo manualmente. (Para modificar manualmente, en la GUI) **Application Firewall** > **Directivas** > Panel **Firewall**, seleccione la directiva y haga clic en **Abrir**.

Tipo de perfil

También puede seleccionar un tipo de perfil en esta pantalla. El tipo de perfil determina los tipos de protección avanzada (comprobaciones de seguridad) que se pueden configurar. Debido a que ciertos

tipos de contenido no son vulnerables a ciertos tipos de amenazas de seguridad, restringir la lista de comprobaciones disponibles ahorra tiempo durante la configuración. Los tipos de perfiles de Web App Firewall son:

- Aplicación web (HTML). Cualquier sitio web basado en HTML que no utilice tecnologías XML o Web 2.0.
- Aplicación XML (XML, SOAP). Cualquier servicio web basado en XML.
- Aplicación web 2.0 (HTML, XML, REST). Cualquier sitio web 2.0 que combine contenido basado en HTML y XML, como un sitio basado en ATOM, un blog, una fuente RSS o una wiki.

Nota: Si no está seguro del tipo de contenido que se utiliza en su sitio web, puede elegir Aplicación web 2.0 para asegurarse de proteger todos los tipos de contenido de aplicaciones web.

2. Especificar regla: en esta pantalla, se especifica la regla de directiva (expresión) que define el tráfico que examina la configuración actual. Si crea una configuración inicial para proteger sus sitios web y servicios web, puede aceptar el valor predeterminado, **true**, que selecciona todo el tráfico web.

Si quiere que esta configuración de seguridad examine, no todo el tráfico HTTP que se enruta a través del dispositivo, sino el tráfico específico, puede escribir una regla de directiva que especifique el tráfico que quiere que examine. Las reglas se escriben en el lenguaje de expresiones Citrix ADC, que es un lenguaje de programación totalmente funcional orientado a objetos.

Nota: Además de la sintaxis de expresiones predeterminada, para obtener compatibilidad con versiones anteriores, el sistema operativo Citrix ADC admite la sintaxis de expresiones clásicas de Citrix ADC en dispositivos y dispositivos virtuales Citrix ADC Classic y nCore. Las expresiones clásicas no se admiten en los dispositivos Citrix ADC Cluster ni en los dispositivos virtuales. Los usuarios actuales que quieran migrar sus configuraciones existentes al clúster de Citrix ADC deben migrar las directivas que contengan expresiones clásicas a la sintaxis de expresiones predeterminadas.

- Para obtener una descripción sencilla del uso de la sintaxis de expresiones Citrix ADC para crear reglas de Web App Firewall y una lista de reglas útiles, consulte Directivas del firewall.
- Para obtener una explicación detallada de cómo crear reglas de directiva en la sintaxis de expresiones Citrix ADC, consulte Directivas y expresiones.

4. Seleccionar firmas: en esta pantalla, selecciona las categorías de firmas que quiere utilizar para proteger sus sitios web y servicios web.

Este paso no es obligatorio y puede omitirlo si lo quiere e ir a la pantalla **Especificar protecciones profundas**. Si se omite la pantalla Seleccionar firmas, solo se crean un perfil y directivas asociadas y no se crean las firmas.

Puede seleccionar **Crear nueva firma** o **Seleccionar firma existente**.

Si está creando una nueva configuración de seguridad, las categorías de firmas seleccionadas están habilitadas y, de forma predeterminada, se registran en un nuevo objeto de firmas. Al nuevo objeto

de firmas se le asigna el mismo nombre que el especificado en la pantalla Especificar nombre que el nombre de la configuración de seguridad.

Si ha configurado anteriormente objetos de firmas y quiere utilizar uno de ellos como objeto de firmas asociado a la configuración de seguridad que está creando, haga clic en **Seleccionar firma existente** y seleccione un objeto de firmas de la lista Firmas.

Si está modificando una configuración de seguridad existente, puede hacer clic en Seleccionar firma existente y asignar un objeto de firmas diferente a la configuración de seguridad.

Si hace clic en Crear nueva firma, puede elegir el modo de edición como **Simple** o **Avanzado**.

1. **Especificar protecciones de firma (modo simple)**

El modo simple permite una fácil configuración de la firma, con una lista preestablecida de definiciones de protección para aplicaciones comunes como IIS (Internet Information Server), PHP y ActiveX. Las categorías predeterminadas en el modo Simple son:

- CGI. Protección contra ataques a sitios web que utilizan scripts CGI en cualquier idioma, incluidos scripts PERL, scripts de shell Unix y scripts de Python.
- Fusión fría. Protección contra ataques a sitios web que utilizan la plataforma de desarrollo web de Adobe Systems® ColdFusion®.
- FrontPage. Protección contra ataques a sitios web que utilizan la plataforma de desarrollo web Microsoft® FrontPage®.
- PHP. Protección contra ataques a sitios web que utilizan el lenguaje de scripting de desarrollo web de código abierto de PHP.
- Del lado del cliente. Protección contra ataques a herramientas del lado del cliente utilizadas para acceder a los sitios web protegidos, como Microsoft Internet Explorer, Mozilla Firefox, el explorador Opera y Adobe Acrobat Reader.
- Microsoft IIS. Protección contra ataques a sitios web que ejecutan Microsoft Internet Information Server (IIS)
- Varios. Protección contra ataques a otras herramientas del lado del servidor, como servidores web y servidores de bases de datos.

En esta pantalla, seleccione las acciones asociadas a las categorías de firmas seleccionadas en la pantalla Seleccionar firmas. Las acciones que puede configurar son:

- Bloquear
- Registro
- Estadísticas

De forma predeterminada, las acciones Registro y Estadísticas están habilitadas, pero no la acción Bloquear. Para configurar acciones, haga clic en **Configuración**. Puede cambiar la configuración de acción de todas las categorías seleccionadas mediante la lista desplegable **Acción**.

1. **Especificar protecciones de firma (modo avanzado)**

El modo avanzado permite un control más granular sobre las definiciones de firmas y proporciona significativamente más información. Utilice el modo avanzado si quiere un control completo sobre la definición de la firma.

El contenido de esta pantalla es el mismo que el contenido del cuadro de diálogo Modificar objeto de firmas, tal y como se describe en Configuración o modificación de un objeto de firmas. En esta pantalla, puede configurar acciones haciendo clic en la lista desplegable **Acciones** o en el menú Acciones, que aparece como un círculo con tres puntos.

7. Especificar protecciones profundas: en esta pantalla, usted elige las protecciones avanzadas (también denominadas comprobaciones de seguridad o simplemente comprobaciones) que quiere utilizar para proteger sus sitios web y servicios web. Las comprobaciones disponibles dependen del tipo de perfil que haya elegido en la pantalla Especificar nombre. Todas las comprobaciones están disponibles para perfiles de aplicación web 2.0.

Para obtener más información, consulte Descripción general de las comprobaciones de seguridady consulte Comprobaciones avanzadas de protecciones de formularios.

Configure las acciones para las protecciones avanzadas que ha habilitado.Las acciones que puede configurar son:

- Bloque: Bloquea las conexiones que coinciden con la firma. Inhabilitado de forma predeterminada.
- Registro: Registra las conexiones que coinciden con la firma para un análisis posterior. Habilitado de forma predeterminada.
- Estadísticas: Mantiene estadísticas, para cada firma, que muestran cuántas conexiones coincide y proporcionan cierta otra información sobre los tipos de conexiones que se bloquearon. Inhabilitado de forma predeterminada.
- Aprender. Observe el tráfico a este sitio web o servicio web y utilice conexiones que violen repetidamente esta comprobación para generar excepciones recomendadas a la comprobación, o nuevas reglas para la comprobación. Disponible solo para algunos cheques. Para obtener más información sobre la función de aprendizaje, consulte Configuración y uso de la funciónde aprendizaje y cómo funciona el aprendizaje y cómo configurar excepciones (relajaciones) o implementar reglas aprendidas para una comprobación, consulte Configuración manual mediante la GUI.

Para configurar acciones, active la protección haciendo clic en la casilla de verificación y, a continuación, haga clic en **Configuración de acción** para seleccionar las acciones necesarias. Seleccione otros parámetros, si es necesario, y haga clic en **Aceptar** para cerrar la ventana Configuración de acción.

Para ver todos los registros de una comprobación específica, selecciónela y, a continuación, haga clic en **Registros** para mostrar el Visor de Syslog, tal y como se describe en Registros de Web App Firewall.

Si una comprobación de seguridad bloquea el acceso legítimo a su sitio web protegido o servicio web, puede crear e implementar una relajación para esa comprobación de seguridad seleccionando un registro que muestre el bloqueo no deseado y, a continuación, haga clic en **Implementar**.

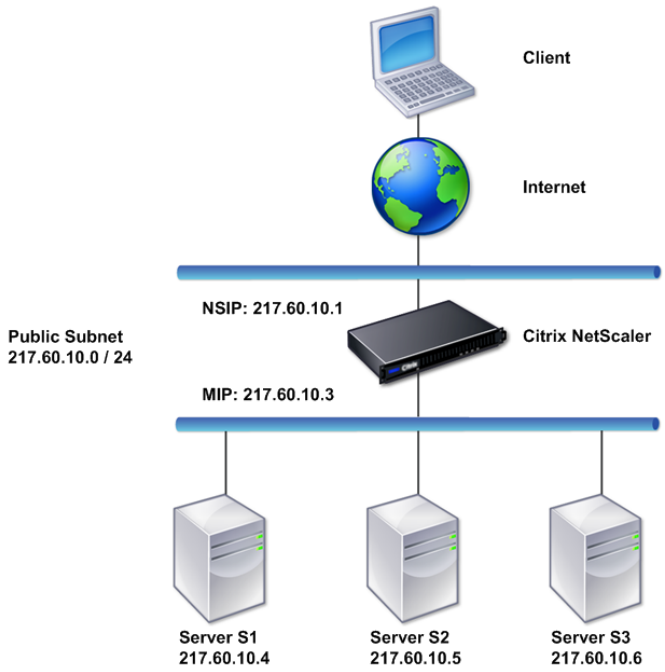
Después de completar la especificación de configuración de acción, haga clic en **Finalizar** para completar el asistente.

Los siguientes son cuatro procedimientos que muestran cómo realizar tipos específicos de configuración mediante el Asistente para Web App Firewall.

Crear una nueva configuración

Siga estos pasos para crear una nueva configuración de firewall y objetos de firma mediante el asistente Applicaiton Firewall.

1. Vaya a **Seguridad** > **Firewall de aplicaciones**.
2. En el panel de detalles, en **Introducción**, haga clic en Firewall de **aplicaciones. Se abrirá el asistente.



3. En la pantalla **Especificar nombre**, seleccione **Crear nueva configuración.
4. En el campo **Nombre**, escriba un nombre y, a continuación, haga clic en **Siguiente**.
5. En la pantalla **Especificar regla**, vuelva a hacer clic en **Siguiente** .

6. En la pantalla **Seleccionar firmas**, seleccione **Crear nueva firma** y **Simple** como modo de edición y, a continuación, haga clic en **Siguiente**.
7. En la pantalla **Especificar protecciones de firma**, configure los valores necesarios. Para obtener más información sobre qué firmas debe tener en cuenta para bloquear y cómo determinar cuándo puede habilitar de forma segura el bloqueo de una firma, consulte Firmas.
8. En la pantalla **Especificar protecciones profundas**, configure las acciones y los parámetros necesarios en **Configuración de acción**.
9. Cuando termine, haga clic en **Finalizar** para cerrar el asistente de Firewall de aplicaciones.

Modificar una configuración existente

Siga estos pasos para modificar una configuración existente y las categorías de firmas existentes.

1. Vaya a **Seguridad** > **Firewall de aplicaciones**.
2. En el panel de detalles, en **Introducción**, haga clic en **Asistente para firewall de aplicaciones**. Se abrirá el asistente.
3. En la pantalla **Especificar nombre**, seleccione Modificar configuración existente y, en la lista desplegable **Nombre**, elija la configuración de seguridad que creó durante la nueva configuración y, a continuación, haga clic en **Siguiente**.
4. En la pantalla **Especificar regla**, haga clic en Siguiente para mantener el valor predeterminado “true”. Si desea modificar la regla, siga los pasos descritos en Configurar una expresión de directiva personalizada.
5. En la pantalla **Seleccionar firmas**, haga clic en **Seleccionar firma existente**. En la lista desplegable **Firma existente**, seleccione la opción adecuada y, a continuación, haga clic en **Siguiente**. Aparecerá la pantalla de protección avanzada de firma.
   Nota: Si selecciona una firma existente, el modo de edición predeterminado para la firma protegida es avanzado.
6. En la pantalla Especificar protecciones de firma, configure los valores necesarios y haga clic en **Siguiente**. Para obtener más información sobre qué firmas debe tener en cuenta para bloquear y cómo determinar cuándo puede habilitar de forma segura el bloqueo de una firma, consulte Firmas.
7. En la pantalla **Especificar protecciones profundas**, configure los parámetros y haga clic en **Siguiente**.
8. Después de completar, haga clic en **Finalizar** para cerrar el **Asistente para Web App Firewall**.

Crear una nueva configuración sin firmas

Siga estos pasos para utilizar el Asistente de Firewall de aplicaciones para omitir la pantalla Seleccionar firmas y crear una nueva configuración con solo el perfil y las directivas asociadas, pero sin ninguna firma.

1. Vaya a **Seguridad** > **Firewall de aplicaciones**.
2. En el panel de detalles, en **Introducción**, haga clic en **Asistente para firewall de aplicaciones**. Se abrirá el asistente.
3. En la pantalla **Especificar nombre**, seleccione **Crear nueva configuración**.
4. En el campo **Nombre**, escriba un nombre y, a continuación, haga clic en **Siguiente**.
5. En la pantalla **Especificar regla**, haga clic de nuevo en **Siguiente**.
6. En la pantalla **Seleccionar firmas**, haga clic en **Omitir.**
7. En la pantalla **Especificar protecciones profundas**, configure las acciones y los parámetros necesarios en **Configuración de acción**.
8. Cuando haya terminado, haga clic en **Finalizar** para cerrar el Asistente de firewall de aplicaciones.

Configurar una expresión de directiva personalizada

Siga estos pasos para utilizar el Asistente para Firewall de aplicaciones con el fin de crear una configuración de seguridad especializada para proteger solo contenido específico. En este caso, se crea una nueva configuración de seguridad en lugar de modificar la configuración inicial. Este tipo de configuración de seguridad requiere una regla personalizada, de modo que la directiva aplica la configuración solo al tráfico Web seleccionado.

1. Vaya a **Seguridad** > **Firewall de aplicaciones**.
2. En el panel de detalles, en **Introducción**, haga clic en **Asistente para firewall de aplicaciones**.
3. En la pantalla Especificar nombre, escriba un nombre para la nueva configuración de seguridad en el cuadro de texto Nombre, seleccione el tipo de configuración de seguridad en la lista desplegable Tipo y, a continuación, haga clic en **Siguiente**.
4. En la pantalla **Especificar regla**, escriba una regla que coincida únicamente con el contenido que quiere que proteja esta aplicación web. Utilice la lista desplegable **Expresiones de uso frecuente** y el **Editor** de expresiones para crear una expresión personalizada. Cuando termine, haga clic en **Siguiente**.
5. En la pantalla **Seleccionar firmas**, seleccione el modo de edición y, a continuación, haga clic en **Siguiente**.
6. En la pantalla **Especificar protecciones de firma**, configure los valores necesarios.
7. En la pantalla **Especificar protecciones profundas**, configure las acciones y los parámetros necesarios en **Configuración de acción**.
8. Cuando termine, haga clic en **Finalizar** para cerrar el **Asistente para Firewall de aplicaciones**.

Configuración manual

August 20, 2021

Si quiere enlazar un perfil a un punto de enlace distinto de Global, debe configurar manualmente el enlace. Además, algunas comprobaciones de seguridad requieren que introduzca manualmente las excepciones necesarias o habilite la función de aprendizaje para generar las excepciones que necesitan los sitios web y los servicios web. Algunas de estas tareas no se pueden realizar mediante el Asistente para Web App Firewall.

Si está familiarizado con el funcionamiento del Web App Firewall y prefiere la configuración manual, puede configurar manualmente un objeto de firmas y un perfil, asociar el objeto de firmas con el perfil, crear una directiva con una regla que coincida con el tráfico web que quiere configurar y asociar la directiva con el perfil. A continuación, vincula la directiva a Global, o a un punto de enlace, para ponerla en vigor, y ha creado una configuración de seguridad completa.

Para la configuración manual, puede usar la GUI (una interfaz gráfica) o la línea de comandos. Citrix recomienda utilizar la GUI. No todas las tareas de configuración se pueden realizar en la línea de comandos. Determinadas tareas, como habilitar firmas y revisar datos aprendidos, deben realizarse en la GUI. La mayoría de las demás tareas son más fáciles de realizar en la GUI.

Replicando la configuración

Cuando utiliza la GUI (GUI) o la interfaz de línea de comandos (CLI) para configurar manualmente el Web App Firewall, la configuración se guarda en el archivo /nsconfig/ns.conf. Puede utilizar los comandos de ese archivo para replicar la configuración en otro dispositivo. Puede cortar y pegar los comandos en la CLI uno por uno, o puede guardar varios comandos en un archivo de texto en la carpeta /var/tmp y ejecutarlos como un archivo por lotes. A continuación se muestra un ejemplo de ejecución de un archivo por lotes que contiene comandos copiados del archivo /nsconfig/ns.conf de un dispositivo diferente:

```
> batch -f /var/tmp/appfw_add.txt
```

> **Advertencia:**
>
> Los comandos de importación no se guardan en el archivo ns.conf. Antes de ejecutar comandos desde el archivo ns.conf para replicar la configuración en otro dispositivo, debe importar todos los objetos utilizados en la configuración (por ejemplo, firmas, página de error, WSDL y Esquema) al dispositivo en el que replica la configuración. El comando add para agregar un perfil de Web App Firewall guardado en un archivo ns.conf podría incluir el nombre de un objeto importado, pero tal comando podría fallar cuando se ejecuta en otro dispositivo si el objeto al que se hace referencia no existe en ese dispositivo.

Para obtener más información sobre los detalles de importación o exportación para replicar la configuración, consulte Exportación de firmasy Exportación de importación común .

Configuración manual mediante la GUI de Citrix ADC

August 20, 2021

Si necesita configurar manualmente la función Web App Firewall, Citrix recomienda utilizar el procedimiento de GUI de Citrix ADC.

Para crear y configurar objetos de firmas

Para poder configurar las firmas, debe crear un objeto de firmas a partir de la plantilla de objeto de firmas predeterminada adecuada. Asigne un nuevo nombre a la copia y, a continuación, configure la copia. No puede configurar ni modificar directamente los objetos de firmas predeterminados. El procedimiento siguiente proporciona instrucciones básicas para configurar un objeto de firmas. Para obtener instrucciones más detalladas, consulte Configuración manual de la función Firmas.

1. Vaya a **Seguridad > Citrix Web App Firewall > Firmas**.
2. En el panel de detalles, seleccione el objeto de firmas que quiere utilizar como plantilla y, a continuación, haga clic en **Agregar**.

   Las opciones disponibles son:

   - **Firmas predeterminadas.** Contiene las reglas de firmas, las reglas de inyección SQL y las reglas de scripts entre sitios.
   - **Inyección XPath.** Contiene todos los elementos de las firmas predeterminadas y, además, contiene las reglas de inyección XPath.
3. En el cuadro de diálogo **Agregar objeto de firmas**, escriba un nombre para el nuevo objeto de firmas, haga clic en Aceptar y, a continuación, haga clic en **Cerrar**. El nombre puede comenzar con una letra, un número o un símbolo de subrayado, y puede consistir de una a 31 letras, números y los símbolos de guión (-), punto (.) libra (#), espacio (), at (@), igual (=) y subrayado (_).
4. Seleccione el objeto de firmas que creó y, a continuación, haga clic en **Abrir**.
5. En el cuadro de diálogo **Modificar objeto de firmas**, defina las opciones **Mostrar criterios de filtro** a la izquierda para mostrar los elementos de filtro que quiere configurar.

   Al modificar estas opciones, los resultados que especifique se muestran en la ventana Resultados filtrados de la derecha. Para obtener más información sobre las categorías de firmas, consulte Firmas.
6. En el área **Resultados filtrados**, configure la configuración de una firma seleccionando y desactivando las casillas de verificación adecuadas.
7. Cuando haya terminado, haga clic en **Cerrar**.

Para crear un perfil de Web App Firewall mediante la GUI

La creación de un perfil de Web App Firewall requiere que especifique solo unos pocos detalles de configuración.

1. Vaya a **Seguridad > Citrix Web App Firewall > Perfiles**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En el cuadro de diálogo **Crear perfil de Web App Firewall**, escriba un nombre para su perfil.

   El nombre puede comenzar con una letra, un número o un símbolo de subrayado, y puede constar de una a 31 letras, números y los símbolos de guión (-), punto (.) libra (#), espacio ( ), en (@), igual (=), dos puntos (:) y guión bajo (_).
4. Elija el tipo de perfil en la lista desplegable.
5. Haga clic en **Crear** y, a continuación, en **Cerrar**.

Para configurar un perfil de Web App Firewall mediante la interfaz gráfica de usuario

1. Vaya a **Seguridad > Citrix Web App Firewall > Perfiles**.
2. En el panel de detalles, seleccione el perfil que quiere configurar y, a continuación, haga clic en **Modificar**.
3. En el cuadro de diálogo **Configurar perfil de Web App Firewall**, en la ficha **Comprobaciones de seguridad**, configure las comprobaciones de seguridad.
   - Para habilitar o inhabilitar una acción de una comprobación, en la lista, active o desactive la casilla de verificación de esa acción.
   - Para configurar otros parámetros para las comprobaciones que los tienen, en la lista, haga clic en el botón de contenido adicional azul situado en el extremo derecho de esa comprobación. En el cuadro de diálogo que aparece, configure los parámetros. Estos varían de un cheque a otro.

     También puede seleccionar una verificación y, en la parte inferior del cuadro de diálogo, hacer clic en Abrir para mostrar el cuadro de diálogo Configurar relajacióno Configurar regla para esa comprobación. Estos cuadros de diálogo también varían de una comprobación a otra. La mayoría de ellos incluyen una ficha Comprobaciones y una ficha General. Si la comprobación admite relajantes o reglas definidas por el usuario, la ficha Comprobaciones incluye un botón Agregar, que abre otro cuadro de diálogo, en el que puede especificar una relajación o una regla para la comprobación. (Una relajación es una regla para eximir el tráfico especificado del cheque.) Si ya se han configurado las relajantes, puede seleccionar una y hacer clic en Abrir para modificarla.

- Para revisar las excepciones o reglas aprendidas para una comprobación, selecciónela y, a continuación, haga clic en Violaciones aprendidas. En el cuadro de diálogo Administrar reglas aprendidas, seleccione cada excepción o regla aprendida a su vez.
  - Para modificar la excepción o regla y, a continuación, agregarla a la lista, haga clic en **Modificar e implementar**.
  - Para aceptar la excepción o regla sin modificaciones, haga clic en **Implementar**.
  - Para quitar la excepción o regla de la lista, haga clic en **Omitir**.
- Para actualizar la lista de excepciones o reglas que se van a revisar, haga clic en **Actualizar**.
- Para abrir el **Visualizador de aprendizaje** y utilizarlo para revisar las reglas aprendidas, haga clic en **Visualizador**.
- Para revisar las entradas de registro para las conexiones que coincidían con una comprobación, selecciónela y, a continuación, haga clic en **Registros**. Puede utilizar esta información para determinar qué comprobaciones coinciden con los ataques, de modo que pueda habilitar el bloqueo para dichas comprobaciones. También puede utilizar esta información para determinar qué comprobaciones coinciden con el tráfico legítimo, de modo que pueda configurar una exención adecuada para permitir esas conexiones legítimas. Para obtener más información sobre los registros, consulte Registros, estadísticas e informes.
- Para inhabilitar completamente una comprobación, en la lista, desactive todas las casillas de verificación situadas a la derecha de esa comprobación.

4. En la ficha **Configuración**, configure la configuración del perfil.
   - Para asociar el perfil con el conjunto de firmas que creó y configuró anteriormente, en **Configuración común**, elija ese conjunto de firmas en la lista desplegable Firmas.

     > **Nota:**
     >
     > Debe utilizar la barra de desplazamiento situada a la derecha del cuadro de diálogo para desplazarse hacia abajo y mostrar la sección Configuración común.

   - Para configurar un objeto de error HTML o XML, seleccione el objeto en la lista desplegable correspondiente.

     > **Nota:**
     >
     > Primero debe cargar el objeto de error que quiere utilizar en el panel Importar.

   - Para configurar el tipo de contenido XML predeterminado, escriba la cadena de tipo de contenido directamente en los cuadros de texto Solicitud predeterminada y Respuesta predeterminada, o haga clic en Administrar tipos de contenido permitidos para administrar la lista de tipos de contenido permitidos.

5. Si quiere utilizar la función de aprendizaje, haga clic en Aprendizaje y configure los parámetros de aprendizaje para el perfil. Para obtener más información, consulte Función Configurar y aprender.
6. Haga clic en **Aceptar** para guardar los cambios y volver al panel Perfiles.

Configuración de una regla o relajación de Web App Firewall

Puede configurar dos tipos diferentes de información en este cuadro de diálogo, en función de la comprobación de seguridad que esté configurando. En la mayoría de los casos, se configura una excepción (o relajación) a la comprobación de seguridad. Si está configurando la comprobación Denegar URL o la comprobación Formatos de campo, debe configurar una adición (o regla). El proceso para cualquiera de estos es el mismo.

Para configurar una regla de relajación mediante la GUI de Citrix ADC

1. Vaya a **Seguridad** > **Citrix Web App Firewall** > **Perfiles**.
2. En el panel **Perfiles**, seleccione el perfil que quiere configurar y, a continuación, haga clic en **Modificar**.
3. En la página **Configurar perfil de Web App Firewall**, haga clic en **Regla de relajación** en la sección **Configuración avanzada**. La sección **Regla de relajación** contiene la lista completa de reglas de relajación de Web App Firewall.
4. Haga clic en una regla de seguridad que quiera configurar y, a continuación, haga clic en **Modificar**.
5. La página Reglas de relajación de URL contiene una lista de acciones que puede configurar para esta regla y una lista de relajaciones o reglas existentes. La lista puede estar vacía si no ha agregado manualmente ninguna relajación o aprobado ninguna relajación recomendada por el motor de aprendizaje. Debajo de la lista hay una fila de botones que le permiten agregar, modificar, eliminar, habilitar o inhabilitar las relajantes de la lista.
6. Para agregar o modificar una relajación o una regla, siga uno de estos procedimientos:
   - Para agregar una nueva relajación, haga clic en **Agregar**.
   - Para modificar una relajación existente, seleccione la relajación que quiera modificar y, a continuación, haga clic en **Abrir**.

   Aparecerá la página **Regla de relajación de URL de inicio**. Excepto por el título, estos cuadros de diálogo son idénticos.
7. Rellene el cuadro de diálogo como se describe a continuación. Los cuadros de diálogo para cada comprobación son diferentes. La siguiente lista cubre todos los elementos que pueden aparecer en cualquier cuadro de diálogo.

- **Casilla de verificación Activada**: Seleccione esta opción para colocar esta relajación o regla en uso activo; desactive para desactivarla.
- **Tipo de contenido de datos adjuntos**: El atributo Content-Type de un archivo adjunto XML. En el área de texto, escriba una expresión regular que coincida con el atributo Content-Type de los datos adjuntos XML que se va a permitir.
- **URL de acción**: En el área de texto, introduzca una expresión regular con formato PCRE- que defina la dirección URL a la que se entregan los datos introducidos en el formulario web.
- **Cookie**: En el área de texto, introduzca una expresión regular en formato PCRE-que defina la cookie.
- **Nombre de campo**: El elemento de nombre de campo de formulario web puede tener la etiqueta Nombre de campo, Campo de formulario u otro nombre similar. En el área de texto, escriba una expresión regular con formato PCRE-que defina el nombre del campo de formulario.
- **Desde URL de origen**: En el área de texto, introduzca una expresión regular en formato PCRE que defina la dirección URL que aloja el formulario web.
- **Desde URL de acción**: En el área de texto, introduzca una expresión regular en formato PCRE que defina la dirección URL a la que se entregan los datos introducidos en el formulario web.
- **Name**—Un elemento XML o nombre de atributo. En el área de texto, escriba una expresión regular de formato PCRE-que defina el nombre del elemento o atributo.
- **URL**: Un elemento URL puede estar etiquetado como URL de acción, URL de rechazo, URL de acción de formulario, URL de origen de formulario, URL de inicio o simplemente URL. En el área de texto, escriba una expresión regular con formato PCRE-que defina la dirección URL.
- **Formato**: La sección de formato contiene varios parámetros que incluyen cuadros de lista y cuadros de texto. Puede aparecer cualquiera de las siguientes opciones:
  - **Tipo**: Seleccione un tipo de campo en la lista desplegable Tipo. Para agregar una nueva definición de tipo de campo, haga clic en Administrar:
  - **Longitud mínima**: Escriba un entero positivo que represente la longitud mínima en caracteres si quiere forzar a los usuarios a rellenar este campo. Valor predeterminado: 0 (permite que el campo se deje en blanco.)
  - **Longitud máxima**: Para limitar la longitud de los datos en este campo, escriba un entero positivo que represente la longitud máxima en caracteres. Valor predeterminado: 65535

- **Ubicación**: Seleccione el elemento de la solicitud al que se aplica su relajación en la lista desplegable. Para las comprobaciones de seguridad HTML, las opciones son:
  - FormField: Campos de formulario en formularios web.
  - Encabezado: Encabezados de solicitud.
  - Cookie: Establecer encabezados de cookies.

  Para las comprobaciones de seguridad XML, las opciones son:
  - ELEMENT: Elemento XML.
  - ATTRIBUE: Atributo XML.
- **Tamaño máximo de datos adjuntos**: El tamaño máximo en bytes permitido para un archivo adjunto XML.
- **Comentarios**: En el área de texto, escriba un comentario. Opcional.

Nota: Para cualquier elemento que requiera una expresión regular, puede escribir la expresión regular, utilizar el menú Fichas de expresión regular para insertar elementos y símbolos de expresión regular directamente en el cuadro de texto, o hacer clic en **Editor de expresiones** regulares para abrir el cuadro de texto **Agregar expresión regular** y utilícelo para construir la expresión.

8. Para eliminar una relajación o regla, selecciónela y, a continuación, haga clic en **Eliminar**.
9. Para habilitar una relajación o regla, selecciónela y, a continuación, haga clic en **Habilitar**.
10. Para inhabilitar una relajación o regla, selecciónela y, a continuación, haga clic en **Inhabilitar**.
11. Para configurar los parámetros y las relaciones de todas las relajaciones existentes en una pantalla gráfica interactiva integrada, haga clic en **Visualizador** y utilice las herramientas de visualización.

    > **Nota:**
    >
    > El botón **Visualizador** no aparece en todos los cuadros de diálogo de relajación de verificación.

12. Para revisar las reglas aprendidas para esta comprobación, haga clic en Aprendizaje y lleve a cabo los pasos de Para configurar y utilizar la función Aprendizaje.
13. Haga clic en **Aceptar**.

Para configurar las reglas aprendidas mediante la GUI de Citrix ADC

1. Vaya a **Seguridad** > **Citrix Web App Firewall** > **Perfiles**.
2. En el panel **Perfiles**, seleccione el perfil y, a continuación, haga clic en **Modificar**.

3. En la página **Perfil de Citrix Web App Firewall**, haga clic en **Reglas aprendidas** de **configuración avanzada**. En la sección **Reglas aprendidas** puede ver una lista de comprobaciones de seguridad disponibles en el perfil actual y que admiten la función de aprendizaje.
4. Para configurar los umbrales de aprendizaje, seleccione una comprobación de seguridad y haga clic en **Configuración**.
5. En la página **Configuración de reglas de aprendizaje y perfiles dinámicos**, puede establecer la configuración. Para obtener más información, consulte Configuración del perfil dinámico
   - **Umbral de número mínimo.** Dependiendo de la configuración de aprendizaje de la comprobación de seguridad que esté configurando, el umbral de número mínimo puede referirse al número mínimo de sesiones totales de usuario que se deben observar, el número mínimo de solicitudes que se deben observar o el número mínimo de veces que se debe observar un campo de formulario específico. antes de que se genere una relajación aprendida. Predeterminado: 1
   - **Porcentaje de veces umbral.** Dependiendo de la configuración de aprendizaje de la comprobación de seguridad que esté configurando, el porcentaje de veces umbral puede hacer referencia al porcentaje del total de sesiones de usuario observadas que infringieron la comprobación de seguridad, el porcentaje de solicitudes o el porcentaje de veces que un campo de formulario coincide con un tipo de campo determinado, antes de un aprendida relajación se genera. Predeterminado: 0
6. Para eliminar todos los datos aprendidos y restablecer la función de aprendizaje, de modo que debe iniciar sus observaciones de nuevo desde el principio, seleccione la acción **Eliminar todos los datos aprendidos**.

   > **Nota:**
   >
   > Este botón elimina solo las recomendaciones aprendidas que no se han revisado y que se han aprobado u omitido. No elimina las relajaciones aprendidas que se han aceptado e implementado.

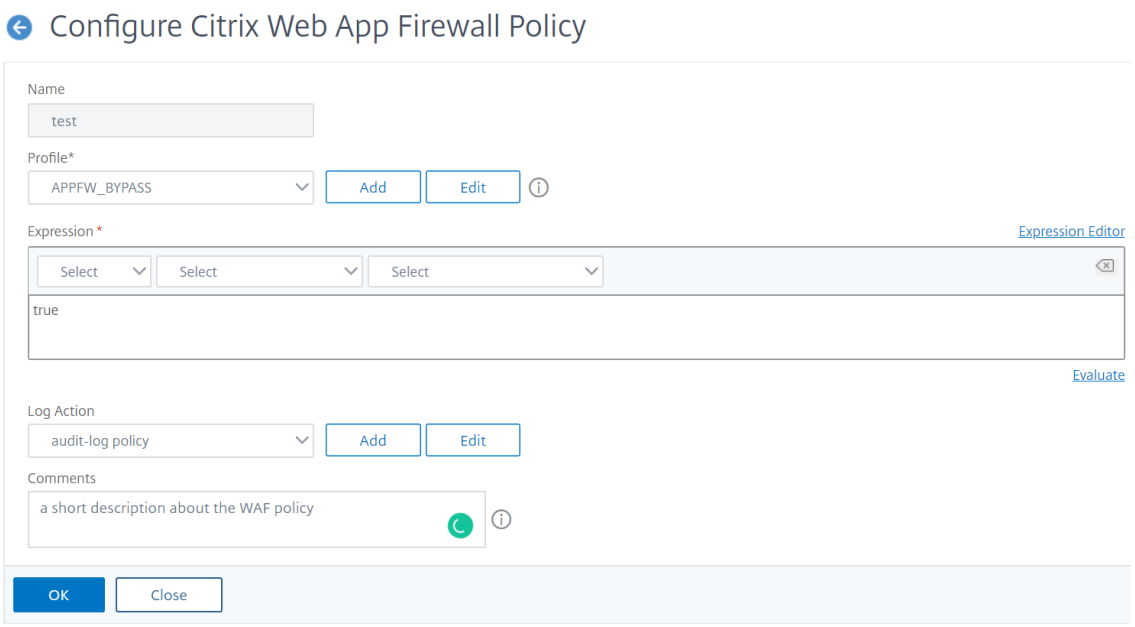
7. Para restringir el motor de aprendizaje al tráfico de un conjunto específico de IP, haga clic en **Clientes de aprendizaje de confianza** y agregue las direcciones IP que quiera utilizar a la lista.
   a) Para agregar una dirección IP o un intervalo de direcciones IP a la lista Clientes de aprendizaje de confianza, haga clic en **Agregar**.
   b) En la página **Perfil de AppFirewall a Enlace de Clint de confianza**, haga clic en **Agregar**.
   c) Active la casilla de verificación **Habilitado** para habilitar la función.
   d) En el ** cuadro Cliente de aprendizaje de confianza, escriba la dirección IP o un intervalo de direcciones IP en formato CIDR.
   e) En el área de texto **Comentarios**, escriba un comentario que describa esta dirección IP o intervalo.

f) Haga clic en **Crear** y **cerrar**.

8. Para modificar una dirección IP o rango existente, haga clic en la dirección IP o el intervalo y, a continuación, haga clic en **Modificar**. Excepto por el nombre, el cuadro de diálogo que aparece es idéntico al cuadro de diálogo Agregar clientes de aprendizaje de confianza.
9. Para inhabilitar o habilitar una dirección IP o un rango, pero dejarlo en la lista, haga clic en la dirección IP o en el rango y, a continuación, en **Inhabilitar** o **Activar**, según corresponda.
10. Para quitar una dirección IP o un intervalo por completo, haga clic en la dirección IP o el intervalo y, a continuación, haga clic en **Eliminar**.
11. Haga clic en **Cerrar** para volver a la página **Perfil de Citrix Web App Firewall**.

Para crear una directiva de Citrix Web App Firewall mediante la GUI de Citrix ADC

1. Vaya a **Seguridad** > **Firewall de Citrix Web App** > **Directivas**.
2. En la página **Directivas**, haga clic en el vínculo **Directiva de Citrix Web App Firewall**.
3. En la página Directivas de Citrix Web App Firewall, haga clic en **Agregar**.
4. En la página Crear directiva de Citrix Web App Firewall, establezca los siguientes parámetros.
   a) Name. El nombre puede comenzar con una letra, un número o un símbolo de subrayado, y puede constar de una a 128 letras, números y los símbolos de guión (-), punto (.) libra (#), espacio (), en (@), igual (=), dos puntos (:) y guión bajo (_).
   b) Perfil. Seleccione el perfil que quiere asociar a esta directiva en la lista desplegable Perfil. Puede crear un perfil para asociarlo a la directiva haciendo clic en Nuevo y puede modificar un perfil existente haciendo clic en **Modificar**.
   c) Expresión. En el área de texto Expresión, cree una regla para la directiva.
   d) Acción de registro. Agregue una acción de registro o puede modificar una acción de registro existente.
   e) Comentarios. Una breve descripción de la directiva.
5. Haga clic en **Crear** o **Aceptar**y, a continuación, en **Cerrar**.



Para crear o configurar una regla de Web App Firewall (expresión)

La regla de directiva, también denominada *expresión*, define el tráfico web que filtra el Web App Firewall mediante el perfil asociado a la directiva. Al igual que otras reglas de directivas de Citrix ADC (o *expresiones*), las reglas de Web App Firewall utilizan la sintaxis de expresiones Citrix ADC. Esta sintaxis es potente, flexible y extensible. Es demasiado complejo para describir completamente en este conjunto de instrucciones. Puede utilizar el siguiente procedimiento para crear una regla de directiva de firewall simple o puede leerla como una descripción general del proceso de creación de directivas.

1. Si aún no lo ha hecho, vaya a la ubicación adecuada en el asistente de Web App Firewall o en la GUI de Citrix ADC para crear la regla de directiva:
    - Si está configurando una directiva en el Asistente para Web App Firewall, en el panel de navegación, haga clic en **Citrix Web App Firewall Wizard** y, a continuación, en el panel de detalles, haga clic en **Citrix Web App Firewall Wizard** y, a continuación, vaya a la página de ficha **Especificar regla**.
    - En la página **Especificar regla**, elija el prefijo de la expresión en la lista desplegable. Las opciones disponibles son:
    - **HTTP.** El protocolo HTTP. Elija esto si quiere examinar algún aspecto de la solicitud que pertenece al protocolo HTTP.
    - **SYS.** Uno o más sitios web protegidos. Elija esta opción si quiere examinar algún aspecto de la solicitud que pertenece al destinatario de la solicitud.
    - **CLIENT.** El equipo que envió la solicitud. Elija esto si quiere examinar algún aspecto del remitente de la solicitud.

- **SERVER.** El equipo al que se envió la solicitud. Elija esto si quiere examinar algún aspecto del destinatario de la solicitud.

Después de elegir un prefijo, Web App Firewall muestra una ventana de solicitud de dos partes que muestra las posibles opciones siguientes en la parte superior y una breve explicación de lo que significa la opción seleccionada en la parte inferior.

2. Elija su próximo mandato.

   Si eligió HTTP como prefijo, su única opción es REQ, que especifica el par Request/Response. (El Web App Firewall funciona en la solicitud y respuesta como una unidad en lugar de en cada una por separado.) Si elige otro prefijo, sus opciones son más variadas. Para obtener ayuda sobre una opción específica, haga clic en esa opción una vez para mostrar información sobre ella en la ventana de solicitud inferior.

   Cuando haya decidido qué término quiere, haga doble clic en él para insertarlo en la ventana Expresión.

3. Escriba un período después del término que acaba de elegir. A continuación, se le pedirá que elija su próximo término, como se describe en el paso anterior. Cuando un término requiera que escriba un valor, rellene el valor apropiado. Por ejemplo, si elige HTTP.REQ.HEADER(“”), escriba el nombre del encabezado entre las comillas.

4. Siga eligiendo términos de las solicitudes y rellenando los valores necesarios hasta que finalice la expresión.

   A continuación se presentan algunos ejemplos de expresiones para fines específicos.

   - **Host web específico.** Para hacer coincidir el tráfico de un host web concreto:

```
HTTP.REQ.HEADER("Host").EQ("shopping.example.com")
```

Para shopping.example.com, sustituya el nombre del host web que quiere que coincida.

- **Carpeta web o directorio específico.** Para hacer coincidir el tráfico de una carpeta o directorio determinado en un host Web:

```
HTTP.REQ.URL.STARTSWITH("https//www.example.com/folder")
```

Para www.example.com, sustituya el nombre del host web. En el caso de carpeta, sustituya la carpeta o la ruta de acceso al contenido que quiere que coincida. Por ejemplo, si su carrito de la compra está en una carpeta llamada /solutions/orders, sustituya esa cadena por carpeta.

- **Tipo específico de contenido: Imágenes GIF.** Para hacer coincidir imágenes con formato GIF:

```
HTTP.REQ.URL.ENDSWITH(".png")
```

Para que coincidan con otras imágenes de formato, sustituya otra cadena en lugar de .png.

- **Tipo específico de contenido: Scripts.** Para hacer coincidir todos los scripts CGI ubicados en el directorio CGI-BIN:


```
HTTP.REQ.URL.STARTSWITH("https//www.example.com/CGI-BIN")
```

Para hacer coincidir todos los JavaScripts con extensiones.js:

```
HTTP.REQ.URL.ENDSWITH(".js")
```

Para obtener más información sobre la creación de expresiones de directiva, consulte Directivas y expresiones.

> **Nota:**
>
> Si utiliza la línea de comandos para configurar una directiva, recuerde evitar las comillas dobles dentro de las expresiones Citrix ADC. Por ejemplo, la siguiente expresión es correcta si se introduce en la GUI:

```
HTTP.REQ.HEADER("Host").EQ("shopping.example.com")
```

Sin embargo, si se introduce en la línea de comandos, debe escribir esto en su lugar:

```
HTTP.REQ.HEADER("Host").EQ("shopping.example.com")
```

```
1 ![Policy expression configuration](/en-us/citrix-adc/media/waf-rule.png
    )
```

Para agregar una regla de firewall (expresión) mediante el cuadro de diálogo Agregar expresión

El cuadro de diálogo **Agregar expresión** (también denominado Editor de expresiones) ayuda a los usuarios que no están familiarizados con el lenguaje de expresiones de Citrix ADC a crear una directiva que coincida con el tráfico que desean filtrar.

1. Si aún no lo ha hecho, desplácese hasta la ubicación adecuada en el Asistente para Web App Firewall o en la GUI de Citrix ADC:
   - Si va a configurar una directiva en el asistente de **Web App Firewall**, en el panel de navegación, haga clic en **Web App Firewall**y, a continuación, en el panel de detalles, haga clic en Asistente de **Web App Firewall** y, a continuación, vaya a la pantalla **Especificar regla** .
   - Si está configurando una directiva manualmente, en el panel de exploración, expanda **Web App Firewall**, **Directivas** y, a continuación, **Firewall**. En el panel de detalles, para crear una directiva, haga clic en **Agregar**. Para modificar una directiva existente, selecciónela y, a continuación, haga clic en **Abrir**.
2. En la pantalla **Especificar regla**, en el cuadro de diálogo **Crear perfil de Web App Firewall** o en el cuadro de diálogo **Configurar perfil de Web App Firewall**, haga clic en **Agregar**.
3. En el cuadro de diálogo **Agregar expresión**, en el área Construir expresión, en el primer cuadro de lista, elija uno de los prefijos siguientes:

- **HTTP.** El protocolo HTTP. Elija esto si quiere examinar algún aspecto de la solicitud que pertenece al protocolo HTTP. La opción predeterminada.
- **SYS.** Uno o más sitios web protegidos. Elija esta opción si quiere examinar algún aspecto de la solicitud que pertenece al destinatario de la solicitud.
- **CLIENT.** El equipo que envió la solicitud. Elija esto si quiere examinar algún aspecto del remitente de la solicitud.
- **SERVER.** El equipo al que se envió la solicitud. Elija esto si quiere examinar algún aspecto del destinatario de la solicitud.

4. En el segundo cuadro de lista, elija su próximo término. Los términos disponibles varían según la elección realizada en el paso anterior, ya que el cuadro de diálogo ajusta automáticamente la lista para que contenga solo los términos válidos para el contexto. Por ejemplo, si seleccionó HTTP en el cuadro de lista anterior, la única opción es REQ, para las solicitudes. Dado que Web App Firewall trata las solicitudes y las respuestas asociadas como una sola unidad y filtra ambas, no es necesario que las respuestas específicas se presenten por separado. Después de elegir su segundo término, aparece un tercer cuadro de lista a la derecha del segundo. La ventana Ayuda muestra una descripción del segundo término y la ventana Vista previa de expresión muestra la expresión.
5. En el tercer cuadro de lista, elija el siguiente término. Aparecerá un nuevo cuadro de lista a la derecha y la ventana de Ayuda cambia para mostrar una descripción del nuevo término. La ventana Vista previa de expresión se actualiza para mostrar la expresión tal y como la ha especificado en ese punto.
6. Continúe eligiendo términos y, cuando se le solicite, rellenando argumentos, hasta que se complete la expresión. Si comete un error o quiere cambiar su expresión después de haber seleccionado un término, simplemente puede elegir otro término. La expresión se modifica y se borran los argumentos o más términos que haya agregado después del término modificado.
7. Cuando haya terminado de construir la expresión, haga clic en Aceptar para cerrar el cuadro de diálogo Agregar expresión. La expresión se inserta en el área de texto Expresión.

Para enlazar una directiva de Web App Firewall mediante la GUI de Citrix ADC

1. Lleve a cabo una de las siguientes acciones:
   - Vaya a **Seguridad** > **Web App Firewall** y, en el panel de detalles, haga clic en **Administrador de directivas de firewall de aplicaciones**.
   - Vaya a **Seguridad** > **Citrix Web App Firewall** > **Directivas** > **Firewall** y, en el panel "Directivas de Citrix Web App Firewall", haga clic en **Administrador de directivas**.
2. En el cuadro de diálogo **Administrador de directivas de Application Firewall**, elija el punto de enlace al que quiere vincular la directiva en la lista desplegable. Las opciones son:
   - **Anular Global.** Las directivas enlazadas a este punto de enlace procesan todo el tráfico de todas las interfaces del dispositivo Citrix ADC y se aplican antes que cualquier otra directiva.

- **Servidor virtual LB.** Las directivas enlazadas a un servidor virtual de equilibrio de carga se aplican solo al tráfico procesado por ese servidor virtual de equilibrio de carga y se aplican antes de cualquier directiva global predeterminada. Después de seleccionar LB Virtual Server, también debe seleccionar el servidor virtual de equilibrio de carga específico al que quiere enlazar esta directiva.
- **Servidor virtual CS.** Las directivas enlazadas a un servidor virtual de conmutación de contenido se aplican solo al tráfico procesado por ese servidor virtual de conmutación de contenido y se aplican antes de cualquier directiva global predeterminada. Después de seleccionar CS Virtual Server, también debe seleccionar el servidor virtual de conmutación de contenido específico al que quiere enlazar esta directiva.
- **Global predeterminada.** Las directivas vinculadas a este punto de enlace procesan todo el tráfico de todas las interfaces del dispositivo Citrix ADC.
- **Etiqueta de directiva.** Las directivas enlazadas a una etiqueta de directiva procesan el tráfico que la etiqueta de directiva les enruta. La etiqueta de directiva controla el orden en que se aplican las directivas a este tráfico.
- **Ninguno.** No vincule la directiva a ningún punto de enlace.

3. Haga clic en **Continuar**. Aparecerá una lista de las directivas existentes de Web App Firewall.
4. Seleccione la directiva que quiere vincular haciendo clic en ella.
5. Realice ajustes adicionales en el enlace.
   - Para modificar la prioridad de directiva, haga clic en el campo para habilitarla y, a continuación, escriba una nueva prioridad. También puede seleccionar **Regenerar Prioridades** para volver a numerar las prioridades de manera uniforme.
   - Para modificar la expresión de directiva, haga doble clic en ese campo para abrir el cuadro de diálogo **Configurar directiva de Web App Firewall**, donde puede modificar la expresión de directiva.
   - Para establecer la expresión Goto, haga doble clic en el campo del encabezado de columna **Goto Expression** para mostrar la lista desplegable, donde puede elegir una expresión.
   - Para definir la opción Invocar, haga doble clic en el campo del encabezado de columna Invocar para mostrar la lista desplegable, donde puede elegir una expresión.
6. Repita los pasos 3 a 6 para agregar cualquier directiva adicional de Web App Firewall que quiera enlazar globalmente.
7. Haga clic en **Aceptar**. Aparece un mensaje en la barra de estado que indica que la directiva se ha enlazado correctamente.

Configuración manual mediante la interfaz de línea de comandos

August 20, 2021

> **Nota:**
>
> Si necesita configurar manualmente la función Web App Firewall, Citrix recomienda utilizar el procedimiento de GUI de Citrix ADC.

Puede configurar las funciones de Web App Firewall desde la interfaz de comandos de **Citrix ADC**. Sin embargo, hay excepciones importantes. No puede habilitar firmas desde la interfaz de comandos. Hay alrededor de 1.000 firmas predeterminadas en siete categorías y la tarea es demasiado compleja para la interfaz de comandos. Puede habilitar o inhabilitar funciones y configurar parámetros desde la línea de comandos, pero no puede configurar relajaciones manuales. Aunque puede configurar la función de aprendizaje adaptativo y habilitar el aprendizaje desde la línea de comandos, no puede revisar las relajaciones aprendidas o las reglas aprendidas y aprobarlas u omitirlas. La interfaz de línea de comandos está diseñada para usuarios avanzados que están familiarizados con el uso del dispositivo Citrix ADC y Web App Firewall.

Para configurar manualmente Web App Firewall mediante la línea de comandos de Citrix ADC, utilice un cliente telnet o de shell seguro de su elección para iniciar sesión en la línea de comandos de Citrix ADC.

Para crear un perfil mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos:

- `add appfw profile <name> [-defaults ( basic | advanced )]`
- `set appfw profile <name> -type ( HTML | XML | HTML XML )`
- `save ns config`

Ejemplo

En el ejemplo siguiente se agrega un perfil denominado pr-basic, con valores predeterminados básicos, y se asigna un tipo de perfil de HTML. Esta es la configuración inicial adecuada para que un perfil proteja un sitio web HTML.

```
1 add appfw profile pr-basic -defaults basic
2 set appfw profile pr-basic -type HTML
3 save ns config
4 <!--NeedCopy-->
```

Para configurar un perfil mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos:

- `set appfw profile <name> <arg1> [<arg2> ...]` donde `<arg1>` representa un parámetro y `<arg2>` representa otro parámetro o el valor a asignar al parámetro representado por `<arg1>`. Para obtener descripciones de los parámetros que se deben utilizar al configurar comprobaciones de seguridad específicas, consulte Protecciones avanzadas y sus subtemas. Para obtener descripciones de los otros parámetros, consulte "Parámetros para la creación de un perfil".
- `save ns config`

Ejemplo

El siguiente ejemplo muestra cómo configurar un perfil HTML creado con valores predeterminados básicos para comenzar a proteger un sitio web basado en HTML simple. Este ejemplo activa el registro y el mantenimiento de las estadísticas para la mayoría de las comprobaciones de seguridad, pero permite el bloqueo solo para aquellas comprobaciones que tienen tasas bajas de falsos positivos y que no requieren configuración especial. También activa la transformación de HTML inseguro y SQL inseguro, lo que evita ataques pero no bloquea las solicitudes a sus sitios web. Con el registro y las estadísticas habilitadas, puede revisar posteriormente los registros para determinar si quiere habilitar el bloqueo para una comprobación de seguridad específica.

```
set appfw profile -startURLAction log stats
set appfw profile -denyURLAction block log stats
set appfw profile -cookieConsistencyAction log stats
set appfw profile -crossSiteScriptingAction log stats
set appfw profile -crossSiteScriptingTransformUnsafeHTML ON
set appfw profile -fieldConsistencyAction log stats
set appfw profile -SQLInjectionAction log stats
set appfw profile -SQLInjectionTransformSpecialChars ON
set appfw profile -SQLInjectionOnlyCheckFieldsWithSQLChars ON
set appfw profile -SQLInjectionParseComments checkall
set appfw profile -fieldFormatAction log stats
set appfw profile -bufferOverflowAction block log stats
set appfw profile -CSRFtagAction log stats
save ns config
<!--NeedCopy-->
```

Para crear y configurar una directiva

En el símbolo del sistema, escriba los siguientes comandos:

- `add appfw policy <name> <rule> <profile>`
- `save ns config`

Ejemplo

En el ejemplo siguiente se agrega una directiva denominada pl-blog, con una regla que intercepta todo el tráfico hacia o desde el host blog.example.com, y se asocia esa directiva con el perfil pr-blog.

```
add appfw policy pl-blog "HTTP.REQ.HOSTNAME.DOMAIN.EQ("blog.example.com")" pr-blog
<!--NeedCopy-->
```

Para enlazar una directiva de Web App Firewall

En el símbolo del sistema, escriba los siguientes comandos:

- `bind appfw global <policyName> <priority>`
- `save ns config`

Ejemplo

En el ejemplo siguiente se vincula la directiva denominada pl-blog y se le asigna una prioridad de 10.

```
bind appfw global pl-blog 10
save ns config
<!--NeedCopy-->
```

Para configurar el límite de sesión por PE

En el símbolo del sistema, escriba los siguientes comandos:

- `set appfw settings <session limit>`

Ejemplo

En el ejemplo siguiente se configura el límite de sesión por PE.

```
> set appfw settings -sessionLimit 500000`

Done

Default value:100000   Max value:500000 per PE
```



```
<!--NeedCopy-->
```

Firmas

August 20, 2021

Las firmas de Web App Firewall proporcionan reglas específicas y configurables para simplificar la tarea de proteger sus sitios web contra ataques conocidos. Una firma representa un patrón que es un componente de un ataque conocido en un sistema operativo, servidor web, sitio web, servicio web basado en XML u otro recurso. Un amplio conjunto de reglas integradas o nativas preconfiguradas de Web App Firewall ofrece una solución de seguridad fácil de usar, aplicando el poder de la coincidencia de patrones para detectar ataques y proteger contra vulnerabilidades de aplicaciones.

Puede crear sus propias firmas o usar firmas en las plantillas integradas. El Web App Firewall tiene dos plantillas integradas:

- **Firmas por Defecto**: Esta plantilla contiene una lista preconfigurada de más de 1.300 firmas, además de una lista completa de palabras clave de inyección SQL, cadenas especiales de SQL, reglas de transformación SQL y caracteres comodín SQL. También contiene patrones denegados para scripts entre sitios y atributos y etiquetas permitidos para scripts entre sitios. Esta es una plantilla de solo lectura. Puede ver el contenido, pero no puede agregar, modificar o eliminar nada de esta plantilla. Para usarlo, debes hacer una copia. En su propia copia, puede habilitar las reglas de firma que quiere aplicar al tráfico y especificar las acciones que se deben realizar cuando las reglas de firma coincidan con el tráfico.

Las firmas de Web App Firewall se derivan de las reglas publicadas por Snort, que es un sistema de prevención de intrusiones de código abierto capaz de realizar análisis de tráfico en tiempo real para detectar varios ataques y sondeos.

- ***Patrones de inyección de Xpath**: Esta plantilla contiene un conjunto preconfigurado de palabras clave literales y PCRE y cadenas especiales que se utilizan para detectar ataques de inyección de XPath (XML Path Language).

Firmas en blanco: Además de hacer una copia de la plantilla incorporada *Default Signatures, puede usar una plantilla de firmas en blanco para crear un objeto de firma. El objeto de firma que se crea con la opción de firmas en blanco no tiene reglas de firma nativas, pero, al igual que la plantilla *Default, tiene todas las entidades integradas en scripts SQL/Cross Site.

Firmas de formato externo: Web App Firewall también admite firmas de formato externo. Puede importar el informe de análisis de terceros mediante los archivos XSLT compatibles con Citrix Web App Firewall. Hay disponible un conjunto de archivos XSLT integrados para que las siguientes herramientas de análisis traduzcan archivos de formato externo a formato nativo:

- Cenzic
- Seguridad profunda para aplicaciones web
- IBM AppScan Enterprise
- IBM AppScan Standard.
- Qualys
- Nube de Qualys
- Whitehat
- Hewlett Packard Enterprise WebInspect
- Rapid7 Appspider
- Acunetix

Protección de seguridad para su aplicación

Una seguridad más estricta aumenta la sobrecarga de procesamiento. Las firmas proporcionan las siguientes opciones de implementación para ayudarle a optimizar la protección de sus aplicaciones:

- **Modelo de seguridad negativa**: Con el modelo de seguridad negativa, se utiliza un conjunto completo de reglas de firma preconfiguradas para aplicar el poder de la coincidencia de patrones para detectar ataques y proteger contra vulnerabilidades de aplicaciones. Bloqueas solo lo que no quieres y permites el resto. Puede agregar sus propias reglas de firma, basadas en las necesidades de seguridad específicas de sus aplicaciones, para diseñar sus propias soluciones de seguridad personalizadas.
- **Modelo de seguridad híbrida**: Además de utilizar firmas, puede utilizar comprobaciones de seguridad positivas para crear una configuración ideal para sus aplicaciones. Use firmas para bloquear lo que no quiere y use comprobaciones de seguridad positivas para imponer lo que está permitido.

Para proteger la aplicación mediante firmas, debe configurar uno o varios perfiles para utilizar el objeto signatures. En una configuración de seguridad híbrida, los patrones de inyección SQL y scripts entre sitios, y las reglas de transformación SQL, en el objeto de firmas se utilizan no solo por las reglas de firma, sino también por las comprobaciones de seguridad positivas configuradas en el perfil de Web App Firewall que utiliza el objeto de firmas.

El Web App Firewall examina el tráfico de los sitios web y servicios web protegidos para detectar el tráfico que coincide con una firma. Una coincidencia se activa solo cuando cada patrón de la regla coincide con el tráfico. Cuando se produce una coincidencia, se invocan las acciones especificadas para la regla. Puede mostrar una página de error u objeto de error cuando se bloquea una solicitud. Los mensajes de registro pueden ayudarle a identificar los ataques que se están iniciando contra su aplicación. Si habilita las estadísticas, Web App Firewall mantiene los datos sobre las solicitudes que coinciden con una firma o comprobación de seguridad de Web App Firewall.

Si el tráfico coincide tanto con una firma como con una comprobación de seguridad positiva, se apli-

cará la más restrictiva de las dos acciones. Por ejemplo, si una solicitud coincide con una regla de firma para la que está inhabilitada la acción de bloqueo, pero la solicitud también coincide con una comprobación de seguridad positiva de SQL Injection para la que la acción es bloque, la solicitud se bloquea. En este caso, la infracción de firma puede registrarse como <not blocked>, aunque la solicitud está bloqueada por la comprobación de inyección SQL.

Personalización: Si es necesario, puede agregar sus propias reglas a un objeto de firmas. También puede personalizar los patrones de scripts SQL/sitios cruzados. La opción de agregar sus propias reglas de firma, basadas en las necesidades de seguridad específicas de sus aplicaciones, le brinda la flexibilidad para diseñar sus propias soluciones de seguridad personalizadas. Bloqueas solo lo que no quieres y permites el resto. Un patrón de coincidencia rápida específico en una ubicación especificada puede reducir significativamente la sobrecarga de procesamiento para optimizar el rendimiento. Puede agregar, modificar o quitar patrones de scripts entre sitios e inyección SQL. Los editores de expresiones y expresiones incorporados le ayudan a configurar sus patrones y verificar su precisión.

Actualización automática: Puede actualizar manualmente el objeto de firma para obtener las reglas de firma más recientes, o puede aplicar la función de actualización automática para que el Web App Firewall pueda actualizar automáticamente las firmas desde el servicio de actualizaciones de Web App Firewall basado en la nube.

> **Nota:**
>
> Si se agregan nuevas reglas de firma durante la actualización automática, se inhabilitan de forma predeterminada. Debe revisar periódicamente las firmas actualizadas y habilitar las reglas recién agregadas pertinentes para proteger las aplicaciones.
>
> Debe configurar CORS para alojar firmas en servidores IIS.
>
> La función de actualización automática de firmas no funciona en el servidor web local cuando se accede a la URL desde la GUI de Citrix ADC.

Introducción

El uso de firmas Citrix para proteger su aplicación es fácil y se puede realizar en unos sencillos pasos:

1. Agregue un objeto de firma.

- Puede utilizar el Asistente que le pide que cree toda la configuración de Web App Firewall, incluida la adición del perfil y la directiva, la selección y habilitación de firmas y la especificación de acciones para firmas y comprobaciones de seguridad positivas. El objeto signatures se crea automáticamente.
- Puede crear una copia del objeto signatures a partir de la plantilla *Default Signatures, usar una plantilla en blanco para crear una firma con sus propias reglas personalizadas o agregar una firma de formato externo. Habilite las reglas y configure las acciones que quiere aplicar.

1. Configure el perfil de Web App Firewall de destino para utilizar este objeto de firmas.

2. Enviar tráfico para validar la funcionalidad

Resumen

- El objeto Firmas predeterminadas es una plantilla. No se puede modificar ni eliminar. Para usarlo, debe crear una copia. En su propia copia, puede habilitar las reglas y la acción deseada para cada regla según sea necesario para su aplicación. Para proteger la aplicación, debe configurar el perfil de destino para utilizar esta firma.
- El procesamiento de patrones de firma tiene sobrecarga. Intente habilitar solo las firmas que sean aplicables para proteger su aplicación, en lugar de habilitar todas las reglas de firma.
- Cada patrón de la regla debe coincidir para activar una coincidencia de firma.
- Puede agregar sus propias reglas personalizadas para inspeccionar las solicitudes entrantes y detectar varios tipos de ataques, como ataques de inyección SQL o scripts entre sitios. También puede agregar reglas para inspeccionar las respuestas a fin de detectar y bloquear la fuga de información confidencial, como números de tarjetas de crédito.
- Puede hacer una copia de un objeto de firma existente y modificarlo agregando o modificando reglas y patrones de scripting SQL/Cross Site, para proteger otra aplicación.
- Puede utilizar la actualización automática para descargar la versión más reciente de las reglas predeterminadas de Web App Firewall sin necesidad de supervisión continua para comprobar la disponibilidad de la nueva actualización.
- Un objeto de firma puede ser utilizado por más de un perfil. Incluso después de haber configurado uno o más perfiles para utilizar un objeto de firma, puede habilitar o inhabilitar firmas o cambiar la configuración de la acción. Puede crear y modificar manualmente sus propias reglas de firma personalizadas. Los cambios se aplican a todos los perfiles que están configurados actualmente para utilizar este objeto de firma.
- Puede configurar firmas para detectar infracciones en varios tipos de cargas útiles, como HTML, XML, JSON y GWT.
- Puede exportar un objeto de firmas configurado e importarlo a otro dispositivo Citrix ADC para facilitar la replicación de las reglas de firma personalizadas.

Las firmas son patrones asociados a una vulnerabilidad conocida. Puede utilizar la protección de firmas para identificar el tráfico que intenta explotar estas vulnerabilidades y realizar acciones específicas.

Las firmas se organizan en categorías. Puede optimizar el rendimiento y reducir la sobrecarga de procesamiento activando solo las reglas de las categorías adecuadas para proteger la aplicación.

Configuración manual de la función de firmas

August 20, 2021

Para utilizar firmas para proteger los sitios web, debe revisar las reglas y habilitar y configurar las que quiere aplicar. Las reglas están inhabilitadas de forma predeterminada. Citrix recomienda habilitar todas las reglas aplicables al tipo de contenido que utiliza su sitio web.

Para configurar manualmente la función de firmas, utilice un explorador para conectarse a la GUI. A continuación, cree un objeto de firmas a partir de una plantilla integrada, un objeto de firmas existente o importando un archivo. A continuación, configure el nuevo objeto firmas como se explica en Configuración o modificación de un objeto Signatures.

Adición o eliminación de un objeto de firma

April 21, 2022

Puede agregar un nuevo objeto de firma a Web App Firewall de las siguientes maneras:

- Copiar una plantilla integrada.
- Copiar un objeto de firmas existente.
- Importar un objeto de firmas desde un archivo externo.

El archivo de firma incluye el uso de la CPU, el último año aplicable y los detalles del nivel de gravedad. Puede ver el uso de la CPU, el último año y el nivel de gravedad de CVE cada vez que un archivo de firma se modifica y se carga periódicamente. Después de observar estos valores, puede decidir habilitar o inhabilitar la firma en el dispositivo.

Debe usar la interfaz gráfica de usuario para copiar una plantilla o un objeto de firmas existente. Puede usar la GUI o la línea de comandos para importar un objeto de firmas. También puede usar la GUI o la línea de comandos para eliminar un objeto de firmas.

Para crear un objeto de firmas a partir de una plantilla

1. Vaya a **Seguridad > Citrix Web App Firewall > Firmas**.
2. En el panel de detalles, seleccione el objeto de firmas que quiere usar como plantilla.

   Las opciones disponibles son:

   - **Firmas predeterminadas.** Contiene las reglas de firmas, las reglas de inyección de SQL y las reglas de scripting de sitios.
   - **Inyección de XPath.** Contiene los patrones de inyección de XPath.
   - **Cualquier objeto de firmas existente.**

   > **Atención:**
   >
   > Si no elige un tipo de firma para usar como plantilla, Web App Firewall le pedirá que cree

> firmas desde cero.

3. Haga clic en **Agregar**.
4. En el cuadro de diálogo Agregar objeto de firmas, escriba un nombre para el nuevo objeto de firmas y, a continuación, haga clic en Aceptar. El nombre puede comenzar con una letra, un número o un símbolo de subrayado, y puede constar de una a 31 letras, números y los símbolos de guión (-), punto (.), almohadilla (#), espacio ( ), en (@), igual (=) y guión bajo (_).
5. Haga clic en **Cerrar**.

Para crear un objeto de firmas mediante la importación de un archivo

1. Vaya a **Seguridad > Citrix Web App Firewall > Firmas**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En el cuadro de diálogo **Agregar objeto de firmas**, seleccione el formato de las firmas que quiere importar.
   - Para importar un archivo de firmas en formato Citrix ADC, seleccione la ficha **Formato nativo**.
   - Para importar un archivo con formato de firmas externas, seleccione la ficha **Formato externo**.
4. Elija el archivo que quiere usar para crear el objeto de firmas.
   - Para importar un archivo de firmas en formato Citrix ADC nativo, en la sección Importar, seleccione Importar desde archivo local o Importar desde URL y, a continuación, escriba o vaya a la ruta o URL del archivo.
   - Para importar un archivo en formato Cenzic, IBM AppScan, Qualys o Whitehat, en la sección XSLT, seleccione Usar archivo XSLT incorporado, Usar archivo local o Referencia desde URL. A continuación, si elige Usar archivo XSLT integrado, seleccione el formato de archivo apropiado de la lista. Si seleccionó Usar archivo local o referencia desde URL, escriba o vaya a la ruta o la URL del archivo.
5. Haga clic en **Agregar** y, a continuación, en **Cerrar**.

Para crear un objeto de firmas mediante la importación de un archivo mediante la línea de comandos

En el símbolo del sistema, escriba los comandos siguientes:

- `import appfw signatures <src> <name> [-xslt <string>] [-comment <string>] [-overwrite] [-merge] [-sha1 <string>]`
- `save ns config`

Ejemplo #1

En el siguiente ejemplo, se crea un objeto signatures a partir de un archivo denominado signatures.xml y se le asigna el nombre MySignatures.

```
import appfw signatures local:signatures.xml MySignatures
save ns config
<!--NeedCopy-->
```

Para eliminar un objeto de firmas mediante la interfaz gráfica de usuario

1. Vaya a **Seguridad > Citrix Web App Firewall > Firmas**.
2. En el panel de detalles, seleccione el objeto de firmas que quiere eliminar.
3. Haga clic en **Quitar**.

Para eliminar un objeto de firmas mediante la línea de comandos

En el símbolo del sistema, escriba los comandos siguientes:

- `rm appfw signatures <name>`
- `save ns config`

Configuración o modificación de un objeto de firmas

August 20, 2021

Configurar un objeto de firmas después de crearlo, o modificar un objeto de firmas existente, para habilitar o inhabilitar categorías de firmas o firmas específicas, y configurar cómo responde el Web App Firewall cuando una firma coincide con una conexión.

Para configurar o modificar un objeto de firmas

1. Vaya a **Seguridad > Citrix Web App Firewall > Firmas**.
2. En el panel de detalles, seleccione el objeto de firmas que quiere configurar y, a continuación, haga clic en **Abrir**.
3. En el cuadro de diálogo **Modificar objeto de firmas**, defina las opciones **Mostrar criterios de filtro** a la izquierda para mostrar los elementos de filtro que quiere configurar.

Al modificar estas opciones, los resultados solicitados se muestran en la ventana Resultados filtrados de la derecha.

- Para mostrar solo las categorías de firmas seleccionadas, active o desactive las casillas de verificación de categoría de firma adecuadas. Las categorías de firmas son:

Nombre	Tipo de ataque contra el que esta firma protege
CGI	Scripts CGI. Incluye scripts de shell de Perl y UNIX.
cliente	Exploradores y otros clientes.
Coldfusion	sitios web que utilizan el servidor de aplicaciones ColdFusion de Adobe Systems.
página principal	sitios web que utilizan el servidor FrontPage de Microsoft.
iis	sitios web que utilizan Microsoft Internet Information Server (IIS).
Misc	Ataques varios.
php	sitios web que usan PHP
web-activex	sitios web que contienen controles ActiveX.
puntales web	sitios web que contienen puntales Apache, que son applets basados en java-ee.

- Para mostrar solo las firmas que tienen activadas acciones de comprobación específicas, active la casilla de verificación ON para cada una de esas acciones, desactive las casillas de verificación ON para las demás acciones y desactive todas las casillas de verificación OFF. Para mostrar solo las firmas que tengan desactivada una acción de comprobación específica, active sus respectivas casillas de verificación OFF y desactive todas las casillas de verificación Activadas. Para mostrar firmas independientemente de si tienen activada o desactivada una acción de comprobación, active o desactive las casillas de verificación Activada y Desactivada de dicha acción. Las acciones de comprobación son:

Criterio	Descripción
Habilitado	La firma está habilitada. El Web App Firewall solo comprueba si hay firmas habilitadas cuando procesa el tráfico.
Bloquear	Las conexiones que coinciden con esta firma están bloqueadas.

Criterio	Descripción
Registro	Se produce una entrada de registro para cualquier conexión que coincida con esta firma.
Estadísticas	El Web App Firewall incluye cualquier conexión que coincida con esta firma en las estadísticas que genera para esa comprobación.

- Para mostrar solo las firmas que contienen una cadena específica, escriba la cadena en el cuadro de texto bajo los criterios de filtro y, a continuación, haga clic en Buscar.
- Para restablecer todos los criterios de filtro de visualización a la configuración predeterminada y mostrar todas las firmas, haga clic en Mostrar todo.

4. Para obtener información acerca de una firma específica, seleccione la firma y, a continuación, haga clic en la flecha doble azul del campo Más. Aparece el cuadro de mensaje Detalle de vulnerabilidad de regla de firma. Contiene información sobre el propósito de la firma y proporciona enlaces a información externa basada en web acerca de la vulnerabilidad o vulnerabilidades que aborda esta firma. Para acceder a un vínculo externo, haga clic en la flecha doble azul situada a la izquierda de la descripción de ese vínculo.
5. Configure los valores de una firma seleccionando las casillas de verificación correspondientes.
6. Si desea agregar una regla de firma local al objeto firmas o modificar una regla de firma local existente, consulte Editor de firmas.
7. Si no necesita una inyección SQL, scripts entre sitios o patrones de inyección Xpath, haga clic en Aceptar y, a continuación, haga clic en Cerrar. De lo contrario, en la esquina inferior izquierda del panel de detalles, haga clic en Administrar patrones de scripts SQL/Cross Site Site.
8. En el cuadro de diálogo Administrar patrones de scripts SQL/sitios cruzados, ventana Resultados filtrados, vaya a la categoría de patrón y el patrón que quiera configurar. Para obtener información sobre los patrones de inyección SQL, consulte Comprobación de inyección SQL HTML. Para obtener información sobre los patrones de scripts entre sitios, consulte Comprobación de scripts de sitios cruzados en HTML.
9. Para agregar un nuevo patrón:
   a) Seleccione la rama a la que quiere agregar el nuevo patrón.
   b) Haga clic en el botón **Agregar** directamente debajo de la sección inferior de la ventana **Resultados filtrados**.
   c) En el cuadro de diálogo Crear elemento de firma, rellene el cuadro de texto Elemento con el patrón que quiere agregar. Si va a agregar un patrón de transformación a la rama de reglas

de transformación, en Elementos, rellene el cuadro de texto De con el patrón que quiere cambiar y el cuadro de texto A con el patrón al que quiere cambiar el patrón anterior.

d) Haga clic en **Aceptar**.

10. Para modificar un patrón existente:

    a) En la ventana **Resultados filtrados**, seleccione la rama que contiene el patrón que quiere modificar.
    b) En la ventana de detalles situada debajo de la ventana **Resultados filtrados**, seleccione el patrón que quiere modificar.
    c) Haga clic en **Modificar**.
    d) En el cuadro de diálogo **Modificar elemento de firma**, cuadro de texto **Elemento**, modifique el patrón. Si está modificando un patrón de transformación, puede modificar uno o ambos patrones en Elementos, en los cuadros de texto Desde y Hasta.
    e) Haga clic en **Aceptar**.

11. Para eliminar un patrón, seleccione el patrón que quiere eliminar y, a continuación, haga clic en el botón **Quitar** situado debajo del panel de detalles situado debajo de la ventana **Resultados filtrados**. Cuando se le solicite, confirme su elección haciendo clic en **Cerrar**.

12. Para agregar la categoría de patrones a la rama de scripts entre sitios:

    a) Seleccione la rama a la que quiere agregar la categoría de patrones.
    b) Haga clic en el botón **Agregar** directamente debajo de la ventana **Resultados filtrados**.

    > **Nota:** Actualmente solo puede agregar una categoría, patrones con nombre, a la rama de scripts entre sitios, por lo que después de hacer clic en **Agregar**, debe aceptar la opción predeterminada, que es patrones.

    c) Haga clic en **Aceptar**.

13. Para quitar una rama, seleccione esa rama y, a continuación, haga clic en el botón Eliminar directamente debajo de la ventana **Resultados filtrados**. Cuando se le solicite, confirme su elección haciendo clic en **Aceptar**.

    > **Nota:** Si elimina una rama por defecto, elimina todos los patrones de esa rama. Si lo hace, se pueden desactivar las comprobaciones de seguridad que utilizan esa información.

14. Cuando haya terminado de modificar la inyección SQL, los scripts entre sitios y los patrones de inyección XPath, haga clic en **Aceptar** y, a continuación, en **Cerrar**para volver al cuadro de diálogo **Modificar objeto de firmas**.

15. Haga clic en **Aceptar** en cualquier momento para guardar los cambios y, cuando haya terminado de configurar el objeto de firmas, haga clic en **Cerrar**.

Protección de aplicaciones JSON mediante firmas

August 20, 2021

JavaScript Object Notation (JSON) es un estándar abierto basado en texto derivado del lenguaje de scripts JavaScript. JSON es preferido para la representación legible por humanos de estructuras de datos simples y matrices asociativas, llamadas objetos. Sirve como una alternativa a XML y se utiliza principalmente para transmitir estructuras de datos serializados para comunicarse con aplicaciones web. Los archivos JSON normalmente se guardan con una extensión.json.

La carga JSON normalmente se envía con el tipo MIME especificado como **application/json**. Los otros tipos de contenido "estándar" para JSON son:

- **application/x-javascript**
- **text/javascript**
- **text/x-javascript**
- **text/x-json**

Uso de las firmas de Citrix Web App Firewall para proteger las aplicaciones JSON

Para permitir solicitudes JSON, el dispositivo está preconfigurado con el tipo de contenido JSON como se muestra en el siguiente resultado de show-command:

```
> sh appfw jsonContentType
1)      JSONContenttypevalue:  "^application/json$" IsRegex:  REGEX
Done
<!--NeedCopy-->
```

Citrix Web App Firewall procesa el cuerpo de publicación solo para los siguientes tipos de contenido:

- **application/x-www-form-urlencoded**
- **multipart/form-data**
- **text/x-gwt-rpc**

Las solicitudes que se reciben con otros encabezados de tipo de contenido incluyendo application/json (o cualquier otro tipo de contenido permitido) se reenvían al back-end después de la inspección de encabezado. El cuerpo de publicación en dichas solicitudes no se inspecciona en busca de infracciones de comprobación de seguridad, incluso cuando las comprobaciones de seguridad del perfil, como SQL o scripts entre sitios están habilitadas.

Con el fin de proteger las aplicaciones JSON y detectar infracciones, se pueden usar firmas de Web App Firewall. Todas las solicitudes que contienen el encabezado de tipo de contenido permitido son

procesadas por Web App Firewall para la coincidencia de firmas. Puede agregar sus propias reglas de firma personalizadas para procesar la carga útil JSON para realizar varias inspecciones de comprobación de seguridad (por ejemplo, scripts entre sitios, SQL y coherencia de campo), para detectar infracciones en los encabezados, así como en el cuerpo de la publicación, y realizar las acciones especificadas.

> **Sugerencia**
>
> A diferencia de los otros valores predeterminados incorporados, el tipo de contenido JSON preconfigurado se puede modificar o eliminar mediante la CLI o la GUI (GUI). Si las solicitudes legítimas para aplicaciones JSON se bloquean y desencadenan violaciones de tipo de contenido, compruebe que el valor del tipo de contenido está configurado con precisión. Para obtener más información sobre cómo Web App Firewall procesa el encabezado de tipo de contenido, consulte Protección de tipos de contenido

Para agregar o quitar el tipo de contenido JSON mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba uno de los siguientes comandos:

```
add appfw jsonContentType ^application/json$ IsRegEx REGEX
```

```
rm appfw JSONContentType ”^application/json$”
```

Para administrar tipos de contenido JSON mediante la interfaz gráfica de usuario

Vaya a **Seguridad** > **Web App Firewall** y, en la sección **Configuración**, seleccione **Administrar tipos de contenido JSON**.

En el panel **Configurar Web App Firewall JSON Content Type**, agregue, modifique o elimine tipos de contenido JSON para que se adapten a las necesidades de sus aplicaciones.

Configurar la protección de firmas para detectar ataques en la carga JSON

Además de un tipo de contenido JSON válido, debe configurar firmas para especificar los patrones que, cuando se detectan en una solicitud JSON, indican una infracción de seguridad. Las acciones especificadas, como bloque y registro, se realizan cuando una solicitud entrante activa una coincidencia para todos los patrones de destino en la regla de firma.

Para agregar una regla de firma personalizada, Citrix recomienda utilizar la GUI. Vaya a **Sistema** > **Seguridad** > **Web App Firewall** > **Firmas**. Haga doble clic en el objeto de firma de destino para acceder al panel **Modificar firmas de Web App Firewall**. Haga clic en el botón **Agregar** para configurar las acciones, la categoría, la cadena de registro, los patrones de reglas, etc. Aunque Web App Firewall

inspecciona toda la carga útil de tipo de contenido permitida para que coincida con la firma, puede optimizar el procesamiento especificando la expresión JSON en la regla. Cuando **agregue** un nuevo patrón de regla, seleccione **Expresión** en las opciones desplegables de **Coincidencia** y proporcione la expresión de coincidencia de destino de su carga útil JSON para identificar las solicitudes específicas que deben inspeccionarse. Una expresión debe comenzar con un **TEXT.** prefijo. Puede agregar otros patrones de regla para especificar patrones de coincidencia adicionales para identificar el ataque.

En el ejemplo siguiente se muestra una regla de firma. Si se detecta cualquier etiqueta de script entre sitios en el cuerpo POST de la carga JSON que coincida con la expresión XPATH_JSON especificada, se activa una coincidencia de firma.

Ejemplo de una firma para detectar scripts entre sitios en carga útil JSON

```
<SignatureRule actions="log,stats" category="JSON" enabled="ON" id="
    1000001" severity="" source="" type="" version="1">

  <PatternList>

    <RequestPatterns>

      <Pattern>

        <Location area="HTTP_POST_BODY"/>

        <Match type="Expression">TEXT.XPATH_JSON(xp%/glossary/title%).
            CONTAINS("example glossary")</Match>

      </Pattern>

      <Pattern>

        <Location area="HTTP_METHOD"/>

        <Match type="LITERAL">POST</Match>

      </Pattern>

      <Pattern>

        <Location area="HTTP_POST_BODY"/>

        <Match type="CrossSiteScripting"/>

```



```
29          </Pattern>
30
31        </RequestPatterns>
32
33     </PatternList>
34
35     <LogString>Cross-site scripting violation detected in json payload</
          LogString>
36
37     <Comment/>
38
39  </SignatureRule>
40  <!--NeedCopy-->
```

Ejemplo de la carga útil

La siguiente carga activa la coincidencia de firma, ya que incluye la etiqueta de script entre sitios **<Gotcha!!>**.

```
1  {
2   ”glossary”: {
3   ”title”: ”example glossary”,”GlossDiv”: {
4   ”title”: ”S”,”GlossList”: {
5   ”GlossEntry”: {
6   ”ID”: ”SGML”,”SortAs”: ”SGML”,”GlossTerm”: ”Standard Generalized
       Markup Language”,”Acronym”: ”SGML”,”Abbrev”: ”ISO 8879:1986”,”
       GlossDef”: {
7   ”para”: ”A meta-markup language, used to create markup languages \*\*<
       Gotcha!!>\*\* such as DocBook.”,”GlossSeeAlso”: [”GML”, ”XML”] }
8   ,”GlossSee”: ”markup” }
9    }
10   }
11   }
12   }
13
14  <!--NeedCopy-->
```

Ejemplo del mensaje de registro


```
1 Aug 21 12:21:42 <local0.info> 10.217.31.239 08/21/2015:23:21:42 GMT ns
     0-PPE-1 : APPFW APPFW_SIGNATURE_MATCH 1471 0 :  10.217.253.62 990-
     PPE0 NtJnVMNnvPeQJnaUzXYW/GTvAQsA010 prof1 http://10.217.31.212/FFC/
     login_post.php Signature violation rule ID 1000001: cross-site
     scripting violation detected in json payload  <not blocked>
2 <!--NeedCopy-->
```

> **Nota**
>
> Si envía la misma carga después de eliminar la etiqueta de script entre sitios (**<Gotcha!!>**), la coincidencia de regla de firma no se activa.

Resumen

- Para proteger la carga útil de JSON, utilice firmas de Web App Firewall para detectar scripts entre sitios, SQL y otras infracciones.
- Compruebe que el tipo de contenido JSON esté configurado en el dispositivo como el tipo de contenido permitido.
- Asegúrese de que el tipo de contenido de la carga útil coincida con el tipo de contenido JSON configurado.
- Asegúrese de que todos los patrones configurados en la regla de firma coinciden con la infracción de firma que se va a desencadenar.
- Cuando agrega una regla de firma, DEBE tener al menos un patrón de regla para que coincida con la expresión en la carga útil JSON. Todas las expresiones PI de las reglas de firma deben comenzar con el prefijo TEXTO. y deben ser booleanas.

Proteja el tipo de contenido de aplicaciones o JSON con SQL y carga útil codificada por scripts entre sitios mediante directivas y firmas

Citrix Web App Firewall puede proteger el tipo de contenido JSON o aplicación mediante directivas y firmas.

Inspeccionar el tipo de contenido JSON o aplicación para la inyección SQL mediante directivas

Debe agregar las siguientes directivas y vincularlo al servidor virtual globalmente para admitir la inyección SQL.

```
add appfw policy sqli_1 HTTP.REQ.BODY(10000).SET_TEXT_MODE(IGNORECASE).
SET_TEXT_MODE(URLENCODED).DECODE_USING_TEXT_MODE.REGEX_MATCH(re##(((\\A)
|(?<=[^a-zA-Z0-9_])))(select|insert|delete|update|drop|create|alter|grant
|revoke|commit|rollback|shutdown|union|intersect|minus|case|decode|where
```



```
|group|begin|join|exists|distinct|add|modify|constraint|null|like|exec|
execute|char|or|and|sp_sdidebug)((Z)|(?=[^a-zA-Z0-9_]))##)APPFW_BLOCK

add appfw policy sqli_2 HTTP.REQ.BODY(10000).SET_TEXT_MODE(IGNORECASE).
SET_TEXT_MODE(URLENCODED).DECODE_USING_TEXT_MODE.REGEX_MATCH(re##((\\A)
|(?<=[^a-zA-Z0-9_]))(xp_availablemedia|xp_cmdshell|xp_deletemail|xp_dirtree
|xp_dropwebtask|xp_dsninfo|xp_enumdsn|xp_enumerrorlogs|xp_enumgroups|
xp_enumqueuedtasks|xp_eventlog|xp_findnextmsg|xp_fixeddrives|xp_getfiledetails
|xp_getnetname|xp_grantlogin|xp_logevent|xp_loginconfig|xp_logininfo|
xp_makewebtask|xp_msver|xp_regread|xp_perfend|xp_perfmonitor|xp_perfsample
|xp_perfstart|xp_readerrorlog|xp_readmail|xp_revokelogin|xp_runwebtask|
xp_schedulersignal|xp_sendmail|xp_servicecontrol|xp_snmp_getstate|xp_snmp_raisetrap
|xp_sprintf|xp_sqlinventory|xp_sqlregister|xp_sqltrace|xp_sscanf|xp_startmail
|xp_stopmail|xp_subdirs|xp_unc_to_drive)((Z)|(?=[^a-zA-Z0-9_]))##)APPFW_BLOCK


add appfw policy sqli_3 HTTP.REQ.BODY(10000).SET_TEXT_MODE(IGNORECASE).
SET_TEXT_MODE(URLENCODED).DECODE_USING_TEXT_MODE.REGEX_MATCH(re##((\\A)
|(?<=[^a-zA-Z0-9_]))(sysobjects|syscolumns|MSysACEs|MSysObjects|MSysQueries
|MSysRelationships)((Z)|(?=[^a-zA-Z0-9_]))##)APPFW_BLOCK

add appfw policy sqli_4 HTTP.REQ.BODY(10000).SET_TEXT_MODE(IGNORECASE).
SET_TEXT_MODE(URLENCODED).DECODE_USING_TEXT_MODE.REGEX_MATCH(re##((\\A
)|(?<=[^a-zA-Z0-9_]))(SYS\.USER_OBJECTS|SYS\.TAB|SYS\.USER_TABLES|SYS\.
USER_VIEWS|SYS\.ALL_TABLES|SYS\.USER_TAB_COLUMNS|SYS\.USER_CONSTRAINTS|SYS
\.USER_TRIGGERS|SYS\.USER_CATALOG|SYS\.ALL_CATALOG|SYS\.ALL_CONSTRAINTS|SYS
\.ALL_OBJECTS|SYS\.ALL_TAB_COLUMNS|SYS\.ALL_TAB_PRIVS|SYS\.ALL_TRIGGERS|SYS
\.ALL_USERS|SYS\.ALL_VIEWS|SYS\.USER_ROLE_PRIVS|SYS\.USER_SYS_PRIVS|SYS\.
USER_TAB_PRIVS)((Z)|(?=[^a-zA-Z0-9_]))##)APPFW_BLOCK
```

Inspeccionar el tipo de contenido JSON o aplicación mediante firmas

Puede agregar las siguientes reglas de firma al objeto de firma en el perfil de firewall de la aplicación para admitir la inyección SQL para el tipo de contenido JSON.

> **Nota:**
>
> Las firmas de los cuerpos de las publicaciones requieren un uso intensivo de la CPU.

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <!-- Copyright 2013-2018 Citrix Systems, Inc. All rights reserved. -->
```



```
<SignaturesFile schema_version="6" version="0" minor_schema_version="0"
    >
     <Signatures>
         <SignatureRule id="4000000" enabled="ON" actions="log,block"
            category="sql" source="" severity="" type="" version="1"
            sourceid="" harmscore="">
             <PatternList>
                 <RequestPatterns>
                     <Pattern>
                         <Location area="HTTP_POST_BODY"/>
                         <Match type="Expression">TEXT.SET_TEXT_MODE(
                            IGNORECASE).SET_TEXT_MODE(URLENCODED).
                            DECODE_USING_TEXT_MODE.REGEX_MATCH(re#(((\A)
                            |(?<=[^a-zA-Z0-9_])))(select|insert|delete|
                            update|drop|create|alter|grant|revoke|commit
                            |rollback|shutdown|union|intersect|minus|
                            case|decode|where|group|begin|join|exists|
                            distinct|add|modify|constraint|null|like|
                            exec|execute|char|or|and|sp_sdidebug)((
Z)|(?=[^a-zA-Z0-9_]))#)</Match>
                     </Pattern>
                     <Pattern type="fastmatch">
                         <Location area="HTTP_METHOD"/>
                         <Match type="LITERAL">T</Match>
                     </Pattern>
                 </RequestPatterns>
             </PatternList>
             <LogString>sql Injection</LogString>
             <Comment/>
         </SignatureRule>
         <SignatureRule id="4000001" enabled="ON" actions="log,block"
            category="sql" source="" severity="" type="" version="1"
            sourceid="" harmscore="">
             <PatternList>
                 <RequestPatterns>
                     <Pattern>
                         <Location area="HTTP_POST_BODY"/>
                         <Match type="Expression">TEXT.SET_TEXT_MODE(
                            IGNORECASE).SET_TEXT_MODE(URLENCODED).
                            DECODE_USING_TEXT_MODE.REGEX_MATCH(re#((\A)
                            |(?<=[^a-zA-Z0-9_]))(xp_availablemedia|
                            xp_cmdshell|xp_deletemail|xp_dirtree|
                            xp_dropwebtask|xp_dsninfo|xp_enumdsn|
                            xp_enumerrorlogs|xp_enumgroups|
                            xp_enumqueuedtasks|xp_eventlog|
```

```
                                xp_findnextmsg|xp_fixeddrives|
                                xp_getfiledetails|xp_getnetname|
                                xp_grantlogin|xp_logevent|xp_loginconfig|
                                xp_logininfo|xp_makewebtask|xp_msver|
                                xp_regread|xp_perfend|xp_perfmonitor|
                                xp_perfsample|xp_perfstart|xp_readerrorlog|
                                xp_readmail|xp_revokelogin|xp_runwebtask|
                                xp_schedulersignal|xp_sendmail|
                                xp_servicecontrol|xp_snmp_getstate|
                                xp_snmp_raisetrap|xp_sprintf|xp_sqlinventory
                                |xp_sqlregister|xp_sqltrace|xp_sscanf|
                                xp_startmail|xp_stopmail|xp_subdirs|
                                xp_unc_to_drive)((
Z)|(?=[^a-zA-Z0-9_]))#)</Match>
                        </Pattern>
                        <Pattern type="fastmatch">
                            <Location area="HTTP_METHOD"/>
                            <Match type="LITERAL">T</Match>
                        </Pattern>
                    </RequestPatterns>
                </PatternList>
                <LogString>sql Injection</LogString>
                <Comment/>
            </SignatureRule>
            <SignatureRule id="4000002" enabled="ON" actions="log,block"
               category="sql" source="" severity="" type="" version="1"
               sourceid="" harmscore="">
                <PatternList>
                    <RequestPatterns>
                        <Pattern>
                            <Location area="HTTP_POST_BODY"/>
                            <Match type="Expression">TEXT.SET_TEXT_MODE(
                               IGNORECASE).SET_TEXT_MODE(URLENCODED).
                               DECODE_USING_TEXT_MODE.REGEX_MATCH(re#((\A)
                               |(?<=[^a-zA-Z0-9_]))(sysobjects|syscolumns|
                               MSysACEs|MSysObjects|MSysQueries|
                               MSysRelationships)((
Z)|(?=[^a-zA-Z0-9_]))#)</Match>
                        </Pattern>
                        <Pattern type="fastmatch">
                            <Location area="HTTP_METHOD"/>
                            <Match type="LITERAL">T</Match>
                        </Pattern>
                    </RequestPatterns>
                </PatternList>
```



```
53              <LogString>sql Injection</LogString>
54              <Comment/>
55          </SignatureRule>
56          <SignatureRule id="4000003" enabled="ON" actions="log,block"
               category="sql" source="" severity="" type="" version="1"
               sourceid="" harmscore="">
57              <PatternList>
58                  <RequestPatterns>
59                      <Pattern>
60                          <Location area="HTTP_POST_BODY"/>
61                          <Match type="Expression">TEXT.SET_TEXT_MODE(
                               IGNORECASE).SET_TEXT_MODE(URLENCODED).
                               DECODE_USING_TEXT_MODE.REGEX_MATCH(re#((\A)
                               |(?<=[^a-zA-Z0-9_]))(SYS.USER_OBJECTS|SYS.
                               TAB|SYS.USER_TABLES|SYS.USER_VIEWS|SYS.
                               ALL_TABLES|SYS.USER_TAB_COLUMNS|SYS.
                               USER_CONSTRAINTS|SYS.USER_TRIGGERS|SYS.
                               USER_CATALOG|SYS.ALL_CATALOG|SYS.
                               ALL_CONSTRAINTS|SYS.ALL_OBJECTS|SYS.
                               ALL_TAB_COLUMNS|SYS.ALL_TAB_PRIVS|SYS.
                               ALL_TRIGGERS|SYS.ALL_USERS|SYS.ALL_VIEWS|SYS
                               .USER_ROLE_PRIVS|SYS.USER_SYS_PRIVS|SYS.
                               USER_TAB_PRIVS)((
62  Z)|(?=[^a-zA-Z0-9_]))#)</Match>
63                      </Pattern>
64                      <Pattern type="fastmatch">
65                          <Location area="HTTP_METHOD"/>
66                          <Match type="LITERAL">T</Match>
67                      </Pattern>
68                  </RequestPatterns>
69              </PatternList>
70              <LogString>sql Injection</LogString>
71              <Comment/>
72          </SignatureRule>
73      </Signatures>
74  </SignaturesFile>
75
76  <!--NeedCopy-->
```

Actualizar un objeto de firma

August 20, 2021

Debe actualizar los objetos de firmas con frecuencia para asegurarse de que el Web App Firewall proporciona protección contra las amenazas actuales. Debe actualizar regularmente tanto las firmas predeterminadas de Web App Firewall como las firmas que importe desde una herramienta de análisis de vulnerabilidades admitida.

Citrix actualiza regularmente las firmas predeterminadas para Web App Firewall. Puede actualizar las firmas predeterminadas de forma manual o automática. En cualquier caso, solicite a su representante de Citrix o a su distribuidor Citrix la dirección URL para acceder a las actualizaciones. Puede habilitar las actualizaciones automáticas de las firmas de formato nativo de Citrix en los cuadros de diálogo "Configuración del motor" y "Configuración de actualización automática de firmas".

La mayoría de los fabricantes de herramientas de análisis de vulnerabilidades actualizan regularmente las herramientas. La mayoría de los sitios web también cambian frecuentemente. Debe actualizar la herramienta y volver a analizar los sitios web regularmente, exportando las firmas resultantes a un archivo e importándolas a la configuración de Web App Firewall.

> **Sugerencia**
>
> Al actualizar las firmas de Web App Firewall desde la línea de comandos de Citrix ADC, primero debe actualizar las firmas predeterminadas y, a continuación, ejecutar más comandos de actualización para actualizar cada archivo de firmas personalizado basado en las firmas predeterminadas. Si no actualiza primero las firmas predeterminadas, un error de coincidencia de versión impide la actualización de los archivos de firmas personalizadas.
>
> **Nota**
>
> Lo siguiente se aplica a la combinación de un objeto de firma de terceros con un objeto de firma definido por el usuario con reglas nativas y reglas agregadas por el usuario:
>
> Cuando una versión 0 se fusiona con un nuevo archivo importado, las firmas resultantes permanecen como versión 0.
>
> Esto significa que todas las reglas nativas (o integradas) del archivo importado se ignorarán después de la fusión. Esto es para garantizar que las firmas de la versión 0 se mantengan tal como está después de una combinación.
>
> Para incluir las reglas nativas en el archivo importado para la combinación, primero debe actualizar las firmas existentes de la versión 0 antes de la combinación. Esto significa que debe abandonar la naturaleza de la versión 0 de las firmas existentes.
>
> Cuando hay una actualización de la versión de Citrix ADC, el archivo "default_signatures.xml" se agrega a la nueva compilación y el archivo "updated_signature.xml" se elimina de la versión anterior. Después de la actualización, si la función de actualización automática de firma está habilitada, el dispositivo actualiza la firma existente a la versión más reciente de la compilación y genera el archivo "updated_signature.xml".

Para actualizar las firmas de Web App Firewall desde el origen mediante la línea de comandos

En el símbolo del sistema, escriba los siguientes comandos:

- `update appfw signatures <name> [-mergedefault]`
- `save ns config`

Ejemplo

En el ejemplo siguiente se actualiza el objeto signatures denominado MySignatures desde el objeto signatures predeterminado, combinando nuevas firmas en el objeto signatures predeterminado con las firmas existentes. Este comando no sobrescribe las firmas creadas por el usuario ni las firmas importadas de otro origen, como una herramienta de análisis de vulnerabilidades aprobada.

```
1 update appfw signatures MySignatures -mergedefault
2 save ns config
3 <!--NeedCopy-->
```

Actualización de un objeto de firmas desde un archivo de formato Citrix

Citrix actualiza regularmente las firmas para Web App Firewall. Debe actualizar regularmente las firmas del Web App Firewall para asegurarse de que el Web App Firewall utiliza la lista más reciente. Solicite a su representante de Citrix o a su distribuidor Citrix la dirección URL para acceder a las actualizaciones.

Para actualizar un objeto de firmas desde un archivo de formato Citrix mediante la línea de comandos

En el símbolo del sistema, escriba los siguientes comandos:

- `update appfw signatures <name> [-mergeDefault]`
- `save ns config`

Para actualizar un objeto de firmas desde un archivo de formato Citrix mediante la interfaz gráfica de usuario

1. Vaya a **Seguridad** > **Web App Firewall** > **Firmas**.
2. En el panel de detalles, seleccione el objeto de firmas que quiere actualizar.
3. En la lista desplegable **Acción**, seleccione **Combinar**.

4. En el cuadro de diálogo **Actualizar objeto de firmas**, elija una de las siguientes opciones.
   - **Importar desde URL**: Seleccione esta opción si descarga actualizaciones de firmas desde una URL web.
   - **Importar desde archivo local**: Seleccione esta opción si importa actualizaciones de firmas desde un archivo en el disco duro local, el disco duro de red u otro dispositivo de almacenamiento.
5. En el área de texto, escriba la dirección URL o escriba o busque el archivo local.
6. Haga clic en **Update**. El archivo de actualización se importa y el cuadro de diálogo Actualizar firmas cambia a un formato casi idéntico al del cuadro de diálogo **Modificar objeto de firmas**. El cuadro de diálogo **Actualizar objeto de firmas** muestra todas las ramas con reglas de firma nuevas o modificadas, patrones de inyección SQL o scripts entre sitios y patrones de inyección XPath, si los hay.
7. Revise y configure las firmas nuevas y modificadas.
8. Cuando haya terminado, haga clic en **Aceptar** y, a continuación, haga clic en **Cerrar**.

Actualización de un objeto de firmas desde una herramienta de análisis de vulnerabilidades compatible

> **Nota:**
>
> Antes de actualizar un objeto de firmas desde un archivo, debe crear el archivo exportando firmas desde la herramienta de análisis de vulnerabilidades.

Para importar y actualizar firmas desde una herramienta de análisis de vulnerabilidades

1. Vaya a **Seguridad** > **Web App Firewall** > **Firmas**.
2. En el panel de detalles, seleccione el objeto de firmas que quiere actualizar y, a continuación, haga clic en **Combinar**.
3. En el cuadro de diálogo **Actualizar objeto de firmas**, en la ficha **Formato externo**, sección Importar, elija una de las siguientes opciones.
   - **Importar desde URL**: Seleccione esta opción si descarga actualizaciones de firmas desde una dirección URL Web.
   - **Importar desde archivo local**: Seleccione esta opción si importa actualizaciones de firmas desde un archivo en el disco duro local o de red u otro dispositivo de almacenamiento.
4. En el área de texto, escriba la dirección URL o busque o escriba la ruta de acceso al archivo local.
5. En la sección XSLT, elija una de las siguientes opciones.
   - **Usar archivo XSLT integrado**: Seleccione esta opción si quiere utilizar un archivo XSLT integrado.
   - **Usar archivo XSLT local**: Elija esta opción para utilizar un archivo XSLT en el equipo local.
   - **Referencia XSLT desde URL**: Seleccione esta opción para importar un archivo XSLT desde una URL web.

6. Si ha elegido Usar archivo XSLT integrado, en la lista desplegable XSLT integrado seleccione el archivo que quiere utilizar de las siguientes opciones:
   - **Cenzic.**
   - **Deep_Security_for_Web_Apps.**
   - **Hewlett_Packard_Enterprise_WebInspect.**
   - **IBM-AppScan-Enterprise.**
   - **IBM-AppScan-Standard.**
   - **Qualys.**
   - **Whitehat.**
7. Haga clic en **Update**. El archivo de actualización se importa y el cuadro de diálogo Actualizar firmas cambia a un formato casi idéntico al del cuadro de diálogo Modificar objeto de firmas, que se describe en Configuración o modificación de un objeto de firmas. El cuadro de diálogo **Actualizar objeto de firmas** muestra todas las ramas con reglas de firma nuevas o modificadas, patrones de inyección SQL o scripts entre sitios y patrones de inyección XPath, si los hay.
8. Revise y configure las firmas nuevas y modificadas.
9. Cuando haya terminado, haga clic en **Aceptar** y, a continuación, haga clic en **Cerrar**.

Actualización automática de firmas

July 15, 2022

La funcionalidad Signature Auto Update del Firewall de aplicaciones web permite al usuario obtener las firmas más recientes para proteger la aplicación web contra nuevas vulnerabilidades. La función de actualización automática proporciona una mejor protección sin necesidad de intervención manual continua para obtener las últimas actualizaciones.

Las firmas se actualizan automáticamente cada hora y no requieren una comprobación periódica de la disponibilidad de la actualización más reciente. Una vez habilitado Signature Auto Update, el dispositivo Citrix ADC se conecta al servidor que aloja las firmas para comprobar si hay una versión más reciente disponible.

Ubicación personalizable

Las firmas más recientes de Application Firewall se alojan en Amazon, que está configurada como URL de firma predeterminada para comprobar la última actualización.

Sin embargo, el usuario tiene la opción de descargar estos archivos de asignación de firmas en su servidor interno. A continuación, el usuario puede configurar una ruta URL de firma diferente para descargar los archivos de asignación de firmas desde un servidor local. Para que funcione la función

de actualización automática, es posible que tenga que configurar el servidor DNS para acceder al sitio externo.

Actualizar firmas

Todos los objetos de firma definidos por el usuario que se crean mediante el objeto de firma predeterminado appfw tienen una versión superior a cero. Si habilita la actualización automática de firma, todas las firmas se actualizan automáticamente.

Si el usuario ha importado firmas con el formato externo como Cenzic o Qualys, las firmas se importan con la versión como cero. Del mismo modo, si el usuario ha creado un objeto de firma mediante la plantilla en blanco, se crea como firma de versión cero. Estas firmas no se actualizan automáticamente, porque es posible que el usuario no esté interesado en la sobrecarga de la administración de las firmas predeterminadas que no se utilizan.

Sin embargo, Web Application Firewall también permite al usuario la flexibilidad de seleccionar manualmente estas firmas y actualizarlas para agregar las reglas de firma predeterminadas a las reglas existentes. Una vez que las firmas se hayan actualizado manualmente, la versión cambia y, a continuación, las firmas también se actualizarán automáticamente junto con las demás firmas.

Configurar la actualización automática de firmas

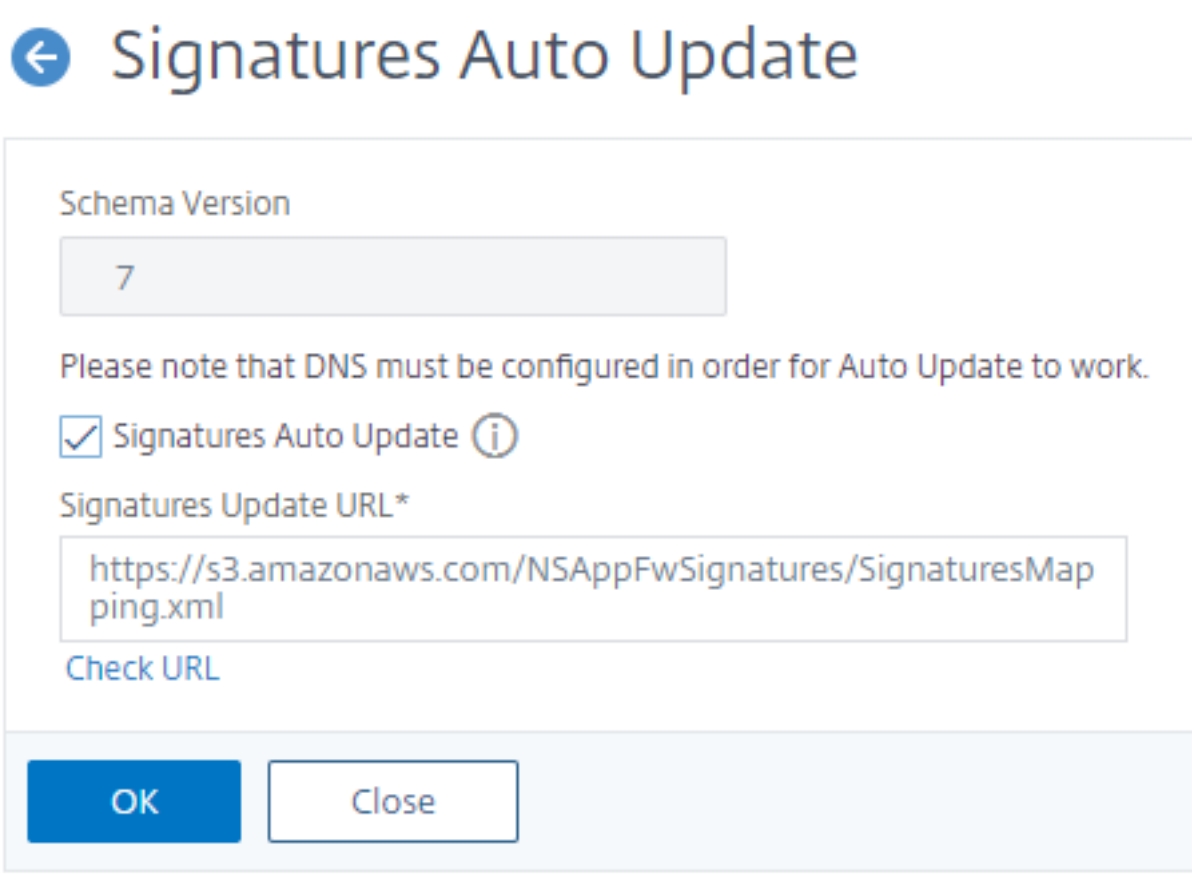
Para configurar la función de actualización automática de firmas mediante la CLI:

En el símbolo del sistema, escriba:

```
1 set appfw settings SignatureAutoUpdate on
2 set appfw settings SignatureUrl https://s3.amazonaws.com/
     NSAppFwSignatures/SignaturesMapping.xml
3 <!--NeedCopy-->
```

Para configurar la actualización automática de firmas mediante la GUI:

1. Vaya a **Seguridad > Citrix Web App Firewall > Firmas**.
2. Seleccione **Configuración de actualización automática** en **Acción**.
3. **Habilite la opción Actualización automática de firmas**.
4. Puede especificar una ruta personalizada para la URL de actualización de firmas, si es necesario. Haga clic en **Restablecer** para restablecer el valor predeterminado `s3.amazonaws.com server`.
5. Haga clic en **Aceptar**.



Actualizar firmas manualmente

Para actualizar manualmente una firma de versión cero o cualquier otra firma definida por el usuario, primero debe obtener la última actualización de las firmas predeterminadas y, a continuación, utilizarla para actualizar la firma definida por el usuario de destino.

Ejecute los siguientes comandos desde la CLI para actualizar un archivo de firma:

```
update appfw signatures "*Default Signatures"
update appfw signatures cenzic -mergedefault
<!--NeedCopy-->
```

> **Nota:**
>
> `Default Signatures` Es distintivo entre mayúsculas Cenzic en el comando anterior es el nombre del archivo de firma que se actualiza.

Importación de firmas predeterminadas sin acceso a Internet

Se recomienda configurar un servidor proxy para que apunte al servidor Amazon (AWS) para obtener la última actualización. Sin embargo, si el dispositivo NetScaler no tiene conexión a Internet a los sitios externos, el usuario puede almacenar los archivos de firma actualizados en un servidor local. A continuación, el dispositivo puede descargar las firmas del servidor local. En este caso, el usuario debe revisar constantemente el **sitio de Amazon** para obtener las últimas actualizaciones. Puede descargar y verificar el archivo de firma con el archivo sha1 correspondiente creado mediante la clave **pública de Citrix** para protegerse contra manipulaciones.

Para copiar los archivos de firmas en un servidor local, realice el siguiente procedimiento:

1. Cree un directorio local, como <MySignatures> en un servidor local.
2. Abra el sitio de AWS.
3. Copie el archivo SignaturesMapping.xml en la carpeta <MySignatures>.

Si abre el archivo SignaturesMapping.xml, podrá ver todos los archivos xml de las firmas y sus correspondientes archivos sha1 para diferentes versiones compatibles. Uno de estos pares se resalta en la siguiente captura de pantalla:

1. Cree un subdirectorio <sigs> en la carpeta <MySignatures>.
2. Copie todos los pares de etiquetas *.xml files listed in the <file> y los archivos *.xml.sha1 enumerados en los etiquetas <sha1> correspondientes del archivo SignaturesMapping.xml en la carpeta <sigs>. A continuación se muestran algunos archivos de ejemplo que se copian en la carpeta <sigs>:

```
https://s3.amazonaws.com/NSAppFwSignatures/sigs/sig-r10.1b86v3s3.xml
https://s3.amazonaws.com/NSAppFwSignatures/sigs/sig-r10.1b86v3s3.xml.sha1
https://s3.amazonaws.com/NSAppFwSignatures/sigs/sig-r10.1b0v3s2.xml
https://s3.amazonaws.com/NSAppFwSignatures/sigs/sig-r10.1b0v3s2.xml.sha1
```

> **Nota:**
>
> Puede asignar cualquier nombre a la carpeta <MySignatures> y puede estar en cualquier ubicación, pero el subdirectorio <sigs> debe ser un subdirectorio de la carpeta <MySignatures> en la que se copia el archivo de asignación. Además, asegúrese de que, como se muestra en SignaturesMapping.xml, el nombre del subdirectorio <sigs> debe tener el nombre exacto y distingue mayúsculas de minúsculas. Todos los archivos de firma y sus correspondientes archivos sha1 deben copiarse en este <sigs> directorio.

Después de duplicar el contenido del servidor web de Amazon alojado al servidor local, cambie la ruta del nuevo servidor web local para configurarlo como SignatureUrl para la actualización automática. Por ejemplo, ejecute el siguiente comando desde la interfaz de línea de comandos del dispositivo:


```
set appfw settings SignatureUrl https://myserver.example.net/
    MySignatures/SignaturesMapping.xml
<!--NeedCopy-->
```

La operación de actualización puede tardar varios minutos, en función del número de firmas que se van a actualizar. Deje tiempo suficiente para que se complete la operación de actualización.

Si se produce un error "Error al acceder a la URL! "mientras configuras, sigue los pasos para resolverlo.

1. Agregue la url `https://myserver.example.net` a para `/netscaler/ns_gui/admin_ui/php/application/controllers/common/utils.php` que la seguridad de la directiva de seguridad de contenido (CSP) no bloquee el acceso a la url. Tenga en cuenta que esta configuración no persiste en una actualización. El usuario tiene que volver a agregarlo después de la actualización.

```
$configuration_view_connect_src = "connect-src 'self' https://app.pendo
    .io https://s3.amazonaws.comhttps://myserver.example.net;";
<!--NeedCopy-->
```

1. El usuario debe configurar el servidor `https://myserver.example.net` web para que responda a los siguientes encabezados CORS para `https://myserver.example.net/MySignatures/SignaturesMapping.xml`

```
Access-Control-Allow-Methods: GET
Access-Control-Allow-Origin: *
Access-Control-Max-Age: 3000
<!--NeedCopy-->
```

Directrices para actualizar firmas

Se utilizan las siguientes pautas para actualizar las firmas:

- Las firmas se actualizan cuando la URL de actualización de firmas tiene un objeto de firma que tiene la misma versión o más reciente.
- Cada regla de firma está asociada a un ID de regla y un número de versión. Por ejemplo: `< SignatureRule id="803"version="16"···>`
- La regla de firma del archivo Firmas entrante con el mismo ID y número de versión que el existente se ignora incluso si tiene patrones o cadenas de registro diferentes.
- Se agrega la regla de firma con un nuevo ID. Todas las acciones y el indicador habilitado se utilizan desde el nuevo archivo.

> **Nota:**
>
> Es posible que deba revisar periódicamente las firmas actualizadas para habilitar estas reglas recién agregadas y cambiar otros ajustes de acción según los requisitos de la aplicación.

- Las reglas con el mismo ID pero con un número de versión más reciente reemplazan a la existente. Se conservan todas las acciones y el indicador habilitado de la regla existente.

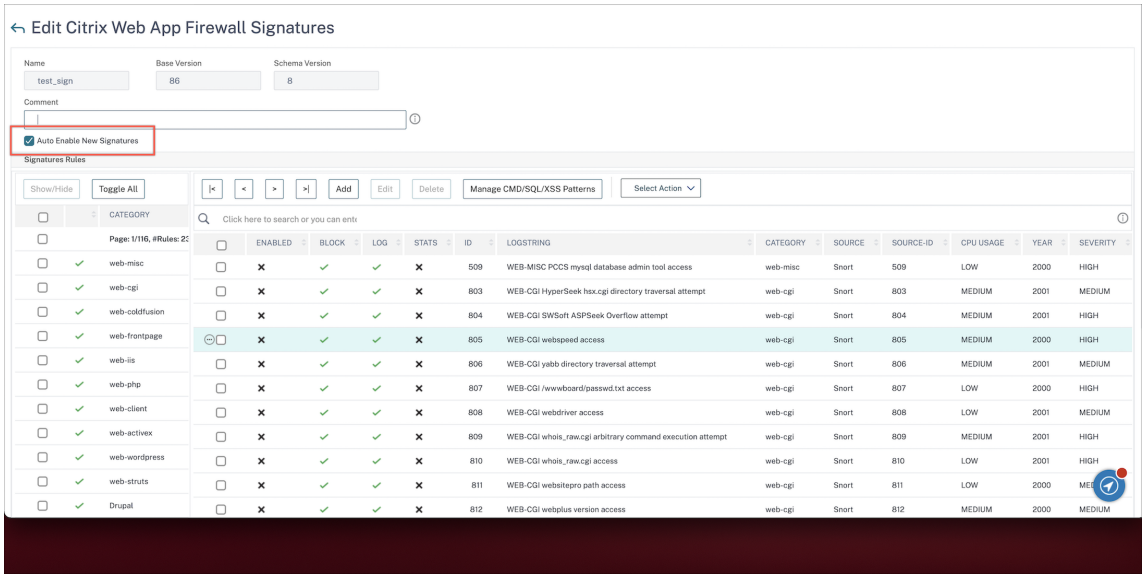
> **Sugerencia:**
>
> Cuando actualiza las firmas desde la CLI, primero debe actualizar las firmas predeterminadas. A continuación, debe agregar comandos de actualización para actualizar cada archivo de firma personalizado basado en las firmas predeterminadas. Si no actualiza primero las firmas predeterminadas, un error de discrepancia de versión impide la actualización del archivo de firmas personalizadas.

Habilitar firmas nuevas automáticamente

A partir de la versión 13.1, compilación 27.x, y posteriores, puede seleccionar **Activar automáticamente nuevas firmas** para permitir que las nuevas reglas predeterminadas de firmas de WAF se habiliten automáticamente después de una actualización.

Habilitación automática de nuevas firmas mediante la GUI

1. Vaya a **Seguridad > Citrix Web App Firewall > Firmas**.
2. Seleccione una firma y haga clic en **Modificar**.
3. Seleccione **Activar automáticamente nuevas firmas**.



Habilitar automáticamente nuevas firmas mediante la CLI

En el símbolo del sistema, escriba:

```
import appfw signatures <src> <name> [-xslt <string>] [-comment <string>]
[-overwrite] [-merge [-preservedefactions]] [-sha1 <string>] [-VendorType
Snort] [-autoEnableNewSignatures ( ON | OFF )]
```

Ejemplo:

```
import signatures http://www.example.com/ns/signatures.xml my-signature -
autoEnableNewSignatures ON
```

Integración de reglas de Snort

August 20, 2021

Con ataques maliciosos en aplicaciones web, es importante proteger su red interna. Los datos maliciosos no solo afectan a sus aplicaciones web a nivel de interfaz, sino que los paquetes maliciosos también llegan a la capa de aplicación. Para superar estos ataques, es importante configurar un sistema de detección y prevención de intrusiones que examine su red interna.

Las reglas de Snort se integran en el dispositivo para examinar los ataques maliciosos en paquetes de datos en la capa de aplicación. Puede descargar las reglas de snort y convertirlas en reglas de firmas WAF. Las firmas tienen una configuración basada en reglas que puede detectar actividades maliciosas como ataques DOS, desbordamientos de búfer, escaneos de puertos ocultos, ataques CGI, sondas SMB e intentos de huellas dactilares del SO. Al integrar las reglas de Snort, puede fortalecer su solución de seguridad en la interfaz y en el nivel de la aplicación.

Configurar reglas de snort

La configuración comienza descargando primero las reglas de Snort y luego importándolas a las reglas de firma WAF. Una vez que haya convertido las reglas en firmas WAF, las reglas se pueden utilizar como comprobaciones de seguridad WAF. Las reglas de firma basadas en snort examinan el paquete de datos entrante para detectar si hay ataques maliciosos en la red.

Se agrega un nuevo parámetro, “VendorType” al comando import para convertir las reglas de Snort en firmas WAF.

El parámetro “VendorType” se establece en Snort solo para las reglas de Snort.

Descargar reglas de snort mediante la interfaz de comandos

Puede descargar las reglas de Snort como un archivo de texto desde la siguiente URL:


```
https://www.snort.org/downloads/community/snort3-community-rules.tar.gz
```

Importar reglas de snort mediante la interfaz de comandos

Después de descargar, puede importar las reglas de Snort en el dispositivo.

En el símbolo del sistema, escriba:

```
import appfw signatures <src> <name> [-xslt <string>] [-comment <string>]
[-overwrite] [-merge [-preservedefactions]] [-sha1 <string>] [-VendorType
Snort]
```

Ejemplo:

```
import appfw signatures http://www.example.com/ns/signatures.xml sig-snort -
comment "signatures from snort rules" -VendorType snort
```

Cliente:

Sr.c. URL (protocolo, host, ruta de acceso y nombre de archivo) para la ubicación en la que almacenar el objeto de firmas importadas.

> **Nota:**
>
> Se produce un error en la importación si el objeto que se va a importar está en un servidor HTTPS que requiere autenticación de certificado de cliente para el acceso. Argumento obligatorio de longitud máxima: 2047

Name. Nombre que se asignará al objeto de firmas en Citrix ADC. Argumento obligatorio de longitud máxima: 31

Comentario. Descripción de cómo conservar información sobre el objeto firmas. Longitud máxima: 255
sobrescribir. Sobrescribir cualquier objeto de firmas existente del mismo nombre.

Fusionar. Combina Firma existente con nuevas reglas de firma.

Preservedefactions. Conserva las acciones de def de las reglas de firma.

VendorType. Proveedor externo para generar las firmas WAF. Valores posibles: Snort.

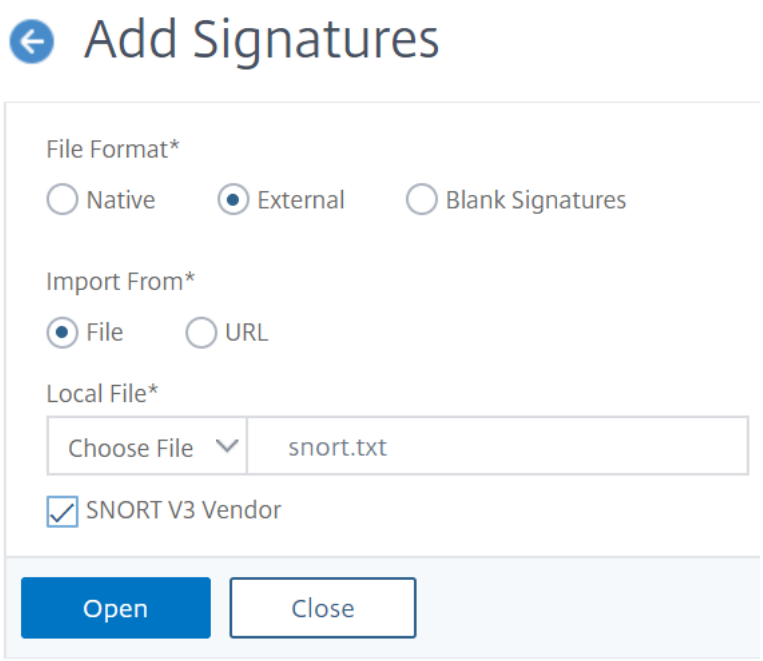
Configurar reglas de snort mediante la GUI de Citrix ADC

La configuración de GUI para las reglas de Snort es similar a la configuración de otros escáneres externos de aplicaciones web como Cenzic, Qualys, Whitehat.

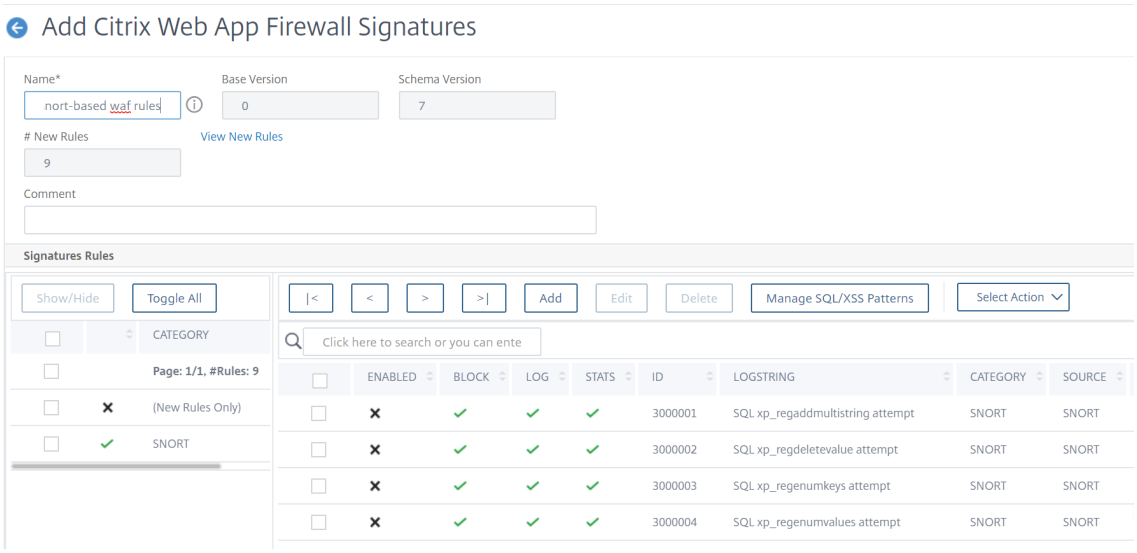
Siga los pasos que se indican a continuación para configurar Snort:

1. Vaya a **Configuración > Seguridad > Citrix Web App Firewall > Firmas**.

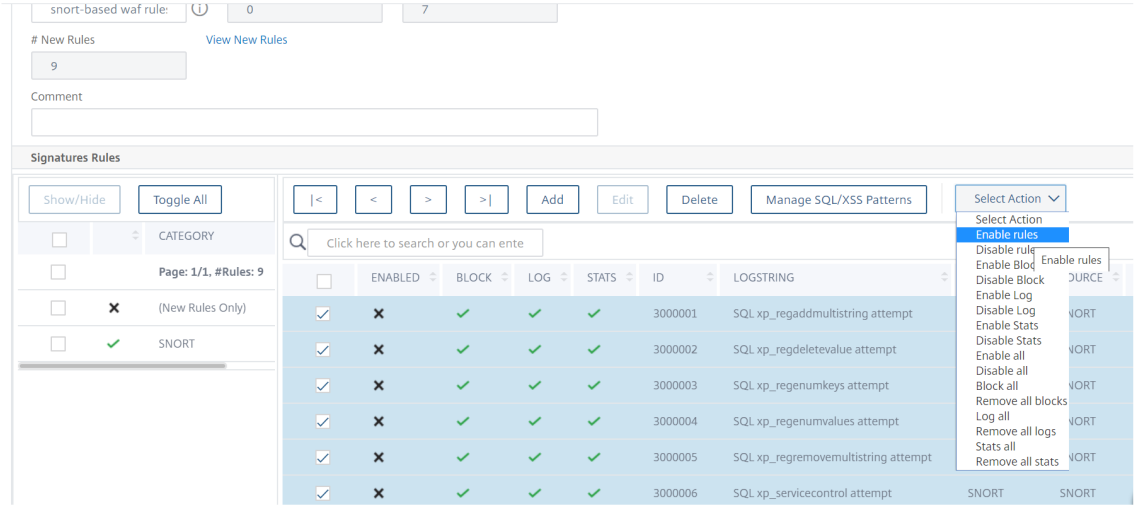
2. En la página **Firmas**, haga clic en **Agregar**.
3. En la página **Agregar firmas**, establezca los siguientes parámetros para configurar las reglas de Snort.
   a) Formato de archivo. Seleccione el formato de archivo como externo.
   b) Importar desde. Seleccione la opción de importación como archivo de snort o URL para introducir la URL.
   c) Snort V3 proveedor. Active la casilla de verificación para importar reglas de Snort desde un archivo o desde una dirección URL.
4. Haga clic en **Abrir**.



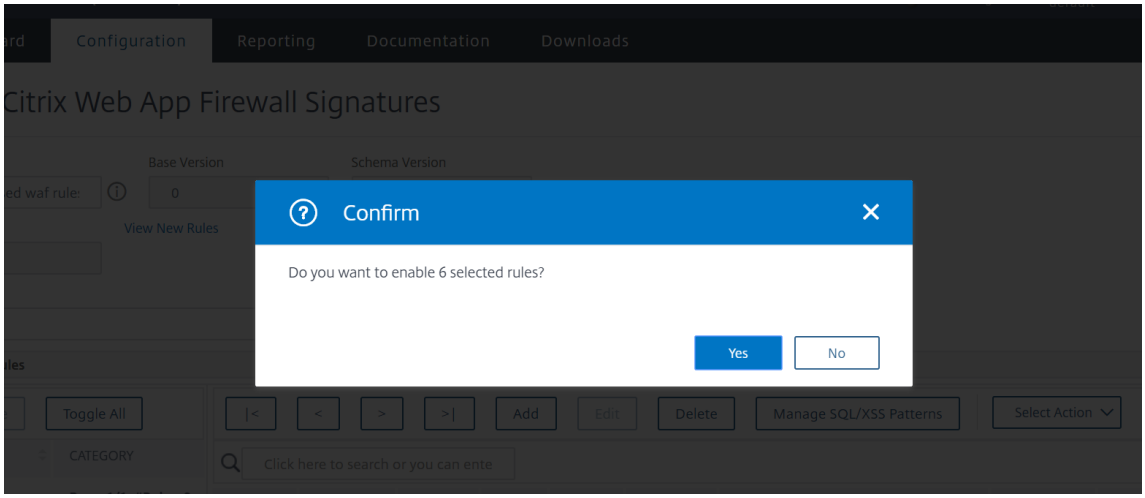
El dispositivo importa las reglas de Snort como reglas de firma WAF basadas en snort.



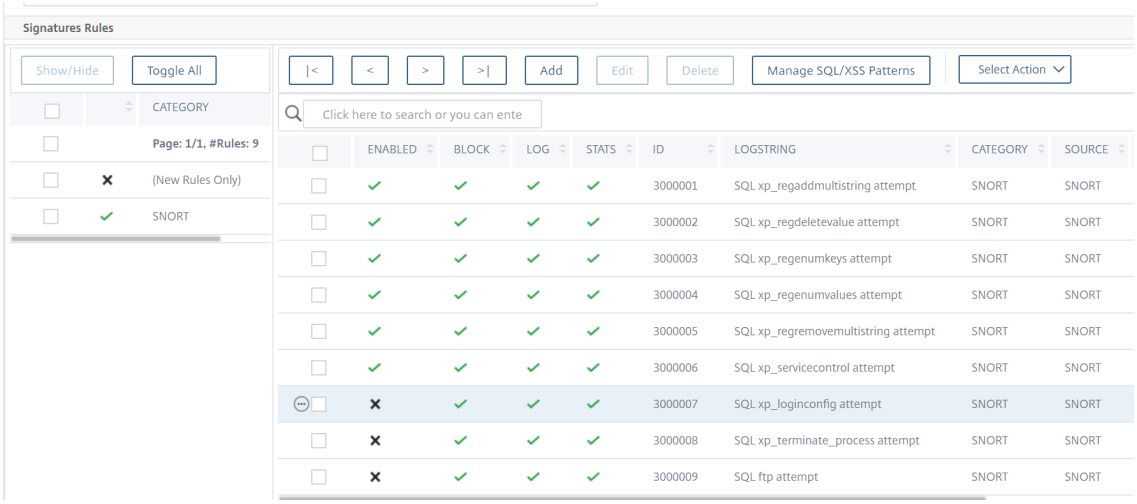
Como práctica recomendada, debe utilizar acciones de filtro para habilitar las reglas de snort que prefiera importar como reglas de firma WAF en el dispositivo.



5. Para confirmar, haga clic en **Sí**.



6. Las reglas seleccionadas están habilitadas en el dispositivo.



7. Haga clic en **Aceptar**.

Exportar un objeto de firmas a un archivo

January 12, 2021

Exportar un objeto de firmas a un archivo para poder importarlo a otro Citrix ADC.

Para exportar un objeto de firmas a un archivo

1. Vaya a **Seguridad > Citrix Web App Firewall > Firmas**.
2. En el panel de detalles, seleccione el objeto de firmas que quiere configurar.
3. En la lista desplegable **Acciones**, seleccione **Exportar**.

4. En el cuadro de diálogo **Exportar objeto de firmas**, cuadro de texto **Archivo local**, escriba la ruta de acceso y el nombre del archivo al que quiere exportar el objeto de firmas, o utilice el cuadro de diálogo **Examinar** para designar una ruta de acceso y un nombre.
5. Haga clic en **Aceptar**.

Editor de firmas

August 20, 2021

Puede utilizar el editor de firmas para agregar o modificar una regla de firma definida por el usuario (local) a un objeto de firmas existente. Una regla de firma local tiene los mismos atributos que una regla de firma predeterminada de Citrix y funciona del mismo modo. La habilita o inhabilita y configura las acciones de firma para ella, al igual que para una firma predeterminada.

Agregue una regla local si necesita proteger sus sitios web y servicios de un ataque conocido que las firmas existentes no coinciden. Por ejemplo, puede descubrir un nuevo tipo de ataque y determinar sus funciones examinando los registros del servidor web, o bien obtener información de terceros sobre un nuevo tipo de ataque.

En el corazón de una regla de firma se encuentran los *patrones*de regla, que describen colectivamente las funciones del ataque para el que la regla está diseñada. Cada patrón puede consistir en una cadena simple, una expresión regular de formato PCRE-o la inyección SQL incorporada o los patrones de scripts entre sitios.

Es posible que quiera modificar una regla de firma agregando un nuevo patrón o modificando un patrón existente para que coincida con un ataque. Por ejemplo, es posible que descubra los cambios realizados en un ataque o que determine un patrón mejor examinando los registros de su servidor web o a partir de información de terceros.

Para agregar o modificar una regla de firma local mediante el Editor de firmas

1. Vaya a **Seguridad > Citrix Web App Firewall > Firmas**.
2. En el panel de detalles, seleccione el objeto de firmas que quiere modificar y, a continuación, haga clic en **Abrir**.
3. En el cuadro de diálogo **Modificar objeto de firmas**, en el centro de la pantalla debajo de la ventana **Resultados filtrados**, realice una de las siguientes acciones:
    - Para agregar una nueva regla de firma local, haga clic en Agregar.
    - Para modificar una regla de firma local existente, selecciónela y, a continuación, haga clic en **Abrir**.

4. En el cuadro de diálogo **Agregar regla** de **firma local o Modificar regla** de firma local, configure las acciones de una firma seleccionando las casillas de verificación correspondientes.

   - **Habilitada**. Habilita la nueva regla de firma. Si no selecciona esta opción, esta nueva regla de firma se agrega a la configuración, pero está inactiva.
   - **Bloque.** Bloquea las conexiones que infringen esta regla de firma.
   - **Registrar.** Registra infracciones de esta regla de firma en el registro Citrix ADC.
   - **Rápido.** Incluye infracciones de esta regla de firma en las estadísticas.
   - **Remove:** Elimina la información que coincide con la regla de firma de la respuesta. (Solo se aplica a las reglas de respuesta.)
   - **X-Out.** Enmascara la información que coincide con la regla de firma con la letra X. (Solo se aplica a las reglas de respuesta).
   - **Permitir duplicados.** Permite duplicados de esta regla de firma en este objeto de firmas.

5. Elija una categoría para la nueva regla de firma en la lista desplegable **Categoría**.

   También puede crear una categoría haciendo clic en el icono situado a la derecha de la lista y mediante el cuadro de diálogo Agregar categoría de regla de firma para agregar una nueva categoría a la lista. La regla que está modificando se agrega automáticamente a la nueva categoría. Para obtener instrucciones, consulte Para agregar una categoría de regla de firma.

6. En el cuadro de texto **LogString**, escriba una breve descripción de la regla de firma que se va a utilizar en los registros.

7. En el cuadro de texto **Comentario**, escriba un comentario. (Opcional)

8. Haga clic en Más… y modifique las opciones avanzadas.

   a) Para eliminar comentarios HTML antes de aplicar esta regla de firma, en la lista desplegable Eliminar comentarios elija Todo o Excluir etiqueta de script.
   b) Para configurar la comprobación del encabezado de referencia CSRF, en la matriz de botones de opción Comprobación de encabezado de referencia CSRF, seleccione el botón de opción Si está presente o Siempre.
   c) Para modificar manualmente el Id. de regla asignado a esta regla de firma local, modifique el número en el cuadro de texto Id. de regla. El ID debe ser un entero positivo entre 1000000 y 1999999 que aún no se haya asignado a una regla de firma local.
   d) Para asignar un número de versión a la nueva regla de firma, modifique el número en el cuadro de texto Número de versión.
   e) Para asignar un Id. de origen, modifique la cadena en el cuadro de texto Id. de origen.
   f) Para especificar el origen, elija Local o Roncar en la lista desplegable Origen o haga clic en el icono Agregar situado a la derecha de la lista y agregue una nueva fuente.
   g) Para asignar una puntuación de daño a infracciones de esta regla de firma local, escriba un número entre 1 y 10 en el cuadro de texto Puntuación de daño.
   h) Para asignar una clasificación de gravedad a esta regla de firma local, en la lista desple-

gable Gravedad elija Alta, Media o Baja, o haga clic en el icono Agregar situado a la derecha de la lista y agregue una nueva clasificación de gravedad.

i) Para asignar un tipo de infracción a esta regla de firma local, en la lista desplegable Tipo seleccione Vulnerable o Advertencia, o haga clic en el icono Agregar situado a la derecha de la lista y agregue un nuevo tipo de infracción.

9. En la lista **Patrones**, agregue o modifique un patrón.

   - Para agregar un patrón, haga clic en **Agregar**. En el cuadro de diálogo **Crear nuevo patrón de regla de firma**, agregue uno o varios patrones para la regla de firma y, a continuación, haga clic en **Aceptar**.
   - Para modificar un patrón, selecciónelo y, a continuación, haga clic en **Abrir**. En el cuadro de diálogo **Modificar patrón de regla de firma**, modifique el patrón y, a continuación, haga clic en **Aceptar**.

   Para obtener más información sobre cómo agregar o modificar patrones, consulte Patrones de reglas de firma.

10. Haga clic en **Aceptar**.

Para agregar una categoría de regla de firma

January 12, 2021

Poner reglas de firma en una categoría le permite configurar las acciones para un grupo de firmas en lugar de para cada firma individual. Es posible que quiera hacerlo por las siguientes razones:

- **Facilidad de selección.** Por ejemplo, suponga que todas las reglas de firma de un grupo determinado protegen contra ataques a un tipo específico de software o tecnología de servidor web. Si sus sitios web protegidos utilizan ese software o tecnología, quiere habilitarlos todos. Si no lo hacen, no quiere habilitar ninguno de ellos.
- **Facilidad de configuración inicial.** Es más fácil establecer valores predeterminados para un grupo de firmas como categoría, en lugar de uno por uno. A continuación, puede realizar cualquier cambio en firmas individuales según sea necesario.
- **Facilidad de configuración continua.** Es más fácil configurar firmas si solo puede mostrar aquellas que cumplen criterios específicos, como pertenecer a una categoría específica.

1. Vaya a **Seguridad** > **Web App Firewall** > **Firmas**.
2. En el panel de detalles, seleccione el objeto de firmas que quiere configurar y, a continuación, haga clic en **Abrir**.
3. En el cuadro de diálogo **Modificar objeto de firmas**, en el centro de la pantalla, debajo de la ventana **Resultados filtrados**, haga clic en **Agregar**.

4. En el cuadro de diálogo **Agregar regla de firma local**, haga clic en el icono situado a la derecha de la lista desplegable Categoría.
5. En el cuadro de diálogo **Agregar categoría de regla de firma**, cuadro de texto **Nueva categoría**, escriba un nombre para la nueva categoría de firma. El nombre puede constar de uno a 64 caracteres.
6. Haga clic en **Aceptar**.

Patrones de reglas de firma

August 20, 2021

Puede agregar un patrón o modificar un patrón existente para especificar una cadena o expresión que caracterice un ataque si la firma coincide. Para detectar los patrones que exhibe un ataque, puede examinar los registros de su servidor web. Puede utilizar una herramienta para observar los datos de conexión en tiempo real, u obtener la cadena o expresión de un informe de terceros sobre el ataque.

> **Precaución:**
>
> Cualquier patrón nuevo que agregue a una regla de firma tiene una relación AND con los patrones existentes. No agregue un patrón a una regla de firma existente si no quiere que un ataque potencial tenga que coincidir con todos los patrones para que coincida con la firma.

Cada patrón puede consistir en una cadena simple, una expresión regular de formato PCRE-o la inyección SQL incorporada o el patrón de scripts entre sitios. Antes de intentar agregar un patrón basado en una expresión regular, debe asegurarse de que comprende las expresiones regulares de formato PCR. Las expresiones PCRE son complejas y poderosas. Si no entiende cómo funcionan, puede crear involuntariamente un patrón que coincida con algo que no quería (un *falso positivo*) o que no coincida con algo que quería (un *falso negativo*).

Patrón de firma personalizado para tipos de contenido no predeterminados

Citrix ADC Web App Firewall (WAF) admite ahora una nueva ubicación para inspeccionar contenido canonicalizado. De forma predeterminada, WAF no bloquea la carga útil codificada con tipos de contenido no predeterminados. Cuando estos tipos de contenido se incluyen en la lista de permitidos y no se aplica ninguna acción configurada, la comprobación de protección de scripts SQL y entre sitios no filtra los ataques de scripts SQL o entre sitios en las cargas útiles codificadas. Para resolver el problema, un usuario puede crear una regla de firma personalizada con esta nueva ubicación (HTTP_CANON_POST_BODY) que examina las cargas útiles codificadas para tipos de contenido no predeterminados y si hay algún ataque de scripts SQL o entre sitios, bloquea el tráfico después de la canonización del cuerpo de la publicación.

> **Nota:**
>
> Ese soporte solo es aplicable a las solicitudes HTTP.

Si aún no está familiarizado con las expresiones regulares de formato PCRE-Format, puede utilizar los siguientes recursos para aprender los conceptos básicos o para obtener ayuda con algún problema específico:

- "Dominar expresiones regulares", tercera edición. Copyright (c) 2006 por Jeffrey Friedl. O'Reilly Media, ISBN: 9780596528126.
- "Libro de cocina de expresiones regulares". Copyright (c) 2009 por Jan Goyvaerts y Steven Levithan. O'Reilly Media, ISBN: 9780596520687
- **PCRE Página/Especificación** (texto/oficial): http://www.pcre.org/pcre.txt
- **Página/especificación del hombre PCRE**

http://www.gammon.com.au/pcre/index.html

- **Entrada PCRE de Wikipedia**: http://en.wikipedia.org/wiki/PCRE
- **Lista de correo PCRE**
  PCRE-dev - PCRE Development

Si necesita codificar caracteres no ASCII en una expresión regular con formato PCRE-formato, la plataforma Citrix ADC admite la codificación de códigos hexadecimales UTF-8. Para obtener más información, consulte Formato de codificación de caracteres PCRE.

Para configurar un patrón de regla de firma

1. Vaya a **Seguridad > Citrix Web App Firewall > Firmas**.
2. En el panel de detalles, seleccione el objeto de firmas que quiere configurar y, a continuación, haga clic en **Abrir**.
3. En el cuadro de diálogo **Modificar objeto de firmas**, en el medio de la pantalla debajo de la ventana **Resultados filtrados**, haga clic en **Agregar** para crear una regla de firma o seleccione una regla de firma existente y haga clic en **Abrir**.

   > **Nota:**
   >
   > Solo puede modificar las reglas de firma que haya agregado. No se pueden modificar las reglas de firma predeterminadas.

   Según la acción, aparecerá el cuadro de diálogo Agregar regla de firma local o Modificar regla de firma local. Ambos cuadros de diálogo tienen el mismo contenido.
4. En la **ventana Patrones** del cuadro de diálogo, haga clic en **Agregar** para agregar un nuevo patrón o seleccione un patrón existente en la lista situada debajo del botón **Agregar** y haga clic

en **Abrir**. Según la acción, aparecerá el cuadro de diálogo **Crear nuevo patrón de regla** de **firma o Modificar patrón de regla** de firma. Ambos cuadros de diálogo tienen el mismo contenido.

5. En la lista desplegable **Tipo de patrón**, elija el tipo de conexión que debe coincidir el patrón.
   - Si el patrón está pensado para que coincida con elementos o funciones de solicitud, como código SQL inyectado, ataques a formularios web, scripts entre sitios o direcciones URL inapropiadas, elija **Solicitar**.
   - Si el patrón está pensado para que coincida con elementos u operaciones de respuesta, como números de tarjetas de crédito u objetos seguros, elija **Respuesta**.
6. En el área Ubicación, defina los elementos que se van a examinar con este patrón.
   El área Ubicación describe qué elementos de la solicitud o respuesta HTTP examinar para este patrón. Las opciones que aparecen en el área Ubicación dependen del tipo de patrón elegido. Si elige Solicitud como tipo de patrón, aparecerán elementos relevantes para las solicitudes HTTP. Si seleccionó Respuesta, aparecerán elementos relevantes para las respuestas HTTP.
   Además, a medida que elija un valor de la lista desplegable Área, las partes restantes del área Ubicación cambian de forma interactiva. Los siguientes son todos los elementos de configuración que pueden aparecer en esta sección.
   - Área. Lista desplegable de elementos que describen una parte determinada de la conexión HTTP. Las opciones son las siguientes:
     - **HTTP_ANY**. Todas las partes de la conexión HTTP.
     - **HTTP_Cookie**. Todas las cookies en los encabezados de solicitud HTTP después de cualquier transformación de cookies se realizan.
       Nota: No busca encabezados de respuesta HTTP “Set-Cookie:”.
     - **HTTP_FORM_FIELD** Campos de formulario y su contenido, después de la decodificación de URL, decodificación de porcentaje y eliminación del exceso de espacio en blanco. Puede utilizar la etiqueta <Location> para restringir aún más la lista de nombres de campos de formulario que se van a buscar.
     - **HTP_HEADER** Las partes de valor del encabezado HTTP después de cualquier transformación de scripts entre sitios o decodificación de URL.
     - **HTTP_METHOD** El método de solicitud HTTP.
     - **HTTP_ORIGIN_URL**. Dirección URL de origen de un formulario web.
     - **HTTP_POST_BODY** El cuerpo de la publicación HTTP y los datos del formulario web que contiene.
     - **HTTP_RAW_Cookie**. Todas las cookies de solicitud HTTP, incluida la parte del nombre “Cookie:”.
       Nota: No busca encabezados de respuesta HTTP “Set-Cookie:”.
     - **HTTP_RAW_HEADER**. El encabezado HTTP completo, con encabezados individuales separados por caracteres de avance de línea (\n) o cadenas de retorno de carretera/avance de línea (\r\n).

- **HTTP_RAW_RESP_HEADER**. El encabezado de respuesta completo, incluidas las partes de nombre y valor del encabezado de respuesta después de la transformación de URL se ha realizado, y el estado de respuesta completo. Al igual que con HTTP_RAW_HEADER, los encabezados individuales están separados por caracteres de avance de línea (\n) o cadenas de retorno de carro o avance de línea (\r\n).
- **HTTP_RAW_SET_Cookie**. Toda la cabecera Set-Cookie después de realizar cualquier transformación de URL

  Nota: La transformación de URL puede cambiar tanto las partes de dominio como de ruta del encabezado Set-Cookie.
- **HTTP_RAW_URL**. La URL de solicitud completa antes de realizar cualquier transformación de URL, incluidas las partes de consulta o fragmentos.
- **HTTP_RESP_HEADER**. La parte del valor de los encabezados de respuesta completos después de que se hayan realizado las transformaciones de URL.
- **HTTP_RESP_BODY**. El cuerpo de respuesta HTTP
- **HTTP_SET_Cookie**. Todos los encabezados “Set-Cookie” en los encabezados de respuesta HTTP.
- **HTTP_STATUS_CODE**. El código de estado HTTP.
- **HTTP_STATUS_Message**. El mensaje de estado HTTP.
- **HTTP_URL**. La parte de valor de la URL en los encabezados HTTP, excluyendo cualquier puerto de consulta o fragmento, después de la conversión al conjunto de caracteres UTF-*, la decodificación de URL, la eliminación de espacios en blanco y la conversión de URL relativas a absolutas. No incluye la decodificación de entidades HTML.
- URL. Examina las URL encontradas en los elementos especificados por la configuración

  Área. Seleccione una de las siguientes opciones de configuración.
- **Cualquiera.** Comprueba todas las URL.
- Literalmente. Comprueba las URL que contienen una cadena literal. Después de seleccionar Literal, se muestra un cuadro de texto. Escriba la cadena literal que quiera en el cuadro de texto.
- PCRE. Comprueba las URL que coinciden con una expresión regular con formato PCRE-format. Después de seleccionar esta opción, se muestra la ventana de expresión regular. Escriba la expresión regular en la ventana. Puede utilizar los **Tokens de expresiones regulares** para insertar elementos de expresiones regulares comunes en el cursor, o puede hacer clic en Editor de expresiones regulares para mostrar el cuadro de diálogo Editor de expresiones regulares, que proporciona más ayuda para construir la expresión regular que quiera.
- Expresión. Comprueba las direcciones URL que coinciden con una expresión predeterminada de Citrix ADC.

- Nombre del campo. Examina los nombres de campos de formulario encontrados en los elementos especificados por la selección
  Área. **Cualquiera.** Comprueba todas las URL.
- Literalmente. Comprueba las URL que contienen una cadena literal. Después de seleccionar Literal, se muestra un cuadro de texto. Escriba la cadena literal que quiera en el cuadro de texto.
- PCRE. Comprueba las URL que coinciden con una expresión regular con formato PCRE-format. Después de seleccionar esta opción, se muestra la ventana de expresión regular. Escriba la expresión regular en la ventana. Puede utilizar los **tokens de expresión regular** para insertar elementos comunes de expresión regular o puede utilizar el Editor de expresiones regulares para obtener ayuda en la construcción de una expresión regular que quiera.
- Expresión. Comprueba las direcciones URL que coinciden con una expresión predeterminada de Citrix ADC.

7. En el área Patrón, defina el patrón. Un patrón es una cadena literal o expresión regular de formato PCRE-que define el patrón que quiere hacer coincidir. El área Patrón contiene los siguientes elementos:
- Coincidir. Una lista desplegable de métodos de búsqueda que puede utilizar para la firma. Esta lista varía en función de si el tipo de patrón es Solicitud o Respuesta.

Solicitar tipos de coincidencia
PCRE. Expresión regular de formato PCRE-.

> **Nota:**
>
> Al seleccionar PCRE, se activan las herramientas de expresión regular situadas debajo de la ventana Patrón. Estas herramientas no son útiles para la mayoría de los otros tipos de patrones.

- **Inyección**. Indica al Web App Firewall que busque SQL inyectado en la ubicación especificada. La ventana Patrón desaparece, porque Web App Firewall ya tiene los patrones para la inyección SQL.
- **CrossSitescripting**. Indica al Web App Firewall que busque scripts entre sitios en la ubicación especificada. La ventana Patrón desaparece porque Web App Firewall ya tiene los patrones para scripts entre sitios.
- **Expresión**. Una expresión en el lenguaje de expresiones predeterminado de Citrix ADC es el mismo idioma de expresión para crear directivas de Web App Firewall en el dispositivo Citrix ADC. Aunque el lenguaje de expresiones Citrix ADC se desarrolló originalmente para reglas de directivas, es un lenguaje de propósito general altamente flexible que también se puede usar para definir un patrón de firma.

Al elegir Expresión, el Editor de expresiones de Citrix ADC aparece debajo de la ventana Patrón.

Para obtener más información sobre el Editor de expresiones e instrucciones sobre cómo utilizarlo, consulte Para agregar una regla de firewall (expresión) mediante el cuadro de diálogo Agregar expresión

Tipos de coincidencia de respuesta:

```
1 -  Literal. A literal string
2 -  PCRE. A PCRE-format regular expression.
```

> Nota
>
> Al seleccionar PCRE, se activan las herramientas de expresión regular situadas debajo de la ventana Patrón. Estas herramientas no son útiles para la mayoría de los otros tipos de patrones.

- **Tarjeta de crédito**. Un patrón integrado que coincide con uno de los seis tipos admitidos de número de tarjeta de crédito.

> Nota:
>
> El tipo de coincidencia de expresión no está disponible para las firmas del lado de respuesta.

- Ventana de patrón (sin etiqueta)

En esta ventana, escriba el patrón que quiere que coincida y complete los datos adicionales.

- Literalmente. Escriba la cadena que quiere buscar en el área de texto.
- CRE. Escriba la expresión regular en el área de texto. Utilice el Editor de expresiones regulares para obtener más ayuda en la construcción de la expresión regular que quiera, o los Tokens de expresiones regulares para insertar elementos comunes de expresiones regulares en el cursor. Para habilitar caracteres UTF-8, haga clic en UTF-8.
- Expresión. Escriba la expresión avanzada de Citrix ADC en el área de texto. Utilice Prefijo para elegir el primer término de la expresión u Operador para insertar operadores comunes en el cursor. Haga clic en Agregar para abrir el cuadro de diálogo Agregar expresión para obtener más ayuda en la construcción de la expresión regular que quiera. Haga clic en Evaluar para abrir el Evaluador de expresiones avanzadas para ayudar a determinar el efecto que tiene la expresión.
- Desplazamiento. El número de caracteres que se deben omitir antes de comenzar a coincidir en este patrón. Utilice este campo para comenzar a examinar una cadena en algún momento distinto del primer carácter.
- Profundidad. Cuántos caracteres desde el punto de partida examinar para buscar coincidencias. Este campo se utiliza para limitar las búsquedas de una cadena grande a un número específico de caracteres.

- Longitud mínima. La cadena que se va a buscar debe tener al menos el número especificado de bytes de longitud. Las cadenas más cortas no coinciden.
- Longitud máxima. La cadena que se va a buscar no debe ser mayor que el número especificado de bytes de longitud. Las cadenas más largas no coinciden.
- Método de búsqueda. Una casilla de verificación etiquetada fastmatch. Puede habilitar fastmatch solo para un patrón literal, para mejorar el rendimiento.

8. Haga clic en **Aceptar**.
9. Repita los cuatro pasos anteriores para agregar o modificar más patrones.
10. Cuando termine de agregar o modificar patrones, haga clic en **Aceptar** para guardar los cambios y volver al panel Firmas.

> **Precaución:**
>
> Hasta que haga clic en **Aceptar** en el cuadro de diálogo **Agregar regla** de **firma local o Modificar regla** de firma local, los cambios no se guardarán. No cierre ninguno de estos cuadros de diálogo sin hacer clic en **Aceptar** a menos que quiera descartar los cambios.

Para importar y combinar reglas

August 20, 2021

Al utilizar el editor de firmas para realizar una operación de importación y fusión desde la GUI, ahora puede ver las reglas nuevas, actualizadas, duplicadas e inválidas.

El editor de firmas muestra las siguientes cuatro filas nuevas:

1. Nuevas reglas
2. Reglas actualizadas
3. Reglas duplicadas
4. Reglas no válidas

La salida de los filtros Solo reglas nuevas y Solo reglas actualizadas también aparece en el panel Filtro categoría de la ventana Modificar del editor de firmas.

Deberá importar los archivos desde la GUI para ver los enlaces correspondientes a las reglas nuevas, duplicadas, no válidas y actualizadas.

Procedimiento para importar reglas de firma:

1. En la GUI web de Citrix ADC, vaya a **Configuración > Seguridad > Firmas de Citrix Web App Firewall**. En la ventana Firmas, haga clic en **Agregar**. A continuación, seleccione **Formato de archivo** > **Nativo** , **Importar desde** > **URL** y, en el campo URL, agregue el enlace anterior. Si no puede acceder a la URL, puede descargar los datos XML en formato de archivo de texto.

2. Después de hacer clic en **Abrir**, se abrirá el archivo de firma y podrá ver vínculos para nuevas reglas y reglas no válidas.
3. Si importa una regla de firma de grupo 3rd, puede ver 90 reglas nuevas y 9 reglas duplicadas en el archivo .xml importado. Si no puede acceder a la URL, puede descargar los datos XML en formato de archivo de texto.

Actualizaciones de firma en implementaciones de alta disponibilidad y actualizaciones de compilación

January 12, 2021

La actualización de la firma se produce en el nodo principal. Mientras las firmas se actualizan en el nodo principal, en paralelo los archivos actualizados se sincronizan simultáneamente con el nodo secundario.

La firma predeterminada siempre se actualiza primero y, a continuación, se actualizan el resto de las firmas definidas por el usuario.

Conexión a Amazon AWS

La ruta predeterminada NSIP se utiliza para conectarse a Amazon AWS. Si hay un caso de uso específico en el que se utiliza SNIP, y si hay varios SNIP, el primero en recibir la respuesta ARP del sitio de alojamiento mantendrá la ruta.

Actualizaciones de firmas durante las actualizaciones de versiones

En caso de una actualización, si el NS tiene una versión base anterior para las firmas, *La firma predeterminada se actualiza automáticamente si hay disponible una versión de firma más reciente.

Si el esquema ha cambiado, la versión del esquema de todos los objetos de firma se actualiza cuando se actualiza la versión.

Sin embargo, para la versión base de las firmas definidas por el usuario, el comportamiento es diferente en la versión 10.5 frente a la versión 11.0.

En la versión 10.5, solo se actualizó la firma predeterminada y la versión base del resto de firmas permaneció sin cambios después de la actualización de compilación.

En la versión 11.0, este comportamiento ha cambiado. Cuando se actualiza el dispositivo para instalar una nueva compilación, no solo el objeto de firma *Default, sino todas las demás firmas definidas por el usuario que actualmente existen en el dispositivo también se actualizan y tendrán la misma versión después de la actualización de compilación.

Tanto en versiones 10.5 como 11.0, si se configura la actualización automática, las firmas *Default, así como todas las firmas de versiones distintas de cero, se actualizan automáticamente a la última versión de firma publicada y tendrán la misma versión base.

Descripción general de las comprobaciones de seguridad

August 20, 2021

Las protecciones avanzadas de Web App Firewall (comprobaciones de seguridad) son un conjunto de filtros diseñados para detectar ataques complejos o desconocidos en sus sitios web y servicios web protegidos. Las comprobaciones de seguridad utilizan heurística, seguridad positiva y otras técnicas para detectar ataques que pueden no ser detectados por firmas solas. Las comprobaciones de seguridad se configuran mediante la creación y configuración de un perfil de Web App Firewall, que es una colección de opciones definidas por el usuario que indican al Web App Firewall qué comprobaciones de seguridad se deben utilizar y cómo manejar una solicitud o respuesta que falla una comprobación de seguridad. Un perfil está asociado a un objeto de firmas y a una directiva para crear una configuración de seguridad.

El Web App Firewall proporciona veinte comprobaciones de seguridad, que difieren ampliamente en los tipos de ataques a los que se dirigen y la complejidad de configurar. Las comprobaciones de seguridad se organizan en las siguientes categorías:

- **Controles de seguridad comunes.** Controles que se aplican a cualquier aspecto de la seguridad web que no involucre contenido o sea igualmente aplicable a todos los tipos de contenido.
- **Comprobaciones de seguridad HTML.** Comprueba que examinan las solicitudes y respuestas HTML. Estas comprobaciones se aplican a sitios web basados en HTML y a las partes HTML de los sitios web 2.0, que contienen contenido HTML y XML mixto.
- **Comprobaciones de seguridad XML.** Comprueba que examinan las solicitudes y respuestas XML. Estas comprobaciones se aplican a los servicios web basados en XML y a las partes XML de los sitios web 2.0.

Las comprobaciones de seguridad protegen contra una amplia gama de tipos de ataques, incluidos ataques a vulnerabilidades de software del sistema operativo y del servidor web, vulnerabilidades de bases de datos SQL, errores en el diseño y codificación de sitios web y servicios web, y fallas en la protección de sitios web que alojan o pueden acceder a información confidencial.

Todas las comprobaciones de seguridad tienen un conjunto de opciones de configuración, las acciones de comprobación, que controlan cómo el Web App Firewall gestiona una conexión que coincide con una comprobación. Hay tres acciones de comprobación disponibles para todas las comprobaciones de seguridad. Se trata de:

- **Bloque.** Bloquear conexiones que coincidan con la firma. Inhabilitado de forma predeterminada.
- **Registrar.** Registre las conexiones que coincidan con la firma, para su análisis posterior. Habilitado de forma predeterminada.
- **Estadísticas.** Mantener estadísticas, para cada firma, que muestran cuántas conexiones coincidieron y proporcionar cierta otra información sobre los tipos de conexiones que se bloquearon. Inhabilitado de forma predeterminada.

Una cuarta acción de comprobación, **Aprender**, está disponible para más de la mitad de las acciones de comprobación. Observa el tráfico hacia un sitio web protegido o servicio web y utiliza conexiones que violan repetidamente la comprobación de seguridad para generar excepciones recomendadas (relajaciones) a la comprobación, o nuevas reglas para la comprobación. Además de las acciones de comprobación, ciertas comprobaciones de seguridad tienen parámetros que controlan las reglas que utiliza la comprobación para determinar qué conexiones violan esa comprobación o que configuran la respuesta del Web App Firewall a las conexiones que infringen la comprobación. Estos parámetros son diferentes para cada comprobación, y se describen en la documentación de cada comprobación.

Para configurar las comprobaciones de seguridad, puede utilizar el asistente Web App Firewall, tal y como se describe en el Asistente para Web App Firewall, o bien configurar las comprobaciones de seguridad manualmente, como se describe en Configuración manual mediante la GUI. Algunas tareas, como la introducción manual de relajaciones o reglas o la revisión de datos aprendidos, solo se pueden realizar mediante la GUI, no la línea de comandos. El uso del asistente suele ser el mejor método de configuración, pero en algunos casos la configuración manual puede ser más fácil si está completamente familiarizado con él y simplemente quiere ajustar la configuración para una única comprobación de seguridad.

Independientemente del método que utilice para configurar las comprobaciones de seguridad, cada comprobación de seguridad requiere que se realicen determinadas tareas. Muchas comprobaciones requieren que especifique excepciones (relajación) para evitar el bloqueo del tráfico legítimo antes de habilitar el bloqueo para esa comprobación de seguridad. Puede hacerlo manualmente, observando las entradas de registro después de que se haya filtrado una cierta cantidad de tráfico y, a continuación, creando las excepciones necesarias. Sin embargo, generalmente es mucho más fácil habilitar la función de aprendizaje y dejar que observe el tráfico y recomendar las excepciones necesarias.

Web App Firewall utiliza motores de paquetes (PE) durante el procesamiento de las transacciones. Cada motor de paquetes tiene un límite de 100K sesiones que es suficiente para la mayoría de los casos de implementación. Sin embargo, cuando Web App Firewall está procesando tráfico pesado y el tiempo de espera de la sesión se configura en un valor más alto, es posible que las sesiones se acumulen. Si el número de sesiones activas de Web App Firewall supera el límite de 100 000 por PE, es posible que las infracciones de comprobación de seguridad de Web App Firewall no se envíen al dispositivo Security Insight. Reducir el tiempo de espera de la sesión a un valor menor o utilizar el modo sin sesión para las comprobaciones de seguridad con cierre de URL sin sesión o coherencia de

campo sin sesión puede ayudar a evitar que las sesiones se acumulen. Si esta opción no es viable en casos en los que las transacciones pueden requerir sesiones más largas, se recomienda actualizar a una plataforma de gama superior con más motor de paquetes.

Se agrega compatibilidad con AppFirewall almacenado en caché, y la configuración máxima de sesión a través de la CLI por núcleo se establece en sesiones de 50K.

Protecciones de nivel superior

August 20, 2021

Cuatro de las protecciones de Web App Firewall son especialmente eficaces contra tipos comunes de ataques web y, por lo tanto, se utilizan más comúnmente que cualquiera de los demás. Se trata de:

- **Scripting entre sitios HTML.** Examina las solicitudes y respuestas para scripts que intentan acceder o modificar contenido en un sitio web diferente al en el que se encuentra el script. Cuando esta comprobación encuentra un script de este tipo, lo hace inofensivo antes de reenviar la solicitud o respuesta a su destino, o bloquea la conexión.
- **Inyección HTML SQL.** Examina las solicitudes que contienen datos de campos de formulario para intentar inyectar comandos SQL en una base de datos SQL. Cuando esta comprobación detecta código SQL inyectado, bloquea la solicitud o hace que el código SQL inyectado sea inofensivo antes de reenviar la solicitud al servidor web.

  Nota: Si las dos condiciones siguientes se aplican a la configuración, debe asegurarse de que el Web App Firewall está configurado correctamente:

  - Si habilita la comprobación HTML Cross-Site Scripting o la comprobación HTML SQL Injection (o ambas), y
  - Los sitios web protegidos aceptan cargas de archivos o contienen formularios web que pueden contener datos de cuerpo POST grandes.

  Para obtener más información sobre cómo configurar Web App Firewall para que se ocupe de este caso, consulte Configuración del firewall de aplicaciones.
- **Desbordamiento de búfer.** Examina las solicitudes para detectar los intentos de provocar un desbordamiento de búfer en el servidor web.
- **Consistencia de cookies.** Examina las cookies devueltas con las solicitudes de los usuarios para comprobar que coinciden con las cookies establecidas por el servidor web para ese usuario. Si se encuentra una cookie modificada, se elimina de la solicitud antes de que la solicitud se reenvíe al servidor web.

La comprobación de desbordamiento de búfer es simple; por lo general, puede habilitar el bloqueo inmediatamente. Las otras tres comprobaciones de nivel superior son considerablemente más com-

plejas y requieren configuración antes de poder usarlas de forma segura para bloquear el tráfico. Citrix recomienda encarecidamente que, en lugar de intentar configurar estas comprobaciones manualmente, habilite la función de aprendizaje y permita que genere las excepciones necesarias.

Comprobación de scripts de sitios HTML

March 9, 2022

La comprobación de scripts de sitios HTML (scripts de sitios) examina tanto los encabezados como los cuerpos POST de las solicitudes de los usuarios para detectar posibles ataques de scripts de sitios. Si encuentra un script de sitios, modifica (*transforma*) la solicitud para que el ataque sea inofensivo o bloquea la solicitud.

> **Nota:**
>
> La comprobación de scripts de sitios HTML (scripts de sitios) solo funciona para el tipo de contenido, la longitud del contenido, etc. Asegúrese también de tener habilitada la opción "CheckRequestHeaders" en su perfil de Firewall de aplicaciones web.

Puede evitar el uso indebido de las secuencias de comandos en sus sitios web protegidos mediante secuencias de comandos HTML de sitios que infrinjan la *misma regla de origen*, que establece que los scripts no deben acceder ni modificar el contenido de ningún servidor, excepto el servidor en el que se encuentran. Cualquier script que infrinja la misma regla de origen se denomina secuencia de comandos de sitios y la práctica de utilizar scripts para acceder o modificar el contenido de otro servidor se denomina script de sitios. La razón por la que los scripts de sitios son un problema de seguridad es que un servidor web que permite la creación de scripts de sitios puede ser atacado con una secuencia de comandos que no esté en ese servidor web, sino en un servidor web diferente, como uno que sea propiedad y esté controlado por el atacante.

Desafortunadamente, muchas empresas tienen una gran base instalada de contenido web mejorado con JavaScript que infringe la misma regla de origen. Si habilita la comprobación de scripts de sitios HTML en un sitio de este tipo, debe generar las excepciones apropiadas para que la comprobación no bloquee la actividad legítima.

Web App Firewall ofrece varias opciones de acción para implementar la protección de scripts HTML de sitios. Además de las acciones **Bloquear**, **Registrar**, **Estadísticas** y **Aprender**, también tiene la opción de **Transformar scripts de sitios** para que un ataque sea inofensivo por parte de la entidad que codifica las etiquetas de script en la solicitud enviada. Puede configurar el parámetro Comprobar URL completas para scripts de sitios para especificar si quiere inspeccionar no solo los parámetros de consulta, sino toda la URL para detectar ataques de scripts de sitios. Puede configurar el parámetro **InspectQueryContentTypes** para inspeccionar la parte de la consulta de solicitud en busca del ataque de scripts de sitios para los tipos de contenido específicos.

Puede implementar relajaciones para evitar falsos positivos. El motor de aprendizaje de Web App Firewall puede proporcionar recomendaciones para configurar reglas de relajación.

Para configurar una protección optimizada de scripts de sitios HTML para su aplicación, configure una de las siguientes acciones:

- **Bloquear**: si habilita el bloqueo, la acción de bloqueo se desencadena si se detectan las etiquetas de scripts de sitios en la solicitud.
- **Registro**: si habilita la función de registro, la comprobación de scripts de sitios HTML genera mensajes de registro que indican las acciones que lleva a cabo. Si el bloqueo está inhabilitado, se genera un mensaje de registro independiente para cada encabezado o campo de formulario en el que se detectó la infracción de scripts de sitios. Sin embargo, solo se genera un mensaje cuando se bloquea la solicitud. Del mismo modo, se genera 1 mensaje de registro por solicitud para la operación de transformación, incluso cuando las etiquetas de scripts de sitios se transforman en varios campos. Puede supervisar los registros para determinar si las respuestas a las solicitudes legítimas se están bloqueando. Un gran aumento en la cantidad de mensajes de registro puede indicar intentos de lanzar un ataque.
- **Estadísticas**: si está habilitada, la función de estadísticas recopila estadísticas sobre infracciones y registros. Un aumento inesperado en el contador de estadísticas podría indicar que su aplicación está siendo atacada. Si las solicitudes legítimas se bloquean, es posible que tenga que volver a visitar la configuración para ver si debe configurar las nuevas reglas de relajación o modificar las existentes.
- **Aprender**: si no está seguro de qué reglas de relajación podrían ser las más adecuadas para su aplicación, puede utilizar la función de aprendizaje para generar recomendaciones de reglas de scripts de sitios HTML basadas en los datos aprendidos. El motor de aprendizaje de Web App Firewall supervisa el tráfico y proporciona recomendaciones de aprendizaje basadas en los valores observados. Para obtener un beneficio óptimo sin comprometer el rendimiento, es posible que desee habilitar la opción de aprendizaje durante un tiempo breve para obtener una muestra representativa de las reglas y, a continuación, implementar las reglas y inhabilitar el aprendizaje.
- **Transformar scripts de sitios**: Si está habilitada, Web App Firewall realiza los siguientes cambios en las solicitudes que coinciden con la comprobación de scripts de sitios HTML:
  - Corchete angular izquierdo (<) a equivalente de entidad de caracteres HTML (<)
  - Corchete angular derecho (>) a equivalente de entidad de caracteres HTML (>)

Esto garantiza que los navegadores no interpreten etiquetas html inseguras, como, y, por lo tanto `<script>`, ejecuten código malicioso. Si habilitas tanto la verificación como la transformación de encabezados de solicitud, también se modifican los caracteres especiales que se encuentren en los encabezados de solicitud. Si los scripts de su sitio web protegido contienen funciones de scripts de sitios, pero su sitio web no depende de esos scripts para funcionar correctamente, puede inhabilitar el bloqueo y habilitar la transformación de forma segura. Esta configuración garantiza que no se bloquee el tráfico web legítimo y, al mismo tiempo, detiene los posibles ataques de scripts de sitios.

- **Compruebe las URL completas para scripts de sitios**. Si la verificación de las URL completas está habilitada, Web App Firewall examina las URL completas en busca de ataques de scripts de sitios HTML en lugar de comprobar solo las partes de consulta de las URL.
- **Marque los encabezados de solicitud**. Si la comprobación de encabezados de solicitud está habilitada, Web App Firewall examina los encabezados de las solicitudes de ataques de scripts de sitios HTML, en lugar de solo las URL. Si usa la GUI, puede habilitar este parámetro en la ficha Configuración del perfil de Web App Firewall.
- **Inspeccionar los tipos de contenido de la consulta**. Si la inspección de consultas de solicitudes está configurada, App Firewall examina la consulta de las solicitudes de ataques de scripts de sitios para los tipos de contenido específicos. Si usa la GUI, puede configurar este parámetro en la ficha Configuración del perfil de App Firewall.

> **Importante:**
>
> Como parte de los cambios de transmisión, el procesamiento de Web App Firewall de las etiquetas de scripts de sitios ha cambiado. Este cambio se aplica a las compilaciones 11.0 en adelante. Este cambio también es relevante para las compilaciones de mejora de 10.5.e que admiten la transmisión en el lado de la solicitud. En versiones anteriores, la presencia de corchetes abiertos (<), corquetes cerrados (>) o corchetes abiertos y cerrados (<>) se marcaba como Infracción de scripts de sitios. El comportamiento ha cambiado en las compilaciones que incluyen soporte para la transmisión en el lado de la solicitud. Solo el carácter de corchete cerrado (>) ya no se considera un ataque. Las solicitudes se bloquean incluso cuando hay un carácter de corchete abierto (<) y se consideran un ataque. El ataque de scripts de sitios se marca.

Scripting de sitios Relajaciones de grano fino

Web App Firewall le ofrece la opción de eximir un campo de formulario, encabezado o cookie específicos de la verificación de la inspección de scripts de sitios. Puede omitir por completo la inspección de uno o más de estos campos configurando las reglas de relajación.

Web App Firewall le permite implementar una seguridad más estricta ajustando las reglas de relajación. Una aplicación puede requerir la flexibilidad para permitir patrones específicos, pero configurar una regla de relajación para eludir la inspección de seguridad puede hacer que la aplicación sea vulnerable a los ataques, ya que el campo de destino está exento de la inspección de cualquier patrón de ataque de scripts de sitios. La relajación detallada de scripts de sitios proporciona la opción de permitir atributos, etiquetas y patrones específicos. El resto de los atributos, etiquetas y patrones están bloqueados. Por ejemplo, Web App Firewall tiene actualmente un conjunto predeterminado de más de 125 patrones denegados. Como los piratas informáticos pueden utilizar estos patrones en ataques de scripts de sitios, Web App Firewall los marca como amenazas potenciales. Puede relajar uno o más patrones que se consideran seguros para la ubicación específica. El resto de los patrones de scripts de sitios potencialmente peligrosos aún se comprueban para la ubicación de destino y continúan des-

encadenando las infracciones de la verificación de seguridad. Ahora tienes un control mucho más estricto.

Los comandos utilizados en las relajaciones tienen parámetros opcionales para **Tipo de valor** y **Expresión de valor**. El tipo de valor se puede dejar en blanco o tiene la opción de seleccionar **Etiqueta**, **Atributo** o **Patrón**. Si deja el tipo de valor en blanco, el campo configurado de la URL especificada queda exento de la inspección de comprobación de scripts de sitios. Si selecciona un tipo de valor, debe proporcionar una expresión de valor. Puede especificar si la expresión de valor es una expresión regular o una cadena literal. Cuando la entrada se compara con la lista de permitidos y denegados, solo se excluyen las expresiones especificadas configuradas en las reglas de relajación.

Web App Firewall tiene las siguientes listas integradas de scripts de sitios:

1. **Atributos permitidos de scripts de sitios**: Hay 52 atributos permitidos predeterminados, como **abbr**, **accesskey**, **align**, **alt**, **axis**, **bgcolor**, **border**, **cell padding**, **cell spacing**, **char**, **charoff**, **charset**, etc.
2. **Etiquetas permitidas de scripts de sitios**: Hay 47 etiquetas permitidas predeterminadas, como **address**, **basefont**, **bgsound**, **big**, **blockquote**, **bg**, **br**, **caption**, **center**, **cite**, **dd**, **del**, etc.
3. **Patrones denegados de scripts de sitios**: hay 129 patrones denegados predeterminados, como **FSCommand**, **javascript:**, **onAbort**, **onActivate**, etc.

> **Advertencia**
>
> Las URL de acción de Web App Firewall son expresiones regulares. Al configurar reglas de relajación de scripts de sitios HTML, puede especificar **Nombre**y **Expresión de valor** para que sean literales o RegEx. Las expresiones regulares son potentes. Especialmente si no está familiarizado con las expresiones regulares en formato PCRE, compruebe las expresiones regulares que escriba. Asegúrese de que definen exactamente la regla que quiere agregar como excepción y nada más. El uso descuidado de caracteres comodín, y especialmente del metacarácter punto-asterisco (.*) o la combinación de caracteres comodín, puede tener resultados que no quiere, como bloquear el acceso al contenido web que no pretendía bloquear o permitir un ataque que la comprobación de scripts de sitios HTML habría bloqueado de otro modo.

Puntos a considerar:

- La expresión de valor es un argumento opcional. Es posible que un nombre de campo no tenga ninguna expresión de valor.
- Un nombre de campo se puede enlazar a varias expresiones de valor.
- A las expresiones de valor se les debe asignar un tipo de valor. El tipo de valor de scripts de sitios puede ser: 1) Etiqueta, 2) Atributo o 3) Patrón.
- Puede tener varias reglas de relajación por combinación de nombre de campo/URL
- Los nombres de los campos del formulario y las URL de acción no distinguen entre mayúsculas y minúsculas.

Uso de la línea de comandos para configurar la comprobación de scripts de sitios HTML

Para configurar las acciones de comprobación de scripts de sitios HTML y otros parámetros mediante la línea de comandos

Si utiliza la interfaz de línea de comandos, puede introducir los siguientes comandos para configurar la comprobación de scripts de sitios HTML:

- set appfw profile topic.
- <name> -crossSiteScriptingAction (([block] [learn] [log] [stats])| [** none**])
- [set appfw profile topic.
- <name> **-crossSiteScriptingTransformUnsafeHTML** (ON | OFF)
- set appfw profile topic.
- <name> -crossSiteScriptingCheckCompleteURLs (ON | OFF)
- set appfw profile topic.
- ‘ - checkRequestHeaders (ON \| OFF)
- <name> - CheckRequestQueryNonHtml (ON | OFF)

Para configurar una regla de relajación de comprobación de scripts de sitios HTML mediante la línea de comandos

Utilice el comando bind o unbind para agregar o eliminar enlaces, como se indica a continuación:

- bind appfw profile <name> -crossSiteScripting <String> [isRegex (REGEX | NOTREGEX)] <formActionURL> [-location <location>] [-valueType (Tag| Attribute|Pattern)[<valueExpression>] [-isValueRegex (REGEX | NOTREGEX)]]
- unbind appfw profile <name> -crossSiteScripting <String> <formActionURL > [-location <location>] [-valueType (Tag |Attribute|Pattern)[<valueExpression >]]

Uso de la interfaz gráfica de usuario para configurar la comprobación de scripts de sitios HTML

En la GUI, puede configurar la comprobación HTML Cross-Site Scripting en el panel para el perfil asociado a su aplicación.

Para configurar o modificar la comprobación de scripts de sitios HTML mediante la interfaz gráfica de usuario

1. Vaya a **Firewall de aplicaciones** > **Perfiles**, resalte el perfil de destino y haga clic en **Modificar**.
2. En el panel **Configuración avanzada**, haga clic en **Comprobaciones de seguridad**.

La tabla de comprobación de seguridad muestra los valores de acción configurados actualmente para todas las comprobaciones de seguridad. Tiene 2 opciones de configuración:

a. Si quiere habilitar o inhabilitar las acciones **Bloquear**, **Registrar**, **Estadísticas** y **Aprender** para los scripts HTML de sitios, puede marcar o desmarcar las casillas de la tabla, hacer clic en **Aceptar** y, a continuación, hacer clic en **Guardar y cerrar** para cerrar el panel **Comprobación de seguridad**.

b. Si quiere configurar más opciones para esta comprobación de seguridad, haga doble clic en **HTML Cross-Site Scripting**o seleccione la fila y haga clic en **Configuración de acciones**para mostrar las siguientes opciones:

Transformar scripts de sitios: Transforma etiquetas de scripts no seguros.

Comprobar las URL completas para scripts de sitios: En lugar de verificar solo la parte de consulta de la URL, verifique la URL completa para detectar infracciones de scripts de sitios.

Después de cambiar cualquiera de las configuraciones anteriores, haga clic en **Aceptar** para guardar los cambios y volver a la tabla Comprobaciones de seguridad. Puede proceder a configurar otras comprobaciones de seguridad si es necesario. Haga clic en **Aceptar** para guardar todos los cambios que ha realizado en la sección **Comprobaciones de seguridad** y, a continuación, haga clic en **Guardar y cerrar** para cerrar el panel **Comprobación de seguridad**.

Para habilitar o inhabilitar la configuración **Comprobar encabezado de solicitud**, en el panel **Configuración avanzada**, haga clic en **Configuración de perfil**. En **Configuración común**, marque o desmarque la casilla **Comprobar encabezados de solicitud**. Haga clic en **Aceptar**. Puede usar el icono **X** en la parte superior derecha del panel **Configuración del perfil** para cerrar esta sección o, si ha terminado de configurar este perfil, puede **hacer clic en Listo** para volver a **Firewall de aplicaciones** > **Perfil**.

Para habilitar o inhabilitar la configuración **Consulta de solicitud de verificación no HTML**, en el panel **Configuración avanzada**, haga clic en **Configuración de perfil**. En **Configuración común**, marque o desmarque la casilla **Comprobar solicitud de consulta que no es HTML**. Haga clic en **Aceptar**. Puede usar el icono X en la parte superior derecha del panel **Configuración del perfil** para cerrar esta sección o, si ha terminado de configurar este perfil, puede **hacer clic en Listo** para volver a **App Firewall > Perfil**.

Para configurar una regla de relajación de scripts de sitios HTML mediante la interfaz gráfica de usuario

1. Vaya a **Firewall de aplicaciones** > **Perfiles**, resalte el perfil de destino y haga clic en **Modificar**.
2. En el panel **Configuración avanzada**, haga clic en **Reglas de relajación**.
3. En la tabla Reglas de relajación, haga doble clic en la entrada **HTML Cross-Site Scripting** o selecciónela y haga clic en **Modificar**.
4. En el cuadro de diálogo **Reglas de relajación de scripts de sitios HTML**, realice las operaciones **Agregar**, **Modificar**, **Eliminar**, **Habilitar**o **Inhabilitar** para las reglas de relajación.

> **Nota**
>
> Al agregar una nueva regla, el campo **Expresión de valor** no se muestra a menos que seleccione

> la opción **Etiqueta**, **Atributo** o **Patrón** en el campo **Tipo de valor**.

Para administrar las reglas de relajación de scripts de sitios HTML mediante el visualizador

Para obtener una vista consolidada de todas las reglas de relajación, puede resaltar la fila **HTML Cross-Site Scripting** en la tabla Reglas de relajación y hacer clic en **Visualizador**. El visualizador de relajaciones desplegadas le ofrece la opción de **agregar** una nueva regla o **modificar** una existente. También puede **habilitar** o **inhabilitar** un grupo de reglas seleccionando un nodo y haciendo clic en los botones correspondientes en el visualizador de relajación.

Para ver o personalizar los patrones de scripts de sitios mediante la interfaz gráfica de usuario

Puede utilizar la interfaz gráfica de usuario para ver o personalizar la lista predeterminada de atributos o etiquetas permitidas de scripts de sitios. También puede ver o personalizar la lista predeterminada de patrones denegados de scripts de sitios.

Las listas predeterminadas se especifican en **Firewall de aplicaciones** > **Firmas > Firmaspredeterminadas**. Si no vincula ningún objeto de firma a su perfil, el perfil utilizará la lista predeterminada de scripts de sitios permitidas y denegadas especificada en el objeto Firmas predeterminadas para el procesamiento de la comprobación de seguridad de scripts de sitios. Las etiquetas, atributos y patrones, especificados en el objeto de firmas predeterminado, son de solo lectura. No puede modificarlos ni modificarlos. Si quiere modificarlos o cambiarlos, haga una copia del objeto Firmas predeterminadas para crear un objeto de firma definido por el usuario. Realice cambios en las listas permitidas o denegadas en el nuevo objeto de firma definido por el usuario y use este objeto de firma en su perfil que procesa el tráfico para el que quiere usar estas listas personalizadas de permitidos y denegados.

1. Para ver los patrones de scripts de sitios predeterminados:

a. Vaya a **Firewall de aplicaciones** > **Firmas**, seleccione **Firmas predeterminadas**y haga clic en **Modificar**. A continuación, haga clic en **Administrar patrones de scripts SQL/de sitios**.

En la tabla **Administrar rutas de scripts SQL/de sitios** se muestran las tres filas siguientes relacionadas con los scripts de sitios:

`xss/allowed/attribute`

`xss/allowed/tag`

`xss/denied/pattern`

b. Seleccione una fila y haga clic en **Administrar elementos** para mostrar los elementos de scripts de sitios correspondientes (etiqueta, atributo, patrón) utilizados por la comprobación de scripts de sitios** de Web App Firewall.

1. **Para personalizar elementos de scripts de sitios**: puede modificar el objeto de firma definido por el usuario para personalizar la etiqueta, los atributos permitidos y los patrones denegados permitidos. Puede agregar nuevas entradas o eliminar las existentes.

a. Vaya a **Firewall de aplicaciones** > **Firmas**, resalte la firma definida por el usuario de destino y haga clic en **Modificar**. Haga clic en **Administrar patrones de scripts SQL/de sitios** para mostrar la tabla **Administrar rutas de scripts SQL/de sitios**.

b. Seleccione la fila de scripts de sitios de destino.

i. Haga clic en **Administrar elementos**para **agregar**, **modificar** o **eliminar** el elemento de scripts de sitios correspondiente.

ii. Haga clic en **Eliminar** para quitar la fila seleccionada.

> **Advertencia:**
>
> Debe tener cuidado antes de eliminar o modificar cualquier elemento predeterminado de scripts de sitios, o eliminar la ruta de scripts de sitios para eliminar toda la fila. Las reglas de firma y la comprobación de seguridad de scripts de sitios se basan en estos elementos para detectar ataques con el fin de proteger sus aplicaciones. Personalizar los elementos de scripts de sitios puede hacer que su aplicación sea vulnerable a los ataques de scripts de sitios si se elimina el patrón requerido durante la edición.

Aprender las infracciones de scripts de sitios HTML (scripts de sitios)

Con el aprendizaje habilitado, el motor de aprendizaje de Citrix Web App Firewall supervisa el tráfico y aprende las infracciones de URL de scripts de sitios. Puede inspeccionar periódicamente las reglas de URL de scripts de sitios e implementarlas en escenarios de falsos positivos.

> **Nota:**
>
> En una configuración de clúster, todos los nodos deben ser de la misma versión para implementar las reglas de URL de scripts de sitios.

Como parte de la configuración de aprendizaje, Web App Firewall ofrece un aprendizaje detallado de scripts de sitios HTML. El motor de aprendizaje hace recomendaciones con respecto al tipo de valor observado (etiqueta, atributo, patrón) y la expresión de valor correspondiente observada en los campos de entrada. Además de comprobar las solicitudes bloqueadas para determinar si la regla actual es demasiado restrictiva y necesita ser relajada, puede revisar las reglas generadas por el motor de aprendizaje para determinar qué tipo de valor y expresiones de valor están desencadenando infracciones y deben abordarse en las reglas de relajación.

> **Nota:**
>
> El motor de aprendizaje de Web App Firewall puede distinguir solo los primeros 128 bytes del nombre. Si un formulario tiene varios campos con nombres que coinciden con los primeros 128 bytes, es posible que el motor de aprendizaje no pueda distinguir entre ellos. Del mismo modo, la regla de relajación implementada podría relajar inadvertidamente todos esos campos de la

> inspección de scripts de sitios HTML.
>
> **Sugerencia:**
>
> Las etiquetas de scripts de sitios que tienen más de 12 caracteres no se aprenden ni se registran correctamente.
>
> Si necesita una longitud de etiqueta mayor para el aprendizaje, puede agregar una etiqueta grande que no aparezca en **AS_cross-site Scripting_allowed_tags_list** para una longitud 'x'.

El proceso de aprendizaje de scripts de sitios HTML reduce los falsos positivos en los ataques de scripts de sitios. Con el aprendizaje habilitado, puede aprender todas las infracciones en una solicitud y, potencialmente, aplicar relajación a varias etiquetas, atributos o patrones sin necesidad de repetición.

Por ejemplo, si hay 15 etiquetas personalizadas en una carga útil, cada una de las cuales resulta en una infracción, puede aplicar la relajación de grano fino a todas las etiquetas marcadas como infracción, en lugar de repetir el proceso para aplicar la relajación de una etiqueta a la vez.

Escenario 1: aprendizaje habilitado y bloqueo habilitado:
en este escenario, el dispositivo Citrix ADC detecta todas las infracciones en etiquetas/atributos/patrones personalizados, y la solicitud se bloquea y se registra cada infracción. El comportamiento es coherente para las infracciones identificadas en el campo del formulario, el encabezado o la cookie.

Escenario 2: aprendizaje habilitado y bloqueo inhabilitado:
en este escenario, el dispositivo Citrix ADC aprende las infracciones en etiquetas/atributos/patrones personalizados y se registra cada una de las infracciones. La solicitud no está bloqueada. El comportamiento es coherente para las infracciones identificadas en el campo del formulario, el encabezado o la cookie.

Para ver o utilizar datos aprendidos mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba uno de los siguientes comandos:

- `show appfw learningdata <profilename> crossSiteScripting`
- `rm appfw learningdata <profilename> -crossSiteScripting <string> <formActionURL> [<location>] [<valueType> <valueExpression>]`
- `export appfw learningdata <profilename> **crossSiteScripting*`

Configurar la relajación de grano fino de scripts de sitios para omitir las etiquetas personalizadas

Puede configurar la relajación de scripts de sitios en el perfil de firewall de aplicaciones web para omitir las etiquetas/atributos/patrones personalizados que no están presentes en la lista de permitidos. En el símbolo del sistema, escriba:

```
bind appfw profile p1 -crossSiteScripting <string> <formActionURL> -valueType
 <valueType> <value expression>
```


Ejemplo:

```
bind appfw profile profile1 -crossSiteScripting formfield1 http://1.1.1.1 -
valueType Tag tag1
```

Para ver o usar datos aprendidos mediante la interfaz gráfica de usuario

1. Vaya a **Firewall de aplicaciones** > **Perfiles**, resalte el perfil de destino y haga clic en **Modificar**.
2. En el panel **Configuración avanzada**, haga clic en **Reglas aprendidas**. Puede seleccionar la entrada **HTML Cross-Site Scripting** en la tabla Reglas aprendidas y hacer doble clic en ella para acceder a las reglas aprendidas. En la tabla se muestran las columnas **Nombre de campo**, **URL de una acción**, **Tipo de valor**, **Valor** y **Visitas**. Puede implementar las reglas aprendidas o modificar una regla antes de implementarla como regla de relajación. Para descartar una regla, puede seleccionarla y hacer clic en el botón **Omitir**. Solo puede modificar una regla a la vez, pero puede seleccionar varias reglas para implementarlas u omitirlas.

También tiene la opción de mostrar una vista resumida de las relajaciones aprendidas seleccionando la entrada **HTML Cross-Site Scripting** en la tabla Reglas aprendidas y haciendo clic en **Visualizador** para obtener una vista consolidada de todas las infracciones aprendidas. El visualizador facilita la gestión de las reglas aprendidas. Presenta una vista completa de los datos en una pantalla y facilita la acción sobre un grupo de reglas con un solo clic. La mayor ventaja del visualizador es que recomienda expresiones regulares para consolidar varias reglas. Puede seleccionar un subconjunto de estas reglas, en función del delimitador y de la URL de acción. Puede mostrar 25, 50 o 75 reglas en el visualizador, seleccionando el número en una lista desplegable. El visualizador de reglas aprendidas ofrece la opción de modificar las reglas e implementarlas como relajaciones. O puede saltarse las reglas para ignorarlas.

Uso de la función de registro con la comprobación de scripts de sitios HTML

Cuando la acción de registro está habilitada, las infracciones de comprobación de seguridad de scripts de sitios HTML se registran en el registro de auditoría como infracciones de **scripts APPFW_cross-site**. El Web App Firewall admite los formatos de registro nativo y CEF. También puede enviar los registros a un servidor syslog remoto.

Para acceder a los mensajes de registro mediante la línea de comandos

Cambie al shell y siga los ns.logs en la carpeta `/var/log/` para acceder a los mensajes de registro relacionados con las infracciones de scripts de sitios HTML:

```
Shell
tail -f /var/log/ns.log | grep APPFW_cross-site scripting
```

Ejemplo de un mensaje de registro de infracciones de comprobación de seguridad de scripts de sitios en formato de registro CEF:


```
Jul 11 00:45:51 <local0.info> 10.217.31.98 CEF:0|Citrix|Citrix ADC|NS11
    .0|APPFW|\*\*APPFW_cross-site scripting\*\*|6|src=10.217.253.62
    geolocation=Unknown spt=4840 method=GET request=http://aaron.
    stratum8.net/FFC/CreditCardMind.html?abc=%3Cdef%3E msg=\*\*Cross-
    site script check failed for field abc=”Bad tag: def”\*\* cn1=133
    cn2=294 cs1=pr_ffc cs2=PPE1 cs3=eUljypvLa0BbabwfGVE52Sewg9U0001 cs4=
    ALERT cs5=2015 act=\*\*not blocked\*\*
<!--NeedCopy-->
```

Ejemplo de mensaje de registro de infracción de comprobación de seguridad de scripts de sitios en formato de registro nativo que muestra la acción de transformación

```
Jul 11 01:00:28 <local0.info> 10.217.31.98 07/11/2015:01:00:28 GMT ns
    0-PPE-0 : default APPFW \*\*APPFW_cross-site scripting\*\* 132 0 :
    10.217.253.62 392-PPE0 eUljypvLa0BbabwfGVE52Sewg9U0001 pr_ffc http:
    //aaron.stratum8.net/FFC/login.php?login_name=%3CBOB%3E&passwd=&
    drinking_pref=on &text_area=&loginButton=ClickToLogin&as_sfid=
    AAAAAAVFqmYL68IGvkrcn2pzehjfIkm5E6EZ9FL8YLvIW_41AvAATuKYe9N7uGThSpEAxbb0iBx55j
    -FC4llF \*\*Cross-site script special characters seen in fields <
    transformed>\*\*
<!--NeedCopy-->
```

Acceder a los mensajes de registro mediante la GUI

La GUI de Citrix incluye una herramienta útil (Syslog Viewer) para analizar los mensajes de registro. Tiene varias opciones para acceder al Visor de Syslog:

- Vaya a **Firewall de aplicaciones** > **Perfiles**, seleccione el perfil de destino y haga clic en **Comprobaciones de seguridad**. Resalte la fila **HTML Cross-Site Scripting** y haga clic en **Registros**. Cuando accede a los registros directamente desde la comprobación HTML Cross-Site Scripting del perfil, la GUI filtra los mensajes de registro y muestra solo los registros relacionados con estas infracciones de comprobación de seguridad.
- También puede acceder al Visor de Syslog navegando a **Citrix ADC** > **Sistema** > **Auditoría**. En la sección **Mensajes de auditoría**, haga clic en el enlace **Mensajes de Syslog** para mostrar el Visor de Syslog, que muestra todos los mensajes de registro, incluidos otros registros de infracciones de comprobación de seguridad. Esto resulta útil para depurar cuando se pueden desencadenar varias infracciones de comprobación de seguridad durante el procesamiento de solicitudes.
- Vaya a **Firewall de aplicaciones** > **directivas** > **Auditoría**. En la sección Mensajes de auditoría, haga clic en el enlace **Mensajes de syslog** para mostrar el Visor de Syslog, que muestra todos los mensajes de registro, incluidos otros registros de infracciones de comprobación de seguridad.

El Visor de Syslog basado en HTML proporciona varias opciones de filtro para seleccionar solo los mensajes de registro que le interesan. Para seleccionar mensajes de registro para la comprobación de scripts de sitios**HTML**, filtre seleccionando **APPFW** en las opciones de la lista desplegable para el **módulo**. La lista **Tipo de evento** ofrece un amplio conjunto de opciones para refinar aún más su selección. Por ejemplo, si marca la casilla **Scripts AppFW_cross-site** y hace clic en el botón **Aplicar**, solo aparecerán en el Visor de Syslog los mensajes de registro relacionados con las infracciones de la comprobación de **seguridad de scripts de sitios HTML**.

Si coloca el cursor en la fila de un mensaje de registro específico, aparecen varias opciones, como **Módulo**, **Tipo de evento**, **ID de evento**, **IP de cliente**, etc., debajo del mensaje de registro. Puede seleccionar cualquiera de estas opciones para resaltar la información correspondiente en el mensaje de registro.

La funcionalidad**Hacer clic para implementar** solo está disponible en la GUI. Puede usar Syslog Viewer no solo para ver los registros, sino también para implementar las reglas de relajación de scripts de sitios HTML basadas en los mensajes de registro de las infracciones de comprobación de seguridad de Web App Firewall. Los mensajes de registro deben estar en formato de registro CEF para esta operación. La funcionalidad Hacer clic para implementar solo está disponible para los mensajes de registro generados por la acción bloquear (o no bloquear). No puede implementar una regla de relajación para un mensaje de registro sobre la operación de transformación.

Para implementar una regla de relajación desde el Visor de Syslog, seleccione el mensaje de registro. Aparece una casilla de verificación en la esquina superior derecha del cuadro **Visor de Syslog** de la fila seleccionada. Seleccione la casilla de verificación y, a continuación, seleccione una opción de la lista **Acción** para implementar la regla de relajación. **Modificar e implementar**, **Implementar** e **Implementar todo** están disponibles como opciones de **Acción**.

Las reglas de scripts de sitios HTML que se implementan mediante la opción **Hacer clic para implementar** no incluyen las recomendaciones de relajación de grano fino.

Configurar la función clic para implementar mediante la interfaz gráfica de usuario

1. En el Visor de Syslog, seleccione **APPFW** en las opciones de **Módulo**.
2. Seleccione **Scripts APP_cross-site** como **Tipo de evento** para filtrar los mensajes de registro correspondientes.
3. Seleccione la casilla de verificación para identificar la regla que se va a implementar.
4. Utilice la lista desplegable **Acción** de opciones para implementar la regla de relajación.
5. Compruebe que la regla aparece en la sección de reglas de relajación correspondiente.

Estadísticas de las infracciones de scripts de sitios HTML

Cuando la acción de estadísticas está habilitada, el contador de la comprobación de scripts de sitios HTML se incrementa cuando Web App Firewall realiza cualquier acción para esta comprobación de se-

guridad. Las estadísticas se recopilan para Rate and Total count para Tráfico, Infracciones y Registros. El tamaño de un incremento del contador de registro puede variar en función de la configuración configurada. Por ejemplo, si la acción de bloqueo está habilitada, la solicitud de una página que contiene 3 infracciones de scripts de sitios HTML aumenta el contador de estadísticas en uno, ya que la página se bloquea cuando se detecta la primera infracción. Sin embargo, si el bloque está inhabilitado, el procesamiento de la misma solicitud aumenta en tres el contador de estadísticas de infracciones y registros, porque cada infracción genera un mensaje de registro independiente.

Para mostrar scripts de sitios HTML, compruebe las estadísticas mediante la línea de comandos

En el símbolo del sistema, escriba:

```
> sh appfw stats
```

Para mostrar las estadísticas de un perfil específico, use el siguiente comando:

```
> **stat appfw profile** <profile name>
```

Mostrar estadísticas de scripts de sitios HTML mediante la interfaz gráfica de usuario

1. Vaya a **Seguridad** > **Firewall de aplicaciones > Perfiles > Estadísticas**.
2. En el panel derecho, acceda al enlace de **Estadísticas**.
3. Use la barra de desplazamiento para ver las estadísticas sobre las infracciones y los registros de scripts de sitios HTML. La tabla de estadísticas proporciona datos en tiempo real y se actualiza cada 7 segundos.

Resumen

- **Compatibilidad integrada para la protección contra ataques de scripts de sitios HTML**: Citrix Web App Firewall protege contra los ataques de scripts de sitios mediante la supervisión de una combinación de atributos y etiquetas permitidos y patrones denegados en la carga recibida. Todas las etiquetas permitidas predeterminadas integradas, los atributos permitidos y los patrones denegados utilizados por la comprobación de scripts de sitios se especifican en el archivo /netscaler/default_custom_settings.xml.
- **Personalización**: puede cambiar la lista predeterminada de etiquetas, atributos y patrones para personalizar la inspección de comprobación de seguridad de scripts de sitios para las necesidades específicas de su aplicación. Realice una copia del objeto de firma predeterminado, modifique las entradas existentes o agregue otras nuevas. Enlaza este objeto de firma a tu perfil para hacer uso de la configuración personalizada.
- **Modelo de seguridad híbrido**: Tanto las firmas como las protecciones de seguridad profundas utilizan los patrones de scripts SQL/de sitios especificados en el objeto de firma que está enlazado al perfil. Si ningún objeto de firma está enlazado al perfil, se utilizan los patrones de scripts SQL/de sitios presentes en el objeto de firma predeterminado.

- **Transformación**: tenga en cuenta lo siguiente sobre la operación de transformación:

La operación de transformación funciona independientemente de las demás configuraciones de acción de scripts de sitios. Si la transformación está habilitada y el bloqueo, el registro, las estadísticas y el aprendizaje están desactivados, las etiquetas de scripts de sitios se transforman.

Si la acción de bloqueo está habilitada, tiene prioridad sobre la acción de transformación.

- **Relajación y aprendizaje de grano fino**. Ajuste la regla de relajación para relajar un subconjunto de elementos de scripts de sitios de la inspección de controles de seguridad, pero para detectar el resto. El motor de aprendizaje recomienda un tipo de valor específico y expresiones de valor basadas en los datos observados.
- **Hacer clic para implementar**: seleccione uno o varios mensajes de registro de infracciones de scripts de sitios en el visor de syslog e impleméntelos como reglas de relajación.
- **Conjunto de caracteres**: el conjunto de caracteres predeterminado para el perfil debe establecerse en función de la necesidad de la aplicación. De forma predeterminada, el conjunto de caracteres del perfil está configurado en inglés de EE. UU. (ISO-8859-1). Si se recibe una solicitud sin el conjunto de caracteres especificado, Web App Firewall procesa la solicitud como si fuera ISO-8859-1. El carácter de corchete abierto (<) o de corchete cerrado (>) no se interpretará como etiquetas de scripts de sitios si estos caracteres están codificados en otros conjuntos de caracteres. Por ejemplo, si una solicitud contiene una cadena de caracteres UTF-8 “%uff1cscript%uff1e**“**pero el juego de caracteres no se especifica en la página de solicitud, es posible que la infracción de scripts de sitios no se active a menos que el juego de caracteres predeterminado para el perfil se especifique como Unicode.

Comprobación de inyección HTML SQL

April 21, 2022

Muchas aplicaciones web tienen formularios web que usan SQL para comunicarse con los servidores de bases de datos relacionales. El código malicioso o un hacker pueden usar un formulario web inseguro para enviar comandos SQL al servidor web. La comprobación de inyección SQL HTML de Web App Firewall proporciona defensas especiales contra la inyección de código SQL no autorizado que podría afectar la seguridad. Si Web App Firewall detecta código SQL no autorizado en una solicitud de usuario, transforma la solicitud para que el código SQL esté inactivo o bloquea la solicitud. El Web App Firewall examina la carga útil de solicitud para el código SQL inyectado en tres ubicaciones: 1) cuerpo POST, 2) encabezados y 3) cookies. Para examinar una parte de consulta en las solicitudes de código SQL inyectado, configure una configuración de perfil de firewall de aplicaciones ‘InspectQueryContentTypes’ para los tipos de contenido específicos.

Un conjunto predeterminado de palabras clave y caracteres especiales proporciona palabras clave

conocidas y caracteres especiales que se utilizan comúnmente para lanzar ataques SQL. Puede agregar nuevos patrones y modificar el conjunto por defecto para personalizar la inspección de comprobación SQL. Web App Firewall ofrece varias opciones de acción para implementar la protección de inyección de SQL. Además de las acciones **Bloquear**, **Registrar**, **Estadísticas** y **Aprender**, el perfil de Web App Firewall también ofrece la opción de **transformar caracteres especiales de SQL** para que un ataque sea inofensivo.

Además de las acciones, hay varios parámetros que se pueden configurar para el procesamiento de inyección SQL. Puede comprobar si hay **caracteres comodín SQL**. Puede cambiar el tipo de inyección SQL y seleccionar una de las 4 opciones (**SQLKeyword**, **SQLSplChar**, **SQLSplCharAndKeyword**, **SQLSplcharorKeyword**) para indicar cómo evaluar las palabras clave SQL y los caracteres especiales SQL al procesar la carga útil. El **parámetro Gestión de comentarios SQL** le da la opción de especificar el tipo de comentarios que deben inspeccionarse o eximirse durante la detección de inyección SQL.

Puede implementar relajaciones para evitar falsos positivos. El motor de aprendizaje de Web App Firewall puede proporcionar recomendaciones para configurar reglas de relajación.

Están disponibles las siguientes opciones para configurar una protección de inyección SQL optimizada para la aplicación:

Bloquear—La acción de bloqueo se activa solo si la entrada coincide con la especificación de tipo de inyección SQL. Por ejemplo, si **SQLSplCharANDKeyword** está configurado como el tipo de inyección SQL, una solicitud no se bloquea si no contiene palabras clave, incluso si se detectan caracteres especiales de SQL en la entrada. Dicha solicitud se bloquea si el tipo de inyección SQL se establece en **SQLSplChar**o **SQLSplcharorKeyword**.

Log: Si habilita la función de registro, la comprobación de SQL Injection genera mensajes de registro que indican las acciones que realiza. Si la acción de bloqueo está inhabilitada, se genera un mensaje de registro independiente para cada campo de entrada en el que se detectó la infracción de SQL. Sin embargo, solo se genera un mensaje cuando se bloquea la solicitud. Del mismo modo, se genera un mensaje de registro por solicitud para la operación de transformación, incluso cuando los caracteres especiales de SQL se transforman en varios campos. Puede supervisar los registros para determinar si las respuestas a las solicitudes legítimas se están bloqueando. Un gran aumento en la cantidad de mensajes de registro puede indicar intentos de lanzar un ataque.

Estadísticas: si está habilitada, la función de estadísticas recopila estadísticas sobre infracciones y registros. Un aumento inesperado en el contador de estadísticas podría indicar que su aplicación está siendo atacada. Si las solicitudes legítimas se bloquean, es posible que tenga que volver a revisar la configuración para ver si necesita configurar nuevas reglas de relajación o modificar las existentes.

Aprender: si no está seguro de qué reglas de relajación de SQL podrían ser las más adecuadas para su aplicación, puede usar la función de aprendizaje para generar recomendaciones basadas en los datos aprendidos. El motor de aprendizaje de Web App Firewall supervisa el tráfico y proporciona recomendaciones de aprendizaje de SQL en función de los valores observados. Para obtener un benefi-

cio óptimo sin comprometer el rendimiento, es posible que desee habilitar la opción de aprendizaje durante un tiempo breve para obtener una muestra representativa de las reglas y, a continuación, implementar las reglas y inhabilitar el aprendizaje.

Transformar caracteres especiales de SQL: Web App Firewall considera tres caracteres, comillas simples (') (\), barra invertida y punto y coma (;) como caracteres especiales para el procesamiento de comprobaciones de seguridad de SQL. La función Transformación SQL modifica el código de inyección SQL en una solicitud HTML para garantizar que la solicitud se convierta en inofensiva. La solicitud HTML modificada se envía al servidor. Todas las reglas de transformación predeterminadas se especifican en el archivo /netscaler/default_custom_settings.xml.

La operación de transformación hace que el código SQL esté inactivo al realizar los siguientes cambios en la solicitud:

- Comilla simple (') a comilla recta doble (").
- Barra invertida (\) a barra invertida doble (\).
- El punto y coma (;) se elimina por completo.

Estos tres caracteres (cadenas especiales) son necesarios para emitir comandos a un servidor SQL. A menos que un comando SQL vaya precedido de una cadena especial, la mayoría de los servidores SQL ignoran ese comando. Por lo tanto, los cambios que realiza Web App Firewall cuando la transformación está habilitada evitan que un atacante inyecte SQL activo. Una vez realizados estos cambios, la solicitud se puede enviar de forma segura a su sitio web protegido. Cuando los formularios web de su sitio web protegido pueden contener legítimamente cadenas especiales de SQL, pero los formularios web no dependen de las cadenas especiales para funcionar correctamente, puede inhabilitar el bloqueo y habilitar la transformación para evitar el bloqueo de datos legítimos de formularios web sin reducir la protección que Web Application Firewall proporciona a sus sitios web protegidos.

La operación de transformación funciona independientemente de la configuración **Tipo de inyección SQL** . Si la transformación está habilitada y el tipo de inyección SQL se especifica como palabra clave SQL, los caracteres especiales SQL se transforman incluso si la solicitud no contiene palabras clave.

> **Sugerencia**
>
> Normalmente habilita la transformación o el bloqueo, pero no ambos. Si la acción de bloqueo está habilitada, tiene prioridad sobre la acción de transformación. Si tiene activado el bloqueo, la activación de la transformación es redundante.

Buscar caracteres comodín SQL: los caracteres comodín se pueden utilizar para ampliar las selecciones de una instrucción SQL (SQL-SELECT). Estos operadores comodín se pueden utilizar con los operadores **LIKEy NOTE LIKE** para comparar un valor con valores similares. Los caracteres de porcentaje (%) y subrayado (_) se utilizan con frecuencia como comodines. El signo de porcentaje es análogo al carácter comodín de asterisco (*) que se usa con MS-DOS y coincide con cero, uno o varios caracteres en un campo. El guion bajo es similar al signo de interrogación de MS-DOS (?) carácter comodín. Coincide con un solo número o carácter en una expresión.

Por ejemplo, puede usar la siguiente consulta para realizar una búsqueda de cadenas para encontrar todos los clientes cuyos nombres contengan el carácter D.

SELECT * del nombre WHERE del cliente como “%D%”:

El siguiente ejemplo combina los operadores para encontrar cualquier valor salarial que tenga 0 en segundo y tercer lugar.

SELECCIONE* del cliente DONDE el salario como ‘_00%’:

Diferentes proveedores de DBMS han ampliado los caracteres comodín agregando operadores adicionales. Citrix Web App Firewall puede protegerse contra los ataques que se inician mediante la inyección de estos caracteres comodín. Los 5 caracteres comodín predeterminados son porcentaje (%), guión bajo (_), intercalación (^), corchete de apertura ([) y corchete de cierre (]). Esta protección se aplica tanto a perfiles HTML como XML.

Los caracteres comodín predeterminados son una lista de literales especificados en la ***Firmas predeterminadas**:

- `<wildchar type=” LITERAL” >%</wildchar>`
- `<wildchar type=” LITERAL” >_</wildchar>`
- `<wildchar type=” LITERAL” >^</wildchar>`
- `<wildchar type=” LITERAL” >[</wildchar>`
- `<wildchar type=” LITERAL” >]</wildchar>`

Los caracteres comodín en un ataque pueden ser PCRE, como [^A-F]. El Web App Firewall también admite comodines PCRE, pero los caracteres comodín literales anteriores son suficientes para bloquear la mayoría de los ataques.

> **Nota:**
>
> La comprobación de caracteres comodín SQL es diferente de la comprobación de caracteres especiales SQL. Esta opción debe usarse con precaución para evitar falsos positivos.

Solicitud de verificación que contiene el tipo de inyección SQL: Web App Firewall proporciona 4 opciones para implementar el nivel de rigurosidad deseado para la inspección de inyección SQL, en función de las necesidades individuales de la aplicación. La solicitud se compara con la especificación del tipo de inyección para detectar infracciones de SQL. Las 4 opciones de tipo de inyección SQL son:

- **Carácter especial y palabra clave SQL**: tanto una palabra clave SQL como un carácter especial SQL deben estar presentes en la entrada para desencadenar una infracción SQL. Esta configuración menos restrictiva también es la configuración predeterminada.
- **Carácter especial de SQL**: al menos uno de los caracteres especiales debe estar presente en la entrada para desencadenar una infracción de SQL.
- **Palabra clave SQL**: al menos una de las palabras clave SQL especificadas debe estar presente en la entrada para desencadenar una infracción SQL. No seleccione esta opción sin la debida

consideración. Para evitar falsos positivos, asegúrese de que no se espera ninguna de las palabras clave en las entradas.

- **Character especial o palabra clave de SQL**: La palabra clave o la cadena de caracteres especial deben estar presentes en la entrada para desencadenar la infracción de comprobación de seguridad.

> **Sugerencia:**
>
> Si configura Web App Firewall para buscar entradas que contengan un carácter especial de SQL, Web App Firewall omite los campos de formulario web que no contienen caracteres especiales. Dado que la mayoría de los servidores SQL no procesan comandos SQL que no van precedidos de un carácter especial, habilitar esta opción puede reducir significativamente la carga en Web App Firewall y acelerar el procesamiento sin poner en riesgo sus sitios web protegidos.

Gestión de comentarios SQL: de forma predeterminada, Web App Firewall comprueba todos los comentarios SQL en busca de comandos SQL inyectados. Sin embargo, muchos servidores SQL ignoran cualquier cosa en un comentario, incluso si van precedidos de un carácter especial de SQL. Para un procesamiento más rápido, si su servidor SQL ignora los comentarios, puede configurar Web App Firewall para que omita los comentarios al examinar las solicitudes de SQL inyectado. Las opciones de manejo de comentarios SQL son:

- **ANSI**: omite los comentarios SQL en formato ANSI, que normalmente utilizan las bases de datos SQL basadas en UNIX. Por ejemplo:
  - — (Dos guiones) - Este es un comentario que comienza con dos guiones y termina con el final de la línea.
  - {}: Tirantes (Las llaves encierran el comentario. El {precede al comentario y el} lo sigue. Las llaves pueden delimitar los comentarios de una o varias líneas, pero los comentarios no se pueden anidar)
  - `/**/: C style comments (Does not allow nested comments). Please note /*! <comment that begin with slash followed by asterisk and exclamation mark is not a comment > */`
  - MySQL Server admite algunas variantes de comentarios de estilo C. Estos le permiten escribir código que incluye extensiones MySQL, pero que aún es portátil, mediante comentarios de la siguiente forma:`/*! MySQL-specific code */`
  - . #: Comentarios de Mysql: Este es un comentario que comienza con el carácter #.
- **Anidado**: Omita los comentarios de SQL anidados, que normalmente utiliza Microsoft SQL Server. Por ejemplo; — (Dos guiones) y **/* */** (Permite comentarios anidados)
- **ANSI/anidado**: Omite los comentarios que se ajustan a los estándares de comentarios ANSI y SQL anidados. Los comentarios que coincidan solo con el estándar ANSI, o solo con el estándar anidado, aún se comprueban en busca de SQL inyectado.
- **Comprobar todos los comentarios**: compruebe toda la solicitud de SQL inyectado sin omitir nada. Esta es la opción predeterminada.

> **Sugerencia**
>
> Por lo general, no debe elegir la opción Andado o ANSI/anidado a menos que la base de datos back-end se ejecute en Microsoft SQL Server. La mayoría de los otros tipos de software de SQL Server no reconocen los comentarios anidados. Si los comentarios anidados aparecen en una solicitud dirigida a otro tipo de servidor SQL, pueden indicar un intento de violar la seguridad en ese servidor.

Comprobar encabezados de solicitud: habilite esta opción si, además de examinar la entrada en los campos del formulario, quiere examinar los encabezados de solicitud en busca de ataques de inyección HTML SQL. Si utiliza la GUI, puede habilitar este parámetro en el panel **Configuración avanzada -> Configuración** del **perfil** del perfil Web App Firewall.

> **Nota:**
>
> Si habilita el indicador de encabezado Solicitud de comprobación, es posible que tenga que configurar una regla de relajación para el encabezado **User-Agent** . La presencia de la palabra clave SQL **como** y el carácter especial SQL punto y coma (**;**) podría desencadenar solicitudes falsas positivas y bloquear que contienen este encabezado.
>
> **Advertencia**
>
> Si habilita la verificación y la transformación del encabezado de solicitud, los caracteres especiales de SQL que se encuentren en los encabezados también se transforman. Los encabezados Accept, Accept-Charset, Accept-Encoding, Accept-Language, Expect y User-Agent normalmente contienen punto y coma (;). La activación simultánea de la verificación y la transformación de encabezados de solicitud puede provocar errores.

InspectQueryContentTypes: Configure esta opción si quiere examinar la parte de la consulta de solicitud en busca de ataques de inyección SQL para los tipos de contenido específicos. Si usa la GUI, puede configurar este parámetro en el panel **Configuración avanzada -> Configuración** de **perfil** del perfil de App Firewall.

Relajaciones pormenorizadas SQL

Web App Firewall le ofrece la opción de eximir un campo de formulario, encabezado o cookie específicos de la comprobación de inspección de inyección SQL. Puede omitir por completo la inspección de uno o varios de estos campos configurando las reglas de relajación para la comprobación de inyección SQL.

Web App Firewall le permite implementar una seguridad más estricta ajustando las reglas de relajación. Una aplicación puede requerir flexibilidad para permitir patrones específicos, pero configurar una regla de relajación para omitir la inspección de seguridad puede hacer que la aplicación sea vulnerable a ataques, ya que el campo de destino está exento de inspección para cualquier patrón de ataque SQL. La relajación pormenorizada de SQL proporciona la opción de permitir patrones especí-

ficos y bloquear el resto. Por ejemplo, Web App Firewall tiene actualmente un conjunto predeterminado de más de 100 palabras clave SQL. Dado que los hackers pueden usar estas palabras clave en ataques de SQL Injection, Web App Firewall las marca como amenazas potenciales. Puede relajar una o más palabras clave que se consideran seguras para la ubicación específica. El resto de las palabras clave SQL potencialmente peligrosas se siguen comprobando para la ubicación de destino y continúan activando las infracciones de comprobación de seguridad. Ahora tiene un control mucho más estricto.

Los comandos utilizados en las relajaciones tienen parámetros opcionales para **Tipo de valor** y **Expresión de valor**. Puede especificar si la expresión de valor es una expresión regular o una cadena literal. El tipo de valor se puede dejar en blanco o tiene la opción de seleccionar **Palabra clave** o **SpecialString** o **WildChar**.

> **Advertencia:**
>
> Las expresiones regulares son potentes. Especialmente si no está familiarizado con las expresiones regulares en formato PCRE, compruebe las expresiones regulares que escriba. Asegúrese de que definen exactamente la URL que quiere agregar como excepción, y nada más. El uso descuidado de comodines, y especialmente del metacaracter punto-asterisco (.*) o combinación de comodín, puede tener resultados que no quiere, como bloquear el acceso al contenido web que no tenía intención de bloquear o permitir un ataque que la comprobación HTML SQL Injection habría bloqueado de otro modo.

Puntos a considerar:

- La expresión de valor es un argumento opcional. Es posible que un nombre de campo no tenga ninguna expresión de valor.
- Un nombre de campo se puede enlazar a varias expresiones de valor.
- A las expresiones de valor se les debe asignar un tipo de valor. El tipo de valor SQL puede ser: 1) Palabra clave, 2) SpecialString o 3) WildChar.
- Puede tener varias reglas de relajación por combinación de nombre de campo/URL.

Uso de la línea de comandos para configurar la comprobación de inyección SQL

Para configurar las acciones de inyección SQL y otros parámetros mediante la línea de comandos:

En la interfaz de línea de comandos, puede utilizar el comando **set appfw profile** o el comando **add appfw profile** para configurar las protecciones de SQL Injection. Puede habilitar las acciones de bloqueo, aprender, registrar, estadísticas y especificar si quiere transformar los caracteres especiales utilizados en las cadenas de ataque de inyección SQL para inhabilitar el ataque. Seleccione el tipo de patrón de ataque SQL (palabras clave, caracteres comodín, cadenas especiales) que quiere detectar en las cargas útiles e indique si quiere que Web App Firewall también inspeccione los encabezados de solicitud para infracciones de Inyección SQL. Use el comando **unset appfw profile** para revertir

la configuración configurada a sus valores predeterminados. Cada uno de los comandos siguientes establece un solo parámetro, pero puede incluir varios parámetros en un solo comando:

- configurar el perfil de firewall de la aplicación “Descripciones de parámetros proporcionadas en la parte inferior de la página. “
- <name> -SQLInjectionAction (([block] [learn] [log] [stats])| [none])
- configurar el perfil de firewall de la aplicación “Descripciones de parámetros proporcionadas en la parte inferior de la página. “
- <name> -SQLInjectionTransformSpecialChars (**ON** | OFF)
- configurar el perfil de firewall de la aplicación “Descripciones de parámetros proporcionadas en la parte inferior de la página. “
- <name> -**SQLInjectionCheckSQLWildChars** (**ON** |**OFF**)
- configurar el perfil de firewall de la aplicación “Descripciones de parámetros proporcionadas en la parte inferior de la página. “
- **<name> -**SQLInjectionType** ([**SQLKeyword**] | [**SQLSplChar**] | [**SQLSplCharANDKeyword**] | [**SQLSplCharORKeyword**])
- **configurar el perfil de firewall de la aplicación** “Descripciones de parámetros proporcionadas en la parte inferior de la página. “
- <name> -**SQLInjectionParseComments** ([**checkall**] | [**ansi|nested **] | [**ansinested**])
- **configurar el perfil de firewall de la aplicación “Descripciones de parámetros proporcionadas en la parte inferior de la página. “
- <name> -CheckRequestHeaders (ON | OFF) Descripciones de parámetros proporcionadas en la parte inferior de la página.
- <name> - CheckRequestQueryNonHtml (ON | OFF) Descripciones de parámetros proporcionadas en la parte inferior de la página.

Para configurar una regla de relajación de inyección SQL mediante la interfaz de comandos

Utilice el comando bind o unbind para agregar o eliminar enlaces, como se indica a continuación:

- bind appfw profile <name> -SQLInjection <String> [isRegex(REGEX| NOTREGE)] <formActionURL> [-location <location>] [-valueType (Keywor |SpecialString|Wildchar)[<valueExpression>][-isValueRegex (REGEX | NOTREGEX)]]
- unbind appfw profile <name> -SQLInjection <String> <formActionURL> [-location <location>] [-valueTyp (Keyword|SpecialString|Wildchar)[< valueExpression>]]

> **Nota:**
>
> Puede encontrar la lista de palabras clave SQL del contenido del archivo de firma predetermi-

> nado si ve el objeto de firma de vista, que tiene una lista de palabras clave SQL y caracteres especiales SQL.

Uso de la GUI para configurar la comprobación de seguridad de inyección SQL

En la GUI, puede configurar la comprobación de seguridad de inyección SQL en el panel para el perfil asociado a su aplicación.

Para configurar o modificar la comprobación de inyección SQL mediante la interfaz gráfica de usuario

1. Vaya a **Firewall de aplicaciones > Perfiles**, resalte el perfil de destino y haga clic en **Modificar**.
2. En el panel **Configuración avanzada**, haga clic en **Comprobaciones de seguridad**.

La tabla de comprobación de seguridad muestra los valores de acción configurados actualmente para todas las comprobaciones de seguridad. Tiene 2 opciones de configuración:

a. Si quiere habilitar o inhabilitar las acciones Bloquear, Registrar, Estadísticas y Aprender para la inyección HTML SQL, puede seleccionar o desactivar las casillas de verificación de la tabla, hacer clic en **Aceptar**y, a continuación, en **Guardar y cerrar** para cerrar el panel **Comprobación de seguridad** .

b. Si quiere configurar más opciones para esta comprobación de seguridad, haga doble clic en Inyección HTML SQL o seleccione la fila y haga clic en **Configuración de acción**para mostrar las siguientes opciones:

Transformar caracteres especiales de SQL: Transforma los caracteres especiales de SQL de la solicitud.

Comprobar caracteres comodínde SQL: considere que los caracteres comodín de SQL en la carga útil son patrones de ataque.

Comprobar solicitud que contiene: tipo de inyección SQL (sqlKeyword, sqlSplChar, sqlSplCharAndKeyword o sqlSplcharorKeyword) que se va a comprobar.

Gestión de comentarios SQL: tipo de comentarios (Comprobar todos los comentarios, ANSI, anidados o ANSI/anidados) que se van a comprobar.

Después de cambiar cualquiera de las configuraciones anteriores, haga clic en **Aceptar** para guardar los cambios y volver a la tabla Comprobaciones de seguridad. Puede proceder a configurar otras comprobaciones de seguridad si es necesario. Haga clic en **Aceptar** para guardar todos los cambios que ha realizado en la sección Comprobaciones de seguridad y, a continuación, haga clic en **Guardar y cerrar** para cerrar el panel Comprobación de seguridad.

Para configurar una regla de relajación de inyección SQL mediante la interfaz gráfica de usuario

- Vaya a **Firewall de aplicaciones** > **Perfiles**, resalte el perfil de destino y haga clic en **Modificar**.
- En el panel **Configuración avanzada**, haga clic en **Reglas de relajación**.
- En la tabla Reglas de relajación, haga doble clic en la entrada **Inyección HTML SQL** o selecciónela y haga clic en **Modificar**.

- En el cuadro de diálogo **Reglas de relajación de inyección HTML SQL**, realice las operaciones **Agregar**, **Modificar**, **Eliminar**, **Habilitar**o **Inhabilitar** para las reglas de relajación.

> **Nota**
>
> Al agregar una regla nueva, el campo **Expresión de valor** no se muestra a menos que seleccione la opción **Palabra clave** o **SpecialString** o **WildChar** en el campo **Tipo de valor**.

Para administrar las reglas de relajación de inyección SQL mediante el visualizador

Para obtener una vista consolidada de todas las reglas de relajación, puede resaltar la fila **HTML SQL Injection** y hacer clic en **Visualizador**. El visualizador de relajaciones implementadas le ofrece la opción de **agregar** una nueva regla o **modificar** una existente. También puede **habilitar** o **inhabilitar** un grupo de reglas seleccionando un nodo y haciendo clic en los botones correspondientes en el visualizador de relajación.

Visualización o personalización de patrones de inyección mediante la GUI

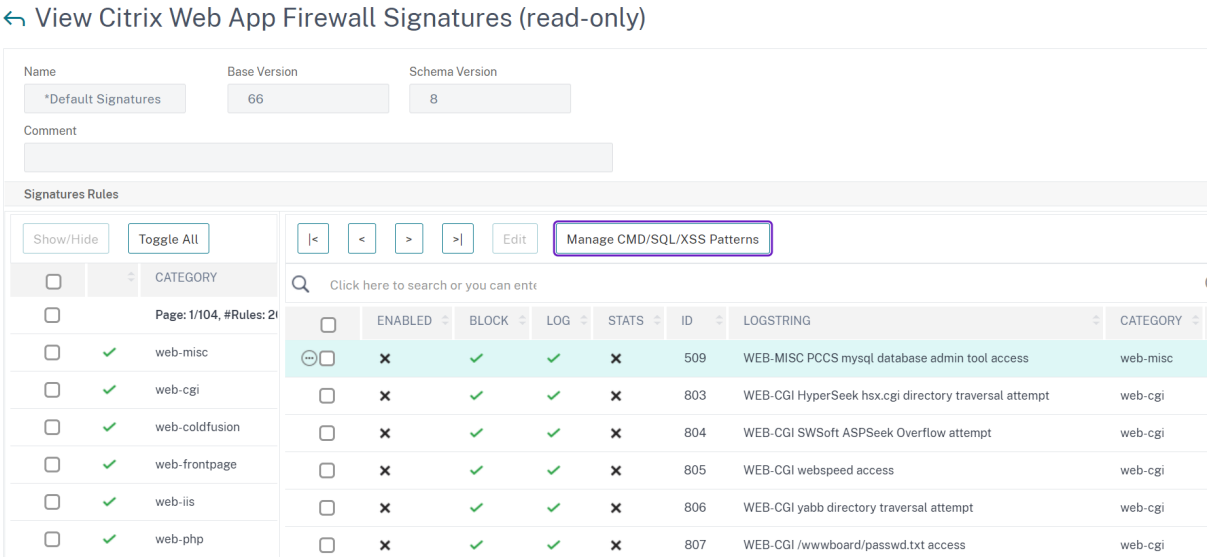
Puede utilizar la GUI para ver o personalizar los patrones de inyección.

Los patrones SQL predeterminados se especifican en el archivo de firmas predeterminado. Si no vincula ningún objeto de firma a su perfil, el perfil utilizará los patrones de inyección predeterminados especificados en el objeto de firmas predeterminado para procesar la comprobación de seguridad de inyección de comandos. Las reglas y patrones, especificados en el objeto de firmas predeterminado, son de solo lectura. No puede modificarlos ni modificarlos. Si quiere modificar o cambiar estos patrones, haga una copia del objeto SSignatures predeterminado para crear un objeto de firma definido por el usuario. Realice cambios en los patrones de inyección de comandos en el nuevo objeto de firma definido por el usuario y utilice este objeto de firma en su perfil que procesa el tráfico para el que quiere utilizar estos patrones personalizados.

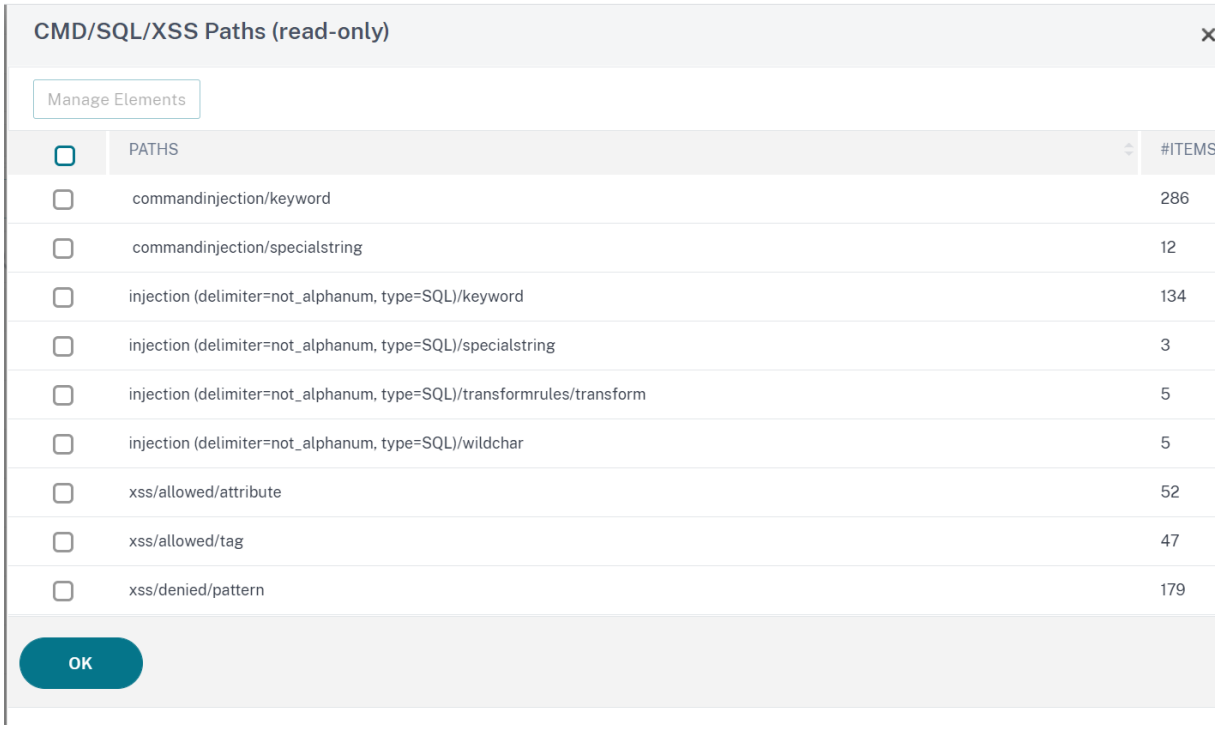
Para obtener más información, consulte Firmas

Para ver los patrones de inyección predeterminados mediante la GUI:

1. Vaya a **Firewall de aplicaciones > Firmas**, seleccione ***Firmas predeterminadas** y haga clic en **Modificar**.



1. Haga clic en **Administrar patrones CMD/SQL/XSS**. La tabla **Administrar rutas de scripts SQL/entre sitios** muestra patrones relacionados con la inyección de CMD/SQL/XS:



1. Seleccione una fila y haga clic en **Administrar elementos** para mostrar los patrones de inyección correspondientes (palabras clave, cadenas especiales, reglas de transformación o caracteres comodín) utilizados por la comprobación de inyección de comandos de Web App Firewall.

Uso de la función Learn con la comprobación de inyección SQL

Cuando la acción de aprendizaje está habilitada, el motor de aprendizaje de Web App Firewall supervisa el tráfico y detecta las infracciones desencadenadas. Puede inspeccionar periódicamente estas reglas aprendidas. Tras la debida consideración, puede implementar la regla aprendida como regla de relajación de inyección SQL.

Mejora del aprendizaje de inyección de SQL: en la versión 11.0 del software Citrix ADC se introdujo una mejora de aprendizaje de Web App Firewall. Para implementar una relajación de inyección SQL detallada, Web App Firewall ofrece un aprendizaje detallado de inyección SQL. El motor de aprendizaje hace recomendaciones sobre el Tipo de Valor observado (palabra clave, SpecialString, Wildchar) y la expresión Valor correspondiente observada en los campos de entrada. Además de comprobar las solicitudes bloqueadas para determinar si la regla actual es demasiado restrictiva y necesita ser relajada, puede revisar las reglas generadas por el motor de aprendizaje para determinar qué tipo de valor y expresiones de valor están desencadenando infracciones y deben abordarse en las reglas de relajación.

> **Importante**
>
> El motor de aprendizaje de Web App Firewall puede distinguir solo los primeros 128 bytes del nombre. Si un formulario tiene varios campos con nombres que coinciden con los primeros 128 bytes, es posible que el motor de aprendizaje no pueda distinguir entre ellos. Del mismo modo, la regla de relajación implementada podría relajar inadvertidamente todos estos campos de la inspección de SQL Injection.
>
> **Nota** Para omitir la entrada SQL del encabezado User-Agent, utilice la siguiente regla de relajación:
>
> ```
> bind appfw profile your_profile_name -SQLInjection User-Agent ".*"-
> location HEADER
> ```

Para ver o utilizar datos aprendidos mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba uno de los siguientes comandos:

- `show appfw learningdata <profilename> SQLInjection`
- `rm appfw learningdata <profilename> -SQLInjection <string> <formActionURL > [<location>] [<valueType> <valueExpression>]`
- `export appfw learningdata <profilename> SQLInjection`

Para ver o usar datos aprendidos mediante la interfaz gráfica de usuario

1. Vaya a **Firewall de aplicaciones > Perfiles**, resalte el perfil de destino y haga clic en **Modificar**.
2. En el panel **Configuración avanzada**, haga clic en **Reglas aprendidas**. Puede seleccionar la entrada **Inyección HTML SQL** en la tabla Reglas aprendidas y hacer doble clic en ella para acceder a las reglas aprendidas. Puede implementar las reglas aprendidas o modificar una regla antes

de implementarla como regla de relajación. Para descartar una regla, puede seleccionarla y hacer clic en el botón **Omitir**. Solo puede modificar una regla a la vez, pero puede seleccionar varias reglas para implementarlas u omitirlas.

También tiene la opción de mostrar una vista resumida de las relajaciones aprendidas seleccionando la entrada **HTML SQL Injection** en la tabla Reglas aprendidas y haciendo clic en **Visualizador** para obtener una vista consolidada de todas las infracciones aprendidas. El visualizador facilita la gestión de las reglas aprendidas. Presenta una vista completa de los datos en una pantalla y facilita la acción sobre un grupo de reglas con un solo clic. La mayor ventaja del visualizador es que recomienda expresiones regulares para consolidar varias reglas. Puede seleccionar un subconjunto de estas reglas, en función del delimitador y de la URL de acción. Puede mostrar 25, 50 o 75 reglas en el visualizador, seleccionando el número en una lista desplegable. El visualizador de reglas aprendidas ofrece la opción de modificar las reglas e implementarlas como relajaciones. O puede saltarse las reglas para ignorarlas.

Uso de la función de registro con la comprobación de inyección SQL

Cuando la acción de registro está habilitada, las infracciones de comprobación de seguridad de HTML SQL Injection se registran en el registro de auditoría como infracciones de **APPFW_SQL**. El Web App Firewall admite los formatos de registro nativo y CEF. También puede enviar los registros a un servidor syslog remoto.

Para acceder a los mensajes de registro mediante la línea de comandos

Cambia al shell y lleva los ns.logs de la carpeta **/var/log/** para acceder a los mensajes de registro relacionados con las infracciones de SQL Injection:

```
> Shell

## tail -f /var/log/ns.log | grep APPFW_SQL
```

Ejemplo de un mensaje de registro de inyección HTML SQL cuando se transforma la solicitud

```
1 Jun 26 21:08:41 <local0.info> 10.217.31.98 CEF:0|Citrix|Citrix ADC|NS11
    .0|APPFW|APPFW_SQL|6|src=10.217.253.62 geolocation=Unknown spt=54001
     method=GET request=http://aaron.stratum8.net/FFC/login.php?
    login_name=%27+or&passwd=and+%3B&drinking_pref=on&text_area=select
    +*+from+%5C+%3B&loginButton=ClickToLogin&as_sfid=AAAAAAXjnGN5gLH-
    hvhTOpIySEIqES7BjFRs5Mq0fwPp-3ZHDi5yWlRWByj0cVbMyy-
    Ens2vaaiULKOcUri4OD4kbXWwSY5s7I3QkDsrvIgCYMC9BMvBwY2wbNcSqCwk52lfE0k
    %3D&as_fid=feeec8758b41740eedeeb6b35b85dfd3d5def30c msg= Special
    characters seen in fields cn1=74 cn2=762 cs1=pr_ffc cs2=PPE1 cs3=9
    ztIlf9p1H7p6Xtzn6NMygTv/QM0002 cs4=ALERT cs5=2015 act=transformed
2 <!--NeedCopy-->
```


Ejemplo de un mensaje de registro de inyección HTML SQL cuando se bloquea la solicitud posterior

```
Jun 26 21:30:34 <local0.info> 10.217.31.98 CEF:0|Citrix|Citrix ADC|NS11
    .0|APPFW|APPFW_SQL|6|src=10.217.253.62 geolocation=Unknown spt=9459
    method=POST request=http://aaron.stratum8.net/FFC/login_post.php msg
    =SQL Keyword check failed for field text_area="(')" cn1=78 cn2=834
    cs1=pr_ffc cs2=PPE1 cs3=eVJMMPtZ2XgylGrHjkx3rZLfBCI0002 cs4=ALERT
    cs5=2015 act=blocked
<!--NeedCopy-->
```

Nota

Como parte de los cambios de streaming en la compilación 10.5.e (compilaciones de mejora) y la compilación 11.0 en adelante, ahora procesamos los datos de entrada en bloques. La coincidencia de patrones RegEx ahora está restringida a 4K para la coincidencia de cadenas de caracteres contiguos. Con este cambio, los mensajes de registro de infracciones SQL pueden incluir información diferente en comparación con las compilaciones anteriores. La palabra clave y el carácter especial de la entrada se pueden separar por muchos bytes. Ahora hacemos un seguimiento de las palabras clave SQL y las cadenas especiales al procesar los datos, en lugar de almacenar en búfer todo el valor de entrada. Además del nombre del campo, el mensaje de registro ahora incluye la palabra clave SQL, el carácter especial SQL, o tanto la palabra clave SQL como el carácter especial SQL, según lo determinado por la configuración configurada. El resto de la entrada ya no se incluye en el mensaje de registro, como se muestra en el ejemplo siguiente:

Ejemplo:

En 10.5, cuando Web App Firewall detecta la infracción SQL, es posible que la cadena de entrada completa se incluya en el mensaje de registro, como se muestra a continuación:

```
SQL Keyword check failed for field text=\"select a name from testbed1
;(;)\".*<blocked>
```

En las compilaciones de mejora de 10.5.e que admiten la transmisión del lado de la solicitud y la compilación 11.0 en adelante, registramos solo el nombre del campo, la palabra clave y el carácter especial (si corresponde) en el mensaje de registro, como se muestra a continuación:

```
SQL Keyword check failed for field **text="select(;)"<blocked>
```

Este cambio se aplica a las solicitudes que contienen application/x-www-form-urlencoded, multipart/form-data o text/x-gwt-rpc content-types. Los mensajes de registro generados durante el procesamiento de cargas **JSON** o **XML** no se ven afectados por este cambio.

Para acceder a los mensajes de registro mediante la interfaz gráfica de usuario

La GUI de Citrix incluye una herramienta útil (**Syslog Viewer**) para analizar los mensajes de registro.

Tiene varias opciones para acceder al Visor de Syslog:

- Vaya a **Firewall de aplicaciones** > **Perfiles**, seleccione el perfil de destino y haga clic en **Comprobaciones de seguridad**. Resalte la fila **Inyección HTML SQL** y haga clic en **Registros**. Cuando accede a los registros directamente desde la comprobación de inyección HTML SQL del perfil, la GUI filtra los mensajes de registro y muestra solo los registros relacionados con estas infracciones de comprobación de seguridad.
- También puede acceder al Visor de Syslog navegando a **Citrix ADC** > **Sistema** > **Auditoría**. En la sección Mensajes de auditoría, haga clic en el enlace **Mensajes de Syslog** para mostrar el Visor de Syslog, que muestra todos los mensajes de registro, incluidos otros registros de infracciones de comprobación de seguridad. Esto resulta útil para depurar cuando se pueden desencadenar varias infracciones de comprobación de seguridad durante el procesamiento de solicitudes.
- Vaya a **Firewall de aplicaciones** > **directivas** > **Auditoría**. En la sección Mensajes de auditoría, haga clic en el enlace **Mensajes de Syslog** para mostrar el Visor de Syslog, que muestra todos los mensajes de registro, incluidos otros registros de infracciones de comprobación de seguridad.

El Visor de Syslog basado en HTML proporciona varias opciones de filtro para seleccionar solo los mensajes de registro que le interesan. Para seleccionar mensajes de registro para la comprobación de **inyección HTML SQL**, filtra seleccionando **APPFW** en las opciones de la lista desplegable del **módulo**. La lista **Tipo de evento** ofrece un amplio conjunto de opciones para refinar aún más su selección. Por ejemplo, si selecciona la casilla de verificación **APPFW_SQL** y hace clic en el botón **Aplicar**, solo aparecerán en el Visor de Syslog los mensajes de registro relacionados con las infracciones de la comprobación de seguridad de **inyección SQL**.

Si coloca el cursor en la fila de un mensaje de registro específico, aparecen varias opciones, como **Módulo**, **Tipo de evento**, **ID de evento**, **IP de cliente**, etc., debajo del mensaje de registro. Puede seleccionar cualquiera de estas opciones para resaltar la información correspondiente en el mensaje de registro.

La funcionalidad**Hacer clic para implementar** solo está disponible en la GUI. Puede usar Syslog Viewer no solo para ver los registros, sino también para implementar reglas de relajación de inyección HTML SQL basadas en los mensajes de registro para las infracciones de comprobación de seguridad de Web App Firewall. Los mensajes de registro deben estar en formato de registro CEF para esta operación. La funcionalidad Hacer clic para implementar solo está disponible para los mensajes de registro generados por la acción bloquear (o no bloquear). No puede implementar una regla de relajación para un mensaje de registro sobre la operación de transformación.

Para implementar una regla de relajación desde el Visor de Syslog, seleccione el mensaje de registro. Aparece una casilla de verificación en la esquina superior derecha del cuadro **Visor de Syslog** de la fila seleccionada. Seleccione la casilla de verificación y, a continuación, seleccione una opción de la lista Acción para implementar la regla de relajación. **Modificar e implementar**, **Implementar** e **Implementar todo** están disponibles como opciones de **Acción**.

Las reglas de inyección SQL que se implementan mediante la opción Haga clic para implementar no

incluyen las recomendaciones de relajación pormenorizada.

Para usar la función Click to Deploy en la GUI:

1. En el Visor de Syslog, seleccione **Firewall de aplicaciones** en las opciones del **módulo**.
2. Seleccione **APP_SQL** como **Tipo de evento** para filtrar los mensajes de registro correspondientes.
3. Seleccione la casilla de verificación para identificar la regla que se va a implementar.
4. Utilice la lista desplegable **Acción** de opciones para implementar la regla de relajación.
5. Compruebe que la regla aparece en la sección de reglas de relajación correspondiente.

Estadísticas de las infracciones de la inyección SQL

Cuando la acción de estadísticas está habilitada, el contador de la comprobación de inyección SQL se incrementa cuando Web App Firewall realiza cualquier acción para esta comprobación de seguridad. Las estadísticas se recopilan para Rate and Total count para Tráfico, Infracciones y Registros. El tamaño de un incremento del contador de registro puede variar en función de la configuración configurada. Por ejemplo, si la acción de bloqueo está habilitada, la solicitud de una página que contiene 3 infracciones de Inyección SQL incrementa el contador de estadísticas en uno, porque la página se bloquea tan pronto como se detecta la primera infracción. Sin embargo, si el bloque está inhabilitado, el procesamiento de la misma solicitud aumenta en tres el contador de estadísticas de infracciones y registros, porque cada infracción genera un mensaje de registro independiente.

Para mostrar las estadísticas de comprobación de SQL Injection mediante la línea de comandos:

En el símbolo del sistema, escriba:

> **sh appfw estado**

Para mostrar las estadísticas de un perfil específico, use el siguiente comando:

```
> stat appfw profile <profile name>
```

Para mostrar estadísticas de inyección HTML SQL mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **Seguridad** > **Firewall de aplicaciones**.
2. En el panel derecho, acceda al enlace de **Estadísticas**.
3. Use la barra de desplazamiento para ver las estadísticas sobre las infracciones y los registros de inyección HTML SQL. La tabla de estadísticas proporciona datos en tiempo real y se actualiza cada 7 segundos.

Resumen

Tenga en cuenta los siguientes puntos sobre la comprobación de inyección SQL:

- **Compatibilidad integrada para la protección de inyección de SQL**: Citrix Web App Firewall protege contra la inyección de SQL mediante la supervisión de una combinación de palabras clave SQL y caracteres especiales en los parámetros del formulario. Todas las palabras clave SQL, los caracteres especiales, los caracteres comodín y las reglas de transformación predeterminadas se especifican en el archivo /netscaler/default_custom_settings.xml.
- **Personalización**: puede cambiar las palabras clave predeterminadas, los caracteres especiales, los caracteres comodín y las reglas de transformación para personalizar la inspección de comprobación de seguridad de SQL para las necesidades específicas de la aplicación. Realice una copia del objeto de firma predeterminado, modifique las entradas existentes o agregue otras nuevas. Enlaza este objeto de firma a su perfil para hacer uso de la configuración personalizada.
- **Modelo de seguridad híbrido**: Tanto las firmas como las protecciones de seguridad profundas utilizan los patrones de scripts SQL/de sitios especificados en el objeto de firma que está enlazado al perfil. Si ningún objeto de firma está enlazado al perfil, se utilizan los patrones de scripts SQL/de sitios presentes en el objeto de firma predeterminado.
- **Transformación**: tenga en cuenta lo siguiente sobre la operación de transformación:
  - La operación de transformación funciona independientemente de la otra configuración de acción de inyección SQL. Si la transformación está habilitada y el bloque, el registro, las estadísticas y el aprendizaje están inhabilitados, se transforman los caracteres especiales de SQL.
  - Cuando la transformación SQL está habilitada, las solicitudes de usuario se envían a los servidores back-end después de que los caracteres especiales de SQL se hayan transformado en modo no bloque. Si la acción de bloqueo está habilitada, tiene prioridad sobre la acción de transformación. Si el tipo de inyección se especifica como carácter especial SQL y el bloque está habilitado, la solicitud se bloquea a pesar de la acción de transformación.
- **Relajación y aprendizaje finos**: ajuste la regla de relajación para relajar un subconjunto de elementos SQL de la inspección de comprobación de seguridad pero detecte el resto. El motor de aprendizaje recomienda un tipo de valor específico y expresiones de valor basadas en los datos observados.
- **Hacer clic para implementar**: seleccione uno o varios mensajes de registro de infracciones de SQL en el visor de syslog e impleméntelos como reglas de relajación.

Protección basada en gramática SQL para cargas útiles HTML y JSON

August 20, 2021

Citrix Web App Firewall utiliza un enfoque de coincidencia de patrones para detectar ataques de inyección SQL en `JSON` cargas útiles `HTTP` y ataques de inyección SQL. El enfoque utiliza un conjunto de palabras clave predefinidas y (o) caracteres especiales para detectar un ataque y marcarlo como una

violación. Aunque este enfoque es efectivo, puede dar lugar a muchos falsos positivos que dan lugar a añadir una o más reglas de relajación. Especialmente cuando se utilizan palabras de uso común como "Seleccionar" y "De" en una solicitud HTTP o JSON. Podemos reducir los falsos positivos implementando la comprobación de protección gramatical SQL `HTML` y la `JSON` carga útil.

En el enfoque de coincidencia de patrones existente, se identifica un ataque de inyección SQL si hay una palabra clave predefinida y/o un carácter especial en una solicitud HTTP. En este caso, la instrucción no tiene por qué ser una sentencia SQL válida. Pero en el enfoque basado en gramática, un ataque de inyección SQL solo se detecta si una palabra clave o un carácter especial están presentes en una instrucción SQL o forma parte de una sentencia SQL, lo que reduce los casos falsos positivos.

Caso de uso de protección basada en gramática SQL

Considere una declaración, "Selecciona mis entradas y veámonos en union station" presente en una solicitud HTTP. Aunque la instrucción no es una sentencia SQL válida, el enfoque de coincidencia de patrones existente detecta la solicitud como un ataque de inyección SQL porque la instrucción utiliza palabras clave como "Seleccionar", "y" y "Unión". Sin embargo, en el caso del enfoque gramatical SQL, la instrucción no se detecta como un ataque de infracción porque las palabras clave no están presentes en una sentencia SQL válida o no forman parte de una sentencia SQL válida.

El enfoque basado en gramática también se puede configurar para detectar ataques de inyección SQL en `JSON` cargas útiles. Para añadir una regla de relajación, puede reutilizar las reglas de relajación existentes. Las reglas de relajación detalladas también se aplican a la gramática SQL, a las reglas con "palabra clave" "ValueType". En la gramática `JSON` SQL, se puede reutilizar el método basado en URL existente.

Configurar la protección basada en gramática SQL mediante la CLI

Para implementar la detección basada en gramática SQL, debe configurar el parámetro "SQLjection-Grammar" en el perfil de Web App Firewall. De forma predeterminada, el parámetro está inhabilitado. Se admiten todas las acciones de inyección SQL existentes excepto el aprendizaje. Cualquier nuevo perfil creado después de una actualización admite la gramática de inyección SQL y sigue teniendo el tipo predeterminado como "carácter especial o palabra clave" y debe habilitarse explícitamente.

En el símbolo del sistema, escriba:

```
1 add appfw profile <profile-name>  - SQLInjectionAction <action-name> -
     SQLInjectionGrammar ON/OFF
2 <!--NeedCopy-->
```

Ejemplo:


```
add appfw profile profile1 -SQLInjectionAction Block -SQLInjectionGrammar ON
```

Configurar la protección de coincidencia de patrones SQL y la protección basada en gramática mediante la CLI

Si ha habilitado enfoques gramaticales y de coincidencia de patrones, el dispositivo realiza primero la detección basada en gramática y, si hay detección de inyección SQL con el tipo de acción establecido para bloquear, la solicitud se bloquea (sin verificar la detección mediante la coincidencia de patrones).

En el símbolo del sistema, escriba:

```
1 add appfw profile <profile-name>  - SQLInjectionAction <action-name> -
     SQLInjectionGrammar ON  - SQLInjectionType <Any action other than  '
     None' : SQLSplCharANDKeyword/ SQLSplCharORKeyword/ SQLSplChar/
     SQLKeyword>
2 <!--NeedCopy-->
```

Ejemplo:

```
add appfw profile p1 -SQLInjectionAction block - SQLInjectionGrammar ON -
SQLInjectionType SQLSplChar
```

Configurar la comprobación de inyección SQL solo con protección basada en gramática mediante la CLI

En el símbolo del sistema, escriba:

```
1 add appfw profile <profile-name>  - SQLInjectionAction <action-name> -
     SQLInjectionGrammar ON  - SQLInjectionType None
2 <!--NeedCopy-->
```

Ejemplo:

```
add appfw profile p1 -SQLInjectionAction block - SQLInjectionGrammar ON -
SQLInjectionType None
```

Vincular reglas de relajación para la protección basada en gramática SQL mediante la CLI

Si su aplicación requiere que `SQL` omita la comprobación de inyección de un “ELEMENTO” o “ATRIBUTO” específico en la carga útil, debe configurar una regla de relajación.

> **Nota:**
>
> Las reglas de relajación con la "palabra clave" de ValueType se evalúan solo cuando el dispositivo realiza la detección mediante SQL gramática.

El SQL comando Reglas de relajación de inspección por inyección tiene la siguiente sintaxis. En el símbolo del sistema, escriba:

```
1 bind appfw profile <name> -SQLInjection <String> [isRegex(REGEX|
     NOTREGE)] <formActionURL> [-location <location>] [-valueType (Keywor
     |SpecialString|Wildchar) [<valueExpression>][-isValueRegex (REGEX |
     NOTREGEX) ]]
2 <!--NeedCopy-->
```

Ejemplo:

```
bind appfw profile p1 -sqlinjection abc http://10.10.10.10/
bind appfw profile p1 -sqlinjection 'abc[0-9]+'http://10.10.10.10/ -isregex
regEX
bind appfw profile p1 -sqlinjection 'name'http://10.10.10.10/ -valueType
Keyword 'selec[a-z]+' -isvalueRegex regEX
```

Configurar la protección basada en gramática SQL para la carga útil JSON mediante la CLI

Para implementar la detección basada en gramática SQL para la carga útil JSON, debe configurar el parámetro "JSONSQLjectionGrammar" en el perfil de Web App Firewall. De forma predeterminada, el parámetro está inhabilitado. Se admiten todas las acciones de inyección SQL existentes excepto el aprendizaje. Cualquier nuevo perfil creado después de una actualización admite la gramática de inyección SQL y sigue teniendo el tipo predeterminado como "carácter especial o palabra clave" y debe habilitarlo explícitamente.

En el símbolo del sistema, escriba:

```
1 add appfw profile <profile-name> -type JSON  - JSONSQLInjectionAction <
     action-name> -JSONSQLInjectionGrammar ON/OFF
2 <!--NeedCopy-->
```

Ejemplo:

```
add appfw profile profile1 -type JSON -JSONSQLInjectionAction Block -JSONSQLInjectionG
 ON
```


Configurar la protección de coincidencia de patrones SQL y la protección basada en gramática mediante la CLI

Si ha habilitado comprobaciones gramaticales y de coincidencia de patrones, el dispositivo realiza primero la detección basada en gramática y, si hay detección de inyección SQL con el tipo de acción establecido para bloquear, la solicitud se bloquea (sin verificar la detección mediante coincidencia de patrones).

> **Nota:**
>
> Las reglas de relajación con la "palabra clave" de ValueType se evalúan solo cuando el dispositivo realiza la detección mediante gramática SQL.

En el símbolo del sistema, escriba:

```
add appfw profile <profile-name> -type JSON  - JSONSQLInjectionAction <
    action-name> -JSONSQLInjectionGrammar ON  - JSONSQLInjectionType <Any
     action other than  'None' : SQLSplCharANDKeyword/
    SQLSplCharORKeyword/ SQLSplChar/ SQLKeyword>
<!--NeedCopy-->
```

Ejemplo:

```
add appfw profile p1 -type JSON -JSONSQLInjectionAction block - JSONSQLInjectionGramma
 ON -JSONSQLInjectionType SQLSplChar
```

Configurar la protección basada en gramática SQL para la carga útil JSON mediante la CLI

En el símbolo del sistema, escriba:

```
add appfw profile <profile-name> -type JSON  - JSONSQLInjectionAction <
    action-name> -JSONSQLInjectionGrammar ON  - JSONSQLInjectionType None
    `\
<!--NeedCopy-->
```

Ejemplo:

```
add appfw profile p1 -type JSON -JSONSQLInjectionAction block - JSONSQLInjectionGramma
 ON -JSONSQLInjectionType None
```


Vincular reglas de relajación basadas en URL para la protección basada en gramática JSON SQL mediante la CLI

Si su aplicación requiere que omita la inspección de inyección de `JSON` comandos para un "ELEMENTO" o "ATRIBUTO" específico en la carga útil, puede configurar una regla de relajación.
El `JSON` comando Reglas de relajación de inspección por inyección tiene la siguiente sintaxis. En el símbolo del sistema, escriba:

```
bind appfw profile <profile name>  - JSONCMDURL <expression> -comment <
    string> -isAutoDeployed ( AUTODEPLOYED | NOTAUTODEPLOYED ) -state (
    ENABLED | DISABLED )
<!--NeedCopy-->
```

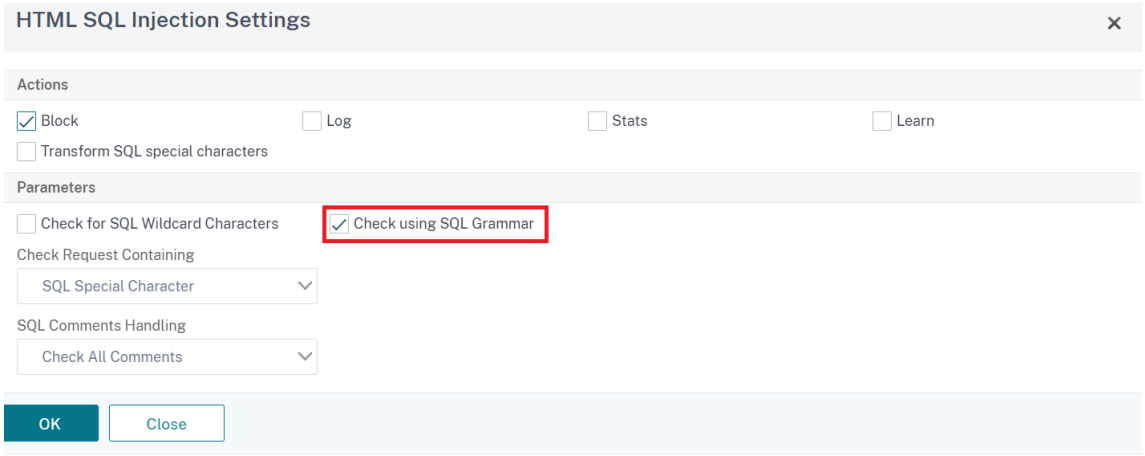
Ejemplo:

```
bind appfw profile p1 -sqlinjection abc http://10.10.10.10/
bind appfw profile p1 -sqlinjection 'abc[0-9]+'http://10.10.10.10/ -isregex
regEX
bind appfw profile p1 -sqlinjection 'name'http://10.10.10.10/ -valueType
Keyword 'selec[a-z]+' -isvalueRegex regEX
```

Configurar la protección basada en gramática SQL mediante la GUI

Complete el procedimiento GUI para configurar la detección de inyección HTML SQL basada en gramática.

1. En el panel de navegación, vaya a **Seguridad > Perfiles**.
2. En la página **Perfiles**, haga clic en **Agregar**.
3. En la página **Perfil de Citrix Web App Firewall**, haga clic en **Comprobaciones de seguridad** en **Configuración avanzada**.
4. En la sección **Comprobaciones de seguridad**, vaya a Configuración de **inyección HTML SQL** .
5. Haga clic en el icono ejecutable situado cerca de la casilla de verificación.
6. Haga clic en **Configuración de acción** para acceder a la página **Configuración de inyección SQL de HMTL** .

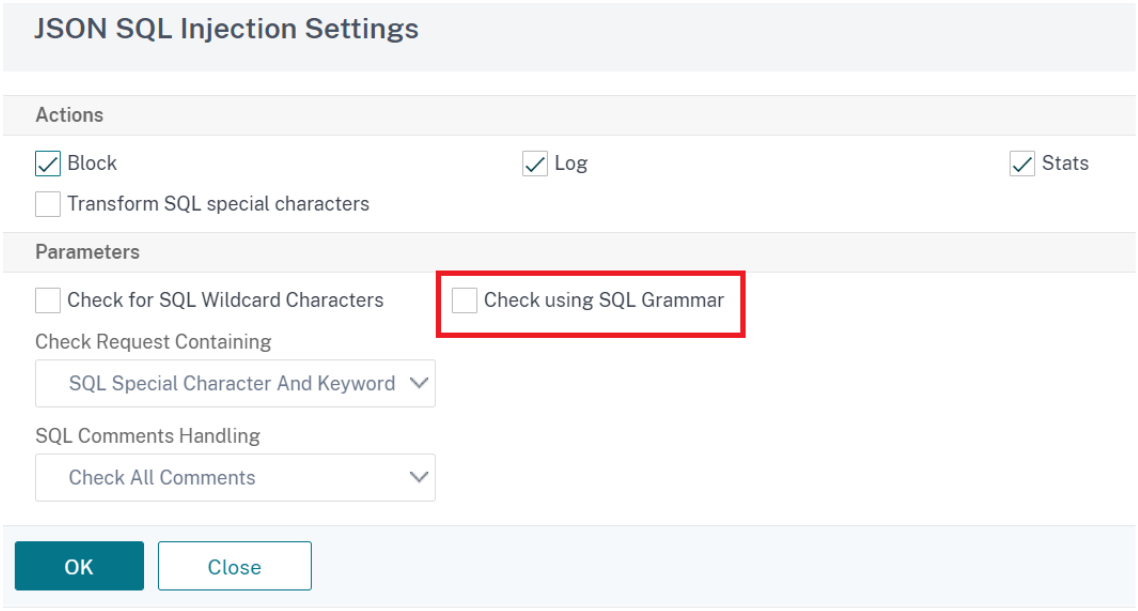


7. Active la **casilla Comprobar mediante gramática SQL** .
8. Haga clic en **Aceptar**.

Configurar la protección basada en gramática SQL para la carga útil JSON mediante la GUI

Complete el procedimiento GUI para configurar la detección de inyección JSON SQL basada en gramática.

1. En el panel de navegación, vaya a **Seguridad > Perfiles**.
2. En la página **Perfiles**, haga clic en **Agregar**.
3. En la página **Perfil de Citrix Web App Firewall**, haga clic en **Comprobaciones de seguridad** en **Configuración avanzada**.
4. En la sección **Comprobaciones de seguridad**, vaya a Configuración de **inyección JSON SQL**.
5. Haga clic en el icono ejecutable situado cerca de la casilla de verificación.
6. Haga clic en **Configuración de acción** para acceder a la página **Configuración de inyección JSON SQL**.
7. Active la **casilla Comprobar mediante gramática SQL** .
8. Haga clic en **Aceptar**.



Protección basada en gramática por inyección de comandos para carga útil HTML

July 15, 2022

Citrix Web App Firewall utiliza un enfoque de coincidencia de patrones para detectar ataques por inyección de comandos en cargas útiles HTML. El enfoque utiliza un conjunto de palabras clave predefinidas y (o) caracteres especiales para detectar un ataque y marcarlo como una infracción. Aunque este enfoque es eficaz, puede dar lugar a muchos falsos positivos que llevan a agregar una o más reglas de relajación. Especialmente, cuando se usa una palabra de uso común, como “Salir”, en una solicitud HTTP. Podemos reducir los falsos positivos implementando la comprobación de protección basada en gramática de inyección de comandos para la carga útil HTML.

En el enfoque de coincidencia de patrones, se identifica un ataque de inyección de comandos si una palabra clave predefinida y (o) un carácter especial están presentes en una solicitud HTTP. En este caso, la sentencia no necesita ser una sentencia de inyección de comandos válida. Pero en el enfoque basado en la gramática, un ataque de inyección de comandos se detecta solo si una palabra clave o un carácter especial está presente en una sentencia de inyección de comandos. Por lo tanto, se reducen los casos de falsos positivos.

Casos de uso de protección basada en gramática por inyección de comandos

Considere la declaración “¡Corra hacia la salida!” presente en una solicitud HTTP. Aunque la sentencia no es una sentencia de inyección de comandos válida, el enfoque de coincidencia de patrones detecta la solicitud como un ataque de inyección de comandos debido a la palabra clave “exit”. Pero en el enfoque basado en la gramática de inyección de comandos, la sentencia no se detecta como un ataque de violación porque las palabras clave no están presentes en una sentencia de inyección de comandos válida.

Configurar el parámetro de protección basado en gramática de inyección de comandos mediante la CLI

Para implementar la detección basada en gramática por inyección de comandos, debe configurar el parámetro “CMDInjectionGrammar” en el perfil de Web App Firewall. De forma predeterminada, el parámetro está inhabilitado. Se admiten todas las acciones de inyección de comandos existentes, excepto el aprendizaje. Cualquier perfil nuevo creado después de una actualización admite la gramática de inyección de comandos. El nuevo perfil sigue teniendo el tipo predeterminado como “carácter especial o palabra clave” y la gramática de inyección de comandos debe estar habilitada explícitamente.

En el símbolo del sistema, escriba:

```
1 add appfw profile <profile-name>  - CMDInjectionAction <action-name> -
     CMDInjectionGrammar ON/OFF
2 <!--NeedCopy-->
```

Ejemplo:

```
1 add appfw profile profile1  - CMDInjectionAction Block  -
     CMDInjectionGrammar ON
2 <!--NeedCopy-->
```

Configurar la protección de coincidencia de patrones por inyección de comandos y la protección basada en gramáticas mediante la CLI

Si ha habilitado los enfoques basados en gramática y de coincidencia de patrones, el dispositivo realiza primero la detección basada en gramática. Si se detecta una inyección de comando con el tipo de acción establecido en “bloquear”, la solicitud se bloquea (sin verificar la detección mediante la coincidencia de patrones).

En el símbolo del sistema, escriba:


```
1 add appfw profile <profile-name>  - CMDInjectionAction <action-name> -
     CMDInjectionGrammar ON  - CMDInjectionType <Any action other than  '
     None' : CMDSplCharANDKeyword/ CMDSplCharORKeyword/ CMDSplChar/
     CMDKeyword>
2 <!--NeedCopy-->
```

Ejemplo:

```
1 add appfw profile p1  - CMDInjectionAction block  -  CMDInjectionGrammar
     ON  - CMDInjectionType CMDSplChar
2 <!--NeedCopy-->
```

Configurar la comprobación de inyección de comandos solo con protección basada en gramáticas mediante la CLI

En el símbolo del sistema, escriba:

```
1 add appfw profile <profile-name>  - CMDInjectionAction <action-name> -
     CMDInjectionGrammar ON  - CMDInjectionType None
2 <!--NeedCopy-->
```

Ejemplo:

```
1 add appfw profile p1  - CMDInjectionAction block  -  CMDInjectionGrammar
     ON  - CMDInjectionType None
2 <!--NeedCopy-->
```

Enlazar reglas de relajación para la protección de inyección de comandos basada en gramáticas mediante la

Si su aplicación requiere que omita la comprobación de inyección de comandos para un “ELEMENTO” o “ATRIBUTO” específico en la carga útil HTML, debe configurar una regla de relajación.

> **Nota:**

> Las reglas de relajación con valueType como “palabra clave” se evalúan solo cuando el dispositivo realiza la detección mediante la gramática de inyección de comandos.

Las reglas de relajación de inspección de inyección de comandos tienen la siguiente sintaxis. En el símbolo del sistema, escriba:

```
bind appfw profile <name> -CMDInjection <String> [isRegex(REGEX|
    NOTREGE)] <formActionURL> [-location <location>] [-valueType (Keywor
    |SpecialString|Wildchar) [<valueExpression>][-isValueRegex (REGEX |
    NOTREGEX) ]]
<!--NeedCopy-->
```

Ejemplo:

```
bind appfw profile p1 -cmdinjection abc http://10.10.10.10/

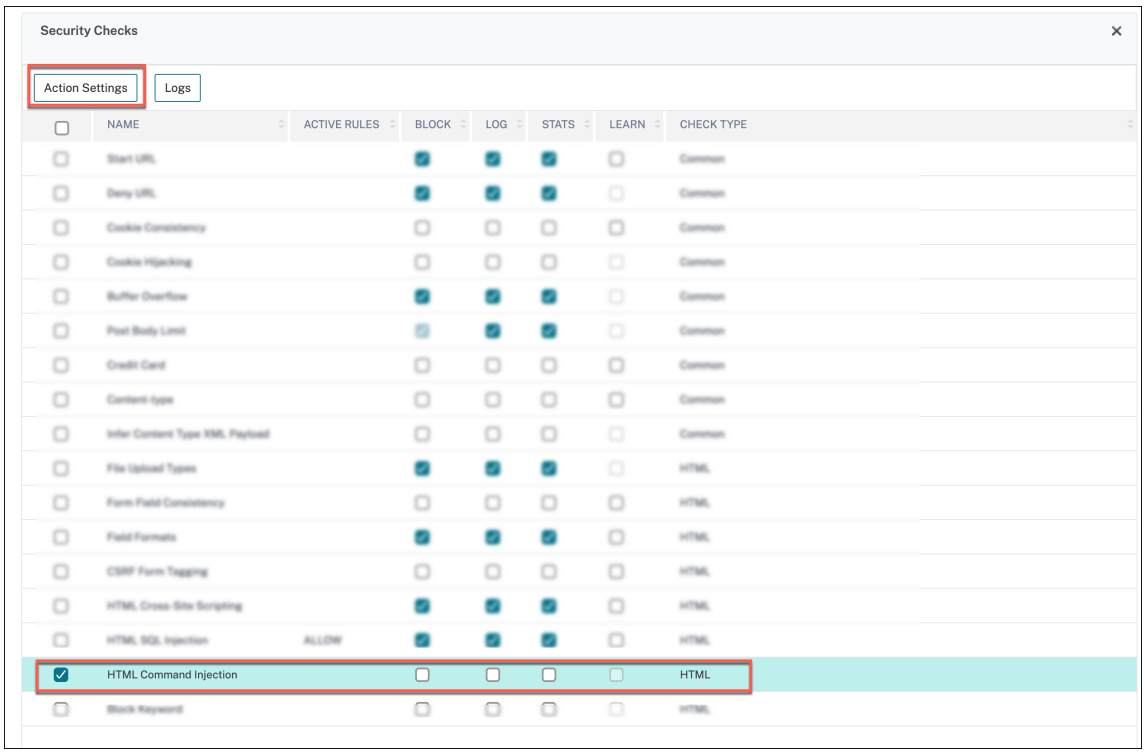
bind appfw profile p1  - cmdinjection 'abc[0-9]+' http://10.10.10.10/ -
    isregex regEX

bind appfw profile p1  - cmdinjection 'name' http://10.10.10.10/ -
    valueType Keyword 'exi[a-z]+' -isvalueRegex regEX
<!--NeedCopy-->
```

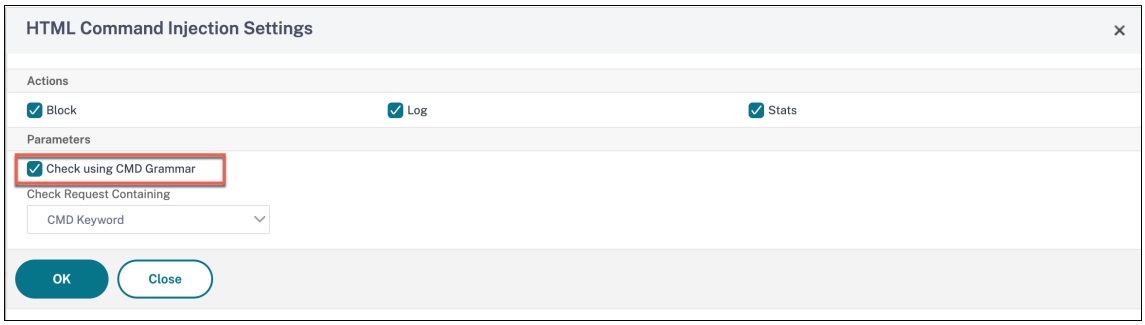
Configurar la protección basada en gramática por inyección de comandos mediante la GUI

Complete los siguientes pasos para configurar la detección de inyección de comandos HTML basada en gramáticas.

1. Vaya a **Seguridad > Perfil de Citrix Web App Firewall > Perfiles**.
2. Seleccione un perfil y haga clic en **Modificar**.
3. Vaya a la sección **Configuración avanzada** y haga clic en **Comprobaciones de seguridad**.
4. Active la casilla de verificación **Inyección de comandos HTML** y haga clic en**Configuración de acciones**.



5. Active la**casilla de verificación Comprobar mediante CMD Grammar**.
6. Seleccione **Ninguno** en la **solicitud de comprobación que contiene**.



7. Haga clic en**Aceptar**.

Reglas de relajación y denegación para gestionar los ataques de inyección HTML SQL

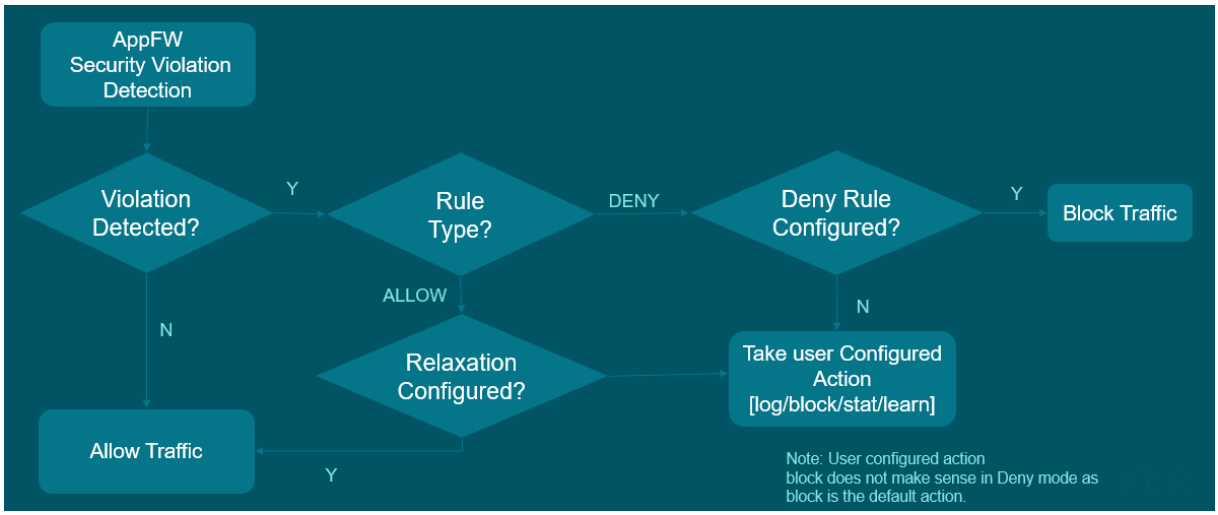
August 20, 2021

Cuando hay tráfico entrante, la lógica de detección de infracciones comprueba si hay infracciones de tráfico. Si no se detectan ataques de inyección HTML SQL, se permite que el tráfico pase. Pero si se detecta una infracción, las reglas de relajación (permitir) y denegar definen cómo manejar las

infracciones. Si la comprobación de seguridad está configurada en modo permitido (modo predeterminado), la infracción detectada se bloquea a menos que el usuario haya configurado explícitamente una regla de relajación o permiso.

Además del modo de permiso, la comprobación de seguridad también se puede configurar en modo deny y utilizar reglas de denegación para gestionar las infracciones. Si la comprobación de seguridad está configurada en este modo, las infracciones detectadas se bloquean si un usuario ha configurado explícitamente una regla de denegación. Si no hay reglas de denegación configuradas, se aplica la acción configurada por el usuario.

En la siguiente ilustración se explica cómo permitir y denegar los modos de trabajo de operación:



1. Cuando se detecta una infracción, las reglas de relajación (permitir) y denegar definen cómo manejar las infracciones.
2. Si la comprobación de seguridad está configurada en modo deny (si se configura en modo de permiso, vaya al paso 5), la infracción se bloquea a menos que haya configurado explícitamente una regla de denegación.
3. Si la infracción coincide con una regla de denegación, el dispositivo bloquea el tráfico.
4. Si la infracción de tráfico no coincide con una regla, el dispositivo aplica una acción definida por el usuario (bloquear, restablecer o soltar).
5. Si la comprobación de seguridad está configurada en modo de permiso, el módulo Web App Firewall comprueba si hay alguna regla de permiso configurada.
6. Si la infracción coincide con una regla de permiso, el dispositivo permite que el tráfico se omite de lo contrario, se bloquea.

Configurar el modo de cumplimiento y relajación de registro de seguridad

En el símbolo del sistema, escriba:


```
set appfw profile <name>   - SQLInjectionAction [block stats learn]  -
    SQLInjectionRuleType [ALLOW DENY]
<!--NeedCopy-->
```

Ejemplo:

```
set appfw profile prof1 sqlInjectionAction block -sqlInjectionRuleType
ALLOW DENY
```

Vincular reglas de relajación y aplicación al perfil de Web Application Firewall

En el símbolo del sistema, escriba:

```
bind appfw profile <name> -SQLInjection <string> <formActionURL>
<!--NeedCopy-->
```

Ejemplo:

```
bind appfw profile p1 -SQLInjection field_f1 ”/login.php”-RuleType ALLOW
bind appfw profile p2 -SQLInjection field_f1 ”/login.php”-RuleType ALLOW
```

comprobación de protección de inyección de comandos HTML

October 5, 2021

La comprobación de inyección de comandos **HTML** examina si el tráfico entrante tiene comandos no autorizados que interrumpen la seguridad del sistema o modifican el sistema. Si el tráfico tiene comandos maliciosos cuando se detecta, el dispositivo bloquea la solicitud o realiza la acción configurada.

El perfil de Citrix Web App Firewall ahora se ha mejorado con una nueva comprobación de seguridad para los ataques de inyección de comandos. Cuando la comprobación de seguridad de inyección de comandos examina el tráfico y detecta cualquier comando malintencionado, el dispositivo bloquea la solicitud o realiza la acción configurada.

En un ataque de inyección de comandos, el atacante tiene como objetivo ejecutar comandos no autorizados en el sistema operativo Citrix ADC. Para lograrlo, el atacante inyecta comandos del sistema operativo mediante una aplicación vulnerable. Un dispositivo Citrix ADC es vulnerable a ataques de inyección si la aplicación transfiere datos no seguros (formularios, cookies o encabezado) al shell del sistema.

Cómo funciona la protección por inyección de comandos

1. Para una solicitud entrante, WAF examina el tráfico en busca de palabras clave o caracteres especiales. Si la solicitud entrante no tiene patrones que coincidan con ninguna de las palabras clave denegadas o caracteres especiales, se permite la solicitud. De lo contrario, la solicitud se bloquea, se elimina o se redirige en función de la acción configurada.
2. Si prefiere excluir una palabra clave o un carácter especial de la lista, puede aplicar una regla de relajación para eludir la comprobación de seguridad bajo condiciones específicas.
3. Puede habilitar el registro para generar mensajes de registro. Puede supervisar los registros para determinar si las respuestas a las solicitudes legítimas se están bloqueando. Un gran aumento en el número de mensajes de registro puede indicar intentos de lanzar un ataque.
4. También puede habilitar la función de estadísticas para recopilar datos estadísticos sobre infracciones y registros. Un aumento inesperado en el contador de estadísticas podría indicar que su aplicación está siendo atacada. Si las solicitudes legítimas se bloquean, es posible que tenga que volver a visitar la configuración para ver si debe configurar la nueva regla de relajación o modificar la existente.

Palabras clave y caracteres especiales denegados para la comprobación de inyección de comandos

Para detectar y bloquear ataques de inyección de comandos, el dispositivo tiene un conjunto de patrones (palabras clave y caracteres especiales) definidos en el archivo de firma predeterminado. A continuación se muestra una lista de palabras clave bloqueadas durante la detección de inyección de comandos.

```
    <commandinjection>
      <keyword type="LITERAL" builtin="ON">7z</keyword>
      <keyword type="LITERAL" builtin="ON">7za</keyword>
      <keyword type="LITERAL" builtin="ON">7zr</keyword>
…
</commandinjection>
<!--NeedCopy-->
```

Los caracteres especiales definidos en el archivo de firma son:
`| ; & $ > < '\ ! >> ##`

Configuración de la comprobación de inyección de comandos mediante la CLI

En la interfaz de línea de comandos, puede utilizar el comando set the profile o el comando add the profile para configurar los parámetros de inyección de comandos. Puede activar las acciones de bloqueo, registro y estadísticas. También debe establecer las palabras clave y los caracteres de cadena que quiere detectar en las cargas útiles.

En el símbolo del sistema, escriba:

```
set appfw profile <profile-name> -cmdInjectionAction <action-name> -CMDInjectionType
 <CMDInjectionType>]
```

> **Nota:**
>
> De forma predeterminada, la acción de inyección de comandos se establece como "Ninguno". Además, el tipo de inyección de comando predeterminado se establece como`CmdSplCharANDKeyWord` .

Ejemplo:

```
set appfw profile profile1 -cmdInjectionAction block -CMDInjectionType
CmdSplChar
```

Donde las acciones de inyección de comandos disponibles son:

- Ninguno: Desactive la protección de inyección de comandos.
- Registro: Registre infracciones de inyección de comandos para la comprobación de seguridad.
- Bloquear: Bloquea el tráfico que infringe la comprobación de seguridad de inyección de comandos.
- Estadísticas: Genera estadísticas de violaciones de seguridad de inyección de comandos.

Donde los tipos de inyección de comando disponibles son:

- Cmd SplChar. Comprueba caracteres especiales
- CmdKeyword. Comprobación palabras clave de inyección
- CmdsPlcharAndKeyword. Comprueba los caracteres especiales y la inyección de comandos. Palabras clave y bloques solo si ambos están presentes.
- CmdSplCharorKeyword. Comprueba los caracteres especiales y la inyección de comandos Palabras clave y bloques si se encuentra alguno de ellos.

Configuración de las reglas de relajación para la comprobación de protección por inyección

Si su aplicación requiere que omita la inspección de inyección de comandos para un ELEMENTO o ATTRIBUTE específico en la carga útil, puede configurar una regla de relajación.

El comando Las reglas de relajación de inspección por inyección tienen la siguiente sintaxis:


```
bind appfw profile <profile name> -cmdInjection <string> <URL> -isregex <
REGEX/NOTREGEX>
```

Ejemplo de regla de relajación para Regex en el encabezado

```
bind appfw profile sample -CMDInjection hdr ”http://10.10.10.10/”-location
heaDER -valueType Keyword '[a-z]+grep'-isvalueRegex REGEX
```

Como resultado, la inyección exime de la comprobación de inyección de comandos permite que el encabezado `hdr` contenga variantes de “grep”. “

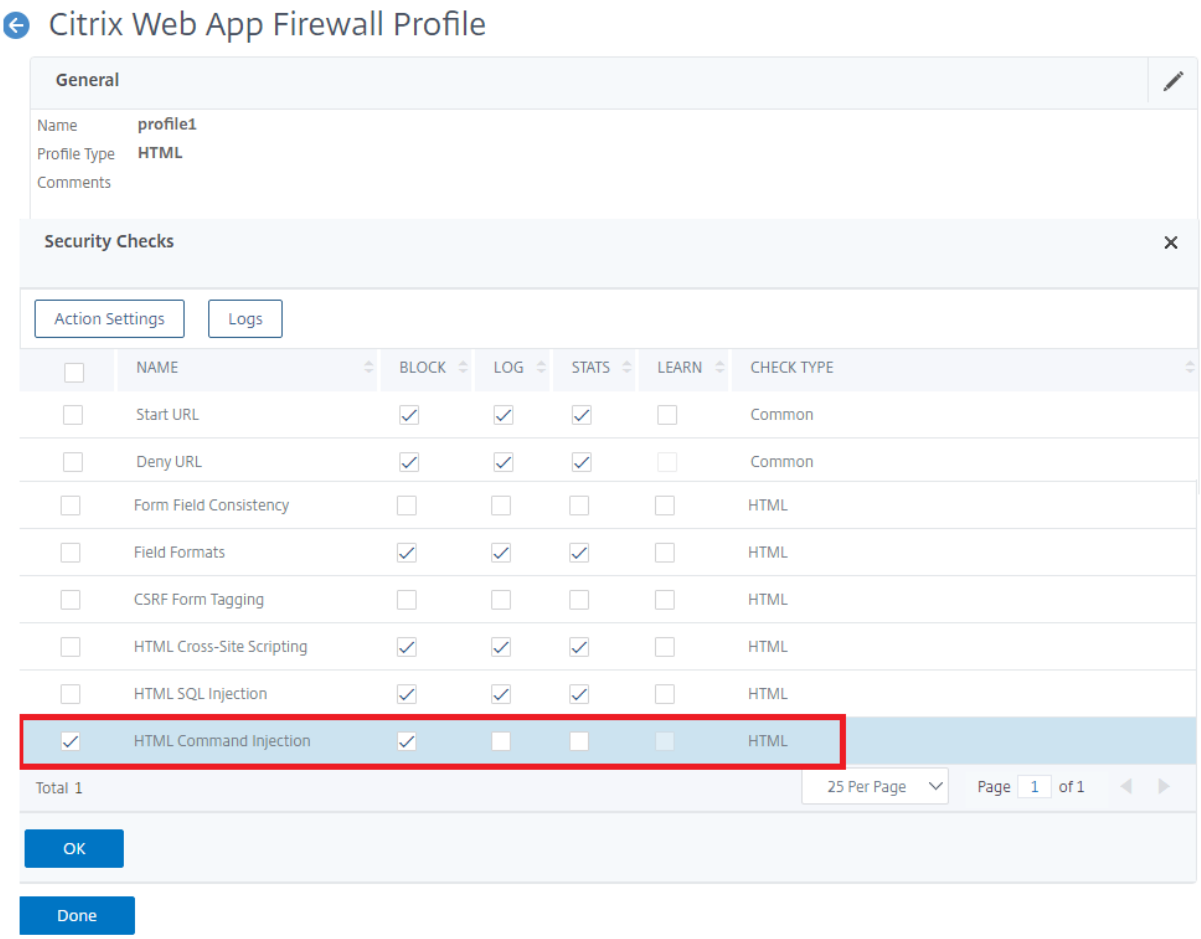
Ejemplo de regla de relajación con ValueType como expresión regular en cookie

```
bind appfw profile sample -CMDInjection ck_login ”http://10.10.10.10/”-
location cookie -valueType Keyword 'pkg[a-z]+'-isvalueRegex REGEX
```

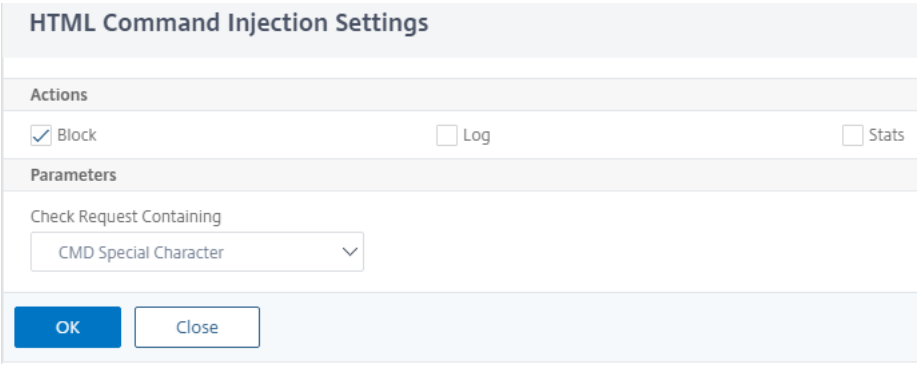
Configuración de la comprobación de inyección de comandos mediante la GUI de Citrix ADC

Complete los siguientes pasos para configurar la comprobación de inyección de comandos.

1. Vaya a **Seguridad > Perfiles y Citrix Web App Firewall**.
2. En la página **Perfiles**, seleccione un perfil y haga clic en **Modificar**.
3. En la página **Perfil de Citrix Web App Firewall**, vaya a la sección **Configuración avanzada** y haga clic en **Comprobaciones de seguridad**.



1. En la sección **Comprobaciones de seguridad**, seleccione **Inyección de comandos HTML** y haga clic en Configuración de **acciones**.
2. En la página **Configuración de inyección de comandos HTML**, establezca los siguientes parámetros:
   a) Acciones. Seleccione una o más acciones para la comprobación de seguridad de inyección de comandos.
   b) Comprobar solicitud que contiene. Seleccione un patrón de inyección de comandos para comprobar si la solicitud entrante tiene el patrón.
3. Haga clic en **Aceptar**.



Visualización o personalización de patrones de inyección de comandos mediante la GUI

Puede utilizar la GUI para ver o personalizar los patrones de inyección de comandos **HTML** .

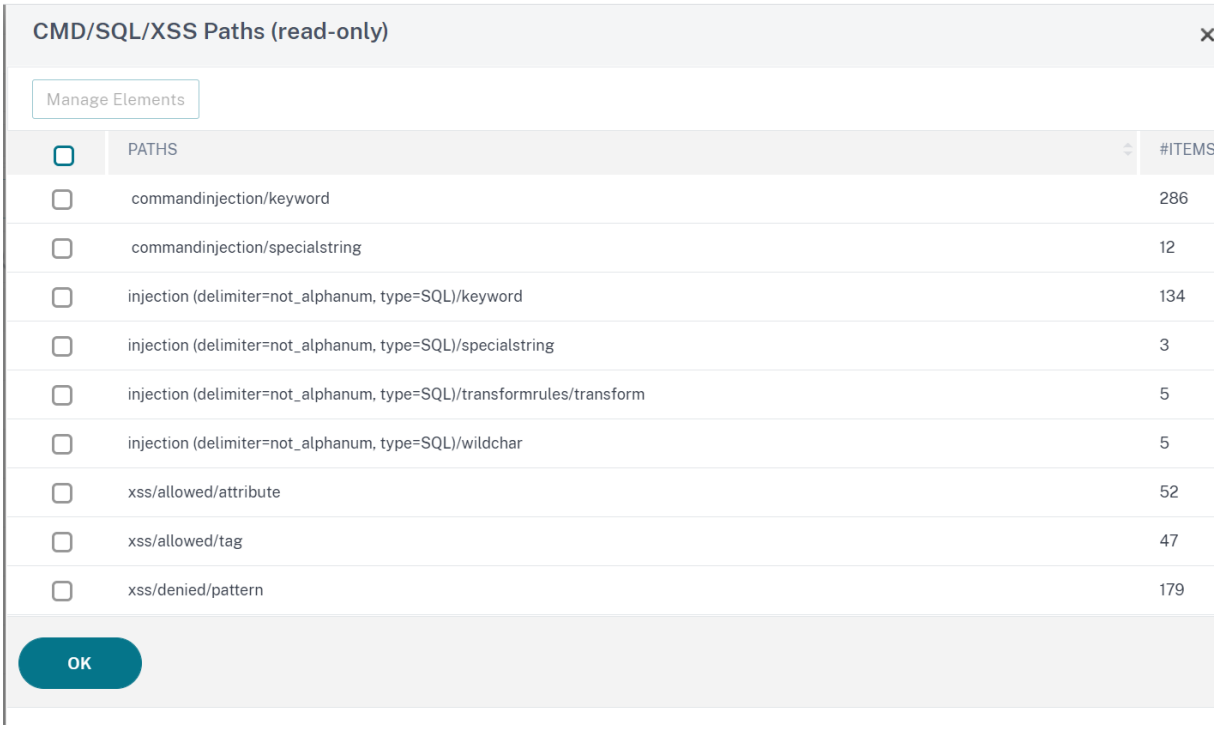
Los patrones de inyección de comandos predeterminados se especifican en el archivo de firmas predeterminado. Si no vincula ningún objeto de firma a su perfil, el perfil utilizará los patrones de inyección de comandos HTML predeterminados especificados en el objeto de firmas predeterminados para procesar la comprobación de seguridad de inyección de comandos. Las reglas y patrones, especificados en el objeto de firmas predeterminado, son de solo lectura. No puede modificarlos ni modificarlos. Si desea modificar o cambiar estos patrones, haga una copia del objeto SSignatures predeterminado para crear un objeto de firma definido por el usuario. Realice cambios en los patrones de inyección de comandos en el nuevo objeto de firma definido por el usuario y utilice este objeto de firma en su perfil que procesa el tráfico para el que desea utilizar estos patrones personalizados.

Para obtener más información, consulte Firmas

Para ver los patrones de inyección de comandos predeterminados mediante la GUI:

1. Vaya a **Firewall de aplicaciones > Firmas**, seleccione ***Firmas predeterminadas** y haga clic en **Modificar**.

1. Haga clic en **Administrar patrones CMD/SQL/XSS**. La tabla **Rutas CMD/SQL/XSS (solo lectura)** muestra patrones relacionados con la `CMD` / `SQL` / `XSS` inyección:



1. Seleccione una fila y haga clic en **Administrar elementos** para mostrar los patrones de inyección de comandos correspondientes (palabras clave, cadenas especiales, reglas de transformación o caracteres comodín) utilizados por la comprobación de inyección de comandos de Web App Firewall.

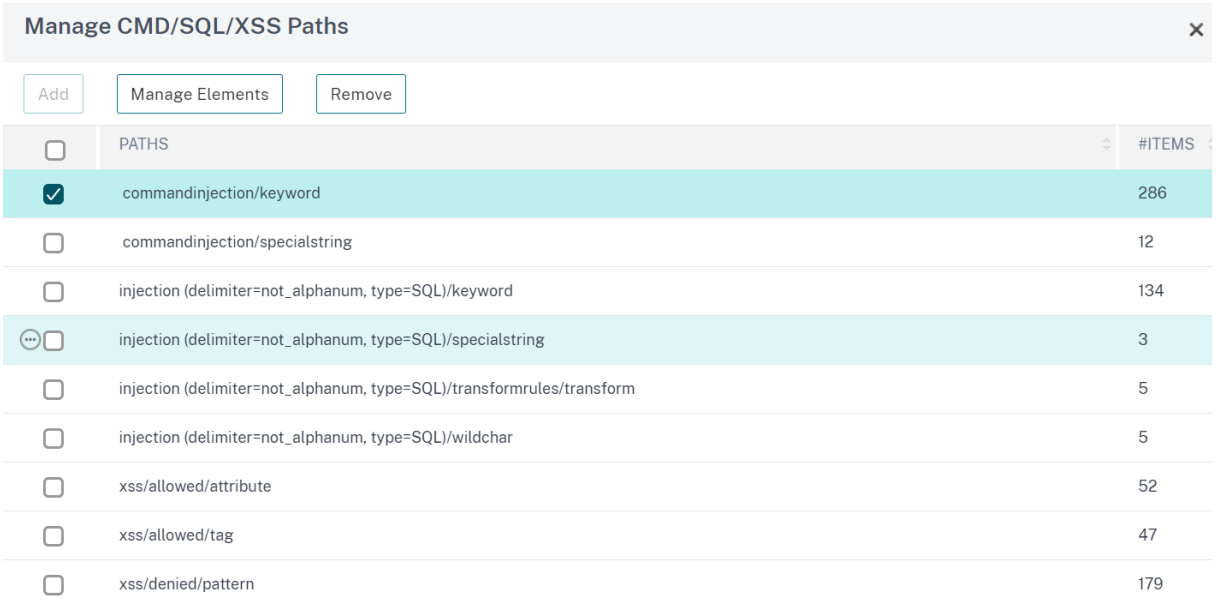
Para personalizar un patrón de inyección de comandos mediante la GUI

Puede modificar el objeto de firma definido por el usuario para personalizar las palabras clave de

CMD, las cadenas especiales y los caracteres comodín. Puede agregar nuevas entradas o eliminar las existentes. Puede modificar las reglas de transformación de las cadenas especiales de inyección de comandos.

1. **Vaya a Firewall de aplicaciones > Firmas**, resalte la firma definida por el usuario de destino y haga clic en **Agregar**. Haga clic en **Administrar patrones CMD/SQL/XSS**.
2. En la página **Administrar rutas CMD/SQL/XSS**, seleccione la fila de inyección CMD de destino.
3. Haga clic en **Administrar elementos**, **Agregar**o **quitar** un elemento de inyección de comandos.

> **Advertencia:**
>
> Debe tener cuidado antes de quitar o modificar cualquier elemento de inyección de comandos predeterminado o eliminar la ruta CMD para eliminar toda la fila. Las reglas de firma y la comprobación de seguridad de inyección de comandos se basan en estos elementos para detectar ataques de inyección de comandos a fin de proteger sus aplicaciones. La personalización de los patrones SQL puede hacer que la aplicación sea vulnerable a los ataques de inyección de comandos si se elimina el patrón necesario durante la edición.



Visualización de estadísticas de tráfico de inyección de comandos e infracciones

La página **Estadísticas de Citrix Web App Firewall** muestra los detalles del tráfico de seguridad y las infracciones de seguridad en un formato tabular o gráfico.

Para ver las estadísticas de seguridad mediante la interfaz de comandos.

En el símbolo del sistema, escriba:

```
stat appfw profile profile1
```


Appfw perfil Estadísticas de tráfico	Tasa (s)	Total
Solicitudes	0	0
Bytes de solicitud	0	0
Respuestas	0	0
Bytes de respuesta	0	0
Aborta	0	0
Redirecciona	0	0
Tiempo de respuesta a largo plazo (ms)	–	0
Tiempo de respuesta reciente Ave (ms)	–	0

Estadísticas de violaciones HTML/XML/JSON	Tasa (s)	Total
URL de inicio	0	0
Denegar URL	0	0
Encabezado de referencia	0	0
Desbordamiento de búfer	0	0
Consistencia de cookies	0	0
Secuestro de cookies	0	0
Etiqueta de formulario CSRF	0	0
Scripting HTML entre sitios	0	0
Inyección HTML SQL	0	0
Formato de campo	0	0
Consistencia de campo	0	0
Tarjeta de crédito	0	0
Objeto seguro	0	0
Violaciones de firma	0	0
Tipo de contenido	0	0
JSON Denegación de Servicio	0	0

Estadísticas de violaciones HTML/XML/JSON	Tasa (s)	Total
Inyección JSON SQL	0	0
Scripting JSON entre sitios	0	0
Tipos de carga de archivos	0	0
Inducir la carga útil XML del tipo de contenido	0	0
Inyección HTML CMD	0	0
Formato XML	0	0
Denegación de servicio XML (XDoS)	0	0
Validación de mensajes XML	0	0
Interoperabilidad de servicios web	0	0
Inyección XML SQL	0	0
Scripting XML entre sitios	0	0
Datos adjuntos XML	0	0
Violaciones de errores SOAP	0	0
Violaciones genéricas de XML	0	0
Total de violaciones	0	0

Estadísticas de registro HTML/XML/JSON	Tasa (s)	Total
Registros de URL de inicio	0	0
Denegar registros de URL	0	0
Registros de encabezado de referer	0	0
Registros de desbordamiento de	0	0
Registros de coherencia de cookies	0	0

Estadísticas de registro HTML/XML/JSON	Tasa (s)	Total
Registros de secuestro de cookies	0	0
CSRF de registros de etiquetas	0	0
Registros de scripts de sitios cruzados HTML	0	0
Registros de transformación de scripts multisitio HTML	0	0
Registros de inyección HTML SQL	0	0
Registros de transformación HTML SQL	0	0
Registros de formato de campo	0	0
Registros de coherencia de campo	0	0
Tarjetas de crédito	0	0
Registro de transformación de tarjetas de crédito	0	0
Registros de objetos seguros	0	0
Registros de firmas	0	0
Registros de tipo de contenido	0	0
Registros de denegación de servicio JSON	0	0
Registros de inyección JSON SQL	0	0
Registros de scripts entre sitios JSON	0	0
Tipos de carga de archivos registros	0	0
Inducir tipo de contenido XML Carga útil L	0	0

Estadísticas de registro HTML/XML/JSON	Tasa (s)	Total
Registros de inyección de comandos HTML	0	0
Registros de formato XML	0	0
Registros XML de denegación de servicio (XDoS)	0	0
Registros de validación de mensajes XML	0	0
Registros WSI	0	0
Registros de inyección XML SQL	0	0
Registros de scripts entre sitios XML	0	0
Registro de datos adjuntos XML	0	0
Registros de errores SOAP	0	0
Registros genéricos XML	0	0
Total de mensajes de registro	0	0

Tasa de estadísticas de respuesta a errores del servidor (/s) > Total			
Errores de cliente HTTP (4xx Resp)	0	0	Errores del servidor
HTTP (5xx Resp)	0	0	

Visualización de estadísticas de inyección de comandos HTML mediante la GUI de Citrix ADC

Complete los siguientes pasos para ver las estadísticas de inyección de comandos:

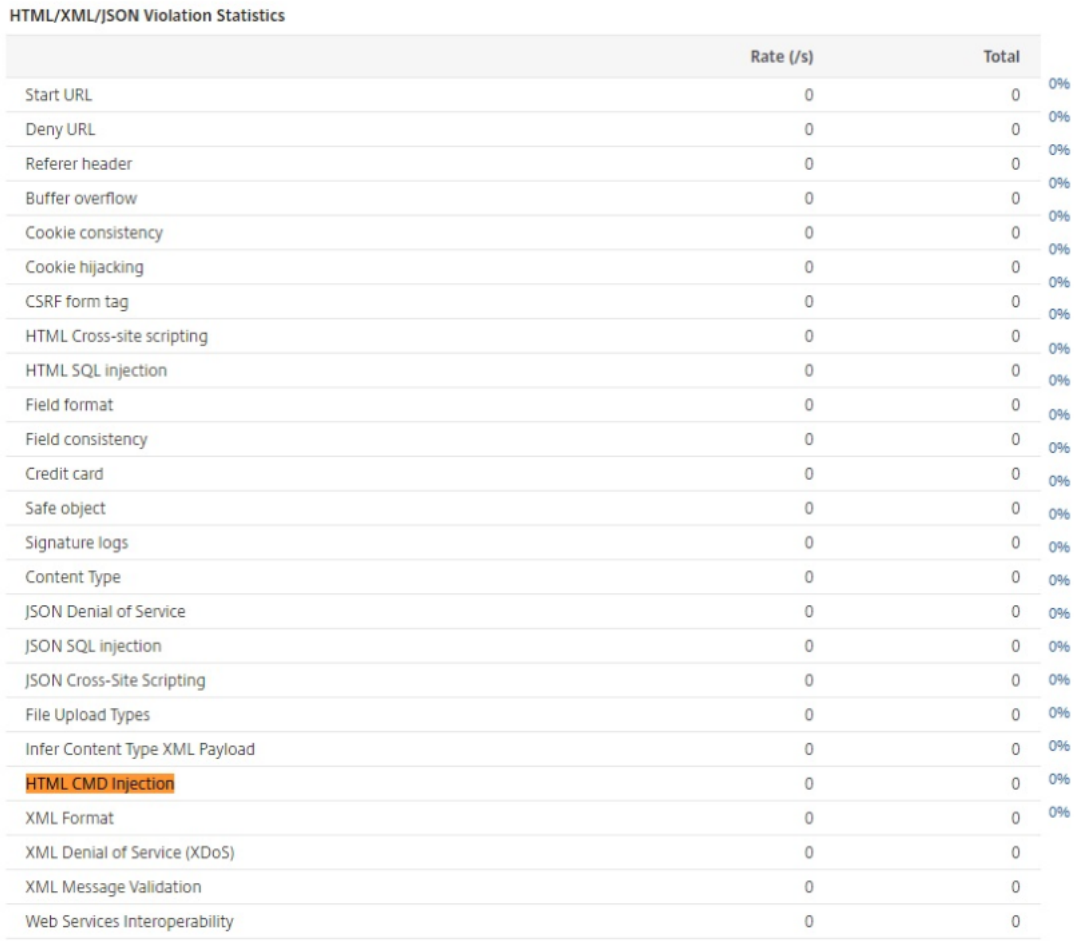
1. Vaya a **Seguridad > Citrix Web App Firewall > Perfiles**.
2. En el panel de detalles, seleccione un perfil de Web App Firewall y haga clic en **Estadísticas**.

3. La página **Estadísticas de Citrix Web App Firewall** muestra los detalles del tráfico de inyección de comandos HTML y la infracción.
4. Puede seleccionar **Vista tabular** o cambiar a **Vista gráfica** para mostrar los datos en formato tabular o gráfico.

Estadísticas de tráfico de inyección de comandos HTML

HTML SQL Injection logs	0	0
HTML SQL transform logs	0	0
Field format logs	0	0
Field consistency logs	0	0
Credit cards	0	0
Credit card transform logs	0	0
Safe object logs	0	0
Signature logs	0	0
Content Type logs	0	0
JSON Denial of Service logs	0	0
JSON SQL injection logs	0	0
JSON Cross-Site Scripting logs	0	0
File upload types logs	0	0
Infer Content Type XML Payload Logs	0	0
HTML Command Injection logs	0	0
XML Format logs	0	0
XML Denial of Service(XDoS) logs	0	0
XML Message Validation logs	0	0
WSI logs	0	0
XML SQL Injection logs	0	0
XML XSS logs	0	0
XML Attachment logs	0	0

Estadísticas de infracción de inyección de comandos HTML



HTML/XML/JSON Violation Statistics

	Rate (/s)	Total	
Start URL	0	0	0%
Deny URL	0	0	0%
Referer header	0	0	0%
Buffer overflow	0	0	0%
Cookie consistency	0	0	0%
Cookie hijacking	0	0	0%
CSRF form tag	0	0	0%
HTML Cross-site scripting	0	0	0%
HTML SQL injection	0	0	0%
Field format	0	0	0%
Field consistency	0	0	0%
Credit card	0	0	0%
Safe object	0	0	0%
Signature logs	0	0	0%
Content Type	0	0	0%
JSON Denial of Service	0	0	0%
JSON SQL injection	0	0	0%
JSON Cross-Site Scripting	0	0	0%
File Upload Types	0	0	0%
Infer Content Type XML Payload	0	0	0%
HTML CMD Injection	0	0	0%
XML Format	0	0	0%
XML Denial of Service (XDoS)	0	0	
XML Message Validation	0	0	
Web Services Interoperability	0	0	

Compatibilidad con palabras clave personalizadas para la carga útil HTML

July 15, 2022

A partir de Citrix ADC versión 13.1 compilación 27.xx, puede agregar palabras clave de su elección y comprobar si estas palabras clave configuradas están presentes en la carga útil HTML.

La inyección SQL y la inyección de comandos tienen un conjunto predefinido de palabras clave o patrones que buscan en las solicitudes entrantes. Es posible que estos conjuntos predefinidos de palabras clave no cubran todas las palabras clave según sus necesidades y podrían provocar un aumento en el número de falsos positivos. Con esta función, puede agregar palabras clave que no están cubiertas en las comprobaciones de inyección de SQL e inyección de comandos y, por lo tanto, reducir los falsos positivos.

Después de agregar las palabras clave, puede configurar el dispositivo Citrix ADC para comprobar si las

palabras clave agregadas se detectan en las solicitudes entrantes. A continuación, puede configurar el dispositivo Citrix ADC para que realice una de las siguientes acciones:

- **Ninguno** : no se realiza ninguna acción. Esta acción es la predeterminada.
- **Registro** : registra todas las solicitudes que coinciden con la URL y tienen las palabras clave configuradas.
- **Bloquear** : bloquea todas las solicitudes que coincidan con la URL y tengan las palabras clave configuradas.
- **Estadísticas** : aumente el contador de registros para cada solicitud que coincida con la URL y tenga las palabras clave configuradas.

Agregar palabras clave personalizadas mediante la CLI

La adición de una palabra clave personalizada mediante la CLI implica los siguientes pasos:

1. Configure un perfil de firewall de aplicaciones web y defina una acción cuando se detecte la palabra clave personalizada en la solicitud entrante.

```
set appfw profile <profile-name>  - blockKeywordAction (block | log
    | stats | none)
<!--NeedCopy-->
```

   De forma predeterminada, -blockKeywordAction se establece en none.

   Ejemplo:

```
set appfw profile test_profile -blockKeywordAction none
<!--NeedCopy-->
```

2. Vincule el perfil de firewall de aplicaciones web con sus palabras clave personalizadas.

```
bind appfw profile <profile_name> -blockKeyword <keyword_name> -
   BlockKeywordType <literal|PCRE > -fieldName <field_name> -
   formURL <URL> -isFieldNameRegex <REGEX|NOTREGEX> -state <enable
   /disable> -comment <text>
<!--NeedCopy-->
```

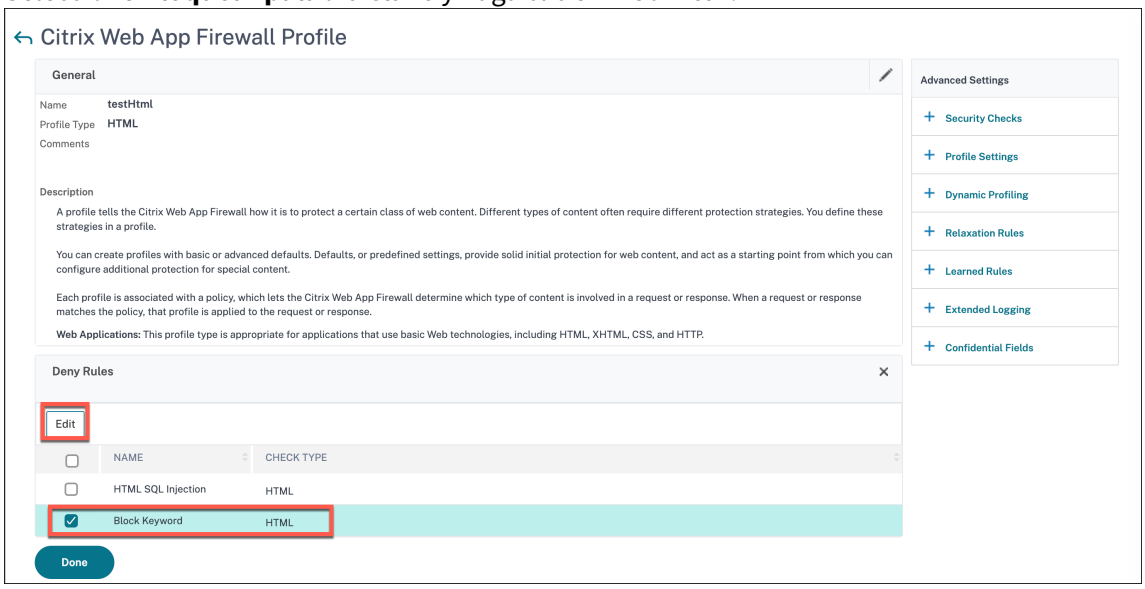
   Ejemplo:

   Para agregar **blockword** como palabra clave personalizada y vincularla a **test_profile**, ejecute el siguiente comando:

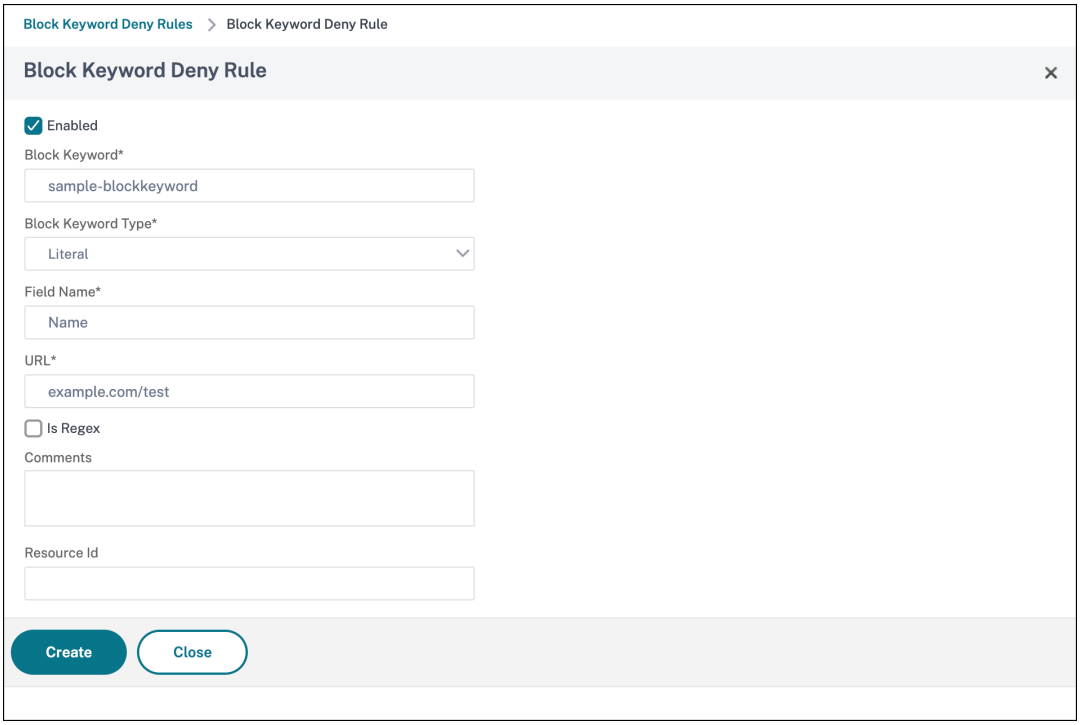

```
1 bind appfw profile test_profile -blockKeyword ”blockword”
    BlockKeywordType literal -fieldName ”firstname” -formURL ”/
    signup.php” -state enable
2 <!--NeedCopy-->
```

Agregar palabras clave personalizadas mediante la GUI

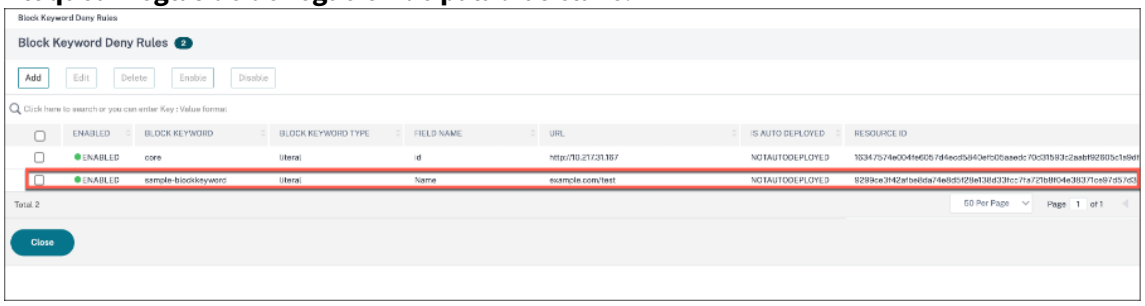
1. Vaya a **Seguridad > Perfil de Citrix Web App Firewall > Perfiles**.
2. Seleccione un perfil y haga clic en **Modificar**.
3. Vaya a la sección**Configuración avanzada**y haga clic en **Denegar reglas**.
4. Seleccione **Bloquear palabra clave** y haga clic en **Modificar**.



5. Haga clic en **Agregar** y defina los siguientes parámetros:
   - Enable
   - Bloquear palabra clave
   - Bloquear tipo palabra clave
   - Nombre de campo
   - URL
   - Es Regex
   - Comentarios
   - ID de recurso



6. Haga clic en **Crear**. La palabra clave personalizada que ha agregado aparece en la página **Bloquear reglas de denegación de palabras clave**.



7. Vaya a la sección **Configuración avanzada** y haga clic en **Comprobaciones de seguridad**.
8. Seleccione **Bloquear palabra clave** y haga clic en **Configuración de acciones**.

9. Seleccione las acciones necesarias y haga clic en **Aceptar**.

Ver estadísticas de palabras clave personalizadas mediante la CLI

Para ver las estadísticas de palabras clave personalizadas, escriba el siguiente comando en el símbolo del sistema:


```
stat appfw profile <profile name>
<!--NeedCopy-->
```

Ejemplo

```
stat appfw profile test_profile
<!--NeedCopy-->
```

Ver estadísticas de palabras clave personalizadas en la interfaz

1. Vaya a**Seguridad > Citrix Web App Firewall > Perfiles**.
2. En el panel de detalles, seleccione un **perfil de Web App Firewall** y haga clic en**Estadísticas**. La página**Estadísticas de Citrix Web App Firewall**muestra los detalles de tráfico e infracción de palabras clave personalizadas.
3. Puede seleccionar**Vista tabular**o cambiar a**Vista gráfica**para mostrar los datos en formato tabular o gráfico.

Protección contra ataques de entidades externas XML (XXE)

August 20, 2021

La protección contra ataques de entidades externas XML (XXE) examina si una carga útil entrante tiene cualquier entrada XML no autorizada con respecto a entidades fuera del dominio de confianza donde reside la aplicación web. El ataque XXE se produce si tiene un analizador XML débil que analiza una carga XML con entrada que contiene referencias a entidades externas.

En un dispositivo Citrix ADC, si el analizador XML está configurado incorrectamente, el impacto de explotar la vulnerabilidad puede ser peligroso. Permite a un atacante leer datos confidenciales en el servidor web. Realiza el ataque de denegación de servicio, etc. Por lo tanto, es importante proteger el dispositivo de ataques XXE. Web Application Firewall puede proteger el dispositivo de ataques XXE siempre que el tipo de contenido se identifique como XML. Para evitar que un usuario malintencionado omite este mecanismo de protección, WAF bloquea una solicitud entrante si el tipo de contenido “inferido” de los encabezados HTTP no coincide con el tipo de contenido del cuerpo. Este mecanismo evita la omisión de la protección contra ataques XXE cuando se utiliza un tipo de contenido predeterminado o no predeterminado en la lista de permitidos.

Algunas de las posibles amenazas XXE que afectan a un dispositivo Citrix ADC son:

- Fugas de datos confidenciales
- Ataques de denegación de servicio (DOS)
- solicitudes de falsificación del lado del servidor
- Exploración de puertos

Configurar la protección de inyección de entidades externas XML (XXE)

Para configurar entidades externas XML (XXE), compruebe mediante la interfaz de comandos:
En la interfaz de línea de comandos, puede agregar o modificar el comando de perfil de firewall de aplicaciones para configurar la configuración de **XXE** . Puede activar las acciones de bloqueo, registro y estadísticas.

En el símbolo del sistema, escriba:

```
set appfw profile <name> [-inferContentTypeXmlPayloadAction <inferContentTypeXmlPaylo
 <block | log | stats | none>]
```

> Nota:
>
> De forma predeterminada, la acción XXE se establece como “ninguno”. “

Ejemplo:

```
set appfw profile profile1 -inferContentTypeXmlPayloadAction Block
```

Donde los tipos de acción son:

Bloqueo: La solicitud se bloquea sin ninguna excepción a las URL de la solicitud.

Registro: Si se produce una discrepancia entre el tipo de contenido en un encabezado de solicitud HTTP y la carga útil, la información sobre la solicitud infractora debe estar contenida en el mensaje de registro.

Estadísticas: Si se detecta una discrepancia en los tipos de contenido, se incrementan las estadísticas correspondientes para este tipo de infracción.

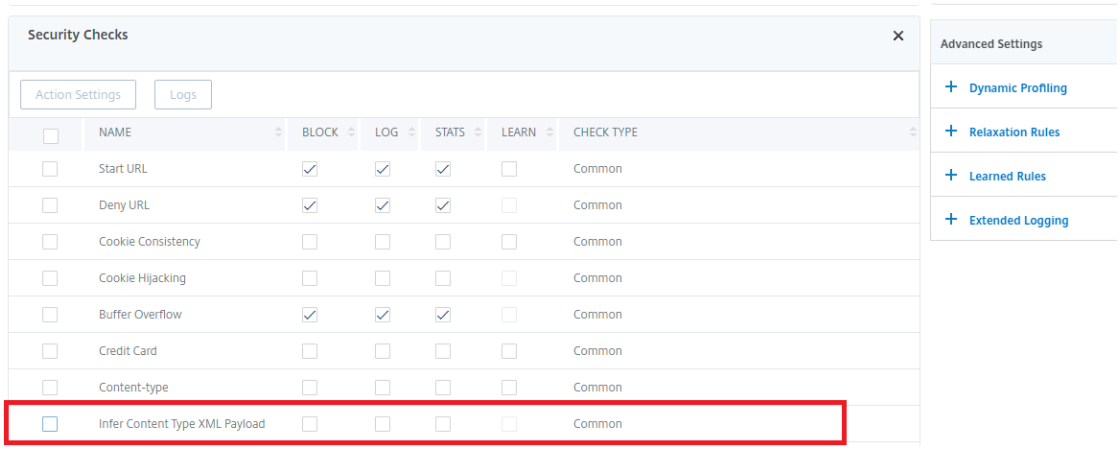
Ninguno: No se realiza ninguna acción si se detecta una discrepancia en los tipos de contenido. Ninguno no se puede combinar con ningún otro tipo de acción. La acción predeterminada se establece en Ninguno.

Configurar la comprobación de inyección XXE mediante la GUI de Citrix ADC

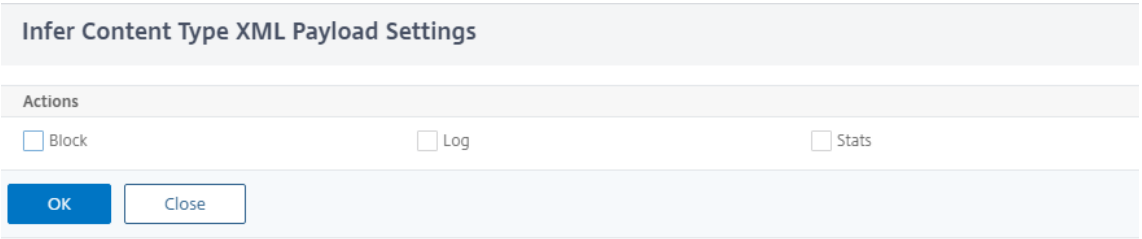
Complete los siguientes pasos para configurar la comprobación de inyección XXE.

1. Vaya a **Seguridad > Citrix Web App Firewall > Perfiles**.
2. En la página **Perfiles**, seleccione un perfil y haga clic en **Modificar**.

3. En la página **Perfil de Citrix Web App Firewall**, vaya a la sección **Configuración avanzada** y haga clic en **Comprobaciones de seguridad**.



4. En la sección **Comprobaciones de seguridad**, seleccione **Deducir tipo de contenido XML Carga útil** y haga clic en Configuración de **acciones**.
5. En la página Deducir configuración de carga útil XML del tipo de contenido, establezca los siguientes parámetros:
   a) Acciones. Seleccione una o más acciones para la comprobación de seguridad de inyección XXE.
6. Haga clic en **Aceptar**.



Visualización de estadísticas de infracciones y tráfico de inyección XXE

La página Estadísticas de Citrix Web App Firewall muestra los detalles del tráfico de seguridad y las infracciones de seguridad en un formato tabular o gráfico.

Para ver las estadísticas de seguridad mediante la interfaz de comandos.

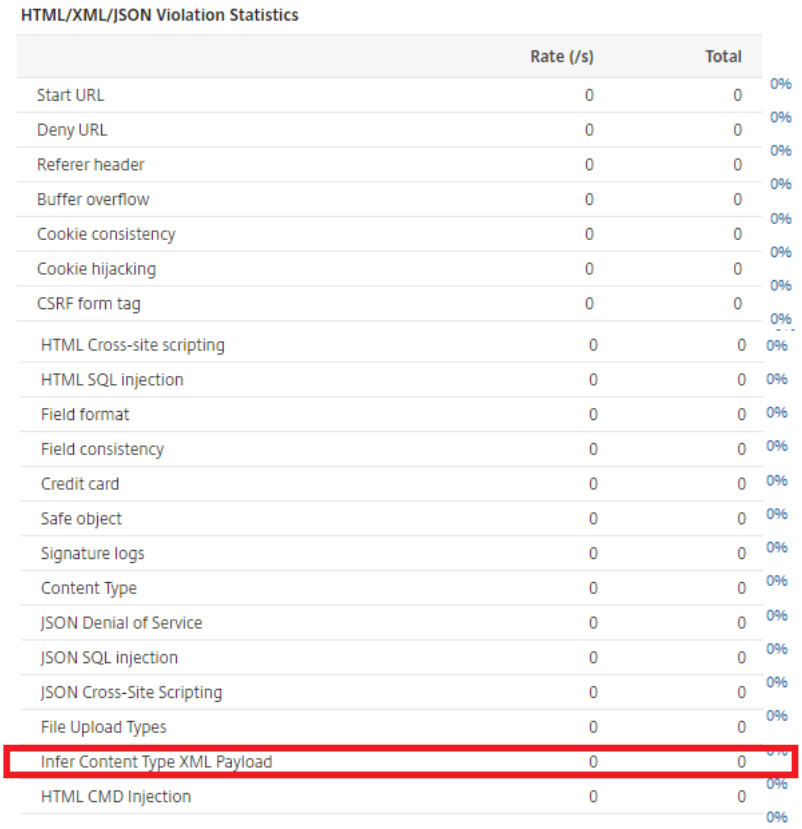
En el símbolo del sistema, escriba:

```
stat appfw profile profile1
```


Visualización de estadísticas de inyección XXE mediante la GUI de Citrix ADC

Complete los siguientes pasos para ver las estadísticas de inyección XXE:

1. Vaya a **Seguridad > Citrix Web App Firewall > Perfiles**.
2. En el panel de detalles, seleccione un perfil de Web App Firewall y haga clic en **Estadísticas**.
3. La página **Estadísticas de Citrix Web App Firewall** muestra los detalles del tráfico de inyección de comandos XXE y la infracción.
4. Puede seleccionar **Vista tabular** o cambiar a **Vista gráfica** para mostrar los datos en formato tabular o gráfico.



HTML/XML/JSON Violation Statistics

	Rate (/s)	Total	
Start URL	0	0	0%
Deny URL	0	0	0%
Referer header	0	0	0%
Buffer overflow	0	0	0%
Cookie consistency	0	0	0%
Cookie hijacking	0	0	0%
CSRF form tag	0	0	0%
HTML Cross-site scripting	0	0	0%
HTML SQL injection	0	0	0%
Field format	0	0	0%
Field consistency	0	0	0%
Credit card	0	0	0%
Safe object	0	0	0%
Signature logs	0	0	0%
Content Type	0	0	0%
JSON Denial of Service	0	0	0%
JSON SQL injection	0	0	0%
JSON Cross-Site Scripting	0	0	0%
File Upload Types	0	0	0%
Infer Content Type XML Payload	0	0	0%
HTML CMD Injection	0	0	0%

Comprobación de desbordamiento de búfer

August 20, 2021

La comprobación de desbordamiento de búfer detecta los intentos de provocar un desbordamiento de búfer en el servidor web. Si Web App Firewall detecta que la URL, las cookies o el encabezado son más largos que la longitud configurada, bloquea la solicitud porque puede provocar un desbordamiento del búfer.

La comprobación de desbordamiento de búfer evita ataques contra software de servidor web o sistema operativo inseguro que puede bloquearse o comportarse de forma impredecible cuando recibe una cadena de datos mayor de lo que puede manejar. Las técnicas de programación adecuadas evitan los desbordamientos de búfer mediante la comprobación de los datos entrantes y el rechazo o truncamiento de cadenas excesivas. Muchos programas, sin embargo, no comprueban todos los datos entrantes y, por lo tanto, son vulnerables a los desbordamientos de búfer. Este problema afecta especialmente a las versiones anteriores del software del servidor web y los sistemas operativos, muchos de los cuales todavía están en uso.

La comprobación de seguridad de desbordamiento de búfer le permite configurar las acciones **Bloque**, **Registro** y **Estadísticas**. Además, también puede configurar los siguientes parámetros:

- **Longitud máxima de URL**. La longitud máxima que permite Web App Firewall en una URL solicitada. Las solicitudes con URL más largas están bloqueadas. **Valores posibles**: 0—65535. **Predeterminado**: 1024
- **Longitud máxima de las cookies**. La longitud máxima que el Web App Firewall permite para todas las cookies en una solicitud. Las solicitudes con cookies más largas desencadenan las infracciones. **Valores posibles**: 0—65535. **Predeterminado**: 4096
- **Longitud máxima del encabezado**. La longitud máxima que el Web App Firewall permite para encabezados HTTP. Las solicitudes con cabeceras más largas están bloqueadas. **Valores posibles**: 0—65535. **Predeterminado**: 4096
- **Longitud de cadena de consulta**. Longitud máxima permitida para la cadena de consulta en una solicitud entrante. Las solicitudes con consultas más largas están bloqueadas. Valores posibles: 0—65535. Predeterminado: 1024
- **Longitud total de la solicitud**. Longitud máxima de solicitud permitida para una solicitud entrante. Las solicitudes con mayor longitud están bloqueadas. Valores posibles: 0—65535. Predeterminado: 24820

Uso de la línea de comandos para configurar la comprobación de seguridad de desbordamiento de búfer

Para configurar acciones de comprobación de seguridad de desbordamiento de búfer y otros parámetros mediante la línea de comandos

En el símbolo del sistema, escriba:

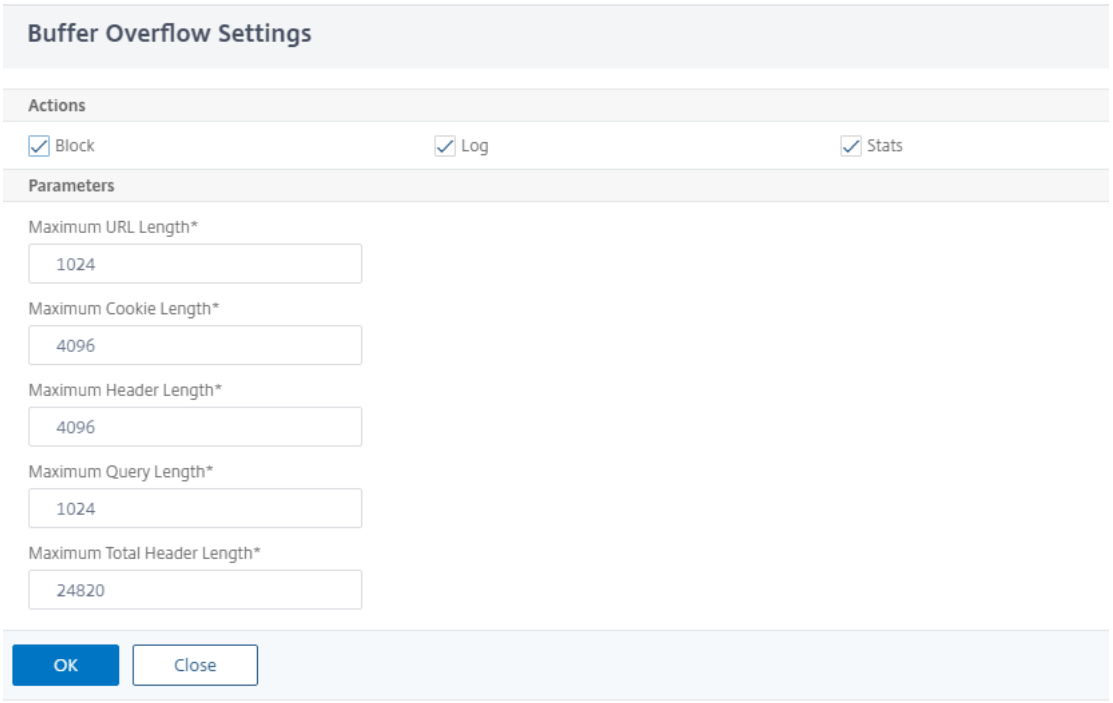
```
add appfw profile <name> -bufferOverflowMaxURLLength <positive_integer> -
bufferOverflowMaxHeaderLength <positive_integer> - bufferOverflowMaxCookieLength
 <positive_integer> -bufferOverflowMaxQueryLength <positive_integer> -
bufferOverflowMaxTotalHeaderLength <positive_integer>
```

Ejemplo:


```
add appfw profile profile1 -bufferOverflowMaxURLLength 7000 -bufferOverflowMaxHeaderLe
 7250 - bufferOverflowMaxCookieLength 7100 -bufferOverflowMaxQueryLength
7300 -bufferOverflowMaxTotalHeaderLength 7300
```

Configurar la comprobación de seguridad de desbordamiento de búfer mediante la GUI de Citrix ADC

1. Vaya a **Seguridad** > **Web App Firewall** y **perfiles**.
2. En la página **Perfiles**, seleccione un perfil y haga clic en **Modificar**.
3. En la página **Perfil de Citrix Web App Firewall**, vaya a la sección **Configuración avanzada** y haga clic en **Comprobaciones de seguridad**.
4. En **la sección Comprobaciones de seguridad**, seleccione **Desbordamiento de búfer** y haga clic en **Configuración de acciones**
5. En la página **Configuración de desbordamiento de búfer**, establezca los siguientes parámetros.
   a. Acciones. Seleccione una o más acciones para la comprobación de seguridad de inyección de comandos.
   b. Longitud máxima de URL. Longitud máxima, en caracteres, para las URL de los sitios web protegidos. Las solicitudes con URL más largas están bloqueadas.
   c. Longitud máxima de cookie. Longitud máxima, en caracteres, para las cookies enviadas a sus sitios web protegidos. Las solicitudes con cookies más largas están bloqueadas.
   d. Longitud máxima de cabecera. Longitud máxima, en caracteres, para los encabezados HTTP en las solicitudes enviadas a los sitios web protegidos. Las solicitudes con cabeceras más largas están bloqueadas.
   e. Longitud máxima de la consulta. Longitud máxima, en bytes, para la cadena de consulta enviada a los sitios web protegidos. Las solicitudes con cadenas de consulta más largas están bloqueadas.
   f. Longitud máxima total del encabezado. Longitud máxima, en bytes, para la longitud total del encabezado HTTP en las solicitudes enviadas a los sitios web protegidos. Se utilizará el valor mínimo de este y MaxHeaderLen en HttpProfile. Las solicitudes con mayor longitud están bloqueadas.
6. Haga clic en **Aceptar** y **Cerrar**.



Uso de la función de registro con la comprobación de seguridad de desbordamiento de búfer

Cuando la acción de registro está habilitada, las infracciones de comprobación de seguridad de desbordamiento de búfer se registran en el registro de auditoría como infracciones **APTFW_BUFFEROVERFLOW_URL**, **APTFW_BUFFEROVERFLOW_COOKIE** y **APTFW_BUFFEROVERFLOW_HDR**. El Web App Firewall admite los formatos de registro nativo y CEF. También puede enviar los registros a un servidor syslog remoto.

Si utiliza la interfaz gráfica de usuario para revisar los registros, puede utilizar la función de clic para implementar para aplicar las relajaciones indicadas por los registros.

Para acceder a los mensajes de registro mediante la línea de comandos

Cambie al shell y coloque los ns.logs en la carpeta **/var/log/** para acceder a los mensajes de registro correspondientes a las violaciones de desbordamiento del búfer:

```
1 > \*\*Shell\*\*
2 > \*\*tail -f /var/log/ns.log | grep APPFW_BUFFEROVERFLOW\*\*
3 <!--NeedCopy-->
```

Ejemplo de un mensaje de registro CEF que muestra la violación BufferOverflowMaxCookieLength en modo no bloque


```
1 Oct 22 17:35:20 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
    .0|APPFW|\*\*APPFW_BUFFEROVERFLOW_COOKIE\*\*|6|src=10.217.253.62
    geolocation=Unknown spt=41198 method=GET request=http://aaron.
    stratum8.net/FFC/sc11.html \*\*msg=Cookie header length(43) is
    greater than maximum allowed(16).\*\* cn1=119 cn2=465 cs1=
    owa_profile cs2=PPE1 cs3=wvOOOb+cJ2ZRbstZpyeNXIqLj7Y0001 cs4=ALERT
    cs5=2015 \*\*act=not blocked\*\*
2 <!--NeedCopy-->
```

Ejemplo de un mensaje de registro CEF que muestra una infracción de BufferOverflowMaxUrlLength en modo no bloque

```
1 Oct 22 18:39:56 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
    .0|APPFW|\*\*APPFW_BUFFEROVERFLOW_URL\*\*|6|src=10.217.253.62
    geolocation=Unknown spt=19171 method=GET request=http://aaron.
    stratum8.net/FFC/sc11.html \*\*msg=URL length(39) is greater than
    maximum allowed(20).\*\* cn1=707 cn2=402 cs1=owa_profile cs2=PPE0
    cs3=kW49GcKbnwKByByi3+jeNzfgWa80000 cs4=ALERT cs5=2015 \*\*act=not
    blocked\*\*
2 <!--NeedCopy-->
```

Ejemplo de un mensaje de registro de formato nativo que muestra una infracción de BufferOverflow-MaxHeaderLength en modo de bloque

```
1 Oct 22 18:44:00 <local0.info> 10.217.31.98 10/22/2015:18:44:00 GMT ns
    0-PPE-2 : default APPFW \*\*APPFW_BUFFEROVERFLOW_HDR\*\* 155 0 :
    10.217.253.62 374-PPE2 khhBEeY4DB8V2D3H2sMLkXmfWnA0002 owa_profile
    \*\*Header(User-Agent) length(82) is greater than maximum allowed
    (10)\*\* : http://aaron.stratum8.net/ \*\*<blocked>\*\*
2 <!--NeedCopy-->
```

Para acceder a los mensajes de registro mediante la interfaz gráfica de usuario

La GUI de Citrix incluye una herramienta útil (**Syslog Viewer**) para analizar los mensajes de registro. Tiene varias opciones para acceder al Visor de Syslog:

- Vaya a **Firewall de aplicaciones** > **Perfiles**, seleccione el perfil de destino y haga clic en **Comprobaciones de seguridad**. Resalte la fila **Desbordamiento de búfer** y haga clic en **Registros**. Cuando accede a los registros directamente desde la comprobación de seguridad de desbordamiento de búfer del perfil, la GUI filtra los mensajes de registro y muestra solo los registros correspondientes a estas infracciones de comprobación de seguridad.

- También puede acceder al Visor de Syslog navegando a **NetScaler** > **Sistema** > **Auditoría**. En la sección Mensajes de auditoría, haga clic en el enlace **Mensajes de syslog** para mostrar el Visor de Syslog, que muestra todos los mensajes de registro, incluidos otros registros de infracciones de comprobación de seguridad. Esto es útil para depurar cuando se pueden desencadenar varias infracciones de comprobación de seguridad durante el procesamiento de solicitudes.
- Vaya a **Firewall de aplicaciones** > **Directivas** > **Auditoría**. En la sección **Mensajes de auditoría**, haga clic en el enlace **Mensajes de syslog** para mostrar el Visor de Syslog, que muestra todos los mensajes de registro, incluidos otros registros de infracciones de comprobación de seguridad.

El Visor de Syslog basado en XML proporciona varias opciones de filtro para seleccionar solo los mensajes de registro que le interesan. Para seleccionar mensajes de registro para la comprobación **Desbordamiento de búfer**, filtre seleccionando **APPFW** en las opciones de la lista desplegable para **Módulo**. La lista **Tipo de evento** ofrece tres opciones, **APTFW_BUFFEROVERFLOW_URL**, **APTFW_BUFFEROVERFLOW_COOKIE** y A**PPFW_BUFFEROVERFLOW_HDR**, para ver todos los mensajes de registro relacionados con la comprobación de seguridad de desbordamiento de búfer. Puede seleccionar una o varias opciones para refinar aún más la selección. Por ejemplo, si activa la casilla de verificación **APPFW_BUFFEROVERFLO_COOKIE** y hace clic en el botón **Aplicar**, solo aparecerán en el Visor de Syslog los mensajes de registro correspondientes a las infracciones de comprobación de **seguridad de desbordamiento de búfer** para el encabezado Cookie. Si coloca el cursor en la fila de un mensaje de registro específico, debajo del mensaje de registro aparecen varias opciones, como **Módulo**, **Tipo**de **evento, Id.**de evento e **IP de cliente**. Puede seleccionar cualquiera de estas opciones para resaltar la información correspondiente en el mensaje de registro.

Hacer clic para implementar: La GUI proporciona funcionalidad de clic para implementar, que actualmente solo se admite para los mensajes de registro de desbordamiento de búfer relacionados con las infracciones de **longitud de URL**. Puede utilizar Syslog Viewer no solo para ver las infracciones desencadenadas, sino también para ejecutar decisiones informadas basadas en la longitud observada de los mensajes bloqueados. Si el valor actual es demasiado restrictivo y está activando falsos positivos, puede seleccionar un mensaje e implementarlo para reemplazar el valor actual por el valor de longitud de URL que aparece en el mensaje. Los mensajes de registro deben estar en formato de registro CEF para esta operación. Si se puede implementar la relajación para un mensaje de registro, aparece una casilla de verificación en el borde derecho del cuadro **Visor de Syslog** en la fila. Active la casilla de verificación y, a continuación, seleccione una opción de la lista **Acción** para implementar la relajación. **Modificar e implementar**, **Implementar** e **Implementar todo**están disponibles como opciones de **acción**. Puede utilizar el filtro **APTFW_BUFFEROVERFLOW_URL** para aislar todos los mensajes de registro relacionados con las infracciones de longitud de URL configuradas.

Si selecciona un mensaje de registro individual, estarán disponibles las tres opciones de acción **Modificar eimplementar, Implementare Implementar todo**. Si selecciona **Modificar e implementar**, se mostrará el diálogo de **configuración de desbordamiento de búfer**. La nueva longitud de URL que se observó en la solicitud se inserta en el campo de **entrada Longitud máxima de URL**. Si hace clic

en **Cerrar** sin modificaciones, los valores configurados actuales permanecen sin cambios. Si hace clic en el botón **Aceptar**, el nuevo valor de la longitud de URL máxima sustituye al valor anterior.

> **Nota**
>
> Las casillas de verificación de acción de **bloque**, **registro** y **estadísticas**no están marcadas en el diálogo de **configuración de desbordamiento de búfer**que se muestra y deben reconfigurarse si selecciona la opción **Modificar e implementar**. Asegúrese de habilitar estas casillas de verificación antes de hacer clic en **Aceptar**; de lo contrario, la nueva longitud de URL se configurará pero las acciones se establecerá en **ninguna**.

Si activa las casillas de verificación de varios mensajes de registro, puede utilizar la opción **Implementar** o **Implementar todo**. Si los mensajes de registro implementados tienen diferentes longitudes de URL, el valor configurado se sustituye por el valor de longitud de URL más alto observado en los mensajes seleccionados. Al implementar la regla solo se cambia el valor **BufferOverflowMaxUrlLength**. Las acciones configuradas se conservan y permanecen sin cambios.

Para utilizar la funcionalidad Click-to-Deploy en la GUI

1. En el Visor de syslog, seleccione **APPFW** en las opciones del **módulo**.
2. Active la casilla de verificación **APTFW_BUFFEROVERFLOW_URL** como **Tipo de evento** para filtrar los mensajes de registro correspondientes.
3. Active la casilla de verificación para seleccionar la regla.
4. Utilice la lista desplegable **Acción** de opciones para implementar la relajación.
5. Vaya a **Firewall de aplicaciones** > **Perfiles**, seleccione el perfil de destino y haga clic en **Comprobaciones de seguridad** para acceder al panel de configuración de **desbordamiento de búfer** para comprobar que se actualiza el valor **Longitud máxima de URL**.

Estadísticas de las infracciones de desbordamiento de búfer

Cuando la acción de estadísticas está habilitada, el contador de la comprobación de seguridad de desbordamiento de búfer se incrementa cuando el Web App Firewall realiza cualquier acción para esta comprobación de seguridad. Las estadísticas se recopilan para Rate and Total count para Tráfico, Violaciones y Registros. El tamaño de un incremento del contador de registro puede variar en función de la configuración configurada. Por ejemplo, si la acción de bloqueo está habilitada, una solicitud de una página que contiene tres infracciones de desbordamiento de búfer incrementa el contador de estadísticas en uno, porque la página se bloquea cuando se detecta la primera infracción. Sin embargo, si el bloque está inhabilitado, el procesamiento de la misma solicitud incrementa el contador de estadísticas para las infracciones porque cada infracción genera un mensaje de registro independiente.

Para mostrar las estadísticas de comprobación de seguridad de desbordamiento de búfer mediante la línea de comandos

En el símbolo del sistema, escriba:


```
> sh appfw stats
```

Para mostrar las estadísticas de un perfil específico, utilice el siguiente comando:

```
> stat appfw profile <profile name>
```

Para mostrar las estadísticas de desbordamiento de búfer mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **Seguridad** > **Firewall de aplicaciones**.
2. En el panel derecho, acceda al enlace de **estadísticas** .
3. Utilice la barra de desplazamiento para ver las estadísticas sobre las infracciones y los registros de desbordamiento de búfer. La tabla de estadísticas proporciona datos en tiempo real y se actualiza cada 7 segundos.

Resumen

- La comprobación de seguridad de desbordamiento de búfer le permite configurar límites para imponer la longitud máxima de las URL permitidas, las cookies y los encabezados.
- Las acciones de**bloqueo**, **registro** y **estadísticas**le permiten supervisar el tráfico y configurar la protección óptima para su aplicación.
- El visor de Syslog permite filtrar y ver todos los mensajes de registro relacionados con violaciones de desbordamiento de búfer.
- La funcionalidad**de clic para implementar** es compatible con las infracciones de **BufferOverflowMaxUrlLength**. Puede seleccionar e implementar una regla individual, o bien puede seleccionar varios mensajes de registro para ajustar y relajar el valor configurado actual de la longitud máxima permitida de la URL. El valor más alto de la dirección URL del grupo seleccionado se establece como el nuevo valor, para permitir todas estas solicitudes que están actualmente marcadas como infracciones.
- El Web App Firewall ahora evalúa las cookies individuales al inspeccionar la solicitud entrante. Si la longitud de cualquier cookie recibida en el encabezado Cookie excede el **BufferOverflowMaxCookieLength**configurado, se desencadena la infracción de desbordamiento de búfer.

> **Importante**
>
> En la versión 10.5.e (en algunas compilaciones provisionales de mejoras anteriores a la compilación 59.13xx.e) y en la versión 11.0 (en compilaciones anteriores a 65.x), se cambió el procesamiento de Web App Firewall del encabezado Cookie. En esas versiones, cada cookie se evalúa individualmente, y si la longitud de cualquier cookie recibida en el encabezado Cookie excede el BufferOverflowMaxCookieLength configurado, se desencadena la infracción de desbordamiento de búfer. Como resultado de este cambio, las solicitudes que se bloquearon en versiones 10.5 y versiones anteriores podrían ser permitidas, ya que la longitud de todo el encabezado de la cookie no se calcula para determinar la longitud de la cookie. ** En algunas situaciones, el

> tamaño total de la cookie reenviada al servidor podría ser mayor que el valor aceptado y el servidor podría responder con “400 solicitudes incorrectas”.
>
> Este cambio se ha revertido. El comportamiento de la versión 10.5.e ->59.13xx.e y posteriores versiones de mejora 10.5.e, además de la versión 11.0 65.x y versiones posteriores, ahora es similar al de las compilaciones no mejoradas de la versión 10.5. Ahora se tiene en cuenta todo el encabezado de Cookie sin procesar al calcular la longitud de la cookie. Los espacios circundantes y los caracteres de punto y coma (;) que separan los pares nombre-valor también se incluyen para determinar la longitud de la cookie.

Soporte de Web App Firewall para el kit de herramientas web de Google

January 12, 2021

Nota: Esta función está disponible en Citrix ADC versión 10.5.e.

Los servidores web que siguen los mecanismos de llamada a procedimiento remoto (RPC) de Google Web Toolkit (GWT) pueden ser protegidos por Citrix Web App Firewall sin necesidad de ninguna configuración específica para habilitar la compatibilidad con GWT.

¿Qué es GWT

GWT se utiliza para crear y optimizar aplicaciones web complejas de alto rendimiento por personas que no tienen experiencia en XMLHttpRequest y JavaScript. Este kit de herramientas de desarrollo gratuito de código abierto se utiliza ampliamente para desarrollar aplicaciones de pequeña y gran escala y se utiliza con bastante frecuencia para mostrar datos basados en el explorador, como resultados de búsqueda para vuelos, hoteles, etc. GWT proporciona un conjunto básico de API Java y widgets para escribir scripts JavaScript optimizados que se pueden ejecutar en la mayoría de los exploradores y dispositivos móviles. El marco GWT RPC facilita que los componentes cliente y servidor de la aplicación web intercambien objetos Java a través de HTTP. Los servicios GWT RPC no son los mismos que los servicios web basados en SOAP o REST. Son simplemente un método ligero para transferir datos entre el servidor y la aplicación GWT en el cliente. GWT maneja la serialización de los objetos Java intercambiando los argumentos en las llamadas al método y el valor devuelto.

Para los sitios web más populares que usan GWT, consulte

https://www.quora.com/What-web-applications-use-Google-Web-Toolkit-%28GWT%29

Cómo funciona una solicitud GWT

La solicitud GWT RPC está delimitada por procesos y tiene un número variable de argumentos. Se lleva como una carga útil de HTTP POST y tiene los siguientes valores:

1. Tipo de contenido = text/x-gwt-rpc. Charset puede ser cualquier valor.
2. Método = POST.

Tanto las solicitudes GET como POST HTTP se consideran solicitudes GWT válidas si el tipo de contenido es “text/x-gwt-rpc”. Las cadenas de consulta ahora son compatibles como parte de las solicitudes GWT. Configure el parámetro “InspectQueryContentTypes” del perfil de App Firewall en “Other” para examinar la porción de consulta de solicitud para el tipo de content-type “text/x-gwt-rpc”.

El siguiente ejemplo muestra una carga útil válida para una solicitud GWT:

```
5|0|8|http://localhost:8080/test/|16878339F02B83818D264AE430C20468| com
    .test.client.TestService|testMethod|java.lang.String|java.lang.
    Integer| myInput1|java.lang.Integer/3438268394|1|2|3|4|2|5|6|7|8|1|
<!--NeedCopy-->
```

La solicitud se puede dividir en tres partes:

a) `Header: 5|0|8|`

Los primeros 3 dígitos`5|0|8|` de la solicitud anterior representan “versión, subversión y tamaño de la tabla”, respectivamente. Estos deben ser enteros positivos.

b) Tabla de cadenas:

```
http://localhost:8080/test/|16878339F02B83818D264AE430C20468| com.test.
client.TestService|testMethod|java.lang.String|java.lang.Integer|myInput1|
java.lang.Integer/3438268394|
```

Los miembros de la tabla de cadenas delimitadas por procesos anteriores contienen las entradas proporcionadas por el usuario. Estas entradas se analizan para las comprobaciones de Web App Firewall y se identifican de la siguiente manera:

- 1.º:`http://localhost:8080/test/`

  Esta es la URL de solicitud.

- 2º:16878339`F02B83818D264AE430C20468`

  Identificador HEX único. Una solicitud se considera mal formada si esta cadena tiene caracteres no hexadecimales.

- 3er:`com.test.client.TestService`

  Nombre de la clase de servicio

- 4º:`testMethod`

  Nombre del método de servicio

- 5ª en adelante:`java.lang.String|java.lang.Integer|myInput1|java.lang.Integer/3438268394`

  Tipos de datos y datos. Los tipos de datos no primitivos se especifican como

  `<container>.<sub-cntnr>.name/<integer><identifier>`

c) `Payload: 1|2|3|4|2|5|6|7|8|1|`

La carga útil consiste en referencias a los elementos de la tabla de cadenas. Estos valores enteros no pueden ser mayores que el número de elementos de la tabla de cadenas.

Protección de Web App Firewall para aplicaciones GWT

El Web App Firewall entiende e interpreta las solicitudes de GWT RPC, inspecciona la carga útil para detectar infracciones de comprobación de seguridad y realiza acciones específicas.

Los encabezados de Web App Firewall y las comprobaciones de cookies para solicitudes GWT son similares a los de otros formatos de solicitud. Después de la decodificación URL apropiada y la conversión del juego de caracteres, se inspeccionan todos los parámetros de la tabla de cadenas. El cuerpo de la solicitud GWT no contiene nombres de campo, solo los valores de campo. Los valores de entrada se pueden validar con el formato especificado mediante la comprobación Formato de campo de Web App Firewall, que también se puede utilizar para controlar la longitud de la entrada. Los ataques de **Scripting entre sitios** y **SQL Injection** en las entradas pueden ser fácilmente detectados y frustrados por el Web App Firewall.

Reglas de aprendizaje y relajación: El aprendizaje y el implementación de reglas de relajación son compatibles con las solicitudes GWT. Las reglas de Web App Firewall están en forma de <actionURL> <fieldName> mapeo. El formato de solicitud GWT no tiene los nombres de campo y, por lo tanto, requiere un manejo especial. El Web App Firewall inserta nombres de campo ficticios en las reglas aprendidas que se pueden implementar como reglas de relajación. El indicador -IsRegex funciona como lo hace para reglas que no son GWT.

- URL de acción:

  Se pueden configurar varios servicios que responden a un RPC en el mismo servidor web. La solicitud HTTP tiene la dirección URL del servidor web, no del servicio real que maneja el RPC. Por lo tanto, la relajación no se aplica sobre la base de la URL de solicitud HTTP, porque eso relajaría todos los servicios de esa URL para el campo de destino. Para las solicitudes GWT, Web App Firewall utiliza la dirección URL del servicio real que se encuentra en la carga útil GWT, en el cuarto campo de la tabla de cadenas.

- Nombre del campo:

  Dado que el cuerpo de la solicitud GWT solo contiene valores de campo, Web App Firewall inserta nombres de campo ficticios como 1, 2, etc. al recomendar reglas aprendidas.

Ejemplo de una regla de GWT aprendida

```
POST /abcd/def/gh HTTP/1.1
Content-type: text/x-gwt-rpc
Host: 10.217.222.75
Content-length: 157

5|0|8|http://localhost:8080/acdtest/|16878339
   F02Baf83818D264AE430C20468|
com.test.client.TestService|testMethod|java.lang.String%3b|java.
   lang.Integer|onblur|

  The learn data will be as follows:
> sh learningdata pr1 crossSiteScripting
Profile: pr1    SecurityCheck: crossSiteScripting
1)  Url:    http://localhost:8080/acdtest/  >> From GWT Payload.
    Field:  10
    Hits:   1
 Done
<!--NeedCopy-->
```

Ejemplo de una regla de relajación GWT

```
bind appfw profile pr1 -crossSiteScripting 1 abcd -isregex NOTREGEX
```

Mensajes de registro: Web App Firewall genera mensajes de registro para las infracciones de comprobación de seguridad detectadas en las solicitudes GWT. Un mensaje de registro generado por una solicitud GWT mal formada contiene la cadena “GWT” para facilitar la identificación.

Ejemplo de un mensaje de registro para solicitud GWT mal formada:

```
Dec 5 21:48:02 <local0.notice> 10.217.31.247 12/05/2014:21:48:02 GMT ns
0-PPE-0 : APPFW Message 696 0 : ”GWT RPC request with malformed payload. <
blocked>”
```

Diferencia en el procesamiento de solicitudes GWT vs no GWT:

La misma carga útil puede desencadenar diferentes infracciones de comprobación de seguridad de Web App Firewall para diferentes tipos de contenido. Considere el siguiente ejemplo:

```
5|0|8|http://localhost:8080/acdtest/|16878339F02Baf83818D264AE430C20468|com
.test.client.TestService|testMethod|java.lang.String%3b|java.lang.Integer|
select|
```

Content-type: Application/x-www-form-urlencoded:

Una solicitud enviada con este tipo de contenido da como resultado una infracción SQL si el tipo de inyección SQL está configurado para utilizar cualquiera de las cuatro opciones disponibles: SQLSplCharANDKeyword, SQLSplCharORKeyword, SQLKeyword o SQLSplChar. El Web App Firewall considera que '&' es el separador de campos y '=' es el separador de nombre-valor al procesar la carga útil anterior. Dado que ninguno de estos caracteres aparece en ninguna parte del cuerpo de la publicación, todo el contenido se trata como un único nombre de campo. El nombre de campo de esta solicitud contiene tanto un carácter especial SQL (;) como una palabra clave SQL (select). Por lo tanto, las violaciones se detectan para las cuatro opciones de tipo de inyección SQL.

Tipo de contenido: Text/x-gwt-rpc:

Una solicitud enviada con este tipo de contenido desencadena una infracción SQL solo si el tipo de inyección SQL está establecido en una de las tres opciones siguientes: SQLSPLCharorKeyword, SQLKeyWord o SQLSplChar. No se desencadena ninguna infracción si el tipo de inyección SQL se establece en SqlsPlCharandKeyword, que es la opción predeterminada. Web App Firewall considera que la barra | vertical es el separador de campos para la carga útil anterior en la solicitud GWT. Por lo tanto, el cuerpo del poste se divide en varios valores de campo de formulario y se agregan nombres de campo de formulario (de acuerdo con la convención descrita anteriormente). Debido a esta división, el carácter especial SQL y la palabra clave SQL se convierten en partes de campos de formulario independientes.

Campo de formulario 8:`java.lang.String%3b -\> %3b is the (;)char`

Campo de formulario 10:`select`

Como resultado, cuando el tipo de inyección SQL se establece en **SQLSplChar**, el campo 8 indica la infracción SQL. Para **SQLKeyword**, el campo 10 indica la infracción. Cualquiera de estos dos campos puede indicar una infracción si el tipo Inject SQL está configurado con la opción **SqlsPlCharorKeyword**, que busca la presencia de una palabra clave o de un carácter especial. No se detecta ninguna infracción para la opción predeterminada **SQLSplCharandKeyword**, porque no hay ningún campo único que tenga un valor que contenga tanto **SQLSplChar** como **SQLKeyword** juntos.

Consejos:

- No se necesita ninguna configuración especial de Web App Firewall para habilitar la compatibilidad con GWT.
- El tipo de contenido debe ser text/x-gwt-rpc.
- El aprendizaje y la implementación de las reglas de relajación para todas las comprobaciones de seguridad pertinentes de Web App Firewall aplicadas a la carga útil GWT funciona igual que para los otros tipos de contenido admitidos.
- Solo las solicitudes POST se consideran válidas para GWT. Todos los demás métodos de solicitud están bloqueados si el tipo de contenido es text/x-gwt-rpc.
- Las solicitudes GWT están sujetas al límite de cuerpo POST configurado del perfil.
- La configuración sin sesión para las comprobaciones de seguridad no es aplicable y se ignorará.
- El formato de registro CEF es compatible con los mensajes de registro GWT.

Protección de cookies

August 20, 2021

Cookie es un pequeño paquete de datos enviado desde un servidor web a un explorador cliente. Las cookies transportan datos confidenciales como contraseñas, detalles de autenticación de usuario y credenciales a través de una conexión HTTP y se almacenan en un explorador web. Por lo tanto, es muy importante proteger las cookies de los atacantes que roban información.

Comprobación de la coherencia de las cookies: examina las cookies devueltas con las solicitudes de los usuarios para verificar que coinciden con las cookies que su servidor web configuró para ese usuario. Si se encuentra una cookie modificada, se elimina de la solicitud antes de que la solicitud se reenvíe al servidor web. Para obtener más información, consulte el tema Comprobación de la coherencia de cookies .

Protección contra el secuestro de cookies: El secuestro se refiere a una situación en la que un atacante obtiene un acceso no autorizado a las cookies. Para proteger las cookies del acceso autorizado, Citrix ADC Web App Firewall (WAF) desafía la conexión TLS del cliente junto con la validación de consistencia de cookies WAF. Para cada nueva solicitud de cliente, el dispositivo valida la conexión TLS y también verifica la coherencia de las cookies de aplicación y sesión en la solicitud. Para obtener más información, consulte el tema Protección contra secuestro de cookies .

Atributo de cookie de SameSite: El `SameSite` atributo de la respuesta HTTP Set-Cookie le permite declarar si su cookie debe estar restringida a un contexto propio o del mismo sitio. La configuración de cookies mitiga los ataques y proporciona una comunicación web segura. Para obtener más información, consulte el tema del atributo de cookie de SameSite .

Comprobación de consistencia de cookies

January 31, 2022

La comprobación de coherencia de cookies examina las cookies devueltas por los usuarios para verificar que coinciden con las cookies que su sitio web ha configurado para ese usuario. Si se encuentra una cookie modificada, se elimina de la solicitud antes de que la solicitud se reenvíe al servidor web. También puede configurar la comprobación de coherencia de cookies para transformar todas las cookies del servidor que procesa, cifrándolas, reenviándolas mediante proxy o agregando marcas a las cookies. Esta comprobación se aplica a las solicitudes y respuestas.

Un atacante normalmente modificaría una cookie para obtener acceso a información privada confidencial haciéndose pasar por un usuario previamente autenticado, o para provocar un desbordamiento del búfer. La comprobación de desbordamiento de búfer protege contra intentos de

provocar un desbordamiento de búfer mediante el uso de una cookie La comprobación de coherencia de cookies se centra en el primer escenario.

Si utiliza el asistente o la GUI, en el cuadro de diálogo
Modificar comprobación de coherencia de cookies, en la ficha
General, puede habilitar o inhabilitar las siguientes acciones:

- Bloquear
- Registro
- Aprender
- Estadísticas
- Transformar. Si se activa, la acción Transformar modifica todas las cookies según se especifica en la siguiente configuración:
  - **Cifrar las cookies del servidor.** Encripte las cookies establecidas por su servidor web, excepto las que figuran en la lista de relajación de la verificación de coherencia de cookies, antes de reenviar la respuesta al cliente. Las cookies cifradas se descifran cuando el cliente envía una solicitud posterior, y las cookies descifradas se vuelven a insertar en la solicitud antes de que se reenvíen al servidor web protegido. Especifique uno de los siguientes tipos de cifrado:
    * **Ninguno**. No cifrar ni descifrar las cookies. El valor por defecto.
    * **Solo descifrar.** Descifrar solo las cookies cifradas. No encripte las cookies.
    * **Solo sesión cifrada.** Cifrar solo las cookies de sesión. No cifre las cookies persistentes. Descifra las cookies cifradas.
    * **Cifrar todo.** Encripta tanto las cookies de sesión como las persistentes. Descifra las cookies cifradas.

      Nota: Al cifrar cookies, Web App Firewall agrega la marca
      HttpOnly a la cookie. Este indicador evita que los scripts accedan a la cookie y la analice. Por lo tanto, el indicador evita que un virus o troyano basado en scripts acceda a una cookie descifrada y utilice esa información para violar la seguridad. Esto se hace independientemente de la configuración de parámetros Indicadores para agregar en las cookies, que se gestionan independientemente de la configuración del parámetro Cifrar cookies del servidor.
- **Cookies de servidor proxy.** Proxy de todas las cookies no persistentes (de sesión) establecidas por su servidor web, excepto las que figuran en la lista de relajación de la verificación de consistencia de cookies. Las cookies se convierten en proxy mediante la cookie de sesión existente de Web App Firewall. Web App Firewall elimina las cookies de sesión establecidas por el servidor web protegido y las guarda localmente antes de reenviar la respuesta al cliente. Cuando el cliente envía una solicitud posterior, Web App Firewall vuelve a insertar las cookies de sesión en la solicitud antes de reenviarla al servidor web protegido. Especifique una de las siguientes configuraciones:
  - **Ninguno**. No utilice cookies proxy. El valor por defecto.

  - **Solo sesión.** Solo cookies de sesión proxy. No usar proxy de cookies persistentes
    Nota: Si inhabilita el proxy de cookie después de haberlo habilitado (establezca este valor en Ninguno después de que se haya establecido en Solo sesión), el proxy de cookie se mantiene para las sesiones que se establecieron antes de inhabilitarlo. Por lo tanto, puede inhabilitar esta función de forma segura mientras Web App Firewall procesa las sesiones de los usuarios.
- **Marcas para agregar en las cookies**. Agregue marcas a las cookies durante la transformación. Especifique una de las siguientes configuraciones:
  - **Ninguno**. No agregue marcas a las cookies. El valor por defecto.
  - **Solo HTTP.** Agregue la marca HttpOnly a todas las cookies. Los exploradores que admiten la marca HttpOnly no permiten que los scripts accedan a las cookies que tienen esta marca configurada.
  - **Segura**. Agregue la marca Secure a las cookies que se enviarán solo a través de una conexión SSL. Los exploradores que admiten el indicador Secure no envían las cookies marcadas a través de una conexión insegura.
  - **Todas.** Agregue la marca HttpOnly a todas las cookies y la marca Secure a las cookies que se enviarán solo a través de una conexión SSL.

Si utiliza la interfaz de línea de comandos, puede introducir los siguientes comandos para configurar la comprobación de coherencia de cookies:

- `set appfw profile <name> -cookieConsistencyAction [**block**] [**learn**] [**log**] [**stats**] [**none**]`
- `set appfw profile <name> -cookieTransforms ([**ON**] | [**OFF**])`
- `set appfw profile <name> -cookieEncryption ([**none**] | [**decryptOnly**] | [**encryptSession**] | [**encryptAll**])`
- `set appfw profile <name> -cookieProxying ([**none**] | [**sessionOnly**])`
- `set appfw profile <name> -addCookieFlags ([**none**] | [**httpOnly**] | [**secure**] | [**all**])`

Para especificar relajaciones para la comprobación de coherencia de cookies, debe utilizar la interfaz gráfica de usuario. En la ficha Comprobaciones del cuadro de diálogo Modificar comprobación de coherencia de cookies, haga clic en Agregar para abrir el cuadro de diálogo Agregar relajación de comprobación de coherencia de cookies, o seleccione una relajación existente y haga clic en Abrir para abrir el cuadro de diálogo Modificar relajación de comprobación de coherencia de cookies. Cualquiera de los dos cuadros de diálogo proporciona las mismas opciones para configurar una relajación.

A continuación se presentan ejemplos de relajaciones de verificación de consistencia de cookies:

- **Campos de inicio de sesión.** La siguiente expresión exime a todos los nombres de cookie que comiencen por la cadena logon_ seguida de una cadena de letras o números que tenga al menos dos caracteres y no más de quince caracteres:


```
^logon_[0-9A-Za-z]{
2,15 }
$
<!--NeedCopy-->
```

- **Campos de inicio de sesión (caracteres especiales).** La siguiente expresión exime a todos los nombres de cookie que comiencen por la cadena türkçe-logon_ seguida de una cadena de letras o números que tenga al menos dos caracteres y no más de quince caracteres:

```
^txC3xBCrkxC3xA7e-logon_[0-9A-Za-z]{
2,15 }
$
<!--NeedCopy-->
```

- **Cadenas arbitrarias.** Permitir cookies que contengan la cadena sc-item_, seguidas del ID de un artículo que el usuario ha agregado a su carrito de la compra ([0-9a-za-z]+), un segundo guión bajo (_) y, finalmente, el número de estos elementos que quiere ([1-9][0-9]?) , para que sea modificable por el usuario:

```
^sc-item_[0-9A-Za-z]+_[1-9][0-9]?$
<!--NeedCopy-->
```

Precaución: Las expresiones regulares son potentes. Especialmente si no está familiarizado con las expresiones regulares en formato PCRE, compruebe las expresiones regulares que escriba. Asegúrese de que definen exactamente la URL que quiere agregar como excepción y nada más. El uso descuidado de comodines, y especialmente de la combinación de metacaracteres/comodín punto-asterisco (.*), puede tener resultados que no quiere o espera, como bloquear el acceso a contenido web que no tenía intención de bloquear o permitir un ataque que la comprobación de consistencia de cookies tendría de otro modo bloqueado.

> **Importante**
>
> En la versión 10.5.e (en algunas compilaciones de mejoras provisionales anteriores a la compilación 59.13xx.e), así como en la versión 11.0 (en compilaciones anteriores a la 65.x), se modificó el procesamiento del encabezado de la cookie por Web App Firewall. En esas versiones, cada cookie se evalúa individualmente, y si la longitud de cualquier cookie recibida en el encabezado Cookie excede la configuración de BufferOverflowMaxCookieLength, se desencadena la infracción de desbordamiento de búfer. Como resultado de este cambio, es posible que se permitan

las solicitudes que se bloquearon en versiones 10.5 y anteriores, porque la longitud de todo el encabezado de la cookie no se calcula para determinar la longitud de la cookie. En algunas situaciones, el tamaño total de las cookie reenviadas al servidor puede ser mayor que el valor aceptado y el servidor puede responder con "400 solicitudes incorrectas".

Tenga en cuenta que este cambio se ha revertido. El comportamiento en las compilaciones 10.5.e ->59.13xx.e y posteriores de la mejora 10.5.e, así como en la versión 11.0 65.x y en las compilaciones posteriores, ahora es similar al de las compilaciones sin mejora de la versión 10.5. Ahora se tiene en cuenta todo el encabezado de Cookie sin procesar al calcular la longitud de la cookie. Los espacios circundantes y los caracteres de punto y coma (;) que separan los pares nombre-valor también se incluyen para determinar la longitud de la cookie.**

Nota

Consistencia de cookie sin sesión: El comportamiento de coherencia de cookies cambió en la versión 11.0. En versiones anteriores, la comprobación de coherencia de cookie invoca la sesión. Las cookies se almacenan en la sesión y se firman. Se agrega un sufijo "wlt_" a las cookies transitorias y se añade un sufijo "wlf_" a las cookies persistentes antes de que se reenvíen al cliente. Incluso si el cliente no devuelve estas cookies wlf/wlt firmadas, Web App Firewall utiliza las cookies almacenadas en la sesión para realizar la comprobación de la coherencia de las cookie.

En la versión 11.0, la comprobación de coherencia de cookie no tiene sesión. Web App Firewall ahora agrega una cookie que es un hash de todas las cookies rastreadas por Web App Firewall. Si esta cookie hash o cualquier otra cookie rastreada falta o se altera, Web App Firewall elimina las cookies antes de reenviar la solicitud al servidor back-end y desencadena una violación de la consistencia de las cookies. El servidor trata la solicitud como una nueva solicitud y envía nuevos encabezados Set-Cookie. La comprobación de coherencia de cookies en Citrix ADC versión 13.0, 12.1 y NetScaler 12.0 y 11.1 no tiene la opción sin sesión.

Protección contra el secuestro de cookies

August 20, 2021

La protección contra el secuestro de cookies mitiga los ataques de robo de cookies de los hackers. En el ataque de seguridad, un atacante se hace cargo de una sesión de usuario para obtener acceso no autorizado a una aplicación web. Cuando un usuario navega por un sitio web, por ejemplo, una aplicación bancaria, el sitio web establece una sesión con el explorador. Durante la sesión, la aplicación guarda los detalles del usuario, como credenciales de inicio de sesión, visitas de página en un archivo de cookies. El archivo cookie se envía a continuación al explorador del cliente en la respuesta. El explorador almacena las cookies para mantener sesiones activas. El atacante puede robar estas cookies manualmente desde el almacén de cookies del explorador o a través de alguna extensión no

autorizada del explorador. A continuación, el atacante utiliza estas cookies para obtener acceso a las sesiones de aplicación web del usuario.

Para mitigar los ataques de cookies, Citrix ADC Web App Firewall (WAF) desafía la conexión TLS del cliente junto con la validación de consistencia de cookies WAF. Para cada nueva solicitud de cliente, el dispositivo valida la conexión TLS y también verifica la coherencia de las cookies de aplicación y sesión en la solicitud. Si un atacante intenta mezclar y hacer coincidir las cookies de aplicación y las cookies de sesión robadas de la víctima, se produce un error en la validación de la coherencia de las cookies y se aplica la acción de secuestro de cookies configurada. Para obtener más información sobre la coherencia de cookie, consulte el tema Comprobación de coherencia de cookies .

> **Nota:**
>
> La función de secuestro de cookies admite el registro y las trampas SNMP. Para obtener más información acerca del registro, vea el tema ADM y para obtener más información acerca de la configuración SNMP, vea el tema SNMP.

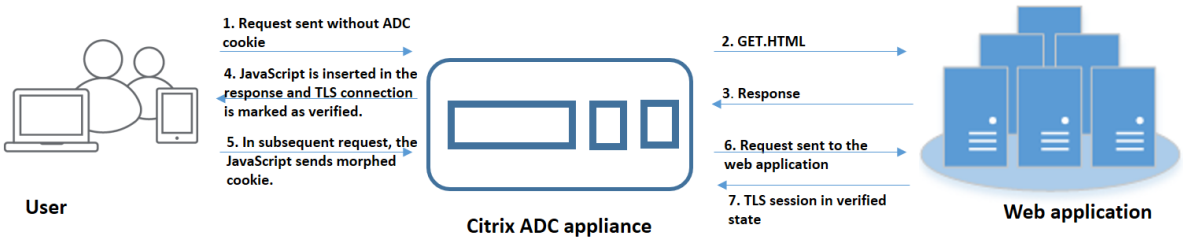
Limitaciones

- JavaScript debe estar habilitado en el explorador del cliente.
- La protección de secuestro de cookies no es compatible con TLS versión 1.3.
- Compatibilidad limitada para el explorador Internet Explorer (IE) porque el explorador no re-utiliza las conexiones SSL. Resulta que se envían varios redireccionamientos para una solicitud que eventualmente provocan un error “MAX REDIRECTS EXCEDEDEDED” en el explorador IE.

Cómo funciona la protección contra el secuestro de cookies

En los siguientes casos se explica cómo funciona la protección contra el secuestro de cookies en un dispositivo Citrix ADC.

Caso 1: Usuario accediendo a la primera página web sin cookie de sesión

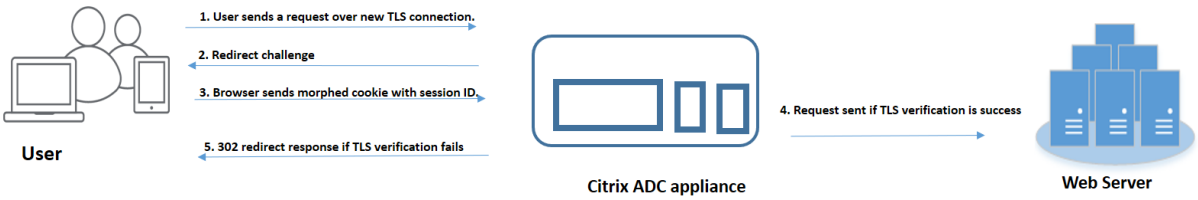


1. El usuario intenta autenticarse en una aplicación web y comienza a acceder a la primera página web sin ninguna cookie de sesión ADC en la solicitud.
2. Cuando se recibe la solicitud, el dispositivo crea una sesión de Application Firewall con un ID de cookie de sesión.
3. Esto inicia una conexión TLS para la sesión. Dado que el JavaScript no se envía ni se ejecuta en el explorador del cliente, el dispositivo marca la conexión TLS como validada y no se requiere ningún desafío.

   > **Nota:**
   >
   > Incluso si un atacante intenta enviar todos los ID de cookies de la aplicación desde una víctima sin enviar la cookie de sesión, el dispositivo detecta el problema y elimina todas las cookies de la aplicación en la solicitud antes de reenviar la solicitud al servidor back-end. El servidor back-end considera esta solicitud sin ninguna cookie de aplicación y toma necesaria según su configuración.

4. Cuando el servidor back-end envía una respuesta, el dispositivo recibe la respuesta y la reenvía con un token de sesión de JavaScript y una cookie inicial. A continuación, el dispositivo marca la conexión TLS como verificada.
5. Cuando el explorador cliente recibe la respuesta, el explorador ejecuta el JavaScript y genera un ID de cookie transformado mediante el token de sesión y la cookie de semilla.
6. Cuando un usuario envía una solicitud posterior a través de la conexión TLS, el dispositivo omite la validación de cookies transformada. Esto se debe a que la conexión TLS ya está validada.

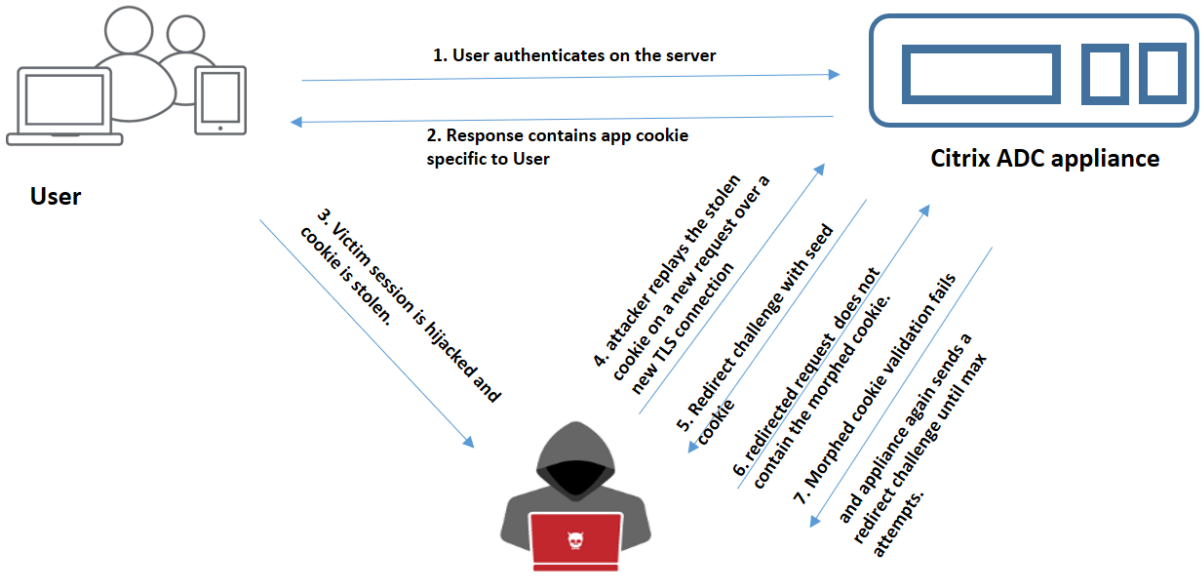
Caso 2: El usuario accede a páginas web sucesivas a través de una nueva conexión TLS con cookie de sesión



1. Cuando un usuario envía una solicitud HTTP para páginas sucesivas a través de una nueva conexión TLS, el explorador envía el ID de cookie de sesión y el ID de cookie transformado.
2. Dado que se trata de una nueva conexión TLS, el dispositivo detecta la conexión TLS y desafía al cliente con respuesta de redirección con cookie de inicio.
3. El cliente al recibir la respuesta del ADC, calcula la cookie transformada mediante el token de la sesión y la nueva cookie de semilla.

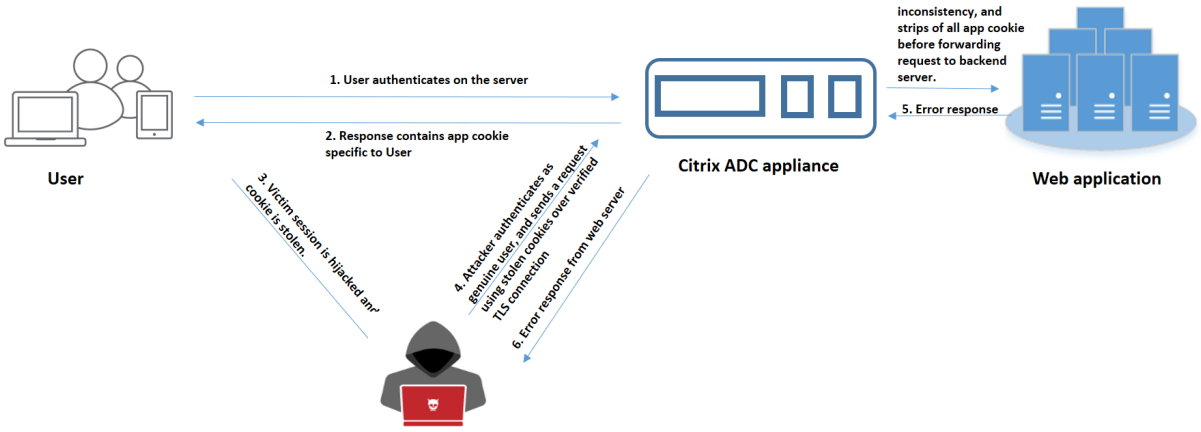
4. A continuación, el cliente envía esta cookie transformada recién calculada junto con un ID de sesión.
5. Si la cookie transformada calculada dentro del dispositivo ADC y la que se envía a través de la solicitud coincide, la conexión TLS se marca como verificada.
6. Si la cookie transformada calculada difiere de la presente en la solicitud del cliente, entonces la validación falla. Después de lo cual, el dispositivo envía el desafío al cliente, para enviar una cookie de transformación adecuada.

Caso 3: Atacante suplantación como usuario no autenticado



1. Cuando un usuario se autentica en la aplicación web, el atacante utiliza diferentes técnicas para robar las cookies y reproducirlas.
2. Dado que se trata de una nueva conexión TLS del atacante, el ADC envía un desafío de redirección junto con una nueva cookie semilla.
3. Dado que el atacante no tiene JavaScript en ejecución, la respuesta del atacante para la solicitud redirigida no contiene la cookie transformada.
4. Esto da como resultado un error de validación de cookies en el lado del dispositivo ADC. El dispositivo vuelve a enviar un desafío de redirección al cliente.
5. Si el número de intentos de validación de cookies transformadas supera el límite de umbral, el dispositivo marca el estado como secuestro de cookies.
6. Si el atacante intenta mezclar y hacer coincidir las cookies de aplicación y las cookies de sesión robadas a la víctima, la comprobación de coherencia de las cookies falla y el dispositivo aplica la acción de secuestro de cookies configurada.

Caso 4: Atacante suplantación como usuario autenticado



1. Los atacantes también pueden intentar autenticarse en una aplicación web como un usuario genuino y reproducir las cookies de la víctima para obtener acceso a la sesión web.
2. El dispositivo ADC también detecta a los atacantes suplantados. Aunque el atacante utiliza una conexión TLS verificada para reproducir la cookie de una víctima, el dispositivo ADC sigue verificando si la cookie de sesión y la cookie de aplicación en la solicitud son coherentes. El dispositivo verifica la coherencia de una cookie de aplicación mediante la cookie de sesión en la solicitud. Dado que la solicitud contiene una cookie de sesión de un atacante y una cookie de aplicación de la víctima, la validación de la coherencia de la cookie falla.
3. Como resultado, el dispositivo aplica la acción de secuestro de cookies configurada. Si la acción configurada se establece como “bloque”, el dispositivo elimina todas las cookies de la aplicación y envía la solicitud al servidor back-end.
4. El servidor back-end recibe una solicitud sin cookie de aplicación y, por lo tanto, responde una respuesta de error al atacante, como “Usuario no conectado”.

Configurar el secuestro de cookies mediante la CLI

Puede seleccionar un perfil de firewall de aplicación específico y establecer una o más acciones que eviten el secuestro de cookies.

En el símbolo del sistema, escriba:

```
set appfw profile <name> [-cookieHijackingAction <action-name> <block | log
 | stats | none>]
```

> **Nota:**
>
> De forma predeterminada, la acción se establece en “none”.

Ejemplo:

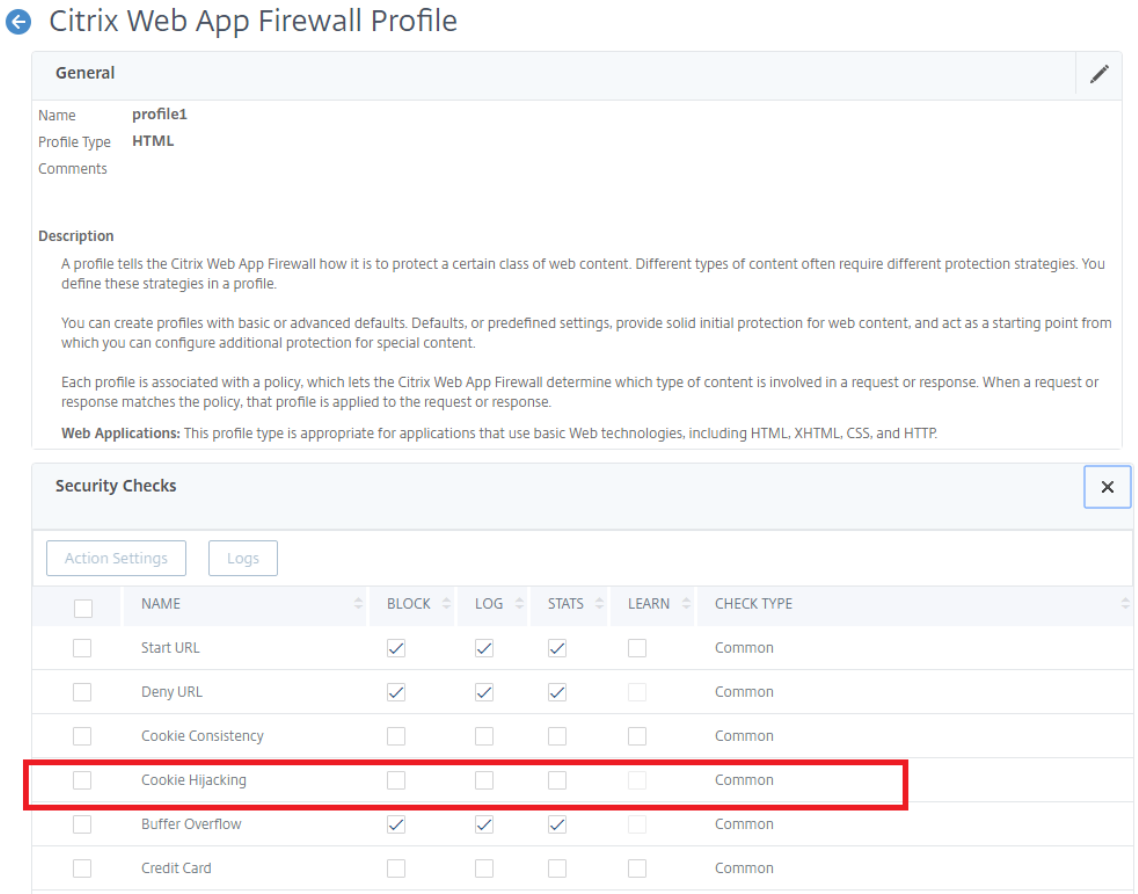
```
set appfw profile profile1 - cookieHijackingAction Block
```


Donde los tipos de acción son:

Bloquear: Bloquear conexiones que infrinjan esta comprobación de seguridad.
Registro: Registrar infracciones de esta comprobación de seguridad.
Estadísticas: Generar estadísticas para esta comprobación de seguridad.
Ninguno: Inhabilite todas las acciones de esta comprobación de seguridad.

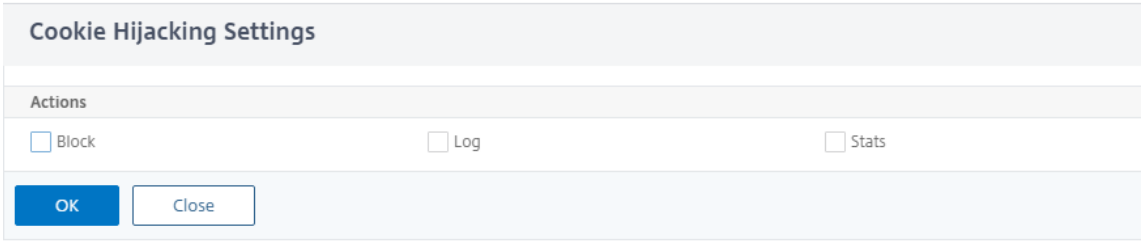
Configurar el secuestro de cookies mediante la GUI de Citrix ADC

1. Vaya a **Seguridad > Citrix Web App Firewall > Perfiles**.
2. En la página **Perfiles**, seleccione un perfil y haga clic en **Modificar**.
3. En la página **Perfil de Citrix Web App Firewall**, vaya a la sección **Configuración avanzada** y haga clic en **Comprobaciones de seguridad**.



4. En la sección **Comprobaciones de seguridad**, seleccione **Secuestro de cookies** y, a continuación, haga clic en Configuración de **acciones**.
5. En la página **Configuración de secuestro de cookies**, seleccione una o más acciones para evitar el secuestro de cookies.

6. Haga clic en **Aceptar**.



Agregar una regla de relajación para la validación de consistencia de cookies mediante la GUI de Citrix ADC

Para manejar falsos positivos en la validación de consistencia de cookies, puede agregar una regla de relajación para las cookies que pueden quedar exentas de la validación de cookies.

1. Vaya a **Seguridad > Citrix Web App Firewall > Perfiles**.
2. En la página **Perfiles**, seleccione un perfil y haga clic en **Modificar**.
3. En la página **Perfil de Citrix Web App Firewall**, vaya a la sección **Configuración avanzada** y haga clic en **Reglas de relajación**.
4. En la sección **Reglas de relajación**, seleccione **Consistencia de cookies** y haga clic en **Acción**.
5. En la página **Regla de relajación de coherencia de cookies**, establezca los siguientes parámetros.
   a) Habilitada. Seleccione si quiere activar la regla de relajación.
   b) Es el nombre de cookie Regex. Seleccione si el nombre de la cookie es una expresión regular.
   c) Nombre de la cookie. Introduzca el nombre de la cookie que puede quedar exenta de la validación de cookies.
   d) Editor de expresiones regulares. Haga clic en esta opción para proporcionar los detalles de la expresión regular.
   e) Comentarios. Una breve descripción de la cookie.
6. Haga clic en **Crear** y **cerrar**.

Ver estadísticas de tráfico de secuestro de cookies y violaciones mediante la CLI

Vea los detalles del tráfico de seguridad y las infracciones de seguridad en un formato tabular o gráfico.

Para ver estadísticas de seguridad:

En el símbolo del sistema, escriba:

```
stat appfw profile profile1
```


Appfw perfil Estadísticas de tráfico	Tasa (s)	Total
Solicitudes	0	0
Bytes de solicitud	0	0
Respuestas	0	0
Bytes de respuesta	0	0
Aborta	0	0
Redirecciona	0	0
Tiempo de respuesta a largo plazo (ms)	–	0
Tiempo de respuesta reciente Ave (ms)	–	0

Estadísticas de violaciones HTML/XML/JSON	Tasa (s)	Total
URL de inicio	0	0
Denegar URL	0	0
Encabezado de referencia	0	0
Desbordamiento de búfer	0	0
Consistencia de cookies	0	0
Secuestro de cookies	0	0
Etiqueta de formulario CSRF	0	0
Scripting HTML entre sitios	0	0
Inyección HTML SQL	0	0
Formato de campo	0	0
Consistencia de campo	0	0
Tarjeta de crédito	0	0
Objeto seguro	0	0
Violaciones de firma	0	0
Tipo de contenido	0	0
JSON Denegación de Servicio	0	0

Estadísticas de violaciones HTML/XML/JSON	Tasa (s)	Total
Inyección JSON SQL	0	0
Scripting JSON entre sitios	0	0
Tipos de carga de archivos	0	0
Inducir la carga útil XML del tipo de contenido	0	0
Inyección HTML CMD	0	0
Formato XML	0	0
Denegación de servicio XML (XDoS)	0	0
Validación de mensajes XML	0	0
Interoperabilidad de servicios web	0	0
Inyección XML SQL	0	0
Scripting XML entre sitios	0	0
Datos adjuntos XML	0	0
Violaciones de errores SOAP	0	0
Violaciones genéricas de XML	0	0
Total de violaciones	0	0

Estadísticas de registro HTML/XML/JSON	Tasa (s)	Total
Registros de URL de inicio	0	0
Denegar registros de URL	0	0
Registros de encabezado de referer	0	0
Registros de desbordamiento de	0	0
Registros de desbordamiento de	0	0

Estadísticas de registro HTML/XML/JSON	Tasa (s)	Total
Registros de coherencia de cookies	0	0
Registros de secuestro de cookies	0	0
Registros de etiquetas de formulario CSRF	0	0
Registros de scripts de sitios cruzados HTML	0	0
Registros de transformación de scripts multisitio HTML	0	0
Registros de inyección HTML SQL	0	0
Registros de transformación HTML SQL	0	0
Registros de formato de campo	0	0
Registros de coherencia de campo	0	0
Tarjetas de crédito	0	0
Registro de transformación de tarjetas de crédito	0	0
Registros de objetos seguros	0	0
Registros de firmas	0	0
Registros de tipo de contenido	0	0
Registros de denegación de servicio JSON	0	0
Registros de inyección JSON SQL	0	0
Registros de scripts entre sitios JSON	0	0
Tipos de carga de archivos registros	0	0

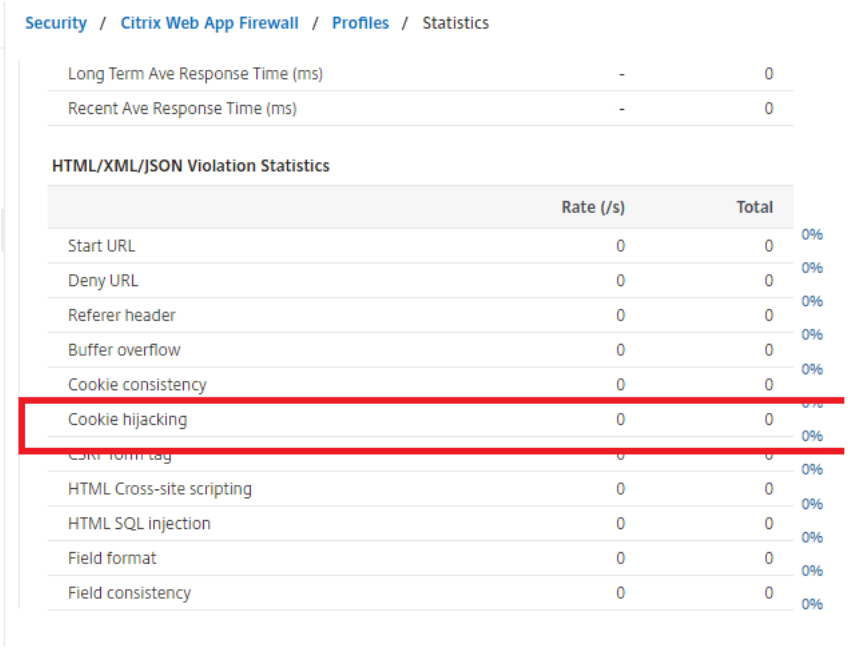
Estadísticas de registro HTML/XML/JSON	Tasa (s)	Total
Inducir tipo de contenido XML Carga útil L	0	0
Registros de inyección de comandos HTML	0	0
Registros de formato XML	0	0
Registros XML de denegación de servicio (XDoS)	0	0
Registros de validación de mensajes XML	0	0
Registros WSI	0	0
Registros de inyección XML SQL	0	0
Registros de scripts entre sitios XML	0	0
Registro de datos adjuntos XML	0	0
Registros de errores SOAP	0	0
Registros genéricos XML	0	0
Total de mensajes de registro	0	0

Estadísticas de respuesta a errores del servidor	Tasa (s)	Total
Errores de cliente HTTP (4xx Resp)	0	0
Errores del servidor HTTP (5xx)	0	0

Ver estadísticas de tráfico de secuestro de cookies y violaciones mediante la interfaz gráfica de usuario

1. Vaya a **Seguridad > Citrix Web App Firewall > Perfiles**.
2. En el panel de detalles, seleccione un perfil de **Web App Firewall** y haga clic en **Estadísticas**.

3. La página **Estadísticas de Citrix Web App Firewall** muestra los detalles del tráfico de secuestro de cookies y la infracción.
4. Puede seleccionar **Vista tabular** o cambiar a **Vista gráfica** para mostrar los datos en formato tabular o gráfico.



Atributo de cookie SameSite

August 20, 2021

Para una comunicación web segura, Google ha ordenado el uso del atributo `SameSite` cookie. Al cumplir con la nueva directiva `SameSite` de Google Chrome, el dispositivo Citrix ADC puede gestionar cookies de terceros con el atributo `SameSite` establecido en el encabezado `set-cookie`. La configuración de cookies mitiga los ataques y proporciona una comunicación web segura.

Hasta febrero de 2020, el `SameSite` atributo no se estableció explícitamente en la cookie. El explorador tomó el valor predeterminado “None”. Sin embargo, con cierta actualización del explorador, como Google Chrome 80, hay un cambio en el comportamiento predeterminado entre dominios en las cookies.

Establecer el valor del atributo de cookie

El atributo `SameSite` se establece en uno de los siguientes valores y para el explorador Google Chrome, el valor predeterminado se establece como “Lax”.

Ninguno. Indica el explorador que utilizará la cookie para solicitudes en el contexto de sitios cruzados solo en conexiones seguras.

Lax. Indica el explorador que utilizará la cookie para solicitudes en el contexto del mismo sitio. En el contexto entre sitios, solo los métodos HTTP seguros como la solicitud GET pueden usar la cookie.

Estricta. Utilice la cookie solo cuando el usuario solicita el dominio explícitamente.

> **Nota:**
>
> Si set-cookies (incluidas las cookies de sesión de firewall) tienen el atributo `SameSite` y si el indicador del atributo `addcookiesamesite` está habilitado en el perfil Firewall de aplicaciones web, el atributo `SameSite` se sobrescribe de acuerdo con el valor configurado en el perfil.

Configurar el atributo SameSite en el perfil de Web App Firewall mediante la CLI

Para configurar el `SameSite` atributo, debe realizar los siguientes pasos:

1. Habilite el atributo `SameSite` cookie.
2. Establezca el atributo cookie para las cookies de sesión appfw.

Habilitar el atributo de cookie 'Samesite'

En el símbolo del sistema, escriba:

```
set appfw profile <profile-name> -insertCookieSameSiteAttribute ( ON | OFF)
```

Ejemplo:

```
set appfw profile p1 -insertCookieSameSiteAttribute ON
```

Establecer el mismo valor de atributo de cookie del sitio para las cookies de sesión del Firewall de

En el símbolo del sistema, escriba:

```
set appfw profile <profile-name> - cookieSameSiteAttribute ( LAX | NONE |
STRICT )
```

Ejemplo:

```
set appfw profile p1 - cookieSameSiteAttribute LAX
```

Donde se encuentran los tipos de atributo,

Ninguno. El atributo de cookie SameSite se establece en "ninguno" y se marca como seguro para todas las cookies de aplicaciones y WAF.

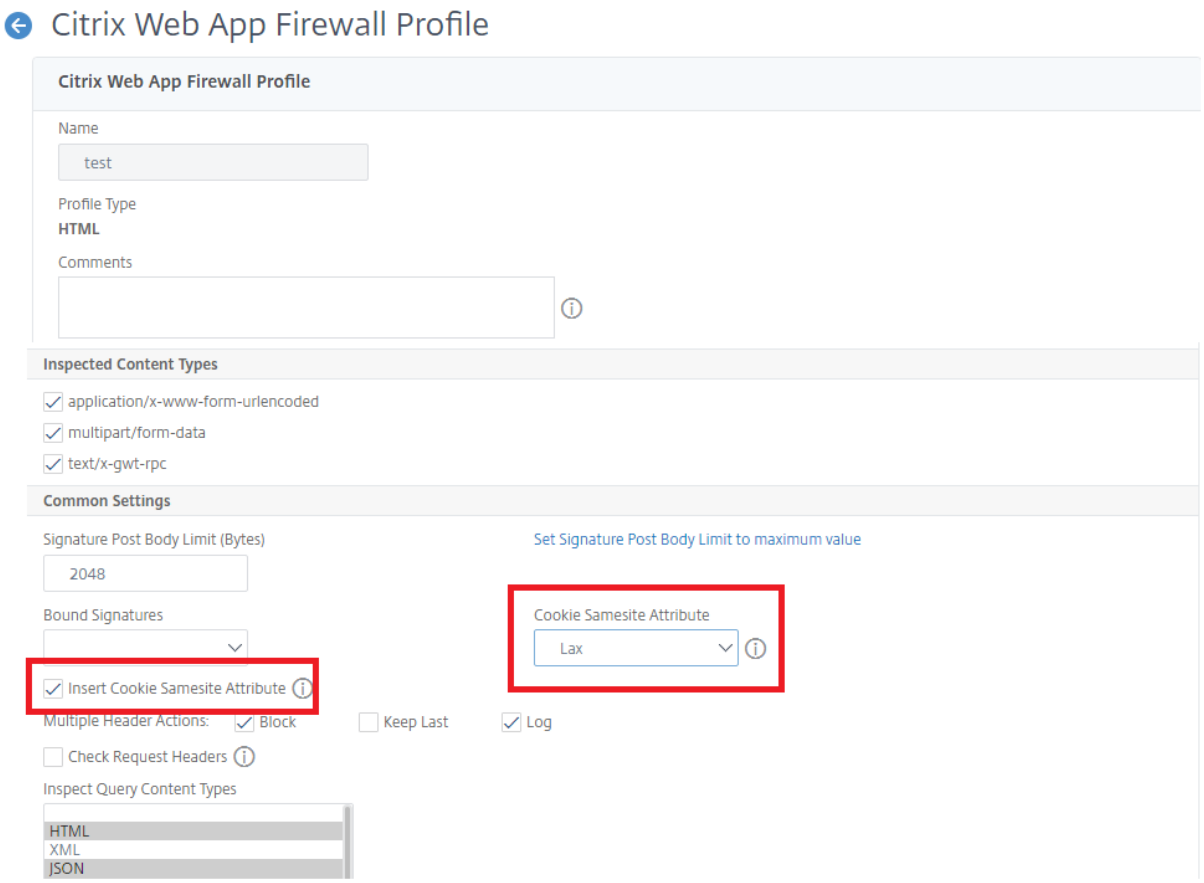
Lax. El atributo de cookie SameSite se establece en "Lax" para todas las cookies WAF y aplicaciones.

Estricta. El atributo de cookie SameSite se establece en “Lax” para todas las cookies WAF y aplicaciones.

Configurar el atributo cookie de SameSite en el perfil de Web App Firewall mediante la interfaz gráfica de usuario

1. Vaya a **Seguridad > Citrix Web App Firewall > Perfiles**.
2. En el panel de detalles, seleccione un perfil y haga clic en **Modificar**.
3. En la página **Perfil de Citrix Web App Firewall**, haga clic en **Configuración de perfil** en **Configuración avanzada**.
4. En la sección **Parámetros de perfil** defina los siguientes parámetros:

   a. Inserte el `Samesite` atributo cookie. Active la casilla de verificación para habilitar el `Samesite` atributo cookie.
   b. Atributo samesite de cookies. Seleccione una opción de la lista desplegable para establecer el valor de la `Samesite` cookie.
5. Haga clic en **Aceptar** y **Listo**.



Comprobaciones de prevención de fugas de datos

January 12, 2021

La prevención de fugas de datos comprueba las respuestas de filtro para evitar fugas de información confidencial, como números de tarjetas de crédito y números de seguridad social, a destinatarios no autorizados.

Cheque de tarjeta de crédito

August 20, 2021

Si tiene una aplicación que acepta tarjetas de crédito o sus sitios web tienen acceso a servidores de bases de datos que almacenan números de tarjetas de crédito, debe utilizar las medidas de prevención de fugas de datos (DLP) y configurar la protección para cada tipo de tarjeta de crédito que acepte.

La comprobación de la tarjeta de crédito de Citrix Web App Firewall evita que los atacantes exploten los defectos de Prevención de fugas de datos para obtener números de tarjeta de crédito de sus clientes. Siguiendo sencillos pasos de configuración, puede aplicar la protección de una o más de las siguientes tarjetas de crédito: 1) Visa, 2) Master Card, 3) Discover, 4) American Express (Amex), 5) JCB y 6) Diners Club.

La comprobación de seguridad de tarjeta de crédito examina las respuestas del servidor para identificar instancias de los números de tarjeta de crédito de destino y aplica una acción especificada cuando se encuentra dicho número. La acción puede ser transformar la respuesta al tachar todos menos el último grupo de dígitos del número de tarjeta de crédito, o bloquear la respuesta si contiene más de un número especificado de números de tarjeta de crédito. Si especifica ambos, la acción de bloqueo tiene prioridad. El valor Máximo de tarjetas de crédito permitidas por página determina cuándo se invoca la acción de bloqueo. La configuración predeterminada, 0 (no se permiten números de tarjeta de crédito en la página), es la más segura, pero puede permitir hasta 255. Dependiendo de dónde se detecte la infracción en la respuesta y se active la acción de bloqueo, es posible que obtenga menos del número máximo permitido de tarjetas de crédito en la respuesta.

Para evitar falsos positivos, puede aplicar relajantes para eximir números específicos de la comprobación de la tarjeta de crédito. Por ejemplo, un número de seguro social, un número de pedido de compra o un número de cuenta de Google pueden ser similares a un número de tarjeta de crédito. Puede especificar números individuales o utilizar una expresión regular para indicar la cadena de dígitos que se van a omitir al procesar la dirección URL de respuesta para la inspección de tarjetas de crédito.

Si no está seguro de qué números de tarjeta de crédito eximir, puede utilizar la función de aprendizaje

para generar recomendaciones basadas en los datos aprendidos. Para obtener un beneficio óptimo sin comprometer el rendimiento, es posible que quiera habilitar esta opción durante un corto período de tiempo para obtener una muestra representativa de las reglas y, a continuación, implementar las relajaciones e inhabilitar el aprendizaje.

Si habilita la función de registro, la comprobación de tarjeta de crédito genera mensajes de registro que indican las acciones que realiza. Puede supervisar los registros para determinar si las respuestas a las solicitudes legítimas se están bloqueando. Un gran aumento en el número de mensajes de registro puede indicar intentos frustrados de obtener acceso. De forma predeterminada, el parámetro doSecureCreditCardLogging es ON, por lo que el número de tarjeta de crédito no se incluye en el mensaje de registro generado por la infracción de comercio seguro (tarjeta de crédito).

La función de estadísticas recopila estadísticas sobre infracciones y registros. Un aumento inesperado en el contador de estadísticas podría indicar que su aplicación está siendo atacada.

Para configurar la comprobación de seguridad de la tarjeta de crédito para proteger su aplicación, configure el perfil que rige la inspección del tráfico hacia y desde esta aplicación.

> **Nota**:
>
> Un sitio web que no tiene acceso a una base de datos SQL generalmente no tiene acceso a información privada confidencial, como números de tarjetas de crédito.

Uso de la línea de comandos para configurar la comprobación de la tarjeta de crédito

En la interfaz de línea de comandos, puede utilizar el comando set appfw profile o el comando add appfw profile para activar la comprobación de tarjetas de crédito y especificar qué acciones realizar. Puede utilizar el comando unset appfw profile para volver a la configuración predeterminada. Para especificar relajantes, utilice el comando bind appfw para enlazar números de tarjetas de crédito al perfil.

Para configurar una comprobación de tarjeta de crédito mediante la línea de comandos

Utilice el comando set appfw profile o el comando add appfw profile, de la siguiente manera:

- `set appfw profile <name> -creditCardAction ( ([block][learn] [log][ stats])| [none])`
- `set appfw profile <name> -creditCard (VISA | MASTERCARD | DISCOVER | AMEX | JCB | DINERSCLUB)`
- `set appfw profile <name> -creditCardMaxAllowed <integer>`
- `set appfw profile <name> -creditCardXOut ([ON] | [OFF])<name> -doSecureCreditCard ([ON] | [OFF])`
- Para configurar una regla de relajación de tarjeta de crédito mediante la línea de comandos

Utilice el comando enlazar para enlazar el número de tarjeta de crédito al perfil. Para quitar un número de tarjeta de crédito de un perfil, utilice el comando unbind, con los mismos argumentos que utilizó para el comando bind. Puede utilizar el comando show para mostrar los números de tarjetas de crédito enlazados a un perfil.

- Para enlazar un número de tarjeta de crédito a un perfil

```
bind appfw profile <profile-name> -creditCardNumber <any number/regex>
 “<url>”
```

Ejemplo: bind appfw profile test_profile -creditCardNumber 378282246310005 http://www.example.com/credit_card_test.html

  - Para desvincular un número de tarjeta de crédito de un perfil

```
unbind appfw profile <profile-name> -creditCardNumber <credit card
number / regex> <url>
```

  - Para mostrar la lista de números de tarjetas de crédito enlazados a un perfil.

```
show appfw profile <profile>
```

Uso de la interfaz gráfica de usuario para configurar la comprobación de la tarjeta de crédito

En la GUI, configure la comprobación de seguridad de la tarjeta de crédito en el panel para el perfil asociado a la aplicación.

Para agregar o modificar la comprobación de seguridad de la tarjeta de crédito mediante la interfaz gráfica de usuario

1. Vaya a **Web App Firewall** > **Perfiles**, resalte el perfil de destino y haga clic en **Modificar**.
2. En el panel **Configuración avanzada**, haga clic en **Comprobaciones de seguridad**.

   La tabla de comprobación de seguridad muestra los valores de acción configurados actualmente para todas las comprobaciones de seguridad. Tiene 2 opciones para la configuración:

   a) Si solo quiere habilitar o inhabilitar las acciones Bloquear, Registrar, Estadísticas y Aprender para la tarjeta de crédito, puede activar o desactivar las casillas de verificación de la tabla, hacer clic en **Aceptar** y, a continuación, en **Guardar** y **Cerrar** para cerrar el panel **Comprobación de seguridad**.
   b) Si quiere configurar opciones adicionales para esta comprobación de seguridad, haga doble clic en Tarjeta de crédito o seleccione la fila y haga clic en **Configuración de acción** para mostrar las opciones adicionales de la siguiente manera:
      - Fuera: Enmascara cualquier número de tarjeta de crédito detectado en una respuesta reemplazando cada dígito, excepto los dígitos del grupo final, por la letra “X”.

- Máximo de tarjetas de crédito permitidas por página: Especifique el número de tarjetas de crédito que se pueden reenviar al cliente sin activar una acción de bloqueo.
- Tarjetas de crédito protegidas. Active o desactive una casilla de verificación para habilitar o inhabilitar la protección para cada tipo de tarjeta de crédito.
- También puede modificar las acciones Bloquear, Registrar, Estadísticas y Aprender en el panel Configuración de tarjeta de crédito.
  Después de realizar cualquiera de los cambios anteriores, haga clic en Aceptar para guardar los cambios y volver a la tabla Comprobaciones de seguridad. Puede proceder a configurar otras comprobaciones de seguridad si es necesario. Haga clic en Aceptar para guardar todos los cambios realizados en la sección Comprobaciones de seguridad y, a continuación, haga clic en Guardar y cerrar para cerrar el panel Comprobación de seguridad.

3. En el panel **Configuración avanzada**, haga clic en **Configuración del perfil**. Para habilitar o inhabilitar el registro seguro de números de tarjetas de crédito, active o desactive la casilla de verificación **Registro seguro de tarjetas de crédito**. (Por defecto, está seleccionado).

   Haga clic en **Aceptar** para guardar los cambios.

- Para configurar una regla de relajación de tarjeta de crédito mediante la interfaz gráfica de usuario

  1. Vaya a **Web App Firewall** > **Perfiles**, resalte el perfil de destino y haga clic en **Modificar**.
  2. En el panel **Configuración avanzada**, haga clic en **Reglas de relajación**. La tabla Reglas de relajación tiene una entrada de tarjeta de crédito. Puede hacer doble clic o seleccionar esta fila y hacer clic en **Modificar** para acceder al diálogo **Reglas de relajación de tarjetas de crédito**. Puede realizar operaciones Agregar, Modificar, Eliminar, Habilitaro Inhabilitar para reglas de relajación.

Uso de la función de aprendizaje con la comprobación de tarjeta de crédito

Cuando la acción de aprendizaje está habilitada, el motor de aprendizaje de Web App Firewall supervisa el tráfico y descubre las infracciones desencadenadas. Puede inspeccionar periódicamente estas reglas aprendidas. Después de tener debidamente en cuenta, si quiere eximir una cadena específica de dígitos de la comprobación de seguridad de la tarjeta de crédito, puede implementar la regla aprendida como regla de relajación.

- Para ver o utilizar datos aprendidos mediante la interfaz de línea de comandos

```
show appfw learningdata <profilename> creditCardNumber

rm appfw learningdata <profilename> -creditcardNumber <credit card
number> "<url>"

export appfw learningdata <profilename> creditCardNumber
```


- Para ver o utilizar datos aprendidos mediante la interfaz gráfica de usuario

    1. Vaya a **Web App Firewall** > **Perfiles**, resalte el perfil de destino y haga clic en **Modificar**.
    2. En el panel **Configuración avanzada**, haga clic en **Reglas aprendidas**. Puede seleccionar la entrada Tarjeta de crédito en la tabla Reglas aprendidas y hacer doble clic en ella para acceder a las reglas aprendidas. Puede implementar las reglas aprendidas o modificar una regla antes de implementarla como regla de relajación. Para descartar una regla, puede seleccionarla y hacer clic en el botón **Omitir**. Solo puede modificar una regla a la vez, pero puede seleccionar varias reglas para implementar u omitir.

    También tiene la opción de mostrar una vista resumida de las relajaciones aprendidas seleccionando la entrada de tarjeta de crédito en la tabla Reglas aprendidas y haciendo clic en Visualizador para obtener una vista consolidada de todas las infracciones aprendidas. El visualizador hace que sea muy fácil administrar las reglas aprendidas. Presenta una visión completa de los datos en una pantalla y facilita la acción en un grupo de reglas con un solo clic. La mayor ventaja del visualizador es que recomienda expresiones regulares para consolidar varias reglas. Puede seleccionar un subconjunto de estas reglas, basado en el delimitador y la URL de acción. Puede mostrar 25, 50 o 75 reglas en el visualizador seleccionando el número de una lista desplegable. El visualizador de reglas aprendidas ofrece la opción de modificar las reglas e implementarlas como relajaciones. O puede omitir las reglas para ignorarlas.

Uso de la función de registro con la comprobación de la tarjeta de crédito

Cuando la acción de registro está habilitada, las infracciones de comprobación de seguridad de tarjeta de crédito se registran en el registro de auditoría como infracciones APTFW_SAFECOMMERCE o APTFW_SAFECOMMERCE_XFORM. El Web App Firewall admite los formatos de registro nativo y CEF. También puede enviar los registros a un servidor syslog remoto.

La configuración predeterminada para doSecureCreditCardLogging es ON. Si lo cambia a OFF, el número y el tipo de tarjeta de crédito se incluyen en el mensaje de registro.

Dependiendo de la configuración configurada para las comprobaciones de tarjeta de crédito, los mensajes de registro generados por el firewall de la aplicación pueden incluir la siguiente información:

- La respuesta se bloqueó o no se bloqueó.
- Los números de tarjetas de crédito se transformaron (X'd out). Se genera un mensaje de registro independiente para cada número de tarjeta de crédito transformado, por lo que se pueden generar varios mensajes de registro durante el procesamiento de una sola respuesta.
- La respuesta contenía el número máximo de posibles números de tarjetas de crédito.
- Números de tarjetas de crédito y sus tipos correspondientes.
- Para acceder a los mensajes de registro mediante la línea de comandos

Cambie al shell y siga los ns.logs en la carpeta /var/log/ para acceder a los mensajes de registro relacionados con las infracciones de la tarjeta de crédito:

- Shell
- cola -f /var/log/ns.log | grep SAFECOMMERCE

- Para acceder a los mensajes de registro mediante la interfaz gráfica de usuario

  1. La GUI de Citrix incluye una herramienta muy útil (Syslog Viewer) para analizar los mensajes de registro. Tiene un par de opciones para acceder al Visor de Syslog: Desplácese hasta el **perfil de destino** > **Comprobaciones de seguridad**. Resalte la fila Tarjeta de crédito y haga clic en Registros. Cuando accede a los registros directamente desde la comprobación de seguridad de la tarjeta de crédito del perfil, filtra los mensajes de registro y muestra solo los registros relacionados con estas infracciones de comprobación de seguridad.

  2. También puede acceder al Visor de Syslog navegando a **NetScaler** > **Sistema** > **Auditoría**. En la sección Mensajes de auditoría, haga clic en el enlace **Mensajes de syslog** para mostrar el Visor de Syslog, que muestra todos los mensajes de registro, incluidos otros registros de infracciones de comprobación de seguridad. Esto es útil para depurar cuando se pueden desencadenar varias infracciones de comprobación de seguridad durante el procesamiento de solicitudes.

     El Visor de Syslog basado en HTML proporciona varias opciones de filtro para seleccionar solo los mensajes de registro que le interesan. Para acceder a los mensajes de registro de infracciones de comprobación de seguridad de la tarjeta de crédito, filtre seleccionando APTFW en las opciones desplegables del módulo. El tipo de evento muestra un amplio conjunto de opciones para refinar aún más la selección. Por ejemplo, si activa las casillas de verificación APTFW_SAFECOMMERCE y APTFW_SAFECOMMERCE_XFORM y hace clic en el botón Aplicar, solo aparecerán mensajes de registro relacionados con las infracciones de comprobación de seguridad de tarjeta de crédito en el Visor de Syslog.

     Si coloca el cursor en la fila de un mensaje de registro específico, aparecen varias opciones, como Module y EventType, debajo del mensaje de registro. Puede seleccionar cualquiera de estas opciones para resaltar la información correspondiente en los registros.

Ejemplo de un mensaje de registro de formato nativo cuando la respuesta no está bloqueada

```
1 May 29 01:26:31 <local0.info> 10.217.31.98 05/29/2015:01:26:31 GMT ns
     0-PPE-0 :
2 default APPFW APPFW_SAFECOMMERCE 2181 0 :  10.217.253.62 1098-PPE0
3 4erNfkaHy0IeGP+nv2S9Rsdu77I0000 pr_ffc http://aaron.stratum8.net/FFC/
     CreditCardMind.html
4 Maximum number of potential credit card numbers seen <not blocked>
```



```
<!--NeedCopy-->
```

Ejemplo de un mensaje de registro de formato CEF cuando se transforma la respuesta

```
May 28 23:42:48 <local0.info> 10.217.31.98
CEF:0|Citrix|NetScaler|NS11.0|APPFW|APPFW_SAFECOMMERCE_XFORM|6|src
   =10.217.253.62
spt=25314 method=GET request=http://aaron.stratum8.net/FFC/
   CreditCardMind.html
msg=Transformed (xout) potential credit card numbers seen in server
   response
cn1=66 cn2=1095 cs1=pr_ffc cs2=PPE2 cs3=xzE7M0g9bovAtG/zLCrLd2zkVl80002
cs4=ALERT cs5=2015 act=transformed
<!--NeedCopy-->
```

Ejemplo de un mensaje de registro de formato CEF cuando la respuesta está bloqueada. El número y el tipo de tarjeta de crédito se pueden ver en el registro, ya que el parámetro doSecureCreditCardLogging está inhabilitado.

```
May 28 23:42:48 <local0.info> 10.217.31.98
CEF:0|Citrix|NetScaler|NS11.0|APPFW|APPFW_SAFECOMMERCE|6|src
   =10.217.253.62
spt=25314 method=GET request=http://aaron.stratum8.net/FFC/
   CreditCardMind.html
msg=Credit Card number 4505050504030302 of type Visa is seen in
   response cn1=68
cn2=1095 cs1=pr_ffc cs2=PPE2 cs3=xzE7M0g9bovAtG/zLCrLd2zkVl80002 cs4=
   ALERT cs5=2015
act=blocked
<!--NeedCopy-->
```

Estadísticas de las violaciones de tarjetas de crédito

Cuando la acción de estadísticas está habilitada, el contador correspondiente para la comprobación de tarjeta de crédito se incrementa cuando el Web App Firewall realiza cualquier acción para esta comprobación de seguridad. Las estadísticas se recopilan para Rate and Total count para Tráfico, Violaciones y Registros. El incremento del contador de registro puede variar en función de la configuración configurada. Por ejemplo, si la acción de bloqueo está habilitada y la configuración de la tarjeta de crédito máxima permitida es 0, la solicitud de una página que contiene 20 números de tarjeta de crédito incrementa el contador de estadísticas en uno cuando se bloquea la página tan pronto

como se detecta el primer número de tarjeta de crédito. Sin embargo, si el bloque está inhabilitado y la transformación está habilitada, el procesamiento de la misma solicitud aumenta en 20 el contador de estadísticas para los registros, ya que cada transformación de tarjeta de crédito genera un mensaje de registro independiente.

- Para mostrar estadísticas de tarjetas de crédito mediante la línea de comandos

  En el símbolo del sistema, escriba:

  ```
  sh appfw stats
  ```

  Para mostrar las estadísticas de un perfil específico, utilice el siguiente comando:

  ```
  stat appfw profile <profile name>
  ```

  Para mostrar las estadísticas de tarjetas de crédito mediante GUI

  1. Vaya a **Sistema** > **Seguridad** > **Web App Firewall**.
  2. En el panel derecho, acceda al enlace de **estadísticas** .
  3. Utilice la barra de desplazamiento para ver las estadísticas sobre infracciones y registros de tarjetas de crédito. La tabla de estadísticas proporciona datos en tiempo real y se actualiza cada 7 segundos.

Resumen

Tenga en cuenta los siguientes puntos sobre la comprobación de seguridad de la tarjeta de crédito:

- El Web App Firewall le permite proteger la información de tarjetas de crédito y detectar cualquier intento de acceder a estos datos confidenciales.
- Para utilizar la comprobación de protección de tarjeta de crédito, debe especificar al menos un tipo de tarjeta de crédito y una acción. A continuación, la comprobación se aplica a los perfiles HTML, XML y Web 2.0.
- Puede canalizar la salida del comando sh appfw profile y grep para CreditCard para ver toda la configuración específica de la tarjeta de crédito. Por ejemplo, sh appfw profile my_profile | grep CreditCard muestra los ajustes configurados de varios parámetros, así como las reglas de relajación correspondientes a la comprobación de tarjeta de crédito para el perfil de Web App Firewall denominado my_profile.
- Puede excluir números específicos de la inspección de tarjetas de crédito sin omitir la inspección de comprobación de seguridad para el resto de los números de tarjetas de crédito.
- La relajación está disponible para todos los patrones de tarjetas de crédito protegidas por Web App Firewall. En la GUI, puede utilizar el visualizador para especificar operaciones Agregar, Modificar, Eliminar, Habilitar o Desactivar en reglas de relajación.
- El motor de aprendizaje de Web App Firewall puede supervisar el tráfico saliente para recomendar reglas basadas en infracciones observadas. La compatibilidad con visualizador también está disponible para administrar las reglas aprendidas de tarjetas de crédito en la GUI. Puede

modificar e implementar las reglas aprendidas, u omitirlas después de una inspección cuidadosa.

- La configuración para el número de tarjetas de crédito permitidas se aplica a cada respuesta. No pertenece al total acumulado de números de tarjetas de crédito observados durante toda la sesión del usuario.
- El número de dígitos de salida X depende de la longitud de los números de la tarjeta de crédito. Diez dígitos son X para tarjetas de crédito que tienen de 13 a 15 dígitos. Doce dígitos son X para tarjetas de crédito que tienen 16 dígitos. Si su aplicación no requiere el envío del número completo de tarjeta de crédito en la respuesta, Citrix recomienda que habilite esta acción para enmascarar los dígitos de los números de tarjeta de crédito.
- La operación X-out transforma todas las tarjetas de crédito y funciona independientemente de los ajustes configurados para el número máximo de tarjetas de crédito permitidas. Por ejemplo, si hay 4 tarjetas de crédito en la respuesta y el parámetro CreditCardMaxAllowed se establece en 10, las 4 tarjetas de crédito son de salida X, pero no están bloqueadas. Si los números de la tarjeta de crédito se distribuyen en el documento, es posible que se envíe al cliente una respuesta parcial con números de salida X'd-out antes de que se bloquee la respuesta.
- No inhabilite el parámetro doSecureCreditCardLogging antes de tener debidamente en cuenta. Cuando este parámetro está desactivado, se muestran los números de tarjeta de crédito y se puede acceder a ellos en los mensajes de registro. Estos números no están enmascarados en los registros, incluso si la acción X-out está habilitada. Si envía registros a un servidor syslog remoto y los registros están comprometidos, los números de tarjeta de crédito se pueden exponer.
- Cuando la página de respuesta está bloqueada debido a una infracción de la tarjeta de crédito, Web App Firewall no redirige a la página de error.

Comprobación segura de objetos

July 8, 2022

La comprobación de objetos seguros proporciona protección configurable por el usuario para la información empresarial confidencial, como números de clientes, números de pedido y números de teléfono o códigos postales específicos de cada país o región. Una expresión regular definida por el usuario o un complemento personalizado le indica a Web App Firewall el formato de esta información y define las reglas que se utilizarán para protegerla. Si una cadena en una solicitud de usuario coincide con una definición de objeto seguro, Web App Firewall bloquea la respuesta, enmascara la información protegida o elimina la información protegida de la respuesta antes de enviarla al usuario, según cómo haya configurado esa regla de objeto seguro en particular.

La comprobación de objetos seguros evita que los atacantes exploten una falla de seguridad en el software de su servidor web o en su sitio web para obtener información privada confidencial, como

números de tarjetas de crédito de la empresa o números de seguridad social. Si sus sitios web no tienen acceso a este tipo de información, no necesita configurar esta comprobación. Si tiene un carrito de compras u otra aplicación que pueda acceder a dicha información, o sus sitios web tienen acceso a servidores de bases de datos que contienen dicha información, debe configurar la protección para cada tipo de información privada confidencial que maneje y almacene.

> **Nota:**
>
> Un sitio web que no accede a una base de datos SQL normalmente no tiene acceso a información privada confidencial.

La comprobación de objetos seguros no se parece a la de cualquier otra comprobación. Cada expresión de objeto seguro que cree es el equivalente de una comprobación de seguridad independiente, similar a la comprobación de la tarjeta de crédito, para ese tipo de información.

Configurar la comprobación de objetos seguros mediante la GUI

> **Nota**
>
> Debe configurar la comprobación de objetos seguros solo mediante la GUI. No se admite la interfaz de línea de comandos.

Para agregar una comprobación de seguridad de objetos seguros mediante la GUI:

1. Vaya a **Seguridad > Citrix Web App Firewall > Perfiles**.
2. Seleccione el perfil correspondiente y haga clic en **Modificar**.
3. En el panel **Configuración avanzada**, haga clic en **Reglas de relajación**.
4. Seleccione **Objeto seguro** y haga clic en **Modificar**.
5. Haga clic en **Agregar** y configure lo siguiente:
   - **Nombre de objeto seguro.** Un nombre para su nuevo objeto seguro. El nombre puede empezar por una letra, un número o el símbolo de subrayado. El nombre puede constar de una a 255 letras, números y los símbolos de guion (-), punto (.) almohadilla (#), espacio ( ), arroba (@), igual (=), dos puntos (:) y guiones bajos (_).
   - **Acciones.** Activa o desactiva las acciones **Bloquear**, **Registrar** y **Estadísticas**, y las siguientes acciones:
     - **X-Out.** Enmascara cualquier información que coincida con la expresión del objeto seguro con la letra “X”.
     - **Remove:** Elimine cualquier información que coincida con la expresión del objeto seguro.
   - **Expresión regular.** Introduzca una expresión regular compatible con PCRE que defina el objeto seguro. Puede crear la expresión regular de una de las siguientes maneras:

- Escribiendo la expresión regular directamente en el cuadro de texto
- Mediante el menú **Fichas** de expresiones regulares para introducir elementos y símbolos de expresiones regulares directamente en el cuadro de texto
- Abriendo el Editor de expresiones regulares y utilizándolo para crear la expresión. La expresión regular debe constar únicamente de caracteres ASCII. No corte ni pegue caracteres que no formen parte del conjunto ASCII básico de 128 caracteres. Si quiere incluir caracteres que no sean ASCII, debe escribirlos manualmente en el formato de codificación de caracteres hexadecimales PCRE.

> **Nota:**
>
> No utilice anclajes iniciales (^) al principio de las expresiones de objetos seguros ni anclajes finales ($) al final de las expresiones de objetos seguros. Estas entidades PCRE no se admiten en las expresiones de objetos seguros y, si se utilizan, hacen que la expresión no coincida con lo que pretendía coincidir.

- **Longitud máxima de coincidencia.** Introduzca un entero positivo que represente la longitud máxima de la cadena con la que quiera que coincida. Por ejemplo, si quiere hacer coincidir los números de la seguridad social de EE. UU., introduzca el número 11 en este campo. Esto permite que tu expresión regular coincida con una cadena con nueve números y dos guiones. Si quiere que coincidan los números de licencia de conducir de California, introduzca el número ocho (8).

> **Precaución:**
>
> Si no establece la longitud máxima de coincidencia, Web App Firewall utiliza el valor predeterminado de uno (1) al filtrar las cadenas que coinciden con las expresiones de objetos seguros. Como resultado, la mayoría de las expresiones de objetos seguros no coinciden con sus cadenas objetivo.

Puede modificar un expreso existente seleccionando la expresión requerida, haciendo clic en **Abrir** y, a continuación, configurando la expresión en el cuadro de diálogo **Modificar objeto seguro**.

Los siguientes son ejemplos de expresiones regulares de comprobación de objetos seguros:

- Busque cadenas que parezcan números de seguro social (SSN) de EE. UU. El SSN consta de los siguientes caracteres en el orden mencionado:
  - Tres números (el primero de los cuales no debe ser cero)
  - Un guion
  - Dos números más
  - Un segundo guion
  - Una cadena de cuatro números más


```
[1-9][0-9]{
3,3 }
-[0-9]{
2,2 }
-[0-9]{
4,4 }

<!--NeedCopy-->
```

- Busque cadenas que parezcan ser identificaciones de licencia de conducir de California, que comiencen con una letra y vayan seguidas de una cadena de exactamente siete números:

```
[A-Za-z][0-9]{
7,7 }

<!--NeedCopy-->
```

- Busca cadenas que parezcan ser ID de clientes. Los ID de cliente constan de lo siguiente en el pedido mencionado:
  - Una cadena de cinco caracteres hexadecimales (todos los números y las letras de la A a la F)
  - Un guion
  - Un código de tres letras
  - Un segundo guion
  - Una cadena de 10 números

```
[0-9A-Fa-f]{
5,5 }
-[A-Za-z]{
3,3 }
-[0-9]{
10,10 }

<!--NeedCopy-->
```

> **Precaución:**
>
> Las expresiones regulares son potentes. Si no conoce tanto las expresiones regulares en formato PCRE, compruebe bien las expresiones regulares que escriba. Asegúrese de que la expresión regular defina exactamente el tipo de cadena que quiera agregar como definición de objeto se-

> gura. El uso descuidado de comodines, y especialmente de la combinación de metacaracteres/-comodín con punto y asterisco (.*), puede tener resultados que no quería o esperaba, como bloquear el acceso a contenido web que no tenía intención de bloquear.

Comprobaciones de protección de formularios avanzadas

December 2, 2021

Las comprobaciones avanzadas de protección de formularios examinan los datos de los formularios web para evitar que los atacantes comprometan su sistema modificando los formularios web en sus sitios web o enviando tipos y cantidades de datos inesperados a su sitio web en un formulario.

> **Nota:**
>
> Las comprobaciones de protección de SQL, scripts entre sitios, FFC y FieldFormat se aplican si **Excluir archivos de carga de las comprobaciones de seguridad** está desestablecida.

Una carga de archivo es también un elemento de formulario que tiene un campo de **nombre** de control que se envía como parte del envío del formulario.

Consulte esta página para obtener más información: Formularios

> **Nota**
>
> Las protecciones de formularios cerrarán los formularios anidados cuando se habiliten las comprobaciones basadas en formularios. Esto es para garantizar que se siga el estándar HTML.

Comprobación de formatos de campo

August 20, 2021

La comprobación Formatos de campo comprueba los datos que los usuarios envían a sus sitios web en formularios web. Examina tanto la longitud como el tipo de datos para asegurarse de que son apropiados para el campo de formulario en el que aparecen. Si el Web App Firewall detecta datos de formularios web inapropiados en una solicitud de usuario, bloquea la solicitud.

Al impedir que un atacante envíe datos inadecuados de formularios web a su sitio web, la comprobación Formatos de campo evita ciertos tipos de ataques contra el sitio web y los servidores de bases de datos. Por ejemplo, si un campo concreto espera que el usuario introduzca un número de teléfono, la comprobación Formatos de campo examina la entrada enviada por el usuario para asegurarse de que los datos coinciden con el formato de un número de teléfono. Si un campo concreto espera un nombre, la comprobación Formatos de campo garantiza que los datos de ese campo sean del tipo y

la longitud adecuados para un nombre. Hace lo mismo para cada campo de formulario que configura para proteger.

Esta comprobación solo se aplica a las solicitudes HTML. No se aplica a las solicitudes XML. Puede configurar comprobaciones de formato de campo en perfiles HTML o perfiles Web 2.0 para inspeccionar la carga útil HTML para proteger las aplicaciones. El Web App Firewall también admite la protección de comprobación de formato de campo para aplicaciones de Google Web Toolkit (GWT).

La comprobación Formatos de campo requiere que habilite una o varias acciones. El Web App Firewall examina las entradas enviadas y aplica las acciones especificadas.

> **Nota**
>
> Las reglas de formato de campo están ajustando las reglas. Agregarlos a la lista de relajación de los datos aprendidos actúa como una regla de bloqueo.
>
> Para relajar las reglas de formato de campo, quite "nombre de campo" particular de la lista de relajaciones de formato de campo.

Tiene la opción de establecer los formatos de campo predeterminados para especificar Tipo de campo y la longitud mínima y máxima de los datos esperados en cada campo de formulario de cada formulario web que quiera proteger. Puede implementar reglas de relajación para configurar un Formato de campo para un campo individual de un formulario específico. Se pueden agregar varias reglas para especificar el nombre del campo, la dirección URL de la acción y los formatos de campo. Especifique Formatos de campo para aceptar diferentes tipos de entradas en diferentes campos de formulario. La función de aprendizaje puede proporcionar recomendaciones para las reglas de relajación.

Acciones de formato de campo: Puede habilitar acciones Bloquear, Registrar, Estadísticas y Aprender. Al menos una de estas acciones debe estar habilitada para activar la protección Comprobación de formato de campo.

- **Bloquear**. Si habilita el bloqueo, la acción de bloqueo se activa si la entrada no se ajusta al formato de campo especificado. Si se ha configurado una regla para el campo de destino, la entrada se comprueba con la regla especificada. De lo contrario, se comprueba con la especificación de formato de campo predeterminada. Cualquier discrepancia en el tipo de campo o la especificación de longitud mínima/máxima provoca el bloqueo de la solicitud.
- **Registro**. Si habilita la función de registro, la comprobación Formato de campo genera mensajes de registro que indican las acciones que realiza. Puede supervisar los registros para determinar si las respuestas a las solicitudes legítimas se están bloqueando. Un gran aumento en el número de mensajes de registro puede indicar intentos maliciosos de lanzar un ataque.
- **Estadísticas**. Si está activada, la función de estadísticas recopila estadísticas sobre infracciones y registros. Un aumento inesperado en el contador de estadísticas podría indicar que su aplicación está siendo atacada, o es posible que tenga que volver a visitar la configuración para ver si el formato de campo especificado es demasiado restrictivo.

- **Aprender**. Si no sabe qué tipos de campo o valores de longitud mínima y máxima pueden ser ideales para su aplicación, puede utilizar la función de aprendizaje para generar recomendaciones basadas en los datos aprendidos. El motor de aprendizaje de Web App Firewall supervisa el tráfico y proporciona recomendaciones de formato de campo basadas en los valores observados. Para obtener un beneficio óptimo sin comprometer el rendimiento, es posible que quiera habilitar la opción de aprendizaje durante un corto tiempo para obtener una muestra representativa de las reglas y, a continuación, implementar las reglas e inhabilitar el aprendizaje.
  Nota: El motor de aprendizaje de Web App Firewall puede distinguir solo los primeros 128 bytes del nombre. Si un formulario tiene varios campos con nombres que coinciden con los primeros 128 bytes, es posible que el motor de aprendizaje no pueda distinguir entre ellos. Del mismo modo, la regla de relajación implementada podría relajar inadvertidamente todos esos campos.

Formato de campo predeterminado: Además de configurar las acciones, puede configurar el formato de campo predeterminado para especificar el tipo de datos que se espera en todos los campos de formulario para la aplicación. Se puede seleccionar un tipo de campo como tipo de formato de campo. Los parámetros Longitud mínima y Longitud máxima se pueden utilizar para especificar la longitud de las entradas permitidas. Como alternativa a Tipos de campo, puede utilizar los mapas de caracteres para especificar lo que está permitido en un campo (excepto en implementaciones de clúster).

- **Tipo de campo**: Los tipos de campo se denominan expresión a la que se asignan valores de prioridad asignados. Las expresiones de tipo de campo especifican las entradas permitidas y se comparan con los datos enviados para determinar si los valores recibidos son coherentes con los valores permitidos. Los tipos de campo se comprueban en el orden de sus números de prioridad. Un número más bajo indica una prioridad más alta. El Web App Firewall le da la opción de agregar sus propios tipos de campo y asignarles las prioridades que quiera. El valor de prioridad puede oscilar entre 0 y 64000. Se proporcionan los siguientes tipos de campo integrados para ayudar a simplificar el proceso de configuración:

```
1  > sh appfw fieldtype
2  1)      Name:  integer           Regex:  "^[+-]?[0-9]+$"
3                  Priority:  30            Comment:  Integer
4                  Builtin:  IMMUTABLE
5  2)      Name:  alpha             Regex:  "^[a-zA-Z]+$"
6                  Priority:  40            Comment:  "Alpha
                      characters"
7               Builtin:  IMMUTABLE
8  3)      Name:  alphanum          Regex:  "^[a-zA-Z0-9]+$"
9                  Priority:  50            Comment:  "Alpha-numeric
                       characters"
```



```
                Builtin:  IMMUTABLE
4)      Name:  nohtml            Regex:  "^[^&<>]\*$"
                Priority:  60            Comment:  "Not HTML"
                Builtin:  IMMUTABLE
5)      Name:  any               Regex:  "^.\*$"
             Priority:  70            Comment:  Anything
                Builtin:  IMMUTABLE
    Done
>
<!--NeedCopy-->
```

> **Nota:** Los tipos de campo integrados son INMUTABLES. No se pueden modificar ni eliminar. Cualquier tipo de campo que agregue es MODIFICABLE. Puede modificarlos o eliminarlos.

Configurar un tipo de campo como formato de campo predeterminado puede ser útil cuando tenga una expresión PCRE que pueda identificar las entradas válidas en todos o en la mayoría de los campos de formulario de la aplicación y excluir las entradas no válidas. Por ejemplo, si se espera que todas las entradas de los formularios de aplicación contengan solo números y letras, es posible que quiera utilizar el alfanum de tipo de campo integrado como el tipo de campo predeterminado. Cualquier carácter no alfanumérico, como una barra invertida () o punto y coma; en la entrada desencadenará una infracción. También puede agregar sus propios tipos de campo personalizados y usarlos para configurar los formatos de campo predeterminados. Por ejemplo, si desea convertir las minúsculas "x", "y" y "z" en los únicos caracteres alfa permitidos, puede configurar un tipo de campo personalizado con la expresión regular "^[x-z]+$". Puede asignarle una prioridad más alta (número de prioridad menor) que los tipos de campo integrados y utilizarlo como tipo de campo predeterminado.

- **Longitud mínima: Longitud** mínima de datos predeterminada asignada a los campos de formulario en formularios web que no tienen una configuración explícita. Este parámetro se establece en 0 de forma predeterminada, lo que permite al usuario dejar el campo en blanco. Cualquier configuración superior obliga a los usuarios a rellenar el campo.

  Precaución: Si el valor de longitud mínima es 0 pero el Tipo de campo es entero, alfa o alfanum, se bloquea una solicitud si algún campo de entrada se deja vacío, a pesar de la configuración de longitud mínima. Esto se debe a que la expresión regular para estos tipos de campo contiene un carácter +, lo que significa uno o más caracteres. Distinguir un entero de un carácter alfa requiere al menos un carácter.

- **Longitud máxima: Longitud máxima** de datos predeterminada asignada a campos de formulario en formularios web que no tienen una configuración explícita. Este parámetro se establece en 65535 de forma predeterminada.

> **Nota:** Caracteres vs bytes. Las longitudes mínima y máxima de los formatos de campo representan el número de bytes, no el número de caracteres. Los idiomas que tienen una representación de caracteres superior a un byte pueden hacer que el límite se supere con menos caracteres que el número configurado para el valor máximo. Por ejemplo, con la representación de caracteres de doble byte, el valor máximo de 9 permite no más de 4 caracteres.
> **Consejo:** La GUI le permite cortar y pegar caracteres UTF-8 directamente en la GUI sin tener que convertirlos en hexadecimal.

- **Mapas de caracteres**: Además de recomendar los tipos de campo, el motor de aprendizaje de Web App Firewall ofrece una opción adicional, Usar mapas de caracteres, para implementar las reglas de comprobación de formato. Un mapa de caracteres es un conjunto de todos los caracteres permitidos en un campo de formulario determinado. Puede ajustar la especificación de formato de campo para permitir o no permitir caracteres específicos mediante mapas de caracteres. Se genera un mapa de caracteres independiente para cada campo de formulario. Los caracteres alfa y numérico se tratan de manera diferente en los mapas de caracteres. Si se ve algún carácter alfa en la entrada, todos los caracteres alfa [A-za-z] estarán permitidos por la expresión PCRE recomendada en el mapa de caracteres. Del mismo modo, si se incluye algún dígito, se permitirán todos los dígitos del [0 al 9] . Los caracteres no imprimibles se especifican mediante el componente fijo x. Para las recomendaciones de mapa de caracteres, solo se tienen en cuenta caracteres individuales con valores entre 0 y 255.

  Un mapa de caracteres puede ser más específico que la recomendación correspondiente de tipo de campo. En algunas situaciones, los mapas de caracteres pueden ser una mejor opción, ya que proporcionan un control más estricto sobre el conjunto de caracteres permitidos como entradas. Los mapas de caracteres implementados se muestran como cadenas que comienzan con el prefijo “CM” seguido de dígitos. La prioridad de los mapas de caracteres comienza en 10000. Al igual que con los tipos de campo agregados por el usuario, puede agregar, modificar o eliminar un mapa de caracteres. Los mapas de caracteres que se utilizan actualmente en las reglas implementadas no se pueden modificar ni quitar.

  Nota: Los mapas de caracteres no se admiten en las implementaciones de clúster.

> **Nota**
>
> Cuando agrega una regla de formatos de campo con cualquier tipo de campo incorporado y usa un mapa de caracteres en lugar de Tipo de campo y lo guarda, los cambios no se guardan y la regla sigue mostrándose con Tipo de campo.
>
> Cuando el mapa de caracteres coincide con uno de los tipos integrados, el tipo de campo se reutiliza en lugar de crear un nuevo mapa de caracteres.

Usar la línea de comandos para configurar la comprobación de formato de campo

En la interfaz de línea de comandos, puede usar el comando add appfw fieldtype para agregar un nuevo tipo de campo. Puede utilizar el comando set appfw profile o el comando add appfw profile para configurar la comprobación Formato de campo y especificar las acciones que quiere realizar. Puede utilizar el comando unset appfw profile para revertir la configuración configurada a sus valores predeterminados. Para especificar una regla Formato de campo, utilice el comando bind appfw para enlazar un tipo de campo a un campo de formulario y a la dirección URL de acción, junto con las especificaciones de longitud mínima y máxima.

Para agregar, quitar o ver un tipo de campo mediante la línea de comandos:

Utilice el comando add para agregar un tipo de campo. Debe especificar el nombre, la expresión regular y la prioridad al agregar un nuevo tipo de campo. También tiene la opción de agregar un Comentario. Puede utilizar el comando show para mostrar los tipos de campo configurados. También puede eliminar un tipo de campo mediante el comando remove, que solo requiere el nombre del tipo de campo.

```
add [appfw] fieldType <name> <regex> <priority> [-comment <string>]
```

donde:

<regex> es una expresión regular

<priority> es un positive_integer

Ejemplo:

```
add fieldtype ”Cust_Zipcode” ”^[0-9]{
 5 }
 [-][0-9]{
 4 }
 $” 4

-  show [appfw] fieldType [<name>]

    Example: sh fieldtype

    sh appfw fieldtype

    sh appfw fieldtype cust_zipcode

-  `rm [appfw] fieldType <name>`

    Example: rm fieldtype cusT_ziPcode

```



```
    `rm appfw fieldtype cusT_ziPcode`
<!--NeedCopy-->
```

> **Nota:** Como se muestra arriba, el uso de “appfw” en el comando es opcional. Por ejemplo, “Add fieldType” o “Add appfw fieldType” son opciones válidas. Los nombres de los tipos de campo no distinguen entre mayúsculas y minúsculas debido a la normalización. Como se muestra en los ejemplos anteriores, Cust_Zipcode, cust_zipcode y Cust_zipCode hacen referencia al mismo tipo de campo.

Para configurar una comprobación de formato de campo mediante la línea de comandos

Utilice el comando set appfw profile o el comando add appfw profile, de la siguiente manera:

- `set appfw profile <name> -fieldFormatAction (([block] [learn] [log] [ stats])| [none])`
- `set appfw profile <name>-defaultFieldFormatType <string>`
- `set appfw profile <name> -defaultFieldFormatMinLength <integer>`
- `set appfw profile <name> -defaultFieldFormatMaxLength <integer>`

Para configurar una regla de relajación Formato de campo mediante la línea de comandos

```
bind appfw profile <name> (-fieldFormat <string> <formActionURL>  <
    fieldType>
[-fieldFormatMinLength <positive_integer>]  [-fieldFormatMaxLength <
    positive_integer>]
[-isRegex ( REGEX | NOTREGEX )])
<!--NeedCopy-->
```

Ejemplo:

```
bind appfw profile pr_ffc -fieldFormat ”login_name” ”.*/login.php”
    integer -fieldformatMinLength 3 -FieldformatMaxlength 6
<!--NeedCopy-->
```

Uso de la GUI para configurar la comprobación de seguridad de los formatos de campo

En la GUI, puede administrar los tipos de campo. También puede configurar la comprobación de seguridad Formatos de campo en el panel del perfil asociado a la aplicación.

Para agregar, modificar o eliminar un tipo de campo mediante la interfaz gráfica de usuario

1. Desplácese hasta el nodo Firewall de aplicaciones. En Configuración, haga clic en **Administrar tipos de campo** para mostrar el cuadro de diálogo Configurar tipo de campo de firewall de aplicación.
2. Haga clic en **Agregar** para agregar un nuevo tipo de campo. Siga las instrucciones de este panel y haga clic en Crear. También puede modificar o eliminar cualquier tipo de campo agregado por el usuario si no está siendo utilizado por una regla implementada.

Para agregar o modificar la comprobación de seguridad Formatos de campo mediante la interfaz gráfica de usuario

1. Vaya a **Firewall de aplicaciones** > **Perfiles**, resalte el perfil de destino y haga clic en **Modificar**.
2. En el panel **Configuración avanzada**, haga clic en **Comprobaciones de seguridad**.

   La tabla de comprobación de seguridad muestra los valores de acción configurados actualmente para todas las comprobaciones de seguridad. Tiene 2 opciones para la configuración:

   a) Si solo quiere habilitar o inhabilitar las acciones **Bloquear**, **Registrar**, **Estadísticas** y **Aprender** para Formatos de campo, puede activar o desactivar las casillas de verificación de la tabla, hacer clic en **Aceptar** y, a continuación, en **Guardar y cerrar** para cerrar el panel Comprobación de seguridad.
   b) Si quiere configurar opciones adicionales para esta comprobación de seguridad, haga doble clic en Formatos de campo o seleccione la fila y haga clic en Configuración de acción para mostrar las siguientes opciones para **Formato de campo predeterminado**:
      - **Tipo de campo**: Seleccione el tipo de campo que quiere configurar como tipo de campo predeterminado. Puede seleccionar los tipos de campo integrados y definidos por el usuario. Los mapas de caracteres implementados también se incluyen en la lista y se pueden seleccionar.
      - **Longitud mínima**: Especifique el número mínimo de caracteres que debe haber en cada campo. Valores posibles: 0-65535.
      - **Longitud máxima**: Especifique el número máximo de caracteres que debe haber en cada campo. Valores posibles: 1-65535.
        También puede modificar las acciones **Bloquear**, **Registro**, **Estadísticas** y **Aprendizaje**en el panel Configuración de formatos de campo.

   Después de realizar cualquiera de los cambios anteriores, haga clic en **Aceptar** para guardar los cambios y volver a la tabla Comprobaciones de seguridad. Puede proceder a configurar otras comprobaciones de seguridad si es necesario. Haga clic en **Aceptar** para guardar todos los cambios realizados en la sección Comprobaciones de seguridad y, a continuación, haga clic en **Guardar y cerrar** para cerrar el panel Comprobación de seguridad.

Para configurar una regla de relajación Formatos de campo mediante la interfaz gráfica de usuario

1. Vaya a **Firewall de aplicaciones** > **Perfiles**, resalte el perfil de destino y haga clic en **Modificar**.

2. En el panel **Configuración avanzada**, haga clic en **Reglas de relajación**. La tabla Reglas de relajación tiene una entrada Formatos de campo. Puede hacer doble clic, o seleccionar esta fila y hacer clic en el botón Modificar, para acceder al diálogo Reglas de relajación de formatos de campo. Puede realizar operaciones **Agregar**, **Modificar**, **Eliminar**, **Habilitar**o **Inhabilitar** para reglas de relajación.

Para obtener una vista consolidada de todas las reglas de relajación, puede resaltar la fila Formatos de campo y hacer clic en Visualizador. El visualizador para las relajaciones implementadas le ofrece la opción de Agregar una nueva regla o Modificar una existente. También puede habilitar o inhabilitar un grupo de reglas seleccionando un nodo y haciendo clic en los botones correspondientes en el visualizador de relajación.

Uso de la función de aprendizaje con la comprobación de formatos de campo

Cuando la acción de aprendizaje está habilitada, el motor de aprendizaje de Web App Firewall supervisa el tráfico y descubre las infracciones desencadenadas. Puede inspeccionar periódicamente estas reglas aprendidas. Después de tener debidamente en cuenta, puede implementar la regla aprendida como regla de relajación Formato de campo.

Mejora de aprendizaje de formatos de campo: En la versión 11.0 se introdujo una mejora de aprendizaje de Web App Firewall. En las versiones anteriores, una vez implementada la recomendación de formato de campo aprendido, el motor de aprendizaje de Web App Firewall deja de supervisar las solicitudes válidas con el fin de recomendar nuevas reglas sobre la base de los nuevos puntos de datos. Esto limita la protección de seguridad configurada, ya que la base de datos de aprendizaje no incluye ninguna representación de los nuevos datos vistos en las solicitudes válidas procesadas por la comprobación de seguridad.

Las violaciones ya no se combinan con el aprendizaje. El motor de aprendizaje aprende y hace recomendaciones para los formatos de campo independientemente de las infracciones. Además de comprobar las solicitudes bloqueadas para determinar si el formato de campo actual es demasiado restrictivo y necesita ser relajado, el motor de aprendizaje también supervisa las solicitudes permitidas para determinar si el formato de campo actual es demasiado permisivo y permite elevar la seguridad mediante la implementación de un regla restrictiva.

A continuación se presenta un resumen del comportamiento de aprendizaje de formatos de campo:

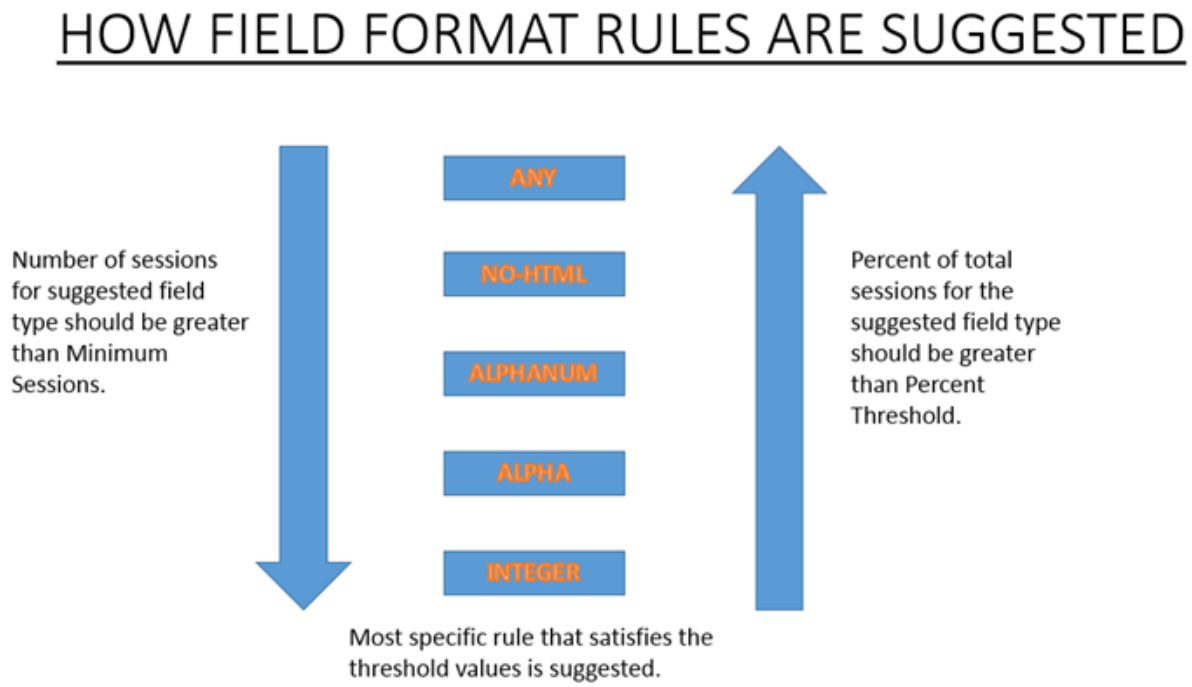
No hay formato de campo enlazado: El comportamiento permanece sin cambios en este caso. Todos los datos de aprendizaje se envían al motor aslearn. El motor de aprendizaje sugiere una regla de formato de campo basada en el conjunto de datos.

El formato de campo está enlazado: En las versiones anteriores, los datos observados se envían al motor aslearn solo en caso de una infracción. El motor de aprendizaje sugiere una regla de formato de campo basada en el conjunto de datos. En la versión 11.0, todos los datos se envían a aslearn

motor incluso si no se desencadena ninguna infracción. El motor de aprendizaje sugiere una regla de formato de campo basada en todo el conjunto de datos de todas las entradas recibidas.

Caso de uso para mejorar el aprendizaje:

Si las reglas aprendidas de formato de campo inicial se basan en una pequeña muestra de datos, algunos valores no típicos podrían dar lugar a una recomendación demasiado indulgente para el campo de destino. El aprendizaje continuo permite al Web App Firewall observar los puntos de datos de cada solicitud para recopilar una muestra representativa para las recomendaciones aprendidas. Esto es útil para reforzar aún más la seguridad para implementar el formato de entrada óptimo con un valor de rango adecuado.



El aprendizaje de formato de campo hace uso de la prioridad de los tipos de campo, así como de la configuración de los siguientes umbrales de aprendizaje:

- **FieldFormatMinThreshold**—Número mínimo de veces que se debe observar un campo de formulario específico antes de generar una relajación aprendida. Valor predeterminado: 1.
- **FieldFormatPercentThreshold**—Porcentaje de veces que un campo de formulario coincide con un tipo de campo determinado, antes de generar una relajación aprendida. Valor predeterminado: 0.

Las recomendaciones de reglas de formato de campo se basan en los siguientes criterios:

- **Recomendaciones de tipo**de campo: Las recomendaciones de tipo de campo están determinadas por las prioridades asignadas de los tipos de campo existentes y los umbrales de formato de campo especificados. Las prioridades determinan el orden en que los tipos de campo se comparan con las entradas. Un número inferior especifica una prioridad más alta. Por ejemplo, el

entero Tipo de campo tiene la prioridad más alta (30) y, por lo tanto, se evalúa antes de Tipo de campo alfanum (50). Los umbrales determinan el número de entradas evaluadas para recopilar una muestra representativa para el punto de datos. Asignar la prioridad correcta a los tipos de campo configurados y configurar un valor de **aprendizaje** adecuado para los parámetros **FieldFormatPercentThreshold** y **FieldFormatMinThreshold**, es esencial para obtener la recomendación correcta de formato de campo. El tipo de campo con la prioridad más alta, basado en los umbrales configurados, se compara primero con las entradas. Si hay una coincidencia, se sugiere este tipo de campo sin tener en cuenta los otros tipos de campo. Por ejemplo, tres tipos de campo predeterminados, integer, alphanum y any coincidirán si todas las entradas contienen solo números. Sin embargo, se recomienda integer ya que tiene la prioridad más alta.

- **Recomendaciones de longitud mínima y máxima**: Los cálculos para las longitudes mínima y máxima del formato de campo se realizan independientemente de la determinación del tipo de campo. Los cálculos de longitud de formato de campo se basan en la longitud media de todas las entradas observadas. La mitad de este promedio calculado se sugiere como valor mínimo, y el doble del valor de este promedio se sugiere como valor máximo. El rango para la longitud mínima es 0-65535 y el rango para la longitud máxima es 1-65535. El valor configurado para la longitud mínima no puede exceder la longitud máxima.
- **Manejo del carácter de espacio**: La comprobación Formato de campo cuenta todos los caracteres de espacio al comprobar la longitud de Formatos de campo. Los espacios iniciales o finales no se eliminan, y varios espacios consecutivos en el centro de la cadena de entrada ya no se consolidan en un solo espacio durante el procesamiento de entrada.

Ejemplo para ilustrar las recomendaciones de formato de campo:

```
Total requests: 100
Number of Req with Field Type:
Int : 22            (22 int values)  -  22%
Alpha : 44                  (44 alpha values)  -  44%
Alphanum: 14            (14 + 44 + 22 = 80 alphanum values) = 80%
noHTML: 10              (80 + 10 = 90 noHTML values) = 90%
any : 10                     (90 + 10 = 100 any values) = 100%

% threshold                              Suggested Field Type
0-22                int
23-44               alpha
45-80               alphanum
81-90               noHTML
91-100              any
<!--NeedCopy-->
```

Para ver o utilizar datos aprendidos mediante la interfaz de línea de comandos


```
show appfw learningdata <profilename> FieldFormat
rm appfw learningdata <profilename> -fieldFormat <string>  <
    formActionURL>
export appfw learningdata <profilename> FieldFormat
<!--NeedCopy-->
```

Para ver o utilizar datos aprendidos mediante la interfaz gráfica de usuario

1. Vaya a **Firewall de aplicaciones** > **Perfiles**, resalte el perfil de destino y haga clic en **Modificar**.
2. En el panel **Configuración avanzada**, haga clic en **Reglas aprendidas**. Puede seleccionar la entrada Formatos de campo en la tabla Reglas aprendidas y hacer doble clic en ella para acceder a las reglas aprendidas. Puede implementar las reglas aprendidas o modificar una regla antes de implementarla como regla de relajación. Para descartar una regla, puede seleccionarla y hacer clic en el botón **Omitir**. Solo puede modificar una regla a la vez, pero puede seleccionar varias reglas para implementar u omitir.

   También tiene la opción de mostrar una vista resumida de las relajaciones aprendidas seleccionando la entrada Formatos de campo en la tabla Reglas aprendidas y haciendo clic en Visualizador para obtener una vista consolidada de todas las infracciones aprendidas. El visualizador hace que sea muy fácil administrar las reglas aprendidas. Presenta una visión completa de los datos en una pantalla y facilita la acción en un grupo de reglas con un solo clic. La mayor ventaja del visualizador es que recomienda expresiones regulares para consolidar varias reglas. Puede seleccionar un subconjunto de estas reglas, basado en el delimitador y la URL de acción. Puede mostrar 25, 50 o 75 reglas en el visualizador seleccionando el número de una lista desplegable. El visualizador de reglas aprendidas ofrece la opción de modificar las reglas e implementarlas como relajaciones. O puede omitir las reglas para ignorarlas.

Mediante la función de registro con los formatos de campo, compruebe

Cuando la acción de registro está habilitada, las infracciones de comprobación de seguridad Formatos de campo se registran en el registro de auditoría como infracciones de APTFW_FIELDFORMAT. El Web App Firewall admite los formatos de registro nativo y CEF. También puede enviar los registros a un servidor syslog remoto.

Para acceder a los mensajes de registro mediante la línea de comandos

Cambie al shell y siga los ns.logs en la carpeta /var/log/ para acceder a los mensajes de registro correspondientes a las infracciones de Formatos de campo:

- `Shell`
- `tail -f /var/log/ns.log | grep APPFW_FIELDFORMAT`

Para acceder a los mensajes de registro mediante la interfaz gráfica de usuario

La GUI de Citrix incluye una herramienta muy útil (Syslog Viewer) para analizar los mensajes de registro. Tiene varias opciones para acceder al Visor de Syslog:

- Vaya a **Firewall de aplicaciones** > **Perfiles**, seleccione el perfil de destino y haga clic en **Comprobaciones de seguridad**. Resalte la fila Formatos de campo y haga clic en **Registros**. Cuando accede a los registros directamente desde la comprobación de **seguridad Formatos de campo** del perfil, filtra los mensajes de registro y muestra solo los registros correspondientes a estas infracciones de comprobación de seguridad.
- También puede acceder al Visor de Syslog navegando a **Citrix ADC** > **Sistema** > **Auditoría**. En la sección **Mensajes de auditoría**, haga clic en el enlace **Mensajes de syslog** para mostrar el **Visor de Syslog**, que muestra todos los mensajes de registro, incluidos otros registros de infracciones de comprobación de seguridad. Esto es útil para depurar cuando se pueden desencadenar varias infracciones de comprobación de seguridad durante el procesamiento de solicitudes.
- Vaya a **Firewall de aplicaciones** > **Directivas** > **Auditoría**. En la sección **Mensajes de auditoría**, haga clic en el enlace Mensajes de syslog para mostrar el Visor de Syslog, que muestra todos los mensajes de registro, incluidos otros registros de infracciones de comprobación de seguridad.

  El Visor de Syslog basado en HTML proporciona varias opciones de filtro para seleccionar solo los mensajes de registro que le interesan. Para acceder a los mensajes de registro de infracciones de comprobación de seguridad Formatos de campo, filtre seleccionando APTFW en las opciones desplegables de Módulo. El tipo de evento muestra un amplio conjunto de opciones para refinar aún más la selección. Por ejemplo, si activa la casilla de verificación **APPFW_FIELDFORMAT** y hace clic en el botón **Aplicar**, en el Visor de Syslog solo aparecen los mensajes de registro correspondientes a las infracciones de comprobación de seguridad de Formatos de campo.

Si coloca el cursor en la fila de un mensaje de registro específico, aparecen varias opciones, como Module y EventType, debajo del mensaje de registro. Puede seleccionar cualquiera de estas opciones para resaltar la información correspondiente en los registros.

Ejemplo de un mensaje de registro de formato nativo cuando la solicitud no está bloqueada

```
1 Jun 10 22:32:26 <local0.info> 10.217.31.98 06/10/2015:22:32:26 GMT ns
     0-PPE-0 :
2 default APPFW APPFW_FIELDFORMAT 97 0 :  10.217.253.62 562-PPE0
3 x1MV+YnNGzQFM3Bsy2wti4bhXio0001 pr_ffc http://aaron.stratum8.net/FFC/
     login_post.php
4 Field format check failed for field passwd=”65568888sz-*_” <not blocked
     >
```



```
Example of a CEF format log message when the request is blocked
Jun 11 00:03:51 <local0.info> 10.217.31.98
CEF:0|Citrix|Citrix ADC|NS11.0|APPFW|APPFW_FIELDFORMAT|6|src
   =10.217.253.62 spt=27076
method=POST requet=http://aaron.stratum8.net/FFC/maxlen_post.php msg=
   Field format check
failed for field text_area="" cn1=108 cn2=644 cs1=pr_ffc cs2=PPE0
cs3=GaUROfl1Nx1jJTvja5twH5BBqI0000 cs4=ALERT cs5=2015 act=blocked
<!--NeedCopy-->
```

Estadísticas de las infracciones de formatos de campo

Cuando la acción de estadísticas está habilitada, el contador correspondiente para la comprobación Formatos de campo se incrementa cuando el Web App Firewall realiza cualquier acción para esta comprobación de seguridad. Las estadísticas se recopilan para Rate and Total count para Tráfico, Violaciones y Registros. El incremento del contador de registro puede variar en función de la configuración configurada. Por ejemplo, si la acción de bloqueo está habilitada, la solicitud de una página que contiene 3 infracciones de formato de campo incrementa el contador de estadísticas en una, porque la página se bloquea tan pronto como se detecta la primera infracción de formatos de campo. Sin embargo, si el bloque está inhabilitado, el procesamiento de la misma solicitud aumenta en 3 el contador de estadísticas para infracciones y los registros, ya que cada infracción de Formatos de campo genera un mensaje de registro independiente.

Para mostrar estadísticas de formatos de campo mediante la línea de comandos

En el símbolo del sistema, escriba:

```
sh appfw stats
```

Para mostrar las estadísticas de un perfil específico, utilice el siguiente comando:

```
stat appfw profile <profile name>
```

Para mostrar estadísticas de formatos de campo mediante GUI

1. Vaya a **Sistema** > **Seguridad** > **Firewall de aplicaciones**.
2. En el panel derecho, acceda al Enlace de estadísticas.
3. Utilice la barra de desplazamiento para ver las estadísticas sobre infracciones y registros de formatos de campo. La tabla de estadísticas proporciona datos en tiempo real y se actualiza cada 7 segundos.

Sugerencia para la implementación

- Habilitar el registro de acciones de formato de campo, aprendizaje y estadísticas.

- Después de ejecutar una muestra representativa del tráfico a la aplicación, revise las recomendaciones aprendidas.
- Si la mayoría de las reglas aprendidas recomiendan un tipo de campo, configure ese tipo de campo como el tipo de campo predeterminado. Para longitudes mínimas y máximas, utilice el rango más amplio sugerido por estas reglas.
- Implementar reglas para otros campos para los que se adapten mejor a diferentes tipos de campo o longitudes mínimas/máximas diferentes.
- Habilite el bloqueo e inhabilite el aprendizaje.
- Supervisar estadísticas y registros. Si todavía se está desencadenando un número significativo de infracciones, es posible que quiera revisar los mensajes de registro para confirmar que las infracciones representan solicitudes maliciosas que deben haberse bloqueado. Si las solicitudes válidas se marcan como infracciones, puede modificar la regla de formato de campo configurada para relajarla aún más o habilitar el aprendizaje de nuevo para obtener recomendaciones basadas en los nuevos puntos de datos.

> **Nota:** Puede ajustar su configuración obteniendo nuevas recomendaciones de aprendizaje.

Resumen

Tenga en cuenta los siguientes puntos acerca de la comprobación de seguridad Formato de campo:

- **Protección**: Mediante la configuración de reglas de formato de campo óptimas, puede protegerse contra muchos ataques. Por ejemplo, si especifica que un campo solo puede tener enteros, los piratas informáticos no podrán iniciar ataques de inyección SQL o scripts entre sitios mediante este campo, ya que las entradas necesarias para lanzar dichos ataques no cumplirán el requisito de formato de campo configurado.
- **Rendimiento**: Puede limitar la longitud mínima y máxima permitida para las entradas en las reglas de formato de campo. Esto puede impedir que un usuario malintencionado introduzca cadenas de entrada excesivamente grandes en un intento de agregar sobrecarga de procesamiento al servidor o, peor aún, hacer que el servidor volque el núcleo debido al desbordamiento de pila. Al limitar el tamaño de entrada, puede acortar el tiempo necesario para procesar solicitudes legítimas.
- **Configuración de formatos de campo**: Debe habilitar una de las acciones (bloquear, registrar, estadísticas, aprender) para activar la protección de formato de campo. También puede especificar las reglas de formato de campo para identificar las entradas permitidas en los campos de formulario.
- **Selección de mapas de caracteres frente a Tipos de campo**: Tanto los mapas de caracteres como los tipos de campo utilizan expresiones regulares. Sin embargo, un mapa de caracteres proporciona una expresión más específica al reducir la lista de caracteres permitidos. Por ejemplo, para una entrada como janedoe@citrix.com, el motor de aprendizaje podría recomendar el tipo de campo nohtml pero el mapa de caracteres [. @-za-z] podría ser más específico, porque

reduce el conjunto permitido de caracteres no alfa. La opción Mapa de caracteres permite, además de los caracteres alfa, solo dos caracteres no alfa: Punto (.) y en (@).

- **Aprendizaje continuo**: El Web App Firewall supervisa y tiene en cuenta todos los datos entrantes (infracciones, así como entradas permitidas) para crear una tabla de aprendizaje para recomendar reglas. Las reglas se revisan y actualizan a medida que llegan nuevos datos entrantes. Se sugieren nuevas reglas de formato de campo para un campo aunque ya tenga una regla de formato de campo enlazado. Si los formatos de campo configurados son demasiado restrictivos y bloquean las solicitudes válidas, puede implementar un formato de campo más relajado. Del mismo modo, si los formatos de campo actuales son demasiado genéricos, puede refinar y reforzar aún más la seguridad implementando un formato de campo más restrictivo.
- **Reglas de sobrescritura**: Si ya se ha implementado una regla para una combinación de campo/URL, la GUI permite al usuario actualizar el formato del campo. Un cuadro de diálogo solicita confirmación para reemplazar la regla existente. Si está usando la interfaz de línea de comandos, debe desvincular explícitamente el enlace anterior y luego enlazar la nueva regla.
- **Coincidencia múltiple**: Si varios formatos de campo coinciden con un nombre de campo determinado y su dirección URL de acción, el Web App Firewall selecciona arbitrariamente uno de ellos para aplicarlo.
- **Límite de búfer**: Si un valor de campo se extiende a través de varios búferes de transmisión y el formato de estas dos partes del valor de campo es diferente, se envía un formato de campo correspondiente a “cualquiera” a la base de datos de aprendizaje.
- **Formato de campo frente a Comprobación de coherencia de campo**: Tanto la comprobación de formato de campo como la comprobación de coherencia de campo son comprobaciones de protección basadas en formularios. La comprobación Formatos de campo proporciona un tipo de protección diferente al de la comprobación Consistencia de campos de formulario. La comprobación Consistencia de campos de formulario comprueba que la estructura de los formularios web devueltos por los usuarios esté intacta, que se respeten las restricciones de formato de datos configuradas en el HTML y que no se hayan modificado los datos de los campos ocultos. Puede hacer esto sin ningún conocimiento específico sobre sus formularios web que no sea lo que deriva del propio formulario web. La comprobación Formatos de campo comprueba que los datos de cada campo de formulario coinciden con las restricciones de formato específicas que configuró manualmente o que la función de aprendizaje generó y aprobó. En otras palabras, la comprobación Consistencia de campos de formulario aplica la seguridad general del formulario web, mientras que la comprobación Formatos de campo aplica las reglas específicas para las entradas permitidas para los formularios web.

Comprobación de coherencia de campos de formulario

August 20, 2021

La comprobación de coherencia del campo de formulario examina los formularios web devueltos por los usuarios de su sitio web y comprueba que los formularios web no fueron modificados incorrectamente por el cliente. Esta comprobación solo se aplica a las solicitudes HTML que contienen un formulario web, con o sin datos. No se aplica a las solicitudes XML.

La comprobación de coherencia del campo del formulario impide que los clientes realicen cambios no autorizados en la estructura de los formularios web de su sitio web cuando rellenen y envíen un formulario. También garantiza que los datos que envía un usuario cumplan las restricciones HTML de longitud y tipo, y que los datos de los campos ocultos no se modifiquen. Esto evita que un atacante manipule un formulario web y utilice el formulario modificado para obtener acceso no autorizado al sitio web, redirigir la salida de un formulario de contacto que utiliza un script inseguro y, por lo tanto, enviar correo electrónico masivo no solicitado, o explotar una vulnerabilidad en el software del servidor web para obtener el control de la web o el sistema operativo subyacente. Los formularios web son un enlace débil en muchos sitios web y atraen una amplia gama de ataques.

La comprobación Consistencia de campos de formulario comprueba todos los elementos siguientes:

- Si se envía un campo al usuario, la comprobación garantiza que el usuario lo devuelve.
- La comprobación aplica longitudes y tipos de campo HTML.

  > **Nota:**
  >
  > - La comprobación Consistencia de campos de formulario aplica restricciones HTML sobre el tipo y la longitud de datos, pero no valida los datos en formularios web. Puede utilizar la comprobación Formatos de campo para configurar reglas que validen los datos devueltos en campos de formulario específicos de los formularios web.
  > - La protección de coherencia de campos de formulario inserta un campo oculto “as_fid” en los formularios de respuesta que se envían al cliente. El mismo campo oculto será eliminado por ADC cuando el cliente envíe el formulario. Si hay algún javascript del lado del cliente haciendo cálculo de suma de comprobación en los campos de formulario y verificando la misma suma de comprobación en el backend puede causar la rotura de la aplicación. En este caso, Se recomienda relajar la consistencia del campo de formulario de firewall de aplicación campo oculto campo “as_fid” de cálculo de suma de comprobación javascript del lado del cliente.

- Si el servidor web no envía un campo al usuario, la comprobación no permite al usuario agregar ese campo y devolver datos en él.
- Si un campo es de solo lectura u oculto, la comprobación comprueba que los datos no han cambiado.
- Si un campo es un campo de cuadro de lista o de botón de opción, la comprobación comprueba que los datos de la respuesta corresponden a uno de los valores de ese campo.

Si un formulario web devuelto por un usuario infringe una o varias de las comprobaciones de coherencia de campos de formulario y no ha configurado el Web App Firewall para permitir que dicho formulario web infrinja las comprobaciones de coherencia de campos de formulario, la solicitud se bloquea.

Si utiliza el asistente o la GUI, en el cuadro de diálogo Modificar comprobación de coherencia de campos de formulario, en la ficha General puede habilitar o inhabilitar las acciones Bloquear, Registro, Aprendizaje y Estadísticas.

También puede configurar la coherencia de campos sin sesión en la ficha General. Si la coherencia de campos sin sesión está habilitada, Web App Firewall comprueba solo la estructura del formulario web, prescindiendo de las partes de la comprobación Consistencia de campos de formulario que dependen del mantenimiento de la información de la sesión. Esto puede acelerar la comprobación de coherencia del campo de formulario con poca penalización de seguridad para sitios web que utilizan muchos formularios. Para utilizar la coherencia de campo sin sesión en todos los formularios web, seleccione Activado. Para usarlo solo para formularios enviados con el método HTTP POST, seleccione postOnly

Si utiliza la interfaz de línea de comandos, puede escribir el siguiente comando para configurar la comprobación de coherencia de campos de formulario:

- `set appfw profile <name> -fieldConsistencyAction [**block**] [**learn **] [**log**] [**stats**] [**none**]`

Para especificar relajantes para la comprobación Consistencia de campos de formulario, debe utilizar la GUI. En la ficha Comprobaciones del cuadro de diálogo Modificar comprobación de coherencia de campos de formulario, haga clic en Agregar para abrir el cuadro de diálogo Agregar relajación de comprobación de coherencia de campos de formulario o seleccione una relajación existente y haga clic en Abrir para abrir el cuadro de diálogo Modificar relajación de comprobación de coherencia de campos de formulario. Cualquiera de los cuadros de diálogo proporciona las mismas opciones para configurar una relajación, como se describe en Configuración manual mediante la GUI.

A continuación se presentan ejemplos de relajación de comprobación de coherencia de campos de formulario:

Nombres de campos de formulario:

- Elija campos de formulario con el nombre UserType:

```
^UserType$
<!--NeedCopy-->
```

- Elija campos de formulario con nombres que comiencen por UserType_ y que estén seguidos de una cadena que comience por una letra o un número y se componga de una a veintiún letras, números o el símbolo apóstrofo o guión:


```
^UserType_[0-9A-Za-z][0-9A-Za-z'-]{
0,20 }
$
<!--NeedCopy-->
```

- Elija campos de formulario con nombres que comiencen por Turkish-userType_ y sean los mismos que la expresión anterior, excepto que pueden contener caracteres especiales turcos en:

```
^T\xC3\xBCrk\xC3\xA7e-UserType_([0-9A-Za-z]|\x[0-9A-Fa-f][0-9A-Fa
   -f])+$
<!--NeedCopy-->
```

> **Nota:**
>
> Consulte Formato de codificación de caracteres PCRE para obtener una descripción completa de los caracteres especiales admitidos y cómo codificarlos correctamente.

- Elija nombres de campo de formulario que comiencen por una letra o un número, que consistan en una combinación de letras y/o números solamente y que contengan la cadena Num en cualquier lugar de la cadena:

```
^[0-9A-Za-z]\*Num[0-9A-Za-z]\*$
<!--NeedCopy-->
```

Direcciones URL de acción de campo de formulario:

- Elija direcciones URL que empiecen por `http://www.example.com/search.pl?` y contengan cualquier cadena después de la consulta, excepto una nueva consulta:

```
^http://www[.]example[.]com/search[.]pl?[^?]*$
<!--NeedCopy-->
```

- Elija direcciones URL que comiencen por `http://www.example-español.com` y tengan rutas y nombres de archivo que constan de letras mayúsculas y minúsculas, números, caracteres especiales no ASCII y símbolos seleccionados en la ruta. El carácter ñ y cualquier otro carácter especial se representan como cadenas UTF-8 codificadas que contienen el código hexadecimal asignado a cada carácter especial en el juego de caracteres UTF-8:


```
^http://www[.]example-espa\xC3\xB1ol[.]com/(([0-9A-Za-z]|\x[0-9A-Fa-f][0-9A-Fa-f])
([0-9A-Za-z_-]|\x[0-9A-Fa-f][0-9A-Fa-f])\*/)\*([0-9A-Za-z]|\x[0-9A-Fa-f][0-9A-Fa-f])
([0-9A-Za-z_-]|\x[0-9A-Fa-f][0-9A-Fa-f])*[.](asp|htp|php|s?html?)$
<!--NeedCopy-->
```

- Elija todas las URL que contengan la cadena /search.cgi? :

```
^[^?<>]\*/search[.]cgi?[^?<>]\*$
<!--NeedCopy-->
```

> **Precaución:**
>
> Las expresiones regulares son potentes. Especialmente si no está completamente familiarizado con las expresiones regulares con formato PCRE-format, compruebe las expresiones regulares que escriba. Asegúrese de que definen exactamente la URL que quiere agregar como excepción, y nada más. El uso descuidado de comodines, y especialmente de la combinación de metacaracteras/comodín punto-asterisco (.*), puede tener resultados que no quiere o espera, como bloquear el acceso a contenido web que no tenía intención de bloquear o permitir un ataque que la comprobación de consistencia de cookies tendría de otro modo bloqueado.

Comprobación de etiquetado de formularios CSRF

January 12, 2021

El etiquetado de formularios de falsificación de solicitudes cruzadas (CSRF) marca cada formulario web enviado por un sitio web protegido a los usuarios con un FormID único e impredecible y, a continuación, examina los formularios web devueltos por los usuarios para asegurarse de que el FormID proporcionado es correcto. Esta comprobación protege contra ataques de falsificación de solicitudes entre sitios. Esta comprobación solo se aplica a las solicitudes HTML que contienen un formulario web, con o sin datos. No se aplica a las solicitudes XML.

La comprobación de etiquetado de formularios CSRF evita que los atacantes utilicen sus propios formularios web para enviar respuestas de formularios de gran volumen con datos a sus sitios web protegidos. Esta comprobación requiere relativamente poca capacidad de procesamiento de CPU en comparación con otras comprobaciones de seguridad que analizan los formularios web en profundidad. Por lo tanto, es capaz de manejar ataques de gran volumen sin degradar seriamente el rendimiento del sitio web protegido o del propio Web App Firewall.

Antes de habilitar la comprobación CSRF Form Etiquetado, debe tener en cuenta lo siguiente:

- Debe habilitar el etiquetado de formularios. La comprobación CSRF depende del etiquetado de formularios y no funciona sin ella.
- Debe inhabilitar la función de almacenamiento en caché integrado de Citrix ADC para todas las páginas web que contengan formularios protegidos por ese perfil. La función de almacenamiento en caché integrado y el etiquetado de formularios CSRF no son compatibles.
- Debe considerar habilitar la comprobación de Referer. La comprobación de referencias forma parte de la comprobación de URL de inicio, pero evita falsificaciones de solicitudes entre sitios, no violaciones de URL de inicio. La comprobación de referer también pone menos carga en la CPU que la comprobación CSRF Form Tagging. Si una solicitud viola la comprobación de Referer, se bloquea inmediatamente, por lo que no se invoca la comprobación CSRF Form Tagging.
- La comprobación de etiquetado de formularios CSRF no funciona con formularios web que utilizan dominios diferentes en la dirección URL de origen del formulario y la dirección URL de acción del formulario. Por ejemplo, el etiquetado de formularios CSRF no puede proteger un formulario web con una dirección URL de origen de formulario `http://www.example.com` y una dirección URL de acción de formulario de `http://www.example.org/form`.pl, porque example.com y example.org son dominios diferentes.

Si utiliza el asistente o la GUI, en el cuadro de diálogo Modificar comprobación de etiquetado de formularios CSRF, en la ficha General puede habilitar o inhabilitar las acciones Bloquear, Registro, Aprendizaje y Estadísticas.

Si utiliza la interfaz de línea de comandos, puede introducir el siguiente comando para configurar la comprobación de etiquetado de formularios CSRF:

- `set appfw profile <name> -CSRFtagAction [**block**] [**log**] [**learn**] [**stats**] [**none**]`

Para especificar relajantes para la comprobación CSRF Form Tagging, debe utilizar la GUI. En la ficha Comprobaciones del cuadro de diálogo Modificar comprobación de etiquetado de formularios CSRF, haga clic en Agregar para abrir el cuadro de diálogo Agregar relajación de comprobación de etiquetado de formularios CSRF o seleccione una relajación existente y haga clic en Abrir para abrir el cuadro de diálogo Modificar comprobación de etiquetado de formularios CSRF. Cualquiera de los dos cuadros de diálogo proporciona las mismas opciones para configurar una relajación.

Se genera una alerta cuando se establece el límite de sesión de Citrix Web App Firewall en un valor de 0 o inferior, ya que dicha configuración afecta a la funcionalidad de comprobación de protección avanzada que requiere una sesión de Web App Firewall que funcione correctamente.

A continuación se presentan ejemplos de relajación de comprobación CSRF Form Tagging:

Nota: Las siguientes expresiones son expresiones URL que se pueden utilizar en las funciones Dirección URL de origen del formulario y Dirección URL de acción del formulario.

- Elija direcciones URL que empiecen por `http://www.example.com/search.pl?` y contengan cualquier cadena después de la consulta, excepto una nueva consulta:

```
^http://www[.]example[.]com/search[.]pl?[^?]*$
<!--NeedCopy-->
```

- Elija direcciones URL que comiencen por `http://www.example-español.com` y tengan rutas y nombres de archivo que constan de letras mayúsculas y minúsculas, números, caracteres especiales no ASCII y símbolos seleccionados en la ruta. El carácter ñ y cualquier otro carácter especial se representan como cadenas UTF-8 codificadas que contienen el código hexadecimal asignado a cada carácter especial en el juego de caracteres UTF-8:

```
^http://www[.]example-espa\xC3\xB1ol[.]com/(([0-9A-Za-z]|\x[0-9A-Fa
   -f][0-9A-Fa-f])
([0-9A-Za-z_-]|\x[0-9A-Fa-f][0-9A-Fa-f])\*/)\*([0-9A-Za-z]|\x[0-9A-Fa-f
   ][0-9A-Fa-f])([0-9A-Za-z_-]|\x[0-9A-Fa-f][0-9A-Fa-f])*[.](asp|htp|
   php|s?html?)$
<!--NeedCopy-->
```

- Elija todas las URL que contengan la cadena /search.cgi? :

```
^[^?<>]\*/search[.]cgi?[^?<>]\*$
<!--NeedCopy-->
```

Importante

Las expresiones regulares son potentes. Si no está completamente familiarizado con las expresiones regulares con formato PCRE-format, compruebe las expresiones regulares que escriba. Asegúrese de que definen exactamente la URL que quiere agregar como excepción, y nada más. El uso descuidado de comodines, y especialmente de la combinación de metacarácter/comodín de punto (.*), puede tener resultados que no quiera, como bloquear el acceso al contenido web que no tenía intención de bloquear o permitir un ataque que la comprobación habría bloqueado de otro modo.

Sugerencia

Cuando el encabezado de referencia enableValidate está habilitado en la acción de URL de inicio, asegúrese de que la URL del encabezado de referencia también se agrega a StartURL.

Nota

> Cuando Citrix ADC alcanza appfw_session_limit y las comprobaciones CSRF están habilitadas, la aplicación web se bloquea.
>
> Para evitar la congelación de aplicaciones web, reduzca el tiempo de espera de la sesión y aumente el límite de sesión mediante los siguientes comandos:
>
> Desde CLI: > set appfw settings —sessiontimeout 300
> Desde shell: Root @ns # nsapimgr_wr.sh -s appfw_session_limit=200000
>
> Registrar y generar alarmas SNMP cuando se alcanza appfw_session_limit le ayuda a solucionar problemas y depurar.

Administración de relajaciones de comprobación de etiquetado de formularios CSRF

August 20, 2021

Puede configurar una excepción (o relajación) en la comprobación de seguridad de etiquetado de formularios CSRF en el cuadro de diálogo Agregar solicitud de falsificación de etiquetas de comprobación de comprobación de relajación o en el cuadro de diálogo Modificar verificación de etiquetado de falsificación de solicitudes entre sitios.

Para configurar un etiquetado de formularios CSRF, compruebe relajación mediante la interfaz gráfica de usuario

1. Vaya a **Seguridad > Citrix Web App Firewall > Perfiles**.
2. En el panel **Perfiles**, seleccione el perfil que quiere configurar y, a continuación, haga clic en **Abrir**.
3. En el cuadro de diálogo **Configurar perfil de Web App Firewall**, haga clic en la ficha **Comprobaciones de seguridad**. La ficha **Comprobaciones de seguridad** contiene la lista de comprobaciones de seguridad de Web App Firewall.
4. Para agregar o modificar una relajación CSRF, realice una de las siguientes acciones:
   - Para agregar una nueva relajación, haga clic en Agregar.
   - Para modificar una relajación existente, seleccione la relajación que quiera modificar y, a continuación, haga clic en **Abrir**.

   Aparece el cuadro de diálogo **Agregar solicitud entre sitios de falsificación Etiquetado de comprobación de relajación** o **Modificar solicitud entre sitios de falsificación Etiquetado de comprobación de relajación**. Excepto por el título, estos cuadros de diálogo son idénticos.

5. Rellene el cuadro de diálogo como se describe a continuación.
   - **Casilla de verificación Activada**: Seleccione esta opción para colocar esta relajación o regla en uso activo; desactive para desactivarla.
   - **Dirección URL de origen de formulario**: En el área de texto, escriba una expresión regular con formato PCRE-que defina la dirección URL que aloja el formulario.
   - **Dirección URL de acción de formulario**: En el área de texto, escriba una expresión regular con formato PCRE-que defina la dirección URL a la que se entregan los datos introducidos en el formulario.
   - **Comentarios**: En el área de texto, escriba un comentario. Opcional.

   > **Nota:**
   >
   > Para cualquier elemento que requiera una expresión regular, puede escribir la expresión regular, utilizar el menú **Tokens de expresiones regulares** para insertar elementos y símbolos de expresiones regulares directamente en el cuadro de texto o hacer clic en **Editor de expresiones** regulares para abrir el cuadro de diálogo **Agregar expresión regular**, y usarlo para construir la expresión.
6. Haga clic en **Aceptar**. **Se cierra el cuadro de diálogo Agregar solicitud de falsificación de etiquetas de comprobación de relajación** o **Modificar solicitud de cruce de sitios Etiquetado de falsificación de comprobación de relajación** y se vuelve al cuadro de diálogo **Modificar comprobación de etiquetado de falsificación de solicitudes entre sitios**.
7. Para quitar una relajación o regla, selecciónela y, a continuación, haga clic en **Quitar**.
8. Para habilitar una relajación o regla, selecciónela y, a continuación, haga clic en **Habilitar**.
9. Para inhabilitar una relajación o regla, selecciónela y, a continuación, haga clic en **Inhabilitar**.
10. Para configurar los parámetros y las relaciones de todas las relajaciones existentes en una pantalla gráfica interactiva integrada, haga clic en **Visualizador** y utilice las herramientas de visualización.
11. Para revisar y configurar las reglas aprendidas para la comprobación CSRF, haga clic en **Aprendizaje** y lleve a cabo los pasos descritos en Para configurar y utilizar la función Aprendizaje.
12. Haga clic en **Aceptar**.

Comprobaciones de protección de URL

January 12, 2021

Las comprobaciones de protección de URL examinan las direcciones URL de solicitud para evitar que los atacantes intenten de manera agresiva acceder a varias URL (exploración forzosa) o utilizar una URL para desencadenar una vulnerabilidad de seguridad conocida en el software del servidor web o los scripts de sitios web.

Iniciar comprobación de URL

August 20, 2021

La comprobación de URL de inicio examina las URL de las solicitudes entrantes y bloquea el intento de conexión si la URL no cumple los criterios especificados. Para cumplir los criterios, la dirección URL debe coincidir con una entrada de la lista URL de inicio, a menos que esté habilitado el parámetro Forzar cierre de URL. Si habilita este parámetro, un usuario que haga clic en un vínculo de su sitio web estará conectado al destino de ese enlace.

El propósito principal de la comprobación de URL de inicio es evitar intentos repetidos de acceder a URL aleatorias en un sitio web, (navegación forzosa) a través de marcadores, enlaces externos o saltar a páginas escribiendo manualmente las URL para omitir las páginas necesarias para llegar a esa parte del sitio web. La exploración forzada se puede utilizar para desencadenar un desbordamiento de búfer, encontrar contenido al que los usuarios no tenían intención de acceder directamente o encontrar una puerta trasera en áreas seguras del servidor web. El Web App Firewall aplica la ruta de acceso o lógica dada de un sitio web al permitir el acceso solo a las URL configuradas como direcciones URL de inicio.

Si utiliza el asistente o la GUI, en el cuadro de diálogo Modificar comprobación de URL de inicio, en la ficha General puede habilitar o inhabilitar acciones Bloquear, Registro, Estadísticas, Aprendizaje y los siguientes parámetros:

- **Exigir cierre de URL.** Permita que los usuarios accedan a cualquier página web de su sitio web haciendo clic en un hipervínculo en cualquier otra página de su sitio web. Los usuarios pueden navegar a cualquier página de su sitio web a la que se pueda acceder desde la página principal o cualquier página de inicio designada haciendo clic en hipervínculos.
  Nota: La función de cierre de URL permite que cualquier cadena de consulta se agregue y envíe con la URL de acción de un formulario web enviado mediante el método HTTP GET. Si los sitios web protegidos utilizan formularios para acceder a una base de datos SQL, asegúrese de que tiene habilitada y configurada correctamente la comprobación de inyección SQL.
- **Cierre de URL sin sesión.** Desde el punto de vista del cliente, este tipo de cierre de URL funciona exactamente de la misma manera que el cierre de URL estándar, consciente de la sesión, pero utiliza un token incrustado en la URL en lugar de una cookie para rastrear la actividad del usuario, que consume considerablemente menos recursos. Cuando el cierre de URL sin sesión

está habilitado, Web App Firewall agrega una etiqueta “as_url_id” a todas las URL que se encuentran en el cierre de URL.

Nota: Al habilitar sin sesión (Cierre de URL sin sesión), también debe habilitar el cierre regular de URL (

Exigir cierre de URL) o el cierre de URL sin sesión no funciona.

- **Validar encabezado de referer.** Compruebe que el encabezado Referer en una solicitud que contenga datos de formulario web de su sitio web protegido en lugar de otro sitio web. Esta acción verifica que su sitio web, no un atacante externo, es el origen del formulario web. Al hacerlo, se protege contra falsificaciones de solicitudes entre sitios (CSRF) sin necesidad de etiquetar formularios, lo que requiere más CPU que las comprobaciones de encabezados. El Web App Firewall puede manejar el encabezado HTTP Referer de una de las cuatro maneras siguientes, en función de la opción que seleccione en la lista desplegable:
  - **Off**: No valida el encabezado Referer.
  - **If-Present**—Validar el encabezado Referer si existe un encabezado Referer. Si se encuentra un encabezado Referer no válido, la solicitud genera una infracción de encabezado referer-referer-header. Si no existe un encabezado Referer, la solicitud no genera una infracción de encabezado referer-referer-referer-header. Esta opción permite al Web App Firewall realizar la validación del encabezado del referer en las solicitudes que contienen un encabezado del referer, pero no bloquear las solicitudes de usuarios cuyos exploradores no establecen el encabezado del referer o que utilizan proxies web o filtros que eliminan ese encabezado.
  - **Siempre excepto URL de inicio**: Valide siempre el encabezado Referer. Si no hay encabezado Referer y la URL solicitada no está exenta por la regla de relajación StartURL, la solicitud genera una infracción del encabezado de referencia. Si el encabezado Referer está presente pero no es válido, la solicitud genera una infracción de encabezado referer-referer-header.
  - **Siempre excepto primera solicitud**: Valide siempre el encabezado del referer. Si no hay encabezado de referer, solo se permite la URL a la que se accede primero. Todas las demás URL están bloqueadas sin un encabezado de referer válido. Si el encabezado Referer está presente pero no es válido, la solicitud genera una infracción de encabezado referer-referer-header.

Una configuración de URL de inicio, **Exención de URL de cierre de comprobaciones de seguridad**, no está configurada en el cuadro de diálogo Modificar comprobación de URL de inicio, pero está configurada en la ficha Configuración del perfil. Si está habilitada, esta configuración indica al Web App Firewall que no ejecute más comprobaciones basadas en formularios (como Scripting entre sitios e inspección de SQL Injection) en direcciones URL que cumplan los criterios de cierre de URL.

> **Nota**
>
> Aunque la comprobación del encabezado del referer y la comprobación de seguridad de la URL

> de inicio comparten la misma configuración de acción, es posible violar la comprobación del encabezado del referer sin violar la comprobación de URL de inicio. La diferencia es visible en los registros, que registran violaciones de encabezado de referencia de registro por separado de violaciones de comprobación de URL de inicio.

La configuración del encabezado Referer (OFF, IF-Present, AlwaysExceptStarTurls y AlwaysExcept-FirstRequest) se organiza en orden de menos restrictiva a la más restrictiva y funciona de la siguiente manera:

OFF:

- Cabecera de referencia No marcada.

Presente:

- La solicitud no tiene encabezado de referer -> Se permite la solicitud.
- La solicitud tiene el encabezado del referer y la URL del referer está en el cierre de URL -> Se permite la solicitud.
- La solicitud tiene el encabezado del referer y la URL del referer **no** está en el cierre de URL -> La solicitud está bloqueada.

AlwaysExceptStarTurls:

- La solicitud no tiene encabezado de referer y la URL de solicitud es una URL de inicio -> Se permite la solicitud.
- La solicitud no tiene encabezado de referer y la URL de solicitud no es una URL de inicio ->La solicitud está bloqueada.
- La solicitud tiene el encabezado del referer y la URL del referer está en el cierre de URL -> Se permite la solicitud.
- La solicitud tiene el encabezado del referer y la URL del referer **no** está en el cierre de URL -> La solicitud está bloqueada.

AlwaysExceptFirstRequest:

- La solicitud no tiene encabezado de referer y es la primera URL de solicitud de la sesión -> Se permite la solicitud.
- La solicitud no tiene encabezado de referer y **no** es la primera URL de solicitud de la sesión -> La solicitud está bloqueada.
- La solicitud tiene encabezado de referer y es la primera URL de solicitud de la sesión o está en cierre de URL -> Se permite la solicitud.
- La solicitud tiene encabezado de referer y no es la primera URL de solicitud de la sesión ni está en el cierre de URL -> La solicitud está bloqueada.

Si utiliza la interfaz de línea de comandos, puede introducir los siguientes comandos para configurar la comprobación de URL de inicio:

- set appfw profile <name> -startURLAction [block] [learn] [log] [stats] [none]
- set appfw profile <name> -startURLClosure ([ON] | [OFF])
- set appfw profile <name> -sessionlessURLClosure ([ON] | [OFF])
- set appfw profile <name> -exemptClosureURLsFromSecurityChecks ([ON] | [OFF)
- set appfw profile <name> -RefererHeaderCheck ([OFF] | [if-present] | [AlwaysExceptStartURLs] | [AlwaysExceptFirstRequest])

Para especificar relajantes para la comprobación de URL de inicio, debe usar la GUI. En la ficha Comprobaciones del cuadro de diálogo Modificar comprobación de URL de inicio, haga clic en Agregar para abrir el cuadro de diálogo Agregar relajación de comprobación de URL de inicio o seleccione una relajación existente y haga clic en Abrir para abrir el cuadro de diálogo Modificar relajación de comprobación de URL de inicio. Cualquiera de los dos cuadros de diálogo proporciona las mismas opciones para configurar una relajación.

A continuación se presentan ejemplos de relajación de comprobación de URL de inicio:

- Permitir a los usuarios acceder a la página principal en www.example.com:

```
^http://www[.]example[.]com$
<!--NeedCopy-->
```

- Permitir a los usuarios acceder a todas las páginas web de formato HTML estático (.htm y.html), HTML analizado por servidor (.htp y.shtml), PHP (.php) y Microsoft ASP (.asp) en www.example.com:

```
^http://www[.]example[.]com/([0-9A-Za-z][0-9A-Za-z_-]\*/)\*
[0-9A-Za-z][0-9A-Za-z_.-]*[.](asp|htp|php|s?html?)$
<!--NeedCopy-->
```

- Permitir a los usuarios acceder a páginas web con nombres de ruta o nombres de archivo que contengan caracteres no ASCII en www.example-español.com:

```
^http://www[.]example-espaxC3xB1ol[.]com/(([0-9A-Za-z]|x[0-9A-Fa-
   f][0-9A-Fa-f])([0-9A-Za-z_-]|x[0-9A-Fa-f][0-9A-Fa-f])\*/)\*
([0-9A-Za-z]|x[0-9A-Fa-f][0-9A-Fa-f])([0-9A-Za-z_-]|x[0-9A-Fa-f
   ][0-9A-Fa-f])*[.](asp|htp|php|s?html?)$
<!--NeedCopy-->
```


Nota: En la expresión anterior, cada clase de caracteres se ha agrupado con la cadena x[0-9a-FA-F][0-9A-Fa-f], que coincide con todas las cadenas de codificación de caracteres construidas correctamente pero no permite caracteres de barra invertida que no estén asociados a una cadena de codificación de caracteres UTF-8. La barra invertida doble () es una barra invertida escapada, que indica al Web App Firewall que la interprete como una barra invertida literal. Si solo incluye una barra invertida, el Web App Firewall interpretaría el siguiente corchete izquierdo ([) como un carácter literal en lugar de abrir una clase de caracteres, lo que rompería la expresión.

- Permitir a los usuarios acceder a todos los gráficos en formato GIF (.png), JPEG (.jpg y.jpeg) y PNG (.png) en www.example.com:

```
1 ^http://www[.]example[.]com/([0-9A-Za-z][0-9A-Za-z_-]\*/)\*
2 [0-9A-Za-z][0-9A-Za-z_.-]*[.](gif|jpe?g|png)$
3 <!--NeedCopy-->
```

- Permitir a los usuarios acceder a los scripts CGI (.cgi) y PERL (.pl), pero solo en el directorio CGI-BIN:

```
1 ^http://www[.]example[.]com/CGI-BIN/[0-9A-Za-z][0-9A-Za-z_
     .-]*[.](cgi|pl)$
2 <!--NeedCopy-->
```

- Permitir a los usuarios tener acceso a Microsoft Office y otros archivos de documento en el directorio docsarchive:

```
1 ^http://www[.]example[.]com/docsarchive/[0-9A-Za-z][0-9A-Za-z_
     -.]*[.](doc|xls|pdf|ppt)$
2 <!--NeedCopy-->
```

> **Nota**
>
> De forma predeterminada, todas las direcciones URL de Web App Firewall se consideran expresiones regulares.

Precaución: Las expresiones regulares son potentes. Especialmente si no está completamente familiarizado con las expresiones regulares con formato PCRE-format, compruebe las expresiones regulares que escriba. Asegúrese de que definen exactamente la URL que quiere agregar como excepción, y nada más. El uso descuidado de comodines, y especialmente de la combinación de metacarácter/-comodín de punto (

.*), puede tener resultados que no quiera, como bloquear el acceso al contenido web que no tenía intención de bloquear o permitir un ataque que la comprobación de URL de inicio habría bloqueado de otro modo.

> **Sugerencia**
>
> Puede agregar el *-y-* a la lista permitida de palabras clave SQL para el esquema de nomenclatura de URL. Por ejemplo, https://FQDN/bread-and-butter.

Denegar comprobación de URL

January 12, 2021

La comprobación Denegar URL examina y bloquea las conexiones a URL a las que suelen acceder los hackers y el código malintencionado. Esta comprobación contiene una lista de direcciones URL que son objetivos comunes de hackers o código malicioso y que rara vez aparecen en solicitudes legítimas. También puede agregar direcciones URL o patrones de URL a la lista. La comprobación Denegar URL evita ataques contra varios puntos débiles de seguridad que se sabe que existen en el software del servidor web o en muchos sitios web.

La comprobación Denegar URL tiene prioridad sobre la comprobación URL de inicio y, por lo tanto, deniega los intentos de conexión malintencionados incluso cuando una relajación de URL de inicio normalmente permitiría que una solicitud continúe.

En el cuadro de diálogo Modificar Denegar comprobación de URL, en la ficha General, puede habilitar o inhabilitar las acciones Bloquear, Registro y Estadísticas.

Si utiliza la interfaz de línea de comandos, puede introducir el siguiente comando para configurar Denegar comprobación de URL:

- `set appfw profile <name> -denyURLAction [**block**] [**log**] [**stats**] [**none**]`

Para crear y configurar sus propias URL de denegación, debe usar la GUI. En la ficha Comprobaciones del cuadro de diálogo Modificar comprobación de URL Denegar, haga clic en Agregar para abrir el cuadro de diálogo Agregar URL Denegar o seleccione una URL de denegación definida por el usuario existente y haga clic en Abrir para abrir el cuadro de diálogo Modificar URL Denegar. Cualquiera de los dos cuadros de diálogo proporciona las mismas opciones para crear y configurar una URL denegada.

A continuación se presentan ejemplos de expresiones Denegar URL:

- No permita que los usuarios accedan directamente al servidor de imágenes en images.example.com:


```
^http://images[.]example[.]com$
<!--NeedCopy-->
```

- No permita que los usuarios accedan directamente a los scripts CGI (.cgi) o PERL (.pl):

```
^http://www[.]example[.]com/([0-9A-Za-z][0-9A-Za-z_-]\*/)\*
[0-9A-Za-z][0-9A-Za-z_.-]*[.](cgi|pl)$
<!--NeedCopy-->
```

- Aquí está la misma URL de denegación, modificada para admitir caracteres no ASCII:

```
^http://www[.]example[.]com/(([0-9A-Za-z]|x[0-9A-Fa-f][0-9A-Fa-f
   ])
([0-9A-Za-z_-]|x[0-9A-Fa-f][0-9A-Fa-f])\*/)\*([0-9A-Za-z]|x[0-9A-
   Fa-f][0-9A-Fa-f])
([0-9A-Za-z_-]|x[0-9A-Fa-f][0-9A-Fa-f])*[.](cgi|pl)$
<!--NeedCopy-->
```

> **Precaución:**
>
> Las expresiones regulares son potentes. Especialmente si no está completamente familiarizado con las expresiones regulares con formato PCRE-format, compruebe las expresiones regulares que escriba. Asegúrese de que definen exactamente la URL o el patrón que quiere bloquear, y nada más. El uso descuidado de los comodines, y especialmente de la combinación de metacarácter/comodín de punto (.*), puede tener resultados que no quiera, como bloquear el acceso al contenido web que no pretendía bloquear.

Comprobaciones de protección XML

January 12, 2021

Las comprobaciones de Protección XML examinan las solicitudes de ataques basados en XML de todos los tipos.

> **Precaución:**
>
> Las comprobaciones de seguridad XML solo se aplican al contenido que se envía con un encabezado de tipo de contenido HTTP text/xml. Si falta el encabezado de tipo de contenido o se establece en un valor diferente, se omiten todas las comprobaciones de seguridad XML. Si

> planea proteger las aplicaciones web XML o Web 2.0, los webmasters de cada servidor web que hospeda esas aplicaciones deben asegurarse de que se envía el encabezado de tipo de contenido HTTP adecuado.

Comprobación de formato XML

January 12, 2021

La comprobación Formato XML examina el formato XML de las solicitudes entrantes y bloquea aquellas solicitudes que no están bien formadas o que no cumplen los criterios de la especificación XML para los documentos XML correctamente formados. Algunos de estos criterios son:

- Un documento XML debe contener solo caracteres Unicode codificados correctamente que coincidan con la especificación Unicode.
- No se pueden incluir en el documento caracteres especiales de sintaxis XML, como <, > y &, excepto cuando se utilizan en el marcado XML.
- Todas las etiquetas de elemento inicial, final y vacío deben estar anidadas correctamente, sin que falte ninguna o se superponga.
- Las etiquetas de elementos XML distinguen entre mayúsculas y minúsculas. Todas las etiquetas inicial y final deben coincidir exactamente.
- Un único elemento raíz debe contener todos los demás elementos del documento XML.

Un documento que no cumple los criterios de XML bien formado no cumple con la definición de un documento XML. Estrictamente hablando, no es XML. Sin embargo, no todas las aplicaciones XML y servicios web aplican el estándar XML bien formado, y no todas manejan XML mal formado o no válido correctamente. El manejo inadecuado de un documento XML mal formado puede provocar infracciones de seguridad. El objetivo de la comprobación de formato XML es evitar que un usuario malintencionado utilice una solicitud XML mal formada para violar la seguridad de su aplicación XML o servicio web.

Si utiliza el asistente o la GUI, en el cuadro de diálogo Modificar comprobación de formato XML, en la ficha General puede habilitar o inhabilitar las acciones Bloquear, Registro y Estadísticas.

Si utiliza la interfaz de línea de comandos, puede introducir el siguiente comando para configurar la comprobación de formato XML:

- `set appfw profile <name> -xmlFormatAction [**block**] [**log**] [**stats**] [**none**]`

No puede configurar excepciones a la comprobación Formato XML. Solo puede habilitarlo o inhabilitarlo.

Verificación de denegación de servicio XML

January 12, 2021

La comprobación XML Denegación de servicio (XML DoS o XDoS) examina las solicitudes XML entrantes para determinar si coinciden con las funciones de un ataque de denegación de servicio (DoS). Si hay una coincidencia, bloquea esas solicitudes. El propósito de la comprobación XML DoS es evitar que un atacante utilice solicitudes XML para iniciar un ataque de denegación de servicio en su servidor web o sitio web.

Si utiliza el asistente o la GUI, en el cuadro de diálogo Modificar comprobación de denegación de servicio XML, en la ficha **General** puede habilitar o inhabilitar las acciones Bloquear, Registrar, Estadísticas y Aprender:

Si utiliza la interfaz de línea de comandos, puede introducir el siguiente comando para configurar la comprobación de denegación de servicio XML:

- `set appfw profile <name> -xmlDoSAction [**block**] [**log**] [**learn**] [**stats**] [**none**]`

Para configurar reglas de denegación de servicio XML individuales, debe usar la GUI. En la ficha **Comprobaciones** del cuadro de diálogo **Modificar comprobación de denegación de servicio XML**, seleccione una regla y haga clic en **Abrir** para abrir el cuadro de diálogo **Modificar denegación de servicio XML** para esa regla. Los cuadros de diálogo individuales difieren en función de las diferentes reglas, pero son sencillos. Algunos solo permiten habilitar o inhabilitar la regla; otros permiten modificar un número escribiendo un nuevo valor en un cuadro de texto.

> **Nota:**
>
> El comportamiento esperado de Learning Engine para el ataque de denegación de servicio se basa en la acción configurada. Si la acción se establece como “Bloquear”, el motor aprende el valor de enlace configurado +1 y el análisis XML se detiene cuando hay una infracción. Si la acción configurada no se establece como “Bloquear”, el motor aprende el valor real de longitud de infracción entrante.

Las reglas de denegación de servicio XML individuales son:

- Profundidad máxima del elemento. Restringir el número máximo de niveles anidados en cada elemento individual a 256. Si esta regla está habilitada y Web App Firewall detecta una solicitud XML con un elemento que tiene más del número máximo de niveles permitidos, bloquea la solicitud. Puede modificar el número máximo de niveles a cualquier valor de uno (1) a 65.535.
- Longitud máxima del nombre del elemento. Restringe la longitud máxima de cada nombre de elemento a 128 caracteres. Esto incluye el nombre dentro del espacio de nombres expandido, que incluye la ruta XML y el nombre del elemento con el siguiente formato:


```
{
http://prefix.example.com/path/ }
target_page.xml
<!--NeedCopy-->
```

El usuario puede modificar la longitud máxima del nombre a cualquier valor entre un (1) carácter y 65.535.

- Número máximo de elementos. Restrinja el número máximo de cualquier tipo de elemento por documento XML a 65.535. Puede modificar el número máximo de elementos a cualquier valor entre uno (1) y 65.535.
- Número máximo de elementos secundarios. Restringir el número máximo de elementos secundarios (incluidos otros elementos, información de caracteres y comentarios) que cada elemento individual puede tener a 65.535. Puede modificar el número máximo de elementos secundarios a cualquier valor entre uno (1) y 65.535.
- Número máximo de atributos. Restringir el número máximo de atributos que cada elemento individual puede tener a 256. Puede modificar el número máximo de atributos a cualquier valor entre uno (1) y 256.
- Longitud máxima del nombre de atributo. Restringir la longitud máxima de cada nombre de atributo a 128 caracteres. Puede modificar la longitud máxima del nombre de atributo a cualquier valor entre uno (1) y 2.048.
- Longitud máxima del valor de atributo. Restringe la longitud máxima de cada valor de atributo a 2048 caracteres. Puede modificar la longitud máxima del nombre de atributo a cualquier valor entre uno (1) y 2.048.
- Longitud máxima de datos de caracteres. Restringir la longitud máxima de datos de caracteres para cada elemento a 65.535. Puede modificar la longitud a cualquier valor entre uno (1) y 65.535.
- Tamaño máximo de archivo. Restringir el tamaño de cada archivo a 20 MB. Puede modificar el tamaño máximo de archivo a cualquier valor.
- Tamaño mínimo de archivo. Requiere que cada archivo tenga una longitud mínima de 9 bytes. Puede modificar el tamaño mínimo de archivo a cualquier entero positivo que represente varios bytes.
- Número máximo de expansiones de entidad. Limite el número de expansiones de entidad permitidas al número especificado. Valor predeterminado: 1024.
- Profundidad máxima de expansión de entidad Restringir el número máximo de expansiones de entidades anidadas a no más del número especificado. Valor predeterminado: 32.

- Número máximo de espacios de nombres. Limite el número de declaraciones de espacio de nombres en un documento XML a no más del número especificado. Valor predeterminado: 16.
- Longitud máxima de URI del espacio de nombres. Limite la longitud de URL de cada declaración de espacio de nombres a no más del número especificado de caracteres. Valor predeterminado: 256.
- Instrucciones de procesamiento de bloques. Bloquee las instrucciones especiales de procesamiento incluidas en la solicitud. Esta regla no tiene valores modificables por el usuario.
- Bloquee DTD. Bloquee cualquier definición de tipo de documento (DTD) incluida con la solicitud. Esta regla no tiene valores modificables por el usuario.
- Bloquear entidades externas. Bloquear todas las referencias a entidades externas en la solicitud. Esta regla no tiene valores modificables por el usuario.
- Comprobación de matriz SOAP. Habilite o inhabilite las siguientes comprobaciones de matriz SOAP:
  - **Tamaño máximo de matriz SOAP.** El tamaño total máximo de todas las matrices SOAP en una solicitud XML antes de bloquear la conexión. Puede modificar este valor. Valor predeterminado: 20000000.
  - **Rango máximo de matriz SOAP.** Rango o dimensiones máximas de cualquier matriz SOAP única en una solicitud XML antes de bloquear la conexión. Puede modificar este valor. Valor predeterminado: 16.

Comprobación de scripts XML entre sitios

August 20, 2021

La comprobación XML Cross-Site Scripting examina las solicitudes de los usuarios para posibles ataques de scripts entre sitios en la carga útil XML. Si encuentra un posible ataque de scripts entre sitios, bloquea la solicitud.

Para evitar el uso indebido de los scripts de los servicios web protegidos para infringir la seguridad de sus servicios web, la comprobación XML Cross-Site Scripting bloquea los scripts que infrinjan la misma regla de origen, lo que indica que los scripts no deben tener acceso ni modificar el contenido de ningún servidor excepto el servidor en el que se encuentran. Cualquier script que infrinja la misma regla de origen se denomina script entre sitios, y la práctica de utilizar scripts para acceder o modificar contenido en otro servidor se denomina script entre sitios. La razón por la que los scripts entre sitios son un problema de seguridad es que un servidor web que permite la creación de scripts entre sitios puede ser atacado con un script que no está en ese servidor web, sino en un servidor web diferente, como uno propiedad y controlado por el atacante.

El Web App Firewall ofrece varias opciones de acción para implementar la protección de scripts XML entre sitios. Tiene la opción de configurar acciones **Bloquear**, **Registrar** y **Estadísticas**.

La comprobación de scripts entre sitios XML de Web App Firewall se realiza en la carga útil de las solicitudes entrantes y las cadenas de ataque se identifican incluso si están distribuidas en varias líneas. La comprobación busca cadenas de ataque de scripts entre sitios en el **elemento** y los valores de **atributo**. Puede aplicar relajantes para eludir la inspección de comprobación de seguridad bajo condiciones especificadas. Los registros y las estadísticas pueden ayudarle a identificar las relajantes necesarias.

La sección CDATA de la carga útil XML podría ser un área de enfoque atractiva para los hackers porque los scripts no son ejecutables fuera de la sección CDATA. Una sección CDATA se utiliza para el contenido que se va a tratar completamente como datos de caracteres. Los delimitadores de etiquetas de marca HTML **<**, **>** y **/>**no harán que el analizador interprete el código como elementos HTML. El siguiente ejemplo muestra una sección CDATA con cadena de ataque de scripts entre sitios:

```
1     <![CDATA[rn
2     <script language=”Javascript” type=”text/javascript”>alert (”Got
          you”)</script>rn
3     ]]>
4 <!--NeedCopy-->
```

Opciones de acción

Se aplica una acción cuando la comprobación de scripts entre sitios XML detecta un ataque de scripts entre sitios en la solicitud. Las siguientes opciones están disponibles para optimizar la protección de scripts XML entre sitios para su aplicación:

- **Bloquear**: la acción de bloqueo se desencadena si se detectan las etiquetas de scripts entre sitios en la solicitud.
- **Registro**: Genera mensajes de registro que indican las acciones realizadas por la comprobación XML Cross-Site Scripting. Si el bloque está inhabilitado, se genera un mensaje de registro independiente para cada ubicación (ELEMENT, ATTRIBUTE) en la que se detecta la infracción de scripts entre sitios. Sin embargo, solo se genera un mensaje cuando se bloquea la solicitud. Puede supervisar los registros para determinar si las respuestas a las solicitudes legítimas se están bloqueando. Un gran aumento en el número de mensajes de registro puede indicar intentos de lanzar un ataque.
- **Estadísticas**: Permite recopilar estadísticas sobre infracciones y registros. Un aumento inesperado en el contador de estadísticas podría indicar que su aplicación está siendo atacada. Si las solicitudes legítimas se bloquean, es posible que tenga que volver a visitar la configuración para ver si necesita configurar nuevas reglas de relajación o modificar las existentes.

Reglas de relajación

Si la aplicación requiere que omita la comprobación Cross-Site Scripting para un ELEMENT o ATTRIBUTE específico en la carga útil XML, puede configurar una regla de relajación. Las reglas de relajación de comprobación XML Cross-Site Scripting tienen los siguientes parámetros:

- **Name**—Puede utilizar cadenas literales o expresiones regulares para configurar el nombre del ELEMENTO o del Atributo. La siguiente expresión exime a todos los ELEMENTOS que comiencen con la cadena name_ seguida de una cadena de letras mayúsculas o minúsculas, o números, que tenga al menos dos y no más de quince caracteres de longitud:

  ```
  ^name_[0-9A-Za-z]{ 2,15 } $
  ```

> **Nota**
>
> Los nombres distinguen mayúsculas de minúsculas. No se permiten entradas duplicadas, pero puede utilizar mayúsculas y minúsculas de los nombres y las diferencias de ubicación para crear entradas similares. Por ejemplo, cada una de las siguientes reglas de relajación es única:
>
> 1. `XMLcross-site scripting: ABC IsRegex: NOTREGEX Location: ATTRIBUTE State: ENABLED`
> 2. `XMLcross-site scripting: ABC IsRegex: NOTREGEX Location: ELEMENT State: ENABLED`
> 3. `XMLcross-site scripting: abc IsRegex: NOTREGEX Location: ELEMENT State: ENABLED`
> 4. `XMLcross-site scripting: abc IsRegex: NOTREGEX Location: ATTRIBUTE State: ENABLED`

- **Ubicación**: Puede especificar la ubicación de la excepción Comprobación de scripts entre sitios en la carga XML. La opción ELEMENT está seleccionada de forma predeterminada. Puede cambiarlo a ATRIBUTO.
- **Comentario**: Se trata de un campo opcional. Puede utilizar hasta una cadena de 255 caracteres para describir el propósito de esta regla de relajación.

> **Advertencia**
>
> Las expresiones regulares son potentes. Especialmente si no está completamente familiarizado con las expresiones regulares con formato PCRE-format, compruebe las expresiones regulares que escriba. Asegúrese de que definen exactamente el nombre que quiere agregar como excepción, y nada más. El uso descuidado de expresiones regulares puede tener resultados que no quiera, como bloquear el acceso al contenido web que no tenía intención de bloquear o permitir un ataque que la comprobación de scripts XML entre sitios habría bloqueado de otro modo.

Comprobación Uso de la línea de comandos para configurar el script XML entre sitios

Para configurar XML Cross-Site Scripting, compruebe las acciones y otros parámetros mediante la línea de comandos

Si utiliza la interfaz de línea de comandos, puede introducir los siguientes comandos para configurar la comprobación de scripts entre sitios XML:

```
> set appfw profile <name> -XMLcross-site scriptingAction (([block] [log] [
stats])| [none])
```

Para configurar una regla de relajación de comprobación de scripts XML entre sitios mediante la línea de comandos

Puede agregar reglas de relajación para omitir la inspección de ataques de scripts entre sitios en una ubicación específica. Utilice el comando bind o unbind para agregar o eliminar el enlace de la regla de relajación, como se indica a continuación:

```
> bind appfw profile <name> -XMLcross-site scripting <string> [isRegex (
REGEX | NOTREGEX)] [-location ( ELEMENT | ATTRIBUTE )] -comment <string> [-
state ( ENABLED | DISABLED )]
```

```
> unbind appfw profile <name> -XMLcross-site scripting <String>
```

Ejemplo:

```
> bind appfw profile test_pr -XMLcross-site scripting ABC
```

Después de ejecutar el comando anterior, se configura la siguiente regla de relajación. La regla está habilitada, el nombre se trata como un literal (NOTREGEX) y ELEMENT se selecciona como la ubicación predeterminada:

```
1)      XMLcross-site scripting:  ABC             IsRegex:  NOTREGEX

        Location:  ELEMENT       State:  ENABLED

`> unbind appfw profile test_pr -XMLcross-site scripting abc`

ERROR: No such XMLcross-site scripting check

`> unbind appfw profile test_pr -XMLcross-site scripting ABC`

 Done
<!--NeedCopy-->
```


Uso de la GUI para configurar la comprobación de scripts XML entre sitios

En la GUI, puede configurar la comprobación de scripts XML entre sitios en el panel del perfil asociado a la aplicación.

Para configurar o modificar la comprobación XML Cross-Site Scripting mediante la interfaz gráfica de usuario

1. Vaya a **Web App Firewall** > **Perfiles**, resalte el perfil de destino y haga clic en **Modificar**.
2. En el panel Configuración avanzada, haga clic en **Comprobaciones de seguridad**.

La tabla de comprobación de seguridad muestra los valores de acción configurados actualmente para todas las comprobaciones de seguridad. Tiene 2 opciones para la configuración:

a) Si solo quiere habilitar o inhabilitar las acciones **Bloquear**, **Registrar** y **Estadísticas** para la **verificación XML Cross-Site Scripting**, puede activar o desactivar las casillas de verificación de la tabla, hacer clic en **Aceptar** y, a continuación, en Guardar y cerrar para cerrar el panel Comprobación de seguridad.

b) Puede hacer doble clic en **XML Cross-Site Scripting**, o seleccionar la fila y hacer clic en **Configuración de acción**, para mostrar las opciones de acción. Después de cambiar cualquiera de las opciones de acción, haga clic en **Aceptar** para guardar los cambios y volver a la tabla Comprobaciones de seguridad.

Puede proceder a configurar otras comprobaciones de seguridad si es necesario. Haga clic en **Aceptar** para guardar todos los cambios realizados en la sección Comprobaciones de seguridad y, a continuación, haga clic en **Guardar y cerrar** para cerrar el panel Comprobación de seguridad.

Para configurar una regla de relajación de scripts XML entre sitios mediante la interfaz gráfica de usuario

1. Vaya a **Web App Firewall** > **Perfiles**, resalte el perfil de destino y haga clic en **Modificar**.
2. En el panel **Configuración avanzada**, haga clic en **Reglas de relajación**.
3. En la tabla Reglas de relajación, haga doble clic en la entrada **XML Cross-Site Scripting**, o selecciónela y haga clic en **Modificar**.
4. En el cuadro de diálogo **Reglas de relajación de scripts entre sitios XML**, realice las operaciones **Agregar**, **Modificar**, **Eliminar**, **Habilitar** o **Inhabilitar** para las reglas de relajación.

Para administrar reglas de relajación de scripts XML entre sitios mediante el visualizador

Para obtener una vista consolidada de todas las reglas de relajación, puede resaltar la fila **XML Cross-Site Scripting** en la tabla Reglas de relajación y hacer clic en **Visualizador**. El visualizador para las relajaciones implementadas le ofrece la opción de **Agregar** una nueva regla o **Modificar** una existente. También puede **habilitar** o **inhabilitar** un grupo de reglas seleccionando un nodo y haciendo clic en los botones correspondientes en el visualizador de relajación.

Para ver o personalizar los patrones de scripts entre sitios mediante la interfaz gráfica de usuario

Puede utilizar la GUI para ver o personalizar la lista predeterminada de atributos permitidos de scripts entre sitios o etiquetas permitidas. También puede ver o personalizar la lista predeterminada de patrones denegados de scripts entre sitios.

Las listas predeterminadas se especifican en **Web App Firewall** > **Firmas** > **Firmas predeterminadas**. Si no enlaza ningún objeto de firma al perfil, el perfil utilizará la lista predeterminada de scripts entre sitios permitidos y denegados especificada en el objeto Firmas predeterminadas para el procesamiento de comprobación de seguridad de scripts entre sitios. Tags, Attributes y Patterns, especificados en el objeto de firmas predeterminado, son de solo lectura. No puede modificarlos ni modificarlos. Si quiere modificarlos o cambiarlos, realice una copia del objeto Signatures Default para crear un objeto Signatures definido por el usuario. Realice cambios en las listas Permitidas o Denegadas del nuevo objeto de firma definido por el usuario y utilice este objeto de firma en el perfil que está procesando el tráfico para el que quiere utilizar estas listas personalizadas permitidas y denegadas.

Para obtener más información acerca de las firmas, consulte http://support.citrix.com/proddocs/topic/ns-security-10-map/appfw-signatures-con.html.

Para ver los patrones predeterminados de scripts entre sitios:

1. Vaya a **Web App Firewall** > **Firmas**, seleccione ***Firmas predeterminadas** y haga clic en **Modificar**. A continuación, haga clic en **Administrar patrones de scripts SQL/entre sitios**.

La tabla **Administrar rutas de scripts SQL/entre sitios** muestra las siguientes tres filas pertenecientes a scripts entre sitios:

```
            xss/allowed/attribute

            xss/allowed/tag

            xss/denied/pattern
<!--NeedCopy-->
```

Seleccione una fila y haga clic en **Administrar elementos** para mostrar los elementos de scripts entre sitios correspondientes (etiqueta, atributo, patrón) utilizados por la comprobación de **scripts entre sitios del** Web App Firewall.

Para personalizar elementos de scripts entre sitios: Puede modificar el objeto de firma definido por el usuario para personalizar la etiqueta permitida, los atributos permitidos y los patrones denegados. Puede agregar nuevas entradas o eliminar las existentes.

1. **Vaya a Web App Firewall** > **Firmas**, resalte la firma definida por el usuario de destino y haga clic en **Modificar**. Haga clic en **Administrar patrones de scripts SQL/entre sitios** para mostrar la tabla **Administrar rutas de scripting SQL/sitios cruzados**.
2. Seleccione la fila de scripts entre sitios de destino.

a) Haga clic en **Administrar elementos**, para **Agregar**, **Modificar** o **Quitar** el elemento de scripting entre sitios correspondiente.

b) Haga clic en **Eliminar** para eliminar la fila seleccionada.

> **Advertencia**
>
> Tenga mucho cuidado al quitar o modificar cualquier elemento predeterminado de scripts entre sitios, o elimine la ruta de scripts entre sitios para eliminar toda la fila. Las firmas, la comprobación de seguridad HTML Cross-Site Scripting y la comprobación de seguridad XML Cross-Site Scripting se basan en estos elementos para detectar ataques con el fin de proteger las aplicaciones. La personalización de los elementos de scripts entre sitios puede hacer que la aplicación sea vulnerable a ataques de scripts entre sitios si se elimina el patrón necesario durante la edición.

Uso de la función de registro con la comprobación de scripts XML entre sitios

Cuando se habilita la acción de registro, las infracciones de comprobación de seguridad de scripts entre sitios XML se registran en el registro de auditoría como infracciones de **scripts entre sitios de Appfw_XML_cross-site**. El Web App Firewall admite los formatos de registro nativo y CEF. También puede enviar los registros a un servidor syslog remoto.

Para acceder a los mensajes de registro mediante la línea de comandos

Cambie al shell y siga los ns.logs en la carpeta /var/log/ para acceder a los mensajes de registro correspondientes a las infracciones XML Cross-Site Scripting:

```
> \*\*Shell\*\*

> \*\*tail -f /var/log/ns.log | grep APPFW_XML_cross-site scripting\*\*
<!--NeedCopy-->
```

Ejemplo de un mensaje de registro de infracción de comprobación de seguridad de scripts XML entre sitios en formato de registro nativo que muestra la acción <blocked>

```
Oct  7 01:44:34 <local0.warn> 10.217.31.98 10/07/2015:01:44:34 GMT ns
    0-PPE-1 : default APPFW APPFW_XML_cross-site scripting 1154 0 :
    10.217.253.69 3466-PPE1 - owa_profile http://10.217.31.101/FFC/login
    .html Cross-site script check failed for field script=”Bad tag:
    script” <\*\*blocked\*\*>
<!--NeedCopy-->
```


Ejemplo de un mensaje de registro de infracción de comprobación de seguridad XML Cross-Site Scripting en formato de registro CEF que muestra la acción <not blocked>

```
1 Oct  7 01:46:52 <local0.warn> 10.217.31.98 CEF:0|Citrix|Citrix ADC|NS11
     .0|APPFW|APPFW_XML_cross-site scripting|4|src=10.217.30.17
     geolocation=Unknown spt=33141 method=GET request=http://
     10.217.31.101/FFC/login.html msg=Cross-site script check failed for
     field script=”Bad tag: script” cn1=1607 cn2=3538 cs1=owa_profile cs2
     =PPE0 cs4=ERROR cs5=2015 act=\*\*not blocked\*\*
2 <!--NeedCopy-->
```

Para acceder a los mensajes de registro mediante la interfaz gráfica de usuario

La GUI de Citrix incluye una herramienta útil (**Syslog Viewer**) para analizar los mensajes de registro. Tiene varias opciones para acceder al Visor de Syslog:

- Vaya a **Web App Firewall** > **Perfiles**, seleccione el perfil de destino y haga clic en **Comprobaciones de seguridad**. Resalte la fila **XML Cross-Site Scripting** y haga clic en **Registros**. Cuando accede a los registros directamente desde la comprobación XML Cross-Site Scripting del perfil, la GUI filtra los mensajes de registro y muestra solo los registros correspondientes a estas infracciones de comprobación de seguridad.
- También puede acceder al Visor de Syslog navegando a **Citrix ADC** > **Sistema** > **Auditoría**. En la sección Mensajes de auditoría, haga clic en el vínculo Mensajes de Syslog para mostrar el Visor de Syslog, que muestra todos los mensajes de registro, incluidos otros registros de infracciones de comprobación de seguridad. Esto es útil para depurar cuando se pueden desencadenar varias infracciones de comprobación de seguridad durante el procesamiento de solicitudes.
- Desplácese hasta **Web App Firewall** > **Directivas** > **Auditoría**. En la sección **Mensajes de auditoría**, haga clic en el enlace **Mensajes de syslog** para mostrar el Visor de Syslog, que muestra todos los mensajes de registro, incluidos otros registros de infracciones de comprobación de seguridad.

El Visor de Syslog basado en XML proporciona varias opciones de filtro para seleccionar solo los mensajes de registro que le interesan. Para seleccionar mensajes de registro para la comprobación **XML Cross-Site Scripting**, filtre seleccionando **APTFW** en las opciones desplegables del **módulo**. La lista **Tipo de evento** ofrece un amplio conjunto de opciones para refinar aún más su selección. Por ejemplo, si activa la casilla de verificación **Appfw_XML_cross-site scripting** y hace clic en el botón **Aplicar**, solo aparecerán los mensajes de registro correspondientes a las infracciones de comprobación de seguridad de scripts entre sitios XML en el Visor de syslog.

Si coloca el cursor en la fila de un mensaje de registro específico, aparecen varias opciones, como **Módulo**, **Tipo de evento, Id.**de evento,**IP de cliente**, etc., debajo del mensaje de registro. Puede

seleccionar cualquiera de estas opciones para resaltar la información correspondiente en el mensaje de registro.

Estadísticas de las infracciones de scripts entre sitios XML

Cuando la acción de estadísticas está habilitada, el contador de la comprobación XML Cross-Site Scripting se incrementa cuando el Web App Firewall realiza cualquier acción para esta comprobación de seguridad. Las estadísticas se recopilan para Rate and Total count para Tráfico, Violaciones y Registros. El tamaño de un incremento del contador de registro puede variar en función de la configuración configurada. Por ejemplo, si la acción de bloqueo está habilitada, una solicitud de una página que contiene tres infracciones de scripts XML entre sitios aumenta el contador de estadísticas en uno, porque la página se bloquea tan pronto como se detecta la primera infracción. Sin embargo, si el bloque está inhabilitado, el procesamiento de la misma solicitud aumenta en tres el contador de estadísticas para infracciones y los registros, ya que cada infracción genera un mensaje de registro independiente.

Para mostrar las estadísticas de comprobación de scripts XML entre sitios mediante la línea de comandos

En el símbolo del sistema, escriba:

```
> **sh appfw stats**
```

Para mostrar las estadísticas de un perfil específico, utilice el siguiente comando:

```
> **stat appfw profile** <profile name>
```

Para mostrar estadísticas XML Cross-Site Scripting mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **Seguridad** > **Web App Firewall**.
2. En el panel derecho, acceda al enlace de **estadísticas** .
3. Utilice la barra de desplazamiento para ver las estadísticas sobre las infracciones y los registros de scripts entre sitios XML. La tabla de estadísticas proporciona datos en tiempo real y se actualiza cada 7 segundos.

Comprobación de inyección XML SQL

August 20, 2021

La comprobación de inyección XML SQL examina las solicitudes del usuario para posibles ataques de inyección SQL XML. Si encuentra SQL inyectado en cargas XML, bloquea las solicitudes.

Un ataque XML SQL puede inyectar código fuente en una aplicación web de modo que pueda interpretarse y ejecutarse como una consulta SQL válida para realizar una operación de base de datos con in-

tención malintencionada. Por ejemplo, los ataques XML SQL se pueden iniciar para obtener acceso no autorizado al contenido de una base de datos o para manipular los datos almacenados. Los ataques XML SQL Injection no solo son comunes, sino que también pueden ser muy dañinos y costosos.

La compartimentación de los privilegios de los usuarios de la base de datos puede ayudar a proteger la base de datos hasta cierto punto. Todos los usuarios de bases de datos solo deben tener los privilegios necesarios para completar las tareas previstas, de modo que no puedan ejecutar consultas SQL para realizar otras tareas. Por ejemplo, no se debe permitir a un usuario de solo lectura escribir o manipular tablas de datos. La comprobación Web App Firewall XML SQL Injection inspecciona todas las solicitudes XML para proporcionar defensas especiales contra la inyección de código SQL no autorizado que podría romper la seguridad. Si Web App Firewall detecta código SQL no autorizado en cualquier solicitud XML de cualquier usuario, puede bloquear la solicitud.

Citrix Web App Firewall inspecciona la presencia de palabras clave SQL y caracteres especiales para identificar el ataque de inyección SQL XML. Un conjunto predeterminado de palabras clave y caracteres especiales proporciona palabras clave conocidas y caracteres especiales que se utilizan comúnmente para lanzar ataques SQL XML. El Web App Firewall considera tres caracteres, comilla simple (‘), barra invertida () y punto y coma (;) como caracteres especiales para el procesamiento de comprobaciones de seguridad SQL. Puede agregar nuevos patrones y modificar el conjunto predeterminado para personalizar la inspección de comprobación SQL XML.

Web App Firewall ofrece varias opciones de acción para implementar la protección XML SQL Injection. Puede **bloquear** la solicitud, **registrar** un mensaje en el archivo ns.log con detalles sobre las violaciones observadas y recopilar **estadísticas** para realizar un seguimiento del número de ataques observados.

Además de las acciones, hay varios parámetros que se pueden configurar para el procesamiento de inyección XML SQL. Puede comprobar si hay **caracteres comodín SQL**. Puede cambiar el tipo XML SQL Injection y seleccionar una de las 4 opciones (**SQLKeyword**, **SQLPlChar**, **SQLSPlCharandKeyword**, **SQLSPlCharorKeyword**) para indicar cómo evaluar las palabras clave SQL y los caracteres especiales SQL al procesar el XML carga útil. El parámetro XML **SQL Comments Handling** ofrece una opción para especificar el tipo de comentarios que deben inspeccionarse o eximirse durante la detección de XML SQL Injection.

Puede implementar relajantes para evitar falsos positivos. La comprobación XML SQL de Web App Firewall se realiza en la carga útil de las solicitudes entrantes, y las cadenas de ataque se identifican incluso si se distribuyen en varias líneas. La comprobación busca cadenas de SQL Injection en el **elemento** y los valores de **atributo**. Puede aplicar relajantes para eludir la inspección de comprobación de seguridad bajo condiciones especificadas. Los registros y las estadísticas pueden ayudarle a identificar las relajantes necesarias.

Opciones de acción

Se aplica una acción cuando la comprobación de inyección SQL XML detecta una cadena de ataque de inyección SQL en la solicitud. Las siguientes acciones están disponibles para configurar una protección optimizada XML SQL Injection para su aplicación:

Bloque: Si habilita el bloque, la acción de bloque se activa solo si la entrada coincide con la especificación del tipo de inyección XML SQL. Por ejemplo, si **SQLSplCharandKeyword** está configurado como el tipo de inyección SQL XML, una solicitud no se bloquea si no contiene palabras clave, incluso si se detectan caracteres especiales de SQL en la carga útil. Tal solicitud se bloquea si el tipo de inyección XML SQL se establece en **SQLSplChar**o **SQLsPlCharorKeyword**.

Log: Si habilita la función de registro, la comprobación XML SQL Injection genera mensajes de registro que indican las acciones que realiza. Si el bloque está inhabilitado, se genera un mensaje de registro independiente para cada ubicación (**ELEMENT**, **ATTRIBUTE**) en la que se detectó la infracción SQL XML. Sin embargo, solo se genera un mensaje cuando se bloquea la solicitud. Puede supervisar los registros para determinar si las respuestas a las solicitudes legítimas se están bloqueando. Un gran aumento en el número de mensajes de registro puede indicar intentos de lanzar un ataque.

Estadísticas: Si está activada, la función de estadísticas recopila estadísticas sobre infracciones y registros. Un aumento inesperado en el contador de estadísticas podría indicar que su aplicación está siendo atacada. Si las solicitudes legítimas se bloquean, es posible que tenga que volver a visitar la configuración para ver si necesita configurar nuevas reglas de relajación o modificar las existentes.

Parámetros XML SQL

Además de las acciones de bloque, registro y estadísticas, puede configurar los siguientes parámetros para la comprobación XML SQL Injection:

Comprobar caracteres comodín SQL XML: Los caracterescomodín se pueden utilizar para ampliar las selecciones de una instrucción SQL-SELECT (lenguaje de consulta estructurado). Estos operadores de comodín se pueden utilizar junto con los operadores **LIKE** y **NOT LIKE** para comparar un valor con valores similares. Los caracteres de porcentaje (%) y subrayado (_) se utilizan con frecuencia como comodines. El signo de porcentaje es análogo al carácter comodín de asterisco (*) utilizado con MS-DOS y para hacer coincidir cero, uno o varios caracteres en un campo. El guión bajo es similar al signo de interrogación de MS-DOS (?) carácter comodín. Coincide con un único número o carácter en una expresión.

Por ejemplo, puede utilizar la siguiente consulta para realizar una búsqueda de cadenas para buscar todos los clientes cuyos nombres contengan el carácter D.

```
SELECT * from customer WHERE name like "%D%"
```

En el ejemplo siguiente se combinan los operadores para buscar cualquier valor de salario que tenga 0 como segundo y tercer carácter.


```
SELECT * from customer WHERE salary like '_00%
```

Diferentes proveedores de DBMS han ampliado los caracteres comodín agregando operadores adicionales. Citrix Web App Firewall puede protegerse contra los ataques que se inician mediante la inyección de estos caracteres comodín. Los 5 caracteres comodín predeterminados son porcentaje (%), guión bajo (_), intercalación (^), corchete de apertura ([) y corchete de cierre (]). Esta protección se aplica tanto a perfiles HTML como XML.

Los caracteres comodín predeterminados son una lista de literales especificados en la ***Firmas predeterminadas**:

```
1 -  <wildchar type=" LITERAL" >%</wildchar>
2 -  <wildchar type=" LITERAL" >_</wildchar>
3 -  <wildchar type=" LITERAL" >^</wildchar>
4 -  <wildchar type=" LITERAL" >[</wildchar>
5 -  <wildchar type=" LITERAL" >]</wildchar>
6 <!--NeedCopy-->
```

Los caracteres comodín de un ataque pueden ser PCRE, como [^A-F]. El Web App Firewall también admite comodines PCRE, pero los caracteres comodín literales anteriores son suficientes para bloquear la mayoría de los ataques.

> **Nota**
>
> La comprobación de **caracteres comodín** SQL XML es diferente de la comprobación de **caracteres especiales** XML SQL. Esta opción debe utilizarse con precaución para evitar falsos positivos.

Check Request Conteniendo SQL Injection Type: Web App Firewall proporciona 4 opciones para implementar el nivel deseado de rigor para la inspección de SQL Injection, en función de las necesidades individuales de la aplicación. La solicitud se comprueba con la especificación de tipo de inyección para detectar infracciones SQL. Las 4 opciones de tipo de inyección SQL son:

- **Caracteres y palabra clave especiales**de SQL: Tanto una palabra clave SQL como un carácter especial SQL deben estar presentes en la ubicación inspeccionada para desencadenar una infracción SQL. Esta configuración menos restrictiva es también la predeterminada.
- **Character especial de SQL**: Al menos uno de los caracteres especiales debe estar presente en la cadena de carga procesada para desencadenar una infracción SQL.
- **Palabra clave SQL**: Al menos una de las palabras clave SQL especificadas debe estar presente en la cadena de carga procesada para desencadenar una infracción SQL. No seleccione esta opción sin tener debidamente en cuenta. Para evitar falsos positivos, asegúrese de que no se espera ninguna de las palabras clave en las entradas.
- **Character especial o palabra clave de SQL**: La palabra clave o la cadena de caracteres especiales deben estar presentes en la carga útil para desencadenar la infracción de comprobación

de seguridad.

> **Sugerencia**
>
> Si selecciona la opción Carácter especial de SQL, el Web App Firewall omite las cadenas que no contienen caracteres especiales. Dado que la mayoría de los servidores SQL no procesan comandos SQL que no están precedidos por un carácter especial, la habilitación de esta opción puede reducir significativamente la carga en el Web App Firewall y acelerar el procesamiento sin poner en riesgo los sitios web protegidos.

Manejo de comentarios SQL: De forma predeterminada, Web App Firewall analiza y comprueba todos los comentarios de los datos XML en busca de comandos SQL inyectados. Muchos servidores SQL ignoran cualquier cosa en un comentario, incluso si están precedidos por un carácter especial SQL. Para un procesamiento más rápido, si el servidor XML SQL ignora los comentarios, puede configurar Web App Firewall para que omita los comentarios al examinar las solicitudes de SQL inyectado. Las opciones de manejo de comentarios SQL XML son:

- **ANSI**—Omitir comentarios SQL con formato ANSI, que normalmente son utilizados por bases de datos SQL basadas en UNIX.
- **Anidado**: Omita los comentarios de SQL anidados, que normalmente utiliza Microsoft SQL Server.
- **ANSI/anidado**: Omite los comentarios que se ajustan a los estándares de comentarios ANSI y SQL anidados. Los comentarios que solo coinciden con el estándar ANSI, o solo el estándar anidado, se siguen comprobando si se inyecta SQL.
- **Comprobar todos los comentarios**: Comprueba toda la solicitud de SQL inyectado, sin omitir nada. Esta es la opción predeterminada.

> **Sugerencia**
>
> En la mayoría de los casos, no debe elegir la opción Anidada o ANSI/anidada a menos que la base de datos back-end se ejecute en Microsoft SQL Server. La mayoría de los otros tipos de software de SQL Server no reconocen los comentarios anidados. Si aparecen comentarios anidados en una solicitud dirigida a otro tipo de servidor SQL, pueden indicar un intento de violar la seguridad en ese servidor.

Reglas de relajación

Si la aplicación requiere que omita la inspección XML SQL Injection para un ELEMENT o ATTRIBUTE específico en la carga útil XML, puede configurar una regla de relajación. Las reglas de relajación de inspección XML SQL Injection tienen los siguientes parámetros:

- **Nombre:** Puede utilizar cadenas literales o expresiones regulares para configurar el nombre del **ELEMENTO** o del **ATTRIBUTE**. La siguiente expresión exime a todos los **ELEMENTOS** que empiecen por la cadena **PurchaseOrder_** seguida de una cadena de números que tenga al menos

dos y no más de diez caracteres de longitud:

Comentario: “Exención de Comprobación SQL XML para Elementos de Pedido de Compra”

```
    XMLSQLInjection:  ”PurchaseOrder_[0-9A-Za-z]{
 2,10 }
 ”

    IsRegex:  REGEX          Location:  ELEMENT

    State:  ENABLED
<!--NeedCopy-->
```

Nota: Los nombres distinguen entre mayúsculas y minúsculas. No se permiten entradas duplicadas, pero puede utilizar mayúsculas y minúsculas de los nombres y las diferencias de ubicación para crear entradas similares. Por ejemplo, cada una de las siguientes reglas de relajación es única:

```
1)      XMLSQLInjection:  XYZ    IsRegex:  NOTREGEX

        Location:  ELEMENT       State:  ENABLED

2)      XMLSQLInjection:  xyz    IsRegex:  NOTREGEX

        Location:  ELEMENT       State:  ENABLED

3)      XMLSQLInjection:  xyz    IsRegex:  NOTREGEX

        Location:  ATTRIBUTE     State:  ENABLED

4)      XMLSQLInjection:  XYZ    IsRegex:  NOTREGEX

        Location:  ATTRIBUTE     State:  ENABLED
<!--NeedCopy-->
```

- **Ubicación**: Puede especificar la ubicación de la excepción Inspección SQL XML en la carga útil XML. La opción **ELEMENT** está seleccionada de forma predeterminada. Puede cambiarlo a **ATRIBUTO**.
- **Comentario**: Este es un campo opcional. Puede utilizar hasta una cadena de 255 caracteres para describir el propósito de esta regla de relajación.

> **Advertencia**
>
> Las expresiones regulares son potentes. Especialmente si no está completamente familiarizado con las expresiones regulares con formato PCRE-format, compruebe las expresiones regulares que escriba. Asegúrese de que definen exactamente el nombre que quiere agregar como excepción, y nada más. El uso descuidado de expresiones regulares puede tener resultados que no quiera, como bloquear el acceso al contenido web que no tenía intención de bloquear o permitir un ataque que la inspección XML SQL Injection habría bloqueado de otro modo.

Uso de la línea de comandos para configurar XML SQL Injection Check

Para configurar acciones de inyección SQL XML y otros parámetros mediante la línea de comandos:

En la interfaz de línea de comandos, puede utilizar el comando **set appfw profile** o el comando **add appfw profile** para configurar las protecciones XML SQL Injection. Puede habilitar las acciones de bloqueo, registro y estadísticas. Seleccione el tipo de patrón de ataque SQL (palabras clave, caracteres comodín, cadenas especiales) que quiere detectar en las cargas útiles. Utilice el comando **unset appfw profile** para revertir la configuración configurada a sus valores predeterminados. Cada uno de los comandos siguientes establece un solo parámetro, pero puede incluir varios parámetros en un solo comando:

- `set appfw profile <name> **-XMLSQLInjectionAction** ([block] [log] [stats])| [none])`
- `set appfw profile <name> -XMLSQLInjectionCheckSQLWildChars (ON |OFF)`
- `set appfw profile <name> -XMLSQLInjectionType ([SQLKeyword] | [SQLSplChar] | [SQLSplCharANDKeyword] | [SQLSplCharORKeyword])`
- `set appfw profile <name> -XMLSQLInjectionParseComments ([checkall] | [ansi|nested] | [ansinested])`

Para configurar una regla de relajación de SQL Injection mediante la línea de comandos

Utilice el comando enlazar o desenlazar para agregar o eliminar reglas de relajación, como se indica a continuación:

```
1 - bind appfw profile <name> -XMLSQLInjection <string> [isRegex (REGEX
    | NOTREGEX)] [-location ( ELEMENT | ATTRIBUTE )] -comment <string>
    [-state ( ENABLED | DISABLED )]
2 - unbind appfw profile <name> -XMLSQLInjection <String>
3 <!--NeedCopy-->
```

Ejemplo:


```
> bind appfw profile test_profile -XMLSQLInjection ”PurchaseOrder_[0-9A-Za-z]{2,15 }” -isregex REGEX -location ATTRIBUTE

> unbind appfw profile test_profile  - XMLSQLInjection ”PurchaseOrder_[0-9A-Za-z]{2,15 }” -location ATTRIBUTE
<!--NeedCopy-->
```

Uso de la GUI para configurar la comprobación de seguridad de inyección XMLSQL

En la GUI, puede configurar la comprobación de seguridad XML SQL Injection en el panel para el perfil asociado a la aplicación.

Para configurar o modificar la comprobación XML SQL Injection mediante la interfaz gráfica de usuario

1. Vaya a **Web App Firewall** > **Perfiles**, resalte el perfil de destino y haga clic en **Modificar**.
2. En el panel Configuración avanzada, haga clic en **Comprobaciones de seguridad**.

La tabla de comprobación de seguridad muestra los valores de acción configurados actualmente para todas las comprobaciones de seguridad. Tiene 2 opciones para la configuración:

a. Si solo quiere habilitar o inhabilitar las acciones Bloquear, Registrar y Estadísticas para XML SQL Injection, puede activar o desactivar las casillas de verificación de la tabla, hacer clic en Aceptar y, a continuación, en Guardar y cerrar para cerrar el panel Comprobación de seguridad.

b. Si quiere configurar opciones adicionales para esta comprobación de seguridad, haga doble clic en Inyección SQL XML o seleccione la fila y haga clic en **Configuración de acción** para mostrar las siguientes opciones:

Comprobar caracteres comodín SQL: considere los caracteres comodín SQL en la carga útil como patrones de ataque.

Comprobar solicitud que contiene: Tipo de inyección SQL (SQLKeyWord, SQLSPlchar, SQLSPlcharAndKeyword o SQLSPLCharOrKeyword) que se va a comprobar.

Control decomentarios SQL: Tipo de comentarios (Comprobar todos los comentarios, ANSI, anidados o anidados) que se van a comprobar.

Después de cambiar cualquiera de los parámetros anteriores, haga clic en **Aceptar** para guardar los cambios y volver a la tabla Comprobaciones de seguridad. Puede proceder a configurar otras comprobaciones de seguridad si es necesario. Haga clic en **Aceptar** para guardar todos los cambios real-

izados en la sección Comprobaciones de seguridad y, a continuación, haga clic en **Guardar** y **cerrar** para cerrar el panel Comprobación de seguridad.

Para configurar una regla de relajación XML SQL Injection mediante la interfaz gráfica de usuario

1. Vaya a **Web App Firewall** > **Perfiles**, resalte el perfil de destino y haga clic en **Modificar**.
2. En el panel **Configuración avanzada**, haga clic en **Reglas de relajación**.
3. En la tabla Reglas de relajación, haga doble clic en la entrada **XML SQL Injection**, o selecciónela y haga clic en **Modificar**.
4. En el cuadro de diálogo **Reglas de relajación de inyección SQL XML**, realice las operaciones **Agregar**, **Modificar**, **Eliminar**, **Habilitar** o **Inhabilitar** para las reglas de relajación.

Para administrar reglas de relajación de inyección SQL XML mediante el visualizador

Para obtener una vista consolidada de todas las reglas de relajación, puede resaltar la fila **Inyección SQL XML** en la tabla Reglas de relajación y hacer clic en **Visualizador**. El visualizador para las relajaciones implementadas le ofrece la opción de **Agregar** una nueva regla o **Modificar** una existente. También puede **habilitar** o **inhabilitar** un grupo de reglas seleccionando un nodo y haciendo clic en los botones correspondientes en el visualizador de relajación.

Para ver o personalizar los patrones de SQL Injection mediante la GUI:

Puede utilizar la GUI para ver o personalizar los patrones SQL.

Los patrones SQL predeterminados se especifican en **Web App Firewall** > **Firmas** > ***Firmas predeterminadas**. Si no vincula ningún objeto de firma al perfil, el perfil utilizará los patrones SQL predeterminados especificados en el objeto Firmas predeterminadas para el procesamiento de comprobación de seguridad XML SQL Injection. Las reglas y patrones del objeto Signatures Default son de solo lectura. No puede modificarlos ni modificarlos. Si quiere modificar o cambiar estos patrones, cree un objeto de firma definido por el usuario realizando una copia del objeto Signatures Default y cambiando los patrones SQL. Utilice el objeto de firma definido por el usuario en el perfil que procesa el tráfico para el que quiere utilizar estos patrones SQL personalizados.

Para obtener más información, consulte Firmas.

Para ver patrones SQL predeterminados:

a. Vaya a **Web App Firewall** > **Firmas**, seleccione ***Firmas predeterminadas** y haga clic en **Modificar**. A continuación, haga clic en **Administrar patrones de scripts SQL/entre sitios**.

La tabla Administrar rutas de scripting SQL/Cross-Site muestra las siguientes cuatro filas pertenecientes a la inyección SQL:

```
1 Injection (not_alphanum, SQL)/ Keyword
2
3 Injection (not_alphanum, SQL)/ specialstring
```



```
4
5 Injection (not_alphanum, SQL)/ transformrules/transform
6
7 Injection (not_alphanum, SQL)/ wildchar
8 <!--NeedCopy-->
```

b. Seleccione una fila y haga clic en **Administrar elementos** para mostrar los patrones SQL correspondientes (palabras clave, cadenas especiales, reglas de transformación o caracteres comodín) utilizados por la comprobación de inyección SQL de Web App Firewall.

Para personalizar patrones SQL: puede modificar un objeto de firma definido por el usuario para personalizar las palabras clave SQL, cadenas especiales y caracteres comodín. Puede agregar nuevas entradas o eliminar las existentes. Puede modificar las reglas de transformación para las cadenas especiales de SQL.

a. Vaya a **Web App Firewall** > **Firmas**, resalte la firma definida por el usuario de destino y haga clic en **Modificar**. Haga clic en **Administrar patrones de scripts SQL/entre sitios** para mostrar la tabla **Administrar rutas de scripting SQL/sitios cruzados**.

b. Seleccione la fila SQL de destino.

i. Haga clic en **Administrar elementos**para **agregar**, **modificar**o **quitar**el elemento SQL correspondiente.

ii. Haga clic en **Quitar** para eliminar la fila seleccionada.

> **Advertencia**
>
> Debe tener mucho cuidado al quitar o modificar cualquier elemento SQL predeterminado, o eliminar la ruta SQL para eliminar toda la fila. Las reglas de firma, así como la comprobación de seguridad XML SQL Injection, se basan en estos elementos para detectar ataques de SQL Injection y proteger sus aplicaciones. Personalizar los patrones SQL puede hacer que la aplicación sea vulnerable a los ataques SQL XML si se quita el patrón requerido durante la edición.

Uso de la función de registro con la comprobación de inyección XML SQL

Cuando se habilita la acción de registro, las infracciones de comprobación de seguridad de **XML SQL Injection** se registran en el registro de auditoría como infracciones de **APTFW_XML_SQL**. El Web App Firewall admite los formatos de registro nativo y CEF. También puede enviar los registros a un servidor syslog remoto.

Para acceder a los mensajes de registro mediante la línea de comandos:

Cambie al shell y siga los ns.logs en la carpeta /var/log/ para acceder a los mensajes de registro correspondientes a las infracciones XML Cross-Site Scripting:


```
> Shell

> tail -f /var/log/ns.log | grep APPFW_XML_SQL
<!--NeedCopy-->
```

Para acceder a los mensajes de registro mediante la interfaz gráfica de usuario

La GUI de Citrix incluye una herramienta útil (Visor de syslog) para analizar los mensajes de registro. Tiene varias opciones para acceder al Visor de Syslog:

- Vaya a **Web App Firewall** > **Perfiles**, seleccione el perfil de destino y haga clic en **Comprobaciones de seguridad**. Resalte la fila **XML SQL Injection** y haga clic en **Registros**. Cuando accede a los registros directamente desde la comprobación de XML SQL Injection del perfil, la GUI filtra los mensajes de registro y muestra solo los registros correspondientes a estas infracciones de comprobación de seguridad.
- También puede acceder al Visor de Syslog navegando a **Sistema** > **Auditoría**. En la sección Mensajes de auditoría, haga clic en el enlace **Mensajes de syslog** para mostrar el Visor de Syslog, que muestra todos los mensajes de registro, incluidos otros registros de infracciones de comprobación de seguridad. Esto es útil para depurar cuando se pueden desencadenar varias infracciones de comprobación de seguridad durante el procesamiento de solicitudes.
- Vaya a **Web App Firewall** > **Directivas** > **Auditoría**. En la sección Mensajes de auditoría, haga clic en el vínculo **Mensajes de Syslog** para mostrar el **Visor de Syslog**, que muestra todos los mensajes de registro, incluidos otros registros de infracciones de comprobación de seguridad.

El Visor de Syslog basado en XML proporciona varias opciones de filtro para seleccionar solo los mensajes de registro que le interesan. Para seleccionar mensajes de registro para la comprobación **XML SQL Injection**, filtre seleccionando **APTFW** en las opciones desplegables para **Módulo**. La lista **Tipo de evento** ofrece un amplio conjunto de opciones para refinar aún más su selección. Por ejemplo, si activa la casilla de verificación **APTFW_XML_SQL** y hace clic en el botón **Aplicar**, solo aparecerán mensajes de registro relacionados con las infracciones de comprobación de seguridad de **XML SQL Injection** en el Visor de Syslog.

Si coloca el cursor en la fila de un mensaje de registro específico, debajo del mensaje de registro aparecen varias opciones, como **Módulo**, **Tipo**de **evento, Id.**de evento e **IP de cliente**. Puede seleccionar cualquiera de estas opciones para resaltar la información correspondiente en el mensaje de registro.

Estadísticas de las infracciones de inyección XML SQL

Cuando la acción de estadísticas está habilitada, el contador para la comprobación **XML SQL Injection** se incrementa cuando el Web App Firewall realiza cualquier acción para esta comprobación de seguridad. Las estadísticas se recopilan para Rate and Total count para Tráfico, Violaciones y Registros. El

tamaño de un incremento del contador de registro puede variar en función de la configuración configurada. Por ejemplo, si la acción de bloqueo está habilitada, una solicitud de una página que contiene tres infracciones de **Inyección SQL XML** incrementa el contador de estadísticas en uno, porque la página se bloquea tan pronto como se detecta la primera infracción. Sin embargo, si el bloque está inhabilitado, el procesamiento de la misma solicitud aumenta en tres el contador de estadísticas para infracciones y los registros, ya que cada infracción genera un mensaje de registro independiente.

Para mostrar las estadísticas de comprobación de XML SQL Injection mediante la línea de comandos

En el símbolo del sistema, escriba:

```
> sh appfw stats
```

Para mostrar las estadísticas de un perfil específico, utilice el siguiente comando:

```
> stat appfw profile <profile name>
```

Para mostrar las estadísticas de XML SQL Injection mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **Seguridad** > **Web App Firewall**.
2. En el panel derecho, acceda al enlace de **estadísticas** .
3. Utilice la barra de desplazamiento para ver las estadísticas sobre infracciones y registros de **XML SQL Injection**. La tabla de estadísticas proporciona datos en tiempo real y se actualiza cada 7 segundos.

Comprobación de datos adjuntos XML

January 12, 2021

La comprobación de datos adjuntos XML examina las solicitudes entrantes de datos adjuntos malintencionados y bloquea las solicitudes que contienen datos adjuntos que podrían infringir la seguridad de las aplicaciones. El objetivo de la comprobación de datos adjuntos XML es evitar que un atacante utilice un archivo adjunto XML para violar la seguridad del servidor.

Si utiliza el asistente o la GUI, en el cuadro de diálogo Modificar comprobación de datos adjuntos XML, en la ficha General puede habilitar o inhabilitar las acciones Bloquear, Aprender, Registro, Estadísticas y Aprender:

Si utiliza la interfaz de línea de comandos, puede introducir el siguiente comando para configurar la comprobación de datos adjuntos XML:

- `set appfw profile <name> -xmlAttachmentAction [block] [learn] [log] [stats] [none]`

Debe configurar las otras opciones de comprobación de datos adjuntos XML en la GUI. En el cuadro de diálogo`Modify XML Attachment` Comprobar, en la ficha Comprobaciones, puede configurar los siguientes parámetros:

- **Tamaño máximo de los datos adjuntos.** Permitir adjuntos que no sean mayores que el tamaño máximo de datos adjuntos especificado. Para habilitar esta opción, active primero la casilla de verificación Habilitado y, a continuación, escriba el tamaño máximo de datos adjuntos en bytes en el cuadro de texto `Size`.
- **Tipo de contenido de datos adjuntos.** Permitir adjuntos del tipo de contenido especificado. Para habilitar esta opción, active primero la casilla Habilitado y, a continuación, escriba una expresión regular que coincida con el atributo Content-Type de los datos adjuntos que quiere permitir.
  - Puede escribir la expresión URL directamente en la ventana de texto. Si lo hace, puede utilizar el menú `Regex Tokens` para introducir varias expresiones regulares útiles en el cursor en lugar de escribirlas manualmente.
  - Puede hacer clic en Editor de expresiones regulares para abrir el cuadro de diálogo `Add Regular Expression` y utilizarlo para crear la expresión URL.

Comprobación de interoperabilidad de servicios web

January 12, 2021

La comprobación de Interoperabilidad de Servicios web (WS-I) examina tanto las solicitudes como las respuestas para el cumplimiento del estándar WS-I, y bloquea aquellas solicitudes y respuestas que no se ajustan a este estándar. El propósito de la comprobación WS-I es bloquear las solicitudes que podrían no interactuar con otro XML de forma adecuada. Un atacante puede utilizar incoherencias en la interoperabilidad para lanzar un ataque a la aplicación XML.

Si utiliza el asistente o la GUI, en el cuadro de diálogo Modificar comprobación de interoperabilidad de servicios web, en la ficha General puede habilitar o inhabilitar las acciones Bloquear, Registro, Estadísticas y Aprendizaje.

Si utiliza la interfaz de línea de comandos, puede escribir el siguiente comando para configurar la comprobación de interoperabilidad de servicios web:

- `set appfw profile <name> -xmlWSIAction [block] ][log] [learn] [stats] [ none]`

Para configurar reglas individuales de interoperabilidad de servicios web, debe usar la GUI. En la ficha Comprobaciones del cuadro de diálogo Modificar comprobación de interoperabilidad de servicios web, seleccione una regla y haga clic en Habilitar o Inhabilitar para habilitar o inhabilitar la regla. También puede hacer clic en Abrir para abrir el cuadro de mensaje Detalle de interoperabilidad de

servicios web para esa regla. El cuadro de mensaje muestra información de solo lectura sobre la regla. No puede modificar ni realizar otros cambios de configuración en ninguna de estas reglas.

La comprobación WS-I utiliza las reglas enumeradas en WS-I Basic Profile 1.0. WS-I ofrece las mejores prácticas para desarrollar soluciones de servicios web interoperables. Las comprobaciones WS-I se realizan solo en mensajes SOAP.

A continuación se proporciona una descripción de cada regla estándar de WSI:

Regla	Descripción
BP1201	El cuerpo del mensaje debe ser un jabón:sobre con espacio de nombres.
R1000	Cuando un SOBRE es un error, el elemento SOAP:Fault NO DEBE tener elementos secundarios que no sean faultcode, faultstring, faultactor y detail.
R1001	Cuando un SOBRE es un error, los elementos secundarios del elemento SOAP:Fault DEBE estar sin calificación.
R1003	Un RECEPTOR DEBE aceptar mensajes de error que tengan cualquier número de atributos calificados o no calificados, incluido cero, que aparecen en el elemento de detalle. El espacio de nombres de atributos calificados puede ser cualquier otra cosa que no sea el espacio de nombres del elemento de documento calificado Envelope.
R1004	Cuando un ENVELOPE contiene un elemento faultcode, el contenido de ese elemento debe ser uno de los códigos de error definidos en SOAP 1.1 (proporcionando información adicional si es necesario en el elemento de detalle), o un Qname cuyo espacio de nombres está controlado por la autoridad especificadora de la falla (en ese orden de preferencia).

Regla	Descripción
R1005	Un SOBRE NO DEBE contener el atributo SOAP:encodingStyle en cualquiera de los elementos cuyo espacio de nombres es el mismo que el espacio de nombres del elemento de documento calificado Envelope.
R1006	Un sobre NO DEBE contener atributos SOAP:encodingStyle en cualquier elemento secundario de SOAP:Body.
R1007	Un sobre descrito en un enlace rpc-literal NO DEBE contener el atributo SOAP:encodingStyle en cualquier elemento que sea nieto de SOAP:body.
R1011	Un sobre NO DEBE tener ningún elemento secundario de SOAP:Envelope siguiendo el elemento SOAP:Body.
R1012	Un MENSAJE DEBE serializarse como UTF-8 o UTF-16.
R1013	Un SOBRE que contenga un atributo SOAP:mustUnderstand DEBE utilizar solo las formas léxicas 0 y 1.
R1014	Los secundarios del elemento SOAP:Body en un SOBRE DEBE tener el espacio de nombres calificado.
R1015	Un RECEPTOR DEBE generar un error si encuentra un sobre cuyo elemento de documento no es SOAP:Envelope.
R1031	Cuando un ENVELOPE contiene un elemento faultcode, el contenido de ese elemento NO debe usar la notación de punto SOAP 1.1 para refinar el significado de la falla.
R1032	Los elementos SOAP:Envelope, SOAP:Header y SOAP:Body en un SOBRE NO DEBE tener atributos en el mismo espacio de nombres que el del elemento de documento calificado Envelope

Regla	Descripción
R1033	Un SOBRE NO DEBERÍA contener la declaración de espacio de nombres: `xmlns:xml=http://www.w3.org/XML/1998/namespace.`
R1109	El valor del campo de encabezado HTTP SoapAction en una solicitud HTTP MESSAGE DEBE ser una cadena entre comillas.
R1111	Una INSTANCIA DEBEN utilizar un código de estado HTTP 200 OK en un mensaje de respuesta que contiene un sobre que no es un error.
R1126	Una INSTANCIA DEBE devolver un código de estado HTTP de 500 Error interno del servidor si el sobre de respuesta es un error.
R1132	Un mensaje de solicitud HTTP DEBE utilizar el método HTTP POST.
R1140	Se debe enviar un MENSAJE mediante HTTP/1.1.
R1141	DEBE enviarse un MENSAJE mediante HTTP/1.1 o HTTP/1.0.
R2113	Un SOBRENC:ArrayType NO DEBE incluir el atributo soapenc:ArrayType.
R2211	Un SOBRE descrito con un enlace rpc-literal NO DEBE tener el atributo xsi:nil con un valor de 1 o true en los accesores de pieza.
R2714	Para operaciones unidireccionales, una INSTANCIA NO DEBE devolver una respuesta HTTP que contenga un sobre. Específicamente, la entidad de respuesta HTTP debe estar vacía.
R2729	Un SOBRE descrito con un enlace rpc-literal que es una respuesta DEBE tener un elemento contenedor cuyo nombre es el wsdl:nombre_de_operación correspondiente sufijo con stringResponse.

Regla	Descripción
R2735	Un SOBRE descrito con un enlace rpc-literal DEBE colocar los elementos de acceso de pieza para los parámetros y devolver el valor en ningún espacio de nombres.
R2738	Un SOBRE DEBE incluir todos los encabezados soapbind:especificados en un wsdl:input o wsdl:output de un wsdl:operation de un wsdl:binding que lo describe.
R2740	Un wsdl:binding en una DESCRIPCIÓN DEBEN contener un soapbind:fault que describa cada falla conocida.
R2744	Un mensaje de solicitud HTTP DEBE contener un campo de encabezado HTTP SoapAction con un valor comillas igual al valor del atributo SoapAction de soapbind:operation, si está presente en la descripción WSDL correspondiente.

Comprobación de validación de mensajes XML

January 19, 2021

La comprobación de validación de mensajes XML examina las solicitudes que contienen mensajes XML para asegurarse de que son válidos. Si una solicitud contiene un mensaje XML no válido, Web App Firewall bloquea la solicitud. El objetivo de la comprobación de validación XML es evitar que un atacante utilice mensajes XML no válidos especialmente construidos para violar la seguridad de la aplicación.

Si utiliza el asistente o la GUI, en el cuadro de diálogo Modificar comprobación de validación de mensajes XML, en la ficha General puede habilitar o inhabilitar las acciones Bloquear, Registro y Estadísticas.

Si utiliza la interfaz de línea de comandos, puede introducir el siguiente comando para configurar la comprobación de validación de mensajes XML:

- `set appfw profile <name> -xmlValidationAction [**block**] [**log**] [**stats**] [**none**]`

Debe utilizar la interfaz gráfica de usuario para configurar las otras opciones de comprobación de validación XML. En el cuadro de diálogo
Modificar comprobación de validación de mensajes XML, en la ficha
Comprobaciones, puede configurar los siguientes valores:

- **Validación de mensajes XML.** Utilice una de las siguientes opciones para validar el mensaje XML:
  - **Sobre SOAP.** Validar solo el sobre SOAP de los mensajes XML.
  - **WSDL.** Validar mensajes XML mediante un XML SOAP WSDL. Si elige validación WSDL, en la lista desplegable Objeto WSDL debe elegir un WSDL. Si quiere validar con un WSDL que aún no se haya importado al Web App Firewall, puede hacer clic en el botón Importar para abrir el cuadro de diálogo Administrar importaciones de WSDL e importar su WSDL. Consulte WSDL para obtener más información.
    * Si quiere validar toda la URL, deje seleccionado el botón de opción Absoluto en la matriz de botones Comprobación de punto final. Si quiere validar solo la parte de la URL después del host, seleccione el botón de opción Relativo.
    * Si quiere que Web App Firewall aplique estrictamente el WSDL y no permita encabezados XML adicionales no definidos en el WSDL, debe desactivar la casilla de verificación Permitir encabezados adicionales no definidos en el WSDL.
      Precaución: Si desmarca la casilla de verificación
      Permitir encabezados adicionales no definidos en WSDL y WSDL no define todos los encabezados XML que espera la aplicación XML protegida o la aplicación web 2.0 o que envía un cliente, puede bloquear el acceso legítimo al servicio protegido.
  - **Esquema XML.** Validar mensajes XML mediante un esquema XML. Si elige la validación de esquema XML, en la lista desplegable Objeto de esquema XML debe elegir un esquema XML. Si quiere validar con un esquema XML que aún no se ha importado al Web App Firewall, puede hacer clic en el botón Importar para abrir el cuadro de diálogo Administrar importaciones de esquemas XML e importar su WSDL. Consulte WSDL para obtener más información.
- **Validación de respuesta.** De forma predeterminada, Web App Firewall no intenta validar las respuestas. Si quiere validar las respuestas de la aplicación protegida o del sitio web 2.0, active la casilla de verificación Validar respuesta. Cuando lo haga, se activarán la casilla de verificación Reutilizar el esquema XML especificado en la validación de solicitud y la lista desplegable Objeto de esquema XML.
  - Active la casilla de verificación Reutilizar esquema XML para utilizar el esquema especificado para la validación de solicitudes para realizar también la validación de respuestas.
    Nota: Si activa esta casilla de verificación, la lista desplegable Objeto de esquema XML aparece atenuada.
  - Si quiere utilizar un esquema XML diferente para la validación de respuestas, utilice la lista desplegable Objeto de esquema XML para seleccionar o cargar ese esquema XML.

Comprobación de filtrado de errores XML SOAP

January 12, 2021

La comprobación de filtrado de errores SOAP XML examina las respuestas de los servicios web protegidos y filtra las fallas SOAP XML. Esto evita que se filtre información confidencial a los atacantes.

Si utiliza el asistente o la GUI, en el cuadro de diálogo Modificar comprobación de filtrado de errores SOAP XML, en la ficha **General** puede habilitar o inhabilitar las acciones Bloquear, Registro y Estadísticas, y la acción Quitar, que elimina los errores SOAP antes de reenviar la respuesta al usuario.

Si utiliza la interfaz de línea de comandos, puede introducir el siguiente comando para configurar la comprobación de filtrado de errores SOAP XML:

```
set appfw profile <name> -XMLSOAPFaultAction [block] [log] [stats] [none]
```

No puede configurar excepciones a la comprobación XML SOAP Fault Filtering. Solo puede habilitarlo o inhabilitarlo.

Comprobaciones de protección JSON

January 12, 2021

Citrix Web App Firewall protege sus aplicaciones JSON frente a ataques DoS de nivel de contenido, SQL o scripts entre sitios. Cuando una solicitud JSON tiene un ataque de scripts DoS, SQL o entre sitios, debe proteger su aplicación configurando límites en estructuras JSON como matrices y cadenas.

> **Nota:**
>
> Las comprobaciones de seguridad JSON se aplican solo al contenido que se envía con un encabezado de tipo de contenido JSON. Si falta el encabezado de tipo de contenido o se establece en un valor diferente, se omiten todas las comprobaciones de seguridad JSON. Si quiere proteger sus aplicaciones JSON, los webmasters de cada servidor web que aloja esas aplicaciones deben asegurarse de que se envíe un encabezado de tipo de contenido JSON adecuado.
>
> La función de aprendizaje no es compatible con JSON SQL, scripts entre sitios, tipos de contenido DOS.

Comprobación de protección de denegación de servicio JSON

April 21, 2022

La comprobación de denegación de servicio (DoS) de JSON examina una solicitud JSON entrante y valida si hay datos que coincidan con las características de un ataque DoS. Si la solicitud tenía infracciones de JSON, el dispositivo bloquea la solicitud, registra los datos, envía una alerta SNMP y también muestra una página de error de JSON. El propósito de la comprobación DoS de JSON es evitar que un atacante envíe una solicitud JSON para lanzar ataques DoS en sus aplicaciones JSON o sitio web.

Cuando un cliente envía una solicitud a un dispositivo Citrix ADC, el analizador JSON analiza la carga útil de la solicitud y, si se observa una infracción, el dispositivo impone restricciones en la estructura JSON. La restricción impone un límite de tamaño en la solicitud JSON. Como resultado, si se observó alguna infracción de JSON, el dispositivo aplica una acción y responde con la página de error de JSON.

Reglas DoS JSON

Cuando el dispositivo recibe una solicitud JSON, la protección JSON DOS impone un límite de tamaño en los siguientes parámetros DoS en la carga útil de la solicitud.

1. profundidad máxima: anidamiento máximo (profundidad) del documento JSON. Esta comprobación protege contra documentos que tienen una profundidad de jerarquía excesiva.
2. longitud máxima del documento: longitud máxima del documento JSON.
3. longitud máxima de la matriz: longitud máxima de la matriz en cualquiera de los objetos JSON. Esta comprobación protege contra las matrices que tienen longitudes grandes.
4. longitud máxima de cadena: longitud máxima de cadena en el JSON. Esta comprobación protege contra las cuerdas que tienen una longitud grande.
5. recuento máximo de claves de objetos: recuento máximo de claves en cualquiera de los objetos JSON. Esta comprobación protege contra objetos que tienen un gran número de teclas.
6. longitud máxima de clave de objeto: longitud máxima de clave en cualquiera de los objetos JSON. Esta comprobación protege contra objetos que tienen teclas grandes.

A continuación se muestra una lista de reglas DoS de JSON validadas durante el análisis JSON.

1. Profundidad máxima del contenedor JSON. Esta verificación se puede habilitar configurando la verificación JSONMaxContainerDepth y, de forma predeterminada, la opción está desactivada.
2. Profundidad máxima del contenedor JSON. Esta comprobación se puede habilitar/inhabilitar mediante la opción configurable jsonMaxContainerDepthCheck y el valor predeterminado se puede cambiar mediante la opción jsonMaxContainerDepth. Sin embargo, puede variar los niveles máximos a un valor comprendido entre 1 y 127. Valor predeterminado: 5, Valor mínimo: 1, Valor máximo: 127
3. JSONMaxDocumentLength. Esta comprobación se puede habilitar configurando la comprobación JSONMaxDocumentLength y la opción predeterminada es OFF.
4. JSONMaxDocumentLength. Esta comprobación se puede habilitar configurando la comprobación JSONMaxDocumentLength y la longitud predeterminada se establece en 20000000

bytes. Valor mínimo: 1, Valor máximo: 2147483647

5. JSONMaxObjectKeyCount. La regla valida si la comprobación de recuento máximo de claves de objetos JSON está activada o desactivada. Valores posibles: ON, OFF, Valor por defecto: OFF
6. JSONMaxObjectKeyCount. Esta comprobación se puede habilitar configurando la comprobación JSONMaxObjectKeyCount. La comprobación protege contra objetos que tienen un gran número de claves y el valor predeterminado se establece en 1000 bytes. Valor mínimo: 0, Valor máximo: 2147483647
7. JSONMaxObjectKeyLength. Esta comprobación se puede habilitar configurando la comprobación JSONMaxObjectKeyLength. La regla valida si la verificación de longitud máxima de clave de objeto JSON está activada o desactivada. De forma predeterminada, está DESACTIVADO.
8. JSONMaxObjectKeyLength. La marca protege contra objetos que tienen una longitud de clave grande. Valor por defecto: 128. Valor mínimo: 1, Valor máximo: 2147483647
9. JSONMaxArrayLength. La regla valida si la comprobación de longitud máxima de matriz JSON está ACTIVADA o DESACTIVADA. De forma predeterminada, está desactivada.
10. JSONMaxArrayLength. La comprobación protege contra matrices que tienen longitudes grandes. De forma predeterminada, el valor se establece en 10000. Valor mínimo: 1, Valor máximo: 2147483647
11. Longitud máxima de la cadena JSON. Esta comprobación se puede habilitar configurando la comprobación JSONMaxStringLength. La comprobación valida si la longitud máxima de cadena JSON está ACTIVADA o DESACTIVADA. De forma predeterminada, está desactivada.
12. Longitud máxima de la cadena JSON. El cheque protege contra cuerdas de gran longitud. De forma predeterminada, se establece en 1000000. Valor mínimo: 1, Valor máximo: 2147483647

Configurar la comprobación de la protección DoS

Para configurar la protección DoS de JSON, debe completar los siguientes pasos:

1. Agregue el perfil de firewall de aplicaciones para JSON.
2. Establece el perfil de firewall de aplicaciones para la configuración de DoS
3. Configure variables DoS de JSON vinculando el perfil de firewall de aplicaciones.

Agregar perfil de firewall de aplicaciones para la protección contra DoS

Primero debe crear un perfil que especifique cómo el firewall de la aplicación debe proteger el contenido web JSON del ataque DoS de JSON.
En el símbolo del sistema, escriba:

```
add appfw profile <name> -type (HTML | XML | JSON)
```


> *Nota*:
>
> Cuando establece el tipo de perfil como JSON, no se aplicarán otras comprobaciones, como HTML o XML.

Ejemplo

```
add appfw profile profile1 -type JSON
```

Establecer el perfil de firewall de aplicaciones para la protección DoS

Debe configurar el perfil para que se establezcan una o más acciones DoS JSON y un objeto de error DoS JSON en el perfil del firewall de la aplicación.
En el símbolo del sistema, escriba:

```
set appfw profile <name> -JSONDoSAction [block] | [log] | [stats] | [none]
```

Bloquear: bloquea las conexiones que infrinjan esta comprobación de seguridad.
Registro: Registrar infracciones de esta comprobación de seguridad.
Estadísticas: genera estadísticas para esta comprobación de seguridad.
Ninguno: inhabilite todas las acciones de esta comprobación de seguridad.

> *Nota*:
>
> Para habilitar una o más acciones, escriba “set appfw profile -jsondosAction” seguido de las acciones que se habilitarán.

Ejemplo

```
set appfw profile profile1 -JSONDoSAction block log stat
```

Configurar variables DoS vinculando el perfil de firewall de aplicaciones

Para proporcionar protección DoS de JSON, debe vincular el perfil de firewall de aplicaciones con la configuración de DoS de JSON.
En el símbolo del sistema, escriba:

```
bind appfw profile <name> -JSONDoSURL <expression> [-JSONMaxContainerDepthCheck
 ( ON | OFF )[-JSONMaxContainerDepth <positive_integer>]] [-JSONMaxDocumentLengthCheck
 ( ON | OFF )[-JSONMaxDocumentLength <positive_integer>]] [-JSONMaxObjectKeyCountCheck
 ( ON | OFF )[-SONMaxObjectKeyCount <positive_integer>]] [-JSONMaxObjectKeyLengthCheck
 ( ON | OFF )[-JSONMaxObjectKeyLength <positive_integer>]] [-JSONMaxArrayLengthCheck
 ( ON | OFF )[-JSONMaxArrayLength <positive_integer>]] [-JSONMaxStringLengthCheck
 ( ON | OFF )[-JSONMaxStringLength <positive_integer>]]
```


Ejemplo

```
bind appfw profile profile1 -JSONDoSURL “.*” -JSONMaxContainerDepthCheck ON
```

> *Nota*:
>
> Las comprobaciones DoS de JSON solo se aplicarán si el tipo de perfil se selecciona como JSON. Además, las firmas de campo SQL, scripting de sitios, formato de campo y formulario se aplican en los parámetros de consulta en los casos de perfil JSON.

Importar página de error JSON

Si una solicitud entrante tuvo un ataque DoS y cuando bloquea la solicitud, el dispositivo muestra un mensaje de error. Para ello, debe importar la página de error de JSON.
En el símbolo del sistema, escriba:

```
import appfw jsonerrorpage <src> <name> [-comment <string>] [-overwrite]
```

Donde:

src. URL (protocolo, host, ruta y nombre) de la ubicación en la que se almacena el objeto de error JSON importado.

> *Nota*:
>
> La importación falla si el objeto que se va a importar está en un servidor HTTPS que requiere autenticación de certificado de cliente para el acceso. Se trata de un argumento obligatorio. Longitud máxima: 2047.

Nombre. Nombre que se va a asignar al objeto de error JSON en Citrix ADC. Se trata de un argumento obligatorio. Longitud máxima: 31
Comentario. Cualquier comentario para conservar la información sobre el objeto de error JSON. Longitud máxima: 255
Sobrescritura. Sobrescriba cualquier objeto de error JSON existente con el mismo nombre.

Configuración de ejemplo

```
1 Add appfw prof profjson - type JSON
2 Bind appfw prof profjson - JSONDoSURL “.*” -
    JSONMaxDocumentLengthCheck ON -JSONMaxDocumentLength 30 -
    JSONMaxContainerDepthCheck ON -JSONMaxContainerDepth 3
    JSONMaxObjectKeyCountCheck ON -JSONMaxObjectKeyCount 4 -
    JSONMaxObjectKeyLengthCheck ON -JSONMaxObjectKeyLength 10 -
    JSONMaxArrayLengthCheck ON -JSONMaxArrayLength 5 -
    JSONMaxStringLengthCheck ON -JSONMaxStringLength 30
```



```
<!--NeedCopy-->
```

Cargas útiles, mensajes de registro y contadores de ejemplo:

Infracción de JSONMaxDocumentLength

JSONMaxDocumentLength: 30
Carga útil: {“a”:”A”,”b”:”B”,”c”:”C”,”d”:”D”,”e”:”E”}

Mensaje de registro:

```
Document Length exceeds 20000000 May 29 20:23:32 <local0.info>
    10.217.31.243 05/29/2019:20:23:32 GMT 0-PPE-0 : default APPFW
    APPFW_JSON_DOS_MAX_DOCUMENT_LENGTH 136 0 : 10.217.32.134 114-PPE0 -
    profjson http://10.217.30.120/forms/login.html Document exceeds
    maximum document length (30). cn1=30467 cn2=115 cs1=profjson cs2=
    PPE0 cs4=ALERT cs5=2019 act=blocked
<!--NeedCopy-->
```

Contadores:

```
1 0 6 as_viol_json_dos
2 0 3 as_viol_json_dos_max_document_length
3 0 6 as_log_json_dos
4 0 3 as_log_json_dos_max_document_length
5 0 6 as_viol_json_dos_profile appfw__(profile1)
6 0 3 as_viol_json_dos_max_document_length_profile appfw__(profile1)
7 0 6 as_log_json_dos_profile appfw__(profile1)
8 0 3 as_log_json_dos_max_document_length_profile appfw__(profile1)
<!--NeedCopy-->
```

Infracción de JSONMaxContainerDepth

JSONMaxContainerDepth: 3
Carga útil: {“a”: {”b”: {“c”: {“d”: { ”e” : “f” }}}}}

Mensaje de registro:


```
May 29 19:33:59 <local0.info> 10.217.31.243 05/29/2019:19:33:59 GMT 0-PPE-1 : default APPFW APPFW_JSON_DOS_MAX_CONTAINER_DEPTH 4626 0 : 10.217.31.247 22-PPE1 - profjson http://10.217.30.120/forms/login.html Document at offset (15) exceeds maximum container depth (3). cn1=30466 cn2=113 cs1=profjson cs2=PPE0 cs4=ALERT cs5=2019 act=blocked
<!--NeedCopy-->
```

Contadores:

```
36 20999 7 1 0 as_viol_json_dos
37 0 6 1 0 as_viol_json_dos_max_container_depth
38 0 7 1 0 as_log_json_dos
39 0 6 1 0 as_log_json_dos_max_container_depth
40 0 7 1 0 as_viol_json_dos_profile appfw__(profile1)
41 0 6 1 0 as_viol_json_dos_max_container_depth_profile appfw__(profile1)
42 0 7 1 0 as_log_json_dos_profile appfw__(profile1)
43 0 6 1 0 as_log_json_dos_max_container_depth_profile appfw__(profile1)
<!--NeedCopy-->
```

Infracción de JSONMaxObjectKeyCount

JSONmaxObjectKeyCount: 4

Carga útil: {“a”: ”A”, “b”: “B”, “c”:“C”, “d” :“D”, ”e” : “E” }

Mensaje de registro:

```
May 30 19:42:41 <local0.info> 10.217.31.243 05/30/2019:19:42:41 GMT 0-PPE-1 : default APPFW APPFW_JSON_DOS_MAX_OBJECT_KEY_COUNT 457 0 : 10.217.32.134 219-PPE1 - profjson http://10.217.30.120/forms/login.html Object at offset (41) that exceeds maximum key count (4). cn1=30468 cn2=118 cs1=profjson cs2=PPE0 cs4=ALERT cs5=2019 act=blocked
<!--NeedCopy-->
```

Contadores:

```
94 119105 15 1 0 as_viol_json_dos
95 0 4 1 0 as_viol_json_dos_max_object_key_count
```



```
96 0 15 1 0 as_log_json_dos
97 0 4 1 0 as_log_json_dos_max_object_key_count
98 0 15 1 0 as_viol_json_dos_profile appfw__(profile1)
99 0 4 1 0 as_viol_json_dos_max_object_key_count_profile appfw__(
   profile1)
100 0 15 1 0 as_log_json_dos_profile appfw__(profile1)
101 0 4 1 0 as_log_json_dos_max_object_key_count_profile appfw__(
   profile1)
<!--NeedCopy-->
```

Infracción de JSONMaxObjectKeyLength

JSONMaxObjectKeyLength: 10
Carga útil: {“a”: ”A”, “b1234567890”: “B”, “c”:“C”, “d” :“D”, ”e” : “E” }

Mensaje de registro:

```
May 31 20:26:10 <local0.info> 10.217.31.243 05/31/2019:20:26:10 GMT 0-
   PPE-1 : default APPFW APPFW_JSON_DOS_MAX_OBJECT_KEY_LENGTH 102 0 :
   10.217.32.134 89-PPE1 - profjson http://10.217.30.120/forms/login.
   html Object key(b1234567890) at offset (12) exceeds maximum key
   length (10). cn1=30469 cn2=118 cs1=profjson cs2=PPE0 cs4=ALERT cs5
   =2019 act=blocked
<!--NeedCopy-->
```

Contadores:

```
242172 6 1 0 as_viol_json_dos
0 1 1 0 as_viol_json_dos_max_object_key_length
10 0 5 1 0 as_log_json_dos
11 0 1 1 0 as_log_json_dos_max_object_key_length
12 0 6 1 0 as_viol_json_dos_profile appfw__(profile1)
13 0 1 1 0 as_viol_json_dos_max_object_key_length_profile appfw__(
   profile1)
14 0 5 1 0 as_log_json_dos_profile appfw__(profile1)
15 0 1 1 0 as_log_json_dos_max_object_key_length_profile appfw__(
   profile1)
<!--NeedCopy-->
```

Infracción JSONMaxArrayLength

JSONMaxArrayLength: 5
Carga útil: {“a”: ”A”, “c”:[”d”,”e”,”f”,”g”,”h”,”i”],”e”:[“E”,”e”]}

Mensaje de registro:

```
May 29 20:58:39 <local0.info> 10.217.31.243 05/29/2019:20:58:39 GMT 0-PPE-1 : default APPFW APPFW_JSON_DOS_MAX_ARRAY_LENGTH 4650 0 : 10.217.32.134 153-PPE1 -profjson http://10.217.30.120/forms/login.html Array at offset (37) that exceeds maximum array length (5). cn1=30469 cn2=120 cs1=profjson cs2=PPE0 cs4=ALERT cs5=2019 act=blocked
<!--NeedCopy-->
```

Contadores:

```
36 182293 10 1 0 as_viol_json_dos
37 0 1 1 0 as_viol_json_dos_max_array_length
38 0 10 1 0 as_log_json_dos 39 0 1 1 0 as_log_json_dos_max_array_length
40 0 10 1 0 as_viol_json_dos_profile appfw__(profile1)
41 0 1 1 0 as_viol_json_dos_max_array_length_profile appfw__(profile1)
42 0 10 1 0 as_log_json_dos_profile appfw__(profile1)
43 0 1 1 0 as_log_json_dos_max_array_length_profile appfw__(profile1))
<!--NeedCopy-->
```

Infracción de longitud de cadena máxima de JSON

Longitud máxima de la cadena JSON: 10

Carga útil: {“a”: ”A”, “c”:”CcCcCcCcCcCcCcCcCc”,”e”:[“E”,”e”]}

Mensaje de registro:

```
May 29 20:05:02 <local0.info> 10.217.31.243 05/29/2019:20:05:02 GMT 0-PPE-0 : default APPFW APPFW_JSON_DOS_MAX_STRING_LENGTH 134 0 : 10.217.32.134 80-PPE0 - profjson http://10.217.30.120/forms/login.html String(CcCcCcCcCcCcCc) at offset (27) that exceeds maximum string length (10). n1=30470 cn2=122 cs1=profjson cs2=PPE0 cs4=ALERT cs5=2019 act=blocked
<!--NeedCopy-->
```

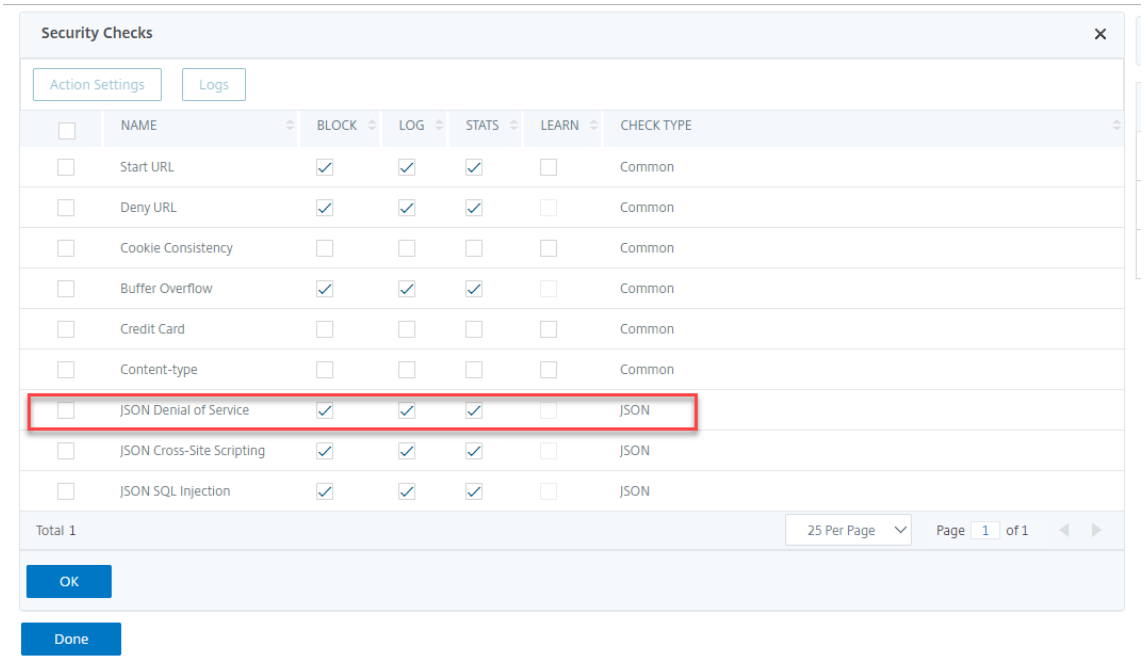
Contadores:


```
44 91079 3 1 0 as_viol_json_dos
45 0 1 1 0 as_viol_json_dos_max_string_length
46 0 3 1 0 as_log_json_dos
47 0 1 1 0 as_log_json_dos_max_string_length
48 0 3 1 0 as_viol_json_dos_profile appfw__(profile1)
49 0 1 1 0 as_viol_json_dos_max_string_length_profile appfw__(profile1)
50 0 3 1 0 as_log_json_dos_profile appfw__(profile1)
51 0 1 1 0 as_log_json_dos_max_string_length_profile appfw__(profile1
<!--NeedCopy-->
```

Configurar la protección DoS de JSON mediante Citrix GUI

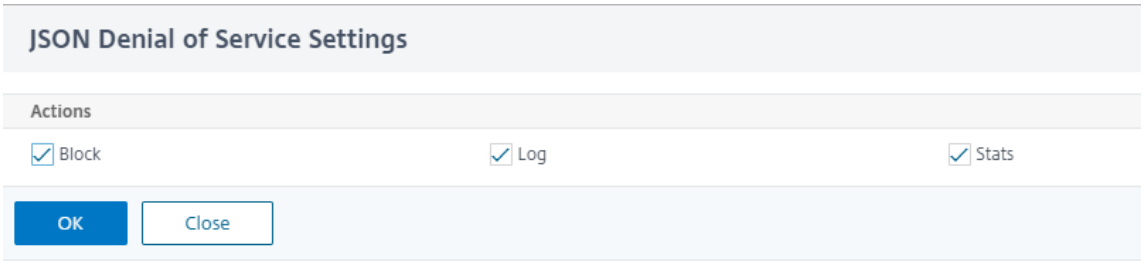
Siga el procedimiento a continuación para establecer la configuración de protección DoS de JSON.

1. En el panel de navegación, vaya a **Seguridad** > **Perfiles**.
2. En la página **Perfiles**, haga clic en **Agregar**.
3. En la página **Perfil de Citrix Web App Firewall**, haga clic en **Comprobaciones de seguridad en Configuración avanzada**.
4. En la sección **Comprobaciones de seguridad**, vaya a Configuración de **denegación de servicio de JSON**.
5. Haga clic en el icono ejecutable cerca de la casilla de verificación.

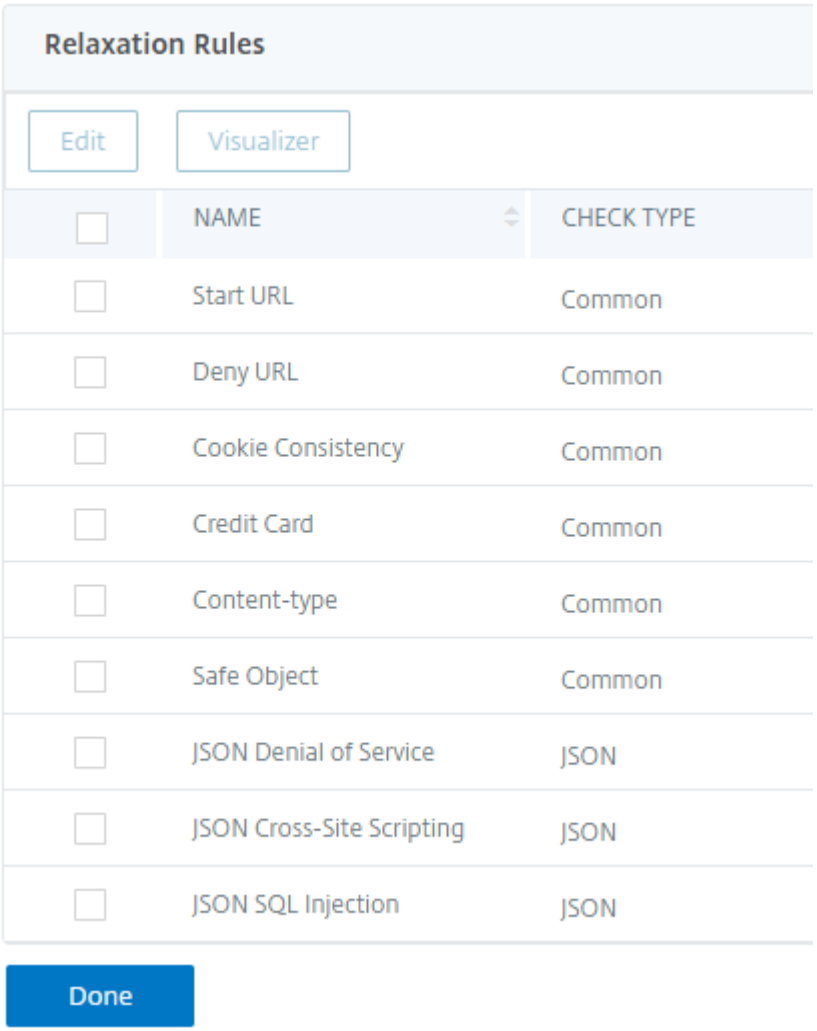


6. Haga clic en **Configuración de acción** para acceder a la página **Configuración de denegación de servicio JSON**.

7. Seleccione la acción DoS de JSON.
8. Haga clic en **OK**.



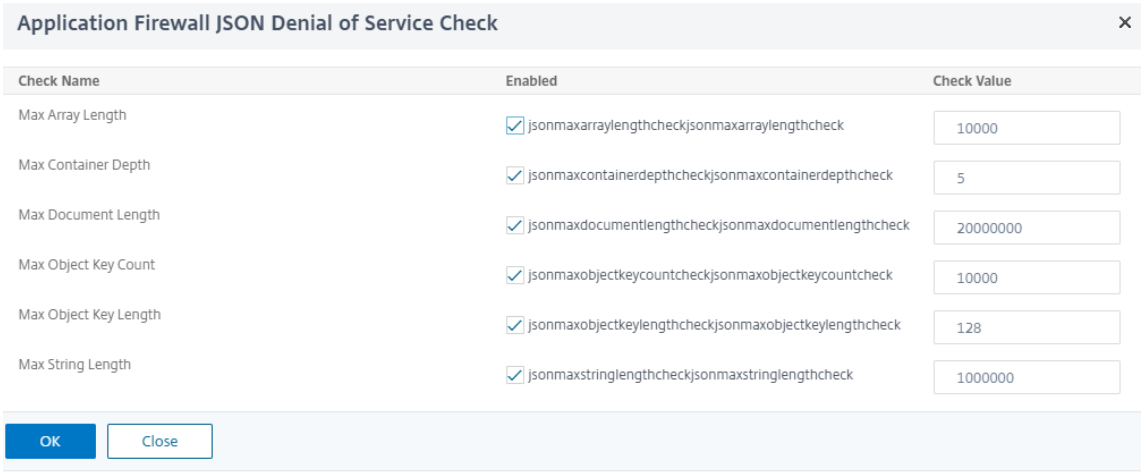
9. En la página **Perfil de Citrix Web App Firewall**, haga clic en **Reglas de relajación** en **Configuración avanzada**.
10. En la sección **Reglas de relajación**, seleccione Configuración **de denegación de servicio JSON** y haga clic en **Modificar**.



11. En la **comprobación de denegación de servicio JSON de Application Firewall**, establezca los

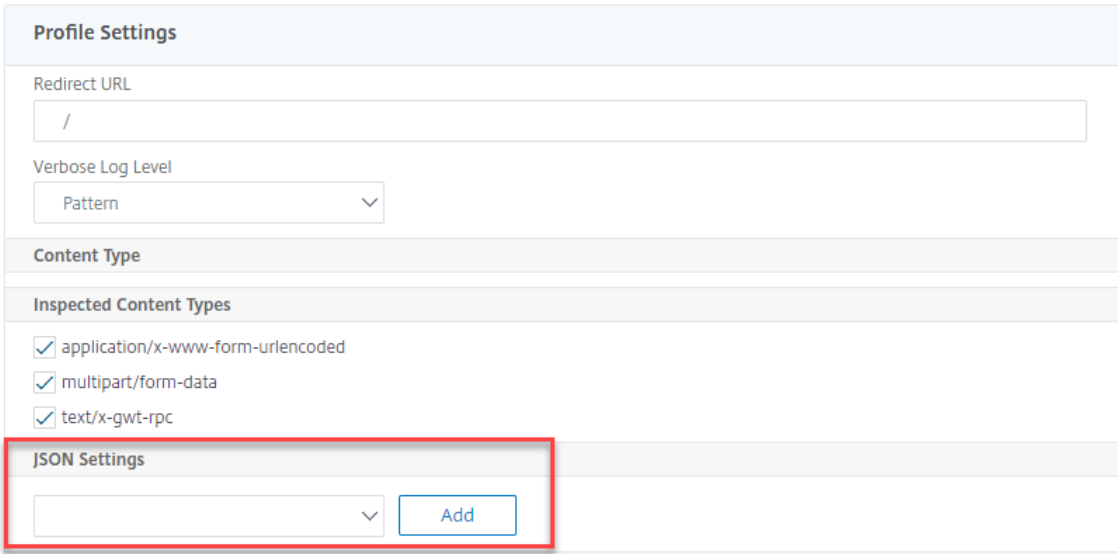
valores de validación de DoS

12. Haga clic en **OK**.



13. En la página **Perfil de Citrix Web App Firewall**, haga clic en **Configuración de perfil** en **Configuración avanzada**.

14. En la sección **Configuración del perfil**, vaya a la subsección **Configuración de errores de JSON** para establecer la página de **error DoS de JSON**.

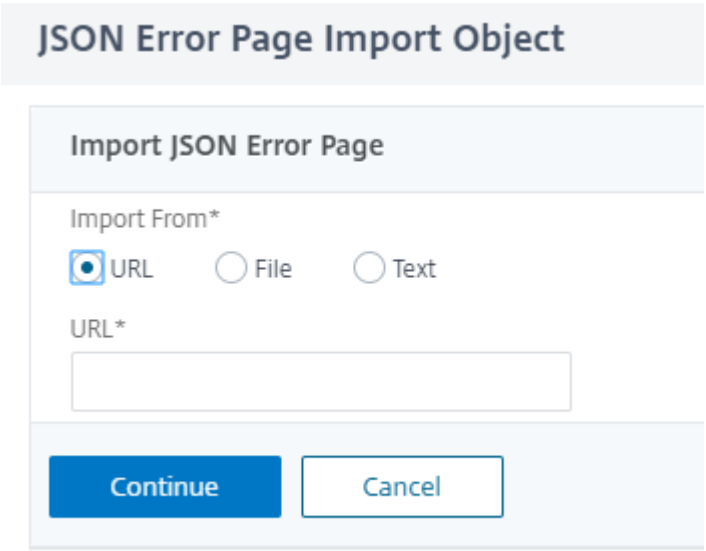


15. En la página **Objeto Importar página de error JSON**, defina los siguientes parámetros:

    a) Importar desde. Importe la página de error como texto, archivo o URL.
    b) URL. URL para redirigir al usuario a la página de error.
    1 archivo. Seleccione un archivo para importarlo como archivo de error DoS de JSON.
    c) Texto. Introduzca el contenido del archivo JSON.
    d) Haga clic en Continue.
    e) archivo. Introduzca el nombre del archivo.

f) Contenido del archivo. Agregue el contenido del archivo de errores.

g) Haga clic en **OK**.



16. Haga clic en **OK**.
17. Haga clic en **Listo**.

Comprobación de protección de inyección JSON SQL

April 21, 2022

Una solicitud JSON entrante puede tener una inyección SQL en forma de cadenas de consulta SQL parciales o comandos no autorizados en el código. Esto lleva al robo de datos de la base de datos JSON de sus servidores web. Al recibir dicha solicitud, el dispositivo bloquea dicha solicitud para proteger sus datos.

Considere un caso en el que un cliente envía una solicitud JSON SQL a un dispositivo Citrix ADC, el analizador JSON analiza la carga útil de la solicitud y, si se observa una inyección SQL, el dispositivo impone restricciones en el contenido JSON SQL. La restricción impone un límite de tamaño en la solicitud JSON SQL. Como resultado, si se observa alguna inyección JSON SQL, el dispositivo aplica una acción y responde con la página de error JSON SQL.

Configurar la protección de inyección JSON SQL

Para configurar la protección JSON SQL, debe completar los siguientes pasos:

1. Agregue el perfil de firewall de aplicaciones como JSON.

2. Establecer el perfil de firewall de aplicaciones para la configuración de inyección JSON
3. Configure la acción JSON SQL vinculando el perfil de firewall de la aplicación.

Agregar perfil de firewall de aplicaciones de tipo JSON

Primero debe crear un perfil que especifique cómo el firewall de la aplicación debe proteger el contenido web JSON del ataque de inyección JSON SQL.
En el símbolo del sistema, escriba:

```
add appfw profile <name> -type (HTML | XML | JSON)
```

> *Nota*:
>
> Cuando establece el tipo de perfil como JSON, no se aplicarán otras comprobaciones, como HTML o XML.

Ejemplo

```
add appfw profile profile1 -type JSON
```

Acción Configurar inyección JSON SQL

Debe configurar una o más acciones de inyección JSON SQL para proteger su aplicación de los ataques de inyección JSON SQL.
En el símbolo del sistema, escriba:

```
set appfw profile <name> - JSONSQLInjectionAction [block] [log] [stats] [
none]
```

Las acciones de inyección SQL son:
Bloquear: bloquear las conexiones que infrinjan esta comprobación de seguridad.
Registro: Registrar infracciones de esta comprobación de seguridad.
Estadísticas: genera estadísticas para esta comprobación de seguridad.
Ninguno: inhabilite todas las acciones de esta comprobación de seguridad.

Configurar el tipo de inyección JSON SQL

Para configurar el tipo de inyección JSON SQL en un perfil de firewall de aplicaciones, en el símbolo del sistema, escriba:

```
set appfw profile <name> - JSONSQLInjectionType <JSONSQLInjectionType>
```


Ejemplo

```
set appfw profile profile1 -JSONSQLInjectionType SQLKeyword
```

Donde los tipos de inyección SQL
disponibles son: Tipos de inyección SQL disponibles.
SqlSplChar. Comprueba si hay caracteres especiales de
SQL, palabra clave SQL. Comprueba las palabras clave de SQL.
SQL Splchar y palabra clave. Comprueba si hay bloques y si se encuentran.
Palabra clave SQL Splcharor. Bloquea si se encuentra un carácter especial SQL o una palabra clave spl.
Valores posibles: SQLSplChar, SQLKeyword, SQLSplcharorKeyword, SQLSplcharAndKeyword.

> *Nota*:
> Para habilitar una o más acciones, escriba “set appfw profile - JSONSQLInjectionAction” seguido de las acciones que se habilitarán.

Ejemplo

```
set appfw profile profile1 -JSONSQLInjectionAction block log stat
```

El siguiente ejemplo muestra una carga útil de ejemplo, sus correspondientes contadores de mensajes de registro y estadísticas:

```
Payload:
=======
{

  ”test”: ”data”,
  ”username”: ”waf”,
  ”password”: ”select * from t1;”,
  ”details”: {

    ”surname”: ”test”,
    ”age”: ”23”
   }

 }


Log Message:
===========
08/19/2019:08:49:46 GMT pegasus121 Informational 0-PPE-0 : default
   APPFW APPFW_JSON_SQL 6656 0 :  10.217.32.165 18402-PPE0 - profjson
```

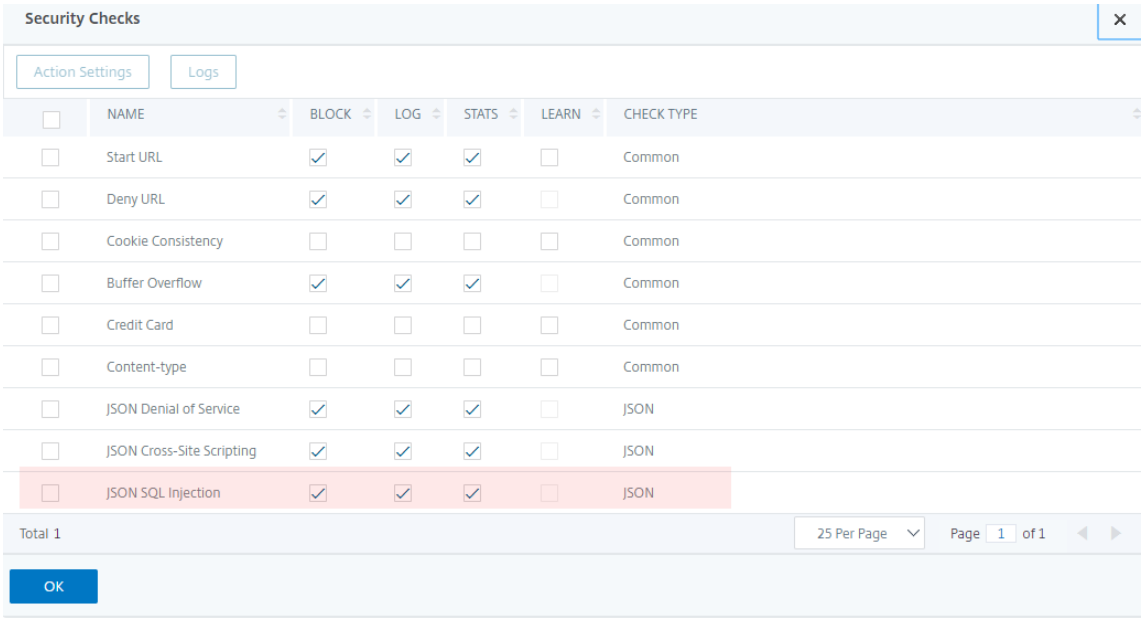


```
    http://10.217.32.147/test.html SQL Keyword check failed for object
    value(with violation="select(;)") starting at offset(52) <blocked>
Counters:
========
   1  441083             1 as_viol_json_sql
   3       0             1 as_log_json_sql
   5       0             1 as_viol_json_sql_profile appfw__(profjson)
   7       0             1 as_log_json_sql_profile appfw__(profjson)
<!--NeedCopy-->
```

Configurar la protección de inyección JSON SQL mediante la GUI de Citrix

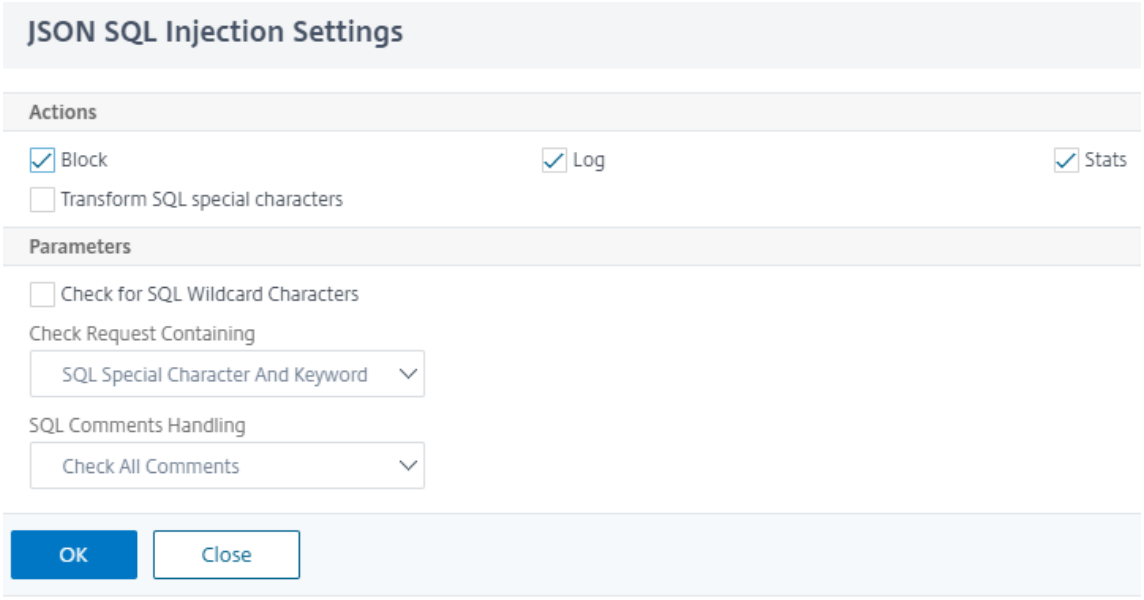
Siga el procedimiento a continuación para establecer la configuración de protección de inyección JSON SQL.

1. En el panel de navegación, vaya a **Seguridad** > **Perfiles**.
2. En la página **Perfiles**, haga clic en **Agregar**.
3. En la página **Perfil de Citrix Web App Firewall**, haga clic en **Comprobaciones de seguridad** en **Configuración avanzada**.
4. En la sección **Comprobaciones de seguridad**, vaya a la configuración de **inyección JSON SQL**.
5. Haga clic en el icono ejecutable situado cerca de la casilla de verificación.

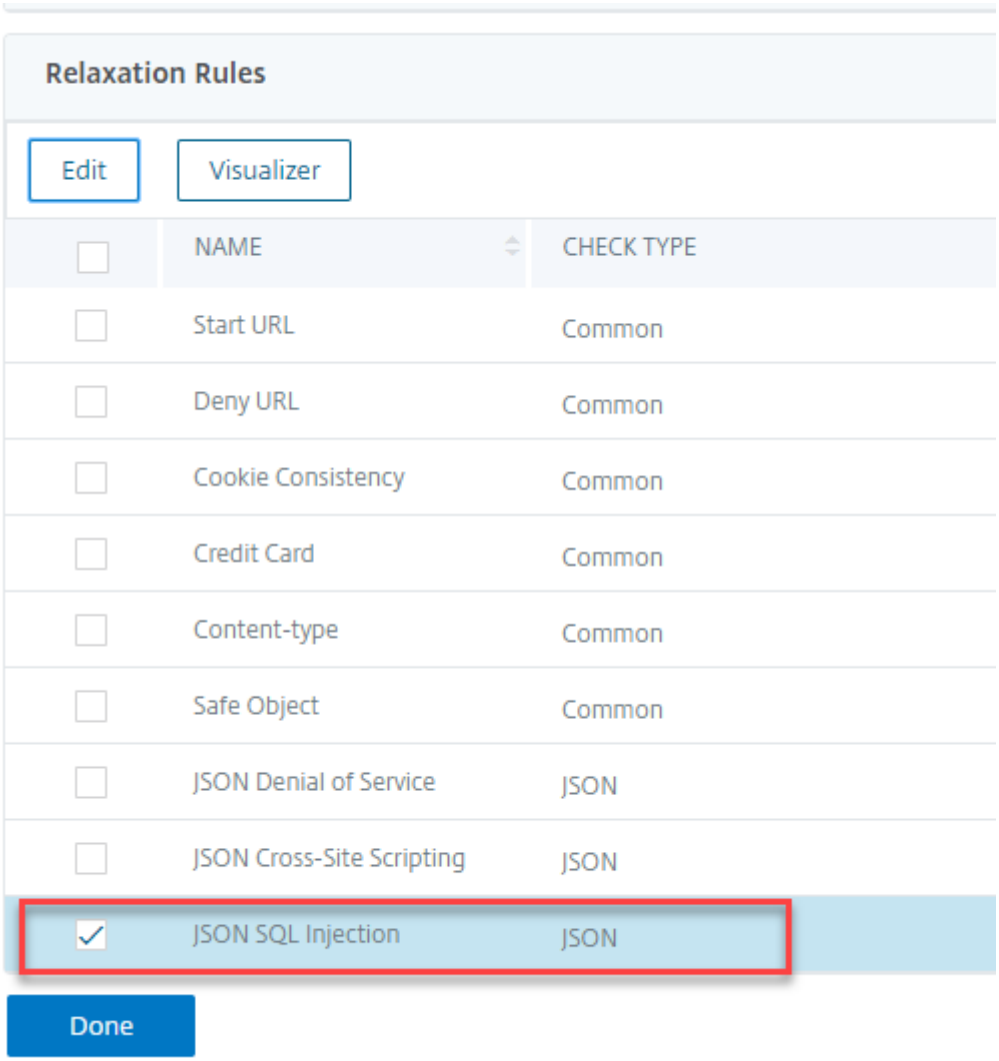


6. Haga clic en **Configuración de acción** para acceder a la página **Configuración de inyección JSON SQL**.
7. Seleccione las acciones de **inyección de JSON SQL**.

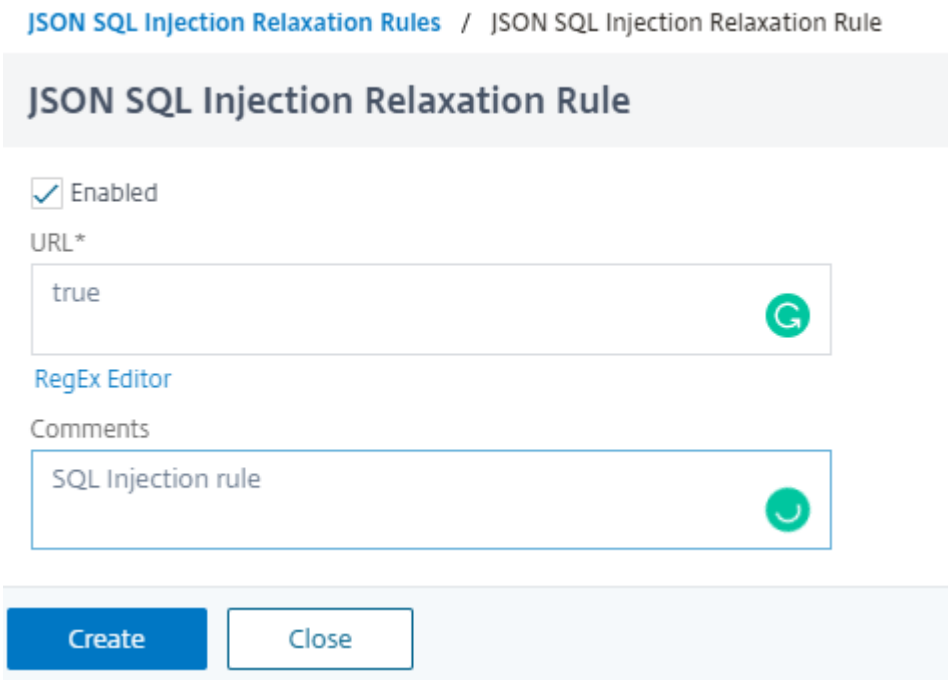
8. Haga clic en **OK**.



9. En la página **Perfil de Citrix Web App Firewall**, haga clic en **Reglas de relajación** en **Configuración avanzada**.
10. En la sección **Reglas de relajación**, seleccione Configuración de **inyección JSON SQL** y haga clic en **Modificar**.



11. En la página Regla de relajación de inyección JSON SQL, introduzca la URL a la que se debe enviar la solicitud. Todas las solicitudes enviadas a esta URL no se bloquearán.
12. Haga clic en **Crear**.



Configurar la relajación pormenorizada para la protección de inyección JSON SQL

Web App Firewall le ofrece la opción de relajar una clave o valor JSON específico de la comprobación de inspección de inyección SQL basada en JSON. Puede configurar varias opciones para relajar las cargas JSON mediante reglas de relajación pormenorizada.

Anteriormente, la única forma de configurar relajaciones para las comprobaciones de protección JSON era especificar la URL completa y eso evitaría la verificación de toda la URL.

La protección de seguridad SQL basada en JSON proporciona relajación para lo siguiente:

- Nombres clave
- Valores clave

La comprobación de protección SQL basada en JSON le permite configurar relajaciones que permiten patrones específicos y bloquean el resto. Por ejemplo, Web App Firewall tiene actualmente un conjunto predeterminado de más de 100 palabras clave SQL. Como los piratas informáticos pueden usar estas palabras clave en los ataques de inyección SQL, Web App Firewall marca todas como amenazas potenciales. Si quiere relajar una o más palabras clave que se consideran seguras para la ubicación específica, puede configurar una regla de relajación que pueda omitir el control de seguridad y bloquear el resto. Los comandos utilizados en las relajaciones tienen parámetros opcionales para Tipo de valor y Expresión de valor. Puede especificar si la expresión de valor es una expresión regular o una cadena literal. El tipo de valor se puede dejar en blanco o tiene la opción de seleccionar Palabra clave o Cadena especial.

> **Nota:**
>
> Las expresiones regulares son potentes. Especialmente si no está familiarizado con las expresiones regulares en formato PCRE, compruebe las expresiones regulares que escriba. Asegúrese de que definen exactamente la URL que quiere agregar como excepción, y nada más. El uso descuidado de caracteres comodín, y especialmente de la combinación de metacarácter o comodín punto-asterisco (.*), puede tener resultados que no quiere, como bloquear el acceso al contenido web que no pretendía bloquear o permitir un ataque que la comprobación de inyección JSON SQL habría bloqueado de otro modo.

Puntos a tener en cuenta

- La expresión de valor es un argumento opcional. Es posible que un nombre de campo no tenga ninguna expresión de valor.
- Un nombre de clave se puede enlazar a varias expresiones de valor.
- A las expresiones de valor se les debe asignar un tipo de valor. El tipo de valor puede ser: 1) Palabra clave, 2) SpecialString.
- Puede tener varias reglas de relajación por nombre de clave o combinación de URL.

Configurar la relajación pormenorizada JSON para los ataques de inyección de comandos mediante la interfaz

Para configurar la regla de relajación pormenorizada de archivos JSON, debe vincular las entidades de relajación pormenorizada al perfil de Web App Firewall.

En el símbolo del sistema, escriba:

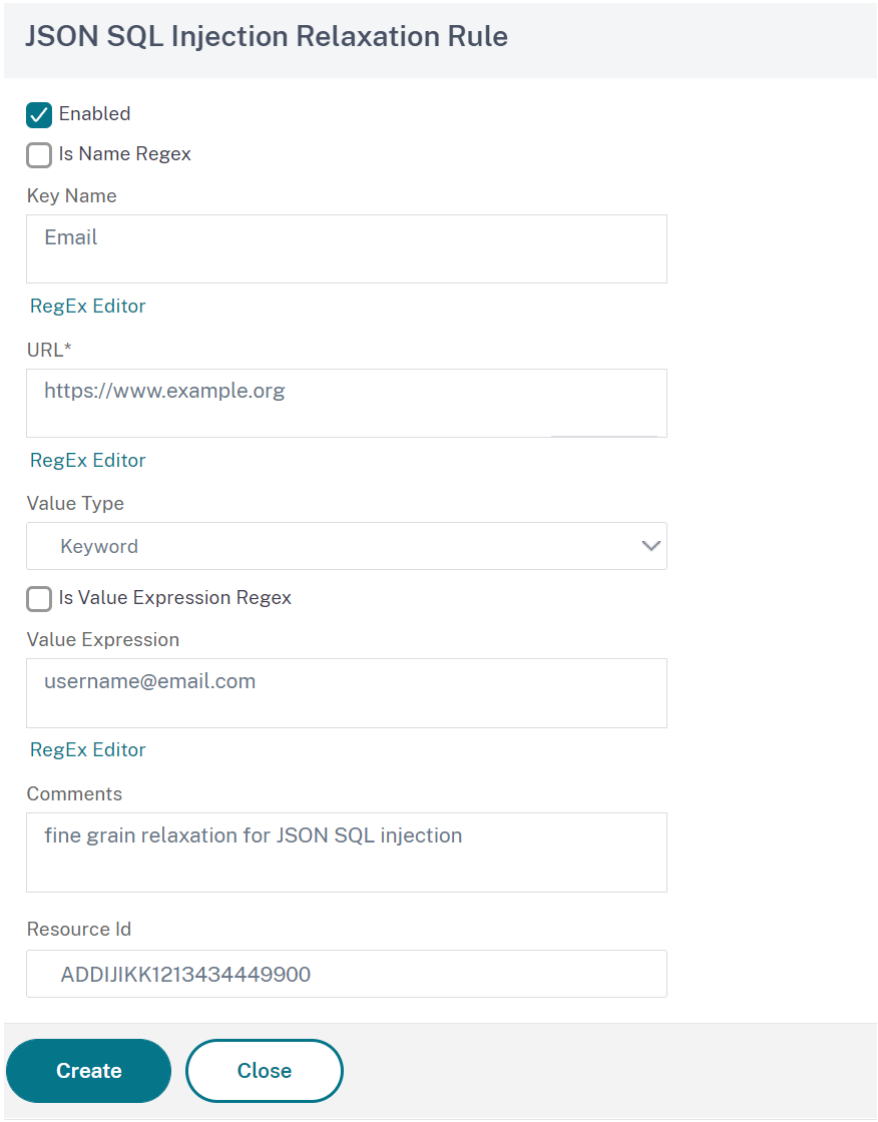
```
1 bind appfw profile <profile name> -jsoncmdURL <URL> -key <key name> -
     isregex <REGEX/NOTREGEX> -valueType <keyword/SpecialString> <value
     Expression> -isvalueRegex <REGEX/NOTREGEX>
2 <!--NeedCopy-->
```

Ejemplo:

```
1 bind appfw profile appprofile1 -jsonsqlurl www.example.com -key
     stn_name  -isRegex NOTREGEX -valueType Keyword  “union”  -
     isvalueRegex NOTREGEX
2 <!--NeedCopy-->
```


Para configurar la regla de relajación pormenorizada para ataques de inyección de comandos basados en JSON mediante la interfaz gráfica de usuario

1. Vaya a **Firewall de aplicaciones > Perfiles**, seleccione un perfil y haga clic en **Modificar**.
2. En el panel **Configuración avanzada**, haga clic en **Reglas de relajación**.
3. En la sección **Reglas de relajación**, seleccione un registro de **inyección JSON SQL** y haga clic en **Modificar**.
4. En el control deslizante **Regla de relajación de inyección JSON SQL**, haga clic en **Agregar**.
5. En la página **Regla de relajación de inyección JSON SQL**, defina los siguientes parámetros.
    a) Habilitado
    b) Is Name Regex
    c) Nombre de la clave
    d) URL
    e) Tipo de valor
    f) Comentarios
    g) ID de recurso
6. Haga clic en **Crear**.



Comprobación de protección de scripting de sitios JSON

April 21, 2022

Si una carga útil JSON entrante tiene datos de scripting de sitios maliciosos, WAF bloquea la solicitud. Los siguientes procedimientos explican cómo puede configurarlo a través de interfaces CLI y GUI.

Configurar la protección contra scripting de sitios JSON

Para configurar la protección contra scripting de sitios JSON, debe completar los siguientes pasos:

1. Agregue el perfil de firewall de aplicaciones como JSON.

2. Configurar la acción de scripting de sitios JSON para bloquear la carga maliciosa de scripting de sitios

Agregar perfil de firewall de aplicaciones de tipo JSON

Primero debe crear un perfil que especifique cómo el firewall de la aplicación debe proteger el contenido web JSON del ataque por scripting de sitios JSON.

En el símbolo del sistema, escriba:

```
add appfw profile <name> -type (HTML | XML | JSON)
```

> **Nota**:
>
> Cuando establece el tipo de perfil como JSON, no se aplicarán otras comprobaciones, como HTML o XML.

Ejemplo

```
add appfw profile profile1 -type JSON
```

Salida de ejemplo para la infracción de scripting de sitios JSON

```
JSONcross-site scriptingAction: block log stats
Payload: {
 ”username”:”<a href=”jAvAsCrIpT:alert(1)”>X</a>”,”password”:”xyz” }


Log message: Aug 19 06:57:33 <local0.info> 10.106.102.21
    08/19/2019:06:57:33 GMT  0-PPE-0 : default APPFW APPFW_JSON_cross-
    site scripting 58 0 :  10.102.1.98 12-PPE0 - profjson http://
    10.106.102.24/ Cross-site script check failed for object value(with
    violation=”Bad URL: jAvAsCrIpT:alert(1)”) starting at offset(12). <
    blocked>

Counters
    1  357000                  1 as_viol_json_xss
    3  0                       1 as_log_json_xss
    5  0                       1 as_viol_json_xss_profile appfw__(
       profjson)
    7  0                       1 as_log_json_xss_profile appfw__(
       profjson)

<!--NeedCopy-->
```


Configurar la acción de scripting de sitios JSON

Debe configurar una o más acciones de scripting de sitios JSON para proteger su aplicación de los ataques de scripting de sitios JSON.
En el símbolo del sistema, escriba:

```
set appfw profile <name> - JSONcross-site scriptingAction [block] [log] [
stats] [none]
```

Ejemplo

```
set appfw profile profile1 -JSONcross-site scriptingAction block
```

Las acciones de scripting de sitios disponibles son:
Bloquear: bloquear las conexiones que infrinjan esta comprobación de seguridad.
Registro: Registrar infracciones de esta comprobación de seguridad.
Estadísticas: genera estadísticas para esta comprobación de seguridad.
Ninguno: inhabilite todas las acciones de esta comprobación de seguridad.

> **Nota**:
> Para habilitar una o más acciones, escriba “set appfw profile - JSONCross-site ScriptingAction” seguido de las acciones que se van a habilitar.

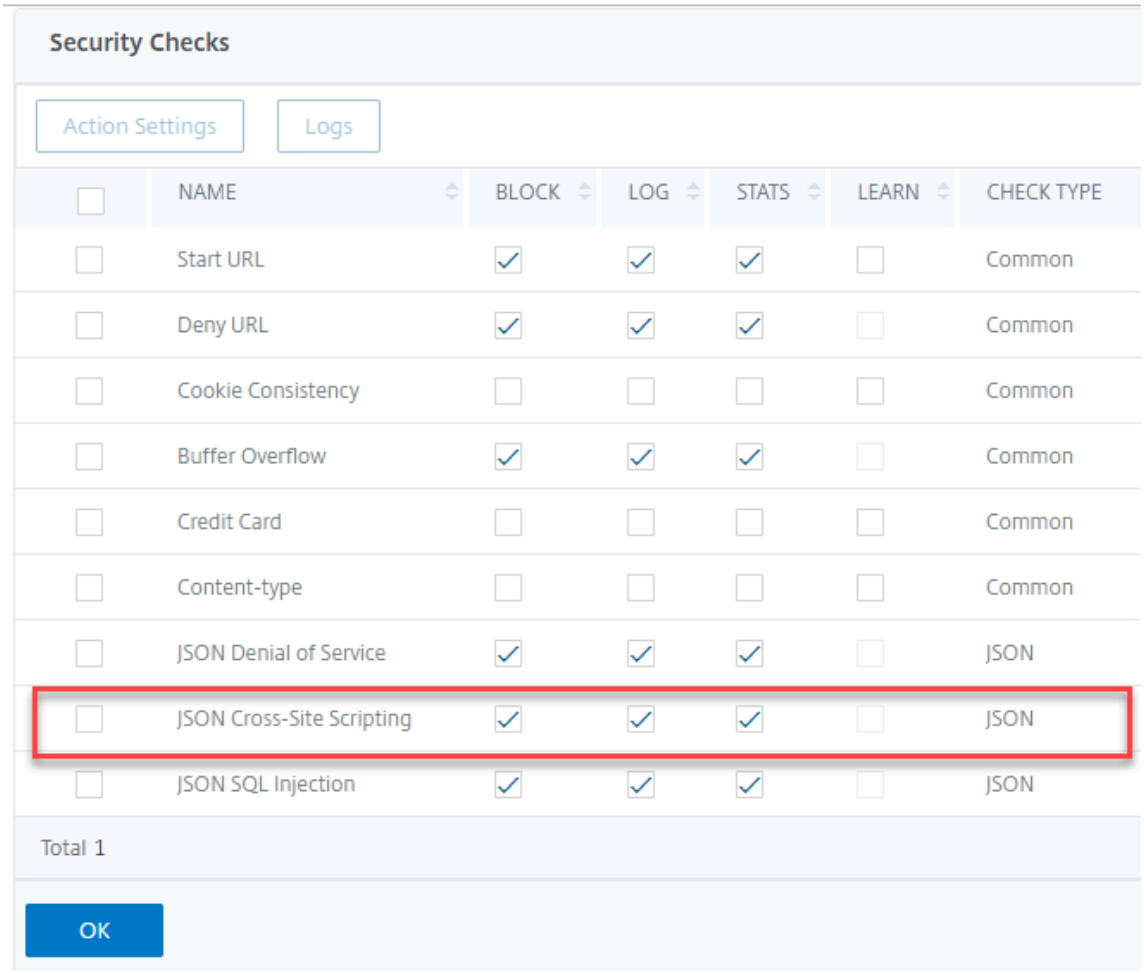
Ejemplo

```
set appfw profile profile1 -JSONSQLInjectionAction block log stat
```

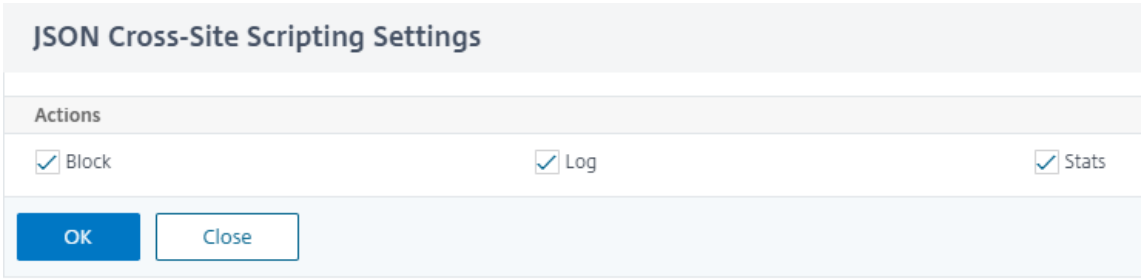
Configurar la protección contra scripting de sitios JSON (scripting de sitios) mediante la GUI de Citrix

Siga el procedimiento que se indica a continuación para establecer la configuración de protección contra scripting de sitios (scripting de sitios).

1. En el panel de navegación, vaya a **Seguridad** > **Perfiles**.
2. En la página **Perfiles**, haga clic en **Agregar**.
3. En la página **Perfil de Citrix Web App Firewall**, haga clic en **Comprobaciones de seguridad** en **Configuración avanzada**.
4. En la sección **Comprobaciones de seguridad**, vaya a Configuración **de scripting de sitios JSON (scripting de sitios)**.
5. Haga clic en el icono ejecutable cerca de la casilla de verificación.

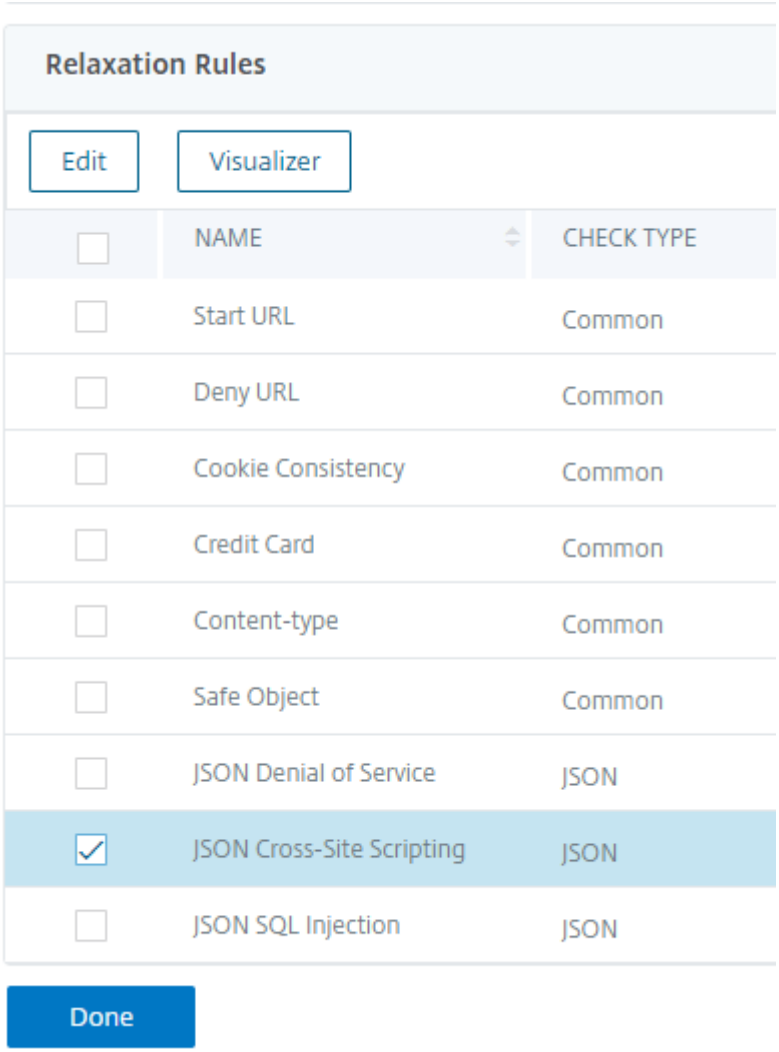


6. Haga clic en **Configuración de acción** para acceder a la página **Configuración de scripting de sitios JSON**.
7. Seleccione las acciones de scripting de sitios JSON.
8. Haga clic en **OK**.

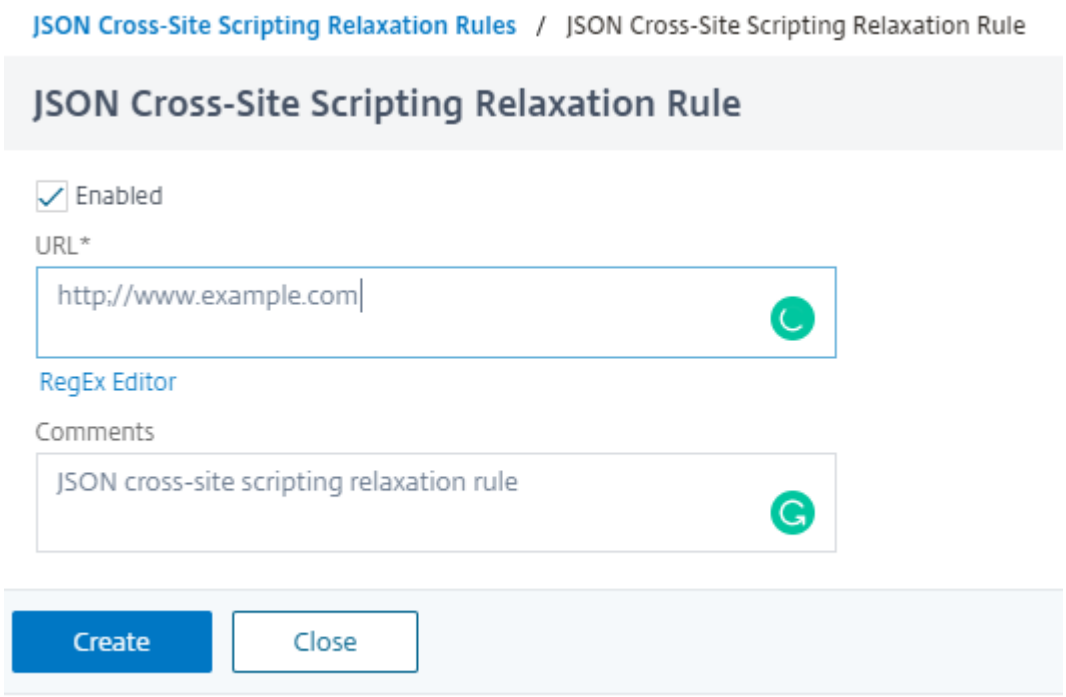


9. En la página **Perfil de Citrix Web App Firewall**, haga clic en **Reglas de relajación** en **Configuración avanzada**.
10. En la sección **Reglas de relajación**, seleccione Configuración de scripting de sitios JSON y haga

clic en **Modificar**.



11. En la página **Regla de relajación de scripting de sitios JSON**, haga clic en **Agregar** para agregar una regla de relajación de scripting de sitios JSON.
12. Introduzca la URL a la que se debe enviar la solicitud. Todas las solicitudes enviadas a esta URL no se bloquearán.
13. Haga clic en **Crear**.



Configurar una relajación pormenorizada para scripting de sitios basadas en JSON

Web App Firewall le ofrece la opción de relajar una clave o valor JSON específicos de la comprobación de inspección de scripting de sitios (XSS) basada en JSON. Puede configurar varias opciones para relajar las cargas JSON mediante reglas de relajación pormenorizada.
Anteriormente, la única forma de configurar relajaciones para las comprobaciones de protección JSON era especificar la URL completa y eso evitaría la verificación de toda la URL.
La protección de seguridad SQL basada en JSON proporciona relajación para lo siguiente:

- Nombres clave
- Valores clave

La protección contra scripting de sitios (XSS) basada en JSON le permite configurar relajaciones que permiten patrones específicos y bloquean el resto. Por ejemplo, Web App Firewall tiene actualmente un conjunto predeterminado de más de 100 palabras clave SQL. Como los piratas informáticos pueden usar estas palabras clave en los ataques de inyección SQL, Web App Firewall marca todas como amenazas potenciales. Si quiere relajar una o más palabras clave que se consideran seguras para la ubicación específica, puede configurar una regla de relajación que pueda omitir el control de seguridad y bloquear el resto. Los comandos utilizados en las relajaciones tienen parámetros opcionales para Tipo de valor y Expresión de valor. Puede especificar si la expresión de valor es una expresión regular o una cadena literal. El tipo de valor se puede dejar en blanco o tiene la opción de seleccionar Palabra clave o Cadena especial.

> **Nota:**
>
> Las expresiones regulares son potentes. Especialmente si no está familiarizado con las expresiones regulares en formato PCRE, compruebe las expresiones regulares que escriba. Asegúrese de que definen exactamente la URL que quiere agregar como excepción, y nada más. El uso descuidado de caracteres comodín, y especialmente de la combinación de metacarácter o comodín punto-asterisco (.*), puede tener resultados que no quiere, como bloquear el acceso al contenido web que no pretendía bloquear o permitir un ataque que la comprobación de inyección JSON SQL habría bloqueado de otro modo.

Puntos a tener en cuenta

- La expresión de valor es un argumento opcional. Es posible que un nombre de campo no tenga ninguna expresión de valor.
- Un nombre de clave se puede enlazar a varias expresiones de valor.
- A las expresiones de valor se les debe asignar un tipo de valor. Los tipos de valores son etiqueta, atributo y patrón.
- Puede tener varias reglas de relajación por combinación de nombre de clave/URL.

Configurar la relajación pormenorizada de JSON para ataques de inyección de scripting de sitios (XSS) mediante la interfaz de comandos

Para configurar la regla de relajación pormenorizada de archivos JSON, debe vincular las entidades de relajación pormenorizada al perfil de Web App Firewall.

En el símbolo del sistema, escriba:

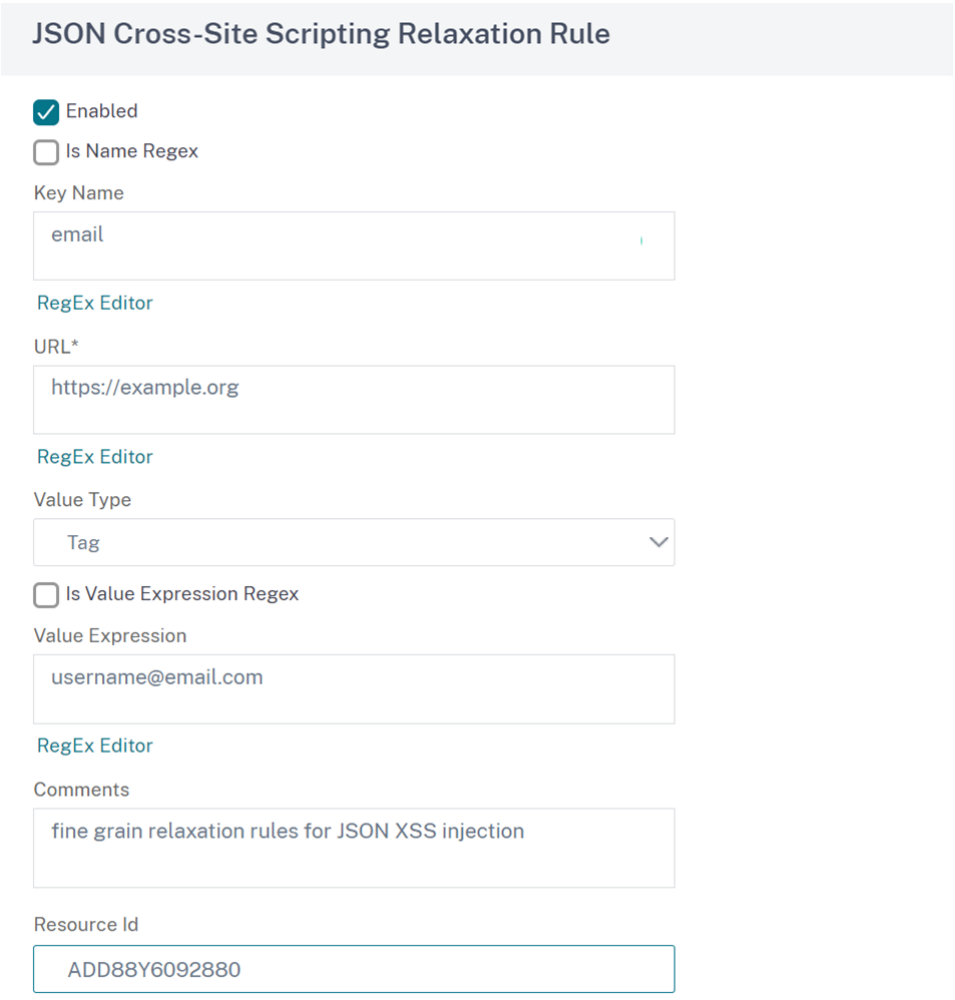
```
bind appfw profile <profile name> -jsonxssURL <URL> -key <key name> -
    isregex <REGEX/NOTREGEX> -valueType <keyword/SpecialString> <value
    Expression> -isvalueRegex <REGEX/NOTREGEX>
<!--NeedCopy-->
```

Ejemplo:

```
bind appfw profile appprofile1 -jsonxssurl www.example.com -key name  -
    isRegex NOTREGEX -valueType Tag  “sname”  -isvalueRegex NOTREGEX
<!--NeedCopy-->
```

Para configurar una regla de relajación pormenorizada de inyección de scripting de sitios (XSS) basada en JSON mediante la interfaz gráfica de usuario

1. Vaya a **Firewall de aplicaciones > Perfiles**, seleccione un perfil y haga clic en **Modificar**.
2. En el panel **Configuración avanzada**, haga clic en **Reglas de relajación**.
3. En la sección **Reglas de relajación**, seleccione un registro de inyección JSON SQL y haga clic en **Modificar**.
4. En el control deslizante **Reglas de relajación de scripting de sitios JSON**, haga clic en **Agregar**.
5. En la página **Regla de relajación de scripting de sitios JSON**, defina los siguientes parámetros.
   a) Habilitado
   b) Is Name Regex
   c) Nombre de la clave
   d) URL
   e) Tipo de valor
   f) Comentarios
   g) ID de recurso
6. Haga clic en **Crear**.



Comprobación de la protección de inyección de comandos

April 21, 2022

La comprobación de inyección de comandos JSON examina el tráfico JSON entrante en busca de comandos no autorizados que rompan la seguridad del sistema o lo modifican. Al examinar el tráfico, si se detectan comandos maliciosos, el dispositivo bloquea la solicitud o realiza la acción configurada.

En un ataque de inyección de comandos, el atacante intenta ejecutar comandos no autorizados en el sistema operativo Citrix ADC o en el servidor back-end. Para lograr esto, el atacante inyecta comandos del sistema operativo mediante una aplicación vulnerable. La aplicación back-end es vulnerable a los ataques de inyección si el dispositivo simplemente reenvía una solicitud sin ninguna comprobación de seguridad. Por lo tanto, es muy importante configurar una comprobación de seguridad para que el dispositivo Citrix ADC pueda proteger su aplicación web bloqueando los datos no seguros.

Cómo funciona la protección de inyección de comandos

1. Para una solicitud JSON entrante, WAF examina el tráfico en busca de palabras clave o caracteres especiales. Si la solicitud JSON no tiene patrones que coincidan con ninguna de las palabras clave o caracteres especiales denegados, se permite la solicitud. De lo contrario, la solicitud se bloquea, se descarta o se redirige en función de la acción configurada.
2. Si prefiere excluir una palabra clave o un carácter especial de la lista, puede crear una regla de relajación para evitar el control de seguridad en condiciones específicas.
3. Puede habilitar el registro para generar mensajes de registro. Puede supervisar los registros para determinar si las respuestas a las solicitudes legítimas se están bloqueando. Un gran aumento en la cantidad de mensajes de registro puede indicar intentos de lanzar un ataque.
4. También puede habilitar la función de estadísticas para recopilar datos estadísticos sobre infracciones y registros. Un aumento inesperado en el contador de estadísticas podría indicar que su aplicación está siendo atacada. Si las solicitudes legítimas se bloquean, es posible que tenga que volver a visitar la configuración para ver si debe configurar la nueva regla de relajación o modificar la existente.

Palabras clave y caracteres especiales denegados para la comprobación de inyección de comandos

Para detectar y bloquear los ataques de inyección de comandos JSON, el dispositivo tiene un conjunto de patrones (palabras clave y caracteres especiales) definidos en el archivo de firma predeterminado. A continuación se muestra una lista de palabras clave bloqueadas durante la detección de inyección de comandos


```
<commandinjection>
      <keyword type="LITERAL" builtin="ON">7z</keyword>
      <keyword type="LITERAL" builtin="ON">7za</keyword>
      <keyword type="LITERAL" builtin="ON">7zr</keyword>
...
</commandinjection>

<!--NeedCopy-->
```

Los caracteres especiales definidos en el archivo de firma son:
`| ; & $ > < '\ ! >> ##`

Configuración de la comprobación de inyección de comandos JSON mediante la CLI

En la interfaz de línea de comandos, puede usar el comando set appfw profile o agregar un comando appfw profile para configurar los ajustes de inyección de comandos JSON. Puede habilitar las acciones de bloqueo, registro y estadísticas. También debe establecer el tipo de inyección de comandos, como palabras clave y caracteres de cadena que quiere detectar en las cargas útiles.

En el símbolo del sistema, escriba:

```
set appfw profile <profile-name> -cmdInjectionAction <action-name> -CMDInjectionType
 <CMDInjectionType>]
```

> **Nota:**
>
> De forma predeterminada, la acción de inyección de comandos se establece como "estadísticas de registro de bloques". Además, el tipo de inyección de comando predeterminado se establece como`CmdSplCharANDKeyWord`. Después de una actualización, los perfiles de Firewall de aplicaciones web existentes tienen la acción configurada como "Ninguno".

Ejemplo:

```
set appfw profile profile1 -JSONCMDInjectionAction block -JSONCMDInjectionType
 CmdSplChar
```

Donde las acciones de inyección de comandos JSON disponibles son:

Ninguno: desactive la protección de inyección de comandos.
Registro: registra las infracciones de inyección de comandos para la comprobación de seguridad.
Bloquear: bloquea el tráfico que infringe la comprobación de seguridad de la inyección de comandos.
Estadísticas: genera estadísticas de infracciones de seguridad de inyección de comandos.

Donde los tipos de inyección de comandos JSON disponibles son:

`Cmd SplChar` - Comprueba los caracteres especiales
`CmdKeyWord` - Comprueba las palabras clave de inyección de comandos

`CmdSplCharANDKeyWord` - Esta es la acción predeterminada. La acción comprueba los caracteres especiales y la inyección de comandos. Palabras clave y bloques solo si ambos están presentes.
`CmdSplCharORKeyWord` - Comprueba los caracteres especiales y las palabras clave de inyección de comandos y los bloques si se encuentra alguno de ellos.

Configuración de reglas de relajación para la comprobación de protección de inyección de comandos

Si su aplicación requiere que omita la inspección de inyección de comandos JSON para un ELEMENTO o ATRIBUTO específico en la carga útil, puede configurar una regla de relajación.

Las reglas de relajación de inspección de inyección del comando JSON tienen la siguiente sintaxis.

```
bind appfw profile <profile name> -JSONCMDURL <expression> -comment <string
> -isAutoDeployed ( AUTODEPLOYED | NOTAUTODEPLOYED )-state ( ENABLED |
DISABLED )
```

Ejemplo de regla de relajación para Regex en el encabezado

```
bind appfw profile abc_json -jsoncmDURL http://1.1.1.1/hello.html
```

Visto y considerando: Que lo siguiente relaja las solicitudes de todas las URL alojadas en 1.1.1.1:

```
bind appfw profile abc_json -jsoncmDURL http://1.1.1.1/*"
```

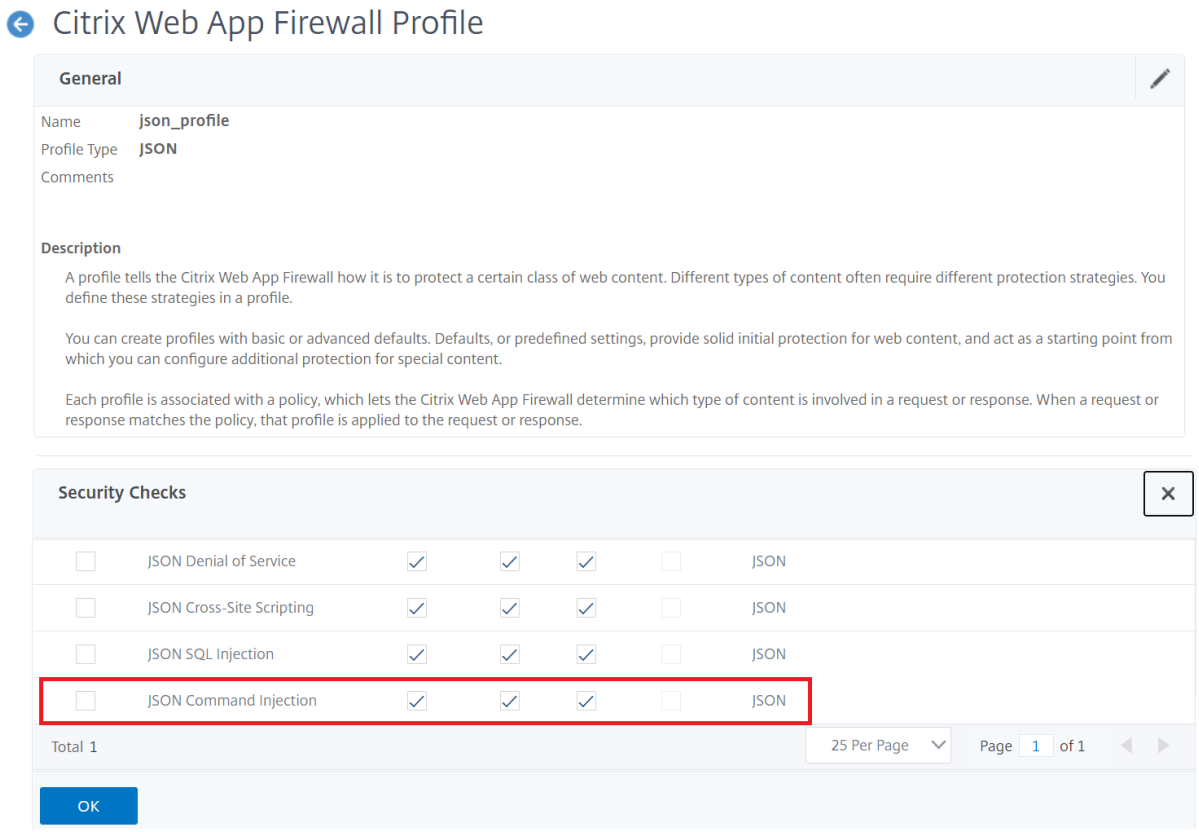
Para eliminar la relajación, use “desvincular”.

```
unbind appfw profile abc_json -jsoncmDURL  " http://1.1.1.1/*"
```

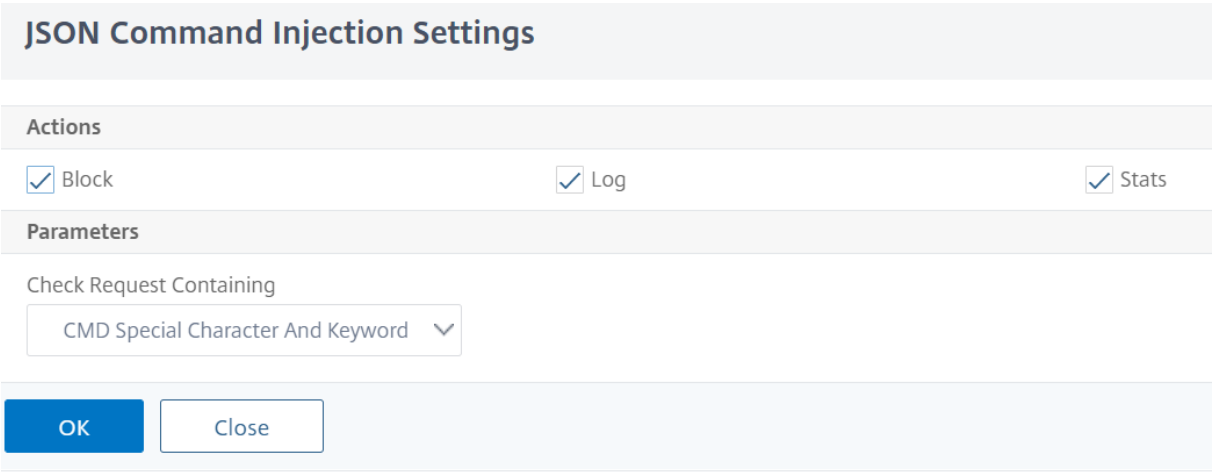
Configurar la comprobación de inyección de comandos JSON mediante la GUI

Complete los siguientes pasos para configurar la comprobación de inyección de comandos JSON.

1. Vaya a **Seguridad > Perfiles y Citrix Web App Firewall**.
2. En la página **Perfiles**, seleccione un perfil y haga clic en **Modificar**.
3. En la página **Perfil de Citrix Web App Firewall**, vaya a la sección **Configuración avanzada** y haga clic en **Comprobaciones de seguridad**.



1. En **la sección Controles de seguridad**, seleccione **Inyección de comandos JSON** y haga clic en Configuración de **acción**
2. En la página **Configuración de inyección de comandos JSON**, defina los siguientes parámetros:
   a) Acciones. Seleccione una o más acciones para realizar la comprobación de seguridad de la inyección de comandos JSON.
   b) Comprobar solicitud que contiene. Seleccione un patrón de inyección de comandos para comprobar si la solicitud entrante tiene el patrón.
3. Haga clic en **OK**.



Visualización de estadísticas de tráfico de inyección de comandos e infracciones

La página **Estadísticas de Citrix Web App Firewall** muestra los detalles del tráfico de seguridad y las infracciones de seguridad en formato tabular o gráfico.

Para ver las estadísticas de seguridad mediante la interfaz de comandos.

En el símbolo del sistema, escriba:

```
stat appfw profile profile1
```

Estadísticas de tráfico del perfil Appfw	Tasa (/s)	Total
Solicitudes	0	0
Bytes de solicitud	0	0
Respuestas	0	0
Bytes de respuesta	0	0
Aborta	0	0
Redireccionamientos	0	0
Tiempo de respuesta promedio a largo plazo (ms)	–	0
Tiempo de respuesta promedio reciente (ms)	–	0

Estadísticas de infracciones de HTML/XML/	Tasa (/s)	Total
URL de inicio	0	0
Denegar URL	0	0
Encabezado referer	0	0
Desbordamiento de	0	0
Consistencia de cookies	0	0
Secuestro de cookies	0	0
Etiqueta de formulario CSRF	0	0
Scripts HTML entre sitios	0	0
Inyección HTML SQL	0	0
Formato de campo	0	0
Coherencia de	0	0
Tarjeta de crédito	0	0
Objeto seguro	0	0
Infracciones de firma	0	0
Tipo de contenido	0	0
Denegación de servicio JSON	0	0
Inyección JSON SQL	0	0
Scripting entre sitios JSON	0	0
Tipos de carga de archivos	0	0
Deducir carga útil XML del tipo de contenido	0	0
Inyección de HTML CMD	0	0
Formato XML	0	0
Denegación de servicio XML (XDoS)	0	0
Validación de mensajes XML	0	0
Interoperabilidad de servicios web	0	0
Inyección XML SQL	0	0

Estadísticas de infracciones de HTML/XML/	Tasa (/s)	Total
Scripting entre sitios XML	0	0
Datos adjuntos XML	0	0
Infracciones de errores de	0	0
Infracciones genéricas XML	0	0
Infracciones totales	0	0

Estadísticas de registro HTML/XML/J	Tasa (/s)	Total
Iniciar registros de URL	0	0
Denegar registros de URL	0	0
Registros de encabezado de referencia	0	0
Registros de desbordamiento	0	0
Registros de consistencia de cookies	0	0
Registros de secuestro de cookies	0	0
CSRF a partir de registros de etiquetas	0	0
Registros de scripts HTML entre sitios	0	0
Registros de transformación de scripting de sitios HTML	0	0
Registros de inyección HTML SQL	0	0
Registros de transformación HTML SQL	0	0
Registros de formato de campo	0	0
Registros de coherencia de campo	0	0

Estadísticas de registro HTML/XML/J	Tasa (/s)	Total
Tarjetas de crédito	0	0
Registros de transformación de tarjetas de crédito	0	0
Registros de objetos seguros	0	0
Registros de firmas	0	0
Registros de tipos de contenido	0	0
Registros de denegación de servicio JSON	0	0
Registros de inyección JSON SQL	0	0
Registros de scripts JSON entre sitios	0	0
Registros de tipos de carga de archivos	0	0
Deducir carga útil XML del tipo de contenido L	0	0
Inyección de CMD JSON	0	0
Registros de inyección de comandos HTML	0	0
Registros en formato XML	0	0
Registros de denegación de servicio (XDoS) XML	0	0
Registros de validación de mensajes XML	0	0
Registros de WSI	0	0
Registros de inyección XML SQL	0	0
Registros de scripts XML entre sitios	0	0
Registros de datos adjuntos XML	0	0

Estadísticas de registro HTML/XML/J	Tasa (/s)	Total
Registros de errores SOAP	0	0
Registros genéricos XML	0	0
Mensajes de registro totales	0	0

Tasa (/s) de estadísticas de respuesta a errores del servidor | Total |
|—|–|–|
Errores de cliente HTTP (4xx Resp) | 0 | 0| Errores del servidor
HTTP (5xx Resp) | 0 | 0 |

Estadísticas de registro HTML/XML/J	Tasa (/s)	Total
Registros de inyección de comandos JSON	0	0
Registros en formato XML	0	0

Ver las estadísticas de inyección de comandos JSON mediante la GUI de Citrix ADC

Complete los siguientes pasos para ver las estadísticas de inyección de comandos:

1. Vaya a **Seguridad > Citrix Web App Firewall > Perfiles**.
2. En el panel de detalles, seleccione un perfil de Web App Firewall y haga clic en **Estadísticas**.
3. La página **Estadísticas de Citrix Web App Firewall** muestra los detalles del tráfico y la infracción de la inyección de comandos JSON.
4. Puede seleccionar **Vista tabular** o cambiar a **Vista gráfica** para mostrar los datos en formato tabular o gráfico.

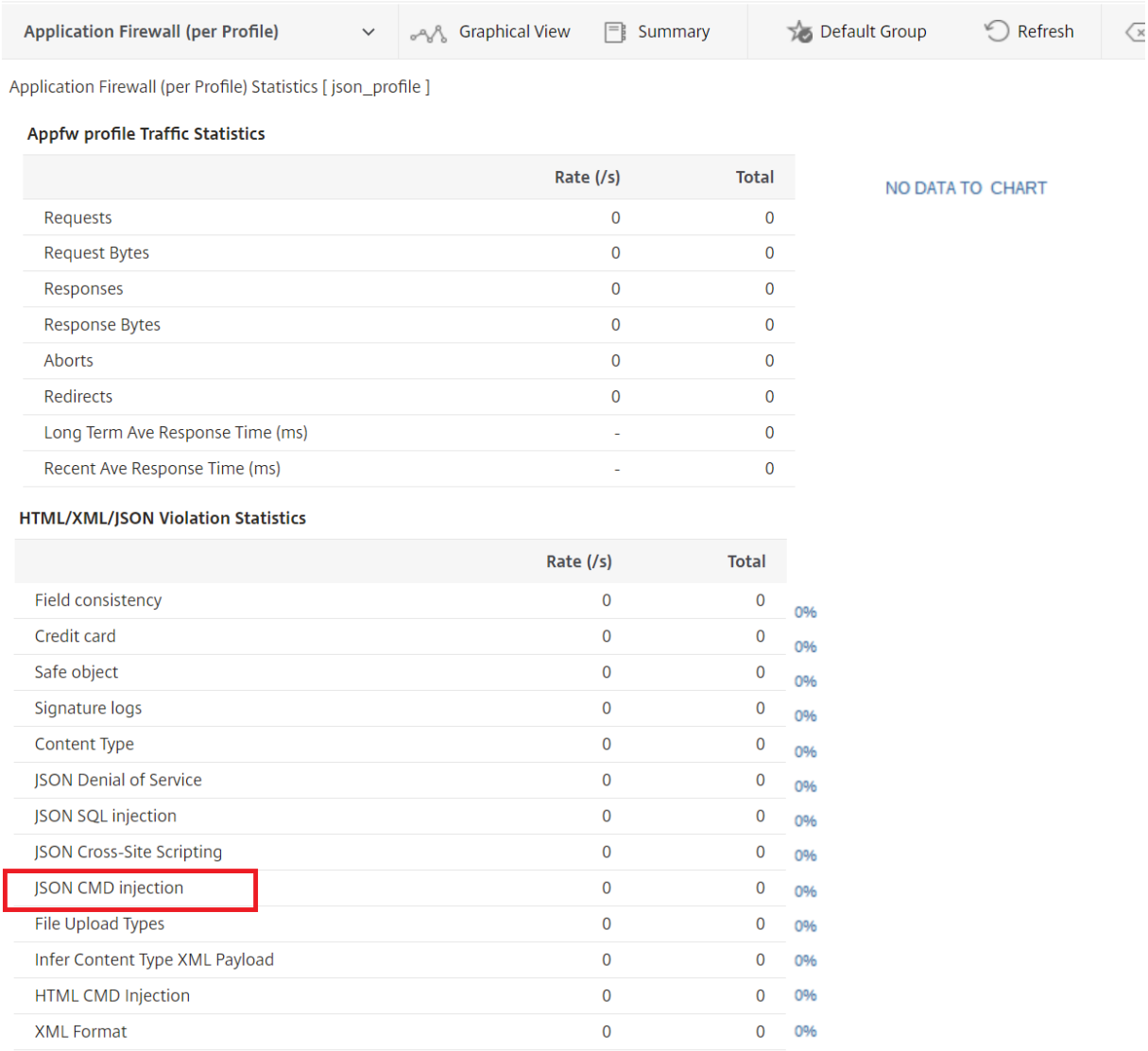
Estadísticas de tráfico de inyección de comandos J

HTML/XML/JSON Log Statistics

	Rate (/s)	Total
Start URL logs	0	0
Deny URL logs	0	0
Field consistency logs	0	0
Credit cards	0	0
Credit card transform logs	0	0
Safe object logs	0	0
Signature logs	0	0
Content Type logs	0	0
JSON Denial of Service logs	0	0
JSON SQL injection logs	0	0
JSON Cross-Site Scripting logs	0	0
JSON CMD injection logs	0	0
File upload types logs	0	0
Infer Content Type XML Payload Logs	0	0

JSON CMD injection logs: X
Number of JSON Command Injection security check log messages generated by the Application Firewall.

Estadísticas de infracción de la inyección de comandos



Configurar relajación pormenorizada para la inyección de comandos JSON

Web App Firewall le ofrece la opción de relajar una clave o valor JSON específicos de la comprobación de inyección de comandos basada en JSON. Puede omitir por completo la inspección de uno o más campos configurando las reglas de relajación pormenorizada.

Anteriormente, la única forma de configurar relajaciones para las comprobaciones de protección JSON era especificar la URL completa y eso evitaría la verificación de toda la URL.

La protección de seguridad de inyección de comandos basada en JSON proporciona relajación para lo siguiente:

- Nombres clave
- Valores clave

La protección de inyección de comandos basada en JSON le permite configurar relajaciones que permiten patrones específicos y bloquean el resto. Por ejemplo, Web App Firewall tiene actualmente un conjunto predeterminado de más de 100 palabras clave SQL. Como los piratas informáticos pueden usar estas palabras clave en los ataques de inyección de comandos, Web App Firewall marca todas ellas como amenazas potenciales. Si quiere relajar una o más palabras clave que se consideran seguras para la ubicación específica, puede configurar una regla de relajación que pueda omitir el control de seguridad y bloquear el resto. Los comandos utilizados en las relajaciones tienen parámetros opcionales para Tipo de valor y Expresión de valor. Puede especificar si la expresión de valor es una expresión regular o una cadena literal. El tipo de valor se puede dejar en blanco o tiene la opción de seleccionar Palabra clave o Cadena especial.

> **Nota:**
>
> Las expresiones regulares son potentes. Especialmente si no está familiarizado con las expresiones regulares en formato PCRE, compruebe las expresiones regulares que escriba. Asegúrese de que definen exactamente la URL que quiere agregar como excepción, y nada más. El uso descuidado de caracteres comodín, y especialmente de la combinación de metacarácter o comodín punto-asterisco (.*), puede tener resultados que no quiere, como bloquear el acceso al contenido web que no pretendía bloquear o permitir un ataque que la comprobación de inyección JSON SQL habría bloqueado de otro modo.

Puntos a tener en cuenta

- La expresión de valor es un argumento opcional. Es posible que un nombre de campo no tenga ninguna expresión de valor.
- Un nombre de clave se puede enlazar a varias expresiones de valor.
- A las expresiones de valor se les debe asignar un tipo de valor. El tipo de valor puede ser: 1) Palabra clave, 2) SpecialString.
- Puede tener varias reglas de relajación por combinación de nombre de clave/URL.

Configurar la relajación pormenorizada JSON para los ataques de inyección de comandos mediante la interfaz

Para configurar la regla de relajación pormenorizada de archivos JSON, debe vincular las entidades de relajación pormenorizada al perfil de Web App Firewall.

En el símbolo del sistema, escriba:

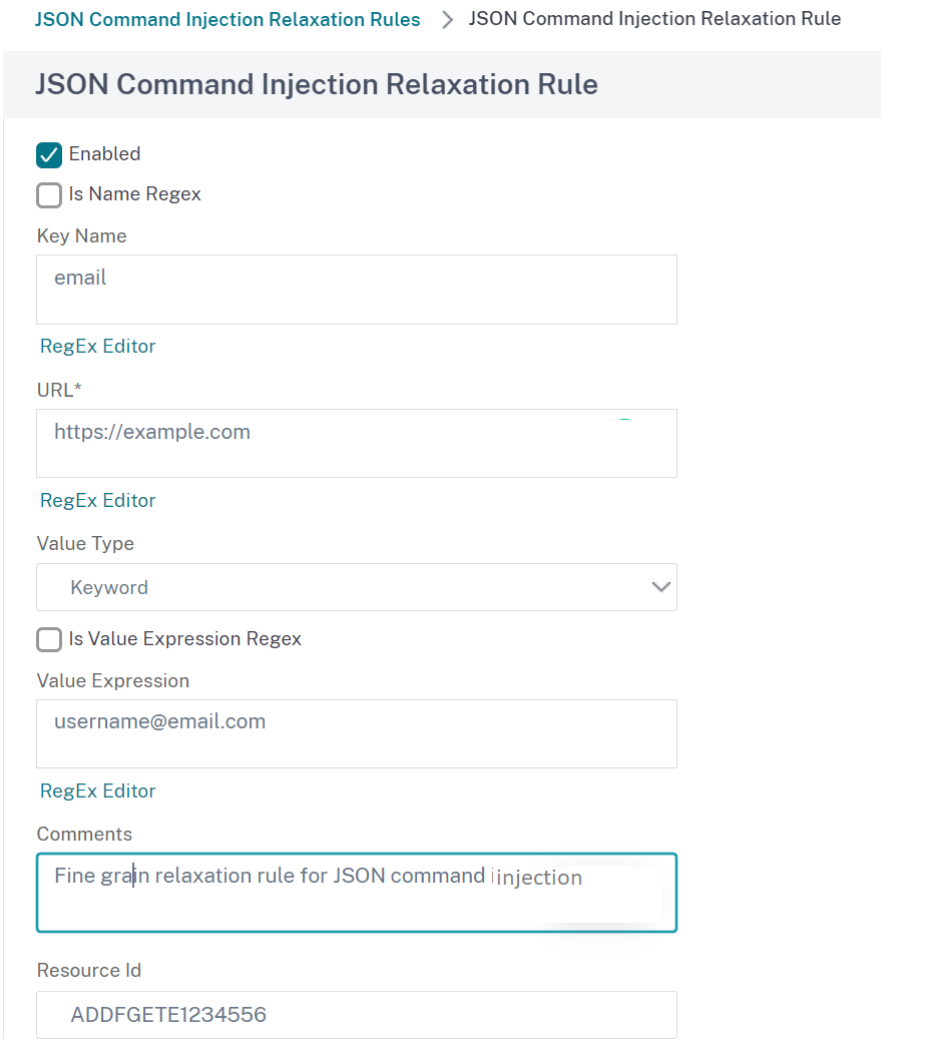
```
1 bind appfw profile <profile name> -jsoncmdURL <URL> -key <key name> -
     valueType <keyword/SpecialString> <value Expression>
2 <!--NeedCopy-->
```


Ejemplo:

```
bind appfw profile appprofile1 -jsoncmdurl www.example.com -key blg_cnt -
isRegex NOTREGEX -valueType Keyword “cat” -isvalueRegex NOTREGEX
```

Para configurar la regla de relajación pormenorizada para ataques de inyección de comandos basados en JSON mediante la interfaz gráfica de usuario

1. Vaya a **Firewall de aplicaciones > Perfiles**, seleccione un perfil y haga clic en **Modificar**.
2. En el panel **Configuración avanzada**, haga clic en **Reglas de relajación**.
3. En la sección **Reglas de relajación**, seleccione un registro de **inyección de comandos JSON** y haga clic en **Modificar**.
4. En el regulador **Regla de relajación de inyección de comandos JSON**, haga clic en **Agregar**.
5. En la página **Regla de relajación de inyección de comandos JSON**, defina los siguientes parámetros.
    a) Habilitado
    b) Is Name Regex
    c) Nombre de la clave
    d) URL
    e) Tipo de valor
    f) Comentarios
    g) ID de recurso
6. Haga clic en **Crear**.



Administración de tipos de contenido

January 12, 2021

Los servidores web agregan un encabezado Content-Type con una definición MIME/Type para cada tipo de contenido. Los servidores web sirven muchos tipos diferentes de contenido. Por ejemplo, HTML estándar tiene asignado el tipo MIME "text/html". A las imágenes JPG se les asigna el tipo de contenido "image/jpeg" o "image/jpg". Un servidor web normal puede servir diferentes tipos de contenido, todo definido en el encabezado Tipo de contenido por el MIME/tipo asignado.

Muchas reglas de filtrado de Web App Firewall están diseñadas para filtrar un tipo de contenido específico. Las reglas de filtrado se aplican a un tipo de contenido, como HTML, y a menudo son inapropiadas al filtrar un tipo diferente de contenido (como imágenes). Como resultado, Web App Firewall

intenta determinar el tipo de contenido de las solicitudes y respuestas antes de filtrarlas. Si un servidor web o explorador no agrega un encabezado Content-Type a una solicitud o respuesta, el Web App Firewall aplica un tipo de contenido predeterminado y filtra el contenido en consecuencia.

El tipo de contenido predeterminado suele ser "application/octet-stream" con la definición MIME y tipo más genérica. El MIME/tipo es apropiado para cualquier tipo de contenido que un servidor web pueda servir. Pero no proporciona mucha información al Web App Firewall para permitirle elegir el filtrado adecuado. Si un servidor web protegido está configurado para agregar encabezados de tipo de contenido precisos, puede crear un perfil para el servidor web y asignarle un tipo de contenido predeterminado. Esto se hace para mejorar tanto la velocidad como la precisión del filtrado.

También puede configurar una lista de tipos de contenido de solicitud permitidos para un perfil específico. Cuando se configura esta función, si Web App Firewall filtra una solicitud que no coincide con uno de los tipos de contenido permitidos, bloquea la solicitud. Después de la actualización de la versión 10.5 a la 11.0, los tipos de contenido desconocidos que no están en la lista predeterminada de tipos de contenido permitidos no se vinculan. Puede agregar otros tipos de contenido que quiere que se les permita a las reglas relajadas.

Las solicitudes siempre deben ser de los tipos "application/x-www-form-urlencoded", "multipart/form-data" o "text/x-gwt-rpc". El Web App Firewall bloquea cualquier solicitud que tenga cualquier otro tipo de contenido designado.

> **Nota**
>
> No puede incluir los tipos de contenido "application/x-www-form-urlencoded" o "multipart/form-data" en la lista de tipos de contenido de respuesta permitidos.

Para establecer el tipo de contenido de solicitud predeterminado mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos:

- `set appfw profile <name> -requestContentType <type>`
- `save ns config`

Ejemplo

En el ejemplo siguiente se establece el tipo de contenido "text/html" como predeterminado para el perfil especificado:

```
1 set appfw profile profile1 -requestContentType "text/html"
2 save ns config
3 <!--NeedCopy-->
```


Para quitar el tipo de contenido de solicitud predeterminado definido por el usuario mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos:

- `unset appfw profile <name> -requestContentType <type>`
- `save ns config`

Ejemplo

En el ejemplo siguiente se desactiva el tipo de contenido predeterminado de “text/html” para el perfil especificado, lo que permite que el tipo vuelva a “application/octet-stream”:

```
1 unset appfw profile profile1 -requestContentType ”text/html”
2 save ns config
3 <!--NeedCopy-->
```

> **Nota**
>
> Utilice siempre el último encabezado de tipo de contenido para procesar y elimine los encabezados de tipo de contenido restantes si hay alguno que garantice que el servidor back-end recibe una solicitud con un solo tipo de contenido.
>
> Para bloquear las solicitudes que se pueden omitir, agregue una directiva de Web App Firewall con la regla HTTP.REQ.HEADER (“content-type”).COUNT.GT(1)’ y el perfil como *appfw_block*.
>
> Si se recibe una solicitud sin un encabezado Content-Type o si la solicitud tiene encabezado Content-Type sin ningún valor, Web App Firewall aplica el valor **RequestContentType** configurado y procesa la solicitud en consecuencia.

Para establecer el tipo de contenido de respuesta predeterminado mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos:

- `set appfw profile <name> -responseContentType <type>`
- `save ns config`

Ejemplo

En el ejemplo siguiente se establece el tipo de contenido “text/html” como predeterminado para el perfil especificado:


```
set appfw profile profile1 -responseContentType ”text/html”
save ns config
<!--NeedCopy-->
```

Para quitar el tipo de contenido de respuesta predeterminado definido por el usuario mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos:

- `unset appfw profile <name> -responseContentType <type>`
- `save ns config`

Ejemplo

En el ejemplo siguiente se desactiva el tipo de contenido predeterminado de “text/html” para el perfil especificado, lo que permite que el tipo vuelva a “application/octet-stream”:

```
unset appfw profile profile1 -responseContentType ”text/html”
save ns config
<!--NeedCopy-->
```

Para agregar un tipo de contenido a la lista de tipos de contenido permitidos mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos:

- `bind appfw profile <name> -ContentType <contentTypeName>`
- `save ns config`

Ejemplo

En el ejemplo siguiente se agrega el tipo de contenido “text/shtml” a la lista de tipos de contenido permitidos para el perfil especificado:

```
bind appfw profile profile1 -contentType ”text/shtml”
save ns config
<!--NeedCopy-->
```


Para quitar un tipo de contenido de la lista de tipos de contenido permitidos mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos:

- `unbind appfw profile <name> -ContentType <contentTypeName>`
- `save ns config`

Ejemplo

En el ejemplo siguiente se quita el tipo de contenido “text/shtml” de la lista de tipos de contenido permitidos para el perfil especificado:

```
1 unbind appfw profile profile1 -contentType ”text/shtml”
2 save ns config
3 <!--NeedCopy-->
```

Administrar tipos de contenido con código urlencoded y multipart-form

Citrix ADC Web App Firewall ahora le permite configurar tipos de contenido codificado por Urlencoded y Multipart-Form para formularios. La configuración del tipo de contenido es similar a la lista XML y JSON. En función de la configuración, Web App Firewall clasifica las solicitudes e inspecciona el tipo de contenido codificado por urlencoded o multipart-form.

Para configurar el perfil de Web App Firewall con tipos de contenido codificado por Urlencoded y Multipart-Form
En el símbolo del sistema, escriba:

```
bind appfw profile p2 -contentType <string>
```

Ejemplo:

```
bind appfw profile p2 -contentType UrlencodedFormContentType
```

```
bind appfw profile p2 -ContentType appfwmultipartform
```

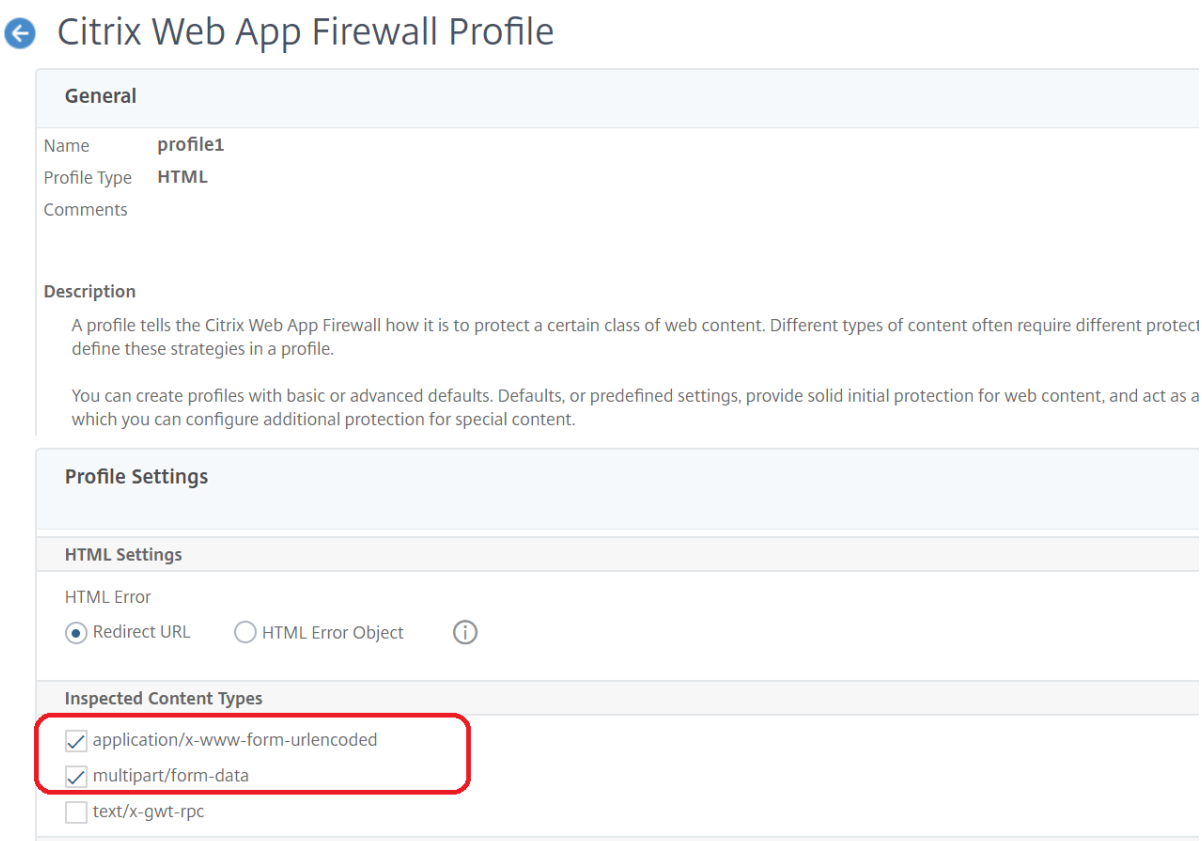
Para administrar los tipos de contenido predeterminados y permitidos mediante la interfaz gráfica de usuario

1. Vaya a **Seguridad** > **Web App Firewall** > **Perfiles**.
2. En el panel de detalles, seleccione el perfil que quiere configurar y, a continuación, haga clic en **Modificar**. Aparece el cuadro de diálogo **Configurar perfil de Web App Firewall**.

3. En el cuadro de diálogo **Configurar perfil de Web App Firewall**, haga clic en la ficha **Configuración**.
4. En la ficha **Configuración**, desplácese hacia abajo hasta la mitad del área Tipo de contenido.
5. En el área Tipo de contenido, configure el tipo de contenido de solicitud o respuesta predeterminado:
   - Para configurar el tipo de contenido de solicitud predeterminado, escriba la definición MIE/tipo del tipo de contenido que quiere utilizar en el cuadro de texto Solicitud predeterminada.
   - Para configurar el tipo de contenido de respuesta predeterminado, escriba la definición MIE/tipo del tipo de contenido que quiere utilizar en el cuadro de texto Respuesta predeterminada.
   - Para crear un nuevo tipo de contenido permitido, haga clic en **Agregar**. Aparece el cuadro de diálogo **Agregar tipo de contenido permitido**.
   - Para modificar un tipo de contenido permitido existente, seleccione ese tipo de contenido y, a continuación, haga clic en **Abrir**. Aparece el cuadro de diálogo **Modificar tipo de contenido permitido**.
6. Para administrar los tipos de contenido permitidos, haga clic en Administrar tipos de contenido permitidos.
7. Para agregar un nuevo tipo de contenido o modificar un tipo de contenido existente, haga clic en Agregar o Abrir y, en el cuadro de diálogo **Agregar tipo** de **contenido permitido o Modificar tipo** de contenido permitido, siga estos pasos.
   a) Active o desactive la casilla de verificación Activado para incluir el tipo de contenido en la lista de tipos de contenido permitidos o excluirlo de ella.
   b) En el cuadro de texto Tipo de contenido, escriba una expresión regular que describa el tipo de contenido que quiere agregar o cambie la expresión regular de tipo de contenido existente.
      Los tipos de contenido tienen el mismo formato que las descripciones de tipos MIME.
      > **Nota:**
      > Puede incluir cualquier tipo MIME válido en la lista de tipos de contenido permitidos. Dado que muchos tipos de documentos pueden contener contenido activo y, por lo tanto, pueden contener contenido malintencionado, debe tener precaución al agregar tipos MIME a esta lista.
   c) Proporcione una breve descripción que explique el motivo de agregar este tipo MIME concreto a la lista de tipos de contenido permitidos.
   d) Haga clic en **Crear** o en **Aceptar** para guardar los cambios.
8. Haga clic en **Cerrar** para cerrar el cuadro de diálogo Administrar tipos de contenido permitidos y volver a la ficha **Configuración**.
9. Haga clic en **Aceptar** para guardar los cambios.

Para administrar los tipos de contenido con código Urlencoded y Multipart-form mediante la GUI de Citrix ADC

1. Vaya a **Seguridad** > **Web App Firewall** > **Perfiles**.
2. En el panel de detalles, seleccione el perfil que quiere configurar y, a continuación, haga clic en **Modificar**.
3. En la página **Configurar perfil de Web App Firewall**, seleccione **Configuración de perfil** en la sección **Configuración avanzada**.
4. En la sección **Tipo de contenido inspeccionado**, defina los siguientes parámetros:
   a) application/x-www-form-urlencoded. Active la casilla de verificación para inspeccionar el tipo de contenido codificado por Urlencoded.
   b) multipart/form-datos. Seleccione la comprobación para inspeccionar el tipo de contenido de formulario Multipart-form.
5. Haga clic en **Aceptar**.



Perfiles

August 20, 2021

Un perfil es una colección de configuraciones de seguridad que se utilizan para proteger tipos específicos de contenido web o partes específicas de su sitio web. En un perfil, se determina cómo aplica el Web App Firewall cada uno de sus filtros (o comprobaciones) a las solicitudes a los sitios web y a las respuestas de los mismos. El Web App Firewall admite dos tipos de perfiles: Cuatro perfiles integrados (predeterminados) que no requieren configuración adicional y perfiles definidos por el usuario que requieren configuración adicional.

Perfiles integrados

Los cuatro perfiles integrados de Web App Firewall proporcionan una protección sencilla para aplicaciones y sitios web que no requieren protección o a los que los usuarios no deben acceder directamente en absoluto. Estos tipos de perfil son:

- **APPFW_BYPASS.** Omite todo el filtrado de Web App Firewall y envía el tráfico no modificado a la aplicación protegida o al sitio web, o al cliente.
- **APPFW_RESET.** Restablece la conexión, lo que requiere que el cliente restablezca su sesión visitando una página de inicio designada.
- **APPFW_DROP.** Deja caer todo el tráfico hacia o desde la aplicación protegida o sitio web, y no envía ninguna respuesta de ningún tipo al cliente.
- **APPFW_BLOCK.** Bloquea el tráfico hacia o desde la aplicación protegida o el sitio web.

Los perfiles integrados se utilizan exactamente igual que los perfiles definidos por el usuario, configurando una directiva que seleccione el tráfico al que quiere aplicar el perfil y asociando el perfil a la directiva. Dado que no es necesario configurar una directiva integrada, proporciona una forma rápida de permitir o bloquear tipos especificados de tráfico o tráfico que se envía a aplicaciones o sitios web específicos.

Perfiles definidos por el usuario

Los perfiles definidos por el usuario son perfiles creados y configurados por los usuarios. A diferencia de los perfiles predeterminados, debe configurar un perfil definido por el usuario antes de que sea útil filtrar el tráfico hacia y desde las aplicaciones protegidas.

Hay tres tipos de perfil definido por el usuario:

- **HTML.** Protege páginas web basadas en HTML.
- **XML.** Protege los sitios web y los servicios web basados en XML.

- **Web 2.0.** Protege el contenido web 2.0 que combina contenido HTML y XML, como fuentes ATOM, blogs y fuentes RSS.

El Web App Firewall tiene una serie de comprobaciones de seguridad, todas las cuales se pueden habilitar o inhabilitar y configurar de varias maneras en cada perfil. Cada perfil también tiene una serie de configuraciones que controlan cómo maneja los diferentes tipos de contenido. Por último, en lugar de configurar manualmente todas las comprobaciones de seguridad, puede habilitar y configurar la función de aprendizaje. Esta función observa el tráfico normal hacia los sitios web protegidos durante un período de tiempo y utiliza esas observaciones para proporcionarle una lista personalizada de excepciones recomendadas (*relajaciones*) a algunas comprobaciones de seguridad y reglas adicionales para otras comprobaciones de seguridad.

Durante la configuración inicial, ya sea mediante el Asistente para Web App Firewall o manualmente, normalmente se crea un perfil de propósito general para proteger todo el contenido de los sitios web que no esté cubierto por un perfil más específico. Después de eso, puede crear tantos perfiles específicos como quiera para proteger contenido más especializado.

El panel Perfiles consta de una tabla que contiene los siguientes elementos:

nombre. Muestra todos los perfiles de Web App Firewall configurados en el dispositivo.

Firma encuadernada. Muestra el objeto de firmas enlazado al perfil de la columna anterior, si lo hay.

Directivas. Muestra la directiva Web App Firewall que invoca el perfil en la columna situada más a la izquierda de esa fila, si la hay.

Comentarios. Muestra el comentario asociado al perfil en la columna situada más a la izquierda de esa fila, si lo hay.

Tipo de perfil. Muestra el tipo de perfil. Los tipos son Integrado, HTML, XML y Web 2.0.

Encima de la tabla hay una fila de botones y una lista desplegable que le permiten crear, configurar, eliminar y ver información sobre sus perfiles:

- **Add:** Agregue un nuevo perfil a la lista.
- **Modificar.** Modifique el perfil seleccionado.
- **Eliminar.** Elimine el perfil seleccionado de la lista.
- **Estadísticas.** Ver las estadísticas del perfil seleccionado.
- **Acción.** Lista desplegable que contiene comandos adicionales. Actualmente le permite importar un perfil exportado desde otra configuración de Web App Firewall.

Creación de perfiles de Web App Firewall

July 8, 2022

Puede crear un perfil de Web App Firewall de dos formas: mediante la línea de comandos y mediante la interfaz gráfica de usuario. Para crear un perfil mediante la línea de comandos, es necesario especificar opciones en la línea de comandos. El proceso es similar al de configurar un perfily, salvo algunas excepciones, los dos comandos toman los mismos parámetros.

La creación de un perfil mediante la interfaz gráfica de usuario requiere que especifique solo dos opciones. Especifica *los valores predeterminados*básicos o avanzados, la configuración predeterminada de las distintas comprobaciones y configuraciones de seguridad que forman parte de un perfil, y elige el *tipo* de perfil para que coincida con el tipo de contenido que el perfil pretende proteger. También puede, opcionalmente, agregar un comentario. Después de crear el perfil, debe configurarlo seleccionándolo en el panel de datos y, a continuación, haciendo clic en **Modificar**.

Si piensa utilizar la función de aprendizaje o habilitar y configurar muchas protecciones avanzadas, debe elegir los valores predeterminados avanzados. En particular, si va a configurar cualquiera de las comprobaciones de inyección SQL, las comprobaciones de scripts entre sitios, cualquier comprobación que ofrezca protección contra ataques de formularios web o la comprobación de coherencia de cookie, debe planear utilizar la función de aprendizaje. A menos que incluya las excepciones adecuadas para sus sitios web protegidos al configurar estas comprobaciones, pueden bloquear el tráfico legítimo. Anticipar todas las excepciones sin crear ninguna demasiado amplia es difícil. La función de aprendizaje facilita mucho esta tarea. De lo contrario, los valores predeterminados básicos son rápidos y deben proporcionar la protección que necesitan sus aplicaciones web.

Existen tres tipos de perfiles:

- **HTML.** Protege los sitios web estándar basados en HTML.
- **XML.** Protege los servicios web y los sitios web basados en XML.
- **Web 2.0 (HTML XML).** Protege sitios web que contienen elementos HTML y XML, como feeds ATOM, blogs y fuentes RSS.

También hay algunas restricciones sobre el nombre que puede dar a un perfil. El nombre de un perfil no puede ser el mismo que el nombre asignado a cualquier otro perfil o acción de ninguna función del dispositivo NetScaler. Ciertos nombres de acción o perfil se asignan a acciones o perfiles integrados y nunca se pueden usar para perfiles de usuario. Encontrará una lista completa de nombres no permitidos en la información complementariadel perfil de Web App Firewall. Si intenta crear un perfil con un nombre que ya se ha utilizado para una acción o un perfil, se muestra un mensaje de error y no se crea el perfil.

Para crear un perfil de Web App Firewall mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los comandos siguientes:

- `add appfw profile <name> [-defaults ( **basic** | **advanced** )]`
- `set appfw profile <name> -type ( **HTML** | **XML** | **HTML XML** )`
- `set appfw profile <name> -comment "<comment>"`

- `save ns config`

Ejemplo

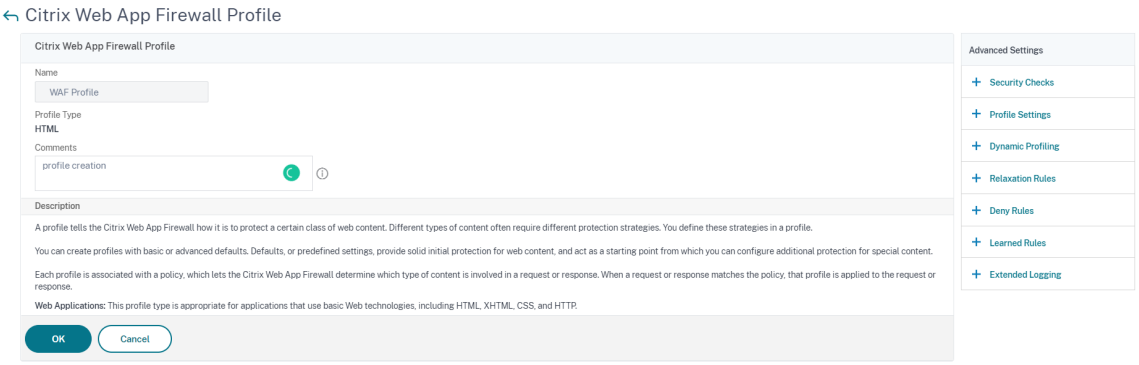
En el ejemplo siguiente se agrega un perfil denominado pr-basic, con valores predeterminados básicos, y se asigna un tipo de perfil HTML. Esta es la configuración inicial adecuada para que un perfil proteja un sitio web HTML.

```
1 add appfw profile pr-basic -defaults basic -comment ”Simple profile for
      websites.”
2 set appfw profile pr-basic -type HTML
3 save ns config
4 <!--NeedCopy-->
```

Para crear un perfil de Web App Firewall mediante la interfaz gráfica de usuario

Complete el procedimiento siguiente para crear un perfil de Web App Firewall:

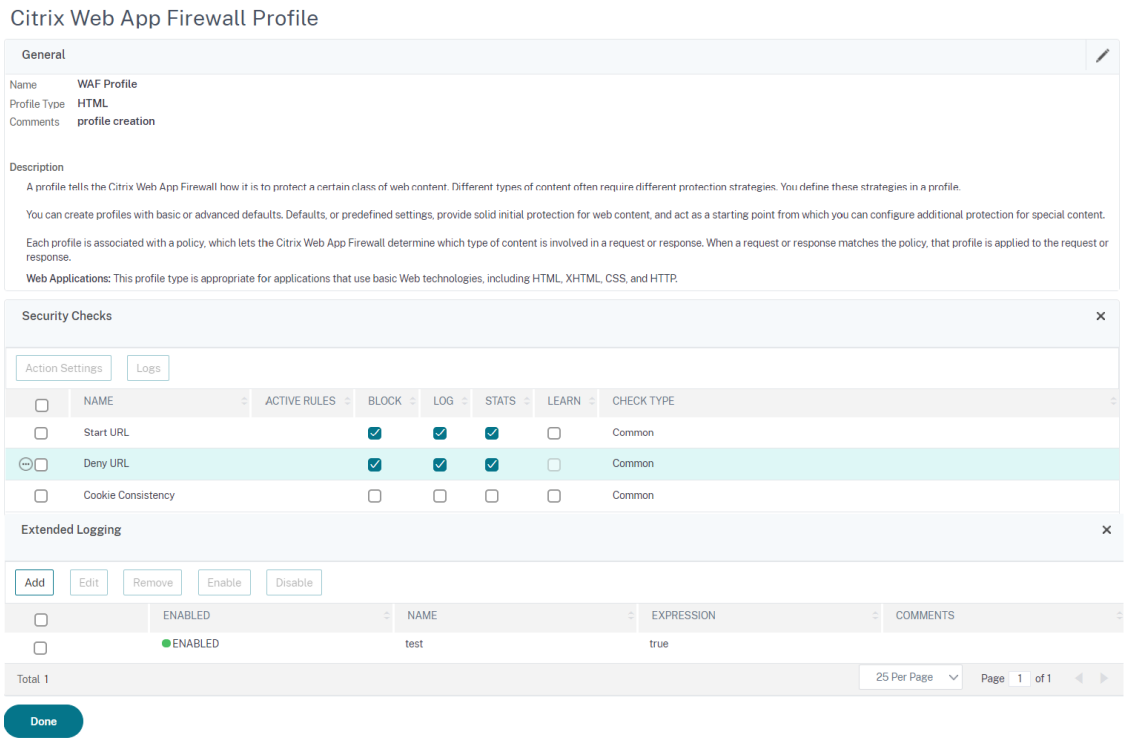
1. Vaya a **Seguridad > Citrix Web App Firewall > Perfiles**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En la página **Crear perfil de Web App Firewall**, defina los siguientes parámetros básicos:
   a) Nombre
   b) Tipo de perfil
   c) Comentarios
   d) Valores predeterminados
   e) Descripción
4. Haga clic en **Aceptar**.
5. En la sección **Configuración avanzada**, complete las siguientes configuraciones:
   a) Controles de seguridad
   b) Configuración de perfil
   c) Creación de perfiles dinámicos
   d) Reglas de relajación
   e) Reglas de denegación
   f) Regla aprendida
   g) Registro extendido



6. En la sección **Comprobaciones de seguridad**, seleccione una protección de seguridad y haga clic en Configuración de **acción*.
7. En la página de comprobación de seguridad, defina los parámetros.

   > **Nota:**
   >
   > La configuración **Regla activa** solo está disponible para la comprobación de **inyección SQL HTML** para activar la regla de relajación o la regla de denegación para la comprobación de inyección SQL. Para obtener más información, consulte el tema Reglas de relajación y denegación.

8. Haga clic en **Aceptar** y **cerrar**.
9. En la sección **Configuración de perfil**, defina los parámetros del perfil. Para obtener más información, consulte el tema Configurar la configuración del perfil de Web App Firewall.
10. En la sección Creación de **perfiles dinámicos**, seleccione una comprobación de seguridad para agregar la configuración del perfil dinámico. Para obtener más información, consulte el tema Perfil dinámico.
11. En la sección **Reglas de relajación**, haga clic en **Modificar** para agregar una regla de relajación para una comprobación de seguridad. Para obtener más información, consulte Regla de relajación para obtener más información.
12. En la sección **Reglas de denegación**, agregue una regla de denegación para la comprobación de inyección SQL HTML. Para obtener más información, consulte el tema Reglas de denegación de HTML.
13. En la sección **Regla aprendiz**, defina la configuración de aprendizaje. Para obtener más información, consulte el tema Aprendizaje de Web App Firewall.
14. En la sección **Registro ampliado**, haga clic en **Agregar** para enmascarar datos confidenciales. Para obtener más información, consulte el tema Registro ampliado.
15. Haga clic en **Listo** y, a continuación, en **Cerrar**.



Configurar reglas de detección de cuentas falsas

La creación de cuentas falsas es un proceso automatizado para crear muchas cuentas de usuario que no están asociadas a una persona real o crear cuentas de usuario con los datos de la persona real sin su consentimiento. Las cuentas falsas que los usuarios no legítimos crean utilizan detalles de registro que no se corresponden con la verdadera identidad de una persona. Estas cuentas se crean para abusar de los servicios ofrecidos por una aplicación web con fines no legítimos, como ataques de phishing, difusión de noticias falsas, scalping, etc. La mayoría de las veces, estas cuentas son creadas por bots administrados por usuarios malintencionados.

El dispositivo Citrix ADC se ha mejorado para detectar cuentas falsas al vincular reglas de detección de cuentas falsas a un perfil de Web App Firewall. La regla consiste en URL de formulario y parámetros de formulario para cada URL. Si una solicitud entrante coincide con una URL de expresión o formulario (páginas de registro) configurada para una regla de detección de cuenta falsa, la evaluación es verdadera para un intento de registro sospechoso y los datos de la solicitud se envían al servidor ADM para su posterior inspección.

Complete los siguientes pasos para configurar la detección de cuentas falsas mediante la interfaz de comandos:

1. Activar la función de detección de cuentas falsas
2. Reglas de cuentas falsas

Activar la función de detección de cuentas falsas

En el símbolo del sistema, escriba:

```
add/set appfw profile <name> -FakeAccountDetection ( ON | OFF )
```

Ejemplo:

```
add appfw profile profile1 -FakeAccountDetection ON
```

Reglas de cuentas falsas

En el símbolo del sistema, escriba:

```
bind appfw profile <name> -FakeAccount (string|expression)isFieldNameRegex
 (ON|OFF)-tag <TagExpression> ([-formUrl <FormURL>]| [-formExpression <
FormExpression>)])-state (ENABLED|DISABLED)
```

Donde:

`formUrl`: URL de acción del formulario HTTP.
dormExpression: expresión de forma que se evaluará.
`fakeaccount`: Nombre de la cuenta falsa.
tag: expresión de etiqueta.
`isFieldNameRegex`: especifica si el fieldName es regex. Valor predeterminado DESACTIVADO.

Ejemplo:

```
bind appfw profile profile1 -FakeAccount john -formURL  “/signup.php”-tag ”
smith”
bind appfw profile profile2 -FakeAccount Will -formExpression ”HTTP.REQ.
HEADER(\”Authorization\”).CONTAINS(\”/test_accounts\”).NOT && HTTP.REQ.URL.
CONTAINS(\”/login.php\”)”-fieldName -tag ”smith”
```

Entrada de ejemplo para una página de registro `example.com` de solicitud de publicación HTTP.

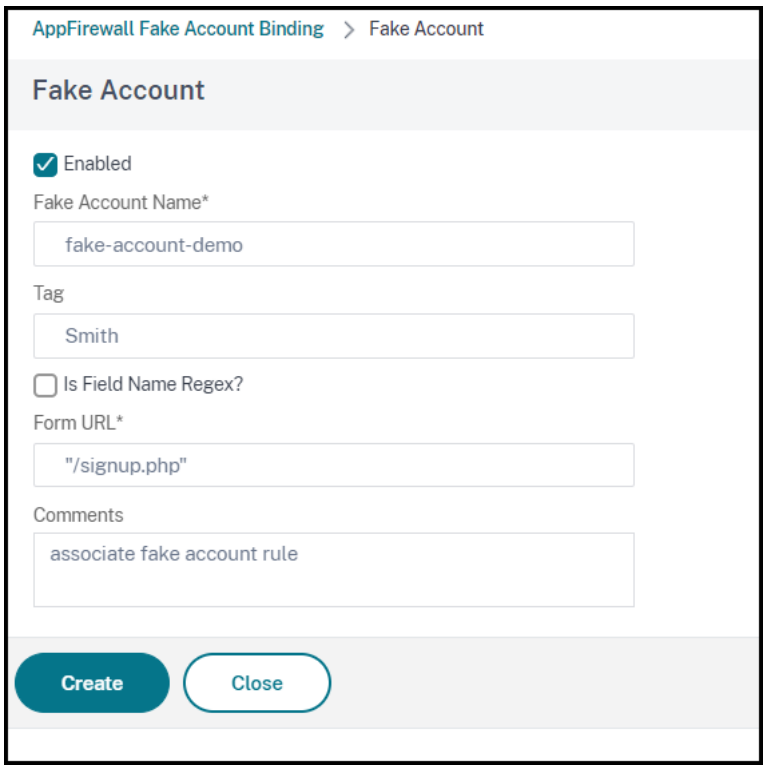
S.no	Entrada	Ejemplo
1	URL de punto de enlace de solicitud HTTP POST de registro	`https://webapi.example.com/account/api/v1.0/contacts/`
2	Nombre del campo de correo electrónico en la solicitud HTTP post	Dirección de correo electrónico
3	Nombre del campo Firstname en la solicitud HTTP post	Nombre de pila

S.no	Entrada	Ejemplo
4	Nombre del campo Lastname en la solicitud HTTP post	Apellidos

Configurar la regla de detección de cuentas falsas de Web App Firewall mediante la interfaz gráfica de usuario

Complete los siguientes pasos para configurar la regla de detección de cuentas falsas mediante la GUI.

1. Vaya a **Configuración** > **Seguridad** > **Citrix Web App Firewall** > **Perfil**.
2. Seleccione un perfil y haga clic en **Modificar**.
3. En la página **Perfil de Citrix Web App Firewall**, haga clic en **Comprobaciones de seguridad** en **Configuración avanzada**.
4. En la sección **Comprobaciones integradas con Citrix Cloud**, seleccione una regla de cuenta falsa y haga clic en **Modificar**.
5. En el control deslizante **Vinculación de cuentas falsas de AppFirewall**, seleccione una regla para modificarla o haga clic en **Agregar**.
6. En la página de **reglas de cuentas falsas**, establezca los siguientes parámetros:
    a) **Habilitada**. Seleccione para activar la regla de cuenta falsa.
    b) **Nombre de cuenta falso**. Nombre de la regla de cuenta falsa.
    c) **Etiqueta**. Nombre en el formulario de registro de cuenta falsa.
    d) **¿El nombre de campo es Regex?** Seleccione si el campo del formulario es una expresión regular.
    e) **Expresión de formulario**. Expresión regular que define la cuenta falsa.
    f) **URL del formulario**. Introduzca la URL de detección de cuentas falsas
    g) **Comentarios**. Una breve descripción de la regla de detección de cuentas falsas.
7. Haga clic en **Crear**.



Exigir el cumplimiento de HTTP RFC

June 22, 2022

Citrix Web App Firewall inspecciona el tráfico entrante en busca de cumplimiento de HTTP RFC y elimina cualquier solicitud que tenga infracciones de RFC de forma predeterminada. Sin embargo, hay ciertos casos en los que el dispositivo puede tener que omitir o bloquear una solicitud de cumplimiento que no sea de RFC. En tales casos, puede configurar el dispositivo para que omita o bloquee dichas solicitudes a nivel global o de perfil.

Bloquee o evite las solicitudes que no cumplen con RFC a nivel global

El módulo HTTP identifica una solicitud como no válida si está incompleta y WAF no puede procesar dichas solicitudes. Por ejemplo, una solicitud HTTP entrante a la que falta un encabezado de host. Para bloquear o evitar estas solicitudes no válidas, debe configurar la opción `malformedReqAction` en la configuración global del firewall de aplicaciones.

El parámetro 'MalformedReqAction' valida la solicitud entrante por longitud de contenido no válida, solicitud fragmentada no válida, sin versión HTTP y encabezado incompleto.

> **Nota:**
>
> Si inhabilita la opción de bloqueo en el parámetro `malformedReqAction`, el dispositivo omite todo el procesamiento del firewall de la aplicación para todas las solicitudes de cumplimiento que no son RFC y las reenvía al siguiente módulo.

Para bloquear u omitir solicitudes HTTP de quejas no válidas que no sean de RFC mediante la interfaz de línea de comandos

Para bloquear u omitir solicitudes no válidas, introduzca el siguiente comando:

```
set appfw settings -malformedreqaction <action>
```

Ejemplo:

```
set appfw settings -malformedReqAction block
```

Para mostrar la configuración de acción de solicitud mal formada

Para mostrar la configuración de acción de solicitud mal formada, introduzca el siguiente comando:

```
show appfw settings
```

Salida:

```
1 DefaultProfile: APPFW_BYPASS UndefAction: APPFW_BLOCK SessionTimeout:
      900 LearnRateLimit: 400 SessionLifetime: 0
    SessionCookieName: citrix_ns_id ImportSizeLimit: 134217728
    SignatureAutoUpdate: OFF SignatureUrl:"https://s3.amazonaws.com/
    NSAppFwSignatures/SignaturesMapping.xml" CookiePostEncryptPrefix:
    ENC GeoLocationLogging: OFF CEFLogging: OFF EntityDecoding:
     OFF UseConfigurableSecretKey: OFF SessionLimit: 100000
    MalformedReqAction: block log stats
2  Done
3 <!--NeedCopy-->
```

Para bloquear u omitir solicitudes HTTP no válidas de quejas no RFC mediante la GUI de Citrix ADC

1. Vaya a **Seguridad** > **Citrix Web App Firewall**.
2. En la página **Citrix Web App Firewall**, haga clic en **Cambiar configuración del motor** en **Configuración**.

3. En la página **Configurar la configuración de Citrix Web App Firewall**, seleccione la opción **Registrar solicitud mal formada** como Bloque, Registro o Estadísticas.
4. Haga clic en **Aceptar** y **cerrar**.

> **Nota:**
>
> Si anula la selección de la acción de bloqueo o no selecciona ninguna acción de solicitud mal formada, el dispositivo omite la solicitud sin intimidar al usuario.

Bloquear u omitir solicitudes que no cumplan con RFC a nivel de perfil

Otras solicitudes no compatibles con RFC se pueden configurar para bloquear u omitir a nivel de perfil. Debe configurar el perfil RFC en modo Bloque o Bypass. Al realizar esta configuración, cualquier tráfico no válido que coincida con el perfil de Web App Firewall se omite o se bloquea en consecuencia. El perfil RFC valida las siguientes comprobaciones de seguridad:

- Solicitudes de GWT-RPC no válidas
- Encabezados de tipos de contenido no válidos
- Solicitudes multiparte no válidas
- Solicitudes JSON no válidas
- Comprobaciones de pares de valores de nombres de cookie

> **Nota:**
>
> Cuando establece el perfil `RFC` en modo "Omitir", debe asegurarse de inhabilitar la opción de transformación en las secciones **Configuración de scripts HTML entre sitios** y en las secciones **Configuración de inyección HTML SQL**. Si habilita y establece el perfil `RFC` en modo Omisión, el dispositivo muestra un mensaje de advertencia: "Transformar scripts entre sitios" y "Transformar caracteres especiales de SQL" están activadas actualmente. Se recomienda apagarlo cuando se use con `APPFW_RFC_BYPASS`.
>
> **Importante:**
>
> Además, el dispositivo muestra una nota de advertencia: "Las comprobaciones de seguridad de Appfw habilitadas podrían no ser aplicables a las solicitudes que infrinjan las comprobaciones de RFC cuando se establece este perfil. No se recomienda habilitar ninguna configuración de transformación, ya que las solicitudes podrían transformarse parcialmente que contengan infracciones de RFC. "

Para configurar un perfil RFC en el perfil de Web App Firewall mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los comandos siguientes:

```
set appfw profile <profile_name> -rfcprofile <rfcprofile_name
```


Ejemplo

```
set appfw profile P1 -rfcprofile APPFW_RFC_BLOCK
```

> **Nota:**
>
> De forma predeterminada, el perfil `RFC` está enlazado al perfil de Web App Firewall en modo Bloquear.

Para configurar un perfil RFC en el perfil de Web App Firewall mediante la GUI

1. Vaya a **Seguridad > Citrix Web App Firewall > Perfiles**.
2. En la página **Perfiles**, seleccione un perfil y haga clic en **Modificar**.
3. En la página **Perfil de Web App Firewall**, haga clic en **Configuración de perfil** en la sección **Configuración avanzada**.
4. En la sección **Configuración HTML**, establece el perfil `RFC` en modo `APPFW_RFC_BYPASS`.
   El sistema muestra un mensaje de advertencia: "Las comprobaciones de seguridad de Appfw habilitadas podrían no ser aplicables a las solicitudes que infrinjan las comprobaciones de RFC cuando se establece este perfil. No se recomienda habilitar ninguna configuración de transformación, ya que las solicitudes pueden transformarse parcialmente que contengan infracciones de RFC".

Configuración de perfiles de Web App Firewall

July 15, 2022

Para configurar un perfil de Web App Firewall definido por el usuario, primero configure las comprobaciones de seguridad, que se denominan *protecciones profundas* o *protecciones avanzadas* en el asistente de Web App Firewall. Determinadas comprobaciones requieren configuración si se van a utilizar. Otros tienen configuraciones predeterminadas que son seguras pero con un alcance limitado; es posible que sus sitios web necesiten o se beneficien de una configuración diferente que aproveche más funciones de ciertas comprobaciones de seguridad.

Después de configurar las comprobaciones de seguridad, también puede configurar otras opciones que controlen el comportamiento, no de una sola comprobación de seguridad, sino de la función Web App Firewall. La configuración predeterminada es suficiente para proteger la mayoría de los sitios web, pero debe revisarlos para asegurarse de que son adecuados para sus sitios web protegidos.

> **Nota:**
>
> La longitud del nombre de perfil y toda la longitud del nombre de objeto de importación se pueden configurar hasta 127 caracteres.

Para obtener más información sobre las comprobaciones de seguridad de Web App Firewall, consulte Protecciones avanzadas.

Para configurar un perfil de Web App Firewall mediante la línea de comandos

En el símbolo del sistema, escriba los comandos siguientes:

- `set appfw profile <name> <arg1> [<arg2> ...]`

  Donde:

  - `<arg1>` = un parámetro y cualquier opción asociada.
  - `<arg2>` = un segundo parámetro y cualquier opción asociada.
  - … = parámetros y opciones adicionales.

  Para obtener descripciones de los parámetros que se deben utilizar al configurar comprobaciones de seguridad específicas, consulte Protecciones avanzadas.

- `save ns config`

Ejemplo

El siguiente ejemplo muestra cómo habilitar el bloqueo para las comprobaciones de HTML SQL Injection y HTML Cross-Site Scripting en un perfil denominado `pr-basic`. Este comando permite bloquear esas acciones sin realizar otros cambios en el perfil.

```
1 set appfw profile pr-basic -crossSiteScriptingAction block -
     SQLInjectionAction block
2 <!--NeedCopy-->
```

Vincular la regla de relajación a un perfil de Web App Firewall

Cuando un Web App Firewall detecta una infracción, el usuario tiene la capacidad de omitir la acción aplicada mediante reglas de relajación. La regla de relajación es una excepción que se aplica a la infracción de seguridad detectada. Por ejemplo, las reglas de relajación de URL de inicio protegen contra la navegación forzada. Las vulnerabilidades conocidas del servidor web que explotan los piratas informáticos se pueden detectar y bloquear activando un conjunto de reglas predeterminadas de denegar URL. Los ataques lanzados comúnmente, como desbordamiento de búfer, SQL o scripts entre sitios también se pueden detectar fácilmente.

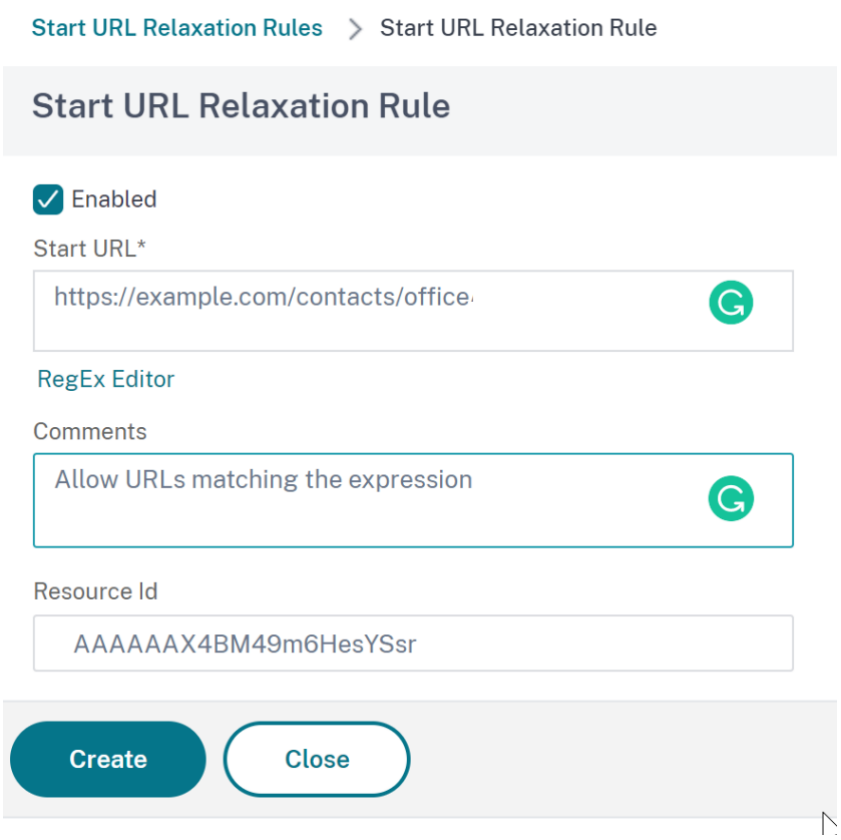
Para vincular reglas de exención o relajación de seguridad mediante la CLI

En el símbolo del sistema, escriba:

```
bind appfw profile <name> ((-startURL <expression> [-resourceId  <
    string>]) | -denyURL <expression> | (-fieldConsistency <string>   <
    formActionURL> [-isRegex ( REGEX | NOTREGEX )]) | (-
    cookieConsistency <string> [-isRegex ( REGEX | NOTREGEX )]) | (-
    SQLInjection <string> <formActionURL> [-isRegex ( REGEX | NOTREGEX )
    ] [-location <location>] [-valueType <valueType> <valueExpression
    >....
<!--NeedCopy-->
```

Para vincular reglas de exención o relajación de seguridad mediante la interfaz gráfica de usuario

1. Vaya a **Seguridad > Citrix Web App Firewall > Perfiles**.
2. En el panel de detalles, seleccione un perfil y haga clic en **Modificar**.
3. En la página **Perfil de Citrix Web App Firewall**, haga clic en **Reglas de relajación** en la sección **Configuración avanzada**.
4. En la sección **Reglas de relajación**, haga clic en **StartURL** y haga clic en **Modificar**.
5. En la página **Iniciar reglas de relajación de URL**, haga clic en **Agregar**.
6. En la página **Iniciar regla de relajación de URL**, establezca los siguientes parámetros:
    a) Habilitada. Seleccione la casilla de verificación para activar la regla de relajación
    b) URL de inicio. Introduzca el valor de la expresión regular
    c) Comentarios. Proporciona una breve descripción sobre la regla de relajación.
7. Haga clic en **Crear** y **cerrar**.



Para configurar un perfil de Web App Firewall mediante la GUI

1. Vaya a **Seguridad > Citrix Web App Firewall > Perfiles**.
2. En el panel de detalles, seleccione el perfil que quiere configurar y, a continuación, haga clic en **Modificar**.
3. En el cuadro de diálogo **Configurar perfil de Web App Firewall**, en la ficha **Comprobaciones de seguridad**, configure las comprobaciones de seguridad.
   - Para habilitar o inhabilitar una acción para una verificación, en la lista, active o desactive la casilla de verificación de la acción.
   - Para configurar los parámetros de las comprobaciones de seguridad de la lista, active la casilla de verificación y haga clic en **Configuración activa**.
   - Para revisar las entradas de registro de la comprobación de seguridad seleccionada, active la casilla de verificación y haga clic en **Registros**. Puede utilizar esta información para determinar las comprobaciones de seguridad que coinciden con los ataques, de modo que pueda bloquear el tráfico para las comprobaciones de seguridad. También puede usar la información para determinar las comprobaciones que coinciden con el tráfico legítimo, de modo que pueda configurar una exención adecuada para permitir esas conexiones legíti-

mas. Para obtener más información sobre los registros, consulte Registros, estadísticas e informes.

- Para inhabilitar completamente una comprobación, en la lista, desactive todas las casillas de verificación situadas a la derecha de esa comprobación.

4. En la ficha **Configuración**, configure los ajustes del perfil.
   - Para asociar el perfil al conjunto de firmas que creó y configuró anteriormente, en Configuración común, elija ese conjunto de firmas en la lista desplegable **Firmas**.

     > **Nota:**
     >
     > Debe utilizar la barra de desplazamiento a la derecha del cuadro de diálogo para desplazarse hacia abajo y mostrar la sección Configuración común.

   - Para configurar un objeto de error HTML o XML, seleccione el objeto en la lista desplegable apropiada.

     > **Nota:**
     >
     > Primero debe cargar el objeto de error que quiere utilizar en el panel Importaciones. Para obtener más información sobre la importación de objetos de error, consulte Importaciones.

   - Para configurar el tipo de contenido XML predeterminado, escriba la cadena de tipo de contenido directamente en los cuadros de texto Solicitud predeterminada y Respuesta predeterminada o haga clic en Administrar tipos de contenido permitidos para administrar la lista de tipos de contenido permitidos. »Más….
5. Si quiere utilizar la función de aprendizaje, haga clic en Aprendizaje y configure los ajustes de aprendizaje del perfil, tal y como se describe en Configuración y uso de la función de aprendizaje.
6. Haga clic en **Aceptar** para guardar los cambios y volver al panel **Perfiles**.

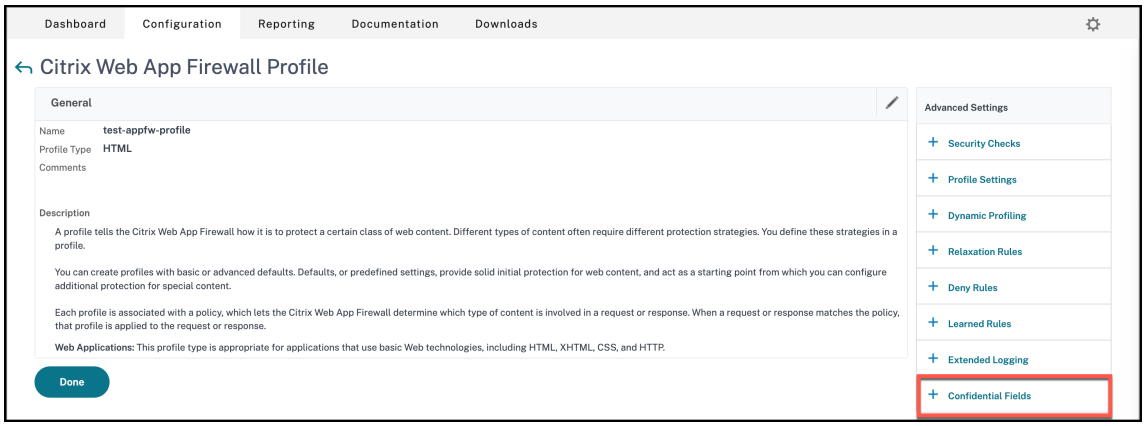
Campos confidenciales en el perfil WAF

> **Nota**
>
> Esta función está disponible en la versión 13.1 compilación 27.x y posteriores.

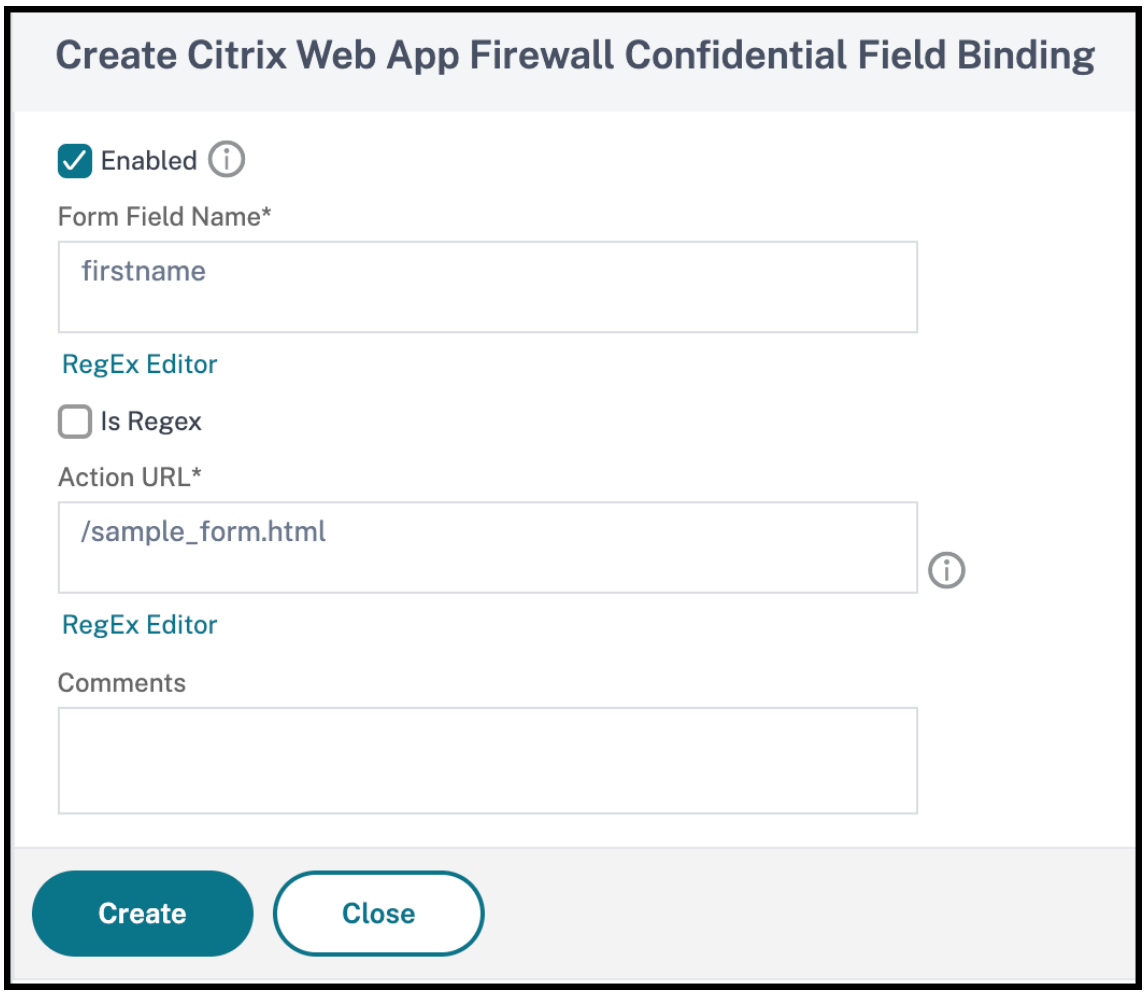
Ahora puede agregar campos confidenciales en un perfil WAF. Estos campos están enmascarados y no se capturan en los registros de ADC cuando se produce una infracción. Anteriormente, podía agregar estos campos solo con la configuración. Para obtener más información sobre cómo agregar campos confidenciales mediante la configuración, consulte Campos confidenciales.

1. Vaya a **Seguridad > Citrix Web App Firewall > Perfiles**.

2. Seleccione un perfil y haga clic en **Modificar**.
3. En **Configuración avanzada**, haga clic en **Campos confidenciales**.



4. Haga clic en **Agregar**.
5. Introduzca valores para los siguientes parámetros:
    - Nombre del campo del formulario*
    - URL de acción*
    - Comentarios



Un * indica un campo obligatorio

6. Haga clic en **Crear**.
7. Haga clic en **Done**.

Configuración del perfil de Firewall de aplicaciones web

October 5, 2021

A continuación se indican los ajustes de perfil que debe configurar en el dispositivo.

En el símbolo del sistema, escriba:

```
add appfw profile <name> [-invalidPercentHandling <invalidPercentHandling
>] [-checkRequestHeaders ( ON | OFF )] [-URLDecodeRequestCookies ( ON |
 OFF )] [-optimizePartialReqs ( ON | OFF )] [-errorURL <expression>] [-
logEveryPolicyHit ( ON | OFF )] [-stripHtmlComments <stripHtmlComments>] [-
```



```
stripXmlComments ( none | all )] [-postBodyLimitSignature <positive_integer
>][-fileUploadMaxNum <positive_integer>][-canonicalizeHTMLResponse ( ON
| OFF )][-percentDecodeRecursively ( ON | OFF )] [-multipleHeaderAction
<multipleHeaderAction> ...][-inspectContentTypes <inspectContentTypes>
...][-semicolonFieldSeparator ( ON | OFF )]
```

Ejemplo:

```
add appfw profile profile1 [-invalidPercentHandling secure_mode] [-checkRequestHeaders
 ON] [-URLDecodeRequestCookies OFF] [-optimizePartialReqs OFF]
```

Donde:

La**manipulación porcentual no es válida**. Configure el método de gestión de nombres y valores codificados por porcentaje.

Los ajustes disponibles funcionan de la siguiente manera:

asp_mode - Elimina y analiza el porcentaje no válido para el análisis. Ejemplo curl -v "http://<vip>/forms/login.html?field=sel%zzect -> Invalid percent encoded char(%zz) se despoja y se inspecciona el resto del contenido y se toman medidas para la comprobación de SQLInjection.
secure_mode - Detectamos el valor codificado por porcentaje no válido y lo ignoramos. Ejemplo curl -v "http://<vip>/forms/login.html?field=sel%zzect -> Invalid percent encoded char(%zz) se detecta, los contadores se incrementan y el contenido se pasa tal cual al servidor.
apache_mode - Este modo funciona de forma similar al modo seguro.
Valores posibles: apache_mode, asp_mode, secure_mode Valor
por defecto: secure_mode

Optimizar las solicitudes parciales. Cuando está DESACTIVADO/ENCENDIDO (sin objeto seguro), un dispositivo Citrix ADC envía la solicitud parcial al servidor back-end. Esta respuesta parcial se devuelve al cliente. OptimizePartialReqs tiene sentido cuando se configura el objeto Safe. El dispositivo envía solicitudes de respuesta completa desde el servidor cuando está DESACTIVADO y solo solicita una respuesta parcial cuando está activado.

Los ajustes disponibles son los siguientes:

ON : Las solicitudes parciales del cliente dan como resultado solicitudes parciales al servidor back-end.
DESACTIVADO: las solicitudes parciales del cliente se cambian a solicitudes completas al servidor back-end Valores
posibles: ON, OFF Valor
predeterminado: ON

Cookies de solicitud de decodificación de URL. URL Decode solicita cookies antes de someterlas a

comprobaciones de scripts SQL y entre sitios.

Valores posibles: ON, OFF Valor
por defecto: OFF

Límite del cuerpo de la publicación de firma (bytes). Limita la carga útil de la solicitud (en bytes) inspeccionada en busca de firmas con la ubicación especificada como 'HTTP_POST_BODY'.

Valor por defecto: 8096 Valor
mínimo: 0 Valor
máximo: 4294967295

Límite del cuerpo de la publicación (bytes). Limita la carga útil de la solicitud (en bytes) inspeccionada por Web Application Firewall.

Valor predeterminado: 20000000 Valor
mínimo: 0 Valor
máximo: 10 GB

Para obtener más información sobre la configuración Seguridad y su procedimiento de GUI, consulte el tema Configurar perfil de Web App Firewall .

PostbodyLimitAction. PostBodyLimit respeta la configuración de error cuando especifica el tamaño máximo del cuerpo HTTP que se va a permitir. Para respetar la configuración de errores, debe configurar una o más acciones de límite de cuerpo de la publicación. La configuración también se aplica a las solicitudes en las que el encabezado de codificación de transferencia está fragmentado.

```
set appfw profile <profile_name> -PostBodyLimitAction block log stats
```

Dónde,
Bloquear: Esta acción bloquea la conexión que infringe la comprobación de seguridad y se basa en el tamaño máximo del cuerpo HTTP configurado (límite de cuerpo de publicación). Debe activar siempre la opción.

Registro: Registrar infracciones de esta comprobación de seguridad.

Estadísticas: genera estadísticas para esta comprobación de seguridad.

> **Nota:**
>
> El formato de registro de la acción de límite del cuerpo de la publicación se ha cambiado para que siga el formato de registro de auditoría
> estándar, por ejemplo:
> `ns.log.4.gz:Jun 25 1.1.1.1. <local0.info> 10.101.10.100 06/25/2020:10:10:28 GMT 0-PPE-0 : default APPFW APPFW_POSTBODYLIMIT 1506 0 : <Netscaler IP> 4234-PPE0 - testprof ><URL> Request post body length(<Post Body Length >)exceeds post body limit.`

InspectQueryContentTypes Inspeccione la consulta de solicitud y los formularios web de SQL inyectados y scripts entre sitios para los siguientes tipos de contenido.

```
set appfw profile p1 -inspectQueryContentTypes HTML XML JSON OTHER
```

Valores posibles: HTML, XML, JSON, OTHER

De forma predeterminada, este parámetro se establece como “inspectQueryContentTypes: HTML JSON OTHER” para perfiles appfw básicos y avanzados.

Ejemplo de tipo de contenido de consulta de inspección como XML:

```
1 > set appfw profile p1 -type XML
2 Warning: HTML, JSON checks except “InspectQueryContentTypes” & “
     Infer Content-Type XML Payload Action” will not be applicable when
     profile type is not HTML or JSON respectively.
3 <!--NeedCopy-->
```

Ejemplo de tipo de contenido de consulta de inspección como HTML:

```
1 > set appfw profile p1 -type HTML
2 Warning: XML, JSON checks except “InspectQueryContentTypes” & “Infer
     Content-Type XML Payload Action” will not be applicable when
     profile type is not XML or JSON respectively
3 Done
4 <!--NeedCopy-->
```

Ejemplo de tipo de contenido de consulta de inspección como JSON:

```
1 > set appfw profile p1 -type JSON
2 Warning: HTML, XML checks except “InspectQueryContentTypes” & “Infer
     Content-Type XML Payload Action will not be applicable when profile
     type is not HTML or XML respectively
3 Done
4 <!--NeedCopy-->
```

Expresión errorURL. Dirección URL que Citrix Web App Firewall utiliza como URL de error. Longitud máxima: 2047.

> **Nota:**

> Para bloquear infracciones en una URL solicitada, si la URL de error es similar a la URL de firma, el dispositivo restablece la conexión.

LogEveryPolicyHit : registra todas las coincidencias de perfil, independientemente de los resultados de las comprobaciones de seguridad.
Valores posibles: ON, OFF.
Valor predeterminado: OFF.

stripXMLComments - Elimina los comentarios XML antes de reenviar una página web enviada por un sitio web protegido en respuesta a una solicitud del usuario.
Valores posibles: none, all, exclude_script_tag.
Valor predeterminado: none

PostBodyLimitSignature - Tamaño máximo permitido del cuerpo de la publicación HTTP para la inspección de firmas para la ubicación HTTP_POST_BODY en las firmas, en bytes.
Los cambios en el valor pueden afectar a la CPU y al perfil de latencia.
Valor por defecto: 2048.
Valor mínimo: 0 Valor
máximo: 4294967295

FileUploadMaxNum : número máximo permitido de cargas de archivos por solicitud de envío de formularios. La configuración máxima (65535) permite un número ilimitado de cargas.
Valor por defecto: 65535 Valor
mínimo: 0 Valor
máximo: 65535

CanonicalizeHTMLResponse - Realiza la codificación de entidad HTML para cualquier carácter especial en las respuestas enviadas por tus sitios web protegidos.
Valores posibles: ON, OFF Valor
por defecto: ON

PercentDecodeRecursively : configure si el firewall de la aplicación debe utilizar decodificación recursiva porcentual.
Valores posibles: ON, OFF Valor
por defecto: ON

multipleHeaderAction : una o varias acciones de encabezado. Los ajustes disponibles funcionan de la siguiente manera:

- Bloquear. Bloquea las conexiones que tienen varios encabezados.
- Registro. Registra las conexiones que tienen varios encabezados.
- KeepLast. Mantenga solo el último encabezado cuando haya varios encabezados presentes.

InspectContentTypes : una o varias listas de InspectContentType.

- aplicación/x-www-form-urlencoded

- multipart/form-data
- text/x-gwt-rpc

Valores posibles: ninguno, application/x-www-form-urlencoded, multipart/form-data, text/x-gwt-rpc

SemiColonFieldSeparator : permite ';' como separador de campos de formulario en consultas URL y cuerpos de formulario POST.
Valores posibles: ON, OFF Valor
por defecto: OFF

Cambio de un tipo de perfil de Web App Firewall

January 12, 2021

Si ha elegido un tipo de perfil incorrecto para un perfil de Web App Firewall o el tipo de contenido del sitio web protegido ha cambiado, puede cambiar el tipo de perfil.

> **Nota** Al cambiar el tipo de perfil, perderá todos los valores de configuración y las relajaciones o reglas aprendidas para las entidades que el nuevo tipo de perfil no admite. Por ejemplo, si cambia el tipo de perfil de web 2.0 a XML, perderá las opciones de configuración de URL de inicio, comprobación de coherencia de campos de formulario y otras comprobaciones de seguridad específicas de HTML. La configuración de las opciones admitidas por los tipos de perfil antiguo y nuevo permanece sin cambios.

Para cambiar un tipo de perfil de Web App Firewall mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos:

- `set appfw profile <name> -type ( **HTML** | **XML** | **HTML XML** )`
- `save ns config`

Ejemplo

En el ejemplo siguiente se cambia el tipo de perfil denominado pr-basic, de HTML a HTML XML, que es equivalente al tipo Web 2.0 de la GUI.

```
set appfw profile pr-basic -type HTML XML
save ns config
<!--NeedCopy-->
```


Para cambiar un tipo de perfil de Web App Firewall mediante la interfaz gráfica de usuario

1. Vaya a **Seguridad > Citrix Web App Firewall > Directivas**.
2. En el panel de detalles, haga clic en **Acción** y, a continuación, en **Cambiar tipo de perfil**.
3. En el cuadro de diálogo **Cambiar tipo de perfil de Web App Firewall**, en la lista desplegable **Tipo de perfil**, seleccione un nuevo tipo de perfil.
4. Haga clic en **Aceptar** para guardar los cambios y volver al panel **Perfiles**.

Exportación e importación de un perfil de Web App Firewall

January 12, 2021

Puede replicar toda la configuración de un perfil de Web App Firewall (incluidos todos los objetos enlazados, como el objeto de error HTML, el objeto de error XML, el esquema WSDL o XML, las firmas, etc.) en varios dispositivos. Puede seleccionar un perfil de destino y exportar la configuración para guardarlo en el sistema de archivos local del equipo, o puede transferir la configuración archivada para almacenarla en un servidor. Del mismo modo, puede examinar el sistema de archivos local del equipo o importar el archivo desde el servidor para seleccionar un perfil exportado anteriormente e importarlo en el dispositivo NetScaler.

La opción de exportar toda la configuración del perfil e importarla a otro dispositivo puede ser útil en varios casos de uso. Por ejemplo, puede que quiera configurar un perfil de Web App Firewall en una configuración de banco de pruebas para probar y validar que funciona como se esperaba. Una vez que esté satisfecho, puede exportar el perfil e importar la configuración del perfil a los dispositivos NetScaler de producción. Esta funcionalidad también es útil para realizar copias de seguridad de la configuración. Puede exportar el perfil antes de realizar cambios, de modo que pueda deshacer fácilmente la configuración a un estado conocido si es necesario.

> **Nota**
>
> Los perfiles de Web App Firewall que se exportan y archivan desde una compilación no se pueden restaurar en un sistema que ejecute una compilación diferente, ya que los cambios introducidos en las versiones más recientes pueden provocar problemas de compatibilidad. Si intenta restaurar un perfil archivado en una compilación diferente a la desde la que se exportó, se registra un mensaje de error en ns.log.

La funcionalidad de perfil de exportación e importación está disponible tanto en la GUI (GUI) como en la interfaz de línea de comandos (CLI). Se recomienda la interfaz gráfica de usuario, ya que ofrece opciones de **acción** fáciles de usar. Con un clic de un botón, puede **exportar** o **importar** toda la configuración de un perfil.

Exportación de perfiles de Web App Firewall con la CLI

Si utiliza CLI para **exportar** un perfil, debe **archivar** la configuración y, a continuación, **exportarla**. Para **importar** un perfil, debe **importar** el archivo en el dispositivo NetScaler y, a continuación, ejecutar el comando **restore** para extraer la configuración. El siguiente conjunto de comandos CLI se puede utilizar para exportar, importar y administrar las configuraciones de perfil.

Comandos CLI para exportar archivos:

- `archive appfw profile <name> <archivename> [-comment <string>]`
- `export appfw archive <name> <target>`

Comandos CLI para importar archivos:

- **`import`** `appfw archive <src> <name> [-comment <string>]`
- `restore appfw profile <archivename>`

Comandos CLI para administrar archivos:

- `show appfw archive`
- `rm appfw archive <name>`

La exportación de un perfil desde un dispositivo e importarlo a otro requiere cinco pasos en la CLI. Los tres primeros pasos se realizan en el dispositivo de origen en el que se crea originalmente la configuración del perfil y los dos siguientes se realizan en el dispositivo de destino en el que se va a replicar la configuración del perfil.

Exportar perfil desde el dispositivo NetScaler de origen:

Paso 1: Cree un archivo del perfil configurado.

Paso 2: Exporte el archivo al sistema de archivos NetScaler.

Paso 3: Utilice una utilidad de transferencia de archivos como scp para transferir el archivo de archivo exportado desde el dispositivo NetScaler A al dispositivo NetScaler de destino.

Importar perfil al dispositivo NetScaler de destino:

Paso 4: Ejecute el comando import para importar el archivo archivado. Puede importar el archivo desde el sistema de archivos local de NetScaler, o puede utilizar el protocolo HTTP o HTTPS para importar el archivo desde un servidor mediante la URL.

Paso 5: Ejecute el comando restore para restaurar la configuración del perfil desde el archivo importado

Para exportar un perfil de Web App Firewall mediante la interfaz de línea de comandos:

Primero, **archive** la configuración del perfil y, a continuación, **exporte** el archivo a una ubicación de destino. En el símbolo del sistema, escriba los siguientes comandos:

```
archive appfw profile <profileName> <archiveName>
```


donde:

- <profileName> es el nombre del perfil que se va a archivar.
- <archiveName> es el nombre del archivo de archivo que se va a crear.

La ejecución del comando anterior crea 2 instancias del archivo de archivo. Uno en la carpeta /var/tmp y otro en la carpeta /var/archive/appfw.

```
export appfw archive <archiveName> <target>
```

donde:

- <archiveName> es el nombre del archivo que se va a exportar. (El mismo nombre que en el comando anterior.
- <target> es una ruta de archivo que comienza con local: Como prefijo, seguido de <archiveName>.

La ejecución del comando export guarda el archivo de archivo exportado en el sistema de archivos del dispositivo NetScaler en la carpeta /var/tmp.

Ejemplos:

```
> archive appfw profile test_pr archived_test_pr
```

```
> export appfw archive archived_test_pr local:dutA_test_pr
```

Después de ejecutar los dos comandos anteriores, la carpeta /var/tmp contiene el archivo archived_test_pr y la copia exportada, duta_test_pr, que son idénticos en tamaño. Desde la CLI, puede caer en el shell para navegar a la carpeta para verificar que estos archivos están allí.

Después de exportar el archivo de archivo, puede utilizar **scp** o alguna otra utilidad de transferencia de archivos para transferir una copia del archivo de archivo desde el dispositivo NetScaler en el que se crearon al dispositivo NetScaler de destino.

Importación de perfiles de Web App Firewall con la CLI

Una vez que haya desplazado correctamente el archivo archivado desde el dispositivo de origen al dispositivo de destino, estará listo para **importar** el archivo del perfil y, a continuación, ejecutar el comando **restore** para replicar la configuración del perfil en el dispositivo de destino.

Inicie sesión en el dispositivo de destino. Colóquelos en el shell y en el cd a la carpeta /var/tmp para comprobar que el tamaño del archivo scp'd de este dispositivo coincide con el tamaño del archivo archivado original del dispositivo de origen. Salga del shell para volver a la línea de comandos.

Para importar un perfil mediante la CLI:

En el símbolo del sistema, escriba los siguientes comandos:

```
import appfw archive <src> <name> [-comment <string>]
```


donde

- <src> es la ubicación del archivo de archivo después de que se haya transferido desde el dispositivo de origen en el que se creó. Puede utilizar un sistema de archivos local y un nombre de archivo. Si ha colocado el archivo en un servidor, puede utilizar una URL para importar el archivo archivado. Si la ruta de acceso o el nombre del archivo contiene espacios, escriba la dirección URL entre comillas dobles rectas.
- <name> es el nombre del archivo de archivo que se va a importar.
- <string> es una descripción opcional del propósito del archivo.

```
restore appfw profile <archiveName>
```

Ejemplos:

A. Importar desde el archivo local seguido de restauración:

```
> import appfw archive local:dutA_test_pr dut2_test_pr
```

```
> restore appfw profile dut2_test_pr
```

B. Importar desde URL seguido de restauración:

```
import appfw archive http://10.217.30.16/FFC/Profile_ImportExport/
dutA_test_pr.tgz my_archive
restore appfw profile my_archive
```

En este ejemplo se restaura el perfil test_pr junto con todos los objetos enlazados (como firmas, página de error html, reglas de relajación, etc.) en el dispositivo NetScaler de destino.

Puede utilizar los siguientes comandos de CLI para acceder a las páginas de comando man para obtener más detalles.

- man archive appfw perfil
- man export archivo appfw
- man import archivo appfw
- man restore appfw perfil
- archivo man show appfw
- archivo man rm appfw

Exportación e importación de perfiles de Web App Firewall con la GUI

La GUI es más fácil de usar que la CLI. La utilidad realiza operaciones de archivado y exportación al hacer clic en **Exportar**. Del mismo modo, se ejecuta tanto la importación como la restauración al hacer clic en **Importar**. La GUI puede acceder al sistema de archivos local del equipo desde el que accede a la utilidad. Puede exportar una copia del archivo y guardarlo en su equipo local. A continuación, puede importar esta copia directamente en el dispositivo de destino sin tener que transferir manualmente el archivo de archivo de un dispositivo a otro.

Para exportar un perfil de Web App Firewall mediante la GUI:

1. Vaya a **Configuración** > **Seguridad** > **Web App Firewall** > **Perfiles**.
2. En el panel de detalles, seleccione el perfil que quiere exportar. Haga clic en **Acciones** y seleccione **Exportar** para descargar y guardar una copia en el sistema de archivos local del equipo.

Para importar un perfil de Web App Firewall mediante la GUI:

1. Vaya a **Configuración** > **Seguridad** > **Web App Firewall** > **Perfiles**.
2. En el panel de detalles, haga clic en **Acciones** y seleccione **Importar**. En el panel Importar perfil de Web App Firewall, el cuadro de selección Importar desde* ofrece 2 opciones:

URL: puede elegir importar un archivo especificando una **URL**. Cuando esta opción está seleccionada, debe proporcionar una ruta absoluta para el archivo archivado en el cuadro de entrada de **URL**.

Archivo: Puede elegir importar un archivo desde el **archivo** local. Cuando se selecciona esta opción, se muestra un campo de selección **Archivo local**. Puede examinar los archivos locales del equipo para seleccionar el archivo de archivo de destino.

Haga clic en **Crear** para importar el archivo especificado. La finalización correcta de la operación de importación crea la configuración del perfil en el dispositivo de destino.

Resumen

- Puede replicar toda la configuración (incluidos todos los objetos de importación, así como las reglas de relajación configuradas para el perfil) en varios dispositivos, sin necesidad de repetir los pasos de configuración, mediante la funcionalidad de exportación e importación de perfiles.
- Los objetos importados, como firmas, WSDL, esquema, página de error, etc., se incluyen en el archivo tar archivado y se replican en el dispositivo de destino.
- Los tipos de campo personalizados se incluyen en el archivo tar archivado y se replican en el dispositivo de destino.
- Los enlaces de directivas del perfil archivado no se replican cuando se restaura la configuración. Debe configurar la directiva y vincularla al perfil después de importar el perfil al dispositivo.
- El nombre del archivo de archivo puede tener hasta 31 caracteres de longitud. Al igual que con los nombres de perfil, un nombre de archivo debe comenzar con un carácter alfanumérico o de subrayado y contener solo caracteres alfanuméricos y de subrayado (_), número (#), punto (.), espacio (), dos puntos (:), en (@), igual a (=) o guión (-).
- Los comentarios asociados al archivo deben ser lo suficientemente descriptivos como para transmitir el propósito de la configuración archivada. La longitud máxima permitida para un comentario es de 255 caracteres.
- El`clear config -force basic` comando no elimina los perfiles archivados.
- La funcionalidad de perfil de importación y exportación se admite en implementaciones de alta disponibilidad (HA).

Sugerencias de depuración

- Supervise el /var/log/ns.log durante las ejecuciones de comandos para ver si hay algún mensaje de ERROR.
- Se generan registros adicionales (_restore.log, remove.log, import.log) en la carpeta /var/tmp/. Pueden ayudar a depurar problemas durante las operaciones correspondientes. Cuando estos registros alcanzan un tamaño de un MB, los mensajes de registro se purgan para reducir el archivo de registro a una cuarta parte del tamaño original.
- Si se produce un error en el comando de importación cuando se utiliza la opción URL en lugar del sistema de archivos local, compruebe que la configuración del servidor de nombres DNS y de la ruta estén correctamente configurados.
- Si utiliza el protocolo HTTPS para importar el archivo, el comando puede fallar si el servidor HTTPS requiere autenticación de certificado de cliente.

Fácil solución de problemas con registros de firewall de aplicaciones web

January 21, 2022

Cuando se produce un ataque de seguridad, es importante capturar registros WAF detallados en el dispositivo. Para ello, puede configurar el parámetro “VerboseLogLevel” en un perfil de Application Firewall.

Considere que un tráfico web está sufriendo un ataque de seguridad. Cuando el dispositivo recibe el tráfico, los detalles de la infracción, como los detalles del encabezado HTTP, el patrón de registro y la información de carga útil del patrón, se registran y se envían al servidor ADM. El servidor ADM supervisa los registros detallados y los muestra en la página Security Insight con fines de supervisión y seguimiento.

Configuración del nivel de registro detallado mediante la interfaz de comandos

Para capturar registros WAF detallados, configure el siguiente comando.
En la interfaz de comandos, escriba:

```
set appfw profile <profile_name> -VerboseLogLevel (pattern|patternPayload|
patternPayloadHeader)
```

Ejemplo

```
set appfw profile profile1 -VerboseLogLevel patternPayloadHeader
```

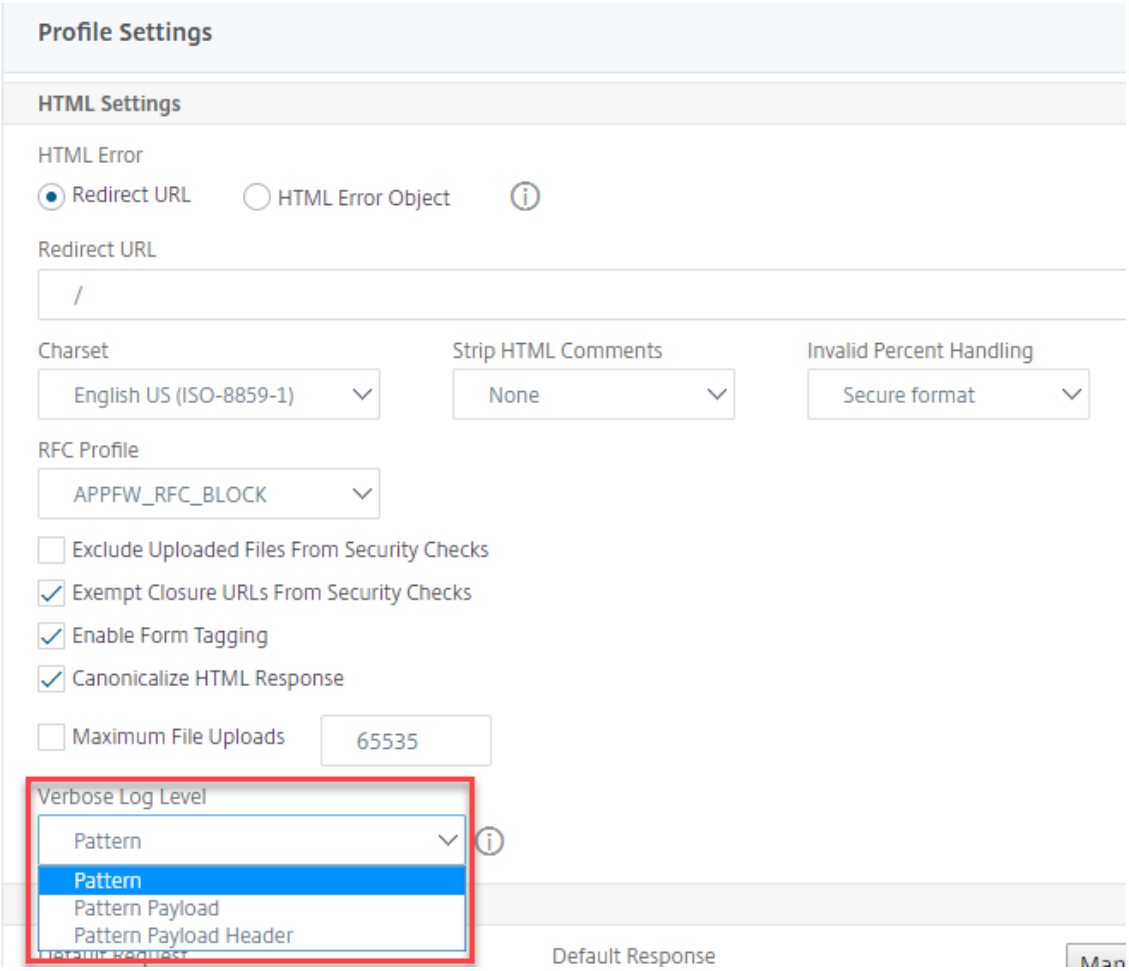

Los niveles de registro disponibles son:

1. patrón. Registra solo el patrón de infracción.
2. Carga útil de patrón. Registra el patrón de infracción y 150 bytes de carga útil de elementos de campo adicionales.
3. Encabezado de carga de patrón. Registra el patrón de infracción, 150 bytes de carga útil de elementos de campo adicionales e información de encabezado HTTP.

Configuración del nivel de registro detallado mediante la GUI de Citrix ADC

Complete el siguiente procedimiento para configurar el nivel de registro detallado en el perfil WAF.

1. En el panel de navegación, vaya a **Seguridad** > **Perfiles**.
2. En la página **Perfiles**, haga clic en **Agregar**.
3. En la página **Perfil de Citrix Web App Firewall**, haga clic en **Configuración de perfil** en **Configuración avanzada**.
4. En la sección **Configuración del perfil**, seleccione el nivel de registro WAF detallado en el campo Nivel de registro detallado.
5. Haga clic en **Aceptar** y **Listo**.



Registro detallado para comprobaciones de seguridad JSON (SQL, CMD y secuencias de comandos entre sitios)

Cuando un tipo de solicitud entrante es de JSON, puede configurar el parámetro de nivel de registro detallado para capturar registros de infracciones detallados, como información de patrón, carga de patrón y encabezado HTTP. Los detalles del registro se envían al servidor Citrix ADM para supervisar y solucionar problemas de infracciones de JSON. El mensaje de registro verboso no se almacena en el archivo ns.log.

El registro detallado para la protección de seguridad del tipo de contenido JSON se puede configurar para los siguientes tipos de infracción:

- Inyección SQL
- Scripts entre sitios
- Inyección de

Configurar el registro detallado para la protección de seguridad JSON mediante la CLI

Para capturar información detallada del encabezado HTTP como registros, puede configurar el parámetro de registro detallado en el perfil de Web App Firewall. En el símbolo del sistema, escriba:

```
set appfw profile <profile_name> -VerboseLogLevel ( pattern |
   patternPayload | patternPayloadHeader )
<!--NeedCopy-->
```

Ejemplo:

```
set appfw profile profile1 -VerboseLogLevel patternPayloadHeader
```

Los niveles de registro disponibles son:

patrón. Registra solo el patrón de infracción.

Carga útil de patrón. Registra el patrón de infracción y 150 bytes de carga adicional de JSON.

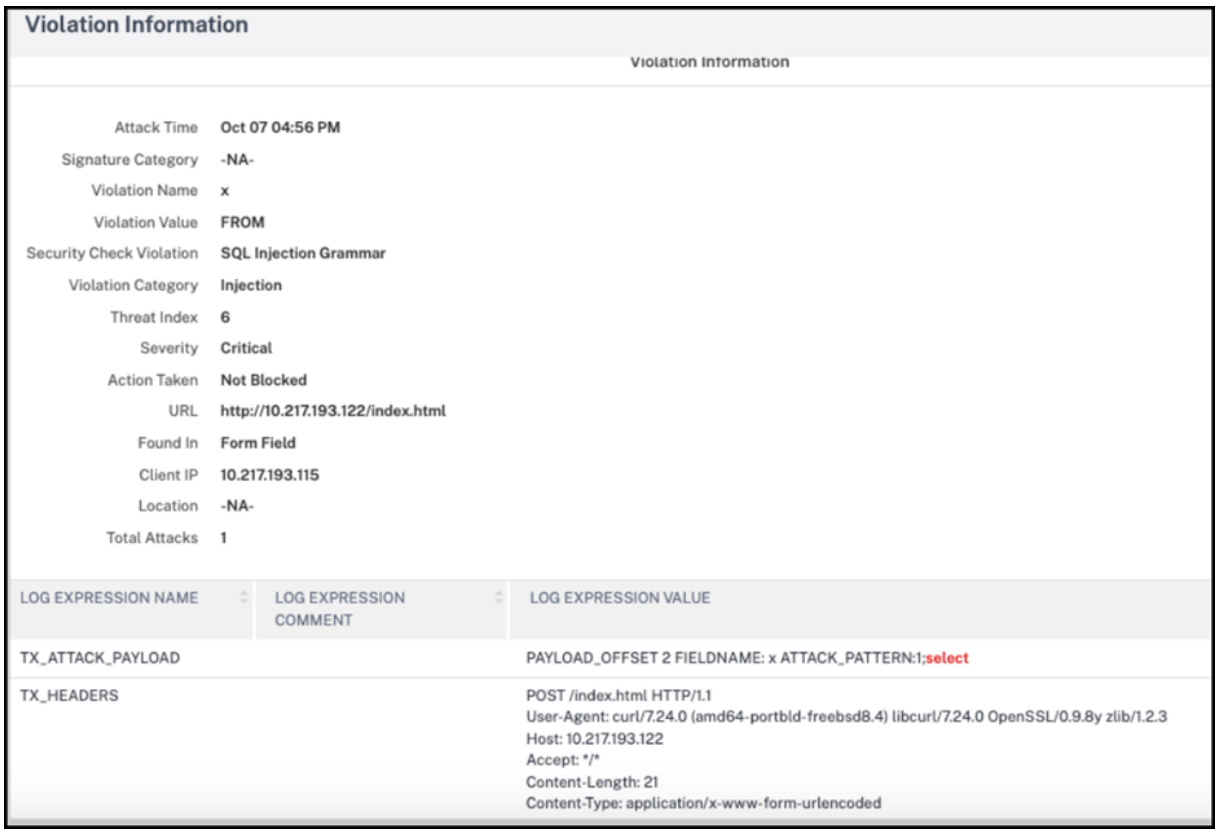
Encabezado de carga de patrón. Registra el patrón de infracción, 150 bytes de carga adicional de JSON e información de encabezado HTTP.

Configuración del nivel de registro detallado mediante la GUI de Citrix ADC

Siga el procedimiento a continuación para configurar el nivel de registro detallado para la protección de seguridad JSON.

1. En el panel de navegación, vaya a **Seguridad > Perfiles**.
2. En la página **Perfiles**, haga clic en **Agregar**.
3. En la página **Perfil de Citrix Web App Firewall**, haga clic en **Comprobaciones de seguridad** en **Configuración avanzada**.
4. En la sección **Verificaciones de seguridad**, seleccione **JSON** y haga clic en **Configuración de acción**.
5. En la página **Configuración de seguridad de JSON**, defina el parámetro de **nivel de registro detallado**.
6. Haga clic en **Aceptar** y **Listo**.

Según los detalles capturados por el registro detallado JSON de Citrix ADC WAF, se pueden inspeccionar los siguientes detalles de infracción en el servidor Citrix ADM.



Protección de subida de archivos

October 5, 2021

Muchos atacantes intentan cargar código malicioso, virus o malware como archivos adjuntos durante el envío de varios formularios. Es importante proteger nuestra red y superar estas amenazas. Para evitar este tipo de cargas de archivos maliciosas, un administrador de Citrix ADC ahora puede configurar un conjunto de formatos de carga de archivos permitidos en el perfil WAF. De este modo, restringe la carga de archivos a formatos específicos y protege el dispositivo contra cargas de archivos malintencionadas. Sin embargo, la protección solo funciona cuando se inhabilita la opción “excludeFileUploadFormChecks” en el perfil WAF.

Cómo funciona la carga de archivos

Al configurar los formatos de carga de archivos permitidos, la interacción del componente es la siguiente:

- La solicitud del cliente tiene un envío de formulario con un tipo de carga de archivo, por ejemplo, PDF.

- Como parte de la comprobación de seguridad, WAF inspecciona la carga útil de la solicitud y valida el tipo de archivo (según los números de firma mágica).
- Si el tipo de archivo es un formato de archivo permitido, se aplica la acción correspondiente basada en el enlace de tipo de archivo.
- Para validar el tipo de archivo, el dispositivo inspecciona la carga útil y comprueba los números mágicos conocidos en los desplazamientos conocidos. Cada tipo de archivo tiene una secuencia de números mágicos que valida el tipo de archivo.
- Solo si se aprueba la validación, WAF identifica el archivo como un formato permitido y se aplica la acción asociada.

Configurar la carga de tipos de archivo mediante la CLI de Citrix ADC

Para configurar los formatos de archivo permitidos, el dispositivo utiliza un perfil WAF vinculado a los parámetros de carga de archivos.

1. Configurar el perfil de firewall de aplicaciones web

Para configurar un perfil de firewall de aplicaciones web, escriba lo siguiente:

```
set appfw profile <profile_name> [-fileUploadTypesAction <fileUploadTypesAction
>]<fileUploadTypesAction> = ( none | block | log | stats )
```

Ejemplo

```
set appfw profile profile1 -fileUploadTypesAction block
```

1. Vincular el perfil de Firewall de aplicaciones web con los parámetros de carga de archivos. El comando vincula la exención (relajación) o regla especificada al perfil de firewall de aplicaciones especificado.

Para enlazar un perfil con parámetros de carga de archivos, escriba lo siguiente:

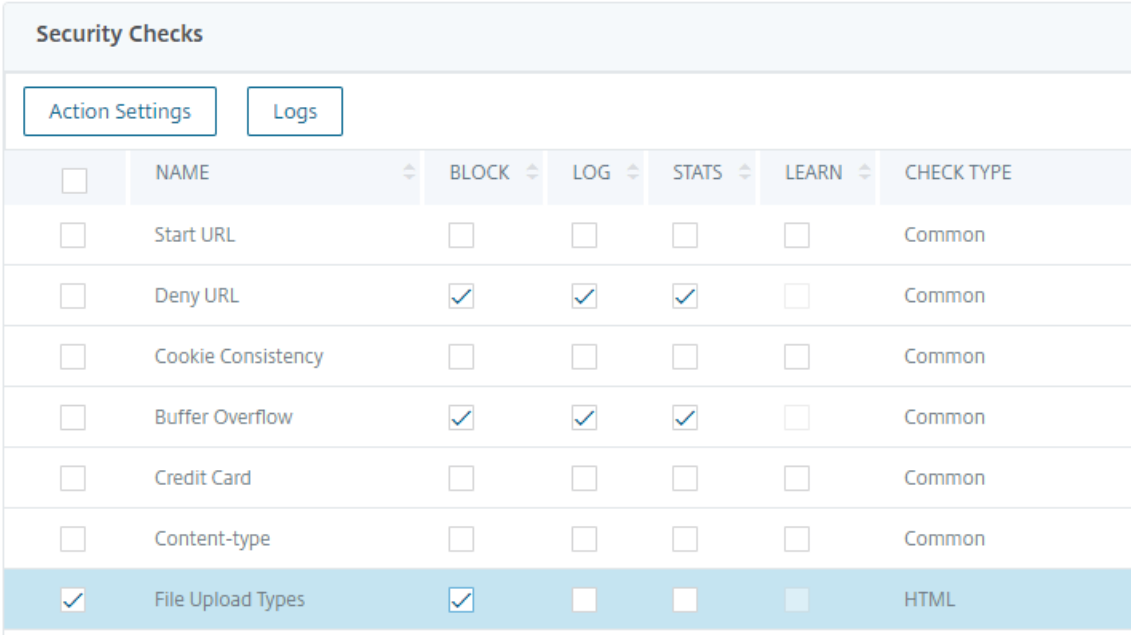
```
bind appfw profile <profile_name> - fileUploadType <form_field > <form_action_url
> -fileType <fileType> ( pdf | msdoc | text | image | any)
```

\[-isNameRegex REGEX (REGEX) | NO REGEX)\]
> **Nota:**
>
> El nombre del campo de formulario es un tipo de expresión regular. El valor por defecto es 'NOTREGEX'.
Ejemplo
'> bind appfw profile test -fileuploadType thefile "http://10.10.10.10/fileupload_sample/upload.php" -filetype image -isNameRegex'
-->

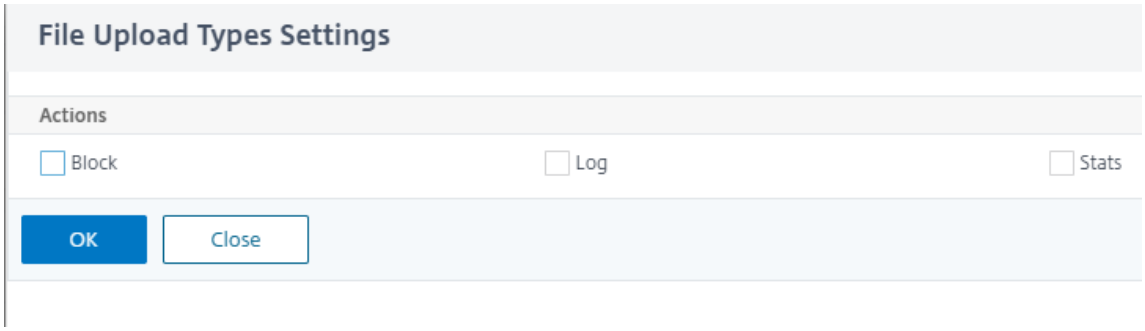
Configurar la protección de seguridad de carga de archivos mediante la GUI de Citrix ADC

Siga el procedimiento que se indica a continuación para establecer la configuración de carga de archivos.

1. En el panel de navegación, vaya a **Seguridad** > **Perfiles**.
2. En la página Perfiles, haga clic en **Agregar**.
3. En la página **Perfil de Citrix Web App Firewall**, haga clic en **Comprobaciones de seguridad** en **Configuración avanzada**.
4. En la sección **Comprobaciones de seguridad**, vaya a la configuración **Tipos de carga de archivos** .



5. Seleccione la casilla de verificación y haga clic en **Configuración de acciones**.
6. En la página **Configuración de tipos de carga de archivos**, defina la acción de carga de archivos.
7. Haga clic en **OK**.
8. En la página **Perfil de Citrix Web App Firewall**, haga clic en **Aceptar** y **listo**.

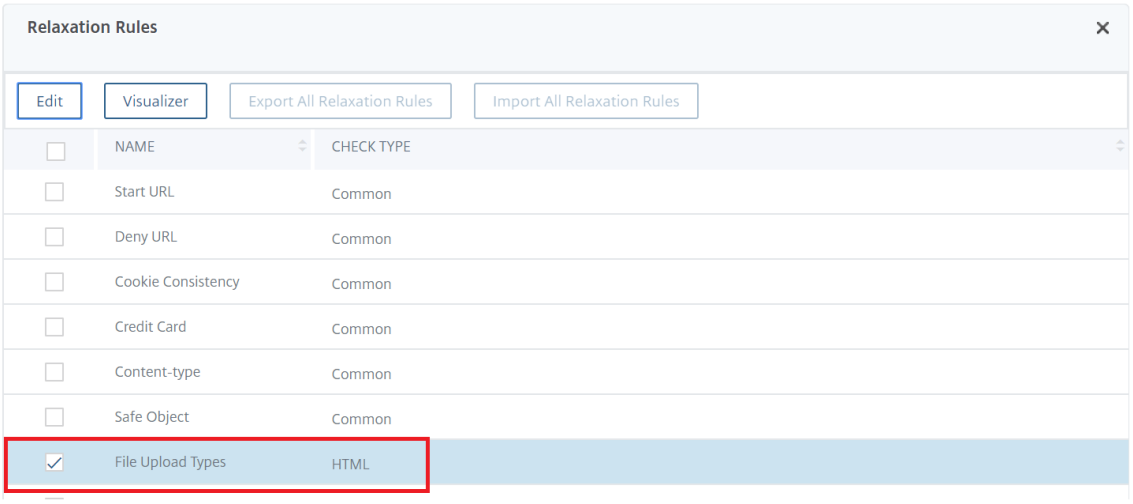


Configurar la regla de relajación de carga de archivos mediante la GUI de Citrix ADC

Puede relajar la protección de seguridad de carga de archivos para evitar falsos positivos. Por ejemplo, el dispositivo puede bloquear la carga de archivos, pero puede agregar una regla de relajación para permitir la subida de archivos desde sitios web específicos. De este modo, el dispositivo omite la inspección de seguridad del campo de formulario especificado y permite a los usuarios cargar archivos del sitio web mencionado en la URL de acción.

Siga el procedimiento que se indica a continuación para crear una regla de relajación.

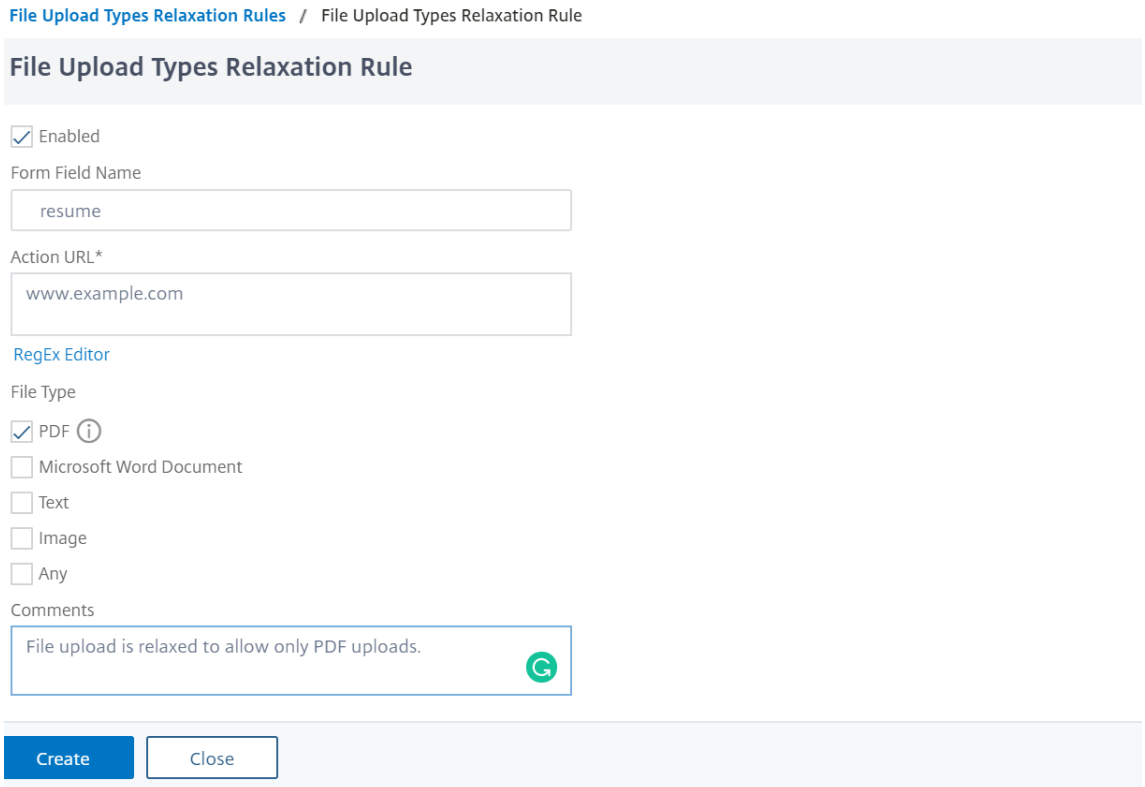
1. En el panel de navegación, vaya a **Seguridad** > **Citrix Web App Firewall** < **Perfiles**.
2. En la página Perfiles, haga clic en **Agregar**.
3. En la página **Perfil de Citrix Web App Firewall**, haga clic en **Reglas de relajación** en **Configuración avanzada**.
4. En la sección **Reglas de relajación**, seleccione **Tipos de carga de archivos** y haga clic en **Modificar**.



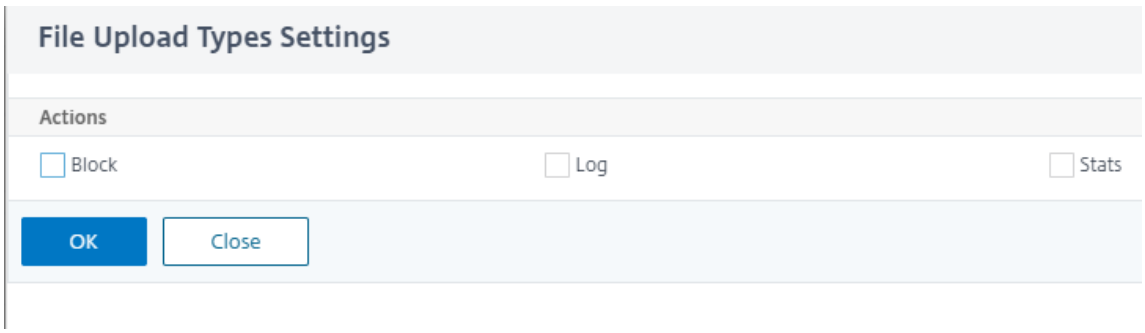
5. En la página **Reglas de relajación de tipos de carga de archivos**, haga clic en **Agregar**.
6. En la página **Regla de relajación de tipos de carga de archivos**, defina los siguientes parámetros:

a) Habilitada. Active esta casilla de verificación para habilitar la regla de relajación.
b) Nombre del campo del formulario. Introduzca el nombre del campo que no requiere comprobación de seguridad.
c) URL de acción. La URL de envío del formulario que debe quedar exenta de la comprobación de seguridad.
d) Tipo de archivo. Tipo de archivo que debe permitirse que el usuario cargue.
e) Comentarios. Una breve descripción de la subida del archivo.

7. Haga clic en **Crear**.



8. En la página **Perfil de Citrix Web App Firewall**, haga clic en **Aceptar** y **listo**.



Configuración y uso de la función de aprendizaje

December 2, 2021

La función de aprendizaje es un filtro de patrón repetitivo que observa la actividad en un sitio web o aplicación protegida por Web App Firewall, para determinar qué constituye la actividad normal en ese sitio web o aplicación. A continuación, genera una lista de hasta 2000 reglas o excepciones sugeridas (relajaciones) para cada comprobación de seguridad que incluyen asistencia para la función de aprendizaje. A los usuarios normalmente les resulta más fácil configurar las relajaciones mediante el uso de la función de aprendizaje que introduciendo las relajaciones necesarias manualmente.

Las comprobaciones de seguridad que admiten la función de aprendizaje son:

- Comprobar URL de inicio
- Comprobación de coherencia de cookies
- Comprobación de coherencia del campo
- Comprobación Formatos de campo
- Comprobación de etiquetado de formularios CSRF
- Comprobación de inyección HTML SQL
- Comprobación de scripts HTML entre sitios
- Comprobación de denegación de servicio XML
- Comprobación de datos adjuntos XML
- Comprobación de interoperabilidad de servicios web

Realizas dos tipos de actividades diferentes cuando utilizas la función de aprendizaje. Primero, habilita y configura la función para usarla. Puede aprender todo el tráfico a sus aplicaciones web protegidas o puede configurar una lista de direcciones IP (denominada lista *Agregar clientes de aprendizaje de confianza*) a partir de la cual la función de aprendizaje puede generar recomendaciones. En segundo lugar, una vez que la función se haya habilitado y haya procesado cierta cantidad de tráfico a sus sitios web protegidos, revise la lista de reglas y relajaciones sugeridas (reglas aprendidas) y marque cada una con una de las siguientes designaciones:

- **Modificar e implementar.** La regla se inserta en el cuadro de diálogo Modificar para que pueda modificarla y se implementa el formulario modificado.
- **Implementación.** La regla aprendida no modificada se coloca en la lista de reglas o relajaciones para esta comprobación de seguridad.
- **Omitir.** La regla aprendida se coloca en una lista de reglas o relajaciones que no se implementan. La regla aprendida se elimina cuando se omite. Sin embargo, como no se agregan a las relajaciones, es posible que vuelvan a aprender.

El aprendizaje no se realiza solo cuando existen relajaciones, excepto las reglas de formato de campo. Cuando se omiten las reglas, solo se eliminan de la base de datos aprendida. Como no se agregan relajaciones, es posible que se vuelvan a aprender. Cuando se implementan las reglas, se eliminan de

la base de datos aprendida y también se agregan relajaciones para las reglas. A medida que se agregan relajaciones, no volverían a aprenderse. Para la protección del formato de campo, el aprendizaje se realiza independientemente de las relajaciones.

Aunque puede utilizar la interfaz de línea de comandos para la configuración básica de la función de aprendizaje, la función está diseñada principalmente para la configuración a través del asistente Web App Firewall o la GUI. Solo puede realizar una configuración limitada de la función de aprendizaje mediante la línea de comandos.

El asistente integra la configuración de las funciones de aprendizaje con la configuración de Web App Firewall en su conjunto y, por lo tanto, es el método más sencillo para configurar esta función en un nuevo dispositivo Citrix ADC o cuando se administra una configuración simple de Web App Firewall. El visualizador GUI y la interfaz manual proporcionan acceso directo a todas las reglas aprendidas para todas las comprobaciones de seguridad y, por lo tanto, a menudo son preferibles cuando debe revisar las reglas aprendidas para muchas comprobaciones de seguridad.

La base de datos de aprendizaje tiene un tamaño de 20 MB, que se alcanza después de que se generan aproximadamente 2000 reglas o relajaciones aprendidas por comprobación de seguridad para la que está habilitado el aprendizaje. Si no revisa y aprueba o ignora las reglas aprendidas con regularidad y se alcanza este límite, se registra un error en el registro de NetScaler y no se generarán más reglas aprendidas hasta que revise las reglas aprendidas y las relajaciones existentes.

Si el aprendizaje se detiene porque la base de datos ha alcanzado su límite de tamaño, puede reiniciar el aprendizaje revisando las reglas y relajaciones aprendidas existentes o restableciendo los datos de aprendizaje. Una vez que se aprueban o ignoran las reglas o relajaciones aprendidas, se eliminan de la base de datos. Después de restablecer los datos de aprendizaje, todos los datos de aprendizaje existentes se eliminan de la base de datos y se restablecen a su tamaño mínimo. Cuando la base de datos tiene un tamaño inferior a 20 MB, el aprendizaje se reinicia automáticamente.

Para configurar los ajustes de aprendizaje mediante la interfaz de línea de comandos

Especifique el perfil de Web App Firewall que se va a configurar y, para cada comprobación de seguridad que desee incluir en ese perfil, especifique el umbral mínimo o el umbral porcentual. El umbral mínimo es un número entero que representa el número mínimo de sesiones de usuario que Web App Firewall debe procesar antes de aprender una regla o relajación (por defecto: 1). El umbral porcentual es un número entero que representa el porcentaje de sesiones de usuario en las que el Web App Firewall debe observar un patrón particular (URL, cookie, campo, archivo adjunto o infracción de reglas) antes de que aprenda una regla o relajación (por defecto: 0). Utilice los siguientes comandos:

- `set appfw learningsettings <profileName> [-startURLMinThreshold <positive_integer>] [-startURLPercentThreshold <positive_integer>] [-cookieConsistencyMinThreshold <positive_integer>] [-cookieConsistencyPercentThres <positive_integer>] [-CSRFtagMinThreshold <positive_integer>] [-`

CSRFtagPercentThreshold <positive_integer>] [-fieldConsistencyMinThreshold <positive_integer>] [-fieldConsistencyPercentThreshold <positive_integer>] [-crossSiteScriptingMinThreshold <positive_integer>] [-crossSiteScriptingPerce <positive_integer>] [-SQLInjectionMinThreshold <positive_integer>] [-SQLInjectionPercentThreshold <positive_integer>] [-fieldFormatMinThreshold <positive_integer>] [-fieldFormatPercentThreshold <positive_integer>] [-XMLWSIMinThreshold <positive_integer>] [-XMLWSIPercentThreshold <positive_integer>] [-XMLAttachmentMinThreshold <positive_integer>] [-XMLAttachmentPercentThreshold <positive_integer>]

- save ns config

Ejemplo

El siguiente ejemplo habilita y configura la configuración de aprendizaje en el perfil para la comprobación de seguridad de HTML SQL Injection. Esta es una configuración de aprendizaje del banco de pruebas inicial adecuada, donde usted tiene un control total sobre el tráfico que se envía a Web App Firewall.

```
1 set appfw learningsettings pr-basic -SQLInjectionMinThreshold 10
2 set appfw learningsettings pr-basic -SQLInjectionPercentThreshold 70
3 save ns config
4 <!--NeedCopy-->
```

Para restablecer la configuración de aprendizaje a sus valores predeterminados mediante la interfaz de línea de comandos

Para eliminar cualquier configuración personalizada de los ajustes de aprendizaje para el perfil especificado y la comprobación de seguridad, y devolver la configuración de aprendizaje a sus valores predeterminados, en el símbolo del sistema escriba los siguientes comandos:

- unset appfw learningsettings <profileName> [-startURLMinThreshold] [-startURLPercentThreshold] [-cookieConsistencyMinThreshold] [-cookieConsistencyPercentThreshold] [-CSRFtagMinThreshold] [-CSRFtagPercentThresh] [-fieldConsistencyMinThreshold] [-fieldConsistencyPercentThreshold] [-crossSiteScriptingMinThreshold] [-crossSiteScriptingPercentThreshold] [-SQLInjectionMinThreshold] [-SQLInjectionPercentThreshold] [-fieldFormatMinThreshold] [-fieldFormatPercentThreshold] [-XMLWSIMinThreshold] [-XMLWSIPercentThreshold] [-XMLAttachmentMinThreshold] [-XMLAttachmentPercen]

- save ns config

Para mostrar la configuración de aprendizaje de un perfil mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba el siguiente comando:

```
show appfw learningsettings <profileName>
```

Para mostrar reglas o relajaciones aprendidas sin revisar para un perfil mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba el siguiente comando:

```
show appfw learningdata <profileName> <securityCheck>
```

Para eliminar reglas o relajaciones aprendidas no revisadas específicas de la base de datos de aprendizaje mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba el siguiente comando:

```
rm appfw learningdata <profileName> (-startURL <expression> | -cookieConsistency
 <string> | (-fieldConsistency <string> <formActionURL>)| (-crossSiteScripting
 <string> <formActionURL>)| (-SQLInjection <string> <formActionURL>)| (-
fieldFormat <string><formActionURL>)| (-CSRFTag <expression> <CSRFFormOriginURL
>)| -XMLDoSCheck <expression> | -XMLWSICheck <expression> | -XMLAttachmentCheck
 <expression>)[-TotalXMLRequests]
```

Ejemplo

El siguiente ejemplo elimina todas las relajaciones aprendidas no revisadas para el perfil, la comprobación de seguridad HTML SQL Injection, que se aplican al campo de **formulario LastName**.

```
1 rm appfw learningdata pr-basic -SQLInjection LastName
2 <!--NeedCopy-->
```

Para eliminar todos los datos aprendidos no revisados mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba el siguiente comando:

```
reset appfw learningdata
```


Para exportar datos de aprendizaje mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba el siguiente comando:

```
export appfw learningdata <profileName> <securitycheck>[-target <string>]
```

Ejemplo

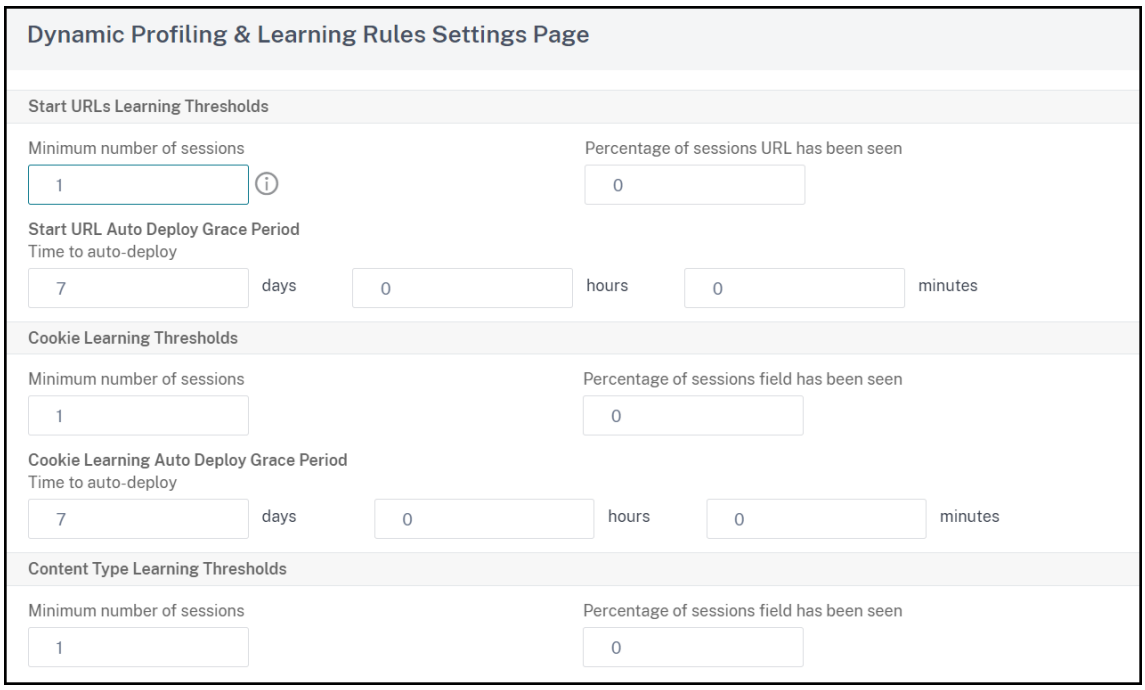
El siguiente ejemplo exporta las relajaciones aprendidas para el perfil y la comprobación de seguridad HTML SQL Injection a un archivo con formato de valores separados por comas (CSV) en el directorio /var/learnt_data/ con el nombre de archivo especificado en el parámetro -target.

```
1 export appfw learningdata pr-basic SQLInjection -target sqli_ld
2 <!--NeedCopy-->
```

Para configurar la función de aprendizaje mediante la interfaz gráfica de usuario

1. Vaya a **Seguridad** > **Web App Firewall** > **Perfiles**.
2. En el panel **Perfiles**, seleccione el perfil y, a continuación, haga clic en **Modificar**.
3. Haga clic en **Reglas aprendidas** en la sección **Configuración avanzada**.
4. En la sección **Reglas aprendidas**, seleccione una comprobación de seguridad y haga clic en **Configuración**.
5. En la página **Configuración de comprobación de seguridad**, establezca los siguientes parámetros:
    a) **Umbral de número mínimo.** Según la configuración de aprendizaje de la comprobación de seguridad que esté configurando, el umbral de número mínimo puede referirse al número mínimo de sesiones de usuario totales que se deben observar, el número mínimo de solicitudes que deben observarse o el número mínimo de veces que se debe observar un campo de formulario específico, antes de que se genere una relajación aprendida. Predeterminado: 1
    b) **Porcentaje de veces el umbral.** Según la configuración de aprendizaje de la comprobación de seguridad que esté configurando, el umbral de porcentaje de veces puede referirse al porcentaje del total de sesiones de usuarios observadas que infringió la comprobación de seguridad, el porcentaje de solicitudes o el porcentaje de veces que un campo de formulario coincidió con un tipo de campo en particular, antes de se genera la relajación aprendida. Predeterminado: 0

6. Haga clic en **Aceptar** y **cerrar**.



7. Haga clic en **Eliminar todos los datos aprendidos** para eliminar todos los datos aprendidos y restablecer la función de aprendizaje, de modo que debe iniciar sus observaciones nuevamente desde el principio.

> **Nota:**
>
> Este botón elimina solo las recomendaciones aprendidas que no se han revisado y se han aprobado u omitido. No elimina las relajaciones aprendidas que se han aceptado e implementado.

8. Para restringir el motor de aprendizaje al tráfico de un conjunto específico de IP, haga clic en **Clientes de aprendizaje de confianza**y agregue las direcciones IP que quiere utilizar a la lista.
   a) Para agregar una dirección IP o un rango de direcciones IP a la lista de clientes de aprendizaje de confianza, haga clic en **Agregar**.
   b) En el cuadro de diálogo **Agregar clientes de aprendizaje** de confianza, en el cuadro de lista IP de clientes de confianza, escriba la dirección IP o un rango de direcciones IP en formato CIDR.
   c) En el área de texto Comentarios, escriba un comentario que describa esta dirección o rango IP.
   d) Haga clic en **Crear** para agregar su nueva dirección IP o rango a la lista.
   e) Para modificar una dirección o rango IP existente, haga clic en la dirección IP o el rango y, a continuación, haga clic en **Abrir**. Excepto por el nombre, el cuadro de diálogo que aparece es idéntico al cuadro de diálogo **Agregar clientes de aprendizaje de confianza**.
   f) Para inhabilitar o habilitar una dirección o rango IP, pero dejarlo en la lista, haga clic en

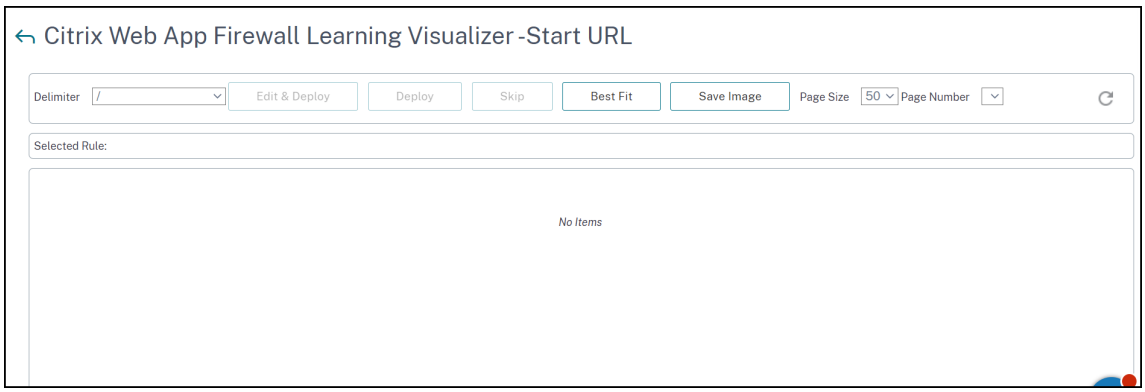
la dirección o rango IP y, a continuación, haga clic en **Inhabilitar o Habilitar**, según corresponda.

g) Para eliminar una dirección IP o un rango por completo, haga clic en la dirección IP o el rango y, a continuación, haga clic en **Eliminar**.

9. Haga clic en **Cerrar** para volver a la página Configurar perfil de Web App Firewall.
10. Haga clic en **Listo**.

Para revisar las reglas o relajaciones aprendidas mediante la interfaz gráfica de usuario

1. Vaya a **Seguridad** > **Web App Firewall** > **Perfiles**.
2. En el panel **Perfiles**, seleccione el perfil y, a continuación, haga clic en **Modificar**.
3. Haga clic en **Reglas aprendidas** en la sección **Configuración avanzada**.
4. En la sección **Reglas aprendidas**, seleccione una comprobación de seguridad y haga clic en **Configuración**.
5. Para revisar los datos aprendidos jerárquicamente como un árbol ramificado, lo que le permite elegir patrones generales que coincidan con muchos de los patrones aprendidos, haga clic en **Visualizador**.
6. Si ha optado por revisar los patrones aprendidos reales, lleve a cabo los siguientes pasos.
7. Seleccione la primera relajación aprendida y elija cómo gestionarla.
   a) Para modificar y, a continuación, aceptar la relajación, haga clic en **Modificar e implementar**, modifique la expresión regular de relajación y, a continuación, haga clic en **Aceptar**.
   b) Para aceptar la relajación sin modificaciones, haga clic en **Implementar**.
   c) Para eliminar la relajación de la lista sin implementarla, haga clic en **Omitir**.
   d) Repita el paso anterior para revisar cada relajación aprendida adicional.
8. Haga clic en **Cerrar** para volver al cuadro de diálogo **Administrar reglas aprendidas**.
9. Haga clic en **Listo**.



Perfilado dinámico

October 5, 2021

La función de aprendizaje es un filtro de patrones que observa y aprende las actividades en el servidor back-end. Basándose en la observación, el motor de aprendizaje genera hasta 2000 reglas o excepciones (relajaciones) para cada comprobación de seguridad. Para automatizar el proceso e implementar automáticamente las reglas de relajación, el dispositivo Citrix ADC utiliza la creación de perfiles dinámicos.

Con la creación de perfiles dinámicos, el dispositivo registra los datos aprendidos para un umbral predefinido y envía una alerta SNMP al usuario. Si el usuario no omite los datos en un período de gracia, el dispositivo los implementa automáticamente como regla de relajación. Anteriormente, el usuario tenía que implementar manualmente las reglas de relajación. Actualmente, la creación de perfiles dinámicos solo está disponible para las siguientes comprobaciones de seguridad:

1. Inyección HTML SQL
2. Scripts HTML entre sitios
3. Formato de campo
4. URL de inicio
5. Tipo de contenido
6. formatos de campo
7. Etiquetado de formularios CSRF
8. Consistencia de cookies
9. Denegar URL
10. Desbordamiento de búfer
11. Tarjeta de crédito
12. Protección por tipo de contenido
13. Protección contra inyección JSON Cmd

Por ejemplo, considere la comprobación de seguridad HTML SQL Injection habilitada con la creación de perfiles dinámicos. Puede utilizar el aprendizaje para obtener una lista de IP (denominada lista de clientes de aprendizaje de confianza) a partir de la cual la función de aprendizaje debe generar recomendaciones. Para configurar una lista de clientes de confianza, consulte el tema Learning Trusted Clients. Si el tráfico entrante presenta infracciones, se registra como datos aprendidos. Si los datos aprendidos se registran en el motor de aprendizaje, el dispositivo envía una alerta SNMP al usuario. Si el usuario no reconoce un falso positivo y no omite los datos aprendidos en un período de gracia, el dispositivo lo implementa automáticamente como regla de relajación.

> **Nota:**
> Después de configurar el perfil dinámico, debe revisar periódicamente la configuración del dis-

> positivo para la implementación automática de las reglas de relajación y guardarla en el dispositivo.

Configurar perfiles dinámicos mediante la interfaz de comandos de Citrix ADC

La creación de perfiles dinámicos está disponible para las comprobaciones de seguridad de URL de inicio, scripts HTML entre sitios, formato de campo o inyección SQL HTML. Para configurar la creación de perfiles dinámicos, debe completar los pasos siguientes.

1. Configurar el aprendizaje dinámico
2. Configurar período de gracia de implementación automática

Configurar el aprendizaje dinámico

Como primer paso, debe configurar el aprendizaje dinámico en el dispositivo. En el símbolo del sistema, escriba:

```
set appfw profile <profile_name> dynamicLearning <security_checks>
```

Ejemplo

```
set appfw profile test1 dynamicLearning SQLInjection CrossSiteScripting
fieldFormat startURL
```

Configurar período de gracia de implementación automática

Una vez habilitada la función en comprobaciones de seguridad específicas, debe configurar el período de gracia para la implementación automática.

```
set appfw learningsettings <profile name> -crossSiteScriptingAutoDeployGracePeriod
 <seconds>

set appfw learningsettings <profile name> fieldFormatAutoDeploymentGracePeriod
 <seconds>

set appfw learningsettings <profile name> SQLInjectionAutoDeploymentGracePeriod
 <seconds>

set appfw learningsettings <profile name> -startURLAutoDeployGracePeriod <
seconds>
```

Ejemplo

```
set appfw learningsettings test1 -crossSiteScriptingAutoDeployGracePeriod 30
```

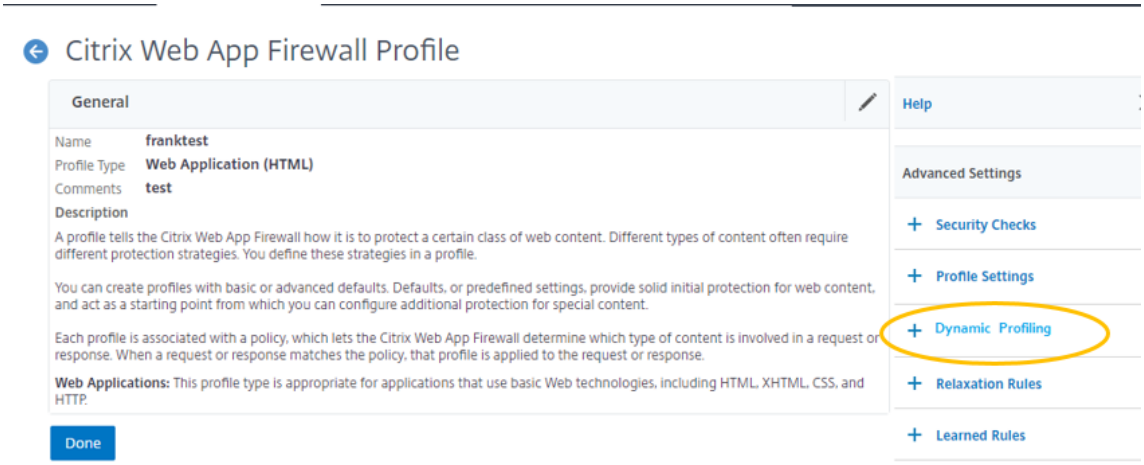


```
set appfw learningsettings test1 -startURLAutoDeployGracePeriod 7
set appfw learningsettings test1 -fieldFormatAutoDeploymentGracePeriod 10
set appfw learning settings test1 -SQLInjectionAutoDeploymentGracePeriod 12
```

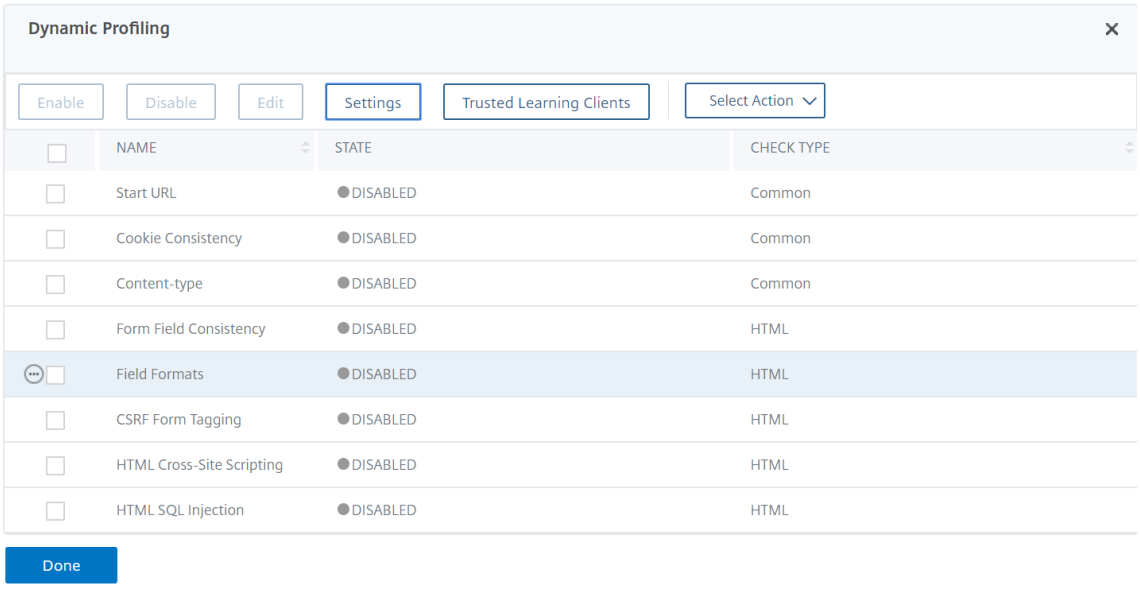
> **Nota:**
>
> En este caso, el período de gracia de implementación automática es en minutos.

Configuración de perfiles dinámicos mediante la GUI de Citrix ADC

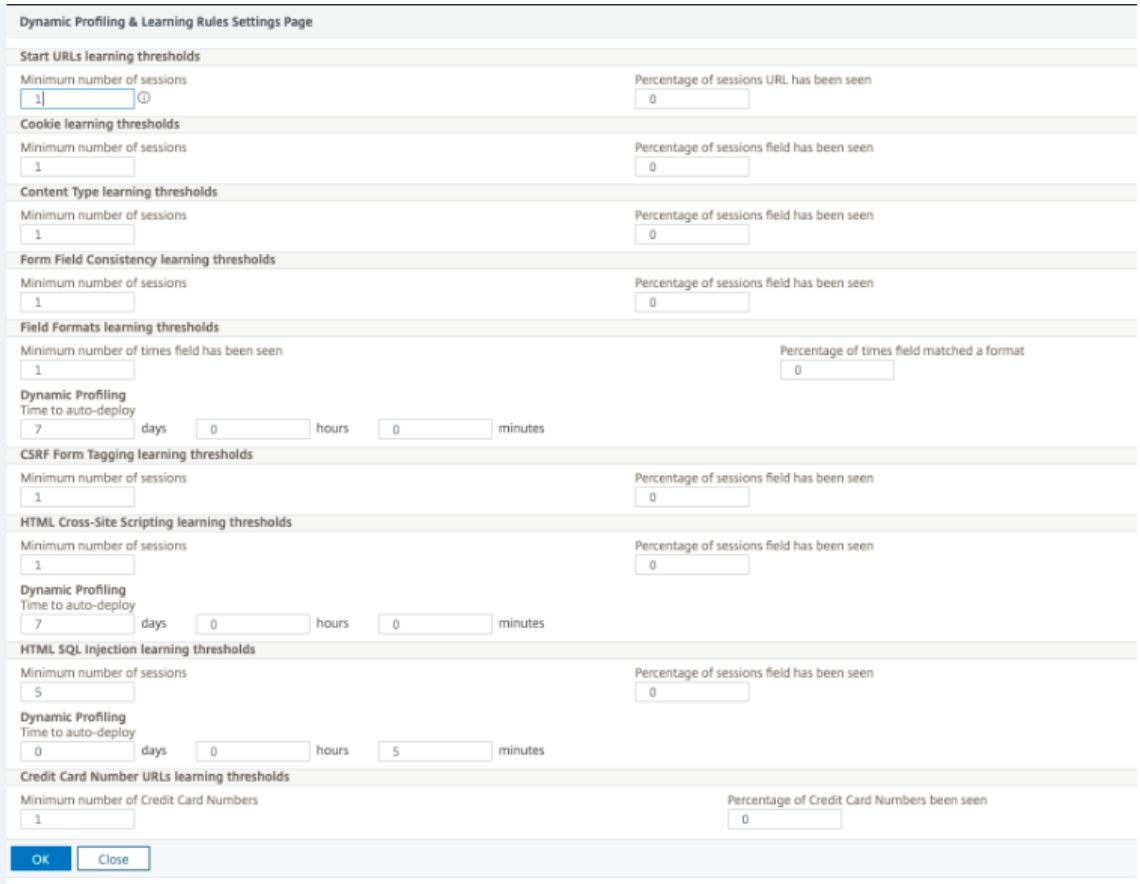
1. Vaya a **Seguridad > Citrix Web App Firewall > Perfil**.
2. En el panel de detalles, seleccione un perfil y haga clic en **Modificar**.
3. En la página **Perfil de la aplicación web de Citrix**, haga clic en **Generación de perfiles dinámicos** en **Configuración avanzada**.



4. En la sección Creación de **perfiles dinámicos**, seleccione una comprobación de seguridad y haga clic en **Modificar**.



5. En la página **Configuración dinámica de perfiles y aprendizaje**, defina el período de gracia de la comprobación de seguridad.



6. Haga clic en **Aceptar** y **Listo**.

Exportación e importación de normas de relajación

Al habilitar la creación de perfiles dinámicos, los datos aprendidos se implementan automáticamente como reglas de relajación. Junto con esto, el dispositivo también le permite exportar las reglas de relajación basadas en perfiles dinámicos y las reglas de relajación regulares. Puede exportar las reglas del entorno de ensayo e importarlas al entorno de producción.

> **Nota:**
>
> Al importar reglas al entorno de producción, debe asegurarse de que el proceso es aditivo y no invalida la configuración existente.

Cómo exportar e importar reglas de relajación

Para exportar e importar las reglas de relajación, debe completar los siguientes pasos:

1. En primer lugar, debe exportar los datos basados en perfiles dinámicos. Para ello, la opción de exportación está disponible para las reglas de relajación del perfil WAF. Al seleccionar esta opción, se exportan las reglas de relajación de perfiles dinámicos y las reglas de relajación regulares. Puede utilizar la opción de exportación para descargar la configuración como un paquete comprimido en el dispositivo.
2. Una vez exportados los datos del entorno provisional, debe importarlos a otro dispositivo Citrix ADC. Para ello, debe utilizar la opción de importación disponible en las reglas de relajación del perfil WAF. Al seleccionar esta opción, el dispositivo importa las reglas de relajación especificadas incluidas y las restaura en el perfil WAF del dispositivo seleccionado.

> **Nota:**
>
> Si va a importar reglas de relajación en un perfil WAF, existen dos tipos de acción:
> Aumentar: esta acción garantiza que la importación sea aditiva y, por lo tanto, no anula ninguna configuración existente.
> Sobrescribir: esta acción sobrescribe la configuración existente con la configuración presente en el paquete de exportación comprimido".

Importar archivo de reglas de relajación archivado mediante CLI

Para importar las reglas de relajación, debe importar el archivo en el dispositivo Citrix ADC y, a continuación, ejecutar el comando de restauración para extraer la configuración. El siguiente conjunto de comandos CLI se puede utilizar para exportar, importar y administrar las configuraciones.

Para importar el archivo archivado desde la ubicación específica y restaurarlo, en el símbolo del sistema, escriba:

```
import appfw archive <src> <name> [-comment <string>]
```


Donde:
“src”: Indica el origen del archivo tar en el formulario, <protocol>://<host>[:<port>][/<path>]
“nombre”: Indica el nombre del archivo.
“ comentario”: Comentarios asociados a este archivo.

```
restore appfw profile <archivename> [-relaxationRules] [-importProfileName
 <string>] [-matchUrlString <string>] [-replaceUrlString <string>] [-
overwrite] [-augment]
```

Dónde,
archivename: Indica el origen del archivo tar. Este es un argumento obligatorio.
“RelaxationRules”: Opción para importar todas las reglas de relajación de appfw.

importProfileName: Indica el nombre del perfil creado o actualizado para asociar las reglas de relajación durante la operación de restauración.
“ MatChurlString”: Indica la cadena URL de acción para coincidir en las reglas de relajación archivadas.

replaceUrlString: Indica una cadena que se va a reemplazar en la URL de acción mientras restaura las reglas de relajación.

overwrite: acción de reglas existentes para purgar las reglas de relajación existentes y sustituirlas durante la importación.

augment: acción de reglas existentes para aumentar las reglas de relajación durante la importación.

Ejemplo:

```
import appfw archive local: dutA_test_pr.tgz demo
restore appfw profile dutA_test_pr
```

Exportar el archivo archivado al dispositivo seleccionado mediante la CLI

Si utiliza la CLI para exportar las reglas de relajación appfw, debe archivar la configuración y, a continuación, exportarla.
Para archivar y exportar el archivo archivado, en el símbolo del sistema, escriba:

```
archive appfw profile <name> <archivename> [-comment <string>]
```

Dónde,
archive name: Indica el origen del archivo tar. Este es un argumento obligatorio.
name: Indica el nombre del perfil appfw que contiene las reglas de relajación que se van a exportar

```
export appfw archive <name> <target>
```

Dónde,
Nombre. Nombre del archivo tar. Este es un argumento obligatorio. Longitud máxima: 31

objetivo. Ruta del archivo que se va a exportar. Este es un argumento obligatorio. Longitud máxima: 2047

Ejemplo:

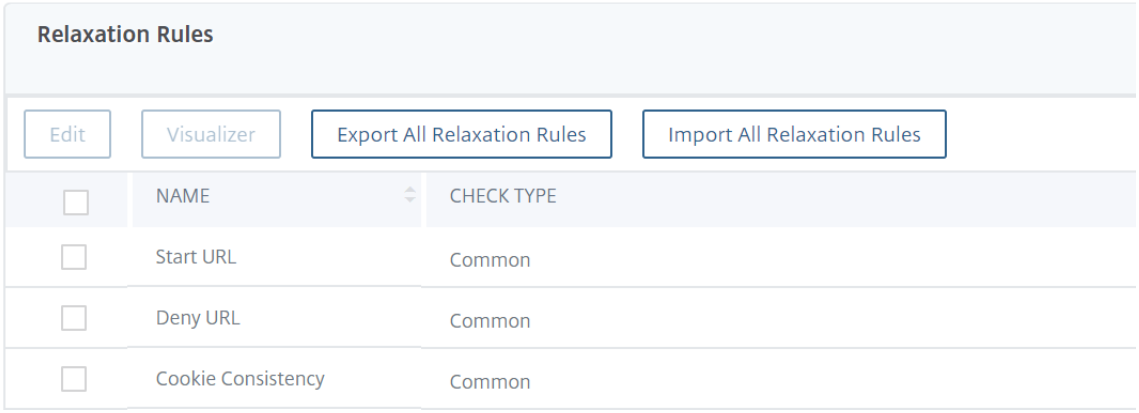
```
> archive appfw profile test_pr archived_test_pr

> export appfw archive archived_test_pr local:dutA_test_pr
```

Para exportar reglas de relajación mediante la GUI de Citrix ADC

Siga los pasos que se indican a continuación para exportar las reglas de relajación:

1. Vaya a **Seguridad** > **Citrix Web App Firewall**.
2. En la página de detalles, haga clic en el enlace **Perfiles de Citrix Web App Firewall** en la sección **Resumen de configuración** .
3. En la página **Perfil de Citrix Web App Firewall**, haga clic en el enlace **Reglas de relajación** de la sección **Configuración avanzada** .
4. En la sección **Reglas de relajación**, haga clic en **Exportar todas las reglas de relajación**. La acción se aplica a todas las comprobaciones de seguridad y a las que el aprendizaje dinámico está habilitado en ese perfil.

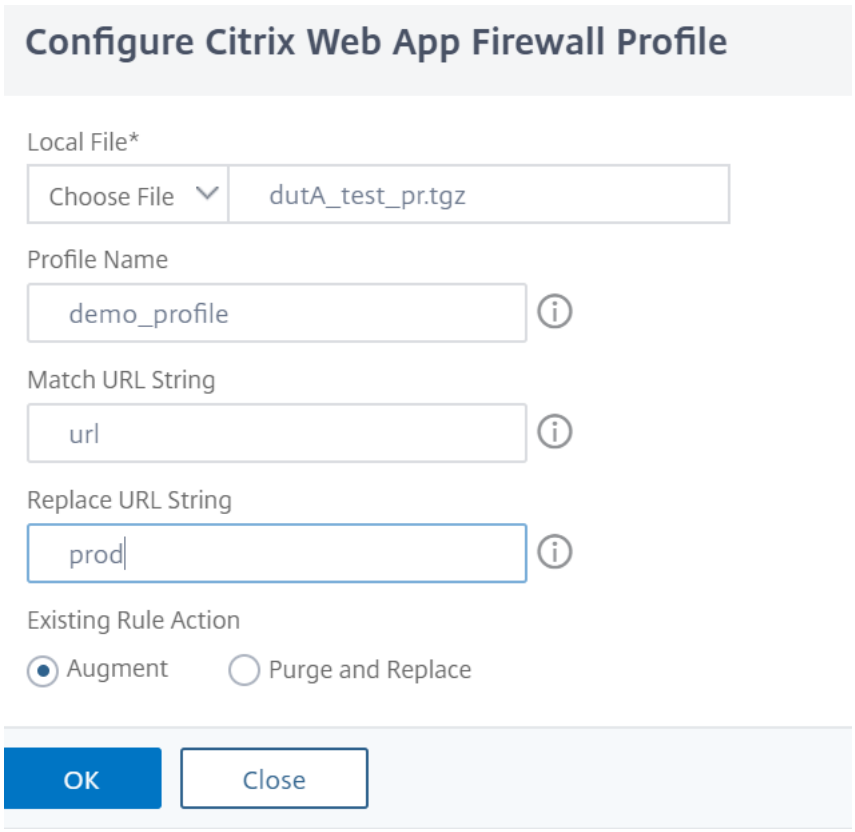


Para importar reglas de relajación mediante la GUI de Citrix ADC

Complete los pasos para importar reglas de relajación:

1. Vaya a **Seguridad** > **Citrix Web App Firewall**.
2. En la página de detalles, haga clic en el enlace **Perfiles de Citrix Web App Firewall** en la sección **Resumen de configuración** .
3. En la página **Perfil de Citrix Web App Firewall**, haga clic en el enlace **Reglas de relajación** de la sección **Configuración avanzada** .

4. En la sección **Reglas de relajación**, haga clic en **Importar todas las reglas de relajación**.
5. En la página **Configurar perfil de Citrix Web App Firewall**, defina los siguientes parámetros:
   a) Archivo local. Nombre del archivo archivado comprimido que contiene las reglas de relajación.
   b) Nombre del perfil. Nombre del perfil al que están vinculadas las reglas de relajación.
   c) Cadena URL coincidente. Parte de la URL que coincide.
   d) Reemplazar cadena URL. Parte de la URL que sustituye a la cadena URL.
   e) Acción de regla existente. Seleccione si la regla debe sobrescribir las reglas existentes o aumentar las reglas existentes.
6. Haga clic en **OK**.



Información complementaria sobre los perfiles

April 5, 2022

A continuación, encontrará información complementaria sobre aspectos concretos de los perfiles de Web App Firewall. Esta información explica cómo incluir caracteres especiales en una regla de comprobación de seguridad o relajación, y cómo utilizar variables al configurar perfiles.

Soporte de variables de configuración

En lugar de usar valores estáticos, para configurar las comprobaciones de seguridad y la configuración de Web App Firewall, ahora puede usar variables con nombre Citrix ADC estándar. Al crear variables, puede exportar y, a continuación, importar configuraciones a nuevos dispositivos Citrix ADC o actualizar los dispositivos Citrix ADC existentes desde un único conjunto de archivos de configuración. Esto simplifica las actualizaciones cuando utiliza una configuración de banco de pruebas para desarrollar una configuración compleja de Web App Firewall que se ajuste a su red y servidores locales y, a continuación, transferir esa configuración a sus dispositivos Citrix ADC de producción.

Puede crear variables de configuración de Web App Firewall de la misma manera que cualquier otra variable con nombre de Citrix ADC, siguiendo las convenciones estándar de Citrix ADC. Puede crear una variable de expresión con nombre mediante la línea de comandos de Citrix ADC o la GUI de Citrix.

Las siguientes URL y expresiones se pueden configurar con variables en lugar de valores estáticos:

- **URL de inicio** (-starturl)
- **Denegar URL** (-denyurl)
- **URL de acción** de *formulario para la comprobación de coherencia de campos de formulario* (-fieldconsistency)
- **URL de acción** para la *comprobación de inyección XML SQL* (-xmlSQLInjection)
- **URL de acción** para la *comprobación de scripts entre sitios de XML* (scripts -xmlcross-site)
- **URL de acción de formulario** para la *comprobación de inyección HTML SQL* (-sqlInjection)
- **URL de acción de formulario** para *comprobación de formato de campo* (-fieldFormat)
- **URL de origen de formulario** y **URL de acción de formulario** para la *verificación de falsificación de solicitudes entre sitios (CSRF)* (-csrfTag)
- **URL de acción de formulario** para la *comprobación de scripts entre sitios HTML* (-crossSiteScripting)
- **Objeto seguro** (-safeObject)
- **URL de acción** para la *comprobación de denegación de servicio XML (XDoS)* (-XMLDoS)
- **URL** para la *comprobación de interoperabilidad de servicios web* (-XMLWSIURL)
- <**URL** para la *comprobación de validación XML* (-XMLValidationURL)
- **URL** para la *comprobación de datos adjuntos XML* (-XMLAttachmentURL)

Para obtener más información, consulte Directivas y expresiones.

Para utilizar una variable en la configuración, debe incluir el nombre de la variable entre dos símbolos en (@) y luego usarlo exactamente como lo haría con el valor estático que reemplaza. Por ejemplo, si está configurando la comprobación Denegar URL mediante la interfaz gráfica de usuario y desea agregar la variable de expresión con nombre myDenyURL a la configuración, escribiría @myDenyURL @ en el cuadro de diálogo Agregar URL denegada, área de texto Denegar URL. Para realizar la misma tarea mediante la línea de comandos de Citrix ADC, debe escribir add appfw profile <name> -denyURLAction @myDenyURL@.

Formato de codificación de caracteres PCRE

El sistema operativo Citrix ADC solo admite la entrada directa de caracteres en el conjunto de caracteres ASCII imprimibles, caracteres con códigos hexadecimales entre HEX 20 (ASCII 32) y HEX 7E (ASCII 127). Para incluir un carácter con un código fuera de ese rango en la configuración de Web App Firewall, debe escribir su código hexadecimal UTF-8 como expresión regular de PCRE.

Varios tipos de caracteres requieren codificación mediante una expresión regular de PCRE si los incluye en la configuración de Web App Firewall como URL, nombre de campo de formulario o expresión de objeto seguro. Entre ellas se encuentran:

- **Caracteres ASCII superiores.** Caracteres con codificaciones desde HEX 7F (ASCII 128) hasta HEX FF (ASCII 255). Según el mapa de caracteres utilizado, estas codificaciones pueden hacer referencia a códigos de control, caracteres ASCII con acentos u otras modificaciones, caracteres del alfabeto no latino y símbolos no incluidos en el conjunto ASCII básico. Estos caracteres pueden aparecer en URL, nombres de campos de formulario y expresiones de objetos seguros.
- **Caracteres de doble byte.** Caracteres con codificaciones que usan dos palabras de 8 bytes. Los caracteres de doble byte se utilizan principalmente para representar texto en chino, japonés y coreano en formato electrónico. Estos caracteres pueden aparecer en URL, nombres de campos de formulario y expresiones de objetos seguros.
- **Caracteres de control ASCII.** Caracteres no imprimibles que se utilizan para enviar comandos a una impresora. Todos los caracteres ASCII con códigos hexadecimales inferiores a HEX 20 (ASCII 32) entran en esta categoría. Sin embargo, estos caracteres nunca deben aparecer en una URL o en un nombre de campo de formulario, y rara vez aparecerían en una expresión de objeto segura.

El dispositivo Citrix ADC no admite todo el conjunto de caracteres UTF-8, sino solo los caracteres que se encuentran en los siguientes ocho conjuntos de caracteres:

- **Inglés de EE. UU. (ISO-8859-1).** Aunque la etiqueta dice “inglés de EE. UU.”, Web App Firewall admite todos los caracteres del conjunto de caracteres ISO-8859-1, también denominado conjunto de caracteres Latin-1. Este conjunto de caracteres representa completamente la mayoría de los idiomas modernos de Europa occidental y representa todos los caracteres menos comunes en el resto.
- **Chino tradicional (Big5).** Web App Firewall admite todos los caracteres del conjunto de caracteres BIG5, que incluye todos los caracteres chinos tradicionales (ideografías) comúnmente utilizados en el chino moderno tal como se habla y escribe en Hong Kong, Macao, Taiwán y por muchas personas de ascendencia étnica china que viven fuera de China continental.
- **Chino simplificado (GB2312).** Web App Firewall admite todos los caracteres del conjunto de caracteres GB2312, que incluye todos los caracteres en chino simplificado (ideogramas) que se utilizan comúnmente en el chino moderno tal como se habla y escribe en China continental.

- **Japonés (SJIS).** Web App Firewall admite todos los caracteres del conjunto de caracteres Shift-JIS (SJIS), que incluye la mayoría de los caracteres (ideogramas) que se usan comúnmente en japonés moderno.
- **Japonés (EUC-JP).** Web App Firewall admite todos los caracteres del conjunto de caracteres EUC-JP, que incluye todos los caracteres (ideogramas) que se usan comúnmente en japonés moderno.
- **Coreano (EUC-KR).** Web App Firewall admite todos los caracteres del conjunto de caracteres EUC-KR, que incluye todos los caracteres (ideogramas) que se utilizan comúnmente en el coreano moderno.
- **Turco (ISO-8859-9).** Web App Firewall admite todos los caracteres del conjunto de caracteres ISO-8859-9, que incluye todas las letras usadas en turco moderno.
- **Unicode (UTF-8).** Web App Firewall admite ciertos caracteres adicionales en el conjunto de caracteres UTF-8, incluidos los que se usan en ruso moderno.

Al configurar Web App Firewall, se escriben todos los caracteres que no son ASCII como expresiones regulares en formato PCRE mediante el código hexadecimal asignado a ese carácter en la especificación UTF-8. A los símbolos y caracteres del conjunto de caracteres ASCII normal, a los que se les asignan códigos únicos de dos dígitos en ese conjunto de caracteres, se les asignan los mismos códigos en el conjunto de caracteres UTF-8. Por ejemplo, el signo de exclamación (!) , al que se le asigna el código hexadecimal 21 en el conjunto de caracteres ASCII, también es hexadecimal 21 en el conjunto de caracteres UTF-8. Los símbolos y caracteres de otro conjunto de caracteres admitidos tienen un conjunto pareado de códigos hexadecimales asignados en el conjunto de caracteres UTF-8. Por ejemplo, a la letra a con acento agudo (á) se le asigna el código UTF-8 C3 A1.

La sintaxis que utiliza para representar estos códigos UTF-8 en la configuración de Web App Firewall es “xNN” para caracteres ASCII; “\ xNN\ xNN” para caracteres no ASCII utilizados en inglés, ruso y turco; y “\ xNN\ xNN\ xNN” para caracteres usados en chino, japonés y coreano. Por ejemplo, si quieres representar a! en una expresión regular de Web App Firewall como un carácter UTF-8, escribiría\ x21. Si desea incluir un á, debe escribir\ xC3\ xA1.

> **Nota:**
>
> Normalmente, no es necesario representar caracteres ASCII en formato UTF-8, pero cuando esos caracteres pueden confundir un explorador web o un sistema operativo subyacente, puede usar la representación UTF-8 del personaje para evitar esta confusión. Por ejemplo, si una URL contiene un espacio, es posible que desee codificar el espacio como x20 para evitar confundir ciertos exploradores web y software de servidor web.

A continuación, se muestran ejemplos de direcciones URL, nombres de campos de formulario y expresiones de objetos seguros que contienen caracteres no ASCII que deben escribirse como expresiones regulares en formato PCRE para que se incluyan en la configuración de Web App Firewall. En cada

ejemplo se muestra primero la URL, el nombre de campo o la cadena de expresión reales, seguidos de una expresión regular en formato PCR.

- Una URL que contiene caracteres ASCII extendidos.

  URL real: `http://www.josénuñez.com`

  URL codificada: `^http://www\[.\]jos\xC3\xA9nu\xC3\xB1ez\[.\]com$`

- Otra URL que contiene caracteres ASCII extendidos.

  URL real: `http://www.example.de/trömso.html`

  URL codificada: `^http://www[.]example\[.]de/tr\xC3\xB6mso[.]html$`

- Nombre de campo de formulario que contiene caracteres ASCII extendidos.

  `Actual Name: nome_do_usuário`

  Nombre codificado: `^nome_do_usu\xC3\xA1rio$`

- Expresión de objeto seguro que contiene caracteres ASCII extendidos.

  Expresión no codificada [A-Z] {3,6} ¥[1-9][0-9]{6,6}

  Expresión codificada: [A-Z] {3,6}\ xC2\ xA5[1-9][0-9]{6,6}

Puede encontrar una serie de tablas que incluyen todo el conjunto de caracteres Unicode y codificaciones UTF-8 coincidentes en Internet. En la siguiente URL se encuentra un sitio web útil que contiene esta información:

`http://www.utf8-chartable.de/unicode-utf8-table.pl`

Para que los caracteres de la tabla de este sitio web se muestren correctamente, debe tener una fuente Unicode apropiada instalada en el equipo. Si no lo hace, la visualización del personaje puede ser errónea. Sin embargo, incluso si no tiene instalada una fuente adecuada para mostrar un carácter, la descripción y los códigos UTF-8 y UTF-16 de este conjunto de páginas web serán correctos.

Expresiones PCRE invertidas

Además de hacer coincidir el contenido que contiene un patrón, puede hacer coincidir el contenido que no contiene un patrón mediante una expresión PCRE invertida. Para invertir una expresión, simplemente debes incluir un signo de exclamación (!) seguido de un espacio en blanco como primer carácter de la expresión.

> **Nota:** Si una expresión consiste solo en un signo de exclamación sin nada a continuación, el signo de exclamación se trata como un carácter literal, no como una sintaxis que indica una expresión invertida.

Los siguientes comandos de Web App Firewall admiten expresiones PCRE invertidas:

- URL de inicio (URL)
- Denegar URL (URL)
- Coherencia de campos de formulario (URL de acción de formulario)
- Coherencia de cookies (URL de acción de formulario)
- Falsificación de solicitudes entre sitios (CSRF) (URL de acción de formulario)
- Scripting entre sitios HTML (URL de acción de formulario)
- Formato de campo (URL de acción de formulario)
- Tipo de campo (tipo)
- Campo confidencial (URL)

Nota: Si la comprobación de seguridad contiene una marca o casilla de verificación IsRegex, debe establecerse en YES o marcarse para habilitar expresiones regulares en el campo. De lo contrario, el contenido de ese campo se trata como literal y no se analizan expresiones regulares (invertidas o no).

Nombres no permitidos para los perfiles de Web App Firewall

Los siguientes nombres se asignan a las acciones y los perfiles integrados en el dispositivo Citrix ADC y no se pueden usar como nombres para un perfil de Web App Firewall creado por el usuario.

- AGRESSIVE
- ALLOW
- BASIC
- CLIENTAUTH
- COMPRESS
- CSSMINIFY
- DEFLATE
- DENY
- DNS-NOP
- DROP
- GZIP
- HTMLMINIFY
- IMGOPTIMIZE
- JSMINIFY
- MODERATE
- NOCLIENTAUTH
- NOCOMPRESS
- NONE
- NOOP
- NOREWRITE
- RESET
- SETASLEARNNSLOG_ACT

- SETNSLOGPARAMS_ACT
- SETSYSLOGPARAMS_ACT
- SETTMSESSPARAMS_ACT
- SETVPNPARAMS_ACT
- SET_PREAUTHPARAMS_ACT
- default_DNS64_action
- dns_default_act_Cachebypass
- dns_default_act_Drop
- nshttp_default_profile
- nshttp_default_strict_validation
- nstcp_default_mobile_profile
- nstcp_default_XA_XD_profile
- nstcp_default_profile
- nstcp_default_tcp_interactive_stream
- nstcp_default_tcp_lan
- nstcp_default_tcp_lan_thin_stream
- nstcp_default_tcp_lfp
- nstcp_default_tcp_lfp_thin_stream
- nstcp_default_tcp_lnp
- nstcp_default_tcp_lnp_thin_stream
- nstcp_internal_apps

Estado y mensaje de error personalizados para objetos de error HTML, XML y JSON

August 20, 2021

Cuando Citrix Web App Firewall detecta una infracción, el dispositivo gestiona el caso de error mediante una URL de redirección o un objeto de error (importado en el perfil y habilitado). Si el caso se gestiona mediante una configuración de objeto de error, el perfil WAF proporciona un código y un mensaje de estado de respuesta personalizados. Puede personalizar los detalles de error de respuesta de un objeto de error HTML, XML o JSON en el perfil WAF.

> **Nota:**
>
> De forma predeterminada, el código de error y el mensaje de error se establecen como “200” y “Aceptar” si se configura la configuración del objeto de error.

Al gestionar casos de error, es importante que el dispositivo responda con el código de estado de la respuesta HTTP y el mensaje adecuados para resolver problemas. Al proporcionar un mensaje de

estado de error personalizado y un código de estado de error personalizado, el dispositivo puede proporcionar una mejor intervención del usuario para resolver un problema cuando se produce una infracción. Por ejemplo, si establece el código de error de respuesta en “404” y el mensaje de estado en “No encontrado”, el usuario puede inspeccionar el código de estado de la respuesta y el mensaje para comprobar si se ha producido una infracción. Esto puede ayudar al usuario a filtrar las respuestas que contienen el objeto de error.

Configurar el código de estado y el mensaje personalizados para un objeto de error HTML en un perfil WAF mediante la CLI

En el símbolo del sistema, escriba:

```
1 set appfw profile <profile-name> -HTMLErrorStatusCode <value> -
     HTMLErrorStatusMessage <value> -useHTMLErrorObject ON
2 <!--NeedCopy-->
```

Ejemplo:

```
set appfw profile profile_1 -HTMLErrorStatusCode 404 -HTMLErrorStatusMessage
  “Not Found”  -useHTMLErrorObject ON
```

Configurar el código de estado y el mensaje personalizados para un objeto de error XML en un perfil WAF mediante la CLI

En el símbolo del sistema, escriba:

```
1 set appfw profile <profile-name> -XMLErrorStatusCode <value> -
     XMLErrorStatusMessage <value>
2 <!--NeedCopy-->
```

Ejemplo:

```
set appfw profile profile_1 -XMLErrorStatusCode 406 - XMLErrorStatusMessage
  “Not Acceptable”
```

Configurar el código de estado y el mensaje personalizados para el objeto de error JSON en un perfil WAF mediante la CLI

En el símbolo del sistema, escriba:


```
set appfw profile <profile-name> -JSONErrorStatusCode <value> -
    JSONErrorStatusMessage <value>
<!--NeedCopy-->
```

Ejemplo:

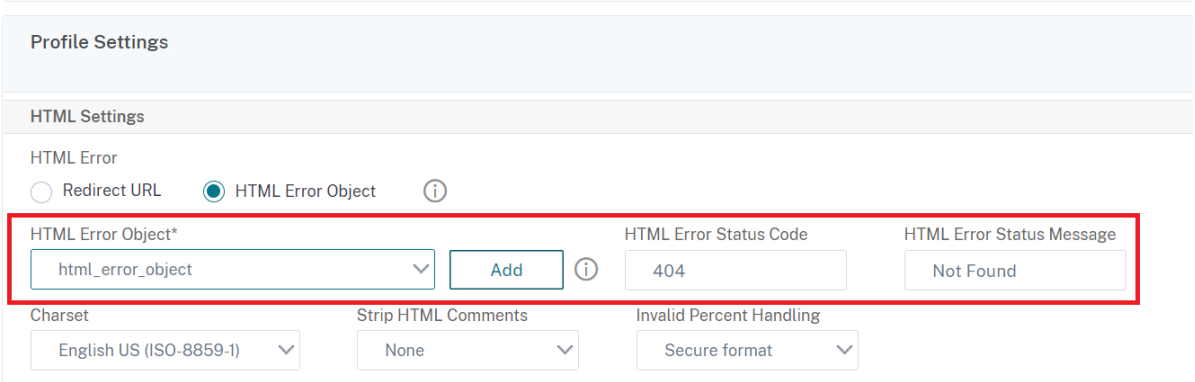
```
set appfw profile profile_1 -JSONErrorStatusCode 500 - JSONErrorStatusMessage
  “Internal Server Error”
```

Configurar el código de estado y el mensaje personalizados para un objeto de error HTML, JSON o XML en un perfil WAF mediante la GUI

1. Vaya a **Seguridad > Citrix Web App Firewall > Perfiles**.
2. En el panel de detalles, haga clic en **Modificar**.
3. En la página **Crear perfil de Web App Firewall**, haga clic en **Configuración del perfil** en la sección **Configuración avanzada** .
4. En la sección **Configuración del perfil**, defina los siguientes parámetros.

   a. Objeto de error HTML. Seleccione la opción para gestionar casos de error mediante un objeto de error HTML. Importe el objeto de error desde una URL, un archivo o un texto.
   b. Código de estado de error HTML. Proporcione un código de estado de error personalizado.
   c. Mensaje de estado de error HTML. Proporciona un mensaje de error del cliente.
5. Haga clic en **Aceptar** y **Listo**.

> **Nota:**
>
> El mismo procedimiento se aplica a la configuración de objetos de error personalizados JSON y XML.



Etiquetas de directivas

October 5, 2021

Una etiqueta de directiva consta de un conjunto de directivas, otras etiquetas de directivas y bancos de directivas específicos de servidores virtuales. Web App Firewall evalúa cada directiva vinculada a la etiqueta de directiva por orden de prioridad. Si la directiva coincide, filtra la conexión según lo especificado en el perfil asociado. A continuación, hace lo que especifique el parámetro Goto, que puede ser terminar la evaluación de directivas, ir a la siguiente directiva o ir a la directiva con la prioridad especificada. Si se establece el parámetro Invoke, finaliza el procesamiento de la etiqueta de directiva actual y comienza a procesar la etiqueta de directiva o el servidor virtual especificados.

Para crear una etiqueta de directiva de Web App Firewall mediante la línea de comandos

En el símbolo del sistema, escriba los siguientes comandos:

- `add appfw policylabel <labelName> http_req`
- `save ns config`

Ejemplo

En el ejemplo siguiente se crea una etiqueta de directiva denominada policylbl1.

```
1 add appfw policylabel policylbl1 http_req
2 save ns config
3 <!--NeedCopy-->
```

Para enlazar una directiva a una etiqueta de directiva mediante la línea de comandos

En el símbolo del sistema, escriba los siguientes comandos:

- `bind appfw policylabel <labelName> <policyName> <priority> [<gotoPriorityExpressi >] [-invoke (<labelType> <labelName>)]`
- `save ns config`

Ejemplo

En el ejemplo siguiente se vincula la directiva1 a la etiqueta de directiva policylbl1 con una prioridad de 1.


```
bind appfw policylabel policylbl1 policy1 1
save ns config
<!--NeedCopy-->
```

Para configurar una etiqueta de directiva de Web App Firewall mediante la interfaz gráfica de usuario

1. Vaya a **Seguridad > Citrix Web App Firewall > Etiquetas de directivas**.
2. En el panel de detalles, realice una de las acciones siguientes:
   - Para agregar una nueva etiqueta de directiva, haga clic en **Agregar**.
   - Para configurar un rótulo de directiva existente, seleccione el rótulo de directiva y, a continuación, haga clic en **Abrir**.

   Se abre el cuadro de diálogo **Crear etiqueta de directiva** de **Web App Firewall o Configurar etiqueta de directiva** de Web App Firewall. Los cuadros de diálogo son casi idénticos.
3. Si va a crear una nueva etiqueta de directiva, en el cuadro de diálogo Crear etiqueta de directiva de Web App Firewall, escriba un nombre para la nueva etiqueta de directiva.

   El nombre puede comenzar con una letra, un número o un símbolo de subrayado, y puede constar de una a 127 letras, números y los símbolos de guión (-), punto (.), almohadilla (#), espacio ( ), en (@), igual (=), dos puntos (:) y guión bajo (_).
4. Seleccione **Insertar directiva** para insertar una nueva fila y mostrar una lista desplegable con todas las directivas de Web App Firewall existentes.
5. Seleccione la directiva que quiere enlazar a la etiqueta de directiva o seleccione Nueva directiva para crear una nueva directiva y siga las instrucciones de Para crear y configurar una directiva mediante la GUI. La directiva que ha seleccionado o creado se inserta en la lista de directivas de Web App Firewall enlazadas globalmente.
6. Realice los ajustes adicionales.
   - Para modificar la prioridad de la directiva, haga clic en el campo para habilitarla y, a continuación, escriba una nueva prioridad. También puede seleccionar Regenerar prioridades para volver a numerar las prioridades de manera uniforme.
   - Para modificar la expresión de la directiva, haga doble clic en ese campo para abrir el cuadro de diálogo Configurar directiva de Web App Firewall, en el que puede modificar la expresión de directiva.
   - Para establecer la expresión Goto, haga doble clic en el campo del encabezado de columna Goto Expression para mostrar la lista desplegable, donde puede elegir una expresión.

- Para establecer la opción Invocar, haga doble clic en el campo del encabezado de columna Invocar para mostrar la lista desplegable, donde puede elegir una expresión

7. Repita los pasos 5 a 7 para vincular las directivas adicionales de Web App Firewall que quiera a la etiqueta de directiva.
8. Haga clic en **Crear** o **Aceptar**y, a continuación, en **Cerrar**. En la barra de estado aparece un mensaje que indica que ha creado o modificado correctamente la etiqueta de directiva.

Directivas

January 12, 2021

El Web App Firewall utiliza dos tipos de directivas: Directivas de firewall y directivas de auditoría. Las directivas de firewall controlan el tráfico que se envía al Web App Firewall. Las directivas de auditoría controlan el servidor de registro al que se envían los registros de Web App Firewall.

Las directivas de firewall pueden ser complejas porque la regla de directiva puede consistir en varias expresiones en el lenguaje de expresiones Citrix ADC, que es un lenguaje de programación completo orientado a objetos capaz de definir con extrema precisión exactamente qué conexiones filtrar. Dado que las directivas de firewall operan en el contexto del Web App Firewall, deben cumplir ciertos criterios que están conectados al funcionamiento del Web App Firewall y al tráfico que filtra adecuadamente. Sin embargo, siempre que tenga en cuenta estos criterios, las directivas de firewall son similares a las directivas de otras funciones de Citrix ADC. Las instrucciones aquí no tratan de cubrir todos los aspectos de la escritura de directivas de firewall, sino que solo proporcionan una introducción a las directivas y cubren los criterios que son exclusivos de Web App Firewall.

Las directivas de auditoría son sencillas porque la regla de directiva siempre es ns_true. Solo necesita especificar el servidor de registro al que quiere enviar registros, los niveles de registro que quiere utilizar y algunos otros criterios que se explican en detalle.

Directivas de Web App Firewall

October 5, 2021

Una directiva de firewall es una regla asociada a un perfil. La regla es una expresión o grupo de expresiones que definen los tipos de pares de solicitud y respuesta que el Web App Firewall filtrará aplicando el perfil. Las expresiones de directivas de firewall se escriben en el lenguaje de expresiones de Citrix ADC, un lenguaje de programación orientado a objetos con funciones especiales para admitir funciones específicas de Citrix ADC. El perfil es el conjunto de acciones que utilizará Web App Firewall para filtrar los pares de solicitudes y respuestas que coinciden con la regla.

Las directivas del firewall permiten asignar diferentes reglas de filtrado a distintos tipos de contenido web. No todos los contenidos web son iguales. Un sitio web sencillo que no utiliza scripts complejas y que no accede ni gestiona datos privados puede requerir únicamente el nivel de protección que proporciona un perfil creado con valores predeterminados básicos. El contenido web que contiene formularios web mejorados con JavaScript o accede a una base de datos SQL probablemente requiera una protección más personalizada. Puede crear un perfil diferente para filtrar ese contenido y crear una directiva de firewall independiente que determine qué solicitudes intentan acceder a ese contenido. A continuación, asocia la expresión de directiva con un perfil creado y vincula globalmente la directiva para ponerla en vigor.

Web App Firewall procesa únicamente las conexiones HTTP y, por lo tanto, utiliza un subconjunto del lenguaje general de expresiones de Citrix ADC. La información aquí contenida se limita a temas y ejemplos que pueden resultar útiles al configurar Web App Firewall. A continuación se presentan vínculos a información adicional y procedimientos para las directivas de firewall:

- Para obtener información sobre los procedimientos que explican cómo crear y configurar una directiva, consulte Creación y configuración de directivas de Web App Firewall.
- Para obtener un procedimiento que explica en detalle cómo crear una regla de directiva (expresión), consulte Para crear o configurar una regla de Web App Firewall (expresión).
- Para obtener un procedimiento que explica cómo utilizar el cuadro de diálogo Agregar expresión para crear una regla de directiva, consulte Para agregar una regla de firewall (expresión) mediante el cuadro de diálogo Agregar expresión.
- Para obtener un procedimiento que explica cómo ver los enlaces actuales de una directiva, consulte Visualización de los enlaces de una directiva de firewall.
- Para obtener información sobre los procedimientos que explican cómo vincular una directiva de Web App Firewall, consulte Vinculación de directivas de Web App Firewall.
- Para obtener información detallada sobre el lenguaje de expresiones Citrix ADC, consulte Directivas y expresiones.

> **Nota**
>
> Web App Firewall evalúa las directivas en función de las expresiones de prioridad y goto configuradas. Al final de la evaluación de la directiva, se utiliza la última directiva que se evalúa como verdadera y se invoca la configuración de seguridad del perfil correspondiente para procesar la solicitud.
>
> Por ejemplo, considere un caso en el que hay dos directivas.
>
> - Policy_1 es una directiva genérica con expression=NS_TRUE y tiene un profile_1 correspondiente, que es un perfil básico. La prioridad se establece en 100.
> - Policy_2 es más específico con expression=http.req.url.contains (“XYZ”) y tiene un profile_2 correspondiente, que es un perfil avanzado. La expresión GoTo se establece en NEXT y la prioridad se establece en 95, lo que es una prioridad más alta en comparación con Policy_1.

> En este caso, si se detecta la cadena de destino “XYZ” en la URL de la solicitud procesada, se activa la coincidencia Policy_2 porque tiene una prioridad más alta, aunque Policy_1 también coincida. Sin embargo, según la configuración de expresión GoTo de Policy_2, la evaluación de directivas continúa y también se procesa la siguiente policy_1. Al final de la evaluación de directivas, Policy_1 se evalúa como true y se invocan las comprobaciones de seguridad básicas configuradas en Profile_1.
>
> Si se modifica Policy_2 y la expresión GoTo se cambia de **NEXT** a **END**, la solicitud procesada que tiene la cadena de destino “XYZ” desencadena la coincidencia Policy_2 debido a la consideración de prioridad y, según la configuración de expresión GoTo, la evaluación de directivas finaliza en este punto. Policy_2 se evalúa como true y se invocan las comprobaciones de seguridad avanzadas configuradas en Profile_2.
>
> **PRÓXIMO**
> **FIN**
>
> La evaluación de directivas se completa en una sola pasada. Una vez que se completa la evaluación de la directiva de la solicitud y se invocan las acciones de perfil correspondientes, la solicitud no pasa por otra ronda de evaluación de directivas.

Creación y configuración de políticas de Web App Firewall

September 8, 2021

Una política de cortafuegos consta de dos elementos: una *regla* y un *perfil* asociado. La regla selecciona el tráfico HTTP que coincide con los criterios establecidos y lo envía a Web App Firewall para filtrarlo. El perfil contiene los criterios de filtrado que utiliza Web App Firewall.

La regla de política consta de una o más expresiones en el lenguaje de expresiones Citrix ADC. La sintaxis de expresiones Citrix ADC es un potente lenguaje de programación orientado a objetos que le permite designar con precisión el tráfico que desea procesar con un perfil específico. Para los usuarios que no están familiarizados con la sintaxis del lenguaje de expresiones Citrix ADC o que prefieren configurar su dispositivo Citrix ADC mediante una interfaz basada en web, la GUI proporciona dos herramientas: el menú **Prefijo** y el cuadro de diálogo **Agregar expresión** . Ambos le ayudan a escribir expresiones que seleccionan exactamente el tráfico que desea procesar. Los usuarios experimentados que están completamente familiarizados con la sintaxis pueden preferir utilizar la línea de comandos de Citrix ADC para configurar sus dispositivos Citrix ADC.

> **Nota:**
>
> Además de la sintaxis de expresiones predeterminada, para obtener compatibilidad con versiones anteriores, el sistema operativo Citrix ADC admite la sintaxis de expresiones clásicas de

> Citrix ADC en dispositivos y dispositivos virtuales Citrix ADC Classic y nCore. Las expresiones clásicas no se admiten en los dispositivos y dispositivos virtuales Citrix ADC Cluster. Los usuarios actuales de Citrix ADC que quieran migrar configuraciones existentes al clúster Citrix ADC deben migrar las directivas que contengan expresiones clásicas a la sintaxis de expresiones predeterminadas.

Para obtener información detallada sobre los lenguajes de expresiones Citrix ADC, consulte Directivas y expresiones.

Puede crear una directiva de firewall mediante la GUI o la línea de comandos de Citrix ADC.

Para crear y configurar una directiva mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos:

- `add appfw policy <name><rule> <profileName>`
- `save ns config`

Ejemplo

En el siguiente ejemplo se agrega una política denominada pl-blog, con una regla que intercepta todo el tráfico hacia o desde el blog.example.com del host, y asocia esa política al perfil pr-blog. Esta es una política adecuada para proteger un blog alojado en un nombre de host específico.

```
1 add appfw policy pl-blog "HTTP.REQ.HOSTNAME.DOMAIN.EQ("blog.example.com
     ")" pr-blog
2 <!--NeedCopy-->
```

Para crear y configurar una política mediante la GUI

1. Vaya a **Seguridad** > **Web App Firewall** > **Directivas**.
2. En el panel de detalles, realice una de las acciones siguientes:
   - Para crear una política de cortafuegos, haga clic en **Agregar**. Aparece la **directiva Create Web App Firewall** .
   - Para editar una política de firewall existente, selecciónela y, a continuación, haga clic en **Editar**.

   Se muestra la **directiva Crear Web App Firewall** o la **directiva Configurar Web App Firewall**.
3. Si va a crear una política de cortafuegos, en el cuadro de diálogo **Crear política de Web App Firewall**, cuadro de texto Nombre de directiva, escriba un nombre para la nueva política.

El nombre puede comenzar con una letra, un número o un símbolo de guión bajo, y puede constar de una a 128 letras, números y el guión (-), punto (.) libra (#), espacio (), at (@), igual a (=), dos puntos (:) y guión bajo (_).

Si va a configurar una política de cortafuegos existente, este campo es de solo lectura. No puedes modificarlo.

4. Seleccione el perfil que desea asociar a esta política en la lista desplegable Perfil. Puede crear un perfil para asociarlo a su política haciendo clic en Nuevo y puede modificar un perfil existente haciendo clic en Modificar.
5. En el área de texto Expresión, cree una regla para la política.
   - Puede escribir una regla directamente en el área de texto.
   - Puede hacer clic en Prefijo para seleccionar el primer término de la regla y seguir las instrucciones.
   - Puede hacer clic en Agregar para abrir el cuadro de diálogo Agregar expresión y utilizarlo para construir la regla.
6. Haga clic en **Crear** o **Aceptar**y, a continuación, en **Cerrar**.

Para crear o configurar una regla de Web App Firewall (expresión)

La regla de directiva, también denominada *expresión*, define el tráfico web que filtra Web App Firewall mediante el perfil asociado a la política. Al igual que otras reglas de política (o *expresiones*) de Citrix ADC, las reglas de Web App Firewall utilizan la sintaxis de expresiones de Citrix ADC. Esta sintaxis es potente, flexible y extensible. Es demasiado complejo describirlo por completo en este conjunto de instrucciones. Puede utilizar el siguiente procedimiento para crear una regla de política de cortafuegos simple o leerla como descripción general del proceso de creación de políticas.

1. Si aún no lo ha hecho, vaya a la ubicación adecuada en el asistente de **Web App Firewall** o en la GUI de Citrix ADC para crear la regla de política:
   - Si está configurando una directiva en el asistente **Web App Firewall**, en el panel de navegación, haga clic en **Web App Firewall** y, a continuación, en el panel de detalles haga clic en **Asistente para Web App Firewall** y, a continuación, vaya a la pantalla **Especificar regla**.
   - Si va a configurar una directiva manualmente, en el panel de navegación, expanda **Web App Firewall**, **Políticas**y, a continuación, **Firewall**. En el panel de detalles, para crear una política, haga clic en **Agregar**. Para modificar una política existente, selecciónela y, a continuación, haga clic en **Abrir**.
2. En la pantalla **Especificar regla**, en el cuadro de diálogo **Crear perfil de Web App Firewall** o en el cuadro de diálogo **Configurar perfil de firewall de aplicaciones web**, haga clic en **Prefijo**y,

a continuación, elija el prefijo de su expresión en la lista desplegable. Las opciones disponibles son:

- **HTTP.** Elija un protocolo HTTP si desea examinar algún aspecto de la solicitud que pertenece al protocolo.
- **SYS.** Elija sitios web protegidos si desea examinar algún aspecto de la solicitud que pertenece al destinatario de la solicitud.
- **CLIENTE.** Elija un cliente que envió la solicitud. Elija esta opción si desea examinar algún aspecto del remitente de la solicitud.
- **SERVIDOR.** Elija un cliente al que se envió la solicitud y si desea examinar algún aspecto del destinatario de la solicitud.

Después de elegir un prefijo, Web App Firewall muestra una ventana de solicitud de dos partes que muestra las siguientes opciones posibles en la parte superior y una breve explicación de lo que significa la elección seleccionada en la parte inferior.

3. Elige tu próximo trimestre.

   Si ha elegido el protocolo HTTP como prefijo, la única opción es REQ, que especifica el par Solicitud/Respuesta. (Web App Firewall funciona según la solicitud y la respuesta como unidad en lugar de en cada uno por separado). Si eliges otro prefijo, tus elecciones son más variadas. Para obtener ayuda sobre una elección específica, haga clic en esa opción una vez para mostrar información sobre ella en la ventana de solicitud inferior.

   Cuando haya decidido qué término desea, haga doble clic en él para insertarlo en la ventana **Expresión** .

4. Escriba un periodo después del plazo que acaba de elegir. A continuación, se le pedirá que elija su próximo término, tal como se describe en el paso anterior. Cuando un término requiera escribir un valor, rellene el valor adecuado. Por ejemplo, si elige HTTP.REQ.HEADER («»), escriba el nombre del encabezado entre las comillas.

5. Siga eligiendo los términos de las solicitudes y rellenando los valores necesarios hasta que finalice la expresión.

   A continuación se presentan algunos ejemplos de expresiones para fines específicos.

   - **Host web específico.** Para hacer coincidir el tráfico de un host web concreto:

     ```
     1 HTTP.REQ.HEADER("Host").EQ("shopping.example.com")
     2 <!--NeedCopy-->
     ```

     Para `shopping.example.com`, sustituye el nombre del host web que quieres que coincida.

- **Carpeta o directorio web específicos.** Para hacer coincidir el tráfico de una carpeta o directorio concretos de un host web:

```
HTTP.REQ.URL.STARTSWITH("https//www.example.com/folder")
<!--NeedCopy-->
```

En www.example.com, sustituya el nombre del host web. En el caso de la carpeta, sustituya la carpeta o la ruta del contenido que desea que coincida. Por ejemplo, si el carrito de la compra se encuentra en una carpeta llamada /solutions/orders, sustituye esa cadena por carpeta.

- **Tipo específico de contenido: imágenes GIF.** Para hacer coincidir imágenes en formato GIF:

```
HTTP.REQ.URL.ENDSWITH(".png")
<!--NeedCopy-->
```

Para que coincidan con otras imágenes de formato, sustituya otra cadena en lugar de .png.

- **Tipo específico de contenido: scripts.** Para hacer coincidir todos los scripts CGI ubicados en el directorio CGI-BIN:

```
HTTP.REQ.URL.STARTSWITH("https//www.example.com/CGI-BIN")
<!--NeedCopy-->
```

Para hacer coincidir todos los JavaScript con las extensiones.js:

```
HTTP.REQ.URL.ENDSWITH(".js")
<!--NeedCopy-->
```

Para obtener más información sobre la creación de expresiones de directiva, consulte Directivas y expresiones.

> **Nota:**
>
> Si utiliza la línea de comandos para configurar una directiva, recuerde escapar cualquier comillas dobles dentro de las expresiones de Citrix ADC. Por ejemplo, la siguiente expresión es correcta si se introduce en la GUI:


```
HTTP.REQ.HEADER("Host").EQ("shopping.example.com")
<!--NeedCopy-->
```

Sin embargo, si se introduce en la línea de comandos, debe escribir el siguiente comando en su lugar:

```
HTTP.REQ.HEADER("Host").EQ("shopping.example.com")
<!--NeedCopy-->
```

Para agregar una regla de cortafuegos (expresión) mediante el cuadro de diálogo Agregar expresión

El cuadro de diálogo **Agregar expresión** (también denominado Editor de expresiones) ayuda a los usuarios que no están familiarizados con el lenguaje de expresiones Citrix ADC a crear una política que coincida con el tráfico que desean filtrar.

1. Si aún no lo ha hecho, vaya a la ubicación adecuada en el asistente de **Web App Firewall** o en la GUI de Citrix ADC:
   - Si está configurando una directiva en el asistente **Web App Firewall**, en el panel de navegación, haga clic en **Web App Firewall** y, a continuación, en el panel de detalles haga clic en **Asistente para Web App Firewall** y, a continuación, vaya a la pantalla **Especificar regla**.
   - Si va a configurar una directiva manualmente, en el panel de navegación, expanda **Web App Firewall**, **Políticas**y, a continuación, **Firewall**. En el panel de detalles, para crear una política, haga clic en **Agregar**. Para modificar una política existente, selecciónela y, a continuación, haga clic en **Abrir**.
2. En la pantalla **Especificar regla**, en el cuadro de diálogo **Crear perfil de Web App Firewall** o en el cuadro de diálogo **Configurar perfil de Web App Firewall**, haga clic en **Agregar**.
3. En el cuadro de **diálogo Agregar expresión**, en el área Construir expresión, en el primer cuadro de lista, elija uno de los prefijos siguientes:
   - **HTTP.** Elija el protocolo HTTP si desea examinar algún aspecto de la solicitud que pertenece al protocolo HTTP. La elección predeterminada.
   - **SYS.** Elija sitios web protegidos si desea examinar algún aspecto de la solicitud que pertenece al destinatario de la solicitud.
   - **CLIENTE.** Elija el equipo que envió la solicitud si desea examinar algún aspecto del remitente de la solicitud.
   - **SERVIDOR.** Elija el equipo al que se envió la solicitud y examine algún aspecto del destinatario de la solicitud.

4. En el segundo cuadro de lista, elige tu próximo término. Los términos disponibles varían según la elección que haya realizado en el paso anterior, porque el cuadro de diálogo ajusta automáticamente la lista para que contenga únicamente los términos válidos para el contexto. Por ejemplo, si ha seleccionado HTTP en el cuadro de lista anterior, la única opción es REQ, para las solicitudes. Dado que Web App Firewall trata las solicitudes y las respuestas asociadas como una sola unidad y filtra ambas, no necesita respuestas específicas por separado. Después de elegir el segundo término, aparece un tercer cuadro de lista a la derecha del segundo. La ventana Ayuda muestra una descripción del segundo término y la ventana **Vista previa de expresión** muestra la expresión.
5. En el tercer cuadro de lista, elige el siguiente término. Aparece un nuevo cuadro de lista a la derecha y la ventana Ayuda cambia para mostrar una descripción del nuevo término. La ventana **Vista previa de expresión** se actualiza para mostrar la expresión tal y como la ha especificado hasta ese punto.
6. Siga eligiendo términos y, cuando se le solicite rellenar argumentos, hasta que se complete la expresión. Si comete un error o desea cambiar la expresión después de haber seleccionado un término, simplemente puede elegir otro término. La expresión se modifica y se borran los argumentos o más términos que haya agregado después del término modificado.
7. Cuando haya terminado de construir la expresión, haga clic en **Aceptar** para cerrar el cuadro de diálogo **Agregar expresión** . La expresión se inserta en el área de texto **Expresión**.

Vinculación de directivas de Web App Firewall

August 20, 2021

Después de configurar las directivas de Web App Firewall, las vincula a Global o a un punto de enlace para ponerlas en vigor. Después del enlace, cualquier solicitud o respuesta que coincida con una directiva de Web App Firewall se transforma mediante el perfil asociado a dicha directiva.

Cuando vincula una directiva, le asigna una prioridad. La prioridad determina el orden en que se evalúan las directivas definidas. Puede establecer la prioridad en cualquier entero positivo. En el sistema operativo Citrix ADC, las prioridades de directivas funcionan en orden inverso: Cuanto mayor sea el número, menor será la prioridad.

Debido a que la función Web App Firewall implementa solo la primera directiva que coincide con una solicitud, no las directivas adicionales que también podrían coincidir, la prioridad de directiva es importante para lograr los resultados deseados. Si asigna a su primera directiva una prioridad baja (como 1000), configure el Web App Firewall para que lo realice solo si otras directivas con una prioridad mayor no coinciden con una solicitud. Si asigna a su primera directiva una prioridad alta (por ejemplo, 1), configure Web App Firewall para que la ejecute primero y omita cualquier otra directiva que también pueda coincidir. Puede dejar mucho espacio para agregar otras directivas en cualquier

orden, sin tener que reasignar prioridades, estableciendo prioridades con intervalos de 50 o 100 entre cada directiva cuando vincule las directivas.

Para obtener más información sobre las directivas de enlace en el dispositivo Citrix ADC, consulte "Directivas y expresiones. "

Para enlazar una directiva de Web App Firewall mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos:

- `bind appfw global <policyName>`
- `bind appfw profile <profile_name> -crossSiteScripting data`

Ejemplo

En el ejemplo siguiente se vincula la directiva denominada pl-blog y se le asigna una prioridad de 10.

```
1 bind appfw global pl-blog 10
2 save ns config
3 <!--NeedCopy-->
```

Configurar expresiones de registro

La compatibilidad con expresiones de registro para enlazar Web App Firewall se agrega a la información de encabezado HTTP de registro cuando se produce una infracción.

La expresión de registro se vincula en el perfil de aplicación y el enlace contiene la expresión que debe evaluarse y enviarse a los marcos de registro cuando se produce una infracción.

Se registra el registro de infracciones de Web App Firewall con información de encabezado http. Puede especificar una expresión de registro personalizada y ayuda en el análisis y el diagnóstico cuando se generan violaciones para el flujo actual (solicitud/respuesta).

Ejemplo de configuración

```
1 bind appfw profile <profile> -logexpression <string> <expression>
2 add policy expression headers "" HEADERS(100):"+HTTP.REQ.FULL_HEADER"
3 add policy expression body_100 ""BODY:"+HTTP.REQ.BODY(100)"
4 bind appfw profile test -logExpression log_body body_100
5 bind appfw profile test -logExpression log_headers  headers
```



```
bind appfw profile test -logExpression ""URL:"+HTTP.REQ.URL+" IP:"+
    CLIENT.IP.SRC"
<!--NeedCopy-->
```

Registros de ejemplo

```
Dec 8 16:55:33 <local0.info> 10.87.222.145 CEF:0|Citrix|NetScaler|NS12
    .1|APPFW|APPFW_LOGEXPRESSION|6|src=10.217.222.128 spt=26409 method=
    POST request=http://10.217.222.44/test/credit.html msg= HEADERS(100)
    :POST /test/credit.html HTTP/1.1^M User-Agent: curl/7.24.0 (amd64-
    portbld-freebsd8.4) libcurl/7.24.0 OpenSSL/0.9.8y zlib/1.2.3^M Host:
     10.217.222.44^M Accept: /^M Content-Length: 33^M Content-Type:
    application/x-www-form-urlencoded^M ^M  cn1=58 cn2=174 cs1=test cs2=
    PPE1 cs4=ALERT cs5=2017 act=not blocked
<!--NeedCopy-->
```

```
Dec 8 16:55:33 <local0.info> 10.87.222.145 CEF:0|Citrix|NetScaler|NS12
    .1|APPFW|APPFW_LOGEXPRESSION|6|src=10.217.222.128 spt=26409 method=
    POST request=http://10.217.222.44/test/credit.html msg=BODY:ata=
    asdadasdasdasddddddddddddddddd cn1=59 cn2=174 cs1=test cs2=PPE1 cs4=
    ALERT cs5=2017 act=not blocked
<!--NeedCopy-->
```

```
Dec 8 16:55:33 <local0.info> 10.87.222.145 CEF:0|Citrix|NetScaler|NS12
    .1|APPFW|APPFW_LOGEXPRESSION|6|src=10.217.222.128 spt=26409 method=
    POST request=http://10.217.222.44/test/credit.html msg=URL:/test/
    credit.html IP:10.217.222.128 cn1=60 cn2=174 cs1=test cs2=PPE1 cs4=
    ALERT cs5=2017 act=not blocked
<!--NeedCopy-->
```

```
Other violation logs
Dec 8 16:55:33 <local0.info> 10.87.222.145 CEF:0|Citrix|NetScaler|NS12
    .1|APPFW|APPFW_STARTURL|6|src=10.217.222.128 spt=26409 method=POST
    request=http://10.217.222.44/test/credit.html msg=Disallow Illegal
    URL. cn1=61 cn2=174 cs1=test cs2=PPE1 cs4=ALERT cs5=2017 act=not
    blocked
<!--NeedCopy-->
```



```
Dec 8 16:55:33 <local0.info> 10.87.222.145 CEF:0|Citrix|NetScaler|NS12
    .1|APPFW|APPFW_SAFECOMMERCE|6|src=10.217.222.128 spt=26409 method=
    POST request=http://10.217.222.44/test/credit.html msg=Maximum
    number of potential credit card numbers seen cn1=62 cn2=174 cs1=test
     cs2=PPE1 cs4=ALERT cs5=2017 act=not blocked
<!--NeedCopy-->
```

Nota

1. Solo está disponible el soporte de registro de auditoría. Se agregaría compatibilidad con logstream y visibilidad en información de seguridad en versiones futuras.
2. Si se generan auditlogs, solo se pueden generar 1024 bytes de datos por mensaje de registro.
3. Si se utiliza la transmisión de registros, los límites se basan en el tamaño máximo admitido de las limitaciones de tamaño del protocolo de flujo de registro/protocolo ipfix. El tamaño máximo de soporte para la secuencia de registro es mayor que 1024 bytes.

Para enlazar una directiva de Web App Firewall mediante la interfaz gráfica de usuario

1. Lleve a cabo una de las siguientes acciones:
   - Vaya a **Seguridad** > **Web App Firewall** y, en el panel de detalles, haga clic en Administrador de directivas de Web App Firewall.
   - Vaya a **Seguridad** > **Web App Firewall** > **Directivas > Directivas** de **firewall** y, en el panel de detalles, haga clic en **Administrador de directivas**.
2. En el cuadro de diálogo **Administrador de directivas de Web App Firewall**, seleccione el punto de enlace al que quiere enlazar la directiva en la lista desplegable. Las opciones son:
   - **Anular Global.** Las directivas enlazadas a este punto de enlace procesan todo el tráfico de todas las interfaces del dispositivo Citrix ADC y se aplican antes que cualquier otra directiva.
   - **Servidor virtual LB.** Las directivas enlazadas a un servidor virtual de equilibrio de carga se aplican solo al tráfico procesado por ese servidor virtual de equilibrio de carga y se aplican antes de cualquier directiva global predeterminada. Después de seleccionar LB Virtual Server, también debe seleccionar el servidor virtual de equilibrio de carga específico al que quiere enlazar esta directiva.
   - **Servidor virtual CS.** Las directivas enlazadas a un servidor virtual de conmutación de contenido se aplican solo al tráfico procesado por ese servidor virtual de conmutación de contenido y se aplican antes de cualquier directiva global predeterminada. Después de seleccionar CS Virtual Server, también debe seleccionar el servidor virtual de conmutación de contenido específico al que quiere enlazar esta directiva.

- **Global predeterminada.** Las directivas vinculadas a este punto de enlace procesan todo el tráfico de todas las interfaces del dispositivo Citrix ADC.
- **Etiqueta de directiva.** Las directivas enlazadas a una etiqueta de directiva procesan el tráfico que la etiqueta de directiva les enruta. La etiqueta de directiva controla el orden en que se aplican las directivas a este tráfico.
- **Ninguno.** No vincule la directiva a ningún punto de enlace.

3. Haga clic en **Continuar**. Aparecerá una lista de las directivas existentes de Web App Firewall.
4. Seleccione la directiva que quiere vincular haciendo clic en ella.
5. Realice ajustes adicionales en el enlace.
   - Para modificar la prioridad de directiva, haga clic en el campo para habilitarla y, a continuación, escriba una nueva prioridad. También puede seleccionar Regenerar Prioridades para volver a numerar las prioridades de manera uniforme.
   - Para modificar la expresión de directiva, haga doble clic en ese campo para abrir el cuadro de diálogo **Configurar directiva Web App Firewall**, donde puede modificar la expresión de directiva.
   - Para establecer la expresión Goto, haga doble clic en el **campo** del encabezado de columna Goto Expression para mostrar la lista desplegable, donde puede elegir una expresión.
   - Para establecer la opción Invocar, haga doble clic en el campo del encabezado de columna Invocar para mostrar la lista desplegable, donde puede elegir una expresión
6. Repita los pasos 3 a 6 para agregar cualquier directiva adicional de Web App Firewall que quiera enlazar globalmente.
7. Haga clic en **Aceptar**. Aparece un mensaje en la barra de estado que indica que la directiva se ha enlazado correctamente.

Visualización de enlaces de directivas

August 20, 2021

Puede comprobar rápidamente para determinar qué enlaces existen para cualquier directiva de firewall al ver los enlaces en la GUI.

Para ver los enlaces de una directiva de Web App Firewall

1. Vaya a **Seguridad > Citrix Web App Firewall > Directivas > Directivas > Directivas de firewall**
2. En el panel de detalles, seleccione la directiva que quiere comprobar y, a continuación, haga clic en Mostrar enlaces. Aparece el cuadro de mensaje Detalles de enlace para directiva: Directiva, con una lista de enlaces para la directiva seleccionada.
3. Haga clic en **Cerrar**.

Información complementaria sobre las directivas de Web App Firewall

January 12, 2021

A continuación se presenta información complementaria sobre aspectos concretos de las directivas de Web App Firewall que los administradores del sistema que administran el Web App Firewall podrían necesitar conocer.

Comportamiento correcto pero inesperado

La seguridad de las aplicaciones web y los sitios web modernos son complejos. En varios casos, una directiva Citrix ADC puede provocar que el Web App Firewall se comporte de manera diferente en determinadas situaciones de lo que un usuario familiarizado con las directivas esperaría normalmente. A continuación se presentan una serie de casos en los que el Web App Firewall puede comportarse de una manera inesperada.

- **Solicitud con un encabezado HTTP Host que falta y una URL absoluta.** Cuando un usuario envía una solicitud, en la mayoría de los casos la URL de la solicitud es relativa. Es decir, toma como punto de partida la URL del Referer, la URL donde se encuentra el explorador del usuario cuando envía la solicitud. Si una solicitud se envía sin un encabezado Host y con una URL relativa, la solicitud se bloquea normalmente porque infringe la especificación HTTP y porque una solicitud que no especifica el host puede constituir en algunas circunstancias un ataque. Sin embargo, si una solicitud se envía con una URL absoluta, incluso si falta el encabezado Host, la solicitud omite el Web App Firewall y se reenvía al servidor web. Aunque dicha solicitud infringe la especificación HTTP, no representa ninguna amenaza posible porque una URL absoluta contiene el host.

Directivas de auditoría

August 20, 2021

Las directivas de auditoría determinan los mensajes generados y registrados durante una sesión de Web App Firewall. Los mensajes se registran en formato SYSLOG en el servidor NSLOG local o en un servidor de registro externo. Se registran diferentes tipos de mensajes según el nivel de registro seleccionado.

Para crear una directiva de auditoría, primero debe crear un servidor NSLOG o un servidor SYSLOG. Y luego crea la directiva y especifica el tipo de registro y el servidor al que se envían los registros.

Para crear un servidor de auditoría mediante la interfaz de línea de comandos

Puede crear dos tipos diferentes de servidor de auditoría: Un servidor NSLOG o un servidor SYSLOG. Los nombres de los comandos son diferentes, pero los parámetros de los comandos son los mismos.

Para crear un servidor de auditoría, en el símbolo del sistema, escriba los comandos siguientes:

- `add audit syslogAction <name> <serverIP> [-serverPort <port>] -logLevel <logLevel> ... [-dateFormat (MMDDYYYY | DDMMYYYY)] [-logFacility <logFacility>] [-tcp (NONE | ALL)] [-acl (ENABLED | DISABLED)] [-timeZone (GMT_TIME | LOCAL_TIME)] [-userDefinedAuditlog (YES | NO)] [-appflowExport (ENABLED | DISABLED)]`
- `save ns config`

Ejemplo

En el ejemplo siguiente se crea un servidor syslog denominado syslog1 en IP 10.124.67.91, con niveles de registro de emergencia, crítico y de advertencia, servicio de registro establecido en LOCAL1, que registra todas las conexiones TCP:

```
1 add audit syslogAction syslog1 10.124.67.91 -logLevel emergency
     critical warning -logFacility
2 LOCAL1 -tcp ALL
3 save ns config
4 <!--NeedCopy-->
```

Para modificar o quitar un servidor de auditoría mediante la interfaz de línea de comandos

- Para modificar un servidor de auditoría, escriba el comando `<type>` set audit, el nombre del servidor de auditoría y los parámetros que se van a cambiar, con sus nuevos valores.
- Para quitar un servidor de auditoría, escriba el comando `<type>` rm audit y el nombre del servidor de auditoría.

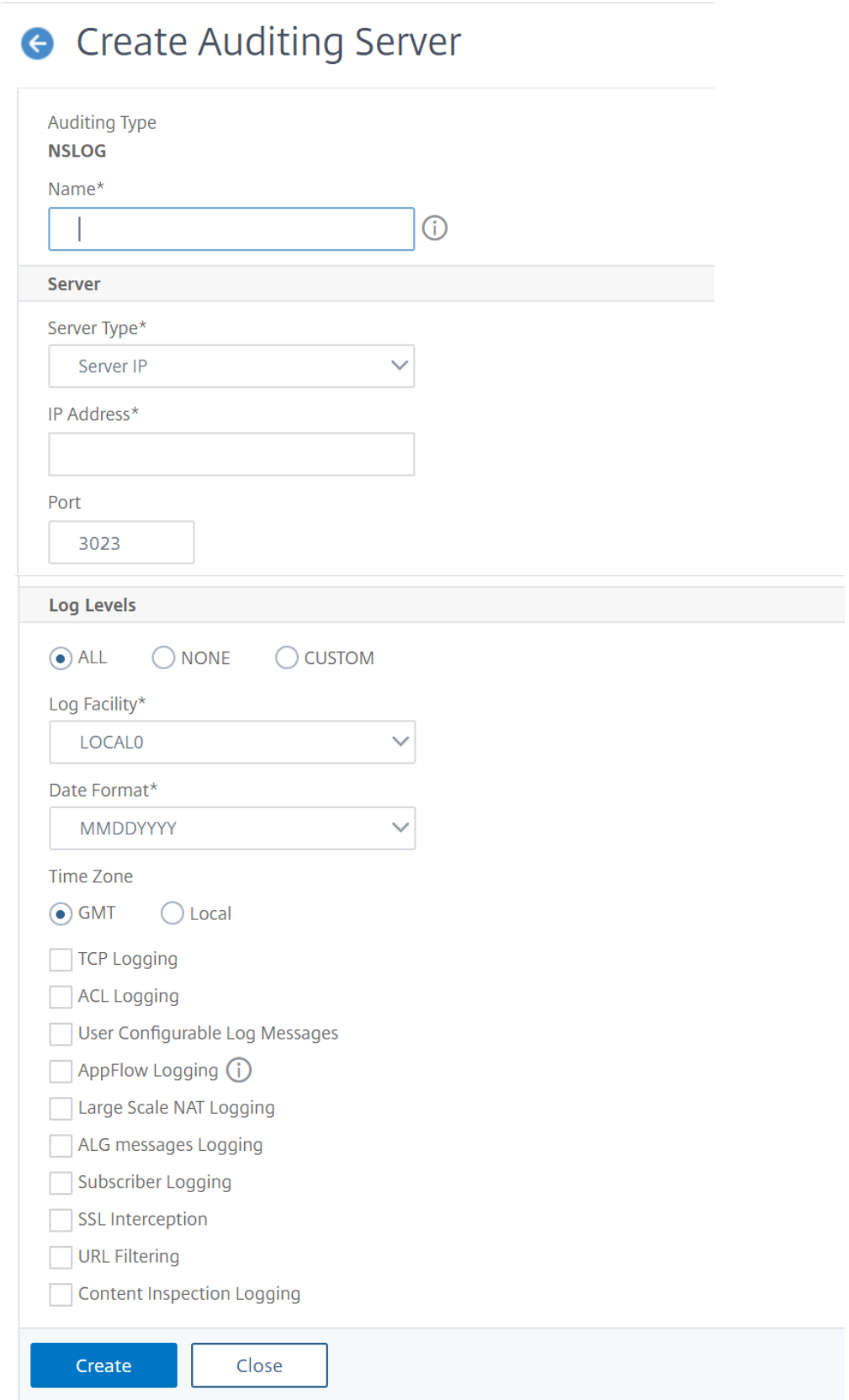
Ejemplo

En el ejemplo siguiente se modifica el servidor syslog denominado syslog1 para agregar errores y alertas al nivel de registro:


```
set audit syslogAction syslog1 10.124.67.91 -logLevel emergency
    critical warning alert error
-logFacility LOCAL1 -tcp ALL
save ns config
<!--NeedCopy-->
```

Para crear o configurar un servidor de auditoría mediante la interfaz gráfica de usuario

1. Vaya a **Seguridad** > **Citrix Web App Firewall** > **Directivas** > **Auditoría** > **Nslog**.
2. En la página Auditoría de Nslog, haga clic en la ficha **Servidores**.
3. Lleve a cabo una de las siguientes acciones:
   - Para agregar un nuevo servidor de auditoría, haga clic en **Agregar**.
   - Para modificar un servidor de auditoría existente, seleccione el servidor y, a continuación, haga clic en **Modificar**.
4. En la página **Crear servidor de auditoría**, establezca los siguientes parámetros:
   - Nombre
   - Tipo de servidor
   - Dirección IP
   - Port
   - Nivel de registro
   - Instalación de registro
   - Formato de fecha
   - Zona horaria
   - Registro TCP
   - Registro de ACL
   - Mensajes de registro configurables por el usuario
   - Captura de registros de AppFlow
   - Registro NAT a gran escala
   - Registro de mensajes ALG
   - Registro del suscriptor
   - Intercepción SSL
   - Filtrado de URL
   - Registro de inspección de contenido
5. Haga clic en **Crear** y **cerrar**.



Para crear una directiva de auditoría mediante la interfaz de línea de comandos

Puede crear una directiva NSLOG o una directiva SYSLOG. El tipo de directiva debe coincidir con el tipo de servidor. Los nombres de comandos de los dos tipos de directiva son diferentes, pero los parámetros de los comandos son los mismos.

En el símbolo del sistema, escriba los siguientes comandos:

- `add audit syslogPolicy <name> <-rule > <action>`
- `save ns config`

Ejemplo

En el ejemplo siguiente se crea una directiva denominada SysLogp1 que registra el tráfico de Web App Firewall en un servidor syslog denominado syslog1.

```
add audit syslogPolicy syslogP1 rule ”ns_true”action syslog1
save ns config
```

Para configurar una directiva de auditoría mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos:

- `set audit syslogPolicy <name> [-rule <expression>] [-action <string>]`
- `save ns config`

Ejemplo

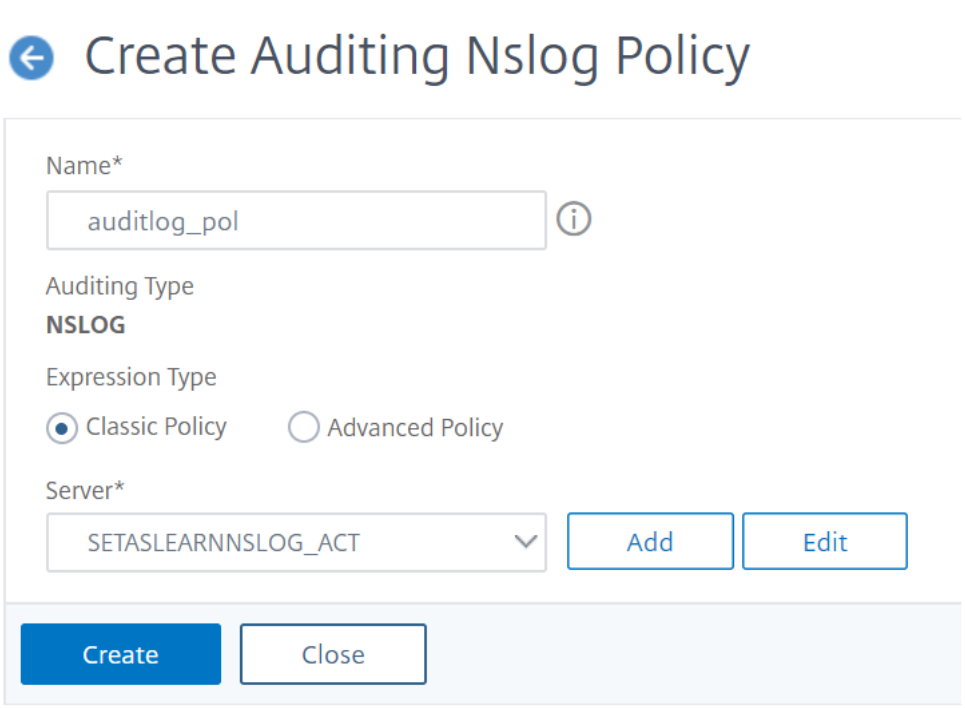
En el ejemplo siguiente se modifica la directiva denominada SysLogp1 para registrar el tráfico de Web App Firewall en un servidor syslog denominado syslog2.

```
set audit syslogPolicy syslogP1 rule ”ns_true”action syslog2
save ns config
```

Para configurar una directiva de auditoría mediante la interfaz gráfica de usuario

1. Vaya a **Seguridad** > **Citrix Web App Firewall** > **Directivas**.
2. En el panel de detalles, haga clic en **Auditar directiva Nslog**.
3. En la página Auditoría de Nslog, haga clic en la ficha **Directivas** y realice una de las acciones siguientes:
   - Para agregar una nueva directiva, haga clic en **Agregar**.
   - Para modificar una directiva existente, selecciónela y, a continuación, haga clic en **Modificar**.

4. En la página **Crear Directiva Nslog de Auditoría**, establezca los siguientes parámetros:
   - Nombre
   - Tipo de auditoría
   - Tipo de expresión
   - Servidor
5. Haga clic en **Crear**.



Importaciones

January 12, 2021

Varias funciones de Web App Firewall utilizan archivos externos que se cargan al Web App Firewall al configurarlo. Mediante la GUI, puede administrar esos archivos en el panel Importaciones, que tiene cuatro fichas correspondientes a los cuatro tipos de archivos que puede importar: Objetos de error HTML, objetos de error XML, esquemas XML y archivos WSDL (Lenguaje de descripción de servicios web). Con la línea de comandos de Citrix ADC, puede importar estos tipos de archivos, pero no puede exportarlos.

Objeto de error HTML

Cuando se bloquea la conexión de un usuario a una página HTML o Web 2.0, o un usuario solicita una página HTML o Web 2.0 inexistente, Web App Firewall envía una respuesta de error basada en HTML al explorador del usuario. Al configurar qué respuesta de error debe usar el Web App Firewall, tiene dos opciones:

- Puede configurar una dirección URL de redirección, que se puede alojar en cualquier servidor web al que los usuarios también tengan acceso. Por ejemplo, si tiene una página de error personalizada en el servidor web, 404.html, puede configurar Web App Firewall para redirigir a los usuarios a esa página cuando se bloquea una conexión.
- Puede configurar un objeto de error HTML, que es una página web basada en HTML alojada en el propio Web App Firewall. Si elige esta opción, debe cargar el objeto de error HTML en el Web App Firewall. Esto se hace en el panel Importaciones, en la ficha Objeto de error HTML.

El objeto de error debe ser un archivo HTML estándar que no contenga sintaxis que no sea HTML, excepto para las variables de personalización del objeto de error de Web App Firewall. No puede contener ningún script CGI, código analizado por el servidor o código PHP. Las variables de personalización permiten incrustar información de solución de problemas en el objeto de error que recibe el usuario cuando se bloquea una solicitud. Aunque la mayoría de las solicitudes que bloquean Web App Firewall son ilegítimas, incluso un Web App Firewall configurado correctamente puede bloquear ocasionalmente solicitudes legítimas, especialmente cuando se implementan por primera vez o después de realizar cambios significativos en los sitios web protegidos. Al incrustar información en la página de error, usted proporciona al usuario la información que él o ella necesita dar a la persona de soporte técnico para que pueda solucionarse cualquier problema.

Las variables de personalización de la página de error de Web App Firewall son:

- $ {NS_TRANSACTION_ID}. El identificador de transacción que el Web App Firewall asignó a esta transacción.
- $ {NS_APPFW_SESSION_ID}. El ID de sesión de Web App Firewall.
- $ {NS_APPFW_VIOLATION_CATEGORY}. La comprobación de seguridad o regla específica de Web App Firewall que se ha infringido.
- $ {NS_APPFW_VIOLATION_LOG}. El mensaje de error detallado asociado con la infracción.
- ${COOKIE El contenido de la cookie especificada. Para <CookieName>, sustituya el nombre de la cookie específica que quiere mostrar en la página de error. Si tiene varias cookies cuyo contenido quiere mostrar para la solución de problemas, puede utilizar varias instancias de esta variable de personalización, cada una con el nombre de la cookie correspondiente.
  Nota: Si tiene activado el bloqueo para la comprobación de coherencia de cookies, las cookies bloqueadas no se muestran en la página de error porque el Web App Firewall las bloquea.

Para utilizar estas variables, se incrustan en el HTML o XML del objeto de página de error como si

fueran una cadena de texto normal. Cuando el objeto de error se muestra al usuario, para cada variable de personalización, el Web App Firewall sustituye la información a la que se refiere la variable. A continuación se muestra una página de error HTML de ejemplo que utiliza variables personalizadas.

```
<!doctype html public "-//w3c//dtd html 4.0//en"> <html> <head> <title>Page Not Accessible</title> </head> <body> <h1>Page Not Accessible</h1> <p>The page that you accessed is not available. You can:</p> <ul> <li>return to the <b><a href="[homePage]">home page</a></b>, re-establish your session, and try again, or,</li> <li>report this incident to the help desk via <b><a href="mailto:[helpDeskEmailAddress]">email</a></b> or by calling [helpDeskPhoneNumber].</li> </ul> <p>If you contact the help desk, please provide the following information:</p> <table cellpadding=8 width=80%> <tr><th align="right" width=30%>Transaction ID:</th><td align="left" valign="top" width=70%>${
NS_TRANSACTION_ID }
</td></tr> <tr><th align="right" width=30%>Session ID:</th><td align="left" valign="top" width=70%>${
NS_APPFW_SESSION_ID }
</td></tr> <tr><th align="right" width=30%>Violation Category:</th><td align="left" valign="top" width=70%>${
NS_APPFW_VIOLATION_CATEGORY }
</td></tr> <tr><th align="right" width=30%>Violation Log:</th><td align="left" valign="top" width=70%>${
NS_APPFW_VIOLATION_LOG }
</td></tr> <tr><th align="right" width=30%>Cookie Name:</th><td align="left" valign="top" width=70%>${
COOKIE("[cookieName]") }
</td></tr> </table> <body> <html>
<!--NeedCopy-->
```

Para utilizar esta página de error, cópiela en un editor de texto o HTML. Sustituya la información local apropiada por las siguientes variables, que están entre corchetes para distinguirlas de las variables Citrix ADC. (Déjelos sin cambios.):

- `[homePage]`. La URL de la página de inicio de su sitio web.
- `[helpDeskEmailAddress]`. La dirección de correo electrónico que quiere que los usuarios utilicen para informar de incidentes de bloqueo.
- `[helpDeskPhoneNumber]`. El número de teléfono al que quiere que los usuarios llamen para informar de incidentes de bloqueo.
- `[cookieName]`. El nombre de la cookie cuyo contenido quiere mostrar en la página de error.

Objeto de error XML

Cuando se bloquea la conexión de un usuario a una página XML o un usuario solicita una aplicación XML inexistente, Web App Firewall envía una respuesta de error basada en XML al explorador del usuario. Para configurar la respuesta de error, cargue una página de error basada en XML en el Web App Firewall en el panel Importaciones, en la ficha Objeto de error XML. Todas las respuestas de error XML se hospedan en Web App Firewall. No se puede configurar una dirección URL de redirección para aplicaciones XML.

> **Nota**:
> Puede utilizar las mismas variables de personalización en un objeto de error XML que en un objeto de error HTML.

Esquema XML

Cuando Web App Firewall realiza una comprobación de validación en la solicitud de un usuario para una aplicación XML o Web 2.0, puede validar la solicitud con el esquema XML o documento de tipo de diseño (DTD) de esa aplicación y rechazar cualquier solicitud que no siga el esquema o DTD. Tanto un esquema XML como un DTD son archivos de configuración XML estándar que describen la estructura de un tipo específico de documento XML.

WSDL

Cuando el Web App Firewall realiza una comprobación de validación en la solicitud de un usuario para un servicio web basado en XML SOAP, puede validar la solicitud en el archivo de definición de tipo de servicios web (WSDL) para ese servicio web. Un archivo WSDL es un archivo de configuración XML SOAP estándar que define los elementos de un servicio web XML SOAP específico.

Importación y exportación de archivos

August 20, 2021

Puede importar objetos de error HTML o XML, esquemas XML, DTD y WSDL al Web App Firewall mediante la GUI o la línea de comandos. Puede modificar cualquiera de estos archivos en un área de texto basada en web después de importarlos, para realizar pequeños cambios directamente en el Citrix ADC en lugar de tener que realizarlos en el equipo y volver a importarlos. Por último, puede exportar cualquiera de estos archivos a su equipo, o eliminar cualquiera de estos archivos, mediante la GUI.

> **Nota:**
>
> No se puede eliminar ni exportar un archivo importado mediante la línea de comandos.

Para importar un archivo mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos:

- `import appfw htmlerrorpage <src> <name>`
- `<save> ns config`

Ejemplo

En el ejemplo siguiente se importa un objeto de error HTML de un archivo denominado error.html y se le asigna el nombre HTMLError.

```
import htmlerrorpage error.html HTMLError
save ns config
<!--NeedCopy-->
```

Para importar un archivo mediante la interfaz gráfica de usuario

Antes de intentar importar un esquema XML, un archivo DTD o WSDL, o un objeto de error HTML o XML desde una ubicación de red, compruebe que Citrix ADC se puede conectar al equipo de Internet o LAN donde se encuentra el archivo. De lo contrario, no puede importar el archivo u objeto.

1. Vaya a **Seguridad > Citrix Web App Firewall > Importaciones**.
2. Vaya a **Firewall de aplicaciones** > **Importaciones**.
3. En el panel **Importaciones de firewall de aplicaciones**, seleccione la ficha correspondiente al tipo de archivo que quiere importar y, a continuación, haga clic en **Agregar**.

   Las fichas son Página de error HTML, Página de error XML, Esquema XML o WSDL. El proceso de carga es idéntico en las cuatro fichas desde el punto de vista del usuario.
4. Rellene los campos de diálogo.
   - **Name**: Nombre para el objeto importado.
   - **Importar desde**: Elija la ubicación del archivo HTML, archivo XML, esquema XML o WSDL que quiere importar en la lista desplegable:
     - **URL: URL** web de un sitio web al que puede acceder el dispositivo.

- **Archivo:** archivo en un disco duro local o en red u otro dispositivo de almacenamiento de información.
- **Texto:** Escriba o pegue el texto de la respuesta personalizada directamente en un campo de texto en la GUI.

El tercer cuadro de texto cambia al valor adecuado. Los tres valores posibles se proporcionan a continuación.

- **URL**: Escriba la dirección URL en el cuadro de texto.
- **Archivo**: Escriba directamente la ruta y el nombre de archivo del archivo HTML, o haga clic en Examinar y busque el archivo HTML.
- **Texto**: Se elimina el tercer campo, dejando un espacio en blanco.

5. Haga clic en **Continuar**. Aparece el cuadro de diálogo Contenido del archivo. Si elige URL o Archivo, el cuadro de texto Contenido del archivo contiene el archivo HTML especificado. Si selecciona Texto, el cuadro de texto Contenido del archivo está vacío.
6. Si elige Texto, escriba o copie y pegue el HTML de respuesta personalizada que quiere importar.
7. Haga clic en **Done**.
8. Para eliminar un objeto, selecciónelo y, a continuación, haga clic en **Eliminar**.

Para exportar un archivo mediante la interfaz gráfica de usuario

Antes de intentar exportar un esquema XML, un archivo DTD o WSDL, o un objeto de error HTML o XML, compruebe que el dispositivo Web App Firewall pueda tener acceso al equipo en el que se va a guardar el archivo. De lo contrario, no podrá exportar el archivo.

1. Vaya a **Seguridad** > **Web App Firewall** > **Importaciones**.
2. En el panel **Importaciones de Web App Firewall**, seleccione la ficha correspondiente al tipo de archivo que quiere exportar.

   El proceso de exportación es idéntico en las cuatro fichas desde el punto de vista del usuario.
3. Seleccione el archivo que quiere exportar.
4. Expanda la lista desplegable Acción y seleccione **Exportar**.
5. En el cuadro de diálogo, elija **Guardar archivo** y haga clic en **Aceptar**.
6. En el cuadro de diálogo **Examinar**, desplácese hasta el sistema de archivos local y el directorio donde quiere guardar el archivo exportado y haga clic en **Guardar**.

Para modificar un objeto de error HTML o XML en la GUI

Modificar el texto de los objetos de error HTML y XML en la GUI sin exportarlos y, a continuación, volver a importarlos.

1. Vaya a **Seguridad > Citrix Web App Firewall > Importaciones**y, a continuación, seleccione la ficha correspondiente al tipo de archivo que quiere modificar.
2. Vaya a **Firewall de aplicaciones** > **Importaciones** y, a continuación, seleccione la ficha correspondiente al tipo de archivo que quiere modificar.
3. Seleccione el archivo que quiere modificar y, a continuación, haga clic en **Modificar**.

   El texto del objeto de error HTML o XML se muestra en un área de texto del explorador. Puede modificar el texto mediante las herramientas y métodos de edición estándar basados en explorador para el explorador.

   Nota: La ventana de edición está diseñada para permitirle realizar cambios menores en el objeto de error HTML o XML. Para realizar cambios extensos, puede que prefiera exportar el objeto de error al equipo local y utilizar herramientas de edición de páginas web HTML o XML estándar.
4. Haga clic en **Aceptar** y, a continuación, haga clic en **Cerrar**.

Configuración global

January 12, 2021

La configuración global de Web App Firewall afecta a todos los perfiles y directivas. Los elementos de configuración global son:

- **Configuración del motor.** Conjunto de configuraciones globales (nombre de cookie de sesión, tiempo de espera de sesión, duración máxima de la sesión, nombre de encabezado de registro, perfil indefinido, perfil predeterminado y límite de tamaño de importación) que pertenecen a todas las conexiones que procesa el Web App Firewall, en lugar de a un subconjunto específico de conexiones.
- **Campos confidenciales.** Conjunto de campos de formulario en formularios web que contienen información confidencial que no debe registrarse en los registros del Web App Firewall. Los campos de formulario, como los campos de contraseña en una página de inicio de sesión o la información de la tarjeta de crédito en un formulario de retirada del carrito de la compra, normalmente se designan como campos confidenciales.
- **Tipos de campo.** Lista de tipos de campos de formulario web utilizados por la comprobación de seguridad Formatos de campo. Cada uno de estos tipos de campo está definido por una expresión regular compatible con PCR que define el tipo de datos y la longitud mínima/máxima de los datos que se debe permitir en ese tipo de campo de formulario.

- **Tipos de contenido XML.** Lista de tipos de contenido reconocidos como XML y sometidos a comprobaciones de seguridad específicas de XML. Cada uno de estos tipos de contenido se define mediante una expresión regular compatible con PCRE-que define el tipo MIME exacto asignado a ese contenido.
- **Tipos de contenido JSON.** Lista de tipos de contenido reconocidos como JSON y sometidos a comprobaciones de seguridad específicas de JSON. Cada uno de estos tipos de contenido se define mediante una expresión regular compatible con PCRE-que define el tipo MIME exacto asignado a ese contenido.

Configuración del motor

January 12, 2021

La configuración del motor afecta a todas las solicitudes y respuestas que procesa Citrix Web App Firewall. Los siguientes son los ajustes:

- **Nombre de la cookie**: Nombre de la cookie que almacena el ID de sesión de Citrix ADC.
- **Tiempo de espera de sesión**: El período máximo de inactividad permitido. Si una sesión de usuario no muestra ninguna actividad durante este período de tiempo, la sesión finaliza y el usuario debe restablecerla visitando una página de inicio designada.
- **Prefijo de cifrado posterior de cookies**: La cadena que precede a la parte cifrada de las cookies cifradas.
- **Duración máxima de la sesión**: La cantidad máxima de tiempo, en segundos, que se permite que una sesión permanezca activa. Una vez alcanzado este período, la sesión finaliza y el usuario debe restablecerla visitando una página de inicio designada. Esta configuración no puede ser inferior al tiempo de espera de la sesión. Para inhabilitar esta configuración, de modo que no haya una duración máxima de la sesión, establezca el valor en cero (0).
- **Nombre de encabezado de registro**: Nombre del encabezado HTTP que contiene la IP del cliente, para el registro.
- **Perfil indefinido**: El perfil aplicado cuando la acción de directiva correspondiente se evalúa como indefinido.
- **Perfil predeterminado**: Perfil aplicado a conexiones que no coinciden con una directiva.
- **Límite de tamaño de importación**: El recuento máximo de bytes de todos los archivos importados al dispositivo, incluidas firmas, WSDL, esquemas, páginas de error HTML y XML. Durante una importación, si el tamaño del objeto importado hace que el recuento acumulativo de todos los archivos importados supere el límite configurado, se producirá un error en la operación de importación. Y el dispositivo muestra el siguiente mensaje de error: "*ERROR: Error de importación: Excediendo el límite de tamaño total configurado en los objetos importados*".
- **Límite de velocidad de mensajes de aprendizaje**: El número máximo de solicitudes y respues-

tas por segundo que el motor de aprendizaje va a procesar. Las solicitudes o respuestas adicionales que superen este límite no se envían al motor de aprendizaje.

- **Decodificación de entidades**: Decodifica entidades HTML al ejecutar comprobaciones de Web App Firewall.
- **Solicitud de registro malformada**: Permite el registro de solicitudes HTTP mal formadas.
- **Usar clave secreta configurable**: Utilice una clave secreta configurable para las operaciones de Web App Firewall. Esta clave secreta se utiliza para firmar y verificar datos. Cuando "UseConfigurableSecretKey" está activado, debe utilizar la clave habilitada en el parámetro "set ns EncryptionParams".
- **Restablecer datos aprendidos**: Elimina todos los datos aprendidos del Web App Firewall. Reinicia el proceso de aprendizaje mediante la recopilación de datos nuevos.

Se encuentran dos opciones, *Restablecer datos aprendidos* y *Actualización automática de firmas*, en diferentes lugares, en función de si usa la interfaz de comandos o la GUI de Citrix ADC para configurar Citrix Web App Firewall. Al utilizar la interfaz de comandos, puede configurar Restablecer datos aprendidos mediante el comando reset appfw learning data. Esto no toma parámetros y no tiene otras funciones. Puede configurar la firma Auto-Update en el comando set appfw settings. El parámetro -SignatureAutoUpdate habilita o inhabilita la actualización automática de las firmas y -signatureURL configura la dirección URL que aloja el archivo de firmas actualizado.

Cuando se utiliza la GUI de Citrix ADC, se configura **Restablecer datos aprendidos** en **Seguridad > Citrix Web App Firewall > Configuración del motor**. La opción **Restablecer datos aprendidos** se encuentra en la parte inferior del cuadro de diálogo. Para configurar la actualización automática de firmas para cada conjunto de firmas en **Seguridad** > **Citrix Web App Firewall** > **Firmas**, seleccione el archivo de firmas, haga clic con el botón derecho del mouse y seleccione **Configuración de actualización automática**.

Normalmente, los valores predeterminados de la configuración de **Web App Firewall** son correctos. Sin embargo, si la configuración predeterminada causa un conflicto con otros servidores o causa una desconexión prematura de los usuarios, debe modificarlos.

El límite de sesión de **Web App Firewall** se puede configurar mediante el siguiente comando:

```
1 > set appfw settings -sessionLimit 500000
2
3 Done
4
5 Default value:100000   Max value:500000 per PE
6 <!--NeedCopy-->
```


Para configurar los parámetros del motor mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos:

- `set appfw settings [-sessionCookieName <name>] [-sessionTimeout <positiveInteger>] [-sessionLifetime <positiveInteger>][-clientIPLoggingHeader <headerName>] [-undefaction <profileName>] [-defaultProfile <profileName>] [-importSizeLimit <positiveInteger>] [-logMalformedReq (ON | OFF)] [-signatureAutoUpdate (ON | OFF)] [-signatureUrl <expression>] [-cookiePostEncryptPrefix <string>] [-entityDecoding (ON | OFF)] [-useConfigurableSecretKey (ON | OFF)][-learnRateLimit <positiveInteger>]`
- `save ns config`

Ejemplo

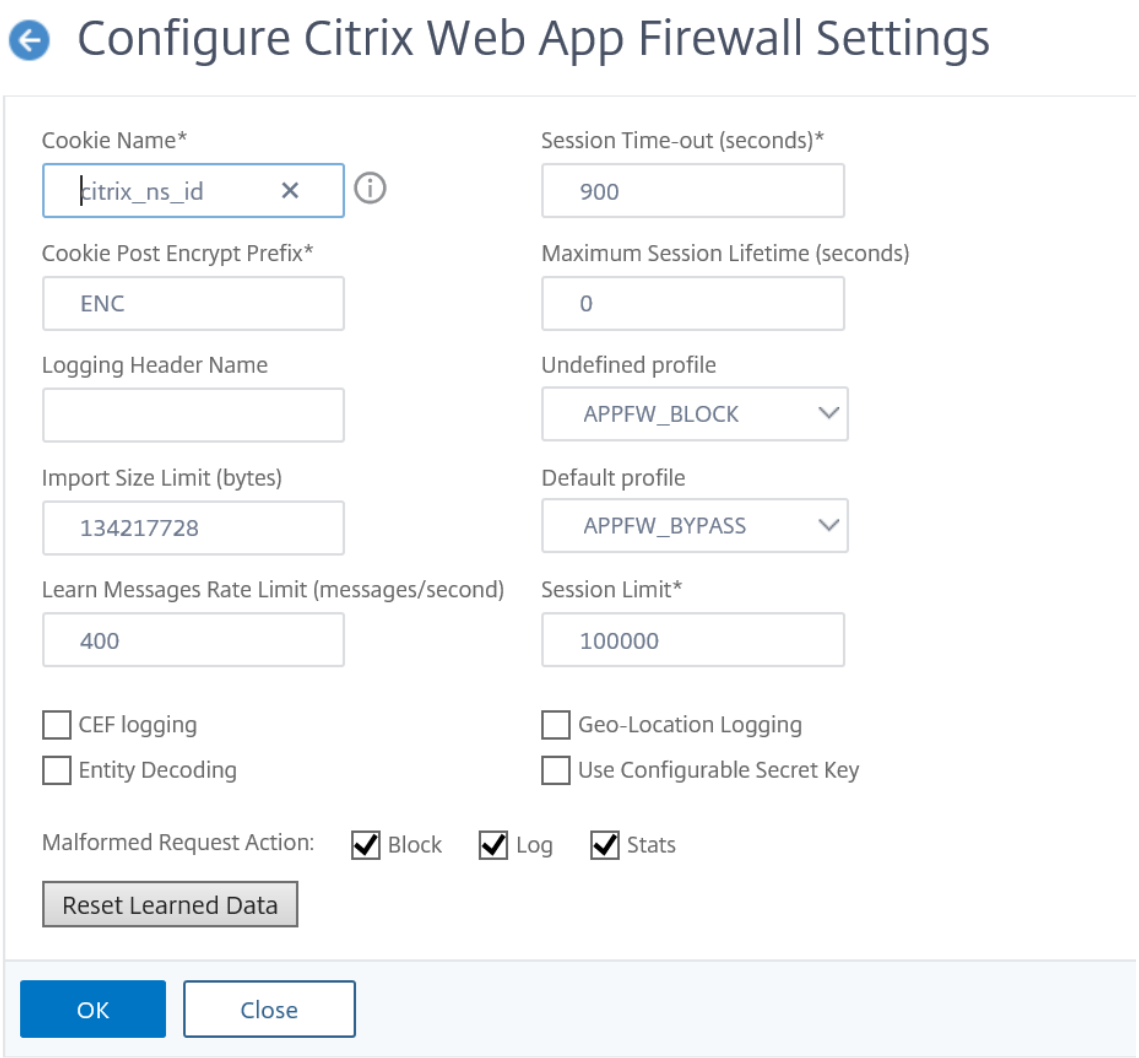
```
set appfw settings -sessionCookieName citrix-appfw-id -sessionTimeout
    3600
-sessionLifetime 14400 -clientIPLoggingHeader NS-AppFW-Client-IP -
    undefaction APPFW_RESET
-defaultProfile APPFW_RESET -importSizeLimit 4096
save ns config
<!--NeedCopy-->
```

Para configurar la configuración del motor mediante la GUI de Citrix ADC

1. Vaya a **Seguridad** > **Citrix Web App Firewall**
2. En el panel de detalles, haga clic en **Cambiar configuración del motor** en **Configuración**.
3. En el cuadro de diálogo **Configuración del motor de Web App Firewall**, establezca los siguientes parámetros:
   - Nombre de la cookie
   - Tiempo de espera de la sesión
   - Prefijo de cifrado de publicación de cookies
   - Duración máxima de la sesión
   - Nombre de encabezado de registro
   - Perfil indefinido
   - Perfil predeterminado
   - Límite de tamaño de importación
   - Límite de velocidad de mensajes de aprendizaje

- Decodificación de entidades
- Registro de solicitud mal formada
- Usar clave secreta
- Límite de velocidad de mensajes de aprendizaje
- Actualización automática de firmas

4. Haga clic en **Aceptar**.



Campos confidenciales

July 15, 2022

Puede designar los campos de formulario web como confidenciales para proteger la información que los usuarios escriben en ellos. Normalmente, cualquier información que un usuario escriba en un

formulario web en uno de sus servidores web protegidos se registra en los registros de Citrix ADC. Sin embargo, la información escrita en un campo de formulario web designado como confidencial no se registra. Esa información se guarda solo cuando el sitio web está configurado para guardar dichos datos, normalmente en una base de datos segura.

Los tipos comunes de información que puede desear proteger con una designación de campo confidencial incluyen:

- contraseñas
- Números de tarjetas de crédito, códigos de validación y fechas de caducidad
- Números de la seguridad social
- Números de identificación fiscal
- Domicilios
- Números de teléfono privados

Además de ser una buena práctica, el uso adecuado de las designaciones de campo confidenciales puede ser necesario para el cumplimiento de PCI-DSS en los servidores de comercio electrónico, el cumplimiento de la HIPAA en los servidores que administran información médica en los Estados Unidos y el cumplimiento de otras normas de protección de datos.

> **Importante**:
>
> En los dos casos siguientes, la designación de Campo confidencial no funciona como se esperaba:

- Si un formulario web tiene un campo confidencial o una URL de acción de más de 256 caracteres, la URL del campo o de la acción se trunca en los registros de Citrix ADC.
- Con ciertas transacciones SSL, los registros se truncan si el campo confidencial o la URL de la acción tienen más de 127 caracteres.

En cualquiera de estos casos, Web App Firewall enmascara una cadena de quince caracteres con la letra “x”, en lugar de la cadena normal de ocho caracteres. Para garantizar que se elimine cualquier información confidencial, el usuario debe usar expresiones de nombre de campo de formulario y URL de acción que coincidan con los primeros 256 o (en los casos en que se utilice SSL) con los primeros 127 caracteres.

Para configurar Web App Firewall para tratar un campo de formulario web en un sitio web protegido como confidencial, agregue ese campo a la lista Campos confidenciales. Puede escribir el nombre del campo como una cadena o puede escribir una expresión regular compatible con PCRE que especifique uno o más campos. Puede habilitar la designación de campo confidencial cuando agrega el campo o puede modificar la designación más adelante.

> **Nota**
>
> A partir de la versión 13.1 compilación 27.x, los campos confidenciales también se admiten en los

> perfiles WAF. Para obtener más información, consulte Campos confidenciales en el perfil WAF.

Para agregar un campo confidencial mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los comandos siguientes:

- `add appfw confidField <fieldName> <url> [-isRegex ( REGEX | NOTREGEX )] [-comment "<string>"] [-state ( ENABLED | DISABLED )]`
- `save ns config`

Ejemplo

El siguiente ejemplo agrega todos los campos de formulario web cuyos nombres comiencen por Contraseña a la lista de campos confidenciales.

```
1 add appfw confidField Password "https?://www[.]example[.]com/[^<>]\*[^a
    -z]password[0-9a-z._-]\*[.](asp|cgi|htm|html|htp|js|php)" -isRegex
    REGEX -state ENABLED
2 save ns config
3 <!--NeedCopy-->
```

Para modificar un campo confidencial mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los comandos siguientes:

- `set appfw confidField <fieldName> <url> [-isRegex ( REGEX | NOTREGEX )][-comment "<string>"] [-state ( ENABLED | DISABLED )]`
- `save ns config`

Ejemplo

El siguiente ejemplo modifica la designación del campo confidencial para agregar un comentario.

```
1 set appfw confidField Password "https?://www[.]example[.]com/[^<>]\*[^a
    -z]password[0-9a-z._-]\*[.](asp|cgi|htm|html|htp|js|php)" -comment "
    Protect password fields." -isRegex REGEX -state ENABLED
2 save ns config
3 <!--NeedCopy-->
```


Para eliminar un campo confidencial mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los comandos siguientes:

- `rm appfw confidField <fieldName> <url>`
- `save ns config`

Para configurar un campo confidencial mediante la GUI

1. Vaya a **Seguridad** > **Firewall de aplicaciones**.
2. En el panel de detalles, en **Configuración**, haga clic en **Administrar campos confidenciales**.
3. En el cuadro de diálogo Administrar campos confidenciales, realice una de las siguientes acciones:
   - Para agregar un nuevo campo de formulario a la lista, haga clic en Agregar.
   - Para cambiar una designación de campo confidencial existente, seleccione el campo y, a continuación, haga clic en **Modificar**.

     Aparece el cuadro de diálogo **Campos confidenciales de Web App Firewall**.

     > **Nota**:
     > Si selecciona una designación de campo confidencial existente y, a continuación, hace clic en **Agregar**, el cuadro de diálogo **Crear campo de formulario confidencial** muestra la información de ese campo confidencial. Puede modificar esa información para crear su nuevo campo confidencial.
4. En el cuadro de diálogo, rellene los elementos. Se trata de:
   - **Casilla de verificación Activada.** Seleccione o desactive para activar o desactivar esta designación de campo confidencial.
   - **Es una casilla de verificación del nombre del campo del formulario una expresión regular.** Seleccione o desactive para habilitar las expresiones regulares con formato PCRE en el nombre del campo del formulario.
   - **Nombre de campo.** Introduzca una cadena literal o una expresión regular con formato PCRE que represente un nombre de campo específico o que coincida con varios campos con nombres que sigan un patrón.
   - **URL de acción.** Introduzca una URL literal o una expresión regular que defina una o más URL de las páginas web en las que se encuentran los formularios web que contienen el campo confidencial.
   - **Comentarios.** Introduzca un comentario. Opcional.
5. Haga clic en **Crear** o **Aceptar**.
6. Para eliminar una designación de campo confidencial de la lista de campos confidenciales, seleccione la lista de campos confidenciales que desea eliminar y, a continuación, haga clic en Eliminar para eliminarla y, a continuación, haga clic en **Aceptar** para confirmar su elección.
7. Cuando haya terminado de agregar, modificar y eliminar designaciones de campos confidenciales, haga clic en **Cerrar**.

Ejemplos

A continuación se presentan algunas expresiones regulares que definen nombres de campos de formulario que pueden resultarle útiles:

- `^passwd_ (Applies confidential-field status to all field names that begin with the “passwd_” string.)`
- `^((\[0-9a-zA-Z._-]*||\\x\[0-9A-Fa-f][0-9A-Fa-f])+-)?passwd_ (Applies confidential-field status to all field names that begin with the string passwd_, or that contain the string -passwd_ after another string that might contain non-ASCII special characters.)`

A continuación se muestran algunas expresiones regulares que definen tipos de URL específicos que pueden resultarle útiles. Sustituya sus propios servidores web y dominios por los de los ejemplos.

- Si el formulario web aparece en varias páginas web del servidor web www.example.com, pero todas esas páginas web se denominan logon.pl?, puede usar la siguiente expresión regular:

```
https?://www[.]example[.]com/([0-9A-Za-z][0-9A-Za-z_.-]*/)*logon[.]pl?
<!--NeedCopy-->
```

- Si el formulario web aparece en varias páginas web en el servidor web www.example-español.com, que contiene el carácter especial n-tilde (ñ), puede usar la siguiente expresión regular, que representa el carácter especial n-tilde como una cadena UTF-8 codificada que contiene C3 B1, el código hexadecimal asignado a esa en el conjunto de caracteres UTF-8:

```
https?://www[.]example-espa\xC3\xB1ol[.]com/([0-9A-Za-z][0-9A-Za-z_.-]\*/)\* logon[.]pl?
<!--NeedCopy-->
```

- Si el formulario web que contiene query.pl aparece en varias páginas web en diferentes hosts dentro del dominio example.com, puede usar la siguiente expresión regular:

```
https?://([0-9A-Za-z][0-9A-Za-z_-.]*[.])\*example[.]com/([0-9A-Za-z][0-9A-Za-z_-.]\*/)*logon[.]pl?
<!--NeedCopy-->
```

- Si el formulario web que contiene query.pl aparece en varias páginas web en diferentes hosts en diferentes dominios, puede usar la siguiente expresión regular:


```
https?://([0-9A-Za-z][0-9A-Za-z_-.]\*[.])\*[0-9A-Za-z][0-9A-Za-z_
   -.]+[.][a-z]{
2,6 }
/([0-9A-Za-z][0-9A-Za-z_-.]*/)*logon[.]pl?
<!--NeedCopy-->
```

- Si el formulario web aparece en varias páginas web del servidor web www.example.com, pero todas esas páginas web se denominan logon.pl?, puede usar la siguiente expresión regular:

```
https?://www[.]example[.]com/([0-9A-Za-z][0-9A-Za-z_-.]*/)*logon
   [.]pl?
<!--NeedCopy-->
```

Tipos de campo

August 20, 2021

Un tipo de campo es una expresión regular con formato PCRE-que define un formato de datos determinado y longitudes de datos mínimas/máximas para un campo de formulario en un formulario web. Los tipos de campo se utilizan en la comprobación Formatos de campo.

El Web App Firewall incluye varios tipos de campos predeterminados, que son:

- integer. Cadena de cualquier longitud que consta únicamente de números, sin un punto decimal y con un signo menos anterior opcional (-).
- alpha. Una cadena de cualquier longitud que consiste únicamente en letras.
- alphanum. Cadena de cualquier longitud que consta de letras y/o números.
- nohtml. Cadena de cualquier longitud que consta de caracteres, incluidos signos de puntuación y espacios, que no contiene símbolos HTML ni consultas.
- any. Cualquier cosa.

> **Importante:**
>
> Asignar el tipo de campo cualquier como tipo de campo predeterminado, o a un campo, permite enviar scripts activos, comandos SQL y otro contenido posiblemente peligroso a los sitios web y aplicaciones protegidos en ese campo de formulario. Debe usar el cualquier tipo con moderación, si lo usa en absoluto.

También puede agregar sus propios tipos de campo a la lista Tipos de campo. Por ejemplo, es posible que quiera agregar un tipo de campo para un número de seguridad social, un código postal o un número de teléfono en su país. También es posible que quiera agregar un tipo de campo para un número de identificación de cliente o un número de tarjeta de crédito de almacén.

Para agregar un tipo de campo a la lista Tipos de campo, escriba el nombre del campo como una cadena literal o expresión regular con formato PCRE-Format.

Para agregar un tipo de campo mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos:

- `add appfw fieldType <name> <regex> <priority> [-comment "<string>"]`
- `save ns config`

Ejemplo

En el ejemplo siguiente se agrega un tipo de campo denominado SSN que coincide con los números del Seguro Social de Estados Unidos a la lista Tipos de campo y se establece su prioridad en 1.

```
1  add appfw fieldType SSN "^[1-9][0-9]{
2   2,2 }
3   -[0-9 }
4   {
5   2,2 }
6   -[0-9]{
7   4,4 }
8   $" 1
9  save ns config
10 <!--NeedCopy-->
```

Para modificar un tipo de campo mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos:

- `set appfw fieldType <name> <regex> <priority> [-comment "<string>"]`
- `save ns config`

Ejemplo

En el ejemplo siguiente se modifica el tipo de campo para agregar un comentario.


```
set appfw fieldType SSN ”^[1-9][0-9]{
 2,2 }
 -[0-9 }
 {
 2,2 }
 -[0-9]{
 4,4 }
 $” 1 -comment ”US Social Security Number”
save ns config
<!--NeedCopy-->
```

Para eliminar un tipo de campo mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos:

- >rm appfw fieldType <name>
- save ns config

Para configurar un tipo de campo mediante la interfaz gráfica de usuario

1. Vaya a Seguridad > Firewall de aplicaciones.
2. En el panel de detalles, en **Configuración**, haga clic en **Administrar tipos de campo**.
3. En el cuadro de diálogo **Administrar tipos de campo**, realice una de las acciones siguientes:
   - Para agregar un nuevo tipo de campo a la lista, haga clic en **Agregar**.
   - Para cambiar un tipo de campo existente, seleccione el tipo de campo y, a continuación, haga clic en **Modificar**.
     Aparece el cuadro de diálogo **Configurar tipo de campo**.

   > **Nota:**
   >
   > Si selecciona una designación de tipo de campo existente y, a continuación, hace clic en **Agregar**, el cuadro de diálogo muestra la información de ese tipo de campo. Puede modificar esa información para crear el nuevo tipo de campo.

4. En el cuadro de diálogo, rellene los elementos. Se trata de:
   - Nombre
   - Expresión regular
   - Prioridad
   - Comentario

5. Haga clic en Crear o Aceptar.
6. Para quitar un tipo de campo de la lista Tipos de campo, seleccione la lista de tipos de campo que quiere quitar, haga clic en **Quitar** para quitarlo y, a continuación, haga clic en **Aceptar** para confirmar su elección.
7. Cuando haya terminado de agregar, modificar y quitar tipos de campo, haga clic en **Cerrar**.

Ejemplos

A continuación se presentan algunas expresiones regulares para los tipos de campo que puede ser útil:

`^[1-9][0-9]{ 2,2 } -[0-9 } { 2,2 } -[0-9]{ 4,4 } $` Números de la Seguridad Social de los Estados Unidos

`^\[A-C\]\[0-9\]{ 7,7 } $` Números de permiso de conducir de California

`^+[0-9]{ 1,3 } [0-9()-]{ 1,40 } $` Números de teléfono internacionales con códigos de país

`^[0-9]{ 5,5 } -[0-9]{ 4,4 } $` Números de código postal de EE. UU.

`^[0-9A-Za-z][0-9A-Za-z.+_-]{ 0,25 } @([0-9A-Za-z][0-9A-Za-z_-]*[.]){ 1,4 } [A-Za-z]{ 2,6 } $` Direcciones de correo electrónico

Tipos de contenido XML

February 16, 2021

De forma predeterminada, Web App Firewall trata los archivos que siguen determinadas convenciones de nomenclatura como XML. Puede configurar Web App Firewall para examinar el contenido web en busca de cadenas o patrones adicionales que indiquen que esos archivos son archivos XML. Esto puede garantizar que Web App Firewall reconozca todo el contenido XML del sitio, incluso si determinado contenido XML no sigue las convenciones de nomenclatura XML normales, lo que garantiza que el contenido XML está sujeto a comprobaciones de seguridad XML.

Para configurar los tipos de contenido XML, agregue los patrones adecuados a la lista Tipos de contenido XML. Puede escribir un tipo de contenido como una cadena, o bien puede escribir una expresión regular compatible con PCRE-que especifique una o más cadenas. También puede modificar los patrones de tipos de contenido XML existentes.

Para agregar un patrón de tipo de contenido XML mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos:

- `add appfw XMLContentType <XMLContenttypevalue> [-isRegex ( REGEX | NOTREGEX )]`
- `save ns config`

Ejemplo

En el ejemplo siguiente se agrega el patrón. */xml a la lista Tipos de contenido XML y la designa como una expresión regular.

```
1 add appfw XMLContentType ".*/xml" -isRegex REGEX
2 <!--NeedCopy-->
```

Para eliminar un patrón de tipo de contenido XML mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos:

- `rm appfw XMLContentType <XMLContenttypevalue>`
- `save ns config`

Para configurar la lista de tipos de contenido XML mediante la interfaz gráfica de usuario

1. Vaya a **Seguridad** > **Web App Firewall**.
2. En el panel de detalles, en **Configuración**, haga clic en **Administrar tipos de contenido XML**.
3. En el cuadro de diálogo **Administrar tipos de contenido XML**, realice una de las acciones siguientes:
   - Para agregar un nuevo tipo de contenido XML, haga clic en Agregar.
   - Para modificar un tipo de contenido XML existente, selecciónelo y, a continuación, haga clic en Modificar.Aparece
     el cuadro de diálogo Configurar tipo de contenido XML de Web App Firewall. Nota: Si selecciona un patrón de tipo de contenido XML existente y, a continuación, hace clic en Agregar, el cuadro de diálogo mostrará la información correspondiente a ese patrón de tipo de contenido XML. Puede modificar esa información para crear el nuevo patrón de tipo de contenido XML.
4. En el cuadro de diálogo, rellene los elementos. Se trata de:
   - **IsRegex.** Seleccione o desactive para habilitar expresiones regulares con formato PCRE-format en el nombre del campo de formulario.

- **Tipo de contenido XML** Escriba una cadena literal o una expresión regular de formato PCRE-que coincida con el patrón de tipo de contenido XML que quiere agregar.

5. Haga clic en **Crear**.
6. Para quitar un patrón de tipo de contenido XML de la lista, selecciónelo, haga clic en **Quitar** para quitarlo y, a continuación, haga clic en **Aceptar** para confirmar su elección.
7. Cuando haya terminado de agregar y quitar patrones de tipo de contenido XML, haga clic en **Cerrar**.

Tipos de contenido JSON

February 16, 2021

De forma predeterminada, Web App Firewall trata los archivos con el tipo de contenido "application/json" como archivos JSON. La configuración predeterminada permite que Web App Firewall reconozca contenido JSON en solicitudes y respuestas, y que gestione ese contenido de forma adecuada.

Puede configurar Web App Firewall para examinar el contenido web en busca de cadenas o patrones adicionales que indiquen que esos archivos son archivos JSON. Esto puede garantizar que Web App Firewall reconozca todo el contenido JSON en su sitio, incluso si determinado contenido JSON no sigue las convenciones de nomenclatura JSON normales, lo que garantiza que el contenido JSON esté sujeto a comprobaciones de seguridad JSON.

Para configurar los tipos de contenido JSON, agregue los patrones apropiados a la lista Tipos de contenido JSON. Puede escribir un tipo de contenido como una cadena, o bien puede escribir una expresión regular compatible con PCRE-que especifique una o más cadenas. También puede modificar los patrones de tipos de contenido JSON existentes.

Para agregar un patrón de tipo de contenido JSON mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos:

- `add appfw JSONContentType <JSONContenttypevalue> [-isRegex ( REGEX | NOTREGEX )]`
- `save ns config`

Ejemplo

En el ejemplo siguiente se agrega el patrón. */json a la lista Tipos de contenido JSON y la designa como una expresión regular.


```
add appfw JSONContentType ".*/json" -isRegex REGEX
<!--NeedCopy-->
```

Para configurar la lista de tipos de contenido JSON mediante la interfaz gráfica de usuario

1. Vaya a **Seguridad** > **Firewall de aplicaciones**.
2. En el panel de detalles, en **Configuración**, haga clic en **Administrar tipos de contenido JSON**.
3. En el cuadro de diálogo Administrar tipos de contenido JSON, realice una de las siguientes acciones:
   - Para agregar un nuevo tipo de contenido JSON, haga clic en Agregar.
   - Para modificar un tipo de contenido JSON existente, seleccione ese tipo y, a continuación, haga clic en Modificar.Aparece
     el cuadro de diálogo Configurar Web App Firewall JSON Content Type.
     Nota: Si selecciona un patrón de tipo de contenido JSON existente y, a continuación, hace clic en Agregar, el cuadro de diálogo mostrará la información de ese patrón de tipo de contenido JSON. Puede modificar esa información para crear su nuevo patrón de tipo de contenido JSON.
4. En el cuadro de diálogo, rellene los elementos. Se trata de:
   - **IsRegex.** Seleccione o desactive para habilitar expresiones regulares con formato PCRE-format en el nombre del campo de formulario.
   - **Tipo de contenido JSON** Introduzca una cadena literal o una expresión regular de formato PCRE-que coincida con el patrón de tipo de contenido JSON que quiere agregar.
5. Haga clic en **Crear** o **Aceptar**.
6. Para quitar un patrón de tipo de contenido JSON de la lista, selecciónelo, haga clic en **Quitar** para quitarlo y, a continuación, haga clic en **Aceptar** para confirmar su elección.
7. Cuando haya terminado de agregar y quitar patrones de tipo de contenido XML, haga clic en **Cerrar**.

Estadísticas e informes

December 2, 2021

La información que se mantiene en los registros y las estadísticas, y que se muestra en los informes, proporciona una guía importante para configurar y mantener Web App Firewall.

Estadísticas de Web App Firewall

Cuando habilita la acción estadística para las firmas o las comprobaciones de seguridad de Web App Firewall, Web App Firewall mantiene la información sobre las conexiones que coinciden con esa firma o comprobación de seguridad. Puede ver la información estadística acumulada en la ficha **Supervisión** seleccionando una de las siguientes opciones en el cuadro de lista Seleccionar grupo:

- **Web App Firewall.** Un resumen de toda la información estadística recopilada por el dispositivo Web App Firewall para todos los perfiles.
- **Web App Firewall (por perfil).** La misma información, pero se muestra por perfil en lugar de resumirla.

Puede utilizar esta información para supervisar el funcionamiento de su Web App Firewall y determinar si hay alguna actividad anormal o cantidades anormales de visitas en una firma o comprobación de seguridad. Si ve un patrón de actividad anormal de este tipo, puede comprobar los registros de esa firma o comprobación de seguridad para diagnosticar y tomar medidas correctivas.

Contador estadístico de resultados

Según la relajación que se aplica al tráfico infringido, también puede mostrar detalles estadísticos, como el número de veces que se produce una infracción en el dispositivo, el número de reglas de relajación aplicadas en el momento de la infracción y su última marca de tiempo aplicada. Al realizar esto, el motor de aprendizaje centralizado puede eliminar automáticamente enlaces de relajación no utilizados o redundantes. Para obtener más información, consulte el tema de WAF Learn Engine.

El contador estadístico de impacto de relajación solo está disponible para las siguientes comprobaciones de seguridad.

- Scripts entre sitios
- Inyección SQL
- Consistencia de cookies
- JSON SQL
- Scripting entre sitios JSON
- DoS de JSON
- Inyección de CMD JSON
- Falsificación de solicitudes entre sitios
- Formato de campo
- Starturl
- Denyurl
- Protección de tipo contenido

Para mostrar estadísticas de los contadores de acierto de reglas de relajación mediante la CLI

En el símbolo del sistema, escriba:

```
stat appfw profile p1
```

Ejemplo:

```
stat appfw profile p1 -fullvalues
```

Estadísticas de Starturl Rules

Regla	éxitos	Tasa	Tiempo del último resultado
87a4…51177	0	0	Jue… 1970
5b83…dc12a	0	0	Jue… 1970
12345	0	0	Jue… 1970

Para mostrar estadísticas de los contadores de acierto de reglas de relajación mediante la interfaz gráfica de usuario

Complete los siguientes pasos para ver las estadísticas del contador de visitas de la regla de relajación:

1. Vaya a **Seguridad > Citrix Web App Firewall > Perfiles**.
2. En el panel de detalles, seleccione un **perfil de Web App Firewall** y haga clic en **Estadísticas**.
3. La página **Estadísticas de Citrix Web App Firewall** muestra los detalles de las estadísticas.
4. Puede seleccionar Vista tabular o cambiar a Vista gráfica para mostrar los datos en formato tabular o gráfico.

Informes de Web App Firewall

Los informes de Web App Firewall proporcionan información sobre la configuración de Web App Firewall y cómo gestiona el tráfico de sus sitios web protegidos.

El informe de PCI DSS

El Estándar de seguridad de datos (DSS) de la Industria de Tarjetas de Pago (PCI), versión 1.2, consta de 12 criterios de seguridad que la mayoría de las compañías de tarjetas de crédito exigen a las empresas que aceptan pagos en línea a través de tarjetas de crédito y débito que cumplan. Los criterios están diseñados para evitar el robo de identidad, la piratería y otros tipos de fraude. Si un ISP no cumple con los criterios del PCI DSS, el ISP o el comerciante podrían perder la autorización para aceptar pagos con tarjeta de crédito a través del sitio web.

Los ISP y los comerciantes en línea demuestran que cumplen con PCI DSS al tener una auditoría realizada por una empresa de asesores de seguridad calificados (QSA) de PCI DSS. El informe PCI DSS está diseñado para ayudarlos tanto antes como durante la auditoría. Antes de la auditoría, muestra qué ajustes de Web App Firewall son relevantes para PCI DSS, cómo deben configurarse y (lo más importante) si su configuración actual de Web App Firewall cumple con el estándar. Durante la auditoría, el informe se puede utilizar para demostrar el cumplimiento de un criterio PCI DSS relevante.

El informe PCI DSS consiste en una lista de los criterios que son relevantes para su configuración de Web App Firewall. En cada criterio, enumera las opciones de configuración actuales, indica si su configuración actual cumple con el criterio PCI DSS y explica cómo configurar Web App Firewall para que sus sitios web protegidos cumplan con el criterio.

El informe de PCI DSS se encuentra en **Sistema > Informes**. Para generar el informe como un archivo PDF de Adobe, haga clic en **Generar informe PCI DSS**. Según la configuración del explorador, el informe se muestra en la ventana emergente o se le pedirá que lo guarde en el disco duro.

> **Nota:**
>
> Para ver este y otros informes, debe tener el programa Adobe Reader instalado en el equipo.

El informe de PCI DSS consta de las siguientes secciones:

- **Descripción.** Descripción del informe Resumen de cumplimiento de PCI DSS.
- **Licencia y estado de las funciones del firewall.** Le indica si Web App Firewall tiene licencia y está habilitado en su dispositivo Citrix ADC.
- **Resumen ejecutivo.** Una tabla que enumera los criterios de PCI DSS y le indica cuáles de esos criterios son relevantes para Web App Firewall.
- **Información detallada de los criterios de PCI DSS.** Para cada criterio de PCI DSS que sea relevante para la configuración de Web App Firewall, el informe de PCI DSS proporciona una sección que contiene información sobre si su configuración cumple y, si no lo está, cómo cumplirla.
- **Configuración.** Datos para perfiles individuales, a los que accede haciendo clic en Configuración de Web App Firewall en la parte superior del informe o directamente desde el panel Informes. El informe de configuración de Web App Firewall es el mismo que el informe de PCI DSS, con el resumen específico de PCI DSS omitido.

Informe de configuración de Web App Firewall

El informe de configuración de Web App Firewall se encuentra en **Sistema > Informes**. Para mostrarlo, haga clic en **Generar informe de configuración de Web App Firewall**. Según la configuración del explorador, el informe se muestra en la ventana emergente o se le pedirá que lo guarde en el disco duro.

El informe de configuración de Web App Firewall comienza con una página de resumen, que consta de las siguientes secciones:

- **Directivas de Web App Firewall.** Una tabla que enumera las directivas actuales de Web App Firewall y muestra el nombre de la directiva, el contenido de la directiva, la acción (o perfil) con la que está asociada y la información de enlace global.
- **Perfiles de Web App Firewall.** Tabla que muestra los perfiles actuales de Web App Firewall e indica a qué directiva está asociado cada perfil. Si un perfil no está asociado a una directiva, la tabla muestra INACTIVO en esa ubicación.

Para descargar todas las páginas de informes de todas las directivas, en la parte superior de la página Resumen de perfiles, haga clic en **Descargar todos los perfiles**. Para mostrar la página del informe de cada perfil individual, seleccione ese perfil en la tabla en la parte inferior de la pantalla. La página Perfil de un perfil individual muestra si cada acción de verificación está habilitada o inhabilitada para cada comprobación y las demás opciones de configuración para la comprobación.

Para descargar un archivo PDF que contiene la página del informe PCI DSS del perfil actual, haga clic en **Descargar perfil actual** en la parte superior de la página. Para volver a la página Resumen de perfiles, haga clic en **Perfiles de Web App Firewall**. Para volver a la página principal, haga clic en **Inicio**. Puede actualizar el informe PCI DSS en cualquier momento haciendo clic en **Actualizar** en la esquina superior derecha del explorador.

Registros de Web App Firewall

June 22, 2022

Web App Firewall genera mensajes de registro para realizar un seguimiento de la configuración, la invocación de directivas y los detalles de infracción de la comprobación de seguridad

Cuando habilita la acción de registro para las comprobaciones de seguridad o las firmas, los mensajes de registro resultantes proporcionan información sobre las solicitudes y respuestas que Web App Firewall ha observado al proteger sus sitios web y aplicaciones. La información más importante es la acción que realiza Web App Firewall cuando se observa una infracción de firma o de comprobación de seguridad. Para algunas comprobaciones de seguridad, el mensaje de registro puede proporcionar información útil, como la ubicación del usuario o el patrón detectado que desencadenó una infracción. Un aumento excesivo en la cantidad de mensajes de infracción en los registros puede indicar un aumento en las solicitudes maliciosas. El mensaje le avisa de que su aplicación podría estar siendo atacada para aprovechar una vulnerabilidad específica que las protecciones de Web App Firewall detectan y frustran.

> **Nota:**
>
> El registro de Citrix Web App Firewall debe utilizarse únicamente con servidores SYSLOG externos.

Registros de formato Citrix ADC (nativo)

Web App Firewall utiliza los registros de formato de Citrix ADC (también denominados registros de formato nativo) de forma predeterminada. Estos registros tienen el mismo formato que los generados por otras funciones de Citrix ADC. Cada registro contiene los campos siguientes:

- Marca de tiempo. Fecha y hora en que se produjo la conexión.
- Gravedad. Nivel de gravedad del registro.
- Módulo. Módulo Citrix ADC que generó la entrada de registro.
- Tipo de evento. Tipo de suceso, como infracción de firma o de comprobación de seguridad.
- ID de evento. ID asignado al evento.
- IP del cliente. Dirección IP del usuario cuya conexión se ha registrado.
- ID de transacción. ID asignado a la transacción que ha provocado el registro.
- ID de sesión. ID asignado a la sesión de usuario que ha provocado el registro.
- Mensaje. El mensaje de registro. Contiene información que identifica la firma o la comprobación de seguridad que ha desencadenado la entrada del registro.

Puede buscar cualquiera de estos campos o cualquier combinación de información de distintos campos. Su selección está limitada únicamente por las capacidades de las herramientas que utiliza para ver los registros. Puede observar los mensajes de registro de Web App Firewall en la GUI accediendo al visor de syslog de Citrix ADC, o puede conectarse manualmente al dispositivo Citrix ADC y acceder a los registros desde la interfaz de línea de comandos, o puede colocar en el shell y seguir los registros directamente desde `/var/log/folder`.

Ejemplo de mensaje de registro en formato nativo

```
1 Jun 22 19:14:37 <local0.info> 10.217.31.98 06/22/2015:19:14:37 GMT ns
     0-PPE-1 :
2 default APPFW APPFW_cross-site scripting 60 0 :  10.217.253.62 616-PPE1
      y/3upt2K8ySWWId3Kavbxyni7Rw0000
3 pr_ffc http://aaron.stratum8.net/FFC/login.php?login_name=abc&passwd=
4 12345&drinking_pref=on&text_area=%3Cscript%3E%0D%0A&loginButton=
     ClickToLogin&as_sfid=
5 AAAAAAWEXcNQLlSokNmqaYF6dvfqlChNzSMsdyO9JXOJomm2v
6 BwAMOqZIChv21EcgBc3rexIUcfm0vckKlsgoOeC_BArx1Ic4NLxxkWMtrJe4H7SOfkiv9NL7AG4juPIan

7 %3D&as_fid=feeec8758b41740eedeeb6b35b85dfd3d5def30c Cross-site script
     check failed for
```



```
field text_area="Bad tag: script" <blocked>
<!--NeedCopy-->
```

Registros de formato de eventos comunes (CEF)

Web App Firewall también admite registros CEF. CEF es un estándar de administración de registros abiertos que mejora la interoperabilidad de la información relacionada con la seguridad de diferentes dispositivos y aplicaciones de seguridad y red. CEF permite a los clientes utilizar un formato de registro de eventos común para que un sistema de gestión empresarial recopile y agregue datos fácilmente para su análisis. El mensaje de registro se divide en diferentes campos para que pueda analizar fácilmente el mensaje y escribir scripts para identificar información importante.

Análisis del mensaje de registro CEF

Además de la fecha, la marca de tiempo, la IP del cliente, el formato de registro, el dispositivo, la empresa, la versión de compilación, el módulo y la información de comprobación de seguridad, los mensajes de registro CEF de Web App Firewall incluyen los siguientes detalles:

- src — dirección IP de origen
- spt — número de puerto de origen
- request — URL de solicitud
- act — acción (por ejemplo, bloqueada, transformada)
- msg — message (Mensaje sobre la infracción de la comprobación de seguridad observada)
- cn1 — ID de evento
- cn2 — ID de transacción HTTP
- cs1 — nombre del perfil
- cs2 — ID de PPE (por ejemplo, PPE1)
- cs3 - ID de sesión
- cs4 — Gravedad (por ejemplo, INFO, ALERT)
- cs5 — año del evento
- cs6 - Categoría de infracción de firma
- method — Método (por ejemplo, GET/POST)

Por ejemplo, considere el siguiente mensaje de registro de formato CEF, que se generó cuando se desencadenó una infracción de URL de inicio:

```
Jun 12 23:37:17 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
   .0
|APPFW|APPFW_STARTURL|6|src=10.217.253.62 spt=47606 method=GET
request=http://aaron.stratum8.net/FFC/login.html msg=Disallow Illegal
   URL. cn1=1340
```



```
cn2=653 cs1=pr_ffc cs2=PPE1 cs3=EsdGd3VD0OaaURLcZnj05Y6DOmE0002 cs4=
    ALERT cs5=2015
act=blocked
<!--NeedCopy-->
```

El mensaje anterior se puede dividir en diferentes componentes. Consulte la tabla de componentes del registro CEP.

Ejemplo de una infracción de comprobación de solicitud en formato de registro CEF: La solicitud no está bloqueada

```
Jun 13 00:21:28 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
    .0|APPFW|
APPFW_FIELDCONSISTENCY|6|src=10.217.253.62 spt=761 method=GET request=
http://aaron.stratum8.net/FFC/login.php?login_name=abc&passwd=
123456789234&drinking_pref=on&text_area=&loginButton=ClickToLogin&
    as_sfid
=
    AAAAAAWIahZuYoIFbjBhYMP05mJLTwEfIY0a7AKGMg3jIBaKmwtK4t7M7lNxOgj7Gmd3SZc8KUj6CP

7W5kIWDRHN8PtK1Zc-txHkHNx1WknuG9DzTuM7t1THhluevXu9I4kp8%3D&as_fid=
    feeec8758b4174
0eedeeb6b35b85dfd3d5def30c msg=Field consistency check failed for field
     passwd cn1=1401
cn2=707 cs1=pr_ffc cs2=PPE1 cs3=Ycby5IvjL6FoVa6Ah94QFTIUpC80001 cs4=
    ALERT cs5=2015 act=
not blocked
<!--NeedCopy-->
```

Ejemplo de infracción de comprobación de respuestas en formato CEF: la respuesta se transforma

```
Jun 13 00:25:31 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
    .0|APPFW|
APPFW_SAFECOMMERCE|6|src=10.217.253.62 spt=34041 method=GET request=
http://aaron.stratum8.net/FFC/CreditCardMind.html msg=Maximum number of
     potential credit
card numbers seen cn1=1470 cn2=708 cs1=pr_ffc cs2=PPE1
cs3=Ycby5IvjL6FoVa6Ah94QFTIUpC80001 cs4=ALERT cs5=2015 act=transformed
<!--NeedCopy-->
```

Ejemplo de infracción de firma del lado de la solicitud en formato CEF: la solicitud está bloqueada


```
Jun 13 01:11:09 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
    .0|APPFW|
APPFW_SIGNATURE_MATCH|6|src=10.217.253.62 spt=61141 method=GET request=
http://aaron.stratum8.net/FFC/wwwboard/passwd.txt msg=Signature
    violation rule ID 807:
web-cgi /wwwboard/passwd.txt access  cn1=140 cn2=841 cs1=pr_ffc cs2=
    PPE0
cs3=OyTgjbXBqcpBFeENKDlde3OkMQ00001 cs4=ALERT cs5=2015 cs6=web-cgi act=
    blocked
<!--NeedCopy-->
```

Registrar la geolocalización en los mensajes de infracción de Web App Firewall

Los detalles del registro identifican la ubicación desde la que se originan las solicitudes y lo ayudan a configurar Web App Firewall para obtener el nivel de seguridad óptimo. Para evitar implementaciones de seguridad como la limitación de velocidad, que dependen de las direcciones IP de los clientes, el malware o los equipos no fiables pueden seguir cambiando la dirección IP de origen en las solicitudes. Identificar la región específica de la que provienen las solicitudes puede ayudar a determinar si las solicitudes provienen de un usuario válido o de un dispositivo que intenta lanzar ciberataques. Por ejemplo, si se recibe un número excesivamente elevado de solicitudes de un área específica, es fácil determinar si los usuarios o una máquina no autorizada las envían. El análisis de geolocalización del tráfico recibido puede ser útil para desviar ataques como los ataques de denegación de servicio (DoS).

Web App Firewall le ofrece la comodidad de utilizar la base de datos integrada de Citrix ADC para identificar las ubicaciones correspondientes a las direcciones IP desde las que se originan las solicitudes malintencionadas. A continuación, puede aplicar un mayor nivel de seguridad para las solicitudes de esas ubicaciones. Las expresiones de sintaxis (PI) predeterminadas de Citrix le brindan la flexibilidad de configurar directivas basadas en la ubicación que se pueden usar con la base de datos de ubicaciones integrada para personalizar la protección del firewall, lo que refuerza su defensa contra los ataques coordinados lanzados desde clientes no autorizados en una región específica.

Puede utilizar la base de datos integrada de Citrix ADC o cualquier otra base de datos. Si la base de datos no tiene ninguna información de ubicación para la dirección IP del cliente en particular, el registro CEF muestra la geolocalización como una geolocalización desconocida.

> **Nota:**
>
> El registro de geolocalización utiliza el formato de eventos comunes (CEF). De forma predeterminada, `CEF logging` y `GeoLocationLogging` están DESACTIVADOS. Debe habilitar explícitamente ambos parámetros.

Ejemplo de mensaje de registro CEF que muestra información de geolocalización


```
June 8 00:21:09 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
    .0|APPFW|
APPFW_STARTURL|6|src=10.217.253.62 geolocation=NorthAmerica.US.Arizona.
    Tucson.\*.\*
spt=18655 method=GET request=http://aaron.stratum8.net/FFC/login.html
msg=Disallow Illegal URL. cn1=77 cn2=1547 cs1=test_pr_adv cs2=PPE1
cs3=KDynjg1pbFtfhC/nt0rBU1o/Tyg0001 cs4=ALERT cs5=2015 act=not blocked
<!--NeedCopy-->
```

Ejemplo de mensaje de registro que muestra geolocation= Unknown

```
June 9 23:50:53 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
    .0|
APPFW|APPFW_STARTURL|6|src=10.217.30.251 geolocation=Unknown spt=5086
method=GET request=http://aaron.stratum8.net/FFC/login.html msg=
    Disallow Illegal URL.
cn1=74 cn2=1576 cs1=test_pr_adv cs2=PPE2 cs3=
    PyR0eOEM4gf6GJiTyauiHByL88E0002
cs4=ALERT cs5=2015 act=not blocked
<!--NeedCopy-->
```

Configurar la acción de registro y otros parámetros de registro mediante la interfaz de comandos

Para configurar la acción de registro para una comprobación de seguridad de un perfil mediante la línea de comandos

En el símbolo del sistema, escriba uno de los siguientes comandos:

- `set appfw profile <name> SecurityCheckAction ([log] | [none])`
- `unset appfw profile <name> SecurityCheckAction`

Ejemplos

```
set appfw profile pr_ffc StartURLAction log
```

```
unset appfw profile pr_ffc StartURLAction
```

Para configurar el registro CEF mediante la línea de comandos

El registro CEF está inhabilitado de forma predeterminada. En el símbolo del sistema, escriba uno de los comandos siguientes para cambiar o mostrar la configuración actual:

- `set appfw settings CEFLogging on`

- `unset appfw settings CEFLogging`
- `sh appfw settings | grep CEFLogging`

Para configurar el registro de los números de tarjetas de crédito mediante la línea de comandos

En el símbolo del sistema, escriba uno de los siguientes comandos:

- `set appfw profile <name> -doSecureCreditCardLogging ([ON] | [OFF])`
- `unset appfw profile <name> -doSecureCreditCardLogging`

Para configurar el registro de geolocalización mediante la línea de comandos

1. Utilice el comando set para habilitar GeoLocationLogging. Puede habilitar el registro CEF al mismo tiempo. Utilice el comando unset para inhabilitar el registro de geolocalización. El comando show muestra la configuración actual de todos los parámetros de Web App Firewall, a menos que incluya el comando grep para mostrar la configuración de un parámetro específico.

   - `set appfw settings GeoLocationLogging ON [CEFLogging ON]`
   - `unset appfw settings GeoLocationLogging`
   - `sh appfw settings | grep GeoLocationLogging`

2. Especificar la base de datos

   ```
   add locationfile /var/netscaler/inbuilt_db/Citrix_netscaler_InBuilt_GeoIP_DB
   .csv
   ```

   O bien:

   ```
   add locationfile <path to database file>
   ```

Personalizar registros de Web App Firewall

Las expresiones de formato predeterminado (PI) le dan la flexibilidad de personalizar la información incluida en los registros. Tiene la opción de incluir los datos específicos que quiere capturar en los mensajes de registro generados por Web App Firewall. Por ejemplo, si está usando la autenticación AAA-TM junto con las comprobaciones de seguridad de Web App Firewall y quiere saber la dirección URL a la que se ha accedido que desencadenó la infracción de comprobación de seguridad, el nombre del usuario que solicitó la dirección URL, la dirección IP de origen y el puerto de origen desde el que el usuario envió la solicitud, debe puede utilizar los siguientes comandos para especificar mensajes de registro personalizados que incluyan todos los datos:

```
1 > sh version
2 NetScaler NS12.1: Build 50.0013.nc, Date: Aug 28 2018, 10:51:08   (64-
     bit)
3  Done
4 <!--NeedCopy-->
```



```
> add audit messageaction custom1 ALERT 'HTTP.REQ.URL + " " + HTTP.REQ.
    USER.NAME + " " + CLIENT.IP.SRC + ":" + CLIENT.TCP.SRCPORT'
Warning: HTTP.REQ.USER has been deprecated. Use AAA.USER instead.
 Done
<!--NeedCopy-->
```

```
> add appfw profile test_profile
 Done
<!--NeedCopy-->
```

```
> add appfw policy appfw_pol true test_profile -logAction custom1
 Done
<!--NeedCopy-->
```

Configurar la directiva Syslog para segregar los registros de Web App Firewall

Web App Firewall le ofrece la opción de aislar y redirigir los mensajes de registro de seguridad de Web App Firewall a otro archivo de registros. Esto puede resultar deseable si Web App Firewall genera muchos registros, lo que dificulta la visualización de otros mensajes de registro de Citrix ADC. También puede utilizar esta opción si solo le interesa ver los mensajes de registro de Web App Firewall y no quiere ver los demás mensajes de registro.

Para redirigir los registros de Web App Firewall a un archivo de registros diferente, configure una acción syslog para enviar los registros de Web App Firewall a una instalación de registro diferente. Puede utilizar esta acción al configurar la directiva syslog y vincularla globalmente para que la use Web App Firewall.

> **Nota:**
>
> Para vincular de forma global las directivas de Web App Firewall, puede configurar el parámetro de enlace global, "APPFW_GLOBAL" en los comandos "bind audit syslogGlobal" y "bind audit nslogGlobal". Las directivas de registro de auditoría enlazadas globales pueden evaluar los mensajes de registro en el contexto de registro de Web App Firewall.

Ejemplo:

1. Cambie al shell y utilice un editor como vi para modificar el archivo /etc/syslog.conf. Agregue una nueva entrada para utilizar local2.* para enviar registros a un archivo independiente, como se muestra en el siguiente ejemplo:


```
local2.\* /var/log/ns.log.appfw
```

2. Reinicie el proceso syslog. Puede utilizar el comando grep para identificar el ID del proceso syslog (PID), como se muestra en el siguiente ejemplo:

```
root@ns\## **ps -A | grep syslog**

1063 ?? Ss 0:03.00 /usr/sbin/syslogd -b 127.0.0.1 -n -v -v -8 -C

root@ns## **kill -HUP** 1063
```

3. Desde la interfaz de línea de comandos, configure la directiva SYSLOG avanzada o clásica con la acción y enlácela como una directiva global de Web App Firewall. Citrix recomienda configurar la directiva SYSLOG avanzada.

   Configuración de directivas SYSLOG avanzada

```
add audit syslogAction sysact1 1.1.1.1 -logLevel ALL -logFacility
LOCAL2

add audit syslogPolicy syspol1 true sysact1

bind audit syslogGlobal -policyName syspol1 -priority 100 -globalBindType
 APPFW_GLOBAL
```

   Configuración de directivas SYSLOG clásica

```
add audit syslogAction sysact1 1.1.1.1 -logLevel ALL -logFacility
LOCAL2

add audit syslogPolicy syspol1 ns_true sysact1

bind appfw global syspol1 100
```

4. Todas las infracciones de las comprobaciones de seguridad de Web App Firewall ahora se redirigirán al archivo `/var/log/ns.log.appfw`. Puede seguir este archivo para ver las infracciones de Web App Firewall que se desencadenan durante el procesamiento del tráfico en curso.

```
root@ns## tail -f ns.log.appfw
```

Advertencia: Si ha configurado la directiva syslog para redirigir los registros a un recurso de registro diferente, los mensajes de registro de Web App Firewall ya no aparecerán en el archivo `/var/log/ns.log`.

> **Nota:**
>
> Si desea enviar registros a un archivo de registro diferente en el dispositivo Citrix ADC local, puede crear un servidor syslog en ese dispositivo Citrix ADC local. Agregue `syslogaction` a su propia IP y configure el ADC como configuraría un servidor externo. El ADC actúa como servidor para almacenar los registros. No se pueden agregar dos acciones con la misma IP y puerto. En `syslogaction`, de forma predeterminada, el valor de IP se establece en `127.0.0.1` y el valor

> de port se establece en 514.

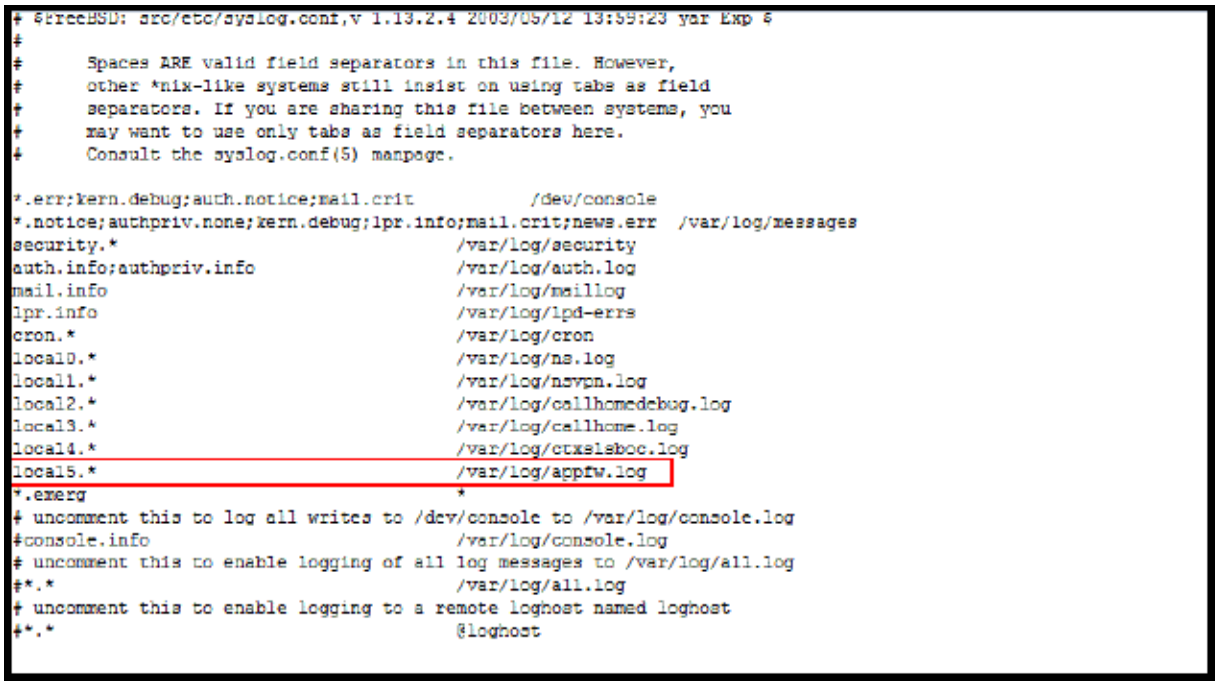
Enviar los mensajes de Application Firewall a un servidor SYSLOG independiente

Para enviar los mensajes de Application Firewall a un servidor SYSLOG independiente, debe completar los siguientes pasos:

- Una utilidad de transferencia de archivos segura como WinSCP
- Una utilidad para abrir una consola SSH en el dispositivo, como PuTTY

Los siguientes pasos están involucrados para enviar los mensajes de Application Firewall a un servidor SYSLOG independiente:

1. Inicie sesión en el dispositivo Citrix ADC a través de WinSCP.
2. Actualice el archivo /etc/syslog.conf y agregue esta línea en el archivo:
   `local5.* /var/log/appfw.log`

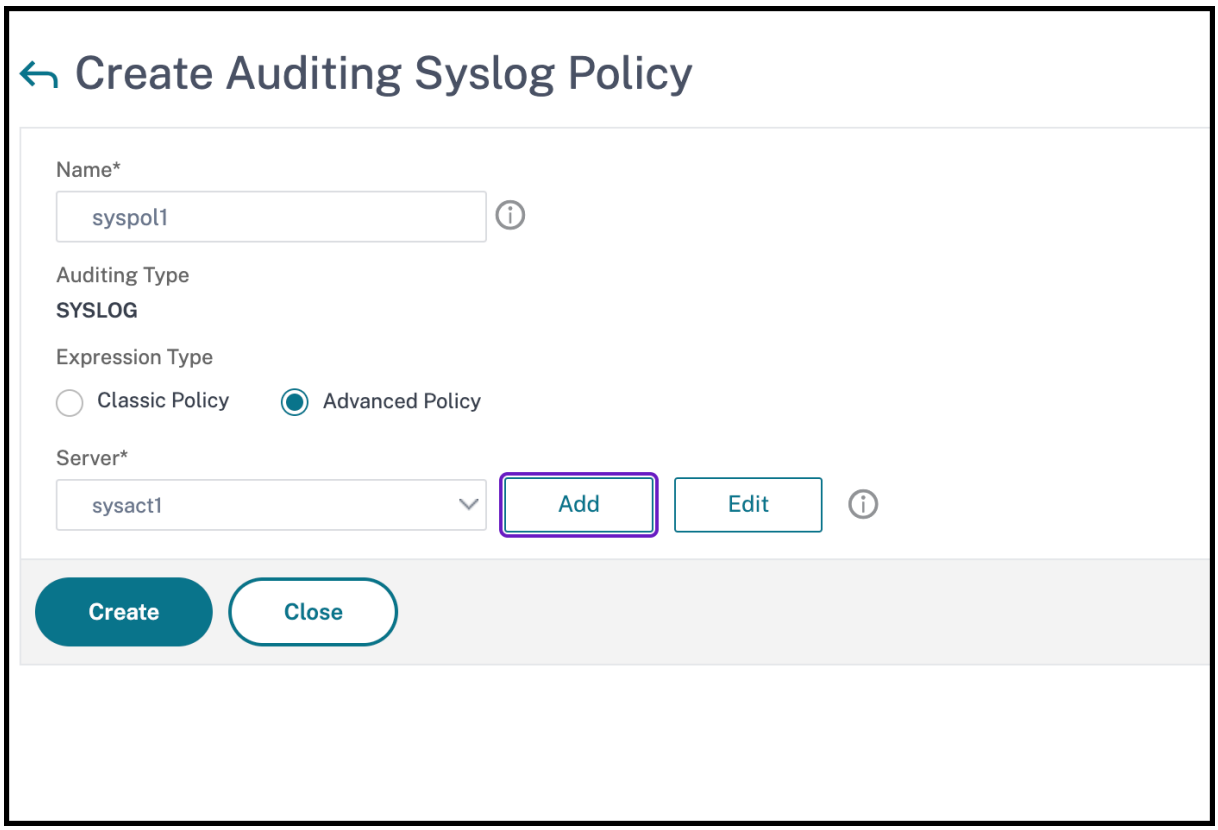


```
# $FreeBSD: src/etc/syslog.conf,v 1.13.2.4 2003/05/12 13:59:23 yar Exp $
#
#       Spaces ARE valid field separators in this file. However,
#       other *nix-like systems still insist on using tabs as field
#       separators. If you are sharing this file between systems, you
#       may want to use only tabs as field separators here.
#       Consult the syslog.conf(5) manpage.

*.err;kern.debug;auth.notice;mail.crit           /dev/console
*.notice;authpriv.none;kern.debug;lpr.info;mail.crit;news.err  /var/log/messages
security.*                                      /var/log/security
auth.info;authpriv.info                         /var/log/auth.log
mail.info                                       /var/log/maillog
lpr.info                                        /var/log/lpd-errs
cron.*                                          /var/log/cron
local0.*                                        /var/log/ns.log
local1.*                                        /var/log/nsvpn.log
local2.*                                        /var/log/callhomedebug.log
local3.*                                        /var/log/callhome.log
local4.*                                        /var/log/ctxsladoc.log
local5.*                                        /var/log/appfw.log
*.emerg                                         *
# uncomment this to log all writes to /dev/console to /var/log/console.log
#console.info                                   /var/log/console.log
# uncomment this to enable logging of all log messages to /var/log/all.log
#*.*                                            /var/log/all.log
# uncomment this to enable logging to a remote loghost named loghost
#*.*                                            @loghost
```

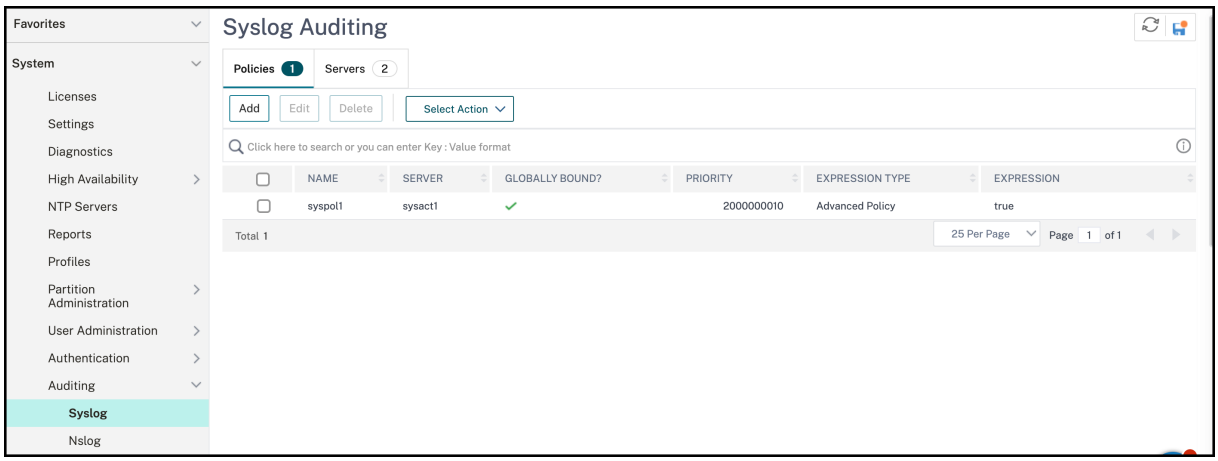
1. Ejecute el siguiente comando desde la interfaz de línea de comandos para reiniciar el PID de syslog:
   `kill -HUP <PID>`
2. Ejecute el siguiente comando desde la interfaz de línea de comandos para agregar una acción syslog como sysact1:
   `add audit syslogAction sysact1 127.0.0.1 -logLevel ALL -logFacility LOCAL5`

3. Ejecute el siguiente comando para agregar la directiva syspol1, que usa el servidor sysact1:
   ```
   add audit syslogPolicy syspol1 ns_true sysact1
   ```
   O bien agregue una directiva de syslog avanzada:
   ```
   add audit syslogPolicy syspol1 true sysact1
   ```



1. Ejecute el siguiente comando para vincular la directiva de Application Firewall y asegurarse de que se guarda en el archivo ns.conf:
   ```
   bind appfw global syspol1 100
   ```
   O bien, ejecute el siguiente comando para vincular la directiva de Syslog avanzada:

```
bind audit syslogGlobal -policyName syspol1 -priority 100 -globalBindType
APPFW_GLOBAL
```

Todas las infracciones de las comprobaciones de seguridad de Application Firewall se redirigen a `/var/log/appfw.log` y ya no aparecerán en `ns.log`. Ahora puede ejecutar el comando tail y ver las últimas entradas en `/var/log/appfw.log`.

Ver registros de Web App Firewall

Puede ver los registros mediante el visor de syslog o iniciando sesión en el dispositivo Citrix ADC, abriendo un shell de UNIX y mediante el editor de texto de UNIX de su elección.

Para acceder a los mensajes de registro mediante la línea de comandos

Cambie al shell y siga los ns.logs en la carpeta **/var/log/** para acceder a los mensajes de registro relacionados con las infracciones de comprobación de **seguridad de Web App Firewall**:

- `Shell`
- `tail -f /var/log/ns.log`

Puede utilizar el editor vi, o cualquier editor de texto Unix o herramienta de búsqueda de texto, para ver y filtrar los registros de entradas específicas. Por ejemplo, puede usar el comando `grep` para acceder a los mensajes de registro relacionados con las infracciones de tarjeta de crédito:

- `tail -f /var/log/ns.log | grep SAFECOMMERCE`

Para acceder a los mensajes de registro mediante la interfaz gráfica de usuario

La GUI de Citrix incluye una herramienta útil (Syslog Viewer) para analizar los mensajes de registro. Tiene varias opciones para acceder al Visor de Syslog:

- Para ver los mensajes de registro de una comprobación de seguridad específica de un perfil, vaya a **Web App Firewall** > **Perfiles**, seleccione el perfil de destino y haga clic en Comprobaciones de seguridad. Resalte la fila de la comprobación de seguridad de destino y haga clic en Registros. Cuando accede a los registros directamente desde la comprobación de seguridad seleccionada del perfil, filtra los mensajes de registro y muestra solo los registros relativos a las infracciones de la comprobación de seguridad seleccionada. El visor de syslog puede mostrar

registros de Web App Firewall en formato nativo y en formato CEF. Sin embargo, para que el visor de syslog filtre los mensajes de registro específicos del perfil de destino, los registros deben estar en el formato de registro CEF cuando se accede desde el perfil.

- También puede acceder al Visor de Syslog navegando a **Citrix ADC** > **Sistema** > **Auditoría**. En la sección Mensajes de auditoría, haga clic en el enlace Mensajes de Syslog para mostrar el Visor de Syslog, que muestra todos los mensajes de registro, incluidos todos los registros de infracciones de comprobación de seguridad de Web App Firewall para todos los perfiles. Los mensajes de registro son útiles para depurar cuando se pueden desencadenar varias infracciones de comprobación de seguridad durante el procesamiento de la solicitud.
- Vaya a **Web App Firewall** > **directivas** > **Auditoría**. En la sección Mensajes de auditoría, haga clic en el enlace Mensajes de Syslog para mostrar el Visor de Syslog, que muestra todos los mensajes de registro, incluidos todos los registros de infracciones de comprobación de seguridad para todos los perfiles.

Syslog Viewer basado en HTML proporciona las siguientes opciones de filtro para seleccionar solo los mensajes de registro que le interesan:

- **Archivo**: El archivo `/var/log/ns.log` actual se selecciona de forma predeterminada y los mensajes correspondientes aparecen en el Visor de Syslog. Una lista de otros archivos de registros en el directorio /var/log está disponible en formato comprimido .gz. Para descargar y descomprimir un archivo de registros archivado, seleccione el archivo de registros en la opción de la lista desplegable. Los mensajes de registro correspondientes al archivo seleccionado se muestran en el visor de syslog. Para actualizar la pantalla, haga clic en el icono Actualizar (un círculo de dos flechas).
- **Cuadro de lista de módulos**: puede seleccionar el módulo Citrix ADC cuyos registros quiere ver. Puede configurarlo en APPFW para los registros de Web App Firewall.
- **Cuadro de lista Tipo de evento**: este cuadro contiene un conjunto de casillas de verificación para seleccionar el tipo de evento que le interesa. Por ejemplo, para ver los mensajes de registro relativos a las infracciones de firma, puede seleccionar la casilla **APPFW_SIGNATURE_MATCH**. Del mismo modo, puede seleccionar una casilla de verificación para habilitar la comprobación de seguridad específica que le interese. Puede seleccionar varias opciones.
- **Gravedad**: puede seleccionar un nivel de gravedad específico para mostrar solo los registros de ese nivel de gravedad. Deje todas las casillas de verificación en blanco si quiere ver todos los registros.

  Para acceder a los mensajes de registro de infracciones de la comprobación de seguridad de Web App Firewall para una comprobación de seguridad específica, filtre seleccionando **APPFW** en las opciones de la lista desplegable para el módulo. El tipo de evento muestra un amplio conjunto de opciones para refinar aún más la selección. Por ejemplo, si selecciona la casilla **APPFW_FIELDFORMAT** y hace clic en el botón Aplicar, en Syslog Viewer solo aparecerán los mensajes de registro relacionados con las infracciones de comprobación de seguridad de

formatos de campo. Del mismo modo, si selecciona las casillas de verificación **APPFW_SQLy APPFW_STARTURL** y hace clic en el botón **Aplicar**, solo los mensajes de registro relacionados con estas dos infracciones de comprobación de seguridad aparecerán en el visor de syslog.

Si coloca el cursor en la fila de un mensaje de registro específico, se muestran varias opciones, como **Module**, **EventType**, **EventID**o **Message** debajo del mensaje de registro. Puede seleccionar cualquiera de estas opciones para resaltar la información correspondiente en los registros.

Resumen

- **Compatibilidad con el formato de registro**CEF: la opción de formato de registro CEF proporciona una opción conveniente para supervisar, analizar y analizar los mensajes de registro de Web App Firewall para identificar ataques, ajustar la configuración con precisión para reducir los falsos positivos y recopilar estadísticas.
- **Opción para personalizar el mensaje de registro**: puede utilizar expresiones PI avanzadas para personalizar los mensajes de registro e incluir los datos que quiere ver en los registros.
- **Segregar registros específicos de Web App Firewall**: tiene la opción de filtrar y redirigir los registros específicos del firewall de aplicaciones a un archivo de registros independiente.
- **Registro remoto**: puede redirigir los mensajes de registro a un servidor syslog remoto.
- **Registro de geolocalización**: puede configurar Web App Firewall para incluir la geolocalización del área desde la que se recibe la solicitud. Hay disponible una base de datos de geolocalización integrada, pero tiene la opción de utilizar una base de datos de geolocalización externa. El dispositivo Citrix ADC admite bases de datos de geolocalización estática IPv4 e IPv6.
- **Mensaje de registro rico en información**: a continuación se muestran algunos ejemplos del tipo de información que se puede incluir en los registros, según la configuración:
  - Se activó una directiva de Web App Firewall.
  - Se ha desencadenado una infracción de la comprobación de seguridad.
  - Se consideró que una solicitud estaba mal formada.
  - Se ha bloqueado o no se ha bloqueado una solicitud o una respuesta.
  - Se han transformado los datos de solicitud (como caracteres especiales de scripts SQL o de scripts de sitios) o datos de respuesta (como números de tarjetas de crédito o cadenas de objetos seguros).
  - El número de tarjetas de crédito de la respuesta superó el límite configurado.
  - Número y tipo de tarjeta de crédito.
  - Las cadenas de registro configuradas en las reglas de firma y el ID de firma.
  - Información de geolocalización sobre el origen de la solicitud.
  - Entrada de usuario enmascarada (eliminada) para campos confidenciales protegidos.

Enmascarar datos confidenciales mediante un patrón de expresiones

La función de directiva avanzada REGEX_REPLACE (PI) en una expresión de registro (vinculada a un perfil de firewall de aplicaciones web (WAF)) le permite enmascarar datos confidenciales en registros WAF. Puede utilizar la opción para enmascarar los datos mediante un patrón de expresiones regulares y proporcionar un carácter o un patrón de cadena para enmascarar los datos. Además, puede configurar la función PI para reemplazar la primera aparición o todas las apariciones del patrón de expresiones regulares.

De forma predeterminada, la interfaz GUI de Citrix proporciona la siguiente máscara:

- SSN
- Tarjeta de crédito
- Contraseña
- Nombre de usuario

Enmascarar datos confidenciales en los registros de firewall de aplicaciones web

Puede enmascarar datos confidenciales en registros WAF configurando la expresión de directiva avanzada REGEX_REPLACE en la expresión de registro enlazada a un perfil WAF.
Para enmascarar datos confidenciales, debe completar los siguientes pasos:

1. Agregar un perfil de Firewall de aplicaciones web
2. Enlazar una expresión de registro al perfil WAF

Agregar un perfil de Firewall de aplicaciones web

En el símbolo del sistema, escriba:

```
add appfw profile <name>
```

Ejemplo:

```
Add appfw profile testprofile1
```

Enlazar una expresión de registro con el perfil de Web Application Firewall

En el símbolo del sistema, escriba:

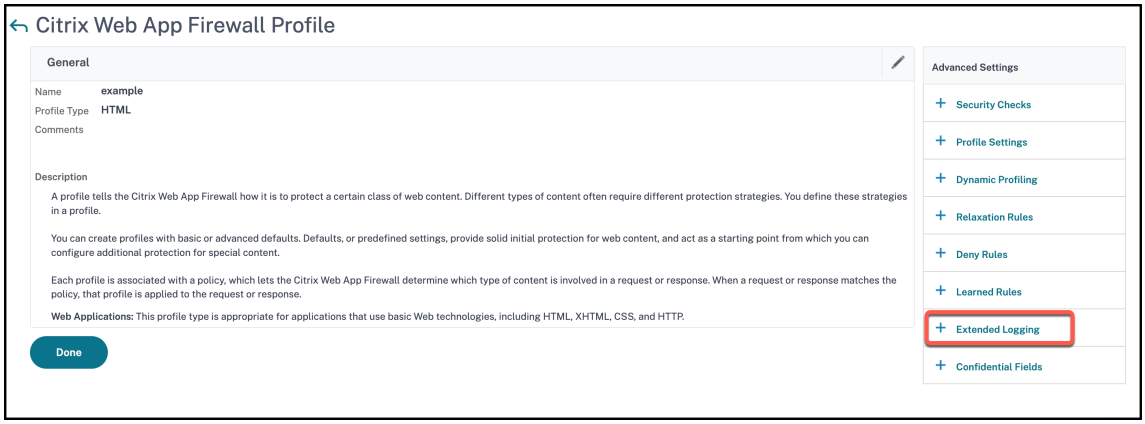
```
bind appfw profile <name> -logExpression <string> <expression> -comment <
string>
```

Ejemplo:

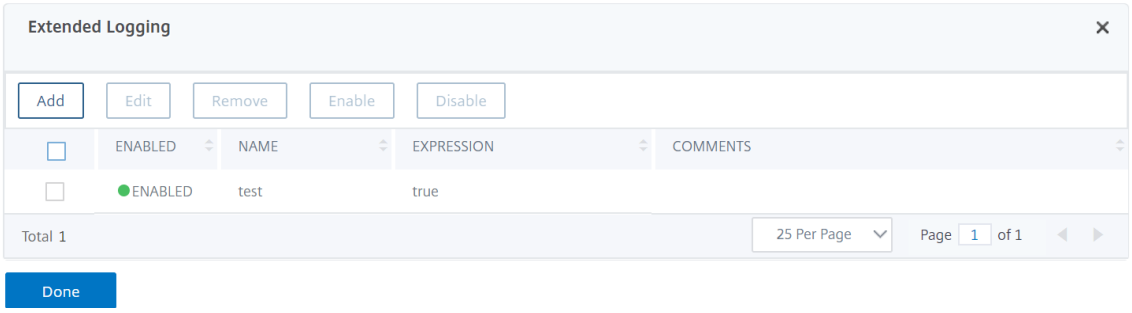
```
bind appfw profile testProfile -logExpression ”MaskSSN””HTTP.REQ.BODY
(10000).REGEX_REPLACE(re!\b\d{ 3 } -\d{ 2 } -\d{ 4 } \b!, “xxx” , ALL)”-
comment ”SSN Masked”
```


Enmascarar datos confidenciales en los registros de Web Application Firewall mediante la GUI de Citrix ADC

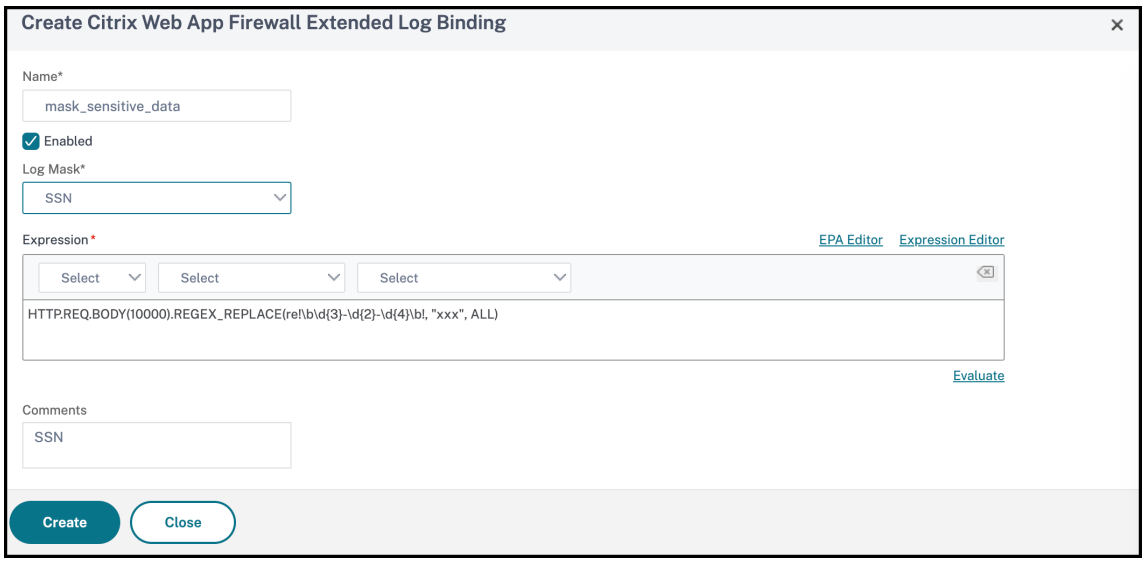
1. En el panel de navegación, expanda **Seguridad** > **Citrix Web App Firewall** > **Perfiles**.
2. En la página **Perfiles**, haga clic en **Modificar**.
3. En la página **Perfil de Citrix Web App Firewall**, vaya a la sección **Configuración avanzada** y haga clic en **Registro extendido**.



4. En la sección **Registro extendido**, haga clic en **Agregar**.



5. En la página **Crear enlace de registro extendido de Citrix Web App Firewall**, defina los siguientes parámetros:
   a) Nombre. Nombre de la expresión de registro.
   b) Habilitada. Seleccione esta opción para enmascarar los datos confidenciales.
   c) Máscara de troncos. Seleccione los datos que se van a enmascarar.
   d) Expresión. Introduzca la expresión de directiva avanzada que le permite enmascarar datos confidenciales en los registros WAF
   e) Comentarios. Breve descripción del enmascaramiento de datos confidenciales.
6. Haga clic en **Crear** y **cerrar**.



Apéndices

January 12, 2021

El siguiente material complementario proporciona detalles adicionales sobre las tareas complejas o periféricas de Web App Firewall.

Formato de codificación de caracteres PCRE

August 20, 2021

El **sistema operativo Citrix ADC solo admite la entrada directa** de caracteres en el conjunto de caracteres ASCII imprimible, caracteres con códigos hexadecimales entre HEX 20 (ASCII 32) y HEX 7E (ASCII 127). Para incluir un carácter con un código fuera de ese rango en la configuración de Web App Firewall, debe escribir su código hexadecimal UTF-8 como expresión regular PCRE.

Muchos tipos de caracteres requieren codificación mediante una expresión regular PCRE si los incluye en la configuración de Web App Firewall como una dirección URL, un nombre de campo de formulario o una expresión de objeto seguro. Entre ellas figuran:

- **Caracteres ASCII superior.** Caracteres con codificaciones de HEX 7F (ASCII 128) a HEX FF (ASCII 255). Dependiendo del mapa de caracteres utilizado, estas codificaciones pueden referirse a códigos de control, caracteres ASCII con acentos u otras modificaciones, caracteres alfabéticos no latinos y símbolos no incluidos en el conjunto ASCII básico. Estos caracteres pueden aparecer en direcciones URL, nombres de campos de formulario y expresiones de objetos seguros.

- **Caracteres de doble byte.** Caracteres con codificaciones que utilizan dos palabras de 8 bytes. Los caracteres de doble byte se utilizan principalmente para representar texto chino, japonés y coreano en formato electrónico. Estos caracteres pueden aparecer en direcciones URL, nombres de campos de formulario y expresiones de objetos seguros.

  Caracteres de control ASCII. Caracteres no imprimibles utilizados para enviar comandos a una impresora. Todos los caracteres ASCII con códigos hexadecimales menores a HEX 20 (ASCII 32) entran en esta categoría. Sin embargo, estos caracteres nunca deben aparecer en una dirección URL o en un nombre de campo de formulario y rara vez aparecerán en una expresión de objeto segura.

El dispositivo Citrix ADC no admite todo el conjunto de caracteres UTF-8, sino solo los caracteres que se encuentran en los ocho conjuntos de caracteres siguientes:

- **Inglés EE. UU. (ISO-8859-1).** Aunque la etiqueta dice "Inglés EE. UU.", Web App Firewall admite todos los caracteres del conjunto de caracteres ISO-8859-1, también llamado conjunto de caracteres Latin-1. Este conjunto de caracteres representa completamente la mayoría de las lenguas europeas occidentales modernas y representa todos menos algunos caracteres poco comunes en el resto.
- **Chino tradicional (Big5).** El Web App Firewall admite todos los caracteres del conjunto de caracteres BIG5, que incluye todos los caracteres chinos tradicionales (ideogramas) comúnmente utilizados en chino moderno como hablado y escrito en Hong Kong, Macao, Taiwán, y por muchas personas de herencia étnica china que viven fuera de China continental.
- **Chino simplificado (GB2312).** El Web App Firewall admite todos los caracteres del juego de caracteres GB2312, que incluye todos los caracteres chinos simplificados (ideogramas) comúnmente utilizados en chino moderno como hablados y escritos en China continental.
- **Japonés (SJIS).** El Web App Firewall admite todos los caracteres del conjunto de caracteres Shift-JIS (SJIS), que incluye la mayoría de los caracteres (ideogramas) utilizados comúnmente en el japonés moderno.
- **japonés (EUC-JP).** El Web App Firewall admite todos los caracteres del conjunto de caracteres EUC-JP, que incluye todos los caracteres (ideogramas) utilizados comúnmente en el japonés moderno.
- **Coreano (EUC-KR).** El Web App Firewall admite todos los caracteres del conjunto de caracteres EUC-KR, que incluye todos los caracteres (ideogramas) utilizados comúnmente en coreano moderno.
- **Turco (ISO-8859-9).** El Web App Firewall admite todos los caracteres del conjunto de caracteres ISO-8859-9, que incluye todas las letras utilizadas en el turco moderno.
- **Unicode (UTF-8).** El Web App Firewall admite ciertos caracteres más en el conjunto de caracteres UTF-8, incluidos los utilizados en ruso moderno.

Al configurar Web App Firewall, escriba todos los caracteres que no sean ASCII como expresiones regulares de formato PCRE-con el código hexadecimal asignado a ese carácter en la especificación UTF-8. A los símbolos y caracteres del juego de caracteres ASCII normal, al que se le asignan códigos sencillos y de dos dígitos en ese juego de caracteres, se les asignan los mismos códigos en el juego de caracteres UTF-8. Por ejemplo, el signo de exclamación (!), al que se le asigna el código hexadecimal 21 en el juego de caracteres ASCII, también es hexadecimal 21 en el juego de caracteres UTF-8. Los símbolos y caracteres de otro juego de caracteres admitido tienen asignado un conjunto emparejado de códigos hexadecimales en el juego de caracteres UTF-8. Por ejemplo, a la letra a con acento agudo (á) se le asigna el código UTF-8 C3 A1.

La sintaxis que se utiliza para representar estos códigos UTF-8 en la configuración de Web App Firewall es "\ xNN" para caracteres ASCII; "\ xNN\ xNN" para caracteres no ASCII utilizados en inglés, ruso y turco; y "\ xNN\ xNN\ xNN" para caracteres utilizados en chino, japonés y coreano. Por ejemplo, si quiere representar un! en una expresión regular de Web App Firewall como un carácter UTF-8, escriba \x21. Si quiere incluir una á, escriba \xC3\xA1.

> **Nota:**
>
> Normalmente no es necesario representar caracteres ASCII en formato UTF-8, pero cuando esos caracteres pueden confundir un explorador web o un sistema operativo subyacente, puede usar la representación UTF-8 del personaje para evitar esta confusión. Por ejemplo, si una dirección URL contiene un espacio, es posible que quiera codificar el espacio como x20 para evitar confundir ciertos exploradores y software de servidor web.

A continuación se muestran ejemplos de direcciones URL, nombres de campos de formulario y expresiones de objetos seguros que contienen caracteres no ASCII que deben escribirse como expresiones regulares de formato PCRE-para incluirlos en la configuración de Web App Firewall. Cada ejemplo muestra primero la dirección URL real, el nombre de campo o la cadena de expresión, seguida de una expresión regular de formato PCRE-para ello.

- Una URL que contiene caracteres ASCII extendidos.

  URL real: URL`http://www.josénuñez.com`
  codificada:`^http://www\[.\]jos\\xC3\\xA9nu\\xC3\\xB1ez\[.\]com$`

- Otra URL que contiene caracteres ASCII extendidos.

  URL real: URL`http://www.example.de/trömso.html`
  codificada:`^http://www[.]example[.\]de/tr\xC3\xB6mso[.]html$`

  Nombre de campo de formulario que contiene caracteres ASCII extendidos.

  Nombre real: Nome_do_usuário Nombre
  codificado: ^nome_do_usu\ xC3\ xA1rio$

- Expresión de objeto seguro que contiene caracteres ASCII extendidos.

Expresión sin codificar [A-Z]{3,6} ¥[1-9\][0-9]{6,6} Expresión codificada: [A-Z]{3,6}\ xC2\ xA5 [1-9] [0-9] {6,6}

Puede encontrar varias tablas que incluyen todo el conjunto de caracteres Unicode y codificaciones UTF-8 coincidentes en Internet. Un sitio web útil que contiene esta información está disponible en la siguiente tabla.

http://www.utf8-chartable.de/unicode-utf8-table.pl

Para que los caracteres de la tabla de este sitio web se muestren correctamente, debe tener instalada en el equipo una fuente Unicode adecuada. Si no lo hace, la visualización visual del carácter puede ser un error. Aunque no tenga instalada una fuente adecuada para mostrar un carácter, la descripción y los códigos UTF-8 y UTF-16 en este conjunto de páginas web son correctos.

Tipos de firma WASC de Whitehat para uso WAF

August 20, 2021

Citrix Web App Firewall acepta y genera reglas de bloqueo para todos los tipos de vulnerabilidades que generan los analizadores de Whitehat. Sin embargo, ciertas vulnerabilidades son más aplicables a un firewall de aplicaciones web. A continuación se presentan listas de esas vulnerabilidades, clasificadas según los tipos de firma de WASC 1.0, WASC 2.0 o prácticas recomendadas.

Tipos de firma WASC 1.0

- Contrabando de solicitudes HTTP
- División de respuesta HTTP
- Contrabando de respuesta HTTP
- Inyección de bytes nulos
- Inclusión remota de archivos
- Abuso del redirector de URL

Tipos de firma WASC 2.0

- Abuso de funcionalidad
- Fuerza bruta
- Suplantación de contenido
- Denegación de servicio
- Indexación de directorios
- Fuga de información
- Antiautomatización insuficiente

- Autenticación insuficiente
- Autorización insuficiente
- Vencimiento insuficiente de la sesión
- Inyección LDAP
- Fijación de Sesión

Prácticas recomendadas

- Atributo de autocompletar
- Control de acceso a cookies insuficiente
- Intensidad insuficiente de la contraseña
- Uso del método HTTP no válido
- Cookie de sesión no HTTPOnly
- Cookie de sesión persistente
- Información de identificación personal
- Mensajes HTTP protegidos en caché
- Cookie de sesión no segura

Función de streaming para el procesamiento de solicitudes

February 19, 2022

Citrix Web App Firewall admite la transmisión en el lado de solicitudes para proporcionar un aumento significativo del rendimiento. En lugar de almacenar en búfer una solicitud, el dispositivo examina el tráfico entrante en busca de infracciones de seguridad, como SQL, scripts entre sitios, consistencia de campos y formatos de campo. Cuando el dispositivo completa el procesamiento de datos de un campo, la solicitud se reenvía al servidor back-end mientras el dispositivo continúa evaluando otros campos. Este procesamiento de datos mejora significativamente el tiempo de procesamiento en formularios de manejo tienen muchos campos.

Citrix recomienda habilitar el streaming para el contenido de carga útil de más de 20 MB. Además, el servidor back-end debe aceptar las solicitudes fragmentadas si la transmisión está habilitada.

> **Nota:**
>
> La acción Post Body Limit siempre está configurada para bloquear y es aplicable tanto para los modos de transmisión como sin transmisión. Si el tráfico entrante supera los 20 MB, Citrix recomienda configurar `PostBodyLimit` en el valor esperado.

Aunque el proceso de transmisión es transparente para los usuarios, se requieren pequeños ajustes de configuración debido a los siguientes cambios:

RegEx Pattern Match: la coincidencia de patrones RegEx ahora está restringida a 4K para la coincidencia de cadenas de caracteres contiguos.

Coincidencia de nombre de campo: el motor de aprendizaje de Web App Firewall solo puede distinguir los primeros 128 bytes del nombre. Si un formulario tiene varios campos con nombres que tienen una coincidencia de cadena idéntica para los primeros 128 bytes, el motor de aprendizaje no los distingue. Del mismo modo, la regla de relajación implementada podría relajar inadvertidamente todos esos campos.

La eliminación de espacios en blanco, la decodificación porcentual, la decodificación Unicode y la conversión de juego de caracteres se realizan durante la canonización para proporcionar una inspección de comprobación de seguridad. El límite de 128 bytes es aplicable a la representación canonizada del nombre del campo en formato de caracteres UTF-8. Los caracteres ASCII tienen una longitud de 1 byte, pero la representación UTF-8 de los caracteres en algunos idiomas internacionales puede variar de 1 byte a 4 bytes. Si cada carácter de un nombre requiere 4 bytes para convertirse a formato UTF-8, solo los primeros 32 caracteres del nombre pueden distinguirse por la regla aprendida.

Comprobación de coherencia de campos: cuando habilita la coherencia de campos, todos los formularios de la sesión se almacenan en función de la etiqueta “as_fid” insertada por Web App Firewall sin tener en cuenta la “action_url”.

- **Etiquetado obligatorio de formulario para coherencia de campo de formulario:** cuando la comprobación de coherencia de campo está habilitada, la etiqueta de formulario también debe estar habilitada. Es posible que la protección de coherencia de campo no funcione si el etiquetado de formularios está desactivado.
- **Consistencia de campos de formulario sin sesión:** Web App Firewall ya no lleva a cabo la conversión de formularios “GET” a “POST” cuando el parámetro de coherencia de campos sin sesión está habilitado. La etiqueta de formulario también es necesaria para la coherencia de los campos sin sesión.
- **Manipulación de as_fid:** Si un formulario se envía después de manipular as_fid, desencadena una infracción de consistencia del campo incluso si no se ha alterado ningún campo. En las solicitudes que no son de transmisión, esto se permitió porque los formularios se pueden validar con la “action_url” almacenada en la sesión.

Firmas: Las firmas ahora tienen las siguientes especificaciones:

- **Ubicación:** Ahora es un requisito obligatorio que la ubicación debe especificarse para cada patrón. Todos los patrones de la regla **DEBE** tener una etiqueta `<Location>`.
- **Coincidencia rápida:** Todas las reglas de firma deben tener un patrón de coincidencia rápida. Si no hay un patrón de coincidencia rápida, se intenta seleccionar uno si es posible. La coincidencia rápida es una cadena literal, pero `PCRE` se puede usar para la coincidencia rápida si contienen una cadena literal utilizable.
- **Ubicaciones en desuso:** las siguientes ubicaciones ya no son compatibles con las reglas de

firma.

- HTTP_ANY
- HTTP_RAW_COOKIE
- HTTP_RAW_HEADER
- HTTP_RAW_RESP_HEADER
- HTTP_RAW_SET_COOKIE

Script entre sitios/SQL Transform: Los datos sin procesar se utilizan para la transformación porque los caracteres especiales de SQL como comillas simples (‘), barra invertida (\) y punto y coma (;) y las etiquetas de scripts entre sitios son los mismos y no requieren la canonización de los datos. La representación de caracteres especiales como codificación de entidades HTML, codificación porcentual o ASCII se evalúa para la operación de transformación.

Web App Firewall ya no inspecciona el nombre y el valor del atributo para la operación de transformación de scripts entre sitios. Ahora solo se transforman los nombres de atributos de scripting entre sitios cuando se activa la transmisión.

Procesamiento de etiquetas de scripts entre sitios: como parte de los cambios de streaming en la compilación de NetScaler 10.5.e y versiones posteriores, el procesamiento de las etiquetas de scripts entre sitios ha cambiado. En versiones anteriores, la presencia de corchetes abiertos (<), or close bracket (>) o de ambos corchetes abiertos y cerrados (<>) se marcaba como infracción de scripts entre sitios. El comportamiento ha cambiado en la compilación 10.5.e en adelante. La presencia del carácter de corchete abierto (<) o del carácter de corchete cerrado (>) ya no se considera un ataque. Esto es cuando un carácter de corchete de apertura (<) va seguido de un carácter de corchete de cierre (>), se detecta el ataque de scripting entre sitios. Ambos caracteres deben estar presentes en el orden correcto (< seguido de >) para activar la infracción de scripts entre sitios.

> **Nota:**
>
> **Mensaje de cambio en el registro de infracciones de SQL:** Como parte de los cambios de transmisión en la versión 10.5.e de Citrix ADC en adelante, ahora procesamos los datos de entrada en bloques. La coincidencia de patrones RegEx ahora está restringida a 4K para la coincidencia de cadenas de caracteres contiguos. Con este cambio, los mensajes de registro de infracciones SQL pueden incluir información diferente en comparación con las compilaciones anteriores. La palabra clave y el carácter especial de la entrada están separados por muchos bytes. El dispositivo tiene un seguimiento de las palabras clave SQL y cadenas especiales al procesar los datos, en lugar de almacenar en búfer todo el valor de entrada. Además del nombre del campo, el mensaje de registro incluye la palabra clave SQL, el carácter especial SQL o tanto la palabra clave SQL como el carácter especial SQL. El resto de la entrada ya no se incluye en el mensaje de registro, como se muestra en el ejemplo siguiente:
>
> **Ejemplo:**

> En 10.5, cuando Web App Firewall detecta la infracción de SQL, la cadena de entrada completa podría incluirse en el siguiente mensaje de registro:
>
> Error en la comprobación de palabras clave SQL para **text=”select a name from testbed1\;\(\;\)”.*<blocked>**
>
> En 11.0, registramos solo el nombre del campo, la palabra clave y el carácter especial (si corresponde) en el siguiente mensaje de registro.
>
> Error en la comprobación de palabras clave SQL para el campo `text=”select(;)”<blocked>`
>
> Este cambio se aplica a las solicitudes que contienen **application/x-www-form-urlencoded**, **multipart/form-data** o **text/x-gwt-rpc** content-types. Los mensajes de registro generados durante el procesamiento de cargas útiles **JSON** o **XML** no se ven afectados por este cambio.

Cuerpo RAW POST: Las inspecciones de control de seguridad siempre se realizan en el cuerpo RAW POST.

ID de formulario: Web App Firewall insertó la etiqueta “as_fid”, que es un hash calculado del formulario que ya es único para la sesión del usuario. Es un valor idéntico para un formulario específico, independientemente del usuario o de la sesión.

Juego de caracteres: si una solicitud no tiene un juego de caracteres, el juego de caracteres predeterminado especificado en el perfil de la aplicación se utiliza al procesar la solicitud.

Contadores:

Se agregan contadores con un prefijo “se” y “appfwreq” para rastrear los contadores de solicitudes del motor de transmisión y del motor de transmisión.

```
nsconsmg -d statswt0 -g se_err_
nsconsmg -d statswt0 -g se_tot_
nsconsmg -d statswt0 -g se_cur_
nsconsmg -d statswt0 -g appfwreq_err_
nsconsmg -d statswt0 -g appfwreq_tot_
nsconsmg -d statswt0 -g appfwreq_cur_
```

`_err counters`: indica el evento raro que debe haber tenido éxito pero falló debido a un problema de asignación de memoria o alguna otra crisis de recursos.

`_tot counters`: contadores cada vez mayores.

`_cur counters`: contadores que indican valores actuales que siguen cambiando según el uso de las transacciones actuales.

Sugerencias:

- Las comprobaciones de seguridad de Web App Firewall deben funcionar igual que antes.

- No hay ningún orden establecido para el procesamiento de los controles de seguridad.
- El procesamiento del lado de respuesta no se ve afectado y permanece sin cambios.
- La transmisión no se activa si se utiliza VPN sin cliente.

> **Importante:**
>
> **Calcular la longitud de la cookie:** en la versión 10.5.e, además de la versión 11.0 de Citrix ADC (en compilaciones anteriores a la 65.x), se cambió la forma en que Web App Firewall procesaba el encabezado de la cookie. El dispositivo evaluó la cookie individualmente y, si la longitud de una cookie en el encabezado de la cookie excedió la longitud configurada, se activó la infracción de desbordamiento de búfer. Como resultado, es posible que se permitan solicitudes bloqueadas en la versión 10.5 de NetScaler o en versiones anteriores. La longitud de todo el encabezado de la cookie no se calcula para determinar la longitud de la cookie. En algunas situaciones, el tamaño total de la cookie puede ser mayor que el valor aceptado, y el servidor puede responder con "400 Bad Request".
>
> **Nota:**
> El cambio se ha revertido. El comportamiento de NetScaler versión 10.5.e a la versión 59.13xx.e y sus compilaciones posteriores es similar a las compilaciones no mejoradas de la versión 10.5. Ahora se tiene en cuenta todo el encabezado de Cookie sin procesar al calcular la longitud de la cookie. Los espacios circundantes y los caracteres de punto y coma (;) que separan los pares nombre-valor también se incluyen para determinar la longitud de la cookie.

Seguimiento de solicitudes HTML con registros de seguridad

August 20, 2021

> **Nota:**
>
> Esta función está disponible en Citrix ADC versión 10.5.e.

La solución de problemas requiere el análisis de los datos recibidos en la solicitud del cliente y puede ser un reto. Especialmente si hay tráfico pesado que fluye a través del dispositivo. El diagnóstico de problemas puede afectar a la funcionalidad o la seguridad de la aplicación puede requerir una respuesta rápida.

Citrix ADC aísla el tráfico de un perfil de Web App Firewall y lo recopila `nstrace` para las solicitudes HTML. El `nstrace` recopilado en modo appfw incluye detalles de solicitud con mensajes de registro. Puede utilizar "Follow TCP stream" en el seguimiento para ver los detalles de la transacción individual, incluidos los encabezados, la carga útil y el mensaje de registro correspondiente en la misma pantalla.

Esto le ofrece una visión general completa sobre su tráfico. Tener una vista detallada de la solicitud, la carga útil y los registros asociados puede ser útil para analizar la infracción de comprobación de

seguridad. Puede identificar fácilmente el patrón que está desencadenando la infracción. Si se debe permitir el patrón, puede tomar la decisión de modificar la configuración o agregar una regla de relajación.

Ventajas

1. **Aislar tráfico para un perfil específico**: Esta mejora resulta útil cuando se aísla tráfico para un solo perfil o transacciones específicas de un perfil para solucionar problemas. Ya no tiene que revisar todos los datos recopilados en el rastreo o necesita filtros especiales para aislar las solicitudes que le interesan, lo que puede ser tedioso con el tráfico pesado. Puede ver los datos que prefiera.
2. **Recopilar datos para solicitudes específicas**: El seguimiento se puede recopilar durante una duración determinada. Puede recopilar seguimiento solo para un par de solicitudes para aislar, analizar y depurar transacciones específicas si es necesario.
3. **Identificar restablecencias o anulaciones**: el cierre inesperado de las conexiones no es fácil de ver. La traza recopilada en el modo —appfw captura un reinicio o un aborto, desencadenado por el Web App Firewall. Esto permite un aislamiento más rápido de un problema cuando no aparece un mensaje de infracción de comprobación de seguridad. Las solicitudes mal formadas u otras solicitudes no compatibles con RFC terminadas por Web App Firewall ahora serán más fáciles de identificar.
4. **Ver tráfico SSL descifrado**: El tráfico HTTPS se captura en texto sin formato para facilitar la solución de problemas.
5. **Proporciona una vista completa**: Le permite ver toda la solicitud en el nivel de paquete, comprobar la carga útil, mirar los registros para comprobar qué infracción de comprobación de seguridad se está desencadenando e identificar el patrón de coincidencia en la carga útil. Si la carga se compone de datos inesperados, cadenas no deseadas o caracteres no imprimibles (carácter nulo,\ r o\ n, etc.), son fáciles de descubrir en la traza.
6. **Modificar configuración**: la depuración puede proporcionar información útil para decidir si el comportamiento observado es el correcto o si la configuración debe modificarse.
7. **Acelerar el tiempo de respuesta**: una depuración más rápida del tráfico objetivo puede mejorar el tiempo de respuesta para proporcionar explicaciones o análisis de causa raíz por parte del equipo de ingeniería y soporte de Citrix.

Para obtener más información, consulte Configuración manual mediante el tema de la interfaz de línea de comandos .

Para configurar el seguimiento de depuración para un perfil mediante la interfaz de línea de comandos

Paso 1. Habilitar seguimiento ns.

Puede utilizar el comando show para verificar la configuración configurada.

- `set appfw profile <profile> -trace ON`

Paso 2. Recoge rastros. Puede seguir mediante todas las opciones que son aplicables para el `nstrace` comando.

- `start nstrace -mode APPFW`

Paso 3: Detén el rastro.

- `stop nstrace`

Ubicación de la traza: El `nstrace` se almacena en una carpeta con sello de tiempo que se crea en el directorio /var/nstrace y se puede ver mediante `wireshark`. Puede seguir el `/var/log/ns.log` para ver los mensajes de registro que proporcionan detalles sobre la ubicación de la nueva traza.

Sugerencias:

- Cuando se utiliza la opción de modo appfw, el solo `nstrace` recogerá los datos de uno o más perfiles para los que se habilitó el "nstrace".
- Habilitar el seguimiento en el perfil no comenzará a recopilar automáticamente los rastros hasta que ejecute explícitamente el comando "start ns trace" para recopilar el seguimiento.
- Aunque la habilitación de seguimiento en un perfil puede no tener ningún efecto adverso en el rendimiento del Web App Firewall, pero puede que quiera habilitar esta función solo durante el tiempo durante el que quiera recopilar los datos. Se recomienda desactivar el indicador —trace después de haber recopilado el seguimiento. La opción evita el riesgo de obtener datos inadvertidamente de los perfiles para los que había habilitado este indicador en el pasado.
- La acción de bloque o registro debe estar habilitada para que la comprobación de seguridad del registro de transacción se incluya en `nstrace`.
- Los restabres y los abortos se registran independientemente de las acciones de comprobación de seguridad cuando el seguimiento está "On" para los perfiles.
- La función solo es aplicable para solucionar problemas de las solicitudes recibidas del cliente. Los rastros en el modo —appfw no incluyen las respuestas recibidas del servidor.
- Puede seguir mediante todas las opciones que son aplicables para el `nstrace` comando. Por ejemplo:

  ```
  start nstrace -tcpdump enabled -size 0 -mode appFW
  ```

- Si una solicitud desencadena varias infracciones, el `nstrace` para ese registro incluye todos los mensajes de registro correspondientes.
- El formato de mensaje de registro CEF es compatible con esta funcionalidad.
- Las infracciones de firma que activan la acción de bloqueo o registro para las comprobaciones del lado de la solicitud también se incluirán en el seguimiento.
- Solo las solicitudes HTML (no XML) se recopilan en el seguimiento.

Compatibilidad con Web App Firewall para configuraciones de clúster

August 20, 2021

> **Nota:**
>
> Citrix Web App Firewall para configuraciones rayadas y parcialmente rayadas se introdujo en la versión de Citrix ADC 11.0.

Un clúster es un grupo de dispositivos Citrix ADC configurados y administrados como un único sistema. Cada dispositivo del clúster se denomina nodo. Dependiendo del número de nodos en los que estén activas las configuraciones, las configuraciones de clúster se denominan configuraciones seccionados, parcialmente seccionados o manchados. El Web App Firewall es totalmente compatible con todas las configuraciones.

Las dos ventajas principales de la compatibilidad con servidores virtuales seccionados y parcialmente seccionados en configuraciones de clúster son las siguientes:

1. Compatibilidad con conmutación por error de sesión: Las configuraciones de servidores virtuales seccionados y parcialmente seccionados admiten la conmutación por error de sesión. Las funciones avanzadas de seguridad de Web App Firewall, como el cierre de URL de inicio y la coherencia de campos de formulario comprueban, mantienen y utilizan sesiones durante el procesamiento de transacciones. En una configuración de alta disponibilidad o en una configuración de clúster detectado, cuando se produce un error en el nodo que está procesando el tráfico de Web App Firewall, se pierde toda la información de la sesión y el usuario tiene que restablecer la sesión. En configuraciones de servidores virtuales seccionados, las sesiones de usuario se replican en varios nodos. Si un nodo falla, un nodo que ejecuta la réplica se convierte en el propietario. La información de la sesión se mantiene sin ningún impacto visible para el usuario.
2. Escalabilidad: Cualquier nodo del clúster puede procesar el tráfico. Varios nodos del clúster pueden procesar las solicitudes entrantes servidas por el servidor virtual seccionado. Esto mejora la capacidad del Web App Firewall para gestionar múltiples solicitudes simultáneas, mejorando así el rendimiento general.

Las comprobaciones de seguridad y las protecciones de firmas se pueden implementar sin necesidad de ninguna configuración adicional de Web App Firewall específica del clúster. Puede realizar la configuración habitual de Web App Firewall en el nodo Coordinador de configuración (CCO) para propagarse a todos los nodos.

> **Nota:**
>
> La información de sesión se replica en varios nodos, pero no en todos los nodos de la configuración seccionada. Por lo tanto, la compatibilidad con failover admite un número limitado de

> fallas simultáneas. Si varios nodos fallan simultáneamente, el Web App Firewall podría perder la información de la sesión si se produce un error antes de replicar la sesión en otro nodo.

Resumen

- Web App Firewall ofrece escalabilidad, alto rendimiento y compatibilidad con conmutación por error de sesión en implementaciones de clústeres.
- Todas las comprobaciones de seguridad de Web App Firewall y las protecciones de firma son compatibles con todas las configuraciones de clúster.
- Los mapas de caracteres aún no son compatibles con un clúster. El motor de aprendizaje recomienda Tipos de campo en reglas aprendidas para la comprobación de seguridad Formato de campo.
- Las estadísticas y las reglas aprendidas se agregan desde todos los nodos de un clúster.
- Distributed Hash Table (DHT) proporciona el almacenamiento en caché de la sesión y ofrece la capacidad de replicar información de sesión en varios nodos. Cuando una solicitud llega al servidor virtual, el dispositivo Citrix ADC crea sesiones de Web App Firewall en el DHT y también puede recuperar la información de sesión desde el DHT.
- La agrupación en clústeres tiene licencia con las licencias Advanced y Premium. Esta función no está disponible con la licencia estándar.

Depuración y solución de problemas

January 19, 2021

Consulte la siguiente información de solución de problemas y depuración relacionada con cada una de las funciones de Web App Firewall:

- Firewall de aplicaciones: CPU alta
- Memoria
- Error de carga de archivos grandes
- Aprendizaje
- Firmas
- Registro de seguimiento
- Otros

CPU alta

January 12, 2021

A continuación se presentan algunos de los problemas de depuración relacionados con la funcionalidad y la alta CPU y las prácticas recomendadas a seguir cuando se trabaja con Web App Firewall:

Compruebe las visitas a directivas, los enlaces, la configuración de red, la configuración de Web App Firewall:

- Identificar errores de configuración
- Identificar *el servidor virtual* que está sirviendo el tráfico afectado

Inspeccione los registros de los siguientes archivos de registro en busca de infracciones de seguridad y cambios recientes de configuración:

- `/var/log/ns.log`
- `/var/nslog/import.log`
- `/var/nslog/aslearn.log`
- `tail -f /var/log/ns.log | grep APPFW_SIGNATURE_MATCH`

Ejemplo:

```
1 Jun 13 01:11:09 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
    .0|APPFW| APPFW_SIGNATURE_MATCH|6|src=10.217.253.62 spt=61141 method
    =GET request= http://aaron.stratum8.net/FFC/wwwboard/passwd.txt msg=
    Signature violation rule ID 807: web-cgi /wwwboard/passwd.txt access
     cn1=140 cn2=841 cs1=pr_ffc cs2=PPE0 cs3=
    OyTgjbXBqcpBFeENKDlde3OkMQ00001 cs4=ALERT cs5=2015 cs6=web-cgi act=
    not blocked
2 <!--NeedCopy-->
```

Aísle el tráfico que se efectúa:

- Aislar el perfil
- Aislar la comprobación de seguridad
- Aísle la URL, el servidor virtual y los parámetros de tráfico

El seguimiento de nivel de perfil condicional ayuda a identificar los registros de tráfico e infracciones:

- `set appfw profile <profile> -trace ON`
- `start nstrace -mode APPFW -size 0`
- `stop nstrace`

Nota: Asegúrese de que la traza se recopila con la opción -size 0.

Compruebe appfw, dht, contadores de actividad de reputación IP:

- `nsconmsg -g as_ -g appfwreq_ -g iprep -d current`

Tamaño de la ventana del monitor para los reajustes en la conexión:

Appfw establece el tamaño de la ventana en 9845 cuando Citrix ADC restablece la conexión debido a un mensaje http no válido.

Ejemplos:

- Solicitud mal formada recibida: Restablecimiento de la conexión
- Problemas relacionados con la CPU alta
- Comprobar las hojas de datos para los límites del sistema
- Inspeccione el uso de la CPU, appfw, DHT y la actividad relacionada con la memoria. Supervisar sesiones de appfw
- nsconmsg -g cc_cpu_use -g appfwreq -g as -g dht -g mem_as_obj -g mem_as_component -d current

Supervisar la memoria asignada y liberada de los componentes y objetos de Web App Firewall durante el período de tiempo de destino. Ayuda a aislar la protección que conduce a un alto uso de CPU.

- Salida del generador de perfiles
- Observar registros

Aislar la comprobación de appfw que conduce a una CPU alta:

- startURLClosure
- Formfiledconsistency
- CSRF
- Protecciones de cookies
- Comprobación del encabezado del referer

Compruebe que la actualización automática de firmas no conduce a una CPU alta (Inhabilitar para confirmar).

Memoria

August 20, 2021

Las siguientes son algunas de las prácticas recomendadas a seguir cuando se encuentran con problemas relacionados con la memoria de uso de Web App Firewall:

uso del comando nsconmsg:

- Busque estadísticas globales de memoria para determinar que hay suficiente memoria en el sistema y que no hay errores de asignación de memoria ejecutando el siguiente comando:

  ```
  * *- nsconmsg -d memstats
  ```


- Observe los límites actuales de memoria asignados y máximos para appsecure, reputación IP, caché y compresión ejecutando el siguiente comando:

  ```
  nsconmsg -d memstats | egrep -i APPSECURE|IPREP|CACHE|CMP
  ```

- Compruebe appfw, DHT, contadores de actividad de reputación IP ejecutando el siguiente comando:

  ```
  nsconmsg -g as -g appfwreq_ -g iprep -d current
  ```

- Compruebe todos los contadores de errores de Web App Firewall ejecutando el siguiente comando:

  ```
  nsconmsg -g as_ -g appfwreq_ -g iprep_ -d stats | grep err
  ```

- Compruebe todos los contadores de errores del sistema ejecutando el siguiente comando:

  ```
  nsconmsg -g err -d current
  ```

- Inspeccione los contadores CPU, APTFWREQ, AS y DHT ejecutando el siguiente comando:

  ```
  nsconmsg -g cc_cpu_use -g appfwreq -g as -g dht -d current
  ```

- Compruebe la memoria caché configurada ejecutando el siguiente comando:
- `show cacheparameter`
- Compruebe la memoria configurada ejecutando el siguiente comando:

  ```
  nsconmsg -d memstats | egrep -i CACHE
  ```

- Identificar la distribución de memoria en los componentes y objetos de Web App Firewall:

Display AS_OBJ_ memory:

```
nsconmsg -K newnslog -d stats | grep AS_OBJ | egrep -v AppFW_cpu0|total |
sort -k3
```

Display AS_COMPONENT_ memory:

```
nsconmsg -K newnslog -d stats | grep AS_COMPONENT | egrep -v AppFW_cpu0|
total | sort -k3
```

Compruebe el número de sesiones activas ejecutando el siguiente comando:

Supervisar/trazar recuentos de sesiones activas:

```
nsconmsg -g as_alive_sessions -d current
```

Supervisar/trazar el total de sesiones asignadas, gratuitas y actualizadas:

- `nsconmsg -g as_tot_alloc_sessions -g as_tot_free_sessions -d current`
- `nsconmsg -g as_tot_update_sessions -d current`

Si es necesario, reduzca el tiempo de espera de la sesión para asegurarse de que no se utilizan los límites de sesión ejecutando el siguiente comando:

```
set appfwsettings -sessionTimeout <300>
```

Si es necesario, establezca la duración máxima de la sesión ejecutando el siguiente comando:

```
set appfwsettings -sessionLifetime <7200>
```

Comprobación de la memoria asignada y usada

Para comprobar el total de la memoria asignada y la memoria usada:

- Utilice el comando **nsconmsg —d memstats**. Observe el campo **MEM_APPSECURE**.
- Utilice el comando **stat appfw** para obtener información de consumo de memoria.

Web App Firewall no elimina automáticamente los registros después de cierto período de tiempo o tamaño.

- `All AppFw logs are archived in the */var/log/ns.log*` archivo. El archivo *ns.log* realiza la tarea de sustitución.

Para obtener más información, consulte el siguiente enlace: `<http://support.citrix.com/article/CTX121898>`

Aumento de la memoria de Web App Firewall:

- No hay ninguna opción CLI para aumentar la memoria de Web App Firewall. La memoria de Web App Firewall es específica de la plataforma.
- Puede usar la opción *nsapimgr* para aumentar la memoria, pero no se recomienda.

La plataforma determina la memoria máxima permitida para Web App Firewall y la desactivación de IC no afecta a la asignación de memoria.

Fallas de carga de archivos grandes

January 12, 2021

Cuando encuentre errores de carga de archivos grandes, asegúrese de comprobar lo siguiente:

— Límite de correo del firewall de aplicaciones mal configurado
— Se habilitó el análisis de carga de archivos, lo que aumenta el tiempo de procesamiento.
— Golpear los límites del sistema.

Para cargas útiles superiores a 20 MB, Citrix recomienda habilitar la transmisión por secuencias en el perfil del firewall de la aplicación. Además, debe asegurarse de que el servidor back-end admite solicitudes fragmentadas antes de habilitar la transmisión por secuencias.

Desde la versión 11.0, el indicador de transmisión se puede habilitar por perfil para evitar el almacenamiento en búfer ejecutando el siguiente comando:

```
set appfw profile <profile name> -streaming on
```

Aprendizaje

January 12, 2021

Las siguientes son algunas de las prácticas recomendadas cuando se encuentran con problemas de funcionalidad de aprendizaje:

Proceso aslearn:

- Compruebe que el proceso *aslearn* se está ejecutando.
- Comprobar la salida del comando superior
- Compruebe la salida del comando ps ejecutando el siguiente comando:

  ```
  ps -ax | grep aslearn | grep -v "grep"
  ```

  Ejemplo:

  ```
  root@ns# ps -ax | grep aslearn | grep -v "grep"
  1439  ??  Ss     0:03.86 /netscaler/aslearn -start -f /netscaler/
     aslearn.conf
  <!--NeedCopy-->
  ```

- Identifique los comandos de configuración recientes ejecutados antes del problema observado verificando el archivo *ns.log* :

  ```
  /var/log/ns.log
  ```

- Inspeccione registros aslearn para comprobar los mensajes aslearn:

  ```
  /var/log/aslearn.log
  ```

- Aislar el perfil y la comprobación de seguridad que se efectúa
- Identifique el comando GUI y CLI que está fallando ejecutando el siguiente comando:

  ```
  show appfw learningdata <profileName> <securityCheck>
  ```

  Ejemplos:

  - `show learningdata test_profile starturl`
  - `show learningdata test_profile crosssiteScripting`

- show learningdata test_profile sqLInjection
- show learningdata test_profile csRFtag
- show learningdata test_profile fieldformat
- show learningdata test_profile fieldconsistency

- Realice la comprobación de integridad de sqlite desde el símbolo del shell bsd:

```
nsshell ## sqlite3 /var/nslog/asl/<profile_name_in_lowercase>.db '
pragma integrity_check;
```

Ejemplos:

```
root@ns# sqlite3 /var/nslog/asl/tsk0247284.db 'pragma
   integrity_check;'
ok
<!--NeedCopy-->
```

- Implementar o quitar reglas para empezar a aprender de nuevo:
  - Si se alcanzan 2000 elementos de aprendizaje (por protección), no podrá empezar a aprender más sobre esa protección
  - Si se alcanza el tamaño de 20 MB para la base de datos, deje de aprender para todas las protecciones
  - Reiniciar como proceso de aprendizaje

```
*/netscaler/aslearn -start -f/netscaler/aslearn.conf*
```

- Compruebe el espacio en la carpeta /var ejecutando lo siguiente:

```
du -h /var
```

- Compruebe los límites del umbral de aprendizaje ejecutando el siguiente comando:

```
show appfwlearningsettings <profile_name> <securityCheck>
```

- Recopilar datos aprendidos ejecutando el siguiente comando:

```
export appfwlearningdata <profile_name> <securityCheck>
```

- Comprobar que los datos aprendidos se cargan en el recopilador.

Firmas

January 12, 2021

Introducción a las firmas

Para agregar firma:

1. Seleccione la firma **predeterminada** y haga clic en **Agregar**para realizar una copia.
2. Dé un nombre significativo. El nuevo objeto sig se agrega como objeto Definido por el usuario.
3. Habilite las reglas de destino que sean pertinentes a su necesidad específica.
    - Las reglas están inhabilitadas de forma predeterminada.
    - más reglas requieren más procesamiento
4. Configure las acciones:

    Las acciones de bloqueo y registro están habilitadas de forma predeterminada. Estadísticas es otra opción
5. Establezca la firma que utilizará su perfil.

Sugerencias para usar firmas

- Optimice la sobrecarga de procesamiento habilitando solo las firmas aplicables para proteger la aplicación.
- Cada patrón de la regla debe coincidir para activar una coincidencia de firma.
- Puede agregar sus propias reglas personalizadas para inspeccionar las solicitudes entrantes y detectar varios tipos de ataques, como ataques de inyección SQL o scripts entre sitios.
- También puede agregar reglas para inspeccionar las respuestas a fin de detectar y bloquear la fuga de información confidencial, como números de tarjetas de crédito.
- Agregue varias condiciones de comprobación de seguridad para crear su propia comprobación personalizada.

Prácticas recomendadas para el uso de firmas

A continuación se presentan algunas de las prácticas recomendadas que puede seguir cuando se encuentra con problemas relacionados con las firmas:

- Compruebe que el comando de importación se ha realizado correctamente tanto en el primario como en el secundario.
- Verifique que las salidas CLI y GUI sean consistentes.
- Compruebe ns.log para identificar cualquier error durante la importación de firmas y la actualización automática.
- Compruebe si el servidor de nombres DNS está configurado correctamente.

- Compruebe la incompatibilidad de la versión del esquema.
- Compruebe si el dispositivo no puede acceder a la URL de actualización de firma alojada en AWS para la actualización automática.
- Compruebe si la versión no coincide entre la firma predeterminada y las agregadas por el usuario.
- Compruebe si la versión no coincide entre los objetos de firma en los nodos principal y secundario.
- Monitor de alta utilización de CPU (inhabilite la actualización automática para descartar un problema con la actualización de firma).

Registro de seguimiento

January 12, 2021

Para registrar registros de seguimiento:

1. Habilitar el rastreo para el perfil. Puede utilizar el comando show para verificar la configuración configurada.

```
set appfw profile <profile> -trace ON
```

1. Empieza a recoger rastros. Puede seguir mediante todas las opciones aplicables al comando nstrace.

```
start nstrace -mode APPFW
```

1. Dejar de recoger el rastro

```
stop nstrace
```

Ubicación de la traza: El nstrace se almacena en una carpeta con sello de tiempo que se crea en el directorio */var/nstrace* y se puede ver mediante wireshark. Puede seguir el archivo */var/log/ns.log* para ver los mensajes de registro que proporcionan detalles sobre la ubicación de la nueva traza.

Ventajas de los registros de seguimiento:

- Aislar el tráfico para un perfil específico
- Recopilar datos para solicitudes específicas
- Identificar reinicios o anulaciones
- Ver tráfico SSL descifrado: El tráfico HTTPS se captura en texto sin formato para facilitar la solución de problemas.
- Proporciona una vista completa: Le permite ver toda la solicitud en el nivel de paquete, comprobar la carga útil, ver los registros para comprobar qué infracción de comprobación de seguridad

se está desencadenando e identificar el patrón de coincidencia en la carga útil. Si la carga útil consiste en datos inesperados, cadenas basura o caracteres no imprimibles (carácter nulo, r o n, etc.), son fáciles de descubrir en la traza.
- Acelere el tiempo de respuesta: Depuración más rápida en el tráfico de destino para realizar análisis de causa raíz.

Otros

August 20, 2021

A continuación se presentan las soluciones para algunos de los problemas que puede encontrar al utilizar Web App Firewall.

- Web App Firewall establece el tamaño de la ventana en 9845 cuando se restablece la conexión para mensajes http no válidos.

  — Solicitud mal formada recibida - restablecimiento de conexión [Cliente/Servidor enviando encabezado de longitud de contenido no válido]
  — Tipo de contenido desconocido en los encabezados de solicitud

- Límite del sistema: La aplicación parece congelada

  — Se produce cuando se alcanza el límite máximo de sesión. (100K)
  — Menos memoria del sistema para la operación.

  - **La función Reputación IP no funciona** el proceso iprep tarda unos cinco minutos en iniciarse después de habilitar la función de reputación. Es posible que la función de reputación IP no funcione durante ese período.

- Infracciones inesperadas de Web App Firewall que se activan

  — El tiempo de espera de la sesión tiene un valor predeterminado de 900 segundos. Si el tiempo de espera de la sesión se establece en un valor bajo, el explorador puede desencadenar falsos positivos para las comprobaciones que se basan en la sesión (por ejemplo, CSRF, FFC). Compruebe el tiempo de espera de la sesión y observe el ID de sesión (cs3 en los registros CEF). Si el ID de sesión es diferente, el tiempo de espera de la sesión podría ser el motivo.
  — Si el formulario es generado dinámicamente por javaScript, puede desencadenar falsas violaciones de FFC.

- Nombre de campo vacío en los registros de infracciones de FFC (antes de la versión 11.0)

  Esto puede verse en casos donde nos encontramos con un campo de formulario que no está en los formularios de nuestra sesión.

  Casos en los que esto puede ocurrir:

— Se ha agotado el tiempo de espera de la sesión desde el momento en que se envió el formulario al cliente y cuando se recibió.
— El formulario se generó en el lado del cliente mediante un script java.

Referencias

January 21, 2022

Consulte los siguientes recursos adicionales para obtener información sobre las funciones de Web App Firewall.

- Cómo Citrix Web App Firewall modifica el tráfico de datos de aplicaciones.
- Rastrear y cómo las solicitudes HTML con los registros de infracciones de seguridad de Web App Firewall en el dispositivo Citrix ADC
- Protección de nivel superior
- Relajaciones de seguridad
- Información sobre la configuración e implementación de una aplicación:
  - Application
  - Firewall
  - troncos
- Artículos de actualización de firmas
- Administración de bots

Artículos de alerta de firma

January 12, 2021

Citrix Web Application Firewall (WAF) anuncia actualizaciones de firmas que puede descargar y aplicar en su dispositivo. Cuando detecte un ataque de seguridad, recibirá una notificación por correo electrónico sobre la nueva actualización de la firma. Puede descargar la firma y aplicarla en el dispositivo.

Cómo recibir una notificación de alerta de firma

March 9, 2022

En este artículo se explica cómo configurar la configuración de alerta de firma para recibir notificaciones por correo electrónico para nuevas actualizaciones de firmas.

> **Nota:**
>
> - Para obtener actualizaciones sobre las firmas de Web App Firewall, debe configurar la función de actualización automática de firmas. Para obtener más información, consulte el tema Actualización automática de firmas.
> - Para obtener actualizaciones sobre las nuevas firmas de bots, debe configurar la función de actualización automática de firmas de bots. Para obtener más información, consulte el tema Actualización automática de firmas de bots.

Resumen

Los administradores de red quieren recibir una notificación por correo electrónico para las nuevas actualizaciones y notificaciones de firma de Web App Firewall.

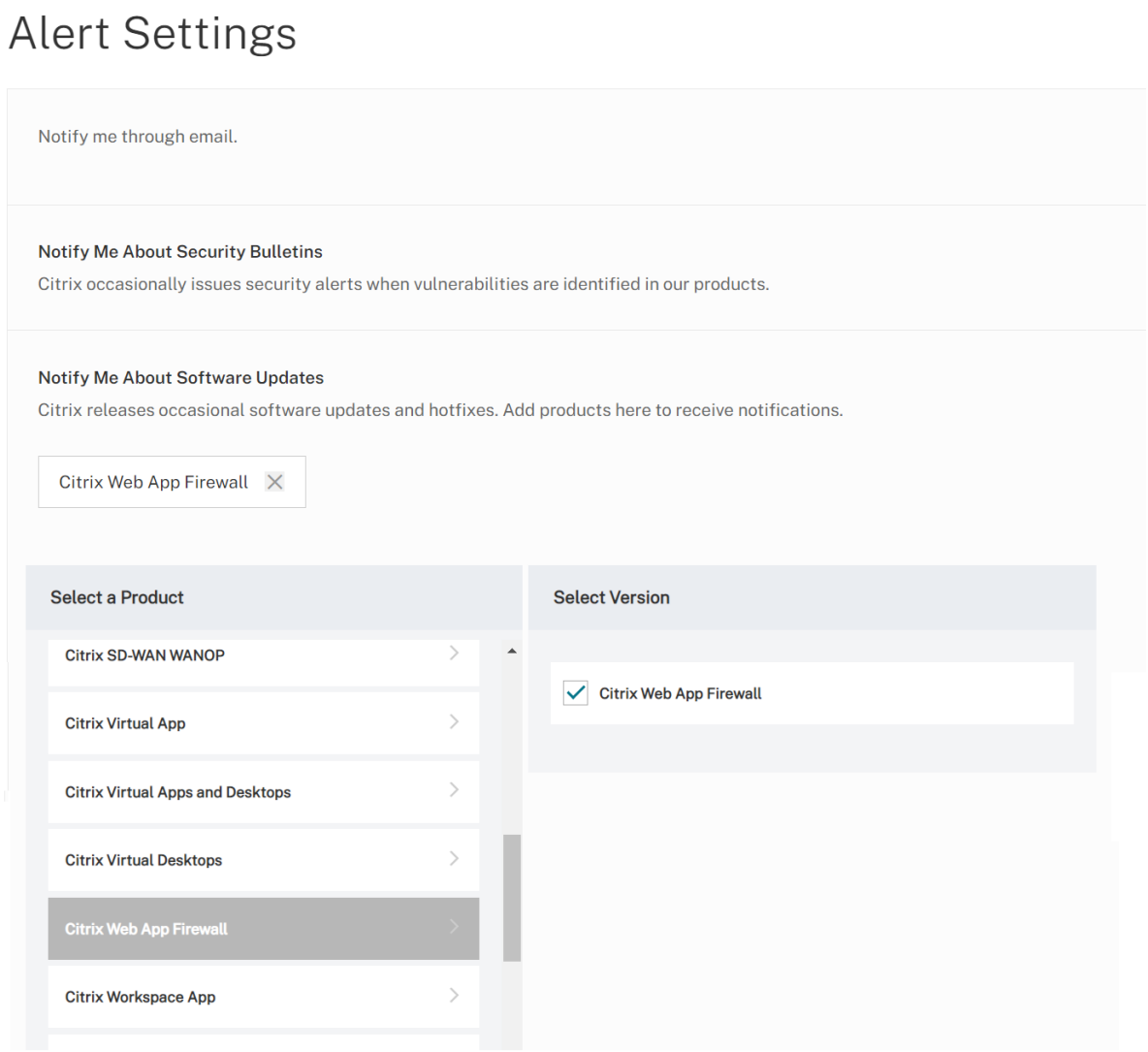
Problema

Un administrador de red que quiera recibir una notificación cuando haya una nueva firma disponible para el Web App Firewall puede elegir recibir una notificación por correo electrónico. El administrador recibirá una notificación por correo electrónico cuando haya nuevas firmas disponibles para su descarga.Administradores
de red para recibir notificaciones por correo electrónico para nuevas actualizaciones de firmas.

Solución

Para recibir notificaciones por correo electrónico de nuevas actualizaciones de firmas, siga los pasos que se indican a continuación:

1. Inicie sesión en el sitio web de asistencia de Citrix: `https://support.citrix.com/user/alerts`
2. En la sección **Configuración de alertas**, habilite la opción Notificarme a través de correo electrónico.
3. Seleccione **Agregar productos** para ver el catálogo de productos.
4. Haga clic en **Citrix Web App Firewall** y, a continuación, active la casilla de verificación **Citrix Web App Firewall**.
5. Haga clic en **Guardar configuración**.



1. En la sección **Configuración de alertas**, habilite la opción Notificarme a través de correo electrónico.
2. Seleccione **Agregar productos** para ver el catálogo de productos.
3. Haga clic en **Firewall de aplicaciones** y, a continuación, haga clic en la casilla de verificación **Firmas**.
4. Haga clic en **Guardar configuración**.

Versión 27 de la actualización de firmas

January 21, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la versión 27. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables

a la seguridad. La actualización de firma incluye el identificador de firma, la versión de la firma y la lista de CVE a los que se dirige.

Versión de firma

Las firmas son compatibles con las siguientes versiones de software de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 y 13.1.

La versión 12.0 de Citrix ADC ha llegado al final de su vida útil (EOL). Para obtener más información, consulte la página del ciclo de vida de la versión

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999921	cve-2018-1002000	Vulnerabilidad WEB-MISCWordpress Arigato Autoresponder e inyección SQL de boletín informativo.
999920		WEB-MISCWordPress Plug-in Corner Ad 1.0.7: Scripts entre sitios almacenados
999919	cve-2018-1002009	WEB-MISCWordpress Arigato Autoresponder y boletín bft_unsubscribe vulnerabilidad de scripts entre sitios.
999918	cve-2018-1002002	WEB-MISCWordpress Arigato Autoresponder y Newsletter vulnerabilidad de scripts entre sitios.
999918	cve-2018-1002003	WEB-MISCWordpress Arigato Autoresponder y Newsletter vulnerabilidad de scripts entre sitios.

Regla de firma	ID de CVE	Descripción
999918	cve-2018-1002004	WEB-MISCWordpress Arigato Autoresponder y Newsletter vulnerabilidad de scripts entre sitios.
999918	cve-2018-1002005	WEB-MISCWordpress Arigato Autoresponder y Newsletter vulnerabilidad de scripts entre sitios.
999918	cve-2018-1002006	WEB-MISCWordpress Arigato Autoresponder y Newsletter vulnerabilidad de scripts entre sitios.
999918	cve-2018-1002007	WEB-MISCWordpress Arigato Autoresponder y Newsletter vulnerabilidad de scripts entre sitios.
999917	cve-2018-1002001	WEB-MISCWordpress Arigato Autoresponder y Newsletter vulnerabilidad de scripts entre sitios.
999917	cve-2018-1002008	WEB-MISCWordpress Arigato Autoresponder y Newsletter vulnerabilidad de scripts entre sitios.
999916	cve-2018-8719	Plug-in WEB-MISCWordPress Registro de auditoría de seguridad de WP: wp-content/uploads/wp-security-audit-log/* acceso sin restricciones
999915	cve-2019-7743	WEB-MISC- Joomla phar://ejecución de vulnerabilidad de inyección de objetos de envoltura de flujo de archivos no phar cargados

Regla de firma	ID de CVE	Descripción
999914		Plug-in WEB-MISCWordpress Suscriptores de correo electrónico y boletines 3.4.7 vulnerabilidad de divulgación
999913		WEB-MISCWordPress plug-in AD Manager WD v1.0.11: wd_ads_admin_class.php Descarga arbitraria de archivos
999912		WEB-IISMicrosoft IIS: Divulgación del nombre abreviado de archivo/carpeta

Versión 28 de la actualización de firmas

January 21, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la versión 28. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad. La actualización de firma incluye el identificador de firma, la versión de la firma y la lista de CVE a los que se dirige.

Versión de firma

Las firmas son compatibles con las siguientes versiones de software de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 y 13.1.

La versión 12.0 de Citrix ADC ha llegado al final de su vida útil (EOL). Para obtener más información, consulte la página del ciclo de vida de la versión

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999898	CVE-2018-12895	WEB-MISC WordPress antes de 4.9.7: Vulnerabilidad de recorrido de directorios.
999899	CVE-2019-9618	WEB-MISC-GraceMedia Media Player Complemento de WordPress 1.0 Vulnerabilidad de inclusión de archivos locales arbitrarios
999900	CVE-2018-20714	Plug-in WEB-MISC WordPress WooCommerce antes de 3.4.6: Vulnerabilidad de eliminación de archivos.
999901	CVE-2018-11868	WEB-MISC FlowPaper FlexPaper anterior a la 2.3.7 puede permitir la ejecución remota de código y el restablecimiento de los archivos de configuración.
999902	CVE-2018-11868	WEB-MISC FlowPaper FlexPaper anterior a 2.3.7 puede permitir la ejecución remota de código.
999903	CVE-2019-9184	WEB-MISC-Joomla! El complemento J2Store 3.x antes de 3.3.7 permite la inyección de SQL.
999904	CVE-2019-9168	Plug-in WEB-MISC de WordPress WooCommerce antes de la creación de scripts entre sitios 3.5.5 a través del título de Photoswipe.
999905		Plug-in WEB-MISC WordPress Abandoned Cart antes de 5.1.3 para secuencias de comandos entre sitios almacenados en WooCommerce.

Regla de firma	ID de CVE	Descripción
999906	CVE-2019-8942	WEB-MISC WordPress antes de 4.9.9 y 5.x antes de la ejecución de código remoto 5.0.1.
999907	CVE-2019-8942	WEB-MISC WordPress antes de 4.9.9 y 5.x antes de la ejecución de código remoto 5.0.1.
999908	CVE-2019-8942	WEB-MISC WordPress antes de 4.9.9 y 5.x antes de la ejecución de código remoto 5.0.1
999909	CVE-2017-16562	Plug-in de WordPress del tema WEB-MISC-Deluxe UserPro: Vulnerabilidad de omisión de seguridad a través del parámetro up_auto_log=true
999910	CVE-2018-20782	Plug-in WEB-MISC de WordPress GloBee antes de 1.1.2 para la suplantación de mensajes de WooCommerce-IPN
999911	CVE-2019-6340	Ejecución de código remoto arbitrario de Drupal en Drupal Core 8 RESTful WebServices

Versión 29 de la actualización de firmas

January 21, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la versión 29. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

Las firmas son compatibles con las siguientes versiones de software de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 y 13.1.

La versión 12.0 de Citrix ADC ha llegado al final de su vida útil (EOL). Para obtener más información, consulte la página del ciclo de vida de la versión

Nota:

> La activación de las reglas de firma del cuerpo de la publicación y del cuerpo Citrix ADC respuesta puede afectar a la CPU

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999896	CVE-2019-2725	Ejecución remota de código de Weblogic 10.3.6
999897	CVE-2019-2725	Ejecución remota de código de Weblogic 10.3.6

Versión 30 de la actualización de firmas

January 21, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la versión 30. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

Las firmas son compatibles con las siguientes versiones de software de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 y 13.1.

La versión 12.0 de Citrix ADC ha llegado al final de su vida útil (EOL). Para obtener más información, consulte la página del ciclo de vida de la versión

> **Nota:**
>
> La activación de las reglas de firma del cuerpo de la publicación y del cuerpo Citrix ADC respuesta puede afectar a la CPU

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999879	<>	Plug-in WEB-MISC WordPress WooCommerce Checkout Manager: Vulnerabilidad de carga arbitraria
999880	<>	Plug-in WEB-MISC WordPress Formulario de contacto avanzado 7 DB anterior a 1.6.1: Vulnerabilidad de inyección SQL
999881	<>	Plug-in WEB-MISC WordPress Contact Form Builder antes de 1.0.67: Vulnerabilidad de inclusión de archivos locales
999882	<>	Intento de inyección ciego de URI HTTP SQL
999883	<>	Plug-in WEB-MISC Loco Translate WordPress 2.1.1 y anteriores: Vulnerabilidad de inclusión de archivos locales
999884	<>	Plug-in WEB-MISC WordPress Duplicate-Page antes de 3.4: Vulnerabilidad de inyección SQL
999885	CVE-2019-0232	WEB-MISC Apache Tomcat RCE a través de scripts CGI de.CMD cuando enableCmd-LineArguments=True en MS Windows

Regla de firma	ID de CVE	Descripción
999886	CVE-2019-0232	WEB-MISC Apache Tomcat RCE a través de scripts CGI de.BAT cuando enableCmd-LineArguments=True en MS Windows
999887	CVE-2019-10692	Complemento de WordPress WWEB-MISC wp-google-maps antes de 7.11.18: Vulnerabilidad de inyección SQL.
999888	CVE-2019-10946	WEB-MISC Joomla! Antes de 3.9.5: Vulnerabilidad de omisión de seguridad
999889	CVE-2019-10945	WEB-MISC Joomla! Antes de 3.9.5: Vulnerabilidad de cruce de directorios
999890	CVE-2019-9912	WEB-MISC WpGoogleMaps Complemento de WordPress anterior a 7.10.41 Vulnerabilidad de scripts entre sitios reflejados
999890	CVE-2019-9912	WEB-MISC WpGoogleMaps Complemento de WordPress anterior a 7.10.41 Vulnerabilidad de scripts entre sitios reflejados
999891	CVE-2019-9911	Plug-in WEB-MISC WordPress Auto-Poster de redes sociales antes de 4.2.8: Vulnerabilidad de scripts entre sitios
999892	CVE-2019-9908	Complemento de WordPress WEB-MISC Font_Organizer 2.1.1: secuencias de comandos reflejadas entre sitios

Regla de firma	ID de CVE	Descripción
999893	CVE-2019-9787	WEB-MISC WordPress antes de 4.9.7: Vulnerabilidad de ejecución remota de código
999894	CVE-2019-9568	Formulario de contacto de WEB-MISC Forminator, Poll & Quiz Builder Complemento de WordPress antes de 1.6 Vulnerabilidad ciega
999895	CVE-2019-9567	Formulario de contacto de WEB-MISC Forminator, complemento WP de Poll & Quiz Builder antes de 1.6 Vulnerabilidad persistente de secuencias de comandos
999877	CVE-2018-20062	WEB-MISC NoneCMS V1.3: Vulnerabilidad de ejecución de código PHP arbitrario del filtro ThinkPHP
999878	CVE-2019-9082	Vulnerabilidad de ejecución remota de código WEB-MISC en ThinkPHP 5.x antes de 5.1.32

Versión 32 de la actualización de firmas

January 21, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la versión 32. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

Las firmas son compatibles con las siguientes versiones de software de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 y 13.1.

La versión 12.0 de Citrix ADC ha llegado al final de su vida útil (EOL). Para obtener más información, consulte la página del ciclo de vida de la versión

> **Nota:**
>
> La activación de las reglas de firma del cuerpo de la publicación y del cuerpo Citrix ADC respuesta puede afectar a la CPU

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999875	CVE-2016-4438, CVE-2016-3087	Vulnerabilidad de ejecución remota a través de URL de WEB-STRUTS Apache Struts 2.3.20 a 2.3.28.1
999876	CVE-2019-10867	WEB-MISC Pimcore anterior a 5.7.1: Vulnerabilidad de deserialización (CVE-2019-10867)

Versión 33 de la actualización de firmas

January 21, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la versión 33. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

Las firmas son compatibles con las siguientes versiones de software de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 y 13.1.

La versión 12.0 de Citrix ADC ha llegado al final de su vida útil (EOL). Para obtener más información, consulte la página del ciclo de vida de la versión

> **Nota:**
>
> La activación de las reglas de firma del cuerpo de la publicación y del cuerpo Citrix ADC respuesta puede afectar a la CPU

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla	CVE	Descripción	Referencia de vulnerabilidades
999860		Plug-in de WordPress Yuzo Publicaciones relacionadas Vulnerabilidad de scripts	https://www.wordfence.com/blog/2019/04/yuzo-related-posts-zero-day-vulnerability-exploited-in-the-wild
999861	CVE-2019-12099		cve,2019-12099
999862		Copia de seguridad de base de datos de complementos de WordPress <= 5.2: Ejecución remota	https://www.wordfence.com/blog/2019/05/os-command-injection-vulnerability-patched-in-wp-database-backup-plug-in
999863		Plug-in de WordPress Slick Popup: Escalada de privilegios	https://www.wordfence.com/blog/2019/05/privilege-escalation-flaw-present-in-slick-popup-plug-in

Regla	CVE	Descripción	Referencia de vulnerabilidades
999864	CVE-2019-10866	Complemento de WordPress Form Maker 1.13.3: Inyección SQL	cve,2019-10866
999865		Plug-in Give de WordPress: Scripts entre sitios almacenados para los donantes	https://blog.sucuri.net/2019/05/wordpress-plug-in-give-stored-xss-for-donors.html
999866		Complemento de WordPress My Calendar <= 3.1.9: Vulnerabilidad de scripts entre sitios no autenticados	https://wpvulndb.com/vulnerabilities/9267
999867		Complemento de WordPress Slimstat <= 4.8: Scripting entre sitios almacenados sin autenticar	https://blog.sucuri.net/2019/05/slimstat-stored-xss-from-visitors.html
999868	CVE-2019-2618	Vulnerabilidad en la carga arbitraria	cve,2019-2618
999869	CVE-2019-11871	Complemento de WordPress WEB-WORDPRESS Custom Field Suite anterior a 2.5.15: Vulnerabilidad de scripts entre sitios	cve,2019-11871

Regla	CVE	Descripción	Referencia de vulnerabilidades
999870		WEB-WORDPRESS Complemento de función de chat en vivo de WordPress: Vulnerabilidad de scripts entre sitios persistentes anteriores a 8.0.27 a través del parámetro wplc_custom_js	https://blog.sucuri.net/2019/05/persistent-cross-site-scripting-in-wp-live-chat-support-plug-in.html
999871		Complemento de WordPress WEB-WORDPRESS W3 Total Cache anterior a 0.9.7.4: Vulnerabilidad de ejecución remota de código PHAR	https://wpvulndb.com/vulnerabilities/9270
999872		Complemento de WordPress WEB-WORDPRESS W3 Total Cache anterior a 0.9.7.4: Vulnerabilidad de ejecución remota de código PHAR	https://wpvulndb.com/vulnerabilities/9269
999873	CVE-2019-0604	WEB-MISC Microsoft Windows Sharepoint Server: Vulnerabilidad de ejecución remota de código	cve,2019-0604

Regla	CVE	Descripción	Referencia de vulnerabilidades
999874		Publicaciones relacionadas con WEB-WORDPRESS Yuzo Vulnerabilidad de scripts entre sitios almacenados no autenticados en 5.12.91	https://www.wordfence.com/blog/2019/04/yuzo-related-posts-zero-day-vulnerability-exploited-in-the-wild

Versión 34 de la actualización de firmas

January 21, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la versión 34. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

Las firmas son compatibles con las siguientes versiones de software de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 y 13.1.

La versión 12.0 de Citrix ADC ha llegado al final de su vida útil (EOL). Para obtener más información, consulte la página del ciclo de vida de la versión

> **Nota:**
>
> La activación de las reglas de firma del cuerpo de la publicación y del cuerpo Citrix ADC respuesta puede afectar a la CPU

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999843		Complemento de WordPress WEB-WORDPRESS Ultimate Member anterior a la versión 2.0.46: Configuración de archivo arbitrario para lectura
999844		WEB-WORDPRESS complemento de WordPress Ultimate Member anterior a la versión 2.0.46: Lectura arbitraria de archivos
999845		WEB-WORDPRESS complemento de WordPress Ultimate Member anterior a la versión 2.0.46: Eliminación de archivos mediante reemplazo de archivos
999846		WEB-WORDPRESS complemento de WordPress Ultimate Member antes de la versión 2.0.46: Eliminación de archivos
999847		Enlaces cortos del complemento WEB-WORDPRESS WordPress anteriores a 2.1.10: Vulnerabilidad de inyección de CSV
999848		Enlaces cortos del complemento de WordPress WEB-WORDPRESS anteriores a 2.1.10: Vulnerabilidad de scripts entre sitios almacenados no autenticados

Regla de firma	ID de CVE	Descripción
999849		Complemento de WordPress WEB-WORDPRESS FV Flowplayer Video Player antes de 7.3.13.727: Vulnerabilidad de scripts entre sitios almacenados no autenticados
999850		Complemento de WordPress WEB-WORDPRESS Descargas digitales fáciles antes de 2.9.16: Vulnerabilidad de scripts entre sitios almacenados no autenticados
999851		Complemento de WordPress WEB-WORDPRESS Crelly Slider anterior a la versión 1.3.5: Vulnerabilidad de carga
999853	CVE-2019-2615	Vulnerabilidad de divulgación de información de WEB-MISC Oracle WebLogic
999854	CVE-2019-11872	Complemento de WordPress Hustle anterior a 6.0.8.1: Vulnerabilidad de inyección de CSV
999855	CVE-2019-11231	WEB-MISC GetSimple CMS versión 3.3.15 y anteriores: Vulnerabilidad de carga arbitraria de archivos
999856	CVE-2019-11231	WEB-MISC GetSimple CMS versión 3.3.15 y anteriores - Divulgación de información clave de API

Regla de firma	ID de CVE	Descripción
999857		WEB-WORDPRESS complemento de WordPress WP Database Backup antes de 5.2: Vulnerabilidad
999858		Complemento de WordPress WEB-WORDPRESS Slick Popup Hasta 1.7.1: Vulnerabilidad de escalada de privilegios
999859	CVE-2019-12099	Vulnerabilidad de ejecución remota de código WEB-MISC PHP Fusion CMS en la versión 9.03.00 y anteriores

Versión 35 de la actualización de firmas

January 21, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la versión 35. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

Las firmas son compatibles con las siguientes versiones de software de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 y 13.1.

La versión 12.0 de Citrix ADC ha llegado al final de su vida útil (EOL). Para obtener más información, consulte la página del ciclo de vida de la versión

> **Nota:**
>
> La activación de las reglas de firma del cuerpo de la publicación y del cuerpo Citrix ADC respuesta puede afectar a la CPU

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999834	CVE-2019-13024	WEB-MISC Centreon versión 19.04 y anteriores: Vulnerabilidad de inyección de comandos
999835	CVE-2019-5420	Modo de desarrollo de rieles WEB-MISC: Vulnerabilidad de divulgación de tokens secretos
999836	CVE-2019-5418	Vista de acción de WEB-MISC Rails: Vulnerabilidad de divulgación
999837	CVE-2018-12426, CVE-2019-11185	Plug-in WEB-WORDPRESS WP Live Chat Support Pro anterior a 8.0.26 - Carga arbitraria de archivos
999838	CVE-2019-10270	WEB-WORDPRESS complemento de WordPress Ultimate Member anterior a la versión 2.0.40: Restablecimiento arbitrario de contraseña
999839	CVE-2019-12826	Lógica del widget del complemento de WordPress WEB-WORDPRESS anterior a 5.10.2: Vulnerabilidad CSRF
999840		Calendario de eventos todo en uno del complemento de WordPress WEB-WORDPRESS anterior a 2.5.39: Vulnerabilidad de scripts entre sitios
999841	CVE-2019-11565	Complemento de WordPress WEB-WORDPRESS Imprimir mi blog antes de 1.6.7: Vulnerabilidad SSRF no autenticada

Regla de firma	ID de CVE	Descripción
999842		WEB-WORDPRESS complemento de WordPress Ultimate Member anterior a la versión 2.0.46: Múltiples `cross-site scripting</LogString`

Versión 36 de la actualización de firmas

January 21, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la versión 36. Puede descargar y configurar las reglas de firma para proteger su dispositivo de ataques vulnerables a la seguridad.

Versión de firma

Las firmas son compatibles con las siguientes versiones de software de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 y 13.1.

La versión 12.0 de Citrix ADC ha llegado al final de su vida útil (EOL). Para obtener más información, consulte la página del ciclo de vida de la versión

> **Nota:**
>
> La activación de las reglas de firma del cuerpo de la publicación y del cuerpo Citrix ADC respuesta puede afectar a la CPU

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999817		Complemento de inserción de anuncios de WordPress WEB-WORDPRESS anterior a la versión 2.4.22: Ejecución remota de código

Regla de firma	ID de CVE	Descripción
999818	CVE-2019-7839	WEB-MISC Adobe ColdFusion Múltiples versiones: Vulnerabilidad de ejecución remota de código a través de HTTP/SOAP dotnet-to-Java (CVE-2019-7839)
999819	CVE-2019-7839	WEB-MISC Adobe ColdFusion Múltiples versiones: Vulnerabilidad de ejecución remota de código a través de HTTP/SOAP Java-to-DotNet (CVE-2019-7839)
999820	CVE-2019-11469	WEB-MISC Zoho ManageEngine Applications Manager antes de la compilación 14 14150 permite SQLi a través del parámetro resourceid (CVE-2019-11469)
999821	CVE-2019-11448	WEB-MISC Zoho ManageEngine Application Manager 11.0 a 14.0 - Inyección SQL no autenticada (CVE-2019-11448)
999822	CVE-2019-1003000	Complemento de seguridad de secuencias de comandos de Jenkins WEB-MISC hasta 1.49: Vulnerabilidad de omisión de sandbox (CVE-2019-1003000)
999823		Plug-in WEB-WORDPRESS Cforms2 de WordPress hasta 15.0.1: Vulnerabilidad de inyección HTML no autenticada

Regla de firma	ID de CVE	Descripción
999824	CVE-2019-0193	WEB-MISC Apache Solr anterior a 8.2: Vulnerabilidad de ejecución remota de código DIH a través del parámetro DataConfig (CVE-2019-0193)
999825	CVE-2019-11580	Complemento de desarrollo WEB-MISC Atlassian Crowd Pdkinstall habilitado: RCE sin autenticar (CVE-2019-11580)
999826	CVE-2019-0192	WEB-MISC Apache Solr hasta 5.5.5/6.6.5: Vulnerabilidad de ejecución remota de código de la API de configuración (CVE-2019-0192)
999827		Plug-in WEB-WORDPRESS WooCommerce Variation Swatches Hasta 1.0.61: Vulnerabilidad de scripts entre sitios reflejados
999828	CVE-2019-1003001	Complemento Groovy de Jenkins Pipeline WEB-MISC hasta 2.61: Vulnerabilidad de omisión de sandbox a través de la creación de trabajos (CVE-2019-1003001)
999829	CVE-2019-1003001	Complemento Groovy de Jenkins Pipeline WEB-MISC hasta 2.61: Vulnerabilidad de omisión de sandbox (CVE-2019-1003001)
999830		Plug-in WEB-WORDPRESS WordPress Bold Page Builder anterior a 2.3.2: Vulnerabilidad de omisión

Regla de firma	ID de CVE	Descripción
999831	CVE-2019-15107	WEB-MISC Webmin anterior a 1.930: Vulnerabilidad de ejecución remota de código no autenticada (CVE-2019-15107)
999832	CVE-2019-2767	WEB-MISC Oracle BI Publisher 11.1.1.9.0 y 12.2.1.4: Vulnerabilidad de XXE (CVE-2019-2767)
999833	CVE-2019-15106	WEB-MISC Zoho ManageEngine OpManager hasta 12.4x: Vulnerabilidad de omisión de autenticación (CVE-2019-15106)
999948	CVE-2014-0114	Apache Struts 1 a 1.3.10 permite la manipulación de ClassLoader, lo que permite la ejecución de código arbitrario a través de HTTP
999949	CVE-2013-4316	Apache Struts 2 anterior a 2.3.15.2 permite la invocación de métodos dinámicos al afectar la confidencialidad, la integridad o la disponibilidad
999950	CVE-2013-4316	Apache Struts 2 anterior a 2.3.15.2 permite la invocación de métodos dinámicos al afectar la confidencialidad, la integridad o la disponibilidad

Nota:

La regla de firma 999947 se elimina debido a un problema de rendimiento.

Versión 37 de la actualización de firmas

January 21, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la versión 37. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

Las firmas son compatibles con las siguientes versiones de software de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 y 13.1.

La versión 12.0 de Citrix ADC ha llegado al final de su vida útil (EOL). Para obtener más información, consulte la página del ciclo de vida de la versión

> **Nota:**
>
> La activación de las reglas de firma del cuerpo de la publicación y del cuerpo Citrix ADC respuesta puede afectar a la CPU

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999806	CVE-2019-3394	WEB-MISC Atlassian Confluence o centro de datos: Vulnerabilidad de divulgación de archivos locales (CVE-2019-3394)
999807	CVE-2019-13569	Complemento de suscriptores de correo electrónico y boletines de WEB-WORDPRESS Icegram antes de 4.1.8 - SQLi a través de ESFPX_lists Param (CVE-2019-13569)

Regla de firma	ID de CVE	Descripción
999808	CVE-2019-13569	Complemento de suscriptores de correo electrónico y boletines de WEB-WORDPRESS Icegram antes de 4.1.8 - SQLi a través de Order Param (CVE-2019-13569)
999809	CVE-2019-2768	WEB-MISC Oracle BI Publisher: Vulnerabilidad de token de sesión predecible (CVE-2019-2768)
999810	CVE-2019-1003001	Complemento Groovy de Jenkins Pipeline WEB-MISC hasta 2.61: Vulnerabilidad de omisión de sandbox mediante actualización de trabajos (CVE-2019-1003001)
999811	CVE-2019-13575	WEB-WORDPRESS WPEverest Complemento de Everest Forms antes de 1.5.0 - Inyección SQL (CVE-2019-13575)
999812	CVE-2019-15896	Plug-in WEB-WORDPRESS LifterLMS hasta 3.34.5: Vulnerabilidad de omisión de seguridad (CVE-2019-15896)
999813	CVE-2019-3396	WEB-MISC Atlassian Confluence o centro de datos: Vulnerabilidad de ejecución remota de código (CVE-2019-3396)
999814	CVE-2019-5475	WEB-MISC Sonatype Nexus Repository Manager anterior a 2.14.14 - Ejecución remota de código a través de la ruta Createrepo (CVE-2019-5475)

Regla de firma	ID de CVE	Descripción
999815	CVE-2019-5475	WEB-MISC Sonatype Nexus Repository Manager anterior a 2.14.14 - Ejecución remota de código a través de la ruta Mergerepo (CVE-2019-5475)
999816	CVE-2019-15104	WEB-MISC Versión de Zoho ManageEngine OpManager anterior a 12.4: Vulnerabilidad de inyección SQL (CVE-2019-15104)

Versión 38 de la actualización de firmas

January 21, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la versión 38. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

Las firmas son compatibles con las siguientes versiones de software de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 y 13.1.

La versión 12.0 de Citrix ADC ha llegado al final de su vida útil (EOL). Para obtener más información, consulte la página del ciclo de vida de la versión

> **Nota:**
>
> La activación de las reglas de firma del cuerpo de la publicación y del cuerpo Citrix ADC respuesta puede afectar a la CPU

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999800	CVE-2019-12517	Plug-in WEB-WORDPRESS SlickQuiz versión 1.3.7.1 y anteriores: Vulnerabilidad de scripts entre sitios (CVE-2019-12517)
999801	CVE-2019-10392	Plug-in WEB-MISC Jenkins Git Client 2.8.4 y anteriores: Vulnerabilidad de inyección de comandos del sistema operativo (CVE-2019-10392)
999802	CVE-2019-8371	WEB-MISC OpenEMR anterior a 5.0.2: Vulnerabilidad de ejecución remota de código a través del campo Form_Filedata (CVE-2019-8371)
999803	CVE-2019-8371	WEB-MISC OpenEMR anterior a 5.0.2: Vulnerabilidad de ejecución remota de código a través del campo Form_Image (CVE-2019-8371)
999804	CVE-2019-12516	Plug-in WEB-WORDPRESS SlickQuiz versión 1.3.7.1 y anteriores: Vulnerabilidad de inyección SQL (CVE-2019-12516)
999805	CVE-2019-1262	WEB-MISC Microsoft Sharepoint Server: Vulnerabilidad de scripts entre sitios (CVE-2019-1262)

Actualización de firmas para diciembre de 2019

January 21, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la semana 2019-12-19. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

Las firmas son compatibles con las siguientes versiones de software de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 y 13.1.

La versión 12.0 de Citrix ADC ha llegado al final de su vida útil (EOL). Para obtener más información, consulte la página del ciclo de vida de la versión

> **Nota:**
>
> La activación de las reglas de firma del cuerpo de la publicación y del cuerpo Citrix ADC respuesta puede afectar a la CPU

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999760		Versiones de WEB-MISC FusionPBX anteriores a 4.4.7 y 4.5.5: Vulnerabilidad de ejecución remota de código a través de /app/exec/exec.php
999761	CVE-2019-12747	WEB-MISC Typo3 anterior a 8.7.27 y 9.5.8: Deserialización de datos no confiables (CVE-2019-12747)
999762	CVE-2019-13608	WEB-MISC Citrix StoreFront Server: Vulnerabilidad de inyección de entidades externas XML (CVE-2019-13608)

Regla de firma	ID de CVE	Descripción
999763		WEB-WORDPRESS WordPress anterior a 5.2.4: Vulnerabilidad de vista no autenticada de publicaciones/páginas privadas o borradores a través de FORM
999764		WEB-WORDPRESS WordPress anterior a 5.2.4: Vulnerabilidad de vista no autenticada de publicaciones/páginas privadas o borradores a través de URL
999765	CVE-2019-15954	WEB-MISC Total.js CMS 12.0.0: Vulnerabilidad de inyección de código JavaScript de widget a través de JSON (CVE-2019-15954)
999766	CVE-2019-15954	WEB-MISC Total.js CMS 12.0.0: Vulnerabilidad de inyección de código JavaScript de widget a través de FORM (CVE-2019-15954)
999767		Plug-in WEB-WORDPRESS SyntaxHighlighter Evolved antes de 5.3.1: Vulnerabilidad de scripting entre sitios almacenados a través de comentarios
999768		Plug-in WEB-WORDPRESS SyntaxHighlighter Evolved antes de 5.3.1: Vulnerabilidad de scripting entre sitios almacenados a través de POST

Regla de firma	ID de CVE	Descripción
999769		Plug-in WEB-WORDPRESS SyntaxHighlighter Evolved antes de 5.3.1: Vulnerabilidad de scripts entre sitios almacenados a través de JSON
999770	CVE-2019-16120	Plug-in de tíquets de eventos WEB-WORDPRESS antes de 4.10.7.2: Vulnerabilidad de inyección de CSV (CVE-2019-16120)
999771	CVE-2019-15029	WEB-MISC FusionPBX anterior a 4.4.8: Vulnerabilidad de ejecución remota de código (CVE-2019-15029)
999772		Complemento Sassy Social Share de WEB-WORDPRESS anterior a 3.3.4: Vulnerabilidad de scripts entre sitios no autenticados
999773		Complemento de suscriptores de correo electrónico y boletines de WEB-WORDPRESS Versión 4.3.1 y anteriores: Vulnerabilidad SQLi ciega no autenticada
999774	CVE-2019-3398	WEB-MISC Atlassian Confluence o centro de datos: Vulnerabilidad downloadallattachments de cruce de ruta (CVE-2019-3398)
999775	CVE-2019-15952	WEB-MISC Total.js CMS 12.0.0: Vulnerabilidad de recorrido de ruta de plantilla de página (CVE-2019-15952)

Regla de firma	ID de CVE	Descripción
999776	CVE-2019-17236	WEB-WORDPRESS IgniteUp Próximamente y Modo de Mantenimiento Plug-in hasta 3.4.0: Scripts entre sitios almacenados (CVE-2019-17236)
999777	CVE-2019-10475	Plug-in WEB-MISC Jenkins Build-Metrics 1.3: Vulnerabilidad de scripts entre sitios reflejados (CVE-2019-10475)
999778	CVE-2019-17132	WEB-MISC vBulletin anterior a 5.5.4 parche nivel 2: Vulnerabilidad de ejecución remota de código de extremo de la API UpdateAvatar (CVE-2019-17132)
999779	CVE-2019-14994	WEB-MISC Atlassian Jira Service Desk: Vulnerabilidad de recorrido de ruta (CVE-2019-14994)
999780	CVE-2019-19367	WEB-MISC FusionPBX 4.4.1 y anteriores: Vulnerabilidad de scripts entre sitios (CVE-2019-19367)
999781	CVE-2019-18668	Plug-in WEB-WORDPRESS Currency Switcher antes de 2.11.2: Vulnerabilidad de omisión de configuración de moneda a través de POST (CVE-2019-18668)

Regla de firma	ID de CVE	Descripción
999782	CVE-2019-18668	Plug-in WEB-WORDPRESS Currency Switcher antes de 2.11.2: Vulnerabilidad de omisión de configuración de moneda a través de GET (CVE-2019-18668)
999783	CVE-2019-16663	WEB-MISC RConfig 3.9.2 y anteriores: Vulnerabilidad de ejecución remota de código a través de Search.crud.php (CVE-2019-16663)
999784		WEB-MISC Apache Solr hasta 8.3.0 - Ejecución remota de código sin autenticar a través de la plantilla personalizada VelocityResponseWriter
999785	CVE-2019-17235	WEB-WORDPRESS IgniteUp próximamente y complemento de modo de mantenimiento hasta 3.4.0 - Divulgación de información a través de Csv (CVE-2019-17235)
999786	CVE-2019-17235	WEB-WORDPRESS IgniteUp próximamente y complemento de modo de mantenimiento hasta 3.4.0 - Divulgación de información a través de CCO (CVE-2019-17235)
999787	CVE-2019-12276	WEB-MISC GrandNode 4.40: Vulnerabilidad de recorrido de ruta LetsEncryptController (CVE-2019-12276)

Regla de firma	ID de CVE	Descripción
999788		Complemento de suscriptores de correo electrónico y boletines informativos de WEB-WORDPRESS anterior a la versión 4.2.3 - Divulgación de información
999789	CVE-2019-4013	WEB-MISC IBM BigFix Platform 9.5 - Carga arbitraria de archivos autenticados con privilegios de root (CVE-2019-4013)
999790	CVE-2019-11409	WEB-MISC FusionPBX versión 4.4.3 y anteriores: ejecución remota de código a través de /app/basic_operator_panel/exec.php (CVE-2019-11409)
999791	CVE-2019-11409	WEB-MISC FusionPBX versión 4.4.3 y anteriores: ejecución remota de código a través de /app/operator_panel/exec.php (CVE-2019-11409)
999792	CVE-2019-16662	WEB-MISC RConfig 3.9.2 y anteriores: ejecución remota de código sin autenticar mediante AjaxServerSettingsChk.php (CVE-2019-16662)
999793	CVE-2019-7609	WEB-MISC Elastic Kibana anterior a 5.6.15 y 6.6.1: La vulnerabilidad a la contaminación de prototipos permite un RCE no autenticado (CVE-2019-7609)

Regla de firma	ID de CVE	Descripción
999794	CVE-2019-10092	Servidor HTTP Apache WEB-MISC hasta 2.4.39: secuencias de comandos multisitio limitadas mod_proxy (CVE-2019-10092)
999795	CVE-2019-16520	Complemento de WEB-WORDPRESS All In One SEO Pack antes de 3.2.7: Vulnerabilidad de scripts entre sitios almacenados (CVE-2019-16520)
999796	CVE-2019-17234	WEB-WORDPRESS IgniteUp próximamente y complemento de modo de mantenimiento hasta 3.4.0 - Eliminación arbitraria de archivos (CVE-2019-17234)
999797	CVE-2019-16525	Complemento de lista de verificación de WEB-WORDPRESS anterior a la versión 1.1.9: Vulnerabilidad de scripts entre sitios (CVE-2019-16525)
999798		Complemento SVG seguro de WEB-WORDPRESS anterior a 1.9.6: Vulnerabilidad de scripts entre sitios
999799		Complemento de suscriptores de correo electrónico y boletines de WEB-WORDPRESS anterior a la versión 4.2.3: Creación de opciones arbitrarias no autenticadas

Versión 40 de la actualización de firmas

January 21, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas para la semana 2020-01-14. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad. La actualización de firma incluye el identificador de firma, la versión de la firma y la lista de CVE a los que se dirige.

Versión de firma

Las firmas son compatibles con las siguientes versiones de software de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 y 13.1.

La versión 12.0 de Citrix ADC ha llegado al final de su vida útil (EOL). Para obtener más información, consulte la página del ciclo de vida de la versión

> **Nota:**
>
> La versión 40 de actualización de firma incluye una corrección para la regla 1861 de firma incorrecta.
> La activación de las reglas de firma del cuerpo de la publicación y del cuerpo Citrix ADC respuesta puede afectar a la CPU

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999732	CVE-2019-1620	WEB-MISC Cisco Data Center Network Manager anterior a 11.2 (1): Vulnerabilidad de carga arbitraria de archivos (CVE-2019-1620)
999733	CVE-2019-16702	WEB-MISC Integard Pro 2.2.0.9026: Vulnerabilidad de desbordamiento de búfer NoJS (CVE-2019-16702)

Regla de firma	ID de CVE	Descripción
999734	CVE-2019-1621	WEB-MISC Cisco Data Center Network Manager anterior a 11.2 (1): Vulnerabilidad de descarga arbitraria de archivos (CVE-2019-1621)
999735	CVE-2019-8451	WEB-MISC Atlassian Jira Server anterior a 8.4.0: Vulnerabilidad de falsificación de solicitudes del lado del servidor (CVE-2019-8451)
999736		Complemento de cumplimiento de cookies GDPR de WEB-WORDPRESS anterior a 4.0.3: Vulnerabilidad de eliminación de parámetros arbitrarios autenticados
999737	CVE-2019-11287	WEB-MISC Pivotal RabbitMQ 3.7.x antes de 3.7.21 y 3.8.x antes de 3.8.1: Vulnerabilidad de denegación de servicio (CVE-2019-11287)
999738		Complementos definitivos de WEB-WORDPRESS para Elementor antes de 1.20.1 - Omisión de autenticación a través de la vulnerabilidad de inicio
999739		Complementos de WEB-WORDPRESS Ultimate para Elementor antes de 1.20.1 - Omisión de autenticación a través de la vulnerabilidad de inicio

Regla de firma	ID de CVE	Descripción
999740	CVE-2019-19366	WEB-MISC FusionPBX anterior a 4.4.10: Vulnerabilidad de scripts entre sitios en xml_cdr_search.php a través del parámetro de redireccionamiento (CVE-2019-19366)
999741	CVE-2019-16931	Complemento del visualizador WEB-WORDPRESS anterior a la versión 3.3.1: Vulnerabilidad de scripts entre sitios no autenticados (CVE-2019-16931)
999742	CVE-2019-16932	Complemento visualizador WEB-WORDPRESS anterior a la versión 3.3.1 - SSRF no autenticada (CVE-2019-16932)
999743	CVE-2019-1619	WEB-MISC Cisco Data Center Network Manager anterior a 11.1 (1): Vulnerabilidad de omisión de autenticación (CVE-2019-1619)
999744	CVE-2019-12562	WEB-MISC DotNetNuke antes de 9.4.0: Vulnerabilidad de scripts entre sitios almacenados (CVE-2019-12562)
999745	CVE-2019-8371	WEB-MISC OpenEMR anterior a 5.0.2: Vulnerabilidad de ejecución remota de código a través del campo Form_Filedata (CVE-2019-8371)

Regla de firma	ID de CVE	Descripción
999746	CVE-2019-8371	WEB-MISC OpenEMR anterior a 5.0.2: Vulnerabilidad de ejecución remota de código a través del campo Form_Image (CVE-2019-8371)
999747		Complementos de WEB-WORDPRESS Beaver Builder Ultimate antes de 1.24.1 - Omisión de autenticación mediante vulnerabilidad de inicio de sesión de Facebook
999748		Complementos de WEB-WORDPRESS Beaver Builder Ultimate antes de 1.24.1 - Omisión de autenticación mediante vulnerabilidad de inicio de sesión de Google
999749	CVE-2019-19650	WEB-MISC Zoho ManageEngine AM antes de la compilación 13640: SQLi a través del servlet del agente (CVE-2019-19650)
999750		WEB-MISC Zoho ManageEngine AM antes de la compilación 13620 - Divulgación de clave de API a través del servlet OPMRequestHandlerServlet
999751	CVE-2019-1622	WEB-MISC Cisco Data Center Network Manager 11.0 (1): Vulnerabilidad de divulgación de información (CVE-2019-1622)

Regla de firma	ID de CVE	Descripción
999752	CVE-2019-16759	WEB-MISC vBulletin anterior al parche 5.5.4 Nivel 1: Vulnerabilidad de ejecución remota de código (CVE-2019-16759)
999753		Imagen destacada de WEB-WORDPRESS del complemento de URL anterior a 2.7.8: controles de acceso faltantes en la vulnerabilidad de la API
999754	CVE-2019-10098	Servidor HTTP Apache WEB-MISC hasta 2.4.39: Vulnerabilidad de redireccionamiento autorreferencial de mod_rewrite (CVE-2019-10098)
999755	CVE-2019-1936	WEB-MISC Cisco UCS Director 6.0 a 6.6.1.0 y 6.7.0.0 a 6.7.1.0: Vulnerabilidad de inyección de comandos (CVE-2019-1936)
999756	CVE-2019-19649	WEB-MISC Zoho ManageEngine AM antes de la compilación 13620: SQLi no autenticado a través del parámetro EventID (CVE-2019-19649)
999757	CVE-2019-19649	WEB-MISC Zoho ManageEngine AM antes de la compilación 13620: SQLi no autenticado a través del parámetro de entidad (CVE-2019-19649)

Regla de firma	ID de CVE	Descripción
999758	CVE-2019-15036	WEB-MISC JetBrains TeamCity antes de 2019.1: Vulnerabilidad de inyección de comandos del sistema operativo (CVE-2019-15036)
999759	CVE-2019-17239	WEB-WORDPRESS Descarga complementos y temas desde el complemento Dashboard Hasta 1.5: Vulnerabilidad de scripts entre sitios almacenados (CVE-2019-17239)

Versión 41 de la actualización de firmas

January 21, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas para la semana 2020-02-04. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad. La actualización de firma incluye el identificador de firma, la versión de la firma y la lista de CVE a los que se dirige.

Versión de firma

Las firmas son compatibles con las siguientes versiones de software de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 y 13.1.

La versión 12.0 de Citrix ADC ha llegado al final de su vida útil (EOL). Para obtener más información, consulte la página del ciclo de vida de la versión

> **Nota:**
>
> La versión de actualización de firma 41 incluye una corrección para la regla de firma incorrecta 1861.
> La activación de las reglas de firma del cuerpo de la publicación y del cuerpo Citrix ADC respuesta puede afectar a la CPU

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999717		WEB-WORDPRESS WordPress versión 5.3.x y anteriores: Vulnerabilidad de denegación de servicio a través del método pingback.ping de xmlrpc.php
999718		WEB-WORDPRESS Copia de seguridad y staging del plug-in Time Capsule de WP antes de 1.21.16: Vulnerabilidad en la omisión de autenticación
999719	CVE-2019-19731	WEB-MISC Roxy Fileman para.NET 1.4.5: Vulnerabilidad de recorrido de ruta a través de RENAMEFILE (CVE-2019-19731)
999720	CVE-2019-19915	Redirecciones WEB-WORDPRESS 301 - Complemento Easy Redirect Manager hasta 2.4.0 - Múltiples vulnerabilidades (CVE-2019-19915)
999721	CVE-2019-17662	WEB-MISC Cybele Software ThinVNC anterior a la versión 1.0b1: Vulnerabilidad de cruce de directorios (CVE-2019-17662)

Regla de firma	ID de CVE	Descripción
999722	CVE-2020-6168	WEB-WORDPRESS Mínimo Próximamente y complemento de modo de mantenimiento anterior a 2.17: Vulnerabilidad de configuración de mantenimiento (CVE-2020-6168)
999723	CVE-2020-6166	Complemento mínimo de WEB-WORDPRESS Próximamente y modo de mantenimiento antes de 2.17: Vulnerabilidad de cambio de tema (CVE-2020-6166)
999724	CVE-2020-6166	Complemento mínimo de WEB-WORDPRESS Próximamente y modo de mantenimiento anterior a 2.17: Vulnerabilidad de configuración de exportación (CVE-2020-6166)
999725		Complemento de cliente InifiniteWP de WEB-WORDPRESS anterior a 1.9.4.5: Vulnerabilidad de omisión de autenticación
999726	CVE-2019-16773	Versiones de WordPress de WEB-WORDPRESS anteriores a 5.3.1: Vulnerabilidad de scripts entre sitios a través de la API REST con objeto JSON (CVE-2019-16773)

Regla de firma	ID de CVE	Descripción
999727	CVE-2019-16773	Versiones de WordPress de WEB-WORDPRESS anteriores a 5.3.1: Vulnerabilidad de scripts entre sitios a través de la API REST con FORM FIELD (CVE-2019-16773)
999728	CVE-2019-16773	Versiones de WEB-WORDPRESS WordPress anteriores a 5.3.1: Vulnerabilidad de scripts entre sitios a través de user-edit.php (CVE-2019-16773)
999729	CVE-2019-16773	Versiones de WEB-WORDPRESS WordPress anteriores a 5.3.1: Vulnerabilidad de scripts entre sitios a través de profile.php (CVE-2019-16773)
999730	CVE-2019-16113	WEB-MISC Bludit 3.9.2: Vulnerabilidad de ejecución remota de código de carga de imágenes a través de uuid (CVE-2019-16113)
999731	CVE-2019-16113	WEB-MISC Bludit 3.9.2: Vulnerabilidad de ejecución remota de código de carga de imágenes a través del nombre de archivo (CVE-2019-16113)

Actualización de firma para febrero de 2020

January 21, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la semana 2020-02-11.

Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

Las firmas son compatibles con las siguientes versiones de software de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 y 13.1.

La versión 12.0 de Citrix ADC ha llegado al final de su vida útil (EOL). Para obtener más información, consulte la página del ciclo de vida de la versión

> **Nota: La**
>
> habilitación de las reglas de firma de cuerpo posterior y cuerpo de respuesta puede afectar a la CPU de Citrix ADC.

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999707		Plug-in WEB-WORDPRESS WPCentral anterior a la versión 1.4.8: Vulnerabilidad de escalada de privilegios
999708	CVE-2019-15979	Administrador de red de centro de datos de Cisco WEB-MISC anterior a 11.3 (1): Vulnerabilidad de inyección de comandos (CVE-2019-15979)
999709	CVE-2019-15978	Administrador de red de centro de datos de Cisco WEB-MISC anterior a 11.3 (1): Vulnerabilidad de inyección de comandos (CVE-2019-15978)

Regla de firma	ID de CVE	Descripción
999710	CVE-2019-15975	WEB-MISC Cisco Data Center Network Manager anterior a 11.3 (1): Vulnerabilidad de omisión de autenticación (CVE-2019-15975)
999711	CVE-2019-15976	WEB-MISC Cisco Data Center Network Manager anterior a 11.3 (1): Vulnerabilidad de omisión de autenticación (CVE-2019-15976)
999712	CVE-2019-16405	WEB-MISC Centreon anterior a la versión 19.10.2: Vulnerabilidad de ejecución remota de código (CVE-2019-16405)
999713	CVE-2020-7048	Complemento de restablecimiento de base de datos WEB-WORDPRESS WP hasta 3.1: Vulnerabilidad de restablecimiento de tabla de base de datos no autenticada (CVE-2020-7048
999714	CVE-2020-7108	Plug-in WEB-WORDPRESS LearnDash anterior a la versión 3.1.2: Vulnerabilidad de scripts entre sitios reflejados (CVE-2020-7108)
999715	CVE-2019-15977	WEB-MISC Cisco Data Center Network Manager anterior a 11.3 (1): Vulnerabilidad de omisión de autenticación (CVE-2019-15977)

Regla de firma	ID de CVE	Descripción
999716	CVE-2020-2096	Plug-in WEB-MISC Jenkins Gitlab Hook versión 1.4.2 y anteriores: Vulnerabilidad de scripts entre sitios (CVE-2020-2096)

Actualización de firma para febrero de 2020

January 21, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la semana 2020-02-27. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

Las firmas son compatibles con las siguientes versiones de software de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 y 13.1.

La versión 12.0 de Citrix ADC ha llegado al final de su vida útil (EOL). Para obtener más información, consulte la página del ciclo de vida de la versión

> **Nota: La**
>
> habilitación de las reglas de firma de cuerpo posterior y cuerpo de respuesta puede afectar a la CPU de Citrix ADC.

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999696	CVE-2019-15983	WEB-MISC Cisco Data Center Network Manager anterior a 11.3 (1): Vulnerabilidad de entidad externa XML (CVE-2019-15983) a través de CablePlans

Regla de firma	ID de CVE	Descripción
999697	CVE-2019-20197	WEB-MISC Nagios XI 5.6.9: Vulnerabilidad de ejecución de comandos arbitrarios autenticados (CVE-2019-20197)
999698	CVE-2020-8417	Complemento de fragmentos de código de WEB-WORDPRESS anterior a 2.14.0: Vulnerabilidad CSRF (CVE-2020-8417)
999699		Plug-in WEB-WORDPRESS WPCentral anterior a la versión 1.4.8: Vulnerabilidad de escalada de privilegios
999700	CVE-2020-8596	Complemento de base de datos de participantes de WEB-WORDPRESS anterior a 1.9.5.6: Vulnerabilidad de inyección de SQL autenticada (CVE-2020-8596)
999701	CVE-2020-8426	Plug-in WEB-WORDPRESS Elementor Page Builder anterior a 2.8.5: Vulnerabilidad de scripts entre sitios reflejados autenticados (CVE-2020-8426)
999702	CVE-2019-19509	WEB-MISC RConfig 3.9.3: Vulnerabilidad de ejecución remota de código a través de ajaxArchiveFiles.php (CVE-2019-19509)

Regla de firma	ID de CVE	Descripción
999703	CVE-2019-8449	WEB-MISC Atlassian Jira Server anterior a 8.4.0: Vulnerabilidad de divulgación de información (CVE-2019-8449)
999704	CVE-2019-9194	WEB-MISC elFinder anterior a 2.1.48: Vulnerabilidad de inyección de comandos de PHP Connector (CVE-2019-9194)
999705	CVE-2019-15985	WEB-MISC Cisco Data Center Network Manager anterior a 11.3 (1): Vulnerabilidad de inyección SQL (CVE-2019-15985) a través de GetVMHostData
999706	CVE-2020-8549	Complemento de testimonios fuertes de WEB-WORDPRESS anterior a 2.40.1: Vulnerabilidad de scripts entre sitios almacenados (CVE-2020-8549)

Actualización de la firma para abril de 2020

January 21, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la semana 2020-04-27. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

Las firmas son compatibles con las siguientes versiones de software de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 y 13.1.

La versión 12.0 de Citrix ADC ha llegado al final de su vida útil (EOL). Para obtener más información, consulte la página del ciclo de vida de la versión

> **Nota: La**
>
> habilitación de las reglas de firma de cuerpo posterior y cuerpo de respuesta puede afectar a la CPU de Citrix ADC.

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999683	CVE-2020-9043	Plug-in WEB-WORDPRESS WPCentral anterior a 1.5.1: Vulnerabilidad de divulgación de clave de conexión (CVE-2020-9043)
999684		WEB-WORDPRESS Duplicate-Post Plug-in versión 3.2.3 y anterior: Scripts persistentes entre sitios
999685		WEB-WORDPRESS Duplicate-Post Plug-in versión 3.2.3 y anterior: Scripts persistentes entre sitios
999686	CVE-2020-0618	WEB-MISC Microsoft SQL Server Reporting Services: Vulnerabilidad de ejecución remota de código (CVE-2020-0618)
999687	CVE-2019-16278	WEB-MISC Nostromo Nhttpd anterior a 1.3.7 - La función Strcutl permite la ejecución remota de código no autenticado (CVE-2019-16278)

Regla de firma	ID de CVE	Descripción
999688	CVE-2019-1937	WEB-MISC Cisco UCS Director 6.6.0.0 a 6.6.1.0 y 6.7.0.0 a 6.7.1.0: Vulnerabilidad de omisión de autenticación (CVE-2019-1937)
999689		WEB-WORDPRESS Duplicate-Post Plug-in versión 3.2.3 y anterior: Scripts persistentes entre sitios
999690	CVE-2020-9006	Plug-in WEB-WORDPRESS Popup Builder anterior a 3.0 - Inyección SQL a través de la vulnerabilidad de deserialización de PHP (CVE-2020-9006)
999691		WEB-WORDPRESS Duplicate-Post Plug-in versión 3.2.3 y anterior: Scripts persistentes entre sitios
999692		WEB-MISC evita el contrabando de solicitudes a través del encabezado de longitud de contenido y codificación de transferencia
999693		Plug-in WEB-WORDPRESS ThemeGrill Demo Importer anterior a 1.6.3: Vulnerabilidad de omisión de autenticación y borrado de

Regla de firma	ID de CVE	Descripción
999694	CVE-2019-17237	WEB-WORDPRESS IgniteUp próximamente y complemento de modo de mantenimiento anterior a 3.4.1: Vulnerabilidad CSRF a través del mensaje (CVE-2019-17237)
999695	CVE-2019-17237	Próximamente IgniteUp de WEB-WORDPRESS y complemento de modo de mantenimiento anterior a 3.4.1: Vulnerabilidad CSRF a través del tema (CVE-2019-17237)

Actualización de firmas para mayo de 2020

January 21, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la semana 2020-05-26. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

Las firmas son compatibles con las siguientes versiones de software de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 y 13.1.

La versión 12.0 de Citrix ADC ha llegado al final de su vida útil (EOL). Para obtener más información, consulte la página del ciclo de vida de la versión

> **Nota:**
>
> La activación de las reglas de firma del cuerpo de la publicación y del cuerpo Citrix ADC respuesta puede afectar a la CPU Según la última versión de Snort, se han eliminado las reglas de firma con ID 1258, 1306, 2520, 2661, 5695, 10996, 11817, 12056, 15471, 17049 y 21634.

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999666		Complemento duplicador WEB-WORDPRESS anterior a 1.3.28: Vulnerabilidad de descarga de archivos arbitrarios no autenticados
999667	CVE-2020-10220	RConfig WEB-MISC hasta 3.94: Vulnerabilidad de inyección SQL (CVE-2020-10220)
999668	CVE-2020-5844	WEB-MISC Artica Pandora FMS 7.0 - Ejecución de archivos arbitrarios de tipo peligroso a través de /attachment/files_repo/ (CVE-2020-5844)
999669	CVE-2020-8813	Cactus WEB-MISC anteriores a 1.2.10: Vulnerabilidad de ejecución remota de código a través de graph_realtime.php (CVE-2020-8813)
999670	CVE-2020-8654	WEB-MISC EyesOfNetwork 5.3: Vulnerabilidad de ejecución remota de código (CVE-2020-8654)
999671	CVE-2020-10196	Plug-in WEB-WORDPRESS Sygnoos Popup Builder anterior a 3.64.1: Vulnerabilidad de scripts entre sitios no autenticados (CVE-2020-10196)
999672	CVE-2019-15949	WEB-MISC Nagios XI anterior a 5.6.6 - Ejecución remota de código como vulnerabilidad raíz (CVE-2019-15949)

Regla de firma	ID de CVE	Descripción
999673	CVE-2020-10879	WEB-MISC RConfig 3.9.5 y anteriores: Vulnerabilidad de ejecución remota de código a través de search.crud.php (CVE-2020-10879)
999674	CVE-2020-8656	WEB-MISC EyesOfNetwork 5.3: Vulnerabilidad de inyección SQL de la API de EyesOfNetwork 2.4.2 (CVE-2020-8656)
999675	CVE-2020-10195	Plug-in WEB-WORDPRESS Sygnoos Popup Builder anterior a 3.64.1 - Divulgación de información del sistema autenticada (CVE-2020-10195)
999676	CVE-2020-10195	Plug-in WEB-WORDPRESS Sygnoos Popup Builder anterior a 3.64.1 - Divulgación de información de suscriptor autenticado (CVE-2020-10195)
999677	CVE-2020-10195	Plug-in WEB-WORDPRESS Sygnoos Popup Builder anterior a 3.64.1 - Modificación de configuración autenticada (CVE-2020-10195)
999678	CVE-2020-0646	Microsoft SharePoint Server: Vulnerabilidad de ejecución remota de código de flujo de trabajo de .NET Framework mediante SOAP 1.2 (CVE-2020-0646)

Regla de firma	ID de CVE	Descripción
999679	CVE-2020-0646	Microsoft SharePoint Server: Vulnerabilidad de ejecución remota de código de flujo de trabajo de .NET Framework mediante SOAP 1.1 (CVE-2020-0646)
999680	CVE-2020-10221	WEB-MISC RConfig hasta 3.94: Vulnerabilidad de ejecución remota de código (CVE-2020-10221)
999681	CVE-2019-19134	WEB-WORDPRESS Hero Maps Premium anterior a 2.2.3: Vulnerabilidad de scripts entre sitios reflejados no autenticados (CVE-2019-19134)
999682	CVE-2020-10385	Plug-in WPForms de WEB-WORDPRESS anterior a 1.5.9: Vulnerabilidad de scripts entre sitios almacenados (CVE-2020-10385)

Actualización de la firma para junio de 2020

January 21, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la semana 2020-06-03. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

Las firmas son compatibles con las siguientes versiones de software de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 y 13.1.

La versión 12.0 de Citrix ADC ha llegado al final de su vida útil (EOL). Para obtener más información, consulte la página del ciclo de vida de la versión

> **Nota:**
>
> La activación de las reglas de firma del cuerpo de la publicación y del cuerpo Citrix ADC respuesta puede afectar a la CPU

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999643		Plug-in WEB-WORDPRESS 10Web Map Builder para Google Maps anterior a 10.0.64: Vulnerabilidad de scripts entre sitios no autenticados a través de la página gmwd_setup
999644		WEB-WORDPRESS 10Web Map Builder para el complemento 10.0.64 y anteriores de Google Maps: Vulnerabilidad de scripts entre sitios a través de la página options_gmwd
999645	CVE-2020-5187	WEB-MISC DNN Hasta 9.4.4: Vulnerabilidad de recorrido de ruta a través de URL (CVE-2020-5187)
999646	CVE-2020-5187	WEB-MISC DNN hasta 9.4.4: Vulnerabilidad de recorrido de ruta a través de local (CVE-2020-5187)

Regla de firma	ID de CVE	Descripción
999647	CVE-2020-9335	Complemento de galería de fotos WEB-WORDPRESS anterior a 1.5.46: Vulnerabilidad de scripts entre sitios a través del campo image_alt_text_ (CVE-2020-9335)
999648	CVE-2020-9335	Complemento de galería de fotos WEB-WORDPRESS anterior a 1.5.46: Vulnerabilidad de scripts entre sitios a través del campo Nombre (CVE-2020-9335)
999649	CVE-2020-9335	Complemento de galería de fotos WEB-WORDPRESS anterior a 1.5.46: Vulnerabilidad de scripts entre sitios a través de campos de descripción (CVE-2020-9335)
999650	CVE-2020-10189	WEB-MISC Zoho ManageEngine Desktop Central anterior a 10.0.479: Vuln de ejecución de código remoto no autenticado (CVE-2020-10189)
999651	CVE-2020-10189	WEB-MISC Zoho ManageEngine Desktop Central anterior a 10.0.479: Vuln de carga de archivos arbitrarios no autenticados (CVE-2020-10189)

Regla de firma	ID de CVE	Descripción
999652		Campos de pago flexibles de WEB-WORDPRESS para el complemento WooCommerce antes de 2.3.2 - Modificación de configuración no autenticada Vuln
999653	CVE-2020-0688	WEB-MISC Microsoft Exchange Server: Vulnerabilidad de ejecución remota de código de clave de validación (CVE-2020-0688)
999654	CVE-2020-8947, CVE-2019-20224	WEB-MISC Artica Pandora FMS 7.0: Vulnerabilidad de ejecución remota de código a través del parámetro ip_src (CVE-2020-8947, CVE-2019-20224)
999655	CVE-2020-8947, CVE-2019-20224	WEB-MISC Artica Pandora FMS 7.0: Vulnerabilidad de ejecución remota de código a través del parámetro dst_port (CVE-2020-8947, CVE-2019-20224)
999656	CVE-2020-8947, CVE-2019-20224	WEB-MISC Artica Pandora FMS 7.0: Vulnerabilidad de ejecución remota de código a través del parámetro src_port (CVE-2020-8947, CVE-2019-20224)
999657	CVE-2020-8947, CVE-2019-20224	WEB-MISC Artica Pandora FMS 7.0: Vulnerabilidad de ejecución remota de código a través del parámetro ip_dst (CVE-2020-8947, CVE-2019-20224)

Regla de firma	ID de CVE	Descripción
999658	CVE-2020-5186	WEB-MISC DNN hasta 9.5.0: Vulnerabilidad de scripts entre sitios a través de la carga de XML de diario (CVE-2020-5186)
999659		Complemento de página WEB-WORDPRESS WP Sitemap 1.6.2 y anteriores: Vulnerabilidad de scripts entre sitios a través de wsp_exclude_pages
999660	CVE-2020-5188	WEB-MISC DNN hasta 9.5.0: Vulnerabilidad de permisos inseguros a través de UploadFromURL (CVE-2020-5188)
999661	CVE-2020-5188	WEB-MISC DNN hasta 9.5.0: Vulnerabilidad de permisos inseguros a través de UploadFromLocal (CVE-2020-5188)
999662	CVE-2020-7799	WEB-MISC FusionAuth anterior a 1.11.0: Vulnerabilidad de ejecución remota de código a través del tema de la API (CVE-2020-7799)
999663	CVE-2020-7799	WEB-MISC FusionAuth anterior a 1.11.0: Vulnerabilidad de ejecución remota de código a través de una plantilla de correo electrónico de API (CVE-2020-7799)

Regla de firma	ID de CVE	Descripción
999664	CVE-2020-7799	WEB-MISC FusionAuth anterior a 1.11.0: Vulnerabilidad de ejecución remota de código a través del tema GUI (CVE-2020-7799)
999665	CVE-2020-7799	WEB-MISC FusionAuth anterior a 1.11.0: Vulnerabilidad de ejecución remota de código a través de la plantilla de correo electrónico GUI (CVE-2020-7799)

Actualización de la firma para junio de 2020

January 21, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la semana 2020-06-12. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

Las firmas son compatibles con las siguientes versiones de software de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 y 13.1.

La versión 12.0 de Citrix ADC ha llegado al final de su vida útil (EOL). Para obtener más información, consulte la página del ciclo de vida de la versión

> **Nota:**
>
> La activación de las reglas de firma del cuerpo de la publicación y del cuerpo Citrix ADC respuesta puede afectar a la CPU

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999580	CVE-2020-6010	Complemento LMS de WEB-WORDPRESS LearnPress anterior a 3.2.6.9: Vulnerabilidad de inyección SQL (CVE-2020-6010)
999581		WEB-MISC Nagios XI hasta 5.6.13: Vulnerabilidad de ejecución de comandos arbitrarios de Service Command_Test
999582	CVE-2020-0932	Microsoft SharePoint Server: Vulnerabilidad de ejecución remota de código de marcado de origen de WebPart mediante SOAP 1.2 (CVE-2020-0932)
999583	CVE-2020-0932	Microsoft SharePoint Server: Vulnerabilidad de ejecución remota de código de marcado de origen de WebPart a través de SOAP 1.1 (CVE-2020-0932)
999584	CVE-2020-12642	Plug-in WEB-WORDPRESS Ninja Forms anterior a 3.4.24.2: Vulnerabilidad de falsificación de solicitudes entre sitios a través de campos de importación (CVE-2020-12642)
999585	CVE-2020-12642	Plug-in WEB-WORDPRESS Ninja Forms anterior a 3.4.24.2: Vulnerabilidad de falsificación de solicitudes entre sitios a través del formulario de importación (CVE-2020-12642)

Regla de firma	ID de CVE	Descripción
999586	CVE-2020-11450	WEB-MISC Microstrategy Web 10.4: Vulnerabilidad de divulgación de información (CVE-2020-11450)
999587	CVE-2020-7935	WEB-MISC Artica Pandora FMS 7.0 - Carga sin restricciones de archivo con vulnerabilidad de tipo peligroso permite RCE (CVE-2020-7935)
999588	CVE-2020-12116	WEB-MISC Zoho ManageEngine OpManager antes de la compilación 125125: Vulnerabilidad de divulgación de información (CVE-2020-12116)
999589		WEB-WORDPRESS Elementor Page Builder anterior a 2.9.6: Vulnerabilidad de escalada de privilegios
999590	CVE-2020-11738	WEB-WORDPRESS - Complemento duplicador de Snap Creek anterior a 1.3.28: Vulnerabilidad de recorrido de ruta (CVE-2020-11738)
999591	CVE-2020-10389	WEB-MISC Chadha PHPKB Estándar multilingüe 9: Vulnerabilidad de ejecución remota de código (CVE-2020-10389)

Regla de firma	ID de CVE	Descripción
999592	CVE-2020-11516	Formulario de contacto WEB-WORDPRESS 7 Complemento Datepicker Hasta 2.6.0: Vulnerabilidad de scripts entre sitios almacenados (CVE-2020-11516)
999593		WEB-MISC Nagios XI hasta 5.6.13: Vulnerabilidad de ejecución de comandos arbitrarios Export-RRD a través de Step
999594		WEB-MISC Nagios XI hasta 5.6.13: Vulnerabilidad de ejecución de comandos arbitrarios Export-RRD a través de End
999595		WEB-MISC Nagios XI hasta 5.6.13: Vulnerabilidad de ejecución de comandos arbitrarios Export-RRD a través del inicio
999596	CVE-2019-19799	Administrador de aplicaciones de Zoho ManageEngine anterior a 14600: Vulnerabilidad de divulgación de información (CVE-2019-19799)
999597	CVE-2020-10458	WEB-MISC Chadha PHPKB Standard Multi-Language 9: Vulnerabilidad de eliminación arbitraria de carpetas (CVE-2020-10458)

Regla de firma	ID de CVE	Descripción
999598	CVE-2017-9822	WEB-MISC DNN anterior a 9.1.1: Vulnerabilidad de ejecución remota de código a través de la cookie de personalización DNN (CVE-2017-9822)
999599	CVE-2020-7953	WEB-MISC OpServices OpMon 9.3.2: Vulnerabilidad de divulgación de información no autenticada a través del parámetro nmap_options (CVE-2020-7953)
999600	CVE-2020-7953	WEB-MISC OpServices OpMon 9.3.2: Vulnerabilidad de divulgación de información no autenticada a través de host Param (CVE-2020-7953)
999601		WEB-MISC Bolt CMS 3.7.0 - Cambio de nombre de archivo a una vulnerabilidad de tipo peligroso mediante el parámetro newname
999602		WEB-MISC Bolt CMS 3.7.0: Vulnerabilidad de recorrido de ruta a través del parámetro newname
999603		WEB-MISC Bolt CMS 3.7.0: Vulnerabilidad de recorrido de ruta a través del parámetro oldname
999604		WEB-MISC Bolt CMS 3.7.0: Vulnerabilidad de recorrido de ruta mediante el parámetro principal

Regla de firma	ID de CVE	Descripción
999605		WEB-MISC Bolt CMS 3.7.0: Vulnerabilidad de validación de campo incorrecta en el parámetro displayname
999606	CVE-2020-9004	WEB-MISC - Wowza Streaming Engine 4.7.8: Vulnerabilidad de autorización incorrecta en View Logs (CVE-2020-9004)
999607	CVE-2020-9004	WEB-MISC - Wowza Streaming Engine 4.7.8: Vulnerabilidad de autorización incorrecta en la configuración de caché de medios (CVE-2020-9004)
999608	CVE-2020-9004	WEB-MISC - Wowza Streaming Engine 4.7.8: Vulnerabilidad de autorización incorrecta en la configuración de las aplicaciones (CVE-2020-9004)
999609	CVE-2020-9004	WEB-MISC - Wowza Streaming Engine 4.7.8: Vulnerabilidad de autorización incorrecta en la configuración del servidor (CVE-2020-9004)
999610		WEB-MISC PrestaShop 1.7.6.5: Vulnerabilidad CSRF a través de Filemanager
999611	CVE-2020-10238	WEB-MISC Joomla! Anterior a 3.9.16: Vulnerabilidad de omisión de seguridad a través de com_templates (CVE-2020-10238)

Regla de firma	ID de CVE	Descripción
999612	CVE-2020-11510	Complemento LMS de WEB-WORDPRESS LearnPress anterior a 3.2.6.9 - Escalamiento de privilegios a través de learnpress_create_page (CVE-2020-11510)
999613	CVE-2020-11510	Complemento LMS de WEB-WORDPRESS LearnPress anterior a 3.2.6.9 - Escalamiento de privilegios a través de learn-press_update_order_status (CVE-2020-11510)
999614	CVE-2020-8636	WEB-MISC OpServices OpMon 9.3.2: Vulnerabilidad de ejecución remota de código no autenticada mediante el parámetro nmap_options (CVE-2020-8636)
999615	CVE-2020-8636	WEB-MISC OpServices OpMon 9.3.2: Vulnerabilidad de ejecución remota de código no autenticada a través del parámetro de host (CVE-2020-8636)
999616	CVE-2020-11511	Complemento LMS de WEB-WORDPRESS LearnPress anterior a 3.2.6.9 - Escalamiento de privilegios a través de aceptar para ser profesor (CVE-2020-11511)

Regla de firma	ID de CVE	Descripción
999617	CVE-2020-11451	WEB-MISC Microstrategy Web: Vulnerabilidad de carga de tipos de archivos no seguros a través de JSP (CVE-2020-11451)
999618	CVE-2020-11451	WEB-MISC Microstrategy Web: Vulnerabilidad de carga de tipos de archivos no seguros a través de ASP (CVE-2020-11451)
999619	CVE-2020-11515	Plug-in WEB-WORDPRESS WP SEO Rank Math antes de 1.0.41: Vulnerabilidad de redirección a través de la API REST a través de URL (CVE-2020-11515)
999620	CVE-2020-11515	Plug-in WEB-WORDPRESS WP SEO Rank Math antes de 1.0.41: Vulnerabilidad de redirección a través de REST API rest_route Param (CVE-2020-11515)
999621	CVE-2020-10457	WEB-MISC Chadha PHPKB Standard Multi-Language 9: Vulnerabilidad de cambio de nombre arbitrario de archivos a través de ImgName (CVE-2020-10457)
999622	CVE-2020-10457	WEB-MISC Chadha PHPKB Standard Multi-Language 9: Vulnerabilidad de cambio de nombre arbitrario de archivos a través de ImgURL (CVE-2020-10457)

Regla de firma	ID de CVE	Descripción
999623	CVE-2019-1821	WEB-MISC Cisco Prime Infrastructure: Vulnerabilidad de ejecución remota de código (CVE-2019-1821)
999624		Plug-in WEB-WORDPRESS Page Builder anterior a 2.10.16: Vulnerabilidad CSRF a través de Ajax action_builder_content
999625		Plug-in WEB-WORDPRESS Page Builder anterior a 2.10.16: Vulnerabilidad CSRF a través de Live Editor
999626	CVE-2020-11514	Plug-in WEB-WORDPRESS WP SEO Rank Math antes de 1.0.41 - Escalamiento de privilegios a través de la API REST a través de URL (CVE-2020-11514)
999627	CVE-2020-11514	Plug-in WEB-WORDPRESS WP SEO Rank Math antes de 1.0.41 - Escalamiento de privilegios a través de REST API rest_route Param (CVE-2020-11514)
999628	CVE-2019-6713	WEB-MISC ThinkCMF anterior a 5.0.190312: Vulnerabilidad de inyección de código a través de /route/editpost.html (CVE-2019-6713)
999629	CVE-2019-6713	WEB-MISC ThinkCMF anterior a 5.0.190312: Vulnerabilidad de inyección de código a través de /route/addpost.html (CVE-2019-6713)

Regla de firma	ID de CVE	Descripción
999630		Plug-in WEB-WORDPRESS Google Site Kit anterior a 1.8.0: Vulnerabilidad de verificación desprotegida
999631	CVE-2020-9315	WEB-MISC Oracle iPlanet Web Server 7.0.x: Vulnerabilidad de control de acceso incorrecta (CVE-2020-9315)
999632	CVE-2020-1947	WEB-MISC Apache ShardingSphere 4.0.0-RC3 y 4.0.0: Vulnerabilidad de ejecución remota de código de SnakeYAML (CVE-2020-1947)
999633	CVE-2020-7961	Portal de Liferay anterior a 7.2.1 CE GA2: Vulnerabilidad de RCE de deserialización de JSONWS a través de JSON-RPC (CVE-2020-7961)
999634	CVE-2020-7961	Portal de Liferay anterior a 7.2.1 CE GA2: Vulnerabilidad de RCE de deserialización de JSONWS a través de la ruta URL (CVE-2020-7961)
999635	CVE-2020-7961	Liferay Portal anterior a 7.2.1 CE GA2: Vulnerabilidad RCE de deserialización de JSONWS a través de formulario y consulta URI (CVE-2020-7961)
999636	CVE-2020-8518	WEB-MISC Horde Groupware Webmail Edition 5.2.22: Vulnerabilidad de ejecución remota de código (CVE-2020-8518)

Regla de firma	ID de CVE	Descripción
999637	CVE-2020-7351	WEB-MISC Fonality Trixbox CE 2.8.0.4 y anteriores: Vulnerabilidad de ejecución remota de código (CVE-2020-7351)
999638	CVE-2020-12720	WEB-MISC vBulletin anterior a 5.6.1 parche nivel 1: Vulnerabilidad de inyección SQL no autenticada (CVE-2020-12720)
999639	CVE-2019-19800	Administrador de aplicaciones de Zoho ManageEngine anterior a 14520: Vulnerabilidad de recorrido de ruta (CVE-2019-19800)
999640	CVE-2020-10386	WEB-MISC Chadha PHPKB Estándar multilingüe 9 - Ejecución remota de código (CVE-2020-10386)
999641	CVE-2020-8497	WEB-MISC Artica Pandora FMS 7.0: Vulnerabilidad de divulgación de información no autenticada (CVE-2020-8497)
999642	CVE-2020-6009	Complemento LearnDash LMS de WEB-WORDPRESS anterior a 3.1.6: Vulnerabilidad de inyección SQL no autenticada (CVE-2020-6009)

Actualización de la firma para julio de 2020

January 21, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la semana 2020-07-01. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

Las firmas son compatibles con las siguientes versiones de software de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 y 13.1.

La versión 12.0 de Citrix ADC ha llegado al final de su vida útil (EOL). Para obtener más información, consulte la página del ciclo de vida de la versión

> **Nota:**
>
> La activación de las reglas de firma del cuerpo de la publicación y del cuerpo Citrix ADC respuesta puede afectar a la CPU

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999563		Complemento PageLayer de WEB-WORDPRESS Page Builder antes de 1.1.2: Vulnerabilidad de scripts entre sitios a través de pagelayer_cf_to_email
999564		Complemento PageLayer de WEB-WORDPRESS Page Builder antes de 1.1.2: Vulnerabilidad de scripts entre sitios a través de pagelayer-phone

Regla de firma	ID de CVE	Descripción
999565		Complemento PageLayer de WEB-WORDPRESS Page Builder antes de 1.1.2: Vulnerabilidad de scripts entre sitios a través de la dirección de capa de página
999566	CVE-2020-1961	Síncope de Apache WEB-MISC: Vulnerabilidad de inyección de plantillas en el lado del servidor (CVE-2020-1961)
999567	CVE-2019-18935	Interfaz de usuario de Telerik de progreso WEB-MISC para ASP .NET AJAX: Vulnerabilidad de deserialización de RadAsyncUpload .NET (CVE-2019-18935)
999568	CVE-2020-9463	WEB-MISC Centreon 19.10: Vulnerabilidad de inyección de comandos del sistema operativo (CVE-2020-9463)
999569		Plug-in WEB-WORDPRESS Support Review anterior a 3.7.6: Vulnerabilidad de scripts entre sitios almacenados no autenticados
999570		Complemento PageLayer de WEB-WORDPRESS Page Builder antes de 1.1.2: Vuln de control de acceso incorrecto a través de pagelayer_save_template

Regla de firma	ID de CVE	Descripción
999571		Complemento PageLayer de WEB-WORDPRESS Page Builder antes de 1.1.2: Vuln de control de acceso incorrecto a través de pagelayer_update_site_title
999572		Complemento PageLayer de WEB-WORDPRESS Page Builder antes de 1.1.2: Vuln de control de acceso incorrecto a través de pagelayer_save_content
999573		Carga de arrastrar y soltar WEB-WORDPRESS para el formulario de contacto 7 antes de 1.3.3.3: Vulnerabilidad de carga de extensión de archivo
999574	CVE-2020-9314	WEB-MISC Oracle iPlanet Web Server 7.0.x: Vulnerabilidad de inyección de imágenes (CVE-2020-9314)
999575	CVE-2020-9484	WEB-MISC Múltiples versiones de Apache Tomcat: deserialización de datos no confiables (CVE-2020-9484)
999576	CVE-2020-13252	WEB-MISC Centreon anterior al 19.04.15: Vulnerabilidad de ejecución remota de código (CVE-2020-13252)
999577	CVE-2020-11453	WEB-MISC Microstrategy Web: Vulnerabilidad CSRF a través de SOAP (CVE-2020-11453)
999578	CVE-2020-11453	WEB-MISC Microstrategy Web: Vulnerabilidad CSRF (CVE-2020-11453)

Regla de firma	ID de CVE	Descripción
999579	CVE-2020-7237	Cactus WEB-MISC anteriores a 1.2.8: Vulnerabilidad de ejecución remota de código (CVE-2020-7237)

Actualización de firmas para agosto de 2020

January 21, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la semana 2020-08-26. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

Las firmas son compatibles con las siguientes versiones de software de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 y 13.1.

La versión 12.0 de Citrix ADC ha llegado al final de su vida útil (EOL). Para obtener más información, consulte la página del ciclo de vida de la versión

> **Nota: La**
>
> habilitación de las reglas de firma de cuerpo posterior y cuerpo de respuesta puede afectar a la CPU de Citrix ADC.

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999556	CVE-2020-13241	WEB-MISC Microweber 1.1.18 - Carga sin restricciones de archivo con vulnerabilidad de tipo peligroso (CVE-2020-13241)

Regla de firma	ID de CVE	Descripción
999557	CVE-2020-3250	WEB-MISC Cisco UCS Director: Vulnerabilidad de recorrido de ruta de API REST a través de userAPIDownloadFile (CVE-2020-3250)
999558		Plug-in WEB-WORDPRESS PageBuilder KingComposer anterior a 2.9.4 - Eliminación arbitraria de directorios a través de action=bulk-delete
999559		Plug-in WEB-WORDPRESS PageBuilder KingComposer anterior a 2.9.4: Vulnerabilidad de ejecución remota de código a través
999560	CVE-2018-1999024	WEB-MISC Moodle: Vulnerabilidad de scripts entre sitios Unicode en MathJax (CVE-2018-1999024)
999561	CVE-2020-13693	Complemento bbPress de WEB-WORDPRESS anterior a 2.6.5: Vulnerabilidad de escalada de privilegios no autenticada (CVE-2020-13693)
999562	CVE-2020-12847	Celdas Pydio WEB-MISC anteriores a 2.0.7: Vulnerabilidad de ejecución remota de código (CVE-2020-12847)

Actualización de firmas para septiembre de 2020

January 21, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la semana 2020-09-

26. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

Las firmas son compatibles con las siguientes versiones de software de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 y 13.1.

La versión 12.0 de Citrix ADC ha llegado al final de su vida útil (EOL). Para obtener más información, consulte la página del ciclo de vida de la versión

> **Nota: La**
>
> habilitación de las reglas de firma de cuerpo posterior y cuerpo de respuesta puede afectar a la CPU de Citrix ADC.

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999532	CVE-2020-1956	WEB-MISC Apache Kylin - Ejecución remota de código de migración de cubos a través de dest-config (CVE-2020-1956)
999533	CVE-2020-1956	WEB-MISC Apache Kylin - Ejecución remota de código de migración de cubo a través de src-config (CVE-2020-1956)
999534	CVE-2020-1956	WEB-MISC Apache Kylin - Ejecución remota de código de migración de cubo a través de ProjectName (CVE-2020-1956)
999535	CVE-2020-3247	WEB-MISC Cisco UCS Director: Vulnerabilidad de creación de enlaces simbólicos arbitrarios CopyFileRunnable (CVE-2020-3247)

Regla de firma	ID de CVE	Descripción
999536	CVE-2019-16872	Portainer WEB-MISC anterior a 1.22.1: Vulnerabilidad de control de acceso incorrecta a través de pilas de actualizaciones (CVE-2019-16872)
999537	CVE-2019-16872	Portainer WEB-MISC anterior a 1.22.1: Vulnerabilidad de control de acceso incorrecta mediante la creación de pilas (CVE-2019-16872)
999538	CVE-2020-13855	WEB-MISC Artica Pandora FMS 7.44: Vulnerabilidad de carga arbitraria de archivos a través del administrador del repositorio de archivos (CVE-2020-13855)
999539	CVE-2020-5902	WEB-MISC F5 BIG-IP: Vulnerabilidad de RCE de la interfaz de usuario de administración de tráfico a través de /hsqldb (CVE-2020-5902)
999540	CVE-2020-5902	WEB-MISC F5 BIG-IP: Vulnerabilidad de RCE de la interfaz de usuario de gestión de tráfico a través de /tmui (CVE-2020-5902)
999541		WEB-MISC WebERP 4.15.1 y anteriores: Vulnerabilidad de divulgación de información no autenticada

Regla de firma	ID de CVE	Descripción
999542	CVE-2020-7209	WEB-MISC HP LinuxKI anterior a 6.0-2: Vulnerabilidad de RCE no autenticada a través de timeline.php y parámetro de marca de tiempo (CVE-2020-7209)
999543	CVE-2020-7209	WEB-MISC HP LinuxKI anterior a 6.0-2: Vulnerabilidad de RCE no autenticada a través de kivis.php y ts Param (CVE-2020-7209)
999544	CVE-2020-7209	WEB-MISC HP LinuxKI anterior a 6.0-2: Vulnerabilidad de RCE no autenticada a través de kivis.php y end Param (CVE-2020-7209)
999545	CVE-2020-7209	WEB-MISC HP LinuxKI anterior a 6.0-2: Vulnerabilidad de RCE no autenticada a través de kivis.php e inicio de Param (CVE-2020-7209)
999546	CVE-2020-7209	WEB-MISC HP LinuxKI anterior a 6.0-2: Vulnerabilidad de RCE no autenticada a través de kivis.php y pid Param (CVE-2020-7209)

Regla de firma	ID de CVE	Descripción
999547	CVE-2020-7209	WEB-MISC HP LinuxKI anterior a 6.0-2: Vulnerabilidad de RCE no autenticada a través de kidsk_trace_view.php y end Param (CVE-2020-7209)
999548	CVE-2020-7209	WEB-MISC HP LinuxKI anterior a 6.0-2: Vulnerabilidad de RCE no autenticada a través de kidsk_trace_view.php e inicio de Param (CVE-2020-7209)
999549		WEB-MISC PHP-Fusion anterior a 9.03.70: Vulnerabilidad de inyección de objetos PHP
999550	CVE-2020-1181	WEB-MISC Microsoft SharePoint Server: ejecución remota de código a través de elementos web (CVE-2020-1181)
999551	CVE-2020-10547	RConfig WEB-MISC anterior a 3.9.5: Vulnerabilidad de SQLi no autenticada en elementos de directiva a través de SearchColumn (CVE-2020-10547)
999552	CVE-2020-10547	RConfig WEB-MISC anterior a 3.9.5: Vulnerabilidad de SQLi no autenticada en elementos de directiva a través de SearchField (CVE-2020-10547)

Regla de firma	ID de CVE	Descripción
999553	CVE-2020-8605	WEB-MISC Dispositivo virtual de seguridad web Trend Micro InterScan antes de 6.5 SP2 parche 4: Vulnerabilidad de RCE (CVE-2020-8605)
999554	CVE-2019-10068	WEB-MISC Kentico CMS Múltiples versiones: Vulnerabilidad de ejecución remota de código no autenticada (CVE-2019-10068)
999555	CVE-2020-11108	Vulnerabilidad de RCE autenticada (CVE-2020-11108): Vulnerabilidad de IP de WEB-MISC hasta 4.4

Actualización de firmas para octubre de 2020

January 21, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la semana 2020-10-13. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

Las firmas son compatibles con las siguientes versiones de software de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 y 13.1.

La versión 12.0 de Citrix ADC ha llegado al final de su vida útil (EOL). Para obtener más información, consulte la página del ciclo de vida de la versión

> **Nota: La**
>
> habilitación de las reglas de firma de cuerpo posterior y cuerpo de respuesta puede afectar a la CPU de Citrix ADC.

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999505		Complemento de WordPress WEB-WORDPRESS wpDiscuz 7.0.0 hasta 7.0.4: Vulnerabilidad de carga de archivos arbitrarios no autenticados
999506		WEB-WORDPRESS Quiz & Survey Master: Vulnerabilidad de scripts entre sitios en la función de preguntas
999507	CVE-2020-8604	WEB-MISC Trend Micro IWS VA anterior a 6.5 SP2 parche 4 - Ruta transversal Vuln vía /log_search y cf Param (CVE-2020-8604)
999508	CVE-2020-8604	WEB-MISC Trend Micro IWS VA anterior a 6.5 SP2 Patch 4 - Ruta transversal Vuln Vía /collection y cf Param (CVE-2020-8604)
999509	CVE-2020-8604	WEB-MISC Trend Micro IWS VA anterior a 6.5 SP2 parche 4: Vuln de recorrido de ruta a través de /log_search y File Param (CVE-2020-8604)
999510	CVE-2020-8604	WEB-MISC Trend Micro IWS VA anterior a 6.5 SP2 parche 4: ruta transversal Vuln vía /collection y File Param (CVE-2020-8604)

Regla de firma	ID de CVE	Descripción
999511	CVE-2020-7361	WEB-MISC ZenTao Enterprise 8.8.3 y anteriores: Vulnerabilidad de ejecución remota de código a través de Repo-Edit (CVE-2020-7361)
999512	CVE-2020-7361	WEB-MISC ZenTao Pro 8.8.3 y anteriores: Vulnerabilidad de ejecución remota de código a través de Repo-Edit (CVE-2020-7361)
999513	CVE-2020-7361	WEB-MISC ZenTao Enterprise 8.8.3 y anteriores: Vulnerabilidad de ejecución remota de código a través de Repo-Create (CVE-2020-7361)
999514	CVE-2020-7361	WEB-MISC ZenTao Pro 8.8.3 y anteriores: Vulnerabilidad de ejecución remota de código a través de Repo-Create (CVE-2020-7361)
999515	CVE-2020-5768	Complemento de suscriptores de correo electrónico y boletines de WEB-WORDPRESS Icegram antes de 4.5.1: Vulnerabilidad de inyección SQL (CVE-2020-5768)
999516	CVE-2020-5767	Complemento de suscriptores de correo electrónico y boletines de WEB-WORDPRESS Icegram antes de 4.5.1: Vulnerabilidad CSRF (CVE-2020-5767)

Regla de firma	ID de CVE	Descripción
999517	CVE-2020-15299	Plug-in WEB-WORDPRESS KingComposer anterior a 2.9.5: Vulnerabilidad de scripts entre sitios (CVE-2020-15299)
999518	CVE-2020-13854	WEB-MISC Artica Pandora FMS: Vulnerabilidad de aumento de privilegios (CVE-2020-13854)
999519	CVE-2020-13852	WEB-MISC Artica Pandora FMS: Vulnerabilidad de carga arbitraria de archivos a través del administrador de archivos (CVE-2020-13852)
999520	CVE-2020-13700	Complemento de WordPress WEB-WORDPRESS acf-to-rest-api antes de 3.3.0: Vulnerabilidad de divulgación de información a través de URI (CVE-2020-13700)
999521	CVE-2020-13700	Complemento de WordPress WEB-WORDPRESS acf-to-rest-api antes de 3.3.0: Vulnerabilidad de divulgación de información a través de URL (CVE-2020-13700)
999522	CVE-2020-13379	WEB-MISC Grafana 3.0.1 a 7.0.1 - Bypass de CSRF que conduce a una vulnerabilidad de DOS (CVE-2020-13379)
999523	CVE-2020-12851	Celdas Pydio WEB-MISC anteriores a 2.0.7: Vulnerabilidad de escritura arbitraria de archivos (CVE-2020-12851)

Regla de firma	ID de CVE	Descripción
999524	CVE-2020-12848	Celdas Pydio WEB-MISC anteriores a 2.0.7: Vulnerabilidad de inicio de sesión como usuario compartido temporal (CVE-2020-12848)
999525	CVE-2020-11749	WEB-MISC Artica Pandora FMS anterior a 7.47: Vulnerabilidad de scripts entre sitios a través del explorador SNMP (CVE-2020-11749)
999526	CVE-2020-11579	WEB-MISC PHPKBV9: Vulnerabilidad de exfiltración de archivos (CVE-2020-11579)
999527	CVE-2020-10546	WEB-MISC RConfig anterior a 3.9.5: Vulnerabilidad de SQLi no autenticada en las directivas de cumplimiento a través de SearchColumn (CVE-2020-10546)
999528	CVE-2020-10546	RConfig de WEB-MISC anterior a 3.9.5: Vulnerabilidad de SQLi no autenticada en las directivas de cumplimiento a través de SearchField (CVE-2020-10546)
999529	CVE-2019-16876	Portainer WEB-MISC anterior a 1.22.1: Vulnerabilidad de cruce de directorios (CVE-2019-16876)

Regla de firma	ID de CVE	Descripción
999530		WEB-WORDPRESS - Complemento AdNing anterior a 1.5.6: Vulnerabilidad de eliminación arbitraria de archivos no autenticados
999531		WEB-WORDPRESS - Complemento de AdNing anterior a 1.5.6: Vulnerabilidad de carga de archivos arbitrarios no autenticados

Actualización de firmas para octubre de 2020

January 21, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la semana 2020-10-29. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

Las firmas son compatibles con las siguientes versiones de software de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 y 13.1.

La versión 12.0 de Citrix ADC ha llegado al final de su vida útil (EOL). Para obtener más información, consulte la página del ciclo de vida de la versión

> **Nota: La**
>
> habilitación de las reglas de firma de cuerpo posterior y cuerpo de respuesta puede afectar a la CPU de Citrix ADC. Además, las versiones vulnerables se mencionan en algunas de las cadenas de registro de reglas de firma. Debe habilitarlo en consecuencia.

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999500	CVE-2018-14667	WEB-MISC RichFaces Framework 3.X a 3.3.4: inyección EL a través de UserResource (CVE-2018-14667)
999501	CVE-2018-12533	WEB-MISC RichFaces Framework 3.1.0 a 3.3.4 - Inyección EL a través de Paint2dResource (CVE-2018-12533)
999502	CVE-2015-0279, CVE-2018-12532	WEB-MISC RichFaces Framework 4.X a 4.5.17 - Inyección EL a través de MediaOutputResource (CVE-2015-0279, CVE-2018-12532)
999503	CVE-2013-2165	WEB-MISC RichFaces v4 anterior a 4.3.3: Vulnerabilidad de deserialización de objetos Java (CVE-2013-2165)
999504	CVE-2013-2165	WEB-MISC RichFaces v3 anterior a 3.3.4: Vulnerabilidad de deserialización de objetos Java (CVE-2013-2165)

Actualización de firmas para noviembre de 2020

January 21, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la semana 2020-11-10. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

Las firmas son compatibles con las siguientes versiones de software de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 y 13.1.

La versión 12.0 de Citrix ADC ha llegado al final de su vida útil (EOL). Para obtener más información, consulte la página del ciclo de vida de la versión

> **Nota:**
>
> La activación de las reglas de firma del cuerpo de la publicación y del cuerpo Citrix ADC respuesta puede afectar a la CPU

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999411		Complemento de WordPress WEB-WORDPRESS wpDiscuz 7.0.0 hasta 7.0.4: Vulnerabilidad de carga de archivos arbitrarios no autenticados
999412		WEB-WORDPRESS Quiz & Survey Master: Vulnerabilidad de scripts entre sitios en la función de preguntas
999413		Administrador de archivos del complemento WEB-WORDPRESS WordPress anterior a 6.9: Vulnerabilidad de ejecución de comandos elFinder no autenticados
999414	CVE-2020-11700	WEB-MISC Titan SpamTitan anterior a 7.08: Vulnerabilidad de divulgación de información (CVE-2020-11700)

Regla de firma	ID de CVE	Descripción
999415	CVE-2020-9446	WEB-MISC Apache OfBiz 17.12.03: Vulnerabilidad de deserialización insegura XML-RPC (CVE-2020-9446)
999416	CVE-2020-9446	WEB-MISC Apache OfBiz 17.12.03: Vulnerabilidad de scripts entre sitios XML-RPC (CVE-2020-9446)
999417	CVE-2020-9047	Servicio web WEB-MISC exacqVision hasta 20.06.3.0: Vulnerabilidad de inyección de comandos del sistema operativo (CVE-2020-9047)
999418	CVE-2020-8866	WEB-MISC Horde Groupware Webmail Edition 5.2.22: Vulnerabilidad de carga sin restricciones de archivos a través de edit.php (CVE-2020-8866)
999419	CVE-2020-8866	WEB-MISC Horde Groupware Webmail Edition 5.2.22: Vulnerabilidad de carga sin restricciones de archivos a través de add.php (CVE-2020-8866)
999420	CVE-2020-8865	WEB-MISC Horde Groupware Webmail Edition 5.2.22: Vulnerabilidad de inclusión arbitraria de archivos a través de edit.php (CVE-2020-8865)
999421	CVE-2020-8816	Agujero PI WEB-MISC anterior a 4.3.2: Vulnerabilidad de ejecución remota de código a través de removestatic (CVE-2020-8816)

Regla de firma	ID de CVE	Descripción
999422	CVE-2020-8816	Agujero PI WEB-MISC anterior a 4.3.2: Vulnerabilidad de ejecución remota de código a través de AddMac (CVE-2020-8816)
999423	CVE-2020-8243	WEB-MISC Pulse Connect Secure antes de 9.1R8.2: Vulnerabilidad de ejecución remota de código (CVE-2020-8243)
999424	CVE-2020-8218	WEB-MISC Pulse Connect Secure antes de 9.1R8: Vulnerabilidad de ejecución remota de código (CVE-2020-8218)
999425	CVE-2020-6143, CVE-2020-6144	WEB-MISC OS4Ed OpenSIS: Vulnerabilidad de inyección de código a través de /install/Ins1.php (CVE-2020-6143, CVE-2020-6144)
999426	CVE-2020-6142	WEB-MISC OS4Ed OpenSIS: Vulnerabilidad de recorrido de ruta a través de modname (CVE-2020-6142)
999427	CVE-2020-6141	WEB-MISC OS4Ed OpenSIS anterior a 7.4: Vulnerabilidad de SQLi no autenticada a través de USERNAME (CVE-2020-6141)
999428	CVE-2020-6140	WEB-MISC OS4Ed OpenSIS anterior a 7.5: Vulnerabilidad de SQLi no autenticada a través de username_stn_id (CVE-2020-6140)

Regla de firma	ID de CVE	Descripción
999429	CVE-2020-6139	WEB-MISC OS4Ed OpenSIS anterior a 7.5: Vulnerabilidad de SQLi no autenticada a través de username_stf_email (CVE-2020-6139)
999430	CVE-2020-6138	WEB-MISC OS4Ed OpenSIS anterior a 7.5: Vulnerabilidad de SQLi no autenticada a través de uname (CVE-2020-6138)
999431	CVE-2020-6137	WEB-MISC OS4Ed OpenSIS anterior a 7.5: Vulnerabilidad de SQLi no autenticada a través de password_stf_email (CVE-2020-6137)
999432	CVE-2020-6125	WEB-MISC OS4Ed OpenSIS anterior a 7.5: Vulnerabilidad de SQLi a través del parámetro GetSchool.php y u (CVE-2020-6125)
999433	CVE-2020-6124	WEB-MISC OS4Ed OpenSIS anterior a 7.5: Vulnerabilidad de SQLi a través de EmailCheckOthers.php (CVE-2020-6124)
999434	CVE-2020-6123	WEB-MISC OS4Ed OpenSIS anterior a 7.5: Vulnerabilidad de SQLi a través de EmailCheck.php y el parámetro p_id (CVE-2020-6123)

Regla de firma	ID de CVE	Descripción
999435	CVE-2020-6123	WEB-MISC OS4Ed OpenSIS anterior a 7.5: Vulnerabilidad de SQLi a través de EmailCheck.php y el parámetro de correo electrónico (CVE-2020-6123)
999436	CVE-2020-6122	WEB-MISC OS4Ed OpenSIS anterior a 7.5: Vulnerabilidad de SQLi a través del parámetro CheckDuplicateStudent.php y mn (CVE-2020-6122)
999437	CVE-2020-6121	WEB-MISC OS4Ed OpenSIS anterior a 7.5: Vulnerabilidad de SQLi a través del parámetro CheckDuplicateStudent.php y ln (CVE-2020-6121)
999438	CVE-2020-6120	WEB-MISC OS4Ed OpenSIS anterior a 7.5: Vulnerabilidad de SQLi a través del parámetro CheckDuplicateStudent.php y fn (CVE-2020-6120)
999439	CVE-2020-6119	WEB-MISC OS4Ed OpenSIS anterior a 7.5: Vulnerabilidad de SQLi a través de CheckDuplicateStudent.php y el parámetro byear (CVE-2020-6119)
999440	CVE-2020-6118	WEB-MISC OS4Ed OpenSIS anterior a 7.5: Vulnerabilidad de SQLi a través de CheckDuplicateStudent.php y el parámetro bmonth (CVE-2020-6118)

Regla de firma	ID de CVE	Descripción
999441	CVE-2020-6117	WEB-MISC OS4Ed OpenSIS anterior a 7.5: Vulnerabilidad de SQLi a través de CheckDuplicateStudent.php y el parámetro bday (CVE-2020-6117)
999442	CVE-2020-5780	Suscriptores de correo electrónico y boletines de noticias del complemento de WordPress WEB-WORDPRESS anteriores a 4.5.6: Vulnerabilidad de falsificación de correo electrónico (CVE-2020-5780)
999443	CVE-2020-4280	WEB-MISC IBM QRadar SIEM 7.3 y 7.4: Vulnerabilidad de deserialización de Java insegura a través de JSON-RPC (CVE-2020-4280)
999444	CVE-2020-4280	WEB-MISC IBM QRadar SIEM 7.3 y 7.4: Vulnerabilidad de deserialización de Java insegura a través de RemoteMethod (CVE-2020-4280)
999445	CVE-2020-4280	WEB-MISC IBM QRadar SIEM 7.3 y 7.4: Vulnerabilidad de deserialización de Java insegura a través de RemoteJavascript (CVE-2020-4280)
999446	CVE-2020-4280	WEB-MISC IBM QRadar SIEM 7.3 y 7.4: Vulnerabilidad de deserialización de Java insegura a través de JSON-RPC (CVE-2020-4280)

Regla de firma	ID de CVE	Descripción
999447	CVE-2020-4280	WEB-MISC IBM QRadar SIEM 7.3 y 7.4: Vulnerabilidad de deserialización de Java insegura a través de RemoteMethod (CVE-2020-4280)
999448	CVE-2020-4280	WEB-MISC IBM QRadar SIEM 7.3 y 7.4: Vulnerabilidad de deserialización de Java insegura a través de RemoteJavascript (CVE-2020-4280)
999449	CVE-2020-24786	WEB-MISC Zoho ManageEngine AdManager Plus 7.0 antes de la compilación 55: Vulnerabilidad de autenticación incorrecta (CVE-2020-24786)
999450	CVE-2020-24389	Complemento de cargador de archivos múltiples de arrastrar y soltar WEB-WORDPRESS antes de 1.3.5.5: Vulnerabilidad de omisión de seguridad (CVE-2020-24389)
999451	CVE-2020-24046	WEB-MISC TitanHQ SpamTitan Gateway 7.08: Vulnerabilidad de escalada de privilegios (CVE-2020-24046
999452	CVE-2020-17506	WEB-MISC Artica Web Proxy 4.30.000000: Vulnerabilidad de inyección de SQL PreAuth a través del parámetro Apikey (CVE-2020-17506)

Regla de firma	ID de CVE	Descripción
999453	CVE-2020-17505	WEB-MISC Artica Web Proxy 4.30.000000: Vulnerabilidad de inyección de comandos del sistema operativo a través del parámetro Service-cmds-peform (CVE-2020-17505)
999454	CVE-2020-17463	WEB-MISC Fuel CMS 1.4.8: Vulnerabilidad de SQLi a través de /fuel/users/items (CVE-2020-17463)
999455	CVE-2020-17463	WEB-MISC Fuel CMS 1.4.8: Vulnerabilidad de SQLi a través de /fuel/sitevariables/items (CVE-2020-17463)
999456	CVE-2020-17463	WEB-MISC Combustible CMS 1.4.8: Vulnerabilidad de SQLi a través de /fuel/permissions/items (CVE-2020-17463)
999457	CVE-2020-17463	WEB-MISC Combustible CMS 1.4.8: Vulnerabilidad de SQLi a través de /fuel/pages/items (CVE-2020-17463)
999458	CVE-2020-17463	WEB-MISC Combustible CMS 1.4.8: Vulnerabilidad de SQLi a través de /fuel/navigation/items (CVE-2020-17463)
999459	CVE-2020-17463	WEB-MISC Combustible CMS 1.4.8: Vulnerabilidad de SQLi a través de /fuel/logs/items (CVE-2020-17463)

Regla de firma	ID de CVE	Descripción
999460	CVE-2020-17463	WEB-MISC Fuel CMS 1.4.8: Vulnerabilidad de SQLi a través de /fuel/blocks/items (CVE-2020-17463)
999461	CVE-2020-16875	WEB-MISC Microsoft Exchange Server: Vulnerabilidad de ejecución remota de código de directivas DLP (CVE-2020-16875)
999462	CVE-2020-16171	WEB-MISC Acronis Cyber Backup antes de 12.5 compilación 16342: Vulnerabilidad de encabezado de fragmento a través de SSRF (CVE-2020-16171)
999463	CVE-2020-14947	Inventario de OCS WEB-MISC anterior a 2.8: Vulnerabilidad de inyección de comandos del SO a través de SNMP_MIB_DIRECTORY (CVE-2020-14947)
999464	CVE-2020-14947	Inventario de OCS WEB-MISC anterior a 2.8: Vulnerabilidad de inyección de comandos del sistema operativo a través de mib_file (CVE-2020-14947)
999465	CVE-2020-14008	WEB-MISC Zoho ManageEngine Applications Manager hasta 14710: Vulnerabilidad de ejecución remota de código (CVE-2020-14008)

Regla de firma	ID de CVE	Descripción
999466	CVE-2020-13925	WEB-MISC Apache Kylin anterior a 3.1.0: Vulnerabilidad de ejecución remota de código a través de un trabajo (CVE-2020-13925)
999467	CVE-2020-13925	WEB-MISC Apache Kylin anterior a 3.1.0: Vulnerabilidad de ejecución remota de código a través del proyecto (CVE-2020-13925)
999468	CVE-2020-13854	WEB-MISC Artica Pandora FMS: Vulnerabilidad de aumento de privilegios (CVE-2020-13854)
999469	CVE-2020-13405	WEB-MISC Microweber anterior a 1.1.20: Vulnerabilidad de divulgación de información no autenticada (CVE-2020-13405)
999470	CVE-2020-13376	WEB-MISC SecurEnvoy SecurMail 9.3.503: Vulnerabilidad de recorrido de ruta de cookies de SecurEnvoyReply (CVE-2020-13376)
999471	CVE-2020-13159	WEB-MISC Artica Web Proxy anterior a 4.30.000000: Vulnerabilidad de inyección de comandos del sistema operativo a través del dominio (CVE-2020-13159)

Regla de firma	ID de CVE	Descripción
999472	CVE-2020-13159	WEB-MISC Artica Web Proxy anterior a 4.30.000000: Vulnerabilidad de inyección de comandos del sistema operativo a través de netbiosname (CVE-2020-13159)
999473	CVE-2020-13159	WEB-MISC Artica Web Proxy anterior a 4.30.000000: Vulnerabilidad de inyección de comandos del sistema operativo a través de alias (CVE-2020-13159)
999474	CVE-2020-13159	WEB-MISC Artica Web Proxy anterior a 4.30.000000: Vulnerabilidad de inyección de comandos del sistema operativo a través del nombre de host (CVE-2020-13159)
999475	CVE-2020-13159	WEB-MISC Artica Web Proxy anterior a 4.30.000000: Vulnerabilidad de inyección de comandos del sistema operativo a través de dhclient_server (CVE-2020-13159)
999476	CVE-2020-13159	WEB-MISC Artica Web Proxy anterior a 4.30.000000: Vulnerabilidad de inyección de comandos del sistema operativo a través de dhclient_interface (CVE-2020-13159)

Regla de firma	ID de CVE	Descripción
999477	CVE-2020-13159	WEB-MISC Artica Web Proxy anterior a 4.30.000000: Vulnerabilidad de inyección de comandos del sistema operativo a través de dhclient_mac (CVE-2020-13159)
999478	CVE-2020-13158	WEB-MISC Artica Web Proxy anterior a 4.30.000000: Vulnerabilidad de recorrido de ruta a través de una ventana emergente (CVE-2020-13158)
999479	CVE-2020-12851	Celdas Pydio WEB-MISC anteriores a 2.0.7: Vulnerabilidad de escritura arbitraria de archivos (CVE-2020-12851)
999480	CVE-2020-12848	Celdas Pydio WEB-MISC anteriores a 2.0.7: Vulnerabilidad de inicio de sesión como usuario compartido temporal (CVE-2020-12848)
999481	CVE-2020-11699	WEB-MISC Titan SpamTitan anterior a 7.08: Vulnerabilidad de ejecución remota de código (CVE-2020-11699)
999482	CVE-2020-11579	WEB-MISC PHPKBV9: Vulnerabilidad de exfiltración de archivos (CVE-2020-11579)

Regla de firma	ID de CVE	Descripción
999483	CVE-2020-10818	WEB-MISC Artica Web Proxy 4.26: Vulnerabilidad de inyección de comandos del sistema operativo a través de fw.system.info.php (CVE-2020-10818)
999484	CVE-2020-10228	WEB-MISC Vtenext CE anterior a la versión 20: carga sin restricciones de archivo con vulnerabilidad de tipo peligroso (CVE-2020-10228)
999485	CVE-2020-10204	WEB-MISC Sonatype Nexus Repository Manager anterior a 3.21.2: Vulnerabilidad de RCE a través de roles COREUI_user (CVE-2020-10204)
999486	CVE-2020-10204	WEB-MISC Sonatype Nexus Repository Manager anterior a 3.21.2: Vulnerabilidad de RCE a través de los privilegios COREUI_role (CVE-2020-10204)
999487	CVE-2020-10204	WEB-MISC Sonatype Nexus Repository Manager anterior a 3.21.2: Vulnerabilidad de RCE a través de roles COREUI_role (CVE-2020-10204)
999488	CVE-2020-10199	WEB-MISC Sonatype Nexus Repository Manager anterior a 3.21.2: Vulnerabilidad de RCE a través del extremo REST /bower/group (CVE-2020-10199)

Regla de firma	ID de CVE	Descripción
999489	CVE-2020-10199	WEB-MISC Sonatype Nexus Repository Manager anterior a 3.21.2: Vulnerabilidad de RCE a través del extremo REST /go/group (CVE-2020-10199)
999490	CVE-2020-10199	WEB-MISC Sonatype Nexus Repository Manager anterior a 3.21.2: Vulnerabilidad de RCE a través del extremo REST /docker/group (CVE-2020-10199)
999491	CVE-2019-19699	WEB-MISC Centreon hasta 19.10: Vulnerabilidad de ejecución remota de código (CVE-2019-19699)
999492	CVE-2019-19499	WEB-MISC Apache Grafana hasta 6.4.3: Vulnerabilidad de lectura arbitraria de archivos (CVE-2019-19499)
999493	CVE-2019-18394	WEB-MISC Ignite Realtime Openfire hasta 4.4.2: Vulnerabilidad de falsificación de solicitud del lado del servidor de FaviconServlet (CVE-2019-18394)
999494	CVE-2019-18393	WEB-MISC Ignite Realtime Openfire hasta 4.4.2: Vulnerabilidad de cruce de directorios de insertos de complementos (CVE-2019-18393)

Regla de firma	ID de CVE	Descripción
999495	CVE-2019-16759	WEB-MISC vBulletin anterior a 5.6.2: Vulnerabilidad de ejecución remota de código a través de una plantilla anidada (CVE-2019-16759)
999496	CVE-2019-15715	WEB-MISC MantisBT anterior a 1.3.20 y 2.22.1: Vulnerabilidad de ejecución remota de código a través de neato_tool (CVE-2019-15715)
999497	CVE-2019-15715	WEB-MISC MantisBT anterior a 1.3.20 y 2.22.1: Vulnerabilidad de ejecución remota de código a través de dot_tool (CVE-2019-15715)
999498	CVE-2019-11043	WEB-MISC PHP-FPM Múltiples versiones: la vulnerabilidad de escritura fuera de límites permite la ejecución de código arbitrario (CVE-2019-11043)
999499		El complemento de WordPress WEB-WORDPRESS optimiza automáticamente hasta 2.7.6: Vulnerabilidad de carga de archivos arbitrarios autenticados

Actualización de firmas para diciembre de 2020

January 21, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la semana 2020-12-02. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

Las firmas son compatibles con las siguientes versiones de software de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 y 13.1.

La versión 12.0 de Citrix ADC ha llegado al final de su vida útil (EOL). Para obtener más información, consulte la página del ciclo de vida de la versión

> **Nota: La**
>
> habilitación de las reglas de firma de cuerpo posterior y cuerpo de respuesta puede afectar a la CPU de Citrix ADC. Como parte de la actualización de firma de la versión 54, se cambia la cadena de registro de la firma 999720 para garantizar que solo incluya caracteres ASCI.

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999394	CVE-2020-8255	WEB-MISC Pulse Connect Secure antes de 9.1R9: Vulnerabilidad de divulgación de información (CVE-2020-8255)
999395	CVE-2020-6128	WEB-MISC OS4Ed OpenSIS anterior a 7.5: Vulnerabilidad de SQLi a través de CoursePeriodModal.php (CVE-2020-6128)
999396	CVE-2020-6126, CVE-2020-6127	WEB-MISC OS4Ed OpenSIS anterior a 7.5: Vulnerabilidad de SQLi a través de CoursePeriodModal.php (CVE-2020-6126, CVE-2020-6127)
999397	CVE-2020-28328	WEB-MISC SuiteCRM anterior a 7.11.16: Vulnerabilidad de ejecución remota de código (CVE-2020-28328)

Regla de firma	ID de CVE	Descripción
999398	CVE-2020-27995	WEB-MISC Zoho ManageEngine Applications Manager 14 antes de la compilación 14560: Vulnerabilidad de inyección SQL (CVE-2020-27995)
999399	CVE-2020-26879	WEB-MISC Ruckus vRIoT Server anterior a 1.6.0: Vulnerabilidad de omisión de autorización a través de /service/ (CVE-2020-26879)
999400	CVE-2020-26879	WEB-MISC Ruckus vRIoT Server anterior a 1.6.0: Vulnerabilidad de omisión de autorización mediante /reinicio (CVE-2020-26879)
999401	CVE-2020-26879	WEB-MISC Ruckus vRIoT Server anterior a 1.6.0: Vulnerabilidad de omisión de autorización a través de /patch/ (CVE-2020-26879)
999402	CVE-2020-26879	WEB-MISC Ruckus vRIoT Server anterior a 1.6.0: Vulnerabilidad de omisión de autorización a través de /upgrade/ (CVE-2020-26879)
999403	CVE-2020-26879	WEB-MISC Ruckus vRIoT Server anterior a 1.6.0: Vulnerabilidad de omisión de autorización a través de /module/ (CVE-2020-26879)
999404	CVE-2020-26878	WEB-MISC Ruckus vRIoT Server anterior a 1.6.0: Vulnerabilidad de inyección de comandos de SO arbitraria (CVE-2020-26878)

Regla de firma	ID de CVE	Descripción
999405	CVE-2020-25790	WEB-MISC Typesetter CMS 5.x a 5.1: Vulnerabilidad de carga de archivos no seguros (CVE-2020-25790)
999406	CVE-2020-25540	WEB-MISC ThinkAdmin v6: Vulnerabilidad de cruce de directorios (CVE-2020-25540)
999407	CVE-2020-14883	WEB-MISC Oracle WebLogic Server: Vulnerabilidad de ejecución remota de código autenticada (CVE-2020-14883)
999408	CVE-2020-14882, CVE-2020-14750	WEB-MISC Oracle WebLogic Server: Vulnerabilidad de omisión de autenticación (CVE-2020-14882, CVE-2020-14750)
999409	CVE-2020-11975, CVE-2020-13942	WEB-MISC Apache Unomi anterior a 1.5.2: Vulnerabilidad de ejecución remota de código (CVE-2020-11975, CVE-2020-13942)
999410	CVE-2020-11803	WEB-MISC Titan SpamTitan anterior a 7.08: Vulnerabilidad de ejecución remota de código (CVE-2020-11803)

Actualización de firmas para diciembre de 2020

January 21, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la semana 2020-12-17. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulner-

ables a la seguridad.

Versión de firma

Las firmas son compatibles con las siguientes versiones de software de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 y 13.1.

La versión 12.0 de Citrix ADC ha llegado al final de su vida útil (EOL). Para obtener más información, consulte la página del ciclo de vida de la versión

> **Nota: La**
>
> habilitación de las reglas de firma de cuerpo posterior y cuerpo de respuesta puede afectar a la CPU de Citrix ADC.

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999377		WEB-WORDPRESS TI WooCommerce Wishlist Plugin antes de 1.21.11: Vulnerabilidad de divulgación de información a través de tinvwl_export_settings
999378		WEB-WORDPRESS TI WooCommerce Wishlist Plugin antes de 1.21.11 - Las opciones de WP cambian la vulnerabilidad a través de tinvwl_import_settings
999379	CVE-2020-6134	WEB-MISC OS4Ed OpenSIS anterior a 7.5: Vulnerabilidad de SQLi a través de MassDropModal.php (CVE-2020-6134)

Regla de firma	ID de CVE	Descripción
999380	CVE-2020-6133	WEB-MISC OS4Ed OpenSIS anterior a 7.5: Vulnerabilidad de SQLi a través de CourseMoreInfo.php (CVE-2020-6133)
999381	CVE-2020-6132	WEB-MISC OS4Ed OpenSIS anterior a 7.5: Vulnerabilidad de SQLi a través de ChooseCP.php (CVE-2020-6132)
999382	CVE-2020-6131	WEB-MISC OS4Ed OpenSIS anterior a 7.5: Vulnerabilidad de SQLi a través de MassScheduleSessionSet.php (CVE-2020-6131)
999383	CVE-2020-6130	WEB-MISC OS4Ed OpenSIS anterior a 7.5: Vulnerabilidad de SQLi a través de MassDropSessionSet.php (CVE-2020-6130)
999384	CVE-2020-6129	WEB-MISC OS4Ed OpenSIS anterior a 7.5: Vulnerabilidad de SQLi a través de CpSessionSet.php (CVE-2020-6129)
999385	CVE-2020-35234	Complemento SMTP de WEB-WORDPRES Easy WP antes de 1.4.4: Vulnerabilidad de divulgación de información (CVE-2020-35234)
999386	CVE-2020-25042	WEB-MISC Mara CMS 7.5: Vulnerabilidad de carga arbitraria de archivos (CVE-2020-25042)

Regla de firma	ID de CVE	Descripción
999387	CVE-2020-13526	WEB-MISC ProcessMaker: Vulnerabilidad de inyección SQL a través de ClientSetupajax (CVE-2020-13526)
999388	CVE-2020-13525	WEB-MISC ProcessMaker: Vulnerabilidad de inyección SQL a través de Reporttables_ajax (CVE-2020-13525)
999389	CVE-2020-12147	WEB-MISC Silver Peak Unity Orchestrator: Vulnerabilidad de consultas arbitrarias de MySQL a través de la API REST de SQLExecution (CVE-2020-12147)
999390	CVE-2020-12146	WEB-MISC Silver Peak Unity Orchestrator: Vulnerabilidad de recorrido de ruta a través de la API REST de DebugFiles (CVE-2020-12146)
999391	CVE-2020-12145	WEB-MISC Silver Peak Unity Orchestrator: Vulnerabilidad de omisión de autenticación (CVE-2020-12145)
999392	CVE-2019-8394	WEB-MISC Zoho ManageEngine ServiceDesk Plus antes de 10.0 compilación 10012: Vulnerabilidad de carga de archivos arbitrarios (CVE-2019-8394)

Regla de firma	ID de CVE	Descripción
999393	CVE-2019-11447	WEB-MISC CutePHP CuteNews 2.1.2: Vulnerabilidad de ejecución remota de código (CVE-2019-11447)

Actualización de firmas para enero de 2021

January 21, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la semana 2021-01-18. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

Las firmas son compatibles con las siguientes versiones de software de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 y 13.1.

La versión 12.0 de Citrix ADC ha llegado al final de su vida útil (EOL). Para obtener más información, consulte la página del ciclo de vida de la versión

> **Nota: La**
>
> habilitación de las reglas de firma de cuerpo posterior y cuerpo de respuesta puede afectar a la CPU de Citrix ADC.

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999366	CVE-2020-8466	WEB-MISC Trend Micro IWSSVA 6.5 SP2 antes de la compilación 1919: Vulnerabilidad de inyección de comandos de SO no autenticados (CVE-2020-8466)
999367	CVE-2020-6135	WEB-MISC OS4Ed OpenSIS anterior a 7.5: Vulnerabilidad de SQLi a través de Validator.php (CVE-2020-6135)
999368	CVE-2020-4001	WEB-MISC VMware SD-WAN Orchestrator: Vulnerabilidad de pasar el hash (CVE-2020-4001)
999369	CVE-2020-4000	WEB-MISC VMware SD-WAN Orchestrator: Vulnerabilidad de recorrido de ruta (CVE-2020-4000)
999370	CVE-2020-3984	WEB-MISC VMware SD-WAN Orchestrator: Vulnerabilidad de inyección de SQL a través del módulo (CVE-2020-3984)
999371	CVE-2020-35606	WEB-MISC Webmin hasta 1.962: Vulnerabilidad de ejecución remota de código (CVE-2020-35606)
999372	CVE-2020-17143	WEB-MISC Microsoft Exchange Server: Vulnerabilidad de divulgación de información (CVE-2020-17143)

Regla de firma	ID de CVE	Descripción
999373	CVE-2020-17141	WEB-MISC Microsoft Exchange Server: Vulnerabilidad de ejecución remota de código a través de RouteComplaint (CVE-2020-17141)
999374	CVE-2020-10816	WEB-MISC Zoho ManageEngine Applications Manager 14 antes de la compilación 14790: Vulnerabilidad de autenticación incorrecta (CVE-2020-10816)
999375	CVE-2019-5533	WEB-MISC VMware SD-WAN Orchestrator: Vulnerabilidad de divulgación de información (CVE-2019-5533)
999376	CVE-2018-15961	WEB-MISC Adobe ColdFusion 12 antes de la actualización 6 o 14: Vulnerabilidad de carga arbitraria de archivos (CVE-2018-15961)

Actualización de firma para febrero de 2021

January 21, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la semana 2021-02-03. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

Las firmas son compatibles con las siguientes versiones de software de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 y 13.1.

La versión 12.0 de Citrix ADC ha llegado al final de su vida útil (EOL). Para obtener más información,

consulte la página del ciclo de vida de la versión

> **Nota: La**
>
> habilitación de las reglas de firma de cuerpo posterior y cuerpo de respuesta puede afectar a la CPU de Citrix ADC.

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999339		Conector WEB-MISC Zoom Meeting 4.6.348.20201217: Vulnerabilidad de ejecución remota de código a través de proxyPasswd
999340		Conector WEB-MISC Zoom Meeting 4.6.348.20201217: Vulnerabilidad de ejecución remota de código a través de ProxyName
999341	CVE-2021-3129	Ignición WEB-MISC anterior a 2.5.2: Vulnerabilidad de ejecución remota de código no autenticada (CVE-2021-3129)
999342	CVE-2021-3025	WEB-MISC Invision Community IPS Community Suite anterior a 4.5.4.2: Vulnerabilidad de inyección de SQL a través de SortDir (CVE-2021-3025)
999343	CVE-2021-2109	WEB-MISC Oracle WebLogic Server: Vulnerabilidad de ejecución remota de código mediante inyección JNDI (CVE-2021-2109)

Regla de firma	ID de CVE	Descripción
999344	CVE-2020-7200	WEB-MISC HPE Systems Insight Manager 7.6.x: Vulnerabilidad de deserialización no segura de AMF (CVE-2020-7200)
999345	CVE-2020-7199	WEB-MISC HPE EIM anterior a 1.21: Vulnerabilidad de autenticación incorrecta en /private/EIMApplianceIP (CVE-2020-7199)
999346	CVE-2020-7199	WEB-MISC HPE EIM anterior a 1.21: Vulnerabilidad de autenticación incorrecta en /private/adminPassReset (CVE-2020-7199)
999347	CVE-2020-7199	WEB-MISC HPE EIM anterior a 1.21: Vulnerabilidad de autenticación incorrecta en /Private/ResetAppliance (CVE-2020-7199)
999348	CVE-2020-6136	WEB-MISC OS4Ed OpenSIS anterior a 7.5: Vulnerabilidad de SQLi a través de DownloadWindow.php (CVE-2020-6136)
999349	CVE-2020-35729	WEB-MISC KLog Server 2.4.1 y anteriores: Vulnerabilidad de inyección de comandos del sistema operativo (CVE-2020-35729)
999350	CVE-2020-35701	WEB-MISC Cactus 1.2.16 y anteriores: Vulnerabilidad de inyección SQL a través de site_id (CVE-2020-35701)

Regla de firma	ID de CVE	Descripción
999351	CVE-2020-35489	Formulario de contacto WEB-WORDPRESS 7 anterior a 5.3.2: Vulnerabilidad de carga de archivos sin restricciones (CVE-2020-35489)
999352	CVE-2020-27615	Complemento de inicio de sesión de WEB-WORDPRESS anterior a 1.6.4: Vulnerabilidad de inyección SQL (CVE-2020-27615)
999353	CVE-2020-26046	WEB-MISC Fuel CMS 1.4.11 y anteriores: Vulnerabilidad XSS a través de /fuel/sitevariables/create (CVE-2020-26046)
999354	CVE-2020-26046	WEB-MISC Fuel CMS 1.4.11 y anteriores: Vulnerabilidad XSS a través de /fuel/sitevariables/edit (CVE-2020-26046)
999355	CVE-2020-26046	WEB-MISC Fuel CMS 1.4.11 y anteriores: Vulnerabilidad XSS a través de /fuel/navigation/create (CVE-2020-26046)
999356	CVE-2020-26046	WEB-MISC Fuel CMS 1.4.11 y anteriores: Vulnerabilidad XSS a través de /fuel/navigation/edit (CVE-2020-26046)
999357	CVE-2020-26046	WEB-MISC Fuel CMS 1.4.11 y anteriores: Vulnerabilidad XSS a través de /fuel/blocks/create (CVE-2020-26046)

Regla de firma	ID de CVE	Descripción
999358	CVE-2020-26046	WEB-MISC Fuel CMS 1.4.11 y anteriores: Vulnerabilidad XSS a través de /fuel/blocks/edit (CVE-2020-26046)
999359	CVE-2020-26045	WEB-MISC Combustible CMS 1.4.11: Vulnerabilidad de SQLi a través de /fuel/permissions/create (CVE-2020-26045)
999360	CVE-2020-17519	WEB-MISC Apache Flink anterior a 1.11.3: Vulnerabilidad de divulgación arbitraria de archivos (CVE-2020-17519)
999361	CVE-2020-17518	WEB-MISC Apache Flink 1.5.1 a 1.11.2: Vulnerabilidad de carga de archivos de ubicación arbitraria (CVE-2020-17518)
999362	CVE-2019-16010	WEB-MISC Cisco SD-WAN vManage anterior a 19.2.2: Vulnerabilidad XSS almacenada (CVE-2019-16010)
999363	CVE-2019-15000	WEB-MISC VMware Bitbucket Server y centro de datos: Vulnerabilidad de inyección de comandos Git a través de at (CVE-2019-15000)
999364	CVE-2019-15000	WEB-MISC VMware Bitbucket Server y centro de datos: Vulnerabilidad de inyección de comandos Git a través de until/untilID (CVE-2019-15000)

Regla de firma	ID de CVE	Descripción
999365	CVE-2019-15000	WEB-MISC VMware Bitbucket Server y centro de datos: Vulnerabilidad de inyección de comandos Git a través de since/sinceID (CVE-2019-15000)

Actualización de firma para febrero de 2021

January 21, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la semana 2021-02-17. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

Las firmas son compatibles con las siguientes versiones de software de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 y 13.1.

La versión 12.0 de Citrix ADC ha llegado al final de su vida útil (EOL). Para obtener más información, consulte la página del ciclo de vida de la versión

> **Nota: La**
>
> habilitación de las reglas de firma de cuerpo posterior y cuerpo de respuesta puede afectar a la CPU de Citrix ADC.

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999328	CVE-2021-3317	WEB-MISC KLog Server 2.4.1 y anteriores: Vulnerabilidad de inyección de comandos del SO (CVE-2021-3317)

Regla de firma	ID de CVE	Descripción
999329	CVE-2021-3110	WEB-MISC PrestaShop anterior a 1.7.7.1: Vulnerabilidad de inyección SQL a través de id_products (CVE-2021-3110)
999330	CVE-2021-3110	WEB-MISC PrestaShop anterior a 1.7.7.1: Vulnerabilidad de inyección SQL a través de /module/productcomments/-CommentGrade (CVE-2021-3110)
999331	CVE-2021-25646	WEB-MISC Apache Druid anterior a 0.20.1: Vulnerabilidad de ejecución remota de código (CVE-2021-25646)
999332	CVE-2020-36171	Plugin WEB-WORDPRESS Elementor Page Builder antes de 3.0.14: Vulnerabilidad XSS (CVE-2020-36171)
999333	CVE-2020-35765	WEB-MISC Zoho ManageEngine Applications Manager antes de la compilación 15000: Vulnerabilidad de inyección SQL (CVE-2020-35765)
999334	CVE-2020-35589	Límite de intentos de inicio de sesión de WEB-WORDPRESS recargados antes de 2.15.2: Vulnerabilidad reflejada de scripts entre sitios (CVE-2020-35589)

Regla de firma	ID de CVE	Descripción
999335	CVE-2020-26282	WEB-MISC BrowserUp Proxy anterior a la 2.1.2 - Inyección de plantillas que conduce a la vulnerabilidad de RCE a través de mostRecentEntry (CVE-2020-26282)
999336	CVE-2020-26282	WEB-MISC BrowserUp Proxy anterior a la 2.1.2 - Inyección de plantillas que conduce a la vulnerabilidad de RCE a través de entradas (CVE-2020-26282)
999337	CVE-2020-14815	WEB-MISC Oracle Business Intelligence Enterprise Edition: Vulnerabilidad reflejada de scripts entre sitios (CVE-2020-14815)
999338		Complemento de base de datos del formulario de contacto de WEB-WORDPRESS 7 antes de 1.2.5.4: Vulnerabilidad SQLi mediante la eliminación de acción

Actualización de firma para marzo de 2021

January 21, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la semana 2021-03-08. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

Las firmas son compatibles con las siguientes versiones de software de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 y 13.1.

La versión 12.0 de Citrix ADC ha llegado al final de su vida útil (EOL). Para obtener más información, consulte la página del ciclo de vida de la versión

> **Nota: La**
>
> habilitación de las reglas de firma de cuerpo posterior y cuerpo de respuesta puede afectar a la CPU de Citrix ADC.

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999313	CVE-2021-25299	WEB-MISC NagiosXI Hasta 5.7.5: Vulnerabilidad XSS a través de url (CVE-2021-25299)
999314	CVE-2021-25298	WEB-MISC NagiosXI Hasta 5.7.5: Vulnerabilidad de ejecución remota de código mediante el asistente de DigitalOcean (CVE-2021-25298)
999315	CVE-2021-25297	WEB-MISC NagiosXI Hasta 5.7.5: Vulnerabilidad de ejecución remota de código mediante el asistente de conmutador (CVE-2021-25297)
999316	CVE-2021-25296	WEB-MISC NagiosXI Hasta 5.7.5: Vulnerabilidad de ejecución remota de código mediante el asistente WindowsWMI (CVE-2021-25296)

Regla de firma	ID de CVE	Descripción
999317	CVE-2021-24164	Plugin de formularios Ninja de WEB-WORDPRESS antes de 3.4.34.1: Vulnerabilidad de divulgación de información (CVE-2021-24164)
999318	CVE-2021-24163	Plugin de formularios Ninja de WEB-WORDPRESS antes de 3.4.34: Vulnerabilidad de omisión de autorización (CVE-2021-24163)
999319	CVE-2021-21972	WEB-MISC Complemento de VMware vCenter Server: Vulnerabilidad de ejecución remota de código (CVE-2021-21972)
999320	CVE-2020-35129	WEB-MISC Mautic anterior a 3.2.4: Vulnerabilidad XSS mediante un nuevo formulario de supervisión social (CVE-2020-35129)
999321	CVE-2020-35129	WEB-MISC Mautic anterior a 3.2.4: Vulnerabilidad XSS a través del formulario Edit Social Monitoring (CVE-2020-35129)
999322	CVE-2020-35128	WEB-MISC Mautic anterior a 3.2.4: Vulnerabilidad XSS a través del formulario de nuevas empresas (CVE-2020-35128)
999323	CVE-2020-35128	WEB-MISC Mautic anterior a 3.2.4: Vulnerabilidad XSS a través del formulario Edit Companies (CVE-2020-35128)

Regla de firma	ID de CVE	Descripción
999324	CVE-2020-35125	WEB-MISC Mautic anterior a 3.2.4: Vulnerabilidad XSS mediante encabezado de referencia (CVE-2020-35125)
999325	CVE-2020-35125	WEB-MISC Mautic anterior a 3.2.4: Vulnerabilidad XSS mediante mauticform[return] (CVE-2020-35125)
999326	CVE-2020-13933	WEB-MISC Apache Shiro anterior a 1.6.0: Vulnerabilidad de omisión de autenticación mediante punto y coma (CVE-2020-13933)
999327	CVE-2020-13921, CVE-2020-9483	WEB-MISC Apache SkyWalking anterior a 8.4.0: Vulnerabilidad de inyección SQL mediante la función queryLogs (CVE-2020-13921, CVE-2020-9483)

Actualización de firma para marzo de 2021

January 21, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la semana 2021-03-09. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

Las firmas son compatibles con las siguientes versiones de software de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 y 13.1.

La versión 12.0 de Citrix ADC ha llegado al final de su vida útil (EOL). Para obtener más información, consulte la página del ciclo de vida de la versión

> **Nota: La**
>
> habilitación de las reglas de firma de cuerpo posterior y cuerpo de respuesta puede afectar a la CPU de Citrix ADC.

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999311	CVE-2021-26855	WEB-MISC Microsoft Exchange Server: Vulnerabilidad de ejecución remota de código mediante X-AnonResource-Backend (CVE-2021-26855)
999312	CVE-2021-26855	WEB-MISC Microsoft Exchange Server: Vulnerabilidad de ejecución remota de código mediante X-BEResource (CVE-2021-26855)

Actualización de firma para marzo de 2021

January 21, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la semana 2021-03-11. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

Las firmas son compatibles con las siguientes versiones de software de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 y 13.1.

La versión 12.0 de Citrix ADC ha llegado al final de su vida útil (EOL). Para obtener más información, consulte la página del ciclo de vida de la versión

> **Nota: La**
>
> habilitación de las reglas de firma de cuerpo posterior y cuerpo de respuesta puede afectar a la CPU de Citrix ADC.

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999308	CVE-2021-21302	WEB-MISC PrestaShop antes de 1.7.7.2: Vulnerabilidad de inyección CSV (CVE-2021-21302)
999309	CVE-2020-35749	Board de trabajo simple de WEB-WORDPRESS antes de 2.9.4: Vulnerabilidad de divulgación arbitraria de archivos (CVE-2020-35749)
999310	CVE-2019-16012	WEB-MISC Cisco SD-WAN vManage anterior a 19.2.2: Vulnerabilidad de inyección SQL (CVE-2019-16012)

Actualización de firma para marzo de 2021

January 21, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la semana 2021-03-11. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

Las firmas son compatibles con las siguientes versiones de software de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 y 13.1.

La versión 12.0 de Citrix ADC ha llegado al final de su vida útil (EOL). Para obtener más información,

consulte la página del ciclo de vida de la versión

> **Nota: La**
>
> habilitación de las reglas de firma de cuerpo posterior y cuerpo de respuesta puede afectar a la CPU de Citrix ADC.

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999307	CVE-2021-27065	WEB-MISC Microsoft Exchange Server: Vulnerabilidad de ejecución remota de código (CVE-2021-27065)

Actualización de la firma para abril de 2021

January 21, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la semana 2021-04-08. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

Las firmas son compatibles con las siguientes versiones de software de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 y 13.1.

La versión 12.0 de Citrix ADC ha llegado al final de su vida útil (EOL). Para obtener más información, consulte la página del ciclo de vida de la versión

> **Nota: La**
>
> habilitación de las reglas de firma de cuerpo posterior y cuerpo de respuesta puede afectar a la CPU de Citrix ADC.

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999294	CVE-2021-3273	WEB-MISC NagiosXI anterior a 5.7: Vulnerabilidad de inyección de código (CVE-2021-3273)
999295	CVE-2021-3197	WEB-MISC SaltStack anterior a 3002.3: Vulnerabilidad de ejecución remota de código mediante ssh_priv (CVE-2021-3197)
999296	CVE-2021-3197	WEB-MISC SaltStack anterior a 3002.3: Vulnerabilidad de ejecución remota de código mediante ssh_port (CVE-2021-3197)
999297	CVE-2021-3197	WEB-MISC SaltStack anterior a 3002.3: Vulnerabilidad de ejecución remota de código mediante ssh_options (CVE-2021-3197)
999298	CVE-2021-3197	WEB-MISC SaltStack anterior a 3002.3: Vulnerabilidad de ejecución remota de código mediante ProxyCommand en objeto JSON (CVE-2021-3197)
999299	CVE-2021-25282	WEB-MISC SaltStack anterior a 3002.3: Vulnerabilidad de recorrido de ruta a través de pillar_roots.write (CVE-2021-25282)
999300	CVE-2021-24166	Plugin de formularios Ninja de WEB-WORDPRESS antes de 3.4.34: Vulnerabilidad CSRF (CVE-2021-24166)

Regla de firma	ID de CVE	Descripción
999301	CVE-2021-24085	WEB-MISC Microsoft Exchange Server: Vulnerabilidad de suplantación (CVE-2021-24085)
999302	CVE-2021-22986	WEB-MISC F5 iControl REST API: Vulnerabilidad de ejecución remota de código (CVE-2021-22986)
999303	CVE-2021-21978	WEB-MISC VMware View Planner Harness 4.x anterior a 4.6 Parche de seguridad 1: Vulnerabilidad de ejecución remota de código (CVE-2021-21978)
999304	CVE-2020-23132	WEB-MISC Joomla! Antes de 3.9.25: Vulnerabilidad de ruta de carga no segura com_media a través de file_path (CVE-2020-23132)
999305	CVE-2020-23132	WEB-MISC Joomla! Antes de 3.9.25: Vulnerabilidad de ruta de carga no segura de com_media a través de image_path (CVE-2020-23132)
999306	CVE-2020-22425	WEB-MISC Centreon anterior a 20.10.4: Vulnerabilidad de inyección SQL (CVE-2020-22425)

Actualización de la firma para abril de 2021

January 21, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la semana 2021-04-22. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulner-

ables a la seguridad.

Versión de firma

Las firmas son compatibles con las siguientes versiones de software de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 y 13.1.

La versión 12.0 de Citrix ADC ha llegado al final de su vida útil (EOL). Para obtener más información, consulte la página del ciclo de vida de la versión

> **Nota: La**
>
> habilitación de las reglas de firma de cuerpo posterior y cuerpo de respuesta puede afectar a la CPU de Citrix ADC.

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999275	CVE-2021-3378	WEB-MISC FortiLogger 4.4.2.2: Vulnerabilidad de carga arbitraria de archivos no autenticada (CVE-2021-3378)
999276	CVE-2021-28925	WEB-MISC Nagios Network Analyzer anterior a 2.4.3: Vulnerabilidad de inyección SQL (CVE-2021-28925)
999277	CVE-2021-28924	WEB-MISC Nagios Network Analyzer anterior a 2.4.3: Vulnerabilidad XSS (CVE-2021-28924)
999278	CVE-2021-27927	WEB-MISC Zabbix: Vulnerabilidad CSRF a través de ac-tion=authentication.update (CVE-2021-27927)
999279	CVE-2021-26295	WEB-MISC Apache OfBiz 17.12.06: Vulnerabilidad de deserialización arbitraria no autenticada (CVE-2021-26295)

Regla de firma	ID de CVE	Descripción
999280	CVE-2021-25770	WEB-MISC JetBrains YouTrack antes de 2020.5.3123: Vulnerabilidad de inyección de plantillas del lado del servidor (CVE-2021-25770)
999281	CVE-2021-25283	WEB-MISC SaltStack anterior a 3002.5: Vulnerabilidad de ejecución remota de código (CVE-2021-25283)
999282	CVE-2021-25283	WEB-MISC SaltStack anterior a 3002.5: Vulnerabilidad de ejecución remota de código mediante objeto JSON (CVE-2021-25283)
999283	CVE-2021-24218	Plugin WEB-WORDPRESS Facebook for WordPress anterior a 3.0.4: Vulnerabilidad de scripts almacenadas entre sitios (CVE-2021-24218)
999284	CVE-2021-24217	Plugin de Facebook para WordPress WEB-WORDPRESS antes de 3.0.2: Vulnerabilidad de inyección de objetos PHP (CVE-2021-24217)
999285	CVE-2021-24209	Plug-in WEB-WORDPRESS WP Super Cache anterior a 1.7.2: Vulnerabilidad de ejecución remota de código en wp-cache-config.php (CVE-2021-24209)
999286	CVE-2021-24209	Plugin WEB-WORDPRESS WP Super Cache anterior a 1.7.2: Vulnerabilidad de inyección de código arbitraria (CVE-2021-24209)

Regla de firma	ID de CVE	Descripción
999287	CVE-2021-24165	Plugin de formularios Ninja de WEB-WORDPRESS antes de 3.4.34: Vulnerabilidad de redirección abierta (CVE-2021-24165)
999288	CVE-2021-21975	WEB-MISC vRealize Operations Manager: Vulnerabilidad de falsificación de solicitudes del lado del servidor no autenticada (CVE-2021-21975)
999289	CVE-2020-35578	WEB-MISC Nagios XI anterior a 5.8.0: Vulnerabilidad de ejecución remota de código (CVE-2020-35578)
999290	CVE-2020-2766	WEB-MISC Oracle WebLogic Server: Vulnerabilidad SSRF no autenticada (CVE-2020-2766)
999291	CVE-2020-17523	WEB-MISC Apache Shiro anterior a 1.7.1: Vulnerabilidad de omisión de autenticación a través del espacio (CVE-2020-17523)
999292	CVE-2020-17523	WEB-MISC Apache Shiro anterior a 1.7.1: Vulnerabilidad de omisión de autenticación a través de punto (CVE-2020-17523)
999293	CVE-2020-15160	WEB-MISC PrestaShop anterior a 1.7.6.8: Vulnerabilidad de inyección SQL (CVE-2020-15160)

Actualización de la firma para junio de 2021

January 21, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la semana 2021-06-02. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

Las firmas son compatibles con las siguientes versiones de software de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 y 13.1.

La versión 12.0 de Citrix ADC ha llegado al final de su vida útil (EOL). Para obtener más información, consulte la página del ciclo de vida de la versión

> **Nota: La**
>
> habilitación de las reglas de firma de cuerpo posterior y cuerpo de respuesta puede afectar a la CPU de Citrix ADC.

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999243	CVE-2021-31761	WEB-MISC Webmin anterior a 1.974: Vulnerabilidad XSS a través de /servers/link.cgi/ (CVE-2021-31761)
999244	CVE-2021-31761	WEB-MISC Webmin anterior a 1.974: Vulnerabilidad XSS a través de /tunnel/link.cgi/ (CVE-2021-31761)
999245	CVE-2021-31166	WEB-IIS Microsoft HTTP Protocol Stack: Vulnerabilidad de ejecución remota de código (CVE-2021-31166)

Regla de firma	ID de CVE	Descripción
999246	CVE-2021-29447	WEB-WORDPRESS WordPress anterior a la versión 5.7.1: Vulnerabilidad de la biblioteca multimedia XXE (CVE-2021-29447)
999247	CVE-2021-28157	Servidor de devoluciones WEB-MISC anteriores a 2021.1 y 2020.3.18: Vulnerabilidad de inyección SQL mediante la eliminación del usuario (CVE-2021-28157)
999248	CVE-2021-27905	WEB-MISC Apache Solr anterior a 8.2.2: Vulnerabilidad SSRF de ReplicationHandler a través de leaderURL (CVE-2021-27905)
999249	CVE-2021-27905	WEB-MISC Apache Solr anterior a 8.2.2: Vulnerabilidad SSRF de ReplicationHandler a través de masterURL (CVE-2021-27905)
999250	CVE-2021-27890	WEB-MISC MyBB anterior a 1.8.26 - Propiedades del tema Vulnerabilidad de inyección SQL (CVE-2021-27890)
999251	CVE-2021-27850, CVE-2019-0195	WEB-MISC Apache Tapestry: Vulnerabilidad de divulgación de información no autenticada (CVE-2021-27850 y CVE-2019-0195)
999252	CVE-2021-27183	WEB-MISC MDaemon anterior a 20.0.4: Vulnerabilidad de escritura arbitraria de archivos (CVE-2021-27183)

Regla de firma	ID de CVE	Descripción
999253	CVE-2021-27181	WEB-MISC MDaemon anterior a 20.0.4: Vulnerabilidad de fijación de tokens anti-CSRF (CVE-2021-27181)
999254	CVE-2021-27180	WEB-MISC MDaemon anterior a 20.0.4: Vulnerabilidad XSS reflejada (CVE-2021-27180)
999255	CVE-2021-24340	WEB-WORDPRESS WP Statistics anteriores a 13.0.8: Vulnerabilidad de inyección SQL no autenticada (CVE-2021-24340)
999256	CVE-2021-24171	WEB-WORDPRESS WooCommerce Subir archivos Plugin antes de 59.4: Vulnerabilidad de recorrido de ruta (CVE-2021-24171)
999257	CVE-2021-24171	WEB-WORDPRESS Plugin de carga de archivos WooCommerce antes de 59.4: Vulnerabilidad de carga arbitraria de archivos (CVE-2021-24171)
999258	CVE-2021-22658	WEB-MISC Advantech iView anterior a 5.7.03.6112: Vulnerabilidad SQLi a través de UserServlet y user_password (CVE-2021-22658)
999259	CVE-2021-22658	WEB-MISC Advantech iView anterior a 5.7.03.6112: Vulnerabilidad SQLi a través de UserServlet y user_name (CVE-2021-22658)

Regla de firma	ID de CVE	Descripción
999260	CVE-2021-22658	WEB-MISC Advantech iView anterior a 5.7.03.6112: Vulnerabilidad SQLi a través de CommandServlet y user_password (CVE-2021-22658)
999261	CVE-2021-22658	WEB-MISC Advantech iView anterior a 5.7.03.6112: Vulnerabilidad SQLi a través de CommandServlet y user_name (CVE-2021-22658)
999262	CVE-2021-21983	WEB-MISC VMware vRealize Operations Manager anterior a 8.4: Vulnerabilidad de escritura arbitraria de archivos (CVE-2021-21983)
999263	CVE-2020-6754	WEB-MISC dotCMS anteriores a 5.2.4: Vulnerabilidad de recorrido de directorios a través de activos (CVE-2020-6754)
999264	CVE-2020-27128	WEB-MISC Cisco SD-WAN vManage anterior a 20.3.1: Vulnerabilidad de escritura arbitraria de archivos mediante procesamiento remoto (CVE-2020-27128)
999265	CVE-2020-27128	WEB-MISC Cisco SD-WAN vManage anterior a 20.3.1: Vulnerabilidad de escritura arbitraria de archivos a través de dr (CVE-2020-27128)
999266	CVE-2020-15714	WEB-MISC RConfig 3.9.5 y anteriores: Vulnerabilidad de inyección SQL (CVE-2020-15714)

Regla de firma	ID de CVE	Descripción
999267	CVE-2020-15713	WEB-MISC RConfig anterior a 3.9.6: Vulnerabilidad de inyección SQL (CVE-2020-15713)
999268	CVE-2020-14295	Cactus WEB-MISC anteriores a 1.2.13: Vulnerabilidad de inyección SQL (CVE-2020-14295)
999269	CVE-2020-13778	WEB-MISC RConfig anterior a 3.9.5: Vulnerabilidad de ejecución remota de código a través de ajaxEditTemplate.php (CVE-2020-13778)
999270	CVE-2020-13778	WEB-MISC RConfig anterior a 3.9.5: Vulnerabilidad de ejecución remota de código a través de ajaxAddTemplate.php (CVE-2020-13778)
999271	CVE-2020-13592	Aplicación WEB-MISC Rukovoditel Project Management: Vulnerabilidad de inyección SQL a través de selected_fields (CVE-2020-13592)
999272	CVE-2020-13592	WEB-MISC Rukovoditel Project Management App: Vulnerabilidad de inyección SQL a través de lists_id (CVE-2020-13592)
999273	CVE-2020-13591	Aplicación WEB-MISC Rukovoditel Project Management: Vulnerabilidad de inyección SQL (CVE-2020-13591)

Regla de firma	ID de CVE	Descripción
999274	CVE-2020-13550	WEB-MISC Advantech WebAccess/SCADA: Vulnerabilidad de recorrido de ruta mediante nombre de archivo (CVE-2020-13550)

Actualización de la firma para julio de 2021

January 21, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la semana 2021-07-08. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

Las firmas son compatibles con las siguientes versiones de software de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 y 13.1.

La versión 12.0 de Citrix ADC ha llegado al final de su vida útil (EOL). Para obtener más información, consulte la página del ciclo de vida de la versión

> **Nota: La**
>
> habilitación de las reglas de firma de cuerpo posterior y cuerpo de respuesta puede afectar a la CPU de Citrix ADC.

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999231	CVE-2021-34074	WEB-MISC Artica Pandora FMS hasta 7.54: Vulnerabilidad de carga arbitraria de archivos a través de ruta relativa (CVE-2021-34074)

Regla de firma	ID de CVE	Descripción
999232	CVE-2021-32633	WEB-MISC Plone CMS - Plantillas de página de Zope Vulnerabilidad de ejecución remota de código mediante carga (CVE-2021-32633)
999233	CVE-2021-32633	WEB-MISC Plone CMS - Plantillas de página de Zope Vulnerabilidad de ejecución remota de código a través de nuevo (CVE-2021-32633)
999234	CVE-2021-31181	WEB-MISC Microsoft SharePoint Server: Vulnerabilidad de ejecución remota de código (CVE-2021-31181)
999235	CVE-2021-24370	Plugin de diseñador de productos de lujo WEB-WORDPRESS antes de 5.6.9: Vulnerabilidad RCE a través de fpd_custom_uplod_file (CVE-2021-24370)
999236	CVE-2021-24370	Plugin de diseñador de productos de lujo WEB-WORDPRESS antes de 5.6.9: Vulnerabilidad de RCE a través de custom-image-handler.php (CVE-2021-24370)
999237	CVE-2021-24354	WEB-WORDPRESS Simple 301 redirige el complemento antes de la 2.0.4: Vulnerabilidad de instalación arbitraria de complementos (CVE-2021-24354)

Regla de firma	ID de CVE	Descripción
999238	CVE-2021-24352	WEB-WORDPRESS Simple 301 redirige el plugin antes de 2.0.4: Vulnerabilidad de exportación de redirección (CVE-2021-24352)
999239	CVE-2021-1497, CVE-2021-1498	WEB-MISC Cisco HyperFlex HX anterior a 4.0 (2e): Vulnerabilidad de ejecución remota de código (CVE-2021-1497, CVE-2021-1498)
999240	CVE-2020-21057	WEB-MISC FusionPBX 4.5.7: Vulnerabilidad de recorrido de ruta mediante la función de eliminación de carpetas (CVE-2020-21057)
999241	CVE-2020-16245	WEB-MISC Advantech iView anterior a 5.7.03.6112: Vulnerabilidad de recorrido de rutas a través de backupDatabase (CVE-2020-16245)
999242	CVE-2020-10148	WEB-MISC SolarWinds Orion múltiples versiones: Vulnerabilidad de omisión de autenticación (CVE-2020-10148)

Actualización de firmas para agosto de 2021

January 21, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la semana 2021-08-29. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

Las firmas son compatibles con las siguientes versiones de software de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 y 13.1.

La versión 12.0 de Citrix ADC ha llegado al final de su vida útil (EOL). Para obtener más información, consulte la página del ciclo de vida de la versión

> **Nota: La**
>
> habilitación de las reglas de firma de cuerpo posterior y cuerpo de respuesta puede afectar a la CPU de Citrix ADC.

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999183	CVE-2021-37557	Versiones múltiples de WEB-MISC Centreon: Vulnerabilidad de inyección SQL (CVE-2021-37557)
999184	CVE-2021-35501	WEB-MISC Artica Pandora FMS hasta 7.54: Vulnerabilidad XSS almacenada en Visual Console (CVE-2021-35501)
999185	CVE-2021-35464	WEB-MISC ForgeRock Access Management y OpenAM: Vulnerabilidad de ejecución remota de código (CVE-2021-35464)
999186	CVE-2021-34523	WEB-MISC Microsoft Exchange Server: Vulnerabilidad de elevación de privilegios (CVE-2021-34523)

Regla de firma	ID de CVE	Descripción
999187	CVE-2021-34473	WEB-MISC Microsoft Exchange Server: Vulnerabilidad de omisión de autenticación de falsificación de solicitud del lado del servidor mediante consulta (CVE-2021-34473)
999188	CVE-2021-34473	WEB-MISC Microsoft Exchange Server: Vulnerabilidad de omisión de autenticación de falsificación de solicitud del lado del servidor mediante cookie (CVE-2021-34473)
999189	CVE-2021-33203	WEB-MISC Django: Vulnerabilidad de divulgación de existencia de archivos TemplateDetailView a través de la ruta absoluta (CVE-2021-33203)
999190	CVE-2021-33203	WEB-MISC Django: Vulnerabilidad de divulgación de existencia de archivos TemplateDetailView a través de la ruta de acceso (CVE-2021-33203)
999191	CVE-2021-33203	WEB-MISC Django: Vulnerabilidad de divulgación de existencia de archivo TemplateDetailView a través de barra invertida (CVE-2021-33203)
999192	CVE-2021-33203	WEB-MISC Django: Vulnerabilidad de divulgación de existencia de archivo TemplateDetailView a través de barra (CVE-2021-33203)

Regla de firma	ID de CVE	Descripción
999193	CVE-2021-3287, CVE-2020-28653	WEB-MISC Zoho ManageEngine OpManager anterior a 12.5.329: Vulnerabilidad de RCE no autenticada (CVE-2021-3287, CVE-2020-28653)
999194	CVE-2021-32789	Complemento de WooCommerce de WEB-WORDPRESS hasta 5.5.0: Vulnerabilidad de inyección de SQL a través de taxonomía y rest_route (CVE-2021-32789)
999195	CVE-2021-32789	Complemento de WooCommerce de WEB-WORDPRESS hasta 5.5.0: Vulnerabilidad de inyección SQL a través de taxonomía (CVE-2021-32789)
999196	CVE-2021-32604	WEB-MISC SolarWinds Serv-U anterior a 15.2.3: Vulnerabilidad de scripts entre sitios a través del parámetro SenderEmail (CVE-2021-32604)
999197	CVE-2021-32093	Emisario de la Agencia de Seguridad Nacional WEB-MISC 5.9.0: Vulnerabilidad de lectura arbitraria de archivos (CVE-2021-32093)
999198	CVE-2021-31760	WEB-MISC Webmin anterior a 1.974 - La vulnerabilidad CSRF conduce a RCE a través de run.cgi (CVE-2021-31760)

Regla de firma	ID de CVE	Descripción
999199	CVE-2021-31207	WEB-MISC Microsoft Exchange Server: Vulnerabilidad de omisión de funciones de seguridad (CVE-2021-31207)
999200	CVE-2021-31195	WEB-MISC Microsoft Exchange Server: Vulnerabilidad de ejecución remota de código (CVE-2021-31195)
999201	CVE-2021-28474	WEB-MISC Microsoft SharePoint Server: Vulnerabilidad de ejecución remota de código (CVE-2021-28474)
999202	CVE-2021-24385	Plug-in WEB-WORDPRESS FileBird 4.7.3: Vulnerabilidad de inyección SQL a través del parámetro selectedFolder y rest_route (CVE-2021-24385)
999203	CVE-2021-24385	Plug-in WEB-WORDPRESS FileBird 4.7.3: Vulnerabilidad de inyección SQL a través del parámetro selectedFolder (CVE-2021-24385)
999204	CVE-2021-24385	Plug-in WEB-WORDPRESS FileBird 4.7.3: Vulnerabilidad de inyección SQL a través del cuerpo codificado en JSON (CVE-2021-24385)
999205	CVE-2021-24356	Complemento de redirecciones simple 301 de WEB-WORDPRESS anterior a 2.0.4: Vulnerabilidad de activación arbitraria de complementos (CVE-2021-24356)

Regla de firma	ID de CVE	Descripción
999206	CVE-2021-23024	WEB-MISC F5 BIG-IQ Múltiples versiones: Vulnerabilidad de ejecución remota de código (CVE-2021-23024)
999207	CVE-2021-22911	WEB-MISC Rocket.Chat Server 3.11, 3.12 y 3.13: Vulnerabilidad de inyección ciega de NOSQL (CVE-2021-22911)
999208	CVE-2021-22900	WEB-MISC Pulse Connect Secure antes de 9.1R11.4: Vulnerabilidad de ejecución remota de código a través de smimeCert.cgi (CVE-2021-22900)
999209	CVE-2021-22900	WEB-MISC Pulse Connect Secure antes de 9.1R11.4: Vulnerabilidad de ejecución remota de código a través de admincert.cgi (CVE-2021-22900)
999210	CVE-2021-22900	WEB-MISC Pulse Connect Secure antes de 9.1R11.4: Vulnerabilidad de ejecución remota de código a través de clientauthcert.cgi (CVE-2021-22900)
999211	CVE-2021-22160	WEB-MISC Apache Pulsar: Vulnerabilidad de omisión de autenticación de tokens web JSON (CVE-2021-22160)
999212	CVE-2021-21809	WEB-MISC Moodle: Vulnerabilidad de ejecución remota de código a través del complemento Spellchecker y el método getSuggestions (CVE-2021-21809)

Regla de firma	ID de CVE	Descripción
999213	CVE-2021-21809	WEB-MISC Moodle: Vulnerabilidad de ejecución remota de código a través del complemento corrector ortográfico y el método checkWords (CVE-2021-21809)
999214	CVE-2021-21809	WEB-MISC Moodle: Vulnerabilidad de ejecución remota de código a través de s__aspellpath (CVE-2021-21809)
999215	CVE-2021-21805	WEB-MISC Advantech R-SeeNet: Vulnerabilidad de ejecución remota de código no autenticada (CVE-2021-21805)
999216	CVE-2021-21804	WEB-MISC Advantech R-SeeNet: Vulnerabilidad de inclusión de archivos locales a través de sub_opt (CVE-2021-21804)
999217	CVE-2021-21587	WEB-MISC Dell Wyse Management Suite anterior a 3.3: Vulnerabilidad de recorrido de ruta a través de /image/os/listfiles (CVE-2021-21587)
999218	CVE-2021-21587	WEB-MISC Dell Wyse Management Suite anterior a 3.3: Vulnerabilidad de recorrido de ruta a través de /image/app/rsp/listfiles (CVE-2021-21587)

Regla de firma	ID de CVE	Descripción
999219	CVE-2021-21586	WEB-MISC Dell Wyse Management Suite anterior a 3.3: Vulnerabilidad de recorrido de ruta a través de /image/app y FileName (CVE-2021-21586)
999220	CVE-2021-21586	WEB-MISC Dell Wyse Management Suite anterior a 3.3: Vulnerabilidad de recorrido de ruta a través de /image/os y FileName (CVE-2021-21586)
999221	CVE-2021-21586	WEB-MISC Dell Wyse Management Suite anterior a 3.3: Vulnerabilidad de recorrido de ruta a través de /image/os y filePath (CVE-2021-21586)
999222	CVE-2020-25223	WEB-MISC Sophos SG UTM: ejecución remota de código mediante SID y /var (CVE-2020-25223)
999223	CVE-2020-25223	WEB-MISC Sophos SG UTM: ejecución remota de código a través de SID y /webadmin.plx (CVE-2020-25223)
999224	CVE-2020-21056	WEB-MISC FusionPBX 4.5.7: Vulnerabilidad de recorrido de ruta a través de foldernew (CVE-2020-21056)
999225	CVE-2020-21055	WEB-MISC FusionPBX 4.5.7: Vulnerabilidad de recorrido de ruta mediante la función de cambio de nombre de archivo (CVE-2020-21055)

Regla de firma	ID de CVE	Descripción
999226	CVE-2020-16245	WEB-MISC Advantech iView anterior a 5.7.03.6112: Vulnerabilidad de recorrido de ruta en findSummaryUpdateDeviceListExpo (CVE-2020-16245)
999227	CVE-2020-16245	WEB-MISC Advantech iView anterior a 5.7.03.6112: Vulnerabilidad de recorrido de ruta a través de findCfgDeviceListExport (CVE-2020-16245)
999228	CVE-2020-14181	WEB-MISC Atlassian Jira Server: Vulnerabilidad de divulgación de información a través de ViewUserHover.jspa (CVE-2020-14181)
999229	CVE-2020-14005	WEB-MISC SolarWinds Orion antes de 2020.2.1 HF 2 - Ejecución remota de código mediante el tipo de acción ExecuteVBScript (CVE-2020-14005)
999230	CVE-2020-14005	WEB-MISC SolarWinds Orion anterior a 2020.2.1 HF 2 - Ejecución remota de código mediante el tipo de acción ExecuteExternalProgram (CVE-2020-14005)

Actualización de firmas para septiembre de 2021

January 21, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la semana 2021-09-11.

Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

Las firmas son compatibles con las siguientes versiones de software de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 y 13.1.

La versión 12.0 de Citrix ADC ha llegado al final de su vida útil (EOL). Para obtener más información, consulte la página del ciclo de vida de la versión

> **Nota: La**
>
> habilitación de las reglas de firma de cuerpo posterior y cuerpo de respuesta puede afectar a la CPU de Citrix ADC.

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999163	CVE-2021-37556	WEB-MISC Centreon Múltiples versiones: Vulnerabilidad de inyección SQL a través del parámetro End (CVE-2021-37556)
999164	CVE-2021-37556	WEB-MISC Centreon Múltiples versiones: Vulnerabilidad de inyección SQL a través del parámetro Start (CVE-2021-37556)
999165	CVE-2021-37353	WEB-MISC Nagios XI Docker Wizard anterior a 1.1.3: Vulnerabilidad SSRF a través de parámetros de host sin esquema URI (CVE-2021-37353)

Regla de firma	ID de CVE	Descripción
999166	CVE-2021-37353	WEB-MISC Nagios XI Docker Wizard anterior a 1.1.3: Vulnerabilidad SSRF a través de parámetros de host con esquema URI (CVE-2021-37353)
999167	CVE-2021-34638	Complemento de administrador de descargas WEB-WORDPRESS anterior a 3.1.25: Vulnerabilidad de cruce de directorios (CVE-2021-34638)
999168	CVE-2021-33766	WEB-MISC Microsoft Exchange Server: Vulnerabilidad de divulgación de información (CVE-2021-33766)
999169	CVE-2021-32682	WEB-MISC elFinder anterior a 2.1.59: Vulnerabilidad de inyección de comandos a través de archivo (CVE-2021-32682)
999170	CVE-2021-26084	Servidor y centro de datos de WEB-MISC Confluence: Vulnerabilidad de inyección OGNL a través de doenterpagevariables (CVE-2021-26084)
999171	CVE-2021-26084	Servidor y centro de datos de WEB-MISC Confluence: Vulnerabilidad de inyección OGNL a través de createpage-entervariables (CVE-2021-26084)

Regla de firma	ID de CVE	Descripción
999172	CVE-2021-23394	WEB-MISC elFinder anterior a 2.1.59: Vulnerabilidad de ejecución remota de código a través de Phar Makefile (CVE-2021-23394)
999173	CVE-2021-23394	WEB-MISC elFinder anterior a 2.1.59: Vulnerabilidad de ejecución remota de código mediante cambio de nombre de Phar (CVE-2021-23394)
999174	CVE-2021-23394	WEB-MISC elFinder anterior a 2.1.59: Vulnerabilidad de ejecución remota de código mediante carga Phar (CVE-2021-23394)
999175	CVE-2020-36289	WEB-MISC Atlassian Jira Server: Vulnerabilidad de divulgación de información mediante QueryComponentRendererValue (CVE-2020-36289)
999176	CVE-2020-16245	WEB-MISC Advantech iView anterior a 5.7.03.6112: Vulnerabilidad de recorrido de ruta a través de findSummaryCfgDeviceListExport (CVE-2020-16245)
999177	CVE-2020-16245	WEB-MISC Advantech iView anterior a 5.7.03.6112: Vulnerabilidad de recorrido de ruta a través de findUpdateDeviceListExport (CVE-2020-16245)

Regla de firma	ID de CVE	Descripción
999178	CVE-2020-13774	Varias versiones de WEB-MISC Ivanti Endpoint Manager: Vulnerabilidad de RCE a través de EditLaunchPadDialog.aspx (CVE-2020-13774)
999179	CVE-2020-1147	WEB-MISC Microsoft SharePoint Server: Vulnerabilidad de ejecución remota de código mediante página personalizada (CVE-2020-1147)
999180	CVE-2020-1147	WEB-MISC Microsoft SharePoint Server: Vulnerabilidad de ejecución remota de código mediante quicklinksdialogform.aspx (CVE-2020-1147)
999181	CVE-2020-1147	WEB-MISC Microsoft SharePoint Server: Vulnerabilidad de ejecución remota de código mediante quicklinks.aspx (CVE-2020-1147)
999182	CVE-2020-11110	WEB-MISC Apache Grafana hasta 6.7.1: Vulnerabilidad XSS (CVE-2020-11110)
999522	CVE-2020-13379	WEB-MISC Grafana 3.0.1 a 7.0.1 - Bypass de CSRF que conduce a una vulnerabilidad de DOS (CVE-2020-13379)

Actualización de firmas para octubre de 2021

January 21, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la semana 2021-10-09. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

Las firmas son compatibles con las siguientes versiones de software de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 y 13.1.

La versión 12.0 de Citrix ADC ha llegado al final de su vida útil (EOL). Para obtener más información, consulte la página del ciclo de vida de la versión

> **Nota: La**
>
> habilitación de las reglas de firma de cuerpo posterior y cuerpo de respuesta puede afectar a la CPU de Citrix ADC.

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999149	CVE-2021-38312	Biblioteca de plantillas WEB-WORDPRESS Gutenberg y complemento Redux Framework antes de 4.2.12: Vulnerabilidad REST_ROUTE (CVE-2021-38312)
999150	CVE-2021-38312	Biblioteca de plantillas WEB-WORDPRESS Gutenberg y complemento Redux Framework anterior a 4.2.12: Vulnerabilidad de la API REST (CVE-2021-38312)

Regla de firma	ID de CVE	Descripción
999151	CVE-2021-34639	Plug-in WEB-WORDPRESS Download Manager anterior a 3.1.25: Vulnerabilidad de carga de doble extensión (CVE-2021-34639)
999152	CVE-2021-34621	Plug-in WEB-WORDPRESS ProfilePress anterior a 3.1.3 - Elevación de la vulnerabilidad de privilegios a través de wp_capabilities (CVE-2021-34621)
999153	CVE-2021-32682	WEB-MISC elFinder anterior a 2.1.59: Vulnerabilidad de recorrido de ruta mediante el comando Rename (CVE-2021-32682)
999154	CVE-2021-32682	WEB-MISC elFinder anterior a 2.1.59: Vulnerabilidad de recorrido de ruta a través del comando Abort (CVE-2021-32682)
999155	CVE-2021-26086	WEB-MISC Atlassian Jira Server and Data Center: Vulnerabilidad de divulgación de información a través de WEB-INF (CVE-2021-26086)
999156	CVE-2021-26086	WEB-MISC Atlassian Jira Server and Data Center: Vulnerabilidad de divulgación de información a través de META-INF (CVE-2021-26086)
999157	CVE-2021-22005	WEB-MISC VMware vCenter: Vulnerabilidad de carga de archivos a través de la aplicación de datos (CVE-2021-22005)

Regla de firma	ID de CVE	Descripción
999158	CVE-2021-22005	WEB-MISC VMware vCenter: Vulnerabilidad de carga de archivos mediante el registro de etapa de telemetría (CVE-2021-22005)
999159	CVE-2021-22005	WEB-MISC VMware vCenter: Vulnerabilidad de carga de archivos mediante el registro de producto de telemetría (CVE-2021-22005)
999160	CVE-2021-20081	WEB-MISC Zoho ManageEngine Service Desk anterior a 11.2.0.5: Vulnerabilidad de ejecución remota de código (CVE-2021-20081)
999161	CVE-2020-29453	WEB-MISC Atlassian Jira Server and Data Center: Vulnerabilidad de divulgación de información a través de WEB-INF (CVE-2020-29453)
999162	CVE-2020-29453	WEB-MISC Atlassian Jira Server and Data Center: Vulnerabilidad de divulgación de información a través de META-INF (CVE-2020-29453)

Actualización de firmas para octubre de 2021

January 21, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la semana 2021-10-26. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

Las firmas son compatibles con las siguientes versiones de software de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 y 13.1.

La versión 12.0 de Citrix ADC ha llegado al final de su vida útil (EOL). Para obtener más información, consulte la página del ciclo de vida de la versión

> **Nota: La**
>
> habilitación de las reglas de firma de cuerpo posterior y cuerpo de respuesta puede afectar a la CPU de Citrix ADC.

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999127	CVE-2021-42013	Servidor HTTP Apache WEB-MISC 2.4.49 y 2.4.50: Vulnerabilidad de recorrido de ruta a través de %%32 (CVE-2021-42013)
999128	CVE-2021-42013	Servidor HTTP Apache WEB-MISC 2.4.49 y 2.4.50: Vulnerabilidad de recorrido de ruta a través de% 2% (CVE-2021-42013)
999129	CVE-2021-41773	WEB-MISC Apache HTTP Server 2.4.49: Vulnerabilidad de recorrido de ruta a través de %2e%2e (CVE-2021-41773)
999130	CVE-2021-41773	WEB-MISC Apache HTTP Server 2.4.49: Vulnerabilidad de recorrido de ruta a través de.% 2e (CVE-2021-41773)

Regla de firma	ID de CVE	Descripción
999131	CVE-2021-40539	WEB-MISC Zoho ManageEngine ADSelfService Plus 6.1 anterior a la compilación 6114: Vulnerabilidad de omisión de autenticación (CVE-2021-40539)
999132	CVE-2021-34648	Plug-in WEB-WORDPRESS Ninja Forms hasta 3.5.7: Vulnerabilidad REST_ROUTE a través de la acción de correo electrónico de envíos (CVE-2021-34648)
999133	CVE-2021-34648	Plug-in WEB-WORDPRESS Ninja Forms hasta 3.5.7: Vulnerabilidad de la API REST a través de la acción de correo electrónico de envíos (CVE-2021-34648)
999134	CVE-2021-34647	Plug-in WEB-WORDPRESS Ninja Forms hasta 3.5.7: Vulnerabilidad REST_ROUTE mediante la exportación de envíos (CVE-2021-34647)
999135	CVE-2021-34647	Plug-in WEB-WORDPRESS Ninja Forms hasta 3.5.7: Vulnerabilidad de la API REST a través de la exportación de envíos (CVE-2021-34647)
999136	CVE-2021-34623	Plug-in WEB-WORDPRESS ProfilePress anterior a 3.1.4: Vulnerabilidad de carga arbitraria de archivos a través de eup_cover_image (CVE-2021-34623)

Regla de firma	ID de CVE	Descripción
999137	CVE-2021-34623	Plug-in WEB-WORDPRESS ProfilePress anterior a 3.1.4: Vulnerabilidad de carga arbitraria de archivos a través de eup_avatar (CVE-2021-34623)
999138	CVE-2021-2400	WEB-MISC Oracle BI Publisher: Vulnerabilidad de SAXParser XXE a través de Mobile X ReportTemplateService (CVE-2021-2400)
999139	CVE-2021-2400	WEB-MISC Oracle BI Publisher: Vulnerabilidad de SAXParser XXE a través de Mobile ReportTemplateService (CVE-2021-2400)
999140	CVE-2021-2400	WEB-MISC Oracle BI Publisher: Vulnerabilidad de SAXParser XXE a través de xmlpservice X ReportTemplateService (CVE-2021-2400)
999141	CVE-2021-2400	WEB-MISC Oracle BI Publisher: Vulnerabilidad de SAXParser XXE a través de xmlpservice ReportTemplateService (CVE-2021-2400)
999142	CVE-2021-21985	WEB-MISC VMware vCenter: Vulnerabilidad de ejecución remota de código del complemento Virtual SAN Health Check (CVE-2021-21985)

Regla de firma	ID de CVE	Descripción
999143	CVE-2021-20078	WEB-MISC Zoho ManageEngine OpManager 12.5 anterior a la compilación 125362: Vulnerabilidad de recorrido de ruta (CVE-2021-20078)
999144	CVE-2020-29448	WEB-MISC Atlassian Confluence Server and Data Center: Vulnerabilidad de divulgación de información a través de WEB-INF (CVE-2020-29448)
999145	CVE-2020-29448	WEB-MISC Atlassian Confluence Server and Data Center: Vulnerabilidad de divulgación de información a través de META-INF (CVE-2020-29448)
999146	CVE-2020-12442	WEB-MISC Ivanti Avalanche 6.3: Vulnerabilidad de inyección de SQL no autenticada a través del dispositivo de punto final osupdate (CVE-2020-12442)
999147	CVE-2020-12442	WEB-MISC Ivanti Avalanche 6.3: Vulnerabilidad de inyección de SQL no autenticada a través del dispositivo de punto final wapl (CVE-2020-12442)
999148		Plug-in WEB-WORDPRESS BuddyPress anterior a 9.1.1: Vulnerabilidad de inyección SQL a través de la función bp-members-invitations

Actualización de firmas para noviembre de 2021

January 21, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la semana 2021-11-18. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

Las firmas son compatibles con las siguientes versiones de software de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 y 13.1.

La versión 12.0 de Citrix ADC ha llegado al final de su vida útil (EOL). Para obtener más información, consulte la página del ciclo de vida de la versión

> **Nota: La**
>
> habilitación de las reglas de firma de cuerpo posterior y cuerpo de respuesta puede afectar a la CPU de Citrix ADC.

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999098	CVE-2021-41765	WEB-MISC ResourceSpace 9.5 y 9.6 antes de la rev 18274: Vulnerabilidad de inyección SQL (CVE-2021-41765)
999099	CVE-2021-41288	WEB-MISC Zoho ManageEngine OpManager antes de la compilación 125467: Vulnerabilidad de inyección SQL a través de la API getReportData (CVE-2021-41288)

Regla de firma	ID de CVE	Descripción
999100	CVE-2021-40493	WEB-MISC Zoho ManageEngine OpManager antes de la compilación 125437: Vulnerabilidad de inyección SQL a través de DeviceName (CVE-2021-40493)
999101	CVE-2021-40493	WEB-MISC Zoho ManageEngine OpManager antes de la compilación 125437: Vulnerabilidad de inyección SQL a través de pollingObject (CVE-2021-40493)
999102	CVE-2021-40438	Servidor HTTP Apache WEB-MISC: Vulnerabilidad de reenvío de solicitud mod_proxy (CVE-2021-40438)
999103	CVE-2021-39341	Plug-in WEB-WORDPRESS OptinMonster hasta 2.6.4: Vulnerabilidad de omisión de permiso REST_ROUTE (CVE-2021-39341)
999104	CVE-2021-39341	Plug-in WEB-WORDPRESS OptinMonster hasta 2.6.4: Vulnerabilidad de omisión de permiso de la API REST (CVE-2021-39341)
999105	CVE-2021-37344	WEB-MISC Nagios XI Switch Wizard anterior a 2.5.7: Vulnerabilidad de ejecución remota de código a través del parámetro ip_address (CVE-2021-37344)

Regla de firma	ID de CVE	Descripción
999106	CVE-2021-35218	WEB-MISC SolarWinds Orion anterior a 2020.2.6: Vulnerabilidad de deserialización a través de Chart.ashx (CVE-2021-35218)
999107	CVE-2021-35215	WEB-MISC SolarWinds Orion Platform anterior a 2020.2.6: Vulnerabilidad de ejecución remota de código mediante informes (CVE-2021-35215)
999108	CVE-2021-35215	WEB-MISC SolarWinds Orion Platform anterior a 2020.2.6: Vulnerabilidad de ejecución remota de código mediante alertas (CVE-2021-35215)
999109	CVE-2021-24889	Plug-in WEB-WORDPRESS Ninja Forms anterior a 3.6.4: Vulnerabilidad de inyección SQL (CVE-2021-24889)
999110	CVE-2021-24381	Plug-in WEB-WORDPRESS Ninja Forms anterior a 3.5.8.2: Vulnerabilidad de scripts entre sitios almacenadas con nombre de clase personalizado (CVE-2021-24381)
999111	CVE-2021-2401	WEB-MISC Oracle BI Publisher: Vulnerabilidad de DOMParser XXE a través de Mobile X ReportTemplateService (CVE-2021-2401)

Regla de firma	ID de CVE	Descripción
999112	CVE-2021-2401	WEB-MISC Oracle BI Publisher: Vulnerabilidad de DOMParser XXE a través de Mobile ReportTemplateService (CVE-2021-2401)
999113	CVE-2021-2401	WEB-MISC Oracle BI Publisher: Vulnerabilidad de DOMParser XXE a través de xmlpservice X ReportTemplateService (CVE-2021-2401)
999114	CVE-2021-2401	WEB-MISC Oracle BI Publisher: Vulnerabilidad de DOMParser XXE a través de xmlpservice ReportTemplateService (CVE-2021-2401)
999115	CVE-2021-2392	WEB-MISC Oracle BI Publisher: Vulnerabilidad de carga de archivos arbitrarios (CVE-2021-2392)
999116	CVE-2021-2244	WEB-MISC Oracle Hyperion-Essbase Analytic Provider Services: Vulnerabilidad de ejecución remota de código a través de Essbase (CVE-2021-2244)
999117	CVE-2021-2244	WEB-MISC Oracle Hyperion-Essbase Analytic Provider Services: Vulnerabilidad de ejecución remota de código mediante admin (CVE-2021-2244)

Regla de firma	ID de CVE	Descripción
999118	CVE-2021-2244	WEB-MISC Oracle Hyperion-Essbase Analytic Provider Services: Vulnerabilidad de ejecución remota de código a través de JAPI (CVE-2021-2244)
999119	CVE-2021-22205	WEB-MISC GitLab CE/EE: Vulnerabilidad de ejecución remota de código a través de archivos JPEG/TIFF creados con fines malintencionados (CVE-2021-22205)
999120	CVE-2021-22017	WEB-MISC VMware vCenter: Vulnerabilidad de recorrido de ruta a través de rhhtproxy (CVE-2021-22017)
999121	CVE-2021-20837	WEB-MISC Tipo móvil anterior a r.5003 - Ejecución remota de código a través de mt.handler_to_coderef (CVE-2021-20837)
999122	CVE-2021-20131	WEB-MISC Zoho ManageEngine AdManager anterior a la compilación 7115: Vulnerabilidad de ejecución remota de código mediante la carga de archivos (CVE-2021-20131)
999123	CVE-2021-20130	WEB-MISC Zoho ManageEngine AdManager anterior a la compilación 7115: Vulnerabilidad de ejecución remota de código mediante la carga de archivos (CVE-2021-20130)

Regla de firma	ID de CVE	Descripción
999124	CVE-2021-20034	WEB-MISC SonicWALL Secure Mobile Access: Vulnerabilidad de recorrido de ruta (CVE-2021-20034)
999125		Plug-in WEB-WORDPRESS BuddyPress anterior a la versión 9.1.1: Vulnerabilidad de divulgación de información a través de la API REST de registro y rest_route
999126		Plug-in WEB-WORDPRESS BuddyPress anterior a 9.1.1: Vulnerabilidad de divulgación de información a través de la API REST de registro

Actualización de firmas para diciembre de 2021

January 21, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la semana 2021-12-11. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

Las firmas son compatibles con las siguientes versiones de software de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 y 13.1.

La versión 12.0 de Citrix ADC ha llegado al final de su vida útil (EOL). Para obtener más información, consulte la página del ciclo de vida de la versión

> **Nota: La**
>
> habilitación de las reglas de firma de cuerpo posterior y cuerpo de respuesta puede afectar a la CPU de Citrix ADC.

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999077	CVE-2021-44228	WEB-MISC Apache Log4j: Vulnerabilidad de ejecución remota de código a través de FORM (CVE-2021-44228)
999078	CVE-2021-44228	WEB-MISC Apache Log4j: Vulnerabilidad de ejecución remota de código a través de BODY (CVE-2021-44228)
999079	CVE-2021-44228	WEB-MISC Apache Log4j: Vulnerabilidad de ejecución remota de código a través de HEADER (CVE-2021-44228)
999080	CVE-2021-44228	WEB-MISC Apache Log4j: Vulnerabilidad de ejecución remota de código a través de URL (CVE-2021-44228)
999081	CVE-2021-42847	WEB-MISC Zoho ManageEngine ADAudit Plus anterior a 7006: Vulnerabilidad de escritura de archivos arbitrarios no autenticados (CVE-2021-42847)
999082	CVE-2021-42321	WEB-MISC Microsoft Exchange Server: Vulnerabilidad de ejecución remota de código (CVE-2021-42321)
999083	CVE-2021-42258	WEB-MISC BQE BillQuick Web Suite 2021: Vulnerabilidad de inyección de SQL no autenticada a través de txtID (CVE-2021-42258)

Regla de firma	ID de CVE	Descripción
999084	CVE-2021-42258	WEB-MISC BQE BillQuick Web Suite 2020: Vulnerabilidad de inyección de SQL no autenticada a través de txtID (CVE-2021-42258)
999085	CVE-2021-42258	WEB-MISC BQE BillQuick Web Suite 2019: Vulnerabilidad de inyección SQL no autenticada a través de txtID (CVE-2021-42258)
999086	CVE-2021-42258	WEB-MISC BQE BillQuick Web Suite 2018: Vulnerabilidad de inyección de SQL no autenticada a través de txtID (CVE-2021-42258)
999087	CVE-2021-42237	WEB-MISC Sitecore de 7.5.0 a 8.2.7: Vulnerabilidad de ejecución remota de código (CVE-2021-42237)
999088	CVE-2021-41950	WEB-MISC ResourceSpace 9.6 anterior a la rev 18277: Vulnerabilidad de recorrido de ruta no autenticada a través de una variante (CVE-2021-41950)
999089	CVE-2021-41950	WEB-MISC ResourceSpace 9.6 anterior a la rev 18277: Vulnerabilidad de recorrido de ruta no autenticada a través del proveedor (CVE-2021-41950)
999090	CVE-2021-41349	WEB-MISC Microsoft Exchange Server: Vulnerabilidad de scripts entre sitios (CVE-2021-41349)

Regla de firma	ID de CVE	Descripción
999091	CVE-2021-35217	WEB-MISC SolarWinds Orion antes de 2020.2.6 HF1: Vulnerabilidad de deserialización a través de WSAsyncExecuteTasks.aspx (CVE-2021-35217)
999092	CVE-2021-34416	Conector WEB-MISC Zoom Meeting 4.6.360.20210325: Vulnerabilidad de ejecución remota de código (CVE-2021-34416)
999093	CVE-2021-22941	Almacenamiento WEB-MISC Citrix ShareFile anterior a 5.11.20: Vulnerabilidad de control de acceso incorrecta (CVE-2021-22941)
999094	CVE-2020-35136	WEB-MISC Dolibarr anterior a 12.0.4: Vulnerabilidad de ejecución remota de código a través de zipfilename_template y bz (CVE-2020-35136)
999095	CVE-2020-35136	WEB-MISC Dolibarr anterior a 12.0.4: Vulnerabilidad de ejecución remota de código a través de zipfilename_template y gz (CVE-2020-35136)
999096	CVE-2020-2950, CVE-2021-2456	WEB-MISC Oracle BI Publisher: Vulnerabilidad de carga arbitraria de archivos (CVE-2020-2950, CVE-2021-2456)

Regla de firma	ID de CVE	Descripción
999097	CVE-2020-2950, CVE-2021-2456	WEB-MISC Oracle BI Publisher: Vulnerabilidad de ejecución remota de código (CVE-2020-2950, CVE-2021-2456)

Actualización de firmas para diciembre de 2021

January 21, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la semana 2021-12-13. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

Las firmas son compatibles con las siguientes versiones de software de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 y 13.1.

La versión 12.0 de Citrix ADC ha llegado al final de su vida útil (EOL). Para obtener más información, consulte la página del ciclo de vida de la versión

> **Nota: La**
>
> habilitación de las reglas de firma de cuerpo posterior y cuerpo de respuesta puede afectar a la CPU de Citrix ADC.

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, identificadores de CVE y su descripción que se actualizan.

> **Nota:**
>
> Las reglas de firma a continuación (999077, 999078, 999079, 999080) abordan ambos CVE (CVE-2021-44228 y CVE-2021-45046).

Regla de firma	ID de CVE	Descripción
999077	CVE-2021-44228, CVE-2021-45046	WEB-MISC Apache Log4j: Vulnerabilidad de ejecución remota de código a través de FORM (CVE-2021-44228, CVE-2021-45046)
999078	CVE-2021-44228, CVE-2021-45046	WEB-MISC Apache Log4j: Vulnerabilidad de ejecución remota de código a través de BODY (CVE-2021-44228, CVE-2021-45046)
999079	CVE-2021-44228, CVE-2021-45046	WEB-MISC Apache Log4j: Vulnerabilidad de ejecución remota de código a través de HEADER (CVE-2021-44228, CVE-2021-45046)
999080	CVE-2021-44228, CVE-2021-45046	WEB-MISC Apache Log4j: Vulnerabilidad de ejecución remota de código a través de URL (CVE-2021-44228, CVE-2021-45046)

Actualización de firmas para diciembre de 2021

January 21, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la semana 2021-12-21. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

Las firmas son compatibles con las siguientes versiones de software de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 y 13.1.

La versión 12.0 de Citrix ADC ha llegado al final de su vida útil (EOL). Para obtener más información, consulte la página del ciclo de vida de la versión

> **Nota: La**
>
> habilitación de las reglas de firma de cuerpo posterior y cuerpo de respuesta puede afectar a la CPU de Citrix ADC.

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999073	CVE-2021-44077	WEB-MISC Zoho ManageEngine ServiceDesk Plus antes de 11306: Vulnerabilidad de PreAuth RCE a través de ImportTechnicians (CVE-2021-44077)
999074	CVE-2021-43798	WEB-MISC Apache Grafana 8.0.0 hasta 8.3.0: Vulnerabilidad de recorrido de ruta (CVE-2021-43798)
999075	CVE-2021-35216	WEB-MISC SolarWinds Orion antes de 2020.2.6: Vulnerabilidad de deserialización a través de EditTopXX.aspx (CVE-2021-35216)
999076	CVE-2021-34993	WEB-MISC Commvault CommCell: Vulnerabilidad de omisión de autenticación CVSearchService (CVE-2021-34993)

Actualización de firmas para enero de 2022

January 31, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la semana 2022-01-20. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

Firma versión 75 aplicable a las plataformas NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1 y Citrix ADC 13.0.

> **Nota: La**
>
> habilitación de las reglas de firma de cuerpo posterior y cuerpo de respuesta puede afectar a la CPU de Citrix ADC.

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999055	CVE-2021-44224	Servidor HTTP Apache WEB-MISC - Vulnerabilidad UDS mal formada a través de proxy directo e inverso (CVE-2021-44224)
999056	CVE-2021-43815	WEB-MISC Apache Grafana: vulnerabilidad de recorrido de ruta de origen de datos de base de datos de TestData DB (CVE-2021-43815)
999057	CVE-2021-43813	WEB-MISC Apache Grafana: vulnerabilidad de recorrido de ruta a través de Markdown (CVE-2021-43813)
999058	CVE-2021-43405	WEB-MISC FusionPBX anterior a 4.5.30 - Inyección de comandos del SO a través de fax_extension (CVE-2021-43405)

Regla de firma	ID de CVE	Descripción
999059	CVE-2021-42392	Consola H2 WEB-MISC anterior a 2.0.206: vulnerabilidad de ejecución remota de código (CVE-2021-42392)
999060	CVE-2021-42362	Complemento de publicación popular de WEB-WORDPRESS anterior a 5.3.3: vulnerabilidad de carga arbitraria de archivos (CVE-2021-42362)
999061	CVE-2021-42129	WEB-MISC Ivanti Avalanche anterior a 6.3.3 - Vulnerabilidad de inyección de comandos del sistema operativo a través de txtUpass (CVE-2021-42129)
999062	CVE-2021-42129	WEB-MISC Ivanti Avalanche anterior a 6.3.3 - Vulnerabilidad de inyección de comandos del sistema operativo a través de txtUname (CVE-2021-42129)
999063	CVE-2021-42129	WEB-MISC Ivanti Avalanche anterior a 6.3.3 - Vulnerabilidad de inyección de comandos del sistema operativo a través de txtUncPath (CVE-2021-42129)
999064	CVE-2021-40345	WEB-MISC Nagios XI anterior a 5.8.6 - Vulnerabilidad de inyección de comandos del sistema operativo mediante un archivo ZIP creado con fines malintencionados (CVE-2021-40345)

Regla de firma	ID de CVE	Descripción
999065	CVE-2021-37928	WEB-MISC Zoho ManageEngine ADManager Plus antes de 7110: vulnerabilidad de carga de archivos sin restricciones (CVE-2021-37928)
999066	CVE-2021-25037	Plug-in de SEO todo en uno de WEB-WORDPRESS anterior a 4.1.5.3 - Vulnerabilidad de inyección SQL a través de objetos API de REST y rest_route
999067	CVE-2021-25037	Plug-in de SEO todo en uno WEB-WORDPRESS anterior a 4.1.5.3 - Vulnerabilidad de inyección SQL a través de objetos API de REST
999068	CVE-2021-25036	Plug-in de SEO todo en uno de WEB-WORDPRESS anterior a 4.1.5.3 - Vulnerabilidad de escalada de privilegios a través de la API de REST y rest_route
999069	CVE-2021-25036	Plug-in de SEO todo en uno de WEB-WORDPRESS anterior a 4.1.5.3: vulnerabilidad de escalada de privilegios a través de la API de REST
999070	CVE-2021-21917	WEB-MISC Advantech R-SeeNet anterior a 2.4.17: Vulnerabilidad de inyección SQL a través de ord (CVE-2021-21917)

Regla de firma	ID de CVE	Descripción
999071	CVE-2021-20040	WEB-MISC SonicWALL Secure Mobile Access: vulnerabilidad de escritura arbitraria de archivos (CVE-2021-20040)
999072	CVE-2021-20039	WEB-MISC SonicWALL Secure Mobile Access: vulnerabilidad de inyección de comandos (CVE-2021-20039)

Actualización de firmas para febrero de 2022

February 19, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la semana 2022-02-20. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

La versión de firma 76 se aplica a las plataformas NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1 y Citrix ADC 13.0.

> **Nota: La**
>
> habilitación de las reglas de firma de cuerpo posterior y cuerpo de respuesta puede afectar a la CPU de Citrix ADC.

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999047	CVE-2022-23863	WEB-MISC FusionPBX anterior a 4.5.30 - Inyección de comandos del SO a través de fax_page_size (CVE-2021-43406)

Regla de firma	ID de CVE	Descripción
999048	CVE-2021-44515	WEB-MISC JetBrains TeamCity: Vulnerabilidad de ejecución remota de código mediante inserción de agente (CVE-2021-43193)
999049	CVE-2021-43406	WEB-MISC GoAhead anterior a 5.1.5: Vulnerabilidad de inyección de variables de entorno CGI (CVE-2021-42342)
999050	CVE-2021-43193	WEB-MISC SonicWALL Secure Mobile Access: Vulnerabilidad de ejecución remota de código (CVE-2021-20045)
999051	CVE-2021-42342	WEB-MISC GoAhead anterior a 5.1.5: Vulnerabilidad de inyección de variables de entorno CGI (CVE-2021-42342)
999052	CVE-2021-20045	WEB-MISC SonicWALL Secure Mobile Access: Vulnerabilidad de ejecución remota de código (CVE-2021-20045)
999053	CVE-2021-20044	WEB-MISC SonicWALL Secure Mobile Access: Vulnerabilidad de inyección de comandos (CVE-2021-20044)
999054		WEB-WORDPRESS AdSanity Plugin: Vulnerabilidad de ejecución remota de código a través de la carga de archivos HTML5

Actualización de firmas para febrero de 2022

March 9, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la semana 2022-02-25. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

Firma versión 77 aplicable a las plataformas NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0 y Citrix ADC 13.1.

> **Nota: La**
>
> habilitación de las reglas de firma de cuerpo posterior y cuerpo de respuesta puede afectar a la CPU de Citrix ADC.

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999034		WEB-WORDPRESS WordPress 5.9 - Vulnerabilidad XSS almacenada a través de un extracto de página en un objeto Json
999035		WEB-WORDPRESS WordPress 5.9 - Vulnerabilidad XSS almacenada a través de extracto de página en formulario
999036		WEB-WORDPRESS WordPress 5.9 - Vulnerabilidad XSS almacenada a través de post.php
999037		WEB-WORDPRESS WordPress 5.9 - Vulnerabilidad XSS almacenada a través de un extracto de publicación en un objeto Json

Regla de firma	ID de CVE	Descripción
999038		WEB-WORDPRESS WordPress 5.9 - Vulnerabilidad XSS almacenada a través de un extracto de publicación en formulario
999039		Vulnerabilidad de recorrido de ruta WEB-MISC a través de valores de
999040		Vulnerabilidad de recorrido de ruta WEB-MISC mediante URI
999041	CVE-2022-23221	Consola WEB-MISC H2 anterior a 2.1.210: Vulnerabilidad de ejecución remota de código a través de test.do (CVE-2022-23221)
999042	CVE-2022-23221	Consola WEB-MISC H2 anterior a 2.1.210: Vulnerabilidad de ejecución remota de código a través de login.do (CVE-2022-23221)
999043	CVE-2022-21662	WEB-WORDPRESS WordPress anterior a 5.8.3 - Vulnerabilidad de scripts de sitios almacenados (CVE-2022-21662)
999044	CVE-2022-0320	WEB-WORDPRESS Los complementos esenciales para el complemento Elementor antes de 5.0.5 - LFI a través de eael_product_gallery (CVE-2022-0320)

Regla de firma	ID de CVE	Descripción
999045	CVE-2022-0320	WEB-WORDPRESS Los complementos esenciales para el complemento Elementor antes de 5.0.5 - LFI a través de woo_product_pagination_product (CVE-2022-0320)
999046	CVE-2022-0320	WEB-WORDPRESS Los complementos esenciales para el complemento Elementor antes de 5.0.5 - LFI a través de load_more (CVE-2022-0320)

Actualización de firma para marzo de 2022

April 5, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la semana 2022-03-29. Puede descargar y configurar estas reglas de firma para proteger su dispositivo de ataques vulnerables a la seguridad.

Versión de firma

Firma versión 78 aplicable a las plataformas NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0 y Citrix ADC 13.1.

> **Nota: La**
>
> habilitación de las reglas de firma de cuerpo posterior y cuerpo de respuesta puede afectar a la CPU de Citrix ADC.

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999006		WEB-MISC Zabbix Versiones múltiples: vulnerabilidad de ejecución remota de código a través de items.php
999007	CVE-2022-24266	WEB-MISC Cuppa CMS v1.0 - Vulnerabilidad de inyección SQL a través de order_orientation (CVE-2022-24266)
999008	CVE-2022-24266	WEB-MISC Cuppa CMS v1.0 - Vulnerabilidad de inyección SQL a través de order_by (CVE-2022-24266)
999009	CVE-2022-22005	WEB-MISC Microsoft SharePoint - RCE a través de la deserialización de la vulnerabilidad de datos no fiables (CVE-2022-22005)
999010	CVE-2022-21705	WEB-MISC OctoberCMS antes de la compilación 474 y v1.1.10: Vulnerabilidad de ejecución remota de código (CVE-2022-21705)
999011	CVE-2022-0557	WEB-MISC Microweber anterior a 1.2.11: Vulnerabilidad de ejecución remota de código (CVE-2022-0557)
999012	CVE-2022-0513	Complemento de estadísticas WP de WEB-WORDPRESS anterior a 13.1.5 - Vulnerabilidad de inyección SQL ciega (CVE-2022-0513)

Regla de firma	ID de CVE	Descripción
999013	CVE-2022-0332	WEB-MISC Moodle 3.11.0 a 3.11.4: Vulnerabilidad de inyección de SQL de actividad H5P (CVE-2022-0332)
999014	CVE-2021-46088	Versiones múltiples de WEB-MISC Zabbix: vulnerabilidad de ejecución remota de código (CVE-2021-46088)
999015	CVE-2021-43789	WEB-MISC PrestaShop anterior a 1.7.8.2 - Vulnerabilidad de inyección SQL a través de SortOrder (CVE-2021-43789)
999016	CVE-2021-43789	WEB-MISC PrestaShop anterior a 1.7.8.2 - Vulnerabilidad de inyección SQL a través de OrderBy (CVE-2021-43789)
999017	CVE-2021-43408	Complemento de publicación duplicada de WEB-WORDPRESS anterior a 1.1.9: vulnerabilidad de inyección SQL (CVE-2021-43408)
999018	CVE-2021-43319	WEB-MISC Zoho ManageEngine NCM antes de 125488: Vulnerabilidad de inyección de comandos del sistema operativo (CVE-2021-43319)
999019	CVE-2021-41282	WEB-MISC pfSense 2.5.2: Vulnerabilidad de ejecución remota de código (CVE-2021-41282)

Regla de firma	ID de CVE	Descripción
999020	CVE-2021-39115, CVE-2021-43947	WEB-MISC Atlassian Jira Server and Data Center: vulnerabilidad de inyección de plantillas en el lado del servidor (CVE-2021-39115, CVE-2021-43947)
999021	CVE-2021-38452	WEB-MISC Moxa MxView Network Management anterior a 3.2.2 - Vulnerabilidad de recorrido de ruta (CVE-2021-38452)
999022	CVE-2021-37918	WEB-MISC Zoho ManageEngine AdManager Plus anterior a 7111: Vulnerabilidad de recorrido de ruta a través de DomainName (CVE-2021-37918)
999023	CVE-2021-37918	WEB-MISC Zoho ManageEngine AdManager Plus anterior a 7111: vulnerabilidad de recorrido de ruta a través de BM_OperationID (CVE-2021-37918)
999024	CVE-2021-37918	WEB-MISC Zoho ManageEngine AdManager Plus anterior a 7111 - RCE a través de una vulnerabilidad de carga arbitraria de archivos (CVE-2021-37918)
999025	CVE-2021-32649	WEB-MISC OctoberCMS antes de la compilación 473 y v1.1.6: Vulnerabilidad de ejecución remota de código a través de Twig (CVE-2021-32649)

Regla de firma	ID de CVE	Descripción
999026	CVE-2021-32648	WEB-MISC OctoberCMS antes de la compilación 472 y v1.1.5: vulnerabilidad de restablecimiento de contraseña (CVE-2021-32648)
999027	CVE-2021-32099, CVE-2020-26518	WEB-MISC Artica Pandora anterior a 743 - Vulnerabilidad de inyección SQL a través de chart_generator (CVE-2021-32099, CVE-2020-26518)
999028	CVE-2021-32098	WEB-MISC Artica Pandora antes de 743 - Vulnerabilidad de deserialización de Phar a través de progressbubble (CVE-2021-32098)
999029	CVE-2021-32098	WEB-MISC Artica Pandora anterior a 743 - Vulnerabilidad de deserialización de Phar a través de progressbar (CVE-2021-32098)
999030	CVE-2021-30149	WEB-MISC Composer 10.0.36 - Vulnerabilidad de ejecución remota de código (CVE-2021-30149)
999031	CVE-2021-25114	Complemento Pro de membresías pagas de WEB-WORDPRESS anterior a 2.6.7 - Vulnerabilidad de SQLi a través de rest_route y discount_code (CVE-2021-25114)

Regla de firma	ID de CVE	Descripción
999032	CVE-2021-25114	Complemento Pro de membresías pagas de WEB-WORDPRESS anterior a 2.6.7 - Vulnerabilidad de SQLi a través de wp-json y discount_code (CVE-2021-25114)
999033	CVE-2021-21984	WEB-MISC VMware vRealize Business for Cloud 7.x anterior a 7.6.0: vulnerabilidad de ejecución remota de código (CVE-2021-21984)

Actualización de firma para marzo de 2022

April 5, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la semana 2022-03-29. Puede descargar y configurar estas reglas de firma para proteger su dispositivo de ataques vulnerables a la seguridad.

Versión de firma

Firma versión 79 aplicable a las plataformas NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0 y Citrix ADC 13.1.

> **Nota: La**
>
> habilitación de las reglas de firma de cuerpo posterior y cuerpo de respuesta puede afectar a la CPU de Citrix ADC.

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
18959 (regla actualizada)	CVE-2022-22965	WEB-MISC VMware Spring4Shell, SpringSource Spring Framework class.classloader intento de RCE
999005	CVE-2022-22963	Función Spring Cloud WEB-MISC: vulnerabilidad de inyección de código (CVE-2022-22963)

Actualización de la firma para abril de 2022

April 21, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la semana 2022-04-04. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

La versión de firma 80 se aplica a las plataformas NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0 y Citrix ADC 13.1.

> **Nota: La**
>
> habilitación de las reglas de firma de cuerpo posterior y cuerpo de respuesta puede afectar a la CPU de Citrix ADC.

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999004	CVE-2022-22965	WEB-MISC Spring4Shell Spring Core Framework - Vulnerabilidad de RCE (CVE-2022-22965)

Actualización de la firma para abril de 2022

April 21, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la semana 2022-04-08. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

Firma versión 81 aplicable a las plataformas NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0 y Citrix ADC 13.1.

> **Nota**
>
> La activación de las reglas de firma del cuerpo de la publicación y del cuerpo Citrix ADC respuesta puede afectar a la CPU

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
999001	CVE-2022-0479	Complemento de generador de ventanas emergentes WEB-WORDPRESS anterior a 4.1.1 - Vulnerabilidad de inyección SQL (CVE-2022-0479)

Regla de firma	ID de CVE	Descripción
999002	CVE-2021-36393	WEB-MISC Moodle anterior a 3.11.1: Vulnerabilidad de inyección SQL (CVE-2021-36393)
999003	CVE-2021-26599	WEB-MISC ImpressCMS anterior a 1.4.3: Vulnerabilidad de inyección de SQL (CVE-2021-26599)

Actualización de la firma para abril de 2022

May 8, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la semana 2022-04-23. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

La versión de firma 82 se aplica a las plataformas NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0 y Citrix ADC 13.1.

> **Nota La**
>
> habilitación de las reglas de firma del cuerpo de la publicación y del cuerpo de respuesta puede afectar Citrix ADC la CPU de

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
998997	CVE-2022-27924	WEB-MISC Zimbra Collaboration Joule: vulnerabilidad de envenenamiento de caché (CVE-2022-27924)

Regla de firma	ID de CVE	Descripción
998998	CVE-2022-21907	Pila de protocolos HTTP de Microsoft WEB-MISC: vulnerabilidad de ejecución remota de código (CVE-2022-21907)
998999	CVE-2021-37930	WEB-MISC ManageEngine AdManager Plus anterior a 7111: Vulnerabilidad de carga arbitraria de archivos a través de SM_DomainName (CVE-2021-37930)
999000	CVE-2021-37930	WEB-MISC ManageEngine AdManager Plus anterior a 7111: Vulnerabilidad de carga arbitraria de archivos a través de SM_OperationID (CVE-2021-37930)

Actualización de firmas para mayo de 2022

June 2, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la semana 2022-05-04. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

Firma versión 83 aplicable a las plataformas NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0 y Citrix ADC 13.1.

> **Nota**
>
> La activación de las reglas de firma del cuerpo de la publicación y del cuerpo Citrix ADC respuesta puede afectar a la CPU

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
998993	CVE-2022-29464	WEB-MISC WSO2 Productos múltiples: Vulnerabilidad de carga de archivos sin restricciones (CVE-2022-29464)
998994	CVE-2022-22954	WEB-MISC VMware Workspace ONE Access and Identity Manager: Vulnerabilidad de ejecución remota de código a través de deviceType (CVE-2022-22954)
998995	CVE-2022-22954	WEB-MISC VMware Workspace ONE Access and Identity Manager: Vulnerabilidad de ejecución remota de código a través de deviceUdid (CVE-2022-22954)
998996	CVE-2022-1329	WEB-WORDPRESS WordPress Elementor Website Builder anterior a 3.6.3: Vulnerabilidad de acción AJAX no autorizada (CVE-2022-1329)

Actualización de firmas para mayo de 2022

June 2, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la semana 2022-05-08. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

Firma versión 84 aplicable a las plataformas NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0 y Citrix ADC 13.1.

> **Nota**
>
> La activación de las reglas de firma del cuerpo de la publicación y del cuerpo Citrix ADC respuesta puede afectar a la CPU

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
998988	CVE-2022-26986	WEB-MISC ImpressCMS anterior a 1.4.3: Vulnerabilidad de inyección SQL a través de mimetypeid (CVE-2022-26986)
998989	CVE-2022-24112	WEB-MISC Complemento batch-requests de Apache APISIX: Vulnerabilidad de omisión de restricción de IP (CVE-2022-24112)
998990	CVE-2021-37558	WEB-MISC Centreon anterior a 20.04.14, 20.10.8 y 21.04.2: Vulnerabilidad de inyección SQL a través de service_description (CVE-2021-37558)
998991	CVE-2021-37558	WEB-MISC Centreon anterior a 20.04.14, 20.10.8 y 21.04.2: Vulnerabilidad de inyección SQL a través de host_name (CVE-2021-37558)

Regla de firma	ID de CVE	Descripción
998992	CVE-2021-22056	WEB-MISC VMware Workspace ONE Access and Identity Manager: Vulnerabilidad de falsificación de solicitudes del lado del servidor (CVE-2021-22056)

Actualización de firmas para mayo de 2022

June 2, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la semana 2022-05-13. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

La versión de firma 85 se aplica a las plataformas NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0 y Citrix ADC 13.1.

> **Nota**
>
> La activación de las reglas de firma del cuerpo de la publicación y del cuerpo Citrix ADC respuesta puede afectar a la CPU

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
998982	CVE-2022-26352	Web-MISC dotCMS: Vulnerabilidad de carga arbitraria de archivos a través de PUT (CVE-2022-26352)

Regla de firma	ID de CVE	Descripción
998983	CVE-2022-26352	WEB-MISC dotCMS: Vulnerabilidad de carga arbitraria de archivos a través de POST (CVE-2022-26352)
998984	CVE-2022-1388	WEB-MISC F5 BIG-IP: Vulnerabilidad de omisión de autenticación REST de iControl (CVE-2022-1388)
998985	CVE-2022-1162	WEB-MISC Múltiples versiones de Gitlab CE/EE: Vulnerabilidad de credenciales codificadas (CVE-2022-1162)
998986	CVE-2022-0888	WEB-WORDPRESS Complemento Ninja Forms File Uploads anterior a 3.3.1: Vulnerabilidad de carga arbitraria de archivos (CVE-2022-0888)
998987	CVE-2021-35244	WEB-MISC SolarWinds Orion anterior a 2020.2.6 HF3: Vulnerabilidad de carga arbitraria de archivos mediante la acción WriteToFile (CVE-2021-35244)

Actualización de firmas para mayo de 2022

June 2, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la semana 2022-05-20. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

Firma versión 86 aplicable a las plataformas NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0 y Citrix ADC 13.1.

> **Nota**
>
> La activación de las reglas de firma del cuerpo de la publicación y del cuerpo Citrix ADC respuesta puede afectar a la CPU

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
998980	CVE-2022-30525	WEB-MISC Múltiples versiones de Zyxel Firewalls: Vulnerabilidad de inyección de comandos de SO no autenticados en setWanPortSt (CVE-2022-30525)
998981	CVE-2021-25094	WEB-WORDPRESS Plug-in Tatsu Builder anterior a 3.3.12: Vulnerabilidad de ejecución remota de código (CVE-2021-25094)

Actualización de la firma para junio de 2022

June 22, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la semana 2022-06-07. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

Firma versión 87 aplicable a las plataformas NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0 y Citrix ADC 13.1.

> **Nota**
>
> La activación de las reglas de firma del cuerpo de la publicación y del cuerpo Citrix ADC respuesta puede afectar a la CPU

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
998964	CVE-2022-30525	WEB-MISC Múltiples versiones de Zyxel Firewalls: Vulnerabilidad de inyección de comandos de SO no autenticados en setWanPortSt (CVE-2022-30525)
998965	CVE-2022-29108	WEB-MISC Microsoft SharePoint - RCE mediante la deserialización de la vulnerabilidad de datos no fiables (CVE-2022-29108)
998966	CVE-2022-26134	WEB-MISC Atlassian Confluence Multiple Versions - Vulnerabilidad de inyección de OGNL no autenticada (CVE-2022-26134)
998967	CVE-2022-26019	WEB-MISC pfSense CE < 2.6.0 - Vulnerabilidad de ejecución remota de código a través de services_ntpd_gps.php y gpsport (CVE-2022-26019)

Regla de firma	ID de CVE	Descripción
998968	CVE-2022-26019	WEB-MISC pfSense CE < 2.6.0 - Vulnerabilidad de ejecución remota de código a través de services_ntpd.php y gpsport (CVE-2022-26019)
998969	CVE-2022-24288	WEB-MISC Apache Airflow hasta 2.2.3: ejemplo de vulnerabilidad de ejecución remota de código de DAG a través de my_param (CVE-2022-24288)
998970	CVE-2022-24288	WEB-MISC Apache Airflow Up To 2.2.3 - Ejemplo de vulnerabilidad de ejecución remota de código de DAG a través de foo o miff (CVE-2022-24288)
998971	CVE-2022-22978	WEB-MISC Spring Security hasta 5.5.6 y 5.6.3 - Vulnerabilidad de derivación de RegexRequestMatcher a través de alimentación de línea (CVE-2022-22978)
998972	CVE-2022-22978	WEB-MISC Spring Security hasta 5.5.6 y 5.6.3: Vulnerabilidad de derivación de RegexRequestMatcher mediante retorno de carro (CVE-2022-22978)
998973	CVE-2022-22957	WEB-MISC VMware Multiple Products - Vulnerabilidad de ejecución remota de código (CVE-2022-22957)

Regla de firma	ID de CVE	Descripción
998974	CVE-2021-45232	Panel WEB-MISC Apache APISIX anterior a 2.10.1 - Vulnerabilidad de omisión de autenticación mediante exportación (CVE-2021-45232)
998975	CVE-2021-45232	Panel WEB-MISC Apache APISIX anterior a 2.10.1: Vulnerabilidad de omisión de autenticación por importación (CVE-2021-45232)
998976	CVE-2021-41739	WEB-MISC Artica Proxy: vulnerabilidad de inyección de comandos del sistema operativo a través de cyrus.events.php (CVE-2021-41739)
998977	CVE-2021-37927	WEB-MISC ManageEngine AdManager Plus anterior a 7111: Vulnerabilidad de omisión de autenticación (CVE-2021-37927)
998978	CVE-2021-36356	WEB-MISC Kramer VIA VSM Server - Vulnerabilidad de ejecución remota de código no autenticado en WriteBrowseFilePathAjax (CVE-2021-36356)
998979	CVE-2021-25094	WEB-WORDPRESS Plug-in Tatsu Builder anterior a 3.3.12: Vulnerabilidad de ejecución remota de código (CVE-2021-25094)

Actualización de la firma para junio de 2022

July 8, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la semana del 2022-06-16. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

Firma, versión 88, aplicable a las plataformas NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0 y Citrix ADC 13.1.

> **Nota**
>
> La activación de las reglas de firma del cuerpo de la publicación y del cuerpo Citrix ADC respuesta puede afectar a la CPU

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
998958	CVE-2022-28810	WEB-MISC Zoho ManageEngine ADSelfService antes de 6122: Vulnerabilidad de inyección de comandos del sistema operativo a través del script UNLOCK (CVE-2022-28810)
998959	CVE-2022-28810	WEB-MISC Zoho ManageEngine ADSelfService antes de 6122: Vulnerabilidad de inyección de comandos del sistema operativo a través del script RESET (CVE-2022-28810)

Regla de firma	ID de CVE	Descripción
998960	CVE-2022-25237	WEB-MISC Bonita Web antes de 7.14.0: Vulnerabilidad de omisión de autorización a través de i18ntranslation/../(CVE-2022-25237)
998961	CVE-2022-25237	WEB-MISC Bonita Web antes de 7.14.0: Vulnerabilidad de omisión de autorización a través de; i18ntranslation (CVE-2022-25237)
998962	CVE-2022-0540	WEB-MISC Atlassian Jira Server and Data Center: Vulnerabilidad de omisión de autenticación de Jira Seraph (CVE-2022-0540)
998963	CVE-2021-44548	WEB-MISC Apache Solr antes de 8.11.1: Vulnerabilidad de ataques de SMB de DataImportHandler (CVE-2021-44548)

Actualización de la firma para julio de 2022

July 15, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la semana del 2022-07-08. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

Firma, versión 89, aplicable a las plataformas NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0 y Citrix ADC 13.1.

> **Nota**
>
> La activación de las reglas de firma del cuerpo de la publicación y del cuerpo Citrix ADC respuesta puede afectar a la CPU

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
998942	CVE-2022-32532	WEB-MISC Apache Shiro antes de 1.9.1: Vulnerabilidad de omisión de RegexRequestMatcher a través del avance de línea (CVE-2022-32532)
998943	CVE-2022-32532	WEB-MISC Apache Shiro antes de 1.9.1: Vulnerabilidad de omisión de RegexRequestMatcher a través del retorno de carro (CVE-2022-32532)
998944	CVE-2022-30157	WEB-MISC Microsoft SharePoint: RCE a través de la deserialización de la vulnerabilidad de datos no fiables (CVE-2022-30157)
998945	CVE-2022-29847	WEB-MISC In Progress Ipswitch WhatsUp Gold: Vulnerabilidad de falsificación de solicitudes no autenticadas del lado del servidor (CVE-2022-29847)
998946	CVE-2022-29535	WEB-MISC Zoho ManageEngine OpManager Varias versiones: Vulnerabilidad de inyección de SQL a través de bview (CVE-2022-29535)

Regla de firma	ID de CVE	Descripción
998947	CVE-2022-29535	WEB-MISC Zoho ManageEngine OpManager Varias versiones: Vulnerabilidad de inyección de SQL a través de la categoría (CVE-2022-29535)
998948	CVE-2022-28219	WEB-MISC Zoho ManageEngine ADAudit Plus antes de 7060: Vulnerabilidad de ejecución remota de código (CVE-2022-28219)
998949	CVE-2022-28219	WEB-MISC Zoho ManageEngine ADAudit Plus antes de 7060: Vulnerabilidad de inyección de XXE a través del nuevo contenido de la tarea (CVE-2022-28219)
998950	CVE-2022-28219	WEB-MISC Zoho ManageEngine ADAudit Plus antes de 7060: Vulnerabilidad de inyección de XXE a través del contenido de la tarea (CVE-2022-28219)
998951	CVE-2022-23642	WEB-MISC Sourcegraph anterior a 3.37: Vulnerabilidad de ejecución remota de código del servicio gitserver (CVE-2022-23642)
998952	CVE-2022-23206	WEB-MISC Apache Traffic Control Traffic Ops anteriores a 5.1.6 y 6.1.0: Vulnerabilidad de SSRF (CVE-2022-23206)

Regla de firma	ID de CVE	Descripción
998953	CVE-2022-1609	WEB-WORDPRESS Weblizar School Management Pro Plugin antes de 9.9.7: Vulnerabilidad de ejecución remota de código (CVE-2022-1609)
998954	CVE-2022-1209	WEB-WORDPRESS WordPress Plugin Ultimate Member antes de 2.3.2: Vulnerabilidad de redireccionamiento abierto (CVE-2022-1209)
998955	CVE-2021-46360	WEB-MISC Composr-CMS: Vulnerabilidad de ejecución remota de código (CVE-2021-46360)
998956	CVE-2021-43350	WEB-MISC Apache Traffic Control Traffic Ops anteriores a 5.1.4 y 6.0.1: Vulnerabilidad de inyección LDAP (CVE-2021-43350)
998957	CVE-2017-9248	WEB-MISC Telerik UI para ASP.NET AJAX antes de R2 2017 SP1: Vulnerabilidad de divulgación de clave de cifrado (CVE-2017-9248)

Actualización de la firma para julio de 2022

August 11, 2022

Se generan nuevas reglas de firmas para las vulnerabilidades identificadas en la semana 2022-07-30. Puede descargar y configurar estas reglas de firma para proteger su dispositivo contra ataques vulnerables a la seguridad.

Versión de firma

Firma, versión 90, aplicable a las plataformas NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0 y Citrix ADC 13.1.

> **Nota**
>
> La activación de las reglas de firma del cuerpo de la publicación y del cuerpo Citrix ADC respuesta puede afectar a la CPU

Información sobre Common Vulnerability Entry (CVE)

A continuación se muestra una lista de reglas de firma, ID de CVE y su descripción.

Regla de firma	ID de CVE	Descripción
998929	CVE-2022-34871	WEB-MISC Centreon antes de 21.10.6: Vulnerabilidad por inyección de SQL (CVE-2022-34871)
998930	CVE-2022-29846	WEB-MISC In Progress Ipswitch WhatsUp Gold: Vulnerabilidad de divulgación de información (CVE-2022-29846)
998931	CVE-2022-29845	WEB-MISC In Progress Ipswitch WhatsUp Gold: Vulnerabilidad de recorrido de ruta (CVE-2022-29845)
998932	CVE-2022-28055	WEB-MISC FusionPBX anterior a 5.0.1: Vulnerabilidad de ejecución remota de código (CVE-2022-28055)
998933	CVE-2022-26138	WEB-MISC Preguntas de Atlassian para la aplicación Confluence: Vulnerabilidad de credenciales codificadas a través de la API de REST (CVE-2022-26138)

Regla de firma	ID de CVE	Descripción
998934	CVE-2022-26138	WEB-MISC Preguntas de Atlassian para la aplicación Confluence: Vulnerabilidad de credenciales codificadas mediante el formulario de inicio de sesión (CVE-2022-26138)
998935	CVE-2022-26135	WEB-MISC Centro de datos y servidor de Jira: Vulnerabilidad de falsificación de solicitudes del lado del servidor del plug-in móvil (CVE-2022-26135)
998936	CVE-2022-21445	WEB-MISC Oracle OBIEE ADF Faces: Deserialización de la vulnerabilidad de datos no fiables (CVE-2022-21445)
998937	CVE-2022-2143	WEB-MISC Advantech iView anterior a 5.7.04.6469: Vulnerabilidad de RCE a través del URI de NetworkServlet y fwfilename (CVE-2022-2143)
998938	CVE-2022-2143	WEB-MISC Advantech iView anterior a 5.7.04.6469: Vulnerabilidad de RCE a través del URI CommandServlet y fwfilename (CVE-2022-2143)
998939	CVE-2022-2143	WEB-MISC Advantech iView anterior a 5.7.04.6469: Vulnerabilidad de RCE a través del URI NetworkServlet y backup_filename (CVE-2022-2143)

Regla de firma	ID de CVE	Descripción
998940	CVE-2022-2143	WEB-MISC Advantech iView anterior a 5.7.04.6469: Vulnerabilidad de RCE a través del URI CommandServlet y backup_filename (CVE-2022-2143)
998941	CVE-2022-2099	WEB-WORDPRESS Plug-in de WooCommerce anterior a 6.6.0: Vulnerabilidad de inyección HTML de puerta de enlace de pago (CVE-2022-2099)

Administración de bots

August 20, 2021

A veces, el tráfico web entrante se compone de bots y la mayoría de las organizaciones sufren ataques de bots. Las aplicaciones web y móviles son importantes impulsores de ingresos para las empresas y la mayoría de las empresas están bajo la amenaza de ciberataques avanzados, como los bots.

Un bot es un programa de software que realiza automáticamente ciertas acciones repetidamente a un ritmo mucho más rápido que un humano. Los bots pueden interactuar con páginas web, enviar formularios, ejecutar acciones, escanear textos o descargar contenido. Pueden acceder a vídeos, publicar comentarios y tuitear en plataformas de redes sociales. Algunos bots, conocidos como chatbots, pueden mantener conversaciones básicas con usuarios humanos.

Un bot que realiza un servicio útil, como servicio al cliente, chat automatizado y rastreadores de motores de búsqueda son buenos bots. Al mismo tiempo, un bot que puede raspar o descargar contenido de un sitio web, robar credenciales de usuario, contenido de spam y realizar otros tipos de ciberataques son bots malos.

Con un buen número de robots defectuosos que realizan tareas maliciosas, es esencial administrar el tráfico de bots y proteger sus aplicaciones web de ataques de bot. Mediante la administración de bots de Citrix, puede detectar el tráfico de bots entrante y mitigar los ataques de bots para proteger sus aplicaciones web.La administración de bots de

Citrix ayuda a identificar bots defectuosos y a proteger su dispositivo contra ataques de seguridad avanzados. Detecta bots buenos y malos e identifica si el tráfico entrante es un ataque de bot. Medi-

ante el uso de la administración de bots, puede mitigar los ataques y proteger sus aplicaciones web.

La administración de bots de Citrix ADC proporciona las siguientes ventajas:

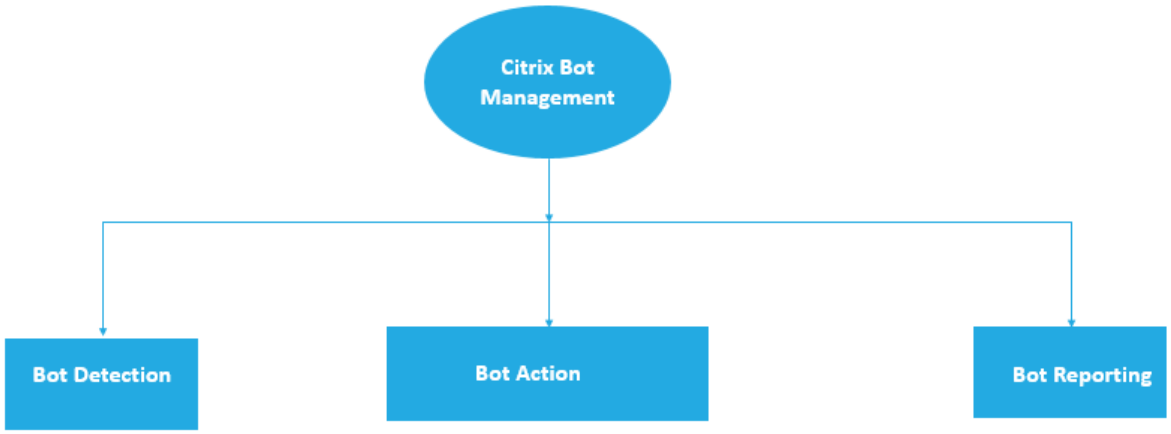
- **Defiende contra bots, scripts y kits de herramientas**. Proporciona mitigación de amenazas en tiempo real mediante defensa basada en firmas estáticas y huellas dactilares de dispositivos.
- **Neutralizar ataques básicos y avanzados automatizados**. Evita ataques, como DDoS de capa de aplicaciones, pulverización de contraseñas, relleno de contraseñas, raspadores de precios y raspadores de contenido.
- **Proteja sus API e inversiones**. Protege sus API del uso indebido injustificado y protege las inversiones en infraestructura del tráfico automatizado.

Algunos casos de uso en los que puede beneficiarse con el sistema de administración de bots de Citrix son:

- Inicio de sesión de fuerza bruta. Un portal web del gobierno está constantemente bajo ataque por bots que intentan forzar los inicios de sesión de usuarios brutos. La organización descubrió el ataque al revisar los registros web y ver a usuarios específicos que se seleccionaban una y otra vez con intentos rápidos de inicio de sesión y contraseñas incrementando mediante un enfoque de ataque de diccionario. Por ley, deben protegerse a sí mismos y a sus usuarios. Al implementar la administración de bots de Citrix, pueden detener el inicio de sesión por fuerza bruta mediante técnicas de identificación digital del dispositivo y limitación de velocidad.
- Bloquear bots malos y robots desconocidos huellas dactilares del dispositivo. Una entidad web recibe 100.000 visitantes cada día. Tienen que mejorar la huella subyacente y están gastando una fortuna. En una auditoría reciente, el equipo descubrió que el 40 por ciento del tráfico provenía de bots, raspando contenido, recogiendo noticias, revisando perfiles de usuario y mucho más. Quieren bloquear este tráfico para proteger a sus usuarios y reducir sus costes de alojamiento. Con la gestión de bots, pueden bloquear los robots malos conocidos, y los robots desconocidos de huellas dactilares que están martillando su sitio. Al bloquear estos bots, pueden reducir el tráfico de bots en un 90 por ciento.

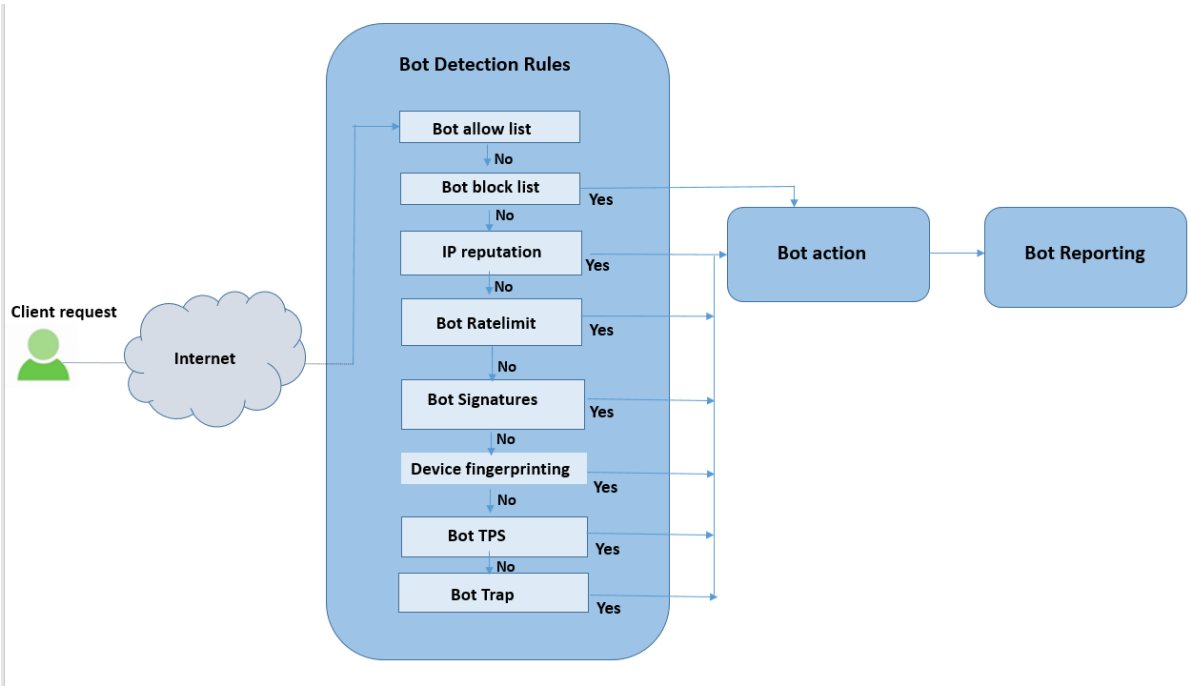
¿Qué hace la administración de bots de Citrix?

La administración de bots de Citrix ayuda a las organizaciones a proteger sus aplicaciones web y sus activos públicos frente a ataques de seguridad avanzados. Cuando un tráfico entrante es un bot, el sistema de administración de bots detecta el tipo de bot, asigna una acción y genera información de bot, como se muestra en el siguiente diagrama.



Cómo funciona la administración de bots de Citrix ADC

El siguiente diagrama muestra cómo funciona la administración de bots de Citrix ADC. El proceso incluye ocho técnicas de detección que ayudan a detectar el tráfico entrante como bot bueno o malo. De forma predeterminada, se permiten los bots correctos detectados por las firmas y se eliminan los bots defectuosos detectados por las firmas.



1. El proceso comienza habilitando la función de administración de bots en el dispositivo.
2. Cuando un cliente envía una solicitud, el dispositivo evalúa el tráfico mediante reglas de directiva bot. Si la solicitud entrante se identifica como un bot, el dispositivo aplica un perfil de detección de bot.
3. Debe vincular el archivo de firma de bot predeterminado o personalizado al perfil de detección

de bot. El archivo de firma bot tiene una lista de reglas de firma bot para identificar el tipo de bot entrante.

4. Las reglas de detección de bots están disponibles en ocho categorías de detección del archivo de firma. Las categorías son lista de permitidos, lista de bloqueo, firma estática, reputación IP, huella digital del dispositivo y limitación de velocidad. En función del tráfico bot, el sistema aplica una regla de detección al tráfico.
5. Si el tráfico de bot entrante coincide con una entrada en la lista de permisos de bot, el sistema omite otras técnicas de detección y la acción asociada registra los datos.
6. Para técnicas de detección distintas de la lista de permitidos de bots, si una solicitud entrante coincide con una regla configurada, se aplica la acción correspondiente. Las acciones posibles son soltar, redirigir, restablecer, mitigar y registrar. CAPTCHA es una acción de mitigación compatible con la reputación IP, las huellas dactilares de los dispositivos y las técnicas de detección de TPS.

Detección de bot

April 21, 2022

El sistema de administración de bots Citrix ADC utiliza seis técnicas diferentes para detectar el tráfico de bots entrante. Las técnicas se utilizan como reglas de detección para detectar el tipo de bot. Las técnicas son lista de permitidos de bots, lista de bloqueo de bots, reputación de IP, huellas digitales de dispositivos, limitación de velocidad, captura de bots, TPS y CAPTCHA.

> **Nota:**
>
> La administración de bots admite un máximo de 32 entidades de configuración para las técnicas de lista de bloqueo, lista de permitidos y limitación de velocidad.

Lista de permitidos de bots. Una lista personalizada de direcciones IP (IPv4 e IPv6), subredes (IPv4 e IPv6) y expresiones de directivas que se pueden omitir como lista permitida.

Lista de prohibidos de robots. Una lista personalizada de direcciones IP (IPv4 e IPv6), subredes (IPv4 e IPv6) y expresiones de directivas a las que se debe bloquear el acceso a las aplicaciones web.

Reputación IP. Esta regla detecta si el tráfico de bot entrante proviene de una dirección IP maliciosa.

Huella digital del dispositivo. Esta regla detecta si el tráfico de bot entrante tiene el ID de huella digital del dispositivo en el encabezado de solicitud entrante y en los atributos del explorador de un tráfico de bot cliente entrante.

> **Limitación:**
>
> 1. JavaScript debe estar habilitado en el explorador del cliente.

2. No funciona para las respuestas XML.

Expresión de registro de bot. La técnica de detección permite capturar información adicional como mensajes de registro. Los datos pueden ser el nombre del usuario que solicitó la URL, la dirección IP de origen y el puerto de origen desde el que el usuario envió la solicitud o los datos generados a partir de una expresión.

Límite de tasa. Esta tasa de regla limita varias solicitudes procedentes del mismo cliente.

Trampa para bots. Detecta y bloquea los bots automatizados anunciando una URL de captura en la respuesta del cliente. La URL parece invisible y no se puede acceder a ella si el cliente es un usuario humano. La técnica de detección es eficaz para bloquear los ataques de bots automatizados.

TPS. Detecta el tráfico entrante como bots si el número máximo de solicitudes y el porcentaje de aumento de solicitudes exceden el intervalo de tiempo configurado.

CAPTCHA. Esta regla utiliza un CAPTCHA para mitigar los ataques de bots. Un CAPTCHA es una validación de respuesta al desafío para determinar si el tráfico entrante proviene de un usuario humano o de un bot automatizado. La validación ayuda a bloquear los bots automatizados que causan infracciones de seguridad en las aplicaciones web. Puede configurar CAPTCHA como acción bot en las técnicas de reputación IP y detección de huellas dactilares del dispositivo.

Ahora, veamos cómo puede configurar cada técnica para detectar y administrar el tráfico de su bot.

Cómo actualizar el dispositivo a la configuración de administración de bots basada en CLI de Citrix ADC

Si va a actualizar el dispositivo desde una versión anterior (versión 13.0 de Citrix ADC versión 58.32 o anterior), primero debe convertir manualmente la configuración de administración de bots existente a la configuración de administración de bots basada en la CLI de Citrix ADC una sola vez. Complete los siguientes pasos para convertir manualmente la configuración de administración de bots.

1. Después de actualizar a la última versión, conéctese a la herramienta de actualización “upgrade_bot_config.py” mediante el siguiente comando

   En el símbolo del sistema, escriba:

   ```
   shell ”/var/python/bin/python /netscaler/upgrade_bot_config.py > /var/bot_upgrade_commands.txt”
   ```

2. Ejecute la configuración mediante el siguiente comando.

   En el símbolo del sistema, escriba:

   ```
   batch -f /var/bot_upgrade_commands.txt
   ```

3. Guarda la configuración actualizada.

```
save ns config
```


Configurar la administración de bots basada en CLI de Citrix ADC

La configuración de administración de bots permite vincular una o más técnicas de detección de bots a un perfil de bot específico. Para comenzar el proceso, habilite la función de administración de bots en su dispositivo. Una vez habilitado, importa el archivo de firma del bot en el dispositivo. Después de la importación, debes crear un perfil de bot. A continuación, crea una directiva de bots con el perfil de bot vinculado a él para evaluar el tráfico entrante como bot y vincular la directiva de forma global o a un servidor virtual.

> **Nota:**
>
> Si va a actualizar el dispositivo desde una versión anterior, primero debe convertir manualmente la configuración de administración de bots existente. Para obtener más información, consulte la sección Cómo actualizar a la configuración de administración de bots basada en CLI de Citrix ADC.

Debe realizar los siguientes pasos para configurar la administración de bots basada en Citrix ADC:

1. Habilitar administración de bots
2. Importar firma de bot
3. Agregar perfil de bot
4. Enlazar perfil bot
5. Agregar directiva de bot
6. Directiva de bots de enlace
7. Configurar los ajustes del bot

Habilitar administración de bots

Antes de empezar, asegúrese de que la función Administración de bots esté habilitada en el dispositivo. Si tiene un Citrix ADC o VPX nuevo, debe habilitar la función antes de configurarla. Si va a actualizar un dispositivo Citrix ADC de una versión anterior a la versión actual, debe habilitar la función antes de configurarla. En el símbolo del sistema, escriba:

```
enable ns feature Bot
```

Importar firma de bot

Puede importar el archivo bot de firma predeterminado y vincularlo al perfil del bot. En el símbolo del sistema, escriba:

```
import bot signature [<src>] <name> [-comment <string>] [-overwrite]
```

Donde:
src. Ruta local y nombre del archivo o URL (protocolo, host, ruta de acceso y nombre de archivo) del archivo en el que se va a almacenar el archivo de firma importado. Nota: La importación falla si el

objeto que se va a importar se encuentra en un servidor HTTPS que requiere autenticación de certificado de cliente para acceder. Longitud máxima: 2047
nombre. Nombre que se va a asignar al objeto de archivo de firma del bot en Citrix ADC. Se trata de un argumento obligatorio. Longitud máxima: 31
comentario. Cualquier comentario para conservar la información sobre el objeto de archivo de firma. Longitud máxima: 255.
Sobrescribir. Sobrescribe el archivo existente.
Nota: Utilice la opción `overwrite` para actualizar el contenido del archivo de firma. Alternativamente, utilice el comando `update bot signature <name>` para actualizar el archivo de firma en el dispositivo Citrix ADC

Ejemplo

```
import bot signature http://www.example.com/signature.json signaturefile -
comment commentsforbot -overwrite
```

> **Nota:**
>
> Puede utilizar la opción sobrescribir para actualizar el contenido del archivo de firma. Además, puede utilizar el comando `update bot signature <name>` para actualizar el archivo de firma en el dispositivo Citrix ADC.

Agregar perfil de bot

Un perfil de bot es un conjunto de ajustes de perfil para configurar la administración de bots en el dispositivo. Puede configurar los ajustes para realizar la detección de bots.

En el símbolo del sistema, escriba:

```
add bot profile <name> [-signature <string>] [-errorURL <string>] [-trapURL
 <string>] [-comment <string>] [-whiteList ( ON | OFF )] [-blackList ( ON
 | OFF )] [-rateLimit ( ON | OFF )] [-deviceFingerprint ( ON | OFF )] [-
deviceFingerprintAction ( none | log | drop | redirect | reset | mitigation
 )] [-ipReputation ( ON | OFF )] [-trap ( ON | OFF )] [-trapAction ( none |
 log | drop | redirect | reset )] [-tps ( ON | OFF )]
```

Ejemplo:

```
add bot profile profile1 -signature signature -errorURL http://www.example
.com/error.html -trapURL /trap.html -whitelist ON -blacklist ON -ratelimit
 ON -deviceFingerprint ON -deviceFingerprintAction drop -ipReputation ON -
trap ON
```


Enlazar perfil bot

Después de crear un perfil de bot, debes enlazar el mecanismo de detección de bots al perfil.

En el símbolo del sistema, escriba:

```
bind bot profile <name> ((-blackList [-type ( IPv4 | SUBNET | IPv6 |
IPv6_SUBNET | Expression )] [-enabled ( ON | OFF )] [-value <string>] [-
action ( log | drop | reset )] [-logMessage <string>] [-comment <string
>])| (-whiteList ( IPv4 | SUBNET | IPv6 | IPv6_SUBNET | Expression )] [-
enabled ( ON | OFF )] [-value <string>] [-log ( ON | OFF )] [-logMessage
<string>] [-comment <string>]))| (-rateLimit [-type ( session |SOURCE_IP
| url )] [-enabled ( ON | OFF )] [-url <string>] [-cookieName <string>] [-
rate <positive_integer>] [-timeslice <positive_integer>] [-action ( none |
 log | drop | redirect | reset )] [-logMessage <string>] [-comment <string
>])| (-ipReputation [-category <ipReputationCategory>] [-enabled ( ON |
OFF )] [-action ( none | log | drop | redirect | reset | mitigation )] [-
logMessage <string>] [-comment <string>])| (-captchaResource [-url <string
>] [-enabled ( ON | OFF )] [-waitTime <positive_integer>] [-gracePeriod <
positive_integer>] [-mutePeriod <positive_integer>] [-requestLengthLimit
<positive_integer>] [-retryAttempts <positive_integer>] [-action ( none |
log | drop | redirect | reset )] [-logMessage <string>] [-comment <string
>])| (-tps [-type ( SOURCE_IP | GeoLocation | REQUEST_URL | Host )] [-
threshold <positive_integer>] [-percentage <positive_integer>] [-action (
 none | log | drop | redirect | reset | mitigation )] [-logMessage <string
>] [-comment <string>])
```

Ejemplo:

El siguiente ejemplo sirve para vincular la técnica de detección de reputación IP a un perfil de bot específico.

```
bind bot profile profile5 -ipReputation -category BOTNET -enabled ON -
action drop -logMessage message
```

Agregar directiva de bot

Debe agregar la directiva de bots para evaluar el tráfico de bots.

En el símbolo del sistema, escriba:

```
add bot policy <name> -rule <expression> -profileName <string> [-undefAction
 <string>] [-comment <string>] [-logAction <string>]
```

Donde:

Nombre. Nombre de la directiva de bots. Debe comenzar con una letra, un número o un carácter de guión bajo (_) y debe contener solo letras, números y guión (-), punto (.), almohadilla (#), espacio ( ), en (@), igual a (=), dos puntos (:) y guión bajo. Se puede cambiar después de agregar la directiva de bots.

Regla. Expresión que utiliza la directiva para determinar si se aplica el perfil de bot en la solicitud especificada. Se trata de un argumento obligatorio. Longitud máxima: 1499

profileName. Nombre del perfil del bot que se va a aplicar si la solicitud coincide con esta directiva de bots. Se trata de un argumento obligatorio. Longitud máxima: 127

undefAction. Acción a realizar si el resultado de la evaluación de directivas no está definido (UNDEF). Un evento UNDEF indica una condición de error interno. Longitud máxima: 127

Comentario. Cualquier tipo de información sobre esta directiva de bots. Longitud máxima: 255

logAction. Nombre de la acción de registro que se va a utilizar para las solicitudes que coinciden con esta directiva. Longitud máxima: 127

Ejemplo:

```
add bot policy pol1 -rule "HTTP.REQ.HEADER(\"header\").CONTAINS(\"custom
\")"- profileName profile1 -undefAction drop -comment commentforbotpolicy -
logAction log1
```

Enlazar directiva de bots global

En el símbolo del sistema, escriba:

```
bind bot global -policyName <string> -priority <positive_integer> [-gotoPriorityExpres
 <expression>][-type ( REQ_OVERRIDE | REQ_DEFAULT )] [-invoke (-labelType (
 vserver | policylabel )-labelName <string>)]
```

Ejemplo:

```
bind bot global -policyName pol1 -priority 100 -gotoPriorityExpression NEXT
-type REQ_OVERRIDE
```

Enlazar la directiva bot a un servidor virtual

En el símbolo del sistema, escriba:

```
bind lb vserver <name>@ ((<serviceName>@ [-weight <positive_integer>] )| <
serviceGroupName>@ | (-policyName <string>@ [-priority <positive_integer>]
 [-gotoPriorityExpression <expression>] [-type ( REQUEST | RESPONSE )] [-
invoke (<labelType> <labelName>)] )| -analyticsProfile <string>@)
```

Ejemplo:


```
bind lb vserver lb-server1 -policyName pol1 -priority 100 -gotoPriorityExpression
 NEXT -type REQ_OVERRIDE
```

Configurar los ajustes del bot

Si es necesario, puede personalizar la configuración predeterminada.
En el símbolo del sistema, escriba:

```
1 set bot settings [-defaultProfile <string>] [-javaScriptName <string>]
      [-sessionTimeout <positive_integer>] [-sessionCookieName <string>]
      [-dfpRequestLimit <positive_integer>] [-signatureAutoUpdate ( ON |
      OFF )] [-signatureUrl <URL>] [-proxyServer <ip_addr|ipv6_addr|\*>]
      [-proxyPort <port|\*>]
2 <!--NeedCopy-->
```

Donde:

defaultProfile. Perfil que se va a utilizar cuando una conexión no coincide con ninguna directiva. La configuración predeterminada es “, que devuelve las conexiones sin coincidencias al Citrix ADC sin intentar filtrarlas más. Longitud máxima: 31

javaScriptName. Nombre del JavaScript que utiliza la función BotNet como respuesta. Debe comenzar con una letra o un número y puede constar de 1 a 31 letras, números y los símbolos de guión (-) y guión bajo (_). El siguiente requisito se aplica únicamente a la CLI de Citrix ADC: Si el nombre incluye uno o más espacios, escriba el nombre entre comillas dobles o simples (por ejemplo, “nombre de mi cookie” o “nombre de mi cookie”). Longitud máxima: 31

sessionTimeout. El tiempo de espera de la sesión, en segundos, tras lo cual finaliza una sesión de usuario.

Valor mínimo: 1, Valor máximo: 65535

sessionCookieName. Nombre de la cookie de sesión que utiliza la función BotNet para realizar el seguimiento. Debe comenzar con una letra o un número y puede constar de 1 a 31 letras, números y los símbolos de guión (-) y guión bajo (_). El siguiente requisito se aplica únicamente a la CLI de Citrix ADC: Si el nombre incluye uno o más espacios, escriba el nombre entre comillas dobles o simples (por ejemplo, “nombre de mi cookie” o “nombre de mi cookie”). Longitud máxima: 31

dfpRequestLimit. Número de solicitudes que se permiten sin cookie de sesión de bot si la huella digital del dispositivo está habilitada.

Valor mínimo: 1, Valor máximo: 4294967295

signatureAutoUpdate. Indicador utilizado para habilitar/inhabilitar firmas de actualización automática de bots.

Valores posibles: ON, OFF

Valor por defecto: OFF

signatureUrl. URL para descargar el archivo de asignación de firmas del bot del servidor.

Valor predeterminado: `https://nsbotsignatures.s3.amazonaws.com/BotSignatureMapping.json`.

Longitud máxima: 2047

ProxyServer. IP del servidor proxy para obtener firmas actualizadas de AWS.

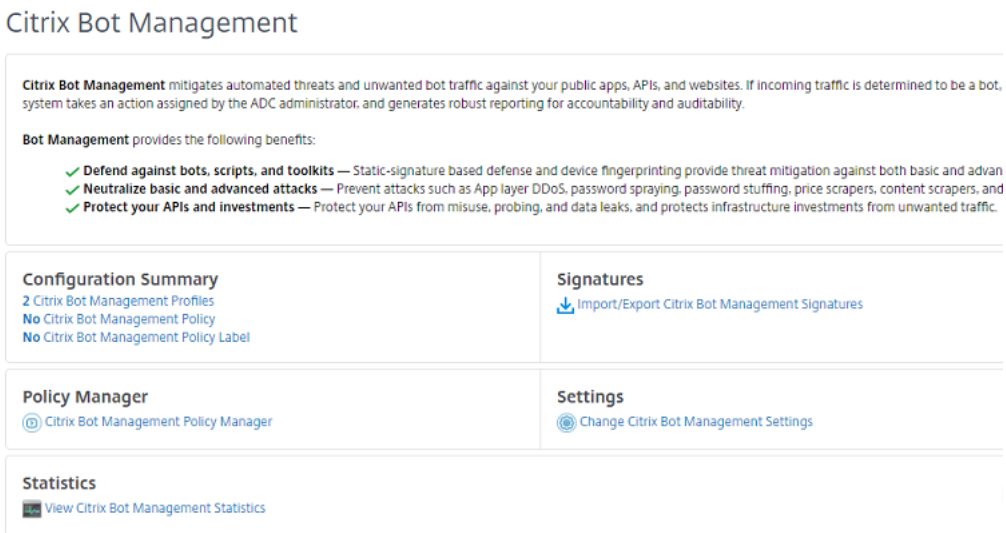
proxyPort. Puerto del servidor proxy para obtener firmas actualizadas de AWS. Valor por defecto: 8080

Ejemplo:

```
set bot settings -defaultProfile profile1 -javaScriptName json.js -sessionTimeout
 1000 -sessionCookieName session
```

Configuración de la administración de bots mediante la GUI de Citrix ADC

Puede configurar la administración de bots de Citrix ADC habilitando primero la función en el dispositivo. Una vez habilitada, puede crear una directiva de bots para evaluar el tráfico entrante como bot y enviar el tráfico al perfil del bot. A continuación, crea un perfil de bot y, a continuación, enlaza el perfil a una firma de bot. Como alternativa, también puede clonar el archivo de firma de bot predeterminado y usar el archivo de firma para configurar las técnicas de detección. Después de crear el archivo de firma, puede importarlo al perfil del bot.



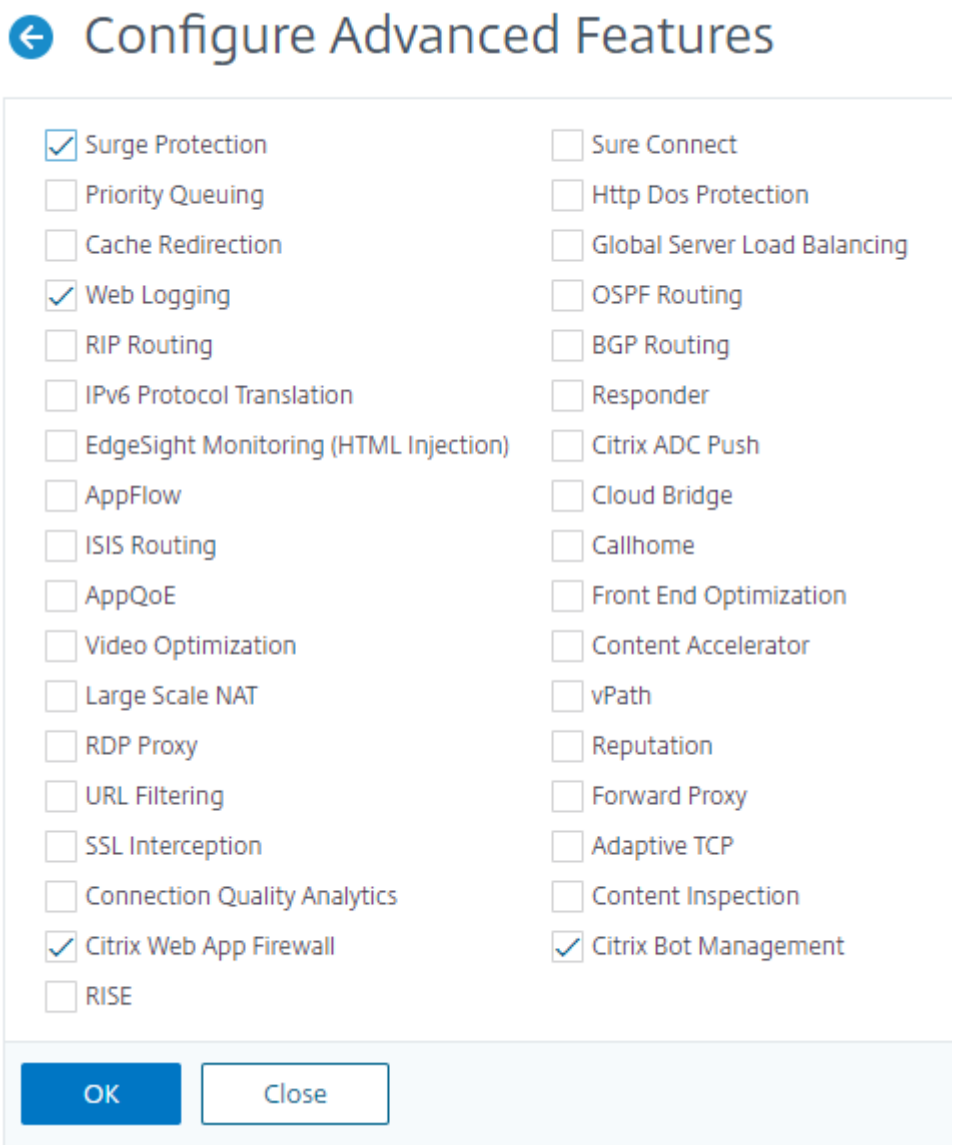
1. Activar función de administración de bots
2. Configurar ajustes de administración de bots
3. Clone la firma predeterminada del bot Citrix

4. Importar firma bot Citrix
5. Configurar los ajustes de firma bot
6. Crear perfil de bot
7. Crear directiva de bots

Activar función de administración de bots

Complete los siguientes pasos para habilitar la administración de bots:

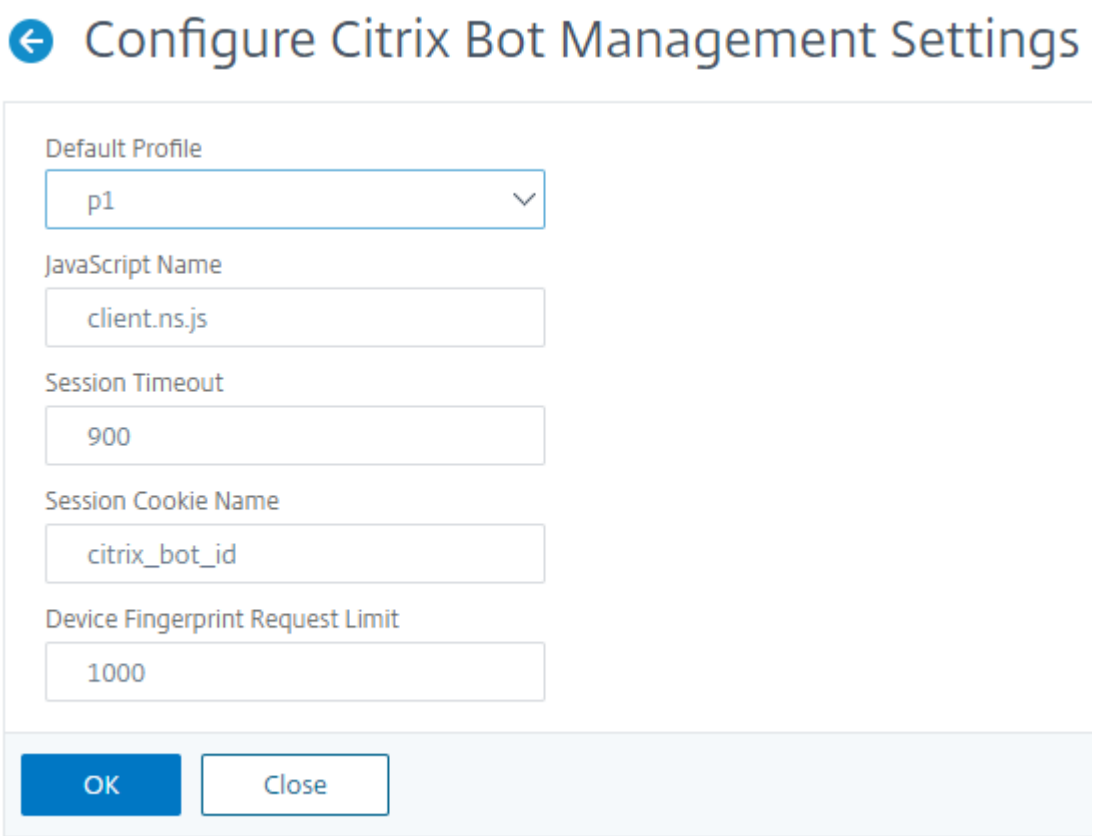
1. En el panel de navegación, expanda **Sistema** y, a continuación, haga clic en **Configuración**.
2. En la página **Configurar funciones avanzadas**, marque la casilla de verificación **Administración de bots**.
3. Haga clic en **Aceptar**y, a continuación, en **Cerrar**.



Configurar los ajustes de administración de bots para la técnica de huella digital

Complete el siguiente paso para configurar la técnica de huellas dactilares del dispositivo:

1. Vaya a **Seguridad** > **Administración de bots de Citrix**.
2. En el panel de detalles, en **Configuración**, haga clic en **Cambiar configuración de administración de bots de Citrix**.
3. En **Configurar opciones de administración de bots de Citrix**, defina los siguientes parámetros.
   a) Perfil predeterminado. Seleccione un perfil de bot.
   b) Nombre JavaScript. Nombre del archivo JavaScript que utiliza la administración de bots en su respuesta al cliente.
   c) Tiempo de espera de sesión. Tiempo de espera en segundos tras el cual finaliza la sesión del usuario.
   d) Cookie de sesión. Nombre de la cookie de sesión que utiliza el sistema de gestión de bots para realizar el seguimiento.
   e) Límite de solicitud de huellas digitales del dispositivo. Número de solicitudes que se permiten sin una cookie de sesión de bot, si la huella digital del dispositivo está habilitada

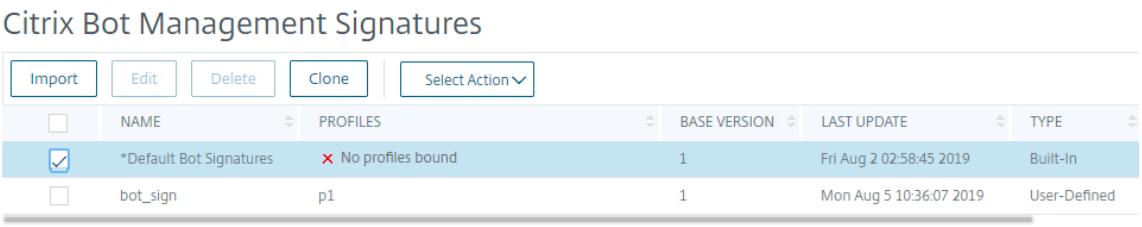


4. Haga clic en **OK**.

Archivo de firma del bot clon

Complete el siguiente paso para clonar el archivo de firma del bot:

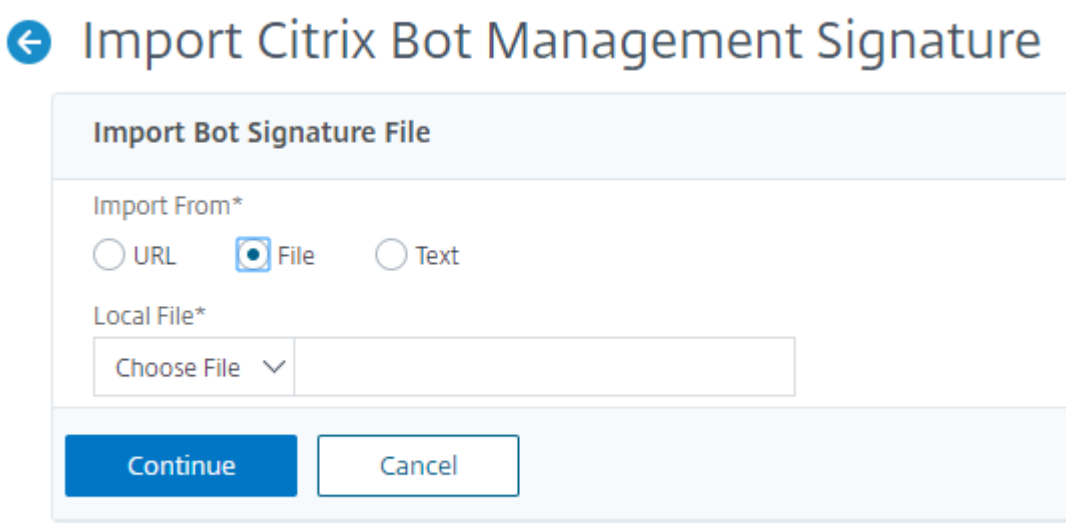
1. Vaya a **Seguridad** > **Administración de bots de Citrix** y **Firmas**.
2. En la página **Firmas de Citrix Bot Management**, seleccione el registro de firmas de bots predeterminado y haga clic en **Clonar**.
3. En la página **Clone Bot Signature**, introduzca un nombre y modifique los datos de firma.
4. Haga clic en **Crear**.



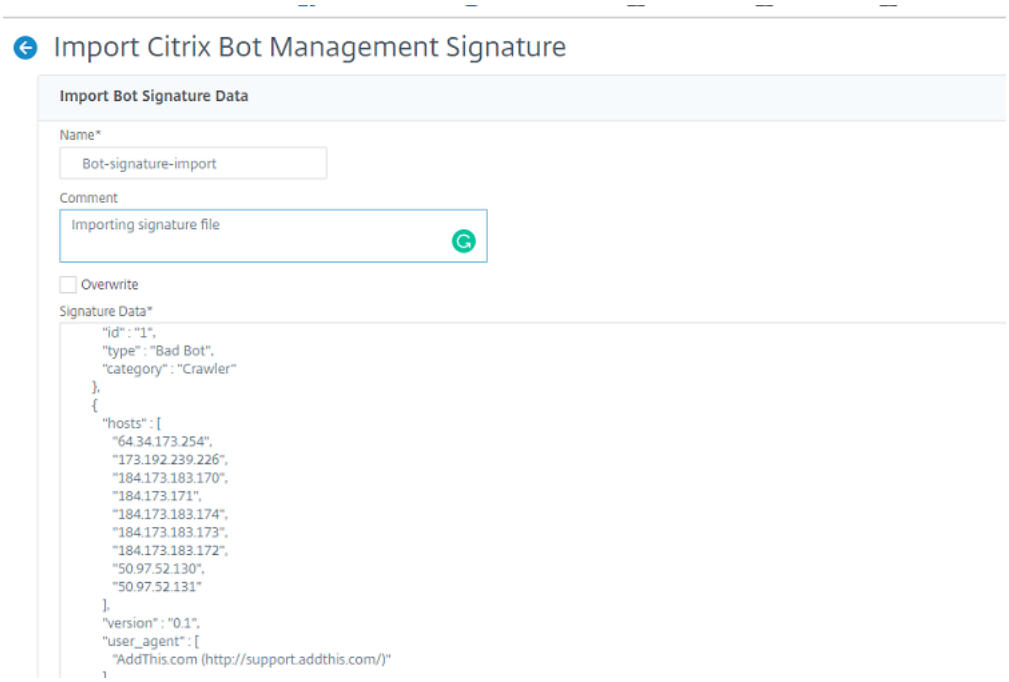
Importar archivo de firma bot

Si tiene su propio archivo de firma, puede importarlo como archivo, texto o URL. Realice los siguientes pasos para importar el archivo de firma del bot:

1. Vaya a **Seguridad** > **Administración de bots de Citrix** y **Firmas**.
2. En la página **Firmas de Citrix Bot Management**, importe el archivo como URL, archivo o texto.
3. Haga clic en **Continue**.



4. En la página Importar firma de Citrix Bot Management, defina los siguientes parámetros.
   a) Nombre. Nombre del archivo de firma del bot.
   b) Comentario. Breve descripción del archivo importado.
   c) Sobrescribir. Marque la casilla para permitir la sobrescritura de datos durante la actualización del archivo.
   d) Datos de firma. Modificar parámetros de firma
5. Haga clic en **Listo**.



Configurar la lista de bots permitidos mediante la GUI de Citrix ADC

Esta técnica de detección le permite omitir las URL que configura en una lista permitida. Complete el siguiente paso para configurar una URL de lista de permitidos:

1. Vaya a **Seguridad** > **Perfiles** y **administración de bots de Citrix**.
2. En la página **Perfiles de administración de bots de Citrix**, seleccione un archivo y haga clic en **Modificar**.
3. En la página **Perfil de administración de bots de Citrix**, vaya a la sección **Configuración de firmas** y haga clic en **Lista de permitidos**.
4. En la sección **Lista de permitidos**, establezca los siguientes parámetros:
   a) Habilitada. Seleccione la casilla de verificación para validar las URL de la lista de permitidos como parte del proceso de detección.

b) Configurar tipos. Configure una URL de lista de permitidos. La URL se omite durante la detección del bot. Haga clic en Agregar para agregar una URL a la lista de bots permitidos.

c) En la página **Configurar enlace de lista de permitidos del perfil de administración de Citrix Bot**, establezca los siguientes parámetros:

i. Tipo. El tipo de URL puede ser una dirección IPv4, una dirección IP de subred o una dirección IP que coincida con una expresión de directiva.

ii. Habilitada. Seleccione la casilla de verificación para validar la URL.

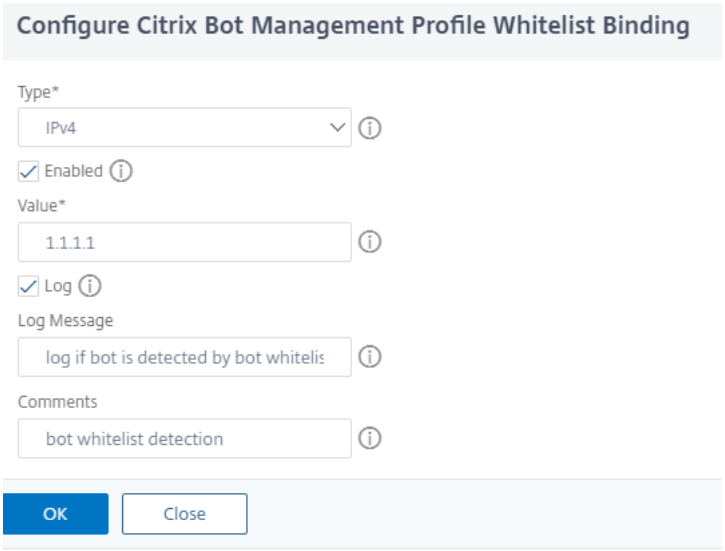
iii. Valor. Dirección URL.

iv. Registro. Seleccione la casilla de verificación para almacenar las entradas de registro.

v. Mensaje de registro. Breve descripción del registro.

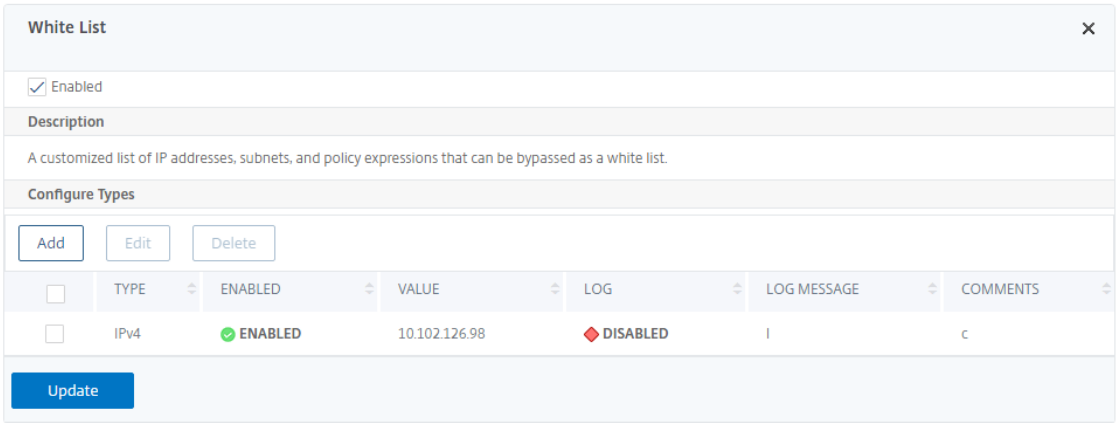
vi. Observaciones. Breve descripción de la URL de la lista de permitidos.

vii. Haga clic en **OK**.



5. Haga clic en **Update**.

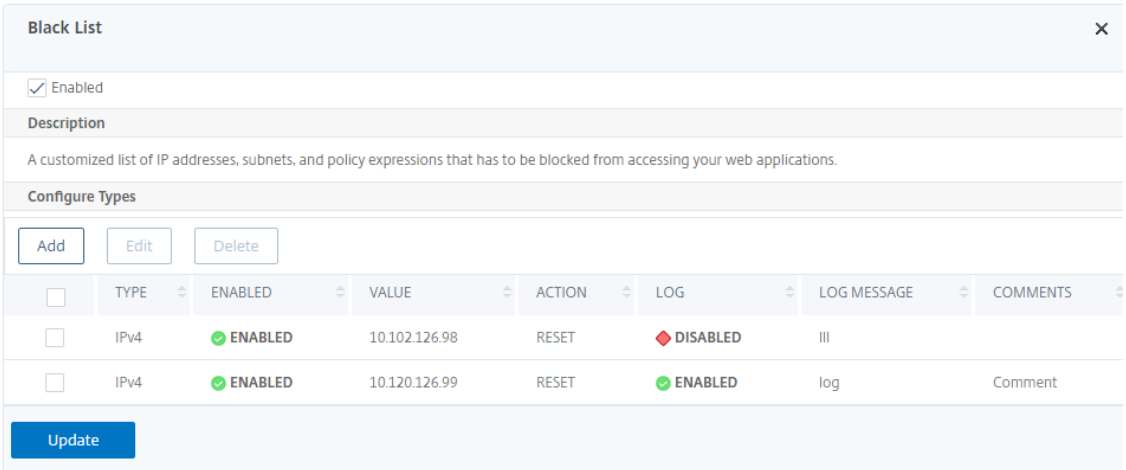
6. Haga clic en **Listo**.



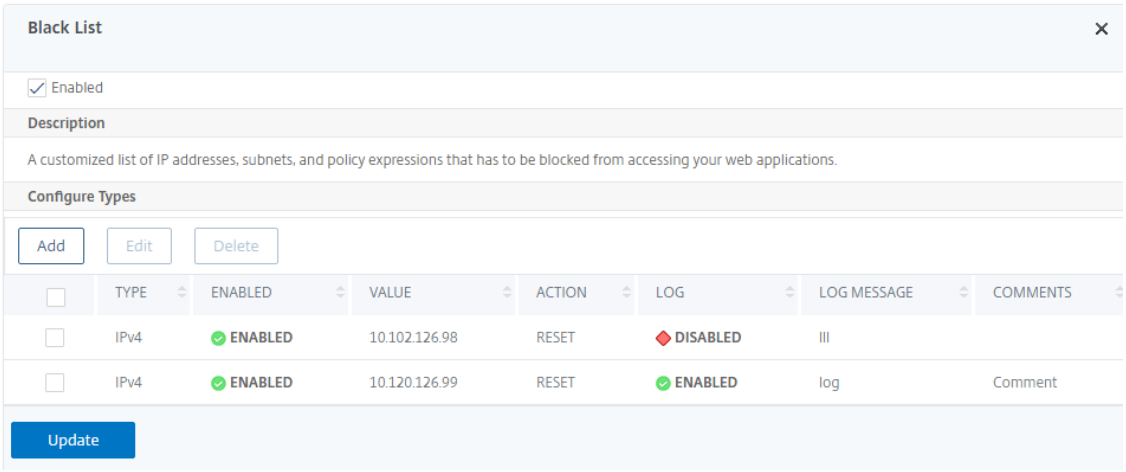
Configurar la lista de bloques de bots mediante la GUI de Citrix ADC

Esta técnica de detección le permite eliminar las URL que configura como una lista de bloqueo. Complete el siguiente paso para configurar una URL de lista de bloqueo.

1. Vaya a **Seguridad** > **Perfiles** y **administración de bots de Citrix**.
2. En la página **Perfiles de administración de bots de Citrix**, seleccione un archivo de firma y haga clic en **Modificar**.
3. En la página **Perfil de administración de bots de Citrix**, vaya a la sección **Configuración de firma** y haga clic en **Lista negra**.
4. En la sección **Lista de prohibidos**, defina los siguientes parámetros:
   a) Habilitada. Active la casilla de verificación para validar las URL de listas bloqueadas como parte del proceso de detección.
   b) Configurar tipos. Configure una URL para que forme parte del proceso de detección de listas de bloqueo de bots. Estas URL se eliminan durante la detección de bots. Haga clic en Agregar para agregar una URL a la lista de bots bloqueados
   c) En la página **Configurar enlace de lista de prohibidos de perfil de administración de Citrix Bot**, establezca los siguientes parámetros.
      i. Tipo. El tipo de URL puede ser una dirección IPv4, una dirección IP de subred o una dirección IP.
      ii. Habilitada. Seleccione la casilla de verificación para validar la URL.
      iii. Valor. Dirección URL.
      iv. Registro. Seleccione la casilla de verificación para almacenar las entradas de registro.
      v. Mensaje de registro. Breve descripción del inicio de sesión.
      vi. Observaciones. Breve descripción de la URL de la lista de bloqueo.
      vii. Haga clic en **OK**.



5. Haga clic en **Update**.
6. Haga clic en **Listo**.



Configurar la reputación de IP mediante la interfaz gráfica de usuario de Citrix ADC

La técnica del bot de reputación IP utiliza la base de datos de reputación IP de Webroot y la base de datos de proveedores de servicios en la nube para verificar si una solicitud de un cliente es una dirección IP maliciosa o una dirección IP de nube pública. Como parte de las categorías de bots se configura y luego se le asocia una acción de bot. Complete los siguientes pasos para configurar la reputación de IP de Webroot y las categorías de base de datos de proveedores de servicios en la nube.

1. Vaya a **Seguridad** > **Perfiles** y **administración de bots de Citrix**.
2. En la página **Perfiles de administración de bots de Citrix**, seleccione un archivo de firma y haga clic en **Modificar**.
3. En la página **Perfil de administración de bots de Citrix**, vaya a la sección **Configuración de firmas** y haga clic en **Reputación de IP**.
4. En la sección **Reputación IP**, defina los siguientes parámetros:
   a) Habilitada. Seleccione la casilla de verificación para validar el tráfico de bot entrante como parte del proceso de detección.
   b) Configurar categorías. Puede utilizar la técnica de reputación de IP para el tráfico de bots entrante en diferentes categorías. Según la categoría configurada, puede eliminar o redirigir el tráfico del bot. Haga clic en **Agregar** para configurar una categoría de bot malintencionado.
   c) En la página **Configurar enlace de reputación IP del perfil de Citrix Bot Management**, defina los siguientes parámetros:

i. Categoría. Seleccione una categoría de bot de reputación IP de Webroot para validar una solicitud de cliente como una dirección IP malintencionada.

   A. IP_BASED: esta categoría comprueba si la dirección IP del cliente (IPv4 e IPv6) es maliciosa o no.
   B. BOTNET: esta categoría incluye canales de Botnet C&C y máquinas zombis infectadas controladas por Bot master.
   C. SPAM_SOURCES: esta categoría incluye la tunelización de mensajes de spam a través de un proxy, las actividades SMTP anómalas y las actividades de spam del foro.
   D. ESCÁNERES: esta categoría incluye todos los reconocimientos, como sondas, escaneo de host, escaneo de dominio y ataque de fuerza bruta de contraseña.
   E. DOS: esta categoría incluye DOS, DDOS, inundación de sincronización anómala y detección de tráfico anómalo.
   F. REPUTACIÓN: esta categoría deniega el acceso desde direcciones IP (IPv4 e IPv6) que actualmente se sabe que están infectadas con malware. Esta categoría también incluye direcciones IP con una puntuación media baja del Índice de Reputación de Webroot. Al habilitar esta categoría se evita el acceso desde las fuentes identificadas a los puntos de distribución de malware de contacto.
   G. PHISHING: Esta categoría incluye las direcciones IP (IPv4 e IPv6) que alojan sitios de phishing y otros tipos de actividades fraudulentas, como el fraude de clics en anuncios o el fraude de juegos.
   H. PROXY: esta categoría incluye las direcciones IP (IPv4 e IPv6) que proporcionan servicios de proxy.
   I. RED: IP que brindan servicios de proxy y anonimización, incluido The Onion Router, también conocido como TOR o dark net.
   J. MOBILE_THREATS: esta categoría comprueba la dirección IP del cliente (IPv4 e IPv6) con la lista de direcciones perjudiciales para los dispositivos móviles.

ii. Categoría. Seleccione una categoría de proveedor de servicios de nube pública de Webroot para validar que la solicitud de un cliente es una dirección IP de nube pública.

   A. AWS: esta categoría comprueba la dirección IP del cliente con una lista de direcciones de nube pública de AWS.
   B. GCP: esta categoría comprueba la dirección IP del cliente con una lista de direcciones de nube pública de Google Cloud Platform.
   C. AZURE: esta categoría comprueba la dirección del cliente con una lista de direcciones de nube pública de Azure.
   D. ORACLE: esta categoría comprueba la dirección IP del cliente con una lista de direcciones de nube pública de Oracle
   E. IBM: esta categoría comprueba la dirección IP del cliente con una lista de direcciones de nube pública de IBM.

F. SALESFORCE: esta categoría comprueba la dirección IP del cliente con una lista de direcciones de nube pública de Salesforce.

Valores posibles para la categoría de bot de reputación IP de Webroot: IP, BOTNETS, SPAM_SOURCES, ESCÁNERES, DOS, REPUTACIÓN, PHISHING, PROXY, RED, MOBILE_THREATENS.

Valores posibles para la categoría de proveedor de servicios de nube pública de Webroot: AWS, GCP, AZURE, ORACLE, IBM, SALESFORCE.

iii. Habilitada. Seleccione la casilla de verificación para validar la detección de firmas de reputación IP.

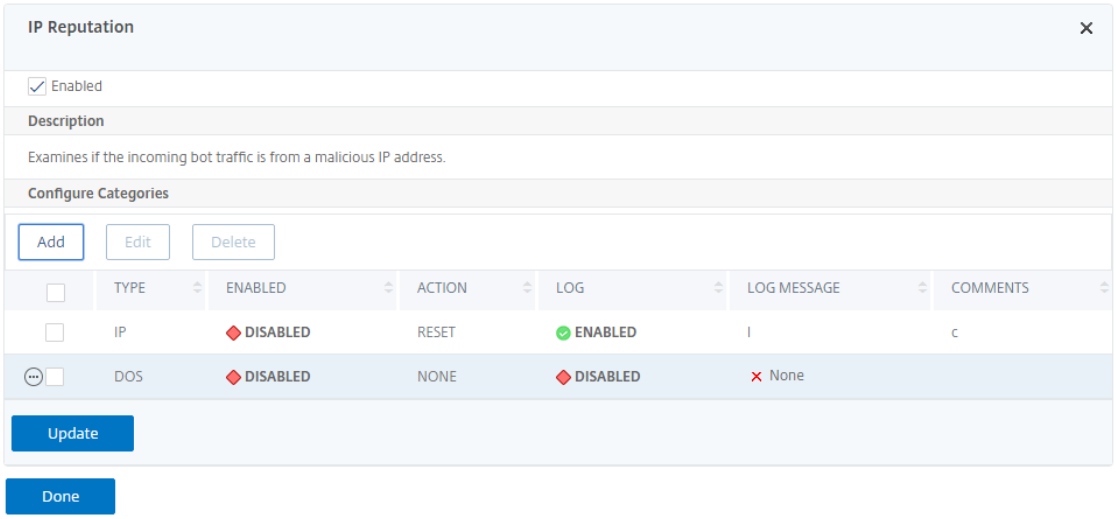
iv. Acción bot. Según la categoría configurada, no puede asignar ninguna acción, rechazo, redirección o acción de mitigación.

v. Registro. Seleccione la casilla de verificación para almacenar las entradas de registro.

vi. Mensaje de registro. Breve descripción del registro.

vii. Observaciones. Breve descripción de la categoría bot.

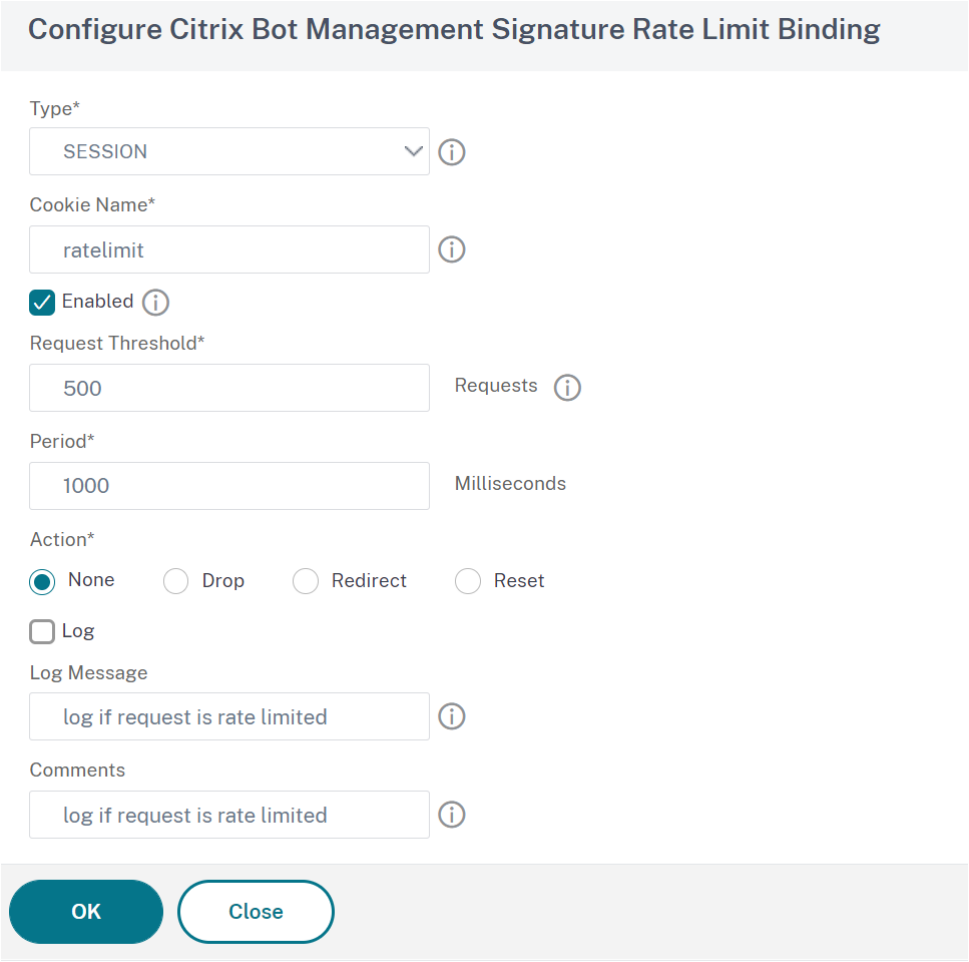
5. Haga clic en **OK**.
6. Haga clic en **Update**.
7. Haga clic en **Listo**.



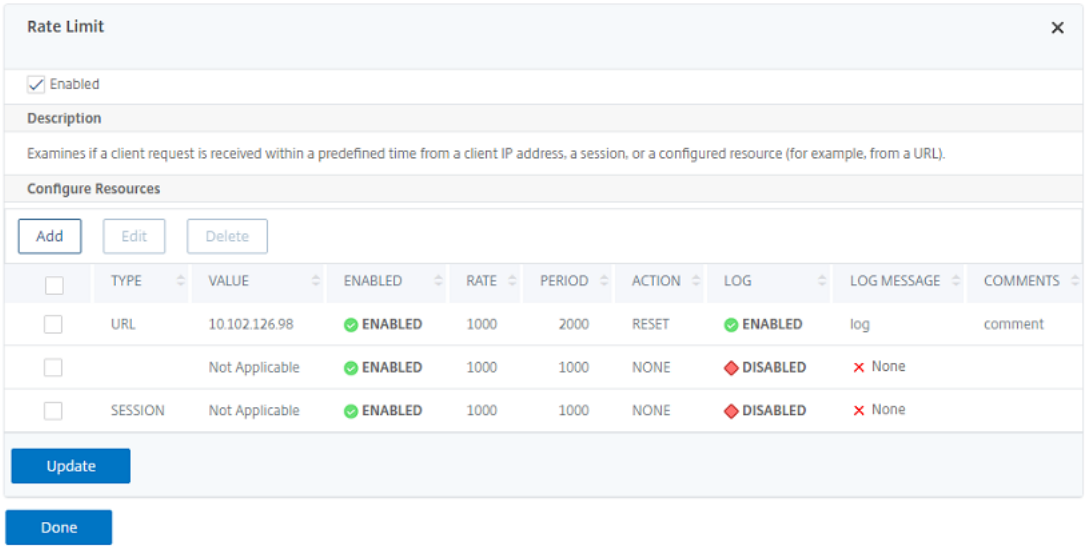
Configurar el límite de velocidad de bots mediante la GUI de Citrix ADC

Esta técnica de detección permite bloquear bots en función del número de solicitudes recibidas en un tiempo predefinido desde la dirección IP de un cliente, una sesión o un recurso configurado (por ejemplo, desde una URL). Complete el siguiente paso para configurar la técnica de límite de velocidad.

1. Vaya a **Seguridad** > **Perfiles** y **administración de bots de Citrix**.
2. En la página **Perfiles de administración de bots de Citrix**, seleccione un archivo de firma y haga clic en **Modificar**.
3. En la página **Perfil de administración de bots de Citrix**, vaya a la sección **Configuración de firmas** y haga clic en **Límite de velocidad**.
4. En la sección **Límite de velocidad**, defina los siguientes parámetros:
    a) Habilitada. Seleccione la casilla de verificación para validar el tráfico de bot entrante como parte del proceso de detección.
    b) Sesión. Solicitudes de límite de velocidad basadas en una sesión. Haga clic en Agregar para configurar las solicitudes de límite de velocidad en función de una sesión.
    c) En la página **Configurar límite de velocidad de firma de Citrix Bot Management**, defina los siguientes parámetros.
        i. Categoría. Seleccione una categoría de bot malicioso de la lista. Asocie una acción basada en la categoría.
        ii. Habilitada. Seleccione la casilla de verificación para validar el tráfico de bot entrante.
        iii. Acción bot. Elige una acción bot para la categoría seleccionada.
        iv. Registro. Seleccione la casilla de verificación para almacenar las entradas de registro.
        v. Mensaje de registro. Breve descripción del registro.
        vi. Observaciones. Breve descripción de la categoría bot.
        vii. Haga clic en **OK**.



5. Haga clic en **Update**.
6. Haga clic en **Listo**.



Configurar la técnica de límite de velocidad de bots basada en la

La técnica de límite de velocidad de bots le permite limitar el tráfico de bots dentro de un plazo determinado en función de la geolocalización del usuario, la dirección IP del cliente, la sesión, la cookie o el recurso configurado (URL).
Al configurar la técnica de límite de velocidad de bots, puede asegurarse de lo siguiente:

- Bloquea la actividad de bots maliciosos.
- Reducir la tensión del tráfico a los servidores web.

En el símbolo del sistema, escriba:

```
bind bot profile <name>... -ratelimit  -type <type> Geolocation -
   countryCode <countryName> -rate  <positive_integer> -timeSlice <
   positive_integer> [-action <action> ...]  [-enabled ( ON | OFF )]
<!--NeedCopy-->
```

Donde:

*SOURCE_IP - Limitación de velocidad en función de la dirección IP del cliente.

*SESSION - Limitación de velocidad en función del nombre de cookie configurado.

*URL - Limitación de velocidad en función de la URL configurada.

*GEOLOCATION- Limitación de velocidad en función del nombre del país configurado.

Possible values: SESIÓN, SOURCE_IP, URL, GEOLOCALIZACIÓN

Ejemplo:

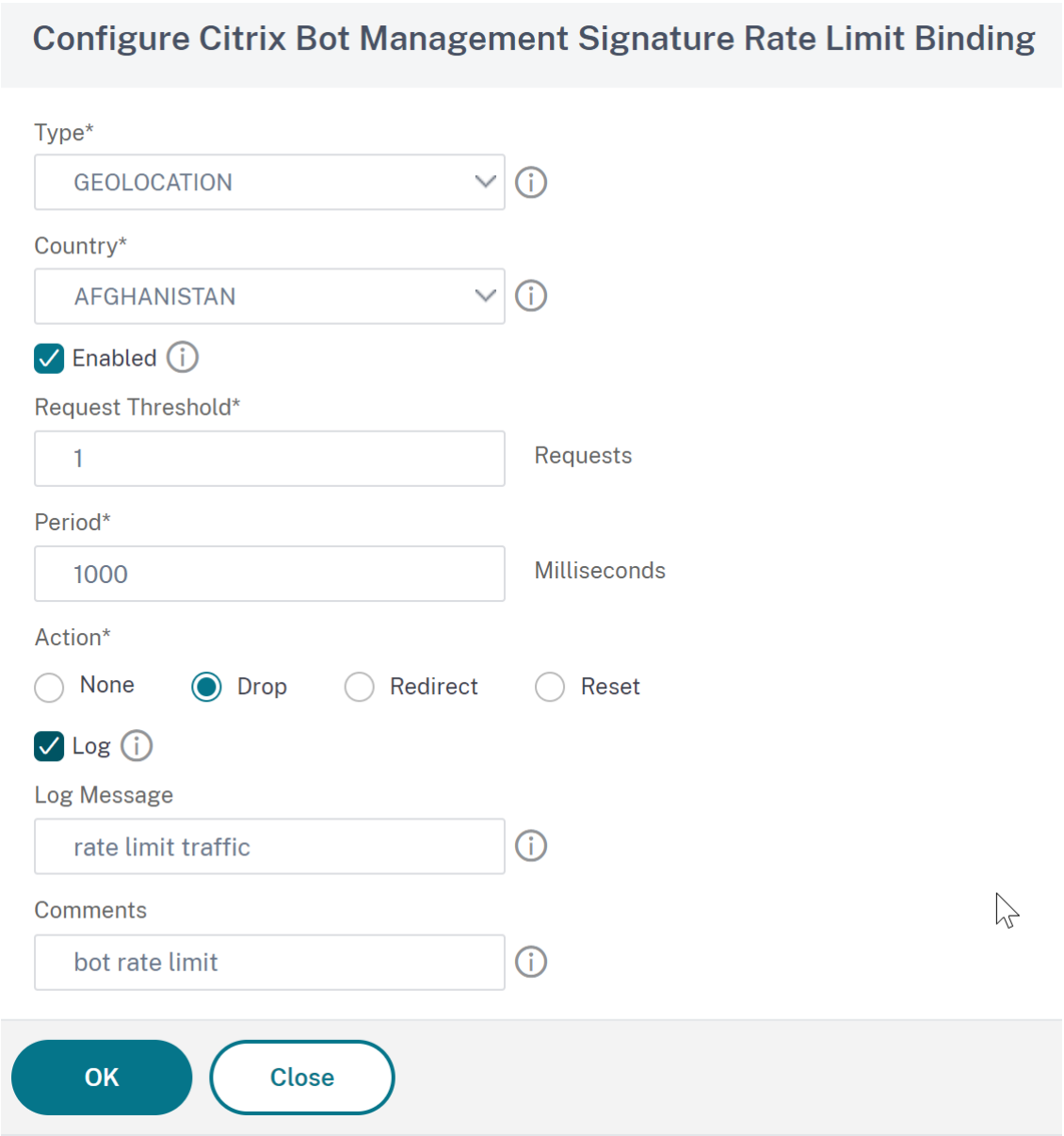
```
 bind bot profile geo_prof -ratelimit -type Geolocation -countryCode IN
     -rate 100 -timeSlice 1000 -action log,drop -enabled on
<!--NeedCopy-->
```

Complete los siguientes pasos para configurar la técnica de detección de límite de velocidad de bots:

1. Vaya a **Seguridad >**Perfiles**y administración de bots de Citrix**.
2. En la página **Perfiles de administración de Bot de Citrix**, seleccione un perfil y haga clic en **Modificar**.
3. En la página **Perfil de Citrix Bot Management**, vaya a la sección **Configuración del perfil** y haga clic en **Límite de velocidad**.
4. En la sección **Límite de velocidad**, defina los siguientes parámetros:

a) Habilitada. Seleccione la casilla de verificación para validar el tráfico de bot entrante como parte del proceso de detección.
b. Haga clic en **Agregar** para configurar los enlaces de límite de velocidad.

5. En la página **Configurar límite de velocidad de administración de bots de Citrix**, defina los siguientes parámetros.
   a) Tipo. Limite el tráfico de bots en función de los siguientes parámetros:
      i. Geolocalización. Límite de tarifas basado en la ubicación geográfica del usuario.
      ii. Source_ip. Limite el tráfico en función de la dirección IP del cliente.
      iii. Sesión. Limite el tráfico de bots según el nombre de la sesión o la cookie.
      iv. URL. Limite el tráfico de bots en función de la URL configurada.
   b) País. Seleccione una geolocalización como país o región.
   c) Habilitada. Seleccione la casilla de verificación para validar el tráfico de bot entrante.
   d) Umbral de solicitud Número máximo de solicitudes permitidas dentro de un plazo determinado.
   e) Período. Plazo en milisegundos.
   f) Acción. Elige una acción bot para la categoría seleccionada.
   g) Registro. Seleccione la casilla de verificación para almacenar las entradas de registro.
   h) Mensaje de registro. Breve descripción del registro.
   i) Observaciones. Breve descripción de la categoría bot.
6. Haga clic en **OK**.
7. Haga clic en **Update**.
8. Haga clic en **Listo**.



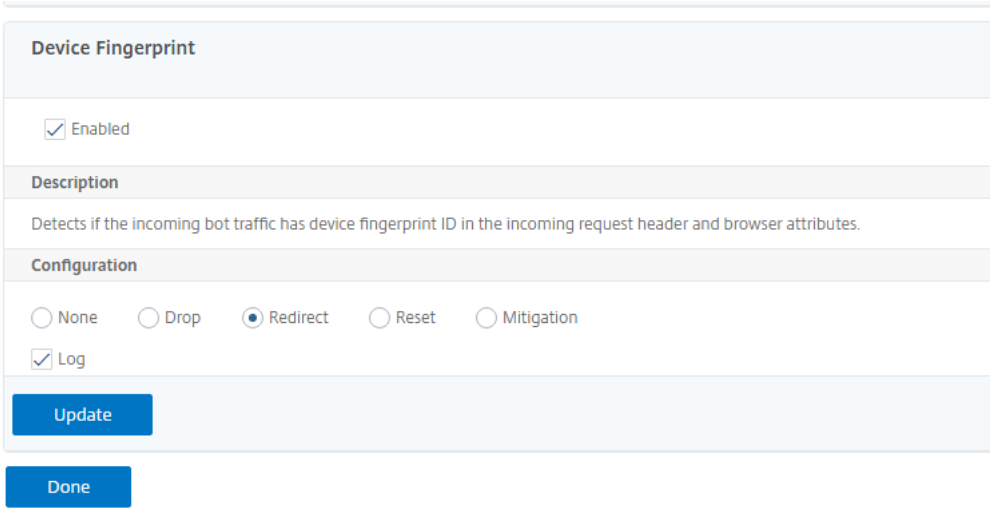
Configurar la técnica de huellas digitales del dispositivo mediante la interfaz gráfica de usuario de Citrix ADC

Esta técnica de detección envía un desafío de script java al cliente y extrae la información del dispositivo. Según la información del dispositivo, la técnica descarta o evita el tráfico del bot. Siga los pasos para configurar la técnica de detección.

1. Vaya a **Seguridad** > **Perfiles** y **administración de bots de Citrix**.
2. En la página **Perfiles de administración de bots de Citrix**, seleccione un archivo de firma y haga clic en **Modificar**.
3. En la página **Perfil de administración de bots de Citrix**, vaya a la sección **Configuración de**

firmas y haga clic en **Huella digital del dispositivo**.

4. En la sección **Huella digital del dispositivo**, defina los siguientes parámetros:
   a) Habilitada. Defina esta opción para habilitar la regla.
   b) Configuración. Para la huella digital del dispositivo dada, no asigne ninguna acción, descarte o redirija, mitigue o actúe CAPTCHA.
   c) Registro. Seleccione la casilla de verificación para almacenar las entradas de registro.
5. Haga clic en **Update**.
6. Haga clic en **Listo**.



Configurar la técnica de huellas dactilares del dispositivo para aplicaciones móviles (Android)

La técnica de huella digital del dispositivo detecta un tráfico entrante como bot insertando un script JavaScript en la respuesta HTML al cliente. El script JavaScript, cuando el explorador lo invoca, recopila los atributos del explorador y del cliente y envía una solicitud al dispositivo. Los atributos se examinan para determinar si el tráfico es un bot o un humano.

La técnica de detección se amplía aún más para detectar bots en una plataforma móvil (Android). A diferencia de las aplicaciones web, en el tráfico móvil (Android), la detección de bots basada en scripts JavaScript no se aplica. Para detectar bots en una red móvil, la técnica utiliza un SDK móvil bot que está integrado con las aplicaciones móviles del lado del cliente. El SDK intercepta el tráfico móvil, recopila los detalles del dispositivo y envía los datos al dispositivo. En el lado del dispositivo, la técnica de detección examina los datos y determina si la conexión procede de un bot o de un humano.

Cómo funciona la técnica de huellas dactilares del dispositivo para la aplicación móvil

En los siguientes pasos se explica el flujo de trabajo de detección de bots para detectar si una solicitud de un dispositivo móvil proviene de un humano o de un bot.

1. Cuando un usuario interactúa con una aplicación móvil, el SDK móvil del bot registra el comportamiento del dispositivo.
2. El cliente envía una solicitud al dispositivo Citrix ADC.
3. Al enviar la respuesta, el dispositivo inserta una cookie de sesión de bot con los detalles de la sesión y los parámetros para recopilar los parámetros del cliente.
4. Cuando la aplicación móvil recibe la respuesta, el SDK de bots de Citrix integrado con la aplicación móvil valida la respuesta, recupera los parámetros de huellas digitales del dispositivo grabados y la envía al dispositivo.
5. La técnica de detección de huellas dactilares del dispositivo valida los detalles del dispositivo y actualiza la cookie de sesión del bot si se sospecha que es un bot o no.
6. Cuando la cookie ha caducado o la protección de huellas dactilares del dispositivo prefiere validar y recopilar los parámetros del dispositivo periódicamente, se repite todo el procedimiento o desafío.

Requisito previo

Para empezar con la técnica de detección de huellas dactilares del dispositivo Citrix ADC para aplicaciones móviles, debe descargar e instalar el SDK móvil bot en su aplicación móvil.

Configurar la técnica de detección de huellas dactilares para aplicaciones móviles (Android) mediante la CLI

En el símbolo del sistema, escriba:

```
set bot profile <profile name> -deviceFingerprintMobile ( NONE | Android )
```

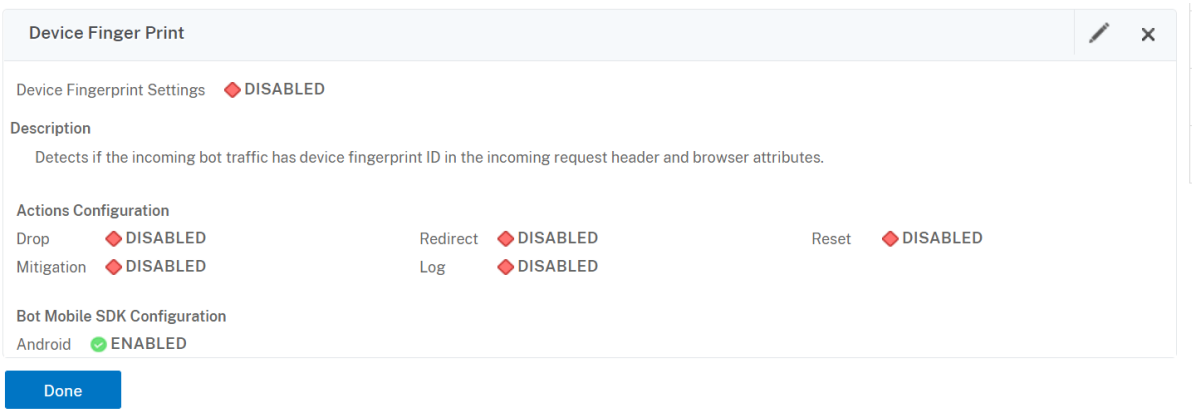
Ejemplo:

```
set bot profile profile 1 -deviceFingerprintMobile Android
```

Configurar la técnica de detección de huellas dactilares del dispositivo para aplicaciones móviles (Android) mediante la interfaz gráfica de usuario

1. Vaya a **Seguridad** > **Perfiles** y **administración de bots de Citrix**.
2. En la página **Perfiles de administración de bots de Citrix**, seleccione un archivo y haga clic en **Modificar**.
3. En la página **Perfil de administración de bots de Citrix**, haga clic en **Huella digital del dispositivo** en **Configuración del perfil**.

4. En la sección **Configurar Bot Mobile SDK**, seleccione el tipo de cliente móvil.
5. Haga clic en **Actualizar** y **listo**.



Configurar expresión de registro de bot

Si el cliente se identifica como bot, la administración de bots de Citrix le permite capturar información adicional como mensajes de registro. Los datos pueden ser el nombre del usuario que solicitó la URL, la dirección IP de origen y el puerto de origen desde el que el usuario envió la solicitud o los datos generados a partir de una expresión. Para realizar un registro personalizado, debe configurar una expresión de registro en el perfil de administración de bots.

Enlazar la expresión de registro en el perfil de bot mediante la CLI

En el símbolo del sistema, escriba:

```
1 bind bot profile <name> (-logExpression -name <string> -expression <
     expression> [-enabled ( ON | OFF )]) -comment <string>
2 <!--NeedCopy-->
```

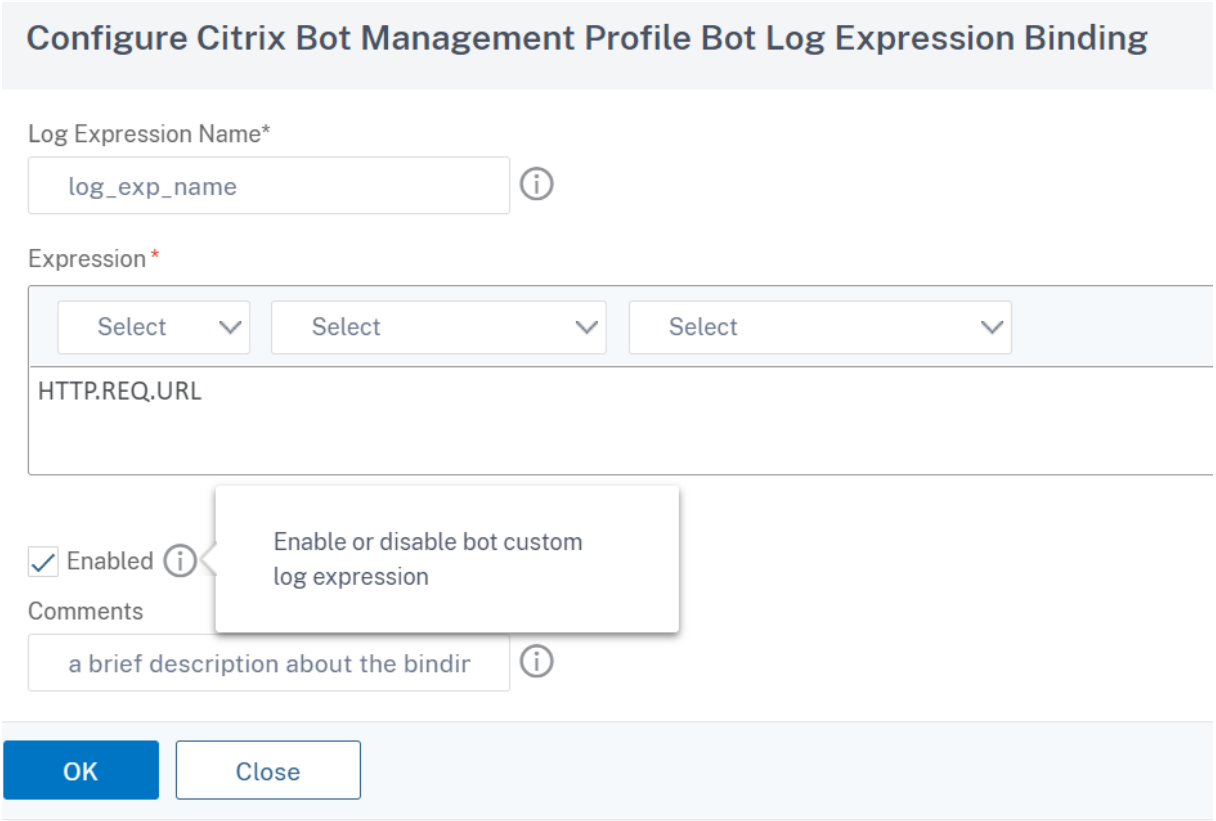
Ejemplo:

```
bind bot profile profile1 -logExpression exp1 -expression HTTP.REQ.URL -
enabled ON -comment "testing log expression"
```

Vincular expresión de registro al perfil de bot mediante la GUI

1. Vaya a **Seguridad > Administración de bots de Citrix > Perfiles**.
2. En la página **Perfiles de administración de bots de Citrix**, seleccione **Expresiones de registro de bots** en la sección **Configuración del perfil**.
3. En la sección Configuración de expresiones de registro de **bots, haga clic en**Agregar**.

4. En la página **Configurar enlace de expresiones de registro de bots de perfil de Citrix Bot Management**, establezca los siguientes parámetros.
   a) Nombre de expresión de registro. Nombre de la expresión de registro.
   b) Expresión. Introduzca la expresión de registro.
   c) Habilitada. Habilitar o inhabilitar el enlace de expresiones de registro.
   d) Observaciones. Breve descripción del enlace de expresiones de registro de bot.
5. Haga clic en**Aceptar** y **Listo**.



Configurar la técnica de captura de bot

La técnica de captura de bots de Citrix inserta de forma aleatoria o periódica una URL de captura en la respuesta del servidor. También puede crear una lista de URL de captura y agregar URL para ello. La URL parece invisible y no se puede acceder a ella si el cliente es un usuario humano. Sin embargo, si el cliente es un bot automatizado, se puede acceder a la URL y, cuando se accede, el atacante se clasifica como bot y se bloquea cualquier solicitud posterior del bot. La técnica de trampa es eficaz para bloquear los ataques de los bots.

La URL de captura es una URL alfanumérica de longitud configurable y se genera automáticamente a

intervalos configurables. Además, la técnica le permite configurar una URL de inserción de capturas para los sitios web más visitados o los sitios web visitados con frecuencia. De esta manera, puede imponer el propósito de insertar la URL de captura de bots para las solicitudes que coincidan con la URL de inserción de trampa.

> **Nota:**
>
> Aunque la URL de captura de bots se genera automáticamente, la administración de bots de Citrix ADC sigue permitiéndole configurar una URL de captura personalizada en el perfil del bot. Esto se hace para reforzar
> la técnica de detección de bots y dificultar que los atacantes accedan a la URL de la trampa.

Para completar la configuración de la trampa de bots, debes completar los siguientes pasos.

1. Habilitar URL de captura de bot
2. Configurar la URL de captura de bots en el perfil del bot
3. Enlace la URL de inserción de capturas de bots al perfil de
4. Configurar la longitud y el intervalo de la URL de captura de bots en la configuración del bot

Habilitar la protección URL de captura de bots

Antes de empezar, debe asegurarse de que la protección URL de captura de bots esté habilitada en el dispositivo. En el símbolo del sistema, escriba:

```
enable ns feature Bot
```

Configurar la URL de captura de bots en el perfil del bot

Puede configurar la URL de captura de bots y especificar una acción de captura en el perfil del bot. En el símbolo del sistema, escriba:

```
add bot profile <name> -trapURL <string> -trap ( ON | OFF )-trapAction <
trapAction>
```

Donde:

`trapURL`. URL que la protección Bot utiliza como URL de captura. Longitud máxima: 127

`trap`. Active la detección de trampas de bots Valores posibles: ON, OFF, Valor por defecto: OFF

`trapAction`. Acción a tomar en función de la detección de bots. Valores posibles: NONE, LOG, DROP, REDIRECT, RESET, MITIGATION. Valor predeterminado: NINGUNO

Ejemplo:

```
add bot profile profile1 -trapURL www.bottrap1.com trap ON -trapAction
RESET
```


Enlace la URL de inserción de capturas de bots al perfil de

Puede configurar la URL de inserción de capturas de bots y vincularla al perfil de bot.
En el símbolo del sistema, escriba:

```
bind bot profile <profile_name> trapInsertionURL -url <url> -enabled ON|OFF
-comment <comment>
```

Donde:

URL. Patrón de expresión regular de URL de solicitud para el que se inserta la URL de captura de bot. Longitud máxima: 127

Ejemplo:

```
bind bot profile profile1 trapInsertionURL -url www.example.com -enabled ON
-comment insert a trap URL randomly
```

Configurar la longitud y el intervalo de la URL de captura de bots en la configuración del bot

Puede configurar la longitud de la URL de la captura de bots y también establecer el intervalo para generar automáticamente la URL de captura de bot.
En el símbolo del sistema, escriba:

```
set bot settings -trapURLAutoGenerate ( ON | OFF )-trapURLInterval <positive_integer
> -trapURLLength <positive_integer>
```

Donde:

trapURLInterval. Tiempo en segundos tras el cual se actualiza la URL de la trampa de bots. Valor predeterminado: 3600, Valor mínimo: 300, Valor máximo: 86400

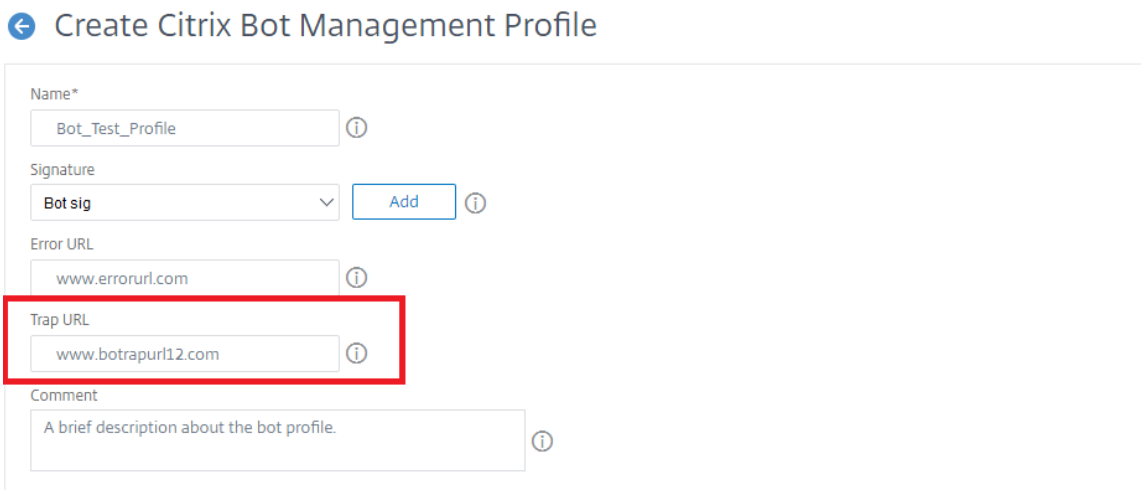
trapURLLength. Longitud de la URL de captura de bots generada automáticamente. Valor predeterminado: 32, Valor mínimo: 10, Valor máximo: 255

Ejemplo:

```
set bot settings -trapURLAutoGenerate ON -trapURLInterval 300 -trapURLLength
 60
```

Configurar la URL de captura de bots mediante la interfaz gráfica de usuario

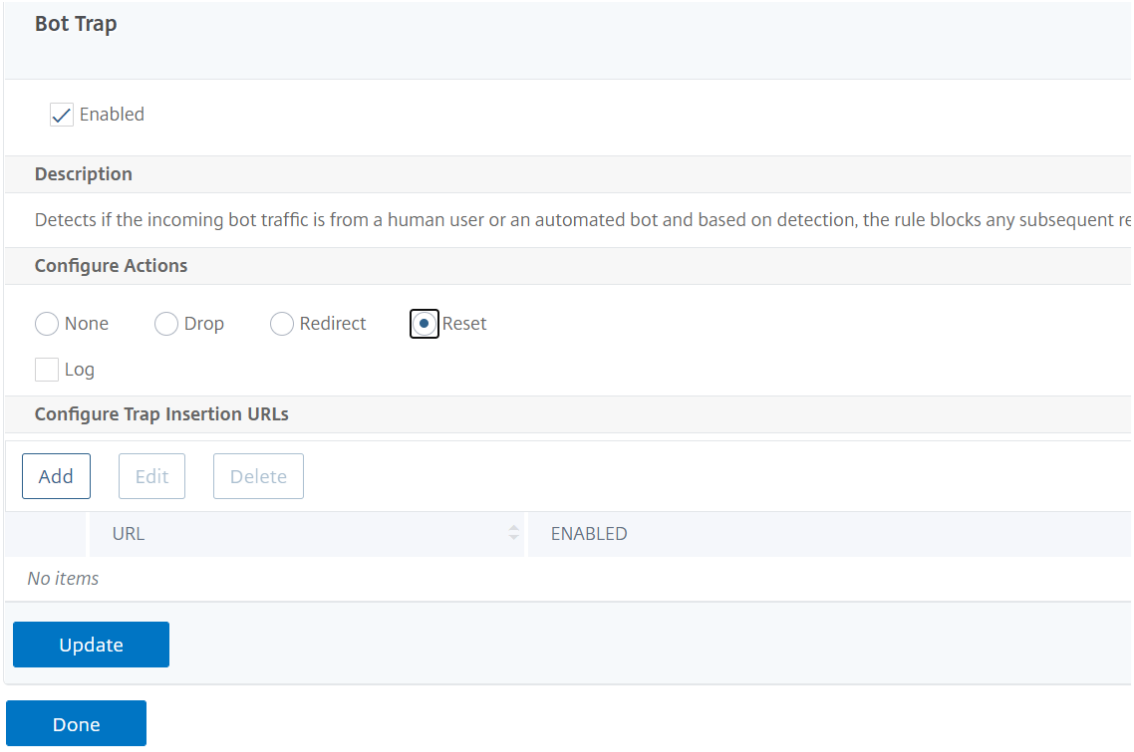
1. Vaya a **Seguridad > Administración de bots de Citrix > Perfiles**.
2. En la página **Perfiles de administración de bots de Citrix**, haga clic en **Modificar** para configurar la técnica URL de captura de bots.
3. En la página **Crear perfil de administración de bots de Citrix**, introduzca la URL de captura de bots en la sección general.



4. En la página **Crear perfil de administración de bots de Citrix**, haga clic en **Bot Trap** en **Configuración del perfil**.

5. En la sección **Bot Trap**, defina los siguientes parámetros.

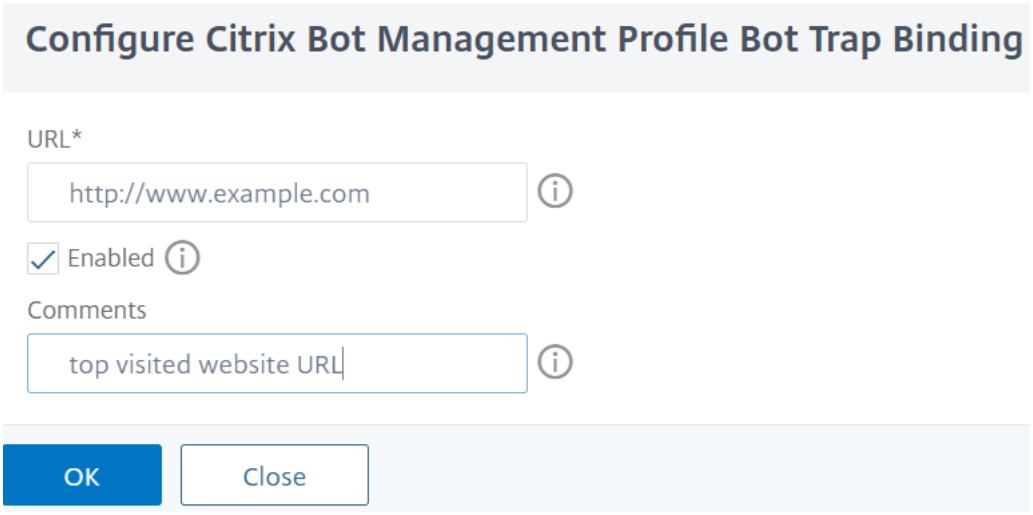
   a. Habilitada. Seleccione la casilla de verificación para habilitar la detección de trampas de bots
   b. Descripción. Breve descripción de la URL.
   c. Configurar acciones. Acción que debe tomarse para el bot detectado por el acceso a la trampa de bots.



6. En la sección **Configurar URL de inserción** de captación, haga clic en **Agregar**.

7. En la página **Configurar enlace de captura de bot de perfil de Citrix Bot Management**, defina los siguientes parámetros.

   a) URL de captura. Escriba la URL que quiere confirmar como la URL de inserción de la trampa de bots.
   b) Habilitada. Habilitar o inhabilitar la URL de inserción de capturas de bots
   c) Comentario. Una breve descripción de la URL de inserción de capturas.



8. En la sección **Configuración de firma**, haga clic en **Bot Trap**.
9. En la sección **Bot Trap**, defina los siguientes parámetros:

   a) Habilitada. Seleccione la casilla de verificación para habilitar la detección de trampas de bots.

   b) En la sección Configurar, defina los siguientes parámetros.

      i. Acción. Acción que debe tomarse para el bot detectado por el acceso a la trampa de bots.
      ii. Registro. Habilita o inhabilita el registro para el enlace de trampas de bots.

10. Haga clic en **Actualizar** y **listo**.

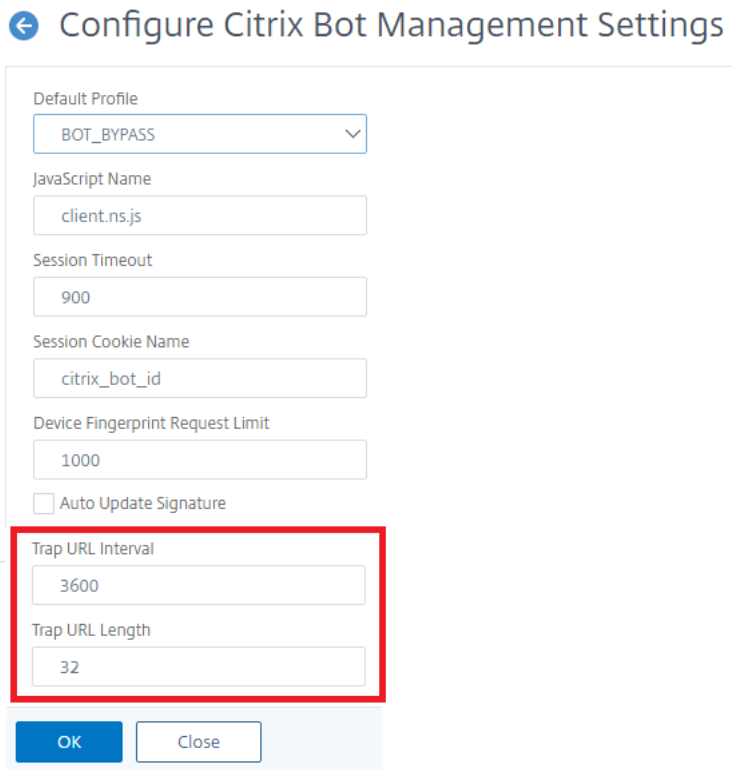
Configurar los ajustes de URL de captura de bots

Complete los siguientes pasos para configurar la URL de captura de bots:

1. Vaya a **Seguridad > Administración de bots de Citrix**.
2. En el panel de detalles, en **Configuración**, haga clic en **Cambiar configuración de administración de bots de Citrix**.
3. En **Configurar opciones de administración de bots de Citrix**, defina los siguientes parámetros.

a) Intervalo de URL de captura. Tiempo en segundos tras el cual se actualiza la URL de la trampa de bots.
b) Longitud de URL de captura. Longitud de la URL de captura de bots generada automáticamente.

4. Haga clic en **Aceptar** y **Listo**.



Expresión de directiva IP de cliente para detección de bots

La administración de bots de Citrix ahora permite configurar una expresión de directiva avanzada para extraer la dirección IP del cliente de un encabezado de solicitud HTTP, cuerpo de solicitud HTTP, URL de solicitud HTTP o mediante una expresión de directiva avanzada. El valor extraído lo puede utilizar un mecanismo de detección de bots (como TPS, captura de bots o límite de velocidad) para detectar si la solicitud entrante es un bot.

> **Nota:**
>
> Si no ha configurado una expresión IP de cliente, se utiliza la dirección IP del cliente de origen predeterminada o existente para la detección de bots. Si se configura una expresión, el resultado de la evaluación proporciona la dirección IP del cliente que se puede utilizar para la detección de bots.

Puede configurar y utilizar la expresión IP del cliente para extraer la dirección IP del cliente real si la

solicitud entrante llega a través de un servidor proxy y si la dirección IP del cliente está presente en el encabezado. Al agregar esta configuración, el dispositivo puede utilizar el mecanismo de detección de bots para proporcionar más seguridad a los clientes y servidores de software.

Configurar la expresión de directiva IP del cliente en el perfil de bot mediante la CLI

En el símbolo del sistema, escriba:

```
add bot profile <name> [-clientIPExpression <expression>]
<!--NeedCopy-->
```

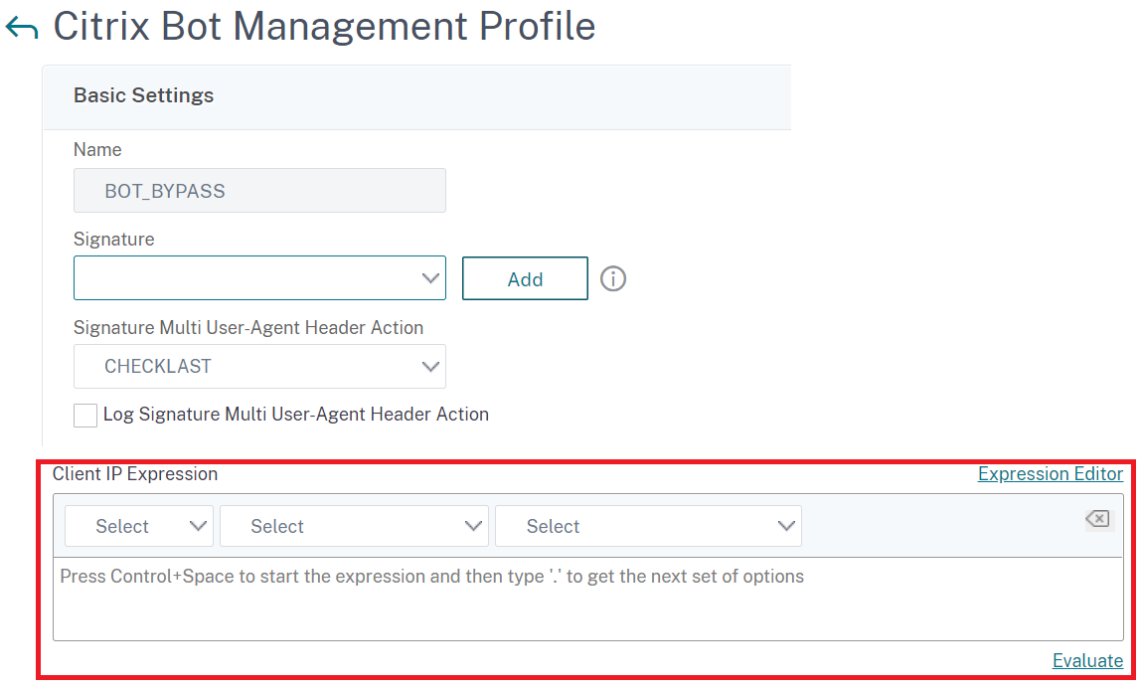
Ejemplo:

```
add bot profile profile1 -clientIPExpression 'HTTP.REQ.HEADER("X-Forwarded-For")ALT CLIENT.IP.SRC.TYPECAST_TEXT_T'
```

```
add bot profile profile1 -clientIPExpression 'HTTP.REQ.HEADER("X-Forwarded-For")ALT CLIENT.IPv6.SRC.TYPECAST_TEXT_T'
```

Configurar la expresión de directiva IP del cliente en el perfil de bot mediante la GUI

1. Vaya a **Seguridad > Administración de bots de Citrix > Perfiles**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En la página **Crear perfil de administración de bots de Citrix**, establezca la expresión IP del cliente.
4. Haga clic en **Crear** y **cerrar**.



Configurar CAPTCHA para la reputación IP y la detección de huellas dactilares del dispositivo

CAPTCHA es un acrónimo que significa “Prueba pública de Turing completamente automatizada para diferenciar a computadoras y humanos”. CAPTCHA está diseñado para comprobar si un tráfico entrante proviene de un usuario humano o de un bot automatizado. CAPTCHA ayuda a bloquear los bots automatizados que causan infracciones de seguridad en las aplicaciones web. En el dispositivo ADC, CAPTCHA utiliza el módulo de respuesta de desafío para identificar si el tráfico entrante procede de un usuario humano y no de un bot automatizado.

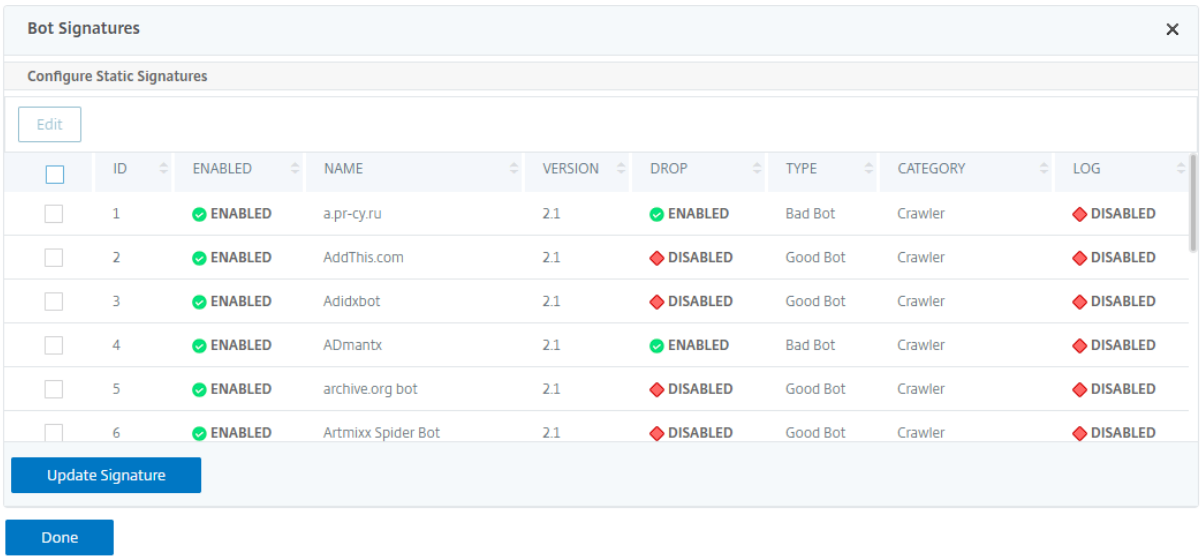
Configurar firmas estáticas de bot

Esta técnica de detección permite identificar la información del agente de usuario a partir de los detalles del explorador. En función de la información del agente de usuario, el bot se identifica como un robot malo o bueno y luego se le asigna una acción de bot. Siga los pasos a continuación para configurar la técnica de firma estática:

1. En el panel de navegación, expanda **Seguridad > Administración de bots de Citrix > Firmas**.
2. En la página **Firmas de administración de bots de Citrix**, seleccione un archivo de firma y haga clic en **Modificar**.
3. En la página **Firma de Citrix Bot Management**, vaya a la sección **Configuración de firmasy haga clic en Firmas de bot**.
4. En la sección **Firmas de bot**, defina los siguientes parámetros:

a) Configurar firmas estáticas. En esta sección se incluye una lista de registros de firmas estáticas de bot. Puede seleccionar un registro y hacer clic en **Modificar** para asignarle una acción de bot.
b) Haga clic en **OK**.

5. Haga clic en **Actualizar firma**.
6. Haga clic en **Listo**.



Delineación de firma estática de bot

La administración de bots de Citrix ADC protege su aplicación web contra los bots. Las firmas estáticas de bots ayudan a identificar bots buenos y malos en función de parámetros de solicitud, como el agente de usuario en la solicitud entrante.
La lista de firmas en el archivo es enorme y también se agregan nuevas reglas y las obsoletas se eliminan periódicamente. Como administrador, es posible que quiera buscar una firma específica o una lista de firmas en una categoría. Para filtrar las firmas fácilmente, la página de firma de bots proporciona una capacidad de búsqueda mejorada. La función de búsqueda permite buscar reglas de firma y configurar su propiedad en función de uno o varios parámetros de firma como acción, ID de firma, desarrollador y nombre de firma.

Acción. Seleccione una acción de bot que prefiera configurar para una categoría específica de reglas de firma. A continuación se presentan los tipos de acción disponibles:

- Habilitar seleccionado. Habilita todas las reglas de firma seleccionadas.
- Inhabilitar Seleccionado. Desactiva todas las reglas de firmas seleccionadas.
- Suéltalo seleccionado. Seleccione la acción “Soltar” en todas las reglas de firma seleccionadas.
- Redirección seleccionada. Aplica la acción “Redirigir” a todas las reglas de firma seleccionadas.
- Restablecer seleccionado. Aplica la acción “Restablecer” a todas las reglas de firma seleccionadas.

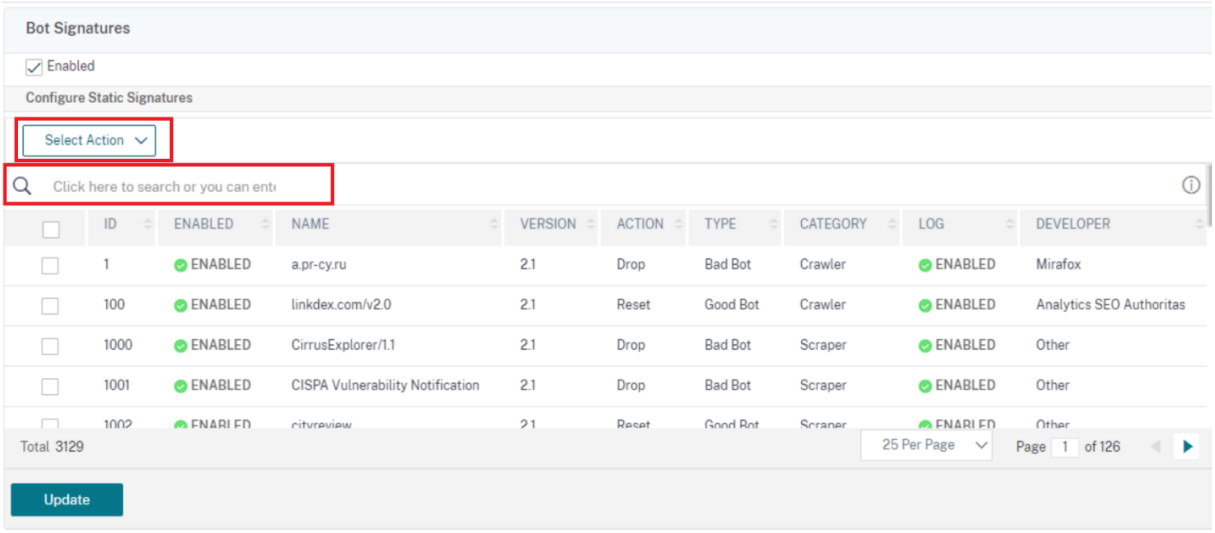
- Registro seleccionado. Aplica la acción “Registro” a todas las reglas de firma seleccionadas.
- Eliminar gota seleccionada. Desestablece la acción de soltar en todas las reglas de firma seleccionadas.
- Eliminar redirección seleccionada. Desestablece la acción de redirección en todas las reglas de firma seleccionadas.
- Eliminar restablecimiento seleccionado. Desestablece la acción de restablecimiento de todas las reglas de firma seleccionadas.
- Eliminar registro seleccionado. Anule la configuración de la acción de registro en todas las reglas de firma seleccionadas.

Categoría. Seleccione una categoría para filtrar las reglas de firma en consecuencia. A continuación se presenta la lista de categorías disponibles para ordenar las reglas de firma.

- Acción. Ordenar en función de la acción del bot.
- Categoría. Ordenar en función de la categoría de bot.
- Desarrollador. Ordenar según el publicador de la empresa host.
- Habilitada. Ordenar según las reglas de firma que están habilitadas.
- Id. Ordenar según el ID de regla de firma.
- Registro. Ordene según reglas de firma que tengan habilitado el registro.
- Nombre. Ordenar según el nombre de la regla de firma.
- Tipo. Ordenar según el tipo de firma.
- Versión. Ordenar según la versión de la regla de firma.

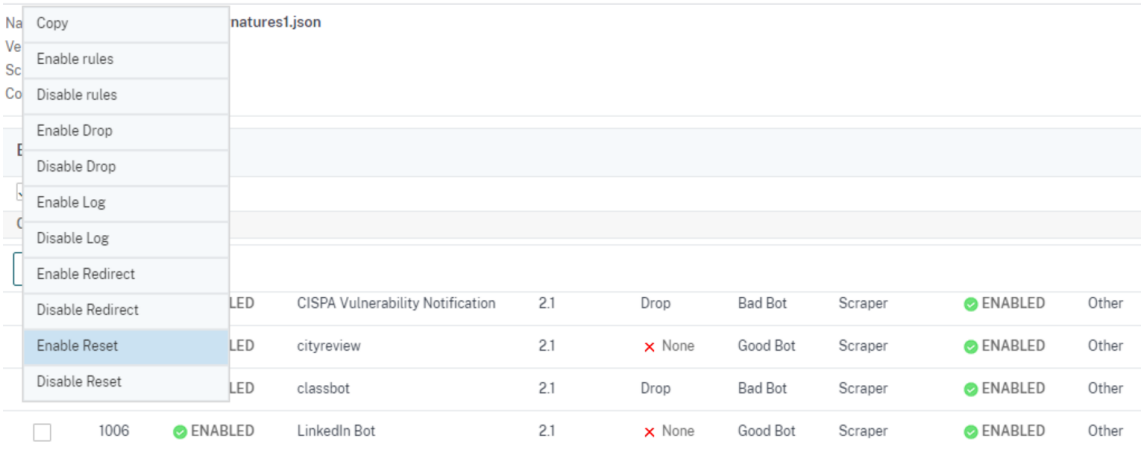
Buscar reglas de firma estática de bot basadas en tipos de acciones y categorías mediante la GUI de Citrix ADC

1. Vaya a **Seguridad > Administración de bots de Citrix > Firma**.
2. En la página de detalles, haga clic en **Agregar**.
3. En la página **Firmas de administración de bots de Citrix**, haga clic en modificar en la sección **Firma estática**.
4. En la sección **Configurar firma estática**, seleccione una acción de firma de la lista desplegable.
5. Utilice la función de búsqueda para seleccionar una categoría y filtrar las reglas según corresponda.
6. Haga clic en **Update**.



Modificar la propiedad de regla de firma estática del bot mediante la GUI de Citrix ADC

1. Vaya a **Seguridad > Administración de bots de Citrix > Firma**.
2. En la página de detalles, haga clic en **Agregar**.
3. En la página **Firmas de administración de bots de Citrix**, haga clic en modificar en la sección **Firma estática**.
4. En la sección **Configurar firma estática**, seleccione una acción de la lista desplegable.
5. Utilice la función de búsqueda para seleccionar una categoría y filtrar las reglas según corresponda.
6. En la lista de firmas estáticas, seleccione una firma para modificar su propiedad.



7. Haga clic en **Aceptar** para confirmar.

Cómo funciona CAPTCHA en la administración de bots de Citrix ADC

En la administración de bots de Citrix ADC, la validación de CAPTCHA se configura como una acción de directiva que se ejecutará después de evaluar la directiva de bots. La acción CAPTCHA solo está disponible para la reputación de IP y las técnicas de detección de huellas dactilares del dispositivo. Los siguientes son los pasos para entender cómo funciona CAPTCHA:

1. Si se observa una infracción de seguridad durante la reputación de IP o la detección de bots de huellas digitales del dispositivo, el dispositivo ADC envía un desafío CAPTCHA.
2. El cliente envía la respuesta CAPTCHA.
3. El dispositivo valida la respuesta CAPTCHA y, si el CAPTCHA es válido, se permite la solicitud y se reenvía al servidor back-end.
4. Si la respuesta CATCHA no es válida, el dispositivo envía un nuevo desafío CAPTCHA hasta que se alcanza el número máximo de intentos.
5. Si la respuesta CAPTCHA no es válida incluso después del número máximo de intentos, el dispositivo descarta o redirige la solicitud a la URL de error configurada.
6. Si ha configurado la acción de registro, el dispositivo almacena los detalles de la solicitud en el archivo ns.log.

Configurar los ajustes de CAPTCHA mediante la GUI de Citrix ADC

La acción CAPTCHA de gestión de bots solo es compatible con la reputación de IP y las técnicas de detección de huellas dactilares del dispositivo. Complete los siguientes pasos para configurar los ajustes de **CAPTCHA**.

1. Vaya a **Seguridad > Perfiles y administración de bots de Citrix**.
2. En la página **Perfiles de administración de Bot de Citrix**, seleccione un perfil y haga clic en **Modificar**.
3. En la página **Perfil de administración de bots de Citrix**, vaya a la sección **Configuración de firma** y haga clic en **CAPTCHA**.
4. En la sección **Configuración de CAPTCHA**, haga clic en **Agregar para configurar los ajustes de CAPTCHA** en el perfil:
5. En la página **Configurar CAPTCHA de Citrix Bot Management**, defina los siguientes parámetros.
    a) URL. URL de bot para la que se aplica la acción CAPTCHA durante la reputación de IP y las técnicas de detección de huellas dactilares del dispositivo.
    b) Habilitada. Defina esta opción para habilitar la compatibilidad con CAPTCHA.
    c) Hora de gracia. Duración hasta que no se envía ninguna nueva impugnación CAPTCHA después de recibir la respuesta CAPTCHA válida actual.

d) Tiempo de espera. Duración que tarda el dispositivo ADC en esperar hasta que el cliente envíe la respuesta CAPTCHA.

e) Período de silencio. Duración durante la cual el cliente que envió una respuesta CAPTCHA incorrecta debe esperar hasta que se le permita intentarlo a continuación. Durante este período de silencio, el dispositivo ADC no permite ninguna solicitud. Intervalo: 60—900 segundos, recomendado: 300 segundos

f) Límite de longitud de solicitud. Duración de la solicitud para la que se envía la impugnación CAPTCHA al cliente. Si la longitud es superior al valor del umbral, la solicitud se descarta. El valor predeterminado es de 10 a 3000 bytes.

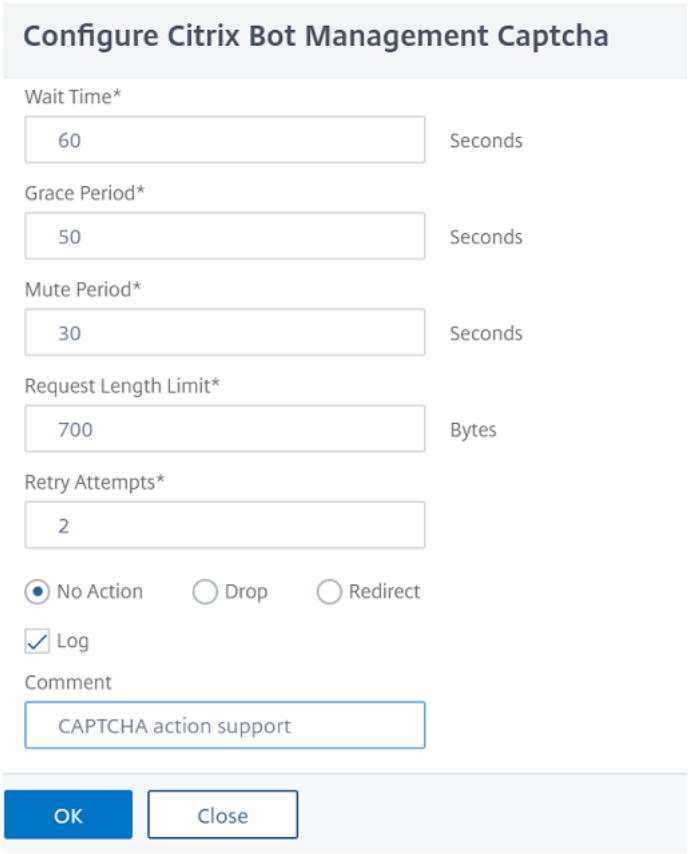
g) Intentos de reintento. Número de intentos que el cliente puede volver a intentar resolver el desafío CAPTCHA. Intervalo: 1-10, recomendado: 5.

h) No se debe realizar ninguna acción, soltar/redirigir si el cliente falla la validación de CAPTCHA.

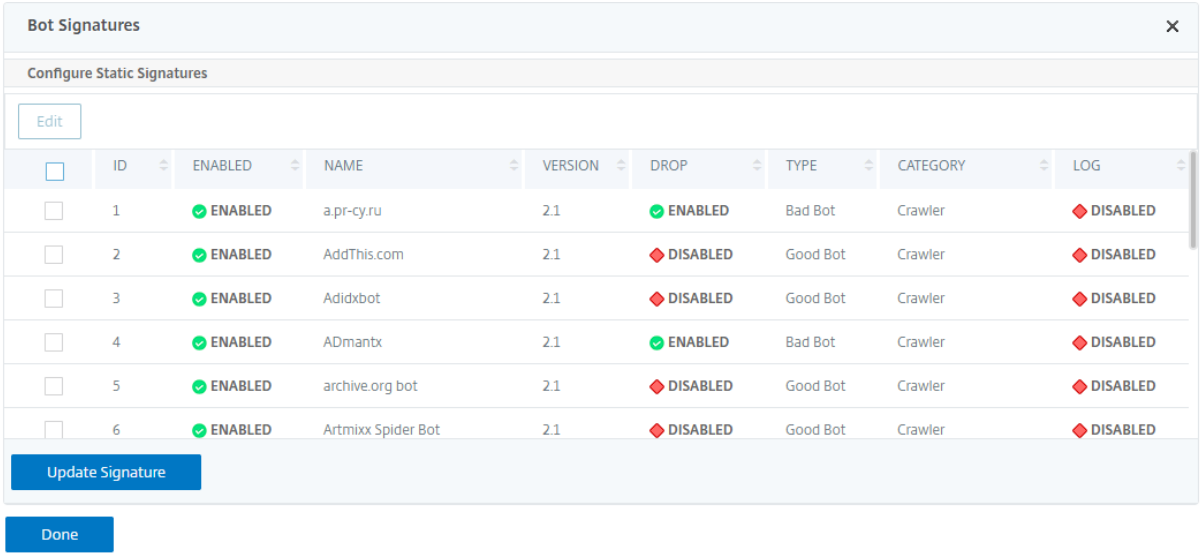
i) Registro. Establezca esta opción para almacenar información de solicitud del cliente cuando la respuesta CAPTCHA falla. Los datos se almacenan en el archivo `ns.log`.

j) Comentario. Breve descripción de la configuración de CAPTCHA.

6. Haga clic en **Aceptar** y **Listo**.



7. Vaya a **Seguridad > Administración de bots de Citrix > Firmas**.
8. En la página **Firmas de administración de bots de Citrix**, seleccione un archivo de firma y haga clic en **Modificar**.
9. En la página **Firma de Citrix Bot Management**, vaya a la sección **Configuración de firmasy haga clic en Firmas de bot**.
10. En la sección **Firmas de bot**, defina los siguientes parámetros:
11. Configurar **firmas estáticas**. Seleccione un registro de firma estática de bot y haga clic en Modificar para asignarle una acción bot.
12. Haga clic en **OK**.
13. Haga clic en **Actualizar firma**.
14. Haga clic en **Listo**.



Actualización automática de firmas de bots

La técnica de firma estática de bots utiliza una tabla de búsqueda de firmas con una lista de bots buenos y bots malos. Los bots se clasifican según la cadena de agente de usuario y los nombres de dominio. Si la cadena de agente de usuario y el nombre de dominio del tráfico de bot entrante coinciden con un valor de la tabla de búsqueda, se aplica una acción bot configurada.
Las actualizaciones de firmas de bots se alojan en la nube de AWS y la tabla de búsqueda de firmas se comunica con la base de datos de AWS para obtener actualizaciones de firmas. El planificador de actualización automática de firmas se ejecuta cada 1 hora para comprobar la **base de datos de AWS** y actualizar la tabla de firmas del dispositivo Citrix ADC.

La URL de actualización automática de firmas que se va a configurar es, `https://nsbotsignatures.s3.amazonaws.com/BotSignatureMapping.json`

> **Nota:**
>
> También puede configurar un servidor proxy y actualizar periódicamente las firmas desde la nube de AWS al dispositivo a través del proxy. Para la configuración del proxy, debe establecer la dirección IP del proxy y la dirección del puerto en la configuración del bot.

Cómo funciona la actualización automática de firmas de bots

En el siguiente diagrama se muestra cómo se recuperan las firmas de bots de la nube de AWS, se actualizan en Citrix ADC y se visualizan en Citrix ADM para obtener un resumen de actualización de firmas.

El planificador de actualización automática de firmas de bot hace lo siguiente:

1. Recupera el archivo de asignación del URI de AWS.
2. Comprueba las firmas más recientes del archivo de asignación con las firmas existentes en el dispositivo ADC.
3. Descarga las nuevas firmas de AWS y verifica la integridad de la firma.
4. Actualiza las firmas de bot existentes con las nuevas firmas del archivo de firma del bot.
5. Genera una alerta SNMP y envía el resumen de actualización de firmas a Citrix ADM.

Configurar actualización automática de firmas de bots

Para configurar la actualización automática de firmas de bots, siga los pasos siguientes:

Habilitar actualización automática de firma de bot

Debe habilitar la opción de actualización automática en la configuración del bot del dispositivo ADC. En el símbolo del sistema, escriba:

```
set bot settings -signatureAutoUpdate ON
```


Configurar los ajustes del servidor proxy (opcional)

Si accede a la base de datos de firmas de AWS a través de un servidor proxy, debe configurar el servidor proxy y el puerto.

```
set bot settings -proxyserver -proxyport
```

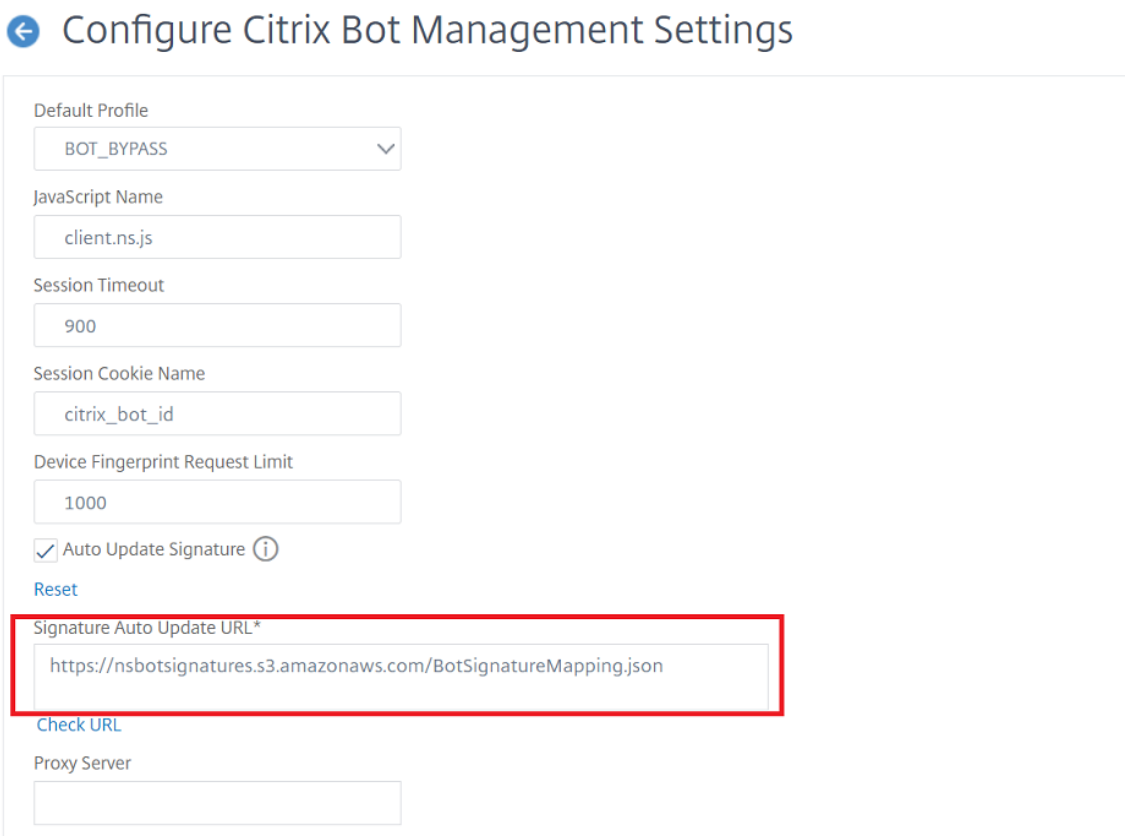
Ejemplo:

```
set bot settings -proxy server 1.1.1.1 -proxyport 1356
```

Configurar la actualización automática de firmas de bots mediante la GUI de Citrix ADC

Complete los siguientes pasos para configurar la actualización automática de firmas de bots:

1. Vaya a **Seguridad > Administración de bots de Citrix**.
2. En el panel de detalles, en **Configuración**, haga clic en **Cambiar configuración de administración de bots de Citrix**.
3. En la casilla **Configurar configuración de Citrix Bot Management**, marque la casilla de verificación **Actualización automática de firma**.



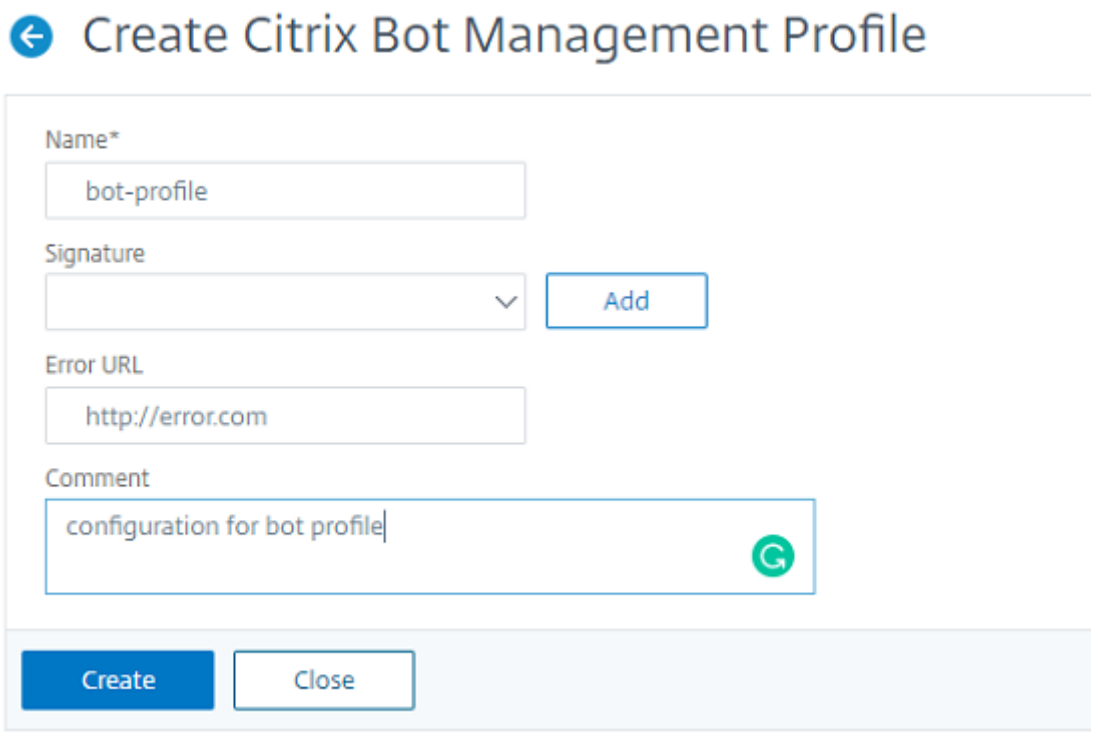
4. Haga clic en **Aceptar** y **cerrar**.

Crear perfil de administración de bots

Un perfil de bot es un conjunto de configuraciones de administración de bots que se utilizan para detectar el tipo de bot. En un perfil, determina cómo aplica Web App Firewall cada uno de sus filtros (o comprobaciones) al tráfico de bots a sus sitios web y las respuestas de ellos.

Complete los siguientes pasos para configurar el perfil del bot:

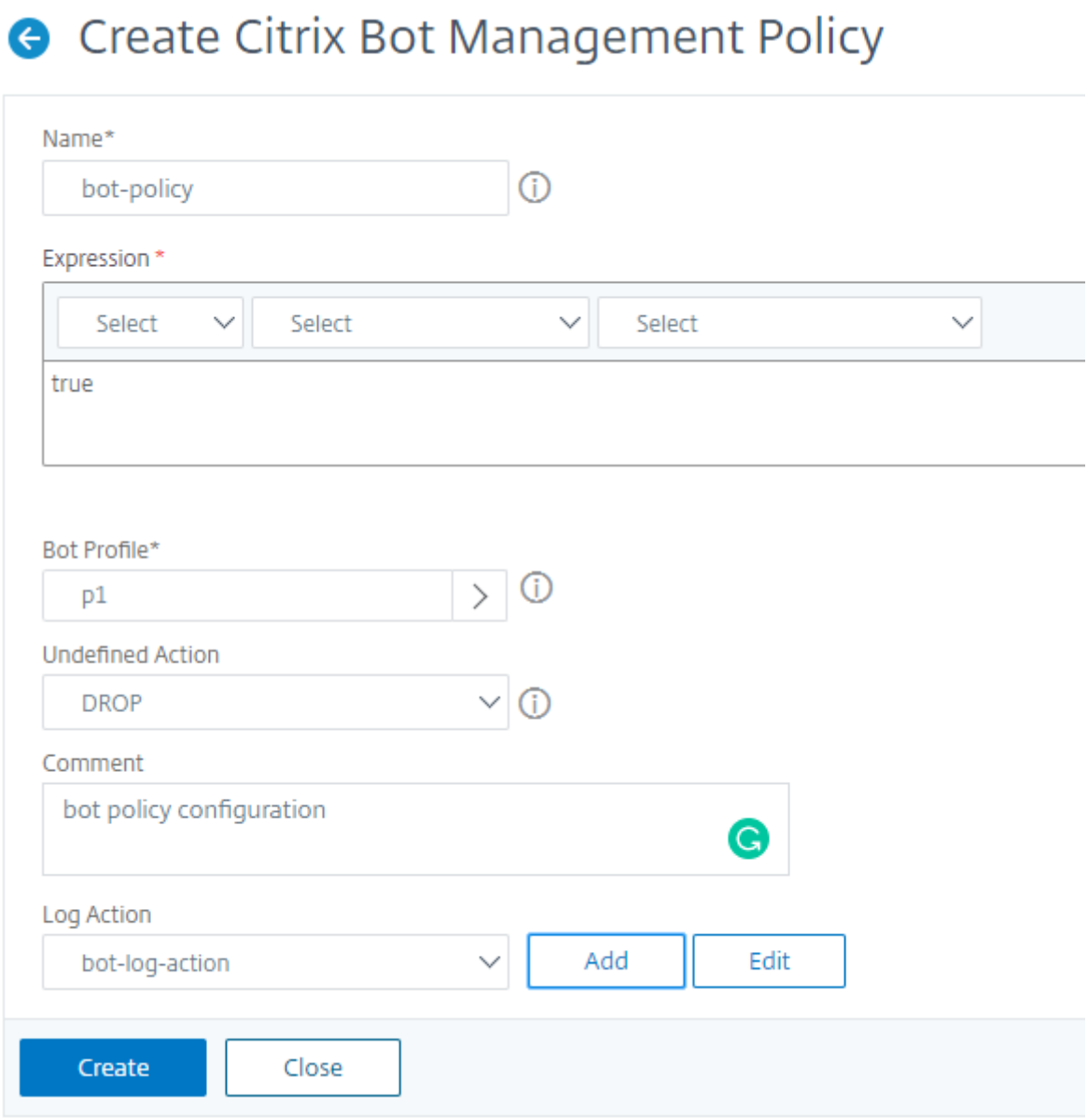
1. Vaya a **Seguridad** > **Administración de bots de Citrix** > **Perfiles**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En la página **Crear perfil de administración de bots de Citrix**, defina los siguientes parámetros.
   a) Nombre. Nombre del perfil del bot.
   b) Firma. Nombre del archivo de firma del bot.
   c) URL de error. URL para redirecciones.
   d) Comentario. Breve descripción del perfil.
4. Haga clic en **Crear** y **cerrar**.



Crear directiva de bots

La directiva de bots controla el tráfico que va al sistema de administración de bots y también controla los registros de bots enviados al servidor de auditlog. Siga el procedimiento para configurar la directiva de bots.

1. Vaya a **Seguridad** > **Administración de bots de Citrix** > **Directivas de bots**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En la página **Crear directiva de administración de bots de Citrix**, defina los siguientes parámetros.
   a) Nombre. Nombre de la directiva de bots.
   b) Expresión. Escriba la expresión o regla de directiva directamente en el área de texto.
   c) Perfil de bot. Perfil de bot para aplicar la directiva de bots.
   d) Acción indefinida. Seleccione la acción que prefiera asignar.
   e) Comentario. Breve descripción de la directiva.
   f) Acción de registro. Acción de mensaje de registro de auditoría para registrar el tráfico de bots. Para obtener más información sobre la acción del registro de auditoría, consulte el tema Registro de auditoría.
4. Haga clic en **Crear** y **cerrar**.



Transacciones de bots por segundo (TPS)

La técnica de bot Transacciones por segundo (TPS) detecta el tráfico entrante como bot si el número de solicitudes por segundo (RPS) y el porcentaje de aumento del RPS superan el valor umbral configurado. La técnica de detección protege sus aplicaciones web de bots automatizados que pueden provocar actividades de raspado web, inicio de sesión forzado bruto y otros ataques maliciosos.

> **Nota:**
>
> La técnica bot detecta un tráfico entrante como bot solo si ambos parámetros están configurados y si ambos valores aumentan más allá del límite umbral.

> Consideremos un caso en el que el dispositivo recibe muchas solicitudes procedentes de una URL específica y quiere que la administración de bots de Citrix ADC detecte si hay un ataque de bot. La técnica de detección de TPS examina el número de solicitudes (valor configurado) procedentes de la URL en 1 segundo y el aumento porcentual (valor configurado) del número de solicitudes recibidas en 30 minutos. Si los valores superan el límite del umbral, el tráfico se considera bot y el dispositivo ejecuta la acción configurada.

Técnica de configuración de transacciones de bot por segundo (TPS)

Para configurar TPS, debe completar los pasos siguientes:

1. Habilitar TPS bot
2. Enlazar la configuración de TPS al perfil de administración de bots

Enlazar la configuración de TPS al perfil de administración de bots

Una vez que habilite la función TPS del bot, debe vincular la configuración de TPS al perfil de administración de bots.

En el símbolo del sistema, escriba:

```
bind bot profile <name>… (-tps [-type ( SourceIP | GeoLocation | RequestURL
 | Host )] [-threshold <positive_integer>] [-percentage <positive_integer
>] [-action ( none | log | drop | redirect | reset | mitigation )] [-
logMessage <string>])
```

Ejemplo:

```
bind bot profile profile1 -tps -type RequestURL -threshold 1 -percentage
100000 -action drop -logMessage log
```

Habilitar transacción bot por segundo (TPS)

Antes de empezar, debe asegurarse de que la función TPS bot esté habilitada en el dispositivo. En el símbolo del sistema, escriba:

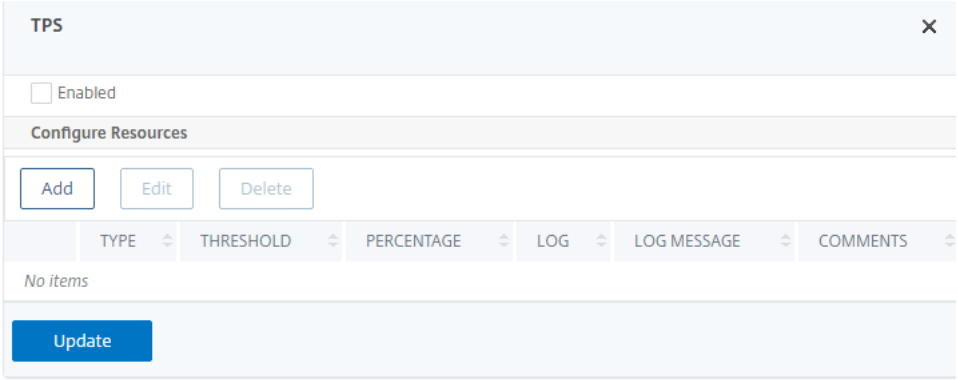
```
set bot profile profile1 -enableTPS ON
```

Configurar transacciones de bots por segundo (TPS) mediante la interfaz gráfica de usuario de Citrix ADC

Complete los siguientes pasos para configurar las transacciones de bots por segundo:

1. Vaya a **Seguridad > Administración de bots de Citrix > Perfiles**.

2. En la página **Perfiles de administración de bots de Citrix**, seleccione un perfil y haga clic en **Modificar**.
3. En la página **Crear perfil de administración de bots de Citrix**, haga clic en **TPS** en la sección **Configuración de firma**.
4. En la sección **TPS**, active la función y haga clic en **Agregar**.



5. En la página **Configurar enlace TPS del perfil de administración de bots de Citrix**, defina los siguientes parámetros.
   a) Tipo. Tipos de entrada permitidos por la técnica de detección. Valores posibles: IP FUENTE, GEOLOCALIZACIÓN, HOST, URL.

      SOURCE_IP — TPS basado en la dirección IP del cliente.

      GEOLOCALIZACIÓN: TPS basado en la ubicación geográfica del cliente.

      HOST: TPS basado en solicitudes de clientes reenviadas a una dirección IP de servidor back-end específica.

      URL: TPS basado en las solicitudes de los clientes procedentes de una URL específica.

   b) Umbral fijo. Número máximo de solicitudes permitidas desde un tipo de entrada TPS en un intervalo de tiempo de 1 segundo.

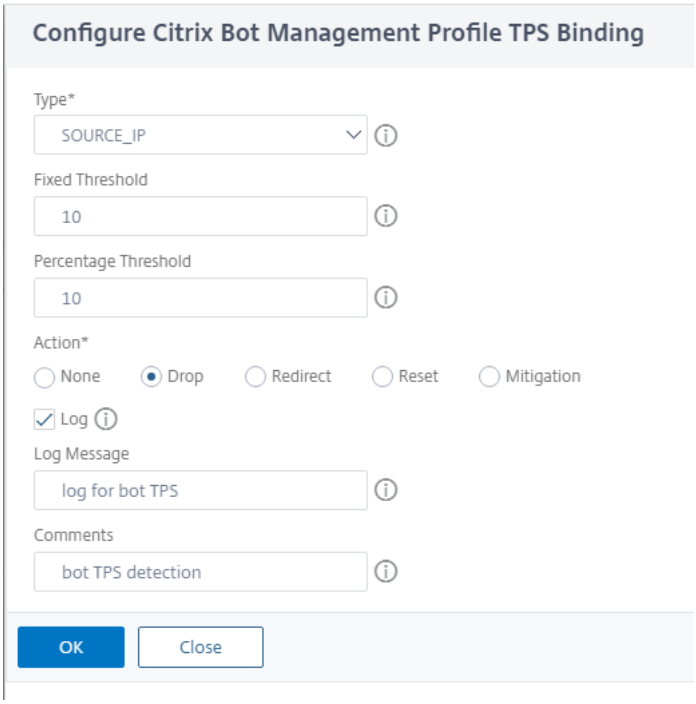
   c) Umbral porcentual. Aumento porcentual máximo de solicitudes de un tipo de entrada TPS en un intervalo de tiempo de 30 minutos.

   d) Acción. Acción que debe tomarse para el bot detectado por el enlace TPS.

   e) Registro. Habilita o inhabilita el registro para el enlace TPS.

   f) Mensaje de registro. Mensaje para registrar el bot detectado por el enlace TPS. Longitud máxima: 255.

   g) Observaciones. Breve descripción de la configuración de TPS. Longitud máxima: 255
6. Haga clic en **Aceptar** y luego en **Cerrar**



Detección de bots basada en la dinámica del ratón y el teclado

Para detectar bots y mitigar las anomalías de raspado web, la administración de bots de Citrix ADC utiliza una técnica de detección de bots mejorada basada en el comportamiento del ratón y el teclado. A diferencia de las técnicas de bots convencionales que requieren interacción humana directa (por ejemplo, validación CAPTCHA), la técnica mejorada monitorea pasivamente la dinámica del ratón y el teclado. A continuación, el dispositivo Citrix ADC recopila los datos del usuario en tiempo real y analiza el comportamiento entre un humano y un bot.

La detección de bots pasivos mediante la dinámica del ratón y el teclado tiene las siguientes ventajas sobre los mecanismos de detección de bots existentes:

- Proporciona supervisión continua durante toda la sesión de usuario y elimina un único punto de control.
- No requiere interacción humana y es transparente para los usuarios.

Cómo funciona la detección de bots mediante la dinámica del ratón y el teclado

La técnica de detección de bots que utiliza la dinámica del teclado y el ratón consta de dos componentes, un registrador de páginas web y un detector de bots. El registrador de páginas web es un JavaScript que registra los movimientos del teclado y del ratón cuando un usuario realiza una tarea en la página web (por ejemplo, rellenando un formulario de registro). A continuación, el registrador envía los datos por lotes al dispositivo Citrix ADC. A continuación, el dispositivo almacena los datos

como registro KM y los envía al detector de bots del servidor Citrix ADM, que analiza si el usuario es humano o bot.

En los siguientes pasos se explica cómo interactúan los componentes entre sí:

1. El administrador de Citrix ADC configura la expresión de directivas mediante el StyleBook de ADM, la CLI o NITRO o cualquier otro método.
2. La URL se establece en el perfil de bot cuando el administrador habilita la función en el dispositivo.
3. Cuando un cliente envía una solicitud, el dispositivo Citrix ADC hace un seguimiento de la sesión y de todas las solicitudes de la sesión.
4. El dispositivo inserta un JavaScript (registrador de páginas web) en la respuesta si la solicitud coincide con la expresión configurada en el perfil de bot.
5. A continuación, JavaScript recopila toda la actividad del teclado y el ratón y envía los datos KM en una URL POST (transitoria).
6. El dispositivo Citrix ADC almacena los datos y los envía al servidor Citrix ADM al final de la sesión. Una vez que el dispositivo recibe los datos completos de una solicitud POST, los datos se envían al servidor ADM.
7. El servicio Citrix ADM analiza los datos y, en función del análisis, el resultado está disponible en la GUI del servicio Citrix ADM.

El registrador de JavaScript registra los siguientes movimientos del ratón y del teclado:

- Eventos de teclado: todos los eventos
- Eventos de ratón: movimiento del ratón, ratón hacia arriba, con el ratón hacia abajo
- Eventos portapapeles - pegar
- Eventos personalizados: autofill, autofillcancel
- marca de hora de cada evento

Configurar la detección de bots mediante la dinámica de ratón y teclado

La configuración de administración de bots de Citrix ADC incluye habilitar o inhabilitar la función de detección basada en teclado y mouse, y configura la URL de JavaScript en el perfil del bot.
Siga los siguientes pasos para configurar la detección de bots mediante la dinámica del ratón y el teclado:

1. Habilitar la detección basada en teclado y ratón
2. Configure la expresión para decidir cuándo se puede inyectar JavaScript en la respuesta HTTP

Habilitar la detección de bots basada en el ratón

Antes de comenzar la configuración, asegúrese de haber habilitado la función de detección de bots basada en teclado y ratón en el dispositivo.

En el símbolo del sistema, escriba:

```
add bot profile <name> -KMDetection ( ON | OFF )
<!--NeedCopy-->
```

Ejemplo:

```
add bot profile profile1 -KMDetection ON
```

Configurar la expresión bot para la inserción de JavaScript

Configure la expresión bot para evaluar el tráfico e insertar JavaScript. El JavaScript se inserta solo si la expresión se evalúa como verdadera.

En el símbolo del sistema, escriba:

```
bind bot profile <name> -KMDetectionExpr -name <string> -expression <
    expression> -enabled ( ON | OFF ) - comment <string>
<!--NeedCopy-->
```

Ejemplo:

```
bind bot profile profile1 -KMDetectionExpr -name test -expression http.req.
url.startswith(”/testsite”)-enabled ON
```

Configurar el nombre de archivo JavaScript insertado en la respuesta HTTP para la detección de bots basada en teclado y ratón

Para recopilar los detalles de la acción del usuario, el dispositivo envía un nombre de archivo JavaScript en la respuesta HTTP. El archivo JavaScript recopila todos los datos de un registro KM y los envía al dispositivo.

En el símbolo del sistema, escriba:

```
set bot profile profile1 - KMJavaScriptName <string>
<!--NeedCopy-->
```

Ejemplo:

```
set bot profile profile1 -KMJavaScriptName script1
```


Configurar el tamaño biométrico del comportamiento

Puede configurar el tamaño máximo de los datos de comportamiento del ratón y el teclado que se pueden enviar como registro KM al dispositivo y procesar en el servidor ADM.

En el símbolo del sistema, escriba:

```
1 set bot profile profile1 -KMEventsPostBodyLimit <positive_integer>
2 <!--NeedCopy-->
```

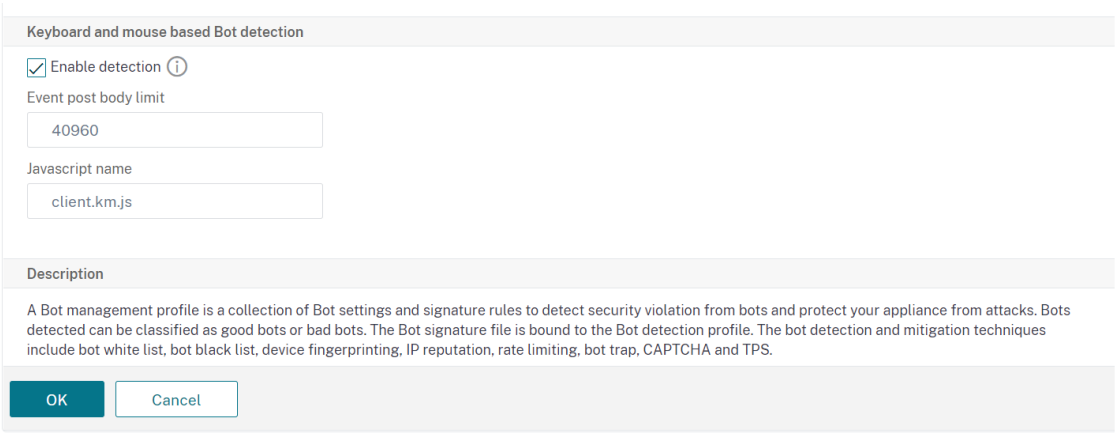
Ejemplo:

```
set bot profile profile1 - KMEventsPostBodyLimit 25
```

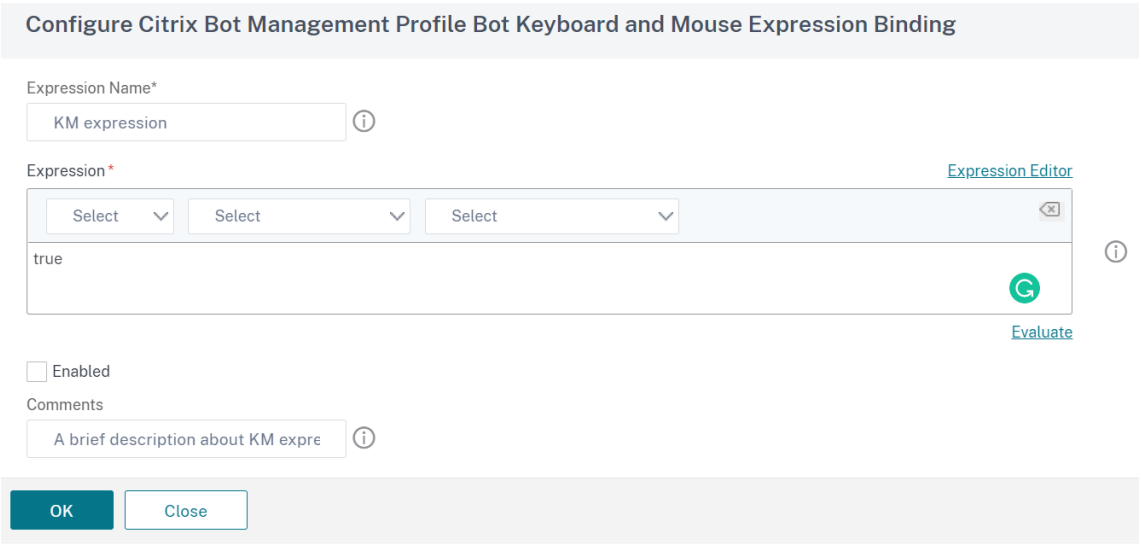
Después de configurar el dispositivo Citrix ADC para configurar JavaScript y recopilar la biometría del comportamiento del teclado y el ratón, el dispositivo envía los datos al servidor Citrix ADM. Para obtener más información sobre cómo el servidor Citrix ADM detecta los bots de la biometría del comportamiento, consulte el tema Infracciones de bots.

Configurar los ajustes de expresión de bot de teclado y ratón mediante la GUI

1. Vaya a **Seguridad > Perfiles y administración de bots de Citrix**.
2. En la página **Perfiles de administración de Bot de Citrix**, seleccione un perfil y haga clic en **Modificar**.
3. En la sección **Detección de bots basada en teclado y ratón**, establezca los siguientes parámetros:
   a) Habilita la detección. Active la casilla de verificación para detectar el comportamiento dinámico del teclado y el ratón basado en bot.
   b) Límite de cuerpo de publicación del evento. Tamaño de los datos dinámicos de teclado y ratón enviados por el explorador para que los procese el dispositivo Citrix ADC.
4. Haga clic en **OK**.



5. En la página **Perfil de administración de bots de Citrix**, vaya a la sección **Configuración del perfil** y haga clic en **Configuración de expresión de bots basada en teclado y ratón**.
6. En la sección **Configuración de expresiones de bot basadas en teclado y ratón**, haga clic en **Agregar**.
7. En la página **Configurar enlace de expresiones de teclado y ratón de Citrix Bot Management Profile Bot Bot**, establezca los siguientes parámetros:
   a) Nombre de expresión. Nombre de la expresión de directiva de bot para la detección de dinámicas de teclado y ratón.
   b) Expresión. Expresión de directiva bot.
   c) Habilitada. Active la casilla de verificación para habilitar el enlace de expresiones del teclado y el teclado y el bot y el ratón.
   d) Observaciones. Breve descripción de la expresión de la directiva de bot y su vinculación al perfil del bot.
   e) Haga clic en **Aceptar** y **cerrar**.
8. En la sección **Configuración de expresiones de bot basadas en teclado y ratón**, haga clic en **Actualizar**.



Registro verboso para el tráfico de bots

Cuando una solicitud entrante se identifica como un bot, el dispositivo Citrix ADC registra más detalles del encabezado HTTP para supervisar y solucionar problemas. La capacidad de registro de bot verbose es similar al registro verboso del módulo Web App Firewall.

Considere el tráfico entrante de un cliente. Si el cliente se identifica como bot, el dispositivo Citrix ADC utiliza la funcionalidad de registro detallada para registrar información completa del encabezado HTTP (como dirección de dominio, URL, encabezado usuario-agente, encabezado de cookie). Los detalles del registro se envían al servidor ADM para supervisar y solucionar problemas del propósito. El mensaje de registro verboso no se almacena en el archivo “ns.log”.

Configurar el registro de bot verbose mediante la CLI

Para capturar información detallada del encabezado HTTP como registros, puede configurar el parámetro de registro detallado en el perfil del bot. En el símbolo del sistema, escriba:

```
1 set bot profile <name> [-verboseLogLevel ( NONE | HTTP_FULL_HEADER ) ]
2 <!--NeedCopy-->
```

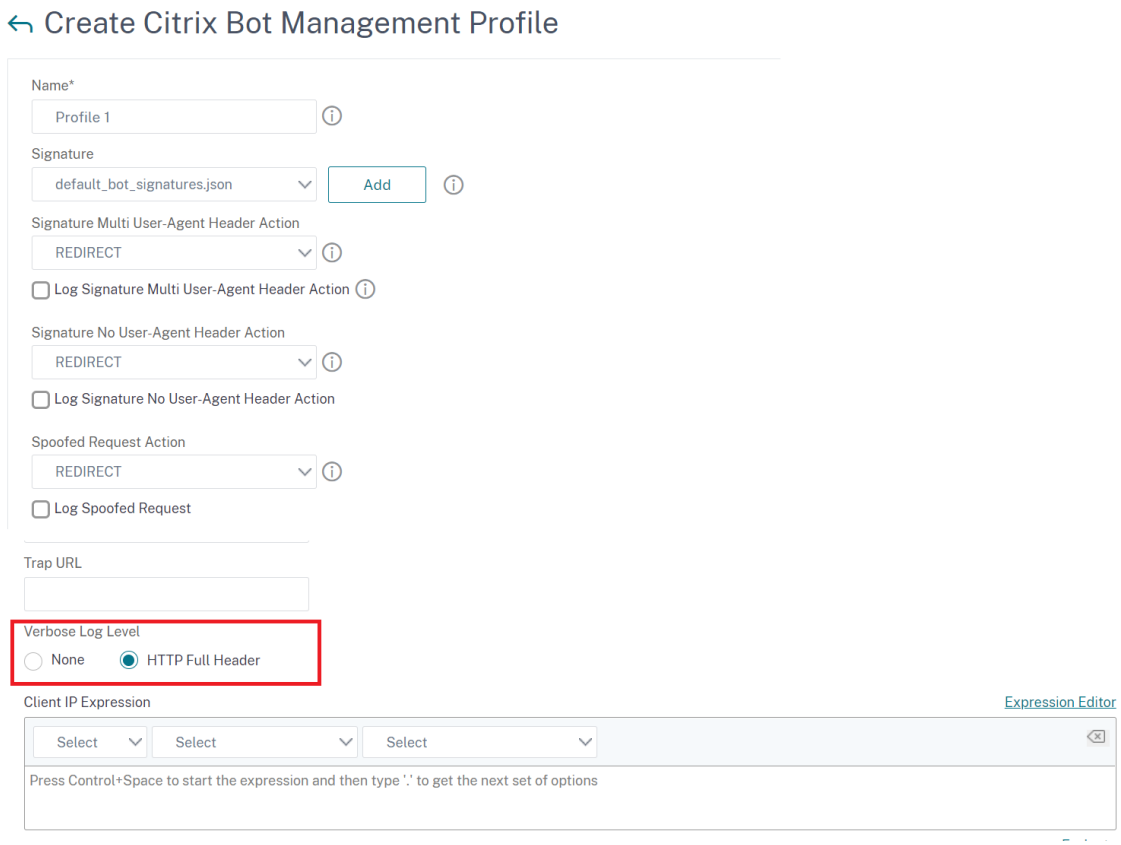
Ejemplo:

```
set bot profile p1 -verboseLogLevel HTTP_FULL_HEADER
```

Configurar el registro de bot verbose mediante la GUI de Citrix ADC

Siga el procedimiento que se indica a continuación para configurar el nivel de registro detallados en el perfil del bot.

1. En el panel de navegación, vaya a **Seguridad > Administración de bots de Citrix**.
2. En la página **Perfiles de administración de bots de Citrix**, haga clic en **Agregar**.
3. En la página **Crear perfil de administración de bots de Citrix**, seleccione el nivel de registro verboso como **Encabezado completo HTTP**.
4. Haga clic en **Aceptar** y **Listo**.



Encabezados de solicitud descartados por Citrix Bot Management

Muchos de los encabezados de solicitud relacionados con el almacenamiento en caché se eliminan para ver cada solicitud en el contexto de una sesión. De manera similar, si la solicitud incluye un encabezado de codificación para permitir que el servidor web envíe respuestas comprimidas, la administración del bot elimina este encabezado para que la administración del bot inspeccione el contenido de la respuesta del servidor sin comprimir para insertar los JavaScript.

La administración de bots elimina los siguientes encabezados de solicitud:

Alcance. Se utiliza para recuperarse de transferencias de archivos fallidas o parciales.

If-Range. Permite a un cliente recuperar un objeto parcial cuando ya contiene una parte de ese objeto en su caché (GET condicional).

Si se modifica desde. Si el objeto solicitado no se modifica desde el momento especificado en este campo, el servidor no devuelve una entidad. Aparece un error HTTP 304 no modificado.

Si no coincide. Permite actualizaciones eficientes de la información almacenada en caché con una cantidad mínima de sobrecarga.

Aceptar-codificación. Qué métodos de codificación se permiten para un objeto en particular, como gzip.

Administración de bots

January 12, 2021

A continuación se presentan algunos de los casos de solución de problemas que se tratan en la administración de bots de Citrix ADC.

1. ¿Cómo manejar casos falsos positivos?

   Puede utilizar la funcionalidad de lista de permitir bot para gestionar casos de falsos positivos y estas transacciones se pueden omitir.

2. ¿Cómo encontrar más detalles sobre el mal tráfico de bots?

   Puede utilizar la funcionalidad de registro de auditoría para obtener detalles sobre el tráfico clasificado como bots defectuosos.

3. ¿Por qué debería cambiar el nombre de firma predeterminado?

   Puede cambiar el nombre de firma predeterminado si se detectan conflictos en los recursos de punto final servidos por el dispositivo Citrix ADC.

Administración de bots

October 5, 2021

1. ¿Qué es la administración de bots de Citrix ADC?

   La administración de bots de Citrix ADC detecta y distingue el tráfico de los bots buenos, los bots malos y los clientes humanos. La funcionalidad de administración de bots protege sus aplicaciones web de los bots maliciosos mediante la aplicación de una acción configurada en las solicitudes entrantes.

2. ¿Por qué Citrix ADC debe administrar los bots de su aplicación web?

Los bots maliciosos constituyen el 30% del tráfico de Internet. Los bots maliciosos afectan a las aplicaciones web de varias maneras, como iniciar un ataque DoS, enviar spam a direcciones de correo electrónico, ralentizar la aplicación mediante programas de descarga, descargar el contenido de sitios web, etc. Además, los bots pueden eludir fácilmente algunos de los mecanismos de detección conocidos que conducen a la pérdida de datos, introduciros y reputación para su organización.

3. ¿Cuáles son las técnicas utilizadas para detectar un bot entrante?

   El dispositivo utiliza técnicas de detección como reputación de IP, limitación de velocidad, huellas digitales del dispositivo, TPS y técnicas de detección de trampas de bots. Además, puede configurar una lista de bloqueo personalizada en la GUI de Citrix ADC para categorizar los bots defectuosos específicos de la organización.

4. ¿Qué es un archivo de firma de bot y su finalidad?

   El archivo de firma del bot contiene la huella de bots buenos y malos conocidos. El archivo de firma se actualiza periódicamente para incluir las firmas de bots más recientes para una mejor protección contra bots.

5. ¿Qué tipo de licencia de Citrix ADC debo adquirir?

   La administración de bots está disponible con la licencia ADC Premium.

6. ¿Dónde puedo encontrar los registros de bots para solucionar problemas?

   Los registros de auditoría de Citrix ADC proporcionan detalles del bot detectados. Para obtener más información, consulte el tema Registro de auditoría .

7. ¿Hay una funcionalidad de actualización automática para los archivos de firma del bot?

   Sí, la administración de bots de Citrix ADC admite la funcionalidad de actualización automática.

8. ¿Existe algún requisito previo para utilizar la técnica de reputación IP del bot?

   Habilite la función de reputación IP antes de habilitar y configurar la reputación IP en el perfil del bot.

Actualización automática de firmas de bots

April 5, 2022

La función de actualización automática de firmas de bots le permite obtener las firmas más recientes que brindan una mejor protección y gestión del tráfico de bots buenos y malos.

Las firmas se actualizan automáticamente cada hora, lo que elimina la necesidad de comprobar constantemente la disponibilidad de la actualización más reciente. Si ha habilitado la función de actual-

ización automática de firmas, el dispositivo Citrix ADC se conecta al servidor que aloja las firmas para comprobar si hay una versión más nueva disponible.

Las firmas de bots más recientes alojadas en la nube de Amazon se configuran como la URL de firma predeterminada para buscar la última actualización. Para que la función de actualización automática funcione, también debe configurar el servidor DNS para que acceda al sitio externo.

Actualizar firmas

Todos los objetos de firma definidos por el usuario que se crean con el objeto de firma predeterminado del bot tienen una versión mayor que cero. Si habilita la actualización automática de firmas, todas las firmas se actualizan automáticamente. Puede actualizar la acción predeterminada para las firmas de bots seleccionando una firma o un grupo de firmas mediante la función de búsqueda en la GUI de administración de bots de Citrix ADC.

URL de actualización de firma de bot: `https://nsbotsignatures.s3.amazonaws.com/BotSignatureMapping.json`

Configurar la actualización automática de firmas

Para habilitar la función Actualización automática de firmas, debe ejecutar el siguiente comando:

En el símbolo del sistema, escriba:

```
1 set bot settings SignatureAutoUpdate ON
2 <!--NeedCopy-->
```

Alerta de firma de bot Artículos

March 9, 2022

Citrix Boot Management anuncia actualizaciones de firmas que puede descargar y aplicar en su dispositivo. Cuando detecte un ataque de bot, recibirá una notificación por correo electrónico sobre la nueva actualización de firma. Puede descargar la firma y aplicarla en el dispositivo.

Para obtener actualizaciones sobre las nuevas firmas de bots, debe configurar la función de actualización automática de firmas. Para obtener más información, consulte el tema Actualización automática de firmas de bots.

Actualización de firma de bots para noviembre de 2020

October 5, 2021

Se generan nuevas reglas de firmas para los bots identificados en la semana del 11 de noviembre de 2020. Puede descargar y configurar estas reglas de firma para proteger su dispositivo de los ataques de bots.

Versión de firma bot

Firma versión 5 aplicable a la plataforma Citrix ADC 13.0.

Nuevas firmas de bot

A continuación se muestra una lista de reglas de firma de bot, categoría y su tipo.

Categoría	Tipo de bot	Número de firmas
raspador	Buen bot	3
Márketing	Buen bot	23
Buscador de alimentación	Buen bot	2
Herramienta	Bot malo	3
Buscador	Buen bot	34
Crawler	Buen bot	6
Sin categoría	Bot malo	6
Analizador de virus	Buen bot	1
Creador de captura de pantalla	Buen bot	7
raspador	Bot malo	1
Herramienta	Buen bot	7

Actualización de firma de bots para enero de 2021

October 5, 2021

Se actualizan algunas de las firmas de bots existentes. Puede descargar y configurar estas reglas de firma para proteger su dispositivo de los ataques de bots.

Versión de firma bot

La firma versión 6 se aplica a las plataformas Citrix ADC con versiones 13.0 61.x o posteriores.

Firmas de bot actualizadas

A continuación se muestra una lista de ID de reglas de firma de bot, categoría y su tipo.

Regla de firma bot	ID	Descripción
143	Crawler	Buen bot
561	raspador	Buen bot
857	Monitor de sitio	Buen bot
892	Monitor de sitio	Bot malo
894	Monitor de sitio	Bot malo
980	raspador	Bot malo
1025	Monitor de sitio	Bot malo
1029	Buscador de alimentación	Bot malo
1030	Creador de captura de pantalla	Bot malo
1034	Herramienta	Bot malo
1039	Márketing	Bot malo
1042	Monitor de sitio	Bot malo
1047	Monitor de sitio	Bot malo
1053	Monitor de sitio	Bot malo
1072	Buscador	Bot malo
1073	Buscador de alimentación	Bot malo
1074	Sin categoría	Bot malo
1078	Creador de captura de pantalla	Bot malo
1109	Márketing	Bot malo
1132	Buscador de alimentación	Bot malo

Regla de firma bot	ID	Descripción
1138	Márketing	Bot malo
1150	Buscador	Bot malo
1164	Buscador	Bot malo
1167	Márketing	Bot malo
1173	Herramienta	Bot malo
1174	Márketing	Bot malo
1176	Buscador	Bot malo
1178	Probador de velocidad	Bot malo
1185	Creador de captura de pantalla	Bot malo
1209	Sin categoría	Bot malo
1244	Monitor de sitio	Bot malo
1251	Buscador	Bot malo
1254	Monitor de sitio	Bot malo
1256	Sin categoría	Bot malo
1259	Herramienta	Bot malo
1287	Buscador	Bot malo
1296	Buscador	Bot malo
1312	Sin categoría	Bot malo
1316	Márketing	Bot malo
1322	Monitor de sitio	Bot malo
1325	Creador de captura de pantalla	Bot malo
1328	Buscador	Bot malo
1330	Márketing	Bot malo
1337	Herramienta	Bot malo
1360	Buscador	Bot malo
1367	Buscador	Bot malo
1374	Herramienta	Bot malo

Regla de firma bot	ID	Descripción
1380	Sin categoría	Bot malo
1388	Buscador	Bot malo
1400	Buscador de alimentación	Bot malo
1413	Sin categoría	Bot malo
1420	Buscador de alimentación	Bot malo
1422	Monitor de sitio	Bot malo
1442	Sin categoría	Bot malo
1447	Buscador	Bot malo
1460	Márketing	Bot malo
1467	Herramienta	Bot malo
1469	Herramienta	Bot malo
1471	Buscador	Bot malo
1484	Sin categoría	Bot malo
1493	Márketing	Bot malo
1502	Monitor de sitio	Bot malo
1504	Sin categoría	Bot malo
1506	Sin categoría	Bot malo
1518	Sin categoría	Bot malo
1520	Buscador	Bot malo
1531	Buscador de alimentación	Bot malo
1533	Sin categoría	Bot malo
1540	Buscador	Bot malo
1556	Márketing	Bot malo
1560	Sin categoría	Bot malo
1564	Herramienta	Bot malo
1570	Monitor de sitio	Bot malo
1575	Buscador	Bot malo
1586	Analizador de virus	Bot malo
1588	Sin categoría	Bot malo

Regla de firma bot	ID	Descripción
1594	Herramienta	Bot malo
1619	Márketing	Bot malo
1623	Herramienta	Bot malo
1626	Buscador	Bot malo
1632	Buscador de alimentación	Bot malo
1648	Buscador	Bot malo
1652	Márketing	Bot malo
1660	Márketing	Bot malo
1713	Herramienta	Bot malo
1719	Buscador	Bot malo
1722	Sin categoría	Bot malo
1744	Sin categoría	Bot malo
1754	Sin categoría	Bot malo
1757	Sin categoría	Bot malo
1762	Sin categoría	Bot malo
1769	Sin categoría	Bot malo
1771	Márketing	Bot malo
1779	Herramienta	Bot malo
1782	Herramienta	Bot malo
1785	Probador de velocidad	Bot malo
1786	Herramienta	Bot malo
1792	Monitor de sitio	Bot malo
1869	Herramienta	Bot malo
1928	Márketing	Bot malo
1942	Monitor de sitio	Bot malo
1949	Márketing	Bot malo
1954	Márketing	Bot malo
1964	Sin categoría	Bot malo
1969	Buscador	Bot malo

Regla de firma bot	ID	Descripción
2294	Buscador	Bot malo
2303	Sin categoría	Bot malo
2308	raspador	Bot malo
2335	Márketing	Bot malo
2374	Sin categoría	Bot malo
2377	Sin categoría	Bot malo
2385	Herramienta	Bot malo
2389	Sin categoría	Bot malo
2414	Sin categoría	Bot malo
2421	Sin categoría	Bot malo
2424	Sin categoría	Bot malo
2427	Sin categoría	Bot malo
2429	Buscador	Bot malo
2437	Sin categoría	Bot malo
2440	Buscador	Bot malo
2443	Sin categoría	Bot malo
2453	Márketing	Bot malo
2472	Márketing	Bot malo
2474	Buscador de alimentación	Bot malo
2482	Sin categoría	Bot malo
2500	Creador de captura de pantalla	Bot malo
2503	Sin categoría	Bot malo
2507	Sin categoría	Bot malo
2516	Herramienta	Bot malo
2536	Márketing	Bot malo
2543	Herramienta	Bot malo
2548	Herramienta	Bot malo
2557	Márketing	Bot malo

Regla de firma bot	ID	Descripción
2561	Sin categoría	Bot malo
2572	Sin categoría	Bot malo
2578	Sin categoría	Bot malo
2584	Sin categoría	Bot malo
2588	Sin categoría	Bot malo
2592	Buscador	Bot malo
2600	Herramienta	Bot malo
2606	Sin categoría	Bot malo
2611	Sin categoría	Bot malo
2622	Herramienta	Bot malo
2625	Herramienta	Bot malo
2631	Herramienta	Bot malo
2635	Herramienta	Bot malo
2637	Creador de captura de pantalla	Bot malo
2641	Buscador	Bot malo
2655	Sin categoría	Bot malo
2657	Márketing	Bot malo
2663	Sin categoría	Bot malo
2666	Herramienta	Bot malo
2672	Buscador de alimentación	Bot malo
2674	Herramienta	Bot malo
2681	Buscador	Bot malo
2684	Márketing	Bot malo
2690	Sin categoría	Bot malo
2704	Sin categoría	Bot malo
2707	Sin categoría	Bot malo
2714	Buscador de alimentación	Bot malo
2722	Sin categoría	Bot malo

Regla de firma bot	ID	Descripción
2726	Buscador de alimentación	Bot malo
2730	Creador de captura de pantalla	Bot malo
2736	Sin categoría	Bot malo
2749	Sin categoría	Bot malo
2753	Herramienta	Bot malo
2756	Herramienta	Bot malo
2760	Probador de velocidad	Bot malo
2780	Herramienta	Bot malo
2785	Monitor de sitio	Bot malo
2789	Sin categoría	Bot malo
2797	Herramienta	Bot malo
2801	Herramienta	Bot malo
2808	Herramienta	Bot malo
2810	Sin categoría	Bot malo
2813	Sin categoría	Bot malo
2816	Sin categoría	Bot malo
2820	Comprobador de vínculos	Bot malo
2824	Comprobador de vínculos	Bot malo
2831	Creador de captura de pantalla	Bot malo
2843	Herramienta	Bot malo
2846	Herramienta	Bot malo
2849	Márketing	Bot malo
2851	Sin categoría	Bot malo
2855	Sin categoría	Bot malo
2859	Herramienta	Bot malo
2873	Sin categoría	Bot malo
2875	Creador de captura de pantalla	Bot malo

Regla de firma bot	ID	Descripción
2879	Sin categoría	Bot malo
2881	Sin categoría	Bot malo
2886	Monitor de sitio	Bot malo
2899	Sin categoría	Bot malo
2916	Sin categoría	Bot malo
2924	Herramienta	Bot malo
2932	Márketing	Bot malo
2935	Comprobador de vínculos	Bot malo
2939	Márketing	Bot malo
2942	Sin categoría	Bot malo
2955	Buscador	Bot malo
2960	Herramienta	Bot malo
2964	Sin categoría	Bot malo
2972	Márketing	Bot malo
2978	Analizador de vulnerabilidades	Bot malo
2980	Herramienta	Bot malo
2985	Márketing	Bot malo
2993	Sin categoría	Bot malo
2999	Creador de captura de pantalla	Bot malo
3003	Buscador de alimentación	Bot malo
3005	Sin categoría	Bot malo
3013	Sin categoría	Bot malo
3016	Sin categoría	Bot malo
3021	Buscador	Bot malo
3026	Sin categoría	Bot malo
3030	Márketing	Bot malo
3065	Márketing	Bot malo

Regla de firma bot	ID	Descripción
3068	Sin categoría	Bot malo
3072	Márketing	Bot malo
3077	Márketing	Bot malo
3080	Sin categoría	Bot malo
3086	raspador	Bot malo
3092	Buscador	Bot malo
3100	Sin categoría	Bot malo
3104	Herramienta	Bot malo
3111	Sin categoría	Bot malo
3116	Monitor de sitio	Bot malo
3118	Herramienta	Bot malo
3120	Márketing	Bot malo
3122	Buscador	Bot malo
3126	Márketing	Bot malo
3141	Herramienta	Bot malo
3143	Sin categoría	Bot malo
3145	raspador	Bot malo
3150	Sin categoría	Bot malo
3173	Comprobador de vínculos	Bot malo
3176	Sin categoría	Bot malo
3186	Probador de velocidad	Bot malo
3190	raspador	Bot malo
3203	Buscador	Bot malo
3216	Sin categoría	Bot malo
3220	Herramienta	Bot malo
3223	Comprobador de vínculos	Bot malo
3241	Sin categoría	Bot malo
3245	Monitor de sitio	Bot malo
3285	Sin categoría	Bot malo

Regla de firma bot	ID	Descripción
3304	Márketing	Bot malo
3307	Comprobador de vínculos	Bot malo
3316	Herramienta	Bot malo
3326	Márketing	Bot malo
3333	Buscador	Bot malo
3340	Buscador	Bot malo
3344	Márketing	Bot malo
3350	Sin categoría	Bot malo
3355	Márketing	Bot malo
3365	Sin categoría	Bot malo
3378	Sin categoría	Bot malo
3388	Herramienta	Bot malo
3396	Sin categoría	Bot malo
3400	Sin categoría	Bot malo
3421	Sin categoría	Bot malo
3439	Sin categoría	Bot malo
3447	Buscador de alimentación	Bot malo
3451	Herramienta	Bot malo
3459	Creador de captura de pantalla	Bot malo
3469	Analizador de vulnerabilidades	Bot malo
3475	Sin categoría	Bot malo
3485	Buscador	Bot malo
3493	Herramienta	Bot malo
3502	Márketing	Bot malo
3507	Buscador	Bot malo
3523	Sin categoría	Bot malo
3535	Probador de velocidad	Bot malo

Regla de firma bot	ID	Descripción
3549	Sin categoría	Bot malo
3556	Sin categoría	Bot malo
3561	Sin categoría	Bot malo
3565	Sin categoría	Bot malo
3572	Buscador	Bot malo
3578	Sin categoría	Bot malo
3610	Buscador	Bot malo
3617	Sin categoría	Bot malo
3621	Márketing	Bot malo
3632	Herramienta	Bot malo
3635	Márketing	Bot malo
3653	Sin categoría	Bot malo
3661	Buscador	Bot malo
3704	Sin categoría	Bot malo
3707	Sin categoría	Bot malo
3711	Sin categoría	Bot malo
3730	Buscador	Bot malo
3740	Monitor de sitio	Bot malo
3759	Buscador	Bot malo
3764	Sin categoría	Bot malo
3770	Sin categoría	Bot malo

Actualización de firma de bots para marzo de 2021

October 5, 2021

Se actualizan algunas de las firmas de bots existentes. Puede descargar y configurar estas reglas de firma para proteger su dispositivo de los ataques de bots.

Versión de firma bot

La firma versión 7 se aplica a las plataformas Citrix ADC con versiones 13.0 61.x o posteriores.

Firmas de bot actualizadas

A continuación se muestra una lista de ID de reglas de firma de bot, categoría y su tipo.

Regla de firma bot	ID	Descripción
278	raspador	Buen bot
378	raspador	Buen bot
379	raspador	Buen bot
380	raspador	Buen bot
381	raspador	Buen bot
382	raspador	Buen bot
383	raspador	Buen bot
384	raspador	Buen bot
385	raspador	Buen bot
386	raspador	Buen bot
387	raspador	Buen bot
389	raspador	Buen bot
390	raspador	Buen bot
391	raspador	Buen bot
494	raspador	Buen bot
627	Buscador	Buen bot
660	Buscador	Buen bot
3840	Crawler	Buen bot

Actualización de firma de bots para agosto de 2021

October 5, 2021

Se agregan nuevas firmas y se actualizan algunas de las firmas de bots existentes. Puede descargar y

configurar estas reglas de firma para proteger su dispositivo de los ataques de bots.

Versión de firma bot

La firma versión 8 se aplica a las plataformas Citrix ADC con versiones 13.0 61.x o posteriores.

Firmas de bot actualizadas

A continuación se muestra una lista de ID de reglas de firma de bot, categoría y su tipo.

Regla de firma bot	ID	Descripción
236	raspador	Buen bot
378	raspador	Buen bot
381	raspador	Buen bot
382	raspador	Buen bot
390	raspador	Buen bot
544	raspador	Buen bot
702	Buscador	Buen bot
979	raspador	Bot malo
3791	Probador de velocidad	Buen bot
3797	Márketing	Buen bot
3800	Márketing	Buen bot
3824	Crawler	Bot malo
3833	Buscador	Buen bot
3849	Crawler	Buen bot
3871	Márketing	Buen bot
3963	Márketing	Buen bot
4027	Buscador	Buen bot

Nueva firma bot

Regla de firma bot	ID	Descripción
4028	Márketing	Buen bot

Regla de firma bot	ID	Descripción
4029	Herramienta	Buen bot
4030	raspador	Buen bot
4031	raspador	Buen bot
4032	Sin categoría	Bot malo
4033	Crawler	Buen bot
4034	Crawler	Buen bot
4035	Márketing	Buen bot
4036	Analizador de vulnerabilidades	Buen bot
4037	Analizador de vulnerabilidades	Buen bot
4038	Sin categoría	Bot malo
4039	Herramienta	Buen bot
4040	Crawler	Buen bot
4041	Herramienta	Buen bot
4042	Crawler	Buen bot
4043	Creador de captura de pantalla	Buen bot
4044	raspador	Bot malo
4045	raspador	Bot malo
4046	raspador	Bot malo
4047	Sin categoría	Bot malo
4048	Buscador de alimentación	Buen bot
4049	Sin categoría	Bot malo
4050	Crawler	Buen bot
4051	Crawler	Buen bot
4052	Herramienta	Buen bot
4053	Herramienta	Buen bot
4054	raspador	Bot malo
4055	Sin categoría	Buen bot

Regla de firma bot	ID	Descripción
4056	Márketing	Buen bot
4057	Creador de captura de pantalla	Buen bot
4058	Crawler	Buen bot
4059	Sin categoría	Bot malo
4060	Buscador	Buen bot
4061	Buscador	Buen bot
4062	Buscador	Buen bot
4063	Buscador	Buen bot
4064	Herramienta	Buen bot
4065	raspador	Buen bot
4066	Márketing	Buen bot
4067	Márketing	Buen bot
4068	Sin categoría	Bot malo
4069	Sin categoría	Bot malo
4070	Sin categoría	Bot malo
4071	Herramienta	Buen bot
4072	Herramienta	Bot malo
4073	Sin categoría	Bot malo
4074	Sin categoría	Bot malo
4075	Herramienta	Bot malo
4076	Márketing	Buen bot
4077	raspador	Buen bot
4078	Crawler	Buen bot
4079	Crawler	Buen bot
4080	Herramienta	Bot malo
4081	Buscador	Buen bot
4082	Herramienta	Buen bot
4083	Sin categoría	Bot malo

Regla de firma bot	ID	Descripción
4084	Sin categoría	Bot malo
4085	Herramienta	Buen bot
4086	Herramienta	Buen bot
4087	Herramienta	Bot malo
4088	Buscador	Buen bot
4089	Márketing	Buen bot
4090	Herramienta	Buen bot
4091	Herramienta	Buen bot
4092	Herramienta	Buen bot
4093	Herramienta	Buen bot
4094	Sin categoría	Buen bot
4095	Monitor de sitio	Buen bot
4096	Monitor de sitio	Buen bot
4097	Monitor de sitio	Buen bot
4098	Crawler	Buen bot
4099	Buscador	Buen bot
4100	Buscador	Buen bot
4101	Buscador	Buen bot
4102	Buscador	Buen bot
4103	Márketing	Buen bot
4104	Márketing	Buen bot
4105	Márketing	Buen bot
4106	Márketing	Buen bot
4107	Márketing	Buen bot
4108	Márketing	Buen bot
4109	Buscador	Buen bot
4110	Crawler	Buen bot
4111	Crawler	Buen bot
4112	Crawler	Buen bot

Regla de firma bot	ID	Descripción
4113	Analizador de vulnerabilidades	Buen bot
4114	Crawler	Buen bot
4115	Herramienta	Buen bot
4116	Sin categoría	Bot malo
4117	Sin categoría	Bot malo
4118	Sin categoría	Bot malo
4119	Sin categoría	Bot malo
4120	Márketing	Buen bot
4121	Márketing	Buen bot
4122	Márketing	Buen bot
4123	Márketing	Buen bot
4124	Márketing	Buen bot
4125	Márketing	Buen bot
4126	Márketing	Buen bot
4127	Márketing	Buen bot
4128	Márketing	Buen bot
4129	Márketing	Buen bot
4130	Márketing	Buen bot
4131	Herramienta	Buen bot
4132	Márketing	Buen bot
4133	Márketing	Buen bot
4134	Herramienta	Buen bot
4135	Márketing	Buen bot
4136	Márketing	Buen bot
4137	Márketing	Buen bot
4138	Márketing	Buen bot
4139	Márketing	Buen bot
4140	Márketing	Buen bot

Regla de firma bot	ID	Descripción
4141	Márketing	Buen bot
4142	Márketing	Buen bot
4143	Márketing	Buen bot
4144	Márketing	Buen bot
4145	Buscador	Buen bot
4146	Buscador	Buen bot
4147	Buscador	Buen bot
4148	Buscador	Buen bot
4149	Buscador	Buen bot
4150	Buscador	Buen bot
4151	Buscador	Buen bot
4152	Buscador	Buen bot
4153	Buscador	Buen bot
4154	Buscador	Buen bot
4155	Buscador	Buen bot
4156	Creador de captura de pantalla	Buen bot
4157	Buscador	Buen bot
4158	Buscador	Buen bot
4159	Buscador	Buen bot
4160	Creador de captura de pantalla	Buen bot
4161	Buscador	Buen bot
4162	Buscador	Buen bot
4163	Herramienta	Buen bot
4164	Buscador	Buen bot
4165	Márketing	Buen bot
4166	Sin categoría	Bot malo
4167	Herramienta	Bot malo

Regla de firma bot	ID	Descripción
4168	Probador de velocidad	Buen bot
4169	raspador	Bot malo
4170	Herramienta	Buen bot
4171	raspador	Bot malo
4172	Web Crawler	Buen bot
4173	Herramienta	Buen bot
4174	Crawler	Buen bot
4175	Crawler	Buen bot
4176	Herramienta	Buen bot
4177	Buscador	Buen bot
4178	Herramienta	Buen bot
4179	Web Crawler	Buen bot
4180	Herramienta	Buen bot
4181	Monitor de sitio	Buen bot
4182	Monitor de sitio	Buen bot
4183	Monitor de sitio	Buen bot
4184	Monitor de sitio	Buen bot
4185	Buscador	Buen bot
4186	Herramienta	Buen bot
4187	Herramienta	Buen bot
4188	Creador de captura de pantalla	Buen bot
4189	Márketing	Buen bot
4190	Buscador	Buen bot
4191	Buscador	Buen bot
4192	Buscador	Buen bot
4193	Buscador	Buen bot
4194	Herramienta	Buen bot
4195	Buscador	Bot malo

Regla de firma bot	ID	Descripción
4196	Herramienta	Buen bot
4197	Herramienta	Buen bot
4198	Márketing	Buen bot
4199	Márketing	Buen bot
4200	Analizador de vulnerabilidades	Buen bot
4201	Herramienta	Buen bot
4202	Herramienta	Buen bot
4203	Sin categoría	Bot malo
4204	Sin categoría	Bot malo
4205	Buscador	Buen bot
4206	Márketing	Buen bot
4207	Márketing	Buen bot
4208	Buscador	Buen bot
4209	Buscador	Buen bot
4210	Probador de velocidad	Buen bot
4211	Herramienta	Buen bot
4212	Buscador de alimentación	Buen bot
4213	Buscador de alimentación	Buen bot
4214	raspador	Bot malo
4215	Herramienta	Buen bot
4216	Herramienta	Buen bot
4217	Herramienta	Bot malo
4218	raspador	Bot malo
4219	Márketing	Buen bot
4220	Herramienta	Buen bot
4221	Herramienta	Bot malo
4222	Monitor de sitio	Buen bot
4223	Márketing	Buen bot

Regla de firma bot	ID	Descripción
4224	Buscador	Buen bot
4225	Buscador	Buen bot
4226	Buscador	Buen bot
4227	Márketing	Buen bot
4228	Márketing	Buen bot
4229	Herramienta	Buen bot
4230	Sin categoría	Bot malo
4231	Creador de captura de pantalla	Buen bot
4232	Herramienta	Buen bot
4233	Monitor de sitio	Buen bot
4234	Monitor de sitio	Buen bot
4235	Monitor de sitio	Buen bot
4236	Monitor de sitio	Buen bot
4237	Monitor de sitio	Buen bot
4238	Monitor de sitio	Buen bot
4239	Sin categoría	Bot malo
4240	Márketing	Buen bot
4241	Márketing	Buen bot
4242	Márketing	Buen bot
4243	Márketing	Buen bot
4244	Márketing	Buen bot
4245	Márketing	Buen bot
4246	Márketing	Buen bot
4247	Buscador	Buen bot
4248	Buscador	Buen bot
4249	Creador de captura de pantalla	Buen bot
4250	Buscador	Buen bot

Regla de firma bot	ID	Descripción
4251	Buscador	Buen bot
4252	Crawler	Buen bot
4253	Crawler	Buen bot
4254	Crawler	Buen bot
4255	Herramienta	Buen bot
4256	Sin categoría	Buen bot
4257	Herramienta	Buen bot
4258	Crawler	Buen bot
4259	Crawler	Buen bot
4260	Herramienta	Buen bot
4261	Herramienta	Buen bot
4262	Herramienta	Buen bot
4263	Márketing	Buen bot
4264	Crawler	Bot malo
4265	Buscador	Buen bot
4266	Sin categoría	Buen bot
4267	Herramienta	Buen bot
4268	Herramienta	Buen bot
4269	Buscador	Buen bot
4270	Buscador	Buen bot
4271	Buscador	Buen bot
4272	Buscador	Buen bot
4273	Buscador	Buen bot
4274	Buscador	Buen bot
4275	Buscador	Buen bot
4276	Sin categoría	Bot malo
4277	Sin categoría	Bot malo
4278	Sin categoría	Bot malo
4279	Márketing	Buen bot

Regla de firma bot	ID	Descripción
4280	Crawler	Buen bot
4281	Sin categoría	Bot malo
4282	Márketing	Buen bot
4283	Márketing	Buen bot
4284	Márketing	Buen bot
4285	Márketing	Buen bot
4286	Márketing	Buen bot
4287	Márketing	Buen bot
4288	Márketing	Buen bot
4289	Márketing	Buen bot
4290	Márketing	Buen bot
4291	Márketing	Buen bot
4292	Márketing	Buen bot
4293	Márketing	Buen bot
4294	Márketing	Buen bot
4295	Buscador	Buen bot
4296	Buscador	Buen bot
4297	Buscador	Buen bot
4298	Buscador	Buen bot
4299	Buscador	Buen bot
4300	Buscador	Buen bot
4301	Buscador	Buen bot
4302	Buscador	Buen bot
4303	Buscador	Buen bot
4304	Buscador	Buen bot
4305	Buscador	Buen bot
4306	Creador de captura de pantalla	Buen bot
4307	Buscador	Buen bot

Regla de firma bot	ID	Descripción
4308	Buscador	Buen bot
4309	Buscador	Buen bot
4310	Buscador	Buen bot
4311	Creador de captura de pantalla	Buen bot
4312	Buscador	Buen bot
4313	Buscador	Buen bot
4314	Buscador	Buen bot
4315	Buscador	Buen bot
4316	Buscador	Buen bot
4317	Buscador	Buen bot
4318	Creador de captura de pantalla	Buen bot
4319	Creador de captura de pantalla	Buen bot
4320	Sin categoría	Bot malo
4321	Sin categoría	Buen bot
4322	Crawler	Buen bot
4323	Herramienta	Buen bot
4324	Herramienta	Buen bot
4325	Herramienta	Buen bot
4326	raspador	Bot malo
4327	Buscador	Buen bot
4328	Márketing	Buen bot
4329	Sin categoría	Bot malo
4330	Monitor de sitio	Buen bot
4331	Buscador	Buen bot
4332	Buscador	Buen bot
4333	Sin categoría	Bot malo
4334	raspador	Buen bot

Regla de firma bot	ID	Descripción
4335	Márketing	Buen bot
4336	Márketing	Buen bot
4337	Herramienta	Buen bot
4338	Herramienta	Buen bot
4339	Herramienta	Buen bot
4340	Crawler	Buen bot
4341	Crawler	Buen bot
4342	Analizador de vulnerabilidades	Buen bot
4343	Analizador de vulnerabilidades	Buen bot
4344	raspador	Buen bot
4345	Márketing	Buen bot
4346	Márketing	Buen bot
4347	Márketing	Buen bot
4348	Márketing	Buen bot
4349	Márketing	Buen bot
4350	Márketing	Buen bot
4351	Márketing	Buen bot
4352	Márketing	Buen bot
4353	Márketing	Buen bot
4354	Márketing	Buen bot
4355	Buscador	Buen bot
4356	Buscador	Buen bot
4357	Buscador	Buen bot
4358	Buscador	Buen bot
4359	Buscador	Buen bot
4360	Buscador	Buen bot
4361	Buscador	Buen bot

Regla de firma bot	ID	Descripción
4362	Buscador	Buen bot
4363	Buscador	Buen bot
4364	Buscador	Buen bot
4365	Creador de captura de pantalla	Buen bot
4366	Buscador	Buen bot
4367	Buscador	Buen bot
4368	Buscador	Buen bot
4369	Buscador	Buen bot
4370	Creador de captura de pantalla	Buen bot
4371	Buscador	Buen bot
4372	Buscador	Buen bot
4373	Buscador	Buen bot
4374	Buscador	Buen bot
4375	Buscador	Buen bot
4376	Creador de captura de pantalla	Buen bot
4377	Crawler	Buen bot
4378	Crawler	Buen bot
4379	Buscador	Buen bot
4380	Buscador	Buen bot
4381	Buscador	Buen bot
4382	Buscador	Buen bot
4383	Crawler	Buen bot
4384	Buscador	Buen bot
4385	Herramienta	Buen bot
4386	Sin categoría	Buen bot
4387	Crawler	Buen bot
4388	Crawler	Buen bot

Regla de firma bot	ID	Descripción
4389	Herramienta	Buen bot
4390	Herramienta	Buen bot
4391	Herramienta	Buen bot
4392	Herramienta	Buen bot
4393	Herramienta	Buen bot
4394	Sin categoría	Buen bot
4395	Herramienta	Buen bot
4396	Monitor de sitio	Buen bot
4397	Monitor de sitio	Buen bot
4398	Herramienta	Bot malo
4399	Herramienta	Bot malo
4400	Herramienta	Bot malo
4401	Herramienta	Bot malo
4402	Herramienta	Bot malo
4403	Herramienta	Bot malo
4404	Buscador	Buen bot
4405	Buscador	Buen bot
4406	Buscador	Buen bot
4407	Sin categoría	Buen bot

Actualización de firmas de bots para septiembre de 2021

January 31, 2022

Se agregan nuevas firmas y se actualizan algunas de las firmas de bots existentes. Puede descargar y configurar estas reglas de firma para proteger su dispositivo de los ataques de bots.

Versión de firma bot

Firma versión 9 aplicable a plataformas Citrix ADC con compilaciones 13.0 61.48 o posteriores.

Firmas de bot actualizadas

A continuación se muestra una lista de ID de reglas de firma de bot, categoría y su tipo.

Regla de firma bot	ID	Descripción
2	Crawler	Buen bot
5	Crawler	Buen bot
9	Crawler	Buen bot
45	Crawler	Buen bot
46	Crawler	Buen bot
48	Crawler	Buen bot
52	Crawler	Buen bot
60	Crawler	Buen bot
61	Crawler	Buen bot
63	Crawler	Buen bot
67	Crawler	Buen bot
71	Crawler	Buen bot
74	Crawler	Buen bot
75	Crawler	Buen bot
76	Crawler	Buen bot
78	Crawler	Buen bot
79	Crawler	Buen bot
80	Crawler	Buen bot
81	Crawler	Buen bot
82	Crawler	Buen bot
83	Crawler	Buen bot
84	Crawler	Buen bot
87	Crawler	Buen bot
90	Crawler	Buen bot
95	Crawler	Buen bot
96	Crawler	Buen bot
97	Crawler	Buen bot

Regla de firma bot	ID	Descripción
100	Crawler	Buen bot
101	Crawler	Buen bot
102	Crawler	Buen bot
103	Crawler	Buen bot
104	Crawler	Buen bot
107	Crawler	Buen bot
108	Crawler	Buen bot
110	Crawler	Buen bot
111	Crawler	Buen bot
114	Crawler	Buen bot
115	Crawler	Buen bot
123	Crawler	Buen bot
135	Crawler	Buen bot
136	Crawler	Buen bot
137	Crawler	Buen bot
140	Crawler	Buen bot
141	Crawler	Buen bot
143	Crawler	Buen bot
144	Crawler	Buen bot
145	Crawler	Buen bot
146	Crawler	Buen bot
147	Crawler	Buen bot
149	Crawler	Buen bot
152	Crawler	Buen bot
155	Crawler	Buen bot
156	Crawler	Buen bot
157	Crawler	Buen bot
158	Crawler	Buen bot
159	Crawler	Buen bot

Regla de firma bot	ID	Descripción
160	Crawler	Buen bot
161	Crawler	Buen bot
162	Crawler	Buen bot
163	Crawler	Buen bot
164	Crawler	Buen bot
165	Crawler	Buen bot
166	Crawler	Buen bot
167	Crawler	Buen bot
172	Crawler	Buen bot
173	Crawler	Buen bot
174	Crawler	Buen bot
176	Crawler	Buen bot
177	Crawler	Buen bot
180	Crawler	Buen bot
187	Crawler	Buen bot
197	Crawler	Buen bot
201	Crawler	Buen bot
202	Crawler	Buen bot
203	Crawler	Buen bot
206	Crawler	Buen bot
211	Buscador de alimentación	Bot malo
217	Buscador de alimentación	Buen bot
219	Buscador de alimentación	Buen bot
229	raspador	Buen bot
235	raspador	Buen bot
236	raspador	Buen bot
237	raspador	Buen bot
248	raspador	Buen bot
250	raspador	Buen bot

Regla de firma bot	ID	Descripción
260	raspador	Buen bot
263	raspador	Buen bot
265	raspador	Buen bot
267	raspador	Buen bot
268	raspador	Buen bot
271	raspador	Buen bot
272	raspador	Buen bot
276	raspador	Buen bot
277	raspador	Buen bot
278	raspador	Buen bot
279	raspador	Buen bot
280	raspador	Buen bot
281	raspador	Buen bot
283	raspador	Buen bot
285	raspador	Buen bot
286	raspador	Buen bot
287	raspador	Buen bot
290	raspador	Buen bot
292	raspador	Buen bot
293	raspador	Buen bot
342	raspador	Buen bot
343	raspador	Buen bot
344	raspador	Buen bot
355	raspador	Buen bot
357	raspador	Buen bot
360	raspador	Buen bot
362	raspador	Buen bot
366	raspador	Buen bot
370	raspador	Buen bot

Regla de firma bot	ID	Descripción
371	raspador	Buen bot
372	raspador	Buen bot
373	raspador	Buen bot
374	raspador	Buen bot
376	raspador	Buen bot
377	raspador	Buen bot
380	raspador	Buen bot
392	raspador	Buen bot
393	raspador	Buen bot
394	raspador	Buen bot
396	raspador	Buen bot
397	raspador	Buen bot
414	raspador	Buen bot
418	raspador	Buen bot
419	raspador	Buen bot
421	raspador	Buen bot
422	raspador	Buen bot
423	raspador	Buen bot
424	raspador	Buen bot
425	raspador	Buen bot
426	raspador	Buen bot
427	raspador	Buen bot
428	raspador	Buen bot
430	raspador	Buen bot
432	raspador	Buen bot
433	raspador	Buen bot
434	raspador	Buen bot
435	raspador	Buen bot
441	raspador	Buen bot

Regla de firma bot	ID	Descripción
445	raspador	Buen bot
446	raspador	Buen bot
451	raspador	Buen bot
452	raspador	Buen bot
454	raspador	Buen bot
455	raspador	Buen bot
456	raspador	Buen bot
457	raspador	Buen bot
458	raspador	Buen bot
461	raspador	Buen bot
465	raspador	Buen bot
466	raspador	Buen bot
469	raspador	Buen bot
473	raspador	Buen bot
474	raspador	Buen bot
476	raspador	Buen bot
477	raspador	Buen bot
484	raspador	Buen bot
485	raspador	Buen bot
487	raspador	Buen bot
488	raspador	Buen bot
489	raspador	Buen bot
490	raspador	Buen bot
493	raspador	Buen bot
494	raspador	Buen bot
495	raspador	Buen bot
497	raspador	Buen bot
498	raspador	Buen bot
499	raspador	Buen bot

Regla de firma bot	ID	Descripción
500	raspador	Buen bot
505	raspador	Buen bot
506	raspador	Buen bot
507	raspador	Buen bot
512	raspador	Buen bot
513	raspador	Buen bot
514	raspador	Buen bot
527	raspador	Buen bot
533	raspador	Buen bot
539	raspador	Buen bot
540	raspador	Buen bot
542	raspador	Buen bot
544	raspador	Buen bot
545	raspador	Buen bot
546	raspador	Buen bot
547	raspador	Buen bot
548	raspador	Buen bot
551	raspador	Buen bot
552	raspador	Buen bot
554	raspador	Buen bot
556	raspador	Buen bot
558	raspador	Buen bot
560	raspador	Buen bot
561	raspador	Buen bot
566	raspador	Buen bot
575	raspador	Buen bot
578	raspador	Buen bot
581	raspador	Buen bot
591	raspador	Buen bot

Regla de firma bot	ID	Descripción
593	raspador	Buen bot
595	raspador	Buen bot
600	raspador	Buen bot
601	raspador	Buen bot
602	raspador	Buen bot
604	raspador	Buen bot
605	raspador	Buen bot
609	raspador	Buen bot
610	raspador	Buen bot
611	raspador	Buen bot
612	raspador	Buen bot
613	raspador	Buen bot
615	raspador	Buen bot
620	Buscador	Buen bot
622	Buscador	Buen bot
623	Buscador	Buen bot
624	Buscador	Buen bot
626	Buscador	Buen bot
627	Buscador	Buen bot
628	Buscador	Buen bot
629	Buscador	Buen bot
633	Buscador	Buen bot
634	Buscador	Buen bot
636	Buscador	Buen bot
637	Buscador	Buen bot
639	Buscador	Buen bot
640	Buscador	Buen bot
641	Buscador	Buen bot
642	Buscador	Buen bot

Regla de firma bot	ID	Descripción
643	Buscador	Buen bot
647	Buscador	Buen bot
649	Buscador	Buen bot
650	Buscador	Buen bot
651	Buscador	Buen bot
654	Buscador	Buen bot
656	Buscador	Buen bot
657	Buscador	Buen bot
658	Buscador	Buen bot
659	Buscador	Buen bot
660	Buscador	Buen bot
663	Buscador	Buen bot
664	Buscador	Buen bot
665	Buscador	Buen bot
666	Buscador	Buen bot
667	Buscador	Buen bot
669	Buscador	Buen bot
670	Buscador	Buen bot
671	Buscador	Buen bot
672	Buscador	Buen bot
673	Buscador	Buen bot
674	Buscador	Buen bot
675	Buscador	Buen bot
676	Buscador	Buen bot
677	Buscador	Buen bot
679	Buscador	Buen bot
680	Buscador	Buen bot
690	Buscador	Buen bot
693	Buscador	Buen bot

Regla de firma bot	ID	Descripción
694	Buscador	Buen bot
697	Buscador	Buen bot
698	Buscador	Buen bot
703	Buscador	Buen bot
706	Buscador	Buen bot
712	Buscador	Buen bot
714	Buscador	Buen bot
715	Buscador	Buen bot
716	Buscador	Buen bot
721	Buscador	Buen bot
723	Buscador	Buen bot
725	Buscador	Buen bot
727	Buscador	Buen bot
728	Buscador	Buen bot
729	Buscador	Buen bot
730	Buscador	Buen bot
731	Buscador	Buen bot
732	Buscador	Buen bot
735	Buscador	Buen bot
736	Buscador	Buen bot
740	Buscador	Buen bot
748	Buscador	Buen bot
749	Buscador	Buen bot
750	Buscador	Buen bot
751	Buscador	Buen bot
756	Buscador	Buen bot
757	Buscador	Buen bot
758	Buscador	Buen bot
759	Buscador	Buen bot

Regla de firma bot	ID	Descripción
760	Buscador	Buen bot
761	Buscador	Buen bot
762	Buscador	Buen bot
763	Buscador	Buen bot
764	Buscador	Buen bot
765	Buscador	Buen bot
766	Buscador	Buen bot
767	Buscador	Buen bot
768	Buscador	Buen bot
769	Buscador	Buen bot
770	Buscador	Buen bot
771	Buscador	Buen bot
772	Buscador	Buen bot
773	Buscador	Buen bot
776	Buscador	Buen bot
777	Buscador	Buen bot
780	Buscador	Buen bot
781	Buscador	Buen bot
784	Buscador	Buen bot
786	Buscador	Buen bot
787	Buscador	Buen bot
788	Buscador	Buen bot
789	Buscador	Buen bot
790	Buscador	Buen bot
791	Buscador	Buen bot
792	Buscador	Buen bot
795	Buscador	Buen bot
796	Buscador	Buen bot
798	Buscador	Buen bot

Regla de firma bot	ID	Descripción
800	Buscador	Buen bot
801	Buscador	Buen bot
802	Buscador	Buen bot
803	Buscador	Buen bot
805	Buscador	Buen bot
806	Buscador	Buen bot
807	Buscador	Buen bot
809	Buscador	Buen bot
810	Buscador	Buen bot
811	Buscador	Buen bot
812	Buscador	Buen bot
814	Buscador	Buen bot
815	Buscador	Buen bot
816	Buscador	Buen bot
817	Buscador	Buen bot
818	Buscador	Buen bot
819	Buscador	Buen bot
820	Buscador	Buen bot
821	Buscador	Buen bot
822	Buscador	Buen bot
823	Buscador	Buen bot
825	Buscador	Buen bot
827	Buscador	Buen bot
830	Buscador	Buen bot
831	Buscador	Buen bot
834	Buscador	Buen bot
837	Buscador	Buen bot
838	Buscador	Buen bot
849	Monitor de sitio	Buen bot

Regla de firma bot	ID	Descripción
850	Monitor de sitio	Buen bot
851	Monitor de sitio	Buen bot
853	Monitor de sitio	Buen bot
857	Monitor de sitio	Buen bot
858	Monitor de sitio	Buen bot
859	Monitor de sitio	Buen bot
860	Monitor de sitio	Buen bot
861	Monitor de sitio	Buen bot
862	Monitor de sitio	Buen bot
863	Monitor de sitio	Buen bot
864	Monitor de sitio	Buen bot
865	Monitor de sitio	Buen bot
866	Monitor de sitio	Buen bot
867	Monitor de sitio	Buen bot
868	Monitor de sitio	Buen bot
869	Monitor de sitio	Buen bot
870	Monitor de sitio	Buen bot
871	Monitor de sitio	Buen bot
872	Monitor de sitio	Buen bot
873	Monitor de sitio	Buen bot
874	Monitor de sitio	Buen bot
875	Monitor de sitio	Buen bot
876	Monitor de sitio	Buen bot
877	Monitor de sitio	Buen bot
880	Monitor de sitio	Buen bot
883	Monitor de sitio	Buen bot
885	Monitor de sitio	Buen bot
886	Monitor de sitio	Buen bot
888	Monitor de sitio	Buen bot

Regla de firma bot	ID	Descripción
889	Monitor de sitio	Buen bot
895	Monitor de sitio	Buen bot
896	Monitor de sitio	Buen bot
897	Monitor de sitio	Buen bot
898	Monitor de sitio	Buen bot
900	Monitor de sitio	Buen bot
901	Monitor de sitio	Buen bot
904	Monitor de sitio	Buen bot
906	Monitor de sitio	Buen bot
908	Monitor de sitio	Buen bot
909	Monitor de sitio	Buen bot
910	Monitor de sitio	Buen bot
911	Monitor de sitio	Buen bot
912	Monitor de sitio	Buen bot
913	Monitor de sitio	Buen bot
917	Monitor de sitio	Buen bot
918	Monitor de sitio	Buen bot
919	Monitor de sitio	Buen bot
920	Monitor de sitio	Buen bot
921	Monitor de sitio	Buen bot
924	Monitor de sitio	Buen bot
926	Monitor de sitio	Buen bot
927	Monitor de sitio	Buen bot
928	Monitor de sitio	Buen bot
929	Monitor de sitio	Buen bot
930	Monitor de sitio	Buen bot
931	Monitor de sitio	Buen bot
938	Monitor de sitio	Buen bot
939	Monitor de sitio	Buen bot

Regla de firma bot	ID	Descripción
943	Monitor de sitio	Bot malo
958	Monitor de sitio	Buen bot
959	Monitor de sitio	Buen bot
960	Monitor de sitio	Buen bot
963	Monitor de sitio	Buen bot
984	raspador	Buen bot
996	raspador	Buen bot
997	raspador	Buen bot
998	raspador	Buen bot
1002	raspador	Buen bot
1006	raspador	Buen bot
1588	Sin categoría	Bot malo
2561	raspador	Bot malo
2810	Crawler	Buen bot
3782	Márketing	Buen bot
3783	Buscador	Buen bot
3788	Herramienta	Buen bot
3789	Herramienta	Buen bot
3790	Crawler	Buen bot
3792	Herramienta	Buen bot
3793	Herramienta	Buen bot
3794	Crawler	Buen bot
3796	raspador	Buen bot
3798	Márketing	Buen bot
3799	Márketing	Buen bot
3801	Márketing	Buen bot
3802	Creador de captura de pantalla	Buen bot
3803	Buscador	Buen bot

Regla de firma bot	ID	Descripción
3804	Creador de captura de pantalla	Buen bot
3805	Buscador	Buen bot
3806	Herramienta	Buen bot
3807	Crawler	Buen bot
3808	Crawler	Buen bot
3809	Herramienta	Buen bot
3810	raspador	Buen bot
3811	Herramienta	Buen bot
3813	Herramienta	Buen bot
3814	Crawler	Buen bot
3815	Sin categoría	Buen bot
3817	Herramienta	Buen bot
3818	Herramienta	Buen bot
3819	Herramienta	Buen bot
3820	Crawler	Buen bot
3821	Buscador	Buen bot
3822	Márketing	Buen bot
3823	Sin categoría	Buen bot
3831	raspador	Buen bot
3834	Buscador	Buen bot
3835	Buscador	Buen bot
3836	Sin categoría	Buen bot
3837	Sin categoría	Buen bot
3838	Sin categoría	Buen bot
3839	Márketing	Buen bot
3840	Crawler	Buen bot
3842	Crawler	Buen bot
3843	Crawler	Buen bot

Regla de firma bot	ID	Descripción
3844	Márketing	Buen bot
3845	Márketing	Buen bot
3846	Márketing	Buen bot
3847	Márketing	Buen bot
3848	Sin categoría	Buen bot
3850	Herramienta	Buen bot
3851	Sin categoría	Buen bot
3852	Herramienta	Buen bot
3853	Analizador de vulnerabilidades	Buen bot
3854	Crawler	Buen bot
3855	Crawler	Buen bot
3856	Herramienta	Buen bot
3861	Márketing	Buen bot
3862	Márketing	Buen bot
3863	Márketing	Buen bot
3864	Márketing	Buen bot
3865	Márketing	Buen bot
3866	Márketing	Buen bot
3867	Márketing	Buen bot
3868	Márketing	Buen bot
3869	Herramienta	Buen bot
3870	Márketing	Buen bot
3872	Márketing	Buen bot
3873	Buscador	Buen bot
3874	Buscador	Buen bot
3875	Buscador	Buen bot
3876	Buscador	Buen bot

Regla de firma bot	ID	Descripción
3877	Creador de captura de pantalla	Buen bot
3878	Buscador	Buen bot
3879	Buscador	Buen bot
3880	Creador de captura de pantalla	Buen bot
3881	Creador de captura de pantalla	Buen bot
3882	Buscador	Buen bot
3883	Buscador	Buen bot
3884	Buscador	Buen bot
3885	Buscador	Buen bot
3886	Herramienta	Buen bot
3887	Crawler	Buen bot
3888	Crawler	Buen bot
3889	Sin categoría	Buen bot
3890	Márketing	Buen bot
3893	Crawler	Buen bot
3894	Herramienta	Buen bot
3895	Herramienta	Buen bot
3896	Buscador	Buen bot
3897	Herramienta	Buen bot
3898	Herramienta	Buen bot
3899	Sin categoría	Buen bot
3901	Crawler	Buen bot
3903	Herramienta	Buen bot
3904	Buscador	Buen bot
3905	Buscador	Buen bot
3906	Buscador	Buen bot
3912	Crawler	Buen bot

Regla de firma bot	ID	Descripción
3918	Crawler	Buen bot
3919	Sin categoría	Buen bot
3920	Sin categoría	Buen bot
3921	Sin categoría	Buen bot
3922	Sin categoría	Buen bot
3923	Sin categoría	Buen bot
3924	Sin categoría	Buen bot
3925	Sin categoría	Buen bot
3926	Márketing	Buen bot
3927	Márketing	Buen bot
3928	Márketing	Buen bot
3929	Herramienta	Buen bot
3930	Márketing	Buen bot
3931	Sin categoría	Buen bot
3932	Crawler	Buen bot
3933	Márketing	Buen bot
3934	Márketing	Buen bot
3935	raspador	Buen bot
3936	Márketing	Buen bot
3937	raspador	Buen bot
3938	Buscador de alimentación	Buen bot
3940	Buscador	Buen bot
3941	Crawler	Buen bot
3942	raspador	Buen bot
3946	Buscador de alimentación	Buen bot
3947	Crawler	Buen bot
3950	Analizador de virus	Buen bot
3951	Márketing	Buen bot
3952	Márketing	Buen bot

Regla de firma bot	ID	Descripción
3953	Márketing	Buen bot
3954	Márketing	Buen bot
3955	Márketing	Buen bot
3956	Márketing	Buen bot
3957	Márketing	Buen bot
3958	Márketing	Buen bot
3959	Márketing	Buen bot
3960	Márketing	Buen bot
3961	Márketing	Buen bot
3962	Márketing	Buen bot
3964	Márketing	Buen bot
3965	Márketing	Buen bot
3966	Márketing	Buen bot
3967	Márketing	Buen bot
3968	Márketing	Buen bot
3969	Márketing	Buen bot
3970	Buscador	Buen bot
3971	Creador de captura de pantalla	Buen bot
3972	Creador de captura de pantalla	Buen bot
3973	Buscador	Buen bot
3974	Buscador	Buen bot
3975	Buscador	Buen bot
3976	Buscador	Buen bot
3977	Buscador	Buen bot
3978	Creador de captura de pantalla	Buen bot
3979	Buscador	Buen bot

Regla de firma bot	ID	Descripción
3980	Creador de captura de pantalla	Buen bot
3981	Buscador	Buen bot
3982	Buscador	Buen bot
3983	Buscador	Buen bot
3984	Buscador	Buen bot
3985	Buscador	Buen bot
3986	Buscador	Buen bot
3987	Creador de captura de pantalla	Buen bot
3988	Buscador	Buen bot
3989	Buscador	Buen bot
3990	Buscador	Buen bot
3991	Buscador	Buen bot
3992	Buscador	Buen bot
3993	Buscador	Buen bot
3994	Buscador	Buen bot
3995	Buscador	Buen bot
3996	Buscador	Buen bot
3997	Buscador	Buen bot
3998	Buscador	Buen bot
3999	Buscador	Buen bot
4000	Creador de captura de pantalla	Buen bot
4001	Buscador	Buen bot
4002	Buscador	Buen bot
4003	Buscador	Buen bot
4004	Buscador	Buen bot
4005	Creador de captura de pantalla	Buen bot

Regla de firma bot	ID	Descripción
4006	Crawler	Buen bot
4007	Márketing	Buen bot
4008	Márketing	Buen bot
4011	Herramienta	Buen bot
4012	Crawler	Buen bot
4013	Buscador	Buen bot
4014	Herramienta	Buen bot
4015	Crawler	Buen bot
4016	Crawler	Buen bot
4017	Herramienta	Buen bot
4018	Herramienta	Buen bot
4019	Herramienta	Buen bot
4020	Herramienta	Buen bot
4021	Márketing	Buen bot
4024	Herramienta	Buen bot
4025	Buscador	Buen bot
4026	Buscador	Buen bot
4028	Márketing	Buen bot
4029	Herramienta	Buen bot
4030	raspador	Buen bot
4031	raspador	Buen bot
4035	Márketing	Buen bot
4037	Analizador de vulnerabilidades	Buen bot
4042	Crawler	Buen bot
4043	Creador de captura de pantalla	Buen bot
4048	Buscador de alimentación	Buen bot
4052	Herramienta	Buen bot

Regla de firma bot	ID	Descripción
4055	Sin categoría	Buen bot
4056	Márketing	Buen bot
4057	Creador de captura de pantalla	Buen bot
4058	Crawler	Buen bot
4060	Buscador	Buen bot
4061	Buscador	Buen bot
4062	Buscador	Buen bot
4063	Buscador	Buen bot
4065	raspador	Buen bot
4066	Márketing	Buen bot
4067	Márketing	Buen bot
4071	Herramienta	Buen bot
4076	Márketing	Buen bot
4078	Crawler	Buen bot
4079	Crawler	Buen bot
4081	Buscador	Buen bot
4082	Herramienta	Buen bot
4085	Herramienta	Buen bot
4086	Herramienta	Buen bot
4090	Herramienta	Buen bot
4091	Herramienta	Buen bot
4092	Herramienta	Buen bot
4093	Herramienta	Buen bot
4094	Sin categoría	Buen bot
4095	Monitor de sitio	Buen bot
4096	Monitor de sitio	Buen bot
4097	Monitor de sitio	Buen bot
4098	Crawler	Buen bot

Regla de firma bot	ID	Descripción
4099	Buscador	Buen bot
4100	Buscador	Buen bot
4101	Buscador	Buen bot
4102	Buscador	Buen bot
4103	Márketing	Buen bot
4104	Márketing	Buen bot
4105	Márketing	Buen bot
4106	Márketing	Buen bot
4107	Márketing	Buen bot
4108	Márketing	Buen bot
4109	Buscador	Buen bot
4110	Crawler	Buen bot
4111	Crawler	Buen bot
4112	Crawler	Buen bot
4113	Analizador de vulnerabilidades	Buen bot
4114	Crawler	Buen bot
4115	Herramienta	Buen bot
4120	Márketing	Buen bot
4121	Márketing	Buen bot
4122	Márketing	Buen bot
4123	Márketing	Buen bot
4124	Márketing	Buen bot
4125	Márketing	Buen bot
4126	Márketing	Buen bot
4127	Márketing	Buen bot
4128	Márketing	Buen bot
4129	Márketing	Buen bot
4130	Márketing	Buen bot

Regla de firma bot	ID	Descripción
4131	Herramienta	Buen bot
4132	Márketing	Buen bot
4133	Márketing	Buen bot
4134	Herramienta	Buen bot
4135	Márketing	Buen bot
4136	Márketing	Buen bot
4137	Márketing	Buen bot
4138	Márketing	Buen bot
4139	Márketing	Buen bot
4140	Márketing	Buen bot
4141	Márketing	Buen bot
4142	Márketing	Buen bot
4143	Márketing	Buen bot
4144	Márketing	Buen bot
4147	Buscador	Buen bot
4148	Buscador	Buen bot
4149	Buscador	Buen bot
4150	Buscador	Buen bot
4151	Buscador	Buen bot
4152	Buscador	Buen bot
4153	Buscador	Buen bot
4154	Buscador	Buen bot
4155	Buscador	Buen bot
4156	Creador de captura de pantalla	Buen bot
4157	Buscador	Buen bot
4158	Buscador	Buen bot
4159	Buscador	Buen bot

Regla de firma bot	ID	Descripción
4160	Creador de captura de pantalla	Buen bot
4161	Buscador	Buen bot
4162	Buscador	Buen bot
4163	Herramienta	Buen bot
4164	Buscador	Buen bot
4168	Probador de velocidad	Buen bot
4170	Herramienta	Buen bot
4172	Crawler	Buen bot
4173	Herramienta	Buen bot
4174	Crawler	Buen bot
4175	Crawler	Buen bot
4176	Herramienta	Buen bot
4177	Buscador	Buen bot
4178	Herramienta	Buen bot
4179	Crawler	Buen bot
4180	Herramienta	Buen bot
4181	Monitor de sitio	Buen bot
4182	Monitor de sitio	Buen bot
4183	Monitor de sitio	Buen bot
4184	Monitor de sitio	Buen bot
4185	Buscador	Buen bot
4186	Herramienta	Buen bot
4187	Herramienta	Buen bot
4190	Buscador	Buen bot
4191	Buscador	Buen bot
4192	Buscador	Buen bot
4193	Buscador	Buen bot
4194	Herramienta	Buen bot

Regla de firma bot	ID	Descripción
4196	Herramienta	Buen bot
4197	Herramienta	Buen bot
4198	Márketing	Buen bot
4199	Márketing	Buen bot
4200	Analizador de vulnerabilidades	Buen bot
4201	Herramienta	Buen bot
4202	Herramienta	Buen bot
4205	Buscador	Buen bot
4206	Márketing	Buen bot
4207	Márketing	Buen bot
4208	Buscador	Buen bot
4209	Buscador	Buen bot
4210	Probador de velocidad	Buen bot
4211	Herramienta	Buen bot
4212	Buscador de alimentación	Buen bot
4213	Buscador de alimentación	Buen bot
4215	Herramienta	Buen bot
4216	Herramienta	Buen bot
4219	Márketing	Buen bot
4220	Herramienta	Buen bot
4222	Monitor de sitio	Buen bot
4223	Márketing	Buen bot
4224	Buscador	Buen bot
4225	Buscador	Buen bot
4226	Buscador	Buen bot
4227	Márketing	Buen bot
4228	Márketing	Buen bot
4229	Herramienta	Buen bot

Regla de firma bot	ID	Descripción
4231	Creador de captura de pantalla	Buen bot
4232	Herramienta	Buen bot
4233	Monitor de sitio	Buen bot
4234	Monitor de sitio	Buen bot
4235	Monitor de sitio	Buen bot
4236	Monitor de sitio	Buen bot
4237	Monitor de sitio	Buen bot
4238	Monitor de sitio	Buen bot
4240	Márketing	Buen bot
4241	Márketing	Buen bot
4242	Márketing	Buen bot
4243	Márketing	Buen bot
4244	Márketing	Buen bot
4245	Márketing	Buen bot
4246	Márketing	Buen bot
4247	Buscador	Buen bot
4248	Buscador	Buen bot
4249	Creador de captura de pantalla	Buen bot
4250	Buscador	Buen bot
4251	Buscador	Buen bot
4252	Crawler	Buen bot
4253	Crawler	Buen bot
4254	Crawler	Buen bot
4255	Herramienta	Buen bot
4256	Sin categoría	Buen bot
4257	Herramienta	Buen bot
4258	Crawler	Buen bot

Regla de firma bot	ID	Descripción
4259	Crawler	Buen bot
4260	Herramienta	Buen bot
4261	Herramienta	Buen bot
4262	Herramienta	Buen bot
4265	Buscador	Buen bot
4266	Sin categoría	Buen bot
4267	Herramienta	Buen bot
4268	Herramienta	Buen bot
4269	Buscador	Buen bot
4270	Buscador	Buen bot
4271	Buscador	Buen bot
4272	Buscador	Buen bot
4273	Buscador	Buen bot
4274	Buscador	Buen bot
4275	Buscador	Buen bot
4279	Márketing	Buen bot
4280	Crawler	Buen bot
4282	Márketing	Buen bot
4283	Márketing	Buen bot
4284	Márketing	Buen bot
4285	Márketing	Buen bot
4286	Márketing	Buen bot
4287	Márketing	Buen bot
4288	Márketing	Buen bot
4289	Márketing	Buen bot
4290	Márketing	Buen bot
4291	Márketing	Buen bot
4292	Márketing	Buen bot
4293	Márketing	Buen bot

Regla de firma bot	ID	Descripción
4294	Márketing	Buen bot
4295	Buscador	Buen bot
4296	Buscador	Buen bot
4297	Buscador	Buen bot
4298	Buscador	Buen bot
4299	Buscador	Buen bot
4300	Buscador	Buen bot
4301	Buscador	Buen bot
4302	Buscador	Buen bot
4303	Buscador	Buen bot
4304	Buscador	Buen bot
4305	Buscador	Buen bot
4306	Creador de captura de pantalla	Buen bot
4307	Buscador	Buen bot
4308	Buscador	Buen bot
4309	Buscador	Buen bot
4310	Buscador	Buen bot
4311	Creador de captura de pantalla	Buen bot
4312	Buscador	Buen bot
4313	Buscador	Buen bot
4314	Buscador	Buen bot
4315	Buscador	Buen bot
4316	Buscador	Buen bot
4317	Buscador	Buen bot
4318	Creador de captura de pantalla	Buen bot
4319	Creador de captura de pantalla	Buen bot

Regla de firma bot	ID	Descripción
4321	Sin categoría	Buen bot
4322	Crawler	Buen bot
4323	Herramienta	Buen bot
4324	Herramienta	Buen bot
4325	Herramienta	Buen bot
4328	Márketing	Buen bot
4330	Monitor de sitio	Buen bot
4331	Buscador	Buen bot
4332	Buscador	Buen bot
4335	Márketing	Buen bot
4336	Márketing	Buen bot
4337	Herramienta	Buen bot
4338	Herramienta	Buen bot
4339	Herramienta	Buen bot
4340	Crawler	Buen bot
4341	Crawler	Buen bot
4342	Analizador de vulnerabilidades	Buen bot
4343	Analizador de vulnerabilidades	Buen bot
4344	raspador	Buen bot
4345	Márketing	Buen bot
4346	Márketing	Buen bot
4347	Márketing	Buen bot
4348	Márketing	Buen bot
4349	Márketing	Buen bot
4350	Márketing	Buen bot
4351	Márketing	Buen bot
4352	Márketing	Buen bot

Regla de firma bot	ID	Descripción
4353	Márketing	Buen bot
4354	Márketing	Buen bot
4355	Buscador	Buen bot
4356	Buscador	Buen bot
4357	Buscador	Buen bot
4358	Buscador	Buen bot
4359	Buscador	Buen bot
4360	Buscador	Buen bot
4361	Buscador	Buen bot
4362	Buscador	Buen bot
4363	Buscador	Buen bot
4364	Buscador	Buen bot
4365	Creador de captura de pantalla	Buen bot
4366	Buscador	Buen bot
4367	Buscador	Buen bot
4368	Buscador	Buen bot
4369	Buscador	Buen bot
4370	Creador de captura de pantalla	Buen bot
4371	Buscador	Buen bot
4372	Buscador	Buen bot
4373	Buscador	Buen bot
4374	Buscador	Buen bot
4375	Buscador	Buen bot
4376	Creador de captura de pantalla	Buen bot
4377	Crawler	Buen bot
4378	Crawler	Buen bot
4379	Buscador	Buen bot

Regla de firma bot	ID	Descripción
4380	Buscador	Buen bot
4381	Buscador	Buen bot
4382	Buscador	Buen bot
4383	Crawler	Buen bot
4384	Buscador	Buen bot
4385	Herramienta	Buen bot
4386	Sin categoría	Buen bot
4387	Crawler	Buen bot
4388	Crawler	Buen bot
4389	Herramienta	Buen bot
4390	Herramienta	Buen bot
4391	Herramienta	Buen bot
4392	Herramienta	Buen bot
4393	Herramienta	Buen bot
4394	Sin categoría	Buen bot
4395	Herramienta	Buen bot
4396	Monitor de sitio	Buen bot
4397	Monitor de sitio	Buen bot
4404	Buscador	Buen bot
4405	Buscador	Buen bot
4406	Buscador	Buen bot
4407	Sin categoría	Buen bot

Actualización de firmas de bots para octubre de 2021

January 31, 2022

Se agregan nuevas firmas y se actualizan algunas de las firmas de bots existentes. Puede descargar y configurar estas reglas de firma para proteger su dispositivo de los ataques de bots.

Versión de firma bot

Firma versión 10 aplicable a plataformas NetScaler Citrix ADC con compilaciones 13.0 76.31 o posteriores.

Firmas de bot actualizadas

A continuación se muestra una lista de ID de reglas de firma de bot, categoría y su tipo.

Regla de firma bot	ID	Descripción
71	Crawler	Buen bot
74	Crawler	Buen bot
75	Crawler	Buen bot
372	raspador	Buen bot
373	raspador	Buen bot
374	raspador	Buen bot
375	raspador	Buen bot
376	raspador	Buen bot
377	raspador	Buen bot
378	raspador	Buen bot
379	raspador	Buen bot
380	raspador	Buen bot
381	raspador	Buen bot
382	raspador	Buen bot
383	raspador	Buen bot
384	raspador	Buen bot
385	raspador	Buen bot
386	raspador	Buen bot
387	raspador	Buen bot
389	raspador	Buen bot
390	raspador	Buen bot
391	raspador	Buen bot
639	Buscador	Buen bot

Regla de firma bot	ID	Descripción
702	Buscador	Buen bot
703	Buscador	Buen bot
1173	Herramienta	Buen bot
1174	Márketing	Buen bot
1176	Buscador	Buen bot
1178	Probador de velocidad	Buen bot
1185	Creador de captura de pantalla	Buen bot
1209	Sin categoría	Buen bot
1531	Buscador de alimentación	Buen bot
2586	Sin categoría	Buen bot
2674	Herramienta	Buen bot
2756	Herramienta	Buen bot
2758	Sin categoría	Buen bot
2759	Herramienta	Buen bot
2784	Herramienta	Buen bot
2952	Herramienta	Buen bot
3163	Herramienta	Buen bot
3554	Herramienta	Buen bot
3782	Márketing	Buen bot
3788	Herramienta	Buen bot
3789	Herramienta	Buen bot
3797	Márketing	Buen bot
3798	Márketing	Buen bot
3799	Márketing	Buen bot
3800	Márketing	Buen bot
3801	Márketing	Buen bot
3802	Creador de captura de pantalla	Buen bot

Regla de firma bot	ID	Descripción
3803	Buscador	Buen bot
3804	Creador de captura de pantalla	Buen bot
3805	Buscador	Buen bot
3861	Márketing	Buen bot
3862	Márketing	Buen bot
3863	Márketing	Buen bot
3864	Márketing	Buen bot
3865	Márketing	Buen bot
3866	Márketing	Buen bot
3867	Márketing	Buen bot
3868	Márketing	Buen bot
3869	Herramienta	Buen bot
3871	Márketing	Buen bot
3872	Márketing	Buen bot
3873	Buscador	Buen bot
3874	Buscador	Buen bot
3875	Buscador	Buen bot
3876	Buscador	Buen bot
3877	Creador de captura de pantalla	Buen bot
3878	Buscador	Buen bot
3879	Buscador	Buen bot
3880	Creador de captura de pantalla	Buen bot
3881	Creador de captura de pantalla	Buen bot
3882	Buscador	Buen bot
3883	Buscador	Buen bot
3884	Buscador	Buen bot

Regla de firma bot	ID	Descripción
3885	Buscador	Buen bot
3963	Márketing	Buen bot
4040	Crawler	Buen bot
4041	Herramienta	Buen bot
4120	Márketing	Buen bot
4122	Márketing	Buen bot
4123	Márketing	Buen bot
4124	Márketing	Buen bot
4125	Márketing	Buen bot
4133	Márketing	Buen bot
4134	Herramienta	Buen bot
4135	Márketing	Buen bot
4136	Márketing	Buen bot
4137	Márketing	Buen bot
4138	Márketing	Buen bot
4139	Márketing	Buen bot
4140	Márketing	Buen bot
4141	Márketing	Buen bot
4142	Márketing	Buen bot
4143	Márketing	Buen bot
4144	Márketing	Buen bot
4145	Buscador	Buen bot
4146	Buscador	Buen bot
4147	Buscador	Buen bot
4148	Buscador	Buen bot
4149	Buscador	Buen bot
4150	Buscador	Buen bot
4151	Buscador	Buen bot
4152	Buscador	Buen bot

Regla de firma bot	ID	Descripción
4153	Buscador	Buen bot
4154	Buscador	Buen bot
4155	Buscador	Buen bot
4156	Creador de captura de pantalla	Buen bot
4157	Buscador	Buen bot
4158	Buscador	Buen bot
4159	Buscador	Buen bot
4160	Creador de captura de pantalla	Buen bot
4161	Buscador	Buen bot
4162	Buscador	Buen bot
4163	Herramienta	Buen bot
4164	Buscador	Buen bot
4209	Buscador	Buen bot
4240	Márketing	Buen bot
4241	Márketing	Buen bot
4248	Buscador	Buen bot
4249	Creador de captura de pantalla	Buen bot
4250	Buscador	Buen bot
4251	Buscador	Buen bot
4282	Márketing	Buen bot
4283	Márketing	Buen bot
4284	Márketing	Buen bot
4285	Márketing	Buen bot
4286	Márketing	Buen bot
4287	Márketing	Buen bot
4288	Márketing	Buen bot
4289	Márketing	Buen bot

Regla de firma bot	ID	Descripción
4290	Márketing	Buen bot
4291	Márketing	Buen bot
4292	Márketing	Buen bot
4293	Márketing	Buen bot
4294	Márketing	Buen bot
4295	Buscador	Buen bot
4296	Buscador	Buen bot
4297	Buscador	Buen bot
4298	Buscador	Buen bot
4299	Buscador	Buen bot
4300	Buscador	Buen bot
4301	Buscador	Buen bot
4302	Buscador	Buen bot
4303	Buscador	Buen bot
4304	Buscador	Buen bot
4305	Buscador	Buen bot
4306	Creador de captura de pantalla	Buen bot
4307	Buscador	Buen bot
4308	Buscador	Buen bot
4309	Buscador	Buen bot
4310	Buscador	Buen bot
4311	Creador de captura de pantalla	Buen bot
4312	Buscador	Buen bot
4313	Buscador	Buen bot
4314	Buscador	Buen bot
4315	Buscador	Buen bot
4316	Buscador	Buen bot

Regla de firma bot	ID	Descripción
4317	Buscador	Buen bot
4318	Creador de captura de pantalla	Buen bot
4319	Creador de captura de pantalla	Buen bot
4337	Herramienta	Buen bot
4338	Herramienta	Buen bot
4345	Márketing	Buen bot
4346	Márketing	Buen bot
4347	Márketing	Buen bot
4348	Márketing	Buen bot
4349	Márketing	Buen bot
4350	Márketing	Buen bot
4351	Márketing	Buen bot
4352	Márketing	Buen bot
4353	Márketing	Buen bot
4354	Márketing	Buen bot
4355	Buscador	Buen bot
4356	Buscador	Buen bot
4357	Buscador	Buen bot
4358	Buscador	Buen bot
4359	Buscador	Buen bot
4360	Buscador	Buen bot
4361	Buscador	Buen bot
4362	Buscador	Buen bot
4363	Buscador	Buen bot
4364	Buscador	Buen bot
4365	Creador de captura de pantalla	Buen bot
4366	Buscador	Buen bot

Regla de firma bot	ID	Descripción
4367	Buscador	Buen bot
4368	Buscador	Buen bot
4369	Buscador	Buen bot
4370	Creador de captura de pantalla	Buen bot
4371	Buscador	Buen bot
4372	Buscador	Buen bot
4373	Buscador	Buen bot
4374	Buscador	Buen bot
4375	Buscador	Buen bot
4376	Creador de captura de pantalla	Buen bot

Actualización de firma de bots para noviembre de 2021

July 8, 2022

Se agregan nuevas firmas y se actualizan algunas de las firmas de bots existentes. Puede descargar y configurar estas reglas de firma para proteger su dispositivo de los ataques de bots.

Versión de firma bot

Firma versión 11 aplicable a plataformas NetScaler Citrix ADC con compilaciones 13.0 76.31 o posteriores.

Nuevas firmas de bots

A continuación se muestra una lista de ID de reglas de firma de bot, categoría y su tipo.

Regla de firma bot	ID	Descripción
4408	raspador	Buen bot
4409	Crawler	Bot malo

Regla de firma bot	ID	Descripción
4411	Márketing	Buen bot
4412	Márketing	Buen bot
4413	Márketing	Buen bot
4421	Creador de captura de pantalla	Buen bot
4422	Crawler	Buen bot
4423	Herramienta	Bot malo
4424	Monitor de sitio	Buen bot
4425	Márketing	Buen bot
4426	Crawler	Bot malo
4427	raspador	Buen bot
4428	raspador	Buen bot
4429	Creador de captura de pantalla	Buen bot
4430	Analizador de virus	Buen bot
4431	Monitor de sitio	Buen bot
4432	Herramienta	Buen bot
4433	Buscador	Buen bot
4434	Buscador	Buen bot
4435	Buscador	Buen bot
4436	Márketing	Buen bot
4437	Márketing	Buen bot
4438	raspador	Buen bot
4439	raspador	Buen bot
4440	raspador	Buen bot
4441	Buscador de alimentación	Buen bot
4442	Márketing	Buen bot
4443	raspador	Buen bot
4445	Sin categoría	Bot malo

Regla de firma bot	ID	Descripción
4446	raspador	Buen bot
4450	Creador de captura de pantalla	Buen bot
4451	Probador de velocidad	Buen bot
4452	Buscador	Buen bot
4466	Sin categoría	Buen bot
4467	Creador de captura de pantalla	Buen bot
4468	Herramienta	Buen bot
4469	Sin categoría	Buen bot
4470	Herramienta	Buen bot
4472	raspador	Buen bot
4473	Sin categoría	Buen bot
4474	Márketing	Buen bot
4476	Crawler	Buen bot
4477	Crawler	Buen bot
4478	Crawler	Buen bot
4479	Crawler	Buen bot
4480	Crawler	Buen bot
4481	Crawler	Buen bot
4482	Crawler	Buen bot
4483	Crawler	Buen bot
4484	Crawler	Buen bot
4485	Crawler	Buen bot
4486	raspador	Buen bot
4487	raspador	Buen bot
4488	raspador	Buen bot
4489	Buscador	Buen bot
4491	Herramienta	Buen bot

Regla de firma bot	ID	Descripción
4492	Sin categoría	Bot malo
4493	Crawler	Buen bot
4494	Herramienta	Buen bot
4496	Herramienta	Buen bot
4497	Crawler	Buen bot
4498	Sin categoría	Bot malo
4499	Sin categoría	Bot malo
4501	Márketing	Buen bot
4502	Márketing	Buen bot
4503	Márketing	Buen bot
4508	Sin categoría	Buen bot
4509	Sin categoría	Buen bot
4510	Sin categoría	Buen bot
4511	Sin categoría	Buen bot
4512	Herramienta	Buen bot
4513	Herramienta	Buen bot
4514	Herramienta	Buen bot
4515	Herramienta	Buen bot
4516	Sin categoría	Buen bot
4518	raspador	Bot malo
4519	Creador de captura de pantalla	Buen bot
4520	Márketing	Buen bot
4521	Sin categoría	Buen bot
4522	Herramienta	Buen bot
4523	Sin categoría	Bot malo
4524	Sin categoría	Bot malo
4525	Crawler	Buen bot
4526	Crawler	Buen bot

Regla de firma bot	ID	Descripción
4527	Crawler	Buen bot
4528	Crawler	Buen bot
4529	Crawler	Buen bot
4530	Sin categoría	Bot malo
4531	Márketing	Buen bot
4532	Márketing	Buen bot
4533	Márketing	Buen bot
4534	Márketing	Buen bot
4535	Márketing	Buen bot
4541	Márketing	Buen bot
4552	Sin categoría	Buen bot
4553	Herramienta	Bot malo
4554	Herramienta	Bot malo
4555	Herramienta	Buen bot
4556	Herramienta	Buen bot
4558	raspador	Buen bot
4559	Crawler	Buen bot
4560	Crawler	Buen bot
4561	Monitor de sitio	Buen bot
4562	Buscador	Buen bot
4563	Buscador	Buen bot
1000000	Explorador web	Buen bot
1000001	raspador	Bot malo
1000002	Application	Bot malo
1000003	Explorador web	Buen bot
1000004	raspador	Buen bot
1000005	raspador	Buen bot
1000006	Crawler	Bot malo
1000007	Explorador web	Bot malo

Regla de firma bot	ID	Descripción
1000008	Sin categoría	Bot malo
1000009	Explorador web	Buen bot
1000010	raspador	Bot malo
1000011	Explorador web	Bot malo
1000012	Explorador web	Buen bot
1000013	Explorador web	Bot malo
1000014	raspador	Buen bot
1000015	raspador	Bot malo
1000016	raspador	Bot malo
1000017	Explorador web	Buen bot
1000018	Explorador web	Bot malo
1000019	Sin categoría	Bot malo
1000020	raspador	Buen bot
1000021	Explorador web	Bot malo
1000022	raspador	Buen bot
1000023	raspador	Buen bot
1000024	Crawler	Buen bot
1000025	Explorador web	Bot malo
1000026	Analizador	Buen bot
1000027	Analizador	Buen bot
1000028	Analizador	Buen bot
1000029	Analizador	Buen bot
1000030	Analizador	Buen bot
1000031	Explorador web	Buen bot
1000032	Analizador	Buen bot
1000033	Analizador	Buen bot
1000034	Explorador web	Bot malo
1000035	raspador	Buen bot
1000036	raspador	Buen bot

Regla de firma bot	ID	Descripción
1000037	Analizador	Buen bot
1000038	Analizador	Buen bot
1000039	Analizador	Buen bot
1000040	Analizador	Buen bot
1000041	raspador	Buen bot
1000042	Analizador	Buen bot
1000043	Analizador	Buen bot
1000044	Crawler	Buen bot
1000045	Explorador web	Bot malo
1000046	Explorador web	Bot malo
1000047	raspador	Buen bot
1000048	Explorador web	Bot malo
1000049	Analizador	Buen bot
1000050	Explorador web	Bot malo
1000051	Explorador web	Buen bot
1000052	Explorador web	Bot malo
1000053	raspador	Buen bot
1000054	Explorador web	Buen bot
1000055	Explorador web	Buen bot
1000056	raspador	Bot malo
1000057	Crawler	Bot malo
1000058	raspador	Bot malo
1000059	Analizador	Buen bot
1000060	Explorador web	Bot malo
1000061	Explorador web	Bot malo
1000062	Explorador web	Bot malo
1000063	raspador	Bot malo
1000064	raspador	Bot malo
1000065	raspador	Bot malo

Regla de firma bot	ID	Descripción
1000066	Application	Bot malo
1000067	raspador	Bot malo
1000068	Explorador web	Bot malo
1000069	raspador	Bot malo
1000070	raspador	Buen bot
1000071	Explorador web	Buen bot
1000072	Explorador web	Buen bot
1000073	Explorador web	Bot malo
1000074	Explorador web	Bot malo
1000075	Application	Bot malo
1000076	raspador	Bot malo

Firmas de bot actualizadas

A continuación se muestra una lista de ID de reglas de firma de bot, categoría y su tipo.

Regla de firma bot	ID	Descripción
2	Crawler	Buen bot
5	Crawler	Buen bot
9	Crawler	Buen bot
30	Crawler	Bot malo
45	Crawler	Buen bot
46	Crawler	Buen bot
48	Crawler	Buen bot
52	Crawler	Buen bot
60	Crawler	Buen bot
61	Crawler	Buen bot
63	Crawler	Buen bot
67	Crawler	Buen bot
76	Crawler	Buen bot

Regla de firma bot	ID	Descripción
78	Crawler	Buen bot
79	Crawler	Buen bot
80	Crawler	Buen bot
81	Crawler	Buen bot
82	Crawler	Buen bot
83	Crawler	Buen bot
84	Crawler	Buen bot
87	Crawler	Buen bot
90	Crawler	Buen bot
95	Crawler	Buen bot
96	Crawler	Buen bot
97	Crawler	Buen bot
100	Crawler	Buen bot
101	Crawler	Buen bot
102	Crawler	Buen bot
103	Crawler	Buen bot
104	Crawler	Buen bot
107	Crawler	Buen bot
108	Crawler	Buen bot
110	Crawler	Buen bot
111	Crawler	Buen bot
114	Crawler	Buen bot
115	Crawler	Buen bot
123	Crawler	Buen bot
135	Crawler	Buen bot
136	Crawler	Buen bot
137	Crawler	Buen bot
140	Crawler	Buen bot
141	Crawler	Buen bot

Regla de firma bot	ID	Descripción
143	Crawler	Buen bot
144	Crawler	Buen bot
145	Crawler	Buen bot
146	Crawler	Buen bot
147	Crawler	Buen bot
149	Crawler	Buen bot
152	Crawler	Buen bot
155	Crawler	Buen bot
156	Crawler	Buen bot
157	Crawler	Buen bot
158	Crawler	Buen bot
159	Crawler	Buen bot
160	Crawler	Buen bot
161	Crawler	Buen bot
162	Crawler	Buen bot
163	Crawler	Buen bot
164	Crawler	Buen bot
165	Crawler	Buen bot
166	Crawler	Buen bot
167	Crawler	Buen bot
172	Crawler	Buen bot
173	Crawler	Buen bot
174	Crawler	Buen bot
176	Crawler	Buen bot
177	Crawler	Buen bot
180	Crawler	Buen bot
182	Crawler	Buen bot
187	Crawler	Buen bot
197	Crawler	Buen bot

Regla de firma bot	ID	Descripción
201	Crawler	Buen bot
202	Crawler	Buen bot
203	Crawler	Buen bot
206	Crawler	Buen bot
217	Buscador de alimentación	Buen bot
219	Buscador de alimentación	Buen bot
229	raspador	Buen bot
235	raspador	Buen bot
236	raspador	Buen bot
237	raspador	Buen bot
248	raspador	Buen bot
250	raspador	Buen bot
252	raspador	Buen bot
260	raspador	Buen bot
263	raspador	Buen bot
265	raspador	Buen bot
267	raspador	Buen bot
268	raspador	Buen bot
271	raspador	Buen bot
272	raspador	Buen bot
276	raspador	Buen bot
277	raspador	Buen bot
278	raspador	Buen bot
279	raspador	Buen bot
280	raspador	Buen bot
281	raspador	Buen bot
283	raspador	Buen bot
285	raspador	Buen bot
286	raspador	Buen bot

Regla de firma bot	ID	Descripción
287	raspador	Buen bot
290	raspador	Buen bot
292	raspador	Buen bot
293	raspador	Buen bot
338	raspador	Buen bot
342	raspador	Buen bot
343	raspador	Buen bot
344	raspador	Buen bot
351	raspador	Buen bot
352	raspador	Buen bot
353	raspador	Buen bot
355	raspador	Buen bot
357	raspador	Buen bot
360	raspador	Buen bot
362	raspador	Buen bot
366	raspador	Buen bot
370	raspador	Buen bot
371	raspador	Buen bot
392	raspador	Buen bot
393	raspador	Buen bot
394	raspador	Buen bot
396	raspador	Buen bot
397	raspador	Buen bot
414	raspador	Buen bot
418	raspador	Buen bot
419	raspador	Buen bot
421	raspador	Buen bot
422	raspador	Buen bot
423	raspador	Buen bot

Regla de firma bot	ID	Descripción
424	raspador	Buen bot
425	raspador	Buen bot
426	raspador	Buen bot
427	raspador	Buen bot
428	raspador	Buen bot
430	raspador	Buen bot
432	raspador	Buen bot
433	raspador	Buen bot
434	raspador	Buen bot
435	raspador	Buen bot
441	raspador	Buen bot
445	raspador	Buen bot
446	raspador	Buen bot
451	raspador	Buen bot
452	raspador	Buen bot
454	raspador	Buen bot
455	raspador	Buen bot
456	raspador	Buen bot
457	raspador	Buen bot
458	raspador	Buen bot
461	raspador	Buen bot
465	raspador	Buen bot
466	raspador	Buen bot
469	raspador	Buen bot
473	raspador	Buen bot
474	raspador	Buen bot
476	raspador	Buen bot
477	raspador	Buen bot
484	raspador	Buen bot

Regla de firma bot	ID	Descripción
485	raspador	Buen bot
487	raspador	Buen bot
488	raspador	Buen bot
489	raspador	Buen bot
490	raspador	Buen bot
493	raspador	Buen bot
494	raspador	Buen bot
495	raspador	Buen bot
497	raspador	Buen bot
498	raspador	Buen bot
499	raspador	Buen bot
500	raspador	Buen bot
505	raspador	Buen bot
506	raspador	Buen bot
507	raspador	Buen bot
512	raspador	Buen bot
513	raspador	Buen bot
514	raspador	Buen bot
527	raspador	Buen bot
533	raspador	Buen bot
539	raspador	Buen bot
540	raspador	Buen bot
542	raspador	Buen bot
544	raspador	Buen bot
545	raspador	Buen bot
546	raspador	Buen bot
547	raspador	Buen bot
548	raspador	Buen bot
551	raspador	Buen bot

Regla de firma bot	ID	Descripción
552	raspador	Buen bot
554	raspador	Buen bot
556	raspador	Buen bot
558	raspador	Buen bot
560	raspador	Buen bot
561	raspador	Buen bot
566	raspador	Buen bot
575	raspador	Buen bot
578	raspador	Buen bot
581	raspador	Buen bot
582	raspador	Buen bot
591	raspador	Buen bot
593	raspador	Buen bot
595	raspador	Buen bot
600	raspador	Buen bot
601	raspador	Buen bot
602	raspador	Buen bot
604	raspador	Buen bot
605	raspador	Buen bot
609	raspador	Buen bot
610	raspador	Buen bot
611	raspador	Buen bot
612	raspador	Buen bot
613	raspador	Buen bot
615	raspador	Buen bot
620	Buscador	Buen bot
622	Buscador	Buen bot
623	Buscador	Buen bot
624	Buscador	Buen bot

Regla de firma bot	ID	Descripción
626	Buscador	Buen bot
627	Buscador	Buen bot
628	Buscador	Buen bot
629	Buscador	Buen bot
633	Buscador	Buen bot
634	Buscador	Buen bot
636	Buscador	Buen bot
637	Buscador	Buen bot
640	Buscador	Buen bot
641	Buscador	Buen bot
642	Buscador	Buen bot
643	Buscador	Buen bot
647	Buscador	Buen bot
649	Buscador	Buen bot
650	Buscador	Buen bot
651	Buscador	Buen bot
654	Buscador	Buen bot
656	Buscador	Buen bot
657	Buscador	Buen bot
658	Buscador	Buen bot
659	Buscador	Buen bot
660	Buscador	Buen bot
663	Buscador	Buen bot
664	Buscador	Buen bot
665	Buscador	Buen bot
666	Buscador	Buen bot
667	Buscador	Buen bot
669	Buscador	Buen bot
670	Buscador	Buen bot

Regla de firma bot	ID	Descripción
671	Buscador	Buen bot
672	Buscador	Buen bot
673	Buscador	Buen bot
674	Buscador	Buen bot
675	Buscador	Buen bot
676	Buscador	Buen bot
677	Buscador	Buen bot
679	Buscador	Buen bot
680	Buscador	Buen bot
690	Buscador	Buen bot
693	Buscador	Buen bot
694	Buscador	Buen bot
697	Buscador	Buen bot
698	Buscador	Buen bot
702	Buscador	Buen bot
706	Buscador	Buen bot
712	Buscador	Buen bot
713	Buscador	Buen bot
714	Buscador	Buen bot
715	Buscador	Buen bot
716	Buscador	Buen bot
721	Buscador	Buen bot
723	Buscador	Buen bot
725	Buscador	Buen bot
727	Buscador	Buen bot
728	Buscador	Buen bot
729	Buscador	Buen bot
730	Buscador	Buen bot
731	Buscador	Buen bot

Regla de firma bot	ID	Descripción
732	Buscador	Buen bot
735	Buscador	Buen bot
736	Buscador	Buen bot
740	Buscador	Buen bot
748	Buscador	Buen bot
749	Buscador	Buen bot
750	Buscador	Buen bot
751	Buscador	Buen bot
756	Buscador	Buen bot
757	Buscador	Buen bot
758	Buscador	Buen bot
759	Buscador	Buen bot
760	Buscador	Buen bot
761	Buscador	Buen bot
762	Buscador	Buen bot
763	Buscador	Buen bot
764	Buscador	Buen bot
765	Buscador	Buen bot
766	Buscador	Buen bot
767	Buscador	Buen bot
768	Buscador	Buen bot
769	Buscador	Buen bot
770	Buscador	Buen bot
771	Buscador	Buen bot
772	Buscador	Buen bot
773	Buscador	Buen bot
776	Buscador	Buen bot
777	Buscador	Buen bot
780	Buscador	Buen bot

Regla de firma bot	ID	Descripción
781	Buscador	Buen bot
784	Buscador	Buen bot
786	Buscador	Buen bot
787	Buscador	Buen bot
788	Buscador	Buen bot
789	Buscador	Buen bot
790	Buscador	Buen bot
791	Buscador	Buen bot
792	Buscador	Buen bot
795	Buscador	Buen bot
796	Buscador	Buen bot
798	Buscador	Buen bot
800	Buscador	Buen bot
801	Buscador	Buen bot
802	Buscador	Buen bot
803	Buscador	Buen bot
805	Buscador	Buen bot
806	Buscador	Buen bot
807	Buscador	Buen bot
809	Buscador	Buen bot
810	Buscador	Buen bot
811	Buscador	Buen bot
812	Buscador	Buen bot
814	Buscador	Buen bot
815	Buscador	Buen bot
816	Buscador	Buen bot
817	Buscador	Buen bot
818	Buscador	Buen bot
819	Buscador	Buen bot

Regla de firma bot	ID	Descripción
820	Buscador	Buen bot
821	Buscador	Buen bot
822	Buscador	Buen bot
823	Buscador	Buen bot
825	Buscador	Buen bot
827	Buscador	Buen bot
830	Buscador	Buen bot
831	Buscador	Buen bot
834	Buscador	Buen bot
837	Buscador	Buen bot
838	Buscador	Buen bot
849	Monitor de sitio	Buen bot
850	Monitor de sitio	Buen bot
851	Monitor de sitio	Buen bot
853	Monitor de sitio	Buen bot
857	Monitor de sitio	Buen bot
858	Monitor de sitio	Buen bot
859	Monitor de sitio	Buen bot
860	Monitor de sitio	Buen bot
861	Monitor de sitio	Buen bot
862	Monitor de sitio	Buen bot
863	Monitor de sitio	Buen bot
864	Monitor de sitio	Buen bot
865	Monitor de sitio	Buen bot
866	Monitor de sitio	Buen bot
867	Monitor de sitio	Buen bot
868	Monitor de sitio	Buen bot
869	Monitor de sitio	Buen bot
870	Monitor de sitio	Buen bot

Regla de firma bot	ID	Descripción
871	Monitor de sitio	Buen bot
872	Monitor de sitio	Buen bot
873	Monitor de sitio	Buen bot
874	Monitor de sitio	Buen bot
875	Monitor de sitio	Buen bot
876	Monitor de sitio	Buen bot
877	Monitor de sitio	Buen bot
880	Monitor de sitio	Buen bot
881	Monitor de sitio	Buen bot
883	Monitor de sitio	Buen bot
885	Monitor de sitio	Buen bot
886	Monitor de sitio	Buen bot
888	Monitor de sitio	Buen bot
889	Monitor de sitio	Buen bot
895	Monitor de sitio	Buen bot
896	Monitor de sitio	Buen bot
897	Monitor de sitio	Buen bot
898	Monitor de sitio	Buen bot
900	Monitor de sitio	Buen bot
901	Monitor de sitio	Buen bot
904	Monitor de sitio	Buen bot
906	Monitor de sitio	Buen bot
908	Monitor de sitio	Buen bot
909	Monitor de sitio	Buen bot
910	Monitor de sitio	Buen bot
911	Monitor de sitio	Buen bot
912	Monitor de sitio	Buen bot
913	Monitor de sitio	Buen bot
917	Monitor de sitio	Buen bot

Regla de firma bot	ID	Descripción
918	Monitor de sitio	Buen bot
919	Monitor de sitio	Buen bot
920	Monitor de sitio	Buen bot
921	Monitor de sitio	Buen bot
924	Monitor de sitio	Buen bot
926	Monitor de sitio	Buen bot
927	Monitor de sitio	Buen bot
928	Monitor de sitio	Buen bot
929	Monitor de sitio	Buen bot
930	Monitor de sitio	Buen bot
931	Monitor de sitio	Buen bot
934	Monitor de sitio	Buen bot
938	Monitor de sitio	Buen bot
939	Monitor de sitio	Buen bot
958	Monitor de sitio	Buen bot
959	Monitor de sitio	Buen bot
960	Monitor de sitio	Buen bot
963	Monitor de sitio	Buen bot
984	raspador	Buen bot
991	raspador	Bot malo
996	raspador	Buen bot
997	raspador	Buen bot
998	raspador	Buen bot
1002	raspador	Buen bot
1006	raspador	Buen bot
1622	Creador de captura de pantalla	Buen bot
2810	Crawler	Buen bot
3432	Sin categoría	Bot malo

Regla de firma bot	ID	Descripción
3783	Buscador	Buen bot
3784	raspador	Bot malo
3788	Herramienta	Buen bot
3790	Crawler	Buen bot
3791	Probador de velocidad	Buen bot
3792	Herramienta	Buen bot
3793	Herramienta	Buen bot
3794	Crawler	Buen bot
3796	raspador	Buen bot
3797	Márketing	Buen bot
3799	Márketing	Buen bot
3800	Márketing	Buen bot
3806	Herramienta	Buen bot
3807	Crawler	Buen bot
3808	Crawler	Buen bot
3809	Herramienta	Buen bot
3810	raspador	Buen bot
3811	Herramienta	Buen bot
3812	Crawler	Buen bot
3813	Herramienta	Buen bot
3814	Crawler	Buen bot
3815	Sin categoría	Buen bot
3817	Herramienta	Buen bot
3818	Herramienta	Buen bot
3819	Herramienta	Buen bot
3820	Crawler	Buen bot
3821	Buscador	Buen bot
3822	Márketing	Buen bot
3823	Sin categoría	Buen bot

Regla de firma bot	ID	Descripción
3831	raspador	Buen bot
3833	Buscador	Buen bot
3834	Buscador	Buen bot
3835	Buscador	Buen bot
3836	Sin categoría	Buen bot
3838	Sin categoría	Buen bot
3839	Márketing	Buen bot
3840	Crawler	Buen bot
3842	Crawler	Buen bot
3843	Crawler	Buen bot
3844	Márketing	Buen bot
3845	Márketing	Buen bot
3846	Márketing	Buen bot
3847	Márketing	Buen bot
3848	Sin categoría	Buen bot
3849	Crawler	Buen bot
3850	Herramienta	Buen bot
3851	Sin categoría	Buen bot
3852	Herramienta	Buen bot
3853	Analizador de vulnerabilidades	Buen bot
3854	Crawler	Buen bot
3855	Crawler	Buen bot
3856	Herramienta	Buen bot
3871	Márketing	Buen bot
3886	Herramienta	Buen bot
3887	Crawler	Buen bot
3888	Crawler	Buen bot
3889	Sin categoría	Buen bot

Regla de firma bot	ID	Descripción
3890	Márketing	Buen bot
3893	Crawler	Buen bot
3894	Herramienta	Buen bot
3895	Herramienta	Buen bot
3896	Buscador	Buen bot
3897	Herramienta	Buen bot
3898	Herramienta	Buen bot
3899	Sin categoría	Buen bot
3901	Crawler	Buen bot
3902	Herramienta	Buen bot
3903	Herramienta	Buen bot
3904	Buscador	Buen bot
3905	Buscador	Buen bot
3906	Buscador	Buen bot
3907	Buscador	Buen bot
3912	Crawler	Buen bot
3917	Sin categoría	Buen bot
3918	Crawler	Buen bot
3919	Sin categoría	Buen bot
3920	Sin categoría	Buen bot
3921	Sin categoría	Buen bot
3922	Sin categoría	Buen bot
3923	Sin categoría	Buen bot
3924	Sin categoría	Buen bot
3925	Sin categoría	Buen bot
3926	Márketing	Buen bot
3927	Márketing	Buen bot
3928	Márketing	Buen bot
3929	Herramienta	Buen bot

Regla de firma bot	ID	Descripción
3930	Márketing	Buen bot
3931	Sin categoría	Buen bot
3932	Crawler	Buen bot
3933	Márketing	Buen bot
3934	Márketing	Buen bot
3935	raspador	Buen bot
3936	Márketing	Buen bot
3937	raspador	Buen bot
3938	Buscador de alimentación	Buen bot
3940	Buscador	Buen bot
3941	Crawler	Buen bot
3942	raspador	Buen bot
3946	Buscador de alimentación	Buen bot
3947	Crawler	Buen bot
3950	Analizador de virus	Buen bot
3951	Márketing	Buen bot
3952	Márketing	Buen bot
3953	Márketing	Buen bot
3954	Márketing	Buen bot
3955	Márketing	Buen bot
3956	Márketing	Buen bot
3957	Márketing	Buen bot
3958	Márketing	Buen bot
3959	Márketing	Buen bot
3960	Márketing	Buen bot
3961	Márketing	Buen bot
3962	Márketing	Buen bot
3963	Márketing	Buen bot
3964	Márketing	Buen bot

Regla de firma bot	ID	Descripción
3965	Márketing	Buen bot
3966	Márketing	Buen bot
3967	Márketing	Buen bot
3968	Márketing	Buen bot
3969	Márketing	Buen bot
3970	Buscador	Buen bot
3971	Creador de captura de pantalla	Buen bot
3972	Creador de captura de pantalla	Buen bot
3973	Buscador	Buen bot
3974	Buscador	Buen bot
3975	Buscador	Buen bot
3976	Buscador	Buen bot
3977	Buscador	Buen bot
3978	Creador de captura de pantalla	Buen bot
3979	Buscador	Buen bot
3980	Creador de captura de pantalla	Buen bot
3981	Buscador	Buen bot
3982	Buscador	Buen bot
3983	Buscador	Buen bot
3984	Buscador	Buen bot
3985	Buscador	Buen bot
3986	Buscador	Buen bot
3987	Creador de captura de pantalla	Buen bot
3988	Buscador	Buen bot
3989	Buscador	Buen bot

Regla de firma bot	ID	Descripción
3990	Buscador	Buen bot
3991	Buscador	Buen bot
3992	Buscador	Buen bot
3993	Buscador	Buen bot
3994	Buscador	Buen bot
3995	Buscador	Buen bot
3996	Buscador	Buen bot
3997	Buscador	Buen bot
3998	Buscador	Buen bot
3999	Buscador	Buen bot
4000	Creador de captura de pantalla	Buen bot
4001	Buscador	Buen bot
4002	Buscador	Buen bot
4003	Buscador	Buen bot
4004	Buscador	Buen bot
4005	Creador de captura de pantalla	Buen bot
4006	Crawler	Buen bot
4007	Márketing	Buen bot
4008	Márketing	Buen bot
4011	Herramienta	Buen bot
4012	Crawler	Buen bot
4013	Buscador	Buen bot
4014	Herramienta	Buen bot
4015	Crawler	Buen bot
4016	Crawler	Buen bot
4017	Herramienta	Buen bot
4018	Herramienta	Buen bot

Regla de firma bot	ID	Descripción
4019	Herramienta	Buen bot
4020	Herramienta	Buen bot
4021	Márketing	Buen bot
4024	Herramienta	Buen bot
4025	Buscador	Buen bot
4026	Buscador	Buen bot
4027	Buscador	Buen bot
4028	Márketing	Buen bot
4029	Herramienta	Buen bot
4030	raspador	Buen bot
4031	raspador	Buen bot
4033	Crawler	Buen bot
4034	Crawler	Buen bot
4035	Márketing	Buen bot
4036	Analizador de vulnerabilidades	Buen bot
4037	Analizador de vulnerabilidades	Buen bot
4038	Sin categoría	Bot malo
4039	Herramienta	Buen bot
4042	Crawler	Buen bot
4043	Creador de captura de pantalla	Buen bot
4048	Buscador de alimentación	Buen bot
4050	Crawler	Buen bot
4051	Crawler	Buen bot
4052	Herramienta	Buen bot
4053	Herramienta	Buen bot
4055	Sin categoría	Buen bot
4056	Márketing	Buen bot

Regla de firma bot	ID	Descripción
4057	Creador de captura de pantalla	Buen bot
4058	Crawler	Buen bot
4060	Buscador	Buen bot
4061	Buscador	Buen bot
4062	Buscador	Buen bot
4063	Buscador	Buen bot
4064	Herramienta	Buen bot
4065	raspador	Buen bot
4066	Márketing	Buen bot
4067	Márketing	Buen bot
4071	Herramienta	Buen bot
4076	Márketing	Buen bot
4077	raspador	Buen bot
4078	Crawler	Buen bot
4079	Crawler	Buen bot
4081	Buscador	Buen bot
4082	Herramienta	Buen bot
4085	Herramienta	Buen bot
4086	Herramienta	Buen bot
4087	Herramienta	Bot malo
4088	Buscador	Buen bot
4089	Márketing	Buen bot
4090	Herramienta	Buen bot
4091	Herramienta	Buen bot
4092	Herramienta	Buen bot
4093	Herramienta	Buen bot
4094	Sin categoría	Buen bot
4095	Monitor de sitio	Buen bot

Regla de firma bot	ID	Descripción
4096	Monitor de sitio	Buen bot
4097	Monitor de sitio	Buen bot
4098	Crawler	Buen bot
4099	Buscador	Buen bot
4100	Buscador	Buen bot
4101	Buscador	Buen bot
4102	Buscador	Buen bot
4103	Márketing	Buen bot
4104	Márketing	Buen bot
4105	Márketing	Buen bot
4106	Márketing	Buen bot
4109	Buscador	Buen bot
4110	Crawler	Buen bot
4111	Crawler	Buen bot
4112	Crawler	Buen bot
4113	Analizador de vulnerabilidades	Buen bot
4114	Crawler	Buen bot
4115	Herramienta	Buen bot
4121	Márketing	Buen bot
4126	Márketing	Buen bot
4127	Márketing	Buen bot
4128	Márketing	Buen bot
4129	Márketing	Buen bot
4130	Márketing	Buen bot
4131	Herramienta	Buen bot
4132	Márketing	Buen bot
4165	Márketing	Buen bot
4168	Probador de velocidad	Buen bot

Regla de firma bot	ID	Descripción
4170	Herramienta	Buen bot
4172	Crawler	Buen bot
4173	Herramienta	Buen bot
4174	Crawler	Buen bot
4175	Crawler	Buen bot
4176	Herramienta	Buen bot
4177	Buscador	Buen bot
4178	Herramienta	Buen bot
4179	Crawler	Buen bot
4180	Herramienta	Buen bot
4181	Monitor de sitio	Buen bot
4182	Monitor de sitio	Buen bot
4183	Monitor de sitio	Buen bot
4184	Monitor de sitio	Buen bot
4185	Buscador	Buen bot
4186	Herramienta	Buen bot
4187	Herramienta	Buen bot
4188	Creador de captura de pantalla	Buen bot
4189	Márketing	Buen bot
4190	Buscador	Buen bot
4191	Buscador	Buen bot
4192	Buscador	Buen bot
4193	Buscador	Buen bot
4194	Herramienta	Buen bot
4196	Herramienta	Buen bot
4197	Herramienta	Buen bot
4198	Márketing	Buen bot
4199	Márketing	Buen bot

Regla de firma bot	ID	Descripción
4200	Analizador de vulnerabilidades	Buen bot
4201	Herramienta	Buen bot
4202	Herramienta	Buen bot
4205	Buscador	Buen bot
4209	Buscador	Buen bot
4210	Probador de velocidad	Buen bot
4211	Herramienta	Buen bot
4212	Buscador de alimentación	Buen bot
4213	Buscador de alimentación	Buen bot
4215	Herramienta	Buen bot
4216	Herramienta	Buen bot
4219	Márketing	Buen bot
4220	Herramienta	Buen bot
4222	Monitor de sitio	Buen bot
4223	Márketing	Buen bot
4224	Buscador	Buen bot
4225	Buscador	Buen bot
4226	Buscador	Buen bot
4227	Márketing	Buen bot
4228	Márketing	Buen bot
4229	Herramienta	Buen bot
4231	Creador de captura de pantalla	Buen bot
4232	Herramienta	Buen bot
4233	Monitor de sitio	Buen bot
4236	Monitor de sitio	Buen bot
4242	Márketing	Buen bot
4243	Márketing	Buen bot

Regla de firma bot	ID	Descripción
4244	Márketing	Buen bot
4245	Márketing	Buen bot
4246	Márketing	Buen bot
4247	Buscador	Buen bot
4252	Crawler	Buen bot
4253	Crawler	Buen bot
4254	Crawler	Buen bot
4255	Herramienta	Buen bot
4256	Sin categoría	Buen bot
4257	Herramienta	Buen bot
4258	Crawler	Buen bot
4259	Crawler	Buen bot
4260	Herramienta	Buen bot
4261	Herramienta	Buen bot
4262	Herramienta	Buen bot
4263	Márketing	Buen bot
4265	Buscador	Buen bot
4266	Sin categoría	Buen bot
4267	Herramienta	Buen bot
4268	Herramienta	Buen bot
4269	Buscador	Buen bot
4270	Buscador	Buen bot
4271	Buscador	Buen bot
4272	Buscador	Buen bot
4273	Buscador	Buen bot
4274	Buscador	Buen bot
4275	Buscador	Buen bot
4279	Márketing	Buen bot
4280	Crawler	Buen bot

Regla de firma bot	ID	Descripción
4321	Sin categoría	Buen bot
4322	Crawler	Buen bot
4323	Herramienta	Buen bot
4324	Herramienta	Buen bot
4325	Herramienta	Buen bot
4327	Buscador	Buen bot
4328	Márketing	Buen bot
4330	Monitor de sitio	Buen bot
4331	Buscador	Buen bot
4334	raspador	Buen bot
4335	Márketing	Buen bot
4336	Márketing	Buen bot
4339	Herramienta	Buen bot
4340	Crawler	Buen bot
4341	Crawler	Buen bot
4342	Analizador de vulnerabilidades	Buen bot
4343	Analizador de vulnerabilidades	Buen bot
4344	raspador	Buen bot
4377	Crawler	Buen bot
4378	Crawler	Buen bot
4379	Buscador	Buen bot
4380	Buscador	Buen bot
4381	Buscador	Buen bot
4382	Buscador	Buen bot
4383	Crawler	Buen bot
4384	Buscador	Buen bot
4385	Herramienta	Buen bot

Regla de firma bot	ID	Descripción
4386	Sin categoría	Buen bot
4387	Crawler	Buen bot
4388	Crawler	Buen bot
4389	Herramienta	Buen bot
4390	Herramienta	Buen bot
4391	Herramienta	Buen bot
4392	Herramienta	Buen bot
4393	Herramienta	Buen bot
4394	Sin categoría	Buen bot
4395	Herramienta	Buen bot
4396	Monitor de sitio	Buen bot
4397	Monitor de sitio	Buen bot
4404	Buscador	Buen bot
4405	Buscador	Buen bot
4406	Buscador	Buen bot
4407	Sin categoría	Buen bot

Actualización de firma de bots para marzo de 2022

July 27, 2022

Se agregan nuevas firmas y se actualizan algunas de las firmas de bots existentes. Puede descargar y configurar estas reglas de firma para proteger su dispositivo de los ataques de bots.

Versión de firma bot

Signature, versión 12, aplicable a plataformas Citrix ADC con compilaciones 13.0 76.31 o una posterior.

Nuevas firmas de bots

A continuación se muestra una lista de ID de reglas de firma de bot, categoría y su tipo.

Regla de firma bot	ID	Descripción
4564	Márketing	Buen bot
4565	Márketing	Buen bot
4566	Márketing	Buen bot
4567	Márketing	Buen bot
4568	Márketing	Buen bot
4569	Sin categoría	Bot malo
4570	Sin categoría	Bot malo
4571	Crawler	Buen bot
4572	Crawler	Buen bot
4573	Sin categoría	Bot malo
4574	Sin categoría	Bot malo
4575	Márketing	Buen bot
4576	Márketing	Buen bot
4577	Márketing	Buen bot
4578	Márketing	Buen bot
4579	Márketing	Buen bot
4580	Márketing	Buen bot
4581	Márketing	Buen bot
4582	Márketing	Buen bot
4583	Creador de captura de pantalla	Buen bot
4584	Buscador	Buen bot
4585	Buscador	Buen bot
4586	Creador de captura de pantalla	Buen bot
4587	Sin categoría	Buen bot
4588	Probador de velocidad	Buen bot
4589	Crawler	Buen bot
4590	Herramienta	Buen bot

Regla de firma bot	ID	Descripción
4591	Herramienta	Buen bot
4592	Crawler	Bot malo
4593	Buscador	Buen bot
4594	Buscador	Buen bot
4595	Buscador	Buen bot
4596	Márketing	Buen bot
4597	Herramienta	Buen bot
4598	Buscador	Buen bot
4599	Márketing	Buen bot
4600	Márketing	Buen bot
4601	Márketing	Buen bot
4602	Buscador	Buen bot
4603	Sin categoría	Buen bot
4604	Márketing	Buen bot
4605	Márketing	Buen bot
4606	Sin categoría	Bot malo
4607	Sin categoría	Bot malo
4608	Herramienta	Buen bot
4609	Sin categoría	Bot malo
4610	Herramienta	Buen bot
4611	Herramienta	Buen bot
4612	raspador	Buen bot
4613	Sin categoría	Buen bot
4614	Sin categoría	Buen bot
4615	Monitor de sitio	Buen bot
4616	Crawler	Buen bot
4617	Monitor de sitio	Buen bot
4618	Buscador	Buen bot
4619	Márketing	Buen bot

Regla de firma bot	ID	Descripción
4620	Márketing	Buen bot
4621	Buscador	Buen bot
4622	Crawler	Buen bot
4623	Crawler	Buen bot
4624	Crawler	Buen bot
4625	raspador	Buen bot
4626	Crawler	Buen bot
4627	Analizador de vulnerabilidades	Buen bot
4628	Herramienta	Buen bot
4629	Sin categoría	Bot malo
4630	Sin categoría	Bot malo
4631	Herramienta	Buen bot
4632	Buscador de alimentación	Buen bot
4633	Crawler	Bot malo
4634	Sin categoría	Buen bot
4635	Buscador de alimentación	Buen bot
4636	Sin categoría	Buen bot
4637	Herramienta	Buen bot
4638	Herramienta	Buen bot
4639	raspador	Bot malo
4640	Sin categoría	Bot malo
4641	Herramienta	Buen bot
4642	Crawler	Bot malo
4643	Monitor de sitio	Buen bot
4644	Monitor de sitio	Buen bot
4645	Buscador	Buen bot
4646	Buscador	Buen bot
4647	Buscador	Buen bot

Regla de firma bot	ID	Descripción
4648	Buscador	Buen bot
4649	Buscador	Bot malo
4650	Sin categoría	Buen bot

Firmas de bot actualizadas

A continuación se muestra una lista de ID de reglas de firma de bot, categoría y su tipo.

Regla de firma bot	ID	Descripción
2554	Sin categoría	Bot malo
3835	Buscador	Buen bot
4027	Buscador	Buen bot
4038	Sin categoría	Bot malo
4085	Herramienta	Buen bot
4098	Crawler	Buen bot
4100	Buscador	Buen bot
4220	Herramienta	Buen bot
4224	Buscador	Buen bot
4281	Sin categoría	Bot malo
4412	Márketing	Buen bot
4425	Márketing	Buen bot
4429	Creador de captura de pantalla	Buen bot
4430	Analizador de virus	Buen bot
4483	Crawler	Buen bot
4552	Sin categoría	Buen bot
4562	Buscador	Buen bot
1000000	Explorador web	Buen bot
1000003	Explorador web	Buen bot
1000004	raspador	Buen bot

Regla de firma bot	ID	Descripción
1000005	Google_Crawler	Bot malo
1000006	Explorador web	Bot malo
1000007	Bot	Bot malo
1000008	Explorador web	Bot malo
1000009	Explorador web	Buen bot
1000010	Bot	Bot malo
1000011	Explorador web	Bot malo
1000012	raspador	Buen bot
1000013	raspador	Bot malo
1000014	raspador	Bot malo
1000015	Explorador web	Buen bot
1000016	Bot	Bot malo
1000017	Explorador web	Bot malo
1000018	Explorador web	Buen bot
1000019	raspador	Buen bot
1000020	raspador	Buen bot
1000021	raspador	Buen bot
1000022	Google_Crawler	Buen bot
1000023	Explorador web	Bot malo
1000024	Analizador	Buen bot
1000025	Analizador	Buen bot
1000026	Analizador	Buen bot
1000027	Analizador	Buen bot
1000028	Analizador	Buen bot
1000029	Explorador web	Buen bot
1000030	Analizador	Buen bot
1000031	Analizador	Buen bot
1000032	Explorador web	Bot malo
1000033	Analizador	Buen bot

Regla de firma bot	ID	Descripción
1000034	Explorador web	Bot malo
1000035	raspador	Buen bot
1000036	raspador	Buen bot
1000037	Explorador web	Buen bot
1000038	Analizador	Buen bot
1000039	Analizador	Buen bot
1000040	Analizador	Buen bot
1000041	Analizador	Buen bot
1000042	Analizador	Buen bot
1000043	Analizador	Buen bot
1000044	Analizador	Buen bot
1000045	Google_App_Engine_Software	Buen bot
1000046	Google_Crawler	Buen bot
1000047	Explorador web	Bot malo
1000048	Explorador web	Bot malo
1000049	Analizador	Buen bot
1000050	Explorador web	Bot malo
1000051	Explorador web	Buen bot
1000052	Explorador web	Bot malo
1000053	raspador	Buen bot
1000054	Google_Crawler	Bot malo
1000055	raspador	Bot malo
1000056	Analizador	Buen bot
1000057	Explorador web	Bot malo
1000058	Explorador web	Bot malo
1000059	Explorador web	Bot malo
1000060	raspador	Bot malo
1000061	Application	Bot malo
1000062	raspador	Bot malo

Regla de firma bot	ID	Descripción
1000063	raspador	Bot malo
1000064	raspador	Buen bot
1000065	raspador	Bot malo
1000066	raspador	Bot malo
1000067	Explorador web	Bot malo
1000068	raspador	Bot malo
1000069	Explorador web	Bot malo
1000070	raspador	Bot malo
1000071	Application	Bot malo

Redirección de caché

January 12, 2021

En una implementación típica, diferentes clientes piden a los servidores web el mismo contenido repetidamente. Para evitar que el servidor web de origen procese cada solicitud, un dispositivo Citrix ADC con redirección de caché habilitada puede servir este contenido desde un servidor de caché en lugar de desde el servidor de origen.

El dispositivo Citrix ADC analiza las solicitudes entrantes, envía solicitudes de datos en caché a servidores de caché y envía solicitudes no en caché y solicitudes HTTP dinámicas a servidores de origen.

La redirección de caché es una función basada en directivas. De forma predeterminada, las solicitudes que coinciden con una directiva se envían al servidor de origen y todas las demás solicitudes se envían a un servidor de caché. Para pruebas o mantenimiento, es posible que quiera omitir la evaluación de directivas y dirigir todas las solicitudes a la caché o al servidor de origen.

Puede combinar el cambio de contenido con la redirección de caché para almacenar contenido selectivo en caché y servir contenido desde servidores de caché específicos para tipos específicos de contenido solicitado.

Un dispositivo Citrix ADC configurado para la redirección de caché se puede implementar en el borde de una red, frente al servidor de origen o en cualquier lugar a lo largo de la red troncal. En una implementación perimetral, comúnmente utilizada por los proveedores de servicios Internet (ISP), las compañías de cable, las redes de distribución de contenido y las redes empresariales, el dispositivo Citrix ADC reside directamente frente a los clientes. En una implementación del lado del servidor, el

dispositivo Citrix ADC está más cerca de los servidores de origen.

La redirección de caché se usa con mayor frecuencia con el tipo de servicio HTTP, pero también admite el protocolo HTTPS seguro.

Directivas de redirección de caché

January 12, 2021

Un servidor virtual de redirección de caché aplica directivas de redirección de caché a cada solicitud entrante. De forma predeterminada, si una solicitud coincide con una de las directivas configuradas, se considera que no se puede almacenar en caché y el dispositivo Citrix ADC la envía al servidor de origen. Otras solicitudes se envían a un servidor de caché. Este comportamiento se puede revertir, de modo que las solicitudes que coinciden con las directivas de redirección de caché configuradas se envían a los servidores de caché.

El dispositivo proporciona un conjunto de directivas para la redirección de caché. Si estas directivas integradas no son adecuadas para la implementación, puede configurar las directivas de redirección de caché definidas por el usuario.

Nota: Una vez que haya determinado qué directivas de redirección de caché integradas utilizar o haya creado directivas definidas por el usuario, proceda a configurar la redirección de caché. Para utilizar esta función, debe configurar al menos un servidor virtual de redirección de caché y, para el funcionamiento normal, debe enlazar al menos una directiva de redirección de caché a ese servidor virtual.

Directivas de redirección de caché integradas

October 5, 2021

El dispositivo Citrix ADC proporciona directivas de redirección de caché integradas que gestionan las solicitudes de caché típicas. Estas directivas se basan en los métodos HTTP, los tokens de URL o URL de la solicitud entrante, la versión HTTP o los encabezados HTTP y sus valores en la solicitud.

Las directivas de redirección de caché integradas se pueden enlazar directamente a un servidor virtual y no necesitan configuración adicional.

Las directivas de redirección de caché utilizan dos tipos de lenguajes de expresiones de dispositivo: la directiva clásica y la directiva avanzada. Para obtener más información sobre estos idiomas, consulte Directivas y expresiones.

Directivas de redirección de caché clásicas integradas

Las directivas de redirección de caché integradas basadas en expresiones clásicas se denominan *directivas de redirección de caché clásicas*. Para obtener una descripción completa de las expresiones clásicas y cómo configurarlas, consulte Directivas y expresiones.

Las directivas clásicas de redirección de caché evalúan las funciones básicas del tráfico y otros datos. Por ejemplo, las directivas clásicas de redirección de caché pueden determinar si una solicitud o respuesta HTTP contiene un tipo concreto de encabezado o URL.

El dispositivo Citrix ADC proporciona las siguientes directivas de redirección de caché clásicas integradas:

Nombre de directiva integrado	Descripción
bypass-no-get	Omitir la caché si la solicitud utiliza un método HTTP distinto de GET.
bypass-cache-control	Omitir la caché si el encabezado de solicitud contiene un encabezado Cache-Control: no-cache o Cache-Control: no-store, o si la solicitud HTTP contiene un encabezado pragma.
bypass-dinámica-url	Omite la caché si la URL sugiere que el contenido es dinámico, como indica la presencia de cualquiera de las siguientes extensiones: cgi, asp, exe, cfm, ex, shtml o htx. También omite la caché si la URL comienza con cualquiera de los siguientes elementos: /cgi-bin/, /bin/ o /exec/.
tokens de bypass-url	Omite la caché porque la solicitud es dinámica, como indica uno de los siguientes tokens en la URL:? ,! , o =.
cookie de bypass	Omite la caché de cualquier URL que tenga un encabezado de cookie y una extensión distinta de .png o .jpg.

Directivas de redirección de caché de directivas avanzadas integradas

Las directivas de redirección de caché integradas basadas en expresiones de directivas avanzadas se denominan *directivas avanzadas de redirección de caché de directivas*. Para obtener una descripción

completa de las expresiones de directivas avanzadas y cómo configurarlas, consulte Directivas y expresiones.

Además de los mismos tipos de evaluaciones que realizan las directivas de redirección de caché clásicas, las directivas de redirección de caché de directivas avanzadas permiten analizar más datos (por ejemplo, el cuerpo de una solicitud HTTP) y configurar más operaciones en la regla de directiva (por ejemplo, dirigir la solicitud a la memoria caché o servidor origen).

Los dispositivos Citrix ADC proporcionan las dos acciones integradas siguientes para las directivas de redirección de caché de directivas avanzadas:

- CACHÉ
- ORIGEN

Según sus nombres, dirigen la solicitud al servidor de caché o al servidor de origen, respectivamente.

Nota: Si utiliza la directiva de redirección de caché avanzada de directivas incorporada, no podrá modificar la acción.

El dispositivo Citrix ADC proporciona las siguientes directivas de redirección de caché de directivas avanzadas integradas:

Nombre de directiva integrado	Descripción
bypass-no-get_adv	Omitir la caché si la solicitud utiliza un método HTTP distinto de GET.
bypass-cache-control_adv	Omitir la caché si el encabezado de solicitud contiene un encabezado Cache-Control: no-cache o Cache-Control: no-store, o si la solicitud HTTP contiene un encabezado pragma.
bypass-dinámica-url_adv	Omite la caché si la URL sugiere que el contenido es dinámico, como indica la presencia de cualquiera de las siguientes extensiones: cgi, asp, exe, cfm, ex, shtml o htx. También omite la caché si la URL comienza con cualquiera de los siguientes elementos: /cgi-bin/, /bin/ o /exec/.
bypass-urltokens_adv	Omite la caché porque la solicitud es dinámica, como indica uno de los siguientes tokens en la URL:? ,! , o =.

Nombre de directiva integrado	Descripción
bypass-cookie_adv	Omite la caché de cualquier URL que tenga un encabezado de cookie y una extensión distinta de .png o .jpg.

Mostrar las directivas de redirección de caché integradas

Puede mostrar las directivas de redirección de caché disponibles mediante la interfaz de línea de comandos o la utilidad de configuración.

Mostrar las directivas de redirección de caché integradas mediante la CLI

En el símbolo del sistema, escriba:

```
show cr policy [<policyName>]
```

Ejemplo:

```
> show cr policy
1)       Cache-By-Pass RULE: NS_NON_GET          Policy:bypass-non-get
2)       Cache-By-Pass RULE: (NS_CACHECONTROL_NOSTORE ||
   NS_CACHECONTROL_NOCACHE || NS_HEADER_PRAGMA)    Policy:bypass-cache-
   control
3)       Cache-By-Pass RULE: (NS_EXT_CGI || NS_EXT_ASP || NS_EXT_EXE ||
    NS_EXT_CFM || NS_EXT_EX || NS_EXT_SHTML || NS_EXT_HTX) || (
   NS_URL_PATH_CGIBIN || NS_URL_PATH_EXEC || NS_URL_PATH_BIN)
   Policy:bypass-dynamic-url
4)       Cache-By-Pass RULE: NS_URL_TOKENS       Policy:bypass-
   urltokens
5)       Cache-By-Pass RULE: (NS_HEADER_COOKIE && NS_EXT_NOT_GIF &&
   NS_EXT_NOT_JPEG)     Policy:bypass-cookie
 Done
<!--NeedCopy-->
```

Mostrar las directivas de redirección de caché integradas mediante la interfaz gráfica de usuario

1. Vaya a Gestión de tráfico > Redirección de caché > Directivas. Las directivas de redirección de caché configuradas aparecen en el panel de detalles.
2. Seleccione una de las directivas configuradas para ver los detalles.

Configurar una directiva de redirección de caché

February 19, 2022

Una directiva de redirección de caché incluye una expresión (también denominada *regla*). La expresión representa una condición que se evalúa cuando la solicitud del cliente se compara con la directiva.

No se configuran acciones explícitamente para directivas de redirección de caché.

Una directiva de redirección de caché tiene un nombre e incluye una expresión de directiva avanzada o un conjunto de cláusulas de expresión de directivas avanzadas que se combinan mediante operadores lógicos y las siguientes acciones integradas:

- CACHÉ
- ORIGEN

Para obtener más información sobre las expresiones de directivas avanzadas, consulte Directivas y expresiones.

Agregar una directiva de redirección de caché mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para agregar una directiva de redirección de caché y comprobar la configuración:

```
1 -  add cr policy <policyName> \*\*-rule\*\* <expression> -action<string
     > [-logAction<string>]
2
3 -  show cr policy [<policyName>]
4
5 <!--NeedCopy-->
```

Ejemplos:

Directiva con una expresión sencilla:

```
1 > add cr policy crpol1 -rule !(HTTP.REQ.URL.ENDSWITH(".jpeg")) -action
     origin
2  Done
3 > show cr policy crpoll
4     Policy: crpol1 Rule: !(HTTP.REQ.URL.ENDSWITH(".jpeg")) Action:
         ORIGIN
```



```
    Hits: 0
 Done

<!--NeedCopy-->
```

Directiva con una expresión compuesta:

```
> add cr policy crpol11 -rule 'http.req.method.eq(post) && (HTTP.REQ.
   URL.ENDSWITH(".png") || HTTP.REQ.URL.ENDSWITH(".cgi"))'  -action
   cache
 Done
> show cr policy crpol11
    Policy: crpol11    Rule: http.req.method.eq(post) && (HTTP.REQ.URL.
       ENDSWITH(".png") || HTTP.REQ.URL.ENDSWITH(".cgi"))  Action:
       CACHE
    Hits: 0
 Done

<!--NeedCopy-->
```

Directiva que evalúa un encabezado:

```
> add cr policy crpol12 -rule http.req.header("If-Modified-Since").
   exists -action origin
 Done
> show cr policy crpol12
    Policy: crpol12    Rule: http.req.header("If-Modified-Since").
       exists   Action: ORIGIN
    Hits: 0
 Done

<!--NeedCopy-->
```

Modificar o quitar una directiva de redirección de caché mediante la CLI

- Para modificar una directiva de redirección de caché, utilice el comando set cr policy, que es igual que el comando add cr policy, excepto que introduce el nombre de una directiva existente y solo tiene que proporcionar los parámetros que quiere modificar.
- Para quitar una directiva, utilice el comando `rm cr policy`, que solo acepta el argumento <name>. Si la directiva está enlazada a un servidor virtual, debe desvincularla antes de poder quitarla.

Para obtener información detallada sobre cómo desvincular una directiva de redirección de caché, consulte Desvincular una directiva de un servidor virtual de redirección de caché.

Configure una directiva de redirección de caché con una expresión simple mediante la interfaz gráfica de usuario

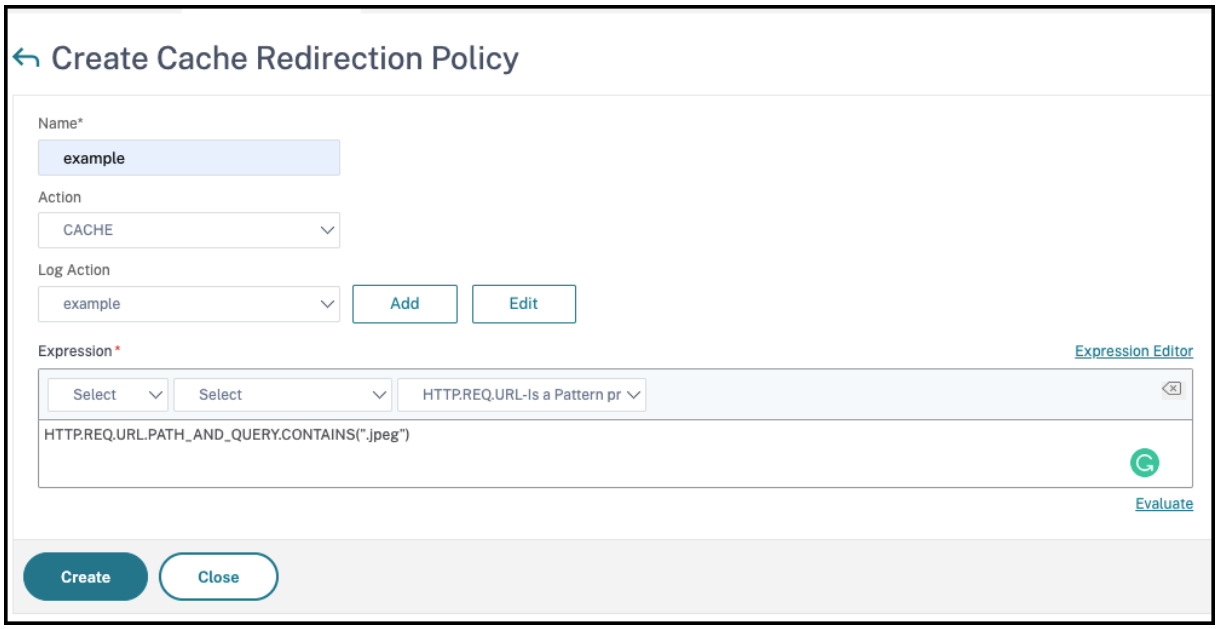
1. Vaya a **Administración del tráfico > Redirección de caché > Directivas**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En el cuadro de diálogo **Crear directiva de redirección de caché**, en el cuadro de texto **Nombre**, escriba el nombre de la directiva.
4. Seleccione la acción adecuada **CACHE** u **ORIGIN** en la lista desplegable **Acción**.
5. En el área **Acción de registro**, haga clic en **Agregar**. Escriba un nombre en el cuadro de diálogo **Crear acción de mensaje de auditoría**.
   - Configure **Log Level** seleccionando el valor adecuado de la lista desplegable:
     - **EMERGENCIA**
     - **ALERTA**
     - **CRÍTICA**
     - **ERROR**
     - **ADVERTENCIA**
     - **NOTIFICACIÓN**
     - **INFORMATIVO**
     - **DEBUG**
   - Introduzca la expresión en el área **Expresión**.
     - Tipo de expresión-General
     - Tipo de flujo -REQ
     - Protocolo -HTTP
     - Calificador -URL
     - Operador -! =
     - Valor - /.jpeg
   - Haga clic en **Crear**.
6. Para configurar una expresión sencilla, introduzca la expresión. A continuación se muestra un ejemplo de expresión que comprueba si hay una extensión `.jpeg` en una URL:
   - Tipo de expresión-General
   - Tipo de flujo -REQ
   - Protocolo -HTTP
   - Calificador -URL

- Operador -! =
- Valor - /.jpeg

La expresión simple del siguiente ejemplo comprueba si hay un encabezado If-Modified-Since en una solicitud:

- Tipo de expresión-General
- Tipo de flujo -REQ
- Protocolo -HTTP
- Calificador -HEADER
- Operador -EXISTS
- Nombre de encabezado -If-Modified-Since

7. Cuando haya terminado de introducir la expresión, haga clic en **Crear**.



Configurar una directiva de redirección de caché con una expresión compuesta mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Redirección de caché > Directivas**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En el cuadro de texto **Nombre**, introduzca un nombre para la directiva.

   El nombre puede comenzar con una letra, un número o un símbolo de subrayado, y puede constar de una a 127 letras, números y los símbolos de guión (-), punto (.), almohadilla (#), espacio ( ), en (@), igual (=) y guión bajo (_). Debe elegir un nombre que facilite a otros saber qué tipo de contenido se creó esta directiva para detectar.

4. Seleccione la acción adecuada **CACHE** u **ORIGIN** en la lista desplegable **Acción**.
5. En el área **Acción de registro**, haga clic en **Agregar**. Escriba un nombre en el cuadro de diálogo **Crear acción de mensaje de auditoría**.
    - Configure **Log Level** seleccionando el valor adecuado de la lista desplegable:
        - **EMERGENCIA**
        - **ALERTA**
        - **CRÍTICA**
        - **ERROR**
        - **ADVERTENCIA**
        - **NOTIFICACIÓN**
        - **INFORMATIVO**
        - **DEBUG**
    - Introduzca la expresión en el área **Expresión**.
        - Tipo de expresión-General
        - Tipo de flujo -REQ
        - Protocolo -HTTP
        - Calificador -URL
        - Operador -! =
        - Valor - /.jpeg
    - Haga clic en **Crear**.
6. Elija el tipo de expresión compuesta que quiere crear. Las opciones disponibles son:
    - **Haga coincidir cualquier expresión**. La directiva coincide con el tráfico si una o más expresiones individuales coinciden con el tráfico.
    - **Coincidir con todas las expresiones**. La directiva coincide con el tráfico solo si cada expresión individual coincide con el tráfico.
    - **Expresiones tabulares**. Cambia la lista Expresiones a un formato tabular con tres columnas. En la columna situada más a la derecha, coloque uno de los siguientes operadores:
        - El operador AND [&&], para exigir que, para que coincida con la directiva, una solicitud debe coincidir tanto con la expresión actual como la siguiente expresión.

El operador OR [	], para exigir que, para que coincida con la directiva, una solicitud debe coincidir con la expresión actual o la siguiente expresión, o ambas. Solo si la solicitud no coincide con ninguna de las expresiones, no coincide con la directiva.

–

También puede agrupar expresiones en subgrupos anidados seleccionando una expresión existente y haciendo clic en uno de los siguientes operadores:

- El operador BEGIN SUBGROUP [+ ( ] que indica al dispositivo Citrix ADC que inicie un subgrupo anidado con la expresión seleccionada. (Para quitar este operador de la expresión, haga clic en: (.)
- Operador END SUBGROUP [+)], que indica al dispositivo Citrix ADC que finalice el subgrupo anidado actual con la expresión seleccionada. (Para quitar este operador de la expresión, haga clic en -).)

- **Formato libre avanzado**. Apaga por completo el Editor de expresiones y convierte la lista Expresiones en un área de texto en la que se puede escribir una expresión compuesta. Este es el método más potente y más difícil para crear una expresión de directiva, y solo se recomienda para aquellos que estén familiarizados con el lenguaje de expresiones clásicas de Citrix ADC.

  Para obtener más información sobre la creación de expresiones clásicas en el área de texto de formato libre avanzado, consulte Configuración de directivas y expresiones clásicas.

  Precaución: Si cambia al modo de edición de expresiones de formato libre avanzado, no podrá volver a ninguno de los otros modos. No elija este modo de edición de expresiones a menos que esté seguro de que quiere utilizarlo.

7. Si ha seleccionado Coincidir con cualquier expresión, Coincidir con todas las expresiones o Expresiones tabulares, haga clic en **Agregar** para mostrar el cuadro de diálogo Agregar expresión.

   Debe dejar el tipo de expresión establecido en General para las directivas de redirección de caché.

8. En la lista desplegable Tipo de flujo, elija un tipo de flujo para su expresión.

El tipo de flujo determina si la directiva examina las conexiones entrantes o salientes. Tienes dos opciones:

- **REQ**. Configura el dispositivo Citrix ADC para examinar las conexiones entrantes o las solicitudes.
- **RES**. Configura el dispositivo para examinar las conexiones salientes o las respuestas.

9. En la lista desplegable Protocolo, elija un protocolo para su expresión.

   El protocolo determina el tipo de información que la directiva examina en la solicitud o respuesta. En función de si ha elegido REQ o RES en la lista desplegable anterior, estarán disponibles las cuatro o solo tres de las siguientes opciones:

   - **HTTP**. Configura el dispositivo para que examine el encabezado HTTP.
   - **SSL**. Configura el dispositivo para que examine el certificado de cliente SSL. Disponible solo si seleccionó REQ (solicitudes) en la lista desplegable anterior.
   - **TCP**. Configura el dispositivo para que examine el encabezado TCP.
   - **IP**. Configura el dispositivo para que examine la dirección IP de origen o de destino.

10. Elija un calificador para su expresión en la lista desplegable Calificador.

    El contenido de la lista desplegable Calificador depende del protocolo elegido. En la tabla siguiente se describen las opciones disponibles para cada protocolo.

    Tabla 1. Calificadores de directivas de redirección de caché disponibles para cada protocolo

Protocolo	Clasificatorio	Definición
HTTP	METHOD	Método HTTP utilizado en la solicitud.
-	URL	Contenido del encabezado URL.
-	URLTOKENS	Tokens de URL en el encabezado HTTP.
-	VERSIÓN	Versión HTTP de la conexión.
-	HEADER	Parte del encabezado de la solicitud HTTP.
-	URLLEN	Longitud del contenido del encabezado URL.
-	URLQUERY	Consulta parte del contenido del encabezado URL.
-	URLQUERYLEN	Longitud de la parte de consulta del encabezado URL.

Protocolo	Clasificatorio	Definición
SSL	CLIENT.CERT	Certificado de cliente SSL en su conjunto.
-	CLIENT.CERT. ASUNTO	Contenido del campo asunto del certificado de cliente.
-	CLIENT.CERT.EMISOR	Emisor del certificado de cliente.
-	CLIENT.CERT.SIGALGO	Algoritmo de firma utilizado en el certificado de cliente.
-	CLIENT.CERT.VERSION	Versión del certificado de cliente.
-	CLIENT.CERT.VALIDFROM	Fecha a partir de la cual el certificado de cliente es válido. (Fecha de inicio).
-	CLIENT.CERT.VALIDO PARA	Fecha tras la cual el certificado de cliente deja de ser válido. (Fecha de finalización).
-	CLIENT.CERT.NÚMERO DE SERIE	Número de serie del certificado de cliente.
-	CLIENT.CIPHER.TYPE	Método de cifrado utilizado en el certificado de cliente.
-	CLIENT.CIPHER.BITS	Número de bits significativos de la clave de cifrado.
-	CLIENT.SSL.VERSION	Versión SSL del certificado de cliente.
TCP	SOURCEPORT	Puerto de origen de la conexión TCP.
-	DESTPORT	Puerto de destino de la conexión TCP.
-	MSS	Tamaño máximo de segmento (MSS) de la conexión TCP.
IP	SOURCEIP	Dirección IP de origen de la conexión.

Protocolo	Clasificatorio	Definición
-	DESTIP	Dirección IP de destino de la conexión.

11. Elija el operador de su expresión en la lista desplegable Operador.

    Tus elecciones dependen del calificador que hayas elegido en el paso anterior. La lista completa de operadores que pueden aparecer en esta lista desplegable es:

    - == . Coincide exactamente con la siguiente cadena de texto.
    - != . No coincide con la cadena de texto siguiente.
      - . Es mayor que el número entero siguiente.
    - CONTAINS . Contiene la siguiente cadena de texto.
    - CONTENTS . El contenido del encabezado, URL o consulta URL designados.
    - EXISTS . El encabezado o la consulta especificados ya existen.
    - NOTCONTAINS . No contiene la siguiente cadena de texto.
    - NOTEXISTS . El encabezado o la consulta especificados no existen.

    Si quiere que esta directiva funcione en solicitudes enviadas a un host específico, puede dejar el signo predeterminado, el signo igual (==).

12. Si el cuadro de texto Valor está visible, escriba la cadena o el número adecuados en el cuadro de texto.

    Por ejemplo, si quiere que esta directiva seleccione las solicitudes enviadas al host shopping.example.com, debe escribir esa cadena en el cuadro de texto Valor.

13. Si ha elegido HEADER como calificador, escriba el encabezado que quiera en el cuadro de texto Nombre del encabezado.
14. Haga clic en **Aceptar** para agregar la expresión a la lista Expresión.
15. Repita los pasos 4 a 11 para crear más expresiones.
16. Haga clic en **Cerrar** para cerrar el cuadro de diálogo Agregar expresión y volver al cuadro de diálogo **Crear directiva de redirección de caché**.
17. Cuando haya terminado de introducir la expresión, haga clic en **Crear**.

Configuraciones de redirección de caché

January 12, 2021

Dependiendo de la implementación y la topología de red, puede configurar uno de los siguientes tipos de redirección de caché:

- **Transparente**. Una caché transparente puede residir en una variedad de puntos a lo largo de una red troncal para aliviar el tráfico a lo largo de la ruta de entrega. En modo transparente, el servidor virtual de redirección de caché intercepta todo el tráfico que fluye hacia el dispositivo Citrix ADC y aplica directivas de redirección de caché para determinar si el contenido debe servirse desde la caché o desde el servidor de origen.
- **Proxy de avance**. Un servidor de caché proxy de reenvío reside en el borde de una LAN empresarial y se enfrenta a la WAN. En el modo proxy de reenvío, el servidor virtual de redirección de caché resuelve el nombre de host de la solicitud entrante mediante un servidor DNS y reenvía las solicitudes de contenido no almacenable en caché a los servidores de origen resueltos. Las solicitudes que se pueden almacenar en caché se envían a los servidores de caché configurados.
- **Proxy inverso**. Las cachés proxy inverso se configuran para servidores de origen específicos. El tráfico entrante dirigido al proxy inverso puede servirse desde un servidor de caché o enviarse al servidor de origen con o sin modificación de la URL.

Configurar la redirección transparente

August 20, 2021

Al configurar la redirección de caché transparente, el dispositivo Citrix ADC evalúa todo el tráfico que recibe para determinar si se puede almacenar en caché. Este modo alivia el tráfico a lo largo de la ruta de entrega y se utiliza a menudo cuando el servidor de caché reside en la columna vertebral de un ISP o un transportista.

De forma predeterminada, las solicitudes que se pueden almacenar en caché se envían a un servidor de caché y las solicitudes que no se pueden almacenar en caché al servidor de origen. Por ejemplo, cuando el dispositivo Citrix ADC recibe una solicitud dirigida a un servidor web, compara los encabezados HTTP de la solicitud con un conjunto de expresiones de directiva. Si la solicitud no coincide con la directiva, el dispositivo reenvía la solicitud a un servidor de caché. Si la solicitud coincide con una directiva, el dispositivo reenvía la solicitud, sin cambios, al servidor web.

Para obtener más información sobre cómo modificar este comportamiento predeterminado, consulte Direct policy hits a la caché en lugar del origen.

Para configurar la redirección transparente, primero habilite la redirección de caché y el equilibrio de carga, y configure el modo de borde. A continuación, cree un servidor virtual de redirección de caché con una dirección IP comodín (*), de modo que este servidor virtual pueda recibir el tráfico que llega al dispositivo en cualquier dirección IP del dispositivo. Para este servidor virtual, vincule directivas de redirección de caché que describen los tipos de solicitudes que no deben almacenarse en caché. A continuación, cree un servidor virtual de equilibrio de carga que recibirá tráfico del servidor virtual de redirección de caché para solicitudes en caché. Por último, cree un servicio que represente un servidor de caché físico y vincularlo al servidor virtual de equilibrio de carga.

Habilitar la redirección de caché y el equilibrio de carga

October 5, 2021

Las funciones de redirección de caché del dispositivo y equilibrio de carga no están habilitadas de forma predeterminada. Deben activarse antes de que surta efecto cualquier configuración de redirección de caché.

Habilitar la redirección de caché y el equilibrio de carga mediante la CLI

En el símbolo del sistema, escriba el siguiente comando para habilitar la redirección de caché y el equilibrio de carga y compruebe la configuración:

```
1 -  enable ns feature cr lb
2 -  show ns feature
3 <!--NeedCopy-->
```


Ejemplo:

```
> enable ns feature cr lb
 Done
> show ns feature

        Feature                         Acronym             Status
        -------                         -------             ------
 1)     Web Logging                     WL                  ON
 2)     Surge Protection                SP                  ON
 3)     Load Balancing                  LB                  ON
 4)     Content Switching               CS                  ON
 5)     Cache Redirection               CR                  ON
            ...
            ...
            ...

 23)    appliance Push                  push                OFF
 Done
<!--NeedCopy-->
```

Habilitar la redirección de caché y el equilibrio de carga mediante la interfaz gráfica de usuario

1. En el panel de navegación, expanda **Sistema**y, a continuación, haga clic en **Configuración**.
2. Para habilitar la redirección de caché, en el panel de detalles, en **Modos y funciones**, haga clic en **Configurar funciones avanzadas**.
   a) En el cuadro de diálogo **Configurar funciones avanzadas**, active la casilla de verificación situada junto a **Redirección de caché**y, a continuación, haga clic en **Aceptar**.
   b) ¿En Activar/Desactivar funciones? cuadro de diálogo, haga clic en Sí.
3. Para habilitar el equilibrio de carga, en el panel de detalles, en **Modos y funciones**, haga clic en **Configurar funciones básicas**.
   a) En el cuadro de diálogo **Configurar funciones básicas**, active la casilla de verificación situada junto al equilibrio de carga y, a continuación, haga clic en **Aceptar**.
   b) ¿En Activar/Desactivar funciones? cuadro de diálogo, haga clic en Sí.

Configurar el modo de borde

August 20, 2021

Cuando se implementa en el borde de una red, el dispositivo Citrix ADC aprende dinámicamente sobre los servidores de esa red. El modo perimetral permite al dispositivo aprender dinámicamente hasta 40.000 servidores HTTP y conexiones TCP proxy para estos servidores.

Este modo activa la recopilación de estadísticas para los servicios aprendidos dinámicamente y se utiliza normalmente en implementaciones transparentes para la redirección de caché.

Habilitar el modo de borde mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para habilitar el modo de borde y compruebe la configuración:

```
-  enable ns mode Edge
-  show ns mode
<!--NeedCopy-->
```

Ejemplo:

```
> enable ns mode edge
 Done

> show ns mode

        Mode                          Acronym             Status
        -------                       -------             ------
          ...
          ...
          ...
 6)     MAC-based forwarding          MBF                 ON
 7)     Edge configuration            Edge                ON
 8)     Use Subnet IP                 USNIP               OFF
          ...
          ...
          ...
 16)    Bridge BPDUs                  BridgeBPDUs         OFF
 Done
<!--NeedCopy-->
```

Habilitar el modo de borde mediante la interfaz gráfica de usuario

1. En el panel de navegación, expanda Sistemay, a continuación, haga clic en Configuración.

2. En el panel de detalles, en Modos y funciones, haga clic en Configurar modos.
3. En el cuadro de diálogo Configurar modos, active la casilla de verificación situada junto a Configuración de borde y, a continuación, haga clic en Aceptar.
4. ¿En Activar/Desactivar función (s)?, haga clic en Sí.

Configurar un servidor virtual de redirección de caché

January 12, 2021

De forma predeterminada, un servidor virtual de redirección de caché reenvía las solicitudes que se pueden almacenar en caché al servidor virtual de equilibrio de carga para la caché y reenvía las solicitudes que no se pueden almacenar en caché al servidor de origen (excepto en una configuración proxy inversa, en la que las solicitudes que no se pueden almacenar en caché se envían a un servidor virtual de equilibrio de carga). Existen tres tipos de servidores virtuales de redirección de caché: Transparente, proxy de reenvío y proxy inverso.

Un servidor virtual de redirección de caché transparente utiliza una dirección IP de * y un número de puerto, normalmente 80, que puede aceptar el tráfico HTTP enviado a cualquier dirección IP que represente el dispositivo. Como resultado, solo puede configurar un servidor virtual de redirección de caché transparente. Los servidores virtuales de redirección de caché adicionales que configure deben ser servidores proxy de reenvío o de redirección de proxy inverso.

agregue un servidor virtual de redirección de caché en modo transparente mediante el comando cli

En el símbolo del sistema, escriba los siguientes comandos para agregar un servidor virtual de redirección de caché y verificar la configuración:

```
1 -  add cr vserver <name> <serviceType> [<IPAddress> <port> ] [-
     cacheType <cacheType>] [-redirect <redirect>]
2 -  show cr vserver [<name>]
3 <!--NeedCopy-->
```

Ejemplo:

```
1 add cr vserver Vserver-CRD-1 HTTP * 80 -cacheType TRANSPARENT -redirect
      POLICY
2 > show cr vserver Vserver-CRD-1
```



```
3          Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
4          State: UP  ARP:DISABLED
5          Client Idle Timeout: 180 sec
6          Down state flush: ENABLED
7          Disable Primary Vserver On Down : DISABLED
8          Default:        Content Precedence: RULE        Cache:
               TRANSPARENT
9          On Policy Match: ORIGIN L2Conn: OFF     OriginUSIP: OFF
10         Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF
11  Done
12 <!--NeedCopy-->
```

Modificar o quitar un servidor virtual de redirección de caché mediante la CLI

- Para modificar un servidor virtual, utilice el comando set cr vserver, que es igual que usar el comando add cr vserver, excepto que introduzca el nombre de un servidor virtual existente.
- Para quitar un servidor virtual, utilice el comando `rm cr vserver`, que acepta solo el argumento <name>.

Agregue un servidor virtual de redirección de caché en modo transparente mediante la interfaz gráfica de usuario

1. Vaya a Administración del tráfico > Redirección de caché > Servidores virtuales.
2. En el panel de detalles, haga clic en Agregar.
3. En el cuadro de diálogo Crear servidor virtual (redirección de caché), especifique los valores para los siguientes parámetros como se muestra:
   - Nombre*: Nombre
   - puerto*: Puerto

   *Un parámetro requerido
4. En la lista desplegable Protocolo, seleccione un protocolo compatible (por ejemplo, **HTTP**). Si el servidor virtual va a recibir tráfico en un puerto distinto del puerto estándar para el protocolo seleccionado, introduzca un nuevo valor en el campo Puerto.
5. Haga clic en la ficha Avanzadas.
6. Verifique que Tipo de caché esté establecido en TRANSPARENTE y Redirigir esté establecido en POLICY.
7. Haga clic en Crear y, a continuación, en Cerrar. El panel Servidores virtuales de redirección de caché muestra el nuevo servidor virtual.

8. Seleccione el nuevo servidor virtual de redirección de caché para mostrar los detalles de su configuración.

Vincular directivas al servidor virtual de redirección de caché

January 12, 2021

Las directivas de redirección de caché no están enlazadas automáticamente al servidor virtual de redirección de caché. Un servidor virtual de redirección de caché basado en directivas no puede funcionar a menos que se vincule al menos una directiva a él.

Vincular directivas a un servidor virtual de redirección de caché mediante la CLI

En el símbolo del sistema, escriba:

```
-  bind cr vserver <name> -policyName <string>
-  show cr vserver [<name>]
<!--NeedCopy-->
```

Ejemplo:

```
> bind cr vserver Vserver-CRD-1 -policyName bypass-cache-control
 Done
> bind cr vserver Vserver-CRD-1 -policyName bypass-dynamic-url
 Done
> bind cr vserver Vserver-CRD-1 -policyName bypass-urltokens
 Done
> bind cr vserver Vserver-CRD-1 -policyName bypass-cookie
 Done

> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: UP  ARP:DISABLED
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: RULE        Cache:
           TRANSPARENT
        On Policy Match: ORIGIN L2Conn: OFF     OriginUSIP: OFF
```



```
18          Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF
19
20  1)      Cache bypass  Policy: bypass-cache-control
21  2)      Cache bypass  Policy: bypass-dynamic-url
22  3)      Cache bypass  Policy: bypass-urltokens
23  4)      Cache bypass  Policy: bypass-cookie
24   Done
25  <!--NeedCopy-->
```

Enlazar una directiva definida por el usuario a un servidor virtual de redirección de caché mediante la interfaz gráfica de usuario

1. Vaya a Administración del tráfico > Redirección de caché > Servidores virtuales.
2. Haga clic en el servidor virtual que quiere configurar y haga clic en Abrir.
3. En la ficha Directivas, seleccione el tipo de directiva y, a continuación, haga clic en Insertar directiva.
4. En la columna Nombre de directiva, seleccione la directiva que quiere enlazar.
5. Haga clic en Aceptar.

Desenlazar una directiva de un servidor virtual de redirección de caché

January 12, 2021

Cuando desvincula una directiva del servidor virtual de redirección de caché, el dispositivo Citrix ADC ya no aplica la directiva al evaluar las solicitudes de cliente.

Desenlazar una directiva de un servidor virtual de redirección de caché mediante el comando CLI

En el símbolo del sistema, escriba:

```
1  -  unbind cr vserver <name> -policyName <string>
2  -  show cr vserver [<name>]
3  <!--NeedCopy-->
```

Ejemplo:


```
unbind cr vserver Vserver-CR-1 -policyName bypass-non-get
> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: UP  ARP:DISABLED
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: RULE        Cache:
           TRANSPARENT
        On Policy Match: ORIGIN L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF

1)      Cache bypass  Policy: bypass-cache-control
 Done
<!--NeedCopy-->
```

Desenlazar una directiva definida por el usuario de un servidor virtual de redirección de caché mediante la interfaz gráfica de usuario

1. Vaya a Administración del tráfico > Redirección de caché > Servidores virtuales.
2. Haga clic en el servidor virtual que quiere configurar y, a continuación, haga clic en Abrir.
3. En la ficha Directivas, en Nombre de directiva, seleccione la directiva que quiere desenlazar.
4. Haga clic en Desenlazar directiva y, a continuación, haga clic en Aceptar.

Crear un servidor virtual de equilibrio de carga

August 20, 2021

El servidor virtual de redirección de caché en el dispositivo Citrix ADC puede enviar solicitudes a una comunidad de servidores de caché, si la solicitud se puede almacenar en caché, o a la comunidad de servidores de origen si la solicitud no se puede almacenar en caché.

Cada servidor de caché está representado en el dispositivo por un servicio, que está enlazado a un servidor virtual de equilibrio de carga que recibe solicitudes del servidor virtual de redirección de caché y las reenvía a los servidores.

Para obtener más información sobre la configuración de servidores virtuales de equilibrio de carga y otras opciones de configuración, consulte Equilibrio de carga.

Crear un servidor virtual de equilibrio de carga mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para crear un servidor virtual de equilibrio de carga y compruebe la configuración:

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

Ejemplo:

```
> add lb vserver Vserver-LB-CR HTTP 10.102.20.30 80
 Done
> show lb vserver Vserver-LB-CR
        Vserver-LB-CR (10.102.20.30:80) - HTTP  Type: ADDRESS
        State: DOWN
        Last state change was at Fri Jul  2 08:47:52 2010
        Time since last state change: 0 days, 00:00:08.470
        Effective State: DOWN
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Port Rewrite : DISABLED
        No. of Bound Services :  0 (Total)       0 (Active)
        Configured Method: LEASTCONNECTION
        Mode: IP
        Persistence: NONE
        Vserver IP and Port insertion: OFF
        Push: DISABLED  Push VServer:
        Push Multi Clients: NO
        Push Label Rule: none
 Done
<!--NeedCopy-->
```

Crear un servidor virtual de equilibrio de carga mediante la interfaz gráfica de usuario

1. Vaya a Administración del tráfico > Equilibrio de carga > Servidores virtuales.
2. En el panel de detalles, haga clic en Agregar.
3. En el cuadro de diálogo Crear servidor virtual (equilibrio de carga), especifique valores para los siguientes parámetros como se muestra:

- Nombre*-Nombre
- Dirección IP*- Dirección IP
- Puerto*-puerto

*Un parámetro requerido

4. En la lista Protocolo, seleccione un protocolo compatible (por ejemplo, **HTTP**). Si el servidor virtual va a recibir tráfico en un puerto distinto del puerto conocido para el protocolo seleccionado, introduzca un nuevo valor en el campo Puerto.
5. Haga clic en Crear y, a continuación, en Cerrar. El panel Servidores virtuales de equilibrio de carga muestra el nuevo servidor virtual.

Configurar un servicio HTTP

January 12, 2021

En el dispositivo Citrix ADC, un servicio representa un servidor físico en la red. En la configuración de redirección de caché transparente, el servicio representa el servidor de caché. Las solicitudes que se pueden almacenar en caché son enviadas por el servidor virtual de redirección de caché al servidor virtual de equilibrio de carga, que a su vez reenvía cada solicitud al servicio correcto, que la transfiere al servidor de caché.

Configurar un servicio HTTP mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para crear un servicio HTTP y compruebe la configuración:

```
-  add service <name> <IP> <serviceType> <port> -cacheType <cacheType>
-  show service [<name>]
<!--NeedCopy-->
```

Ejemplo:

```
> add service Service-HTTP-1 10.102.29.40 HTTP 80 -cacheType
   TRANSPARENT
 Done
> show service Service-HTTP-1
        Service-HTTP-1 (10.102.29.40:80) - HTTP
        State: DOWN
```



```
6           Last state change was at Fri Jul  2 09:14:17 2010
7           Time since last state change: 0 days, 00:00:13.820
8           Server Name: 10.102.29.40
9           Server ID : 0   Monitor Threshold : 0
10          Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
11          Use Source IP: NO
12          Client Keepalive(CKA): NO
13          Access Down Service: NO
14          TCP Buffering(TCPB): NO
15          HTTP Compression(CMP): YES
16          Idle timeout: Client: 180 sec   Server: 360 sec
17          Client IP: DISABLED
18          Cache Type: TRANSPARENT Redirect Mode:
19          Cacheable: NO
20          SC: OFF
21          SP: ON
22          Down state flush: ENABLED
23
24  1)      Monitor Name: tcp-default
25                  State: DOWN     Weight: 1
26                  Probes: 3       Failed [Total: 3 Current: 3]
27                  Last response: Failure - Time out during TCP connection
                        establishment stage
28                  Response Time: N/A
29   Done
30  <!--NeedCopy-->
```

Modificar o quitar un servicio mediante la CLI

- Para modificar un servicio, utilice el comando set service, que es igual que el comando add service, excepto que escriba el nombre de un servicio existente.
- Para eliminar un servicio, utilice el comando `rm service`, que acepta solo el argumento <name>.

Agregar un servicio HTTP mediante la interfaz gráfica de usuario

1. Vaya a Administración del Tráfico > Equilibrio de Carga > Servicios
2. En el panel de detalles, haga clic en Agregar.
3. En el cuadro de diálogo Crear servicio, especifique valores para los siguientes parámetros como se muestra:
    - Nombre del servicio*: Nombre

- Servidor*: IP
- puerto*: Puerto

*Un parámetro requerido

4. En la lista desplegable Protocolo*, seleccione un protocolo compatible (por ejemplo, **HTTP**).
5. Haga clic en Crear y, a continuación, en Cerrar.

Vincular/desvincular un servicio desde/hasta un servidor virtual de equilibrio de carga

August 20, 2021

Debe vincular un servicio al servidor virtual de equilibrio de carga. Esto permite que el equilibrador de carga reenvíe la solicitud al servidor que representa el servicio. Si cambia la configuración, puede desvincular un servicio del servidor virtual de equilibrio de carga.

Enlazar un servicio a un servidor virtual de equilibrio de carga mediante la CLI

En el símbolo del sistema, escriba:

```
-  bind lb vserver <name> <serviceName>
-  show lb vserver [<name>]
<!--NeedCopy-->
```

Ejemplo:

```
> bind lb vserver vserver-LB-CR service-HTTP-1
 Done
> show lb vserver Vserver-LB-CR
        Vserver-LB-CR (10.102.20.30:80) - HTTP  Type: ADDRESS
        State: DOWN
        Last state change was at Fri Jul  2 08:47:52 2010
        Time since last state change: 0 days, 00:42:25.610
        Effective State: DOWN
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Port Rewrite : DISABLED
```



```
13          No. of Bound Services :  1 (Total)       0 (Active)
14          Configured Method: LEASTCONNECTION
15          Mode: IP
16          Persistence: NONE
17          Vserver IP and Port insertion: OFF
18          Push: DISABLED  Push VServer:
19          Push Multi Clients: NO
20          Push Label Rule: none
21
22  1) Service-HTTP-1 (10.102.29.40: 80) - HTTP State: DOWN Weight: 1
23   Done
24  <!--NeedCopy-->
```

Desenlazar un servicio de un servidor virtual de equilibrio de carga mediante la CLI

Para desvincular un servicio, utilice el comando `unbind lb vserver` en lugar de `bind lb vserver`.

Vincular o desvincular un servicio de un servidor virtual de equilibrio de carga mediante la interfaz gráfica de usuario

1. Vaya a Administración del Tráfico > Equilibrio de carga > Servidores virtuales
2. En el panel de detalles, seleccione el servidor virtual desde el que quiere enlazar o desvincular el servicio y, a continuación, haga clic en Abrir.
3. En la ficha Servicios, en la columna Activo, active o desactive la casilla de verificación situada junto al Nombre del servicio.
4. Haga clic en Aceptar.

Inhabilitar el uso de la configuración del puerto proxy para el almacenamiento en caché transparente

August 20, 2021

Si la opción Usar IP de origen (USIP) está inhabilitada en un servicio de caché configurado en el dispositivo Citrix ADC, el dispositivo reenvía las solicitudes de cliente al servicio de caché mediante una dirección IP de subred (SNIP) propiedad del dispositivo o una dirección IP asignada (MIP) como dirección IP de origen y un puerto aleatorio como puerto de origen. El puerto seleccionado aleatoriamente se denomina puerto proxy.

Sin embargo, si quiere configurar una caché totalmente transparente (una configuración de caché en la que el servicio de caché recibe la dirección IP y el número de puerto del cliente), no solo debe habilitar la opción USIP, ya sea globalmente o en el servicio de caché, sino también inhabilitar la configuración Usar puerto proxy, ya sea globalmente o en el servicio de caché. Al inhabilitar la opción Usar puerto proxy, el dispositivo puede utilizar el puerto de origen del cliente como puerto de origen cuando se conecta al servicio de caché, y garantiza una configuración de caché totalmente transparente.

Para obtener más información sobre la configuración de la opción Usar puerto proxy globalmente o en un servicio, consulte Configuración del puerto de origen para conexiones del lado del servidor.

Asignar un intervalo de puertos al dispositivo Citrix ADC

January 12, 2021

Compartir la dirección IP del cliente puede crear un conflicto que haga que los dispositivos de red, como enrutadores, servidores de caché, servidores de origen y otros dispositivos Citrix ADC, no puedan determinar el dispositivo y, por tanto, el cliente, al que se debe enviar la respuesta.

Un método para resolver este problema consiste en asignar un intervalo de puertos de origen al dispositivo Citrix ADC. Esta asignación permite a los dispositivos de red identificar inequívocamente el dispositivo Citrix ADC que envió la solicitud.

Asigne un intervalo de puertos de origen a un dispositivo Citrix ADC mediante la CLI

En el símbolo del sistema, escriba:

```
set ns param -crPortRange <startPortNumber-endPortNumber>
```

Asignar un intervalo de puertos de origen a un dispositivo Citrix ADC mediante la GUI del dispositivo

1. En el panel de navegación, haga clic en Sistema y, a continuación, haga clic en Configuración.
2. En el grupo Configuración, haga clic en el vínculo Cambiar la configuración global del sistema.
3. En el grupo Intervalo de puertos de redirección de caché, especifique el intervalo de puertos del dispositivo escribiendo un número de puerto para el puerto de inicio y un número de puerto para el puerto final.
4. Haga clic en Aceptar.

Habilitar servidores virtuales de equilibrio de carga para redirigir las solicitudes a la caché

January 12, 2021

Si un servidor virtual de equilibrio de carga está configurado para escuchar en una combinación de puertos y dirección IP determinada, tiene prioridad sobre el servidor virtual de redirección de caché para cualquier solicitud destinada a esa combinación de dirección-puerto. Por lo tanto, el servidor virtual de redirección de caché no procesa esas solicitudes.

Si quiere anular esta funcionalidad y dejar que el servidor virtual de redirección de caché decida si la solicitud debe ser servida desde la caché o no, configure el servidor virtual de equilibrio de carga particular para que sea almacenable en caché.

Esta configuración se utiliza normalmente cuando un ISP utiliza un dispositivo Citrix ADC en el borde de su red y todo el tráfico fluye a través del dispositivo.

Habilite los servidores virtuales de equilibrio de carga para redirigir las solicitudes a la caché mediante la CLI

En el símbolo del sistema, escriba:

```
-  set lb vserver <name> [-cacheable ( YES | NO)]
-  show lb vserver [<name>]
<!--NeedCopy-->
```

Ejemplo:

```
set lb vserver Vserver-LB-CR  - cacheable YES
> show lb vserver vserver-LB-CR
        Vserver-LB-CR (10.102.20.30:80) - HTTP  Type: ADDRESS
        State: DOWN
        Last state change was at Fri Jul  2 08:47:52 2010
        Time since last state change: 0 days, 01:05:51.510
        Effective State: DOWN
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Port Rewrite : DISABLED
        No. of Bound Services :  1 (Total)       0 (Active)
```



```
13          Configured Method: LEASTCONNECTION
14          Mode: IP
15          Persistence: NONE
16          Cacheable: YES  PQ: OFF SC: OFF
17          Vserver IP and Port insertion: OFF
18          Push: DISABLED  Push VServer:
19          Push Multi Clients: NO
20          Push Label Rule: none
21
22  1) Service-HTTP-1 (10.102.29.40: 80) - HTTP State: DOWN Weight: 1
23   Done
24  <!--NeedCopy-->
```

Para la redirección de caché transparente, el dispositivo intercepta todo el tráfico y evalúa cada solicitud para determinar si se puede almacenar en caché. Las solicitudes que no se pueden almacenar en caché se envían sin cambios al servidor de origen.

Al utilizar la redirección de caché transparente, es posible que quiera desactivar la redirección de caché para los servidores virtuales de equilibrio de carga que siempre dirigen el tráfico a los servidores de origen.

Desactivar el almacenamiento en caché para un servidor virtual de equilibrio de carga mediante la CLI

Para desactivar el almacenamiento en caché para un virtual de equilibrio de carga, utilice el comando unset lb vserver en lugar de set lb vserver. Especifique un valor de NO valor para el parámetro **almacenable en caché**.

Habilitar o inhabilitar los servidores virtuales de equilibrio de carga para redirigir las solicitudes a la caché mediante la interfaz gráfica de usuario

1. Vaya a Administración del tráfico > Equilibrio de carga > Servidores virtuales.
2. En el panel de detalles, seleccione el servidor virtual desde el que quiere habilitar/inhabilitar el almacenamiento en caché y, a continuación, haga clic en Abrir.
3. En la ficha Avanzadas, active o desactive la casilla de verificación Redirección de caché.
4. Haga clic en Aceptar.

Configurar la redirección de proxy de reenvío

August 20, 2021

Un proxy de reenvío es un único punto de contacto para un cliente o grupo de clientes. En esta configuración, el dispositivo Citrix ADC redirige las solicitudes que no se pueden almacenar en caché a un servidor de origen y redirige las solicitudes que se pueden almacenar en caché a una caché proxy de reenvío o a una caché transparente.

Cuando el dispositivo se configura como un proxy de reenvío, los usuarios deben modificar sus exploradores para que el explorador envíe solicitudes al proxy de reenvío en lugar de a los servidores de destino.

Un servidor virtual de redirección de caché proxy de reenvío en el dispositivo compara la solicitud con una directiva para el almacenamiento en caché. Si la solicitud no se puede almacenar en caché, el dispositivo consulta un servidor virtual de equilibrio de carga DNS para obtener la resolución del destino y, a continuación, envía la solicitud al servidor de origen. Si la solicitud se puede almacenar en caché, el dispositivo reenvía la solicitud a un servidor virtual de equilibrio de carga para la caché.

El dispositivo se basa en un nombre de dominio de host o una dirección IP en el encabezado HOST de la solicitud para determinar el destino solicitado. Si no hay ningún encabezado HOST en la solicitud, el dispositivo inserta un encabezado HOST basado en la dirección IP de destino de la solicitud.

Normalmente, el dispositivo Citrix ADC actúa como un proxy de reenvío en una LAN empresarial. En tal configuración, el dispositivo reside en el borde de una LAN empresarial e intercepta las solicitudes de cliente antes de que se vayan a la WAN. La configuración del dispositivo en el modo proxy de reenvío reduce el tráfico en la WAN.

Para configurar la redirección de caché de proxy de reenvío, habilite primero el equilibrio de carga y la redirección de caché en el dispositivo. A continuación, configure un servidor virtual de equilibrio de carga DNS y los servicios asociados. También configure un servidor virtual de equilibrio de carga y vincule a él los servicios apropiados para la caché. Configure un servidor virtual de redirección de caché de proxy de reenvío y vincule a él los servidores virtuales de equilibrio de carga y DNS. También debe configurar directivas de almacenamiento en caché y vincularlas al servidor virtual de redirección de caché. Para completar la configuración, configure los exploradores cliente para que utilicen el proxy de reenvío.

Para obtener más información sobre cómo habilitar la redirección de caché y el equilibrio de carga en el dispositivo, consulte Habilitar la redirección de caché y el equilibrio de carga.

Para obtener más información sobre cómo crear un servidor virtual de equilibrio de carga, consulte Crear un servidor virtual de equilibrio de carga.

Para obtener más información sobre cómo configurar los servicios que representan el servidor de caché, consulte Configurar un servicio HTTP.

Para obtener más información sobre cómo vincular el servicio a un servidor virtual, consulte Vincular o desvincular un servicio a/desde un servidor virtual de equilibrio de carga.

Para obtener más información sobre cómo crear un servidor de redirección de caché proxy de reen-

vío, consulte Configurar un servidor virtual de redirección de cachéy crear un servidor virtual de tipo TRANSPARENT o FORWARD.

Para obtener más información sobre cómo vincular directivas de redirección de caché al servidor virtual de redirección de caché, consulte Configurar una directiva de redirección de caché.

Crear un servicio DNS

August 20, 2021

Un servicio DNS es una representación, en el dispositivo Citrix ADC, de un servidor DNS físico en la red. Un servidor virtual de equilibrio de carga DNS envía solicitudes DNS al servidor DNS de la red a través de dicho servicio.

Crear un servicio DNS mediante la CLI

En la línea de comandos, escriba los siguientes comandos para crear un servicio DNS y verificar la configuración:

```
-  add service <name> <IP> <serviceType> <port>
-  show service [<name>]
<!--NeedCopy-->
```

Ejemplo:

```
add service Service-DNS-1 10.102.29.41 DNS 53
show service Service-DNS-1
        Service-DNS-1 (10.102.29.41:53) - DNS
        State: DOWN
        Last state change was at Fri Jul  2 10:14:32 2010
        Time since last state change: 0 days, 00:00:13.550
        Server Name: 10.102.29.41
        Server ID : 0   Monitor Threshold : 0
        Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
        Use Source IP: NO
        Client Keepalive(CKA): NO
        Access Down Service: NO
        TCP Buffering(TCPB): NO
        HTTP Compression(CMP): NO
        Idle timeout: Client: 120 sec   Server: 120 sec
```



```
16          Client IP: DISABLED
17          Cacheable: NO
18          SC: OFF
19          SP: OFF
20          Down state flush: ENABLED
21
22  1)      Monitor Name: ping-default
23                  State: DOWN     Weight: 1
24                  Probes: 3       Failed [Total: 3 Current: 3]
25                  Last response: Failure - Probe timed out.
26                  Response Time: 2000.0 millisec
27   Done
28  <!--NeedCopy-->
```

Agregar un servicio DNS mediante la interfaz gráfica de usuario

1. Vaya a Administración de Tráfico > Equilibrio de carga > Servicios.
2. En el panel de detalles, haga clic en Agregar.
3. En el cuadro de diálogo Crear servicio, especifique valores para los siguientes parámetros como se muestra:
   - Nombre del servicio*: Nombre
   - Servidor*: IP
   - puerto*: Puerto

*Un parámetro requerido

1. En la lista desplegable Protocolo*, seleccione un protocolo compatible (por ejemplo, **DNS**).
2. Haga clic en Crear y, a continuación, en Cerrar.

Crear un servidor virtual de equilibrio de carga DNS

January 12, 2021

El servidor virtual DNS permite que el proxy de reenvío realice la resolución DNS antes de reenviar una solicitud de cliente a un servidor de origen. El servidor virtual de equilibrio de carga DNS está asociado con el servicio DNS que representa el servidor DNS físico de la red.

Crear un servidor virtual de equilibrio de carga DNS mediante la CLI

En la línea de comandos, escriba los siguientes comandos para crear un servidor virtual de equilibrio de carga DNS y verificar la configuración:

```
-  add lb vserver <name> <serviceType>
-  show lb vserver [<name>]
<!--NeedCopy-->
```

Ejemplo:

```
> add lb vserver Vserver-DNS-1 DNS
 Done
> show lb vserver Vserver-DNS-1
        Vserver-DNS-1 (0.0.0.0:0) - DNS Type: ADDRESS
        State: DOWN
        Last state change was at Fri Jul  2 10:32:28 2010
        Time since last state change: 0 days, 00:00:08.10
        Effective State: DOWN  ARP:DISABLED
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  0 (Total)       0 (Active)
        Configured Method: LEASTCONNECTION
        Mode: IP
        Persistence: NONE
 Done
<!--NeedCopy-->
```

Crear un servidor virtual de equilibrio de carga DNS mediante la interfaz gráfica de usuario

1. Vaya a Administración del tráfico > Equilibrio de carga > Servidores virtuales.
2. En el panel de detalles, haga clic en Agregar.
3. En el cuadro de diálogo Crear servidor virtual (equilibrio de carga), en el cuadro Nombre, escriba un nombre para el servidor virtual.
4. En la lista desplegable Protocolo*, seleccione un protocolo compatible (por ejemplo, **DNS**).
5. Haga clic en Crear y, a continuación, en Cerrar. El panel Servidores virtuales DNS muestra el nuevo servidor virtual.

Enlazar el servicio DNS al servidor virtual

August 20, 2021

Para que el servidor DNS responda a las solicitudes DNS, el servicio que representa el servidor DNS debe estar enlazado al servidor virtual DNS.

Enlace el servicio DNS al servidor virtual de equilibrio de carga mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para enlazar el servicio DNS al servidor virtual de equilibrio de carga y compruebe la configuración:

```
-  bind lb vserver <name> <serviceName>
-  show lb vserver <name>
<!--NeedCopy-->
```

Ejemplo:

```
> bind lb vserver Vserver-DNS-1 Service-DNS-1
 Done
> show lb vserver Vserver-DNS-1
        Vserver-DNS-1 (0.0.0.0:0) - DNS Type: ADDRESS
        State: DOWN
        Last state change was at Fri Jul  2 10:32:28 2010
        Time since last state change: 0 days, 00:12:16.80
        Effective State: DOWN  ARP:DISABLED
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  1 (Total)       0 (Active)
        Configured Method: LEASTCONNECTION
        Mode: IP
        Persistence: NONE

1) Service-DNS-1 (10.102.29.41: 53) - DNS State: DOWN   Weight: 1
 Done
>
<!--NeedCopy-->
```


Desenlazar un servicio DNS del servidor virtual de equilibrio de carga mediante la CLI

Utilice el comando `unbind lb vserver` en lugar de `bind lb vserver`.

Vincular o desvincular un servicio DNS o un servidor virtual de equilibrio de carga mediante la interfaz gráfica de usuario

1. Vaya a Administración del Tráfico > Equilibrio de carga > Servidores virtuales
2. En el panel de detalles, seleccione el servidor virtual a/desde el que quiere enlazar o desvincular el servicio DNS y, a continuación, haga clic en Abrir.
3. En la ficha Servicios, en la columna Activo, active o desactive la casilla de verificación situada junto al Nombre del servicio.
4. Haga clic en Aceptar.

Configurar un explorador web cliente para utilizar un proxy de reenvío

January 12, 2021

Al configurar el dispositivo Citrix ADC como servidor virtual de redirección de caché de proxy de reenvío en la red, debe configurar el explorador web del cliente para que envíe solicitudes al proxy de reenvío. Normalmente, cuando se utiliza un proxy de reenvío, la única ruta a los servidores de la red es a través del proxy de reenvío.

Consulte la documentación del explorador para configurar el explorador para que utilice un proxy de reenvío. Especifique la dirección IP y el número de puerto del servidor virtual de redirección de caché de proxy de reenvío para esta configuración.

Configurar la redirección de proxy inverso

August 20, 2021

Un proxy inverso reside delante de uno o más servidores web y protege el servidor de origen de las solicitudes del cliente. A menudo, una caché de proxy inverso es un front-end para todas las solicitudes de cliente a un servidor. Un administrador asigna una caché proxy inversa a un servidor de origen específico. La caché proxy inversa es diferente a las cachés proxy transparentes y de reenvío, que almacenan en caché el contenido solicitado con frecuencia para todas las solicitudes a cualquier servidor de origen, y la elección de un servidor se basa en la solicitud.

A diferencia de una caché de proxy transparente, la caché de proxy inverso tiene su propia dirección IP y puede reemplazar dominios y direcciones URL de destino en una solicitud no almacenable en caché por nuevos dominios y direcciones URL de destino.

Puede implementar la redirección de caché de proxy inverso en el lado del servidor de origen o en el borde de una red. Cuando se implementa en el servidor de origen, el servidor virtual de redirección de caché de proxy inverso es un front-end para todas las solicitudes al servidor de origen.

En el modo proxy inverso, cuando el dispositivo recibe una solicitud, un servidor virtual de redirección de caché evalúa la solicitud y la reenvía a un servidor virtual de equilibrio de carga para la caché o a un servidor virtual de equilibrio de carga para el origen. La solicitud entrante se puede transformar cambiando el encabezado del host o la URL del host antes de enviarla al servidor back-end.

Para configurar la redirección de caché de proxy inverso, primero habilite la redirección de caché y el equilibrio de carga. A continuación, configure un servidor virtual de equilibrio de carga y servicios para enviar solicitudes en caché a los servidores de caché. Configure también un servidor virtual de equilibrio de carga y servicios asociados para los servidores de origen. A continuación, configure un servidor virtual de redirección de caché de proxy inverso y vincule las directivas de redirección de caché pertinentes a él. Por último, configure las directivas de asignación y vincularlas al servidor virtual de redirección de caché de proxy inverso.

Las directivas de asignación tienen una acción asociada que permite que el servidor virtual de redirección de caché reenvíe cualquier solicitud no almacenable en caché al servidor virtual de equilibrio de carga para el origen.

Asegúrese de crear el destino predeterminado del servidor de caché.

Para obtener más información sobre cómo habilitar la redirección de caché y el equilibrio de carga en el dispositivo, consulte Habilitar la redirección de caché y el equilibrio de carga.

Para obtener más información sobre cómo crear un servidor virtual de equilibrio de carga, consulte Crear un servidor virtual de equilibrio de carga.

Para obtener más información sobre cómo configurar los servicios que representan el servidor de caché, consulte Configurar un servicio HTTP.

Para obtener más información sobre cómo vincular el servicio a un servidor virtual, consulte Vincular o desvincular un servicio a/desde un servidor virtual de equilibrio de carga.

Para obtener más información sobre cómo crear un servidor de redirección de caché proxy inverso, consulte Configurar un servidor virtual de redirección de cachéy crear un servidor virtual de tipo REVERSE.

Para obtener más información sobre cómo vincular las directivas de redirección de caché integradas al servidor virtual de redirección de caché, consulte Vincular directivas al servidor virtual de redirección de caché.

Configurar directivas de asignación

Si una solicitud entrante no se puede almacenar en caché, el servidor virtual de redirección de caché de proxy inverso reemplaza el dominio y la URL de la solicitud por el dominio y la URL de un servidor de origen de destino y reenvía la solicitud al servidor virtual de equilibrio de carga para el origen.

Una directiva de asignación permite que el servidor virtual de redirección de caché de proxy inverso reemplace el dominio y la URL de destino y reenvíe la solicitud al servidor virtual de equilibrio de carga para el origen.

Una directiva de asignación debe traducir primero el dominio y la dirección URL y, a continuación, pasar la solicitud al servidor virtual de equilibrio de carga de origen.

Una directiva de asignación puede asignar un dominio, un prefijo de URL y un sufijo de URL, como se indica a continuación:

- Asignación de dominio: Puede asignar un dominio sin prefijo o sufijo. La asignación de dominio es la asignación predeterminada para el servidor virtual (por ejemplo, la asignación de www.mycompany.com a www.myrealcompany.com).
- Asignación de prefijo: Puede reemplazar un patrón especificado con prefijo como parte de la URL (por ejemplo, asignar www.mycompany.com/sports/index.html a www.mycompany.com/news/index.h
- Asignación de sufijos: Puede reemplazar el sufijo de archivo en la URL (por ejemplo, asignar www.mycompany.com/sports/index.html a www.mycompany.com/sports/index.asp).

Las cadenas de origen y destino que se están asignando deben ser similares. Si especifica un dominio de origen, debe especificar un dominio de destino y, si especifica un sufijo de origen, debe especificar un sufijo de destino. Del mismo modo, si especifica una URL exacta del origen, la URL de destino también debe ser una URL exacta.

Una vez que configure las directivas de asignación para el modo proxy inverso, debe vincularlas al servidor virtual de redirección de caché.

Puede utilizar combinaciones de la URL de origen, la URL de destino y los dominios de origen y destino para configurar los tres tipos de asignación de dominios.

Configurar una directiva de asignación para el modo proxy inverso mediante la CLI

En el símbolo del sistema, escriba el comando siguiente para agregar una asignación de directivas y verificar la configuración:

```
1 -  add policy map <mapPolicyName> -sd <string> [-su <string>] [-td <
     string>] [-tu <string>]
2 -  show policy map [<mapPolicyName>]
3 <!--NeedCopy-->
```


Ejemplo:

El siguiente comando asigna un dominio de una solicitud de cliente a un dominio de destino:

```
> add policy map myMappingPolicy -sd www.mycompany.com -td www.
   myrealcompany.com
 Done
> show policy map myMappingPolicy
1)      Name: myMappingPolicy
        Source Domain: www.mycompany.com        Source Url:
        Target Domain: www.myrealcompany.com    Target Url:
 Done
<!--NeedCopy-->
```

A continuación se muestra un ejemplo de asignación de un sufijo de URL a un sufijo de URL diferente:

```
> add policy map myOtherMappingPolicy -sd www.mycompany.com -td www.
   myrealcompany.com -su /news.html -tu /realnews.html
 Done
> show policy map myOtherMappingPolicy
1)      Name: myOtherMappingPolicy
        Source Domain: www.mycompany.com        Source Url: /news.html
        Target Domain: www.myrealcompany.com    Target Url: /realnews.
           html
 Done
<!--NeedCopy-->
```

Configurar una directiva de asignación para el modo proxy inverso mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Redirección de caché > Directivas de mapas**.
2. En el panel de detalles, haga clic en Agregar.
3. En el cuadro de diálogo Crear directiva de mapa, especifique valores para los siguientes parámetros como se muestra:
   - Nombre*- MapPolicyName
   - Dominio de origen*-SD
   - Dominio de destino*-TD
   - URL de origen
   - URL de destino

*Un parámetro requerido

4. Haga clic en Crear y, a continuación, en Cerrar. El panel Mapa muestra la nueva directiva de asignación.

Vincular la directiva de asignación al servidor virtual de redirección de caché mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para enlazar la directiva de asignación al servidor virtual de redirección de caché y compruebe la configuración:

```
-  bind cr vserver <name> -policyName <string> [<targetVserver>]
-  show cr vserver <name>
<!--NeedCopy-->
```

Ejemplo:

```
> bind cr vserver Vserver-CRD-3 -policyName myMappingPolicy Vserver-LB-
   CR
 Done
> show cr vserver Vserver-CRD-3
        Vserver-CRD-3 (10.102.29.50:88) - HTTP  Type: CONTENT
        State: UP
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default: Vserver-LB-CR  Content Precedence: RULE        Cache:
           REVERSE
        On Policy Match: ORIGIN L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF

1)      Policy:         Target: Vserver-LB-CR   Priority: 0     Hits: 0
1)      Map: myMappingPolicy Target: Vserver-LB-CR
 Done
<!--NeedCopy-->
```

Vincular la directiva de asignación al servidor virtual de redirección de caché mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Redirección de caché > Servidores virtuales**.
2. En el panel de detalles, seleccione el servidor virtual desde el que desea vincular la directiva de asignación y, a continuación, haga clic en **Abrir**.

3. En **Configurar servidor virtual**(redirección de caché), en la ficha **Directivas**, seleccione **Mapa**y, a continuación, haga clic en **Insertar directiva**.
4. En la columna **Nombre de directiva**, seleccione la directiva de la lista desplegable.
5. En la columna **Destino**, haga clic en la flecha hacia abajo y, a continuación, seleccione el servidor virtual de la lista desplegable.
6. Haga clic en **Aceptar**.

Redirección selectiva de caché

August 20, 2021

La redirección selectiva de caché envía solicitudes para determinados tipos de contenido, por ejemplo, imágenes, a un servidor de caché o grupo de servidores de caché y envía otros tipos de contenido a un servidor de caché o grupo de servidores de caché diferentes. Puede configurar la redirección avanzada de caché en los modos transparente, proxy inverso o proxy de reenvío.

En la redirección selectiva de caché, el dispositivo Citrix ADC intercepta una solicitud de cliente y reenvía las solicitudes que no se pueden almacenar en caché al destino original de la solicitud de cliente. En el caso de las solicitudes que se pueden almacenar en caché, el dispositivo envía las solicitudes al servidor de caché de destino que puede servir contenido de un tipo de contenido específico.

La redirección selectiva de caché implica la configuración de directivas de conmutación de contenido además de las directivas de redirección de caché. En primer lugar, el dispositivo evalúa las directivas de redirección de caché enlazadas al servidor virtual de redirección de caché. Si una solicitud coincide con una directiva de redirección de caché, el servidor virtual de redirección de caché envía la solicitud al servidor de origen o a un servidor virtual de equilibrio de carga para el origen. Si ninguna directiva de redirección de caché coincide con la solicitud, el dispositivo evalúa las directivas de conmutación de contenido enlazadas al servidor virtual de redirección de caché. Si una directiva de conmutación de contenido coincide con la solicitud, el servidor virtual de redirección de caché redirige la solicitud a un servidor virtual de equilibrio de carga para la caché.

Para configurar la redirección selectiva de caché, habilite primero la redirección de caché, el equilibrio de carga y la conmutación de contenido en el dispositivo Citrix ADC. A continuación, configure un servidor virtual de equilibrio de carga para la caché y un servicio HTTP asociado. Después de esto, configure un servidor virtual de redirección de caché y vincule las directivas de redirección de caché y conmutación de contenido a él. Una vez enlazadas las directivas, puede configurar el servidor virtual para que dé prioridad a las directivas de conmutación de contenido basadas en reglas o en URL.

Cuando se configura para la redirección de caché en modo transparente en una topología de implementación perimetral, el dispositivo envía todo el tráfico HTTP en caché a una comunidad de caché transparente. Los clientes acceden a Internet a través del dispositivo, que está configurado como un

conmutador de capa 4 que recibe tráfico en el puerto 80.

El dispositivo puede dirigir solicitudes de imágenes (por ejemplo, archivos.png y.jpg) a un servidor de la comunidad de caché transparente y todas las demás solicitudes de contenido estático a otros servidores de la comunidad. Para esta configuración, puede configurar directivas de conmutación de contenido para enviar imágenes a la caché de imágenes y enviar el resto del contenido que se pueda almacenar en caché a una caché predeterminada.

Nota: La configuración descrita aquí es para la redirección de caché selectiva transparente. Por lo tanto, no requiere un servidor virtual de equilibrio de carga para el origen, al igual que una configuración de proxy inverso.

Para configurar este tipo de redirección selectiva de caché, habilite primero la redirección de caché, el equilibrio de carga y la conmutación de contenido. A continuación, configure un servidor virtual de equilibrio de carga para la caché y configure un servicio HTTP asociado. A continuación, configure un servidor virtual de redirección de caché y cree y vincule directivas de redirección de caché y conmutación de contenido a este servidor virtual.

Para obtener más información sobre cómo habilitar la redirección de caché y el equilibrio de carga en el dispositivo, consulte Habilitar la redirección de caché y el equilibrio de carga.

Habilitar cambio de contenido

October 5, 2021

Para configurar la redirección selectiva de caché, después de habilitar las funciones de equilibrio de carga y redirección de caché en el dispositivo, debe habilitar el cambio de contenido.

Habilitar el cambio de contenido mediante la CLI

En el símbolo del sistema, escriba:

```
1 -  enable ns feature CS
2
3 -  show ns feature
4 <!--NeedCopy-->
```

Ejemplo:

```
1 > enable ns feature cs
```



```
 Done
> show ns feature

        Feature                         Acronym              Status
        -------                         -------              ------
 1)     Web Logging                     WL                   ON
 2)     Surge Protection                SP                   ON
 3)     Load Balancing                  LB                   ON
 4)     Content Switching               CS                   ON
 5)     Cache Redirection               CR                   ON
          ...
          ...
          ...
 23)    appliance Push                  push                 OFF
 Done
<!--NeedCopy-->
```

Habilitar la redirección de caché y el equilibrio de carga mediante la interfaz gráfica de usuario

1. En el panel de navegación, expanda **Sistema**y, a continuación, haga clic en **Configuración**.
2. En el panel de detalles, en Modos y funciones, haga clic en **Configurar funciones básicas**.
3. En el cuadro de diálogo **Configurar funciones básicas**, active la casilla de verificación situada junto a **Content Switching**y, a continuación, haga clic en **Aceptar**.
4. ¿En Activar/Desactivar funciones? cuadro de diálogo, haga clic en Sí.

Configurar un servidor virtual de equilibrio de carga para la caché

August 20, 2021

Cree un servidor virtual de equilibrio de carga y un servicio HTTP para cada tipo de servidor de caché que se utilizará. Por ejemplo, si quiere servir archivos JPEG de un servidor de caché y archivos GIF de otro servidor de caché y utilizar un tercer servidor de caché para el resto del contenido, cree un servicio HTTP y un servidor virtual para cada uno de los tres tipos de servidores de caché. A continuación, enlazar cada servicio a su servidor virtual respectivo.

Para obtener más información sobre cómo crear un servidor virtual de equilibrio de carga, consulte Crear un servidor virtual de equilibrio de carga.

Para obtener más información sobre cómo configurar los servicios que representan el servidor de caché, consulte Configurar un servicio HTTP.

Para obtener más información sobre cómo vincular el servicio a un servidor virtual, consulte Vincular o desvincular un servicio a/desde un servidor virtual de equilibrio de carga.

Para obtener más información sobre cómo crear un servidor de redirección de caché proxy transparente, consulte Configurar un servidor virtual de redirección de cachéy crear un servidor virtual de tipo TRANSPARENT.

Para obtener más información sobre cómo vincular las directivas de redirección de caché integradas al servidor virtual de redirección de caché, consulte Vincular directivas al servidor virtual de redirección de caché.

Configurar una directiva de redirección de caché para un tipo específico de contenido

Para identificar las solicitudes que contienen una extensión.png o.jpeg como almacenables en caché, configure una directiva de redirección de caché y la vincule al servidor virtual de redirección de caché.

Nota: Si una solicitud coincide con una directiva, el dispositivo Citrix ADC la reenvía al servidor de origen. Como resultado, en el procedimiento siguiente, configure directivas para que coincidan las solicitudes que
no tienen extensiones ".png" o ".jpeg".

Para configurar la redirección de caché para un tipo específico de contenido, configure una directiva que utilice una expresión simple, como se describe en Configurar una directiva de redirección de caché.

Configurar directivas para la conmutación de contenido

December 2, 2021

Debe crear una directiva de cambio de contenido para identificar tipos específicos de contenido que se dirigirán a un servidor o comunidad e identificar otros tipos de contenido para servir desde otro servidor o comunidad de caché. Por ejemplo, puede configurar una directiva para determinar la ubicación de los archivos de imagen con las extensiones.png y.jpeg.

Antes de crear la directiva de cambio de contenido, debe definir una acción de cambio de contenido para describir qué servidor virtual de equilibrio de carga debe seleccionar. Esta acción se usa en la directiva de cambio de contenido.

Después de definir la directiva de conmutación de contenido, la vincula a un servidor virtual de conmutación de contenido y especifica un servidor virtual de equilibrio de carga. Las solicitudes que coinciden con la directiva se reenvían al servidor virtual de equilibrio de carga con nombre. Las solicitudes que no coinciden con la directiva de conmutación de contenido se reenvían al servidor virtual de equilibrio de carga predeterminado para la caché.

Para obtener más información sobre la función de cambio de contenido y la configuración de las directivas de conmutación de contenido, consulte Cambio de contenido.

Primero debe crear la directiva de conmutación de contenido y, a continuación, vincularla al servidor virtual de conmutación de contenido.

Crear una directiva de conmutación de contenido mediante el comando CLI

En la línea de comandos, escriba:

```
1 -  add cs action <name> [-targetLBVserver <string> | -targetVserver <
     string> | -targetVserverExpr <expression>]
2 -  add cs policy <policyName> -rule <expression> [-action <string>]
3 -  show cs policy [<policyName>]
4
5 <!--NeedCopy-->
```

Ejemplos:

```
1  > add cs action action-CS-JPEG -targetLBVserver lbcachejpeg
2  Done
3  > show cs action action-CS-JPEG
4      Name: action-CS-JPEG
5      Target LB Vserver: lbcachejpeg
6      Hits: 0
7      Undef Hits: 0
8      Action Reference Count: 0
9  Done
10
11 > add cs policy policy-CS-JPEG -rule 'HTTP.REQ.URL.SUFFIX == ”jpeg”' -
       action action-CS-JPEG
12 Done
13 > show cs policy policy-CS-JPEG
14     Policy: policy-CS-JPEG Rule: HTTP.REQ.URL.SUFFIX == ”jpeg”
15     Action: action-CS-JPEG
16
17     HITS: 0
18 Done
19 >
20
21 > add cs action action-CS-GIF -targetLBVserver lbcachegif
22 Done
```



```
> show cs action action-CS-GIF
    Name: action-CS-GIF
    Target LB Vserver: lbcachegif
    Hits: 0
    Undef Hits: 0
    Action Reference Count: 0

Done
>
> add cs policy policy-CS-GIF -rule 'HTTP.REQ.URL.SUFFIX == "gif"' -
   action action-CS-GIF
Done
> show cs policy policy-CS-GIF
    Policy: policy-CS-GIF Rule: HTTP.REQ.URL.SUFFIX == "gif"
    Action: action-CS-GIF

    Hits: 0
Done
<!--NeedCopy-->
```

Crear una directiva de conmutación de contenido basada en reglas mediante la interfaz gráfica de usuario

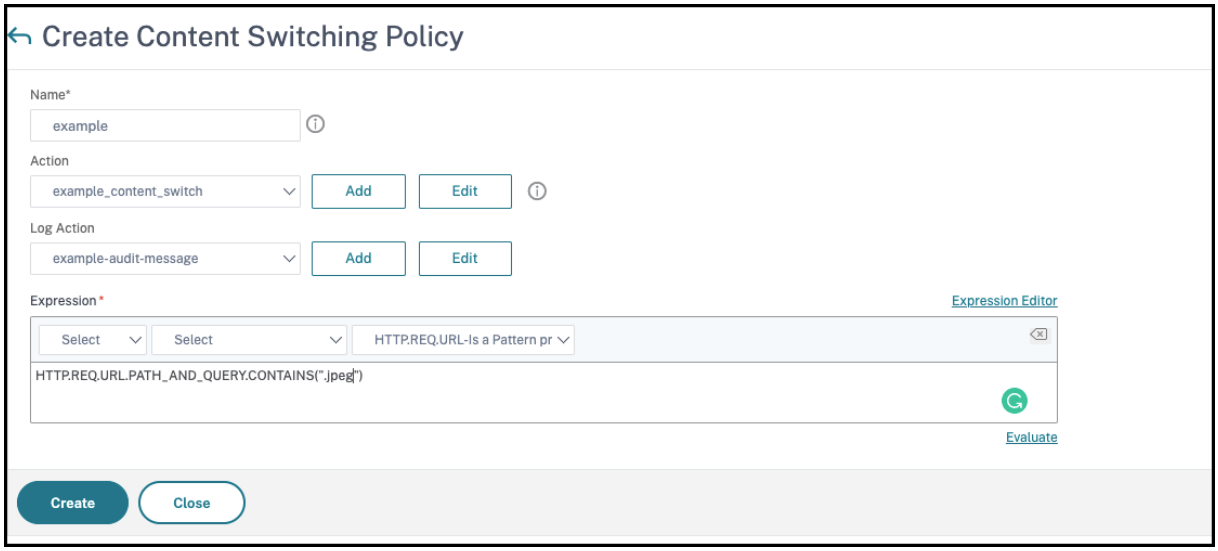
1. Vaya a **Administración del tráfico > Cambio de contenido > Directivas**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En el cuadro de diálogo **Crear directiva de conmutación de contenido**, en el cuadro de texto **Nombre**, escriba un nombre para la directiva.
4. Haga clic en **Agregar** en la ficha **Acción** para crear una acción de cambio de contenido. También puede seleccionar la acción disponible en la lista desplegable.
   - Escriba un nombre para la acción de consigna de contenido en la ficha **Nombre**.
   - Elija el servidor virtual o la expresión de la lista desplegable:
     - **Servidor virtual de equilibrio de carga**
     - **Servidor virtual de equilibrio de carga de servidores globales**
     - **Servidor virtual de autenticación**
     - **servidor virtual NetScalar Gateway**
     - **Expresión**
   - Haga clic en **Agregar** o **modificar** para configurar el **servidor virtual de equilibrio de carga de destino**.
5. Haga clic en **Agregar** en la ficha **Acción de registro** para crear una acción de mensaje de auditoría. También puede seleccionar la acción de mensaje de auditoría disponible en la lista

desplegable.

6. En el área **Expresión**, seleccione el tipo de expresión que desee.
7. En el cuadro de diálogo **Editor de expresiones**, elija la sintaxis de expresión que quiere utilizar.

   En el área **Expresión**, haga clic en **Evaluar** para evaluar un evaluador de expresiones. El evaluador evalúa la expresión que introdujo para verificar que es válida y muestra un análisis del efecto de la expresión en el área **Resultado**.
8. Introduzca las expresiones de directiva.

   Para obtener información sobre el uso de la sintaxis avanzada, consulte Configurar expresión de directiva avanzada: Introducción.
9. Haga clic en **Crear**. La directiva que ha creado aparece en el panel **Directivas de cambio de contenido**.



Enlazar la directiva de conmutación de contenido a un servidor virtual de redirección de caché mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para enlazar la directiva de conmutación de contenido a un servidor virtual de redirección de caché y compruebe la configuración:

```
1 - bind cs vserver <name> (-lbvserver <string> | -vServer <string> (-
    policyName <string> [-targetLBVserver <string>] [-priority<
    positive_integer>] [-gotoPriorityExpression <expression>] [-type <
    type>] [-invoke (<labelType> <labelName>) ] )
2
3 - show cs vserver [<name>]
```



```
<!--NeedCopy-->
```

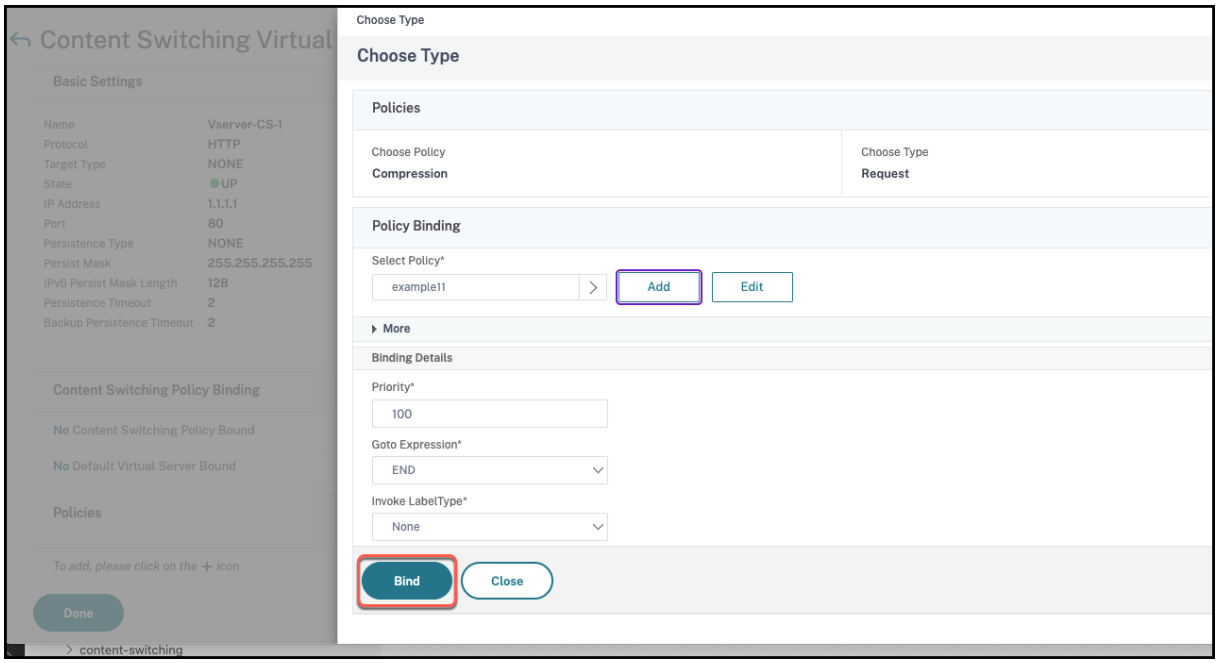
Ejemplo:

```
> bind cs vserver Vserver-CR-1 -policyName Policy-CS-JPEG -priority 100
 Done
> bind cs vserver Vserver-CR-1 -policyName Policy-CS-GIF -priority 200
 Done
> show cs vserver Vserver-CR-1
        Vserver-CR-1 (10.102.29.60:80) - HTTP   Type: CONTENT
        State: UP
        Last state change was at Fri Jul  2 12:53:45 2010
        Time since last state change: 0 days, 00:00:58.920
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Appflow loggig: ENABLED
        Port Rewrite : DISABLED
        State Update: DISABLED
        Default:        Content Precedence: RULE
        Cacheable: YES
        Vserver IP and Port insertion: OFF
        L2Conn: OFF    Case Sensitivity: ON
        Authentication: OFF
        401 Based Authentication: OFF
        Push: DISABLED  Push VServer:
        Push Label Rule: none
        HTTP Redirect Port: 0    Dtls:  OFF
        Persistence: NONE
        Listen Policy: NONE
        IcmpResponse: PASSIVE
        RHIstate: PASSIVE
        Traffic Domain:  0

1)      Content-Switching Policy: Policy-CS-JPEG Priority: 100     Hits
   : 0
2)      Content-Switching Policy: Policy-CS-GIF Priority: 200     Hits:
    0
 Done
>
<!--NeedCopy-->
```


Enlazar la directiva de conmutación de contenido a un servidor virtual de redirección de caché mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico** > **Cambio de contenido** > **Servidores virtuales**.
2. En el panel de detalles, seleccione el servidor virtual para el que quiere vincular la directiva (por ejemplo, **vServer-CS-1**) y, a continuación, haga clic en **Modificar**.
3. En el cuadro de diálogo **Servidor virtual de conmutación de contenido**, en la ficha **Directivas**, en **Configuración avanzada**, haga clic en el icono **Agregar** y, a continuación, elija la directiva y elija el tipo en la lista desplegable **Elegir directiva** y **Elegir tipo**.
4. Haga clic en **Continue**.
5. En la ficha **Enlace de directivas**, seleccione la directiva disponible en la lista y, a continuación, haga clic en **Seleccionar** o haga clic en **Agregar** para crear una nueva directiva y, a continuación, haga clic en **Crear**.
6. Haga clic en **Vincular** para enlazar la directiva de conmutación de contenido al servidor virtual.
7. Haga clic en **Listo**



Configurar precedencia para la evaluación de directivas

January 12, 2021

Puede configurar una directiva de conmutación de contenido basada en una regla, que es una configuración genérica para acomodar varios tipos de contenido, o en una dirección URL, que es más

específica y define exactamente el tipo de contenido que debe enviarse a un servidor de caché determinado. Básicamente, el mismo contenido se puede definir mediante una directiva basada en reglas o una directiva basada en URL.

Una vez que vincule directivas de conmutación de contenido de cualquier tipo a un servidor virtual de redirección de caché, puede configurar el servidor virtual para que dé prioridad a las directivas basadas en reglas o basadas en URL. Esto, a su vez, decidirá a qué servidores se dirigen las solicitudes particulares.

Para configurar la precedencia para la evaluación de directivas, utilice el parámetro precedence, que especifica el tipo de directiva (URL o RULE) que tiene prioridad en el servidor virtual de redirección de contenido.

Valores posibles: RULE, URL

Valor predeterminado: RULE

Configurar la precedencia para la evaluación de directivas mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para configurar la precedencia para la evaluación de directivas y verificar la configuración:

```
-  set cr vserver <name> [-precedence (RULE | URL)]
-  show cr vserver <name>
<!--NeedCopy-->
```

Ejemplo:

```
> set cr vserver Vserver-CRD-1 -precedence URL
 Done
> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: UP  ARP:DISABLED
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: URL Cache: TRANSPARENT
        On Policy Match: ORIGIN L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF

1)      Cache bypass  Policy: bypass-cache-control
2)      Cache bypass  Policy: Policy-CRD
```



```
 Done
>
<!--NeedCopy-->
```

Configurar la precedencia para la evaluación de directivas mediante la interfaz gráfica de usuario

1. Vaya a Administración del tráfico > Cambio de contenido > Servidores virtuales.
2. En el panel de detalles, seleccione el servidor virtual para el que quiere configurar la prioridad (por ejemplo, **Vserver-CS-1**) y, a continuación, haga clic en Abrir.
3. En el cuadro de diálogo Configurar servidor virtual (Content Switching), en la ficha Opciones avanzadas, junto a Prioridad, haga clic en Regla o URL y, a continuación, haga clic en Aceptar.

Administrar un servidor virtual de redirección de caché

January 12, 2021

Para administrar un servidor virtual de redirección de caché, debe ver las estadísticas de redirección de caché. Es posible que tenga que habilitar o inhabilitar los servidores de redirección de caché o dirigir las visitas de directiva a la caché en lugar del origen. Las tareas administrativas también incluyen la copia de seguridad de un servidor virtual de redirección de caché y la administración de conexiones de cliente.

Ver estadísticas del servidor virtual de redirección de caché

January 12, 2021

Puede ver las propiedades de un servidor virtual de redirección de caché y las estadísticas sobre el tráfico que ha pasado a través de un servidor virtual de redirección de caché. También puede ver los servidores virtuales de redirección de caché y las directivas que ha enlazado a los servidores virtuales de equilibrio de carga.

Para ver las estadísticas de un servidor virtual de redirección de caché específico, utilice el parámetro name para especificar el nombre del servidor virtual para el que se mostrarán las estadísticas. De lo contrario, se muestran las estadísticas de todos los servidores virtuales de redirección de caché. Longitud máxima: 127

Ver las estadísticas de un servidor virtual de redirección de caché mediante la CLI

En el símbolo del sistema, escriba:

```
stat cr vserver [<name>]
```

Ejemplo:

```
> stat cr vserver Vserver-CRD-1

Vserver Summary
                          IP  port     Protocol        State
Vser...CRD-1         0.0.0.0    80         HTTP           UP

VServer Stats:
                                        Rate (/s)
                                           Total
Requests                                        0
                       0
Responses                                       0
                       0
Request bytes                                   0
                       0
Response bytes                                  0
                       0

 Done
>
<!--NeedCopy-->
```

Ver las estadísticas de un servidor virtual de redirección de caché mediante la interfaz gráfica de usuario

1. Vaya a Administración de Tráfico > Redirección de Caché > Servidores Virtuales
2. En el panel de detalles, seleccione el servidor virtual para el que quiere ver las estadísticas (por ejemplo, **Vserver-CRD-1**) y, a continuación, haga clic en Estadísticas.

Omita el nombre del servidor para mostrar las estadísticas básicas de todos los servidores virtuales de redirección de caché. Incluir el nombre del servidor para mostrar estadísticas detalladas de ese servidor virtual, incluido el número y el tamaño de las solicitudes y respuestas que pasan a través del servidor virtual

Ver las estadísticas de un servidor virtual de redirección de caché mediante las utilidades de supervisión y panel

1. Para ver las estadísticas mediante las utilidades de supervisión, haga clic en la ficha Supervisión.
2. En el menú desplegable Seleccionar grupo, elija CR Virtual Servers. Aparece una lista de servidores virtuales de redirección de caché.
3. Para ver las estadísticas mediante las utilidades del panel, haga clic en la ficha Panel.
4. Haga clic en Cliente de applet o Cliente de inicio web junto a Utilidad estadística.
5. En el menú desplegable Seleccionar grupo, elija CR Virtual Servers. El panel muestra estadísticas de resumen para los servidores virtuales de redirección de caché.
6. Para ver un gráfico de la actividad del servidor virtual, haga clic en Gráfico. Aparecerá una representación gráfica de las estadísticas del servidor virtual.

Habilitar o inhabilitar un servidor virtual de redirección de caché

January 12, 2021

Cuando se crea un servidor virtual de redirección de caché, se habilita de forma predeterminada. Si inhabilita un servidor virtual de redirección de caché, su estado cambia a OUT DE SERVICIO y deja de redirigir las solicitudes de cliente en caché. Sin embargo, el dispositivo Citrix ADC continúa respondiendo a las solicitudes de ARP y ping para la dirección IP de este servidor virtual.

Habilitar o inhabilitar un servidor virtual de redirección de caché mediante la CLI

En la línea de comandos, escriba uno de los siguientes comandos:

```
- enable cr vserver <name>
- show cr vserver <name>
- disable cr vserver <name>
- show cr vserver <name>
<!--NeedCopy-->
```

Ejemplos:

```
> enable cr vserver Vserver-CRD-1
 Done
> show cr vserver Vserver-CRD-1
```



```
4          Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
5          State: UP  ARP:DISABLED
6          Client Idle Timeout: 180 sec
7          Down state flush: ENABLED
8          Disable Primary Vserver On Down : DISABLED
9          Default:        Content Precedence: URL Cache: TRANSPARENT
10         On Policy Match: ORIGIN L2Conn: OFF     OriginUSIP: OFF
11         Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF
12
13 1)      Cache bypass  Policy: bypass-cache-control
14 2)      Cache bypass  Policy: Policy-CRD
15  Done
16 >
17
18 > disable cr vserver Vserver-CRD-1
19  Done
20 > show cr vserver Vserver-CRD-1
21         Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
22         State: OUT OF SERVICE  ARP:DISABLED
23         Client Idle Timeout: 180 sec
24         Down state flush: ENABLED
25         Disable Primary Vserver On Down : DISABLED
26         Default:        Content Precedence: URL Cache: TRANSPARENT
27         On Policy Match: ORIGIN L2Conn: OFF     OriginUSIP: OFF
28         Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF
29
30 1)      Cache bypass  Policy: bypass-cache-control
31 2)      Cache bypass  Policy: Policy-CRD
32  Done
33 >
34 <!--NeedCopy-->
```

Habilitar o inhabilitar un servidor virtual de redirección de caché mediante la interfaz gráfica de usuario

1. Vaya a Administración del tráfico > Redirección de caché > Servidores virtuales.
2. En el panel de navegación, expanda Redirección de caché y, a continuación, haga clic en Servidores virtuales.
3. En el panel de detalles, seleccione el servidor virtual que quiere habilitar o inhabilitar (por ejemplo, **Vserver-CRD-1**) y, a continuación, haga clic en Estadísticas.
4. En el cuadro de diálogo Continuar, haga clic en Sí.

Solicitudes directas de directivas a la caché en lugar del servidor web de origen

August 20, 2021

De forma predeterminada, cuando una solicitud coincide con una directiva, el dispositivo Citrix ADC reenvía la solicitud directamente al servidor de origen o a un servidor virtual de equilibrio de carga para el origen, en función de cómo haya configurado la redirección de caché.

Puede cambiar el comportamiento predeterminado para que cuando una solicitud coincida con una directiva, la solicitud se reenvíe a un servidor virtual de equilibrio de carga para la caché.

Para cambiar el destino de una solicitud de directiva al origen o a la caché, utilice el `onPolicyMatch` parámetro, que especifica dónde enviar solicitudes que coinciden con la directiva de redirección de caché.

Las opciones válidas son:

1. `CACHE` - Dirige todas las solicitudes coincidentes a la caché.
2. `ORIGIN` - Dirige todas las solicitudes coincidentes al servidor de origen.

> **Nota:**
>
> Para que esta opción funcione, debe seleccionar el tipo de redirección de caché como `POLICY`.

Valores posibles: `CACHE`, `ORIGIN`

Valor predeterminado: `ORIGIN`

Cambiar el destino de una solicitud de directiva al origen o a la caché mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para cambiar el destino de un golpe de directiva y verificar la configuración:

```
set cr vserver <name> [-onPolicyMatch (ORIGIN | CACHE)]
<!--NeedCopy-->
```

```
show cr vserver <name>
<!--NeedCopy-->
```

Ejemplo:


```
> set cr vserver Vserver-CRD-1 -onPolicyMatch CACHE
 Done
> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: UP  ARP:DISABLED
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: URL Cache: TRANSPARENT
        On Policy Match: CACHE  L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF

1)      Cache bypass  Policy: bypass-cache-control
2)      Cache bypass  Policy: Policy-CRD
 Done
<!--NeedCopy-->
```

Cambiar el destino de una directiva de acceso al origen o la caché mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Redirección de caché > Servidores virtuales**.
2. En el panel de detalles, seleccione el servidor virtual para el que desea cambiar el destino de una solicitud de directiva (por ejemplo, **vServer-CRD-1**) y, a continuación, haga clic en Abrir.
3. En el cuadro de diálogo **Configurar servidor virtual (redirección de caché)**, haga clic en **Avanzado**.
4. Seleccione **CACHE** u **ORIGIN** en la lista desplegable **Redirigir a** .
5. Haga clic en **Aceptar**.

Haga una copia de seguridad de un servidor virtual de redirección de caché

August 20, 2021

La redirección de caché puede fallar si el servidor virtual principal falla o si no puede controlar el tráfico excesivo. Puede especificar un servidor virtual de copia de seguridad para que se haga cargo del procesamiento del tráfico cuando se produzca un error en el servidor virtual principal.

Para especificar un servidor virtual de redirección de caché de copia de seguridad, utilice el parámetro BackupVServer, que especifica Servidor virtual de copia de seguridad. Longitud máxima: 127

Especificar un servidor virtual de redirección de caché de copia de seguridad mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para especificar un servidor virtual de redirección de caché de copia de seguridad y compruebe la configuración:

```
-  set cr vserver <name> [-backupVServer <string>]
-  show cr vserver <name>
<!--NeedCopy-->
```

Ejemplo:

```
> set cr vserver Vserver-CRD-1 -backupVServer Vserver-CRD-2
 Done
> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: UP  ARP:DISABLED
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: URL Cache: TRANSPARENT
        On Policy Match: CACHE  L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF
        Backup: Vserver-CRD-2

1)      Cache bypass  Policy: bypass-cache-control
2)      Cache bypass  Policy: Policy-CRD
 Done
<!--NeedCopy-->
```

Especificar un servidor virtual de redirección de caché de copia de seguridad mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Redirección de caché > Servidores virtuales**.
2. En el panel de detalles, seleccione el servidor virtual para el que desea cambiar el destino de una solicitud de directiva (por ejemplo, **vServer-CRD-1**) y, a continuación, haga clic en Abrir.
3. En el cuadro de diálogo Configurar servidor virtual (redirección de caché), seleccione la ficha Avanzadas.
4. En la lista desplegable Servidor virtual de copia de seguridad, seleccione el servidor virtual.
5. Haga clic en Aceptar.

Administrar conexiones de cliente para un servidor virtual

January 12, 2021

Puede configurar los tiempos de espera en un servidor virtual de redirección de caché para que las conexiones de cliente no se mantengan abiertas indefinidamente. También puede insertar encabezados Via en las solicitudes. Para reducir posiblemente la congestión de la red, puede reutilizar las conexiones TCP abiertas. Puede habilitar o inhabilitar la limpieza retardada de conexiones de servidor virtual de redirección de caché.

Puede configurar el dispositivo para que envíe respuestas ICMP a las solicitudes PING según su configuración. En la dirección IP correspondiente al servidor virtual, establezca ICMP RESPONSE en VSVR_CNTRLD y, en el servidor virtual, configure ICMP VSERVER RESPONSE.

Se pueden realizar las siguientes configuraciones en un servidor virtual:

- Cuando establece ICMP VSERVER RESPONSE en PASIVO en todos los servidores virtuales, el dispositivo siempre responde.
- Cuando establece ICMP VSERVER RESPONSE en ACTIVE en todos los servidores virtuales, el dispositivo responde incluso si un servidor virtual está UP.
- Cuando establece ICMP VSERVER RESPONSE en ACTIVE en algunos y PASIVO en otros, el dispositivo responde incluso si un servidor virtual configurado en ACTIVE es UP.

Este documento incluye la siguiente información:

- Configurar tiempo de espera del cliente
- Insertar encabezados Via en las solicitudes
- Reutilizar conexiones TCP
- Configurar la limpieza de conexiones retrasadas

Configurar tiempo de espera del cliente

Puede especificar el vencimiento de las solicitudes de cliente estableciendo un valor de tiempo de espera para el servidor virtual de redirección de caché. El valor de tiempo de espera es el número de segundos durante los que el servidor virtual de redirección de caché espera recibir una respuesta para la solicitud del cliente.

Para configurar un valor de tiempo de espera, utilice el parámetro CLTTimeout, que especifica el tiempo, en segundos, después del cual el dispositivo Citrix ADC cierra las conexiones de cliente inactivas. El valor predeterminado es 180 segundos para los servicios basados en HTTP/SSL y 9000 segundos para los servicios basados en TCP.

Configurar el tiempo de espera del cliente mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para configurar el tiempo de espera del cliente y verificar la configuración:

```
-  set cr vserver <name> [-cltTimeout <secs>]
-  show cr vserver <name>
<!--NeedCopy-->
```

Ejemplo:

```
> set cr vserver Vserver-CRD-1 -cltTimeout 6000
 Done
> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: UP  ARP:DISABLED
        Client Idle Timeout: 6000 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: URL Cache: TRANSPARENT
        On Policy Match: CACHE  L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF
        Backup: Vserver-CRD-2

1)      Cache bypass  Policy: bypass-cache-control
2)      Cache bypass  Policy: Policy-CRD
 Done
<!--NeedCopy-->
```

Configurar el tiempo de espera del cliente mediante la interfaz gráfica de usuario

1. Vaya a Administración del tráfico > Redirección de caché > Servidores virtuales.
2. En el panel de detalles, seleccione el servidor virtual para el que quiere configurar el tiempo de espera del cliente (por ejemplo, **Vserver-CRD-1**) y, a continuación, haga clic en Abrir.
3. En el cuadro de diálogo Configurar servidor virtual (redirección de caché), seleccione la ficha Avanzadas.
4. En el cuadro de texto Tiempo de espera del cliente (segundos), escriba el valor de tiempo de espera en segundos.
5. Haga clic en Aceptar.

Insertar encabezados Via en las solicitudes

Un encabezado Via enumera los protocolos y destinatarios entre los puntos de inicio y final de una solicitud o una respuesta e informa al servidor de proxies a través de los cuales se envió la solicitud. Puede configurar el servidor virtual de redirección de caché para insertar un encabezado Via en cada solicitud HTTP. El parámetro via está habilitado de forma predeterminada al crear un servidor virtual de redirección de caché.

Para habilitar o inhabilitar la inserción de encabezado VIA en las solicitudes de cliente, utilice el parámetro via, que especifica el estado del sistema al insertar un encabezado Via en las solicitudes HTTP.

Valores posibles: ON, OFF

Valor predeterminado: ON

Habilitar o inhabilitar la inserción de encabezado de VIA en las solicitudes de cliente mediante la CLI

En el símbolo del sistema, escriba:

```
-  set cr vserver <name> [-via (ON|OFF)]
-  show cr vserver <name>
<!--NeedCopy-->
```

Ejemplo:

```
> set cr vserver Vserver-CRD-1 -via ON
 Done
> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: UP  ARP:DISABLED
        Client Idle Timeout: 6000 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: URL Cache: TRANSPARENT
        On Policy Match: CACHE  L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF
        Backup: Vserver-CRD-2

1)      Cache bypass  Policy: bypass-cache-control
2)      Cache bypass  Policy: Policy-CRD
```



```
16   Done
17 >
18 <!--NeedCopy-->
```

Habilitar o inhabilitar la inserción de encabezado de VIA en las solicitudes de cliente mediante la interfaz gráfica de usuario

1. Vaya a Administración del tráfico > Redirección de caché > Servidores virtuales.
2. En el panel de detalles, seleccione el servidor virtual para el que quiere configurar el tiempo de espera del cliente (por ejemplo, **Vserver-CRD-1**) y, a continuación, haga clic en Abrir.
3. En el cuadro de diálogo Configurar servidor virtual (redirección de caché), seleccione la ficha Avanzadas.
4. Active la casilla de verificación Vía.
5. Haga clic en Aceptar.

Reutilizar conexiones TCP

Puede configurar el dispositivo Citrix ADC para reutilizar las conexiones TCP a la caché y los servidores de origen a través de las conexiones de cliente. Esto puede mejorar el rendimiento al ahorrar el tiempo necesario para establecer una sesión entre el servidor y el dispositivo. La opción de reutilización está habilitada de forma predeterminada al crear un servidor virtual de redirección de caché.

Para habilitar o inhabilitar la reutilización de conexiones TCP, utilice el parámetro de reutilización, que especifica el estado de reutilización de las conexiones TCP a la caché o servidores de origen a través de las conexiones de cliente.

Valores posibles: ON, OFF

Valor predeterminado: ON

Habilitar o inhabilitar la reutilización de conexiones TCP mediante la CLI

En el símbolo del sistema, escriba:

```
1 -  set cr vserver <name> [-reuse (ON|OFF)]
2 -  show cr vserver <name>
3 <!--NeedCopy-->
```

Ejemplo:


```
> set cr vserver Vserver-CRD-1 -reuse ON
 Done
> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: UP  ARP:DISABLED
        Client Idle Timeout: 6000 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: URL Cache: TRANSPARENT
        On Policy Match: CACHE  L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF
        Backup: Vserver-CRD-2

1)      Cache bypass  Policy: bypass-cache-control
2)      Cache bypass  Policy: Policy-CRD
 Done
<!--NeedCopy-->
```

Habilitar o inhabilitar la reutilización de conexiones TCP mediante la interfaz gráfica de usuario

1. Vaya a Administración del tráfico > Redirección de caché > Servidores virtuales.
2. En el panel de detalles, seleccione el servidor virtual para el que quiere configurar el tiempo de espera del cliente (por ejemplo, **Vserver-CRD-1**) y, a continuación, haga clic en Abrir.
3. En el cuadro de diálogo Configurar servidor virtual (redirección de caché), seleccione la ficha Avanzadas.
4. Active la casilla de verificación Reutilizar.
5. Haga clic en Aceptar.

Configurar la limpieza de conexiones retrasadas

La opción de vaciado de estado inactivo realiza la limpieza retardada de las conexiones en un servidor virtual de redirección de caché. La opción de vaciado de estado inactivo está habilitada de forma predeterminada al crear un servidor virtual de redirección de caché.

Para habilitar o inhabilitar la opción de descarga de estado descendente, establezca el parámetro DownStateFLush.

Valores posibles: ENABLED, DISABLED

Valor predeterminado: ENABLED

Habilitar la opción de descarga de estado descendente mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para configurar la limpieza de la conexión retardada y verificar la configuración:

```
-  set cr vserver <name> [-downStateFlush (ENABLED | DISABLED)]
-  show cr vserver <name>
<!--NeedCopy-->
```

Ejemplo:

```
> set cr vserver Vserver-CRD-1 -downStateFlush ENABLED
 Done
> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: UP  ARP:DISABLED
        Client Idle Timeout: 6000 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: URL Cache: TRANSPARENT
        On Policy Match: CACHE  L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF
        Backup: Vserver-CRD-2

1)      Cache bypass  Policy: bypass-cache-control
2)      Cache bypass  Policy: Policy-CRD
 Done
<!--NeedCopy-->
```

Habilitar o inhabilitar la reutilización de conexiones TCP mediante la interfaz gráfica de usuario

1. Vaya a Administración del tráfico > Redirección de caché > Servidores virtuales.
2. En el panel de detalles, seleccione el servidor virtual para el que quiere configurar el tiempo de espera del cliente (por ejemplo, **Vserver-CRD-1**) y, a continuación, haga clic en Abrir.
3. En el cuadro de diálogo Configurar servidor virtual (redirección de caché), haga clic en la ficha Avanzadas.
4. Active la casilla de verificación Desactivar estado.
5. Haga clic en Aceptar.

Habilitar la comprobación externa del estado de TCP para servidores virtuales UDP

January 12, 2021

En las nubes públicas, puede utilizar el dispositivo Citrix ADC como equilibrador de carga de segundo nivel cuando se utiliza el equilibrador de carga nativo como primer nivel. El equilibrador de carga nativo puede ser un equilibrador de carga de aplicaciones (ALB) o un equilibrador de carga de red (NLB). La mayoría de las nubes públicas no admiten sondas de estado UDP en sus equilibradores de carga nativos. Para supervisar el estado de la aplicación UDP, las nubes públicas recomiendan agregar un extremo basado en TCP al servicio. El punto final refleja el estado de la aplicación UDP.

El dispositivo Citrix ADC admite la comprobación de estado basada en TCP externa para un servidor virtual UDP. Esta función introduce un detector TCP en el VIP del servidor virtual de redirección de caché y el puerto configurado. El agente de escucha TCP refleja el estado del servidor virtual.

Para habilitar la comprobación externa del estado de TCP para servidores virtuales UDP mediante CLI

En el símbolo del sistema, escriba el comando siguiente para habilitar una comprobación de estado TCP externa con la opción TcpProbeport:

```
add cr vserver <name> <serviceType> -tcpProbePort <tcpProbePort>

<!--NeedCopy-->
```

Ejemplo:

```
add cr vserver Vserver-CR-1 HTTP -tcpProbePort 80
<!--NeedCopy-->
```

Para habilitar la comprobación externa del estado de TCP para servidores virtuales UDP mediante GUI

1. Vaya a **Administración del tráfico > Redirección de caché > Servidores virtuales** y, a continuación, cree un servidor virtual.
2. Haga clic en **Agregar** para crear un servidor virtual.

3. En el panel **Configuración básica**, agregue el número de puerto en el campo **Puerto de sondeo TCP**.
4. Haga clic en **Aceptar**.

Redirección de caché de nivel N

August 20, 2021

Para manejar eficientemente grandes cantidades de datos almacenados en caché, normalmente varios gigabytes por segundo, un proveedor de servicios de Internet (ISP) implementa varios servidores de caché dedicados. La función de redirección de caché del dispositivo Citrix ADC puede ayudar a equilibrar la carga de los servidores de caché, pero es posible que un solo dispositivo o un par de dispositivos no gestionen eficazmente el gran volumen de tráfico.

Puede resolver el problema implementando los dispositivos Citrix ADC en dos niveles (capas), donde los dispositivos de la capa superior equilibran la carga de la capa inferior y los dispositivos de la capa inferior equilibran la carga de los servidores de caché. Esta disposición se denomina *redirección de caché de niveles n*.

Para fines como la auditoría y la seguridad, un ISP tiene que realizar un seguimiento de los detalles del cliente, como la dirección IP, la información proporcionada y el momento de la interacción. Por lo tanto, las conexiones de cliente a través de un dispositivo Citrix ADC deben ser totalmente transparentes. Sin embargo, si configura la redirección de caché transparente, con los dispositivos Citrix ADC implementados en paralelo, la dirección IP del cliente debe compartirse entre todos los dispositivos. Compartir la dirección IP del cliente crea un conflicto que hace que los dispositivos de red, como enrutadores, servidores de caché, servidores de origen y otros dispositivos Citrix ADC, no puedan determinar el dispositivo y, por tanto, el cliente, al que se debe enviar la respuesta.

Cómo se implementa la redirección de caché de niveles N

Para resolver el problema, la redirección de caché de n-niveles del dispositivo divide el intervalo de puertos de origen entre los dispositivos de la capa inferior e incluye la dirección IP del cliente en la solicitud enviada a los servidores de caché. Los dispositivos Citrix ADC de nivel superior están configurados para realizar un equilibrio de carga sin sesión a fin de evitar cargas innecesarias en los dispositivos.

Cuando el dispositivo Citrix ADC de nivel inferior se comunica con un servidor de caché, utiliza una dirección IP asignada (MIP) para representar la dirección IP de origen. Por lo tanto, el servidor de caché puede identificar el dispositivo desde el que recibió la solicitud y enviar la respuesta al mismo dispositivo.

El dispositivo Citrix ADC de nivel inferior inserta la dirección IP del cliente en el encabezado de la solicitud enviada al servidor de caché. La IP del cliente en el encabezado ayuda al dispositivo a determinar el cliente al que se debe reenviar el paquete cuando recibe la respuesta de un servidor de caché, o el servidor de origen en caso de que se pierda la memoria caché. El servidor de origen determina la respuesta que se enviará de acuerdo con la IP del cliente insertada en el encabezado de solicitud.

El servidor de origen envía la respuesta a un dispositivo de nivel superior, incluido el número de puerto de origen desde el que el servidor de origen recibió la solicitud. Todo el rango de puertos de origen, 1024 a 65535, se distribuye entre los dispositivos Citrix ADC de nivel inferior. A cada dispositivo de nivel inferior se le asigna exclusivamente un grupo de direcciones dentro del intervalo. Esta asignación permite al dispositivo de nivel superior identificar inequívocamente el dispositivo Citrix ADC de nivel inferior que envió la solicitud al servidor de origen. Por lo tanto, el dispositivo de nivel superior puede reenviar la respuesta al dispositivo de nivel inferior correcto.

Los dispositivos Citrix ADC de nivel superior están configurados para realizar redirección basada en directivas, y las directivas de redirección se definen para determinar la dirección IP del dispositivo de destino desde el intervalo de puertos de origen.

Configuración necesaria para configurar N-Tier CRD

La siguiente configuración es necesaria para el funcionamiento de la redirección de caché de n-niveles:

Para cada dispositivo Citrix ADC de nivel superior:

- Habilite el modo Capa 3.
- Defina directivas para rutas basadas en directivas (PBRs) para que el tráfico se reenvíe de acuerdo con el intervalo del puerto de destino.
- Configure un servidor virtual de equilibrio de carga.
- Configure el servidor virtual para escuchar todo el tráfico procedente del cliente. Establezca el Service Type/Protocol como ANY y la dirección IP como asterisco (*).
- Habilite el equilibrio de carga sin sesión con el modo de redirección basado en Mac para evitar cargas innecesarias en los dispositivos Citrix ADC de nivel superior.
- Asegúrese de que la opción Usar puerto proxy está habilitada.
- Cree un servicio para cada dispositivo de nivel inferior y vincule todos los servicios al servidor virtual.

Para cada dispositivo Citrix ADC de nivel inferior,

- Configure el intervalo de puertos de redirección de caché en el dispositivo. Asigne un rango exclusivo a cada dispositivo de nivel inferior.
- Configure un servidor virtual de equilibrio de carga y habilite la redirección basada en Mac.
- Cree un servicio para cada servidor de caché que este dispositivo debe equilibrar la carga. Al

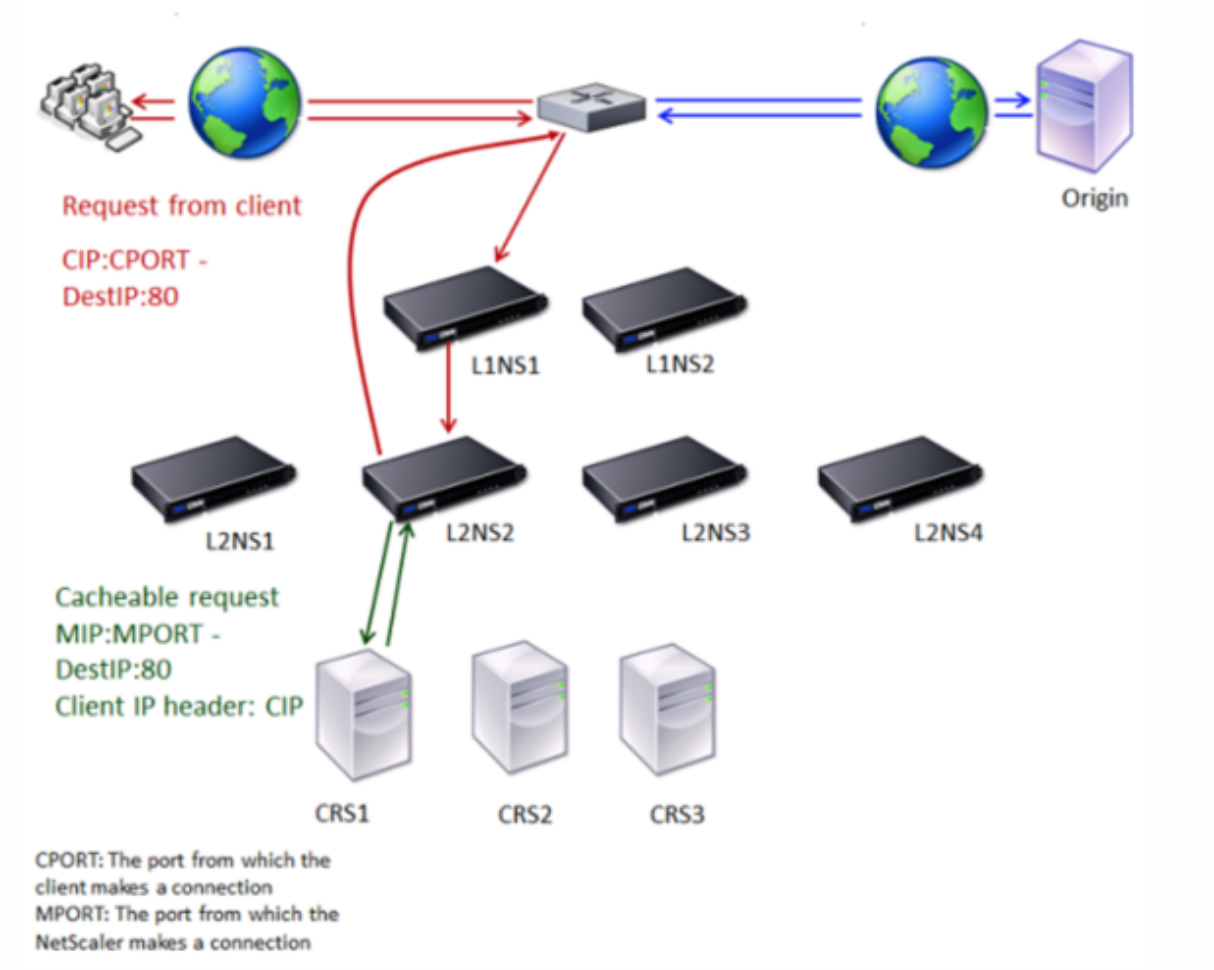
crear el servicio, habilite la inserción de la IP del cliente en el encabezado. A continuación, enlazar todos los servicios al servidor virtual de equilibrio de carga.

- Configure un servidor virtual de redirección de caché en modo transparente con las siguientes opciones:
  - Active la opción Origin USIP.
  - Agregue una expresión IP de origen para incluir la IP del cliente en el encabezado.
  - Active la opción Usar intervalo de puertos.

Cómo funciona la redirección de caché de niveles N durante un golpe de caché

La siguiente ilustración muestra cómo funciona la redirección de caché cuando una solicitud de cliente es almacenable en caché y la respuesta se envía desde un servidor de caché.

Ilustración 1. Redirección de caché en caso de un golpe de caché



Dos dispositivos Citrix ADC, L1NS1 y L1NS2, se implementan en el nivel superior, y cuatro dispositivos Citrix ADC, L2NS1, L2NS2, L2NS3 y L2NS4, se implementan en el nivel inferior. El cliente A envía una solicitud, que es reenviada por el enrutador. Los servidores de caché CRS1, CRS2 y CRS3 atienden las

solicitudes de caché. Origin Server O presta servicios a las solicitudes almacenadas en caché.

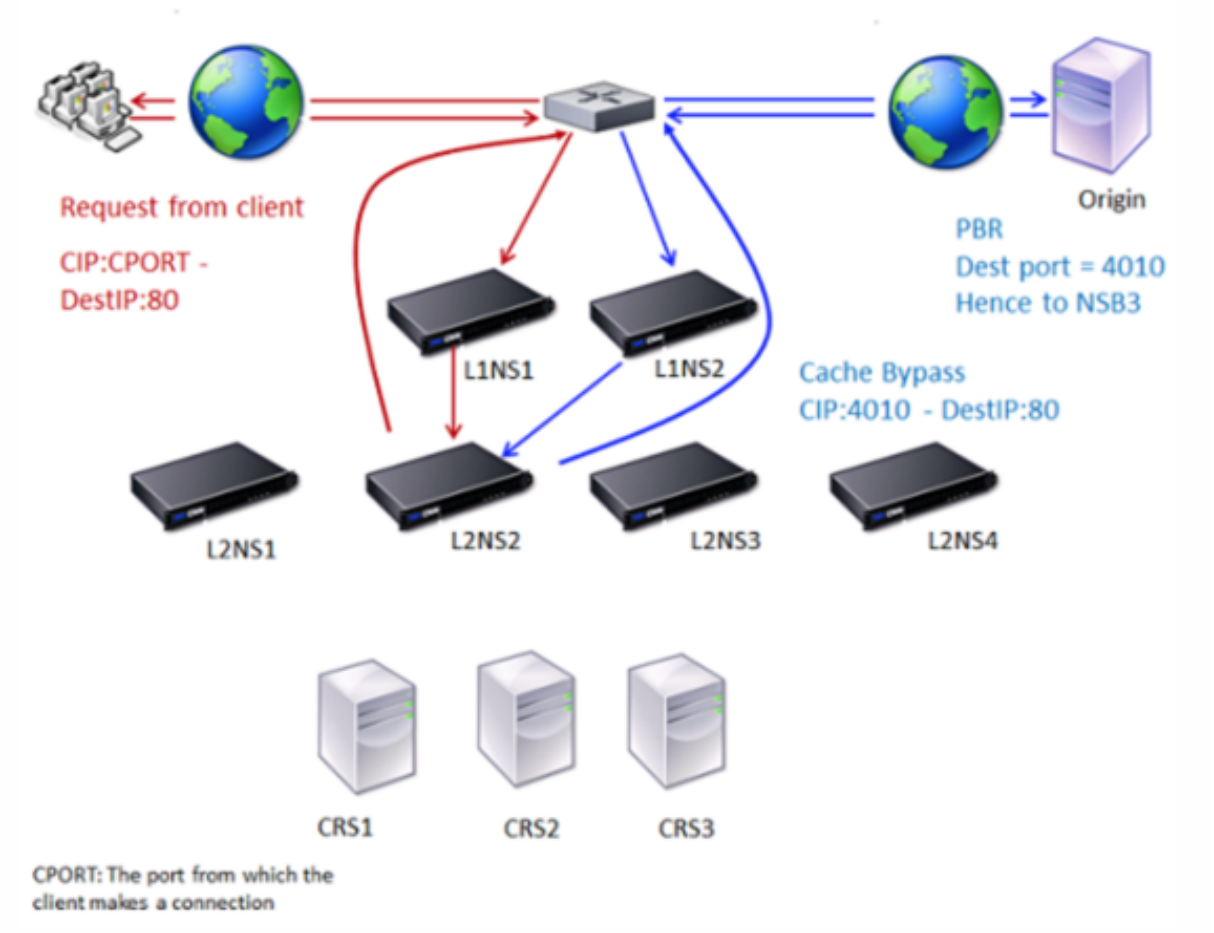
Flujo de tráfico

1. El cliente envía una solicitud y el router la reenvía a L1NS1.
2. La carga L1NS1 equilibra la solicitud a L2NS2.
3. La carga de L2NS2 equilibra la solicitud al servidor de caché CRS1 y la solicitud es almacenable en caché. L2NS2 incluye la IP del cliente en el encabezado de solicitud.
4. CRS1 envía la respuesta a L2NS2 porque L2NS2 utilizó su MIP como dirección IP de origen al conectarse a CRS1.
5. Con la ayuda de la dirección IP del cliente en el encabezado de solicitud, L2NS2 identifica el cliente del que proviene la solicitud. L2NS2 envía directamente la respuesta al router, evitando una carga innecesaria en el dispositivo en el nivel superior.
6. El router reenvía la respuesta al cliente A.

Cómo funciona la redirección de caché de niveles N durante un bypass de caché

La siguiente ilustración muestra cómo funciona la redirección de caché cuando se envía una solicitud de cliente a un servidor de origen para obtener una respuesta.

Ilustración 2. Redirección de caché en caso de omisión de caché



Dos dispositivos Citrix ADC, L1NS1 y L1NS2, se implementan en el nivel superior, y cuatro dispositivos Citrix ADC, L2NS1, L2NS2, L2NS3 y L2NS4, se implementan en el nivel inferior. El cliente A envía una solicitud, que es reenviada por el enrutador. Los servidores de caché CRS1, CRS2 y CRS3 atienden las solicitudes de caché. Origin Server O presta servicios a las solicitudes almacenadas en caché.

Flujo de tráfico

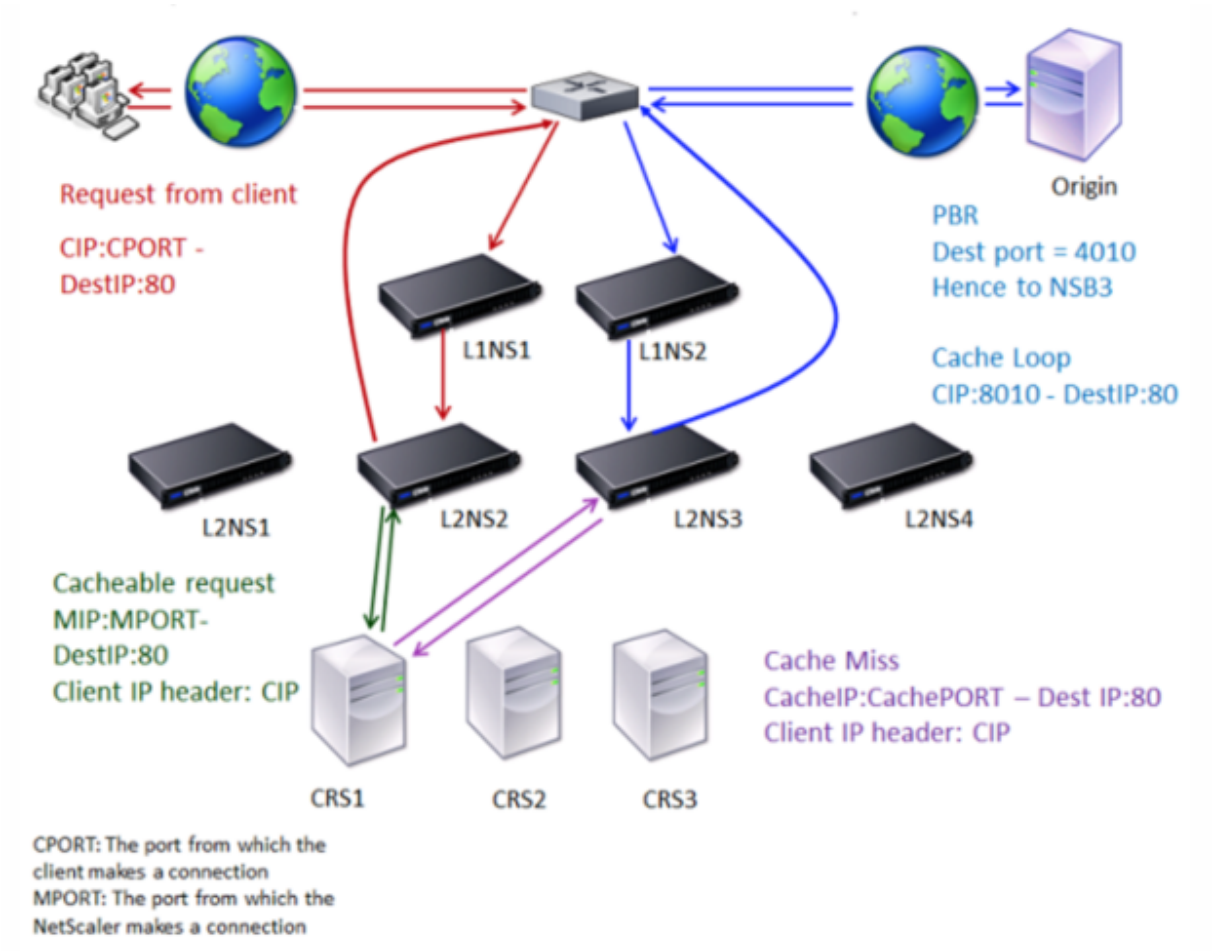
1. El cliente envía una solicitud y el router la reenvía a L1NS1.
2. La carga L1NS1 equilibra la solicitud a L2NS2.
3. La solicitud no se puede guardar en la caché (omisión de caché). Por lo tanto, L2NS2 envía la solicitud al servidor de origen a través del enrutador.
4. El servidor de origen envía la respuesta a un dispositivo de nivel superior, L1NS2.
5. De acuerdo con las directivas PBR, L1NS2 reenvía el tráfico al dispositivo apropiado en el nivel inferior, L2NS2.
6. L2NS2 utiliza la dirección IP del cliente en el encabezado de solicitud para identificar el cliente desde el que procede la solicitud y envía la respuesta directamente al enrutador, evitando una carga innecesaria en el dispositivo en el nivel superior.

7. El router reenvía la respuesta al cliente A.

Cómo funciona la redirección de caché de niveles N durante una pérdida de caché

La siguiente ilustración muestra cómo funciona la redirección de caché cuando no se almacena en caché una solicitud de cliente.

Ilustración 3. Redirección de caché en caso de pérdida de caché



Dos dispositivos Citrix ADC, L1NS1 y L1NS2, se implementan en el nivel superior, y cuatro dispositivos Citrix ADC, L2NS1, L2NS2, L2NS3 y L2NS4, se implementan en el nivel inferior. El cliente A envía una solicitud, que es reenviada por el enrutador. Los servidores de caché CRS1, CRS2 y CRS3 atienden las solicitudes de caché. Origin Server O presta servicios a las solicitudes almacenadas en caché.

Flujo de tráfico

1. El cliente envía una solicitud y el router la reenvía a L1NS1.
2. La carga L1NS1 equilibra la solicitud a L2NS2.

3. La carga de L2NS2 equilibra la solicitud al servidor de caché CRS1 porque la solicitud es almacenable en caché.
4. CRS1 no tiene la respuesta (pérdida de caché). CRS1 reenvía la solicitud al servidor de origen a través del dispositivo en la capa inferior. L2NS3 intercepta el tráfico.
5. L2NS3 toma la IP del cliente del encabezado y reenvía la solicitud al servidor de origen. El puerto de origen incluido en el paquete es el puerto L2NS3 desde el que se envía la solicitud al servidor de origen.
6. El servidor de origen envía la respuesta a un dispositivo de nivel superior, L1NS2.
7. De acuerdo con las directivas PBR, L1NS2 reenvía el tráfico al dispositivo apropiado en el nivel inferior, L2NS3.
8. L2NS3 reenvía la respuesta al enrutador.
9. El router reenvía la respuesta al cliente A.

Configurar los dispositivos Citrix ADC de nivel superior

August 20, 2021

Configure cada uno de los dispositivos Citrix ADC de nivel superior de la siguiente manera.

Configurar un dispositivo de nivel superior para la redirección de caché de n-niveles mediante el comando CLI

En el símbolo del sistema, escriba los siguientes comandos:

- `add service \<name\>@ \<serviceIP\> \<serviceType\> \<port\>`

  Ejecute este comando para cada servicio que se va a agregar.

- `add lb vserver \<name\>@ ANY \* \<port\> -persistenceType \<persistenceMethod \> -lbMethod \<lbMethod\> -m MAC -sessionless ENABLED -cltTimeout \< client\\_Timeout\\_Value\>`

- `bind lb vserver \<name\>@ \<serviceName\>`

  Ejecute este comando para cada servicio que se va a enlazar.

- `enable ns mode l3`

- `add ns pbr \<name\> \<action\> -srcPort \<sourcePortNumber\> -destPort \<startPortNumber-endPortNumber\> -nexthop \<serviceIpAddress\> -protocol TCP`

- `apply ns pbrs`

  Ejecute este comando después de agregar todos los PBRs necesarios.

Configure un dispositivo de nivel superior para la redirección de caché de n-niveles mediante la interfaz gráfica de usuario

1. Habilitar el modo L3:
   a) En el panel de navegación, haga clic en Sistema y, a continuación, haga clic en Configuración.
   b) En el grupo Configuración, haga clic en el vínculo Configurar modos.
   c) Active la casilla de verificación Modo de capa 3 (Reenvío IP).
   d) Haga clic en Aceptar.
2. Configurar redirección basada en directivas (PBR):
   a) Vaya a Sistema > Red > PBRs.
   b) En el panel Redirección basada en directivas (PBRs), haga clic en Agregar.
   c) Escriba un nombre para el PBR.
   d) Seleccione la acción como Permitir.
   e) En el cuadro Siguiente salto, escriba la dirección IP del servicio, que representa un dispositivo de nivel inferior.
   f) Seleccione TCP en la lista desplegable Protocolo.
   g) Escriba el puerto de origen y el intervalo del puerto de destino correspondiente al dispositivo de nivel inferior que se va a agregar.
   h) Haga clic en Crear.
   i) En el panel de detalles, seleccione el PBR y haga clic en Aplicar.
   j) Repita el paso (i) al paso (vii) para cada dispositivo de nivel inferior.
3. Cree un servicio para cada dispositivo de nivel inferior:
   a) Vaya a Administración de Tráfico > Equilibrio de carga > Servicios.
   b) En el panel de detalles, haga clic en Agregar.
   c) Especifique el nombre, el protocolo, la dirección IP y el puerto. El protocolo debe ser CUALQUIER.
   d) Haga clic en Crear.
4. Configurar un servidor virtual de equilibrio de carga:
   a) Vaya a Administración del tráfico > Equilibrio de carga > Servidores virtuales.
   b) En el panel de detalles, haga clic en Agregar.
   c) Especifique el nombre, el protocolo, la dirección IP y el puerto. El protocolo debe ser CUALQUIER y la dirección IP debe ser *.
   d) En la ficha Servicios, seleccione los servicios que representan los dispositivos Citrix ADC de nivel inferior.
   e) En la ficha Avanzadas, seleccione el Modo de redirección como basado en MAC y active la casilla de verificación Sin sesión.
   f) Haga clic en Crear.

Configurar los dispositivos Citrix ADC de nivel inferior

August 20, 2021

Configure cada uno de los dispositivos Citrix ADC de nivel inferior de la siguiente manera.

Configure un dispositivo de nivel inferior para la redirección de caché de n-niveles mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos:

- `add service <name>@ <cacheServiceIP> <serviceType> <port> -cip ENABLED "ClientIP"-cachetype transparent`

  Repita para cada servidor de caché.

- `add lb vserver <name>@ <serviceType> -m MAC`
- `bind lb vserver <name>@ <cacheServiceName>`

  Repita para cada servidor de caché.

- `add cr vserver <name> <serviceType> * <port> -srcIPExpr "HTTP.REQ. HEADER("ClientIP")"-originusip ON -usePortRange ON`
- `set ns param-crPortRange <startPortNumber-endPortNumber>`

Configure un dispositivo de nivel inferior para la redirección de caché de n-niveles mediante la interfaz gráfica de usuario

1. Cree un servicio para cada servidor de caché. Para crear un servicio:
   a) Vaya a Administración de Tráfico > Equilibrio de carga > Servicios.
   b) En el panel de detalles, haga clic en Agregar y especifique el nombre y el protocolo. Desactive la casilla Directamente direccionable.
   c) En la ficha Avanzadas, active la casilla de verificación Anular Global y la casilla de verificación IP del cliente y, a continuación, en el cuadro Encabezado, escriba ClientIP.
   d) En el cuadro Tipo de caché, seleccione Caché transparente.
   e) Haga clic en Crear.
2. Configurar un servidor virtual de equilibrio de carga:
   a) Vaya a Administración del tráfico > Equilibrio de carga > Servicios virtuales.
   b) En el panel de detalles, haga clic en Agregar y especifique el nombre, el protocolo, la dirección IP y el puerto. La dirección IP debe ser un asterisco (*).
   c) En la ficha Servicios, seleccione los servicios que representan los servidores de caché.
   d) En la ficha Avanzadas, para Modo de redirección, seleccione Basado en MAC.

e) Haga clic en Crear.

3. Configurar un servidor virtual de redirección de caché:
   a) Vaya a Administración del tráfico > Equilibrio de carga > Servicios virtuales.
   b) En el panel de detalles, haga clic en Agregar y especifique el nombre, el protocolo, la dirección IP y el puerto. La dirección IP debe ser *.
   c) En Tipo de caché, seleccione Transparente.
   d) En la ficha Avanzadas, en el cuadro Servidor de caché, seleccione el nuevo servidor virtual de equilibrio de carga y active las casillas de verificación Origin USIP y Usar intervalo de puertos. En el cuadro Expresión IP de origen, escriba HTTP.REQ.HEADER ("ClientIP").
   e) Haga clic en Crear.
4. Asigne un intervalo de puertos de origen para el dispositivo:
   a) En el panel de navegación, haga clic en Sistema y, a continuación, haga clic en Configuración.
   b) En el grupo Configuración, haga clic en el vínculo Cambiar la configuración global del sistema.
   c) En el grupo Intervalo de puertos de redirección de caché, especifique el intervalo de puertos del dispositivo escribiendo un número de puerto para el puerto de inicio y un número de puerto para el puerto final.
   d) Haga clic en Aceptar.

Traducir la dirección IP de destino de una solicitud a la dirección IP de origen

January 12, 2021

Puede configurar el servidor virtual de redirección de caché de proxy de reenvío en el dispositivo Citrix ADC para traducir la dirección IP de destino del aterrizaje de solicitud en el servidor virtual de redirección de caché a la dirección IP del servidor de origen. Esta traducción se produce independientemente de si la solicitud se envía a los servidores en caché o al servidor de origen.
Anteriormente, el servidor virtual de redirección de caché de proxy de reenvío en el entorno del proveedor de servicios no se podía utilizar eficazmente para enviar tráfico a través del firewall debido a las limitaciones en la redirección de caché mediante directivas de conmutación de contenido. El servidor virtual de redirección de caché no tradujo la dirección IP de origen en la IP de destino cuando el paquete se envió a la caché. La dirección IP de destino era la del servidor de origen solo cuando las solicitudes se servían desde el servidor en caché.

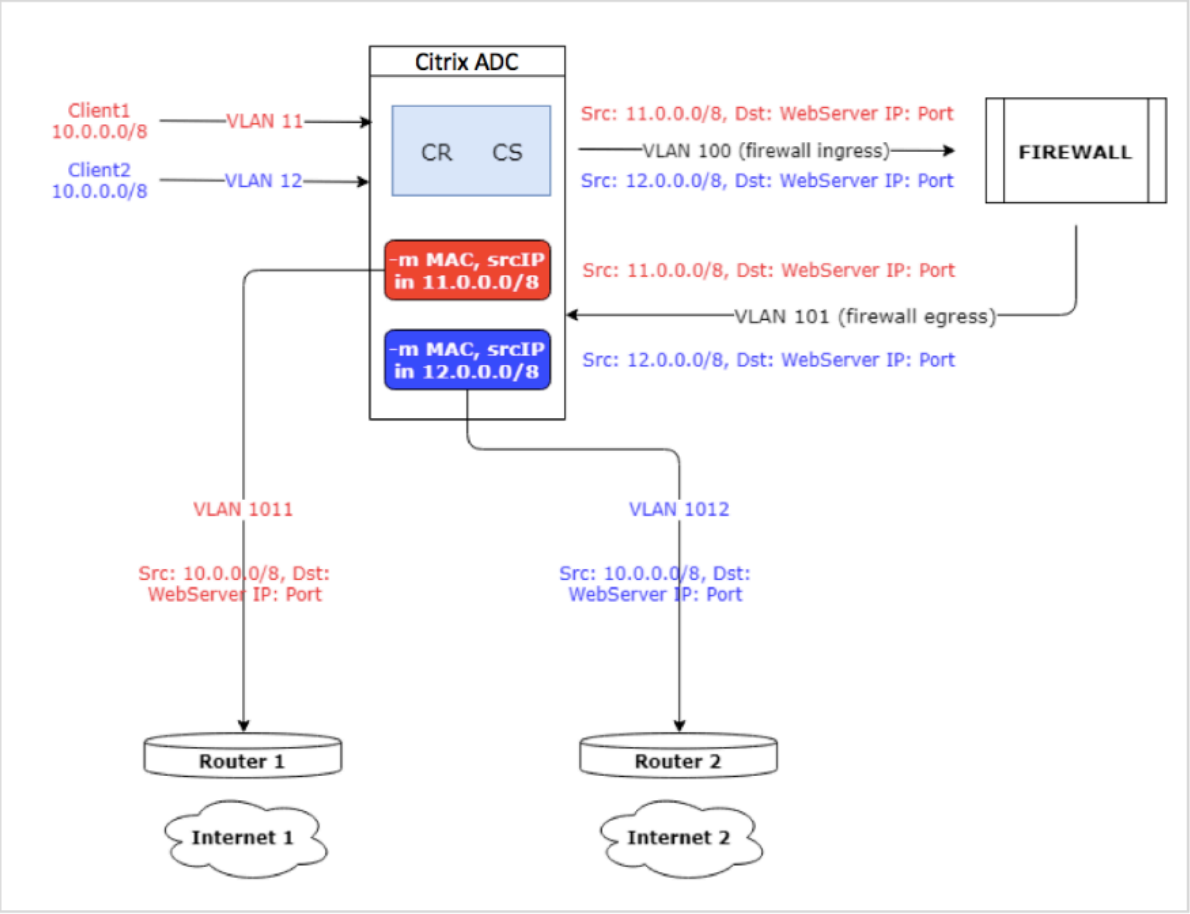
Nota: La traducción de la dirección IP de destino de una solicitud a la dirección IP de origen no se admite para un servidor virtual de redirección de caché transparente. Para un servidor virtual de redirección de caché transparente, esta opción debe establecerse en OFF.

Caso de uso

En una implementación que tiene el dispositivo Citrix ADC configurado para redirección de caché de proxy de reenvío, firewall y direcciones IP de cliente reutilizadas, el firewall no puede distinguir ni usar las direcciones IP reutilizadas. Por lo tanto, estas direcciones IP reutilizadas deben traducirse a direcciones IP diferentes. Para traducir las direcciones IP reutilizadas, el dispositivo Citrix ADC debe realizar lo siguiente:

1. Consulte un servidor virtual de equilibrio de carga DNS para obtener la resolución del destino.
2. Actualice la dirección IP de origen y el número de puerto en el destino.
3. Envíe la solicitud al firewall.

Considere la siguiente implementación que tiene un dispositivo Citrix ADC configurado para redirección de caché de proxy de reenvío, firewall y dos enrutadores (Router 1 y Router 2). El tráfico de red fluye a Internet 1 a través del Router 1 y a Internet 2 a través del Router 2 respectivamente.



En este ejemplo, las solicitudes de entrada de clientes provienen de dos VLAN diferentes, VLAN11 o VLAN12. Se reutiliza la dirección IP del cliente (10.0.0.0).
Según las directivas de redirección de caché y conmutación de contenido, la solicitud puede ir directamente al servidor de origen o al firewall.

- Si la solicitud tiene que omitir el firewall e ir a Internet, a continuación, en base a la solicitud de entrada VLAN, se selecciona el Router 1 o el Router 2 y la solicitud se envía a Internet 1 o Internet 2.
- Si la solicitud tiene que pasar por el firewall, entonces la IP de origen de la solicitud debe traducirse a una dirección IP específica. La dirección IP traducida se puede utilizar para identificar la VLAN a través de la cual ha llegado la solicitud. Por ejemplo, si la solicitud de entrada proviene de VLAN11, la dirección IP de origen se traduce a 11.x.x.x. Si la solicitud proviene de VLAN12, la dirección IP de origen se traduce a 12.x.x.x.

Una vez que el firewall procesa la solicitud, la solicitud se envía de nuevo al dispositivo. Mediante la combinación de perfiles de red y directivas de escucha, el dispositivo vuelve a traducir la dirección IP de origen a la dirección IP original y envía la solicitud al Router 1 o al Router 2 basándose en el ID de VLAN de entrada.

Nota: El modo del servidor virtual de equilibrio de carga enlazado a la caché siempre debe establecerse en modo MAC. Aunque el modo IP para esta función no está bloqueado, la configuración en modo IP genera un comportamiento inesperado.

Para traducir la dirección IP de destino y el número de puerto de la solicitud a la dirección IP de origen mediante la CLI

En el símbolo del sistema, escriba;

```
set cr vserver <vsname> -useoriginIpPortForCache <YES|NO>
<!--NeedCopy-->
```

Ejemplo:

```
set cr vserver cvsrv1 -useoriginIpPortForCache YES
<!--NeedCopy-->
```

Cuando useoriginIpPortForCache se establece en Sí y si la solicitud debe ser servida desde los servidores en caché, la IP de destino de la solicitud se traduce a la dirección IP del servidor de origen.

Nota: Si useoriginIpPortForCache está habilitado, establezca siempre el servidor virtual de equilibrio de carga enlazado a la caché en modo MAC.

Para traducir la dirección IP de destino y el puerto de la solicitud a la dirección IP de origen mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico** > **Redirección de caché** > **Servidores virtuales** y haga clic en **Agregar**.
2. Especifique los detalles del servidor virtual de redirección de caché.
3. Seleccione **Usar puerto IP de origen** para caché para habilitar la traducción de la dirección IP de destino de la solicitud a la dirección IP de origen.
4. Haga clic en **Aceptar**.

Agrupar en clústeres

August 20, 2021

> **Nota**
>
> Esta función está disponible con una licencia Citrix ADC Advanced o Premium Edition.

Un clúster Citrix ADC es un grupo de dispositivos nCore que trabajan juntos como una única imagen del sistema. Cada dispositivo del clúster se denomina nodo. El clúster puede tener un dispositivo o hasta 32 dispositivos virtuales o hardware Citrix ADC nCore como nodos.

El tráfico del cliente se distribuye entre los nodos para proporcionar alta disponibilidad, alto rendimiento y escalabilidad.

Para crear un clúster, debe realizar los siguientes pasos:

- Agregue los dispositivos como nodos de clúster.
- Configure la comunicación entre los nodos.
- Configure vínculos a las redes de cliente y servidor.
- Configure los dispositivos y configure la distribución del tráfico de cliente y servidor.

Tabla de compatibilidad para clúster Citrix ADC

October 5, 2021

La agrupación en clústeres en el dispositivo Citrix ADC admite una amplia variedad de funciones en configuraciones de Citrix ADC.

En la tabla siguiente se enumeran las funciones de Citrix ADC y se proporciona el estado de compatibilidad en las distintas versiones de Citrix ADC de configuraciones de clúster. El estado de compati-

bilidad de algunas funciones de Citrix ADC en un clúster Citrix ADC BLX 13.0 es diferente del clúster de 13,0 Citrix ADC que no es BLX (MPX o VPX, SDX ADC).

> **Importante**
>
> La entrada “Nivel de nodo” de la tabla indica que la función solo se admite en nodos de clúster individuales.

Funciones de Citrix ADC	11,1	12,1	13.0	13.0 Clúster Citrix ADC BLX	Citrix ADC 13.1
FIPS SSL	No	No	No	No	No
Paquete de certificados SSL	No	No	No	No	No
Intercepción SSL	NA	No	No	No	No
Acciones de cambio de contenido	Sí	Sí	Sí	Sí	Sí
Registro basado en directivas para directivas de conmutación de contenido	Sí	Sí	Sí	Sí	Sí
Limitación de velocidad	Sí	Sí	Sí	Sí	Sí
Análisis de acciones	Sí	Sí	Sí	No	Sí
GSLB	Sí	Sí	Sí	Sí	Sí
RTSP	Sí	Sí	Sí	Sí	Sí
DNSSEG	No	No	No	No	No
DNS64	No	No	No	No	No
FTP	Sí	Sí	Sí	No	Sí
TFTP	No	Sí	Sí	Sí	Sí

Funciones de Citrix ADC	11,1	12,1	13.0	13.0 Clúster Citrix ADC BLX	Citrix ADC 13.1
Espejado de conexiones	No	No	No	No	No
Almacenamient en caché integrado	Nivel de nodo	Nivel de nodo	Nivel de nodo	No	Nivel de nodo
Caché compartida grande	Nivel de nodo	Nivel de nodo	Nivel de nodo	No	Nivel de nodo
Optimización de front-end	Nivel de nodo	Nivel de nodo	Nivel de nodo	No	Nivel de nodo
Firewall de aplicaciones	Sí	Sí	Sí	No	Sí
Protección de denegación de servicio HTTP (HDOSP)	Nivel de nodo	Elementos retirados	Elementos retirados	Elementos retirados	Eliminado
Prioridad en cola (PQ)	Nivel de nodo	Nivel de nodo	Nivel de nodo	Elementos retirados	Eliminado
Conexión segura (SC)	Nivel de nodo	Nivel de nodo	Nivel de nodo	Elementos retirados	Eliminado
AppQoE	Sí	Sí	Sí	No	Sí
Protección contra picos de tensión	Nivel de nodo	Nivel de nodo	Nivel de nodo	Sí	Nivel de nodo
MPTCP	Sí	Sí	Sí	No	Sí
Recortes rayados	Sí; **Nota:** Se admite en clústeres L2. No se admite en clústeres L3.	Sí; **Nota:** Se admite en clústeres L2. No se admite en clústeres L3.	Sí; **Nota:** Se admite en clústeres L2. No se admite en clústeres L3.	Sí; **Nota:** Se admite en clústeres L2. No se admite en clústeres L3.	Sí; **Nota:** Se admite en clústeres L2. No se admite en clústeres L3.

Funciones de Citrix ADC	11,1	12,1	13.0	13.0 Clúster Citrix ADC BLX	Citrix ADC 13.1
MSR	Sí; **Nota:** Se admite en clústeres L2. No se admite en clústeres L3.	Sí; **Nota:** Se admite en clústeres L2. No se admite en clústeres L3.	Sí; **Nota:** Se admite en clústeres L2. No se admite en clústeres L3.	Sí; **Nota:** Se admite en clústeres L2. No se admite en clústeres L3.	Sí; **Nota:** Se admite en clústeres L2. No se admite en clústeres L3.
IS-IS (IPv4 e IPv6)	Sí	Sí	Sí	No	Sí
Marcos Jumbo	Sí	Sí	Sí	No	Sí
Túneles IP-IP	Sí	Sí	Sí	No	Sí
Equilibrio de carga de enlaces	Sí	Sí	Sí	Sí	Sí
FIS (conjunto de interfaces de conmutación por error)	Sí	Sí	Sí	No	Sí
Redundancia de enlace (LR)	Sí	Sí	Sí	No	Sí
NAT46	No	No	Sí	Sí	Sí
NAT64	No	No	Sí	Sí	Sí
RNAT6	Sí	Sí	Sí	Sí	Sí
LSN/CGNAT	No	Sí	Sí	No	Sí
Logotipo de lista IPv6	No	Sí	Sí	No	Sí
Dominios de tráfico	Sí; **Nota:** Se admite en clústeres L2. No se admite en clústeres L3.	Sí; **Nota:** Se admite en clústeres L2. No se admite en clústeres L3.	Sí; **Nota:** Se admite en clústeres L2. No se admite en clústeres L3.	No	Sí; **Nota:** Se admite en clústeres L2. No se admite en clústeres L3.

Funciones de Citrix ADC	11,1	12,1	13.0	13.0 Clúster Citrix ADC BLX	Citrix ADC 13.1
Monitor de ruta	Sí; Solo con DR.	Sí; **Nota:** Se admite en clústeres L2. No se admite en clústeres L3.	Sí **Nota:** Compatible con clústeres L2. No se admite en clústeres L3.	No	Sí **Nota:** Compatible con clústeres L2. No se admite en clústeres L3.
Túneles GRE (CB)	No	No	No	No	No
Modo capa 2	Sí	Sí	Sí	No	Sí
Perfiles de red	Sí	Sí	Sí	No	Sí
Llamada HTTPS	Sí	Sí	Sí	Sí	Sí
AAA-TM	Nivel de nodo	Sí	Sí	No	Sí
AppFlow	Nivel de nodo	Nivel de nodo	Nivel de nodo	No	Nivel de nodo
Información web	Sí	Sí	Sí	No	Sí
HDX Insight	Sí	Sí	Sí	No	Sí
vMAC/vRRP	Sí	Sí	Sí	No	Sí
NetScaler Push	No	No	No	No	No
Conmutación por error de conexión con estado	No	No	No	No	No
Cierre con período de gracia	No	Sí	Sí	Sí	Sí
Escala automática de DBS	No	No	Sí	Sí	Sí

Funciones de Citrix ADC	11,1	12,1	13.0	13.0 Clúster Citrix ADC BLX	Citrix ADC 13.1
DSR mediante TOS	No	No	No	Sí	No
Control de Startup-RR más fino	Nivel de nodo	Nivel de nodo	Nivel de nodo	No	Nivel de nodo
XSM XML	No	No	No	No	No
DHCP RA	No	No	No	No	No
Grupo de puentes	Sí	Sí	Sí	No	Sí
Puente de red	No	No	No	No	No
Interfaz Web en Citrix ADC (WionNS)	Sí	Sí	Sí	No	Sí
Supervisión de EdgeSight	Elementos retirados	Elementos retirados	Elementos retirados	No	Elementos retirados
Tablas métricas: Local	No	No	No	No	No
Almacenamiento en memoria caché	Nivel de nodo	Nivel de nodo	Nivel de nodo	Nivel de nodo	Nivel de nodo
Call Home	Nivel de nodo	Nivel de nodo	Nivel de nodo	No	Nivel de nodo
Modo proxy ICA de Citrix Gateway	Sí	Sí	Sí	No	Sí
Citrix Gateway (VPN SSL/VPN completa y VPN sin cliente)	Nivel de nodo	Nivel de nodo	Nivel de nodo	No	Nivel de nodo

Funciones de Citrix ADC	11,1	12,1	13.0	13.0 Clúster Citrix ADC BLX	Citrix ADC 13.1
Conector Citrix CloudBridge	No	Sí	Sí	No	Sí
Redirección basada en directivas (PBR/PBR6)	Sí	Sí	Sí	No	Sí
Redirección basada en directivas IPv4 (PBR) con servidor virtual LLB como salto siguiente	No	No	Sí	No	Sí
Redirección basada en directivas IPv6 (PBR6) con servidor virtual LLB como salto siguiente	No	No	No	No	No
Conciencia del suscriptor	No	No	No	No	No
Redirección dinámica	Sí, con compatibilidad con protocolos v6 (ospfv3 RIPng„ ISIS6, BGP6)	Sí, con compatibilidad con protocolos v6 (ospfv3 RIPng„ ISIS6, BGP6)	Sí, con compatibilidad con protocolos v6 (ospfv3 RIPng„ ISIS6, BGP6)	Sí	Sí, con compatibilidad con protocolos v6 (ospfv3 RIPng„ ISIS6, BGP6)

Funciones de Citrix ADC	11,1	12,1	13.0	13.0 Clúster Citrix ADC BLX	Citrix ADC 13.1
SYSLOG-TCP, equilibrio de carga de servidores syslog, soporte SNIP y soporte FQDN para syslog	Sí; **Nota:** Se admite desde NetScaler 11.1, compilación 54.16 en adelante.	Sí	Sí	Sí	Sí
Gestión de bots	No	No	Sí	No	Sí
VXLAN	No	No	No	No	No

Además, se admiten las siguientes configuraciones de Citrix ADC:

Equilibrio de carga, persistencia del equilibrio de carga, equilibrio de carga DNS, SIP, MaxClient, Spillover (conexión y dinámica). Desbordamiento basado en ancho de banda, DataStream, control de compresión, filtrado de contenido, almacenamiento en búfer TCP, redirección de caché, denegación de servicio distribuida (DDoS). Keep-alive del cliente, redes básicas (IPv4 e IPv6), OSPF (IPv4 e IPv6), RIP (IPv4 e IPv6), RIP (IPv4 e IPv6). VLAN, ICMP, fragmentación, MBF, ACL, ACL simple, MSR, detección de MTU de ruta, IP-IP, SNMP, directivas (clásicas y avanzadas). Reescritura, Respondedor, llamada HTTP, registro del servidor web, registro de auditoría (NSLOG y syslog). USIP, comandos de ubicación, API NITRO, AppExpert, KRPC.

Requisitos previos

March 9, 2022

Los dispositivos Citrix ADC (MPX, VPX, SDX ADC, BLX) que se van a agregar a un clúster deben cumplir los siguientes requisitos previos:

- Todos los dispositivos deben tener la misma versión de software y compilación.
- Todos los dispositivos deben ser del mismo tipo de plataforma. Esto significa que un clúster debe tener todos los dispositivos de hardware (Citrix ADC MPX) o todos los dispositivos Citrix ADC VPX, todos los dispositivos Citrix BLX o todas las instancias Citrix SDX ADC.

Nota:

- Para un clúster de dispositivos de hardware (MPX), los dispositivos deben ser del mismo tipo de modelo.
- Para la formación del clúster heterogéneo, todos los dispositivos deben ser del tipo de plataforma MPX.
- Para un clúster de dispositivos virtuales (VPX), los dispositivos deben implementarse en los siguientes hipervisores: XenServer, Hyper-V, VMware ESX y KVM.
- Para configurar un clúster de instancias Citrix ADC de SDX, consulte Configuración de un clúster de instancias Citrix ADC.
- Las tramas jumbo se admiten en un clúster de Citrix ADC compuesto por instancias de Citrix ADC SDX.
- Puede crear clústeres L3 de instancias SDX.
- Para obtener información sobre la configuración de un clúster de Citrix ADC BLX, consulte clúster de Citrix ADC BLX.

- Los dispositivos pueden pertenecer a redes diferentes.
- Configurarse inicialmente y conectarse a una red común del lado del cliente y del lado del servidor.
- Para un clúster de dispositivos virtuales (Citrix ADC VPX, Citrix ADC BLX o instancia de Citrix SDX ADC) que tiene configuraciones grandes, se recomienda utilizar 6 GB de RAM para cada nodo del clúster.

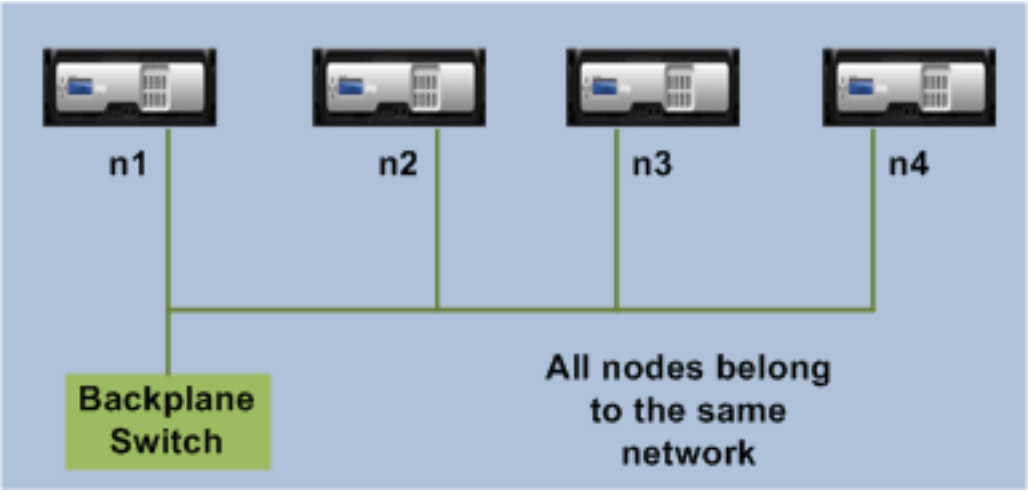
Introducción a los clústeres

August 20, 2021

Un clúster de Citrix ADC se forma agrupando los dispositivos Citrix ADC. En función de la ubicación de red de los dispositivos Citrix ADC que quiere agregar el clúster, debe tener en cuenta las siguientes configuraciones de clúster:

> **Nota**
>
> A menos que se especifique lo contrario, las funciones y configuraciones del clúster son las mismas para los clústeres L2 y L3.

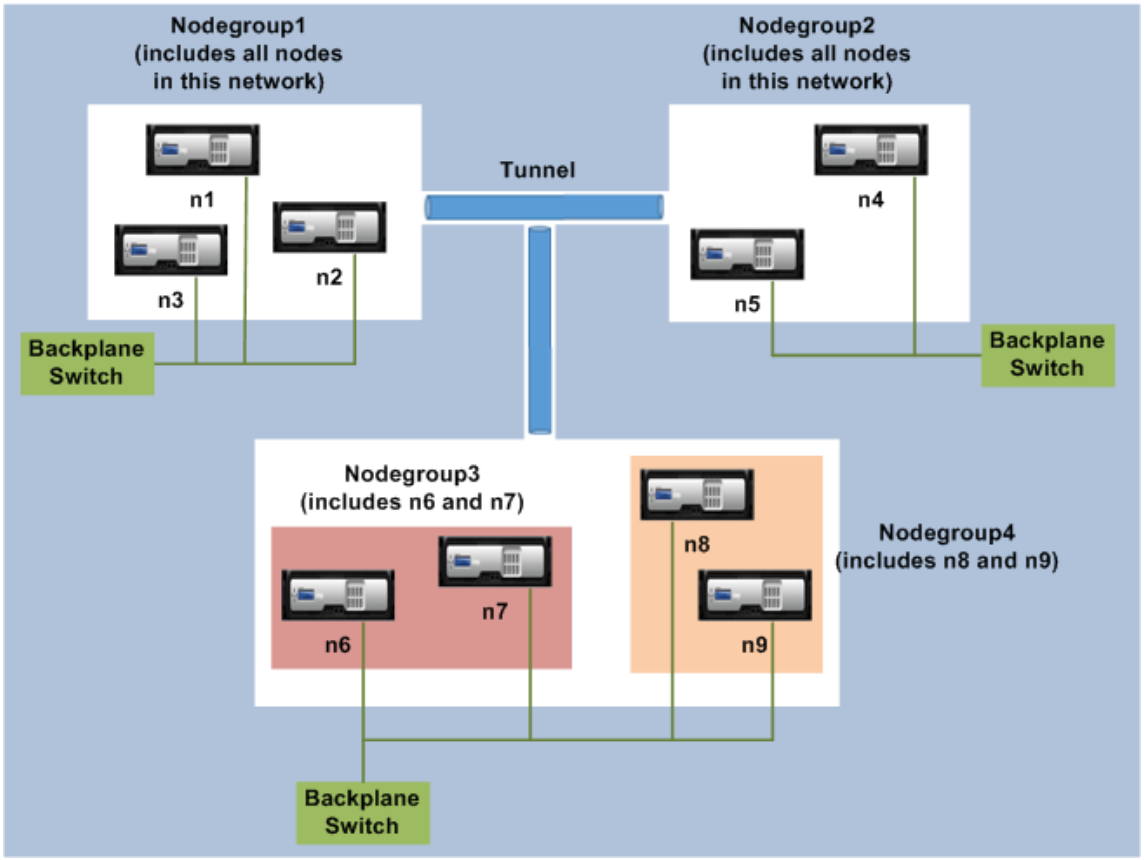
- **Clúster L2:** en esta implementación de clúster, todos los nodos de clúster pertenecen a la misma red.



- **Clúster L3 (también denominado "clúster en modo INC"):** en esta implementación de clúster, los nodos de clúster pueden pertenecer a diferentes redes. Los nodos de clúster de una red específica deben agruparse en grupos de nodos que incluyan solo nodos de esa red. De la siguiente ilustración, vemos que los nodos n1, n2, n3 están en la misma red y se agrupan en Nodegroup1.

  Del mismo modo, el caso de los nodos n4 y n5, que se agrupan en Nodegroup2. En la tercera red, hay dos grupos de nodos. Nodegroup3 incluye n6 y n7 y Nodegroup4 incluye n8 y n9.

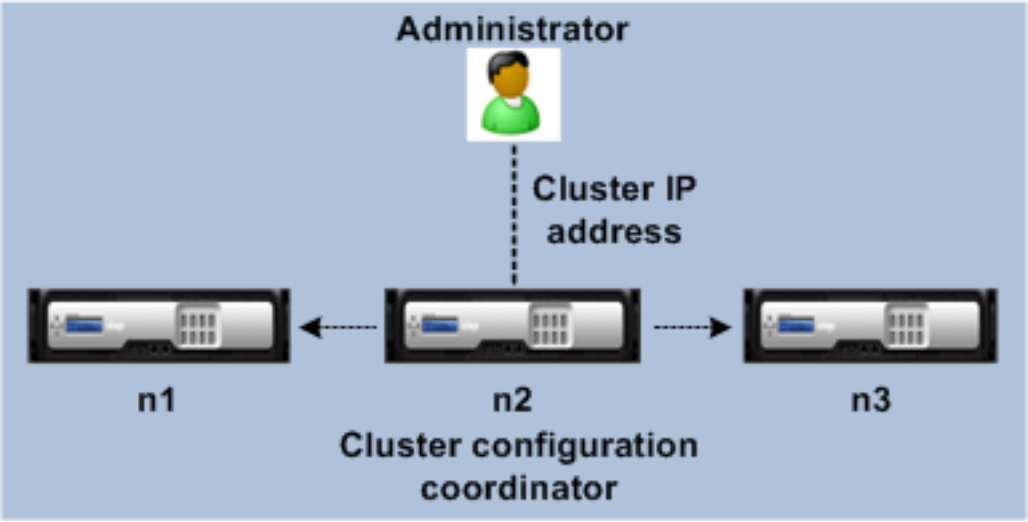
  > **Nota**
  >
  > Compatible con NetScaler 11.0 en adelante.



Sincronización entre nodos de clúster

August 20, 2021

Todas las configuraciones de un clúster de Citrix ADC se realizan en la dirección IP del clúster, que es la dirección de administración del clúster. El nodo del clúster posee la dirección IP del clúster que se conoce como coordinador de configuración de clúster (CCO), como se muestra en la siguiente ilustración:



Las configuraciones disponibles en el CCO se propagan automáticamente a los otros nodos del clúster y, por lo tanto, todos los nodos del clúster tienen las mismas configuraciones.

- Citrix ADC permite realizar solo unas pocas configuraciones en nodos de clúster individuales a través de su dirección NSIP. En estos casos, debe garantizar la coherencia de la configuración manualmente en todos los nodos del clúster. Estas configuraciones no se propagan a través de los otros nodos del clúster. Para obtener más información sobre las operaciones admitidas en cada nodo de clúster, consulte Operaciones admitidas en nodos de clúster individuales.
- Los siguientes comandos cuando se ejecutan en la dirección IP del clúster no se propagan a otros nodos de clúster:
  - **shutdown.** Apaga solo el coordinador de configuración.
  - **reboot.** Reinicia solo el coordinador de configuración.
  - **rm cluster instance.** Quita la instancia de clúster del nodo en el que está ejecutando el comando.
- Para que un comando se propague a otros nodos de clúster:
  - El quórum debe configurarse en la instancia del clúster.
  - La mayor parte del quórum de clúster con (n/2 + 1) de los nodos del clúster debe estar activo para que el clúster esté operativo.
  - Un clúster puede ejecutarse con un número mínimo de nodos cuando la regla mayoritaria (n/2 + 1) está relajada.

Cuando se agrega un nodo a un clúster, las configuraciones y los archivos (certificados SSL, licencias, DNS, etc.) que están disponibles en el CCO se sincronizan con el nodo de clúster recién agregado. Cuando se agrega una vez más un nodo de clúster existente, que se inhabilitó intencionadamente o que había fallado, el clúster compara las configuraciones disponibles en el nodo con las configuraciones disponibles en el CCO. Si hay una discrepancia en las configuraciones, el nodo se sincroniza mediante una de las siguientes opciones:

- **Sincronización completa.** Si la diferencia entre configuraciones supera los 255 comandos, to-

das las configuraciones del CCO se aplican al nodo que vuelve a unirse al clúster. El nodo permanece operacionalmente no disponible durante la sincronización.

- **Sincronización incremental.** Si la diferencia entre configuraciones es menor o igual que 255 comandos, solo las configuraciones que no están disponibles se aplican al nodo que se vuelve a unir al clúster. El estado operativo del nodo no se ve afectado.

> **Nota**
>
> También puede sincronizar manualmente las configuraciones y los archivos. Para obtener más información, consulteSincronización de configuraciones de clúster y Sincronización de archivos de clúster.

Configuraciones rayadas, parcialmente rayadas y manchadas

August 20, 2021

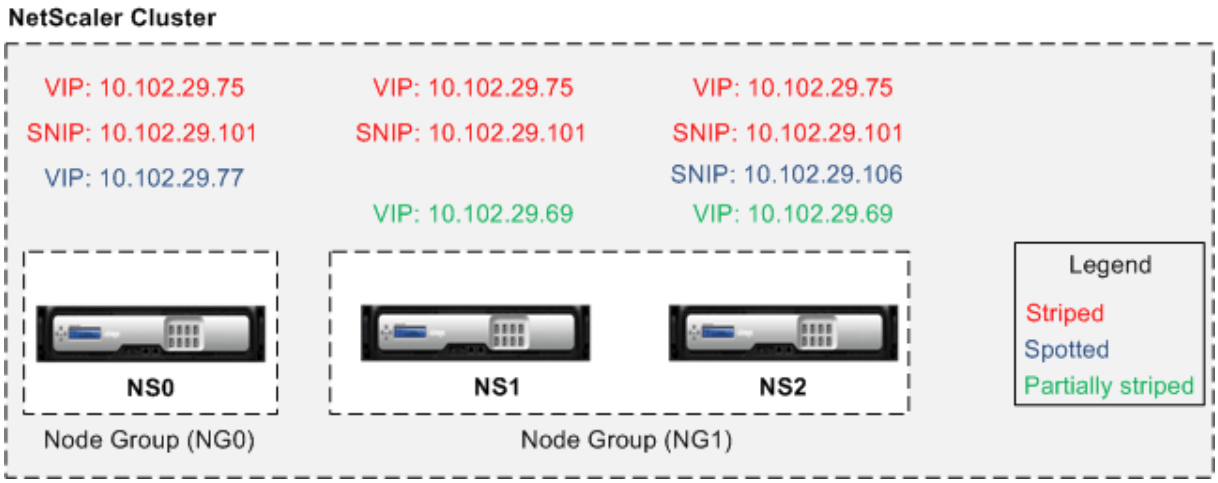
En virtud de la propagación de comandos, todos los nodos de un clúster tienen las mismas configuraciones. Sin embargo, es posible que quiera que algunas configuraciones estén disponibles solo en determinados nodos del clúster. Aunque no puede restringir los nodos en los que están disponibles las configuraciones, puede especificar los nodos en los que están activas las configuraciones.

Por ejemplo, puede:

- definir una dirección SNIP para que esté activa en un solo nodo, o
- definir una dirección SNIP para estar activa en todos los nodos, o
- definir una dirección VIP para estar activa en un solo nodo, o
- definir una dirección VIP para estar activa en todos los nodos, o
- definir una dirección VIP para estar activa solo en dos nodos de un clúster de 3 nodos

Dependiendo del número de nodos en los que estén activas las configuraciones, las configuraciones de clúster se denominan configuraciones seccionados, parcialmente seccionados o manchados.

Ilustración 1. Cluster de tres nodos con configuraciones rayadas, parcialmente rayadas y manchadas



La tabla siguiente proporciona más detalles sobre los tipos de configuraciones:

Tipo de configuración	Activa en	Aplicable a	Configuraciones
Configuración seccionada	Todos los nodos del clúster	Todas las entradas	No se requiere una configuración específica para crear una entidad seccionada. De forma predeterminada, todas las entidades definidas en una dirección IP del clúster se secan en todos los nodos del clúster.
Configuración seccionada parcialmente	Un subconjunto de nodos de clúster	Consulte Grupos de nodos de clúster.	Enlazar las entidades que quiere que estén parcialmente secadas a un grupo de nodos. La configuración solo está activa en los nodos del clúster que pertenecen al grupo de nodos.

Tipo de configuración	Activa en	Aplicable a	Configuraciones
Configuración manchado	Nodo de clúster único	Dirección SNIP, ID de motor SNMP, nombre de host de nodos de clúster, entidades que se pueden enlazar a un grupo de nodos	Una configuración manchada se puede definir mediante uno de estos dos enfoques. **Dirección SNIP** Al crear la dirección SNIP, especifique el nodo en el que quiere que esté activa la dirección SNIP, como nodo propietario. **Ejemplo**, `add ns ip 10.102.29.106 255.255.255.0 -type SNIP -ownerNode 2` (suponiendo que el Id. de nodo NS2 sea 2). **Nota**: No puede cambiar la propiedad de una dirección SNIP detectada en tiempo de ejecución. Para cambiar la propiedad, primero debe eliminar la dirección SNIP y agregarla de nuevo especificando el nuevo propietario. **Entidades que se pueden enlazar a un grupo de nodos.** Al vincular la entidad a un grupo de nodos de un solo miembro.

> **Nota**
>
> - Cuando inhabilita USIP, Citrix recomienda utilizar direcciones SNIP detectada. Solo puede utilizar direcciones SNIP seccionadas si hay escasez de direcciones IP. El uso de direcciones IP seccionadas puede provocar problemas de flujo ARP si no hay direcciones IP detectada en la misma subred para la resolución ARP.
> - Cuando habilita USIP, Citrix recomienda utilizar direcciones SNIP seccionadas como Gateway para el tráfico iniciado por el servidor.

Compatibilidad de propietario de ARP para IP seccionada

En una configuración de clúster, puede configurar un nodo específico para responder a la solicitud ARP para una IP seccionado. El nodo configurado responde al tráfico ARP.

Se introduce un nuevo parámetro “ArPowner” en los comandos “add, set and unset IP”.

Para habilitar el propietario ARP en un nodo mediante la CLI.

En el símbolo del sistema, escriba:

```
add ns ip <ip_address> -arpOwner <node_id>
```

> **Nota**
>
> El parámetro propietario de ARP solo se admite en el clúster L2.

Compatibilidad con propietarios de detección de vecinos para direcciones IPv6 seccionadas

En una configuración de clúster, puede configurar un nodo específico como propietario de detección de vecinos (ND) para la dirección IPv6 seccionada a fin de determinar la dirección de capa de vínculo. Un cliente envía un mensaje de solicitud de vecino (NS) a todos los nodos de la configuración del clúster. El propietario de ND responde con un mensaje de anuncio de vecino (NA) con la dirección de capa de vínculo para la dirección IPv6 seccionada y sirve tráfico.

Para habilitar el propietario de ND en un nodo mediante la CLI

En el símbolo del sistema, escriba:

```
1 add ns ip6 <IPv6Address> -ndOwner <node id>
2
3 set  ns ip6 <IPv6Address> -ndOwner <node id>
4 <!--NeedCopy-->
```


Ejemplo:

```
add ns ip6 2001::21/64 -ndOwner 1

set ns ip6 2001::21/64 -ndOwner 1
<!--NeedCopy-->
```

Para habilitar el propietario de ND en un nodo mediante la GUI

1. Vaya a **Sistema > Red > IP**.
2. En la página **IP**, vaya a la ficha **IPv6s** y haga clic en **Agregar**.
3. En la página **Crear IPv6**, seleccione uno de los ID de nodo enumerados en **NDowner en el menú desplegable Cluster**.

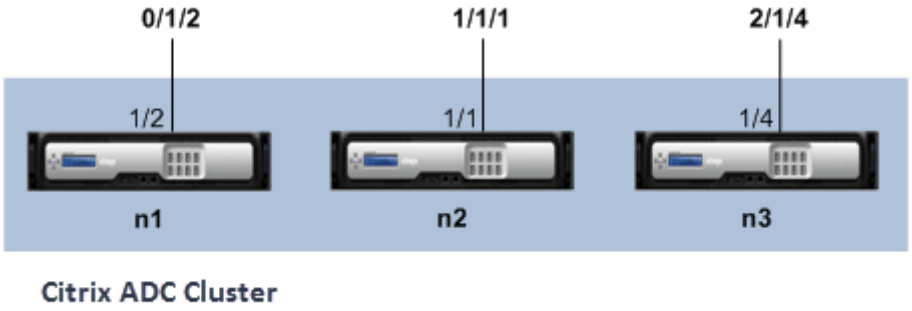
> **Nota**
>
> El parámetro propietario de ND solo se admite en el clúster L2.

Comunicación en una configuración de clúster

August 20, 2021

Las interfaces de los dispositivos Citrix ADC que se agregan a un clúster tienen el prefijo de un identificador de nodo. Ayuda a identificar el nodo del clúster al que pertenece la interfaz. Por lo tanto, el identificador de interfaz c/u, donde c es el número del Controller y u es el número de unidad, ahora se convierte en n/c/u, donde n es el ID del nodo. Por ejemplo, en la siguiente ilustración, la interfaz 1/2 del nodo n1 se representa como 0/1/2, la interfaz 1/1 del nodo n2 se representa como 1/1/1 y la interfaz 1/4 del nodo n3 se representa como 2/1/4.

Ilustración 1. Convención de nomenclatura de interfaz en un clúster



- **Comunicación del servidor**:
  el clúster se comunica con el servidor a través de las conexiones físicas entre el nodo del clúster y el dispositivo de conexión del lado del servidor. La agrupación lógica de estas conexiones físicas se denomina plano de datos del servidor.
- **Comunicación del cliente**: El clúster se comunica con el cliente a través de las conexiones físicas entre el nodo del clúster y el dispositivo de conexión del lado del cliente. La agrupación lógica de estas conexiones físicas se denomina plano de datos del cliente.
- **Comunicación entre nodos**: Los nodos del clúster también pueden comunicarse entre sí. La forma en que se comunican depende de si el nodo existe en la misma red o entre redes.
  - Los nodos del clúster dentro de la misma red se comunican entre sí mediante el backplane del clúster. El backplane es un conjunto de interfaces en las que una interfaz de cada nodo está conectada a un conmutador común, que se denomina conmutador de backplane del clúster. Los diferentes tipos de tráfico que pasa a través del plano posterior, que es utilizado por la comunicación entre nodos son:
    * Mensajería de nodo a nodo (NNM)
    * Tráfico dirigido
    * Propagación y sincronización de la configuración
  - Cada nodo del clúster utiliza una dirección especial del conmutador de backplane del clúster MAC para comunicarse con otros nodos a través del backplane. El MAC especial del clúster tiene la forma: `0x02 0x00 0x6F <cluster_id> <node_id> <reserved>)`, donde `cluster_id` es el identificador de instancia del clúster, `node_id` es el número de nodo del dispositivo Citrix ADC que se agrega a un clúster.

Las siguientes ilustraciones muestran las interfaces de comunicación en clústeres L2 y clústeres L3.

Ilustración 2. Interfaces de comunicación de clúster: Clúster L2

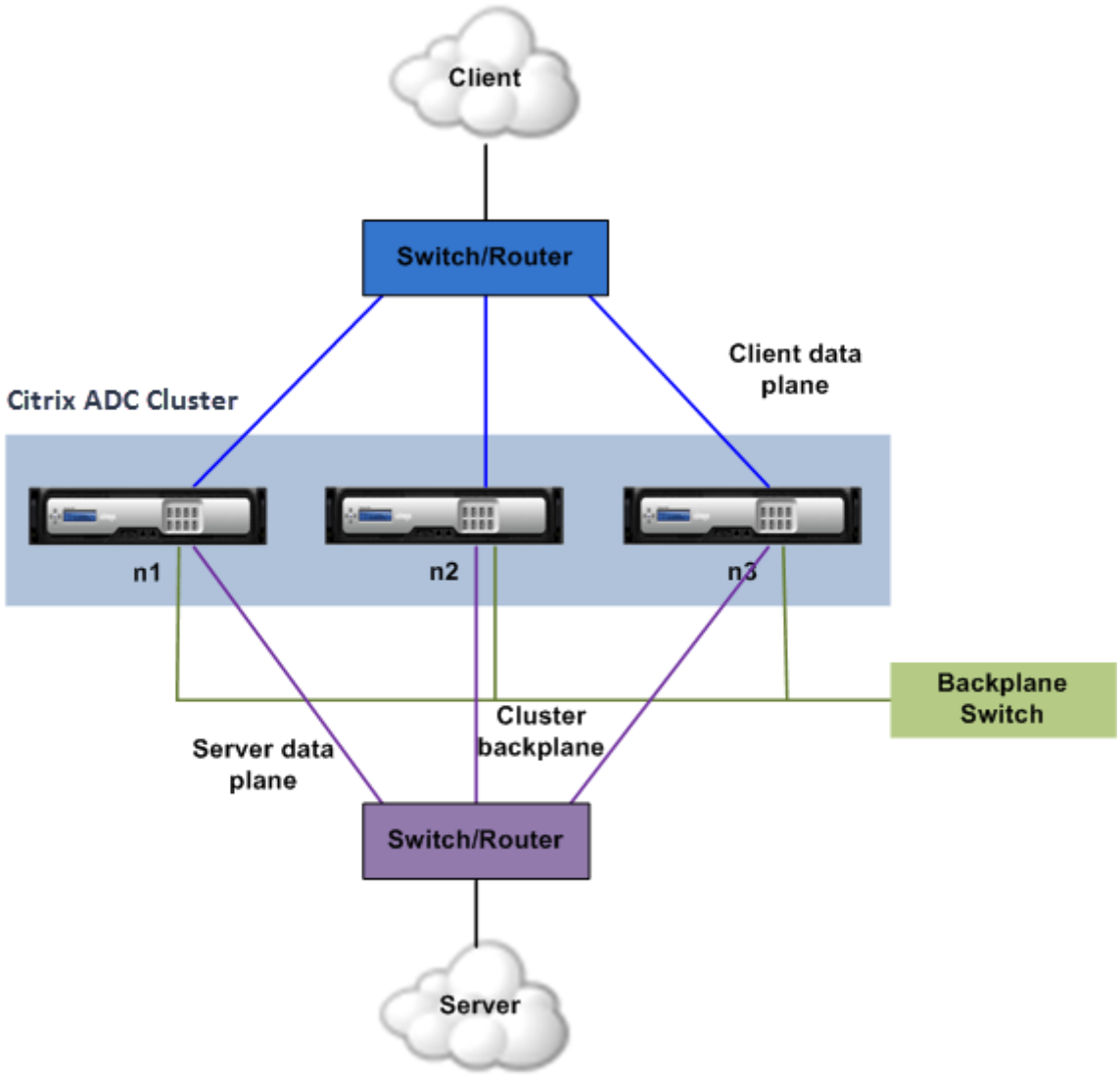
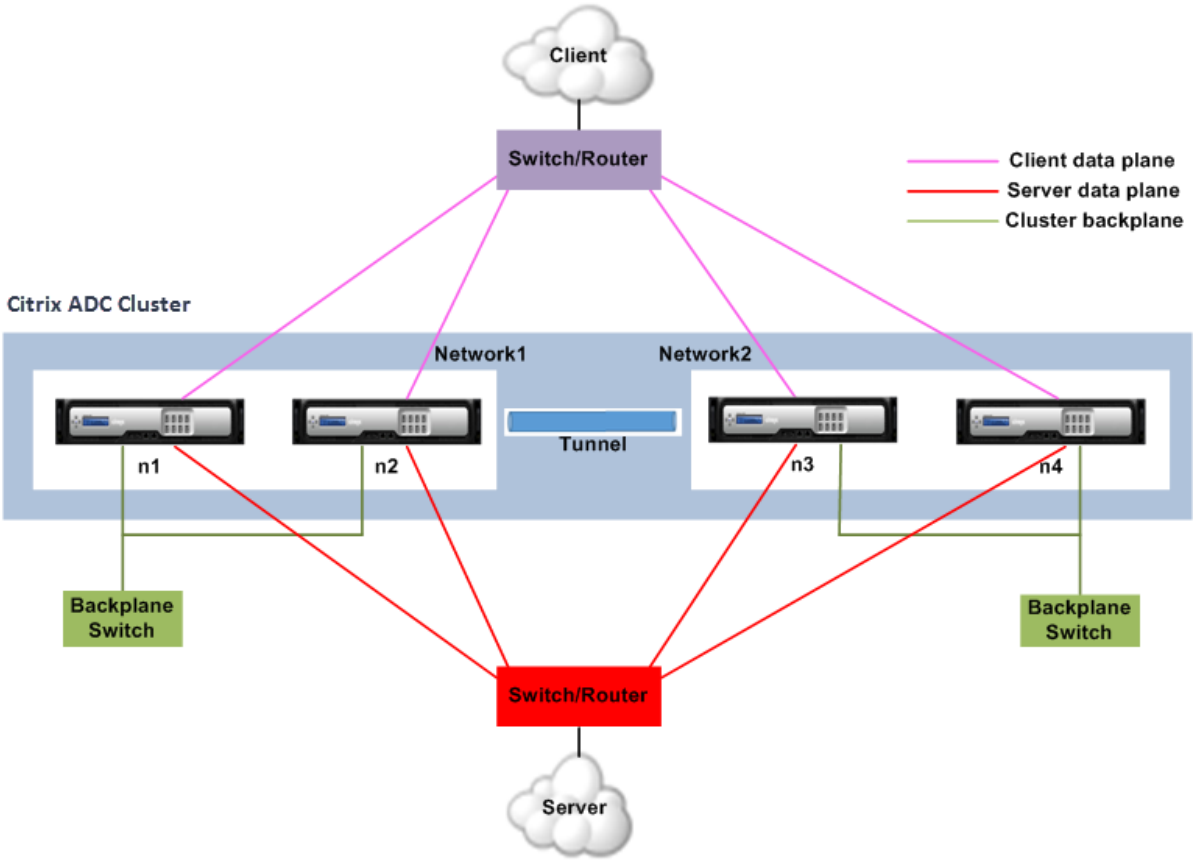


Ilustración 3. Interfaces de comunicación de clúster: Clúster L3



Distribución del tráfico en una configuración de clúster

August 20, 2021

En una configuración de clúster, las redes externas ven la colección de dispositivos Citrix ADC como una sola entidad. Por lo tanto, el clúster debe seleccionar un único nodo que debe recibir el tráfico. El clúster realiza esta selección mediante el mecanismo de distribución de tráfico de agregación de vínculos de agrupación de vínculos de clúster. El nodo seleccionado se denomina receptor de flujo.

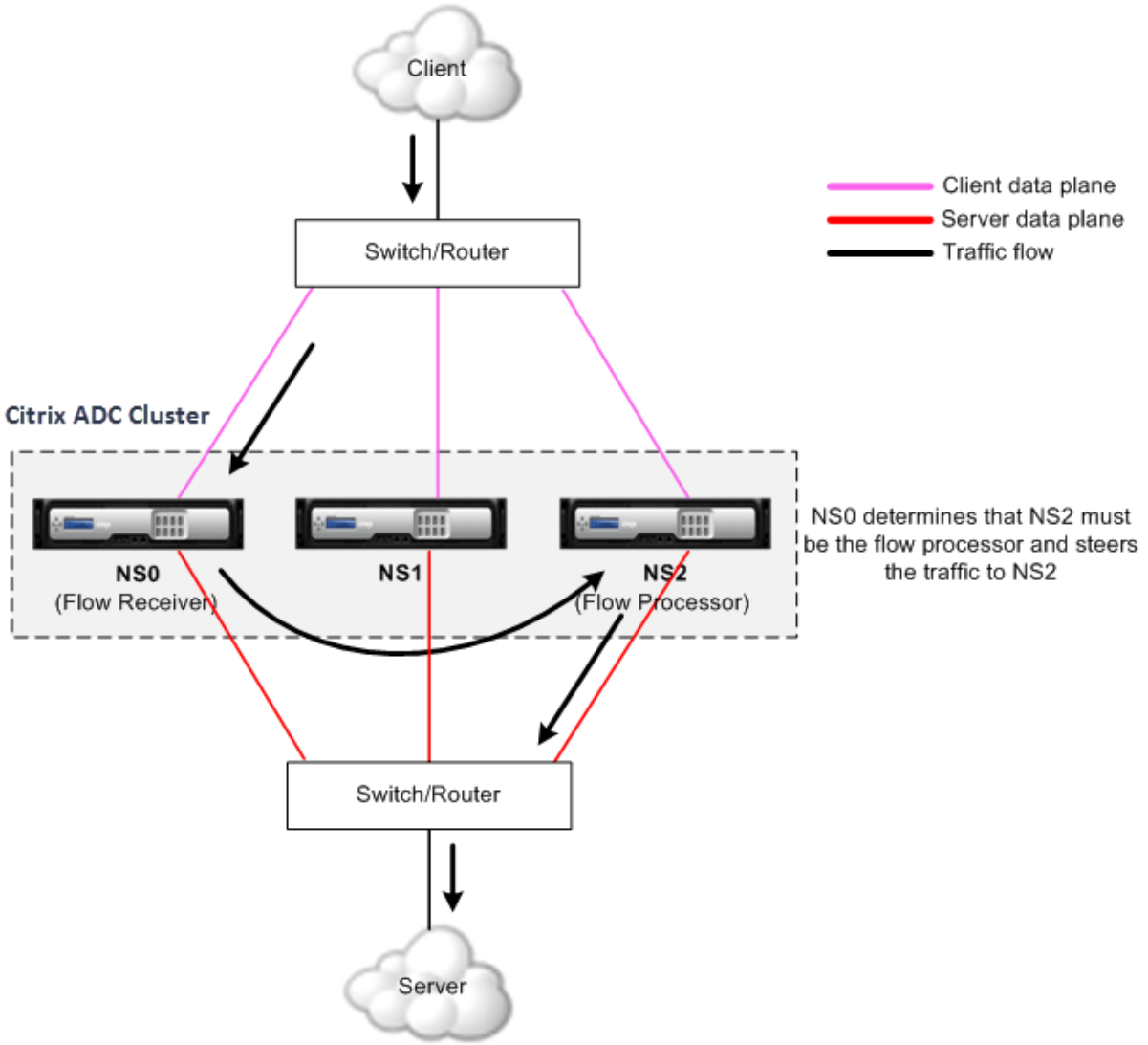
> **Nota**
>
> Para un clúster L3 (nodos en diferentes redes), solo se puede utilizar la distribución del tráfico ECMP.

El receptor de flujo obtiene el tráfico y, a continuación, mediante la lógica de clúster interna, determina el nodo que debe procesar el tráfico. Este nodo se denomina procesador de flujo. El receptor de flujo dirige el tráfico hacia el procesador de flujo sobre el plano posterior si el receptor de flujo y el procesador de flujo están en la misma red. El tráfico se dirige a través del túnel si el receptor de flujo y el procesador de flujo están en redes diferentes.

Nota

- El receptor de flujo y el procesador de flujo deben ser nodos capaces de servir el tráfico.
- A partir de NetScaler 11, puede desactivar la dirección en el backplane del clúster. Para obtener más información, consulte Desactivación de la dirección en el plano posterior del clúster.

Ilustración 1. Distribución del tráfico en un clúster



La ilustración anterior muestra una solicitud de cliente que fluye a través del clúster. El cliente envía una solicitud a una dirección IP virtual (VIP). Un mecanismo de distribución de tráfico configurado en el plano de datos del cliente selecciona uno de los nodos del clúster como receptor de flujo. El receptor de flujo recibe el tráfico, determina el nodo que debe procesar el tráfico y dirige la solicitud a ese nodo (a menos que el receptor de flujo se seleccione a sí mismo como el procesador de flujo).

El procesador de flujo establece una conexión con el servidor. El servidor procesa la solicitud y envía la respuesta a la dirección IP de subred (SNIP) que envió la solicitud al servidor.

- Si la dirección SNIP es una dirección IP seccionada o parcialmente seccionada, el mecanismo de distribución de tráfico configurado en el plano de datos del servidor selecciona uno de los nodos del clúster como receptor de flujo. El receptor de flujo recibe el tráfico, determina el procesador de flujo y dirige la solicitud al procesador de flujo a través del plano anterior del clúster.
- Si la dirección SNIP es una dirección IP detectada, el nodo que posee la dirección SNIP recibe la respuesta del servidor.

En una topología de clúster asimétrica (todos los nodos de clúster no están conectados al conmutador externo), debe utilizar conjuntos de vínculos exclusivamente o combinados con ECMP o agregación de vínculos de clúster. Para obtener más información, consulte Uso de conjuntos de enlaces.

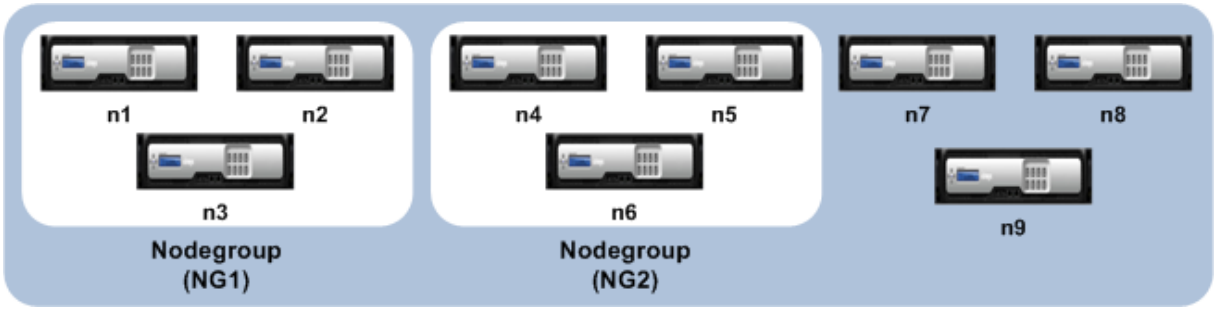
Grupos de nodos de

August 20, 2021

> **Nota**
>
> Los grupos de nodos se admiten desde NetScaler 10.1 en adelante.

Como su nombre indica, un grupo de nodos de clúster es un grupo de nodos de clúster.

Ilustración 1. Clúster de Citrix ADC con grupos de nodos



La ilustración anterior muestra un clúster que tiene grupos de nodos NG1 y NG2 que incluyen 3 nodos de clúster cada uno. El clúster también tiene 3 nodos que no forman parte de ningún grupo de nodos.

Se puede configurar un grupo de nodos para lo siguiente:

- Para definir configuraciones manchadas y parcialmente rayadas. Para obtener más información, consulte Grupos de nodos para configuraciones detectadas y parcialmente rayadas.
- Para configurar la redundancia de grupos de nodos. Para obtener más información, consulte Configuración de redundancia para grupos de nodos.
  Nota: Compatible con NetScaler 10.5 Build 52.1115.e en adelante.

- Para definir un clúster L3 (también denominado clúster en modo INC). En un clúster L3, los nodos de clúster pueden ser de diferentes redes. Debe agrupar los nodos que pertenecen a una red en un solo grupo de nodos. Por ejemplo, si n1, n2, n3 están en red1 y n4, n5, n6 están en red2, entonces NG1 debe incluir nodos de red1 y NG2 debe incluir nodos de red2. Para configurar un clúster de L3, consulte Creación de un clúster de Citrix ADC.

> **Nota**
>
> - Compatible con NetScaler 11 en adelante.
> - Las funciones anteriores de un grupo de nodos son mutuamente excluyentes. Significa que un grupo de nodos puede proporcionar solo una de las funcionalidades mencionadas anteriormente.

Estados de clúster y nodo

January 12, 2021

Para que un clúster funcione, la mayoría de los nodos (n/2 + 1) deben estar activos operacionalmente (el estado operativo es ACTIVO).

> **Importante**
>
> Desde NetScaler versión 10.5, puede configurar el clúster para que funcione incluso cuando no se cumplan los criterios mayoritarios. Esta configuración debe realizarse al crear un clúster.

Para obtener más información sobre los estados de un nodo de clúster, consulte Estados de un nodo de clúster.

Redirección en un clúster

August 20, 2021

La redirección en un clúster funciona de la misma manera que la redirección en un sistema independiente. Algunos puntos a tener en cuenta:

- Todas las configuraciones de redirección deben realizarse desde la dirección IP del clúster y las configuraciones se propagan a los demás nodos del clúster.
- Las rutas están limitadas al número máximo de rutas ECMP admitidas por el enrutador ascendente.
- Las configuraciones de redirección específicas de nodo se deben realizar mediante el argumento owner-node de la siguiente manera:


```
1   router ospf
2     owner-node 0
3       ospf router-id 97.131.0.1
4     exit-owner-node
5   !
6 <!--NeedCopy-->
```

El siguiente comando muestra la configuración del clúster consolidado para todos los nodos de VTYSH.

```
show cluster-config
```

El siguiente comando muestra el estado del clúster en cada nodo.

```
show cluser node
```

Redirección de IPv4 en clúster L2

La siguiente sección contiene configuraciones de ejemplo que le ayudan a configurar la redirección OSPF y BGP IPv4 en el clúster L2.

Agregar dirección SNIP detectada y habilitar el redirección dinámica

En la siguiente configuración, la redirección OSPF y BGP están habilitados. Además, se agregan direcciones SNIP detectada y se habilita el redirección dinámica en estas direcciones SNIP.

```
1 en ns fea ospf bgp
2 add vlan 10
3 add ns ip 10.10.10.1 255.255.255.0 -dynamicrouting enabled -ownernode 1
4 add ns ip 10.10.10.2 255.255.255.0 -dynamicrouting enabled -ownernode 2
5 add ns ip 10.10.10.3 255.255.255.0 -dynamicrouting enabled -ownernode 3
6 bind vlan 10 -ipaddress 10.10.10.1 255.255.255.0
7 <!--NeedCopy-->
```

Configuración OSPF IPv4 de VTYSH

Para configurar IPv4 OSPF en el clúster L2, debe:

- Establezca la prioridad en cero.
- Configure el ID del enrutador como una configuración detectada.

> **Nota**
>
> Las directrices de configuración OSPF para el clúster L2 también son aplicables a OSPFv3.

En la siguiente configuración de ejemplo se configura OSPF IPv4.

```
       interface vlan10
        IP OSPF PRIORITY 0
        !
       router ospf
           owner-node 1
             ospf router-id 97.131.0.1
           exit-owner-node
           owner-node 2
             ospf router-id 97.131.0.2
           exit-owner-node
           owner-node 3
             ospf router-id 97.131.0.3
           exit-owner-node
       network 10.10.10.0/24 area 0
       redistribute kernel
        !
<!--NeedCopy-->
```

Configuración de VTYSH IPv4 BGP

En la siguiente configuración de ejemplo de VTYSH, se configura IPv4 BGP.

```
     router bgp 100
       neighbor 10.10.10.10 remote-as 200
      owner-node 1
       neighbor 10.10.10.10 update-source 10.10.10.1
      exit-owner-node
      owner-node 2
       neighbor 10.10.10.10 update-source 10.10.10.2
      exit-owner-node
      owner-node 3
       neighbor 10.10.10.10 update-source 10.10.10.3
      exit-owner-node
     redistribute kernel
     !
<!--NeedCopy-->
```


> **Nota**
>
> El comando update-source se utiliza para cada vecino con el argumento owner-node en la siguiente configuración para conectarse con la IP de origen adecuada.

Redirección de IPv6 en clúster L2

La siguiente sección contiene configuraciones de ejemplo que le ayudan a configurar la redirección OSPF y BGP IPv6 en el clúster L2.

Habilitar redirección de IPv6

Antes de configurar la redirección IPv6 en un clúster L2, debe habilitar la función IPv6.

Para habilitar la redirección IPv6 mediante el CLI,

En el símbolo del sistema, escriba:

- `enable ns fea ipv6pt`

Agregar la dirección SNIP6 detectada y habilitar el redirección dinámica

En la siguiente configuración, la redirección OSPF y BGP están habilitados. Además, se agregan direcciones SNIP6 detectada y se habilita el redirección dinámica en estas direcciones SNIP6.

```
add ns ip6 3ffa::1/64 -dynamicrouting enabled -ownernode 1
add ns ip6 3ffa::2/64 -dynamicrouting enabled -ownernode 2
add ns ip6 3ffa::3/64 -dynamicrouting enabled -ownernode 3
add vlan 10
bind vlan 10 -ipaddress 3ffa::1/64
<!--NeedCopy-->
```

Configuración de VTYSH IPv6 BGP

En la siguiente configuración de ejemplo de VTYSH, se configura IPv6 BGP.

```
  router bgp 100
   neighbor 3ffa::10 remote-as 200
     owner-node 1
      neighbor 3ffa::10 update-source 3ffa::1
     exit-owner-node
```



```
6       owner-node-2
7        neighbor 3ffa::10 update-source 3ffa::2
8       exit-owner-node
9       owner-node-3
10       neighbor 3ffa::10 update-source 3ffa::3
11      exit-owner-node
12    no neighbor 3ffa::10 activate
13    address-family ipv6
14     redistribute kernel
15     neighbor 3ffa::10 activate
16    exit-address-family
17   !
18 <!--NeedCopy-->
```

Instalar rutas aprendidas de IPv6

El clúster de Citrix ADC puede utilizar rutas aprendidas por varios protocolos de redirección después de instalar las rutas en la tabla de redirecciones del clúster de Citrix ADC.

Para instalar rutas aprendidas de IPv6 en la tabla de redirecciones interno mediante la CLI:

En el símbolo del sistema, escriba:

- `ns route-install ipv6 bgp`
- `ns route-install ipv6 ospf`
- `ns route-install default`

> **Nota**
>
> - Si tiene que intercambiar rutas IPv4 en un vecino IPv6, debe quitar el comando `no neighbor 3ffa::10 active` VTYSH de la configuración anterior.
> - El comando `update-source` VTYSH debe utilizarse para cada nodo propietario para especificar la IP de origen IPv6 correcta mientras se conecta al par BGP como se indica en la configuración IPv4 de BGP.

Redirección en un clúster L3

La redirección de un clúster L3 solo funciona cuando se realizan las siguientes configuraciones en el dispositivo Citrix ADC.

- Habilite el redirección dinámica para una VLAN.

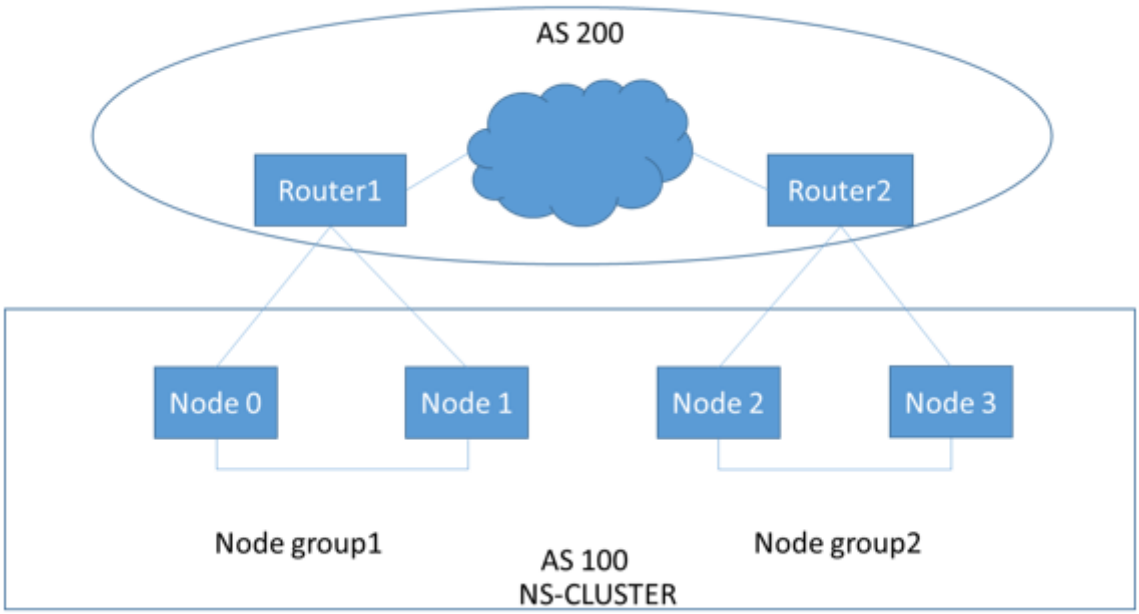

```
set vlan <id> -dynamicrouting enabled
<!--NeedCopy-->
```

- Para llegar a todos los nodos del clúster, los protocolos VIP, CLIP y Citrix ADC IP (NSIP) deben anunciarse mediante protocolos de redirección junto con el `set vlan` comando.

Caso de implementación para BGP en clúster L3

Considere un ejemplo en el que todos los nodos del clúster están agrupados en la red AS 100 y los enrutadores ascendentes están en un AS 200 diferente.

En la siguiente ilustración se muestra la implementación de AS 100 y AS 200 en una configuración de clúster.



En esta implementación, CLIP anuncia CCO a los routers ascendentes. Algunos nodos de clúster descartan el tráfico anunciado, ya que se detecta un bucle AS.

Para resolver el problema, configure el siguiente comando en modo de enrutador VTYSH BGP para cada vecino.

En el símbolo del sistema VTYSH, escriba:

```
neighbor <peer_ip> allowas-in 1
```

Como práctica recomendada, Citrix recomienda configurar cualquiera de las siguientes opciones:

- Configure los mapas de ruta para aprender solo las redes deseadas, como; ruta predeterminada, Citrix ADC IP (NSIP) y subredes NSIP en los nodos del clúster.

- Configure las rutas ascendentes para anunciar solo las redes deseadas como, por ejemplo, CLIP y Citrix ADC IP (NSIP) en el clúster.

Direccionamiento IP para un clúster

August 20, 2021

Además de los tipos estándar de direcciones IP propiedad de Citrix ADC, Citrix ADC NSIP, IP virtual (VIP) e IP de subred (SNIP), un dispositivo Citrix ADC en clúster puede tener una dirección IP de administración de clústeres (CLIP). También puede tener direcciones IP rayadas y manchadas.

- **Dirección CLIP.** Dirección IP propiedad del nodo coordinador de clúster (CCO). La dirección CLIP puede flotar entre diferentes nodos en una configuración de clúster. Si el CLIP se mueve a un nodo diferente del clúster, ese nodo se convierte en el CCO. El CCO es el dispositivo Citrix ADC responsable de las tareas de administración en el clúster. Un administrador de red utiliza la dirección CLIP para conectarse al clúster y realizar tareas de configuración y administración, como el acceso a la GUI unificada, la generación de informes, el seguimiento del flujo de paquetes y la recopilación de registros. Puede agregar varias direcciones CLIP en un clúster en la misma red o en diferentes redes. Solo las configuraciones realizadas en el CCO a través de la dirección IP del clúster se propagan a otros nodos del clúster.
- **Dirección IP rayada**. Una dirección IP lógica disponible en todos los nodos del clúster, puede ser una dirección VIP o SNIP.
- **Dirección IP detectada**. Una IP lógica (preferiblemente una dirección SNIP) solo está disponible en un nodo. Una dirección IP detectada solo tiene visibilidad en ese nodo. Para minimizar la sobrecarga de la dirección del tráfico, Citrix recomienda utilizar una dirección de SNIP detectado para la comunicación de back-end con el servidor.

En la tabla siguiente se proporcionan los detalles de las configuraciones.

Dirección IP	NSIP	VIP	SNIP
Manchado	Sí	Sí	Sí
Rayas	No	Sí	Sí

Por ejemplo, en un grupo de clústeres de cuatro nodos, debe configurar cada nodo con una dirección SNIP detectada. Para obtener más información sobre cómo configurar una configuración IP detectada, consulte Configuraciones rayadas, parcialmente rayadas y detectadas.

Puede definir una dirección SNIP para que esté activa en un solo nodo o activa en todos los nodos.

Si la dirección IP virtual y la dirección IP de la subred solo están disponibles en un nodo específico, es de configuración detectado. La configuración se define como seccionado si la dirección IP de la subred y la dirección IP del servidor virtual están disponibles en todos los nodos. Las direcciones SNIP detectados ayudan a reducir el tráfico de la dirección y el plano posterior.

Prácticas recomendadas para enlaces VLAN y configuración de rutas al unir un nodo al clúster

Enlaces IP de VLAN

Cuando vincula una VLAN con la dirección IP detectado, el clúster Citrix ADC debe configurarse con las direcciones IP detectados en la misma subred en todos los nodos. Por ejemplo, en un clúster de dos nodos con el nodo 0 y el nodo 1, puede tener la siguiente configuración:

```
1 add ns ip 192.254.101.101 255.255.255.0 -vServer DISABLED -
     dynamicRouting ENABLED -ownerNode 1
2 add ns ip 192.254.101.102 255.255.255.0 -vServer DISABLED -
     dynamicRouting ENABLED -ownerNode 0
3 add vlan 100
4 bind vlan 100 -IPAddress 192.254.101.101 255.255.255.0
5 <!--NeedCopy-->
```

Configuración de redirección

Cuando se requiere configuración de redirección con la dirección IP detectada como puerta de enlace predeterminada, el clúster ADC debe configurarse con las direcciones IP detectados en la misma subred en todos los nodos. Por ejemplo, en un clúster de dos nodos con el nodo 0 y el nodo 1, puede tener la siguiente configuración:

```
1 add ns ip 192.254.101.101 255.255.255.0 -vServer DISABLED -
     dynamicRouting ENABLED -ownerNode 1
2 add ns ip 192.254.101.102 255.255.255.0 -vServer DISABLED -
     dynamicRouting ENABLED -ownerNode 0
3
4 add route 192.254.102.0 255.255.255.0 192.254.101.103
5 <!--NeedCopy-->
```


> **Nota**
>
> En una configuración de clúster L3, solo se admite la configuración de SNIP detectado.

Configuración de clústeres de capa 3

August 20, 2021

Descripción del clúster de L3

La demanda de ampliar la implementación de alta disponibilidad y aumentar la escalabilidad del tráfico del cliente a través de diferentes redes guiada para establecer el clúster L3. El clúster L3 le permite agrupar dispositivos Citrix ADC en subredes individuales (clúster L2).

El clúster L3 también se conoce como "clúster en modo de configuración de red independiente (INC)". En la implementación de clúster de L3, los nodos de clúster de la misma red se agrupan para formar un grupo de nodos. El clúster L3 utiliza la tunelización GRE para dirigir los paquetes a través de las redes. Los mensajes de latido de los clústeres L3 se enrutan.

Este documento incluye los siguientes detalles:

- Arquitectura
- Ejemplo

Arquitectura

La arquitectura del clúster L3 consta de los siguientes componentes:

- **Grupo de nodos**. Los nodos de clúster de cada red (n1, n2) y (n3, n4), como se muestra en la siguiente ilustración, se agrupan para formar un grupo de nodos. Estos grupos de nodos terminan en el conmutador de capa 3 a ambos lados de la red.
  - El clúster se comunica con el cliente a través de las conexiones físicas entre el nodo del clúster y el dispositivo de conexión del lado del cliente. La agrupación lógica de estas conexiones físicas se denomina plano de datos del cliente.
  - El clúster se comunica con el servidor a través de las conexiones físicas entre el nodo del clúster y el dispositivo de conexión del lado del servidor. La agrupación lógica de estas conexiones físicas se denomina plano de datos del servidor.
- **Interruptor de backplane.** Los nodos del clúster dentro de la misma red se comunican entre sí mediante el backplane del clúster. El backplane es un conjunto de interfaces en las que una interfaz de cada nodo está conectada a un conmutador común, que se denomina conmutador de backplane del clúster.

- **Túnel GRE.** Los paquetes entre nodos de un clúster L3 se intercambian a través de un túnel GRE sin cifrar que utiliza las direcciones NSIP de los nodos de origen y destino para la redirección. El mecanismo de dirección cambia para los nodos pertenecientes a la red diferente. Los paquetes se dirigen a través de un túnel GRE hasta el nodo de la otra subred, en lugar de volver a escribir el MAC.

Ejemplo

Considere un ejemplo de una implementación de clúster L3 que consta de lo siguiente:

- Tres nodos de dispositivos Citrix ADC (n1, n2 y n3) se agrupan en Nodegroup1.
- Del mismo modo, los nodos n4 y n5 se agrupan en Nodegroup2. En la tercera red, hay dos grupos de nodos. Nodegroup3 incluye n6 y n7 y Nodegroup4 incluye n8 y n9.
- Los dispositivos Citrix ADC que pertenecen a la misma red se combinan para formar un grupo de nodos.

Puntos a tener en cuenta antes de configurar el clúster de L3

Tenga en cuenta los siguientes puntos antes de configurar el clúster de L3 en un dispositivo Citrix ADC:

- El backplane no es obligatorio al configurar subredes L3. Si no se especifica el plano posterior, el nodo no va al estado de error del plano posterior.

  > **Nota**
  >
  > Si tiene más de un nodo en la misma red L2, es obligatorio definir la interfaz del plano posterior. Si no se menciona la interfaz del plano posterior, los nodos van al estado de error del plano posterior.

- Las funciones de L2 y los SNIP de rayas no son compatibles con el clúster L3.
- La distribución de tráfico externo en el clúster L3 solo admite la ruta de acceso múltiple de igual coste (ECMP).
- Los errores ICMP y la fragmentación no se procesan cuando la dirección está desactivada en una implementación de clúster L3:
- Las entidades de red (`route`, `route6`, `pbr`, y `pbr6`) deben estar enlazadas al grupo de nodos de configuración.
- VLAN, RNAT y túnel IP no se pueden enlazar a un grupo de nodos de configuración.
- El grupo de nodos de configuración siempre debe tener la propiedad STRICT “YES.
- Los nodos de clúster no se deben agregar a un grupo de nodos de configuración mediante el comando “add cluster node”.

- El `add cluster instance -INC enabled` comando borra las entidades de red (route, route6, PBR, pb6, RNAT, IP tunnel, ip6tunnel).
- El `clear config extended+` comando no borra las entidades (route, route6, PBR, pb6, RNAT, IP tunnel, ip6tunnel) en un clúster L3.

Configuración del clúster L3

En una configuración de clúster L3, el comando cluster tiene diferentes atributos para configurar que se basan en nodos y grupos de nodos. La configuración del clúster L3 también incluye un perfil IPv6 aparte de los perfiles IPv4.

La configuración de un clúster de L3 en un dispositivo Citrix ADC consta de las siguientes tareas:

- Crear una instancia de clúster
- Crear un grupo de nodos en clúster L3
- Agregar un dispositivo Citrix ADC al clúster y grupo con grupo de nodos
- Agregar dirección IP del clúster al nodo
- Habilitar la instancia del clúster
- Guardar la configuración
- Agregar un nodo a un grupo de nodos existente
- Crear un grupo de nodos en clúster L3
- Agrupar nuevos nodos al grupo de nodos recién creado
- Unir el nodo al clúster

Configurar lo siguiente mediante la CLI

- **Para crear una instancia de clúster**

  ```
  add cluster instance <clid> -inc (<ENABLED|DISABLED>)[-processLocal <
  ENABLED | DISABLED]
  ```

- **Para crear un grupo de nodos en el clúster L3**

  ```
  add cluster nodegroup <name>
  ```

- **Para agregar un dispositivo Citrix ADC al clúster y asociarlo con nodegroup**

  ```
  add cluster node <nodeid> <nodeip> -backplane <interface_name> node
  group <ng>
  ```

- **Para agregar la dirección IP del clúster en este nodo**

  ```
  add ns ip <IPAddress> <netmask> -type clip
  ```

- **Habilitar la instancia del clúster**

  ```
  enable cluster instance <clId>
  ```


- **Guardar la configuración**

  ```
  save ns config
  ```

- **Reinicie el dispositivo en caliente**

  ```
  reboot -warm
  ```

- **Para agregar un nuevo nodo a un grupo de nodos existente**

  ```
  add cluster node <nodeid> <nodeip> -nodegroup <ng>
  ```

- **Para crear un nuevo grupo de nodos en el clúster L3**

  ```
  add cluster nodegroup <ng>
  ```

- **Para agrupar nuevos nodos en el grupo de nodos recién creado**

  ```
  add cluster node <nodeid> <nodeip> -nodegroup <ng>
  ```

- **Para unir el nodo al clúster**

```
1     join cluster  - clip <ip_addr> -password <password>
2
3     add cluster instance 1  - inc ENABLED  - processLocal  ENABLED
4
5        Done
6 <!--NeedCopy-->
```

> **Nota**
>
> El parámetro “inc” debe estar ENABLED para un clúster L3.

```
1     add cluster nodegroup ng1
2
3        Done
4
5     > add cluster node 0 1.1.1.1  - state ACTIVE -backplane 0/1/1  -
          nodegroup ng1
6
7        Done
8
9     > add ns ip 1.1.1.100 255.255.255.255  - type clip
10
11       Done
12
13    > enable cluster instance 1
```



```
14
15        Done
16
17     > save ns config
18
19        Done
20
21     > add cluster node 1 1.1.1.2  -state ACTIVE  -nodegroup ng1
22
23        Done
24
25     > add cluster nodegroup ng2
26
27        Done
28
29     > add cluster node 4 2.2.2.1  -state ACTIVE  -nodegroup ng2
30
31        Done
32
33     > add cluster node 5 2.2.2.2  -state ACTIVE  -nodegroup ng2
34
35        Done
36
37     > join cluster -clip 1.1.1.100 -password nsroot
38 <!--NeedCopy-->
```

Publicidad de la dirección IP del clúster de un clúster de L3

Configure la dirección IP del clúster que se anunciará en el enrutador ascendente para que la configuración del clúster sea accesible desde cualquier subred.Los protocolos de redirección dinámica configurados en un nodo anuncian la dirección IP del clúster como una ruta del núcleo.

La publicidad de la dirección IP del clúster consta de las siguientes tareas:

- **Habilite la opción de ruta de host de la dirección IP del clúster**.La opción de ruta host envía la dirección IP del clúster a una tabla de redirección ZeBos para la redistribución de la ruta del kernel a través de protocolos de redirección dinámica.
- **Configuración de un protocolo de redirección dinámica en un nodo**.Un protocolo de redirección dinámica anuncia la dirección IP del clúster en el enrutador ascendente. Para obtener más información sobre la configuración de un protocolo de redirección dinámica, consulteConfiguración de rutas dinámicas.

Para habilitar la opción de ruta de host de la dirección IP del clúster mediante la CLI

En el símbolo del sistema, escriba:

```
-  add nsip <IPAddress> <netmask> -hostRoute ENABLED

-  show nsip <IPAddress>

    > add ns ip 10.102.29.60 255.255.255.255 -hostRoute ENABLED

       Done
<!--NeedCopy-->
```

Configuraciones manchadas y parcialmente rayadas en clúster L3

Las configuraciones manchadas y parcialmente divisadas en el clúster L3 difieren ligeramente del clúster L2. La configuración puede diferir de un nodo a otro, ya que los nodos residen en diferentes subredes. Las configuraciones de red pueden ser específicas del nodo en el clúster L3, por lo tanto, debe configurar las configuraciones manchadas o parcialmente divisadas en función de los parámetros mencionados a partir de los parámetros mencionados a partir de los siguientes parámetros.

Para configurar configuraciones divisadas parcialmente divisadas en un dispositivo Citrix ADC a través del clúster L3, realice las siguientes tareas:

- Agregar un grupo de propietarios de clúster a una tabla de redirección estática IPv4
- Agregar un grupo de propietarios de clúster a una tabla de redirección estática IPv6
- Agregar un grupo de propietarios de clústeres a una redirección basada en directivas (PBR) IPv4
- Agregar un grupo de propietarios de clúster a un PBR IPv6
- Agregar una VLAN
- Enlazar una VLAN a un grupo de propietarios específico del grupo de nodos de clúster

Configurar lo siguiente mediante la CLI

- **Para agregar un grupo propietario de clúster a una tabla de ruta estática IPv4 del dispositivo Citrix ADC**

  ```
  add route <network> <netmask> <gateway> -owner group <ng>
  ```

- **Para agregar un grupo propietario de clúster a una tabla de redirección estática IPv6 del dispositivo Citrix ADC**

  ```
  add route6 <network> -owner group <ng>
  ```


- **Para agregar un grupo propietario de clústeres a un PBR IPv4**

  ```
  add pbr <name> <action> -owner group <ng>
  ```

- **Para agregar un grupo propietario de clústeres a un PBR IPv6**

  ```
  add pbr6 <name> <action> -owner group <ng>
  ```

- **Para agregar una VLAN**

  ```
  add vlan <id>
  ```

- **Para enlazar una VLAN a un grupo de propietarios específico del grupo de nodos de clúster**

  ```
  bind vlan <id> -ifnum - [IPAddress <ip_addr | ipv6_addr> [-owner group
  <ng>]
  ```

  Los siguientes comandos son ejemplos de configuraciones manchadas y parcialmente divididas que se pueden configurar mediante la CLI.

```
    > add route 10.102.29.0 255.255.255.0 10.102.29.2  - ownergroup ng2

        Done

    > add route6 fe80::9404:60ff:fedd:a464/64  - ownergroup ng1

        Done

    > add pbr pbr1 allow  - ownergroup ng1

        Done

    > add pbr6 pbr2 allow  - ownergroup ng2

        Done

    > add vlan 2

        Done

    > bind vlan 2  - ifnum 1/2  - [IPAddress 10.102.29.80 | fe80::9404:60
       ff:fedd:a464/64-ownergroup ng1

        Done
<!--NeedCopy-->
```


Configurar grupo de nodos

En un clúster L3, para replicar el mismo conjunto de configuraciones en más de un grupo de nodos, se utilizan los siguientes comandos:

Configurar lo siguiente mediante la CLU

- **Para agregar una ruta estática IPv4 a la tabla de redirecciones del dispositivo Citrix ADC**

  ```
  add route <network> <netmask> <gateway> -ownerGroup <ng>
  ```

Configuración de ejemplo:

```
1 add route 0 0 10.102.53.1 - ownerGroup ng1
2
3 add route 0 0 10.102.53.1 - ownerGroup ng2
4 <!--NeedCopy-->
```

Defina un nuevo grupo de nodos 'all' para admitir la configuración anterior y tiene que configurar los siguientes comandos:

Configurar lo siguiente mediante la CLI

- **Para agregar un nuevo grupo de nodos al clúster con un parámetro estricto**

  ```
  add cluster node group <name> -strict <YES | NO>
  ```

- **Para enlazar un nodo de clúster o una entidad al grupo de nodos dado**

  ```
  bind cluster nodegroup <name> -node <nodeid>
  ```

- **Para agregar ruta estática IPv4 a todos los ownergroup**

  ```
  add route <network> <netmask> <gateway> -ownerGroup <ng>
  ```

Configuración de ejemplo:

```
1 add cluster nodegroup all - strict YES
2
3 bind cluster nodegroup all - node 1
4
5 bind cluster nodegroup all - node 2
6
7 add route 0 0 10.102.53.1 - ownerGroup all
8 <!--NeedCopy-->
```


Distribución del tráfico en un clúster L3

En una configuración de clúster, las redes externas ven la colección de dispositivos Citrix ADC como una sola entidad. Por lo tanto, el clúster debe seleccionar un único nodo que debe recibir el tráfico. En el clúster de L3, esta selección se realiza mediante el ECMP. El nodo seleccionado se denomina receptor de flujo.

> **Nota**
>
> Para un clúster L3 (nodos en diferentes redes), solo se puede utilizar la distribución del tráfico ECMP.

El receptor de flujo obtiene el tráfico y, a continuación, mediante la lógica de clúster interna, determina el nodo que debe procesar el tráfico. Este nodo se denomina procesador de flujo. El receptor de flujo dirige el tráfico hacia el procesador de flujo sobre el plano posterior si el receptor de flujo y el procesador de flujo están en la misma red. El tráfico se dirige a través del túnel si el receptor de flujo y el procesador de flujo están en redes diferentes.

> **Nota**
>
> - El receptor de flujo y el procesador de flujo deben ser nodos capaces de servir el tráfico.
> - A partir de NetScaler 11, puede desactivar la dirección en el backplane del clúster. Para obtener más información, consulte Desactivación de la dirección en el plano posterior del clúster.

La ilustración anterior muestra una solicitud de cliente que fluye a través del clúster. El cliente envía una solicitud a una dirección IP virtual (VIP). Un mecanismo de distribución de tráfico configurado en el plano de datos del cliente selecciona uno de los nodos del clúster como receptor de flujo. El receptor de flujo recibe el tráfico, determina el nodo que debe procesar el tráfico y dirige la solicitud a ese nodo (a menos que el receptor de flujo se seleccione a sí mismo como el procesador de flujo). Si el procesador de flujo y el receptor de flujo se encuentran en el mismo grupo de nodos, el paquete se distribuye sobre el plano posterior. Y si el procesador de flujo y el receptor de flujo están en diferentes grupos de nodos, el paquete se dirige a través del túnel por la ruta enrutada.

El procesador de flujo establece una conexión con el servidor. El servidor procesa la solicitud y envía la respuesta a la dirección IP de subred (SNIP) que envió la solicitud al servidor. Dado que en el clúster L3 el SNIP siempre es un SNIP detectado, el nodo que posee la dirección SNIP recibe la respuesta del servidor.

Configurar un clúster de Citrix ADC

August 20, 2021

Los dispositivos Citrix ADC que desea agregar al clúster deben cumplir los criterios especificados en Requisitos previos para los nodos de clúster. Antes de configurar realmente un clúster, debe tener en cuenta los conceptos básicos del clúster. Para obtener información, consulte Descripción general del clúster.

La formación de un clúster requiere que configure la comunicación entre nodos, cree el clúster (agregando el primer dispositivo Citrix ADC) y, a continuación, agregue los demás nodos del clúster. Cada uno de estos pasos se explica con detalles relevantes en temas posteriores.

> **Nota**
>
> Aunque hay algunas diferencias en la configuración de un clúster L2 y L3, también hay muchas similitudes. En los temas siguientes se explica la configuración de ambos tipos de clúster al tiempo que se resaltan las configuraciones específicas de los clústeres L3.

Configuración de la comunicación entre nodos

August 20, 2021

Los nodos de una configuración de clúster se comunican entre sí mediante los siguientes mecanismos de comunicación entre nodos:

- Los nodos que están dentro de la red (misma subred) se comunican entre sí a través del backplane del clúster. El backplane debe configurarse explícitamente. Los siguientes son los pasos detallados.
- A través de las redes, la dirección de los paquetes se realiza a través de un túnel GRE y otras comunicaciones de nodo a nodo se enrutan a través de los nodos según sea necesario.

> **Importante**
>
> - Desde la versión 11.0 todas las compilaciones, un clúster puede incluir nodos de redes diferentes.
> - Desde la versión 13.0 compilación 58.3, la dirección GRE es compatible con las NIC de Fortville en un clúster L3.

Para configurar el backplane del clúster, haga lo siguiente para cada nodo

1. Identifique la interfaz de red que quiere utilizar para el plano anterior.
2. Conecte un cable Ethernet o de fibra óptica desde la interfaz de red seleccionada al conmutador de plano anterior del clúster.

Por ejemplo, para utilizar la interfaz 1/2 como interfaz de plano anterior para el nodo 4, conecte un cable desde la interfaz 1/2 del nodo 4 al conmutador de plano anterior.

Puntos importantes a tener en cuenta al configurar el backplane del clúster

- No utilice la interfaz de administración del dispositivo (0/x) como interfaz del backplane. En un clúster, la interfaz 0/1/x se lee como:

  0 -> ID de nodo 0
  1/x -> interfaz Citrix ADC

- No utilice las interfaces de plano posterior para los planos de datos del cliente o del servidor.
- Citrix recomienda utilizar el canal agregado de enlaces (LA) para el plano posterior del clúster.
- En un clúster de dos nodos, donde el plano posterior está conectado de forma consecutiva, el clúster está operacionalmente ABAJO en cualquiera de las siguientes condiciones:
  - Uno de los nodos se reinicia.
  - La interfaz de plano posterior de uno de los nodos está inhabilitada.

  Por lo tanto, Citrix recomienda que dedique un conmutador independiente para el plano posterior, de modo que el otro nodo del clúster y el tráfico no se vean afectados. No se puede escalar el clúster con un vínculo posterior a posterior. Es posible que encuentre un tiempo de inactividad en el entorno de producción al escalar los nodos del clúster.
- Las interfaces de backplane de todos los nodos de un clúster deben estar conectadas al mismo switch y enlazadas a la misma VLAN L2.
- Si tiene varios clústeres con el mismo Id. de instancia de clúster, asegúrese de que las interfaces de backplane de cada clúster están enlazadas a una VLAN diferente.
- La interfaz del plano anterior siempre se supervisa, independientemente de la configuración de supervisión de alta disponibilidad de dicha interfaz.
- El estado de la simulación MAC en las diferentes plataformas de virtualización puede afectar al mecanismo de dirección en el backplane del clúster. Por lo tanto, asegúrese de que el estado apropiado está configurado:
  - XenServer: Inhabilitar la suplantación de MAC
  - Hyper-V: Habilitar la suplantación de MAC
  - VMware ESX: Habilite la suplantación de MAC (también asegúrese de que “Transmits forjados” esté habilitado)
- La MTU del backplane del clúster se actualiza automáticamente. Sin embargo, si las tramas jumbo están configuradas en el clúster, la MTU del backplane del clúster debe configurarse explícitamente. El valor debe establecerse en 78 + X, donde X es la MTU máxima de los planos de datos de cliente y servidor. Por ejemplo, si la MTU de un plano de datos del servidor es 7500 y del plano de datos del cliente es 8922. La MTU de un plano posterior del clúster debe establecerse en 78 + 8922 = 9000. Para establecer esta MTU, utilice el siguiente comando:

  ```
  > set interface <backplane_interface> -mtu <value>
  ```


- La MTU para las interfaces del conmutador de plano posterior debe especificarse para que sea mayor o igual a 1.578 bytes. Es aplicable si el clúster tiene funciones como MBF, directivas L2, ACL, redirección en implementaciones CLAG y vPath.

Compatibilidad con túnel basado en UDP para clústeres L2 y L3

A partir de Citrix ADC versión 13.0 compilación 36.x, los clústeres de Citrix ADC L2 y L3 pueden dirigir el tráfico mediante túnel basado en UDP. Se define para las comunicaciones entre nodos de dos nodos de un clúster. Mediante el parámetro “modo túnel”, puede establecer el modo de túnel GRE o UDP desde el comando add and set cluster node.

En una implementación de clúster L3, los paquetes entre nodos Citrix ADC se intercambian a través de un túnel GRE sin cifrar que utiliza las direcciones NSIP de los nodos de origen y destino para la redirección. Cuando este intercambio se produce a través de Internet, en ausencia de un túnel IPSec, los NSIP se exponen en Internet y pueden dar lugar a problemas de seguridad.

> **Importante**
>
> Citrix recomienda a los clientes que establezcan su propia solución IPSec cuando utilicen un clúster L3.

La siguiente tabla le ayuda a clasificar el soporte del túnel según diferentes implementaciones.

Tipos de dirección	AWS	Microsoft Azure	En las instalaciones
MAC	No se admite	No se admite	Se admite
Túnel GRE	Se admite	No se admite	Se admite
Túnel UDP	Se admite	Compatible	Se admite

> **Importante**
>
> En un clúster L3, el modo de túnel se establece en GRE de forma predeterminada.

Configuración del túnel basado en UDP

Puede agregar un nodo de clúster estableciendo los parámetros de ID de nodo y mencionando el estado. Configure el plano posterior proporcionando el nombre de la interfaz y seleccione el modo de túnel que quiera (GRE o UDP).

Procedimientos CLI

Para habilitar el modo de túnel UDP mediante la CLI.

En el símbolo del sistema, escriba:

- `add cluster node <nodeId>@ [-state <state>] [-backplane <interface_name>] [-tunnelmode <tunnelmode>]`
- `set cluster node <nodeId>@ [-state <state>] [-tunnelmode <tunnelmode>]`

> **Nota**
>
> Los valores posibles para el modo de túnel son NONE, GRE, UDP.

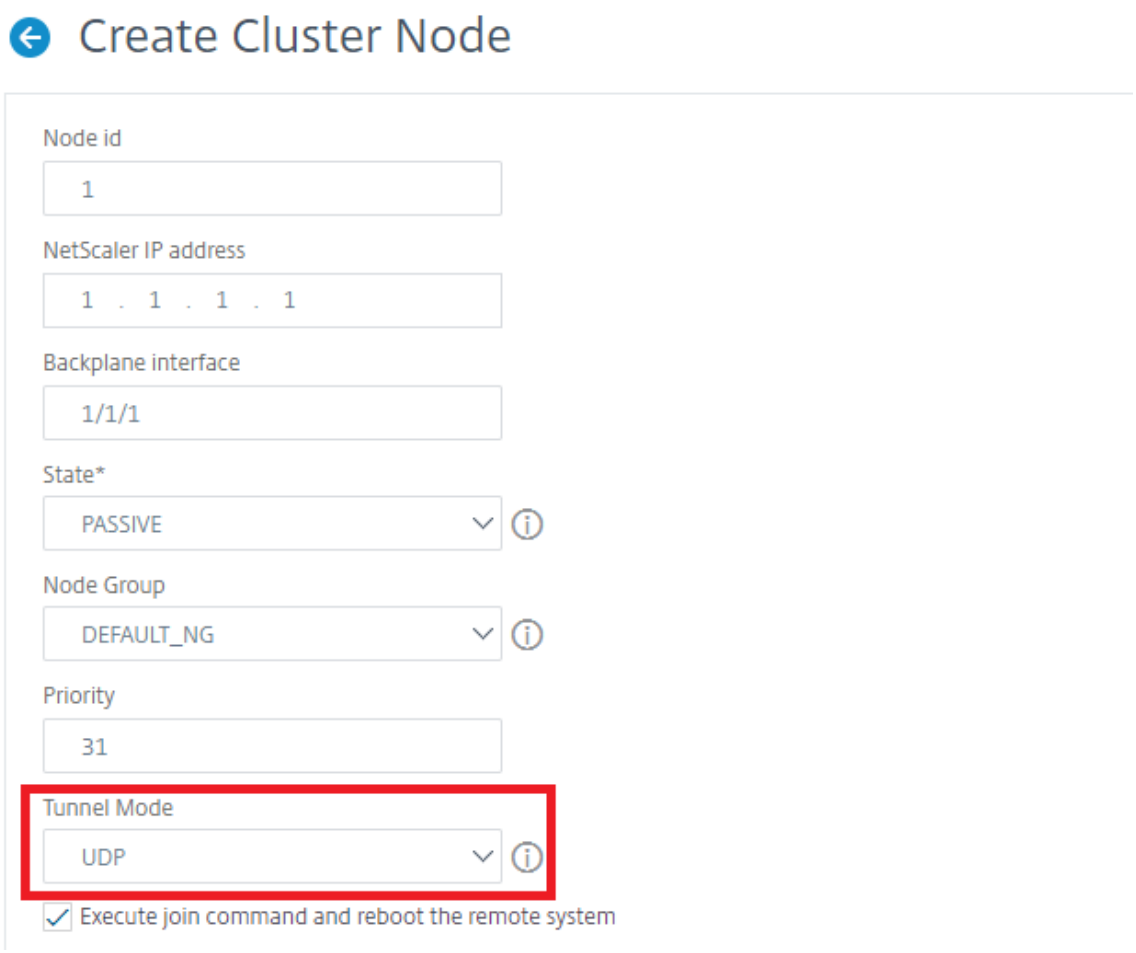
Ejemplo

- `add cluster node 1 -state ACTIVE -backplane 1/1/1 -tunnelmode UDP`
- `set cluster node 1 -state ACTIVE -tunnelmode UDP`

Procedimientos de GUI

Para habilitar el modo de túnel UDP mediante la GUI.

1. Vaya a **Sistema > Cluster > Nodos**.
2. En la página **Nodos de Cluster**, haga clic en **Agregar**.
3. En el **nodo Crear clúster**, establezca el parámetro **Modo de túnel** en UDP y haga clic en **Crear**.



4. Haga clic en **Cerrar**.

Crear un clúster de Citrix ADC

December 2, 2021

Para crear un clúster, comience por tomar uno de los dispositivos Citrix ADC que quiere agregar al clúster. En este nodo, debe crear la instancia de clúster y definir la dirección IP del clúster. Este nodo es el primer nodo de clúster y se denomina coordinador de configuración de clúster (CCO). Todas las configuraciones que se realizan en la dirección IP del clúster se almacenan en este nodo y, a continuación, se propagan a los demás nodos del clúster.

La responsabilidad del CCO en un clúster no se fija en un nodo específico. Puede cambiar con el tiempo según los siguientes factores:

- La prioridad del nodo. El nodo con la prioridad más alta (número de prioridad más bajo) se hace el CCO. Por lo tanto, si se agrega un nodo con un número de prioridad inferior al CCO existente,

el nuevo nodo asume el cargo como CCO.

- Si el CCO actual cae, el nodo con el siguiente número de prioridad más bajo asume el cargo de CCO. Si no se establece la prioridad o si hay varios nodos con el número de prioridad más bajo, el CCO se selecciona de uno de los nodos disponibles.

> **Nota:**
>
> Las configuraciones del dispositivo (incluidas las direcciones SNIP y las VLAN) se borran ejecutando implícitamente el comando `clear ns config extended`. Sin embargo, la VLAN y la NSVLAN predeterminadas no se borran del dispositivo. Por lo tanto, si quiere que la NSVLAN esté en el clúster, asegúrese de que se haya creado antes de que el dispositivo se agregue al clúster. Para un clúster L3 (nodos de clúster en diferentes redes), las configuraciones de red no se borran del dispositivo.
>
> **Importante:**
>
> El monitor HA (HAMON) en una configuración de clúster se usa para supervisar el estado de una interfaz en cada nodo. El parámetro HAMON debe estar habilitado en cada nodo para supervisar el estado de la interfaz. Si el estado operativo de la interfaz habilitada para HAMON deja de funcionar por cualquier motivo, el nodo del clúster respectivo se marca como no saludable (NO ACTIVA) y ese nodo no puede servir el tráfico.

Para crear un clúster mediante la interfaz de línea de comandos

1. Inicie sesión en un dispositivo (por ejemplo, un dispositivo con dirección NSIP 10.102.29.60) que quiera agregar al clúster.
2. Agregar una instancia de clúster.

```
add cluster instance <clId> -quorumType <NONE | MAJORITY> -inc <
    ENABLED | DISABLED> -backplanebasedview <ENABLED | DISABLED>
<!--NeedCopy-->
```

> **Nota:**
>
> - El identificador de instancia de clúster debe ser único dentro de una LAN.
> - El parámetro `-quorumType` debe establecerse en MAYORITARIO y no en NINGUNO en estos casos:
>   - Topologías que no tienen enlaces redundantes entre los nodos del clúster. Estas topologías podrían ser propensas a la partición de la red debido a un único punto de fallo.
>   - Durante cualquier operación de clúster, como la adición o eliminación de nodos.

- Para un clúster L3, asegúrese de que el parámetro `-inc` esté configurado en ENABLED. El parámetro `-inc` debe estar inhabilitado para un clúster L2.
- Cuando el parámetro `-backplanebasedview` está habilitado, la vista operativa (conjunto de nodos que atienden el tráfico) se decide en función de los latidos recibidos solo en la interfaz del plano posterior. De forma predeterminada, este parámetro está inhabilitado. Cuando este parámetro está inhabilitado, un nodo no depende de la recepción de latidos solo en el plano posterior.

3. [Solo para un clúster de L3] Cree un grupo de nodos. En el paso siguiente, el nodo de clúster recién agregado debe estar asociado a este grupo de nodos.

> **Nota:**
>
> Este grupo de nodos incluye todos o un subconjunto de los dispositivos Citrix ADC que pertenecen a la misma red.

```
add cluster nodegroup <name>
<!--NeedCopy-->
```

4. Agregue el dispositivo Citrix ADC al clúster.

```
add cluster node <nodeId> <IPAddress> -state <state> -backplane <
   interface_name> -nodegroup <name>
<!--NeedCopy-->
```

> **Nota:**
>
> Para un clúster L3:
>
> - El parámetro de grupo de nodos debe establecerse en el nombre del grupo de nodos que se crea.
> - El parámetro de plano posterior es obligatorio para los nodos que están asociados con un grupo de nodos que tiene más de un nodo, de modo que los nodos dentro de la red puedan comunicarse entre sí.

Ejemplo:

Agregar un nodo para un clúster L2 (todos los nodos del clúster están en la misma red).

```
  add cluster node 0 10.102.29.60 -state PASSIVE -backplane 0/1/1
  <!--NeedCopy-->
```


Agregar un nodo para un clúster L3 que incluye un único nodo de cada red. Aquí, no tienes que configurar el plano posterior.

```
1   add cluster node 0 10.102.29.60 -state PASSIVE -nodegroup ng1
2   <!--NeedCopy-->
```

Agregar un nodo para un clúster L3 que incluye varios nodos de cada red. Aquí, debe configurar el plano posterior para que los nodos dentro de una red puedan comunicarse entre sí.

```
1   add cluster node 0 10.102.29.60 -state PASSIVE -backplane 0/1/1
       -nodegroup ng1
2   <!--NeedCopy-->
```

5. Agregue la dirección IP del clúster (por ejemplo, 10.102.29.61) en este nodo.

```
1 add ns ip <IPAddress> <netmask> -type clip
2 <!--NeedCopy-->
```

Ejemplo

```
1 add ns ip 10.102.29.61 255.255.255.255 -type clip
2 <!--NeedCopy-->
```

6. Habilite la instancia del clúster.

```
1 enable cluster instance <clId>
2 <!--NeedCopy-->
```

7. Guarde la configuración.

```
1 save ns config
2 <!--NeedCopy-->
```

8. Reinicie el dispositivo en caliente.


```
reboot -warm
<!--NeedCopy-->
```

Compruebe las configuraciones del clúster mediante el comando show cluster instance. Compruebe que el resultado del comando muestre la dirección NSIP del dispositivo como un nodo del clúster.

9. Después de que el nodo esté UP, inicie sesión en el CLIP y cambie las credenciales RPC tanto para la dirección IP del clúster como para la dirección IP del nodo. Para obtener más información sobre cómo cambiar la contraseña de un nodo RPC, consulte Cambiar una contraseña de nodo RPC.

Para crear un clúster mediante la GUI

1. Inicie sesión en un dispositivo (por ejemplo, un dispositivo con la dirección NSIP 10.102.29.60) que pretenda agregar al clúster.
2. Vaya a **Sistema > Clúster.**
3. En el panel de detalles, haga clic en el enlace **Administrar clúster**.
4. En el cuadro de diálogo Configuración del clúster, defina los parámetros necesarios para crear un clúster. Para obtener una descripción de un parámetro, pase el cursor del ratón sobre el cuadro de texto correspondiente.
5. Haga clic en **Crear**.
6. En el cuadro de diálogo Configurar instancia de clúster, active la casilla de verificación Enable cluster instance.
7. En el panel Nodos de clúster, seleccione el nodo y haga clic en **Abrir.**
8. En el cuadro de diálogo Configurar nodo de clúster, defina el estado.
9. Haga clic en **Aceptar**y, a continuación, en **Guardar.**
10. Reinicie el dispositivo en caliente.
11. Después de que el nodo esté UP, inicie sesión en el CLIP y cambie las credenciales RPC tanto para la dirección IP del clúster como para la dirección IP del nodo. Para obtener más información sobre cómo cambiar la contraseña de un nodo RPC, consulte Cambiar una contraseña de nodo RPC.

Compatibilidad de modo estricto para el estado de sincronización del clúster

Ahora puede configurar un nodo de clúster para ver los errores al aplicar la configuración. Se introduce un nuevo parámetro, “SyncStatusStrictMode” en el comando add y set cluster instance para rastrear el estado de cada nodo de un clúster. De forma predeterminada, el parámetro `syncStatusStrictMode` está inhabilitado.

Para habilitar el modo estricto mediante la CLI

En el símbolo del sistema, escriba:

```
set cluster instance <clID> [-syncStatusStrictMode (ENABLED | DISABLED)
    ]
<!--NeedCopy-->
```

Ejemplo:

```
set cluster instance 1  - syncStatusStrictMode ENABLED
<!--NeedCopy-->
```

Para ver el estado del modo estricto mediante la CLI

```
    >show cluster instance
    1) Cluster ID: 1
        Dead Interval: 3 secs
        Hello Interval: 200 msecs
        Preemption: DISABLED
        Propagation: ENABLED
        Quorum Type: MAJORITY
        INC State: DISABLED
        Process Local: DISABLED
        Retain Connections: NO
        Heterogeneous: NO
        Backplane based view: DISABLED
        Cluster sync strict mode: ENABLED
        Cluster Status: ENABLED(admin), ENABLED(operational), UP

      WARNING(s):
        (1) - There are no spotted SNIPs configured on the cluster.
           Spotted SNIPs can help improve cluster performance

        Member Nodes:
        Node ID     Node IP      Health     Admin State  Operational
           State
        -------     -------      ------     -----------
           ------------------
    1)      1           192.0.2.20      UP         ACTIVE       ACTIVE(
       Configuration Coordinator)
```



```
23      2)      2           192.0.2.21      UP          ACTIVE      ACTIVE
24      3)      3           192.0.2.19*     UP          ACTIVE      ACTIVE
25  <!--NeedCopy-->
```

Para ver el motivo del error de sincronización de un nodo de clúster mediante la interfaz gráfica de usuario

1. Vaya a **Sistema > Clúster > Nodos**de clú
2. En la página **Nodos de clúster**, desplácese hasta el extremo derecho para ver los detalles del motivo del error de sincronización de los nodos del clúster.

Agregar un nodo al clúster

August 20, 2021

Puede escalar sin problemas el tamaño de un clúster para incluir un máximo de 32 nodos. Cuando se agrega un dispositivo Citrix ADC al clúster, se borran las configuraciones de ese dispositivo (ejecutando internamente el comando clear ns config -extended). Las direcciones SNIP, la configuración de **MTU** de la interfaz del plano posterior y todas las configuraciones de VLAN (excepto la VLAN y NSVLAN predeterminadas) también se borran del dispositivo.

A continuación, las configuraciones del clúster se sincronizan en este nodo. Puede haber una caída intermitente en el tráfico mientras la sincronización está en curso.

> **Importante**
>
> Antes de agregar un dispositivo Citrix ADC a un clúster:
>
> - Configure la interfaz del backplane para el nodo. Compruebe el tema anterior.
> - Compruebe si las licencias disponibles en el dispositivo coinciden con las disponibles en el coordinador de configuración. El dispositivo solo se agrega si las licencias coinciden.
> - Si quiere que la NSVLAN esté en el clúster, asegúrese de que la NSVLAN se haya creado en el dispositivo antes de agregarla al clúster.
> - Citrix recomienda agregar el nodo como nodo pasivo. A continuación, después de unir el nodo al clúster, complete la configuración específica del nodo desde la dirección IP del clúster. Ejecute el comando force cluster sync si el clúster solo ha detectado direcciones IP. Y que tiene enlace VLAN L3, o tiene rutas estáticas.
> - Cuando se agrega un dispositivo con un canal agregado de vínculos (LA) preconfigurado a un clúster, el canal LA continúa existiendo en el entorno del clúster. El canal LA cambia de nombre de LA/x a nodeId/LA/x, donde LA/x es el identificador del canal LA.

Para agregar un nodo al clúster mediante la CLI

> **Nota**
>
> Cuando agrega un nodo a una configuración de clúster, si el nodo tiene una ruta estática predeterminada, se agrega al nodo coordinador de clúster (CCO). Si esta ruta estática predeterminada apunta a una Gateway incorrecta, podría provocar un tiempo de inactividad de los servicios. Por lo tanto, verifique la ruta estática predeterminada del nuevo nodo, antes de agregarla a la configuración del clúster.

1. Inicie sesión en la dirección IP del clúster, en el símbolo del sistema, haga lo siguiente:
   - Agregue el dispositivo (por ejemplo, 10.102.29.70) al clúster.

   > **Nota**
   >
   > Para un clúster L3:

   ```
   - El parámetro de grupo de nodos debe establecerse en un
     grupo de nodos que tenga nodos de la misma red.
   ```

   - Si este nodo pertenece a la misma red que el primer nodo que se agregó, configure el grupo de nodos que se utilizó para ese nodo.
   - Si este nodo pertenece a una red diferente, cree un grupo de nodos y enlaque este nodo al grupo de nodos.
   - El parámetro de plano posterior es obligatorio para los nodos asociados a un grupo de nodos que tiene más de un nodo, de modo que los nodos de la red puedan comunicarse entre sí.

   ```
   add cluster node <nodeId> <IPAddress> -state <state> -backplane <
      interface_name> -nodegroup <name>

   Example:

   add cluster node 1 10.102.29.70 -state PASSIVE -backplane 1/1/1
   <!--NeedCopy-->
   ```

   - Guarde la configuración.

   ```
   save ns config
   <!--NeedCopy-->
   ```


2. Inicie sesión en el nodo recién agregado (por ejemplo, 10.102.29.70) y únase el nodo al clúster.

```
join cluster -clip <ip_addr> -password <password>

Example:

join cluster -clip 10.102.29.61 -password nsroot
<!--NeedCopy-->
```

3. Configure los siguientes comandos en el CLIP.

   - Vincular VLAN a una interfaz

   ```
   bind vlan <id> -ifnum <interface_name>
   <!--NeedCopy-->
   ```

   Ejemplo:

   ```
   bind vlan 1 -ifnum 2/1/2
   <!--NeedCopy-->
   ```

   - Agregar dirección IP detectado al nodo recién agregado

   ```
   add ns ip <IpAddress> <netmask> -ownerNode <positive_interger
       >
   <!--NeedCopy-->
   ```

   Ejemplo:

   ```
   add ns ip 97.131.0.3 255.0.0.0 -ownerNode 2
   <!--NeedCopy-->
   ```

   - Verificar VLAN en NSIP

   ```
   show vlan <id>
   <!--NeedCopy-->
   ```


Ejemplo:

```
show vlan 1
<!--NeedCopy-->
```

4. Realice las siguientes configuraciones:
   - Si el nodo se agrega a un clúster que solo tiene direcciones IP detectada, las configuraciones se sincronizan antes de que las direcciones IP detectada se asignen a ese nodo. En tales casos, los enlaces de VLAN L3 se pueden perder. Para evitar esta pérdida, agregue una IP seccionada o agregue los enlaces de VLAN L3.
   - Defina las configuraciones detectada necesarias.
   - Defina la MTU para la interfaz del backplane.
5. Guarde la configuración.

```
save ns config
<!--NeedCopy-->
```

6. Reinicie el dispositivo en caliente.

```
reboot -warm
<!--NeedCopy-->
```

7. Después de que el nodo esté UP y la sincronización sea correcta, cambie las credenciales RPC para el nodo desde la dirección IP del clúster. Para obtener más información sobre cómo cambiar la contraseña de un nodo RPC, consulte Cambiar una contraseña de nodo RPC.

```
set rpcNode <node-NSIP> -password <passwd>

Example:

set rpcNode 192.0.2.4 -password mypassword
<!--NeedCopy-->
```

8. Establezca el nodo del clúster en Activo.


```
set cluster node <nodeID> -state active.

Example:

set cluster node 1 -state active
<!--NeedCopy-->
```

Para agregar un nodo al clúster mediante la GUI

1. Inicie sesión en la dirección IP del clúster.
2. Vaya a **Sistema > Cluster > Nodos**.
3. En el panel de detalles, haga clic en **Agregar** para agregar el nuevo nodo (por ejemplo, 10.102.29.70).
4. En el cuadro de diálogo **Crear nodo de clúster**, configure el nuevo nodo. Para obtener una descripción de un parámetro, sitúe el cursor del ratón sobre el cuadro de texto correspondiente.
5. Haga clic en **Crear**. Cuando se le solicite realizar un reinicio en caliente, haga clic en **Sí.**
6. Después de que el nodo esté UP y la sincronización sea correcta, cambie las credenciales RPC para el nodo desde la dirección IP del clúster. Para obtener más información sobre cómo cambiar la contraseña de un nodo RPC, consulte Cambiar una contraseña de nodo RPC.
7. Vaya a **Sistema > Cluster > Nodos > Modificar**.
8. Modifique el estado a **ACTIVO** y confirme.

Para unir un nodo agregado previamente al clúster mediante la GUI

Si ha utilizado la CLI para agregar un nodo al clúster, pero no ha unido el nodo al clúster, puede utilizar el procedimiento siguiente.

> **Nota**
>
> Cuando un nodo se une al clúster, se hace cargo de su parte de tráfico del clúster y, por lo tanto, una conexión existente puede terminar.

1. Inicie sesión en el nodo que quiere unir al clúster (por ejemplo, 10.102.29.70).
2. Vaya a **Sistema > Clúster.**
3. En el panel de detalles, en Introducción, haga clic en el vínculo Unirse al clúster.
4. En el cuadro de diálogo Unirse al clúster existente, establezca la dirección IP del clúster y la `nsroot` contraseña del coordinador de configuración. Para obtener una descripción de un parámetro, sitúe el cursor del ratón sobre el cuadro de texto correspondiente.
5. Haga clic en **Aceptar.**

Visualización de los detalles de un clúster

August 20, 2021

Puede ver los detalles de la instancia del clúster y los nodos del clúster iniciando sesión en la dirección IP del clúster.

Para ver los detalles de una instancia de clúster mediante la CLI

Inicie sesión en la dirección IP del clúster y, en el símbolo del sistema, escriba:

```
show cluster instance <clId>
```

> **Nota**
>
> Cuando se ejecuta el comando anterior desde la dirección NSIP del nodo que no es CCO, el comando muestra el estado del clúster en este nodo.

Para ver los detalles de un nodo de clúster mediante la CLI

Inicie sesión en la dirección IP del clúster y, en el símbolo del sistema, escriba:

```
show cluster node <nodeId>
```

Para ver los detalles de una instancia de clúster mediante la GUI

1. Inicie sesión en la dirección IP del clúster.
2. Vaya a **Sistema > Clúster.**
3. En el panel de detalles, en **Introducción**, haga clic en el vínculo **Administrar clúster**para ver los detalles del clúster.

Para ver los detalles de un nodo de clúster mediante la GUI

1. Inicie sesión en la dirección IP del clúster.
2. Vaya a **Sistema > Clúster > Nodos.**
3. En el panel de detalles, haga clic en el nodo para el que quiere ver los detalles.

Distribuir tráfico entre nodos de clúster

January 12, 2021

Después de crear el clúster de Citrix ADC y realizar las configuraciones necesarias, debe implementar Equal Cost Múltiple Path (ECMP) o Cluster Link Aggregation (LA) en el plano de datos del cliente (para tráfico de cliente) o en el plano de datos del servidor (para tráfico de servidor). Estos mecanismos distribuyen el tráfico externo entre los nodos del clúster.

Dirección del backplane basada en directivas

La dirección del backplane basada en directivas (PBS) es un mecanismo en la implementación del clúster, que dirige el tráfico a través de los nodos del clúster basándose en el método hash definido para el flujo. El flujo se define mediante una combinación de parámetros L2 y L3 similares a la lista de control de acceso (ACL).

El PBS admite tráfico IPv4 e IPv6. En el caso de las implementaciones IPv6, la dirección admite una opción adicional `[dfdprefix <positive_integer>]`. Proporciona la flexibilidad de elegir el mismo procesador de flujo para el mismo prefijo IP. La opción de prefijo solo se admite para los métodos hash IP de origen o IP de destino.

> **Nota**
>
> Si el mecanismo PBS no se utiliza para dirigir el tráfico, el tráfico se dirige a través del método predeterminado.

Para configurar los nuevos atributos de ACL, en la CLI, escriba los siguientes comandos:

Comandos CLI para IPv4

- `add ns acl <aclname> <aclaction> [-type (classic | dfd)] [-dfdhash <dfdhash>]`
- `set ns acl <aclname> <aclaction> [-dfdhash <dfdhash>`
- `show ns acl [<aclname>][-type (classic | DFD)]`
- `apply ns acls [-type (classic | DFD)]`
- `clear ns acls [-type (classic | DFD)]`
- `renumber ns acls [-type (classic | DFD)]`

Comandos CLI para IPv6

- `add ns acl6 <acl6name> <acl6action> [-type (classic | dfd)][-dfdhash <dfdhash>][-dfdprefix <positive_interger>]`

- `set ns acl6 <acl6name> <acl6action> [-dfdhash <dfdhash>][-dfdprefix <positive_interger>]`
- `show ns acl6 [<acl6name>][-type (classic | DFD)]`
- `apply ns acls6 [-type (classic | DFD)]`
- `clear ns acls6 [-type (classic | DFD)]`
- `renumber ns acls6 [-type (classic | DFD)]`

Los siguientes son los diferentes tipos de métodos hash que puede especificar para dirigir el paquete al procesador de flujo:

- SIP-SPORT-DIP-DPORT
- SIP
- DIP
- SIP-DIP
- SIP-SPORT

Limitaciones

1. La distribución del flujo de tráfico entre los nodos del clúster no está garantizada, ya que las reglas configuradas por el administrador deciden el procesador de flujo.
2. No se admite el modo L2.
3. Los grupos de nodos y los SNIP sectados no son compatibles, ya que no hay casos de implementación.
4. No se admite MPTCP.
5. Solo admite tráfico TCP, UDP e ICMP.
6. No se admite el modo de clúster sobre L3.
7. No se admite el proceso local a nivel de servicio.

Uso de la ruta de acceso múltiple de igual coste (ECMP)

August 20, 2021

Mediante el mecanismo ECMP (Equal Cost Múltiple Path) en una implementación de clúster, los nodos de clúster activos anuncian las direcciones IP del servidor virtual. El nodo del clúster que recibe el tráfico anunciado dirige el tráfico al nodo que debe procesar el tráfico. Puede haber una dirección redundante en servidores virtuales manchados y parcialmente seccionados. Por lo tanto, a partir de NetScaler 11, las direcciones IP del servidor virtual detectada y parcialmente rayada anuncian los nodos propietarios, lo que reduce la dirección redundante.

Debe tener un conocimiento detallado de los protocolos de redirección para usar ECMP. Para obtener más información, consulte Configuración de rutas dinámicas. Para obtener más información sobre la

redirección en un clúster, consulte Redirección en un clúster.

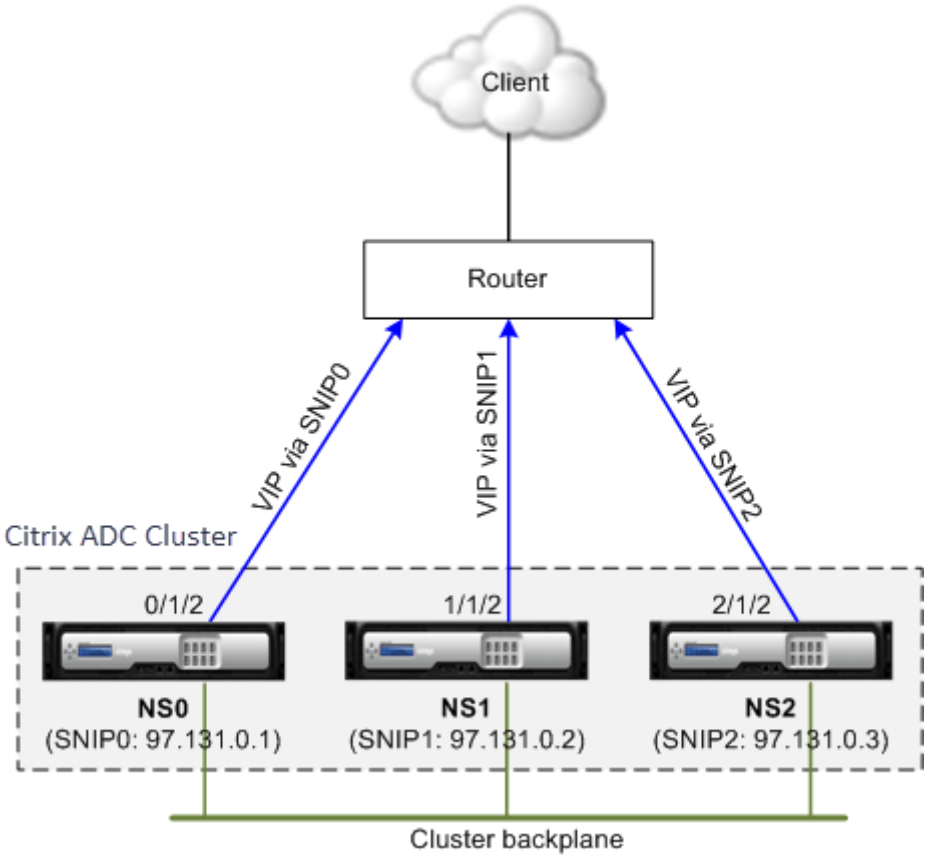
Para utilizar ECMP, primero debe realizar lo siguiente:

- Habilite el protocolo de redirección requerido (OSPF, RIP, BGP o ISIS) en la dirección IP del clúster.
- Enlazar las interfaces y la dirección IP detectada (con redirección dinámica habilitado) a una VLAN.
- Configure el protocolo de redirección seleccionado y redistribuya las rutas del kernel en los ZeBO mediante el shell VTYSH.

Realice configuraciones similares en la dirección IP del clúster y en el dispositivo de conexión externo.

> **Nota**
>
> - Asegúrese de que las licencias del clúster admiten redirección dinámica; de lo contrario, ECMP no funciona.
> - ECMP no es compatible con servidores virtuales comodín ya que RHI necesita una dirección VIP para anunciarse en un enrutador y servidores virtuales comodín. Como no tienen direcciones VIP asociadas.

Ilustración 1. Topología ECMP



Cuando se utiliza el mecanismo ECMP para la distribución de tráfico en una implementación de clúster, los nodos de clúster activos anuncian las direcciones IP del servidor virtual en el enrutador ascendente. El router ECMP puede alcanzar la dirección VIP a través de SNIP0, SNIP1 o SNIP2. El flujo de tráfico de la Ilustración 1 se describe de la siguiente manera:

1. El cliente envía una solicitud al VIP alojado en el clúster.
2. El router ascendente, basado en las rutas aprendidas del VIP, reenvía el paquete a cualquiera de los nodos. Digamos que NS1. El nodo NS1 es el receptor de flujo.
3. El receptor de flujo (NS1) determina el nodo que debe procesar el tráfico, que se denomina procesador de flujo. Por ejemplo, el nodo NS2 es el procesador de flujo.
4. El receptor de flujo (NS1) con SNIP1 (97.131.0.2) dirige la solicitud al procesador de flujo (NS2) con SNIP2 (97.131.0.3).
5. El procesador de flujo (NS2) establece una conexión con el servidor.
6. El servidor procesa la solicitud y envía la respuesta a la dirección SNIP que envió la solicitud al servidor.

Notas:

- Solo los nodos ACTIVO anuncian rutas VIP.
- Los nodos INACTIVO no anuncian rutas VIP.
- Todos los nodos ACTIVOS anuncian VIP rayadas.
- Solo los nodos de propietario ACTIVO anuncian VIPs detectados o parcialmente rayados.

Para configurar ECMP en el clúster mediante la interfaz de línea de comandos

1. Inicie sesión en la dirección IP del clúster.
2. Habilite el protocolo de redirección.

```
enable ns feature <feature>
```

Ejemplo: Para habilitar el protocolo de redirección OSPF.

```
enable ns feature ospf
```

3. Agregue una VLAN.

```
add vlan <id>
```

Ejemplo


```
add vlan 97
```

4. Enlace las interfaces de los nodos del clúster a la VLAN.

```
bind vlan <id> -ifnum <interface_name>
```

Ejemplo

```
bind vlan 97 -ifnum 0/1/2 1/1/2 2/1/2
```

5. Agregue una dirección SNIP detectada para cada nodo y habilite el redirección dinámica en él.

```
add ns ip <SNIP> <netmask> -ownerNode <positive_integer> -
    dynamicRouting ENABLED
```

Ejemplo

```
add ns ip 97.131.0.1 255.0.0.0 -ownerNode 0 -dynamicRouting
    ENABLED -type SNIP
add ns ip 97.131.0.2 255.0.0.0 -ownerNode 1 -dynamicRouting
    ENABLED -type SNIP
add ns ip 97.131.0.3 255.0.0.0 -ownerNode 2 -dynamicRouting
    ENABLED -type SNIP
```

6. Enlazar una de las direcciones SNIP detectada a la VLAN. Cuando vincula una dirección SNIP detectada a una VLAN, todas las demás direcciones SNIP detectada definidas en el clúster de esa subred se vinculan automáticamente a la VLAN.

```
bind vlan <id> -IPAddress <SNIP> <netmask>
```

Ejemplo

```
bind vlan 97 -ipAddress 97.131.0.1 255.0.0.0
```


> **Nota**
>
> Puede usar direcciones NSIP de los nodos del clúster en lugar de agregar direcciones SNIP. Si es así, no tiene que realizar los pasos 3 a 6.

7. Configure el protocolo de redirección en ZEBO mediante el shell de VTYSH.

   Ejemplo:

   Para configurar un protocolo de redirección OSPF en los identificadores de nodo 0, 1 y 2.

```
vtysh
! interface vlan97 !
 router ospf   owner-node 0
ospf router-id 97.131.0.1   exit-owner-node
owner-node 1    ospf router-id 97.131.0.2
exit-owner-node
owner-node 2
ospf router-id 97.131.0.3   exit-owner-node   redistribute kernel
   network 97.0.0.0/8 area 0  !
```

   > **Nota**
   >
   > Para las direcciones VIP que se anunciarán, la configuración RHI se realiza mediante el parámetro vServerRhilevel de la siguiente manera:

```
add ns ip <IPAddress> <netmask> -type VIP -vserverRHILevel <
   vserverRHILevel>
```

   Para la configuración RHI específica de OSPF, hay más configuraciones que se pueden hacer de la siguiente manera:

```
add ns ip <IPAddress> <netmask> -type VIP -ospfLSAType ( TYPE1 |
   TYPE5 ) -ospfArea <positive_integer>
```

   Utilice el comando add ns ip6 para ejecutar los comandos anteriores en direcciones IPv6.

8. Configure ECMP en el conmutador externo. Se proporcionan las siguientes configuraciones de ejemplo para el conmutador Cisco® Nexus 7000 C7010 Release 5.2 (1). Se deben realizar configuraciones similares en otros conmutadores.


```
1 //For OSPF (IPv4 addresses) Global config: Configure terminal
    feature ospf    Interface config:  Configure terminal
    interface Vlan10      no shutdown      ip address 97.131.0.5/8
       Configure terminal  router ospf 1  network 97.0.0.0/8 area
    0.0.0.0  ---------------------------------
2
3 //For OSPFv3 (IPv6 addresses) Global config:  Configure terminal
    feature ospfv3    Configure terminal  interface Vlan10      no
    shutdown      ipv6 address use-link-local-only      ipv6 router
     ospfv3 1 area 0.0.0.0    Configure terminal  router ospfv3 1
```

Nodos de clúster de supervisión de enrutadores en la implementación de ECMP

En una configuración de clúster, en un nodo propietario que tiene una configuración de dirección SNIP detectada, ahora puede inhabilitar la opción OwnerDownResponse. De forma predeterminada, la opción está habilitada, lo que permite que el nodo responda a una solicitud ICMP/ARP/ICMP6/ND6 procedente del router ascendente. Ahora puede inhabilitar esta opción para permitir que el enrutador supervise si un nodo de clúster está activo o inactivo. Cuando el router envía una solicitud, si la opción está inhabilitada, identifica que el nodo propietario está inactivo y no está disponible para la distribución del tráfico.

Para configurar ECMP para la distribución de tráfico de rutas estáticas mediante la interfaz de línea de comandos

```
1 add ns ip <ipddress> <netmask> -ownernode <node-id>  - ownerDownResponse
    disable
```

Caso de uso: ECMP con redirección BGP

August 20, 2021

Para configurar ECMP con el protocolo de redirección BGP, realice los siguientes pasos:

1. Inicie sesión en la dirección IP del clúster.
2. Habilite el protocolo de redirección BGP.


```
1 > enable ns feature bgp
```

3. Agregue VLAN y vincule las interfaces requeridas.

```
1 > add vlan 985
2 > bind vlan 985 -ifnum 0/0/1 1/0/1
```

4. Agregue la dirección IP detectada y enlaza a la VLAN.

```
1 > add ns ip 10.100.26.14 255.255.255.0 -ownerNode 1 -
     dynamicRouting ENABLED
2 > add ns ip 10.100.26.15 255.255.255.0 -ownerNode 2 -
     dynamicRouting ENABLED
3 > bind vlan 985 -ipAddress 10.100.26.10 255.255.255.0
```

5. Configure el protocolo de redirección BGP en ZeBO mediante el shell VTYSH.

```
1 > vtysh conf t router bgp 65535 vecino 10.100.26.1 remoto-como
     65535
```

6. Configure BGP en el conmutador externo. Se proporcionan las siguientes configuraciones de ejemplo para el conmutador Cisco® Nexus 7000 C7010 Release 5.2 (1). Se deben realizar configuraciones similares en otros conmutadores.

```
1 > router bgp 65535 no synchronization
2   bgp log-neighbor-changes neighbor 10.100.26.14 remote-as 65535
       neighbor 10.100.26.15 remote-as 65535 no auto-summary
3   dont-capability-negotiate
4   dont-capability-negotiate
5   no dynamic-capability
```

Configuración del ECMP del clúster mediante el switch Cisco Nexus 7000 con protocolo de redirección

August 20, 2021

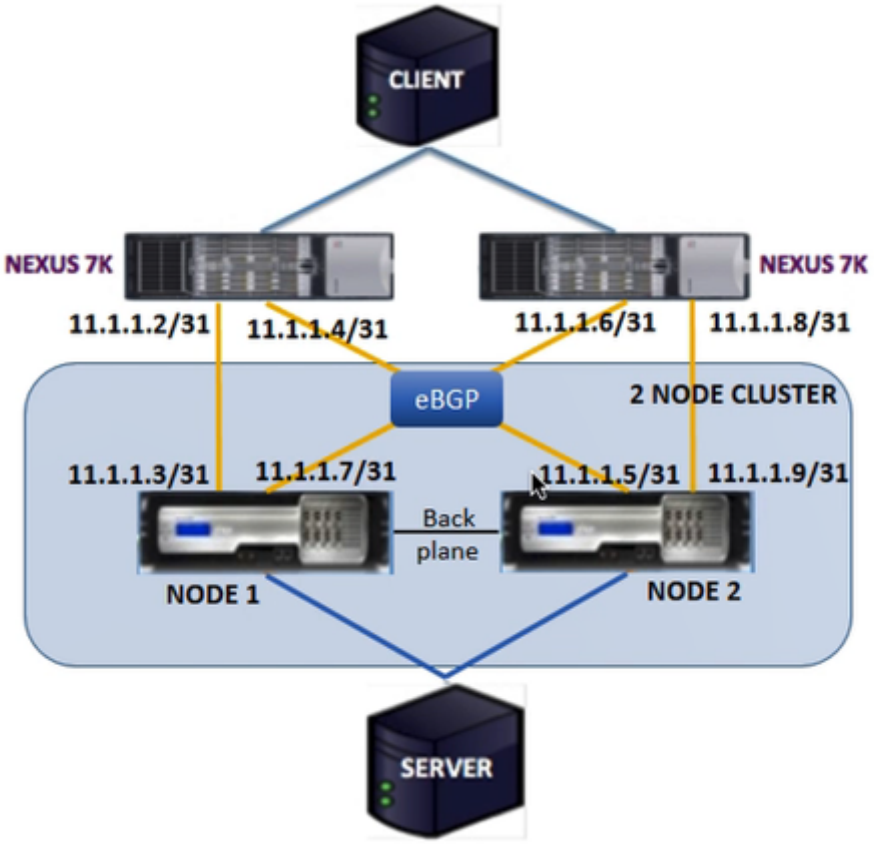
Con ECMP sobre una configuración de clúster, un dispositivo Citrix ADC puede manejar el tráfico a través de un protocolo de redirección. El mecanismo ECMP ayuda a anunciar las direcciones IP del servidor virtual a través de todos los nodos de clúster activos.

Para utilizar ECMP, primero debe habilitar el protocolo BGP en la dirección IP del clúster. Enlazar las interfaces y la dirección IP detectada (con redirección dinámica habilitado) a una VLAN. Configure el protocolo de redirección seleccionado y redistribuya las rutas del kernel en los ZeBO mediante el shell VTYSH.

Caso de uso: Cluster ECMP mediante el switch Cisco Nexus 7000 con protocolo de redirección

Considere un ejemplo de implementación de clústeres con un conmutador Cisco Nexus 7000:

- Dos dispositivos Citrix ADC (nodo 1 y nodo 2), conectados al conmutador Nexus (ascendente).
- Dos conmutadores Cisco Nexus 7000.
- Cliente y servidor (dibujo del tráfico HTTP a través del conmutador Nexus). Con el protocolo de enrutador en espera activa (HSRP) habilitado en el lado del cliente.



Requisitos previos

Tenga en cuenta los siguientes puntos antes de configurar los nodos de clúster en un dispositivo Citrix ADC.

1. Todos los dispositivos deben ser del mismo tipo de plataforma.
2. El protocolo de puerta de enlace de borde (BGP) debe estar habilitado en los nodos del clúster.

Configuración mediante la CLI en un dispositivo Citrix ADC

1. Inicie sesión en un dispositivo (por ejemplo, dispositivo con dirección NSIP 1.1.1.1)
2. Para agregar un nodo de clúster.

```
add cluster node 0 1.1.1.2 -state ACTIVE -backplane 0/10/8
```

3. Para agregar la dirección IP del clúster

```
add ns ip 1.1.1.10 255.255.255.254 -type clip
```

4. Guardar la configuración

```
save ns config
```

5. Reinicie el dispositivo en caliente

```
reboot -warm
```

6. Para agregar el nodo 1 mediante CLIP

```
add cluster node 1 2.2.2.2 -state ACTIVE -backplane 1/10/8
```

7. Para unir un nodo al clúster

```
join cluster -clip 1.1.1.10 -password nsroot
```

8. Realice la siguiente configuración en CLIP

- enable ns feature bgp ospf DYNAMICROUTING
- add ns ip 11.1.1.3 255.255.255.254 -dynamicRouting ENABLED -ownerNode 0
- add ns ip 11.1.1.7 255.255.255.254 -dynamicRouting ENABLED -ownerNode 0
- add ns ip 11.1.1.5 255.255.255.254 -dynamicRouting ENABLED -ownerNode 1
- add ns ip 11.1.1.9 255.255.255.254 -dynamicRouting ENABLED -ownerNode 1

En el router Cisco Nexus (11.1.1.2/31 y 11.1.1.4/31), debe realizar las siguientes configuraciones mediante la línea de comandos:

- feature ospf
- feature bgp
- feature interface-vlan
- feature hsrp

```
>  interface vlan100
    no shutdown
    ip address 50.1.1.1/8
     hsrp 50
      ip 50.50.50.50

>  interface Ethernet 4/15
     ip address 11.1.1.2/31
     no shutdown

>  interface Ethernet 4/19
     ip address 11.1.1.4/31
     no shutdown

>  interface Ethernet 4/22
     switchport
      switchport access vlan 100
```

En el router Cisco Nexus (11.1.1.6/31 y 11.1.1.8/31), debe realizar las siguientes configuraciones mediante la línea de comandos:

- feature ospf

- feature bgp
- feature interface-vlan
- feature hsrp

```
> interface vlan100
  no shutdown
  no ip redirects
  ip address 50.1.1.2/8
   hsrp 50
   ip 50.50.50.50

> interface Ethernet 4/13
  ip address 11.1.1.6/31
  no shutdown

> interface Ethernet 4/15
  ip address 11.1.1.8/31
  no shutdown

> interface Ethernet 4/22
  switchport
  switchport access vlan 100
```

Para el protocolo BGP, debe realizar las siguientes configuraciones en CLIP del dispositivo Citrix ADC:

```
> vtysh
ns# router bgp 1
 redistribute kernel
 owner-node 0
 neighbor 11.1.1.2 remote-as 2
 neighbor 11.1.1.2 as-origination-interval 1
 neighbor 11.1.1.2 advertisement-interval 0
 neighbor 11.1.1.6 remote-as 2
 neighbor 11.1.1.6 as-origination-interval 1
 neighbor 11.1.1.6 advertisement-interval 0
owner-node 1
 neighbor 11.1.1.4 remote-as 2
 neighbor 11.1.1.4 as-origination-interval 1
 neighbor 11.1.1.4 advertisement-interval 0
 neighbor 11.1.1.8 remote-as 2
 neighbor 11.1.1.8 as-origination-interval 1
```



```
 neighbor 11.1.1.8 advertisement-interval 0
exit-owner-node
```

Realice las siguientes configuraciones en el router Cisco Nexus (11.1.1.3 y 11.1.1.5)

```
> ip access-list acl1
  10 permit ip 50.0.0.0/8 any
  route-map test permit
  match ip address acl1
 router bgp 2
  address-family ipv4 unicast
   redistribute direct route-map test
   maximum-paths 2
 neighbor 11.1.1.3 remote-as 1
  address-family ipv4 unicast
  neighbor 11.1.1.5 remote-as 1
 address-family ipv4 unicast
```

Realice las siguientes configuraciones en el router Cisco Nexus (11.1.1.7 y 11.1.1.9)

```
> ip access-list acl1
   10 permit ip 50.0.0.0/8 any
  route-map test permit 1
   match ip address acl1
  router bgp 2
   address-family ipv4 unicast
   redistribute direct route-map test
   maximum-paths 2
  neighbor 11.1.1.7 remote-as 1
   address-family ipv4 unicast
  neighbor 11.1.1.9 remote-as 1
   address-family ipv4 unicast
```

Para el protocolo OSPF, debe realizar las siguientes configuraciones en CLIP del dispositivo Citrix ADC:

```
> vtysh
ns# router osfp 1
redistribute kernel
owner-node 0
 network 15.1.1.2/31 area 0
 network 15.1.1.6/31 area 0
```



```
exit-owner-node

owner-node 1
 network 15.1.1.4/31 area 0
 network 15.1.1.8/31 area 0
exit-owner-node

route-map map2 permit 1
set metric 10
```

En el router Cisco Nexus (11.1.1.2/31 y 11.1.1.4/31), debe realizar las siguientes configuraciones mediante la línea de comandos:

```
> route-map- map2 permit 1
   set metric 10

   interface Ethernet4/15
     ip address 15.1.1.2/31
     ip router ospf 1 area 0.0.0.0
     no shutdown

   interface Ethernet4/19
     ip address 15.1.1.4/31
     ip router ospf 1 area 0.0.0.0
     no shutdown

   router ospf 1
    router-id 1.1.1.1
    redistribute direct route-map map2
```

En el router Cisco Nexus (11.1.1.7/31 y 11.1.1.9/31), debe realizar las siguientes configuraciones mediante la línea de comandos:

```
> route-map- map2 permit 1
    set metric 10

   interface Ethernet4/13
     ip address 15.1.1.6/31
     ip router ospf 1 area 0.0.0.0
     no shutdown

    interface Ethernet4/15
```



```
10       ip address 15.1.1.8/31
11       ip router ospf 1 area 0.0.0.0
12       no shutdown
13
14     router ospf 1
15       router-id 1.1.1.2
16       redistribute direct route-map map2
```

Uso de la agregación de vínculos de clúster

August 20, 2021

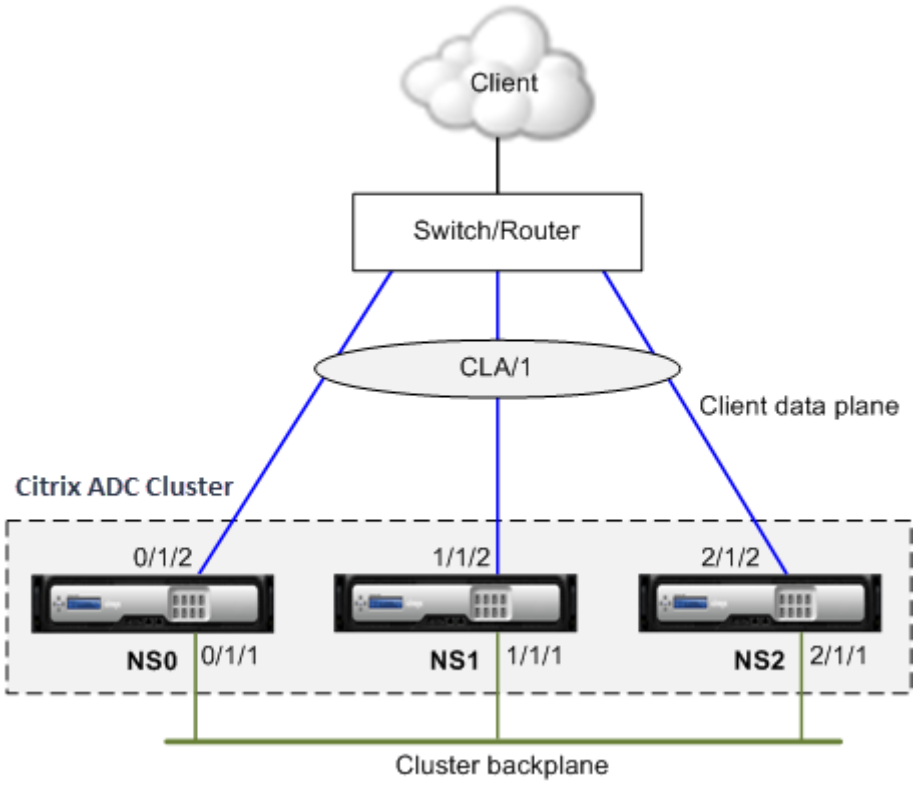
La agregación de vínculos de clúster es un grupo de interfaces de nodos de clúster. Es una extensión de la agregación de enlaces de Citrix ADC. La única diferencia es que, aunque la agregación de enlaces requiere que las interfaces sean del mismo dispositivo, en la agregación de vínculos de clúster, las interfaces provienen de nodos diferentes del clúster. Para obtener más información sobre la agregación de enlaces, consulte Configuración de la agregación de enlaces.

> **Importante**
>
> - La agregación de vínculos de clúster es compatible con un clúster de dispositivos de hardware (MPX).
> - La agregación de vínculos de clúster es compatible con un clúster de dispositivos virtuales (VPX) que se implementan en hipervisores ESX y KVM, con las siguientes restricciones:
> - Deben utilizarse interfaces dedicadas. Significa que las interfaces no deben compartirse con otras máquinas virtuales.
> - Cuando un nodo se vuelve INACTIVO, la interfaz DE LA del clúster correspondiente se marca como apagado, de modo que el tráfico de datos no se envía a un nodo INACTIVO.
> - Cuando un nodo se activa, la interfaz DE LA del clúster correspondiente se marca como encendido.
> - Si las interfaces miembros de agregación de vínculos de clúster se inhabilitan manualmente o si la agregación de vínculos de clúster se inhabilita manualmente, la capacidad de apagado de la interfaz solo se logra mediante el mecanismo de tiempo de espera de LACP.
> - MTU Jumbo no es compatible con la agregación de vínculos de clúster LACP.
>
> **Nota:** La agregación de vínculos de clúster no es compatible con los dispositivos VPX implementados en XenServer, AWS y Hyper-V.

> - A partir de la versión 12. 0, la agregación de vínculos de clúster es compatible con los dispositivos Citrix ADC SDX.
> - El número de interfaces que se pueden enlazar al clúster LA es 16 (de cada nodo). El número máximo de interfaces en el clúster LA puede ser (16 * n), donde n es el número de nodos de un clúster. El número total de interfaces en el clúster LA depende del número de interfaces para cada canal de puerto en el conmutador ascendente.
> - Si un dispositivo Citrix ADC utiliza interfaces Intel Fortville, la conmutación de un nodo de clúster al modo pasivo podría causar algunos segundos de interrupción con CLAG. El problema se produce porque LACP está habilitado para que CLAG funcione correctamente, y el tiempo de interrupción depende de los temporizadores LACP NIC.

Por ejemplo, considere un clúster de tres nodos donde los tres nodos están conectados al conmutador ascendente. Un canal LA de clúster (CLA/1) está formado por interfaces de unión 0/1/2, 1/1/2 y 2/1/2.

Ilustración 1. Topología de agregación de vínculos de clúster



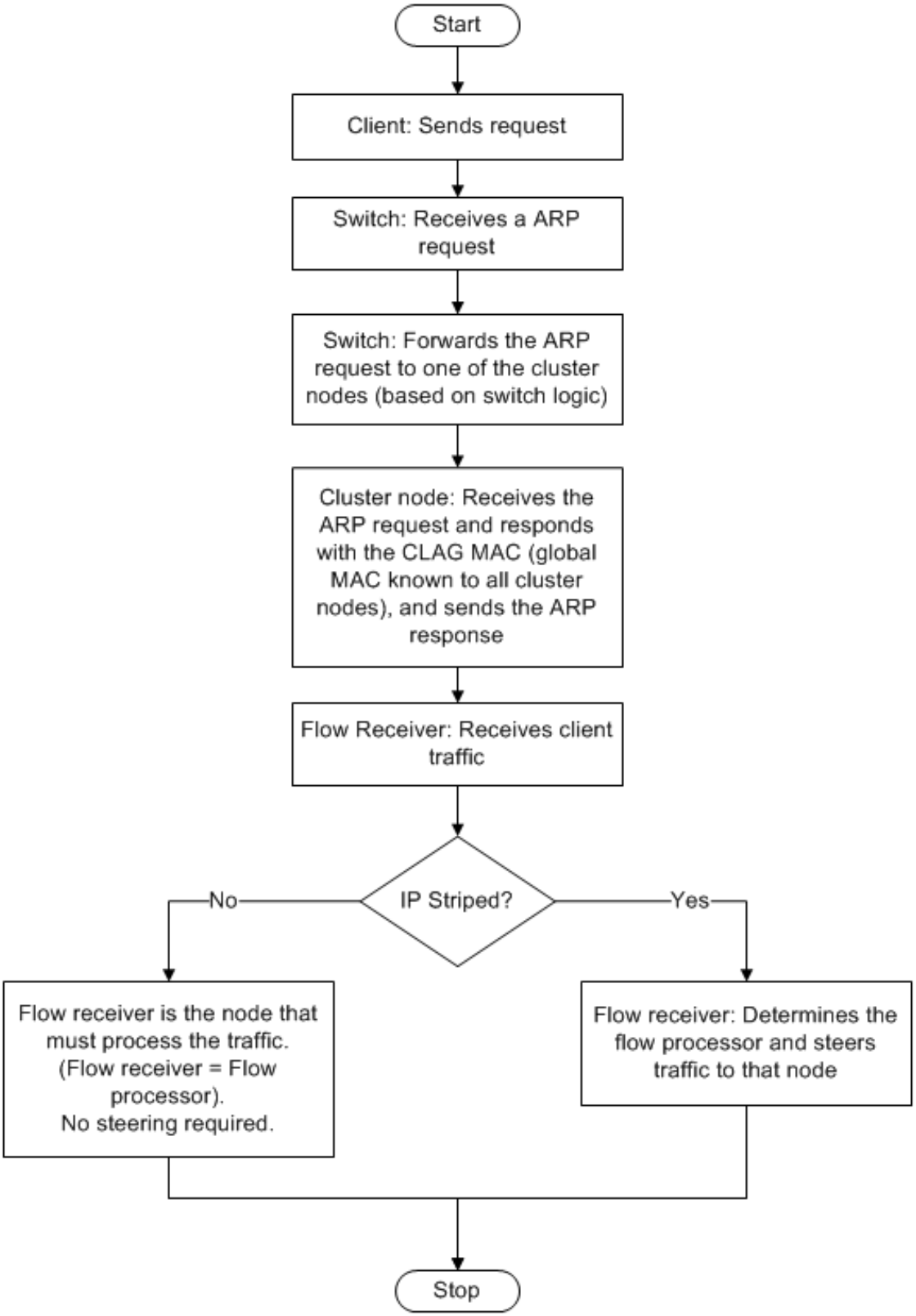
Un canal LA de clúster tiene los siguientes atributos:

- Cada canal tiene un MAC único acordado por los nodos del clúster.
- El canal puede enlazar interfaces de nodos locales y remotos.
- Un clúster admite un máximo de cuatro canales LA de clúster.
- Las interfaces de backplane no pueden formar parte de un canal LA del clúster.
- Cuando una interfaz está enlazada a un canal LA del clúster, los parámetros del canal tienen

prioridad sobre los parámetros de la interfaz de red. Una interfaz de red solo se puede enlazar a un canal.

- El acceso de administración a un nodo de clúster no debe configurarse en un canal LA del clúster (por ejemplo, CLA/1) ni en sus interfaces miembro. Esto se debe a que cuando el nodo está INACTIVO, la interfaz DE LA del clúster correspondiente se marca como apagado y, por lo tanto, pierde el acceso de administración.

Ilustración 2. Flujo de distribución de tráfico mediante el clúster LA



Compatibilidad con copias de seguridad y restauración del clúster LA en Citrix ADC MPX

Puede realizar una copia de seguridad y restaurar la configuración del clúster de LA en Citrix ADC MPX. La dirección MAC DE LA del clúster es independiente de la dirección MAC de la interfaz física de los nodos del clúster y puede cambiar después del proceso de copia de seguridad y restauración. El LA del clúster puede servir el tráfico una vez finalizado el proceso de restauración del clúster. Para obtener más información sobre el backup y la restauración, consulte Copia de seguridad y restauración de la configuración de clúster

Agregación de enlaces de clúster estático

August 20, 2021

Debe configurar un canal LA del clúster estático en la dirección IP del clúster y en el dispositivo de conexión externo. Si es posible, configure el conmutador ascendente para distribuir el tráfico según la dirección IP o el puerto en lugar de la dirección MAC.

Para configurar un canal LA de clúster estático mediante la CLI

1. Inicie sesión en la dirección IP del clúster.

   > **Nota**
   >
   > Asegúrese de configurar el canal LA del clúster en la dirección IP del clúster antes de configurar la agregación de vínculos en el conmutador externo. De lo contrario, el conmutador reenvía el tráfico al clúster aunque el canal LA del clúster no esté configurado. Puede conducir a la pérdida de tráfico.

2. Cree un canal LA de clúster.

```
add channel <id> -speed <speed>
```

Ejemplo

```
add channel CLA/1 -speed 1000
```

> **Nota**
>
> No debe especificar la velocidad como AUTO. Por el contrario, debe especificar explícitamente la velocidad como 10, 100, 1000 o 10000. Solo se agregan a la lista de distribución ac-

> tiva las interfaces que tengan la velocidad que coincida con el <speed> atributo del canal LA del clúster.

3. Enlazar las interfaces necesarias al canal LA del clúster. Asegúrese de que las interfaces no se utilizan para el plano anterior del clúster.

```
bind channel <id> <ifnum>
```

Ejemplo

```
bind channel CLA/1 0/1/2 1/1/2 2/1/2
```

4. Verifique las configuraciones.

```
show channel <id>
```

Ejemplo

```
show channel CLA/1
```

> **Nota**
>
> Puede enlazar el canal LA del clúster a una VLAN mediante el `bind vlan` comando. Las interfaces del canal se vinculan automáticamente a la VLAN.

5. Configure LA estática en el conmutador externo. Se proporcionan las siguientes configuraciones de ejemplo para Cisco® Nexus 7000 C7010 Release 5.2 (1). Se deben realizar configuraciones similares en otros conmutadores.

```
Global config:
Configure terminal

Interface level config:

interface Ethernet2/47
switchport
switchport access vlan 10
channel-group 7 mode on
no shutdown
```



```
11
12 interface Ethernet2/48
13 switchport
14 switchport access vlan 10
15 channel-group 7 mode on
16 no shutdown
```

Agregación dinámica de vínculos de clúster

August 20, 2021

El canal LA de clúster dinámico utiliza el Protocolo de control de agregación de enlaces (LACP).

Debe realizar configuraciones similares en la dirección IP del clúster y en el dispositivo de conexión externo. Si es posible, configure el conmutador ascendente para distribuir el tráfico según la dirección IP o el puerto en lugar de la dirección MAC.

> **Puntos que tener en cuenta**
>
> - Habilite LACP (especificando el modo LACP como ACTIVO o PASIVO).

```
1 >**Note**
2 >
3 > Make sure the LACP mode is not set as PASSIVE on both the Citrix ADC
    cluster and the external connecting device.
```

> - Especifique la misma clave LACP en cada interfaz que quiera que forme parte del canal. Para crear un canal LA de clúster, la clave LACP puede tener un valor de 5 a 8. Por ejemplo, si establece la clave LACP en las interfaces 0/1/2, 1/1/2 y 2/1/2 a 5, se crea CLA/1. Las interfaces 0/1/2, 1/1/2 y 2/1/2 se vinculan automáticamente a CLA/1. Del mismo modo, si establece la tecla LACP en 6, se crea el canal CLA/2.
> - Especifique el tipo de LAG como clúster.

Para configurar un canal LA de clúster dinámico mediante la CLI

En la dirección IP del clúster, para cada interfaz que quiera agregar al canal LA del clúster, escriba:

```
set interface <id> -lacpMode <lacpMode> -lacpKey <positive_integer> -
lagType CLUSTER<!--NeedCopy-->
```

Ejemplo:

Para configurar un clúster LA canal CLA/1 de 3 interfaces.

```
> set interface 0/1/2 -lacpMode active -lacpKey 5 -lagType Cluster
> set interface 1/1/2 -lacpMode active -lacpKey 5 -lagType Cluster
> set interface 2/1/2 -lacpMode active -lacpKey 5 -lagType Cluster
```

> **Nota**
>
> Opcionalmente, puede habilitar la redundancia de vínculos en un clúster con LACP.

Del mismo modo, configure LA dinámica en el conmutador externo. Se proporcionan las siguientes configuraciones de ejemplo para Cisco® Nexus 7000 C7010 Release 5.2 (1). Se deben realizar configuraciones similares en otros conmutadores.

```
Global config:
Configure terminal
feature lacp
Interface level config:

interface Ethernet2/47
switchport
switchport access vlan 10
channel-group 7 mode active
no shutdown

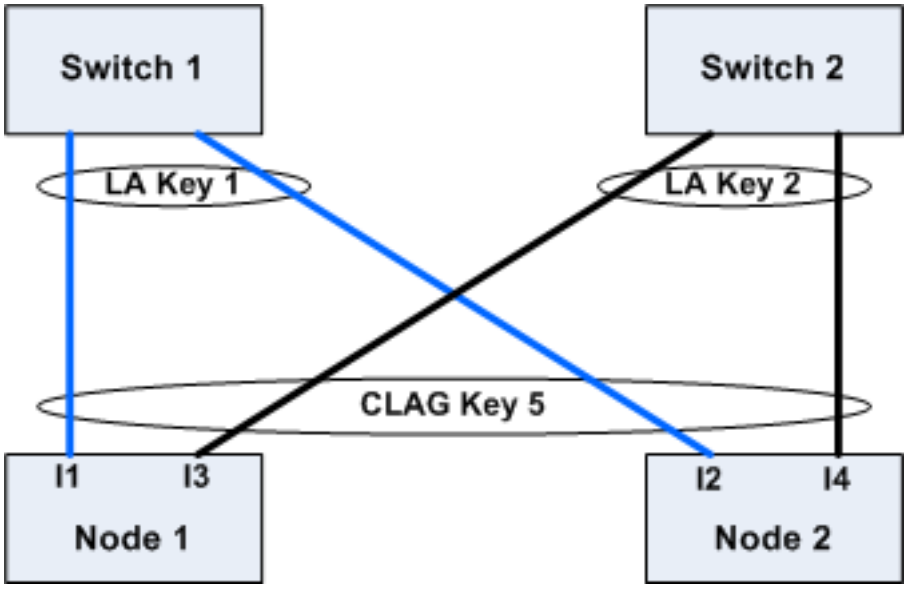
interface Ethernet2/48
switchport
switchport access vlan 10
channel-group 7 mode active
no shutdown
```

Redundancia de vínculos en un clúster con LACP

January 12, 2021

Un clúster de Citrix ADC proporciona redundancia de vínculos para LACP para garantizar que todos los nodos tengan la misma clave de asociado.

Para entender la necesidad de redundancia de enlaces, consideremos el ejemplo de la siguiente configuración del clúster junto con los casos adjuntos (con atención al caso 3):



En esta configuración, las interfaces I1, I2, I3 e I4 están vinculadas al canal LACP con KEY 5. En el lado del socio, I1 e I2 están conectados al conmutador 1 para formar un único canal LA con KEY 1. Del mismo modo, I3 e I4 están conectados al Switch 2 para formar un único canal LA con KEY 2.

Ahora consideremos los siguientes casos para entender la necesidad de redundancia de enlaces:

- **Caso 1: El interruptor 1 está encendido y el interruptor 2 está apagado**

  En este caso, el clúster LA en ambos nodos dejaría de recibir LACPDU desde Key2 y comenzaría a recibir LACPDU desde Key1. En ambos nodos, el clúster LA está conectado a KEY 1 e I1 e I2 es UP y el canal de ambos nodos sería UP.

- **Caso 2: El Switch1 se desconecta y el Switch2 se vuelve UP**

  En este caso, el clúster LA en ambos nodos dejaría de recibir LACPDU desde Key1 y comenzaría a recibir LACPDU desde Key2. En ambos nodos, el clúster LA está conectado a Key2 e I3 e I4 es UP y el canal en ambos nodos sería UP.

- **Caso 3: Tanto el Switch1 como el Switch2 están UP**

  En este caso, es posible que el clúster LA en el nodo1 elija Key1 como socio y el clúster LA en el nodo2 elija Key2 como socio. Significa que I1 en el nodo1 e I4 en el nodo2 están recibiendo tráfico que no es deseable. Puede suceder porque la máquina de estado LACP está a nivel de nodo y elige a sus socios en base al orden de llegar primero en servir.

  Para resolver estas preocupaciones, se admite la redundancia de vínculos del clúster dinámico LA. Para configurar la redundancia de enlace en un canal o interfaz, debe habilitarla y, opcionalmente, especificar el rendimiento del umbral de la siguiente manera:

  ```
  set channel CLA/1 -linkRedundancy ON -lrMinThroughput <positive_integer
  >
  ```


El rendimiento de los canales asociados se compara con el rendimiento umbral configurado. El canal asociado que satisface el rendimiento de umbral se selecciona de forma que primero en salir (FIFO). Si ninguno de los canales asociados cumple el umbral, o si el rendimiento del umbral no está configurado, se selecciona el canal asociado con el número máximo de enlaces.

> **Nota**
>
> El rendimiento umbral se puede configurar a partir de NetScaler 11.

Uso del modo USIP en clúster

August 20, 2021

En el modo IP de origen (USIP), el clúster o el dispositivo Citrix ADC reenvía cada paquete al servidor back-end adecuado con la dirección IP del cliente.

Distribución de tráfico en modo USIP

El comportamiento del modo USIP difiere de la distribución del tráfico entre el plano de datos del cliente y el plano de datos del servidor en la implementación de ECMP y CLAG. En la siguiente sección se proporciona más información sobre el comportamiento del modo USIP. Para obtener más información relacionada con CLAG en modo USIP, consulte Uso de la agregación de enlaces de clúster.

Modo USIP

El clúster utiliza la IP del cliente para abrir la conexión del lado del servidor. El puerto de origen se puede conservar o no según la `useproxyport` configuración.

`useproxyport` Casos USIP

El USIP `useproxyport` está ACTIVADO para el flujo de tráfico, el puerto de origen se selecciona de forma que el tráfico inverso hash hacia el procesador de flujo. Garantiza una sola dirección en el lado del servidor.

El USIP `useproxyport` está DESACTIVADO para el flujo de tráfico, el puerto de origen se conserva y, por lo tanto, hay doble dirección en el lado del servidor.

> **Importante**
>
> - Cuando USIP está ACTIVADO, la IP del cliente se utiliza en la conexión del servidor backend y se necesita una distribución del tráfico para responder entre los nodos de clúster. Puede utilizar la implementación de ECMP o CLAG para la distribución del tráfico en el lado del

> servidor. En ausencia de distribución del tráfico en el lado del servidor, todo el tráfico de retorno podría aterrizar en un solo nodo de clúster, lo que provoca congestión.
> - El `set rsskeytype -rsskey symmetric` comando se utiliza para reducir la dirección doble a la dirección única del tráfico en las implementaciones `useproxyport` fuera. Donde la 4 tupla de la conexión sigue siendo la misma para el servidor y el cliente. Por ejemplo, servidor virtual de modo MAC comodín.

Limitaciones

El USIP no funciona cuando el proceso local está inhabilitado.

Implementación en modo USIP

En la siguiente ilustración se muestra una implementación en modo USIP en una configuración de clúster.

Configure lo siguiente mediante CLI

1. Habilite el protocolo de redirección.

```
enable ns feature <feature>
```

Ejemplo:

```
enable ns feature ospf
```

2. Agregue una dirección SNIP detectada para cada nodo y habilite el redirección dinámica en él.

```
add ns ip <SNIP> <netmask> -dynamicRouting ( ENABLED | DISABLED )
    - ownerNode <positive_interger>  - ownerdownResponse ( YES | NO
    )
```

Ejemplo

```
-  add ns ip 192.0.2.1 255.255.255.0 -dynamicRouting ENABLED  -
    ownerNode 0  - ownerDownResponse NO
```



```
2 - add ns ip 192.0.2.2 255.255.255.0 -dynamicRouting ENABLED -
    ownerNode 1 - ownerDownResponse NO
3 - add ns ip 192.0.2.3 255.255.255.0 -dynamicRouting ENABLED -
    ownerNode 2 - ownerDownResponse NO
```

3. Agregue una VLAN.

```
1 add vlan <id>
```

Ejemplo

```
1 add vlan 300
```

4. Enlace las interfaces de los nodos del clúster a la VLAN.

```
1 bind vlan <id> -ifnum <interface_name>
```

Ejemplo

```
1 bind vlan 300 -ifnum 0/1/2 1/1/2 2/1/2
```

5. Enlazar una de las direcciones SNIP detectada a la VLAN. Cuando vincula una dirección SNIP detectada a una VLAN, todas las demás direcciones SNIP detectada definidas en el clúster de esa subred se vinculan automáticamente a la VLAN.

```
1 bind vlan <id> -IPAddress <ip_addr | ipv6_addr> -netmask
```

Ejemplo

```
1 bind vlan 300 - IPAddress 192.0.2.1 255.255.255.0
```

6. Configure el protocolo de redirección en ZEBO mediante el shell de VTYSH. Configure el protocolo de redirección OSPF en los ID de nodo 0, 1 y 2.


```
vtysh
configure terminal
ns block-sec-rtadv
router ospf
owner -node 0
router-id 192.0.2.1
exit-owner-node
owner-node 1
router-id 192.0.2.2
exit-owner-node
owner-node 2
router-id 192.0.2.3
exit-owner-node
network 192.0.2.0/24 area 0

default-information originate always
```

7. Realice las siguientes configuraciones en el router 3750 de Cisco mediante la CLI.

```
Configure terminal
feature ospf
interface vlan300
no shutdown
ip address 192.0.2.100/24
Configure terminal
router ospf 1
router-id 192.0.2.100
network 192.0.2.0 0.0.0.255 area 0
```

Notas

- La distribución del tráfico en el cliente y el servidor no tiene por qué ser la misma. Por ejemplo, puede configurar ECMP en el lado del cliente y CLAG en el lado del servidor o de la forma opuesta.
- Planifique la capacidad adicional del plano posterior, ya que hay más sobrecarga de dirección en la implementación del USIP.
- La configuración relacionada con CLAG y Monitor Static Route (MSR) debe permanecer igual en el lado del servidor.
- La dirección del tráfico está más en las implementaciones del modo USIP.

Administración del clúster de Citrix ADC

January 12, 2021

Después de crear un clúster y configurar el mecanismo de distribución de tráfico necesario, el clúster puede servir el tráfico. Durante la vida útil del clúster, puede realizar las siguientes tareas de clúster:

- Configuración de grupos de nodos
- Desactivación de nodos de un clúster
- Descubrimiento de dispositivos Citrix ADC
- Visualización de estadísticas
- Sincronización de configuraciones de clúster y archivos de clúster
- Sincronización del tiempo entre los nodos
- Actualizar o degradar el software de los nodos de clúster

Configuración de conjuntos de vínculos

August 20, 2021

Linkset es un grupo de interfaces de nodos de clúster que pertenecen al mismo dominio de difusión. En los conjuntos de vínculos, cada nodo tiene la información sobre qué interfaces de otros nodos están conectadas al mismo dominio de difusión.

> **Nota**
>
> Los conjuntos de vínculos son una configuración obligatoria en los siguientes casos:
>
> - Para implementaciones que requieren reenvío basado en Mac (MBF).
> - Para el modo "-m MAC" que está habilitado en el servidor virtual junto con el modo MBF habilitado globalmente.
> - Mejorar la manejabilidad de las directivas ACL y L2 que involucran interfaces. Se define un conjunto de vínculos de las interfaces y se agregan directivas ACL y L2 basadas en conjuntos de vínculos.

En una configuración de clúster, las siguientes funciones utilizan MBF internamente.

- Sesión de reenvío
- L2Conn
- Servidor virtual en modo MAC
- Monitor transparente
- LLB

Los conjuntos de vínculos solo deben configurarse a través de la dirección IP del clúster.

Considere un ejemplo con un clúster de tres nodos. En la siguiente ilustración, las interfaces 0/1/2, 1/1/2 y 2/1/2 están en el mismo dominio de difusión y, por lo tanto, se pueden configurar como linkset (LS/1).

Ilustración 1. Topología de conjuntos de enlaces

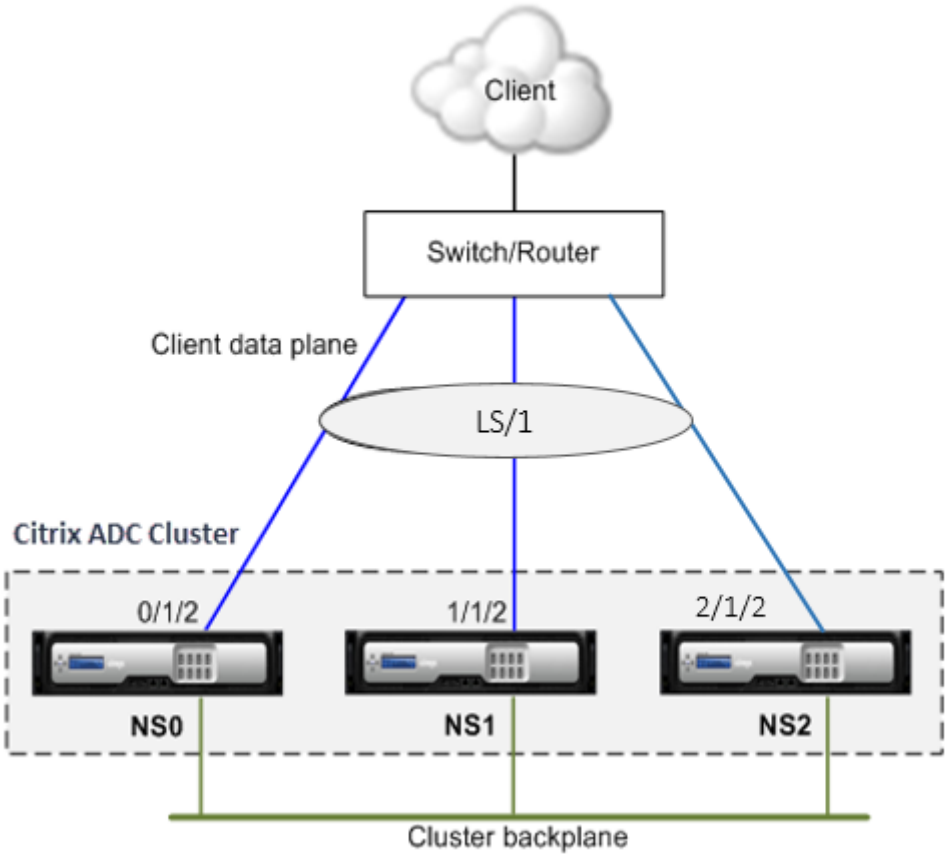
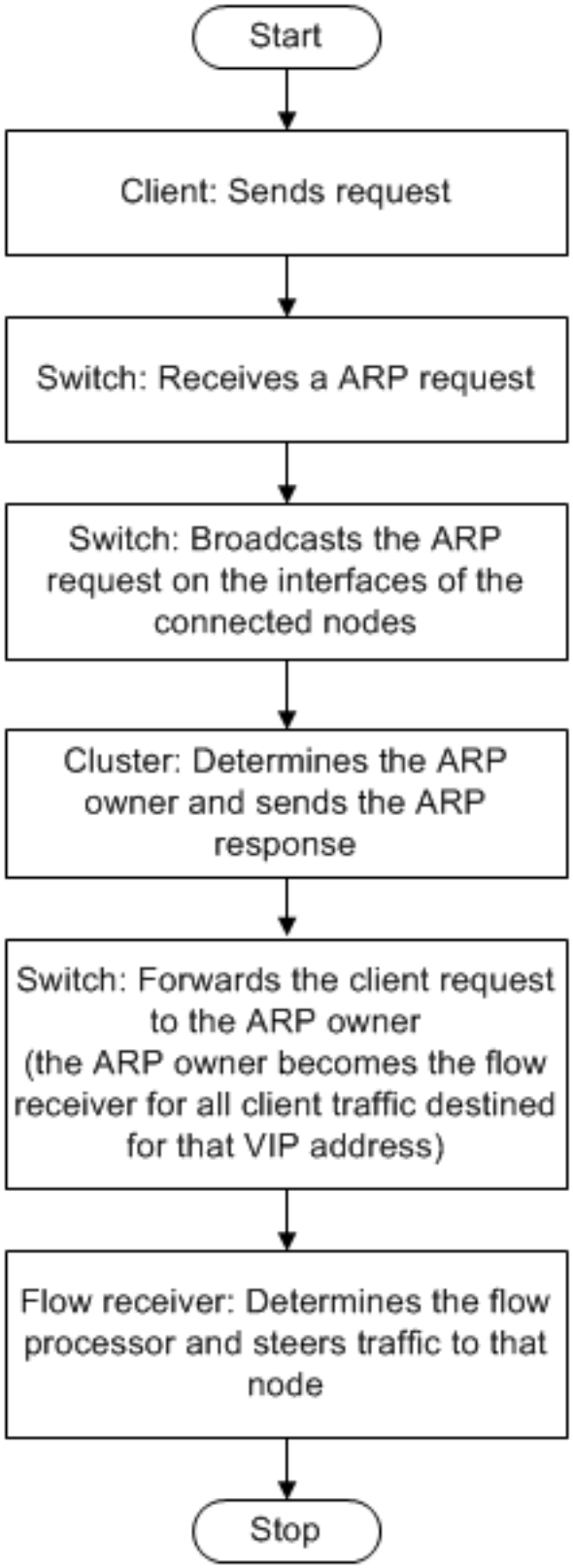


Ilustración 2. Flujo de distribución de tráfico mediante enlaces



Para configurar un conjunto de vínculos mediante la CLI

1. Inicie sesión en la dirección IP del clúster.
2. Cree un conjunto de enlaces.

   “‘add linkset

```
**Ejemplo**

```add linkset LS/1<!--NeedCopy-->
```

3. Enlazar las interfaces requeridas al conjunto de vínculos. Asegúrese de que las interfaces no se utilizan para el plano anterior del clúster.

   “‘bind linkset -ifnum ...

```
**Ejemplo**

```bind linkset LS/1 -ifnum 0/1/2 1/1/2 2/1/2<!--NeedCopy-->
```

4. Compruebe las configuraciones del conjunto de enlaces.

   “‘show linkset

```
**Ejemplo**

```show linkset LS/1<!--NeedCopy-->
```

> **Nota**
>
> Puede enlazar el conjunto de vínculos a una VLAN mediante el `bind vlan` comando. Las interfaces del conjunto de vínculos se vinculan automáticamente a la VLAN.

Para configurar un conjunto de vínculos mediante la interfaz gráfica de usuario

1. Inicie sesión en la dirección IP del clúster.
2. Vaya a **Sistema > Red > Conjuntos de vínculos**.
3. En el panel de detalles, haga clic en **Agregar**.
4. En el cuadro de diálogo **Crear conjunto de enlaces**:
   - Especifique el nombre del conjunto de enlaces estableciendo el parámetro Conjunto de enlaces.


```

- Especifique las interfaces que se van a agregar al conjunto de enlaces y haga clic en Agregar. Repita este paso para cada interfaz que quiera agregar al conjunto de enlaces.

5. Haga clic en **Crear** y, a continuación, en **Cerrar**.

## Grupos de nodos para configuraciones manchadas y parcialmente divisadas

August 20, 2021

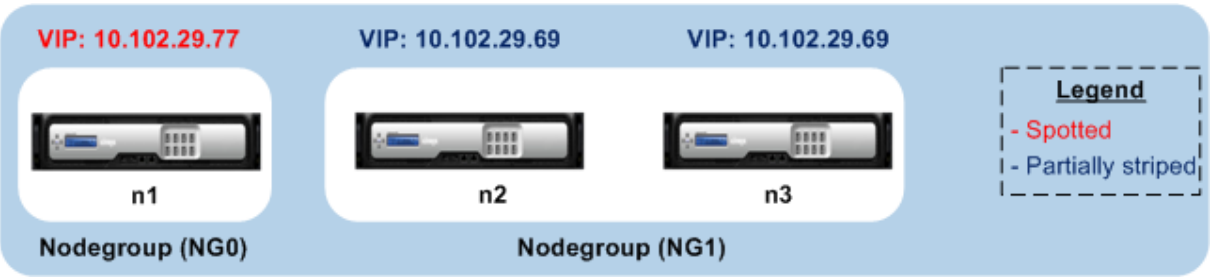
En virtud del comportamiento predeterminado del clúster, todas las configuraciones realizadas en la dirección IP del clúster están disponibles en todos los nodos del clúster. Sin embargo, puede haber casos en los que necesite que algunas configuraciones estén disponibles solo en nodos de clúster específicos.

Puede cumplir este requisito definiendo un grupo de nodos que incluya los nodos de clúster específicos y, a continuación, vincular la configuración a ese grupo de nodos. Garantiza que la configuración esté activa solo en esos nodos de clúster. Estas configuraciones se denominan parcialmente rayadas o manchadas (si están activas solo un solo nodo). Para obtener más información, consulte Configuraciones rayadas, parcialmente rayadas y manchadas.

Por ejemplo, considere un clúster con tres nodos. Se crea un grupo de nodos NG0 que incluye el nodo n1 y otro grupo de nodos NG1 que incluye n2 y n3. Enlazar servidores virtuales de equilibrio de carga 0.77 a NG0 y servidor virtual de equilibrio de carga 0.69 a NG1.

Significa que el servidor virtual 0.77 está activo solo en n1 y, por lo tanto, solo n1 recibe el tráfico que se dirige a 0.77. Del mismo modo, el servidor virtual 0.69 solo está activo en los nodos n2 y n3 y, por lo tanto, solo n2 y n3 reciben el tráfico que se dirige a 0.69.

Ilustración 1. Clúster Citrix ADC con grupos de nodos configurados para configuraciones divididas y divididas parciales




Las entidades o configuraciones que puede enlazar a un grupo de nodos son:

- Equilibrio de carga, conmutación de contenido, redirección de caché, autenticación, autorización y auditoría de servidores virtuales

> **Nota**
>
> Los servidores virtuales de equilibrio de carga FTP no se pueden enlazar a grupos de nodos.

- Servidor virtual VPN (compatible con NetScaler 10.5 Build 50.10 en adelante)
- Sitios de Global Server Load Balancing (GSLB) y otras entidades GSLB (compatible con NetScaler 10.5 Build 52.11 en adelante)
- Identificadores de límite e identificadores de flujo

## Comportamiento de grupos de nodos

January 12, 2021

Debido a la interoperabilidad de los grupos de nodos con diferentes funciones y entidades de Citrix ADC, hay algunos aspectos de comportamiento que deben tenerse en cuenta. También se puede hacer una copia de seguridad de los nodos de un grupo de nodos. Siga leyendo para obtener más información.

### Comportamiento general de un grupo de nodos de cluster

- Un grupo de nodos que tiene entidades enlazadas a él no se puede quitar.
- No se puede quitar un nodo de clúster que pertenece a un grupo de nodos con entidades enlazadas a él.
- No se puede quitar una instancia de clúster que tiene grupos de nodos con entidades vinculadas a ella.
- No se puede agregar una entidad que tenga una dependencia de otra entidad. No debe formar parte del grupo de nodos. Si debe hacerlo, primero elimine la dependencia. A continuación, agregue ambas entidades al grupo de nodos y vuelva a asociar las entidades.

  **Ejemplos:**

  - Supongamos que tiene un servidor virtual, VS1, cuya copia de seguridad es el servidor virtual VS2. Para agregar VS1 a un grupo de nodos, primero asegúrese de que VS2 se quita como servidor de copia de seguridad de VS1. A continuación, vincule cada servidor individualmente al grupo de nodos y, a continuación, configure VS2 como copia de seguridad para VS1.
  - Supongamos que tiene un servidor virtual de conmutación de contenido, CSVS1, cuyo servidor virtual de equilibrio de carga de destino es LBVS1. Para agregar CSVS1 a un grupo

de nodos, primero quite LBVS1 como destino. A continuación, vincule cada servidor individualmente al grupo de nodos y, a continuación, configure LBVS1 como destino.

- Supongamos que tiene un servidor virtual de equilibrio de carga, LBVS1, que tiene una directiva que invoca otro servidor virtual de equilibrio de carga, LBVS2. Para agregar uno de los servidores virtuales, primero quite la asociación. A continuación, vincule cada servidor individualmente al grupo de nodos y, a continuación, vuelva a asociar los servidores virtuales.

- No se puede enlazar una entidad a un grupo de nodos. No tiene nodos y que tiene habilitada la opción estricta. Por lo tanto, no puede desenlazar el último nodo de un grupo de nodos que tiene entidades vinculadas a él y que tiene habilitada la opción estricta.
- La opción estricta no se puede modificar para un grupo de nodos que no tiene nodos pero tiene entidades vinculadas a él.

### Copia de seguridad de nodos en un grupo de nodos

De forma predeterminada, un grupo de nodos está diseñado para proporcionar nodos de copia de seguridad para los miembros de un grupo de nodos. Si un miembro del grupo de nodos desaparece, un nodo de clúster que no es miembro del grupo de nodos reemplaza dinámicamente al nodo con errores. Este nodo se denomina nodo de reemplazo.

> **Nota**
>
> Para un grupo de nodos de un solo miembro, un nodo de copia de seguridad se preselecciona automáticamente cuando una entidad está enlazada al grupo de nodos.

Cuando aparece el miembro original del grupo de nodos, el nodo de reemplazo, de forma predeterminada, se reemplaza por el nodo miembro original.

Sin embargo, a partir de NetScaler 10.5 Build 50.10, Citrix ADC le permite cambiar este comportamiento de reemplazo. Cuando habilita la opción pegajosa, el nodo de reemplazo se conserva incluso después de que aparezca el nodo miembro original. El nodo original se hace cargo solo cuando el nodo de reemplazo se desactiva.

También puede inhabilitar la funcionalidad de copia de seguridad. Para hacerlo, debe habilitar la opción estricta. En este caso, cuando un miembro del grupo de nodos cae, ningún otro nodo de clúster se recoge como nodo de copia de seguridad. El nodo original continúa formando parte del grupo de nodos cuando aparece. Esta opción garantiza que las entidades enlazadas a un grupo de nodos solo estén activas en los miembros del grupo de nodos.

> **Nota**
>
> La opción estricta y adhesiva solo se puede establecer al crear un grupo de nodos.

# Configuración de grupos de nodos para configuraciones manchadas y parcialmente divisadas

August 20, 2021

Para configurar un grupo de nodos para configuraciones manchadas y parcialmente divisadas, primero debe crear un grupo de nodos y, a continuación, enlazar los nodos necesarios al grupo de nodos. A continuación, asocie las entidades necesarias a ese grupo de nodos. Las entidades que están enlazadas al grupo de nodos son de las siguientes:

- **Manchado**: Si está enlazado a un grupo de nodos que tiene un único nodo.
- **Parcialmente rayado**: Si está enlazado a un grupo de nodos que tiene más de un nodo.

**Algunos puntos a recordar:**

- GSLB solo se admite en un clúster cuando los sitios GSLB están enlazados a grupos de nodos que tienen un único nodo de clúster. Para obtener más información, consulte Configuración de GSLB en un clúster.
- Citrix Gateway solo se admite en un clúster cuando los servidores virtuales VPN están enlazados a grupos de nodos que tienen un único nodo de clúster. La opción adhesiva debe estar habilitada en el grupo de nodos.
- Para las versiones anteriores a NetScaler 11, el firewall de la aplicación solo se admite en nodos de clúster individuales (configuración detectada). Los perfiles de firewall de aplicaciones solo se pueden asociar con servidores virtuales enlazados a grupos de nodos que tienen un único nodo de clúster. Significa que la aplicación no se le permite hacer lo siguiente:
  - Enlazar perfiles de firewall de aplicaciones a servidores virtuales seccionados o parcialmente seccionados.
  - Enlazar la directiva a un punto de enlace global o a etiquetas de directiva definidas por el usuario.
  - Desvincular, de un grupo de nodos, un servidor virtual que tenga perfiles de firewall de aplicaciones.
- NetScaler 11 introdujo compatibilidad con firewall de aplicaciones para configuraciones de rayas y parcialmente rayadas. Para obtener más información, consulte Compatibilidad con firewall de aplicaciones para configuraciones de clúster.

Compruebe las funciones de Citrix ADC compatibles en un clúster para ver las versiones de NetScaler desde las que se admiten GSLB, Citrix Gateway y firewall de aplicaciones en un clúster.

### Para configurar un grupo de nodos mediante la interfaz de línea de comandos

1. Inicie sesión en la dirección IP del clúster.

2. Cree un grupo de nodos. Tipo:

   ```
   add cluster nodegroup <name> -strict (YES | NO)<!--NeedCopy-->
   ```

   Ejemplo

   ```
   1 add cluster nodegroup NG0 -strict YES
   ```

3. Enlazar los nodos necesarios al grupo de nodos. Escriba el siguiente comando para cada miembro del grupo de nodos:

   ```
   bind cluster nodegroup <name> -node <nodeId><!--NeedCopy-->
   ```

   Ejemplo

   Para enlazar nodos con identificadores 1, 5 y 6.

   ```
   1 > bind cluster nodegroup NG0 -node 1
   2 > bind cluster nodegroup NG0 -node 5
   3 > bind cluster nodegroup NG0 -node 6
   ```

4. Enlazar la entidad al grupo de nodos. Escriba el siguiente comando una vez para cada entidad que quiera enlazar:

   ```
   bind cluster nodegroup <name> (-vServer <string> | -identifierName <
   string> | -gslbSite <string> -service <string>)<!--NeedCopy-->
   ```

   > **Nota**
   >
   > Los parámetros de servicio y gslbSite están disponibles a partir de NetScaler 10.5.

   Ejemplo

   Para enlazar servidores virtuales VS1 y VS2 y el identificador de límite de velocidad denominado identificador1.

   ```
   1 > bind cluster nodegroup NG0 -vServer VS1
   2 > bind cluster nodegroup NG0 -vServer VS2
   3 > bind cluster nodegroup NG0 -identifierName identifier1
   ```

5. Verifique las configuraciones viendo los detalles del grupo de nodos. Tipo:

   ```
   show cluster nodegroup <name><!--NeedCopy-->
   ```

   Ejemplo


```
> show cluster nodegroup NG0
```

Para configurar un grupo de nodos mediante la utilidad de configuración

1. Inicie sesión en la dirección IP del clúster.
2. Vaya a **Sistema > Cluster > Grupos de nodos.**
3. En el panel de detalles, haga clic en **Agregar.**
4. En el cuadro de diálogo **Crear grupo de nodos**, configure el grupo de nodos:
   a) En **Nodos de clúster**, haga clic en el botón **Agregar**.
      - La lista Disponible muestra los nodos que se pueden enlazar al grupo de nodos y la lista Configurado muestra los nodos enlazados al grupo de nodos.
      - Haga clic en el signo **+** de la lista Disponible para enlazar el nodo. Del mismo modo, haga clic en el signo **-** en la lista Configurado para desenlazar el nodo.
   b) En **Servidores virtuales**, seleccione la ficha correspondiente al tipo de servidor virtual que quiere enlazar al grupo de nodos. Haga clic en el botón **Add**.
      - La lista Disponible muestra los servidores virtuales que se pueden enlazar al grupo de nodos y la lista Configurado muestra los servidores virtuales enlazados al grupo de nodos.
      - Haga clic en el signo **+** en la lista Disponible para enlazar el servidor virtual. Del mismo modo, haga clic en el signo: En la lista Configurado para desenlazar el servidor virtual.

Configuración de redundancia para grupos de nodos

August 20, 2021

> **Nota**
>
> Compatible con NetScaler 10.5 Build 52.1115.e en adelante.

Los grupos de nodos se pueden configurar de manera que cuando un grupo de nodos se desactiva, otro grupo de nodos pueda tomar el control y procesar el tráfico. Por ejemplo, cuando un grupo de nodos NG1 cae, NG2 toma el control.

> **Nota**
>
> Esta funcionalidad se puede utilizar para configurar la redundancia del centro de datos donde cada grupo de nodos está configurado como centro de datos.

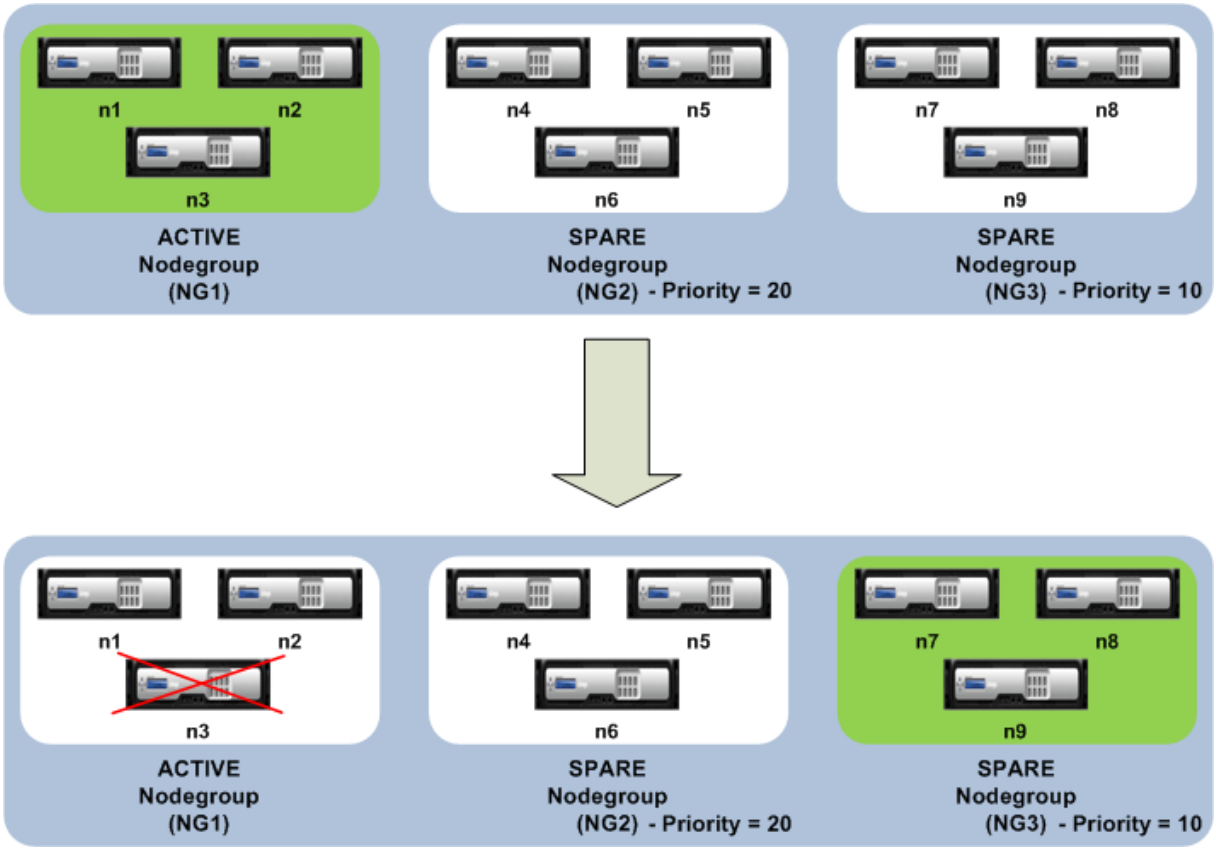
Para lograr este caso de uso, los nodos de clúster deben agruparse lógicamente en grupos de nodos, donde algunos grupos de nodos deben configurarse como ACTIVE y otros como SPARE. El grupo de

nodos activos con la prioridad más alta (es decir, el número de prioridad más bajo) se activa operacionalmente y, por lo tanto, sirve el tráfico. Cuando un nodo de este grupo de nodos operacionalmente activo desaparece, el recuento de nodos de este grupo de nodos se compara con el recuento de nodos de los otros grupos de nodos activos en orden de prioridad. Si un grupo de nodos tiene un recuento de nodos superior o igual, ese grupo de nodos se activa operacionalmente. De lo contrario, se comprueban los grupos de nodos de repuesto.

> **Nota**
>
> - Solo un grupo de nodos específico de estado puede estar activo en un punto determinado en el tiempo.
> - Un nodo de clúster hereda el estado del grupo de nodos. Por lo tanto, si un nodo con el estado "SPARE" se agrega al grupo de nodos con el estado "ACTIVO", el nodo se comporta automáticamente como un nodo activo.
> - El parámetro de preferencia definido para la instancia de clúster decide si el grupo de nodos activo inicial toma el control cuando vuelva a aparecer.
> - Un grupo de nodos de reserva puede ocupar un grupo de nodos y alojar tráfico activo cuando un grupo de nodos activo se desactiva.

En la siguiente ilustración se muestra una configuración de grupo de nodos que tiene definida la redundancia de grupo de nodos. NG1 es inicialmente el grupo de nodos activo. Cuando pierde uno de los nodos, el grupo de nodos de repuesto (NG3) con la prioridad más alta comienza a servir el tráfico.

Ilustración 1. Clúster de Citrix ADC con redundancia de grupo de nodos configurada.



Configuración de redundancia para grupos de nodos

1. Inicie sesión en la dirección IP del clúster.
2. Cree el grupo de nodos activo y enlazar los nodos de clúster necesarios.

```
1 > add cluster nodegroup NG1 -state ACTIVE
2 > bind cluster nodegroup NG1 -node n1
3 > bind cluster nodegroup NG1 -node n2
4 > bind cluster nodegroup NG1 -node n3
```

3. Cree el grupo de nodos de repuesto y vincule los nodos necesarios.

```
1 > add cluster nodegroup NG2 -state SPARE -priority 20
2 > bind cluster nodegroup NG2 -node n4
3 > bind cluster nodegroup NG2 -node n5
4 > bind cluster nodegroup NG2 -node n6
```

4. Cree otro grupo de nodos de repuesto y vincule los nodos necesarios.


```
> add cluster nodegroup NG3 -state SPARE -priority 10
> bind cluster nodegroup NG3 -node n7
> bind cluster nodegroup NG3 -node n8
> bind cluster nodegroup NG3 -node n9
```

Desactivación de la dirección en el plano anterior del clúster

January 12, 2021

> **Nota**
>
> Compatible con NetScaler 11 en adelante.

El comportamiento predeterminado de un clúster de Citrix ADC es dirigir el tráfico que recibe (receptor de flujo) a otro nodo (procesador de flujo). A continuación, el procesador de flujo debe procesar el tráfico. Este proceso de dirigir el tráfico desde el receptor de flujo al procesador de flujo se produce sobre el backplane del clúster y se denomina dirección.

Si es necesario, puede desactivar la dirección para que el proceso se vuelva local para el receptor de flujo y, por lo tanto, haga que el receptor de flujo sea el procesador de flujo. Tal configuración de configuración puede ser útil cuando se tiene un enlace de alta latencia.

> **Nota**
>
> Esta configuración solo es aplicable a los servidores virtuales seccionados.

- Para servidores virtuales parcialmente sectados, si el receptor de flujo es un nodo que no es propietario, el tráfico se dirige a un nodo propietario. Sin embargo, si el receptor de flujo es un nodo propietario, entonces la dirección está desactivada.
- Para los servidores virtuales detectados, el receptor de flujo es el procesador de flujo y, por lo tanto, no hay necesidad de dirección.

Algunos puntos a recordar al desactivar el mecanismo de dirección:

- Los SNIP rayados no son compatibles ya que la dirección está desactivada.
- MPTCP y FTP no funcionan.
- El modo L2 debe estar inhabilitado.
- Si USIP está habilitado, es posible que el tráfico no llegue al mismo nodo que la dirección está desactivada.
- El tráfico que se dirige a la dirección IP del clúster se dirige al coordinador de configuración.
- Cuando un nodo se une o sale de un clúster, es posible que se vean afectadas más de 1/N conexiones. Esto se debe a que un cambio en los nodos disponibles, puede hacer que las rutas se

vuelvan a cifrar. Como resultado, el tráfico se enruta a otro nodo y debido a la no disponibilidad de la dirección, el tráfico no se procesa.

La dirección se puede desactivar en el nivel de servidor virtual individual o en el nivel global. La configuración global tiene prioridad sobre la configuración del servidor virtual.

- Desactivación de la dirección del backplane para todos los servidores virtuales seccionados

  Configurado en el nivel de instancia de clúster. El tráfico destinado a cualquier servidor virtual seccionado no se dirige en el plano posterior del clúster.

  ```
  add cluster instance \<clId\> -processLocal ENABLED<!--NeedCopy-->
  ```

- Desactivación de la dirección del backplane para un servidor virtual seccionado específico

  Configurado en un servidor virtual seccionado. El tráfico destinado al servidor virtual no se dirige en el plano posterior del clúster.

  ```
  add lb vserver <name> <serviceType> -processLocal ENABLED<!--NeedCopy
  -->
  ```

Sincronización de configuraciones de clúster

December 2, 2021

Las configuraciones de Citrix ADC que están disponibles en el coordinador de configuración se sincronizan con los demás nodos del clúster cuando:

- Un nodo se une al clúster
- Un nodo vuelve a unirse al clúster
- Se ejecuta un nuevo comando a través de la dirección IP del clúster

Además, puede sincronizar de manera forzada las configuraciones que están disponibles en el coordinador de configuración (sincronización completa) con un nodo de clúster específico. Asegúrese de sincronizar un nodo de clúster a la vez, de lo contrario, el clúster puede verse afectado.

Para sincronizar las configuraciones del clúster mediante la CLI:

En el símbolo del sistema del dispositivo en el que quiere sincronizar las configuraciones, escriba:

```
1 force cluster sync
```

Para sincronizar las configuraciones del clúster mediante la GUI:

1. Inicie sesión en el dispositivo en el que quiere sincronizar las configuraciones.
2. Vaya a **Sistema > Clúster.**

3. En el panel de detalles, en **Utilidades**, haga clic en Forzar sincronización de clústeres.
4. Haga clic en **Aceptar.**

Mostrar la lista de comandos que fallaron durante la sincronización de la configuración del clúster

En una configuración de clúster, con el modo estricto de estado de sincronización `syncStatusStrictMode` habilitado, puede mostrar la lista de comandos que fallaron durante la sincronización de un clúster en un nodo que no sea CCO.

Puede determinar el estado de sincronización del clúster de un nodo que no sea de CCO ejecutando la operación `show node`. `PARTIAL SUCCESS` El estado de sincronización indica que algunos comandos fallaron en el nodo no CCO durante la sincronización del clúster.

Para ver la lista de comandos que fallaron en un nodo durante la sincronización del clúster mediante la CLI:

- `show cluster syncFailures`

Configuración de ejemplo

```
> show cluster node

1) Node ID: 1
        IP:                   10.102.201.24
        Backplane:            1/1/1
        Health:               UP
        Admin State:          ACTIVE
        Operational State:    ACTIVE(Configuration Coordinator)
        Sync State:           ENABLED
        Priority:             31
        Tunnel Mode:          NONE
        Node Group:           DEFAULT_NG
2) Node ID: 2
        IP:                   10.102.201.62*
        Backplane:            2/1/1
        Health:               UP
        Admin State:          ACTIVE
        Operational State:    ACTIVE
        Sync State:           PARTIAL SUCCESS
(Refer the files clus_sync_batch_status.log, sync_route_status.log
   and sync_clusdiff_status.log in /var/nssynclog directory for
   list of commands failed)
        Priority:             31
```



```
22              Tunnel Mode:          NONE
23              Node Group:           DEFAULT_NG
24      3) Node ID: 3
25              IP:                   10.102.201.64
26              Backplane:            3/1/1
27              Health:               UP
28              Admin State:          ACTIVE
29              Operational State:    ACTIVE
30              Sync State:           PARTIAL SUCCESS
31      (Refer the files clus_sync_batch_status.log, sync_route_status.log
           and sync_clusdiff_status.log in /var/nssynclog directory for
           list of commands failed)
32              Priority:             31
33              Tunnel Mode:          NONE
34              Node Group:           DEFAULT_NG
35      Done
36
37      > show cluster syncFailures
38
39      exec: add system user nsroot "********" -encrypted -externalAuth
           ENABLED -timeout 900 -logging ENABLED -maxsession 20 -
           allowedManagementInterface CLI API -devno 32768
40      ERROR: Resource already exists
41      --
42      exec: set interface 2/LO/1 -autoneg ENABLED -haMonitor OFF -
           haHeartbeat OFF -mtu 1500 -ringtype Elastic -tagall OFF -
           trunkmode OFF -state ENABLED -lagtype NODE -lacpPriority 32768 -
           lacpTimeout LONG -throughput 0 -linkRedundancy OFF -
           bandwidthHigh 0 -bandwidthNormal 0 -intftype Loopback -svmCmd 0
           -ifnum 2/LO/1 -lldpmode NONE -lrsetPriority 1024
43      ERROR: Operation not allowed on loopback interface.
```

Sincronización del tiempo entre nodos del clúster

January 12, 2021

El clúster utiliza un protocolo de tiempo de precisión (PTP) para sincronizar el tiempo entre nodos del clúster. PTP utiliza paquetes de multidifusión para sincronizar la hora. Si hay algunos problemas en la sincronización de tiempo, debe inhabilitar PTP y configurar el Protocolo de hora de red (NTP) en el clúster.

Para habilitar/inhabilitar PTP mediante la interfaz de línea de comandos

En el símbolo del sistema de la dirección IP del clúster, escriba:

```
set ptp -state disable
```

Para activar/inhabilitar PTP mediante la utilidad de configuración

1. Inicie sesión en la dirección IP del clúster.
2. Vaya a **Sistema > Clúster.**
3. En el panel de detalles, en **Utilidades**, haga clic en **Configurar configuración de PTP.**
4. En el cuadro de diálogo **Habilitar/Desactivar PTP**, seleccione si quiere habilitar o inhabilitar PTP.
5. Haga clic en **Aceptar.**

Sincronización de archivos de cluster

October 5, 2021

Los archivos disponibles en el coordinador de configuración se denominan archivos de clúster. Estos archivos se sincronizan automáticamente en los demás nodos del clúster cuando el nodo se agrega al clúster y periódicamente, durante la vida útil del clúster. Además, puede sincronizar manualmente los archivos del clúster.

Importante: La eliminación de cualquier certificado o archivo de clave en un entorno de clúster restringe la configuración adicional del dispositivo ADC. Vuelva a agregar los archivos en la misma ubicación para realizar cualquier cambio de configuración.

Los directorios y archivos del coordinador de configuración que se sincronizan son:

- /nsconfig/ssl/
- /var/netscaler/ssl/
- /var/vpn/marcador/
- /nsconfig/dns/
- /nsconfig/monitores/
- /nsconfig/nstemplates/
- /nsconfig/ssh/
- /nsconfig/rc.netscaler
- /nsconfig/resolv.conf
- /nsconfig/inetd.conf

- /nsconfig/syslog.conf
- /nsconfig/snmpd.conf
- /nsconfig/ntp.conf
- /nsconfig/httpd.conf
- /nsconfig/sshd_config
- /nsconfig/hosts
- /nsconfig/enckey
- /var/nslw.bin/etc/krb5.conf
- /var/nslw.bin/etc/krb5.keytab
- /var/lib/análoga/db/
- /var/descargar/
- /var/wi/tomcat/webapps/
- /var/es/tomcat/conf/catalina/localhost/
- /var/wi/java_home/lib/seguridad/cacerts
- /var/wi/java_home/jre/lib/seguridad/cacerts
- /nsconfig/licencia/
- /nsconfig/rc.conf

> **Sugerencia**
>
> Los archivos (certificados y archivos de claves) que se copian en el coordinador de configuración del clúster manualmente (o a través del shell) no están disponibles automáticamente en los demás nodos del clúster. Ejecute el comando "sync cluster files" desde la dirección IP del clúster antes de ejecutar un comando que dependa de estos archivos.

Para sincronizar archivos de clúster mediante la interfaz de línea de comandos

En el símbolo del sistema de la dirección IP del clúster, escriba:

```
sync cluster files <mode>
```

Para sincronizar archivos de clúster mediante la utilidad de configuración

1. Inicie sesión en la dirección IP del clúster.
2. Vaya a **Sistema > Clúster.**
3. En el panel de detalles, en **Utilidades**, haga clic en Sincronizar archivos de clúster.
4. En el cuadro de diálogo **Sincronizar** archivos de clúster, seleccione los archivos que se van a sincronizar en la lista desplegable Modo.
5. Haga clic en **Aceptar.**

Visualización de las estadísticas de un clúster

August 20, 2021

Puede ver las estadísticas de una instancia de clúster y de los nodos de clúster para evaluar el rendimiento o solucionar problemas del funcionamiento del clúster.

Para ver las estadísticas de una instancia de clúster mediante la interfaz de línea de comandos

En el símbolo del sistema de la dirección IP del clúster, escriba:

```
1 stat cluster instance <clId>
```

Para ver las estadísticas de un nodo de clúster mediante la interfaz de línea de comandos

En el símbolo del sistema de la dirección IP del clúster, escriba:

```
1 stat cluster node <nodeid>
```

> **Nota**
>
> El `stat cluster node <nodeid>` comando muestra las estadísticas de nivel de clúster cuando se ejecuta el comando desde la dirección IP del clúster. Sin embargo, cuando se ejecuta desde la dirección NSIP de un nodo de clúster, el comando muestra estadísticas de nivel de nodo.

Para ver las estadísticas de una instancia de clúster mediante la utilidad de configuración

1. Inicie sesión en la dirección IP del clúster.
2. Vaya a **Sistema > Clúster.**
3. En el panel de detalles, en el centro de la página, haga clic en **Estadísticas.**

Para ver las estadísticas de un nodo de clúster mediante la utilidad de configuración

1. Inicie sesión en la dirección IP del clúster.

2. Vaya a **Sistema > Clúster > Nodos.**
3. En el panel de detalles, seleccione un nodo y haga clic en **Estadísticas** para ver las estadísticas del nodo. Para ver las estadísticas de todos los nodos, haga clic en **Estadísticas** sin seleccionar un nodo específico.

Descubrimiento de dispositivos Citrix ADC

August 20, 2021

Puede detectar los dispositivos presentes en la misma subred que el nodo actual. Los dispositivos detectados necesarios se pueden agregar selectivamente al clúster. Esta operación se puede realizar para crear un clúster o para agregar nodos a un clúster existente.

> **Nota**
>
> - La operación de detección solo se puede realizar a través de la utilidad de configuración.
> - Esta operación no puede detectar dispositivos Citrix ADC de diferentes redes.
> - Al realizar esta operación para agregar nodos a un clúster existente, las configuraciones de VLAN L3 se borran del nodo. Asegúrese de definir estas configuraciones una vez que el dispositivo se haya agregado al clúster.

Para descubrir dispositivos mediante la interfaz gráfica de usuario

1. Inicie sesión en la dirección IP del clúster.
2. Vaya a **Sistema > Clúster > Nodos.**
3. En el panel de detalles, en la parte inferior de la página, haga clic en **Descubrir NetScalers.**
4. En el cuadro de diálogo **Detectar NetScalers**, defina los siguientes parámetros:
   - **Intervalo de direcciones IP**: Especifique el rango de direcciones IP dentro del cual quiere detectar dispositivos. Por ejemplo, puede buscar todas las direcciones NSIP entre 10.102.29.4 y 10.102.29.15 especificando esta opción como 10.102.29.4: 15.
   - **Interfaz de plano posterior**: Especifique las interfaces que se utilizarán como interfaz de plano posterior. Es un parámetro opcional. Si no especifica este parámetro, debe actualizarlo después de agregar el nodo al clúster.
5. Haga clic en **Aceptar.**
6. Seleccione los dispositivos que quiera agregar al clúster.
7. Haga clic en **Aceptar.**

Inhabilitar un nodo de clúster

August 20, 2021

Puede quitar temporalmente un nodo de un clúster inhabilitando la instancia de clúster en ese nodo. Un nodo inhabilitado no se sincroniza con las configuraciones del clúster. Cuando el nodo se vuelve a habilitar, las configuraciones del clúster se sincronizan automáticamente en él. Para obtener más información, consulte Sincronización entre nodos de clúster.

Un nodo inhabilitado no puede servir tráfico y se terminan todas las conexiones existentes en este nodo.

> **Nota**
>
> Si se modifican las configuraciones de un nodo de coordinador no de configuración inhabilitado (a través de la dirección NSIP del nodo), las configuraciones no se sincronizan automáticamente en ese nodo. Puede sincronizar manualmente las configuraciones tal y como se describe en Sincronización de configuraciones de clúster.

Para inhabilitar un nodo de clúster mediante la interfaz de línea de comandos

En el símbolo del sistema del nodo que quiere inhabilitar, escriba:

```
disable cluster instance <clId>
```

> **Nota**
>
> Para inhabilitar el clúster, ejecute el comando
> disable cluster instance en la dirección IP del clúster.

Para inhabilitar un nodo de clúster mediante la utilidad de configuración

1. En el nodo que quiere inhabilitar, vaya a **Sistema > Cluster** y haga clic en **Administrar clúster.**
2. En el cuadro de diálogo **Configurar** instancia de clúster, desactive la casilla de verificación **Habilitar** instancia de clúster.

   > **Nota**
   >
   > Para inhabilitar la instancia de clúster en todos los nodos, realice el procedimiento anterior en la dirección IP del clúster.

Eliminación de un nodo de clúster

August 20, 2021

Cuando se quita un nodo del clúster, las configuraciones del clúster se borran del nodo (ejecutando internamente el comando clear ns config -extended). Las direcciones SNIP, la configuración de **MTU** de la interfaz del plano posterior y todas las configuraciones de VLAN (excepto la VLAN y NSVLAN predeterminadas) también se borran del dispositivo.

> **Nota**
>
> - Si el nodo eliminado era el coordinador de configuración del clúster (CCO), se selecciona automáticamente otro nodo como CCO y la dirección IP del clúster se asigna a ese nodo. Todas las sesiones actuales de dirección IP del clúster no son válidas y debe iniciar una nueva sesión.
> - Para eliminar todo el clúster, debe quitar cada nodo individualmente. Al quitar el último nodo, se eliminan las direcciones IP del clúster.
> - Cuando se quita un nodo activo, la capacidad de servicio de tráfico del clúster se reduce en un nodo. Las conexiones existentes en este nodo finalizan.

Para quitar un nodo de clúster mediante la CLI

Para NetScaler 10.1 y versiones posteriores

1. Inicie sesión en la dirección IP del clúster y, en el símbolo del sistema, escriba:

```
rm cluster node <nodeId>

save ns config
```

2. Inicie sesión en el nodo eliminado, la dirección NSIP y, en el símbolo del sistema, escriba:

```
save ns config
```

> **Nota**
>
> Si no se puede acceder a la dirección IP del clúster desde el nodo, ejecute el comando rm cluster instance en la dirección NSIP de ese nodo.

Para NetScaler 10

1. Inicie sesión en el nodo que quiere quitar del clúster y quite la referencia a la instancia del clúster.

```
rm cluster instance <clId>

save ns config
```

2. Inicie sesión en la dirección IP del clúster y quite el nodo del que ha quitado la instancia del clúster.

```
rm cluster node <nodeId>

save ns config
```

   Asegúrese de que no ejecuta el `rm cluster node` comando desde el nodo local. Esto da como resultado configuraciones incoherentes entre el CCO y el nodo.

Para quitar un nodo de clúster mediante la GUI

En la dirección IP del clúster, vaya a **Sistema > Cluster > Nodos**, seleccione el nodo que quiere quitar y haga clic en **Quitar.**

Quitar un nodo de un clúster implementado mediante la agregación de vínculos de clúster

August 20, 2021

Para quitar un nodo de un clúster que utiliza la agregación de vínculos de clúster como mecanismo de distribución de tráfico, debe asegurarse de que el nodo se convierte en pasivo para que no reciba ningún tráfico y, a continuación, en el conmutador ascendente, quite la interfaz correspondiente del canal.

Para obtener información detallada sobre la agregación de vínculos de clúster, consulte Uso de la agregación de vínculosde clú

Para quitar un nodo de un clúster que utiliza la agregación de vínculos de clúster como mecanismo de distribución de tráfico

1. Inicie sesión en la dirección IP del clúster.
2. Establezca el estado del nodo del clúster que quiere quitar en PASIVO.

```
set cluster node <nodeId> -state PASSIVE
```

3. En el conmutador ascendente, elimine la interfaz correspondiente del canal mediante comandos específicos del conmutador.

> **Nota**
>
> No es necesario quitar manualmente la interfaz de nodos en el canal de agregación de vínculos de clúster. Se elimina automáticamente cuando el nodo se elimina en el siguiente paso.

4. Quite el nodo del clúster.

```
rm cluster node <nodeId>
```

Detección de sondeo jumbo en un clúster

August 20, 2021

Si una trama Jumbo está habilitada en una interfaz de clúster, la interfaz del plano posterior debe ser lo suficientemente grande como para admitir todos los paquetes de la trama Jumbo. Se logra configurando la Unidad de Transmisión Máxima (MTU) del plano posterior como:

Backplane_MTU = máximo (todas las MTU de interfaz de clúster) + 78

Para verificar la configuración anterior, debe enviar un sondeo jumbo (del tamaño computacional anterior) a todos los nodos del mismo nivel de una configuración de clúster. Si el sondeo no se realiza correctamente, el dispositivo muestra un mensaje de advertencia en la salida del comando “show cluster instance”.

En el modo de interfaz de comandos, escriba el siguiente comando:

```
> show cluster instance
  Cluster ID: 1
```



```
3       Dead Interval: 3 secs
4       Hello Interval: 200 msecs
5       Preemption: DISABLED
6       Propagation: ENABLED
7       Quorum Type: MAJORITY
8       INC State: DISABLED
9       Process Local: DISABLED
10      Cluster Status: ENABLED(admin),    ENABLED(operational), UP
```

> **Advertencia**
>
> La MTU para una interfaz de backplane debe ser lo suficientemente grande como para manejar todos los paquetes en la trama. Debe ser igual a <MTU_VAL>. Si el valor recomendado no es configurable por el usuario, debe revisar el valor MTU de las interfaces jumbo.

Sl. no	Nodos de miembro	Estado	Estado de administración	Estado de la operación
1	ID del nodo: 1; Nodo IP: 10.102.53.167	ACTIVO	Active	ACTIVE (Coordinador de configuración)
2	ID del nodo: 2; Nodo IP: 10.102.53.168	ACTIVO	Active	Active

Supervisión de rutas para rutas dinámicas en clúster

August 20, 2021

Puede utilizar un monitor de rutas para hacer que un nodo de clúster dependa de la tabla de redirección interna, ya sea que contenga o no una ruta aprendida dinámicamente. Un monitor de ruta en cada nodo comprueba la tabla de redirección interna para asegurarse de que hay una entrada de ruta para llegar a una red determinada siempre presente. Si la entrada de ruta no está presente, el estado del monitor de ruta cambia a DOWN.

En una implementación de clúster, si el vínculo lateral del cliente o del servidor de un nodo falla, el tráfico se dirige a este nodo a través de los nodos del mismo nivel para su procesamiento. La dirección del tráfico se implementa configurando el redirección dinámica y agregando entradas ARP estáticas, apuntando a la dirección MAC especial de cada nodo, en todos los nodos. Si hay muchos nodos en una implementación de clúster, agregar y administrar entradas ARP estáticas con direcciones MAC

especiales en todos los nodos es una tarea engorrosa. Ahora, los nodos usan implícitamente direcciones MAC especiales para paquetes de dirección. Por lo tanto, ya no es necesario agregar entradas ARP estáticas que apunten a direcciones MAC especiales a los nodos del clúster.

Para enlazar un nodo de clúster mediante la CLI

En el símbolo del sistema, escriba:

```
bind cluster node <nodeId> (-routeMonitor <ip_addr|ipv6_addr|*> [<
    netmask>])
unbind cluster node <nodeId> (-routeMonitor <ip_addr|ipv6_addr|*> [<
    netmask>])
```

Considere un caso en el que el nodo 1 está enlazado al monitor de ruta 1.1.1.0 255.255.255.0. Cuando falla una ruta dinámica, el nodo 1 se convierte en INACTIVE. El estado de mantenimiento está disponible en el `show cluster node` comando por id de nodo como se indica a continuación.

```
Node ID: 1
IP:  10.102.169.96
Backplane:  1/1/2
Health: NOT UP
Reason(s): Route Monitor(s) of the node have failed
Route Monitor -  Network: 1.1.1.0   Netmask: 255.255.255.0   State:
    DOWN
```

Supervisión de la configuración del clúster mediante SNMP MIB con enlace SNMP

August 20, 2021

SNMP MIB es información específica del dispositivo que se configura en el agente SNMP para identificar un dispositivo Citrix ADC. Puede identificar información como, por ejemplo, el nombre del dispositivo, el administrador y la ubicación. En una configuración de clúster, ahora puede configurar la MIB SNMP en cualquier nodo incluyendo el parámetro “OwnerNode” en el comando set SNMP MIB. Sin este parámetro, el comando set SNMP MIB solo se aplica al nodo Coordinador de clústeres (CCO).

Para mostrar la configuración MIB para un nodo de clúster distinto del CCO, incluya el parámetro “OwnerNode” en el comando show SNMP MIB.

Configuración de SNMP MIB en CLIP

Para configurar y ver la configuración de MIB en CLIP mediante la interfaz de línea de comandos.

```
set snmp mib [-contact <string>] [-name <string>] [-location <string>]
      [-customID <string>] [-ownerNode <positive_integer>]
Done
show snmp mib [-ownerNode <positive_integer>]

 > set mib -contact John -name NS59 -location San Jose -customID 123 -
    ownerNode 3
Done
> sh mib -ownerNode 3
        --------------------
         Cluster Node ID: 3
        --------------------
        NetScaler system MIB:
        sysDescr:    NetScaler NS11.1: Build 46.4.a.nc, Date: Jun  7
           2016, 10:27:29
        sysUpTime:   124300
        sysObjectID: .1.3.6.1.4.1.5951.1.1
        sysContact:  John
        sysName:     NS59
        sysLocation: San Jose
        sysServices: 72
        Custom ID: 123
 Done

> unset mib -contact -name -location -customID -ownerNode 3
 Done
> sh mib -ownerNode 3
        --------------------
         Cluster Node ID: 3
        --------------------
        NetScaler system MIB:
        sysDescr:    NetScaler NS11.1: Build 46.4.a.nc, Date: Jun 7
           2016, 10:27:29
        sysUpTime:   146023
        sysObjectID: .1.3.6.1.4.1.5951.1.1
        sysContact:  WebMaster (default)
        sysName:     NetScaler
        sysLocation: POP (default)
        sysServices: 72
        Custom ID: Default
```



```
38  Done
```

Mensajes de captura SNMP de clúster

En la configuración del clúster, las configuraciones de alarma de captura SNMP deben realizarse desde el CLIP. Los comandos se propagan a cada uno de los nodos.

Para obtener más información sobre la configuración de SNMP, consulte Configuración de Citrix ADC para generar capturas SNMP.

Las siguientes son las capturas específicas del clúster que están disponibles:

```
1   >sh snmp alarm | grep cluster
2       CLUSTER-BACKPLANE-HB-MISSING N/A N/A 86400   ENABLED - ENABLED
3       CLUSTER-CCO-CHANGE N/A N/A N/A ENABLED - ENABLED
4       CLUSTER-NODE-HEALTH N/A N/A 86400 ENABLED - ENABLED
5       CLUSTER-NODE-QUORUM N/A N/A 86400 ENABLED - ENABLED
6       CLUSTER-OVS-CHANGE N/A N/A N/A ENABLED - ENABLED
7       CLUSTER-PROP-FAILURE N/A N/A N/A ENABLED - ENABLED
8       CLUSTER-SYNC-FAILURE N/A N/A N/A ENABLED - ENABLED
9       CLUSTER-SYNC-PARTIAL-SUCCESS N/A N/A N/A ENABLED - ENABLED
10      CLUSTER-VERSION-MISMATCH N/A N/A 86400 ENABLED - ENABLED
```

Supervisión de errores de propagación de comandos en una implementación de clúster

January 12, 2021

En una implementación de clúster, puede utilizar el nuevo comando “show prop status” para supervisar y solucionar problemas más rápidos. Los problemas relacionados con el error de propagación de comandos en nodos que no son de CCO. Este comando muestra hasta 20 de los errores de propagación de comandos más recientes en todos los nodos que no son CCO. Puede utilizar la CLI o la GUI del dispositivo Citrix ADC para realizar esta operación. Puede acceder a ellos a través de la dirección CLIP o a través de la dirección NSIP de cualquier nodo de la implementación del clúster.

Apagado estable de nodos

August 20, 2021

En una configuración de clúster, se pierden algunas de las conexiones existentes (1/Nth conexiones, donde N es el tamaño del clúster) en el nivel de clúster o en el nivel de servidor virtual específico. Este comportamiento se observa si un nodo sale o se une al sistema. Para hacer frente a la pérdida, debe manejar con gracia las conexiones existentes. El manejo elegante se realiza configurando la opción "Retener conexiones en clúster" en la dirección CLIP y especificando un intervalo de tiempo de espera en el NSIP del nodo.

El manejo correcto de las conexiones es aplicable en dos casos:

1. Actualización del clúster
2. Nueva adición de nodo

Manejo sencillo de nodos en la actualización del clúster

Para actualizar un clúster, debe actualizar un nodo a la vez. Antes de actualizar un nodo, debe establecerlo en estado pasivo y, a continuación, establecerlo en estado activo después de la actualización. Para evitar terminar las conexiones existentes al actualizar el nodo, apáguelo correctamente con un intervalo de tiempo de espera configurado. De lo contrario, se termina la 1/N (donde N es el tamaño del clúster) de las conexiones del clúster.

> **Nota**
>
> Si las sesiones existentes no se completan dentro del intervalo de tiempo de espera configurado, se terminan después del tiempo de gracia.

Los siguientes son los pasos para manejar correctamente los nodos en un caso de actualización de clúster:

1. Considere una configuración de clúster de cinco nodos (n0, n1, n2, n3, n4).
2. Antes de apagar un nodo, debe configurar la opción "RetainConnectionsOnCluster" opción. Ayuda a conservar todas las conexiones existentes de este nodo a nivel de clúster o servidor virtual durante un intervalo de tiempo específico.

   Ejemplo

   On CLIP

   "'set cluster instance –retainConnectionsOnCluster YES

```
O BIEN

```set lb vserver <vserver name>  - retainConnectionsOnCluster Yes
   <!--NeedCopy-->
```


```

3. Ahora, inicie sesión en la dirección NSIP del nodo n3 y establezca el nodo n3 en PASIVO con un tiempo de espera interno.

   **Ejemplo**

   "'set cluster node n3 –state PASSIVE –delay 60

```
1 ```saveconfig<!--NeedCopy-->
```

4. Una vez que expire el período de gracia, cierre todas las conexiones, cierre n3 y reinicie el dispositivo Citrix ADC.
5. Actualice el dispositivo. A continuación, con la CLI conectada a la dirección NSIP del dispositivo, establezca el nodo en ACTIVE.

   Ejemplo

   "'set cluster node n3 –state ACTIVE

```
1 ```saveconfig<!--NeedCopy-->
```

6. Repita los pasos 4 a 6 para todos los nodos del clúster.
7. Después de actualizar todos los nodos y establecer en ACTIVE, restablezca la opción RetainConnectionSonCluster desde la dirección CLIP.

   Ejemplo

   "'set cluster instance -retainConnectionsOnCluster NO

```
1 O BIEN
2
3 ```set lb vserver <vserver name>  - retainConnectionsOnCluster NO
     <!--NeedCopy-->
```

> **Nota**
>
> Si hay una discrepancia de versión al actualizar un clúster, la propagación del clúster se inhabilita automáticamente y no se permite ningún comando en el CLIP.

Manejo elegante de nodos durante una adición de nodos nuevos

La gestión elegante de los nodos describe cómo se puede agregar un nuevo nodo al clúster de Citrix ADC existente. Tenga en cuenta que tiene un clúster de Citrix ADC que ya está sirviendo tráfico. Además, quiere agregar un dispositivo adicional como nodo al clúster sin terminar sus conexiones existentes. Para llevar a cabo el caso anterior, establezca la opción de conservar las conexiones existentes en un nivel global o en un nivel de servidor virtual específico. Una vez hecho esto, guarde la configuración. Ahora establezca la opción de conservar las conexiones en NO, para permitir que las conexiones existentes de otros nodos se reasignen al nuevo nodo.

Los siguientes son los pasos para manejar correctamente los nodos si un nodo recién agregado:

1. Guarde la configuración existente que tiene habilitada la opción “RetainConnectionSonCluster”. Al hacerlo, puede conservar todas las conexiones existentes de este nodo a nivel de clúster o servidor virtual durante un intervalo de tiempo específico.

   On CLIP

   ```
   set cluster instance x - retainConnectionsOnCluster YES
   ```

   O BIEN

   ```
   set lb vserver xxxx -retainConnectionsOnCluster Yes
   ```

2. Agregue un nodo ‘n5’ a la configuración del clúster.
3. Inhabilite la opción “RetainConnectionOnCluster” en “NO” para distribuir conexiones existentes desde otros nodos al nodo n5 recién agregado.

   On CLIP

   ```
   set cluster instance x - retainConnectionsOnCluster NO
   ```

   O BIEN

   ```
   set lb vserver xxxx -retainConnectionsOnCluster NO
   ```

> **Nota**
>
> La dirección del plano posterior depende del tipo de mecanismo de distribución de tráfico (ECMP, CLAG y USIP) en una configuración de clúster. El aumento en la dirección del backplane se basa

> en el tipo de tráfico.

Configurar el apagado correcto de nodos en un clúster

Para configurar el apagado correcto de nodos en un clúster, haga lo siguiente:

1. Configure la opción “RetainConnectionsOnCluster” en el nivel Global (clúster).
2. Configure la opción “RetainConnectionsOnCluster” en el nivel del servidor virtual.
3. Establezca el nodo (dejando el sistema) en el estado pasivo con un intervalo de tiempo de espera correcto especificado en la dirección NSIP del nodo.
4. Supervisar las conexiones existentes para asegurarse de que todas las transacciones se completan dentro del período de gracia.

Para conservar las conexiones existentes en el nivel global (clúster) mediante la CLI

Puede conservar las conexiones existentes en un nivel global o en un nivel de servidor virtual específico. Esta opción está configurada para conservar todas las conexiones existentes a nivel global. De forma predeterminada, esta opción está inhabilitada.

En el símbolo del sistema, escriba:

```
1 - set cluster instance <clusterID> - retainConnectionsOnCluster YES
2
3 - set cluster instance 60 - retainConnectionsOnCluster YES
```

Para conservar las conexiones existentes de un servidor virtual específico en el clúster mediante la CLI

Esta opción está configurada para conservar las conexiones existentes específicas de un servidor virtual de equilibrio de carga. Para conservar esas conexiones, habilitamos esta opción en el nivel del servidor virtual. De forma predeterminada, esta opción está inhabilitada.

En el símbolo del sistema, escriba:

```
1 - set lb vserver <clusterID> - retainConnectionsOnCluster Yes
2
3 - set lb vserver v1 - retainConnectionsOnCluster Yes
```


Para establecer un nodo de clúster en estado pasivo mediante la CLI

Para establecer un nodo de clúster en estado pasivo con un intervalo de tiempo de espera elegante. Esta configuración se realiza en el NSIP del nodo ya que la propagación se inhabilita durante la actualización del clúster.

En el símbolo del sistema, escriba:

```
-  set cluster node <clusterID> -state passive
-backplane <interface_name>@
-priority <positive_integer>
-delay <mins>

-  set cluster node 4  - state PASSIVE -delay 60

-  set cluster instance 60  -  retainConnectionsOnCluster YES
-  set lb vserver v1  - retainConnectionsOnCluster Yes
-  set cluster node 4  - state PASSIVE -delay 60
```

> **Nota**
>
> Puede observar el siguiente comportamiento en un nodo de clúster cuando se establece en pasivo con una opción de demora configurada desde un CLIP:
>
> - Después del tiempo de espera, el nodo se muestra como pasivo desde el NSIP del nodo.
> - El comando **show cluster instance** en CLIP muestra el nodo como activo desde el CLIP. Mientras que el comando **show cluster node** del CLIP muestra el nodo como pasivo.

Para configurar el apagado correcto de los nodos mediante la interfaz gráfica de usuario

1. Vaya a **Configuración > Sistema > Cluster** y haga clic en **Administrar clúster.**
2. En la página **Administrar clúster**, seleccione la opción **Retener conexiones en clúster**.
3. Haga clic en **Aceptar** y, a continuación, haga clic en **Listo**.

Apagado estable de los servicios

August 20, 2021

A partir de NetScaler 12.1, compilación 49.xx, los clústeres Citrix ADC admiten el apagado correcto de los servicios. Para cerrar correctamente los servicios, puede realizar una de las siguientes tareas.

- Inhabilite explícitamente el servicio y

- Establezca un retraso (en segundos).
- Habilite el apagado correcto.

- Agregue un código o una cadena TROFS al monitor.

Para obtener más información, consulte Cierre correcto de los servicios.

Para configurar el apagado correcto para un servicio mediante la CLI

Inhabilitar solo con la opción graciosa:

En el símbolo del sistema, escriba:

```
disable service <name> [-graceFul (YES|NO)]

show service <name>
<!--NeedCopy-->
```

Ejemplo

```
disable service svc1 -graceFul YES
Done
sh service svc1
                svc1 (10.102.225.11:80) - HTTP
                State: GOING OUT OF SERVICE   Graceful (number of
                   active clients: 1)
                Last state change was at Wed Jul 25 10:46:29 2018
                Time since last state change: 0 days, 00:00:02.680
                ... ... ... .
                ... ... ... .
                Traffic Domain: 0

1)            Monitor Name: tcp-default
                                State: UP              Weight: 1
                                                Passive: 0
                                Probes: 26            Failed [Total: 0
                                   Current: 0]
                                Last response: Success - TCP syn+ack
                                   received.
                                Response Time: 0.0 millisec
<!--NeedCopy-->
```

Inhabilitar con tiempo de espera y opción graciosa:

En el símbolo del sistema, escriba:

```
disable service <name> [<delay>] [-graceFul (YES|NO)]

show service <name>
<!--NeedCopy-->
```

Ejemplo

```
disable service svc1 2000 -graceFul YES

Done
> sh service svc1
                svc1 (10.102.225.11:80) - HTTP
                State: GOING OUT OF SERVICE (Graceful (number of active
                    clients: 1), Out Of Service in 1998 seconds)
                Last state change was at Wed Jul 25 10:49:08 2018
                Time since last state change: 0 days, 00:00:01.710
                ... ... ... .
                ... ... ... .
                Traffic Domain: 0

1)            Monitor Name: tcp-default
                                State: UP              Weight: 1
                                                Passive: 0
                                Probes: 57            Failed [Total: 0
                                   Current: 0]
                                Last response: Success - TCP syn+ack
                                   received.
                                Response Time: 0.0 millisec
Done
<!--NeedCopy-->
```

Inhabilitar el grupo de servicios con tiempo de espera y opción graciosa:

En el símbolo del sistema, escriba:

```
disable serviceGroup <serviceGroupName>@ [<serverName>@ <port>] [-delay
<secs>] [-graceFul ( YES | NO )]
Show service group <serviceGroupName>
<!--NeedCopy-->
```


Ejemplo:

```
disable servicegroup sg -delay 2000 -graceFul yes
sh servicegroup sg
                sg - HTTP
                State: DISABLED                Effective State: OUT OF
                   SERVICE Monitor Threshold : 0
                Max Conn: 0       Max Req: 0          Max Bandwidth: 0
                   kbits
                Use Source IP: NO
                Client Keepalive(CKA): NO
                … … … .
                … … …


                1)   200.200.10.21:80       Server Name: server3
                   Server ID: None Weight: 1
                                State:    GOING OUT OF SERVICE (learnt
                                   from node:2 )     Graceful (number
                                   of active clients: 6), Out Of
                                   Service in 1993 seconds
                                Last state change was at Mon Aug 13
                                   15:15:11 2018
                                … … …

                2)   200.200.10.22:80       Server Name: server4
                   Server ID: None Weight: 1
                                State:    GOING OUT OF SERVICE (learnt
                                   from node:2 )     Graceful (number
                                   of active clients: 7), Out Of
                                   Service in 1993 seconds
                                Last state change was at Mon Aug 13
                                   15:15:11 2018
<!--NeedCopy-->
```

> **Nota**
> CLIP muestra el valor agregado de todas las conexiones de clientes activos desde todos los nodos del clúster.

Para configurar el apagado correcto para un servicio mediante la interfaz gráfica de usuario

1. Vaya a **Administración de Tráfico > Equilibrio de carga > Servicios**.

2. Abra el servicio y, en la lista Acciones, haga clic en **Inhabilitar**. Introduzca un tiempo de espera y seleccione Agraciado.

Para configurar un código o una cadena TROFS en un monitor mediante la CLI

En el símbolo del sistema, escriba uno de los siguientes comandos:

```
add lb monitor <monitor-name> HTTP -trofsCode <respcode>
add lb monitor <monitor-name> HTTP-ECV  -trofsString <resp string>
add lb monitor <monitor-name> TCP-ECV  -trofsString <resp string>
<!--NeedCopy-->
```

Para configurar un código o una cadena TROFS en un monitor mediante la interfaz gráfica de usuario

1. Vaya a **Administración del Tráfico > Equilibrio de carga > Monitores**.
2. En el panel Monitores, haga clic en Agregar y siga uno de los pasos siguientes:
   - Seleccione Tipo como HTTP y especifique un código TROFS.
   - Seleccione Tipo como HTTP-ECV o TCP-ECV y especifique una cadena TROFS.

Compatibilidad con logotipos listos para IPv6 para clústeres

August 20, 2021

Puede probar los dispositivos en clúster para la certificación IPv6 Ready Logo. Los comandos modificados para probar protocolos principales IPv6, como para casos de prueba ND, procesamiento de solicitud de enrutador y envío de anuncios de ruta y mensajes de redirección de enrutador están disponibles en una configuración agrupada. A continuación se presentan las funcionalidades IPv6 disponibles para probar los protocolos principales IPv6.

A continuación se presentan las funcionalidades modificadas disponibles para pasar protocolos principales IPv6, tales como casos de prueba ND, procesamiento de solicitud de enrutador y envío de anuncios de ruta y mensajería de redirección de enrutador en el conjunto de pruebas IPv6ReadyLogo phase2.

- Vincular SNIP locales
- Resolución de direcciones e inaccesibilidad del vecino
- Detección de enrutadores y prefijos

- Redirección del router
- Papá

Con estos comandos modificados, se admiten las siguientes configuraciones en un dispositivo agrupado.

Configuraciones compatibles para probar protocolos principales IPv6

Para que una instalación en clúster supere los casos de prueba del logotipo preparado para IPv6, puede ejecutar las siguientes configuraciones en la dirección IP de administración de clústeres (CLIP).

- configuración global de IP6
- configuración básica de IPv6
- más configuraciones IPv6

Configuración global

Una configuración global de IPv6 le permite establecer los parámetros globales de IPv6 (como relearning, RoutereDirection, NdBaseReachTime, nRetransmissionTime `natprefix`„ td y doodad) para ejecutar la configuración básica de IPv6.

En el símbolo del sistema, escriba lo siguiente:

```
set ipv6 [-ralearning ( ENABLED | DISABLED )] [-routerRedirection (
    ENABLED | DISABLED )] [-ndBasereachTime<positive_integer>][-
    ndRetransmissionTime <positive_integer>] [-natprefix <ipv6_addr|*>[-
    td<positive_integer>]] [-doDAD ( ENABLED | DISABLED )]
```

Configuración básica de IPv6

La configuración básica de IPv6 le permite crear una dirección IPv6 y enlazar a una interfaz VLAN. Puede realizar las siguientes configuraciones para probar los protocolos principales IPv6.

Para agregar una VLAN a la instalación en clúster mediante la CLI

En el símbolo del sistema, escriba:

```
add vlan <id>
```

Para agregar otra VLAN a la configuración en clúster mediante la CLI

En el símbolo del sistema, escriba:


```
1 add vlan <id>
```

Para enlazar una interfaz a una VLAN mediante la CLI

En el símbolo del sistema, escriba:

```
1 bind vlan <id> -ifnum <interface_name>
```

Para enlazar una interfaz a una VLAN mediante la CLI

Este comando agrega el prefijo global como prefijo en el enlace a la información de RA para los anuncios de enrutador posteriores. En el símbolo del sistema, escriba:

```
1 bind vlan <id> -ifnum <interface_name>
```

Para agregar la dirección SNIP IPv6 en una VLAN mediante la CLI

En el símbolo del sistema, escriba lo siguiente:

```
1 add ns ip6 <IPv6Address>@ [-scope ( global | link-local )][-type <type>
```

Para agregar la dirección IPv6 en la VLAN mediante la CLI

En el símbolo del sistema, escriba lo siguiente:

```
1 add ns ip6 <IPv6Address>@ [-scope ( global | link-local )][-type <type>
```

Para enlazar la dirección IPv6 a la VLAN mediante la CLI

En el símbolo del sistema, escriba lo siguiente:

```
1 bind vlan <id> [-ifnum <interface_name> [-tagged]][-IPAddress <ip_addr|
     ipv6_addr|
```

Para enlazar la dirección IPv6 a la VLAN mediante la CLI

En el símbolo del sistema, escriba lo siguiente:


```
bind vlan <id> [-ifnum <interface_name> [-tagged]][-IPAddress <ip_addr|
    ipv6_addr|
```

Para mostrar la dirección IPv6 local del vínculo conectada a la VLAN mediante la CLI

En el símbolo del sistema, escriba lo siguiente:

```
sh VLAN
```

Ejemplo 1

```
add vlan 2
add vlan 3
bind vlan 2 -ifnum 1/2
bind vlan 3 -ifnum 1/3
add ip6 fe80::9404:60ff:fedd:a464/64 -vlan 2 -scope link-local -type
    SNIP
add ip6 fe80::c0ee:7bff:fede:263f/64 -vlan 3 -scope link-local -type
    SNIP
add ip6 3ffe:501:ffff:100:9404:60ff:fedd:a464/64 -vlan 2
add ip6 3ffe:501:ffff:101:c0ee:7bff:fede:263f/64 -vlan 3
bind vlan 2 -ipAddress 3ffe:501:ffff:100:9404:60ff:fedd:a464/64
bind vlan 3 -ipAddress 3ffe:501:ffff:101:c0ee:7bff:fede:263f/64
```

Ejemplo 2

```
sh vlan
1)      VLAN ID: 2      VLAN Alias Name:
        Interfaces : 1/6
        IPs :
             3ffe:501:ffff:100:2e0:edff:fe15:ea2a/64
3)      VLAN ID: 3      VLAN Alias Name:
        Link-local IPv6 addr: fe80::9404:60ff:fedd:a464/64
        Interfaces : 1/5
        IPs :
             3ffe:501:ffff:101:2e0:edff:fe15:ea2b/64
 Done
```


Más configuración de clúster IPv6

Para probar los protocolos principales de IPv6, puede utilizar las siguientes configuraciones IPv6 nuevas o modificadas.

Para establecer parámetros de anuncio de enrutador específicos de VLAN mediante la CLI

En el símbolo del sistema, escriba:

```
set nd6RAvariables -vlan <positive_integer> [-ceaseRouterAdv ( YES | NO
    )] [-sendRouterAdv ( YES | NO )] [-srcLinkLayerAddrOption ( YES | NO
     )][-onlyUnicastRtAdvResponse ( YES | NO )] [-managedAddrConfig (
    YES | NO)] [-otherAddrConfig ( YES | NO )] [-currHopLimit <
    positive_integer>][-maxRtAdvInterval <positive_integer>] [-
    minRtAdvInterval<positive_integer>] [-linkMTU <positive_integer>] [-
    reachableTime<positive_integer>] [-retransTime <positive_integer>]
    [-defaultLifeTime<integer>]
```

Para establecer los parámetros configurables de un prefijo global en el enlace mediante la CLI

En el símbolo del sistema, escriba:

```
set onLinkIPv6Prefix <ipv6Prefix> [-onlinkPrefix ( YES | NO )][-
    autonomusPrefix ( YES | NO )] [-depricatePrefix ( YES | NO )][-
    decrementPrefixLifeTimes ( YES | NO )] [-prefixValideLifeTime   <
    positive_integer>] [-prefixPreferredLifeTime <positive_integer>]
```

Para agregar parámetros configurables a un prefijo global en el enlace mediante la CLI

En el símbolo del sistema, escriba:

```
add onLinkIPv6Prefix <ipv6Prefix> [-onlinkPrefix ( YES | NO )][-
    autonomusPrefix ( YES | NO )] [-depricatePrefix ( YES | NO )][-
    decrementPrefixLifeTimes ( YES | NO )]-prefixValideLifeTime <
    positive_integer>][-prefixPreferredLifeTime <positive_integer>]
```

Para establecer un vínculo en el enlace a los parámetros configurables del prefijo IPv6 mediante la CLI

En el símbolo del sistema, escriba lo siguiente:

```
help set onLinkIPv6Prefix
```


Para enlazar un vínculo en el enlace a los parámetros configurables del prefijo IPv6 mediante la CLI

En el símbolo del sistema, escriba:

```
help bind nd6RAvariables
```

Para mostrar ND6Ravariables mediante la CLI

En el símbolo del sistema, escriba:

```
help sh nd6RAvariables
```

Ejemplo

```
> sh nd6RAvariables
  1) Vlan : 1
     SendAdvert      : NO   CeaseAdv       : NO        SourceLLAddress: YES
     UnicastOnly     : NO   ManagedFlag    : NO        OtherConfigFlag: NO
     CurHopLimit     : 64   MaxRtrAdvInterv: 600       MinRtrAdvInterv: 198
     LinkMTU         : 0    ReachableTime  : 0         RetransTimer   : 0
     DefaultLifetime: 1800 LastRAsentTime : 0         NextRAdelay    : 0

  2) Vlan : 2
     SendAdvert      : NO   CeaseAdv       : NO        SourceLLAddress: YES
     UnicastOnly     : NO   ManagedFlag    : NO        OtherConfigFlag: NO
     CurHopLimit     : 64   MaxRtrAdvInterv: 600       MinRtrAdvInterv: 198
     LinkMTU         : 0    ReachableTime  : 0         RetransTimer   : 0
     DefaultLifetime: 1800 LastRAsentTime : 0         NextRAdelay    : 0
Done
>
> sh nd6Ravariables  - vlan 2
```



```
  1) Vlan : 2
     SendAdvert      : NO   CeaseAdv       : NO         SourceLLAddress:
         YES
     UnicastOnly     : NO   ManagedFlag    : NO         OtherConfigFlag:
         NO
     CurHopLimit     : 64   MaxRtrAdvInterv: 600        MinRtrAdvInterv:
         198
     LinkMTU         : 0    ReachableTime  : 0          RetransTimer   :
         0
     DefaultLifetime: 1800 LastRAsentTime : 0          NextRAdelay    :
         0
     Prefix :
3ffe:501:ffff:100::/64
Done
```

Administrar mensajes de latido del clúster

August 20, 2021

Administrar mensajes de latido en un clúster es similar a administrarlos en una configuración de alta disponibilidad (HA). Los nodos pueden enviar y recibir mensajes de latido entre sí en todas las interfaces habilitadas. Para evitar el aumento del tráfico resultante de mensajes de latidos, ahora puede inhabilitar la opción de latido en las interfaces de nodo. Sin embargo, la opción de latido de la interfaz del backplane no se puede inhabilitar, ya que es necesaria para mantener la conectividad entre los nodos del clúster.

Para obtener más información sobre la administración de mensajes cardíacos, consulte Administración de mensajes de latido de alta disponibilidad en un dispositivo NetScaler Appliance.

Para administrar los mensajes de latido en una interfaz de nodo mediante la CLI de Citrix ADC

En el símbolo del sistema, escriba:

```
set interface <ID> [-HAHeartBeat (ON | OFF)]
Show interface <ID>
```


Configuración del estado de respuesta del nodo propietario

August 20, 2021

Puede configurar la opción OwnerDownResponse en un nodo que tiene una dirección SNIP detectada. De forma predeterminada, la opción está habilitada. Permite que la dirección IP detectado responda a solicitudes PING o ARP (provenientes del enrutador ascendente) cuando el nodo está inactivo. Si inhabilita la opción, la dirección IP no puede responder a las solicitudes del enrutador cuando el nodo propietario está inactivo.

Para saber cómo se utiliza esta función para supervisar las rutas estáticas en la implementación de ECMP, consulte el tema Uso de rutas múltiples de igual coste (ECMP) .

Para establecer el estado de respuesta del nodo propietario mediante la CLI de Citrix ADC

En el símbolo del sistema, escriba:

```
add ns ip <IPAddress> [-ownerNode <positive_integer>] [-
    ownerDownResponse (YES | NO )] [-td <positive_integer>]
```

Ejemplo

```
add ns ip 2.2.2.2 255.255.255.0 -ownernode 6  - ownerdownResponse YES
```

Para establecer el estado de respuesta del nodo propietario mediante la GUI de Citrix ADC

1. Vaya a **Sistema > Red > IPs** y haga clic en **Agregar** para crear una dirección SNIP detectada.
2. En la página **Crear dirección IP**, active o desactive la casilla de verificación **OwnerDownResponse**.

Para modificar el estado de respuesta del nodo propietario mediante la interfaz gráfica de usuario de Citrix ADC

Desplácese hasta **Sistema > Red > IPs**, seleccione una dirección IP y haga clic en **Modificar**para activar o desactivar la casilla de verificación **OwnerDownResponse**.

Supervisar la compatibilidad de rutas estáticas (MSR) para nodos inactivos en una configuración de clúster detectado

January 12, 2021

En un clúster configurado con la opción MSR habilitada en la ruta, solo los nodos activos pueden sondear una ruta estática. Puede llegar a una red mientras que los nodos inactivos y de reserva no tienen ningún vínculo con la ruta y no pueden sondear en ella. Ahora puede configurar un nodo inactivo o de reserva para enviar los sondeos PING y ARP a la ruta IPv4 y enviar los sondeos ping6 y nd6 a la ruta IPv6. Puede realizar esto solo en una configuración de clúster detectado en la que la dirección de recorte esté activa y sea propiedad exclusiva de un nodo.

Enlace de interfaz VRRP en un clúster activo de un solo nodo

August 20, 2021

Al migrar una instalación de alta disponibilidad (HA) a una configuración de clúster, todas las configuraciones deben ser compatibles y ser compatibles en el clúster. Para lograr esto, ahora puede configurar los ID de enrutador virtual (VRID y VR6s) en una interfaz de nodo.

> **Importante**
>
> Actualmente, solo un sistema de clúster activo de un solo nodo admite VRID y VRID6s.

Para obtener instrucciones sobre cómo configurar VRID y VRID6, consulte Configuración de direcciones MAC virtuales.

Para configurar un ID de enrutador virtual en un clúster activo de un solo nodo, agregue el VRID o VRID6 y enlácelo a la interfaz de nodo de clúster.

Para agregar un VRID mediante la CLI de Citrix ADC

En el símbolo del sistema, escriba:

```
1 add vrID <ID>
```

Para enlazar un VRID a la interfaz de nodo de clúster mediante la CLI de Citrix ADC

En el símbolo del sistema, escriba:


```
Bind vrid <ID> -ifnum <interface_name> | -trackifNum <interface_name

Add vrID 100
Bind vrid 100  - ifnum 1/1  1/2
done
```

Para agregar un VRID6 mediante la CLI de Citrix ADC

En el símbolo del sistema, escriba:

```
add vrID6 <ID>
```

Para enlazar un VRID6 a una interfaz de nodo de clúster mediante la CLI

En el símbolo del sistema, escriba:

```
bind vrid6 <ID> -ifnum <interface_name> | -trackifNum <interface_name>

Add vrID6 100
Bind vrid6 100  - ifnum 1/1  1/2
Done
```

Casos de configuración y uso del clúster

January 12, 2021

En esta sección se explican algunos casos en los que se puede configurar el clúster de Citrix ADC y configurarlo para diferentes funciones y topologías de red. Proporcione comentarios si quiere que se documente cualquier otro caso.

Creación de un clúster de dos nodos

January 12, 2021

Un clúster de dos nodos es una excepción a la regla de que un clúster solo funciona cuando un mínimo de nodos (n/2 + 1), donde n es el número de nodos del clúster, son capaces de servir tráfico. Si se aplica la misma fórmula a un clúster de dos nodos, el clúster fallaría si se caía un nodo (n/2 +1=2).

Un clúster de dos nodos funciona incluso si solo un nodo es capaz de servir tráfico.

Crear un clúster de dos nodos es lo mismo que crear cualquier otro clúster. Agregue un nodo como coordinador de configuración y el otro nodo como el otro nodo del clúster.

> **Nota**
>
> La sincronización de configuración incremental no se admite en un clúster de dos nodos. Solo se admite la sincronización completa.

Migración de una configuración de alta disponibilidad a una configuración de clúster

August 20, 2021

Para migrar una configuración de alta disponibilidad (HA) existente a una configuración de clúster, primero debe quitar los dispositivos Citrix ADC de la configuración de HA y crear una copia de seguridad del archivo de configuración de HA. A continuación, puede utilizar los dos dispositivos para crear un clúster y cargar el archivo de configuración de copia de seguridad en el clúster.

> **Nota**
>
> - Antes de cargar el archivo de configuración de HA de copia de seguridad en el clúster, debe modificarlo para que sea compatible con el clúster. Consulte el paso correspondiente del procedimiento.
> - Utilice el comando **batch -f <backup_filename>** para cargar el archivo de configuración de copia de seguridad.

El enfoque anterior es una solución básica de migración que da como resultado un tiempo de inactividad para la aplicación implementada. Como tal, debe usarse solo en implementaciones donde no se tenga en cuenta la disponibilidad de las aplicaciones.

Sin embargo, en la mayoría de las implementaciones, la disponibilidad de la aplicación es de suma importancia. En estos casos, debe utilizar el enfoque en el que se puede migrar una configuración de alta disponibilidad a una configuración de clúster sin ningún tiempo de inactividad resultante. En este enfoque, una instalación de HA existente se migra a una configuración de clúster quitando primero el dispositivo secundario y mediante ese dispositivo para crear un clúster de nodo único. Después de que el clúster entre en funcionamiento y sirve tráfico, el dispositivo principal de la instalación de HA se agrega al clúster.

Para convertir una configuración de alta disponibilidad en configuración de clúster (sin tiempo de inactividad) mediante la interfaz de línea de comandos

Consideremos el ejemplo de una configuración de alta disponibilidad con dispositivo primario (NS1): 10.102.97.131 y dispositivo secundario (NS2): 10.102.97.132.

1. Asegúrese de que las configuraciones del par HA sean estables.
2. Inicie sesión en cualquiera de los dispositivos HA, vaya al shell y cree una copia del archivo ns.conf (por ejemplo, ns_backup.conf).
3. Inicie sesión en el dispositivo secundario, NS2, y borre las configuraciones. Esta operación elimina NS2 de la configuración de alta disponibilidad y lo convierte en un dispositivo independiente.

```
1 > clear ns config full
```

> **Nota**
>
> - Este paso es necesario para asegurarse de que NS2 no comienza a poseer direcciones VIP, ahora que se trata de un dispositivo independiente.
> - En esta etapa, el dispositivo principal, NS1, sigue activo y sigue sirviendo el tráfico.

4. Cree un clúster en NS2 (ahora ya no es un dispositivo secundario) y configúrelo como un nodo PASIVO.

```
1  > add cluster instance 1
2
3  > add cluster node 0 10.102.97.132 -state PASSIVE -backplane
     0/1/1
4
5  > add ns ip 10.102.97.133 255.255.255.255 -type CLIP
6
7  > enable cluster instance 1
8
9  > save ns config
10
11 > reboot -warm
```

5. Modifique el archivo de configuración de copia de seguridad de la siguiente manera:
   - Quite las funciones que no se admiten en un clúster. Para obtener la lista de funciones no compatibles, consulte Funciones de Citrix ADC compatibles con un clúster. Es un paso

opcional. Si no realiza este paso, se produce un error en la ejecución de comandos no compatibles.

- Elimine las configuraciones que tienen interfaces o actualice los nombres de interfaz de la convención c/u a la convención n/c/u.

  Ejemplo

  ```
  > add vlan 10 -ifnum 0/1
  ```

  debe cambiarse a

  ```
  > add vlan 10 -ifnum 0/0/1 1/0/1
  ```

- El archivo de configuración de copia de seguridad puede tener direcciones SNIP. Estas direcciones se seccionan en todos los nodos del clúster. Se recomienda agregar direcciones IP detectada para cada nodo.

  Ejemplo

  ```
  > add ns ip 1.1.1.1 255.255.255.0 -ownerNode 0

  > add ns ip 1.1.1.2 255.255.255.0 -ownerNode 1
  ```

- Actualice el nombre de host para especificar el nodo propietario.

  Ejemplo

  ```
  > set ns hostname ns0 -ownerNode 0

  > set ns hostname ns1 -ownerNode 1
  ```

- Cambie todas las demás configuraciones de red relevantes que dependen de las IP detectados. Por ejemplo, L3 VLAN, configuración RNAT que utiliza SNIP como NATIP, reglas INAT que hace referencia a SNIPS/MIP).

6. En el clúster, haga lo siguiente:

   - Realice los cambios topológicos en el clúster conectando el backplane del clúster, el canal de agregación de vínculos del clúster, etc.

- Aplique configuraciones del archivo de configuración modificado y de copia de seguridad al coordinador de configuración a través de la dirección IP del clúster.

```
> batch -f ns_backup.conf
```

- Configure mecanismos de distribución de tráfico externo como ECMP o agregación de vínculos de clúster.

7. Cambie el tráfico de la configuración de HA al clúster.
   - Inicie sesión en el dispositivo principal, NS1, e inhabilite todas las interfaces en él.

```
> disable interface <interface_id>
```

   - Inicie sesión en la dirección IP del clúster y configure NS2 como nodo ACTIVE.

```
> set cluster node 0 -state ACTIVE
```

> **Nota**
>
> Puede haber una pequeña cantidad (en el orden de segundos) de tiempo de inactividad entre inhabilitar las interfaces y activar el nodo del clúster.

8. Inicie sesión en el dispositivo principal, NS1, y quítelo de la instalación de alta disponibilidad.
   - Borre todas las configuraciones. Esta operación elimina NS1 de la configuración de alta disponibilidad y lo convierte en un dispositivo independiente.

```
> clear ns config full
```

   - Habilite todas las interfaces.

```
> enable interface <interface_id>
```

9. Agregue NS1 al clúster.
   - Inicie sesión en la dirección IP del clúster y agregue NS1 al clúster.


```
> add cluster node 1 10.102.97.131 -state PASSIVE -backplane
   1/1/1
```

- Inicie sesión en NS1 y únete al clúster ejecutando secuencialmente los siguientes comandos:

```
> join cluster -clip 10.102.97.133 -password nsroot

> save ns config

> reboot -warm
```

10. Inicie sesión en NS1 y realice los cambios topológicos y de configuración necesarios.
11. Inicie sesión en la dirección IP del clúster y establezca NS1 como nodo ACTIVE.

```
> set cluster node 1 -state ACTIVE
```

Transición entre un clúster L2 y L3

January 19, 2021

> **Nota**
>
> Compatible con NetScaler 11 en adelante.

Un clúster L2 es aquel en el que todos los nodos son de la misma red y un clúster L3 es uno que puede incluir nodos de diferentes redes. Puede realizar una transición sin problemas de un tipo de clúster a otro sin tiempo de inactividad para las aplicaciones que se implementan en Citrix ADC.

Transición de un clúster de L2 a L3

Puede realizar la transición a un clúster L3 cuando quiera que el clúster incluya nodos de otras redes.

En la dirección IP del clúster, haga lo siguiente:

1. Cree un grupo de nodos.

   Ejemplo


```
1 > add cluster nodegroup NG0
```

Este grupo de nodos se utiliza en el siguiente paso para agrupar todos los nodos del clúster L2 existente.

2. Transición del clúster L2 a un clúster L3.

   Ejemplo

```
1 > set cluster instance 1 -inc ENABLED -nodegroup NG0
```

   Este comando logra el doble propósito de realizar la transición al clúster L3 y también agregar todos los nodos del clúster L2 al grupo de nodos.

3. Ahora, puede agregar más nodos al clúster como se explica en Agregar un nodo al clúster.

Transición de un clúster de L3 a L2

Puede realizar la transición a un clúster L2 cuando quiera conservar los nodos que pertenecen a una sola red.

En la dirección IP del clúster, haga lo siguiente:

1. Quite los nodos del clúster de las redes que no quiere conservar.

   Ejemplo

```
1 > rm cluster node <nodeId>
```

2. Transición del clúster L3 a un clúster L2.

   Ejemplo

```
1 > set cluster instance 1 -inc DISABLED
```

   El clúster ahora incluye nodos solo de una sola red.

Configuración de GSLB en un clúster

August 20, 2021

> **Nota**
>
> Compatible con NetScaler 10.5 Build 52.11 en adelante.

Para configurar GSLB en un clúster, debe vincular las diferentes entidades GSLB a un grupo de nodos. El grupo de nodos debe tener un único nodo miembro.

> **Notas**
>
> - Si ha configurado el método GSLB de proximidad estática, asegúrese de que la base de datos de proximidad estática está presente en todos los nodos del clúster. Sucede de forma predeterminada si el archivo de base de datos está disponible en la ubicación predeterminada. Sin embargo, si el archivo de base de datos se mantiene en un directorio distinto de /var/netscaler/locdb/, debe sincronizar manualmente el archivo con todos los nodos del clúster.
> - El `show gslb domain` comando no se admite en una configuración de clúster.

Para configurar GSLB en un clúster mediante la CLI:

Inicie sesión en la dirección IP del clúster y realice las siguientes operaciones en el símbolo del sistema:

1. Configure las diferentes entidades GSLB. Para obtener información, consulte Entidades de configuración de GSLB.

   > **Nota**
   >
   > Al crear el sitio GSLB, asegúrese de especificar la dirección IP del clúster y la dirección IP del clúster público. La dirección IP del clúster público solo es necesaria cuando el clúster se implementa detrás de un dispositivo NAT. Al configurar un sitio GSLB, debe utilizar la dirección IP del clúster del mismo sitio. Estos parámetros son necesarios para garantizar la disponibilidad de la funcionalidad de sincronización automática de GSLB.

   ```
   add gslb site <siteName> <siteType> <siteIPAddress> -publicIP <ip_addr>
    -clip <ip_addr> <publicCLIP><!--NeedCopy-->
   ```

2. Cree un grupo de nodos de clúster.

   ```
   add cluster nodegroup <name> <name>@ [-strict ( YES | NO )] [-sticky (
   YES | NO )] [-state <state>] [-priority <positive_integer>]<!--NeedCopy
   -->
   ```

   > **Nota**
   >
   > Habilite la opción adhesiva si quiere configurar GSLB basado en usuarios VPN.

3. Enlazar un único nodo de clúster al grupo de nodos.

   ```
   bind cluster nodegroup <name> -node <nodeId><!--NeedCopy-->
   ```

4. Enlazar el sitio GSLB local al grupo de nodos.


```
bind cluster nodegroup <name> -gslbSite <string><!--NeedCopy-->
```

> **Nota**
>
> Asegúrese de que la dirección IP de la dirección IP del sitio GSLB local está seccionada (disponible en todos los nodos del clúster).

5. Enlace el servicio ADNS (o ADNS-TCP) o el servidor virtual de equilibrio de carga DNS (o DNS-TCP) al grupo de nodos.

   Para enlazar el servicio ADNS:

   "'bind cluster nodegroup -service

```
**Para enlazar el servidor virtual de equilibrio de carga DNS:**

```bind cluster nodegroup <name> -vServer <string><!--NeedCopy-->
```

6. Enlace el servidor virtual GSLB al grupo de nodos.

   ```
   bind cluster nodegroup <name> -vServer <string><!--NeedCopy-->
   ```

7. [Opcional] Para configurar GSLB en función de usuarios VPN, vincule el servidor virtual VPN al grupo de nodos GSLB.

   ```
   bind cluster nodegroup <name> -vServer <string><!--NeedCopy-->
   ```

8. Verifique las configuraciones.

   ```
   show gslb runningConfig<!--NeedCopy-->
   ```

Para configurar GSLB en un clúster mediante la GUI:

Inicie sesión en la dirección IP del clúster y realice las siguientes operaciones en la ficha Configuración:

1. Configure las entidades GSLB.

   Vaya a **Traffic Management > GSLB** para realizar las configuraciones requeridas.

2. Cree un grupo de nodos y realice otras configuraciones relacionadas con el grupo de nodos.

   Vaya a **Sistema > Clúster > Grupos de nodos** para realizar las configuraciones necesarias.

Para conocer las configuraciones detalladas que se deben realizar, consulte la descripción proporcionada en el procedimiento anterior de CLI.

Compatibilidad con topología principal-secundario GSLB en un clúster

A partir de NetScaler 12.1, compilación 49.xx, la topología principal-secundario de GSLB se admite en el clúster.


   ```

Para obtener más información sobre la topología principal-secundario, consulte Implementación de topología principal-secundario mediante el protocolo MEP.

**Para configurar la topología principal-secundario de GSLB en un clúster mediante la CLI**

**Sitio principal**

Realice la siguiente configuración:

1. Cree un grupo de nodos de clúster.

   ```
   add cluster nodegroup <name>
   ```

   Ejemplo:

   ```
   add cluster nodegroup parentng
   ```

2. Enlazar un único nodo de clúster al grupo de nodos.

   ```
   bind cluster nodegroup <name> -node <nodeId>
   ```

   Ejemplo:

   ```
   bind cluster nodegroup parentng -node n2
   ```

3. Enlazar el sitio GSLB local al grupo de nodos.

   ```
   bind cluster nodegroup <name> -gslbSite <string>
   ```

   Ejemplo:

   ```
   bind cluster nodegroup parentng -gslbSite site1
   ```

4. Enlace el servicio ADNS (o ADNS-TCP) o el servidor virtual de equilibrio de carga DNS (o DNS-TCP) al grupo de nodos.

   ```
   bind cluster nodegroup <name> -service <string>
   ```

   Ejemplo:

   ```
   bind cluster nodegroup parentng - service ADNS
   ```

5. Enlace el servidor virtual GSLB al grupo de nodos.

   ```
   bind cluster nodegroup <name> -vServer <string>
   ```

   Ejemplo:

   ```
   bind cluster nodegroup parentng -vServce gslbvs1
   ```


Sitio secundario

Realice la siguiente configuración:

1. Cree un grupo de nodos de clúster.

   ```
   add cluster nodegroup <name>
   ```

   Ejemplo:

   ```
   add cluster nodegroup childng
   ```

2. Enlazar un único nodo de clúster al grupo de nodos.

   ```
   bind cluster nodegroup <name> -node <nodeId>
   ```

   Ejemplo:

   ```
   bind cluster nodegroup childng -node -n3
   ```

3. Enlazar el sitio GSLB local al grupo de nodos.

   ```
   bind cluster nodegroup <name> -gslbSite <string>
   ```

   Ejemplo:

   ```
   bind cluster nodegroup childng -gslbSite site1
   ```

> **Nota**
>
> Para que los sitios primarios y secundarios intercambien estadísticas agregadas en métodos de equilibrio de carga basados en métricas, debe agregar servicios GSLB locales en el sitio secundario. Los métodos de equilibrio de carga basados en la métrica son menos conexión, menos ancho de banda y menos paquetes.

Para configurar la topología principal-secundario de GSLB en un clúster mediante la interfaz gráfica de usuario

1. Configure las entidades GSLB.

   Vaya a **Administración del tráfico** > **GSLB** para realizar las configuraciones necesarias.

2. Cree un grupo de nodos.

   Vaya a **Sistema** > **Cluster** > **Grupos de nodos** para realizar las configuraciones necesarias.

3. En la página Grupo de nodos, seleccione el grupo de nodos al que quiere enlazar un nodo, haga clic en **Modificar**y realice las siguientes tareas. También puede realizar estas tareas al agregar un grupo de nodos.

   - Enlazar un nodo al grupo de nodos.

     En **Configuración avanzada**, haga clic en Nodos de **clúster** y realice las siguientes tareas:

- En la sección **Nodos de clúster**, haga clic en **Sin nodo de clúster**
- En **Seleccionar nodo de clúster**, haga clic en > y seleccione el nodo que quiere enlazar al grupo de nodos. También puede agregar un nodo de clúster.

- Enlazar el sitio GSLB local al grupo de nodos.

  En Configuración avanzada, haga clic en Sitios de GSLB y realice las siguientes tareas:

  - En la sección **Sitios GSLB**, haga clic en Sin sitio GSLB.
  - En **Seleccionar sitio GSLB**, haga clic en > y seleccione el sitio GSLB que quiere enlazar al grupo de nodos. También puede agregar un sitio GSLB.

- Enlace el servidor virtual GSLB al grupo de nodos.

  En **Configuración avanzada**, haga clic en **Servidores virtuales** y realice la siguiente tarea:

  - En el panel **Servidores virtuales**, haga clic en +.
  - En **Elegir servidor virtual**, seleccione el servidor que quiere enlazar al grupo de nodos.

- Enlace el servicio ADNS (o ADNS-TCP) o el servidor virtual de equilibrio de carga DNS (o DNS-TCP) al grupo de nodos.

  En **Configuración avanzada**, haga clic en **Servicios** y realice las siguientes tareas:

  - En la sección **Servicios**, haga clic en **Sin servicio**.
  - En **Seleccionar servicio**, seleccione el servicio que quiere enlazar al grupo de nodos. También puede agregar un servicio.

> **Nota**
>
> Para sitios secundarios, solo tiene que enlazar el nodo del clúster y el sitio GSLB local al grupo de nodos.

Uso de la redirección de caché en un clúster

January 19, 2021

La redirección de caché en un clúster funciona de la misma manera que en un dispositivo Citrix ADC independiente. La única diferencia es que las configuraciones se realizan en la dirección IP del clúster. Para obtener más información sobre la redirección de caché, consulte Redirección de caché.

Puntos a recordar cuando se utiliza la redirección de caché en modo transparente en un clúster:

- Antes de configurar la redirección de caché, asegúrese de que ha conectado todos los nodos al conmutador externo y de que tiene configurados los conjuntos de enlaces. De lo contrario, las solicitudes de cliente se eliminan.

- Cuando el modo MAC está habilitado en un servidor virtual de equilibrio de carga, asegúrese de que el modo MBF está habilitado en el clúster mediante el comando enable ns mode MBF. De lo contrario, las solicitudes se envían directamente al servidor de origen en lugar de enviarse al servidor de caché.

Uso del modo L2 en una configuración de clúster

January 12, 2021

> **Nota**
>
> Compatible con NetScaler 10.5 y versiones posteriores.

Para utilizar el modo L2 en una configuración de clúster, debe asegurarse de lo siguiente:

- Las direcciones IP detectada deben estar disponibles en todos los nodos según sea necesario.
- Los conjuntos de vínculos deben utilizarse para comunicarse con la red externa.
- No se admiten topologías asimétricas o grupos LA de clúster asimétrico.
- Se recomienda el grupo de Cluster LA.
- El tráfico se distribuye entre los nodos del clúster solo para las implementaciones donde existen servicios.

Uso del canal LA de clúster con conjuntos de enlaces

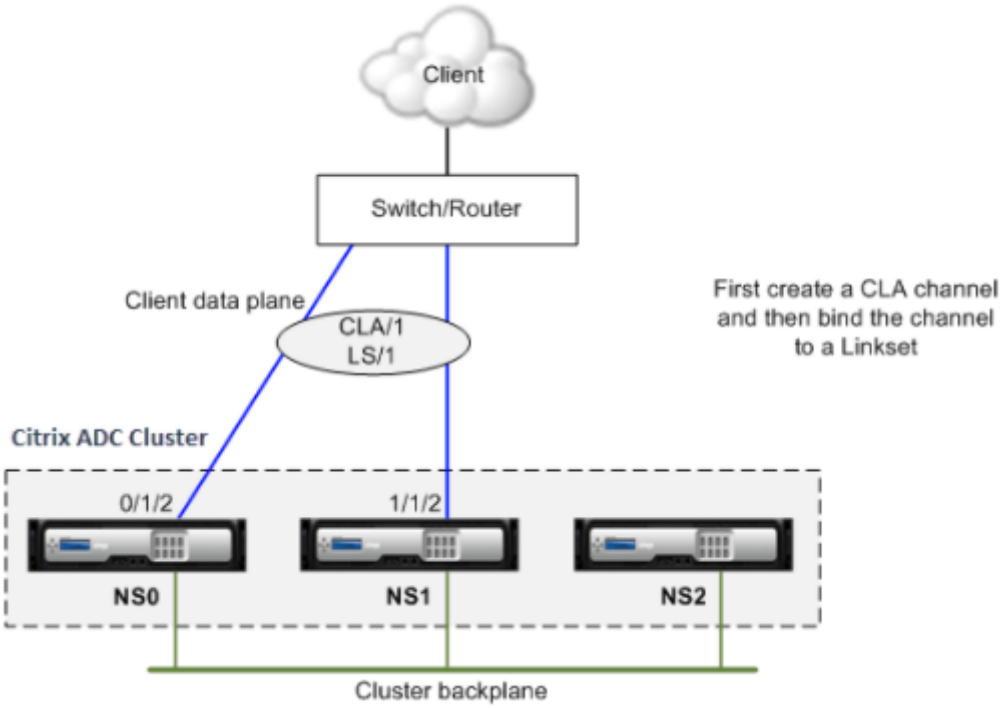
August 20, 2021

En una topología de clúster asimétrica, algunos nodos de clúster no están conectados a la red ascendente. En tal caso, debe usar conjuntos de enlaces. Para optimizar el rendimiento, puede enlazar las interfaces que están conectadas al conmutador como un canal LA de clúster y, a continuación, enlazar el canal a un conjunto de vínculos.

Para comprender cómo se puede utilizar una combinación de canal LA de clúster y conjuntos de vínculos, considere un clúster de tres nodos para el que el conmutador ascendente solo tenga dos puertos disponibles. Puede conectar dos de los nodos del clúster al conmutador y dejar el otro nodo desconectado.

> **Nota**
>
> Del mismo modo, también puede utilizar una combinación de ECMP y conjuntos de vínculos en una topología asimétrica.

Ilustración 1. Conjuntos de vínculos y topología de canal LA de clúster



Para configurar el canal LA del clúster y los conjuntos de vínculos mediante la CLI

1. Inicie sesión en la dirección IP del clúster.
2. Enlazar las interfaces conectadas a un canal LA de clúster.

```
add channel CLA/1 -ifnum 0/1/2 1/1/2
```

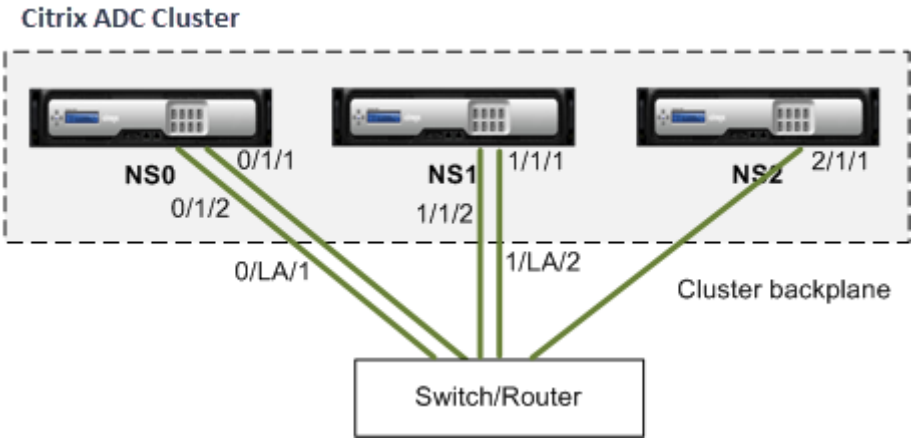
3. Enlace el canal LA del clúster al conjunto de vínculos.

```
add linkset LS/1 -ifnum CLA/1
```

backplane en el canal LA

August 20, 2021

En esta implementación, los canales LA se utilizan para el plano anterior del clúster.



- NS0: NodeId: 0, NSIP: 10.102.29.60
- NS1: NodeId: 1, NSIP: 10.102.29.70
- NS2: NodeId: 2, NSIP: 10.102.29.80

Para implementar un clúster con las interfaces de plano anterior como canales LA

1. Cree un clúster de nodos NS0, NS1 y NS2.

   a) Inicie sesión en el primer nodo que quiera agregar al clúster y haga lo siguiente:

```
> create cluster instance 1
> add cluster node 0 10.102.29.60 -state ACTIVE
> enable cluster instance 1
> add ns ip 10.102.29.61 255.255.255.255 -type CLIP
> save ns config
> reboot -warm
```

   b) Inicie sesión en la dirección IP del clúster y haga lo siguiente:

```
> add cluster node 1 10.102.29.70 -state ACTIVE
> add cluster node 2 10.102.29.80 -state ACTIVE
```

   c) Inicie sesión en los nodos 10.102.29.70 y 10.102.29.80 para unir los nodos al clúster.

```
> join cluster -clip 10.102.29.61 -password nsroot
> save ns config
> reboot -warm
```


Como se ha visto en los comandos anteriores, las interfaces 0/1/1, 1/1/1 y 2/1/1 se configuran como interfaces de plano posterior de los tres nodos de clúster.

2. Inicie sesión en la dirección IP del clúster y haga lo siguiente:

   a) Cree los canales LA para los nodos NS0 y NS1.

```
> add channel 0/LA/1 -ifnum 0/1/1 0/1/2
> add channel 1/LA/2 -ifnum 1/1/1 1/1/2
```

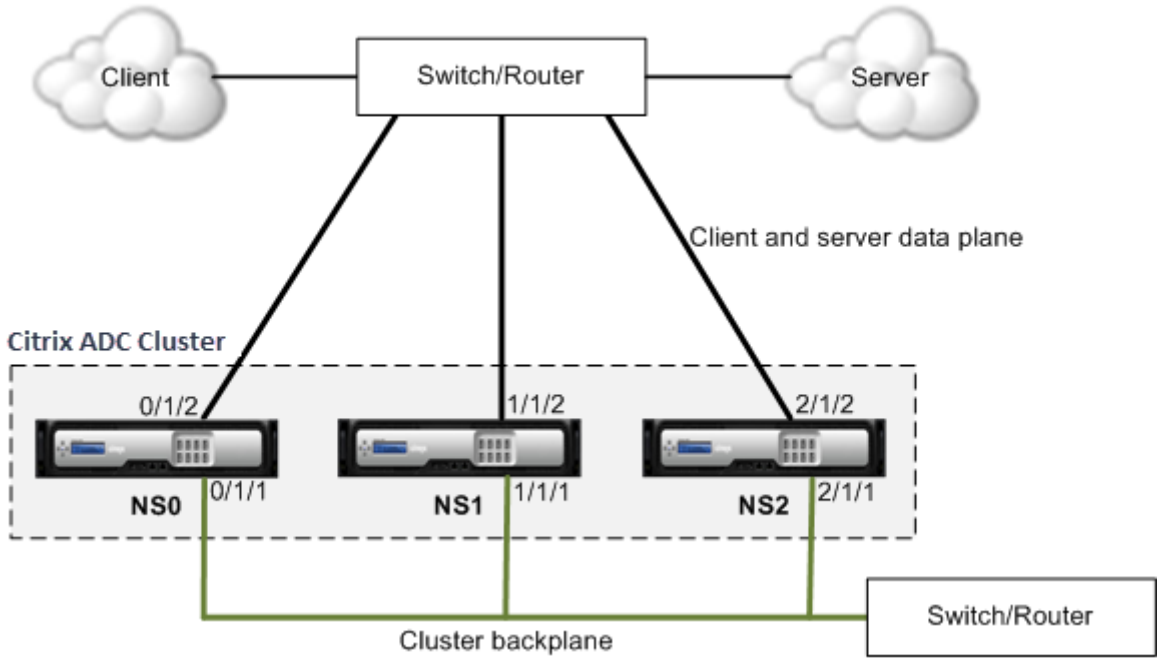
   b) Configure el plano anterior para los nodos del clúster.

```
> set cluster node 0 -backplane 0/LA/1
> set cluster node 1 -backplane 1/LA/2
> set cluster node 2 -backplane 2/1/1
```

Interfaces comunes para cliente y servidor e interfaces dedicadas para plano anterior

August 20, 2021

Se trata de una implementación de un brazo del clúster Citrix ADC. En esta implementación, las redes cliente y servidor utilizan las mismas interfaces para comunicarse con el clúster. El plano anterior del clúster utiliza interfaces dedicadas para la comunicación entre nodos.



- NS0: NodeId: 0, NSIP: 10.102.29.60
- NS1: NodeId: 1, NSIP: 10.102.29.70
- NS2: NodeId: 2, NSIP: 10.102.29.80

Para implementar un clúster con una interfaz común para el cliente y el servidor y una interfaz diferente para el plano anterior del clúster

1. Cree un clúster de nodos NS0, NS1 y NS2.
2. Inicie sesión en el primer nodo que quiera agregar al clúster y haga lo siguiente:

```
1 > create cluster instance 1
2 > add cluster node 0 10.102.29.60 -state ACTIVE -backplane
     0/1/1
3 > enable cluster instance 1
4 > add ns ip 10.102.29.61 255.255.255.255 -type CLIP
5 > save ns config
6 > reboot -warm
```

3. Inicie sesión en la dirección IP del clúster y haga lo siguiente:

```
1 > add cluster node 1 10.102.29.70 -state ACTIVE -backplane
     1/1/1
```



```
2 > add cluster node 2 10.102.29.80 -state ACTIVE -backplane
      2/1/1
```

4. Inicie sesión en los nodos 10.102.29.70 y 10.102.29.80 para unir los nodos al clúster.

```
1 > join cluster -clip 10.102.29.61 -password nsroot
2 > save ns config
3 > reboot -warm
```

Como se ha visto en los comandos anteriores, las interfaces 0/1/1, 1/1/1 y 2/1/1 se configuran como interfaces de plano posterior de los tres nodos de clúster.

1. En la dirección IP del clúster, cree VLAN para las interfaces de plano anterior y para las interfaces de cliente y servidor.

   //Para las interfaces backplane

```
1 > add vlan 10
2 > bind vlan 10 0/1/1 1/1/1 2/1/1
```

   //Para las interfaces que están conectadas a las redes cliente y servidor.

```
1 > add vlan 20
2 > bind vlan 20 0/1/2 1/1/2 2/1/2
```

2. En el switch, cree VLAN para las interfaces correspondientes a las interfaces del plano posterior y las interfaces de cliente y servidor. Se proporcionan las siguientes configuraciones de ejemplo para el conmutador Cisco® Nexus 7000 C7010 Release 5.2 (1). Se deben realizar configuraciones similares en otros conmutadores.

   //Para las interfaces backplane. Repita para cada interfaz…

```
1 > interface Ethernet2/47
2   switchport access vlan 100
3   switchport mode access
4   end
```

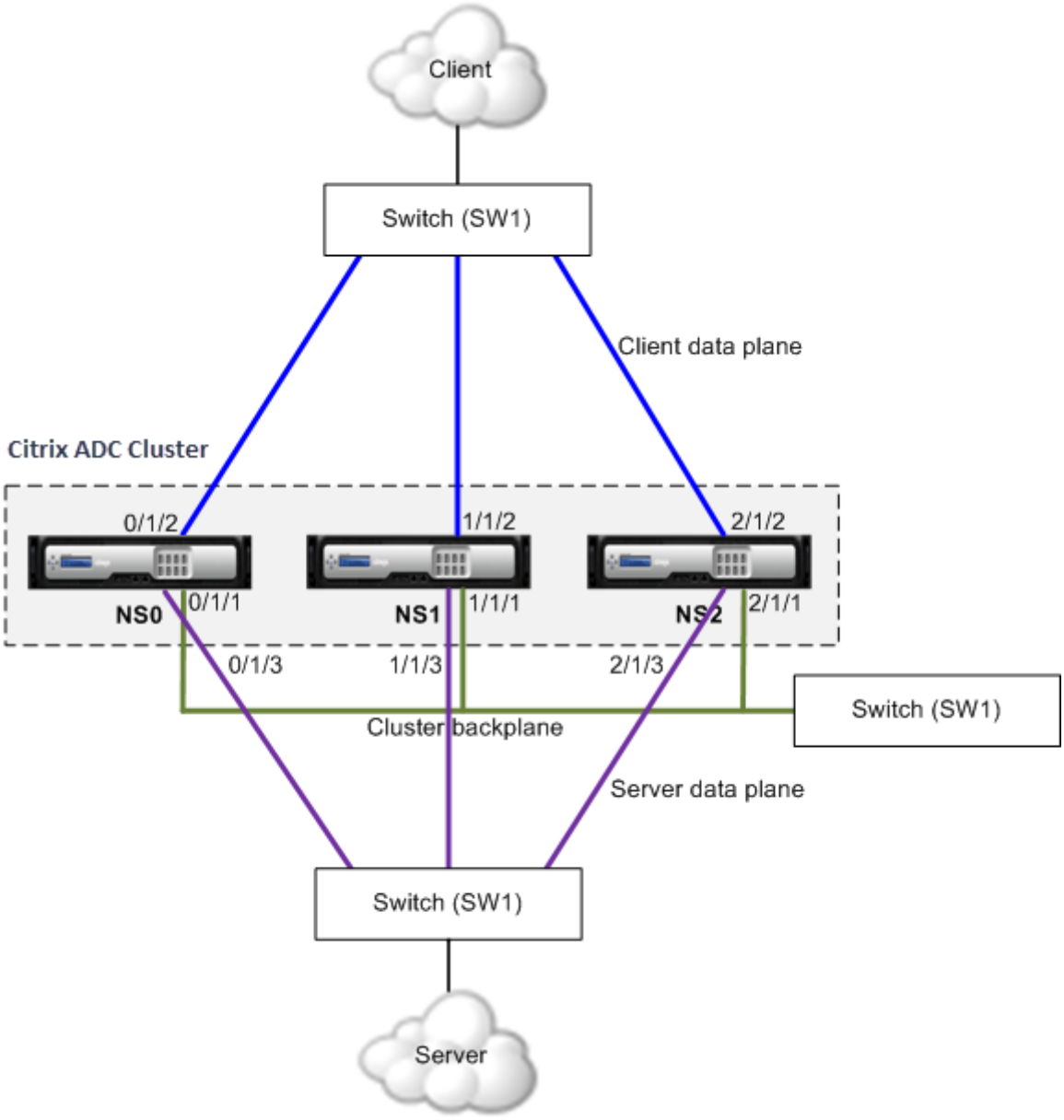
   //Para las interfaces conectadas a las redes cliente y servidor. Repita para cada interfaz…


```
> interface Ethernet2/47
  switchport access vlan 200
  switchport mode access
  end
```

Conmutador común para cliente, servidor y plano anterior

August 20, 2021

En esta implementación, el cliente, el servidor y la placa base utilizan interfaces dedicadas en el mismo conmutador para comunicarse con el clúster de Citrix ADC.



- NS0: NodeId: 0, NSIP: 10.102.29.60
- NS1: NodeId: 1, NSIP: 10.102.29.70
- NS2: NodeId: 2, NSIP: 10.102.29.80

Para implementar un clúster con un conmutador común para el cliente, el servidor y el plano anterior

1. Cree un clúster de nodos NS0, NS1 y NS2.
2. Inicie sesión en el primer nodo que quiera agregar al clúster y haga lo siguiente:


```
> create cluster instance 1
> add cluster node 0 10.102.29.60 -state ACTIVE -backplane
   0/1/1
> enable cluster instance 1
> add ns ip 10.102.29.61 255.255.255.255 -type CLIP
> save ns config
> reboot -warm
```

3. Inicie sesión en la dirección IP del clúster y haga lo siguiente:

```
> add cluster node 1 10.102.29.70 -state ACTIVE -backplane
   1/1/1
> add cluster node 2 10.102.29.80 -state ACTIVE -backplane
   2/1/1
```

4. Inicie sesión en los nodos 10.102.29.70 y 10.102.29.80 para unir los nodos al clúster.

```
> join cluster -clip 10.102.29.61 -password nsroot
> save ns config
> reboot -warm
```

Como se ha visto en los comandos anteriores, las interfaces 0/1/1, 1/1/1 y 2/1/1 se configuran como interfaces de plano posterior de los tres nodos de clúster.

1. En la dirección IP del clúster, cree VLAN para las interfaces de plano anterior, cliente y servidor.

   //Para las interfaces backplane

```
> add vlan 10
> bind vlan 10 0/1/1 1/1/1 2/1/1
```

   //Para las interfaces del lado del cliente

```
> add vlan 20
> bind vlan 20 0/1/2 1/1/2 2/1/2
```

   //Para las interfaces del lado del servidor


```
> add vlan 30
> bind vlan 30 0/1/3 1/1/3 2/1/3
```

2. En el switch, cree VLAN para las interfaces correspondientes a las interfaces del plano posterior y las interfaces de cliente y servidor. Se proporcionan las siguientes configuraciones de ejemplo para el conmutador Cisco® Nexus 7000 C7010 Release 5.2 (1). Se deben realizar configuraciones similares en otros conmutadores.

   //Para las interfaces backplane. Repita para cada interfaz…

```
> interface Ethernet2/47
  switchport access vlan 100
  switchport mode access
  end
```

   //Para las interfaces de cliente. Repita para cada interfaz…

```
> interface Ethernet2/48
  switchport access vlan 200
  switchport mode access
  end
```

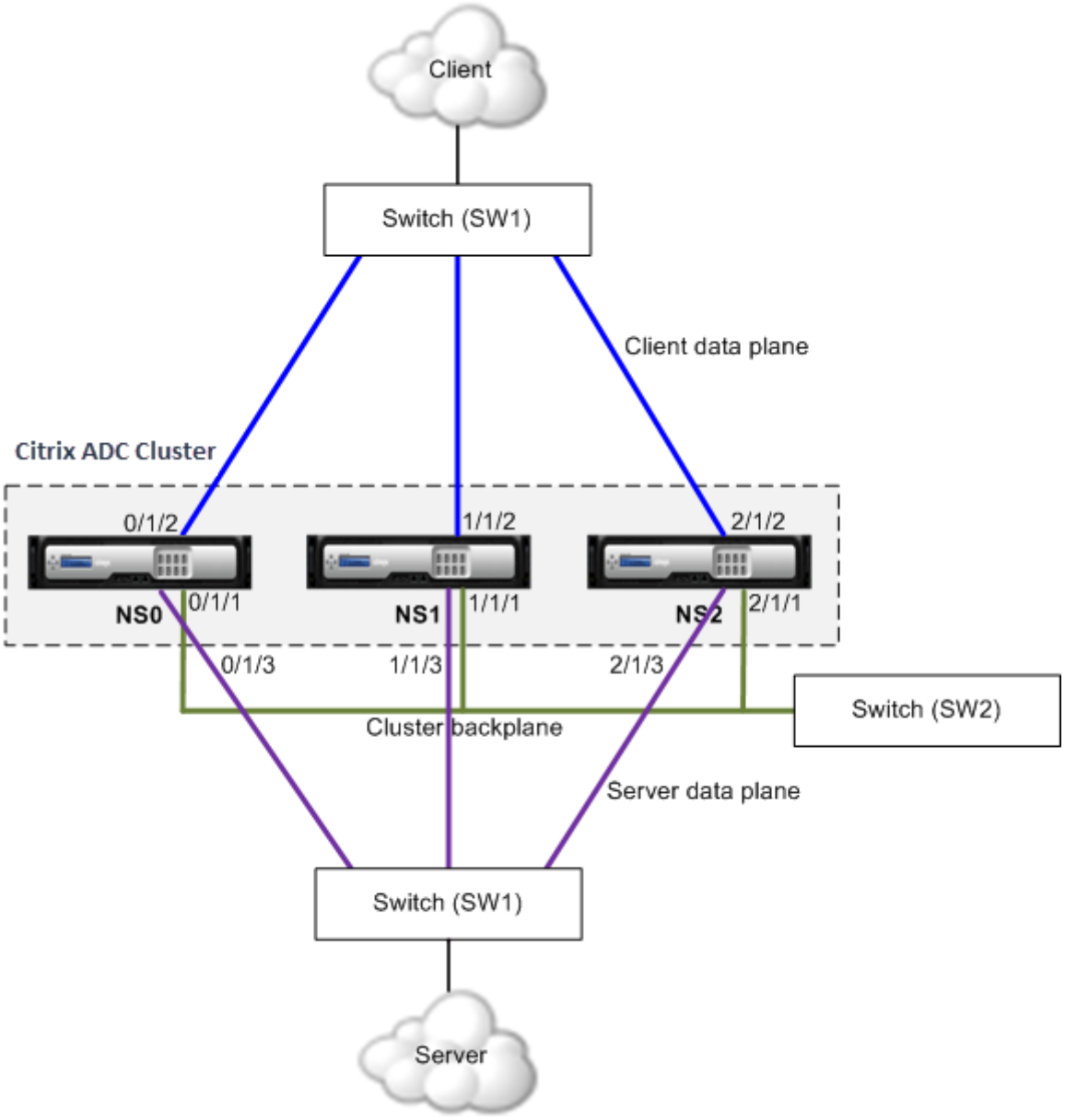
   //Para las interfaces del servidor. Repita para cada interfaz…

```
> interface Ethernet2/49
  switchport access vlan 300
  switchport mode access
  end
```

Conmutador común para cliente y servidor y conmutador dedicado para plano anterior

August 20, 2021

En esta implementación, los clientes y los servidores utilizan interfaces diferentes en el mismo conmutador para comunicarse con el clúster de Citrix ADC. El plano anterior del clúster utiliza un conmutador dedicado para la comunicación entre nodos.



- NS0: NodeId: 0, NSIP: 10.102.29.60
- NS1: NodeId: 1, NSIP: 10.102.29.70
- NS2: NodeId: 2, NSIP: 10.102.29.80

Para implementar un clúster con el mismo conmutador para los clientes y servidores y un conmutador diferente para el plano anterior del clúster

1. Cree un clúster de nodos NS0, NS1 y NS2.
    - Inicie sesión en el primer nodo que quiera agregar al clúster y haga lo siguiente:


```
> create cluster instance 1
> add cluster node 0 10.102.29.60 -state ACTIVE -backplane
   0/1/1
> enable cluster instance 1
> add ns ip 10.102.29.61 255.255.255.255 -type CLIP
> save ns config
> reboot -warm
```

- Inicie sesión en la dirección IP del clúster y haga lo siguiente:

```
> add cluster node 1 10.102.29.70 -state ACTIVE -backplane
   1/1/1
> add cluster node 2 10.102.29.80 -state ACTIVE -backplane
   2/1/1
```

- Inicie sesión en los nodos 10.102.29.70 y 10.102.29.80 para unir los nodos al clúster.

```
> join cluster -clip 10.102.29.61 -password nsroot
> save ns config
> reboot -warm
```

Como se ha visto en los comandos anteriores, las interfaces 0/1/1, 1/1/1 y 2/1/1 se configuran como interfaces de plano posterior de los tres nodos de clúster.

2. En la dirección IP del clúster, cree VLAN para las interfaces de plano anterior, cliente y servidor.

   //Para las interfaces backplane

```
> add vlan 10
> bind vlan 10 0/1/1 1/1/1 2/1/1
```

   //Para las interfaces del lado del cliente

```
> add vlan 20
> bind vlan 20 0/1/2 1/1/2 2/1/2
```

   //Para las interfaces del lado del servidor


```
> add vlan 30
> bind vlan 30 0/1/3 1/1/3 2/1/3
```

3. En el switch, cree VLAN para las interfaces correspondientes a las interfaces del plano posterior y las interfaces de cliente y servidor. Se proporcionan las siguientes configuraciones de ejemplo para el conmutador Cisco® Nexus 7000 C7010 Release 5.2 (1). Se deben realizar configuraciones similares en otros conmutadores.

   //Para las interfaces backplane. Repita para cada interfaz…

```
> interface Ethernet2/47
> switchport access vlan 100
> switchport mode access
> end
```

   //Para las interfaces de cliente. Repita para cada interfaz…

```
> interface Ethernet2/48
> switchport access vlan 200
> switchport mode access
> end
```

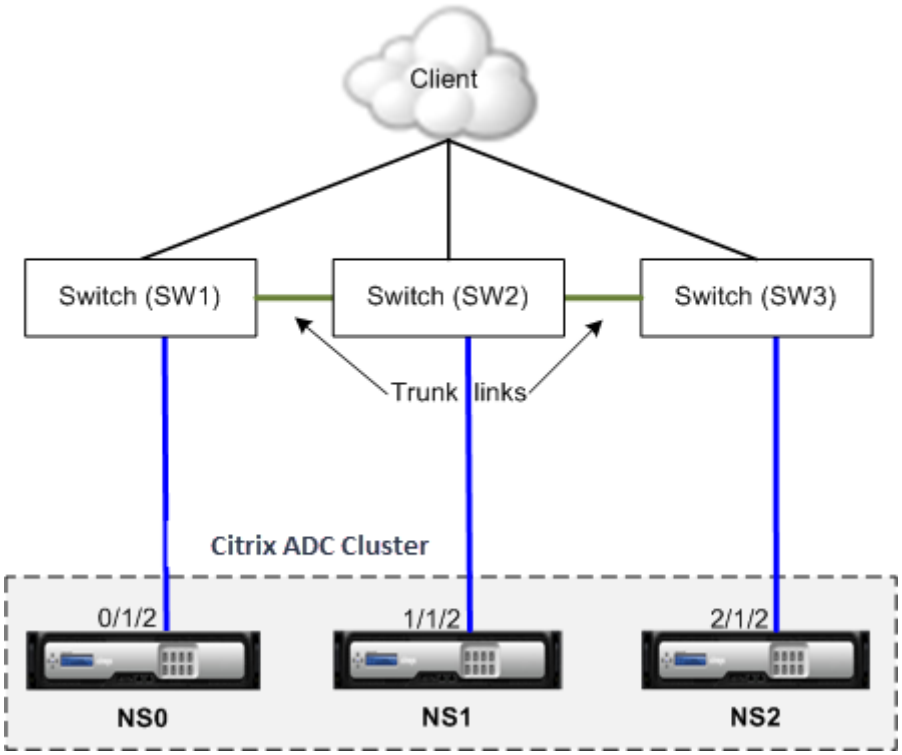
   //Para las interfaces del servidor. Repita para cada interfaz…

```
> interface Ethernet2/49
> switchport access vlan 300
> switchport mode access
> end
```

Conmutador diferente para cada nodo

August 20, 2021

En esta implementación, cada nodo de clúster está conectado a un conmutador diferente y se configuran enlaces troncales entre los switches.



Las configuraciones de clúster son las mismas que las otras implementaciones. La mayoría de las configuraciones del lado del cliente se realizan en los conmutadores del lado del cliente.

Configuraciones de clúster de ejemplo

August 20, 2021

El siguiente ejemplo se puede utilizar para configurar un clúster de cuatro nodos con ECMP, clúster LA o Linksets.

1. Cree el clúster.
    - Inicie sesión en el primer nodo.
    - Agregue la instancia del clúster.

```
1   > add cluster instance 1
```

    - Agregue el primer nodo al clúster.


```
> add cluster node 0 10.102.33.184 -backplane 0/1/1
```

- Habilite la instancia del clúster.

```
> enable cluster instance 1
```

- Agregue la dirección IP del clúster.

```
> add ns ip 10.102.33.185 255.255.255.255 -type CLIP
```

- Guarde las configuraciones.

```
> save ns config
```

- Reinicie el dispositivo en caliente.

```
> reboot -warm
```

2. Agregue los otros tres nodos al clúster.
   - Inicie sesión en la dirección IP del clúster.
   - Agregue el segundo nodo al clúster.

```
> add cluster node 1 10.102.33.187 -backplane 1/1/1
```

   - Agregue el tercer nodo al clúster.

```
> add cluster node 2 10.102.33.188 -backplane 2/1/1
```

   - Agregue el cuarto nodo al clúster.

```
> add cluster node 3 10.102.33.189 -backplane 3/1/1
```

3. Unir los nodos agregados al clúster. Este paso no es aplicable al primer nodo.

- Inicie sesión en cada nodo recién agregado.
- Unir el nodo al clúster.

```
1   > join cluster -clip 10.102.33.185 -password nsroot
```

- Guarde la configuración.

```
1   > save ns config
```

- Reinicie el dispositivo en caliente.

```
1   > reboot -warm
```

4. Configure el clúster de Citrix ADC a través de la dirección IP del clúster.

   // Habilitar la función de equilibrio de carga

```
1      > enable ns feature lb
```

   // Agregar un servidor virtual de equilibrio de carga

```
1      > add lb vserver first_lbvserver http
2      ....
3      ....
```

5. Configure cualquiera de los siguientes mecanismos de distribución de tráfico (ECMP, clúster LA o Linkset) para el clúster.

   ECMP

   - Inicie sesión en la dirección IP del clúster.
   - Habilite el protocolo de redirección OSPF.

```
1   > enable ns feature ospf
```


- Agregue una VLAN.

```
1   > add vlan 97
```

- Enlace las interfaces de los nodos del clúster a la VLAN.

```
1   > bind vlan 97 -ifnum 0/1/4 1/1/4 2/1/4 3/1/4
```

- Agregue un SNIP detectado en cada nodo y habilite el redirección dinámica en él.

```
1   > add ns ip 1.1.1.10 255.255.255.0 -ownerNode 0 -
       dynamicRouting ENABLED
2   > add ns ip 1.1.1.11 255.255.255.0 -ownerNode 1 -
       dynamicRouting ENABLED
3   > add ns ip 1.1.1.12 255.255.255.0 -ownerNode 2 -
       dynamicRouting ENABLED
4   > add ns ip 1.1.1.13 255.255.255.0 -ownerNode 3 -
       dynamicRouting ENABLED
```

- Enlazar una de las direcciones SNIP a la VLAN.

```
1   > bind vlan 97 -ipAddress 1.1.1.10 255.255.255.0
```

- Configure el protocolo de redirección en ZeBO mediante el shell de VTYSH.

  Cluster estático LA

  - Inicie sesión en la dirección IP del clúster.
  - Agregue un canal LA de clúster.

    ```
    1   > add channel CLA/1 -speed 1000
    ```

  - Enlace las interfaces al canal LA del clúster.

    ```
    1   > bind channel CLA/1 0/1/5 1/1/5 2/1/5 3/1/5
    ```


- Realice una configuración equivalente en el conmutador.

  Cluster dinámico LA

  * Inicie sesión en la dirección IP del clúster.
  * Agregue las interfaces al canal LA del clúster.

```
> set interface 0/1/5 -lacpmode active -lacpkey 5 -
   lagtype cluster
> set interface 1/1/5 -lacpmode active -lacpkey 5 -
   lagtype cluster
> set interface 2/1/5 -lacpmode active -lacpkey 5 -
   lagtype cluster
> set interface 3/1/5 -lacpmode active -lacpkey 5 -
   lagtype  cluster
```

  * Realice una configuración equivalente en el conmutador.

  Conjuntos de vínculos. Suponga que el nodo con NodeID 3 no está conectado al conmutador. Debe configurar un conjunto de vínculos para que el nodo no conectado pueda utilizar las otras interfaces de nodo para comunicarse con el conmutador.

a) Inicie sesión en la dirección IP del clúster.

b) Agregar un juego de vínculos.

```
> add linkset LS/1
```

c) Enlazar las interfaces conectadas al conjunto de vínculos.

```
> bind linkset LS/1 -ifnum 0/1/6 1/1/6 2/1/6
```

6. Actualice el estado de los nodos del clúster a ACTIVE.

```
> set cluster node 0 -state ACTIVE
> set cluster node 1 -state ACTIVE
> set cluster node 2 -state ACTIVE
> set cluster node 3 -state ACTIVE
```


Uso de VRRP en una configuración de clúster

August 20, 2021

El protocolo de redundancia de enrutador virtual (VRRP) se admite en una configuración de clúster para IPv4 e IPv6. Las dos funciones VRRP admitidas en una configuración de clúster son VRRP basado en interfaz y VRRP basado en IP.

VRRP basado en IP

En VRRP basado en IP, las direcciones VIP seccionadas enlazadas al mismo VRID se configuran en todos los nodos de una configuración de clúster. Estas direcciones VIP están activas en todos los nodos

Uno de los nodos del clúster actúa como propietario de VRID y envía el anuncio VRRP a otros nodos. Si se produce un error en el nodo propietario de VRID, otro nodo del clúster asume la propiedad del VRID y comienza a enviar anuncios de VRRP. También puede asignar un nodo de clúster específico como propietario del VRID.

> **Nota**
>
> Citrix recomienda utilizar el método basado en IP para la implementación de VRRP en clúster.

Configuración de VRRP basado en IP para IPv4

Realice las siguientes tareas en una configuración de clúster para configurar VRRP basado en IP para IPv4:

- **Agregue un VRID**. Un VRID es un entero utilizado por la configuración del clúster para formar una dirección MAC virtual. La dirección VMAC genérica tiene la forma de 00:00:5 e: 00:02: <VRID>.
- **(Opcional) Asigne un nodo como propietario de la dirección MAC virtual**. Puede establecer el parámetro del nodo propietario (mientras agrega o modifica VRID6) en el ID del nodo del clúster para asignarlo como propietario de la dirección MAC virtual. Si el nodo propietario asignado falla, uno de los nodos del clúster UP se elige dinámicamente como propietario de la dirección MAC virtual. Puede establecer el nodo propietario mediante el `set vrID <id> -ownerNode <positive_interger>` comando.
- **Enlace el VRID a la dirección VIP de los nodos**. Enlazar el VRID creado a la dirección VIP rayada.

Para agregar un VRID mediante la CLI

En el símbolo del sistema, escriba:


```
- add vrid <ID> [-ownerNode <positive_integer>]
- show vrid <ID>
```

Para vincular el VRID a la dirección VIP mediante la CLI

En el símbolo del sistema, escriba:

- `set ns ip <IPv4Address> -vrid <ID><!--NeedCopy-->`
- `show vrid <ID><!--NeedCopy-->`

Para agregar un VRID mediante la GUI

1. Vaya a **Sistema > Red > VMAC** y, en la ficha **VMAC**, haga clic en **Agregar**.
2. En la página Crear **VMAC**, especifique un valor en el campo **Id. de enrutador virtual** y, a continuación, haga clic en **Crear**.

Para vincular el VRID a una dirección VIP mediante la GUI

1. Vaya a **Sistema > Red > IPs**, en la ficha **IPv4s**, seleccione una dirección VIP y haga clic en **Modificar**.
2. Establezca el parámetro **ID del enrutador virtual** mientras modifica la configuración VIP.

```
> add vrid 90
 Done
> set ns ip 192.0.2.90 - vrid 90
 Done
```

Configuración de VRRP basado en IP para IPv6

Realice las siguientes tareas en una configuración de clúster para configurar VRRP basado en IP para IPv6:

- **Agregue un VRID6**. Un VRID6 es un entero utilizado por la configuración del clúster para formar una dirección MAC6 virtual. La dirección VMAC6 genérica tiene la forma de 00:00:5e:00:02 <VRID6>.
- **(Opcional) Asigne un nodo como propietario de la dirección MAC6 virtual**. Puede establecer el parámetro del nodo propietario (mientras agrega o modifica VRID6) en el ID del nodo del clúster para asignarlo como propietario de la dirección MAC6 virtual. Si el nodo propietario

asignado falla, uno de los nodos del clúster UP se elige dinámicamente como propietario de la dirección MAC6 virtual.

- **Enlace el VRID6 a la dirección VIP6 de los nodos**. Enlazar el VRID6 creado a la dirección VIP6 seccionada.

Para agregar un VRID6 mediante la CLI

En el símbolo del sistema, escriba:

- `add vrid6 <ID> [-ownerNode <positive_integer>]<!--NeedCopy-->`
- `show vrid6 <ID><!--NeedCopy-->`

Para vincular la dirección VRID6 a VIP6 mediante la CLI

En el símbolo del sistema, escriba:

- `set ns ip6 <IPv6Address> -vrid6 <ID><!--NeedCopy-->`
- `show vrid6 <ID><!--NeedCopy-->`

Para agregar un VRID6 mediante la GUI

1. Vaya a **Sistema > Red > VMAC** y, en la ficha **VMAC6**, haga clic en **Agregar**.
2. En la página **Crear MAC6 virtual**, especifique un valor en el campo **Id. de enrutador virtual** y, a continuación, haga clic en **Crear**.

Para vincular el VRID6 a una dirección VIP6 mediante el uso de la GUI

1. Vaya a **Sistema > Red > IPs**, en la ficha **IPv6s**, seleccione una dirección VIP y haga clic en **Modificar**.
2. Establezca el parámetro **ID del enrutador virtual** mientras modifica la configuración de VIP6.

```
1 > add vrid6 90
2  Done
3 > set ns ip6 2001:db8::5001  - vrid6 90
4  Done
```

VRRP basado en interfaz

En la función VRRP basada en interfaz, se configura la misma dirección MAC virtual en ambos nodos del clúster. Esta dirección MAC virtual se utiliza en anuncios GARP y respuestas ARP para las direc-

ciones IP configuradas en un nodo. Esta función es útil en una configuración de clúster de dos nodos de repuesto activo que tiene dispositivos/enrutadores externos que no aceptan anuncios GARP.

> **Nota**
>
> La función VRRP basada en la interfaz solo se aplica a un clúster de dos nodos con un nodo en estado activo y el otro nodo que sirve como repuesto.

Con la misma dirección MAC virtual en ambos nodos del clúster, cuando el nodo activo cae y el nodo de reserva toma el control como activo, la dirección MAC de las direcciones IP en el nuevo nodo activo permanece sin cambios y no es necesario actualizar las tablas ARP en los dispositivos o enrutadores externos.

Configuración de VRRP basado en interfaz para IPv4

Realice las siguientes tareas en una configuración de clúster para configurar VRRP basado en interfaz para IPv4:

- **Agregue un VRID**. Un VRID es un entero utilizado por la configuración del clúster para formar una dirección MAC virtual.
- **Enlace el VRID a las interfaces de nodo**. Enlazar las interfaces al VRID creado. Las interfaces enlazadas (en el nodo activo actual) utilizan la dirección MAC virtual en anuncios GARP y respuestas ARP para sus direcciones IPv4. Debe asociar el VRID a las interfaces de ambos nodos de la configuración del clúster de reserva activa. Esto se debe a que, a diferencia de una configuración de alta disponibilidad, los identificadores de interfaz difieren en una configuración de clúster.

Para agregar un VRID mediante la CLI

En el símbolo del sistema, escriba:

```
1 - add vrid <ID>
2 - show vrid <ID>
```

Para vincular el VRID a una interfaz mediante la CLI

En el símbolo del sistema, escriba:

```
1 - bind vrid <ID> -ifnum <interface_name>
2 - show vrid <ID>
```


Para agregar un VRID y vincularlo a interfaces mediante el uso de la GUI

1. Vaya a **Sistema > Red > VMAC** y, en la ficha **VMAC**, haga clic en **Agregar**.
2. En la página **Crear MAC virtual**, especifique un valor en el campo Id. de enrutador **virtual***, enlace interfaces en la sección **Interfaces asociadas** y, a continuación, haga clic en **Crear**.

```
> add vrid 300
 Done
> bind vrid 300 -ifnum 1/1/2 2/1/3
 Done
```

Configuración de VRRP basado en interfaz para IPv6

Realice las siguientes tareas en una configuración de clúster para configurar VRRP basado en interfaz para IPv6:

- **Agregue un VRID6**. Un VRID6 es un entero utilizado por la configuración del clúster para formar una dirección MAC6 virtual. La dirección VMAC6 genérica tiene la forma de 00:00:5 e: 00:01: <VRID6>.
- **Enlace el VRID6 a interfaces de nodo**. Enlazar las interfaces al VRID6 creado. Las interfaces enlazadas (en el nodo activo actual) utilizan la dirección MAC6 virtual en anuncios GARP y respuestas ARP para sus direcciones IPv6. Debe asociar el VRID6 a las interfaces de ambos nodos de la configuración del clúster de reserva activa. Esto se debe a que, a diferencia de una configuración de alta disponibilidad, los identificadores de interfaz difieren en una configuración de clúster.

Para agregar un VRID6 mediante la CLI

En el símbolo del sistema, escriba:

```
-  add vrid6 <ID>
-  show vrid6 <ID>
```

Para vincular el VRID6 a una interfaz mediante la CLI

En el símbolo del sistema, escriba:

- `bind vrid6 <ID> -ifnum <interface_name><!--NeedCopy-->`
- `show vrid6 <ID><!--NeedCopy-->`

Para agregar un VRID6 y vincularlo a interfaces mediante el uso de la GUI

1. Navegue **Sistema > Red > VMAC** y, en la ficha **VMAC6**, haga clic en **Agregar**.
2. En la página **Crear MAC6 virtual**, especifique un valor en el campo **Id. de enrutador virtual**, enlace las interfaces en la sección **Interfaces asociadas** y, a continuación, haga clic en **Crear**.

```
> add vrid6 100
 Done
> bind vrid6 100 -ifnum 0/1/1 1/1/2 2/1/3
 Done
```

Servicios de supervisión en un clúster mediante supervisión de rutas

August 20, 2021

En una configuración de clúster, la propiedad de los servicios de supervisión se distribuye entre los nodos. Por lo tanto, diferentes nodos supervisan diferentes servicios. El nodo que supervisa un servicio se denomina propietario del servicio. Solo el propietario del servicio sondea el servidor para supervisar el estado de los servicios asignados a él. Además, comunica el estado de los servicios a todos los demás nodos del clúster. El inconveniente de la supervisión distribuida es que no se determina la conectividad de red y el estado de enlace entre todos los nodos y el servidor. Para superar este inconveniente, puede usar la supervisión de rutas.

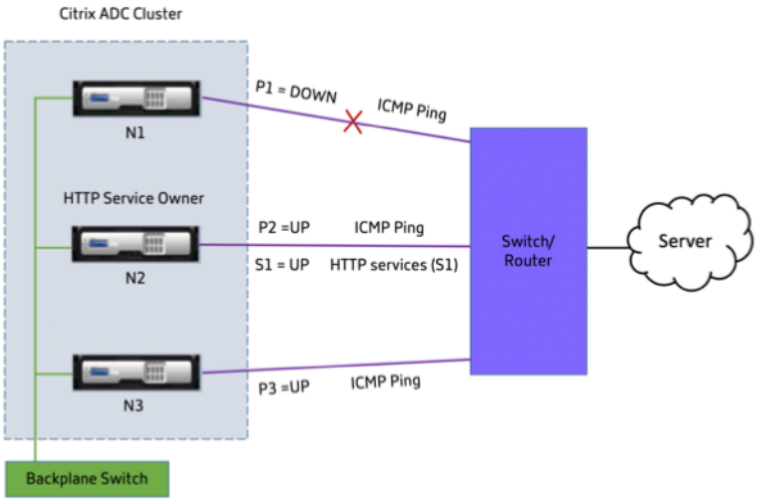
> **Nota**
>
> No puede seleccionar un nodo para supervisar un servicio. La selección de nodos para supervisar un servicio se realiza a través de un mecanismo interno. Puede ver el nodo propietario para supervisar los servicios mediante el `show serviceGroup <service group name>` comando `show service <service name>` y.

La supervisión de rutas comprueba la conectividad de red y el estado del vínculo entre un nodo y el servicio proporcionado por el servidor. Un nodo envía pings ICMP para verificar si el servidor es accesible o no.

Cómo funciona la supervisión de rutas

Considere un ejemplo de un clúster Citrix ADC que consta de tres nodos N1, N2 y N3. N2 es el propietario del servicio que supervisa el estado de los servicios HTTP (S1). Se anuncia el estado del servicio a otros nodos del clúster. La supervisión de rutas está habilitada en todos los nodos del clúster, para todos los servicios. Cada nodo envía solo un ping ICMP al servidor. El propietario del servicio envía

tanto la solicitud de servicio HTTP como un ping ICMP. Cada nodo informa su estado de supervisión de ruta al propietario del servicio.



Los dos parámetros siguientes determinan el estado del servicio de un nodo:

- S = estado del servicio anunciado por el propietario del servicio
- P = estado de supervisión de ruta de cada nodo

Si un nodo puede llegar a un servidor o no, determina el estado de supervisión de ruta para ese nodo.

En la tabla siguiente se muestra el estado del servicio establecido en función del estado de supervisión de rutas, cuando el parámetro pathMonitorIndv está habilitado o inhabilitado.

Parámetro	Estado de supervisión de rutas	Estado del servicio
PathMonitorInDV = NO; Es la configuración predeterminada.	P1 = DOWN	S1 = DOWN
	P2 = UP	S1 = DOWN
	P3 = UP	S1 = DOWN
PathMonitorIndV = SÍ	P1 = DOWN	S1 = DOWN
	P2 = UP	S1 = UP
	P3 = UP	S1 = UP

En este ejemplo, el propietario del servicio decide el estado del servicio para todos los nodos en función del nodo cuyo estado de supervisión de ruta está establecido en DOWN. Si el estado de supervisión de rutas para cualquiera de los nodos es DOWN, el propietario del servicio establece el estado

del servicio para todos los nodos como DOWN. El estado del servicio para todos los nodos se establece en UP solo si el estado de supervisión de ruta para cada uno de los nodos es UP.

Puede utilizar la supervisión de rutas para nodos individuales habilitando el parámetro PathMonitorIndV. Este parámetro permite al propietario del servicio establecer el estado del servicio para cada nodo en función del estado de supervisión de ruta de ese nodo respectivo.

> **Nota**
>
> Si se establece el parámetro PathMonitorInv, algunas funciones como la persistencia podrían romperse.

Configuración de la supervisión de rutas

La supervisión de rutas es aplicable a todos los servicios y grupos de servicios. El parámetro de supervisión de rutas está inhabilitado de forma predeterminada.

Para habilitar la supervisión de rutas para servicios/grupos de servicios mediante la CLI

En el símbolo del sistema, escriba:

```
add service <service name> <IP address> <service type> <port> [-
    pathMonitor <YES | NO>] [-pathMonitorIndv <YES | NO>]

add servicegroup <servicegroup name> <service type> [-pathMonitor <YES
    | NO>] [-pathMonitorIndv <YES | NO>]
<!--NeedCopy-->
```

Ejemplo:

```
add service s1 1.1.1.1 HTTP 80 -pathMonitor YES
add servicegroup sg_1 HTTP -pathMonitor YES

add service s1 1.1.1.1 HTTP 80 -pathMonitor YES -pathMonitorIndv YES
add servicegroup sg_1 HTTP -pathMonitor YES -pathMonitorIndv YES
<!--NeedCopy-->
```

También puede establecer el parámetro de supervisión de rutas desde el comando set, de la siguiente manera:


```
set service <service name> [-pathMonitor <YES | NO>] [-pathMonitorIndv
    <YES | NO>]
set servicegroup <servicegroup name> [-pathMonitor <YES | NO>] [-
    pathMonitorIndv <YES | NO>]
<!--NeedCopy-->
```

Ejemplo:

```
set service s1 -pathMonitor YES
set servicegroup sg_1 -pathMonitor YES


set service s1 -pathMonitorIndv YES
set servicegroup sg_1 -pathMonitorIndv NO
<!--NeedCopy-->
```

Para habilitar la supervisión de rutas para servicios/grupos de servicios mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servicios**.

   Para grupos de servicios, vaya a **Administración del tráfico** > **Equilibrio de carga** > **Grupos de servicio**.

2. En el panel **Servicios/Grupos de servicios**, seleccione un grupo de servicio/servicio de la lista y, a continuación, haga doble clic para abrirlo.
3. En la ficha **Configuración del servicio**, haga clic en **Modificar**.
4. Seleccione **Supervisión de rutas**.
5. Seleccione **Supervisión individual de rutas**, si quiere aplicarla y, a continuación, haga clic en **Aceptar**.

> **Nota**
>
> Solo puede habilitar la supervisión de rutas individuales si habilita la supervisión de rutas.

Copia de seguridad y restauración de la configuración del clúster

January 12, 2021

Puede realizar una copia de seguridad del estado actual de un nodo de clúster de Citrix ADC. Posteriormente, puede utilizar los archivos de copia de seguridad para restaurar el nodo al mismo estado de clúster. Como medida de precaución, debe utilizar esta función antes de realizar una actualización en los nodos del clúster.

Realice una copia de seguridad de la instalación

Puede realizar una copia de seguridad básica o completa dependiendo de lo siguiente:

- Tipo de datos que se va a realizar una copia de seguridad.
- Frecuencia con la que se crea una copia de seguridad.
- **Respaldos básicos.** Solo hace copias de seguridad de los archivos de configuración. Es posible que quiera realizar este tipo de copia de seguridad con frecuencia, ya que los archivos de los que realiza la copia de seguridad cambian constantemente. Los archivos de los que se realiza una copia de seguridad se enumeran en la tabla.

Directorio

Subdirectorio o archivos

/nsconfig/

- ns.conf
- ZebOS.conf
- rc.netscaler
- snmpd.conf
- nsbefore.sh
- nsafter.sh
- inetd.conf
- ntp.conf
- syslog.conf
- newsyslog.conf
- crontab
- host.conf
- anfitriones
- ttys
- sshd_config
- httpd.conf
- monitrc
- rc.conf
- ssh_config
- hora local

- issue
- número.net

/var/

- download/*
- log/wicmd.log
- wi/tomcat/webapps/*
- wi/tomcat/logs/*
- wi/tomcat/conf/catalina/localhost/*
- nslw.bin/etc/krb.conf
- nslw.bin/etc/krb.keytab
- netscaler/locdb/*
- lib/comose/db/*
- vpn/bookmark/*
- netscaler/crl
- nstemplates/*
- learnt_datos/*

/netscaler/

- custom.html
- vsr.html
- **Copia de seguridad completa.** Aparte de los archivos de los que se realiza una copia de seguridad básica, una copia de seguridad completa realiza copias de seguridad de algunos archivos actualizados con menos frecuencia. Los archivos de los que se realiza una copia de seguridad cuando se utiliza la opción de copia de seguridad completa se enumeran en la tabla.

Directorio

Subdirectorio o archivos

/nsconfig/

- ssl/*
- licencia/*
- fips/*

/var/

- netscaler/ssl/*
- wi/java_home/jre/lib/security/cacerts/*
- wi/java_home/lib/seguridad/cacerts/*

> **Importante**
>
> La copia de seguridad y restauración no funcionan si CLAG está configurado en una configuración de clúster SDX.

La copia de seguridad se almacena como un archivo TAR comprimido en el directorio /var/ns_sys_backup/. Para evitar problemas debido a la falta de disponibilidad de espacio en disco, puede almacenar un máximo de 50 archivos de copia de seguridad en este directorio. Puede utilizar el comando rm system backup para eliminar archivos de copia de seguridad existentes, de modo que pueda crear más copias de seguridad.

Cuando realiza la operación de copia de seguridad en un CLIP de una configuración de clúster, se crean archivos de copia de seguridad en cada uno de los nodos del clúster.

Cómo realizar una copia de seguridad de una configuración de clúster

Para realizar una copia de seguridad de la configuración del clúster en CLIP mediante la CLI de Citrix ADC.

En el símbolo del sistema, haga lo siguiente:

- Guarde la configuración.

  ```
  save ns config<!--NeedCopy-->
  ```

- Cree el archivo de copia de seguridad (básico o completo).

  “‘create system backup []–level (basic | full)][-comment]

```
**Ejemplo**

```create system backup cluster-backup-1  -level basic<!--
   NeedCopy-->
```

El comando anterior crea un archivo TAR de copia de seguridad en cada uno de los nodos del clúster con el nombre de archivo especificado. Por ejemplo, el archivo Cluster-Backup-1.tgz se crea en cada uno de los nodos del clúster.

> **Nota**
>
> Si no se especifica el nombre de archivo, se crean copias de seguridad de los archivos TAR en cada uno de los nodos del clúster con la siguiente convención de nomenclatura:
>
> - `backup_<level>_<nsip_address of the cluster node 0>_<date-timestamp >.tgz<!--NeedCopy-->`
> - `backup_<level>_<nsip_address of the cluster node 1>_<date-timestamp`


```

> >.tgz<!--NeedCopy-->
>
> Por ejemplo, en una configuración de clúster de tres nodos,
>
> - backup_<level>_<nsip_address of the cluster node 0>_<date-timestamp >.tgz<!--NeedCopy--> se crea en el node0
> - backup _<level>_<nsip_address of the cluster node 1>_<date-timestamp >.tgz<!--NeedCopy--> se crea en el nodo1
> - backup_<level>_<nsip_address of the cluster node 2>_<date-timestamp >.tgz<!--NeedCopy--> se crea en el nodo2

- Compruebe los archivos de copia de seguridad creados en CLIP.

  ```
  show system backup<!--NeedCopy-->
  ```

Restaurar una configuración de clúster

Cuando un nodo de clúster se vuelve defectuoso, puede reemplazar este nodo por otro nuevo. Puede establecer el nuevo nodo para un clúster mediante un archivo de copia de seguridad del nodo defectuoso.

Por ejemplo, en una configuración de clúster de tres nodos, si node1 resulta defectuoso, puede reemplazar este nodo defectuoso por un nuevo nodo como node1. Mediante la operación de restauración, puede restaurar uno de los archivos de copia de seguridad del nodo defectuoso en el nuevo nodo.

> **Nota**
>
> La operación de restauración no se realiza correctamente si se cambia el nombre del archivo de copia de seguridad o si se modifica el contenido del archivo.

Cómo restaurar un nodo de clúster

Para restaurar un nodo de clúster mediante la CLI

En el símbolo del sistema, haga lo siguiente:

- Obtenga una lista de los archivos de copia de seguridad disponibles en CLIP.

  ```
  show system backup<!--NeedCopy-->
  ```

- Copie el archivo tar de copia de seguridad en el directorio /var/ns_sys_backup del nodo del clúster, que se va a restaurar.
- Agregue el archivo tar de copia de seguridad a la memoria del nodo del clúster ejecutando el siguiente comando en el nodo del clúster.

  “‘add system backup


```
**Ejemplo**

```add system backup CLUSTER-BACKUP-1.tgz<!--NeedCopy-->
```

> **Nota**
>
> El comando debe ejecutarse en el nodo del clúster que se va a restaurar.

- Restaure el nodo del clúster especificando el archivo de copia de seguridad.

  "'restore system backup

```
**Ejemplo**

```restore system backup CLUSTER-BACKUP-1.tgz<!--NeedCopy-->
```

> **Nota**
>
> El comando debe ejecutarse en el nodo del clúster que se va a restaurar.

- Reinicie el nodo del clúster.

  reboot

> **Nota**
>
> El comando debe ejecutarse en el nodo del clúster que se va a restaurar.

Actualizar o degradar el clúster de Citrix ADC

July 27, 2022

Todos los nodos de un clúster de Citrix ADC deben ejecutar la misma versión de software. Por lo tanto, para actualizar o degradar el clúster, debe actualizar o degradar cada dispositivo Citrix ADC del clúster, un nodo a la vez.

Un nodo que se está actualizando o degradando no se elimina del clúster. El nodo sigue siendo parte del clúster y sirve el tráfico sin interrupciones, excepto por el tiempo de inactividad cuando el nodo se reinicia después de actualizarse o bajarse de categoría.

Sin embargo, debido a que las versiones de software no coinciden entre los nodos del clúster, la propagación de la configuración está inhabilitada en el clúster. La propagación de la configuración se habilita solo después de que todos los nodos del clúster tengan la misma versión. Dado que la propagación de la configuración está inhabilitada durante la actualización al degradar un clúster, no puede realizar ninguna configuración a través de la dirección IP del clúster durante este tiempo.

Importante

- En una configuración de clúster con un parámetro global de conexión máxima (maxConn) establecido en un valor distinto de cero, las conexiones CLIP podrían fallar si se cumple alguna de las siguientes condiciones:

```
- Upgrading the setup from Citrix ADC 13.0 76.x build to
  Citrix ADC 13.0 79.x build.
- Restarting the CCO node in a cluster setup running Citrix
  ADC 13.0 76.x build.
```

Solución:

```
\- Antes de actualizar una configuración de clúster desde la
  compilación de Citrix ADC 13.0 76.x a la compilación de
  Citrix ADC 13.0 79.x, el parámetro global de conexión máxima
   (maxConn) debe establecerse en cero. Después de actualizar
  la configuración, puede configurar el parámetro maxConn en
  el valor deseado y, a continuación, guardar la configuración
  .
\- La compilación de  Citrix ADC 13.0 76.x no es adecuada para
  configuraciones de clúster. Citrix recomienda no utilizar la
   compilación Citrix ADC 13.0 76.x para una configuración de
  clúster.
```

- En una configuración de clúster, un dispositivo Citrix ADC podría fallar cuando:

```
- upgrading the setup from Citrix ADC 13.0 47.x or 13.0 52.x
  build to a later build, or
- upgrading the setup to Citrix ADC 13.0 47.x or 13.0 52.x
  build
```

Solución alternativa: Durante el proceso de actualización, lleve a cabo los siguientes pasos:

```
\- Inhabilite todos los nodos de clúster y, a continuación,
  actualice cada nodo
\- Habilite todos los nodos de clúster después de actualizar
  todos los nodos.
```


Puntos a tener en cuenta antes de actualizar o degradar el clúster

> - **IMPORTANTE:**
>
> Es importante que tanto los cambios de actualización como las personalizaciones se apliquen a un dispositivo Citrix ADC actualizado. Por lo tanto, si tiene archivos de configuración personalizados en el directorio `/etc`, consulte Consideraciones sobre la actualización para los archivos de configuración personalizados antes de continuar con la actualización.

- No puede agregar nodos de clúster mientras actualiza o descalifica la versión del software del clúster.
- Puede realizar configuraciones a nivel de nodo a través de la dirección NSIP de nodos individuales. Asegúrese de realizar las mismas configuraciones en todos los nodos para mantenerlos sincronizados.
- No puede ejecutar el comando `start nstrace` desde la dirección IP del clúster cuando se está actualizando el clúster. Sin embargo, puede obtener el seguimiento de nodos individuales realizando esta operación en nodos de clúster individuales mediante su dirección NSIP.
- La compilación de Citrix ADC 13.0 76.x no es adecuada para configuraciones de clúster. Citrix recomienda no utilizar la compilación Citrix ADC 13.0 76.x para una configuración de clúster.
- Las compilaciones de Citrix ADC 13.0 47.x y 13.0 52.x no son adecuadas para una configuración de clúster. Se debe a que las comunicaciones entre nodos no son compatibles en estas compilaciones.
- Cuando se actualiza un clúster, es posible que los nodos actualizados tengan activadas algunas funciones adicionales que no están disponibles en los nodos que aún no se han actualizado. Se genera una advertencia de falta de coincidencia de licencias mientras se actualiza el clúster. Esta advertencia se resuelve automáticamente cuando se actualizan todos los nodos del clúster.

> **Importante**
>
> - Citrix recomienda esperar a que el nodo anterior se active antes de actualizar o degradar el siguiente nodo.
> - Citrix recomienda que el nodo de configuración del clúster se actualice o descienda en último lugar para evitar desconexiones múltiples de las sesiones de IP del clúster.

Para actualizar o degradar el software de los nodos del clúster

1. Asegúrese de que el clúster sea estable y de que las configuraciones estén sincronizadas en todos los nodos.
2. Acceda a cada nodo a través de su dirección NSIP y realice lo siguiente:

- Actualizar o degradar el nodo del clúster. Para obtener información detallada sobre la actualización y la degradación del software de un dispositivo, consulte Actualizar y degradar un dispositivo Citrix ADC.
- Guarde las configuraciones.
- Reinicie el dispositivo.

3. Repita el paso 2 para cada uno de los otros nodos del clúster.

Operaciones admitidas en nodos de clúster individuales

January 12, 2021

Como regla general, los dispositivos Citrix ADC que forman parte de un clúster no se pueden configurar individualmente desde su dirección NSIP. Sin embargo, hay algunas operaciones que son una excepción a esta regla. Estas operaciones, cuando se ejecutan desde la dirección NSIP, no se propagan a otros nodos de clúster.

Las operaciones son:

- cluster instance (set | rm | enable | disable)
- cluster node (set | rm)
- ns traza (inicio | mostrar | detener)
- interface (set | enable | disable)
- route (add | rm | set | unset)
- ARP (add | rm | send -all)
- force cluster sync
- sync cluster files
- inhabilitar la sincronización NTP
- save ns config
- reboot
- shutdown

Por ejemplo, cuando ejecuta el comando `disable interface 1/1/1` desde la dirección NSIP de un nodo de clúster, la interfaz solo se inhabilita en ese nodo. Dado que el comando no se propaga, la interfaz 1/1/1 permanece habilitada en todos los demás nodos del clúster.

Compatibilidad con clústeres heterogéneos

August 20, 2021

El dispositivo Citrix ADC admite un clúster heterogéneo en una implementación de clúster. Un clúster heterogéneo abarca nodos de diferentes hardware Citrix ADC y puede tener una combinación de diferentes plataformas en el mismo clúster.

> **Importante**
>
> La formación o compatibilidad de un clúster heterogéneo es posible y solo se limita a las plataformas de hardware MPX.

La compatibilidad y la formación del clúster heterogéneo dependen de ciertos modelos Citrix ADC. En la siguiente tabla se enumeran las plataformas que se admiten en la formación de un clúster heterogéneo, con un número igual de motores de paquetes.

Número de motores de paquetes	Plataformas de hardware MPX	Plataformas de hardware MPX compatibles para formar clústeres heterogéneos
5	MPX 11500	MPX 14020
7	MPX 11515	MPX 14040
9	MPX 11530	MPX 14060

En la siguiente tabla se enumeran las plataformas que se admiten en la formación de un clúster heterogéneo, con un número desigual de motores de paquetes.

Plataformas de hardware	Plataformas de hardware compatibles para formar clústeres heterogéneos
MPX 150XX	MPX 140XX

Para obtener más información sobre cómo crear una implementación heterogénea en clúster de dispositivos Citrix ADC MPX con el número diferente de motores de paquetes en diferentes chipsets SSL, consulte la sección **Implementaciones de clúster heterogéneas** en configuración de descarga SSL.

> **Nota**
>
> Antes de la versión 13.0 compilación 47.x, si ejecuta el comando “join cluster” desde el nodo que tiene un número desigual de motores de paquetes, aparece el siguiente mensaje de error: “No coinciden en el número de PPE activos entre CCO y nodo local”.

Puntos a tener en cuenta

1. La configuración adicional de CPU de administración debe ser la misma en todos los nodos del clúster.
2. El nodo recién agregado debe tener la misma capacidad en los planos de datos y en el plano posterior que la de los nodos de clúster existentes.
3. Si hay dispositivos de plataforma mixta que admiten diferentes cifrados, entonces el clúster acordaría una lista de cifrado común.

Preguntas frecuentes

August 20, 2021

Una lista de las preguntas frecuentes sobre clústeres.

¿Cuántos dispositivos Citrix ADC se pueden incluir en un único clúster Citrix ADC?

Un clúster de Citrix ADC puede incluir un dispositivo o hasta 32 dispositivos virtuales o hardware Citrix ADC nCore. Cada uno de estos nodos debe cumplir los criterios especificados en Requisitos previos para nodos de clúster.

¿Puede un dispositivo Citrix ADC formar parte de varios clústeres?

No. Un dispositivo Citrix ADC solo puede pertenecer a un clúster.

¿Qué es una dirección IP de clúster? ¿Cuál es su máscara de subred?

La dirección IP del clúster es la dirección de administración de un clúster de Citrix ADC. Todas las configuraciones de clúster deben realizarse accediendo al clúster a través de esta dirección. La máscara de subred de la dirección IP del clúster se fija en 255.255.255.255.

¿Cómo puedo crear un nodo de clúster específico como coordinador de configuración del clúster?

Para establecer manualmente un nodo específico como coordinador de configuración del clúster, debe establecer la prioridad de ese nodo en el valor numérico más bajo (prioridad más alta). Para entender, consideremos un clúster con tres nodos que tienen las siguientes prioridades:

n1: 29, n2: 30, n3: 31

Aquí, n1 es el coordinador de configuración. Si quiere convertir n2 en coordinador de configuración, debe establecer su prioridad en un valor inferior a n1, por ejemplo, 28. Al guardar la configuración, n2 se convierte en el coordinador de configuración.

> **Nota**
>
> n2 con su valor de prioridad original de 30 se convierte en el coordinador de configuración cuando n1 desaparece. El nodo con el siguiente valor de prioridad más bajo se selecciona en caso de que el coordinador de configuración desaparezca.

¿Por qué las interfaces de red de un clúster están representadas en notación de 3 tuplas (n/u/c) en lugar de la notación regular de 2 tuplas (u/c)?

Cuando un dispositivo Citrix ADC forma parte de un clúster, debe poder identificar el nodo al que pertenece la interfaz. Por lo tanto, la convención de nomenclatura de interfaz de red para nodos de clúster se modifica de u/c a n/u/c, donde n indica el ID de nodo.

¿Cómo puedo establecer el nombre de host para un nodo de clúster?

El nombre de host de un nodo de clúster debe especificarse ejecutando el comando **set ns hostname** a través de la dirección IP del clúster. Por ejemplo, para establecer el nombre de host del nodo del clúster con ID 2, el comando es:

set ns hostname hostname1 -**ownerNode** 2

¿Puedo detectar automáticamente dispositivos Citrix ADC para poder agregarlos a un clúster?

Sí. La utilidad de configuración permite detectar dispositivos que están presentes en la misma subred que la dirección NSIP del coordinador de configuración. Para obtener más información, consulte Descubrimiento de dispositivos NetScaler.

¿Se ve afectada la capacidad de servicio de tráfico de un clúster si se quita o inhabilita un nodo o se reinicia o apaga o se inactiva?

Sí. Cuando cualquiera de estas operaciones se realiza en un nodo activo del clúster, el clúster tiene un nodo menos para servir el tráfico. Además, se terminan las conexiones existentes en este nodo.

Tengo varios dispositivos independientes, cada uno de los cuales tiene diferentes configuraciones. ¿Puedo agregarlos a un solo clúster?

Sí. Puede agregar dispositivos con configuraciones diferentes a un único clúster. Sin embargo, cuando se agrega el dispositivo al clúster, se borran las configuraciones existentes. Para utilizar las configuraciones disponibles en cada uno de los dispositivos individuales, debe:

1. Cree un único archivo*.conf para todas las configuraciones.
2. Modifique el archivo de configuración para quitar entidades que no se admiten en un entorno de clúster.
3. Actualice la convención de nomenclatura de las interfaces de formato 2-tupla (u/c) a formato 3-tupla (n/u/c).
4. Aplique las configuraciones al nodo coordinador de configuración del clúster mediante el comando batch.

¿Puedo migrar las configuraciones de un dispositivo Citrix ADC independiente o una configuración de HA a la configuración en clúster?

No. Cuando se agrega un nodo a una configuración agrupada, sus configuraciones se borran implícitamente mediante el comando **clear ns config** (con la opción **extendida**). Además, se borran las direcciones SNIP y todas las configuraciones de VLAN (excepto VLAN y NSVLAN predeterminados). Por lo tanto, se recomienda realizar una copia de seguridad de las configuraciones antes de agregar el dispositivo a un clúster. Antes de utilizar el archivo de configuración de copia de seguridad para el clúster, debe:

1. Modifique el archivo de configuración para quitar entidades que no se admiten en un entorno de clúster.
2. Actualice la convención de nomenclatura de interfaces de formato de dos tuplas (x/y) a formato de tres tuplas (x/y/z).
3. Aplique las configuraciones al nodo coordinador de configuración del clúster mediante el comando **batch**.

¿Las interfaces del plano posterior forman parte de las VLAN L3?

Sí, de forma predeterminada, las interfaces de backplane tienen presencia en todas las VLAN L3 configuradas en el clúster.

¿Cómo puedo configurar un clúster que incluya nodos de diferentes redes?

> **Nota**
>
> Compatible con NetScaler 11.0 en adelante.

Un clúster que incluye nodos de diferentes redes se denomina clúster L3 (a veces denominado clúster en modo INC). En un clúster de L3, todos los nodos que pertenecen a una sola red deben agruparse en un solo grupo de nodos. Por lo tanto, si un clúster incluye dos nodos cada uno de tres redes diferentes, debe crear tres grupos de nodos (uno para cada red) y asociar cada uno de estos grupos de nodos con los nodos que pertenecen a esa red. Para obtener información de configuración, consulte los pasos para configurar un clúster.

¿Cómo puedo configurar/anular la configuración de NSVLAN en un clúster?

Realice una de las siguientes acciones:

- Para que la NSVLAN esté disponible en un clúster, asegúrese de que cada dispositivo tiene la misma NSVLAN configurada antes de agregarlo a un clúster.
- Para quitar la NSVLAN de un nodo de clúster, primero quite el nodo del clúster y, a continuación, elimine la NSVLAN del dispositivo.

Tengo un clúster configurado en el que algunos nodos de Citrix ADC no están conectados a la red externa. ¿Puede el clúster seguir funcionando normalmente?

Sí. El clúster admite un mecanismo denominado linksets, que permite que los nodos no conectados sirvan al tráfico mediante el uso de las interfaces de los nodos conectados. Los nodos no conectados se comunican con los nodos conectados a través del plano anterior del clúster. Para obtener más información, consulte Uso de conjuntos de enlaces.

¿Cómo pueden admitirse las implementaciones que requieren reenvío basado en Mac (MBF) en una configuración agrupada?

Las implementaciones que usan MBF deben usar conjuntos de vínculos. Para obtener más información, consulte Uso de conjuntos de enlaces.

¿Puedo ejecutar comandos desde la dirección NSIP de un nodo de clúster?

No. El acceso a nodos de clúster individuales a través de las direcciones NSIP es de solo lectura. Por lo tanto, cuando inicia sesión en la dirección NSIP de un nodo de clúster, solo puede ver las configuraciones y las estadísticas. No se puede configurar nada. Sin embargo, hay algunas operaciones que puede ejecutar desde la dirección NSIP de un nodo de clúster. Para obtener más información, consulte Operaciones admitidas en nodos individuales.

¿Puedo inhabilitar la propagación de la configuración entre nodos del clúster?

No, no puede inhabilitar explícitamente la propagación de configuraciones de clúster entre nodos de clúster. Sin embargo, durante una actualización o actualización de software, un error de discordancia de versión puede inhabilitar automáticamente la propagación de la configuración.

¿Puedo cambiar la dirección NSIP o cambiar la NSVLAN de un dispositivo Citrix ADC cuando forma parte del clúster?

No. Para realizar estos cambios, primero debe quitar el dispositivo del clúster, realizar los cambios y, a continuación, agregar el dispositivo al clúster.

¿El clúster Citrix ADC admite VLAN L2 y L3?

Sí. Un clúster admite VLAN entre nodos de clúster. Las VLAN deben configurarse en la dirección IP del clúster.

- **VLAN L2.** Puede crear una VLAN layer2 al vincular interfaces que pertenecen a diferentes nodos del clúster.
- **VLAN L3.** Puede crear una VLAN de capa3 vinculando direcciones IP que pertenecen a diferentes nodos del clúster. Las direcciones IP deben pertenecer a la misma subred. Asegúrese de que se cumple uno de los siguientes criterios. De lo contrario, los enlaces de VLAN L3 pueden fallar.
  - Todos los nodos tienen una dirección IP en la misma subred que la enlazada a la VLAN.
  - El clúster tiene una dirección IP seccionada y la subred de esa dirección IP está enlazada a la VLAN.

Cuando agrega un nodo a un clúster que solo ha detectado direcciones IP, la sincronización ocurre antes de que se asignen direcciones IP detectadas a ese nodo. En tales casos, los enlaces de VLAN L3 se pueden perder. Para evitar esta pérdida, agregue una IP seccionada o agregue los enlaces de VLAN L3 en el NSIP del nodo recién agregado.

¿Cómo puedo configurar SNMP en un clúster de Citrix ADC?

SNMP supervisa el clúster y todos los nodos del clúster de la misma manera que supervisa un dispositivo independiente. La única diferencia es que SNMP en un clúster debe configurarse a través de la dirección IP del clúster. Al generar capturas específicas de hardware, se incluyen dos varbinds más para identificar el nodo del clúster: ID de nodo y dirección NSIP del nodo.

¿Qué detalles debo tener disponibles cuando me pongo en contacto con el soporte técnico para problemas relacionados con clústeres?

El dispositivo Citrix ADC proporciona un comando **show techsupport -scope cluster** que extrae datos de configuración, información estadística y registros de todos los nodos del clúster. Ejecute este comando en la dirección IP del clúster.

La salida de este comando se guarda en un archivo denominado **collector_cluster_ <nsip_CCO> _P_ <date-timestamp> .tar.gz que está disponible en el directorio */var/tmp/support/cluster/* del coordinador de configuración.

Envíe este archivo al equipo de soporte técnico para depurar el problema.

¿Puedo usar direcciones IP seccionadas como la Gateway predeterminada de los servidores?

En implementaciones de clústeres, asegúrese de que la puerta de enlace predeterminada del servidor apunta a una dirección IP seccionado (si utiliza una dirección IP propiedad de Citrix ADC). Por ejemplo, en el caso de implementaciones LB con USIP habilitado, la puerta de enlace predeterminada debe ser una dirección SNIP seccionado.

¿Puedo ver las configuraciones de redirección de un nodo de clúster específico desde la dirección IP del clúster?

Sí. Puede ver y borrar las configuraciones específicas de un nodo especificando el nodo propietario al entrar en el shell de VTYSH.

Por ejemplo, para ver la salida de un comando en los nodos 0 y 1, el comando es el siguiente:

```
\> vtysh
ns# owner-node 0 1
ns(node-0 1)\# show cluster state
ns(node-0 1)\# exit-cluster-node
ns\#
```

¿Cómo puedo especificar el nodo para el que quiero establecer la prioridad del sistema LACP?

> **Nota**
>
> Compatible con NetScaler 10.1 en adelante.

En un clúster, debe establecer ese nodo como nodo propietario mediante el comando **set lacp**.

Por ejemplo: Para establecer la prioridad del sistema LACP para un nodo con ID 2:

```
set lacp -sysPriority 5 -ownerNode 2<!--NeedCopy-->
```

¿Cómo se configuran los túneles IP en una configuración de clúster?

> **Nota**
>
> Compatible con NetScaler 10.1 en adelante.

La configuración de túneles IP en un clúster es la misma que en un dispositivo independiente. La única diferencia es que en una configuración de clúster, la dirección IP local debe ser una dirección SNIP seccionada.

¿Cómo puedo agregar un conjunto de interfaces de conmutación por error (FIS) en los nodos de un clúster de Citrix ADC?

> **Nota**
>
> Compatible con NetScaler 10.5 en adelante.

En la dirección IP del clúster, especifique el ID del nodo del clúster en el que se debe agregar el FIS, mediante el comando de la siguiente manera:

```
add fis <name> -ownerNode <nodeId>
```

> **Notas**
>
> - El nombre FIS de cada nodo de clúster debe ser único.
> - Se puede agregar un canal LA de clúster a un FIS. Asegúrese de que el canal LA del clúster tiene una interfaz local como interfaz miembro.

Para obtener más información sobre FIS, consulte Configuración del conjunto de interfaces de conmutación por error.

¿Cómo se configuran los perfiles de red en una configuración de clúster?

> **Nota**
>
> Compatible con NetScaler 10.5 en adelante.

Puede enlazar direcciones IP detectada a un perfil de red. Este perfil de red se puede enlazar a un servidor o servicio virtual de equilibrio de carga detectado (que se define mediante un grupo de nodos). Se deben seguir las siguientes recomendaciones, de lo contrario, las configuraciones de perfil de red no se respetan y se utilizan los parámetros USIP/USNIP:

> **Nota**
>
> - Si el parámetro **estricto** del grupo de nodos se establece en **Sí**, el perfil de red debe contener como mínimo una dirección IP de cada miembro del grupo de nodos.
> - Si el parámetro **estricto** del grupo de nodos se establece en **No**, el perfil de red debe incluir al menos una dirección IP de cada uno de los nodos del clúster.

¿Cómo puedo configurar WionNS en una configuración de clúster?

> **Nota**
>
> Compatible con NetScaler 11.0, compilación 62.x en adelante.

Para utilizar WionNS en un clúster, debe hacer lo siguiente:

1. Asegúrese de que el paquete Java y el paquete WI están presentes en el mismo directorio en todos los nodos del clúster.
2. Cree un servidor virtual de equilibrio de carga que tenga configurada la persistencia.
3. Cree servicios con direcciones IP como la dirección NSIP de cada uno de los nodos del clúster a los que quiere servir el tráfico WI. Este paso solo se puede configurar mediante la CLI de Citrix ADC.
4. Enlazar los servicios al servidor virtual de equilibrio de carga.

> **Nota**
>
> Si está usando WionNS a través de una conexión VPN, asegúrese de que el servidor virtual de equilibrio de carga está establecido como WIHOME.

¿Se puede utilizar el canal LA del clúster para el acceso a la administración?

No. El acceso de administración a un nodo de clúster no debe configurarse en un canal LA del clúster (por ejemplo, CLA/1) ni en sus interfaces miembro. Esto se debe a que cuando el nodo está INACTIVO, la interfaz DE LA del clúster correspondiente se marca como apagado y, por lo tanto, pierde el acceso de administración.

¿Cómo se comunican los nodos de clúster entre sí y cuáles son los diferentes tipos de tráfico que atraviesa el plano posterior?

Un backplane es un conjunto de interfaces en las que una interfaz de cada nodo está conectada a un conmutador común, que se denomina conmutador de backplane del clúster. Los diferentes tipos de tráfico que pasa a través de un plano posterior, que es utilizado por la comunicación entre nodos son:

- Mensajería de nodo a nodo (NNM)
- Tráfico dirigido

- Propagación y sincronización de la configuración

Cada nodo del clúster utiliza una dirección especial del conmutador de backplane del clúster MAC para comunicarse con otros nodos a través del backplane. El MAC especial del clúster tiene la forma: **0x02 0x00 0x6F**<cluster_id> <node_id> <reserved>, donde <cluster_id> es el ID de instancia del clúster. El <node_id> es el número de nodo del dispositivo Citrix ADC que se agrega a un clúster.

> **Nota**
>
> La cantidad de tráfico que maneja un plano posterior tiene una sobrecarga de CPU insignificante.

¿Qué se enruta sobre el túnel GRE para el clúster de Capa 3?

Solo el tráfico de datos dirigidos pasa por el túnel GRE. Los paquetes se dirigen a través del túnel GRE hasta el nodo de la otra subred.

¿Cómo se intercambia la mensajería de nodo a nodo (NNM) y los mensajes de latido, y cómo se enrutan?

El NNM, los mensajes de latido y el protocolo de clúster son tráfico no direccional. Estos mensajes no se envían a través del túnel, pero se enrutan directamente.

¿Cuáles son las recomendaciones de MTU cuando las tramas Jumbo están habilitadas para el tráfico de túnel de clúster de capa 3?

Las siguientes son las recomendaciones de clúster de capa 3 de Jumbo MTU sobre el túnel GRE:

- La MTU Jumbo se puede configurar entre nodos de clúster a través de la ruta L3 para acomodar la sobrecarga del túnel GRE.
- La fragmentación no ocurre para paquetes de tamaño completo que deben ser orientados.
- La dirección del tráfico continúa funcionando incluso si las tramas Jumbo no están permitidas, pero con más sobrecarga debido a la fragmentación.

¿Cómo se genera y comparte la clave hash global en todos los nodos?

El `rsskey` para un dispositivo independiente se genera en el momento del arranque. En una configuración de clúster, el primer nodo contiene el `rsskey` del clúster. Cada nuevo nodo que se une al clúster sincroniza `rsskey`.

¿Cuál es la necesidad de `set rsskeytype -rsskey symmetric` comando para *: *, USIP activado, `useproxyport` off, topologías?

No es específico de un clúster, sino que también se aplica a un dispositivo independiente. Con USIP ON y el uso del puerto proxy inhabilitado, simétrico `rsskey` reduce tanto la dirección Core to Core (C2C) como la dirección de nodo a nodo.

¿Cuáles son los factores que contribuyen a cambiar el nodo CCO?

El primer nodo agregado para formar una configuración de clúster se convierte en el nodo coordinador de configuración (CCO). Los siguientes factores contribuyen a cambiar el nodo CCO en la configuración del clúster:

- Cuando se quita el nodo CCO actual de la configuración del clúster
- Cuando se bloquea el nodo CCO actual
- Cuando se cambia la prioridad del nodo que no es CCO (la prioridad inferior tiene mayor prioridad)
- En condiciones dinámicas como, accesibilidad de red entre los nodos
- Cuando hay cambios en los estados del nodo: activo, spare y pasivo. Los nodos activos se prefieren como CCO.
- Cuando hay un cambio en la configuración, y el nodo que tiene la configuración más reciente se prefiere como CCO.

Solución de problemas del clúster de Citrix ADC

August 20, 2021

Si se produce un error en un clúster de Citrix ADC, el primer paso para solucionar problemas es obtener información sobre la instancia del clúster. Puede obtener la información ejecutando los `show cluster node nodeId` comandos `show cluster instance clId` y en los nodos del clúster respectivamente.

Si no puede encontrar el problema mediante los dos enfoques anteriores, puede usar uno de los siguientes:

- **Aislar el origen del error.** Intente omitir el clúster para llegar al servidor. Si el intento se realiza correctamente, el problema es probablemente con la configuración del clúster.
- **Compruebe los comandos ejecutados recientemente.** Ejecute el comando history para comprobar las configuraciones recientes realizadas en el clúster. También puede revisar el archivo ns.conf para verificar las configuraciones que se han implementado.

- **Compruebe los archivos ns.log.** Utilice los archivos de registro, disponibles en el directorio /var/log/ de cada nodo, para identificar los comandos ejecutados, el estado de los comandos y los cambios de estado.
- **Compruebe los archivos newnslog.** Utilice los `newnslog` archivos, disponibles en el directorio /var/nslog/ de cada nodo, para identificar los eventos que se han producido en los nodos del clúster. Puede ver varios `newnslog` archivos como un único archivo copiándolos en un único directorio y, a continuación, ejecutando el siguiente comando:

```
nsconmsg -K newnslog-node<id> -K     newnslog.node<id> -d current
```

Si aún no puede resolver el problema, puede intentar realizar el seguimiento de los paquetes en el clúster o utilizar el `techsupport -scope cluster` comando show. Puede utilizar el comando para enviar el informe al equipo de soporte técnico.

Rastrear los paquetes de un clúster de Citrix ADC

August 20, 2021

El sistema operativo Citrix ADC proporciona una utilidad denominada *seguimiento ns* para obtener un volcado de los paquetes recibidos y enviados por un dispositivo. La utilidad almacena los paquetes en archivos de seguimiento. Puede utilizar estos archivos para depurar problemas en el flujo de paquetes a los nodos del clúster. Los archivos de seguimiento deben verse con la aplicación Wireshark.

Algunos aspectos más destacados de la utilidad de traza ns son:

- Se puede configurar para rastrear paquetes selectivamente mediante expresiones clásicas y expresiones predeterminadas.
- Puede capturar el seguimiento en varios formatos: formato de traza ns (.cap) y formato de volcado TCP (.pcap).
- Puede agregar los archivos de seguimiento de todos los nodos del clúster en el coordinador de configuración.
- Puede combinar varios archivos de seguimiento en un único archivo de seguimiento (solo para archivos.cap).

Puede utilizar la utilidad ns trace desde la línea de comandos de Citrix ADC o el shell de Citrix ADC.

Para realizar un seguimiento de paquetes de un dispositivo independiente

Ejecute el comando start ns trace en el dispositivo. El comando crea archivos de seguimiento en el <date-timestamp> directorio /var/nstrace/. Los nombres de archivo de seguimiento tienen la forma

nstrace.cap<id\ >.

Puede ver el estado ejecutando el comando show ns trace. Puede detener el seguimiento de los paquetes ejecutando el comando stop ns trace.

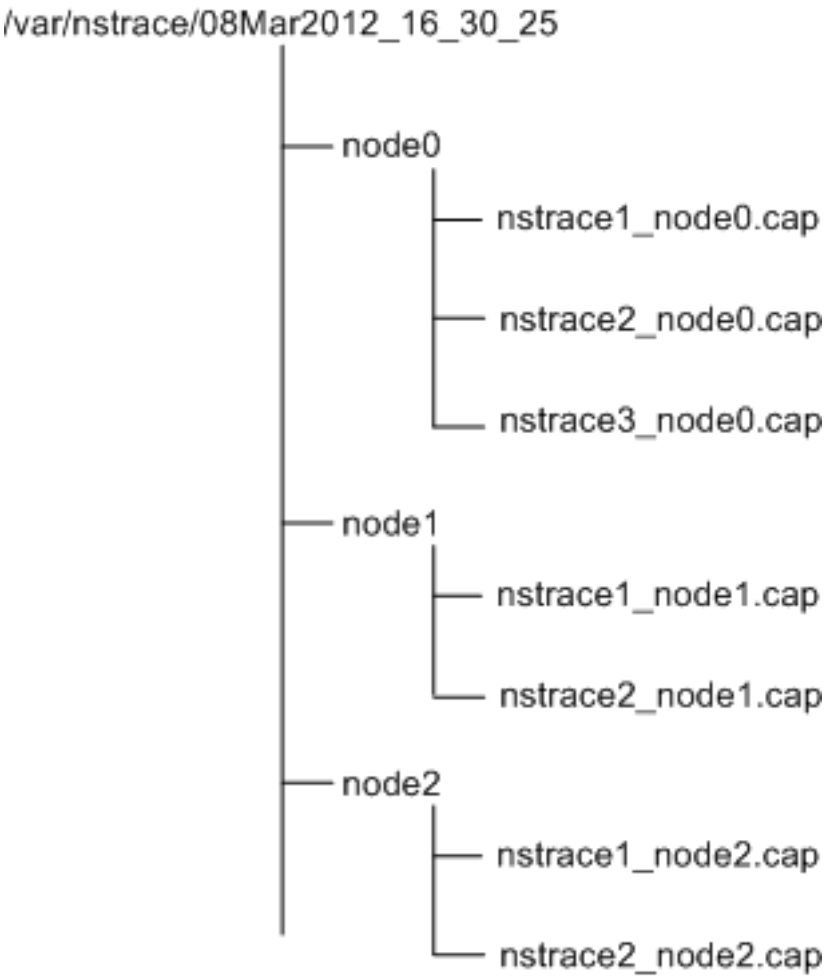
> **Nota**
>
> También puede ejecutar la utilidad de seguimiento ns desde el shell de Citrix ADC ejecutando el archivo
> nstrace.sh. Sin embargo, se recomienda utilizar la utilidad de rastreo ns a través de la interfaz de línea de comandos de Citrix ADC.

Para rastrear paquetes de un clúster

Puede rastrear los paquetes en todos los nodos del clúster y obtener todos los archivos de seguimiento en el coordinador de configuración.

Ejecute el comando start ns trace en la dirección IP del clúster. El comando se propaga y se ejecuta en todos los nodos del clúster. Los archivos de seguimiento se almacenan en nodos individuales de clúster en el<date-timestamp> directorio /var/nstrace/. Los nombres de archivo de seguimiento tienen la forma nstrace <id> _node.cap<id\ >.

Puede utilizar los archivos de seguimiento de cada nodo para depurar las operaciones de nodos. Pero si quiere que los archivos de seguimiento de todos los nodos del clúster estén en una ubicación, debe ejecutar el comando stop ns trace en la dirección IP del clúster. Los archivos de seguimiento de todos los nodos se descargan en el coordinador de configuración del clúster en el<date-timestamp> directorio /var/nstrace/ de la siguiente manera:



Combinar varios archivos de seguimiento

Puede preparar un único archivo a partir de los archivos de seguimiento (solo compatible con. Cap) obtenidos de los nodos del clúster. Los archivos de seguimiento individuales proporcionan una vista acumulativa del seguimiento de los paquetes de clúster. Las entradas de seguimiento del archivo de seguimiento único se ordenan en función de la hora en que se recibieron los paquetes en el clúster.

Para combinar los archivos de seguimiento, en el shell de Citrix ADC, escriba:

```
1 > nstracemerge.sh -srcdir \<DIR\> -dstdir \<DIR\> -filename \<name\> -
     filesize \<num\>
```

Donde:

- `srcdir` es el directorio desde el que se fusionan los archivos de seguimiento. Todos los archivos de seguimiento de este directorio se fusionan en un único archivo.

- `dstdir` es el directorio donde se crea el archivo de seguimiento fusionado.
- `Filename` es el nombre del archivo de seguimiento que se crea.
- `Filesize` es el tamaño del archivo de seguimiento.

Ejemplos

A continuación se presentan algunos ejemplos del uso de la utilidad de rastreo ns para filtrar paquetes.

- Para rastrear los paquetes en las interfaces de plano anterior de tres nodos:

  Usar expresiones clásicas:

```
1   > start nstrace -filter "INTF == 0/1/1 && INTF == 1/1/1 && INTF
      == 2/1/1"
```

  Usar expresiones predeterminadas:

```
1   > start nstrace -filter "CONNECTION.INTF.EQ("0/1/1") &&
      CONNECTION.INTF.EQ("1/1/1") && CONNECTION.INTF.EQ("2/1/1")"
```

- Para rastrear los paquetes desde una dirección IP de origen 10.102.34.201 o desde un sistema cuyo puerto de origen es mayor que 80 y el nombre del servicio no es "s1":

  Usar expresiones clásicas

```
1   > start nstrace -filter "SOURCEIP == 10.102.34.201 || (SVCNAME !=
      s1 && SOURCEPORT > 80)"
```

  Usar expresiones predeterminadas

```
1   > start nstrace -filter "CONNECTION.SRCIP.EQ(10.102.34.201) || (
      CONNECTION.SVCNAME.NE("s1") && CONNECTION.SRCPORT.GT(80))"
```

> **Nota**
>
> Para obtener más información sobre los filtros utilizados en ns trace, consulte ns trace.

Captura de claves de sesión SSL durante un seguimiento

Cuando ejecuta el comando “start ns trace”, puede establecer el nuevo `capsslkeys` parámetro para capturar las claves maestras SSL para todas las sesiones SSL. Si incluye este parámetro, se genera un archivo denominado nstrace.sslkeys junto con el seguimiento del paquete. Este archivo se puede importar a Wireshark para descifrar el tráfico SSL en el archivo de seguimiento correspondiente.

Esta funcionalidad es similar a los exploradores web que exportan claves de sesión que posteriormente se pueden importar a Wireshark para descifrar el tráfico SSL.

Ventajas del uso de claves de sesión SSL

Las siguientes son las ventajas de utilizar claves de sesión SSL:

1. Genera archivos de seguimiento más pequeños que no incluyen los paquetes adicionales creados por el modo SSLPLAIN de captura.
2. Proporciona la capacidad de ver texto sin formato [SP (1] de la traza y elegir si quiere compartir el archivo de claves maestras o proteger los datos confidenciales al no compartirlo.

Limitaciones del uso de claves de sesión SSL

A continuación se presentan las limitaciones del uso de claves de sesión SSL:

1. Las sesiones SSL no se pueden descifrar si no se capturan los paquetes iniciales de la sesión.
2. Las sesiones SSL no se pueden capturar si el modo Federal Information Processing Standard (FIPS) está habilitado.

Para capturar claves de sesión SSL mediante la interfaz de línea de comandos (CLI)

En el símbolo del sistema, escriba los comandos siguientes para habilitar o inhabilitar las claves de sesión SSL en un archivo de seguimiento y verificar la operación de seguimiento.

```
1 > start nstrace -capsslkeys ENABLED
2 > show nstrace
3 Example
4 > start nstrace -capsslkeys ENABLED
5 > show nstrace
6       State:  RUNNING          Scope:  LOCAL            TraceLocation:
            ”/var/nstrace/04May2016_17_51_54/...”
7       Nf:  24                  Time:  3600              Size:  164
                        Mode:  TXB NEW_RX
8       Traceformat:  NSCAP      PerNIC:  DISABLED        FileName:  04
           May2016_17_51_54 Link:  DISABLED
```



```
9       Merge:  ONSTOP          Doruntimecleanup:  ENABLED TraceBuffers:
            5000      SkipRPC:  DISABLED
10      SkipLocalSSH:  DISABLED  Capsslkeys:  ENABLED     InMemoryTrace:
            DISABLED
11  Done
```

Para configurar claves de sesión SSL mediante la GUI de Citrix ADC

1. Vaya a **Configuración > Sistema > Diagnósticos > Herramientas de soporte técnico** y haga clic en **Iniciar nuevo seguimiento** para iniciar el seguimiento de paquetes cifrados en un dispositivo.
2. En la página **Iniciar seguimiento**, active la casilla de verificación **Capturar claves maestras SSL**.
3. Haga clic en **Aceptar** y **Listo**.

Para importar las claves maestras SSL en Wireshark

En la interfaz gráfica de usuario de Wireshark, vaya a **Edición > Preferencias > Protocolos > SSL > nombre de archivo de registro (Pre) -Master-Secret** y especifique los archivos de clave maestra obtenidos del dispositivo.

Solucionar problemas conocidos

August 20, 2021

Al unir un nodo al clúster, aparece el siguiente mensaje, “ERROR: Nombre/número de interfaz no válido” ¿Qué debo hacer para resolver este error?

Dicho error se produce si proporcionó una interfaz de plano posterior no válida o incorrecta mientras utiliza el comando add cluster node para agregar el nodo. Para resolver este error, verifique la interfaz que proporcionó al agregar el nodo. Asegúrese de que no ha especificado la interfaz de administración del dispositivo como interfaz de backplane y de que el <nodeId> bit de la interfaz es el mismo que el Id del nodo. Por ejemplo, si el nodeID es 3, la interfaz del plano posterior debe ser 3/<c>/<u>.

Al unir un nodo al clúster, aparece el siguiente mensaje: "ERROR: El clúster no se puede habilitar porque el nodo local no es miembro del clúster". ¿Qué debo hacer para resolver este error?

Este error se produce cuando intenta unirse a un nodo sin agregar el NSIP del nodo al clúster. Para resolver este error, primero debe agregar la dirección NSIP del nodo al clúster mediante el comando **add cluster node** y, a continuación, ejecutar el comando **join cluster**.

Al unir un nodo al clúster, aparece el siguiente mensaje, "ERROR: Conexión denegada". ¿Qué debo hacer para resolver este error?

Este error puede ocurrir debido a las siguientes razones:

- **Problemas de conectividad.** El nodo no puede conectarse a la dirección IP del clúster. Intente hacer ping a la dirección IP del clúster desde el nodo al que está intentando unirse.
- **Dirección IP del clúster duplicada.** Compruebe si la dirección IP del clúster existe en algún nodo que no sea del clúster. Si lo hace, cree una dirección IP del clúster e intente volver a unirse al clúster.

Al unir un nodo al clúster, aparece el siguiente mensaje, "ERROR: Falta de coincidencia de licencia entre el coordinador de configuración y el nodo local." ¿Qué debo hacer para resolver este error?

El dispositivo que va a unir al clúster debe tener las mismas licencias que el coordinador de configuración. Este error se produce cuando las licencias del nodo al que está uniendo no coinciden con las licencias del coordinador de configuración. Para resolver este error, ejecute los siguientes comandos en ambos nodos y compare las salidas.

Desde la línea de comandos:

- `show ns hardware`
- `show ns license`

Desde el caparazón:

- `nsconmsg -g feature -d stats`
- `ls /nsconfig/license`
- Ver el contenido del archivo /var/log/license.log

¿Qué debo hacer cuando las configuraciones de un nodo de clúster no están sincronizadas con las configuraciones del clúster?

Normalmente, las configuraciones se sincronizan automáticamente entre todos los nodos del clúster. Sin embargo, si considera que las configuraciones no están sincronizadas en un nodo específico, debe forzar la sincronización ejecutando el comando force cluster sync desde el nodo que quiere sincronizar. Para obtener más información, consulte Sincronización de configuraciones de clúster.

Al configurar un nodo de clúster, aparece el siguiente mensaje: "ERROR: Sesión es de solo lectura; conéctese a la dirección IP del clúster para modificar la configuración. "

Todas las configuraciones de un clúster deben realizarse a través de la dirección IP del clúster y las configuraciones se propagan a los demás nodos del clúster. Todas las sesiones establecidas a través de la dirección NSIP de nodos individuales son de solo lectura.

¿Por qué el estado del nodo muestra "INACTIVO" cuando el estado del nodo muestra "UP"?

Un nodo saludable puede estar en estado INACTIVO por varias razones. Un escaneo de ns.log o contadores de errores puede ayudarlo a determinar el motivo exacto.

¿Cómo puedo resolver el estado de un nodo cuando su estado muestra "NO UP"?

El estado del nodo "**Not UP**" indica que hay algunos problemas con el nodo. Para conocer la causa raíz, debe ejecutar el comando **show cluster node**. Este comando muestra las propiedades del nodo y el motivo del error del nodo.

¿Qué debo hacer cuando el estado de un nodo se muestra como "NOT UP" y la razón indica que los comandos de configuración han fallado en un nodo?

Este problema surge cuando algunos comandos no se ejecutan en los nodos del clúster. En tales casos, debe asegurarse de que las configuraciones se sincronicen mediante una de las siguientes opciones:

- Si algunos de los nodos del clúster están en este estado, debe realizar la operación forzar la sincronización del clúster en esos nodos. Para obtener más información, consulte Sincronización de configuraciones de clúster.
- Si todos los nodos del clúster están en este estado, debe inhabilitar y habilitar la instancia del clúster en todos los nodos del clúster.

Cuando ejecuto el comando set virtual server, aparece el siguiente mensaje, “No hay tal recurso.” ¿Qué debo hacer para resolver este problema?

El comando **set vserver** no es compatible con la agrupación en clústeres. **Tampoco se admiten los comandos unset vserver, enable vserver, disablevserver y rm vserver**. Sin embargo, el comando**show vserver** es compatible.

No puedo configurar el clúster a través de una sesión Telnet. ¿Qué debo hacer?

Durante una sesión telnet, solo se puede acceder a la dirección IP del clúster en modo de solo lectura. Por lo tanto, no puede configurar un clúster a través de una sesión telnet.

Observo una diferencia de tiempo significativa en los nodos del clúster. ¿Qué debo hacer para resolver este problema?

Cuando los paquetes PTP se descartan debido al conmutador de plano posterior o si los recursos físicos están excesivamente comprometidos en un entorno virtual, el tiempo no se sincronizará.

Para sincronizar las horas, debe hacer lo siguiente en la dirección IP del clúster:

1. Inhabilitar PTP.

   set ptp -state disable

2. Configure el protocolo de tiempo de red (NTP) para el clúster. Para obtener más información, consulte Configuración de la sincronización del reloj.

¿Qué debo hacer si no hay conectividad con la dirección IP del clúster y la dirección NSIP de un nodo del clúster?

Si no puede acceder a la dirección IP del clúster o al NSIP de un nodo del clúster, debe acceder al dispositivo a través de la consola serie. Si se puede acceder a la dirección NSIP, puede SSH a la dirección IP del clúster desde el shell ejecutando el siguiente comando en el símbolo del shell:

“‘# ssh nsroot@

```
## ¿Qué debo hacer para recuperar un nodo de clúster que tiene
   problemas de conectividad?

Para recuperar un nodo que tiene problemas de conectividad:

1.  Inhabilite la instancia de clúster en ese nodo (ya que no puede
   ejecutar comandos desde el NSIP de un nodo de clúster).
```



```
6
7  1.  Ejecute los comandos necesarios para recuperar el nodo.
8
9  1.  Habilite la instancia del clúster en ese nodo.
10
11 ## Algunos nodos del clúster tienen dos rutas predeterminadas. ¿Cómo
       puedo eliminar la segunda ruta predeterminada del nodo del clúster?
12
13 Para eliminar la ruta predeterminada adicional, haga lo siguiente en
       cada nodo que tenga la ruta adicional:
14
15 1.  Inhabilite la instancia del clúster.
16
17     ```disable cluster instance <clId><!--NeedCopy-->
```

1. Elimine la ruta.

   ```
   rm route <network> <netmask> <gateway><!--NeedCopy-->
   ```

2. Habilite la instancia del clúster.

   ```
   enable cluster instance <clId><!--NeedCopy-->
   ```

La funcionalidad del clúster se ve afectada cuando un nodo de clúster existente entra en línea. ¿Qué debo hacer para resolver este problema?

Si la contraseña RPC de un nodo se cambia desde la dirección IP del clúster cuando ese nodo está fuera del clúster, entonces, cuando el nodo se pone en línea, las credenciales RPC no coinciden y pueden afectar a la funcionalidad del clúster. Para resolver este problema, utilice el comando set ns RpcNode para actualizar la contraseña en el NSIP del nodo que se ha conectado.

Conmutación de contenido

October 5, 2021

En los sitios web complejos de hoy en día, es posible que quieras presentar contenido diferente a diferentes usuarios. Por ejemplo, es posible que quiera permitir que los usuarios del rango de IP de un cliente o socio tengan acceso a un portal web especial. Es posible que quiera presentar contenido relevante para una zona geográfica específica a los usuarios de esa área. Es posible que quieras presentar contenido en diferentes idiomas a los hablantes de esos idiomas. Es posible que quieras presentar contenido adaptado a dispositivos específicos, como smartphones, a quienes usan los dispositivos. La función de cambio de contenido de Citrix ADC permite que el dispositivo distribuya las solicitudes

de cliente en varios servidores en función del contenido específico que quiera presentar a esos usuarios.

Para configurar el cambio de contenido, primero cree una configuración básica de conmutación de contenido y, a continuación, personalícela según sus necesidades. Esto implica habilitar la función de cambio de contenido, configurar el equilibrio de carga para el servidor o los servidores que alojan cada versión del contenido que se está cambiando, crear un servidor virtual de conmutación de contenido, crear directivas para elegir qué solicitudes se dirigen a qué servidor virtual de equilibrio de carga, y vincular las directivas al servidor virtual de conmutación de contenido. A continuación, puede personalizar la configuración para satisfacer sus necesidades estableciendo prioridad para sus directivas, protegiendo su configuración configurando un servidor virtual de reserva y mejorando el rendimiento de la configuración redirigiendo las solicitudes a una caché.

Cómo funciona el cambio de contenido

Content Switching permite al dispositivo Citrix ADC dirigir las solicitudes enviadas al mismo host web a distintos servidores con contenido diferente. Por ejemplo, puede configurar el dispositivo para que dirija las solicitudes de contenido dinámico (como direcciones URL con el sufijo .asp, .dll o .exe) a un servidor y las solicitudes de contenido estático a otro servidor. Puede configurar el dispositivo para que realice el cambio de contenido según los encabezados TCP/IP y la carga útil.

También puede utilizar el cambio de contenido para configurar el dispositivo para que redirija las solicitudes a distintos servidores con contenido diferente en función de los distintos atributos del cliente. Algunos de esos atributos del cliente son:

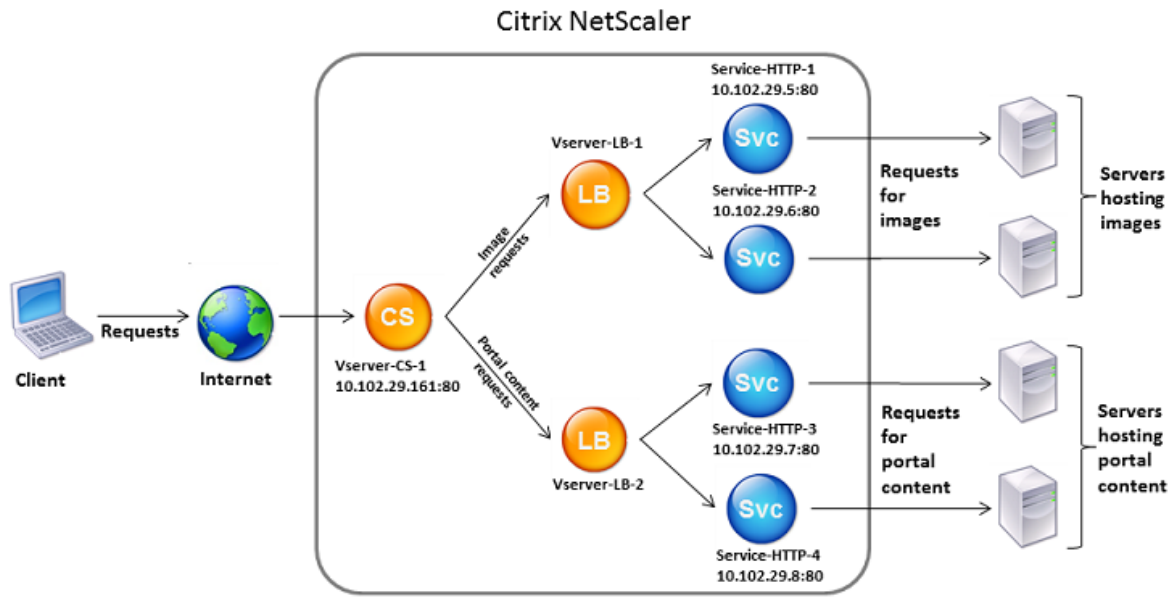
- **Tipo de dispositivo.** El dispositivo examina el agente de usuario o el encabezado HTTP personalizado de la solicitud del cliente para determinar el tipo de dispositivo desde el que se originó la solicitud. Según el tipo de dispositivo, dirige la solicitud a un servidor web específico. Por ejemplo, si la solicitud proviene de un teléfono móvil, la solicitud se dirige a un servidor, capaz de servir contenido que el usuario puede ver en el teléfono móvil. Una solicitud de un equipo se dirige a un servidor diferente, capaz de servir contenido diseñado para una pantalla de equipo.
- **Lenguaje.** El dispositivo examina el encabezado HTTP Accept-Language en la solicitud del cliente y determina el idioma utilizado por el explorador del cliente. A continuación, el dispositivo envía la solicitud a un servidor que distribuya contenido en ese idioma. Por ejemplo, mediante el cambio de contenido según el idioma, el dispositivo puede enviar a alguien cuyo explorador esté configurado para solicitar contenido en francés a un servidor con la versión francesa de un periódico. Puede enviar a otra persona cuyo explorador esté configurado para solicitar contenido en inglés a un servidor con la versión en inglés.
- **Cookie.** El dispositivo examina los encabezados de solicitud HTTP en busca de una cookie configurada previamente por el servidor. Si encuentra la cookie, dirige las solicitudes al servidor apropiado, que aloja contenido personalizado. Por ejemplo, si se encuentra una cookie que indica que el cliente es miembro de un programa de fidelización de clientes, la solicitud se dirige

a un servidor más rápido o a uno con contenido especial. Si no encuentra ninguna cookie, o si la cookie indica que el usuario no es miembro, la solicitud se dirige a un servidor para el público en general.

- **Método HTTP.** El dispositivo examina el encabezado HTTP del método utilizado y envía la solicitud del cliente al servidor correcto. Por ejemplo, las solicitudes GET de imágenes se pueden dirigir a un servidor de imágenes, mientras que las solicitudes POST se pueden dirigir a un servidor más rápido que gestiona contenido dinámico.
- **Datos de capa 3/4.** El dispositivo examina las solicitudes de IP de origen o destino, puerto de origen o destino, o cualquier otra información presente en los encabezados TCP o UDP, y dirige la solicitud del cliente al servidor correcto. Por ejemplo, las solicitudes de las IP de origen que pertenecen a los clientes se pueden dirigir a un portal web personalizado en un servidor más rápido o a uno con contenido especial.

Una implementación típica de conmutación de contenido consta de las entidades descritas en el siguiente diagrama.

Ilustración 1. Arquitectura de cambio de contenido



Una configuración de conmutación de contenido consiste en un servidor virtual de conmutación de contenido, una configuración de equilibrio de carga que consiste en servidores y servicios virtuales de equilibrio de carga y directivas de conmutación de contenido. Para configurar el cambio de contenido, debe configurar un servidor virtual de conmutación de contenido y asociarlo a directivas y servidores virtuales de equilibrio de carga. Este proceso crea un grupo de contenido: *un grupo de todos los servidores virtuales y las directivas involucrados en una configuración de conmutación de contenido concreta.

La conmutación de contenido se puede utilizar con conexiones HTTP, HTTPS, TCP y UDP. Para HTTPS, debes habilitar la descarga SSL.

Cuando una solicitud llega al servidor virtual de conmutación de contenido, el servidor virtual aplica las directivas de conmutación de contenido asociadas a esa solicitud. La prioridad de la directiva define el orden en que se evalúan las directivas vinculadas al servidor virtual de conmutación de contenido. Si utiliza directivas de directivas avanzadas, al enlazar una directiva al servidor virtual de conmutación de contenido, debe asignar una prioridad a esa directiva. Si utiliza directivas clásicas de Citrix ADC, puede asignar una prioridad a las directivas, pero no es obligatorio hacerlo. Si asigna prioridades, las directivas se evalúan en el orden establecido. Si no lo hace, el dispositivo Citrix ADC evalúa las directivas en el orden en que se crearon.

Además de configurar las prioridades de directivas, puede manipular el orden de evaluación de directivas mediante expresiones Goto e invocaciones de bancos de directivas. Para obtener más información sobre la configuración avanzada de directivas, consulte Configuración de directivas avanzadas.

Después de evaluar las directivas, el servidor virtual de cambio de contenido redirige la solicitud al servidor virtual de equilibrio de carga adecuado, que la envía al servicio adecuado.

Los servidores virtuales de conmutación de contenido solo pueden enviar solicitudes a otros servidores virtuales. Si utiliza un equilibrador de carga externo, debe crear un servidor virtual de equilibrio de carga para él y vincular su servidor virtual como servicio al servidor virtual de conmutación de contenido.

Configuración del cambio de contenido básico

December 2, 2021

Antes de configurar el cambio de contenido, debe comprender cómo se configura el cambio de contenido y cómo están conectados los servicios y los servidores virtuales.

Para configurar una configuración básica y funcional de conmutación de contenido, primero active la función de cambio de contenido. A continuación, cree al menos un grupo de contenido. Para cada grupo de contenido, cree un servidor virtual de conmutación de contenido para aceptar solicitudes a un grupo de sitios web que utilizan el cambio de contenido. Cree también una configuración de equilibrio de carga, que incluya un grupo de servidores virtuales de equilibrio de carga a los que el servidor virtual de conmutación de contenido dirige las solicitudes. Para especificar qué solicitudes dirigir a qué servidor virtual de equilibrio de carga, cree al menos dos directivas de conmutación de contenido, una para cada tipo de solicitud que se va a redirigir. Cuando haya creado las directivas y los servidores virtuales, vincule las directivas al servidor virtual de conmutación de contenido. También puede enlazar una directiva a varios servidores virtuales de conmutación de contenido. Al enlazar

una directiva, especifica el servidor virtual de equilibrio de carga al que se van a dirigir las solicitudes que coinciden con la directiva.

Además de vincular directivas individuales a un servidor virtual de conmutación de contenido, puede enlazar etiquetas de directivas. Si crea más grupos de contenido, puede enlazar una etiqueta de directiva o directiva a más de uno de los servidores virtuales de conmutación de contenido.

> **Nota**
>
> Tras crear un grupo de contenido, puede modificar su servidor virtual de conmutación de contenido para personalizar la configuración.

Activación del cambio de contenido

Para utilizar la función de cambio de contenido, debe habilitar el cambio de contenido. Puede configurar entidades de conmutación de contenido aunque la función de cambio de contenido esté desactivada. Sin embargo, las entidades no funcionarán.

Para habilitar el cambio de contenido mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para habilitar el cambio de contenido y verificar la configuración:

```
enable ns feature CS

show ns feature
<!--NeedCopy-->
```

Ejemplo:

```
> enable  feature ContentSwitch
    Done
> show feature

    Feature                       Acronym             Status
    -------                       -------             ------
1)     Web Logging                   WL                  OFF
2)     Surge Protection              SP                  ON
3)     Load Balancing                LB                  ON
4)     Content Switching             CS                  ON
.
.
```

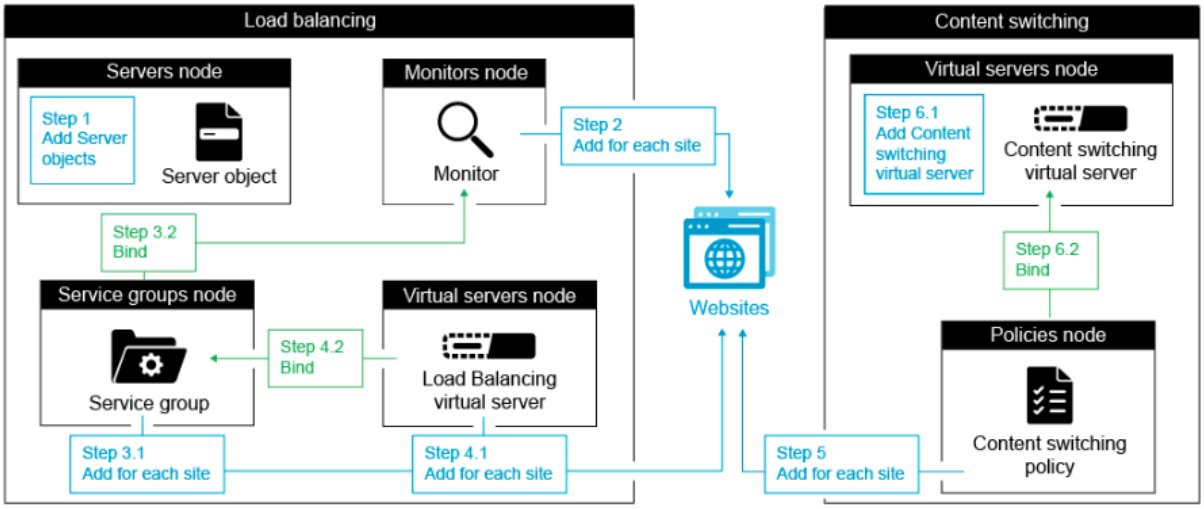


```
.
22)    Responder                      RESPONDER            ON
23)    NetScaler Push                 push                 OFF
Done
<!--NeedCopy-->
```

Para habilitar el cambio de contenido mediante la interfaz gráfica de usuario

Vaya a **Sistema > Configuración** y, en el grupo **Modos y funciones**, seleccione **Configurar funciones básicas**y, a continuación, **Cambio de contenido**.

En la siguiente ilustración se ilustra la configuración escalonada de Content Switching.



Creación de servidores virtuales de conmutación de contenido

Puede agregar, modificar y quitar servidores virtuales de conmutación de contenido. El estado de un servidor virtual es DOWN cuando lo crea, porque el servidor virtual de equilibrio de carga aún no está vinculado a él.

Para crear un servidor virtual mediante la CLI

En el símbolo del sistema, escriba:

```
add cs vserver <name> <protocol> <IPAddress> <port>
<!--NeedCopy-->
```

Ejemplo:


```
add cs vserver Vserver-CS-1 HTTP 10.102.29.161 80
<!--NeedCopy-->
```

Para agregar un servidor virtual de conmutación de contenido mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Cambio de contenido > Servidores virtuales**y agregue un servidor virtual.
2. Especifique un nombre para el servidor virtual de conmutación de contenido.

   > **Nota**
   >
   > Hay un servidor virtual de conmutación de contenido diferente para cada protocolo. (Por ejemplo, HTTP y SSL).

3. Rellene los campos correspondientes y haga clic en **Aceptar**.

Estadísticas del servidor virtual de conmutación de contenido

Las estadísticas del servidor virtual de conmutación de contenido muestran información como la selección del servidor virtual, los bytes de solicitud, los bytes de respuesta, el total de paquetes recibidos, el total de paquetes enviados, el umbral de desbordamiento, la selección de desbordamiento, las conexiones actuales establecidas por el cliente y la selección de copia de seguridad inactiva del servidor virtual.

Las estadísticas del servidor virtual de conmutación de contenido también muestran los detalles de resumen del servidor virtual de equilibrio de carga predeterminado enlazado.

Para ver estadísticas del servidor virtual de conmutación de contenido mediante la CLI

En el símbolo del sistema, escriba:

```
stat cs vserver <name>
<!--NeedCopy-->
```

Ejemplo:

```
stat cs vserver CS_stats
<!--NeedCopy-->
```



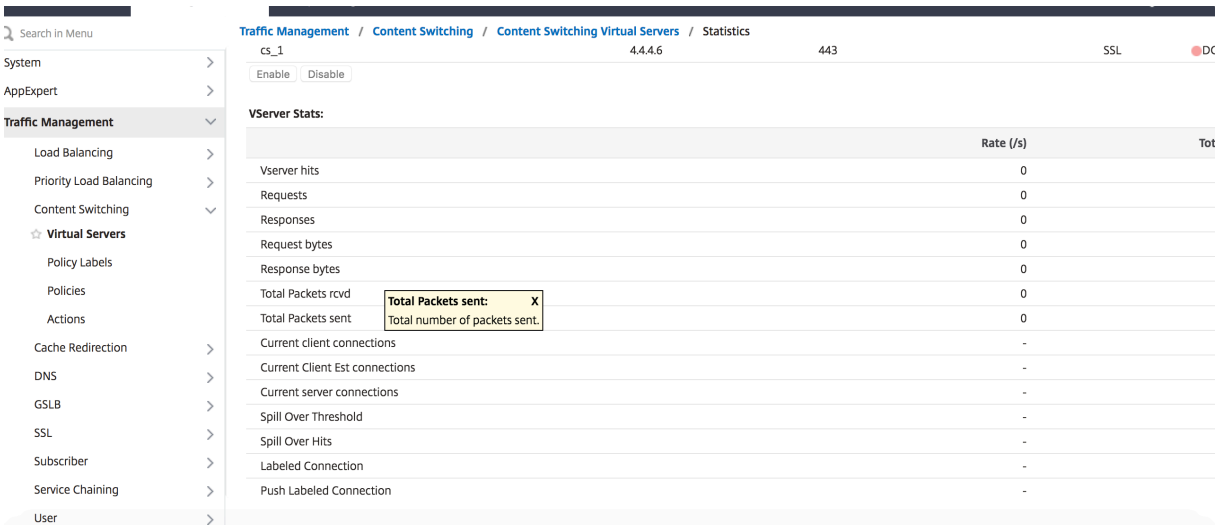
```
Vserver Summary
                          IP  port     Protocol        State
CS_stats             1.1.1.1    80         HTTP           UP

VServer Stats:
                                          Rate (/s)                Total
Vserver hits                                      0                    0
Requests                                          0                    0
Responses                                         0                    0
Request bytes                                     0                    0
Response bytes                                    0                    0
Total Packets rcvd                                0                    0
Total Packets sent                                0                    0
Current client connections                       --                    0
Current Client Est connections                   --                    0
Current server connections                       --                    0
Spill Over Threshold                             --                    0
Spill Over Hits                                  --                    0
Labeled Connection                               --                    0
Push Labeled Connection                          --                    0
Deferred Request                                  0                    0
Invalid Request/Response                         --                    0
Invalid Request/Response Dropped                 --                    0
Vserver Down Backup Hits                         --                    0
Current Multipath TCP sessions                   --                    0
Current Multipath TCP subflows                   --                    0
Apdex for client response times.                 --                 1.00
Average client TTLB                              --                    0

 Done
```

Para ver las estadísticas del servidor virtual de conmutación de contenido mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico** > **Cambio de contenido** > **Servidores virtuales**.
2. Seleccione el servidor virtual y haga clic en **Estadísticas**.



Configuración de una configuración de equilibrio de carga para el cambio de contenido

El servidor virtual de conmutación de contenido redirige todas las solicitudes a un servidor virtual de equilibrio de carga. Debe crear un servidor virtual de equilibrio de carga para cada versión del contenido que se está cambiando. Es cierto incluso cuando la configuración solo tiene un servidor para cada versión del contenido y, por lo tanto, no realiza ningún equilibrio de carga con esos servidores. También puede configurar el equilibrio de carga real con varios servidores con equilibrio de carga que reflejan cada versión del contenido. En cualquier caso, el servidor virtual de conmutación de contenido debe tener un servidor virtual de equilibrio de carga específico asignado a cada versión del contenido que se está cambiando.

A continuación, el servidor virtual de equilibrio de carga reenvía la solicitud a un servicio. Si solo tiene un servicio vinculado a él, seleccione ese servicio. Si tiene varios servicios vinculados a él, utiliza su método de equilibrio de carga configurado para seleccionar un servicio para la solicitud y reenvía esa solicitud al servicio que ha seleccionado.

Para configurar una configuración básica de equilibrio de carga, debe realizar las siguientes tareas:

- Crear servidores virtuales de equilibrio de carga
- Crear servicios
- Enlazar servicios al servidor virtual de equilibrio de carga

Para obtener más información sobre el equilibrio de cargas, consulte Cómo funciona el equilibrio de carga. Para obtener instrucciones detalladas sobre cómo configurar una configuración básica de equilibrio de carga, consulte Configuración del equilibrio de cargas básico.

Configuración de una acción de cambio de contenido

Especifica el servidor virtual de equilibrio de carga de destino para una directiva de conmutación de contenido cuando vincula la directiva al servidor virtual de conmutación de contenido. Por lo tanto, debe configurar una directiva para cada servidor virtual de equilibrio de carga al que dirigir el tráfico.

Sin embargo, si la directiva de cambio de contenido utiliza una regla de directiva avanzada, puede configurar una acción para la directiva. En la acción, puede especificar el nombre del servidor virtual de equilibrio de carga de destino o configurar una expresión basada en solicitudes que, en tiempo de ejecución, calcula el nombre del servidor virtual de equilibrio de carga al que se va a enviar la solicitud. La expresión de acción debe especificarse en la directiva Avanzada.

La opción expression puede reducir drásticamente el tamaño de la configuración de conmutación de contenido, ya que solo necesita una directiva por servidor virtual de conmutación de contenido. Las directivas de conmutación de contenido que utilizan una acción también se pueden enlazar a varios servidores virtuales de conmutación de contenido, ya que el servidor virtual de equilibrio de carga de destino ya no se especifica en la directiva de conmutación de contenido. La capacidad de vincular una única directiva a varios servidores virtuales de conmutación de contenido ayuda a reducir aún más el tamaño de la configuración de conmutación de contenido.

Después de crear una acción, crea una directiva de cambio de contenido y especifica la acción en la directiva para que la acción se lleve a cabo cuando esa directiva coincida con una solicitud.

> **Nota**
>
> También puede, en el caso de una directiva de conmutación de contenido que utiliza una regla de directiva avanzada, especificar el servidor virtual de equilibrio de carga de destino al vincular la directiva a un servidor virtual de conmutación de contenido, en lugar de utilizar una acción independiente. En el caso de directivas basadas en dominios, directivas basadas en URL y directivas basadas en reglas que utilizan expresiones clásicas, no hay ninguna acción disponible. Por lo tanto, para este tipo de directivas, se especifica el nombre del servidor virtual de equilibrio de carga de destino al vincular la directiva a un servidor virtual de conmutación de contenido.

Configuración de una acción que especifica el nombre del servidor virtual de equilibrio de carga de destino

Si elige especificar el nombre del servidor virtual de equilibrio de carga de destino en una acción de cambio de contenido, necesitará tantas directivas de conmutación de contenido como servidores virtuales de equilibrio de carga de destino. Las decisiones de cambio de contenido, en este caso, se basan en la regla de la directiva de conmutación de contenido y la acción se limita a especificar el servidor virtual de equilibrio de carga de destino. Cuando una solicitud coincide con la directiva, la solicitud se reenvía al servidor virtual de equilibrio de carga especificado.

Para crear y comprobar una acción de cambio de contenido que especifique el nombre del servidor virtual de equilibrio de carga de destino mediante la CLI

En el símbolo del sistema, escriba:

```
add cs action <name> -targetLBVserver <string> [-comment <string>]

show cs action <name>
<!--NeedCopy-->
```

Ejemplo:

```
> add cs action mycsaction -targetLBVserver mylbvserver -comment ”
   Forwards requests to mylbvserver.”
 Done
> show cs action mycsaction
    Name: mycsaction
    Target LB Vserver: mylbvserver
    Hits: 0
    Undef Hits: 0
    Action Reference Count: 0
    Comment: ”Forwards requests to mylbvserver.”

 Done
>
<!--NeedCopy-->
```

Para configurar una acción de cambio de contenido que especifique el nombre del servidor virtual de equilibrio de carga de destino mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Cambio de contenido > Acciones**.
2. Configure una acción de cambio de contenido y especifique el nombre del servidor virtual de equilibrio de carga de destino.

Configuración de una acción que especifica una expresión para seleccionar el destino en tiempo de ejecución

Si decide configurar una expresión basada en solicitudes que pueda calcular dinámicamente el nombre del servidor virtual de equilibrio de carga de destino, solo tendrá que configurar una directiva de conmutación de contenido para seleccionar el servidor virtual adecuado. La regla de la directiva

puede ser TRUE (la directiva coincide con todas las solicitudes) porque, en este caso, las decisiones de cambio de contenido se basan en la expresión de la acción. Al configurar una expresión en una acción, puede reducir drásticamente el tamaño de la configuración de conmutación de contenido.

Si decide configurar una expresión basada en solicitudes para calcular el nombre del servidor virtual de equilibrio de carga de destino en tiempo de ejecución, debe considerar detenidamente cómo asignar un nombre a los servidores virtuales de equilibrio de carga en la configuración. Debe poder derivar sus nombres mediante la expresión de directiva basada en solicitudes de la acción.

Por ejemplo, si cambia las solicitudes según el sufijo URL (extensión del recurso solicitado), al asignar un nombre a los servidores virtuales de equilibrio de carga, puede seguir la convención de agregar el sufijo URL a una cadena predeterminada, como `mylb_`. Por ejemplo, los servidores virtuales de equilibrio de carga para páginas HTML y archivos PDF pueden denominarse `mylb_html` y `mylb_pdf`, respectivamente. En ese caso, la regla que puede utilizar en la acción de cambio de contenido para seleccionar el servidor virtual de equilibrio de carga adecuado es `"mylb_"+HTTP.REQ.URL.SUFFIX`. Si el servidor virtual de conmutación de contenido recibe una solicitud de página HTML, la expresión devuelve `mylb_html`y la solicitud se cambia al servidor virtual `mylb_html`.

Para crear una acción de cambio de contenido que especifique una expresión mediante la CLI

En la línea de comandos, escriba los siguientes comandos para crear una acción de cambio de contenido que especifique una expresión y compruebe la configuración:

```
add cs action <name> -targetVserverExpr <expression>) [-comment <string
    >]

show cs action <name>
<!--NeedCopy-->
```

Ejemplo:

```
> add cs action mycsaction1 -targetvserverExpr '"mylb_" + HTTP.REQ.URL.
    SUFFIX'
 Done
> show cs action mycsaction1
    Name: mycsaction1
    Target Vserver Expression: "mylb_" + HTTP.REQ.URL.SUFFIX
    Target LB Vserver: No_Target
                ...
 Done
>
```



```
<!--NeedCopy-->
```

Para configurar una acción de cambio de contenido que especifica una expresión mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Cambio de contenido > Acciones**.
2. Configure una acción de cambio de contenido y especifique una expresión que calcule dinámicamente el nombre del servidor virtual de equilibrio de carga de destino.

Configuración de directivas de conmutación de contenido

Una directiva de conmutación de contenido define un tipo de solicitud que se va a dirigir a un servidor virtual de equilibrio de carga. Estas directivas se aplican en el orden de las prioridades asignadas a ellas o (si utiliza directivas clásicas de Citrix ADC y no asigna prioridades al vincularlas) en el orden en que se crearon las directivas.

> **Nota**
>
> Los parámetros de**URL** y **dominio** han quedado en desuso y no se admitirán en la versión 13.1. Utilice las expresiones de directiva predeterminadas (avanzadas); la utilidad nspepi puede ser útil en la conversión.

Las directivas:

- **Directivas basadas en reglas.** El dispositivo compara los datos entrantes con las expresiones especificadas en las directivas. Las directivas basadas en reglas se crean mediante una expresión clásica o una expresión de directiva avanzada. Tanto las directivas clásicas como las avanzadas son compatibles con las directivas de conmutación de contenido basadas en reglas.

  > **Nota**
  >
  > Una directiva basada en reglas se puede configurar con una acción opcional. Una directiva con una acción se puede enlazar a varios servidores virtuales o rótulos de directivas.

  Si establece una prioridad al vincular las directivas al servidor virtual de conmutación de contenido, las directivas se evalúan por orden de prioridad. Si no establece prioridades específicas al vincular las directivas, las directivas se evalúan en el orden en que se crearon.

Para obtener información sobre las directivas y expresiones clásicas de Citrix ADC, consulte Configuración de directivas y expresiones clásicas. Para obtener información acerca de las directivas avanzadas, consulte Configuración de expresiones de directivas avanzadas.

Para crear una directiva de cambio de contenido mediante la CLI

En el símbolo del sistema, escriba uno de los siguientes comandos:


```
add cs policy <policyName> -rule <RULEValue>

add cs policy <policyName> -rule <RULEValue> -action <actionName>
<!--NeedCopy-->
```

Ejemplo:

```
add cs policy policy-CS-1 -rule "HTTP.REQ.URL.PATH.EQ("http://abcd.com
    ")"

add cs policy policy-CS-4 -rule "HTTP.REQ.HOSTNAME.EQ("example.com")"

add cs policy-CS-1 -rule "CLIENT.IP.SRC.SUBNET(24).EQ(10.217.84.0)"

add cs policy-CS-2 -rule "SYS.TIME.BETWEEN(GMT 2009 Nov,GMT 2009 Dec)"

add cs policy-CS-3 -rule "http.req.method.eq(GET)" -action act1
<!--NeedCopy-->
```

Para cambiar el nombre de una directiva de cambio de contenido mediante la CLI

En el símbolo del sistema, escriba:

```
rename cs policy <policyName> <newName>
<!--NeedCopy-->
```

Ejemplo:

```
rename cs policy myCSPolicy myCSPolicy1
<!--NeedCopy-->
```

Para cambiar el nombre de una directiva de cambio de contenido mediante la interfaz gráfica de usuario

Vaya a **Administración del tráfico > Cambio de contenido > Directivas**, seleccione una directiva y, en la lista Acción, seleccione Cambiar nombre.

Para crear una directiva de conmutación de contenido mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Cambio de contenido > Directivas**y haga clic en **Agregar**.
2. Rellene los campos correspondientes y haga clic en **Crear**.

Configuración de etiquetas de directiva de conmutación de contenido

Una etiqueta de directiva es un punto de enlace definido por el usuario al que están vinculadas las directivas. Cuando se invoca una etiqueta de directiva, todas las directivas vinculadas a ella se evalúan en el orden de prioridad que les asignó. Una etiqueta de directiva puede incluir una o varias directivas, a cada una de las cuales se le puede asignar su propio resultado. Una coincidencia en una directiva del rótulo de directiva puede dar lugar a pasar a la siguiente directiva, invocar una etiqueta de directiva diferente o un recurso apropiado, o poner fin inmediatamente a la evaluación de la directiva y devolver el control a la directiva que invocó la etiqueta de directiva. Solo puede crear rótulos de directiva para directivas avanzadas.

Una etiqueta de directiva de cambio de contenido consta de un nombre, un tipo de etiqueta y una lista de directivas vinculadas a la etiqueta de directiva. El tipo de etiqueta de directiva especifica el protocolo que se ha asignado a las directivas vinculadas a la etiqueta. Debe coincidir con el tipo de servicio del servidor virtual de conmutación de contenido al que está vinculada la directiva que invoca la etiqueta de directiva. Por ejemplo, puede enlazar directivas de carga útil de TCP a una etiqueta de directiva de tipo TCP únicamente. No se admite la vinculación de directivas de carga útil TCP a una etiqueta de directiva de tipo HTTP.

Cada directiva de una etiqueta de directiva de conmutación de contenido está asociada a un destino (que equivale a la acción asociada a otros tipos de directivas, como directivas de reescritura y respuesta) o a una opción GoToPriorityExpression y una opción de invocación. Es decir, para una directiva determinada en una etiqueta de directiva de cambio de contenido, puede especificar un destino o establecer la opción GoToPriorityExpression y la opción invocar. Además, si varias directivas se evalúan como verdaderas, solo se considera el objetivo de la última directiva que se evalúa como verdadera.

Puede utilizar la CLI de Citrix ADC o la GUI para configurar las etiquetas de directiva de cambio de contenido. En la CLI de Citrix ADC, primero debe crear una etiqueta de directiva mediante el comando add cs policy label. A continuación, se enlazan las directivas a la etiqueta de directiva, una directiva a la vez, mediante el comando bind cs policy label. En la GUI de Citrix ADC, se realizan ambas tareas en un solo cuadro de diálogo.

Para crear una etiqueta de directiva de conmutación de contenido mediante la CLI

En el símbolo del sistema, escriba:


```
add cs policylabel <labelName> <cspolicylabelTypetype>`
<!--NeedCopy-->
```

Ejemplo:

```
add cs policylabel testpollab http
<!--NeedCopy-->
```

Para cambiar el nombre de una etiqueta de directiva de conmutación de contenido mediante la CLI

En el símbolo del sistema, escriba:

```
rename cs policylabel <labelName> <newName>`
<!--NeedCopy-->
```

Ejemplo:

```
rename cs policylabel oldPolicyLabelName newPolicyLabelName
<!--NeedCopy-->
```

Para cambiar el nombre de una etiqueta de directiva de conmutación de contenido mediante la interfaz gráfica de usuario

Vaya a **Administración del tráfico > Cambio de contenido > Etiquetas**de directiva, seleccione una etiqueta de directiva y, en la lista Acción, seleccione Cambiar nombre.

Para enlazar una directiva a una etiqueta de directiva de conmutación de contenido mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para enlazar una directiva a una etiqueta de directiva y compruebe la configuración:


```
bind cs policylabel <labelName> <policyName> <priority>[-targetVserver
    <string>] | [-gotoPriorityExpression <expression>] | [-invoke <
    labeltype> <labelName>] ]

show cs policylabel <labelName>
<!--NeedCopy-->
```

Ejemplo:

```
bind cs policylabel testpollab test_Pol 100 -targetVserver LBVIP
show cs policylabel testpollab
        Label Name: testpollab
        Label Type: HTTP
        Number of bound policies: 1
        Number of times invoked: 0
        Policy Name: test_Pol
        Priority: 100
        Target Virtual Server: LBVIP
<!--NeedCopy-->
```

> **Nota**
>
> Si una directiva se configura con una acción, no se requieren los parámetros del servidor virtual de destino (targetVServer), ir a expresión de prioridad (GoToPriorityExpression) e invocar (invocar). Si una directiva no se configura con una acción, debe configurar al menos uno de los siguientes parámetros: targetVServer, goToPriorityExpression e invoke.

Para desvincular una directiva de una etiqueta de directiva mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para desvincular una directiva de una etiqueta de directiva y compruebe la configuración:

```
unbind cs policylabel <labelName> <policyName>

show cs policylabel <labelName>
<!--NeedCopy-->
```

Ejemplo:


```
unbind cs policylabel testpollab test_Pol
show cs policylabel testpollab
        Label Name: testpollab
        Label Type: HTTP
        Number of bound policies: 0
        Number of times invoked: 0
<!--NeedCopy-->
```

Para quitar una etiqueta de directiva mediante la CLI

En el símbolo del sistema, escriba:

```
rm cs policylabel <labelName>
<!--NeedCopy-->
```

Para administrar una etiqueta de directiva de conmutación de contenido mediante la interfaz gráfica de usuario

Vaya a **Administración del tráfico > Cambio de contenido > Etiquetas de directivas**, configure un rótulo de directiva, vincule directivas a la etiqueta y, si lo quiere, especifique una prioridad, una expresión de GoToPriority y una opción de invocación.

Enlace de directivas a un servidor virtual de conmutación de contenido

Después de crear el servidor virtual y las directivas de conmutación de contenido, enlaza cada directiva al servidor virtual de conmutación de contenido. Al vincular la directiva al servidor virtual de conmutación de contenido, se especifica el servidor virtual de equilibrio de carga de destino.

> **Nota**
>
> Si la directiva de cambio de contenido utiliza una regla de directiva avanzada, puede configurar una acción de cambio de contenido para la directiva. Si configura una acción, debe especificar el servidor virtual de equilibrio de carga de destino al configurar la acción, no cuando vincula la directiva al servidor virtual de conmutación de contenido. Para obtener más información sobre cómo configurar una acción de cambio de contenido, consulte la sección Configuración de una acción de cambio de contenido.

Para enlazar una directiva a un servidor virtual de conmutación de contenido y seleccionar un servidor virtual de equilibrio de carga de destino mediante la CLI

En el símbolo del sistema, escriba:

```
bind cs vserver <name>[-lbvserver<string> -targetLBVServer<string> -
    policyname <string> -priority <positive_integer>] [-
    gotoPriorityExpression <expression>] [-type ( REQUEST | RESPONSE )]
    [-invoke (<labelType> <labelName>)]
<!--NeedCopy-->
```

Ejemplo:

```
bind cs vserver csw-vip2 -policyname csw-ape-policy2 -priority 14 -
    gotoPriorityExpression NEXT

bind cs vserver csw-vip3 -policyname rewrite-policy1 -priority 17 -
    gotoPriorityExpression
'q.header(”a”).count' -flowtype REQUEST -invoke policylabel label1

bind cs vserver Vserver-CS-1 Vserver-LB-1 -policyname Policy-CS-1 -
    priority 20
<!--NeedCopy-->
```

> **Nota**
>
> Los parámetros, el servidor virtual de equilibrio de carga de destino (targetVServer), la expresión de prioridad (GoToPriorityExpression) y el método de invocación (invocar) no se pueden utilizar si una directiva tiene una acción.

Para enlazar una directiva a un servidor virtual de conmutación de contenido y seleccionar un servidor virtual de equilibrio de carga de destino mediante la interfaz gráfica de usuario

Vaya a **Administración del tráfico > Cambio de contenido > Servidores virtuales**, abra un servidor virtual y, en la sección Vinculación de directivas de conmutación de contenido, vincule una directiva al servidor virtual y especifique un servidor virtual de equilibrio de carga de destino.

Configuración del registro basado en directivas para la conmutación de contenido

Puede configurar el registro basado en directivas para una directiva de conmutación de contenido. El registro basado en directivas permite especificar un formato para los mensajes de registro. El contenido del mensaje de registro se define mediante una expresión de directiva avanzada en la directiva de cambio de contenido. Cuando se realiza la acción de cambio de contenido especificada en la directiva, el dispositivo Citrix ADC crea el mensaje de registro a partir de la expresión y escribe el mensaje en el archivo de registro. El registro basado en directivas resulta especialmente útil si quiere probar y solucionar problemas de una configuración en la que las acciones de conmutación de contenido identifican el servidor virtual de equilibrio de carga de destino en tiempo de ejecución.

> **Nota**
>
> Si varias directivas enlazadas a un servidor virtual determinado se evalúan como TRUE y se configuran con una acción de mensaje de auditoría, el dispositivo Citrix ADC no realiza todas las acciones de mensajes de auditoría. Realiza únicamente la acción de mensaje de auditoría configurada para la directiva cuya acción de cambio de contenido se lleva a cabo.

Para configurar el registro basado en directivas para una directiva de cambio de contenido, primero debe configurar una acción de mensaje de auditoría. Para obtener más información sobre la configuración de una acción de mensaje de auditoría, consulte Configuración del dispositivo Citrix ADC para el registro de auditoría. Después de configurar la acción de mensaje de auditoría, especifique la acción en una directiva de cambio de contenido.

Para configurar el registro basado en directivas para una directiva de conmutación de contenido mediante la CLI

En la línea de comandos, escriba los siguientes comandos para configurar el registro basado en directivas para una directiva de conmutación de contenido y compruebe la configuración:

```
set cs policy <policyName> -logAction <string>

show cs policy <policyName>
<!--NeedCopy-->
```

Ejemplo:

```
> set cs policy cspol1 -logAction csLogAction
 Done
> show cs policy cspol1

```



```
    Policy: cspol1  Rule: TRUE  Action: csact1
    LogAction: csLogAction
    Hits: 0

1)  CS Vserver: csvs1
    Priority: 10
 Done
>
<!--NeedCopy-->
```

Para configurar el registro basado en directivas para una directiva de conmutación de contenido mediante la interfaz gráfica de usuario

Vaya a **Administración del tráfico > Cambio de contenido > Directivas**, abra una directiva y, en la lista Acción de registro, seleccione una acción de registro para la directiva.

Verificación de la configuración

Para comprobar que la configuración de conmutación de contenido es correcta, debe ver las entidades de conmutación de contenido. Para comprobar el correcto funcionamiento después de implementar la configuración de conmutación de contenido, puede ver las estadísticas que se generan a medida que se accede a los servidores.

Visualización de las propiedades de los servidores virtuales de conmutación de contenido

Puede ver las propiedades de los servidores virtuales de conmutación de contenido que ha configurado en el dispositivo Citrix ADC. Puede utilizar la información para comprobar si el servidor virtual está configurado correctamente y, si es necesario, para solucionar problemas. Además de detalles como el nombre, la dirección IP y el puerto, puede ver las distintas directivas vinculadas a un servidor virtual y su configuración de administración del tráfico.

Las directivas de cambio de contenido se muestran por orden de prioridad. Si más de una directiva tiene la misma prioridad, se muestran en el orden en que están enlazadas al servidor virtual.

> **Nota**
>
> Si ha configurado el servidor virtual de conmutación de contenido para que reenvíe el tráfico a un servidor virtual de equilibrio de carga, también puede ver las directivas de conmutación de contenido mediante la visualización de las propiedades del servidor virtual de equilibrio de carga.

Para ver las propiedades de los servidores virtuales de conmutación de contenido mediante la CLI

Para enumerar las propiedades básicas de todos los servidores virtuales de conmutación de contenido de la configuración o las propiedades detalladas de un servidor virtual de conmutación de contenido específico, en el símbolo del sistema, escriba uno de los siguientes comandos:

```
show cs vserver

show cs vserver <name>
<!--NeedCopy-->
```

Ejemplo

```
1.
show cs vserver Vserver-CS-1
Vserver-CS-1 (10.102.29.161:80) - HTTP Type: CONTENT
State: UP
Last state change was at Thu Jun 30 10:48:59 2011
Time since last state change: 6 days, 20:03:00.760
Client Idle Timeout: 180 sec
Down state flush: ENABLED
Disable Primary Vserver On Down : DISABLED
Appflow logging: DISABLED
Port Rewrite : DISABLED
State Update: DISABLED
Default: Content Precedence: RULE
Vserver IP and Port insertion: OFF
Case Sensitivity: ON
Push: DISABLED Push VServer:
Push Label Rule: none

...
1) Policy : __ESNS_PREBODY_POLICY Priority:0
2) Policy : __ESNS_POSTBODY_POLICY Priority:0

1) Compression Policy Name: __ESNS_CMP_POLICY Priority: 2147483647
GotoPriority Expression: END
Flowtype: REQUEST

2) Rewrite Policy Name: __ESNS_REWRITE_POLICY Priority: 2147483647
```



```
GotoPriority Expression: END
Flowtype: REQUEST

3) Cache Policy Name: dfbx Priority: 10
GotoPriority Expression: END
Flowtype: REQUEST

4) Responder Policy Name: __ESNS_RESPONDER_POLICY Priority: 2147483647
GotoPriority Expression: END

1) Policy: wiki Target: LBVIP2 Priority: 25 Hits: 0
2) Policy: plain Target: LBVIP1 Priority: 90 Hits: 0
3) Policy: DispOrderTest2 Target: KerbAuthLBVS Priority: 91 Hits: 0
4) Policy: test_Pol Target: LBVIP1 Priority: 92 Hits: 0
5) Policy: PolicyNameTesting Target: LBVIP1 Priority: 100 Hits: 0
 Done
>

show cs vserver
1) Vserver-CS-1 (10.102.29.161:80) - HTTP Type: CONTENT
State: UP
…
Appflow logging: DISABLED
Port Rewrite : DISABLED
State Update: DISABLED

2) apubendpt (10.111.111.1:80) - HTTP Type: CONTENT
State: UP
…
Client Idle Timeout: 180 sec
Down state flush: DISABLED
…

3) apubendpt1 (10.111.111.2:80) - HTTP Type: CONTENT
State: UP
…
Disable Primary Vserver On Down : DISABLED
Appflow logging: DISABLED
Port Rewrite : DISABLED
State Update: DISABLED
…
<!--NeedCopy-->
```


Ver directivas de cambio de contenido

Puede ver las propiedades de las directivas de cambio de contenido que ha definido, como el nombre, el dominio y la dirección URL o expresión, y utilizar la información para detectar errores en la configuración o para solucionar problemas si algo no funciona como debe funcionar.

Para ver las propiedades de las directivas de conmutación de contenido mediante la CLI

Para enumerar las propiedades básicas de todas las directivas de cambio de contenido de la configuración o las propiedades detalladas de una directiva de cambio de contenido específica, en el símbolo del sistema, escriba uno de los siguientes comandos:

```
show cs policy

show cs policy <PolicyName>
<!--NeedCopy-->
```

Ejemplo:

```
show cs policy

show cs policy-CS-1
<!--NeedCopy-->
```

Para ver las propiedades de las directivas de conmutación de contenido mediante la interfaz gráfica de usuario

Vaya a **Administración del tráfico** > **Cambio de contenido** > **Directivas**, seleccione una directiva y, en la lista Acción, seleccione **Mostrar enlaces**.

Visualización de una configuración de servidor virtual de conmutación de contenido mediante el visualizador

El visualizador de conmutación de contenido es una herramienta que se puede utilizar para ver una configuración de cambio de contenido en formato gráfico. Puede utilizar el visualizador para ver los siguientes elementos de configuración:

- Resumen de los servidores virtuales de equilibrio de carga a los que está enlazado el servidor virtual de conmutación de contenido.

- Todos los servicios y grupos de servicios enlazados al servidor virtual de equilibrio de carga y todos los monitores vinculados a los servicios.
- Detalles de configuración de cualquier elemento mostrado.
- Todas las directivas vinculadas al servidor virtual de conmutación de contenido. Estas directivas no tienen por qué ser directivas de cambio de contenido. Muchos tipos de directivas, como las directivas de reescritura, se pueden enlazar a un servidor virtual de conmutación de contenido.

Después de configurar los distintos elementos de una configuración de cambio de contenido y equilibrio de carga, puede exportar toda la configuración a un archivo de plantilla de aplicación.

> **Nota**
>
> El visualizador requiere una interfaz gráfica, por lo que solo está disponible a través de la interfaz gráfica de usuario.

Para ver una configuración de conmutación de contenido mediante el visualizador en la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Cambio de contenido > Servidores virtuales**.
2. En el panel de detalles, seleccione el servidor virtual que quiere ver y, a continuación, haga clic en **Visualizador**.
3. En la ventana **Visualizador de conmutación de contenido**, puede ajustar el área visible de la siguiente manera:
   - Haga clic **en** los iconos **Acercar y Alejar** para aumentar o reducir el área visible.
   - Haga clic en el icono **Guardar imagen** para guardar el gráfico como archivo de imagen.
   - En el campo Buscar en texto, empieza a escribir el nombre del elemento que está buscando. Cuando hayas escrito suficientes caracteres para identificar el elemento, se resalta su ubicación. Para restringir la búsqueda, haga clic en el menú desplegable y seleccione el tipo de elemento que quiere buscar.
4. Para ver los detalles de configuración de las entidades enlazadas a este servidor virtual, puede hacer lo siguiente:
   - Para ver las directivas enlazadas al servidor virtual, en la barra de herramientas de la parte superior del cuadro de diálogo, seleccione uno o varios iconos de directivas específicas de la función. Si las etiquetas de directivas están configuradas, aparecen en el área de vista principal.
   - Para ver los detalles de configuración de un servicio vinculado o grupo de servicios, haga clic en el icono del servicio, haga clic en la ficha Tareas relacionadas y, a continuación, haga clic en Mostrar servicios para miembros.

- Para ver los detalles de configuración de un monitor, haga clic en el icono del monitor, haga clic en la ficha **Tareas relacionadas** y, a continuación, haga clic en **Ver monitor**.

5. Para ver estadísticas detalladas de cualquier servidor virtual de la configuración de conmutación de contenido, haga clic en el servidor virtual del que quiere ver las estadísticas, haga clic en la ficha Tareas relacionadas y, a continuación, haga clic en **Estadísticas**.
6. Para ver una lista comparativa de los parámetros cuyos valores difieren o no están definidos en los contenedores de servicios de un servidor virtual de equilibrio de carga, haga clic en el icono de un contenedor, en la ficha **Tareas relacionadas** y, a continuación, en **Diferencia de atributos de servicio**.
7. Para ver los detalles de enlace de supervisión de los servicios de un contenedor, en el cuadro de diálogo Diferencia de atributos de servicio, en la columna Grupo del contenedor, haga clic en **Detalles**. Esta lista comparativa le ayuda a determinar qué contenedor de servicios tiene la configuración que quiere aplicar a todos los contenedores de servicios.
8. Para ver el número de solicitudes recibidas por segundo en un momento dado por los servidores virtuales de la configuración y el número de selecciones por segundo en un momento dado para las directivas de reescritura, respuesta y caché, haga clic en Mostrar estadísticas. La información estadística se muestra en los nodos respectivos del visualizador. Esta información no se actualiza en tiempo real. Se actualiza manualmente. Para actualizar la información, haga clic en Actualizar estadísticas.

   > **Nota**
   >
   > Esta opción solo está disponible en las compilaciones nCore de Citrix ADC.

9. Para copiar los detalles de configuración de un elemento en un documento u hoja de cálculo, haga clic en el icono de ese elemento, haga clic en Tareas relacionadas, haga clic en Propiedades de copia y, a continuación, pegue la información en un documento.
10. Para exportar toda la configuración que se muestra en el Visualizador a un archivo de plantilla de aplicación, haga clic en el icono del servidor virtual de conmutación de contenido, haga clic en Tareas relacionadas y, a continuación, haga clic en Crear plantilla. Al crear la plantilla de aplicación, puede configurar variables en algunas expresiones de directiva y acciones. Para obtener más información sobre la creación del archivo de plantilla de aplicación y la configuración de variables para una plantilla, consulte AppExpert.

Personalización de la configuración básica de conmutación de contenido

October 5, 2021

Después de configurar una configuración básica de cambio de contenido, es posible que deba personalizarla para que se ajuste a sus requisitos. Si sus servidores web están basados en UNIX y dependen de nombres de ruta que distinguen mayúsculas y minúsculas, puede configurar la distinción entre mayúsculas y min También puede establecer prioridad para la evaluación de las directivas de conmutación de contenido que ha configurado. Puede configurar servidores virtuales de conmutación de contenido HTTP y SSL para que escuchen en varios puertos en lugar de crear servidores virtuales independientes. Si quiere configurar el cambio de contenido para una LAN virtual específica, puede configurar un servidor virtual de conmutación de contenido con una directiva de escucha.

Configuración de la distinción de mayúsculas y min

Puede configurar el servidor virtual de conmutación de contenido para que trate las URL como sensibles a mayúsculas y minúsculas en las directivas basadas en URL. Cuando se configura la distinción entre mayúsculas y minúsculas, el dispositivo Citrix ADC considera el caso al evaluar directivas. Por ejemplo, si la distinción entre mayúsculas y minúsculas está desactivada, las URL /a/1.htm y /A/1.HTM se consideran idénticas. Si la distinción entre mayúsculas y minúsculas está activada, esas URL se tratan por separado y se pueden cambiar a destinos diferentes.

Para configurar la distinción entre mayúsculas y minúsculas mediante la

En el símbolo del sistema, escriba:

```
set cs vserver \<name\> -caseSensitive (ON|OFF)
```

Ejemplo:

```
1 set cs vserver Vserver-CS-1 -caseSensitive ON
2 <!--NeedCopy-->
```

Para configurar la distinción entre mayúsculas y minúsculas

1. Vaya a **Administración del tráfico > Cambio de contenido > Servidores virtuales** y abra un servidor virtual.
2. En **Configuración avanzada, seleccione Configuración**de **tráfico**y selecciona Sensibilidad entre mayúsculas y minúsculas.

Establecimiento de la prioridad para la evaluación de directivas

La prioridad hace referencia al orden en que se evalúan las directivas enlazadas a un servidor virtual. No es necesario configurar la prioridad, la precedencia predeterminada suele funcionar correc-

tamente.

Puede configurar la prioridad basada en URL o la prioridad basada en reglas en los siguientes casos:

- Primero se debe aplicar una directiva o un conjunto de directivas
- Solo se aplica otra directiva o conjunto de directivas si el primer conjunto no coincide con una solicitud.

Prioridad con directivas basadas en URL

Si hay varias URL coincidentes para la solicitud entrante, la prioridad (prioridad) de las directivas basadas en URL es:

1. Dominio y URL exacta
2. Dominio, prefijo y sufijo
3. Dominio y sufijo
4. Dominio y prefijo
5. Solo dominio
6. URL exacta
7. Prefijo y sufijo
8. Solo sufijo
9. Solo prefijo
10. Predeterminado

Si configura la prioridad en función de la URL, la URL de solicitud se compara con las URL configuradas. Si ninguna de las URL configuradas coincide con la URL de solicitud, se comprueban las directivas basadas en reglas. Si la URL de la solicitud no coincide con ninguna directiva basada en reglas o si el grupo de contenido seleccionado para la solicitud no funciona, la solicitud se procesa de la siguiente manera:

- Si configura un grupo predeterminado para el servidor virtual de conmutación de contenido, la solicitud se reenvía al grupo predeterminado.
- Si el grupo predeterminado configurado está inactivo o si no se ha configurado ningún grupo predeterminado, se envía al cliente un mensaje de error “HTTP 404 Not Found”.

> **Nota**
>
> Debe configurar la prioridad basada en URL si el tipo de contenido (por ejemplo, imágenes) es el mismo para todos los clientes. Sin embargo, si se deben entregar distintos tipos de contenido en función de los atributos del cliente (como Accept-Language), debe utilizar la prioridad basada en reglas.

Prioridad con directivas basadas en reglas

Si configura la prioridad en función de las reglas, que es la configuración predeterminada, la solicitud se prueba en función de las directivas basadas en reglas que haya configurado. Si la solicitud no coincide con ninguna directiva basada en reglas o si el grupo de contenido seleccionado para la solicitud entrante está caído, la solicitud se procesa de la siguiente manera:

- Si se configura un grupo predeterminado para el servidor virtual de conmutación de contenido, la solicitud se reenvía al grupo predeterminado.
- Si el grupo predeterminado configurado está inactivo o si no se ha configurado ningún grupo predeterminado, se envía al cliente un mensaje de error "HTTP 404 Not Found".

Para configurar la prioridad mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
set cs vserver \<name\> -precedence ( RULE | URL )
```

Ejemplo:

```
set cs vserver Vserver-CS-1 -precedence RULE
```

Para configurar la prioridad mediante la utilidad de configuración

1. Vaya a **Administración del tráfico > Cambio de contenido > Servidores virtuales** y abra un servidor virtual.
2. En Configuración avanzada, seleccione Configuración de **tráfico**y, a continuación, especifique Precedencia.

Compatibilidad con varios puertos para servidores virtuales de conmutación de contenido de tipo HTTP y SSL

Puede configurar Citrix ADC para que los servidores virtuales de conmutación de contenido HTTP y SSL escuchen en varios puertos, sin tener que configurar servidores virtuales independientes. Esta función es especialmente útil si quiere basar una decisión de cambio de contenido en una parte de la URL y otros parámetros de L7. En lugar de configurar varios servidores virtuales con la misma dirección IP y puertos diferentes, puede configurar una dirección IP y especificar el puerto como *. Como resultado, el tamaño de la configuración también se reduce.

Para configurar un servidor virtual de conmutación de contenido HTTP o SSL para que escuche en varios puertos mediante la línea de comandos

En el símbolo del sistema, escriba:

```
add cs vserver \<name\> \<serviceType\> \<IPAddress\> Port \*
```


Ejemplo

```
> add cs vserver cs1 HTTP 10.102.92.215 *
 Done
> sh cs vserver cs1
        cs1 (10.102.92.215:*) - HTTP    Type: CONTENT
        State: UP
        Last state change was at Tue May 20 01:15:49 2014
        Time since last state change: 0 days, 00:00:03.270
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Appflow logging: ENABLED
        Port Rewrite : DISABLED
        State Update: DISABLED
        Default:        Content Precedence: RULE
        Vserver IP and Port insertion: OFF
        L2Conn: OFF     Case Sensitivity: ON
        Authentication: OFF
        401 Based Authentication: OFF
        Push: DISABLED  Push VServer:
        Push Label Rule: none
        IcmpResponse: PASSIVE
        RHIstate:  PASSIVE
        TD: 0
 Done
<!--NeedCopy-->
```

Para configurar un servidor virtual de conmutación de contenido HTTP o SSL para que escuche en varios puertos mediante la utilidad de configuración

1. Vaya a **Administración del tráfico > Cambio de contenido > Servidores virtuales**y cree un servidor virtual de tipo HTTP o SSL.
2. Utilice un asterisco (*) para especificar el puerto.

Configuración de servidores virtuales comodín por VLAN

Si quiere configurar el cambio de contenido para el tráfico en una VLAN específica, puede crear un servidor virtual comodín con una directiva de escucha que restrinja el procesamiento del tráfico solo en la VLAN especificada.

Para configurar un servidor virtual comodín que escucha una VLAN específica mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
1 add cs vserver <name> <serviceType> IPAddress `* Port *` -listenpolicy
     <expression> [-listenpriority <positive_integer>]
2 <!--NeedCopy-->
```

Ejemplo:

```
1 add cs vserver Vserver-CS-vlan1 ANY * *
2 -listenpolicy "CLIENT.VLAN.ID.EQ(2)"  -listenpriority 10
3 <!--NeedCopy-->
```

Para configurar un servidor virtual comodín que escucha una VLAN específica mediante la utilidad de configuración

Vaya a **Administración del tráfico > Cambio de contenido > Servidores virtuales**y configure un servidor virtual. Especifique una directiva de escucha que la restrinja al procesamiento del tráfico solo en la VLAN especificada.

Después de crear este servidor virtual, lo vincula a uno o varios servicios tal y como se describe en Configuración del equilibrio de carga básico.

Configuración de la configuración de la versión de Microsoft SQL Server

Puede especificar la versión de Microsoft® SQL Server® para un servidor virtual de conmutación de contenido de tipo MSSQL. Se recomienda la configuración de versión si espera que algunos clientes no ejecuten la misma versión que su producto Microsoft SQL Server. La configuración de la versión proporciona compatibilidad entre las conexiones del lado del cliente y del lado del servidor al asegurarse de que todas las comunicaciones se ajustan a la versión del servidor.

Para establecer el parámetro de versión de Microsoft SQL Server mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para establecer el parámetro de versión de Microsoft SQL Server para un servidor virtual de conmutación de contenido y compruebe la configuración:

- set cs vserver \<name\> -mssqlServerVersion \<mssqlServerVersion\>
- show cs vserver \<name\>

Ejemplo

```
1 > set cs vserver myMSSQLcsvip -mssqlServerVersion 2008R2 Done > show cs
      vserver myMSSQLcsvip myMSSQLcsvip (192.0.2.13:1433) - MSSQL Type:
     CONTENT State: UP . . . . . MSsql Server Version: 2008R2 . . . . .
      . Done >
2 <!--NeedCopy-->
```

Para establecer el parámetro de versión de Microsoft SQL Server mediante la utilidad de configuración

1. Vaya a **Administración del tráfico > Conmutación de contenido > Servidores virtuales**, configure un servidor virtual y especifique el protocolo como MSSQL.
2. En **Configuración avanzada**, especifique la **versión del servidor**.

Habilitar la comprobación de estado TCP externa para servidores virtuales UDP

En las nubes públicas, puede utilizar el dispositivo Citrix ADC como equilibrador de carga de segundo nivel cuando se utiliza el equilibrador de cargas nativo como primer nivel. El equilibrador de carga nativo puede ser un equilibrador de carga de aplicaciones (ALB) o un equilibrador de carga de red (NLB). La mayoría de las nubes públicas no admiten sondeos de estado UDP en sus equilibradores de cargas nativos. Para supervisar el estado de la aplicación UDP, las nubes públicas recomiendan agregar un endpoint basado en TCP al servicio. El endpoint refleja el estado de la aplicación UDP.

El dispositivo Citrix ADC admite la comprobación de estado basada en TCP externa para un servidor virtual UDP. Esta función introduce un agente de escucha TCP en el VIP del servidor virtual de conmutación de contenido y en el puerto configurado. El agente de escucha TCP refleja el estado del servidor virtual.

Para habilitar la comprobación de estado TCP externa para servidores virtuales UDP mediante CLI

En el símbolo del sistema, escriba el comando siguiente para habilitar una comprobación de estado TCP externa con la opción TcpProbeport:


```
add cs vserver <name> <protocol> <IPAddress> <port> -tcpProbePort <
    tcpProbePort>
<!--NeedCopy-->
```

Ejemplo:

```
add cs vserver Vserver-CS-1 UDP 10.102.29.161 5002 -tcpProbePort 5000
<!--NeedCopy-->
```

Para habilitar la comprobación de estado TCP externa para servidores virtuales UDP mediante la interfaz gráfica de usuario

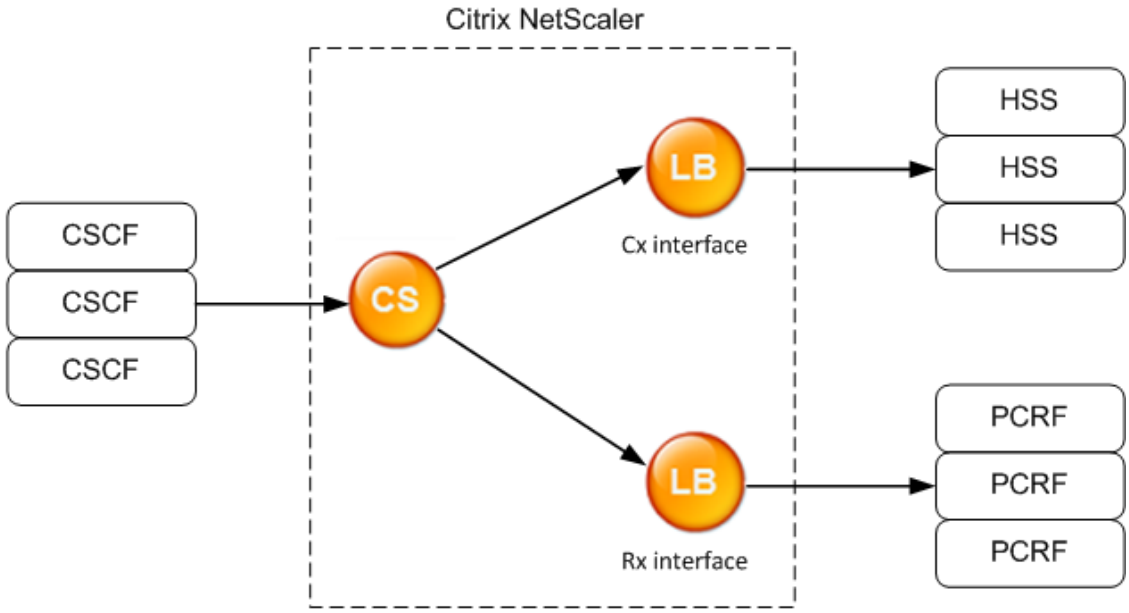
1. Vaya a **Administración del tráfico > Cambio de contenido > Servidores virtuales**y, a continuación, cree un servidor virtual.
2. Haga clic en **Agregar** para crear un servidor virtual.
3. En el panel **Configuración básica**, agregue el número de puerto en el campo **Puerto de sondeo TCP** .
4. Haga clic en **OK**.

Cambio de contenido para protocolo de diameter

February 16, 2021

Para el tráfico de protocolo de diameter, puede configurar el dispositivo Citrix ADC (o dispositivo virtual) para que actúe como un agente de retransmisión que equilibra la carga y reenvía un paquete al destino adecuado sobre la base del contenido del mensaje (valor AVP en el mensaje). Dado que el dispositivo no realiza ningún procesamiento a nivel de aplicación, proporciona servicios de retransmisión para todas las aplicaciones de diameter según lo especificado por las directivas de cambio de contenido configuradas. Por lo tanto, el dispositivo anuncia el ID de aplicación de relé en el mensaje de respuesta de intercambio de capacidades (CEA) cuando el cliente establece una conexión de diameter. Debe configurar un servidor virtual de cambio de contenido, servidores virtuales de equilibrio de carga y servicios para representar los nodos de diameter. Cuando una solicitud llega al servidor virtual de cambio de contenido, el servidor virtual aplica las directivas de cambio de contenido asociadas a ese tipo de solicitud. Después de evaluar las directivas, el servidor virtual de cambio de contenido enruta la solicitud al servidor virtual de equilibrio de carga adecuado, que la envía al servicio adecuado.

Una interfaz de diameter proporciona una conexión entre los diferentes nodos de diameter. La siguiente implementación de ejemplo utiliza interfaces Cx y Rx. Una interfaz Cx proporciona una conexión entre un CSCF y un HSS. Una interfaz Rx proporciona una conexión entre un CSCF y un PCRF. Todos los mensajes llegan al dispositivo Citrix ADC. Dependiendo de si el mensaje es para una interfaz Cx o Rx y de las directivas de cambio de contenido definidas, Citrix ADC selecciona un grupo de servidores de equilibrio de carga adecuado.



CSCF=Call Session Control Function
HSS=Home Subscriber Server
PCRF=Policy and Charging Rules Function

Configuración de ejemplo

1. Para cada entidad, cree un servicio, un servidor de equilibrio de carga y vincule el servicio al servidor virtual.

```
add service svc_pcrf[1-3] 1.1.1.1[1-3] DIAMETER 3868
add service svc_hss[1-3] 1.1.1.2[1-3] DIAMETER 3868
add lb vserver vs_rx DIAMETER -persistenceType DIAMETER -
   persistavpno 263
add lb vserver vs_cx DIAMETER -persistenceType DIAMETER -
   persistavpno 263
bind lb vserver vs_rx svc_pcrf[1-3]
bind lb vserver vs_cx svc_hss[1-3]
<!--NeedCopy-->
```


2. Cree un servidor virtual de cambio de contenido y dos acciones (una para cada servidor virtual de equilibrio de carga). Cree dos directivas de cambio de contenido y vincule estas directivas al servidor virtual de cambio de contenido, especificando una prioridad para cada directiva.

```
add cs vserver cs_diameter DIAMETER 10.1.1.10 3868
add cs action cx_action -targetLBVserver vs_cx
add cs action rx_action  - targetLBvserver vs_rx
add cs policy cx_policy -rule "DIAMETER.REQ.AUTH_APPLICATION_ID.EQ
    (16777216)" -action cx_action
add cs policy rx_policy -rule "DIAMETER.REQ.AUTH_APPLICATION_ID.EQ
    (16777236)" -action rx_action
bind cs vserver cs_diameter -policyName rx_policy -priority 100
bind cs vserver cs_diameter -policyName cx_policy -priority 110
<!--NeedCopy-->
```

Protección de la configuración de cambio de contenido contra fallos

February 16, 2021

La cambio de contenido puede fallar cuando el servidor virtual de cambio de contenido se desactiva o no gestiona el tráfico excesivo, o por otras razones. Para reducir las posibilidades de fallo, puede tomar las siguientes medidas para proteger la configuración de cambio de contenido contra fallos:

Configuración de un servidor virtual de copia de seguridad

Si el servidor virtual de cambio de contenido principal está marcado como DESACTIVado o DESACTIVado, el dispositivo Citrix ADC puede dirigir las solicitudes a un servidor virtual de cambio de contenido de copia de seguridad. También puede enviar un mensaje de notificación al cliente con respecto a la interrupción o mantenimiento del sitio. El servidor virtual de cambio de contenido de copia de seguridad es un proxy y es transparente para el cliente.

Al configurar el servidor virtual de copia de seguridad, puede especificar el parámetro de configuración Inhabilitar primario cuando está caído para asegurarse de que, cuando el servidor virtual principal vuelva a activarse, siga siendo el secundario hasta que lo obligue manualmente a tomar el control como principal. Resulta útil si desea asegurarse de que se conservan las actualizaciones de la base de datos en el servidor para la copia de seguridad, lo que le permite sincronizar las bases de datos antes de restaurar el servidor virtual principal.

Puede configurar un servidor virtual de cambio de contenido de copia de seguridad al crear un servidor virtual de cambio de contenido o al cambiar los parámetros opcionales de un servidor virtual

de cambio de contenido existente. También puede configurar un servidor virtual de cambio de contenido de copia de seguridad para un servidor virtual de cambio de contenido de copia de seguridad existente, creando de este modo contenido de copia de seguridad conmutando servidores virtuales. La profundidad máxima de los servidores virtuales de cambio de contenido de copia de seguridad en cascada es 10. El dispositivo busca un servidor virtual de cambio de contenido de copia de seguridad que esté activo y accede a ese servidor virtual de cambio de contenido para entregar el contenido.

> **Nota**
>
> Si un servidor virtual de cambio de contenido está configurado con un servidor virtual de cambio de contenido de copia de seguridad y una URL de redirección, el servidor virtual de cambio de contenido de copia de seguridad tiene prioridad sobre la URL de redirección. La redirección se utiliza cuando los servidores virtuales principales y de copia de seguridad están inactivos.

Para configurar un servidor virtual de cambio de contenido de copia de seguridad mediante la CLI

En el símbolo del sistema, escriba:

```
set cs vserver <name> -backupVserver <string> -disablePrimaryOnDown (ON
    |OFF)
<!--NeedCopy-->
```

Ejemplo

```
set cs vserver Vserver-CS-1 -backupVserver Vserver-CS-2 -
    disablePrimaryOnDown ON
<!--NeedCopy-->
```

Para configurar un servidor virtual de cambio de contenido de copia de seguridad mediante la GUI

1. Vaya a **Traffic Management > Content Switching > Virtual Servers**, configure un servidor virtual y especifique el protocolo como MYSQL.
2. En **Configuración avanzada**, seleccione **Protección** y especifique un **servidor virtual de copia de seguridad**.

Desviar el exceso de tráfico a un servidor virtual de copia de seguridad

La opción de desbordamiento desvía las nuevas conexiones que llegan a un servidor virtual de cambio de contenido a un servidor virtual de cambio de contenido de copia de seguridad cuando el número de conexiones al servidor virtual de cambio de contenido supera el valor de umbral configurado. El valor de umbral se calcula dinámicamente o puede establecer el valor. El número de conexiones establecidas (en TCP) en el servidor virtual se compara con el valor de umbral. Cuando el número de conexiones alcanza el umbral, las nuevas conexiones se desvían al servidor virtual de cambio de contenido de copia de seguridad.

Si los servidores virtuales de cambio de contenido de copia de seguridad alcanzan el umbral configurado y no pueden asumir la carga, el servidor virtual de cambio de contenido principal desvía todas las solicitudes a la dirección URL de redirección. Si no se configura una dirección URL de redirección en el servidor virtual de cambio de contenido principal, se eliminan las solicitudes posteriores.

Para configurar un servidor virtual de cambio de contenido para desviar nuevas conexiones a un servidor virtual de copia de seguridad mediante la CLI

En el símbolo del sistema, escriba:

```
set cs vserver <name> -soMethod <methodType> -soThreshold <
    thresholdValue> -soPersistence <persistenceValue> -
    soPersistenceTimeout <timeoutValue>
<!--NeedCopy-->
```

Ejemplo

```
set cs vserver Vserver-CS-1 -soMethod Connection -soThreshold 1000 -
    soPersistence enabled -soPersistenceTimeout 2
<!--NeedCopy-->
```

Para establecer un servidor virtual de cambio de contenido para desviar nuevas conexiones a un servidor virtual de copia de seguridad mediante la GUI

1. Vaya a **Traffic Management > Content Switching > Virtual Servers**, configure un servidor virtual y especifique el protocolo como MYSQL.
2. En **Configuración avanzada**, seleccione **Protección** y configure el desbordamiento.

Configuración de una URL de redirección

Puede configurar una dirección URL de redirección para comunicar el estado del dispositivo Citrix ADC si un servidor virtual de cambio de contenido de tipo HTTP o HTTPS está DESACTIVADO o INHABILITADO. Esta URL puede ser local o remota.

Las URL de redirección pueden ser URL absolutas o URL relativas. Si la URL de redirección configurada contiene una URL absoluta, la redirección HTTP se envía a la ubicación configurada, independientemente de la URL especificada en la solicitud HTTP entrante. Si la dirección URL de redirección configurada contiene solo el nombre de dominio (URL relativa), la redirección HTTP se envía a una ubicación después de agregar la dirección URL entrante al dominio configurado en la dirección URL de redirección.

Citrix recomienda utilizar una URL absoluta. Es decir, una URL que termina en/, por ejemplo www.example.com/ en lugar de una URL relativa. Una redirección de URL relativa puede provocar que el analizador de vulnerabilidades informe un falso positivo.

> **Nota**
>
> Si un servidor virtual de cambio de contenido está configurado con un servidor virtual de copia de seguridad y una dirección URL de redirección, el servidor virtual de copia de seguridad tiene prioridad sobre la URL de redirección. Se utiliza una dirección URL de redirección cuando los servidores virtuales principales y de copia de seguridad están inactivos.

Cuando se configura la redirección y el servidor virtual de cambio de contenido no está disponible, el dispositivo emite una redirección HTTP 302 al explorador del usuario.

Para configurar una URL de redireccionamiento para cuando el servidor virtual de cambio de contenido no está disponible mediante la CLI

En el símbolo del sistema, escriba:

```
set cs vserver <name> -redirectURL <URLValue>
<!--NeedCopy-->
```

Ejemplo

```
set cs vserver Vserver-CS-1 -redirectURL http://www.newdomain.com/
   mysite/maintenance
<!--NeedCopy-->
```


Para configurar una dirección URL de redirección para cuando el servidor virtual de cambio de contenido no está disponible mediante la GUI

1. Vaya a **Traffic Management > Content Switching > Virtual Servers**, configure un servidor virtual y especifique el protocolo como MYSQL.
2. En **Configuración avanzada**, seleccione **Protección** y especifique una dirección URL de redirección.

Configuración de la opción de actualización de estado

La función de cambio de contenido permite la distribución de solicitudes de cliente entre varios servidores en función del contenido específico presentado a los usuarios. Para una cambio de contenido eficiente, el servidor virtual de cambio de contenido distribuye el tráfico a los servidores virtuales de equilibrio de carga según el tipo de contenido, y los servidores virtuales de equilibrio de carga distribuyen el tráfico a los servidores físicos según el método de equilibrio de carga especificado.

Para una gestión fluida del tráfico, es importante que el servidor virtual de cambio de contenido conozca el estado de los servidores virtuales de equilibrio de carga. La opción de actualización de estado ayuda a marcar el servidor virtual de cambio de contenido DOWN si el servidor virtual de equilibrio de carga enlazado a él está marcado como DOWN. Un servidor virtual de equilibrio de carga se marca como DOWN si todos los servidores físicos enlazados a él están marcados como DOWN.

Cuando la actualización de estado está inhabilitada:

El estado del servidor virtual de cambio de contenido se marca como UP. Permanece UP incluso si no hay un servidor virtual de equilibrio de carga enlazado que esté UP.

Cuando la actualización de estado está habilitada:

Cuando agrega un servidor virtual de cambio de contenido, inicialmente, su estado se muestra como DOWN. Cuando vincula un servidor virtual de equilibrio de carga cuyo estado es UP, el estado del servidor virtual de cambio de contenido se convierte en UP.

Si hay más de un servidor virtual de equilibrio de carga enlazado y si uno de ellos se especifica como predeterminado, el estado del servidor virtual de cambio de contenido refleja el estado del servidor virtual de equilibrio de carga predeterminado.

Si hay más de un servidor virtual de equilibrio de carga enlazado sin que ninguno de ellos se especifique como predeterminado, el estado del servidor virtual de cambio de contenido se marca UP solo si todos los servidores virtuales de equilibrio de carga enlazados están UP.

Para configurar la opción de actualización de estado mediante la CLI

En el símbolo del sistema, escriba:


```
add cs vserver <name> <protocol> <ipAddress> <port> -stateUpdate
   ENABLED
<!--NeedCopy-->
```

Ejemplo

```
 add cs vserver csw_vserver HTTP 10.18.250.154 80 -stateupdate ENABLED
    -cltTimeout 180
<!--NeedCopy-->
```

Para configurar la opción de actualización de estado mediante la interfaz gráfica de usuario

1. Vaya a **Traffic Management > Content Switching > Virtual Servers**, configure un servidor virtual y especifique el protocolo como MYSQL.
2. En **Configuración avanzada**, seleccione **Configuración de tráfico** y, a continuación, seleccione **Actualización de estado**.

VACIAR LA COLA DE SOBRETENSIONES

Cuando un servidor físico recibe un aumento de solicitudes, se vuelve lento para responder a los clientes que están conectados actualmente a él, lo que deja a los usuarios insatisfechos y descontentos. A menudo, la sobrecarga también hace que los clientes reciban páginas de error. Para evitar tales sobrecargas, el dispositivo Citrix ADC proporciona funciones como la protección contra sobretensiones, que controla la velocidad a la que se pueden establecer nuevas conexiones a un servicio.

El dispositivo realiza multiplexación de conexión entre clientes y servidores físicos. Cuando recibe una solicitud de cliente para acceder a un servicio en un servidor, el dispositivo busca una conexión ya establecida con el servidor que sea gratuita. Si encuentra una conexión libre, utiliza esa conexión para establecer un vínculo virtual entre el cliente y el servidor. Si no encuentra una conexión libre existente, el dispositivo establece una nueva conexión con el servidor y establece un vínculo virtual entre el cliente y el servidor. Sin embargo, si el dispositivo no puede establecer una nueva conexión con el servidor, envía la solicitud del cliente a una cola de sobretensiones. Si todos los servidores físicos vinculados al servidor virtual de equilibrio de carga o de cambio de contenido alcanzan el límite superior de las conexiones de cliente (valor máximo del cliente, umbral de protección contra sobretensiones o capacidad máxima del servicio), el dispositivo no podrá establecer una conexión con ningún servidor. La función de protección contra sobretensiones utiliza la cola de sobretensiones para regular la velocidad a la que se abren las conexiones con los servidores físicos. El dispositivo mantiene una cola de sobretensión diferente para cada servicio vinculado al servidor virtual.

La longitud de una cola de sobretensiones aumenta cada vez que llega una solicitud para la que el dispositivo no puede establecer una conexión, y la longitud disminuye cada vez que se envía una solicitud de la cola al servidor o se agana el tiempo de espera de una solicitud y se elimina de la cola.

Si la cola de sobretensión de un servicio o grupo de servicios es demasiado larga, es posible que desee vaciarla. Puede vaciar la cola de sobretensiones de un servicio o grupo de servicios específico, o de todos los servicios y grupos de servicios vinculados a un servidor virtual de equilibrio de carga. El vaciado de una cola de sobretensión no afecta a las conexiones existentes. Solo se eliminan las solicitudes presentes en la cola de sobretensiones. Para esas solicitudes, el cliente tiene que hacer una nueva solicitud.

También puede vaciar la cola de sobretensiones de un servidor virtual de cambio de contenido. Si un servidor virtual de cambio de contenido reenvía algunas solicitudes a un servidor virtual de equilibrio de carga determinado y el servidor virtual de equilibrio de carga también recibe otras solicitudes, al vaciar la cola de sobretensión del servidor virtual de cambio de contenido, solo las solicitudes recibidas de esta cambio de contenido servidor virtual se vacían. Las demás solicitudes de la cola de sobretensión del servidor virtual de equilibrio de carga no se vacían.

> **Nota**
>
> No puede vaciar las colas de sobretensión de redirección de caché, autenticación, servidores virtuales VPN o GSLB o servicios GSLB.
> No utilice la función Protección contra sobretensiones si Usar IP de origen (USIP) está habilitada.

Para vaciar una cola de sobretensiones mediante la CLI

El comando flush ns SurgeQ funciona de la siguiente manera:

- Puede especificar el nombre de un servicio, grupo de servicios o servidor virtual cuya cola de sobretensiones debe vaciarse.
- Si especifica un nombre mientras se ejecuta el comando, se vacía la cola de sobretensión de la entidad especificada. Si más de una entidad tiene el mismo nombre, el dispositivo vacía las colas de sobretensión de todas esas entidades.
- Si especifica el nombre de un grupo de servicios y un nombre de servidor y un puerto mientras ejecuta el comando, el dispositivo vacía la cola de sobretensión solo del miembro del grupo de servicio especificado.
- No se puede especificar directamente un miembro del grupo de servicios (<serverName> y <port>) sin especificar el nombre del grupo de servicios (<name>) y no se puede especificar <port> sin una <serverName>. Especifique <serverName> y <port> si quiere vaciar la cola de sobretensión para un miembro del grupo de servicios específico.
- Si ejecuta el comando sin especificar ningún nombre, el dispositivo vacía las colas de sobretensión de todas las entidades presentes en el dispositivo.

- Si un miembro del grupo de servicios se identifica con un nombre de servidor, debe especificar el nombre del servidor en este comando; no puede especificar su dirección IP.

En el símbolo del sistema, escriba:

```
flush ns surgeQ [-name <name>] [-serverName <serverName> <port>].
<!--NeedCopy-->
```

Ejemplos

```
1. flush ns surgeQ  - name SVC1ANZGB  - serverName 10.10.10.1 80
The above command flushes the surge queue of the service or virtual
    server that is named SVC1ANZGB and has IP address as 10.10.10

2. flush ns surgeQ
The above command flushes all the surge queues on the appliance.
<!--NeedCopy-->
```

Para vaciar una cola de sobretensiones mediante la interfaz gráfica de usuario

Vaya a **Administración del tráfico > Cambio de contenido > Servidores virtuales**, seleccione un servidor virtual y, en la lista Acción, seleccione **Flush Surge Queue**.

Administración de una configuración de conmutación de contenido

October 5, 2021

Una vez configurada una configuración de conmutación de contenido, es posible que se requieran cambios periódicos. Cuando se actualizan los sistemas operativos o el software, o el hardware se desgasta y se reemplaza, es posible que tengas que desinstalar la configuración. La carga de su configuración podría aumentar y requerir más recursos. También puede modificar la configuración para mejorar el rendimiento.

Estas tareas pueden requerir desvincular directivas del servidor virtual de conmutación de contenido o inhabilitar o quitar los servidores virtuales de conmutación de contenido. Después de cambiar la configuración, es posible que tenga que volver a habilitar los servidores y volver a enlazar las directivas. Es posible que también quieras cambiar el nombre de tus servidores virtuales.

Desvinculación de directivas del servidor virtual de conmutación de contenido

Al desenlazar una directiva de conmutación de contenido de su servidor virtual, el servidor virtual ya no incluye esa directiva al determinar dónde dirigir las solicitudes.

Para desenlazar una directiva de un servidor virtual de conmutación de contenido mediante la CLI

En el símbolo del sistema, escriba:

```
unbind cs vserver <name> -policyname <string>
```

Ejemplo:

```
unbind cs vserver Vserver-CS-1 -policyname Policy-CS-1
```

Para desenlazar una directiva de un servidor virtual de conmutación de contenido mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Cambio de contenido > Servidores virtuales**y abra el servidor virtual.
2. Haga clic en la sección **Directivas**, seleccione la directiva y haga clic en **Desvincular**.

Eliminación de servidores virtuales de conmutación de contenido

Normalmente, se quita un servidor virtual de conmutación de contenido solo cuando ya no lo necesita. Al quitar un servidor virtual de conmutación de contenido, el dispositivo Citrix ADC primero desvincula todas las directivas del servidor virtual de conmutación de contenido y, a continuación, lo quita.

Para quitar un servidor virtual de conmutación de contenido mediante la CLI

En el símbolo del sistema, escriba:

```
rm cs vserver <name>
```

Ejemplo:

```
rm cs vserver Vserver-CS-1
```

Para quitar un servidor virtual de conmutación de contenido mediante la interfaz gráfica de usuario

Vaya a **Administración del tráfico > Cambio de contenido > Servidores virtuales**, seleccione un servidor virtual y haga clic en **Eliminar**.

Desactivación y reactivación de servidores virtuales de conmutación de contenido

Los servidores virtuales de conmutación de contenido están habilitados de forma predeterminada al crearlos. Puede inhabilitar un servidor virtual de conmutación de contenido para realizar tareas de mantenimiento. Si inhabilita el servidor virtual de conmutación de contenido, el estado del servidor virtual de conmutación de contenido cambia a Fuera de servicio. Mientras está fuera de servicio, el servidor virtual de conmutación de contenido no responde a las solicitudes.

Para inhabilitar o volver a habilitar un servidor virtual mediante la CLI

En el símbolo del sistema, escriba uno de los siguientes comandos:

- `disable cs vserver <name>`
- `enable cs vserver <name>`

Ejemplo:

```
disable cs vserver Vserver-CS-1
enable cs vserver Vserver-CS-1
```

Para inhabilitar o volver a habilitar un servidor virtual mediante la interfaz gráfica de usuario

Vaya a **Administración del tráfico > Cambio de contenido > Servidores virtuales**, seleccione un servidor virtual y, en la lista **Acción**, seleccione **Habilitaro Inhabilitar**.

Cambiar nombre de servidores virtuales de conmutación de contenido

Puede cambiar el nombre de un servidor virtual de conmutación de contenido sin desvincularlo. El nuevo nombre se propaga automáticamente a todas las partes afectadas de la configuración de Citrix ADC.

Para cambiar el nombre de un servidor virtual mediante la CLI

En el símbolo del sistema, escriba:

```
rename cs vserver <name> <newName>
```

Ejemplo:

```
1 `rename cs vserver Vserver-CS-1 Vserver-CS-2`
```


Para cambiar el nombre de un servidor virtual mediante la GUI

Vaya a **Administración del tráfico > Cambio de contenido > Servidores virtuales**, seleccione un servidor virtual y, en la lista **Acción**, seleccione **Cambiar nombre**.

Administración de directivas de cambio de contenido

Puede modificar una directiva existente configurando las reglas o cambiando la dirección URL de la directiva, o bien puede quitar una directiva. También puede cambiar el nombre de una directiva de cambio de contenido avanzada existente. Puede crear distintas directivas basadas en la URL. Las directivas basadas en URL pueden ser de diferentes tipos, como se describe en la tabla siguiente.

Para obtener más información, consulte Ejemplos de directivas basadas en URL.

> **Nota**
>
> Puede configurar el cambio de contenido basado en reglas mediante expresiones de directivas clásicas o expresiones de directivas avanzadas.

Para modificar, quitar o cambiar el nombre de una directiva mediante la CLI

En el símbolo del sistema, escriba uno de los siguientes comandos:

- `set cs policy <policyName> [-domain <domainValue>] [-rule <ruleValue>] [-url <URLValue>]`
- `rm cs policy <policyName>`
- `rename cs policy <policyName> <newPolicyName>`

Ejemplo:

```
set cs policy-CS-1 -domain ”www.domainxyz.com”

set cs policy-CS-1 -rule ”CLIENT.IP.SRC.SUBNET(22).EQ(10.100.148.0)”

set cs policy-CS-2 -rule ”SYS.TIME.BETWEEN(GMT 2010 Jun,GMT 2010 Jul)”

set cs policy-CS-1 -url /sports/*

rename cs policy-CS-1 Policy-CS-11

rm cs policy-CS-1
```


Para modificar, quitar o cambiar el nombre de una directiva mediante la GUI

1. Vaya a **Administración del tráfico > Cambio de contenido > Directivas**.
2. Seleccione la directiva y elimínala, edítela o, en la lista **Acción**, haga clic en **Cambiar nombre**.

Administrar conexiones de cliente

February 16, 2021

Para garantizar una administración eficiente de las conexiones de cliente, puede configurar los servidores virtuales de cambio de contenido en el dispositivo Citrix ADC para que utilicen las siguientes funciones:

- **Configuración de la respuesta ICMP.** Puede configurar el dispositivo Citrix ADC para que envíe respuestas ICMP a solicitudes PING de acuerdo con su configuración. En la dirección IP correspondiente al servidor virtual, establezca ICMP RESPONSE en VSVR_CNTRLD y, en el servidor virtual, establezca la respuesta del servidor virtual ICMP.
  Se pueden realizar las siguientes configuraciones en un servidor virtual:
  - Cuando establece la respuesta del servidor virtual ICMP en PASIVE en todos los servidores virtuales, el dispositivo Citrix ADC siempre responde.
  - Cuando configura el servidor virtual ICMP RESPONSE en ACTIVE en todos los servidores virtuales, el dispositivo ADC responde incluso si un servidor virtual está ACTIVADO.
  - Cuando se establece RESPUESTA del servidor virtual ICMP en ACTIVE en algunos y PASIVE en otros, el dispositivo ADC responde incluso si un servidor virtual establecido en ACTIVE está ACTIVADO.

Redirigir las solicitudes de cliente a una caché

La función de redirección de caché Citrix ADC redirige las solicitudes HTTP a una caché. Puede reducir significativamente la carga de responder a las solicitudes HTTP y mejorar el rendimiento del sitio web mediante la implementación adecuada de la función de redirección de caché.

Una caché almacena el contenido HTTP solicitado con frecuencia. Al configurar la redirección de caché en un servidor virtual, el dispositivo Citrix ADC envía solicitudes HTTP que se pueden almacenar en caché a la caché y solicitudes HTTP que no se pueden almacenar en caché al servidor web de origen. Para obtener más información sobre la redirección de caché, consulte “Redirección de caché.

Para configurar la redirección de caché en un servidor virtual mediante la CLI

En el símbolo del sistema, escriba:

```
set cs vserver \<name\> -cacheable \<Value\>
```


Ejemplo

```
set cs vserver Vserver-CS-1 -cacheable yes
```

Para configurar la redirección de caché en un servidor virtual mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Cambio de contenido > Servidores virtuales** y abra un servidor virtual.
2. En **Configuración avanzada**, seleccione **Configuración de tráfico** y seleccione **Caché**.

Habilitación de la limpieza retardada de conexiones de servidor virtual

En determinadas condiciones, puede configurar la configuración de vaciado de estado inactivo para finalizar las conexiones existentes cuando un servicio o un servidor virtual está marcado como DOWN. Terminar las conexiones existentes libera recursos y, en algunos casos, acelera la recuperación de configuraciones de equilibrio de carga sobrecargadas.

Para configurar la configuración de vaciado de estado inactivo en un servidor virtual mediante la CLI

En el símbolo del sistema, escriba:

```
set cs vserver \<name\> -downStateFlush \<Value\>
```

Ejemplo

```
1 set cs vserver Vserver-CS-1 -downStateFlush enabled
2 <!--NeedCopy-->
```

Para configurar la configuración de vaciado de estado inactivo en un servidor virtual mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Cambio de contenido > Servidores virtuales** y abra un servidor virtual.
2. En **Configuración avanzada**, seleccione **Configuración de tráfico** y, a continuación, seleccione **Desactivar estado**.

Reescritura de puertos y protocolos para redirección

Los servidores virtuales y los servicios que están enlazados a ellos pueden utilizar puertos diferentes. Cuando un servicio responde a una conexión HTTP con una redirección, es posible que necesite configurar el dispositivo Citrix ADC para modificar el puerto y el protocolo para asegurarse de que la redirección se realiza correctamente. Para ello, habilita y configura la opción RedirectPortRewrite.

Para configurar la redirección HTTP en un servidor virtual mediante la CLI

En el símbolo del sistema, escriba:

```
set cs vserver \<name\> -redirectPortRewrite \<Value\>
```

Ejemplo

```
1 set cs vserver Vserver-CS-1 -redirectPortRewrite enabled
2 <!--NeedCopy-->
```

Para configurar la redirección HTTP en un servidor virtual mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Cambio de contenido > Servidores virtuales** y abra un servidor virtual.
2. En **Configuración avanzada**, seleccione **Configuración de tráfico** y seleccione **Volver a escribir**.

Inserción de la dirección IP y el puerto de un servidor virtual en el encabezado de solicitud

Si tiene varios servidores virtuales que se comunican con diferentes aplicaciones en el mismo servicio, debe configurar el dispositivo Citrix ADC para que agregue la dirección IP y el número de puerto del servidor virtual apropiado a las solicitudes HTTP que se envían a ese servicio. Esta configuración permite que las aplicaciones que se ejecutan en el servicio identifiquen el servidor virtual que envió la solicitud.

Si el servidor virtual principal está inactivo y el servidor virtual de copia de seguridad está activo, los valores de configuración del servidor virtual de copia de seguridad se agregan a las solicitudes del cliente. Si quiere agregar la misma etiqueta de encabezado, independientemente de si las solicitudes proceden del servidor virtual principal o del servidor virtual de copia de seguridad, debe configurar la etiqueta de encabezado requerida en ambos servidores virtuales.

> **Nota**
>
> Esta opción no es compatible con servidores virtuales comodín o servidores virtuales ficticios.

Para insertar la dirección IP y el puerto del servidor virtual en las solicitudes del cliente mediante la CLI

En el símbolo del sistema, escriba:

```
set cs vserver \<name\> -insertVserverIPPort \<vServerIPPORT\>
```

Ejemplo

```
1 set cs vserver Vserver-CS-1 -insertVserverIPPort 10.201.25.136:80
2 <!--NeedCopy-->
```

Para insertar la dirección IP y el puerto del servidor virtual en las solicitudes del cliente mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Cambio de contenido > Servidores virtuales** y abra un servidor virtual.
2. En **Configuración avanzada**, seleccione **Configuración de tráfico**y, en la lista Inserción de puertos IP del servidor virtual, seleccione VIPADDR o V6TOV4MAPPING y especifique un encabezado de puerto en el valor de inserción de puerto IP del servidor virtual.

Establecimiento de un valor de tiempo de espera para conexiones de cliente inactivas

Puede configurar un servidor virtual para que finalice cualquier conexión de cliente inactiva después de que transcurra un período de tiempo de espera configurado. Al configurar esta configuración, el dispositivo Citrix ADC espera el tiempo especificado y, si el cliente está inactivo después de ese tiempo, cierra la conexión del cliente.

Para establecer un valor de tiempo de espera para las conexiones de cliente inactivas mediante la CLI

En el símbolo del sistema, escriba:

```
set cs vserver \<name\> -cltTimeout \<Value\>
```


Ejemplo

```
set cs vserver Vserver-CS-1 -cltTimeout 100
<!--NeedCopy-->
```

Para establecer un valor de tiempo de espera para las conexiones de cliente inactivas mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Cambio de contenido > Servidores virtuales** y abra un servidor virtual.
2. En **Configuración avanzada**, seleccione **Configuración de tráfico** y especifique un valor de Tiempo de **espera de inactividad del cliente**.

Identificación de conexiones con los parámetros de conexión de 4 tuplas y Capa 2

Ahorapuede establecer la opción L2Conn para un servidor virtual de cambio de contenido. Con la opción L2Conn establecida, las conexiones al servidor virtual de cambio de contenido se identifican mediante la combinación de los parámetros de conexión de 4 tuplas (<source IP><source port><destination IP>:::<destination port>) y Capa 2. Los parámetros de conexión de Capa 2 son la dirección MAC, el ID de VLAN y el ID de canal.

Para establecer la opción L2Conn para un servidor virtual de cambio de contenido mediante la CLI

En la línea de comandos, escriba los siguientes comandos para configurar el parámetro L2Conn para un servidor virtual de cambio de contenido y compruebe la configuración:

```
-  set cs vserver \<name\> -l2Conn (**ON** | **OFF**)
-  show cs vserver \<name\>
```

Ejemplo

```
> set cs vserver mycsvserver -l2Conn ON
Done
> show cs vserver mycsvserver
     mycsvserver (192.0.2.56:80) - HTTP   Type: CONTENT
```



```
5       State: UP
6           . . .
7           . . .
8       L2Conn: ON Case Sensitivity: ON
9           . . .
10          . . .
11  Done
12  >
13  <!--NeedCopy-->
```

Para establecer la opción L2Conn para un servidor virtual de cambio de contenido mediante la GUI

1. Vaya a **Administración del tráfico > Cambio de contenido > Servidores virtuales** y abra un servidor virtual.
2. En **Configuración avanzada**, seleccione **Configuración de tráfico** y, a continuación, seleccione **Parámetros de capa 2**.

Compatibilidad con persistencia para el servidor virtual de cambio de contenido

August 20, 2021

Las aplicaciones están pasando de arquitecturas monolíticas a arquitecturas de microservicios. Diferentes versiones de la misma aplicación pueden coexistir en la arquitectura de microservicios. El dispositivo Citrix ADC debe admitir la implementación continua de aplicaciones. Se logra mediante plataformas que realizan implementaciones Canary (como Spinnaker). En una configuración de implementación continua, una versión más reciente de una aplicación se implementa automáticamente y se expone al tráfico del cliente en etapas hasta que la aplicación se mantiene estable para tomar tráfico completo. Además, debe haber servicios ininterrumpidos para el cliente.

La función de cambio de contenido Citrix ADC permite a Citrix ADC el dispositivo distribuir solicitudes de cliente entre varios servidores virtuales de equilibrio de carga en función de las directivas vinculadas al servidor virtual de cambio de contenido.

Para implementaciones continuas, la cambio de contenido se utiliza para seleccionar el servidor virtual de equilibrio de carga que sirve varias versiones de una aplicación.

En la cambio de contenido, la selección de un servidor virtual de equilibrio de carga para una versión de aplicación específica cambia en tiempo de ejecución debido al cambio en las directivas de cambio de contenido. Durante esta transición, si algunas sesiones están presentes con versiones anteriores

de la aplicación, dicho tráfico debe seguir siendo servido únicamente por versiones anteriores. Para admitir este requisito, el dispositivo Citrix ADC mantiene la persistencia en varios grupos de equilibrio de carga detrás de un servidor virtual de cambio de contenido. La persistencia del servidor virtual de cambio de contenido permite una transición fluida de los clientes de una versión a otra.

Tipos de persistencia admitidos en el servidor virtual de cambio de contenido

Los siguientes tipos de persistencia se admiten en servidores virtuales de cambio de contenido.

Tipo de persistencia	Descripción
IP de origen	**SOURCEIP**. Las conexiones desde la misma dirección IP del cliente forman parte de la misma sesión de persistencia. Para obtener más detalles, vea Persistencia de la dirección IP de origen.
Cookie HTTP	**COOKIEINSERT**. Las conexiones que tienen el mismo encabezado HTTP Cookie son partes de la misma sesión de persistencia. El formato de la cookie que inserta el dispositivo Citrix ADC es: **NSC_ <vid_str of CSvserver> = <vid_str of Lbvserver> donde NSC_XXXX es el identificador del servidor virtual derivado del nombre del servidor virtual. Para obtener más información, consulte Persistencia de cookies HTTP.
ID de sesión SSL	**SSLSESSION**. Las conexiones que tienen el mismo ID de sesión SSL son parte de la misma sesión de persistencia. Para obtener más detalles, vea Persistencia de ID de sesión SSL.

Puede configurar un valor de tiempo de espera para la persistencia basado en cookies HTTP. Si establece el valor de tiempo de espera en 0, el dispositivo ADC no especifica el tiempo de caducidad, independientemente de la versión de la cookie HTTP utilizada. El tiempo de caducidad depende entonces del software cliente, y tales cookies son válidas solo si el software se está ejecutando.

Dependiendo del tipo de persistencia que haya configurado, el servidor virtual puede admitir 250.000 conexiones persistentes simultáneas o cualquier número de conexiones persistentes hasta los límites impuestos por la cantidad de memoria del dispositivo Citrix ADC. La siguiente tabla muestra qué tipos de persistencia pertenecen a cada categoría.

Tipo de persistencia	Número de conexiones persistentes simultáneas admitidas
IP de origen, ID de sesión SSL	250000
Cookie HTTP	Límite de memoria. En CookieInsert, si el tiempo de espera no es 0, el número de conexiones está limitado por la memoria.

Algunos tipos de persistencia son específicos de determinados tipos de servidor virtual. La tabla siguiente muestra cada tipo de persistencia e indica qué tipos de persistencia se admiten en qué tipos de servidor virtual.

Tipo de persistencia	HTTP	HTTPS	TCP	UDP/IP	Puente SSL_Bridge	SSL_TCP	RTSP	SIP_UDP
SOURCEI	Sí	Sí	Sí	Sí	Sí	Sí	No	No
COOKIEINSERT	Sí	Sí	No	No	No	No	No	No
SSLSESSI	No	Sí	No	No	Sí	Sí	No	No

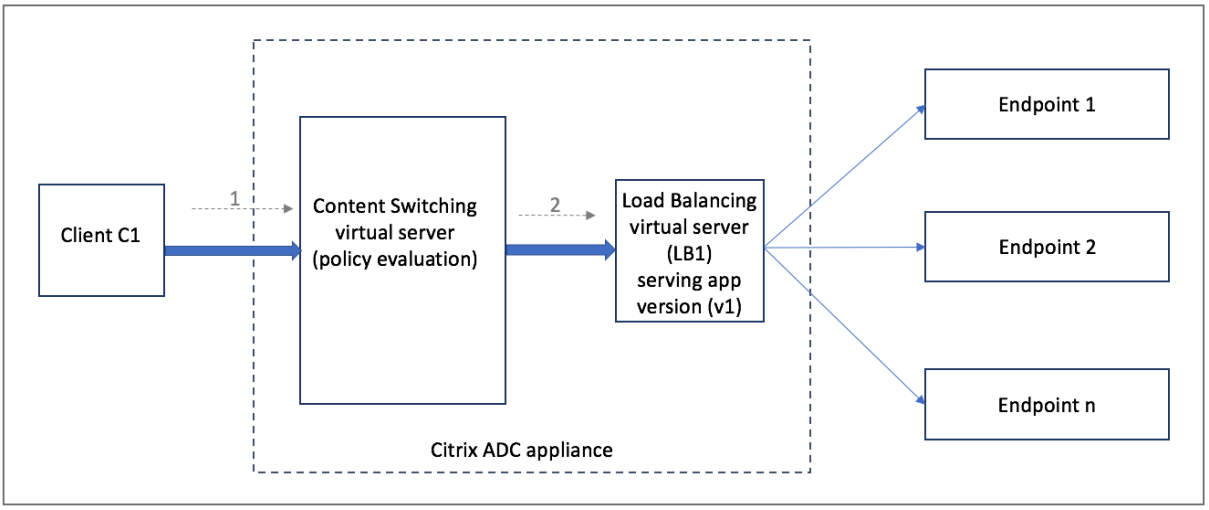
Compatibilidad con persistencia de copias de seguridad

Puede configurar el servidor virtual de cambio de contenido para que utilice el tipo de persistencia IP de origen como tipo de persistencia de copia de seguridad cuando falla el tipo de persistencia de cookies. Es útil para implementaciones Canary en la arquitectura de microservicios.
Cuando se produce un error en el tipo de persistencia de cookies, el dispositivo vuelve a la persistencia basada en IP de origen solo cuando el explorador cliente no devuelve ninguna cookie en la solicitud. Sin embargo, si el explorador devuelve una cookie (no necesariamente la cookie de persistencia), se supone que el explorador admite cookies y, por lo tanto, la persistencia de la copia de seguridad no se activa.También
puede establecer un valor de tiempo de espera para la persistencia de la copia de seguridad. Tiempo de espera es el período de tiempo para el que está en vigor una sesión de persistencia.

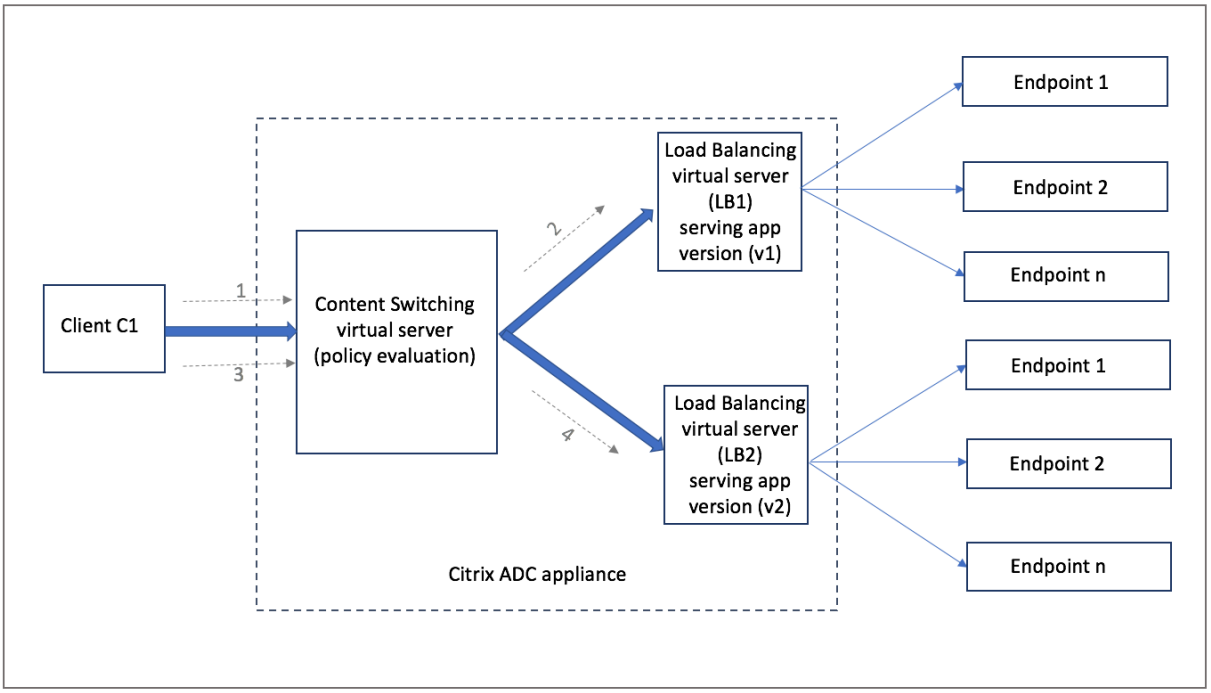
Cómo funciona la persistencia en el cambio de contenido del servidor virtual

Caso 1: Un servidor virtual de cambio de contenido sin persistencia

El siguiente ejemplo ilustra la implementación de varias versiones de una aplicación con un servidor virtual de cambio de contenido sin persistencia.



Cuando el cliente C1 envía una solicitud a la aplicación, la solicitud se envía al servidor virtual de cambio de contenido en el dispositivo Citrix ADC. El servidor virtual de cambio de contenido evalúa la directiva y reenvía la solicitud al servidor virtual de equilibrio de carga (LB1) que está sirviendo la versión v1 de la aplicación.



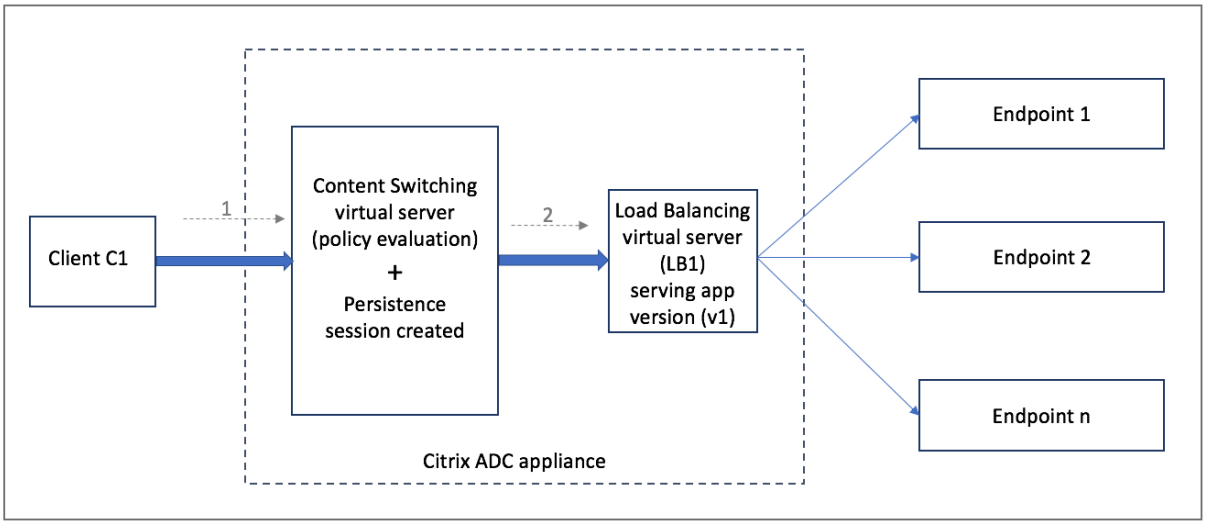
Considere una nueva versión v2 de la aplicación está implementada y tiene que estar expuesta a un subconjunto de usuarios. El nuevo servidor virtual de equilibrio de carga (LB2) que sirve la versión v2 está vinculado al servidor virtual de cambio de contenido mediante la directiva de cambio de contenido adecuada.

Cuando el cliente C1 envía una nueva solicitud, la directiva se evalúa de nuevo y la solicitud se reenvía al servidor virtual de equilibrio de carga LB2. Por lo tanto, las transacciones para aplicaciones con

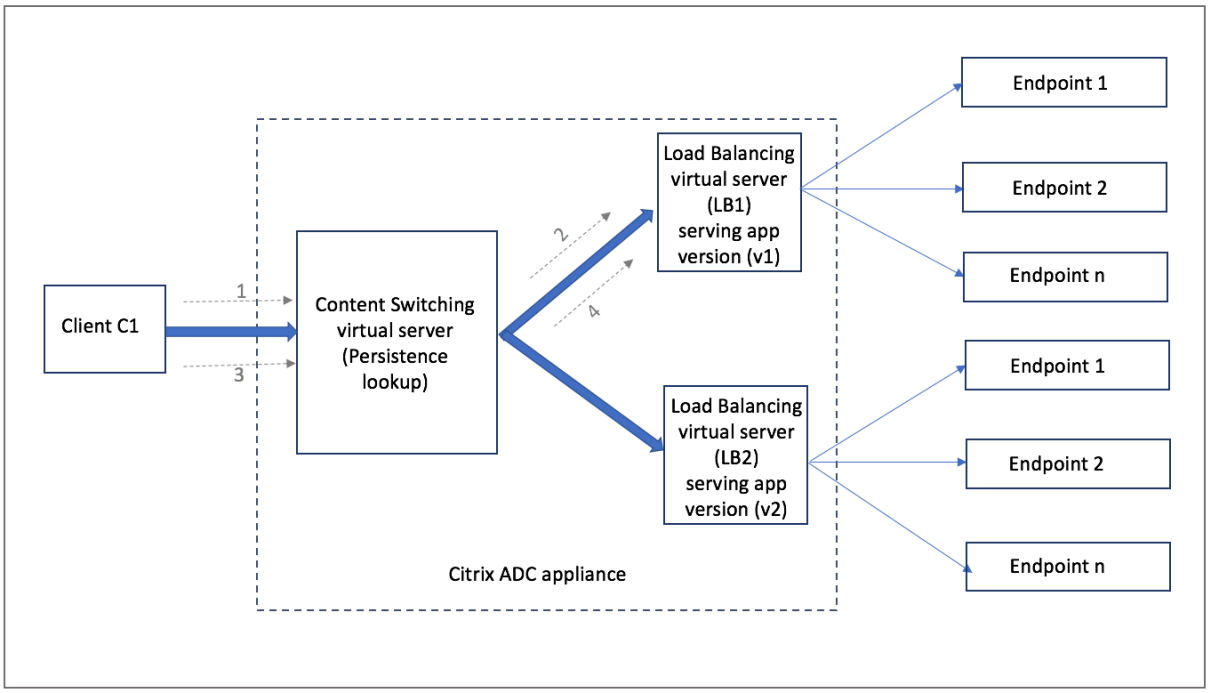
estado fallan si se implementan varias versiones de la aplicación.

Caso 2: Content switching server virtual con persistencia

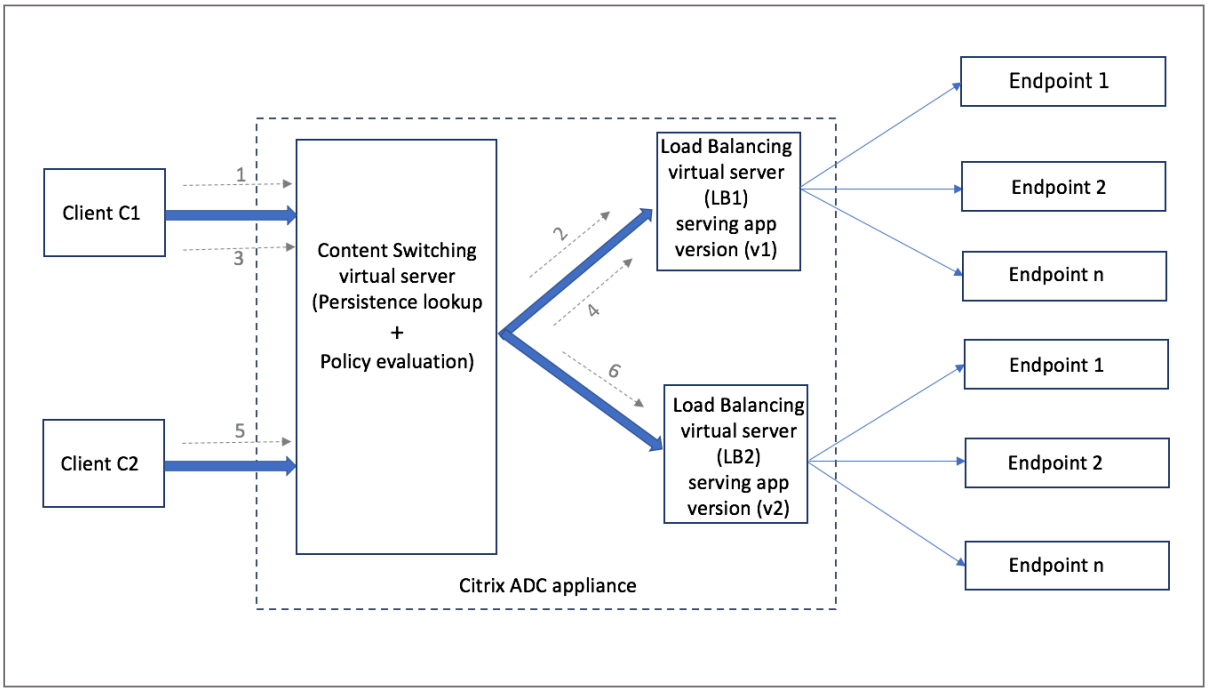
El siguiente ejemplo ilustra la implementación de varias versiones de la aplicación con un servidor virtual de cambio de contenido con persistencia.



Cuando el cliente C1 envía una solicitud a la aplicación, la solicitud se envía al servidor virtual de cambio de contenido en el dispositivo Citrix ADC. El servidor virtual de cambio de contenido evalúa la directiva, crea una entrada de sesión de persistencia y reenvía la solicitud al servidor virtual de equilibrio de carga LB1 que sirve la versión v1 de la aplicación.



El mismo cliente C1 vuelve a solicitar la aplicación y la solicitud se envía al servidor virtual de cambio de contenido en el dispositivo Citrix ADC. Se realiza una búsqueda para la sesión de persistencia y el servidor virtual de equilibrio de carga LB1 se toma de la sesión de persistencia existente y la solicitud se reenvía a LB1. No se produce ninguna rotura de la transacción existente con esta solución; por lo tanto, se mantiene la naturaleza de estado de la aplicación.



Consideremos un nuevo cliente C2. La nueva solicitud C2 se envía a la versión más reciente de la aplicación a través de la evaluación de directivas, ya que no hay ninguna sesión de persistencia existente para este cliente. Resulta en una implementación correcta de la versión más reciente de la aplicación sin romper su estado.

Debido al soporte de persistencia, los clientes pueden implementar múltiples contenidos o diferentes versiones de la aplicación sin afectar las transacciones existentes, específicamente para aplicaciones con estado. No es posible sin persistencia en la imagen.

Configurar el tipo de persistencia en el servidor virtual de cambio de contenido mediante la CLI

En el símbolo del sistema, escriba:

```
set cs vserver <name> -PersistenceType <type> [-timeout <integer>]
<!--NeedCopy-->
```

Ejemplo:


```
set cs vserver Vserver-CS-1 -persistenceType SOURCEIP -timeout 60
<!--NeedCopy-->
```

Configurar el tipo de persistencia en el servidor virtual de cambio de contenido mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico** > **Cambio de contenido** > **Servidores virtuales** y haga clic en **Agregar**.
2. En **Configuración básica**, configure los detalles de persistencia.

Solucionar problemas

August 20, 2021

Si la función de cambio de contenido no funciona como se esperaba después de configurarla, puede utilizar algunas herramientas comunes para acceder a los recursos de Citrix ADC y diagnosticar el problema.

Recursos para solucionar problemas de cambio de contenido

Para obtener los mejores resultados, utilice los siguientes recursos para solucionar un problema de cambio de contenido en un dispositivo Citrix ADC:

- Archivo de configuración
- `newnslog` Archivo relevante
- Archivos de seguimiento
- Diagrama de topología de red para la configuración de red del cliente
- Documentación de Citrix, como notas de la versión, artículos de Knowledge Center y documentación del producto.

Además de los recursos anteriores, las siguientes herramientas agilizan la solución de problemas:

- El `iehttpheaders` o una utilidad similar
- La aplicación Wireshark personalizada para los archivos de seguimiento Citrix ADC
- Una utilidad SSH para el acceso a la línea de comandos
- Una utilidad HyperTerminal para acceder a la consola

Solución de problemas de cambio de contenido

Los problemas más comunes de cambio de contenido implican que la función de cambio de contenido no funciona en absoluto, o que solo funciona de forma intermitente, y respuestas de servicio no disponible.

- **Problema**

  La función de cambio de contenido no funciona.

  Resolución

  Compruebe la configuración de la siguiente manera:

  - Compruebe que el dispositivo tiene licencia para la cambio de contenido.
  - Compruebe que la función está habilitada.
  - En el archivo de configuración, compruebe que las directivas de cambio de contenido válidas estén correctamente enlazadas a los servidores virtuales de equilibrio de carga.

- **Problema**

  El cliente recibe una respuesta 503: Servicio no disponible.

  Resolución

  - Verifique las direcciones URL y los enlaces de directivas. El cliente recibe la respuesta 503 cuando no se evalúa ninguna de las directivas configuradas y no se define ningún servidor virtual de equilibrio de carga predeterminado y se vincula al servidor virtual de cambio de contenido.
  - Desde la configuración, compruebe las directivas y el cliente tiene acceso a la URL.
  - Verifique que para cada tipo de solicitud se evalúe la directiva respectiva. Si la directiva no se evalúa, compruebe la expresión de directiva y actualícela si es necesario.
  - Verifique los encabezados de solicitud y respuesta de URL y HTTP. Para ello, registre un rastro `HTTPHeader` y, si es necesario, registre los rastros de paquetes en el dispositivo y en el cliente.

- **Problema**

  Intermitentemente, la función de cambio de contenido no funciona como se esperaba.

  Resolución

  - Estudie el diagrama de topología de red, si está disponible, de la configuración para comprender los diversos dispositivos instalados entre el cliente y los servidores.
  - Verifique la configuración y los enlaces de directivas. Asegúrese de que la dirección URL de la expresión de directiva coincide con la de la solicitud del cliente.
  - Compruebe que se asignan las prioridades adecuadas a las directivas. Una prioridad o prioridad incorrecta asignada a una directiva puede causar un problema.

- Ejecute los siguientes comandos para verificar los enlaces y los valores de los contadores de selección de directivas en la salida de los comandos:

  ```
  show cs vserver \<CS VServer\>

  show cs policy \<CS Policy\>

  stat cs vserver \<CS VServer\>
  ```

- Mediante `iehttpheaders` o una utilidad similar, determine si los encabezados HTTP para las solicitudes o respuestas proporcionan algún puntero al problema.
- Consulte las notas de la versión y los artículos del Centro de conocimiento.
- Si el problema aún no se ha resuelto, póngase en contacto con el servicio de asistencia técnica de Citrix con los datos adecuados para una investigación más detallada.

DataStream

August 20, 2021

La función Citrix ADC DataStream proporciona un mecanismo inteligente para la conmutación de solicitudes en la capa de base de datos mediante la distribución de solicitudes en función de la consulta SQL que se envía.

Cuando se implementa frente a servidores de bases de datos, un dispositivo Citrix ADC garantiza una distribución óptima del tráfico desde los servidores de aplicaciones y los servidores web. Los administradores pueden segmentar el tráfico según la información de la consulta SQL y en función de los nombres de base de datos, nombres de usuario, juegos de caracteres y tamaño de paquete.

Puede configurar el equilibrio de carga para cambiar solicitudes basándose en algoritmos de equilibrio de carga. Alternativamente, puede elaborar los criterios de conmutación configurando el cambio de contenido para tomar una decisión basada en un parámetro de consulta SQL. Puede configurar monitores para realizar un seguimiento del estado de los servidores de bases de datos.

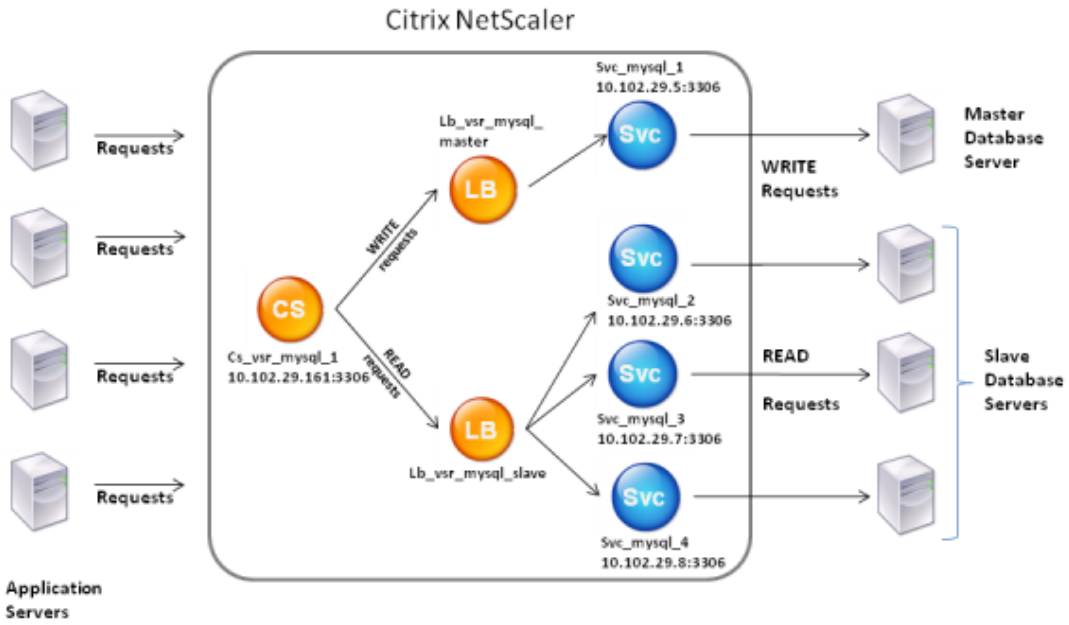
> **Nota**
>
> Citrix ADC DataStream solo es compatible con bases de datos MySQL y MS SQL. Para obtener información acerca de la versión del protocolo, los conjuntos de caracteres, las consultas especiales y las transacciones compatibles, consulte Referencia de DataStream.

Cómo funciona DataStream

En DataStream, el dispositivo ADC se coloca en línea entre la aplicación o los servidores Web y los servidores de base de datos. En el dispositivo, los servidores de base de datos están representados por servicios.

Una implementación típica de DataStream consta de las entidades descritas en el diagrama siguiente.

Ilustración 1. Modelo de entidad DataStream



Como se muestra en esta ilustración, una configuración de DataStream puede consistir en:

- Un servidor virtual opcional de cambio de contenido (CS).
- Configuración de equilibrio de carga que consiste en servidores virtuales de equilibrio de carga (LB1 y LB2).
- Servicios (Svc1, Svc2, Svc3 y Svc4).
- Directivas de cambio de contenido (opcional).

Los clientes (servidores web o aplicaciones) envían solicitudes a la dirección IP de un servidor virtual de cambio de contenido (CS) configurado en el dispositivo Citrix ADC. A continuación, el dispositivo autentica los clientes mediante las credenciales de usuario de la base de datos configuradas en el dispositivo. El servidor virtual de cambio de contenido (CS) aplica las directivas de cambio de contenido asociadas a las solicitudes. Después de evaluar las directivas, el servidor virtual de cambio de contenido (CS) enruta las solicitudes al servidor virtual de equilibrio de carga apropiado (LB1 o LB2). A continuación, el servidor virtual de equilibrio de carga distribuye las solicitudes a los servidores de base de datos apropiados (representados por los servicios del dispositivo) en función del algoritmo de equilibrio de carga. El dispositivo Citrix ADC utiliza las mismas credenciales de usuario de base de

datos para autenticar la conexión con el servidor de base de datos.

Si un servidor virtual de cambio de contenido no está configurado en el dispositivo, los clientes (servidores de aplicaciones o servidores Web) envían sus solicitudes a un servidor virtual de equilibrio de carga configurado en el dispositivo. El dispositivo Citrix ADC autentica el cliente mediante las credenciales de usuario de la base de datos configuradas en el dispositivo y, a continuación, utiliza las mismas credenciales para autenticar la conexión con el servidor de base de datos. El servidor virtual de equilibrio de carga distribuye las solicitudes a los servidores de base de datos según el algoritmo de equilibrio de carga. El algoritmo de equilibrio de carga más efectivo para el cambio de base de datos es el método de conexión menos.

DataStream utiliza la multiplexación de conexión para permitir que se realicen varias solicitudes del lado del cliente a través de la misma conexión del lado del servidor. Se consideran las siguientes propiedades de conexión:

- Nombre de usuario
- Database name
- Tamaño del paquete
- Juego de caracteres

Configurar usuarios de la base de datos

August 20, 2021

En las bases de datos, una conexión siempre tiene estado, lo que significa que cuando se establece una conexión, debe autenticarse.

Configure el nombre de usuario y la contraseña de la base de datos en el dispositivo NetScaler. Por ejemplo, si tiene un usuario John configurado en la base de datos, también debe configurar el usuario John en el ADC. Agregar nombres de usuario y contraseñas de base de datos en el ADC los agrega al `nsconfig` archivo.

> **Nota**
>
> Los nombres distinguen entre mayúsculas y minúsculas.

El ADC utiliza estas credenciales de usuario para autenticar los clientes y, a continuación, autenticar las conexiones del servidor con los servidores de base de datos.

Agregar un usuario de base de datos mediante la CLI

En el símbolo del sistema, escriba:

```
add db user <username> - password <password>
```


Ejemplo:

```
add db user nsdbuser -password dd260427edf
<!--NeedCopy-->
```

Agregar un usuario de base de datos mediante la GUI

Vaya a **Sistema > Administración de usuarios > Usuarios de base de datos** y configure un usuario de base de datos.

Si ha cambiado la contraseña del usuario de base de datos en el servidor de base de datos, debe restablecer la contraseña del usuario correspondiente configurado en el dispositivo ADC.

Restablecer la contraseña de un usuario de base de datos mediante la CLI

En el símbolo del sistema, escriba:

```
set db user <username> -password <password>
<!--NeedCopy-->
```

Ejemplo:

```
set db user nsdbuser -password dd260538abs
<!--NeedCopy-->
```

Restablecer la contraseña de los usuarios de la base de datos mediante la GUI

Vaya a **Sistema > Administración de usuarios > Usuarios de base**de datos, seleccione un usuario e introduzca nuevos valores para la contraseña.

Si ya no existe un usuario de base de datos en el servidor de base de datos, puede quitarlo del dispositivo ADC. Sin embargo, si el usuario sigue existiendo en el servidor de base de datos y se quita el usuario del dispositivo ADC, cualquier solicitud del cliente con este nombre de usuario no se autenticará. Como resultado, la solicitud no se enruta al servidor de base de datos.

Eliminar un usuario de base de datos mediante la CLI

En el símbolo del sistema, escriba:


```
rm db user <username>
<!--NeedCopy-->
```

Ejemplo:

```
rm db user nsdbuser
<!--NeedCopy-->
```

Eliminar un usuario de base de datos mediante la GUI

Vaya a **Sistema > Administración de usuarios > Usuarios de base**de datos, seleccione un usuario y haga clic en **Eliminar**.

Configurar un perfil de base de datos

February 16, 2021

Un perfil de base de datos es una colección con nombre de parámetros que se configura una vez pero que se aplica a varios servidores virtuales que requieren esos parámetros específicos. Después de crear un perfil de base de datos, se vincula al equilibrio de carga o al cambio de contenido de servidores virtuales. Puede crear tantos perfiles como necesite.

Crear un perfil de base de datos mediante la CLI

En la línea de comandos, escriba los siguientes comandos para crear un perfil de base de datos y verificar la configuración:

```
add db dbProfile <name> [-interpretQuery ( YES | NO )] [-stickiness (
    YES | NO )] [-kcdAccount <string>]

show db dbProfile
<!--NeedCopy-->
```

Ejemplo:


```
> add dbProfile myDBProfile -interpretQuery YES -stickiness YES -
   kcdAccount mykcdaccnt
 Done
> show dbProfile myDBProfile
    Name: myDBProfile
    Interpret Query: YES
    Stickyness: YES
    KCD Account: mykcdaccnt
    Reference count: 0

 Done
>
<!--NeedCopy-->
```

Crear un perfil de base de datos mediante la GUI

Desplácese hasta **Sistema > Perfiles** y, en la ficha **Perfiles de base** de datos, configure un perfil de base de datos.

Enlazar un perfil de base de datos a un servidor virtual de equilibrio de carga o cambio de contenido mediante la CLI

En la línea de comandos, escriba:

```
set (lb | cs) vserver <name> -dbProfileName <string>
<!--NeedCopy-->
```

Enlazar un perfil de base de datos a un servidor virtual de equilibrio de carga o cambio de contenido mediante la GUI

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales o Administración del tráfico > Content Switching > Servidores virtuales** y abra un servidor virtual.
2. En **Configuración avanzada**, seleccione **Perfiles** y, en la lista **Perfil de base**de datos, seleccione un perfil para enlazar al servidor virtual. Para crear un perfil, haga clic en más (+).

Configurar el equilibrio de carga para DataStream

August 20, 2021

Antes de configurar una configuración de equilibrio de carga, debe habilitar la función de equilibrio de carga. A continuación, comience creando al menos un servicio para cada servidor de base de datos en el grupo de equilibrio de carga. Con los servicios configurados, está listo para crear un servidor virtual de equilibrio de carga y enlazar los servicios con el servidor virtual.

> **Nota**:
>
> Para las bases de datos, el equilibrio de carga solo puede producirse en servidores de bases de datos homogéneos (servidores de bases de datos que contienen exactamente las mismas bases de datos). Para una configuración que contenga bases de datos únicas en servidores diferentes, debe utilizar la cambio de contenido. Si algunos de los servidores de base de datos alojan contenido idéntico, solo puede utilizar el equilibrio de carga en esos servidores. A continuación, puede utilizar directivas de cambio de contenido para enviar solicitudes al servidor virtual de equilibrio de carga que administra el equilibrio de carga para esas bases de datos.
>
> El dispositivo Citrix ADC almacena actualmente el nombre de la base de datos y la información de inicio de sesión durante la sesión de la base de datos. Cuando se realiza una consulta a la base de datos, utiliza esa información para conectarse al servidor de base de datos específico.

Valores de parámetros específicos de DataStream

- Protocolo

  Utilice el tipo de protocolo MYSQL para bases de datos MySQL y el tipo de protocolo MSSQL para bases de datos MS SQL mientras configura servidores y servicios virtuales. Los protocolos MySQL y TDS son utilizados por los clientes para comunicarse con los respectivos servidores de bases de datos mediante consultas SQL. Para obtener información sobre el protocolo MySQL, consulte http://dev.mysql.com/doc/internals/en/client-server-protocol.html. Para obtener información sobre el protocolo TDS, consulte http://msdn.microsoft.com/en-us/library/dd304523(v=prot.13).aspx.

- Port

  Puerto en el que el servidor virtual escucha las conexiones de cliente. Utilice el puerto 3306 para servidores de bases de datos MySQL.

- Método

  Se recomienda utilizar el método Least Connection para equilibrar mejor la carga y reducir la carga del servidor. Sin embargo, también se admiten otros métodos, como Round Robin, Menos tiempo de respuesta, Hash IP de origen, Hash IP de destino de origen, Menos ancho de banda, Menos paquetes y Hash del puerto de origen IP de origen.

  Nota: El método Hash de URL no es compatible con DataStream.

- Versión de MS SQL Server

Si utiliza Microsoft SQL Server y espera que algunos clientes ejecuten una versión diferente de su producto de Microsoft SQL Server, establezca el parámetro Versión del servidor para el servidor virtual de equilibrio de carga. La configuración de la versión proporciona compatibilidad entre las conexiones del lado del cliente y del lado del servidor al asegurarse de que todas las comunicaciones se ajustan a la versión del servidor. Para obtener más información sobre la configuración del parámetro Versión del servidor, consulte Configuración de la configuración de la versión del servidor MySQL y Microsoft SQL.

- Versión de MySQL Server

  Si está usando MySQL Server y espera que algunos clientes ejecuten una versión diferente de su producto MySQL Server, establezca el parámetro Versión del servidor para el servidor virtual de equilibrio de carga. La configuración de la versión proporciona compatibilidad entre las conexiones del lado del cliente y del lado del servidor al asegurarse de que todas las comunicaciones se ajustan a la versión del servidor. Para obtener más información sobre la configuración del parámetro Versión del servidor, consulte Configuración de la configuración de la versión del servidor MySQL y Microsoft SQL.

Configurar la conmutación de contenido para DataStream

October 5, 2021

Puede segmentar el tráfico según la información de la consulta SQL, en función de los nombres de base de datos, nombres de usuario, juegos de caracteres y tamaño de paquete.

Puede configurar directivas de conmutación de contenido con expresiones de directivas avanzadas para cambiar el contenido en función de las propiedades de conexión. Por ejemplo, nombre de usuario y nombre de base de datos, parámetros de comando y consulta SQL para seleccionar el servidor.

Las expresiones de directivas avanzadas evalúan el tráfico asociado a los servidores de bases de datos MYSQL y MS SQL. Utilice expresiones basadas en solicitudes en directivas avanzadas para tomar decisiones de conmutación de solicitudes en el punto de enlace del servidor virtual de conmutación de contenido. Utilice expresiones basadas en respuesta (expresiones que comienzan con MYSQL.RES) para evaluar las respuestas del servidor a monitores de mantenimiento configurados por el usuario.

Para obtener información sobre las expresiones de directivas avanzadas, consulte Expresiones de directivas avanzadas: DataStream.

> **Nota:**
>
> En el caso de las bases de datos, el equilibrio de carga solo puede producirse en servidores de bases de datos homogéneos (servidores de bases de datos que contienen exactamente las mis-

> mas bases de datos). Para una configuración que contiene bases de datos únicas en distintos servidores, debe utilizar el cambio de contenido. Si algunos de los servidores de base de datos alojan contenido idéntico, puede utilizar el equilibrio de carga solo en esos servidores. A continuación, puede utilizar directivas de conmutación de contenido para enviar solicitudes al servidor virtual de equilibrio de carga que administra el equilibrio de carga de esas bases de datos.
>
> El dispositivo Citrix ADC almacena actualmente el nombre de la base de datos y la información de inicio de sesión durante la sesión de base de datos. Cuando se realiza una consulta en la base de datos, utiliza esa información para conectarse al servidor de base de datos específico.

Valores de parámetros específicos de DataStream

- Protocolo

  Utilice el tipo de protocolo MYSQL para las bases de datos MySQL y el tipo de protocolo MSSQL para las bases de datos MS SQL mientras configura los servidores y servicios virtuales. Los clientes utilizan los protocolos MySQL y TDS para comunicarse con los servidores de base de datos respectivos mediante consultas SQL. Para obtener información sobre el protocolo MySQL, consulte http://dev.mysql.com/doc/internals/en/client-server-protocol.html. Para obtener información sobre el protocolo TDS, consulte http://msdn.microsoft.com/en-us/library/dd304523(v=prot.13).aspx.

- Port

  Puerto en el que el servidor virtual escucha las conexiones del cliente. Utilice el puerto 3306 para los servidores de bases de datos MySQL.

- Versión de MS SQL Server

  Si utiliza Microsoft SQL Server y espera que algunos clientes ejecuten una versión diferente de su producto Microsoft SQL Server, establezca el parámetro Versión del servidor para el servidor virtual de conmutación de contenido. La configuración de la versión proporciona compatibilidad entre las conexiones del lado del cliente y del lado del servidor al asegurarse de que todas las comunicaciones se ajustan a la versión del servidor. Para obtener más información sobre la configuración del parámetro Versión del servidor, consulte Configuración de la configuración de versión de Microsoft SQL Server.

Configurar monitores para DataStream

August 20, 2021

Para realizar un seguimiento del estado de cada servidor de base de datos con equilibrio de carga en tiempo real, debe vincular un monitor a cada servicio. El monitor está configurado para probar el

servicio enviando sondas periódicas al servicio, a veces denominado realizar una comprobación de estado. Si el monitor recibe una respuesta oportuna a sus sondas, marca el servicio como UP. Si no recibe una respuesta oportuna al número designado de sondeos, marca el servicio como DOWN.

Para DataStream, debe usar los monitores integrados: MYSQL-ECV y MSSQL-ECV. Mediante este monitor puede enviar una solicitud SQL y analizar la respuesta para una cadena.

Antes de configurar monitores para DataStream, debe agregar credenciales de usuario de base de datos al dispositivo NetScaler. Para obtener información sobre la configuración de monitores, consulte Configurar monitores en una configuración de equilibrio de carga.

Al crear un monitor, se establece una conexión TCP con el servidor de base de datos y la conexión se autentica mediante el nombre de usuario proporcionado al crear el monitor. A continuación, puede ejecutar una consulta SQL en el servidor de base de datos y evaluar la respuesta del servidor para comprobar si coincide con la regla configurada.

Los siguientes ejemplos son para servidores MYSQL.

Ejemplos:

En el ejemplo siguiente, se evalúa el valor del mensaje de error para determinar el estado del servidor.

```
1 add lb monitor lb_mon1 MYSQL-ECV -sqlQuery ”select * from
2 table2;” -evalrule ”mysql.res.error.message.contains(”Invalid
3 User”)”-database ”NS” -userName ”user1”
4 <!--NeedCopy-->
```

En el siguiente ejemplo, se evalúa el número de filas de la respuesta para determinar el estado del servidor.

```
1 add lb monitor lb_mon4 MYSQL-ECV -sqlQuery ”select * from
2 table4;” -evalrule ”mysql.res.atleast_rows_count(7)” -database ”NS” -
     userName ”user2”
3 <!--NeedCopy-->
```

En el ejemplo siguiente, se evalúa el valor de una columna determinada para determinar el estado del servidor.

```
1 add lb monitor lb_mon3 MYSQL-ECV
2 -sqlQuery ”select * from ABC;” -evalrule ”mysql.res.row(1).double_elem
     (2) == 345.12”
3 -database ”NS” -userName ”user3”
```



```
<!--NeedCopy-->
```

Los siguientes ejemplos son para servidores MSSQL.

Ejemplos:

En el ejemplo siguiente, se evalúa el valor del mensaje de error para determinar el estado del servidor.

```
add lb monitor lb_mon1 MSSQL-ECV -sqlQuery "select * from
table2;" -evalrule "mssql.res.error.message.contains("Invalid
User")"-database "NS" -userName "user1"
<!--NeedCopy-->
```

En el siguiente ejemplo, se evalúa el número de filas de la respuesta para determinar el estado del servidor.

```
add lb monitor lb_mon4 MSSQL-ECV -sqlQuery "select * from
table4;" -evalrule "mssql.res.atleast_rows_count(7)" -database "NS" -
   userName "user2"
<!--NeedCopy-->
```

En el ejemplo siguiente, se evalúa el valor de una columna determinada para determinar el estado del servidor.

```
add lb monitor lb_mon3 MSSQL-ECV
-sqlQuery "select * from ABC;" -evalrule "mssql.res.row(1).double_elem
   (2) == 345.12"
-database "NS" -userName "user3"
<!--NeedCopy-->
```

Caso de uso 1: Configurar DataStream para una arquitectura de base de datos primaria/secundaria

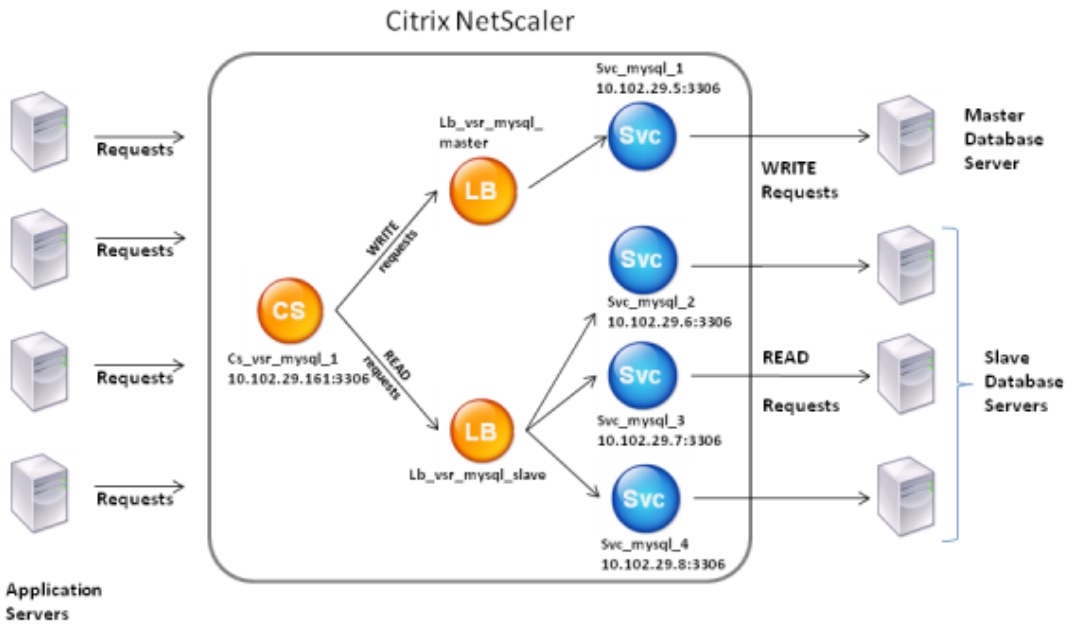
April 21, 2022

Un caso de implementación de uso común es la arquitectura de base de datos primaria/secundaria en la que la base de datos principal replica toda la información en las bases de datos secundarias.

Para la arquitectura de base de datos primaria/secundaria, es posible que desee que todas las solicitudes WRITE se envíen a la base de datos principal y todas las solicitudes READ a las bases de

En la siguiente ilustración se muestran las entidades y los valores de los parámetros que debe configurar en el dispositivo.

Ilustración 1. Modelo de entidad DataStream para configuración de base de datos primaria/secundaria



En este caso de ejemplo, se crea un servicio (SVC_MySQL_1) para representar la base de datos principal y se enlaza a un servidor virtual de equilibrio de carga (LB_vsr_mysql_primary). Se crean tres servicios más (SVC_Mysql_2, SVC_Mysql_3 y SVC_Mysql_4) para representar las tres bases de datos secundarias y se enlazan a otro servidor virtual de equilibrio de carga (LB_vsr_mysql_secondary).

Se configura un servidor virtual de conmutación de contenido (CS_VSR_MySQL_1) con directivas asociadas para enviar todas las solicitudes WRITE al servidor virtual de equilibrio de carga, LB_vsr_mysql_primary. Todas las solicitudes READ se envían al servidor virtual de equilibrio de carga, LB_VSR_Mysql_secondary.

Cuando una solicitud llega al servidor virtual de conmutación de contenido, el servidor virtual aplica las directivas de conmutación de contenido asociadas a esa solicitud. Después de evaluar las directivas, el servidor virtual de conmutación de contenido enruta la solicitud al servidor virtual de equilibrio

de carga apropiado, que la envía al servicio apropiado.

En la siguiente tabla se enumeran los nombres y valores de las entidades y la directiva configurada en el dispositivo Citrix ADC.

Tipo de entidad	Nombre	Dirección IP	Protocolo	Port	Expresión
Servicios	svc_mysql_1	198.51.100.5	MYSQL	3306	NA
	svc_mysql_2	198.51.100.6	MYSQL	3306	NA
	svc_mysql_3	198.51.100.7	MYSQL	3306	NA
	svc_mysql_4	198.51.100.8	MYSQL	3306	NA
Supervisar	lb_mon1	NA	MYSQL-ECV	NA	mysql.res.atleast_rows_cou (1)
Servidores virtuales de equilibrio de carga	lb_vsr_mysql_primary	198.51.100.201	MYSQL	3306	NA
	lb_vsr_mysql_s	198.51.100.202	MYSQL	3306	NA
Servidor virtual de conmutación de contenido	cs_vsr_mysql_1	198.51.100.161	MYSQL	3306	NA
Directiva de cambio de contenido	CS_select	NA	NA	NA	`MYSQL.REQ.QUERY.COMMAND.contains("select")`

Tabla 1. Nombres y valores de entidades y directivas

Para configurar DataStream para una configuración de base de datos primaria/secundaria mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
1 add db user user1 -password user1
2
```



```
3  add service Svc_mysql_1 198.51.100.5 mysql 3306
4
5  add service Svc_mysql_2 198.51.100.6 mysql 3306
6
7  add service Svc_mysql_3 198.51.100.7 mysql 3306
8
9  add service Svc_mysql_4 198.51.100.8 mysql 3306
10
11 add lb monitor lb_mon1 MYSQL-ECV -sqlQuery "select * from table1;" -
       evalrule "mysql.res.atleast_rows_count(1)" -database "NS" -userName
        "user1"
12
13 add lb vserver Lb_vsr_mysql_primary mysql 198.51.100.201 3306
14
15 add lb vserver Lb_vsr_mysql_secondary mysql 198.51.100.202 3306
16
17 bind lb vserver Lb_vsr_mysql_primary svc_mysql_1
18
19 bind lb vserver Lb_vsr_mysql_secondary svc_mysql_2
20
21 bind lb vserver Lb_vsr_mysql_secondary svc_mysql_3
22
23 bind lb vserver Lb_vsr_mysql_secondary svc_mysql_4
24
25 add cs vserver Cs_vsr_mysql_1 mysql 198.51.100.161 3306
26
27 add cs policy Cs_select  -rule "MYSQL.REQ.QUERY.COMMAND.contains("
       select")"
28
29 bind cs vserver Cs_vsr_mysql_1 Lb_vsr_mysql_primary
30
31 bind cs vserver Cs_vsr_mysql_1 Lb_vsr_mysql_secondary  -policy
       Cs_select  -priority 10
32
33 bind service Svc_mysql_1 -monitorName lb_mon1
34
35 bind service Svc_mysql_2 -monitorName lb_mon1
36
37 bind service Svc_mysql_3 -monitorName lb_mon1
38
39 bind service Svc_mysql_4 -monitorName lb_mon1
40 <!--NeedCopy-->
```


Caso de uso 2: Configurar el método de token de equilibrio de carga para DataStream

August 20, 2021

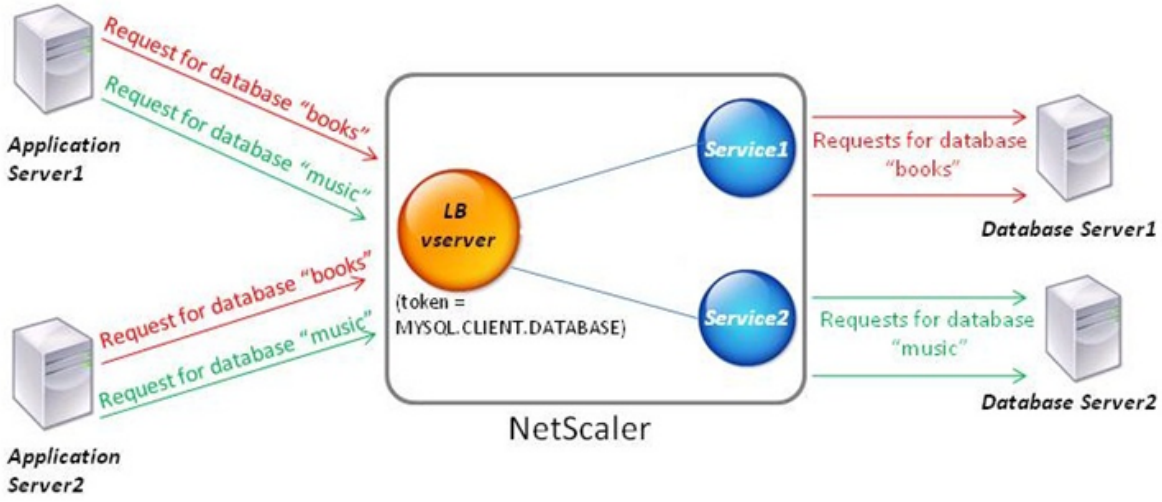
Puede configurar el método token de equilibrio de carga para DataStream para basar la selección de servidores de base de datos en el valor del token extraído de las solicitudes de cliente (aplicación o servidor web). Estos tokens se definen mediante expresiones SQL. Para las solicitudes posteriores con el mismo token, el dispositivo Citrix ADC envía las solicitudes al mismo servidor de base de datos que gestionó la solicitud inicial. Las solicitudes con el mismo token se envían al mismo servidor de base de datos hasta que se alcanza el límite máximo de conexión o la entrada de sesión se ha superado.

Puede utilizar las siguientes expresiones SQL de ejemplo para definir tokens:

MySQL	MS SQL
MYSQL.REQ.QUERY.TEXT	MSSQL.REQ.QUERY.TEXT
MYSQL.REQ.QUERY.TEXT (n)	MSSQL. REQ.QUERY.TEXT (n)
MYSQL.REQ.QUERY.COMMAND	MSSQL.REQ.QUERY.COMMAND
MYSQL.CLIENT.USER	MSSQL.CLIENT.USER
MYSQL.CLIENT.DATABASE	MSSQL.CLIENT.DATABASE
MYSQL.CLIENT.CAPABILITIES	

En el ejemplo siguiente se muestra cómo funciona la función Citrix ADC DataStream cuando se configura el método token de equilibrio de carga.

Ilustración 1. DataStream y el método token de equilibrio de carga



En este ejemplo, el token es el nombre de la base de datos. Una solicitud con libros de tokens se envía al servidor de base de datos1 y una solicitud con música de token se envía al servidor de base de datos2. Todas las solicitudes posteriores con libros de tokens se envían al servidor de base de datos1 y las solicitudes con música de token se envían al servidor de base de datos2. Esta configuración proporciona pseudo persistencia con los servidores de base de datos.

Configure este ejemplo mediante la CLI

En el símbolo del sistema, escriba:

```
add service Service1 192.0.2.9 MYSQL 3306

add service Service2 192.0.2.11 MYSQL 3306

add lb vserver token_lb_vserver MYSQL 192.0.2.15 3306 -lbmethod token -
    rule MYSQL.CLIENT.DATABASE

bind lb vserver token_lb_vserver Service1

bind lb vserver token_lb_vserver Service2
<!--NeedCopy-->
```

Configure este ejemplo mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**, configure un servidor virtual y especifique el protocolo como **MYSQL**.

2. Haga clic en la sección **Servicio** y configure dos servicios especificando el protocolo como MYSQL. Enlazar estos servicios al servidor virtual.
3. En **Configuración avanzada**, haga clic en **Método**y, en la lista **Método de equilibrio de carga**, seleccione **TOKEN** y especifique la expresión como **MYSQL.CLIENT.DATABASE**.

Caso de uso 3: Registrar transacciones MSSQL en modo transparente

February 16, 2021

Puede configurar el dispositivo Citrix ADC para que funcione de manera transparente entre los clientes y servidores MSSQL, y para que solo registre o analice los detalles de todas las transacciones cliente-servidor. El modo transparente está diseñado para que el dispositivo Citrix ADC solo reenvíe las solicitudes MSSQL al servidor y, a continuación, retransmita las respuestas del servidor a los clientes. A medida que las solicitudes y las respuestas pasan por el dispositivo, el dispositivo registra la información recopilada de ellos, según lo especificado por el registro de auditoría o la configuración de AppFlow, o recopila estadísticas, según lo especificado por la configuración de Action Analytics. No es necesario agregar usuarios de base de datos al dispositivo.

Cuando se opera en modo transparente, el dispositivo Citrix ADC no realiza el equilibrio de carga, la cambio de contenido o la multiplexación de conexión para las solicitudes. Sin embargo, responde al paquete previo al inicio de sesión de un cliente en nombre del servidor para que pueda evitar que se acuerde el cifrado durante el protocolo de enlace previo al inicio de sesión. El paquete de inicio de sesión y los paquetes posteriores se reenvían al servidor.

Resumen de las tareas de configuración

Para registrar o analizar solicitudes MSSQL en modo transparente, debe hacer lo siguiente:

- Configure el dispositivo Citrix ADC como la Gateway predeterminada tanto para clientes como para servidores.
- Realice una de las siguientes acciones en el dispositivo Citrix ADC:
  - **Configure la opción USIP de uso global de dirección IP de origen:** cree un servidor virtual de equilibrio de carga con una dirección IP comodín y el número de puerto en el que los servidores MSSQL escuchan las solicitudes (un servidor virtual comodín específico del puerto). A continuación, habilite la opción USIP globalmente. Si configura un servidor virtual comodín específico del puerto, no es necesario crear servicios MSSQL en el dispositivo. El dispositivo detecta los servicios en función de la dirección IP de destino en las solicitudes del cliente.
  - **Si no desea configurar la opción USIP globalmente:** cree servicios MSSQL con la opción

USIP habilitada en cada uno de ellos. Si configura servicios, no es necesario crear un servidor virtual comodín específico del puerto.

- Configure el registro de auditoría, AppFlow o Action Analytics para registrar o recopilar estadísticas sobre las solicitudes. Si configura un servidor virtual, puede enlazar las directivas con el servidor virtual o con el punto de enlace global. Si no configura un servidor virtual, puede enlazar las directivas únicamente al punto de enlace global.

Configurar el modo transparente mediante un servidor virtual comodín

Puede configurar el modo transparente configurando un servidor virtual comodín específico del puerto y habilitando el modo Usar IP de origen (USIP) globalmente. Cuando un cliente envía su Gateway predeterminada (el dispositivo Citrix ADC) una solicitud con la dirección IP de un servidor MSSQL en el encabezado de dirección IP de destino, el dispositivo comprueba si la dirección IP de destino está disponible. Si la dirección IP está disponible, el servidor virtual reenvía la solicitud al servidor. De lo contrario, descarta la solicitud.

Crear un servidor virtual comodín mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para crear un servidor virtual comodín y compruebe la configuración:

```
add lb vserver <name> <serviceType> <IPAddress> <port>

show lb vserver <name>
<!--NeedCopy-->
```

Ejemplo:

```
> add lb vserver wildcardLbVs MSSQL * 1433
 Done
> show lb vserver wildcardLbVs
    wildcardLbVs (*:1433) - MSSQL   Type: ADDRESS
    State: UP
    . . .

 Done
>
<!--NeedCopy-->
```


Crear un servidor virtual comodín mediante la GUI

Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**y cree un servidor virtual. Especifique MSSQL como protocolo y * como dirección IP.

Habilitar el modo USIP (USIP) de forma global mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para habilitar el modo USIP globalmente y verificar la configuración:

```
enable ns mode USIP

show ns mode
<!--NeedCopy-->
```

Ejemplo:

```
> enable ns mode USIP
 Done
> show ns mode

    Mode                                Acronym
       Status
    -------                             -------
       ------
                . . .
 3) Use Source IP                  USIP                            ON
                . . .
 Done
>
<!--NeedCopy-->
```

Habilitar el modo USIP globalmente mediante la interfaz gráfica de usuario

1. Vaya a **Sistema > Configuración** y, en Modos y funciones, seleccione **Configurar modos**.
2. Seleccione **Usar IP de origen**.

Configurar el modo transparente mediante los servicios MSSQL

Puede configurar el modo transparente configurando los servicios MSSQL y habilitando USIP en cada servicio. Cuando un cliente envía su Gateway predeterminada (el dispositivo Citrix ADC) una solicitud

con la dirección IP de un servidor MSSQL en el encabezado de dirección IP de destino, el dispositivo reenvía la solicitud al servidor de destino.

Cree un servicio MSSQL y habilite el modo USIP en el servicio mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para crear un servicio MSSQL, con USIP habilitado, y compruebe la configuración:

```
add service <name> (<IP> | <serverName>) <serviceType> <port> -usip YES
    `

show service <name>
<!--NeedCopy-->
```

Ejemplo

```
> add service myDBservice 192.0.2.0 MSSQL 1433 -usip YES
 Done
> show service myDBservice
    myDBservice (192.0.2.0:1433) - MSSQL
    State: UP
                . . .
    Use Source IP: YES      Use Proxy Port: YES
                . . .
 Done
>
<!--NeedCopy-->
```

Crear un servicio MSSQL, con USIP habilitado, mediante la GUI

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servicios** y configure un servicio.
2. Especifique el protocolo como **MSSQL** y, en **Configuración**, seleccione **Usar IP de origen**.

Caso de uso 4: Equilibrio de carga específico de base de datos

August 20, 2021

Una comunidad de servidores de base de datos debe equilibrarse la carga no solo en función de los estados de los servidores, sino también en función de la disponibilidad de la base de datos en cada servidor. Un servicio puede estar activo y un dispositivo de equilibrio de carga puede mostrarlo como en estado ACTIVO, pero la base de datos solicitada puede no estar disponible en ese servicio. La solicitud no se sirve si se reenvía una consulta a un servicio en el que la base de datos no está disponible. Por lo tanto, un dispositivo de equilibrio de carga debe tener en cuenta la disponibilidad de una base de datos en cada servicio. Y al tomar una decisión de equilibrio de carga, debe considerar solo aquellos servicios en los que la base de datos está disponible.

Como ejemplo, considere que los servidores de base de datos server1, server2 y server3 hospedan bases de datos mydatabase1 y mydatabase2. Si mydatabase1 no está disponible en servidor2, el dispositivo de equilibrio de carga debe ser consciente de ese cambio en el estado. Debe cargar las solicitudes de equilibrio para mydatabase1 solo en servidor1 y servidor3. Después de que mydatabase1 esté disponible en server2, el dispositivo de equilibrio de carga debe incluir server2 en las decisiones de equilibrio de carga. Del mismo modo, si mydatabase2 deja de estar disponible en server3, el dispositivo debe equilibrar la carga de las solicitudes de mydatabase2 solo en servidor1 y servidor2. Debe incluir server3 en sus decisiones de equilibrio de carga solo cuando mydatabase2 esté disponible. Este comportamiento de equilibrio de carga debe ser coherente en todas las bases de datos alojadas en la comunidad de servidores.

El dispositivo Citrix ADC implementa este comportamiento recuperando una lista de todas las bases de datos activas en un servicio. Para recuperar la lista de bases de datos activas, el dispositivo utiliza un monitor configurado con una consulta SQL adecuada. Si la base de datos solicitada no está disponible en un servicio, el dispositivo excluye el servicio de las decisiones de equilibrio de carga hasta que esté disponible. Este comportamiento garantiza un servicio ininterrumpido a los clientes.

> **Nota**
>
> El equilibrio de carga específico de la base de datos solo se admite para los tipos de servicio MSSQL y MySQL. Esta compatibilidad también está disponible para la implementación de alta disponibilidad de Microsoft SQL Server 2012.

Para configurar el equilibrio de carga específico de la base de datos, debe configurar lo siguiente:

- Habilite la función de equilibrio de carga y configure un servidor virtual de equilibrio de carga de tipo MSSQL o MySQL.
- Configure los servicios que alojan la base de datos y vincule los servicios al servidor virtual. El monitor necesita credenciales de usuario válidas para iniciar sesión en el servidor de base de datos, por lo que debe configurar una cuenta de usuario de base de datos en cada uno de los servidores y, a continuación, agregar la cuenta de usuario al dispositivo Citrix ADC.
- A continuación, configure un monitor MSSQL-ECV o MYSQL-ECV y vincule el monitor a cada servicio.
- Por último, debe probar la configuración para asegurarse de que funciona según lo previsto.

Antes de realizar estas tareas de configuración, asegúrese de comprender cómo funciona el equilibrio de carga específico de la base de datos.

Cómo funciona el equilibrio de carga específico de la base de datos

Para el equilibrio de carga específico de la base de datos, configure un monitor que consulta periódicamente a cada servidor de base de datos los nombres de todas las bases de datos activas en él. El dispositivo Citrix ADC almacena los resultados y actualiza regularmente los registros en función de la información recuperada mediante la supervisión. Cuando un cliente consulta una base de datos concreta, el dispositivo utiliza el método de equilibrio de carga configurado para seleccionar un servicio y, a continuación, comprueba sus registros para determinar si la base de datos está disponible en ese servicio. Si los registros indican que la base de datos no está disponible, utiliza el método de equilibrio de carga configurado para seleccionar el siguiente servicio disponible y, a continuación, repite la comprobación. El dispositivo reenvía la consulta al primer servicio disponible en el que está activa la base de datos.

Habilitar equilibrio de carga

Puede configurar entidades de equilibrio de carga como servicios y servidores virtuales cuando la función de equilibrio de carga está inhabilitada. Las entidades no funcionan hasta que se habilita la función.

Habilitar el equilibrio de carga mediante la CLI

En el símbolo del sistema, escriba el siguiente comando para habilitar el equilibrio de carga y verificar la configuración:

```
enable ns feature LB

show ns feature
<!--NeedCopy-->
```

Ejemplo:

```
> enable ns feature LoadBalancing
 Done
> show ns feature

        Feature                         Acronym             Status
```



```
6          -------                        -------              ------
7    1)    Web Logging                    WL                   OFF
8    2)    Surge Protection               SP                   ON
9    3)    Load Balancing                 LB                   ON
10   .
11   .
12   .
13   24)   NetScaler Push                 push                 OFF
14   Done
15  <!--NeedCopy-->
```

Habilitar el equilibrio de carga mediante la GUI

Vaya a **Sistema > Configuración** y, en **Configurar funciones básicas**, seleccione **Equilibrio de carga**.

Configurar un servidor virtual de equilibrio de carga para el equilibrio de carga específico de la base de datos

Para configurar un servidor virtual para equilibrar la carga de las bases de datos en función de la disponibilidad, habilite el parámetro de equilibrio de carga específico de la base de datos en el servidor virtual. Al habilitar el parámetro se modifica la lógica de equilibrio de carga para que el dispositivo Citrix ADC remita los resultados del sondeo de supervisión enviado al servicio seleccionado, antes de reenviar la consulta a ese servicio.

Configurar un servidor virtual de equilibrio de carga para el equilibrio de carga específico de la base de datos mediante la CLI

En el símbolo del sistema, escriba el siguiente comando para configurar un servidor virtual de equilibrio de carga para el equilibrio de carga específico de la base de datos y compruebe la configuración:

```
1  add lb vserver <name> <serviceType> <ipAddress> <port> -dbsLb ENABLED
2
3  show lb vserver <name>
4  <!--NeedCopy-->
```

Configurar servicios

Después de habilitar la función de equilibrio de carga, debe crear al menos un servicio para cada servidor de aplicaciones que se va a incluir en la configuración de equilibrio de carga. Los servicios que

configura proporcionan las conexiones entre el dispositivo Citrix ADC y los servidores con equilibrio de carga. Cada servicio tiene un nombre y especifica una dirección IP, un puerto y el tipo de datos que se sirven.

Si crea un servicio sin crear primero un objeto de servidor, la dirección IP del servicio es también el nombre del servidor que hospeda el servicio. Si prefiere identificar servidores por nombre en lugar de por dirección IP, puede crear objetos de servidor y, a continuación, especificar el nombre de un servidor en lugar de su dirección IP al crear un servicio.

Configurar usuarios de la base de datos

En las bases de datos, una conexión siempre tiene estado, lo que significa que cuando se establece una conexión, debe autenticarse.

Configure el nombre de usuario y la contraseña de la base de datos en Citrix ADC. Por ejemplo, si tiene un usuario John configurado en la base de datos, también debe configurar el usuario John en el ADC. Los nombres de usuario de la base de datos y las contraseñas agregadas al ADC se agregan al `nsconfig` archivo.

> **Nota**
>
> Los nombres distinguen entre mayúsculas y minúsculas.

El ADC utiliza estas credenciales de usuario para autenticar los clientes y, a continuación, autenticar las conexiones del servidor con los servidores de base de datos.

Agregar un usuario de base de datos mediante la CLI

En el símbolo del sistema, escriba:

```
add db user <username> - password <password>
<!--NeedCopy-->
```

Ejemplo:

```
add db user nsdbuser -password dd260427edf
<!--NeedCopy-->
```

Agregar un usuario de base de datos mediante la GUI

Vaya a **Sistema > Administración de usuarios > Usuarios de base de datos** y configure un usuario de base de datos.

Si ha cambiado la contraseña del usuario de base de datos en el servidor de base de datos, debe restablecer la contraseña del usuario correspondiente configurado en el dispositivo Citrix ADC.

Restablecer la contraseña de un usuario de base de datos mediante la CLI

En el símbolo del sistema, escriba:

```
set db user <username> -password <password>
<!--NeedCopy-->
```

Ejemplo:

```
set db user nsdbuser -password dd260538abs
<!--NeedCopy-->
```

Restablecer la contraseña de los usuarios de la base de datos mediante la GUI

Vaya a **Sistema > Administración de usuarios > Usuarios de base**de datos, seleccione un usuario e introduzca nuevos valores para la contraseña.

Si ya no existe un usuario de base de datos en el servidor de base de datos, puede quitarlo del dispositivo Citrix ADC. Sin embargo, si el usuario sigue existiendo en el servidor de base de datos y se quita el usuario del dispositivo ADC, cualquier solicitud del cliente con este nombre de usuario no se autenticará. Por lo tanto, el nombre de usuario no se enruta al servidor de base de datos.

Eliminar un usuario de base de datos mediante la CLI

En el símbolo del sistema, escriba:

```
rm db user <username>
<!--NeedCopy-->
```

Ejemplo:

```
rm db user nsdbuser
<!--NeedCopy-->
```


Eliminar un usuario de base de datos mediante la GUI

Vaya a **Sistema > Administración de usuarios > Usuarios de base**de datos, seleccione un usuario y haga clic en **Eliminar**.

Configurar un monitor para recuperar los nombres de las bases de datos activas

Puede crear un monitor para recuperar la lista de todas las bases de datos activas en una instancia de base de datos. El monitor inicia sesión en el servidor de base de datos mediante credenciales de usuario válidas y ejecuta una consulta SQL adecuada. La consulta SQL que necesita usar depende de la implementación de SQL Server. Por ejemplo, en una instalación de creación de reflejo de base de datos MSSQL, puede utilizar la siguiente consulta para recuperar una lista de bases de datos activas disponibles en una instancia de servidor.

```
1 select name from sys.databases where state=0
2 <!--NeedCopy-->
```

En una configuración de base de datos MySQL puede utilizar las siguientes consultas para recuperar una lista de bases de datos activas disponibles en una instancia de servidor.

Mostrar bases de datos:

También puede configurar el monitor para evaluar la respuesta para una condición de error y para almacenar los resultados si no hay ningún error. Si la respuesta contiene un error, el monitor marca el servicio como DOBAJA. El dispositivo excluye el servicio de las decisiones de equilibrio de carga hasta que ya no se devuelve un error.

> **Nota**
>
> La función de equilibrio de carga específica de la base de datos solo es compatible con los tipos de servicio MSSQL y MySQL. Por lo tanto, el tipo de monitor debe ser MSSQL-ECV o MYSQL-ECV.

Configurar un monitor para recuperar los nombres de todas las bases de datos activas alojadas en un servicio mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para recuperar los nombres de todas las bases de datos activas alojadas en un servicio y verificar la configuración:

```
1 add lb monitor <monitorName> <type> -userName <string> -sqlQuery <text>
      -evalRule <expression> -storedb ENABLED
2
3 show lb monitor <monitorName>
```



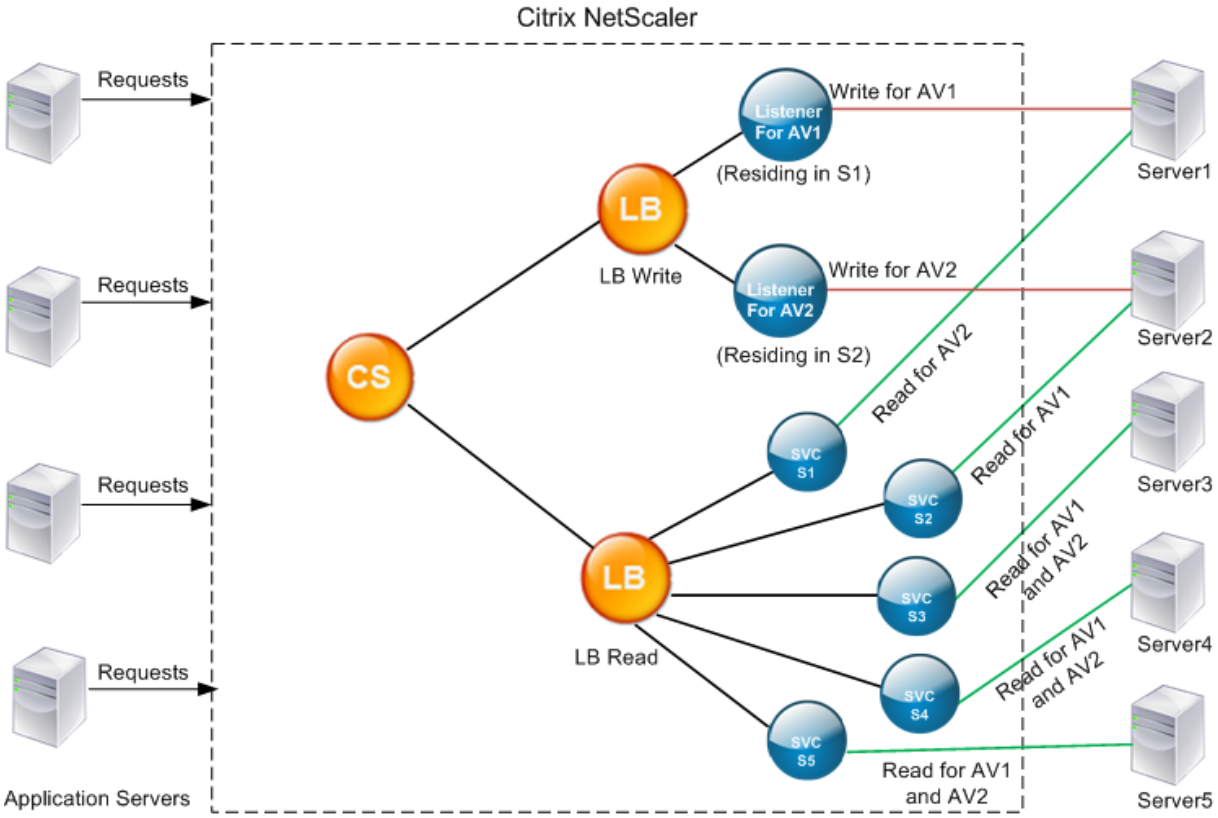
```
4 <!--NeedCopy-->
```

Configurar un monitor para recuperar los nombres de todas las bases de datos activas alojadas en un servicio mediante la GUI

1. Vaya a **Administración del tráfico > Equilibrio de carga > Monitores** y configure un monitor de tipo MSSQL-ECV o MYSQL-ECV.
2. En **Parámetros especiales**, especifique un nombre de usuario, una consulta y una regla. Por ejemplo, para MSSQL-ECV, la consulta debe ser “select name from sys.databases where state=0”), y una regla debe ser MSSQL.RES.TYPE.NE (ERROR). Para MYSQL-ECV, la consulta debe ser “mostrar bases de datos” y una regla debe ser MYSQL.RES.TYPE.NE (ERROR).

Compatibilidad con la implementación de grupos de disponibilidad para MSSQL

Considere el siguiente caso en el que se configura el equilibrio de carga específico de la base de datos en una implementación de grupo de alta disponibilidad. S1 a S5 son los servicios del dispositivo ADC. DB1 a DB4 son las bases de datos en los servidores representados por los servicios S1 a S5. AV1 y AV2 son los grupos de disponibilidad. Cada grupo de disponibilidad contiene hasta una instancia de servidor de base de datos principal y hasta cuatro instancias de servidor de base de datos secundario. Un servicio, que representa los servidores del grupo de disponibilidad, puede ser primario para un grupo de disponibilidad y secundario para otro grupo de disponibilidad. Cada grupo de disponibilidad contiene diferentes bases de datos y un listener, que es un servicio. Todas las solicitudes llegan al servicio de escucha que reside en la base de datos principal. AVI contiene bases de datos DB1 y DB2. AV2 contiene bases de datos DB3 y DB4. L1 y L2 son los oyentes en AV1 y AV2 respectivamente. S1 es el servicio principal para AV1 y S2 es el servicio principal para AV2.



Servicio	Lista de bases de datos activas en el servicio
S1	DB1, DB2, DB3, DB4
S2	DB3, DB4
S3	DB3, DB4
S4	DB1, DB2
S5	DB1, DB2

Grupo de disponibilidad	Bases de datos	Servicios que representan a los servidores del grupo de disponibilidad
AV1	DB1, DB2	S1, S4, S5
AV2	DB3, DB4	S1, S2, S3

Las consultas fluyen de la siguiente manera:

1. Una consulta de lectura para AV1 se equilibra la carga entre S4 y S5. S1 es el principal para AV1.

2. Una consulta WRITE para AV1 se dirige a L1.
3. Una consulta de lectura para AV2 se equilibra la carga entre S1 y S3. S2 es el principal para AV2.
4. Una consulta WRITE para AV1 se dirige a L2.

Configuración de ejemplo

1. Configurar servidores virtuales de equilibrio de carga y cambio de contenido.
   - `add lb vserver lbwrite -dbslb enabled`
   - `add lbvserver lbread MSSQL -dbslb enabled`
   - `add csvserver csv MSSQL 1.1.1.10 1433`
2. Configure dos servicios de escucha, uno para cada grupo de disponibilidad, y cinco servicios S1 a S5 que representan bases de datos DB1 a DB4.
   - `add service L1 1.1.1.11 MSSQL 1433`
   - `add service L2 1.1.1.12 MSSQL 1433`
   - `add service s1 1.1.1.13 MSSQL 1433`
   - `add service s2 1.1.1.14 MSSQL 1433`
   - `add service s3 1.1.1.15 MSSQL 1433`
   - `add service s4 1.1.1.16 MSSQL 1433`
   - `add service s5 1.1.1.17 MSSQL 1433`
3. Enlazar los servicios a los servidores virtuales de equilibrio de carga.
   - `bind lbvserver lbwrite L1`
   - `bind lbvserver lbwrite L2`
   - `bind lbvserver lbread s1`
   - `bind lbvserver lbread s2`
   - `bind lbvserver lbread s3`
   - `bind lbvserver lbread s4`
   - `bind lbvserver lbread s5`
4. Configurar usuarios de bases de datos.
   - `add db user nsdbuser1 -password dd260427edf`
   - `add db user nsdbuser2 -password ccd1234xyzw`
5. Configure dos monitores, Monitor_L1 y Monitor_L2 para cada servicio de escucha, para recuperar la lista de bases de datos activas en ese grupo de disponibilidad. Agregue un monitor, monitor1 para recuperar la lista de bases de datos para la instancia del servidor de base de datos secundario.
   - ```
     add lb monitor monitor_L1 MSSQL-ECV -userName user1 -sqlQuery ”
     SELECT name FROM sys.databases a INNER JOIN sys.dm_hadr_availability_replica_
      b ON a.replica_id=b.replica_id INNER JOIN sys.availability_group_listeners
      c on b.group_id = c.group_id INNER JOIN sys.availability_group_listener_ip_a
      d on c.listener_id = d.listener_id WHERE b.role = 1 and d.ip_address
      like '1.1.1.11'”-evalRule ”MSSQL.RES.TYPE.NE(ERROR)” -storedb
     ```


     ```

```
ENABLED
```

- `add lb monitor monitor_L2 MSSQL-ECV -userNameuser1 -sqlQuery ” SELECT name FROM sys.databases a INNER JOIN sys.dm_hadr_availability_replicca b ON a.replica_id=b.replica_id INNER JOIN sys.availability_group_listeners c on b.group_id = c.group_id INNER JOIN sys.availability_group_listener_ip_a d on c.listener_id = d.listener_id WHERE b.role = 1 and d.ip_address like '1.1.1.12'”-evalRule ”MSSQL.RES.TYPE.NE(ERROR)”-storedb ENABLED`
- `add lb monitor monitor1 MSSQL-ECV -userNameuser1 -sqlQuery ”SELECT name FROM sys.databases a INNER JOIN sys.dm_hadr_availability_replica_states b ON a.replica_id=b.replica_id WHERE b.role = 2”-evalRule ”MSSQL.RES.TYPE.NE(ERROR)”-storedb ENABLED`

6. Configurar directivas de lectura y escritura.
   - `add cs policy pol_write -rule ”MSSQL.REQ.QUERY.TEXT.CONTAINS(” insert”)”`
   - `add cs policy pol_read -rule ”MSSQL.REQ.QUERY.TEXT.CONTAINS(”select ”)”`
7. Enlazar las directivas al servidor virtual de cambio de contenido.
   - `bind csvserver csv -targetLBVserver lbwrite -policyName pol_write -priority 11`
   - `bind csvserver csv -targetLBVserver lbread -policyName pol_read -priority 12`
8. Enlazar monitores a los servicios. Enlazar monitores a los servicios L1 y L2 para obtener la lista de bases de datos activas para el grupo de disponibilidad para el que es el listener. Enlazar monitores a todos los servicios vinculados al servidor virtual de solo lectura.
   - `bind service L1 -monitorName monitor_L1`
   - `bind service L2 -monitorName monitor_L2`
   - `bind service s1 -monitorName monitor1`
   - `bind service s2 -monitorName monitor1`
   - `bind service s3 -monitorName monitor1`
   - `bind service s4 -monitorName monitor1`
   - `bind service s5 -monitorName monitor1`

Ejemplos de configuración para el servidor virtual MSSQL

Para configurar un servidor virtual de equilibrio de carga para el equilibrio de carga específico de la base de datos:

```
1 add lb vserver DBSpecificLB1 MSSQL 192.0.2.10 1433 -dbsLb ENABLED
```



```
2
3 Done
4
5 show lb vserver DBSpecificLB1
6
7 DBSpecificLB1 (192.0.2.10:1433) - MSSQL Type: ADDRESS
8 . . .
9 DBS_LB: ENABLED
10
11 Done
12 <!--NeedCopy-->
```

Para configurar servicios:

agregar servicio msservice1 5.5.5.5 MSSQL 1433

Para configurar un monitor para recuperar los nombres de todas las bases de datos activas alojadas en un servicio mediante la línea de comandos:

```
1 add lb monitor mssql-monitor1 MSSQL-ECV -userName user1 -sqlQuery ”
     select name from sys.databases where state=0” -evalRule ”MSSQL.RES.
     TYPE.NE(ERROR)” -storedb EN
2
3 Done
4
5 show lb monitor mssql-monitor1
6
7 1)   Name.......: mssql-monitor1    Type......: MSSQL-ECV
8
9 ...
10
11 Special parameters: Database.....:””
12
13 User name.....:”user1”
14
15 Query..:select name from sys.databases where state=0 EvalRule...:MSSQL.
     RES.TYPE.NE(ERROR)
16
17 Version...:70 STORE_DB...:ENABLED
18
19 Done
20 <!--NeedCopy-->
```


Ejemplos de configuración para el servidor virtual MySQL

Para configurar un servidor virtual de equilibrio de carga para el equilibrio de carga específico de la base de datos:

```
add lb vserver DBSpecificLB1 MYSQL 192.0.2.10 3306 -dbsLb ENABLED

Done

show lb vserver DBSpecificLB1

DBSpecificLB1 (192.0.2.10:3306) - MYSQL Type: ADDRESS

. . .

DBS_LB: ENABLED

Done
<!--NeedCopy-->
```

Para configurar servicios:

```
add service msservice1 5.5.5.5 MYSQL 3306
<!--NeedCopy-->
```

Para configurar un monitor para recuperar los nombres de todas las bases de datos activas alojadas en un servicio mediante la línea de comandos:

```
add lb monitor mysql-monitor1 MYSQL-ECV -userName user1 -sqlQuery "show
    databases" -evalRule "MYSQL.RES.TYPE.NE(ERROR)" -storedb ENABLED

Done

show lb monitor mysql-monitor1

1)     Name.......: mysql-monitor1  Type......: MYSQL-ECV  State....:
   ENABLED

...

Special parameters: Database.....:""
```



```
12
13 User name.....:"user1" Query..:show databases
14
15 EvalRule...:MYSQL.RES.TYPE.NE(ERROR) STORE_DB...:ENABLED
16
17 Done
18 <!--NeedCopy-->
```

Referencia de DataStream

July 27, 2022

Esta referencia describe los protocolos MySQL y TDS, las versiones de la base de datos, los métodos de autenticación y los conjuntos de caracteres admitidos por la función DataStream. También describe cómo el Citrix ADC gestiona las solicitudes de transacción y las consultas especiales que modifican el estado de una conexión.

También puede configurar el dispositivo Citrix ADC para generar mensajes de registro de auditoría para la función DataStream.

Versiones de bases de datos, protocolos y métodos de autenticación admitidos

	Base de datos MySQL	Base de datos MS SQL
Versiones de base de datos	Versiones de base de datos MySQL 4.1, 5.0, 5.1, 5.4, 5.5, 5.6	Versiones de base de datos MS SQL 2000, 2000SP1, 2005, 2008, 2008R2, 2012, 2014 (compatibilidad con autenticación Kerberos)
Protocolos	Protocolo MySQL versión 10. Para obtener información sobre el protocolo MySQL, consulte Protocolo cliente/servidor de MySQL.	Protocolo de flujo de datos tabular (TDS) versión 7.1 y superior. Para obtener información sobre el protocolo TDS, consulte Protocolo de flujo de datos tabular

	Base de datos MySQL	Base de datos MS SQL
Métodos de autenticación	Se admite la autenticación nativa de MySQL.	Se admiten la autenticación de servidor SQL y la autenticación de Windows (Kerberos/NTLM).

Juegos de caracteres

La función DataStream solo admite el juego de caracteres UTF-8.

El conjunto de caracteres utilizado por el cliente al enviar una solicitud puede ser diferente del conjunto de caracteres utilizado en las respuestas del servidor de base de datos. Aunque el parámetro charset se establece durante el establecimiento de la conexión, se puede cambiar en cualquier momento enviando una consulta SQL. El juego de caracteres está asociado a una conexión y, por lo tanto, las solicitudes de conexiones con un juego de caracteres no se pueden multiplexar en una conexión con un juego de caracteres diferente.

El dispositivo Citrix ADC analiza las consultas enviadas por el cliente y las respuestas enviadas por el servidor de base de datos.

El juego de caracteres asociado a una conexión se puede cambiar después del apretón de manos inicial mediante las dos consultas siguientes:

```
1 SET NAMES <charset> COLLATION <collation>
2
3 SET CHARACTER SET <charset>
4 <!--NeedCopy-->
```

Transacciones

En MySQL, las transacciones se identifican mediante el parámetro de conexión AUTOCOMMIT o las consultas INICI:COMMIT. El parámetro AUTOCOMMIT se puede establecer durante el enlace inicial, o después de establecer la conexión mediante la consulta SET AUTOCOMMIT.

El dispositivo Citrix ADC analiza explícitamente cada consulta para determinar el comienzo y el final de una transacción.

En el protocolo MySQL, la respuesta contiene dos indicadores para indicar si la conexión es una transacción: los indicadores TRANSACTION y AUTOCOMMIT.

Si la conexión es una transacción, se establece el indicador TRANSACTION. O bien, si el modo AutoCommit está desactivado, el indicador AUTOCOMMIT no está establecido. El dispositivo ADC analiza

la respuesta y, si el indicador TRANSACTION está establecido o el indicador AUTOCOMMIT no está establecido, no realiza la multiplexación de conexión. Cuando estas condiciones ya no se cumplen, el dispositivo ADC comienza la multiplexación de conexión.

> **Nota**
>
> Las transacciones también son compatibles con MS SQL.

Consultas especiales

Existen consultas especiales, como SET y PREPARE, que modifican el estado de la conexión y pueden interrumpir el cambio de solicitudes y, por lo tanto, estas consultas deben manejarse de manera diferente.

Al recibir una solicitud con consultas especiales, el dispositivo Citrix ADC envía una respuesta Aceptar al cliente y también almacena la solicitud en la conexión.

Cuando se recibe una consulta no especial, como INSERT y SELECT, junto con una consulta almacenada, el dispositivo ADC busca la conexión del lado del servidor en la que la consulta almacenada ya se ha enviado al servidor de base de datos. Si no existen tales conexiones, el dispositivo ADC crea una conexión, envía primero la consulta almacenada y, a continuación, envía la solicitud con la consulta no especial.

En las consultas especiales SET, USE db e INIT_DB, el dispositivo modifica un campo en la conexión del lado del servidor correspondiente a la consulta especial. Esta modificación da como resultado una mejor reutilización de la conexión del lado del servidor.

Solo 16 consultas se almacenan en cada conexión.

A continuación se muestra una lista de las consultas especiales para las que el dispositivo ADC tiene un comportamiento modificado.

- Consulta SET

  Las consultas SET SQL definen variables asociadas a la conexión. Estas consultas también se utilizan para definir variables globales, pero a partir de ahora, el dispositivo ADC no puede diferenciar entre variables locales y globales. Para esta consulta, el dispositivo ADC utiliza el mecanismo 'almacenar y reenviar'.

- Utilice la consulta <db>

  Mediante esta consulta, el usuario puede cambiar la base de datos asociada a una conexión. En este caso, el dispositivo ADC analiza el valor <db> enviado y modifica un campo en la conexión del lado del servidor para reflejar la nueva base de datos que se va a utilizar.

- INIT_DB (comando)

Mediante esta consulta, el usuario puede cambiar la base de datos asociada a una conexión. En este caso, el dispositivo ADC analiza el valor <init_db> enviado y modifica un campo en la conexión del lado del servidor para reflejar la nueva base de datos que se va a utilizar.

- COM_PREPARE

  El dispositivo ADC detiene la conmutación de solicitud al recibir este comando.

- PREPARE consulta

  Esta consulta se utiliza para crear instrucciones preparadas que están asociadas a una conexión. Para esta consulta, el dispositivo ADC utiliza el mecanismo 'almacenar y reenviar'.

Compatibilidad con mensajes de registro de auditoría

Ahora puede configurar el dispositivo Citrix ADC para generar mensajes de registro de auditoría para la función DataStream. Los mensajes de registro de auditoría se generan cuando se establecen, se cierran o se eliminan las conexiones del lado del cliente y del lado del servidor. Las categorías de mensajes que puede registrar y ver son ERROR e INFO. Los mensajes de error para las conexiones del lado del cliente comienzan con "CS" y los mensajes de error para las conexiones del lado del servidor comienzan con "SS." En caso necesario, se proporciona información adicional. Por ejemplo, los mensajes de registro para conexiones cerradas (CS_CONN_CLOSED) incluyen solo el ID de conexión. Sin embargo, los mensajes de registro para conexiones establecidas (CS_CONN_ESTD) incluyen información como el nombre de usuario, el nombre de la base de datos y la dirección IP del cliente, además del identificador de conexión.

Sistema de nombres de dominio

June 22, 2022

Nota: A partir de la versión 13.0 compilación 41.x, el dispositivo Citrix ADC en modo ADNS y proxy cumple totalmente con el día de la marca DNS 2019.

Puede configurar el dispositivo Citrix ADC para que funcione como un servidor de nombres de dominio autorizado (servidor ADNS) para un dominio. Agregue los registros de recursos DNS que pertenecen al dominio para el que el dispositivo tiene autoridad y configure los parámetros de registro de recursos. También puede configurar el dispositivo como un servidor DNS proxy que equilibre la carga de una comunidad de servidores de nombres DNS que se encuentran dentro o fuera de la red. Configure el dispositivo como una resolución final y un reenviador. Puede configurar sufijos DNS que permitan la resolución de nombres cuando no se configuran nombres de dominio completos. El dispositivo también admite la consulta DNS ANY que recupera todos los registros que pertenecen a un dominio.

Puede configurar el dispositivo para que funcione simultáneamente como un servidor DNS autoritativo para un dominio y un servidor proxy DNS para otro dominio. Cuando configura el dispositivo como el servidor DNS autorizado o el servidor proxy DNS para una zona, puede permitir que el dispositivo utilice el TCP para tamaños de respuesta que superen el límite de tamaño especificado para el Protocolo de datagramas de usuario (UDP).

Cómo funciona el DNS en Citrix ADC

Puede configurar el dispositivo Citrix ADC para que funcione como servidor ADNS, servidor proxy DNS, resolución final y reenviador. Puede agregar registros de recursos DNS en el dispositivo Citrix ADC, incluidos los siguientes registros:

- Registros de servicios (SRV)
- Registros IPv6 (AAAA)
- Registros de direcciones (A)
- Registros de intercambio de correo (MX)
- Registros de nombres canónicos (CNAME)
- Registros de punteros (PTR)
- Registros de inicio de autoridad (SOA)
- Registros de texto (TXT)
- Registros de puntero de autoridad de nombres (NAPTR)
- Registros DNSKEY
- Registros de autorización de la entidad de certificación (CAA)

Además, puede configurar Citrix ADC para equilibrar la carga de servidores de nombres DNS externos.

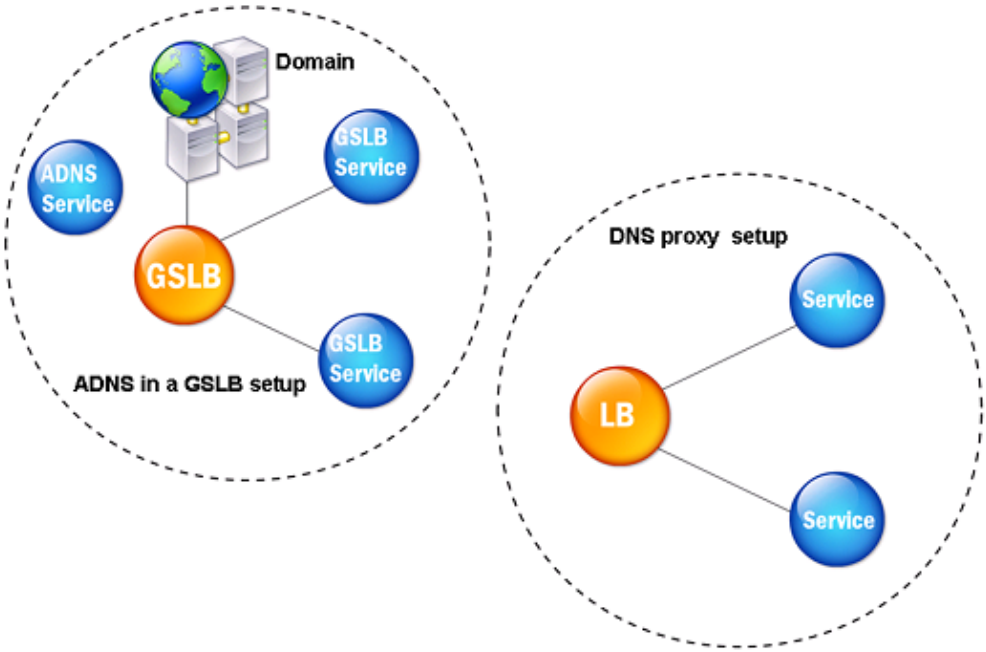
El dispositivo Citrix ADC se puede configurar como la autoridad de un dominio. Agregue registros SOA y NS válidos para el dominio.

Un servidor ADNS es un servidor DNS que contiene información completa sobre una zona.

Para configurar el dispositivo Citrix ADC como un servidor ADNS para una zona, debe agregar un servicio ADNS y, a continuación, configurar la zona. Para hacerlo, agregue registros SOA y NS válidos para el dominio. Cuando un cliente envía una solicitud DNS, el dispositivo Citrix ADC busca el nombre de dominio en los registros de recursos configurados. Puede configurar el servicio ADNS para que se use con la función Citrix ADC Global Server Load Balancing (GSLB).

Puede delegar un subdominio agregando registros NS para el subdominio a la zona del dominio principal. A continuación, puede hacer que Citrix ADC sea autoritativo para el subdominio, agregando un “registro de adhesión” para cada uno de los servidores de nombres de subdominio. Si se configura GSLB, Citrix ADC toma una decisión de equilibrio de carga GSLB en función de su configuración y responde con la dirección IP del servidor virtual seleccionado. La siguiente ilustración muestra las entidades en una configuración de ADNS GSLB y una configuración de proxy DNS.

Ilustración 1. Modelo de entidad proxy DNS



El dispositivo Citrix ADC puede funcionar como un proxy DNS. El almacenamiento en caché de registros DNS, que es una función importante de un proxy DNS, está habilitado de forma predeterminada en el dispositivo Citrix ADC. El almacenamiento en caché permite que el dispositivo Citrix ADC proporcione respuestas rápidas para traducciones repetidas. Cree un servidor virtual DNS de equilibrio de carga y servicios DNS y, a continuación, vincule estos servicios al servidor virtual.

Citrix ADC proporciona dos opciones, el tiempo de vida mínimo (TTL) y el TTL máximo para configurar la vida útil de los datos almacenados en caché. Los datos almacenados en caché agotan el tiempo de espera según lo especificado en la configuración de estas dos opciones. Citrix ADC comprueba el TTL del registro DNS procedente del servidor. Si el TTL es menor que el TTL mínimo configurado, se reemplaza por el TTL mínimo configurado. Si el TTL es mayor que el TTL máximo configurado, se reemplaza por el TTL máximo configurado.

Citrix ADC también permite almacenar en caché las respuestas negativas de un dominio. Una respuesta negativa indica que la información sobre un dominio solicitado no existe o que el servidor no puede proporcionar una respuesta a la consulta. El almacenamiento de esta información se denomina almacenamiento en *caché negativo*. El almacenamiento en caché negativo ayuda a acelerar las respuestas a las consultas en un dominio y, opcionalmente, puede proporcionar el tipo de registro.

Una respuesta negativa puede ser una de las siguientes:

- Mensaje de error NXDOMAIN: si hay una respuesta negativa en la memoria caché local, Citrix ADC devuelve un mensaje de error (NXDOMAIN). Si la respuesta no está en la memoria caché local, la consulta se reenvía al servidor y el servidor devuelve un error NXDOMAIN a Citrix ADC. Citrix ADC almacena en caché la respuesta localmente y, a continuación, devuelve el mensaje de error al cliente.
- Mensaje de error NODATA: Citrix ADC envía un mensaje de error NODATA si el nombre de dominio en la consulta es válido pero los registros del tipo dado no están disponibles.

Citrix ADC admite la resolución recursiva de solicitudes de DNS. En la resolución recursiva, el solucionador (cliente DNS) envía una consulta recursiva a un servidor de nombres para un nombre de dominio. Si el servidor de nombres consultado tiene autoridad para el dominio, responde con el nombre de dominio solicitado. De lo contrario, Citrix ADC consulta los servidores de nombres de forma recursiva hasta que se encuentra el nombre de dominio solicitado.

Antes de poder aplicar la opción de consulta recursiva, primero debe habilitarla. También puede establecer el número de veces que la resolución de DNS debe enviar una solicitud de resolución (reintentos de DNS) si falla una búsqueda de DNS.

Puede configurar Citrix ADC como reenviador de DNS. Un reenviador pasa las solicitudes de DNS a servidores de nombres externos. Citrix ADC le permite agregar servidores de nombres externos y proporciona resolución de nombres para dominios fuera de la red. Citrix ADC también le permite establecer la prioridad de búsqueda de nombres en DNS o en el Servicio de nombres de Internet de Windows (WINS).

Permitir que el dispositivo ADC use DNS para resolver el nombre de host en su dirección IP respectiva

Nota: Necesita una utilidad SSH para acceder a la interfaz de línea de comandos (CLI) del dispositivo.

De forma predeterminada, el dispositivo ADC no puede resolver el nombre de host en su dirección IP respectiva. Realice las siguientes tareas para habilitar la resolución de nombres en el dispositivo:

1. Defina los servidores de nombres.
2. Defina un sufijo DNS.

Puntos que tener en cuenta

Realice la búsqueda de DNS desde la CLI. Las búsquedas de DNS desde el símbolo del shell del sistema operativo FreeBSD fallan porque la entrada en el archivo /etc/resolv.conf apunta a la dirección IP 127.0.0.2.

Los siguientes comandos se sustituyen por el comando `drill` en la CLI de FreeBSD del dispositivo al que se puede acceder con el comando `shell`:


```
- host
- dig
- getent/MIP
- nslookup
<!--NeedCopy-->
```

Por ejemplo, en lugar de ejecutar `dig www.google.com @8.8.8.8` para consultar el registro "A" "www.google.com" en el servidor de nombres "8.8.8.8", puede ejecutar el comando `drill www.google.com @8.8.8.8`. El comando `drill` funciona exactamente igual que el comando `dig`.

```
root@lab# drill www.google.com @8.8.8.8
;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 57980
;; flags: qr rd ra ; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;; www.google.com. IN A

;; ANSWER SECTION:
www.google.com. 300 IN A 142.250.187.196

;; AUTHORITY SECTION:

;; ADDITIONAL SECTION:

;; Query time: 53 msec
;; SERVER: 8.8.8.8
;; WHEN: Thu Jun 9 11:04:55 2022
;; MSG SIZE rcvd: 48
<!--NeedCopy-->
```

Si el dispositivo no puede hacer ping al servidor DNS en su dirección SNIP, el estado del servidor se muestra como inactivo. El ping correcto es importante cuando el dispositivo está detrás de un firewall.

Configuración CLI

En el símbolo del sistema, escriba:

```
add dns nameServer <Name_Server_IP_Address>
add dns suffix <DNS_Suffix>
<!--NeedCopy-->
```


Para verificar la configuración, escriba:

```
show dns nameServer
show dns suffix
<!--NeedCopy-->
```

Para probar la resolución de DNS, escriba:

```
show dns addrec <Host_Name>
<!--NeedCopy-->
```

Configuración de GUI

1. Vaya a **Administración del tráfico > DNS > Servidores de nombres > Agregar**.
2. En el cuadro de diálogo **Crear servidor de nombres**, introduzca la dirección IP del servidor de nombres y haga clic en **Crear**.
3. Vaya a **Administración del tráfico > DNS > Sufijo DNS > Agregar**.
4. En el cuadro de diálogo **Crear sufijo DNS**, introduzca el sufijo DNS, como ejemplo.com, que se utilizará para todas las consultas de host y haga clic en **Crear**.

DNS Round Robin

Cuando un cliente envía una solicitud de DNS para encontrar el registro de recursos de DNS, recibe una lista de direcciones IP que se resuelven con el nombre en la solicitud de DNS. A continuación, el cliente utiliza una de las direcciones IP de la lista, generalmente, el primer registro o dirección IP. Por lo tanto, se utiliza un único servidor para el TTL total de la memoria caché y se sobrecarga cuando llegan muchas solicitudes.

Cuando Citrix ADC recibe una solicitud de DNS, responde cambiando el orden de la lista de registros de recursos DNS en un método round robin. Esta función se denomina *DNS por turnos*. El round robin distribuye el tráfico por igual entre los centros de datos. Citrix ADC realiza esta función automáticamente. No tiene que configurar este comportamiento.

Resumen funcional

Si Citrix ADC está configurado como un servidor ADNS, devuelve los registros DNS en el orden en que se configuran los registros. Cuando Citrix ADC se configura como proxy DNS, devuelve los registros DNS en el orden en que recibe los registros del servidor. El orden de los registros presentes en la memoria caché coincide con el orden en que se reciben los registros del servidor.

A continuación, Citrix ADC cambia el orden en que se envían los registros en la respuesta DNS en un método round robin. La primera respuesta contiene el primer registro en secuencia, la segunda respuesta contiene el segundo registro en secuencia y el orden continúa en la misma secuencia. Por lo tanto, los clientes que soliciten el mismo nombre pueden conectarse a diferentes direcciones IP.

Ejemplo de DNS de Round Robin

Como ejemplo de DNS por turnos, considere los registros DNS que se han agregado de la siguiente manera:

```
1   add dns addRec ns1 1.1.1.1  add dns addRec ns1 1.1.1.2  add dns
       addRec ns1 1.1.1.3  add dns addRec ns1 1.1.1.4
2 <!--NeedCopy-->
```

El dominio, abc.com está vinculado a un registro NS de la siguiente manera:

```
1   add dns nsrec abc.com. ns1
2 <!--NeedCopy-->
```

Cuando Citrix ADC recibe una consulta para el registro A de ns1, los registros de direcciones se sirven en un método round robin de la siguiente manera. En la primera respuesta de DNS, 1.1.1.1 se sirve como el primer registro:

```
1   ns1.                    1H IN A         1.1.1.1  ns1.
                           1H IN A         1.1.1.2  ns1.
                           1H IN A         1.1.1.3  ns1.
                           1H IN A         1.1.1.4
2 <!--NeedCopy-->
```

En la segunda respuesta de DNS, la segunda dirección IP, 1.1.1.2, se sirve como el primer registro:

```
1   ns1.                    1H IN A         1.1.1.2  ns1.
                           1H IN A         1.1.1.3  ns1.
                           1H IN A         1.1.1.4  ns1.
                           1H IN A         1.1.1.1
2 <!--NeedCopy-->
```

En la tercera respuesta de DNS, la tercera dirección IP, 1.1.1.2, se sirve como el primer registro:


```
1   ns1.                    1H IN A         1.1.1.3  ns1.
                           1H IN A         1.1.1.4  ns1.
                           1H IN A         1.1.1.1  ns1.
                           1H IN A         1.1.1.2
2 <!--NeedCopy-->
```

Configurar registros de recursos DNS

June 22, 2022

Los registros de recursos se configuran en el dispositivo Citrix® ADC cuando se configura el dispositivo como un servidor ADNS para una zona. También puede configurar registros de recursos en el dispositivo si los registros de recursos pertenecen a una zona para la que el dispositivo es un servidor proxy DNS. En el dispositivo, puede configurar los siguientes tipos de registro:

- Registros de servicio
- Registros AAAA
- registros de direcciones
- Registros de intercambio de correo
- Registros del servidor de nombres
- Registros canónicos
- Registros de punteros
- Registros NAPTR
- Inicio de registros de autoridad
- Registros de texto
- Registros de autorización de la entidad de certificación (CAA)

En la siguiente tabla se enumeran los tipos de registro que puede configurar para un registro de nombre de dominio en el dispositivo Citrix ADC. Por ejemplo, puede configurar un máximo de 25 direcciones IP para un registro.

Tabla 1. Tipo y número de registro configurables

Tipo de registro	Número de registros
Dirección (A)	25
IPv6 (AAAA)	5
Intercambio de correo (MX)	12
Servidor de nombres (NS)	16

Tipo de registro	Número de registros
Servicio (SRV)	8
Puntero (PTR)	20
Nombre canónico (CNAME)	1
Inicio de la autoridad (SOA)	1
Texto (TXT)	20
Puntero de autoridad de nomenclatura (NAPTR)	20
Autorización de la entidad de certificación (CAA)	20

> **Nota:**
>
> El número máximo de direcciones IP para un nombre de host específico es 25. Sin embargo, el número de registros de direcciones diferentes puede ser superior a 25.

Crear registros SRV para un servicio

February 16, 2021

El registro SRV proporciona información sobre los servicios disponibles en el dispositivo Citrix ADC. Un registro SRV contiene la siguiente información:

- Nombre del servicio y del protocolo
- Nombre del dominio
- TTL
- Clase DNS
- Prioridad del objetivo
- Peso de los registros con la misma prioridad
- Puerto del servicio
- Nombre de host del servicio.

El Citrix ADC elige primero el registro SRV que tiene la configuración de prioridad más baja. Si un servicio tiene varios registros SRV con la misma prioridad, los clientes utilizan el campo de peso para determinar qué host utilizar.

Agregar un registro SRV mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para agregar un registro SRV y verificar la configuración:

```
1 -  add dns srvRec <domain> <target> -priority <positive_integer> -
     weight <positive_integer> -port <positive_integer> [-TTL <secs>]
2 -  sh dns srvRec <domain>
3 <!--NeedCopy-->
```

Ejemplo:

```
1 > add dns srvRec _http._tcp.example.com nameserver1.com -priority 1 -
     weight 1 -port 80
2  Done
3 > show dns srvRec _http._tcp.example.com
4 1)      Domain Name : _http._tcp.example.com
5         Target Host : nameserver1.com
6         Priority : 1    Weight : 1
7         Port : 80       TTL : 3600 secs
8  Done
9 <!--NeedCopy-->
```

Modificar o quitar un registro SRV mediante la CLI

- Para modificar un registro SRV, escriba:
  - El `set dns srvRec` comando
  - El nombre del dominio para el que está configurado el registro SRV
  - El nombre del host de destino que aloja el servicio asociado
  - Los parámetros a cambiar, con sus nuevos valores
- Para quitar un registro SRV, escriba:
  - El `rm dns srvRec` comando
  - El nombre del dominio para el que está configurado el registro SRV
  - El nombre del host de destino que aloja el servicio asociado

Configurar un registro SRV mediante la interfaz gráfica de usuario

Vaya a **Administración del tráfico > DNS > Registros > Registros SRV** y cree un registro SRV.

Crear registros AAAA para un nombre de dominio

February 16, 2021

Un registro de recursos AAAA almacena una única dirección IPv6.

Agregar un registro AAAA mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para agregar un registro AAAA y verificar la configuración:

```
1 -  add dns aaaaRec <hostName> <IPv6Address> ... [-TTL <secs>]
2 -  show dns aaaaRec <hostName>
3 <!--NeedCopy-->
```

Ejemplo:

```
1 > add dns aaaaRec www.example.com 2001:0db8:0000:0000:0000:0000:1428:57
     ab
2  Done
3 > show dns aaaaRec www.example.com
4 1)      Host Name : www.example.com
5         Record Type : ADNS              TTL : 5 secs
6         IPV6 Address : 2001:db8::1428:57ab
7  Done
8 <!--NeedCopy-->
```

Para quitar un registro AAAA y todas las direcciones IPv6 asociadas con el nombre de dominio, escriba el `rm dns aaaaRec` comando y el nombre de dominio para el que está configurado el registro AAAA. Para quitar solo un subconjunto de las direcciones IPv6 asociadas al nombre de dominio en un registro AAAA, escriba lo siguiente:

- `rm dns aaaaRec` comando
- El nombre de dominio para el que está configurado el registro AAAA
- Las direcciones IPv6 que desea quitar

Agregue un registro AAAA mediante la interfaz gráfica de usuario

Vaya a **Administración de Tráfico > DNS > Registros > Registros AAAA** y cree un registro AAAA.

Crear registros de direcciones para un nombre de dominio

February 16, 2021

Los registros de direcciones (A) son registros DNS que asignan un nombre de dominio a una dirección IPv4.

No se pueden eliminar los registros de direcciones de un host que participa en el equilibrio de carga global del servidor (GSLB). Sin embargo, Citrix ADC elimina los registros de direcciones agregados para dominios GSLB cuando se desvincula el dominio de un servidor virtual GSLB. Solo los registros configurados por el usuario se pueden eliminar manualmente. No se puede eliminar un registro de un host al que se hace referencia en registros como NS, MX o CNAME.

Agregar un registro de direcciones mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para agregar un registro de dirección y verificar la configuración:

```
-  add dns addRec <hostName> <IPAddress> [-TTL <secs>]
-  show dns addRec <hostName>
<!--NeedCopy-->
```

Ejemplo:

```
> add dns addRec ns.example.com 192.0.2.0
 Done
> show dns addRec ns.example.com
1)      Host Name : ns.example.com
        Record Type : ADNS                      TTL : 5 secs
        IP Address : 192.0.2.0
 Done
<!--NeedCopy-->
```

Para quitar un registro de direcciones y todas las direcciones IP asociadas al nombre de dominio, escriba el `rm dns addRec` comando y el nombre de dominio para el que está configurado el registro de direcciones. Para quitar solo un subconjunto de las direcciones IP asociadas al nombre de dominio en un registro de direcciones, escriba lo siguiente:

- `rm dns addRec` comando
- El nombre de dominio para el que está configurado el registro de dirección
- Las direcciones IP que desea quitar

Agregar un registro de direcciones mediante la interfaz gráfica de usuario

Vaya a **Administración de Tráfico > DNS > Registros > Registros de direcciones** y cree un registro de direcciones.

Crear registros MX para un servidor de intercambio de correo

February 16, 2021

Los registros de Exchange de correo (MX) se utilizan para dirigir mensajes de correo electrónico a través de Internet. Un registro MX contiene una preferencia MX que especifica el servidor MX que se va a utilizar. Los valores de preferencia MX oscilan entre 0 y 65536. Un registro MX contiene un número de preferencia MX único. Puede establecer la preferencia MX y los valores TTL para un registro MX.

Cuando se envía un mensaje de correo electrónico a través de Internet, un agente de transferencia de correo envía una consulta DNS solicitando el registro MX para el nombre de dominio. Esta consulta devuelve una lista de nombres de host de servidores de intercambio de correo para el dominio, junto con un número de preferencia. Si no hay registros MX, se realiza la solicitud para el registro de dirección de ese dominio. Un solo dominio puede tener varios servidores de intercambio de correo.

Agregar un registro MX mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para agregar un registro MX y verificar la configuración:

```
- add dns mxRec <domain> -mx <string> -pref <positive_integer> [-TTL <
   secs>]
- show dns mxRec <domain>
<!--NeedCopy-->
```

Ejemplo:

```
> add dns mxRec example.com -mx mail.example.com -pref 1
 Done
> show dns mxRec example.com
1)      Domain : example.com    MX Name : mail.example.com
        Preference :   1        TTL : 5 secs
 Done
<!--NeedCopy-->
```


Modificar o quitar un registro MX mediante la CLI

- Para modificar un registro MX, escriba el `set dns mxRec` comando, el nombre del dominio para el que está configurado el registro MX, el nombre del registro MX y los parámetros que se van a cambiar, con sus nuevos valores.
- Para establecer el parámetro TTL en su valor predeterminado, escriba el `unset dns mxRec` comando, el nombre del dominio para el que está configurado el registro MX, el nombre del registro MX y -TTL sin ningún valor TTL. Puede utilizar el `unset dns mxRec` comando para desestablecer solo el parámetro TTL.
- Para quitar un registro MX, escriba el `rm dns mxRec` comando, el nombre del dominio para el que está configurado el registro MX y el nombre del registro MX.

Agregar un registro MX mediante la interfaz gráfica de usuario

Vaya a **Administración de tráfico > DNS > Registros > Registros de intercambio de correo** y cree un registro MX.

Crear registros NS para un servidor autorizado

February 16, 2021

Los registros del servidor de nombres (NS) especifican el servidor autorizado de un dominio. Puede configurar un máximo de 16 registros NS. Puede utilizar un registro NS para delegar el control de un subdominio en un servidor DNS.

Crear un registro NS mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para crear un registro NS y verificar la configuración:

```
1 -  add dns nsRec <domain> <nameServer> [-TTL <secs>]
2 -  show dns nsRec <domain>
3 <!--NeedCopy-->
```

Ejemplo:

```
1 > add dns nsRec example.com nameserver1.example.com
2  Done
```



```
> show dns nsRec example.com
1)      Domain : example.com    NameServer : nameserver1.example.com
        TTL : 5 sec
 Done
<!--NeedCopy-->
```

Para quitar un registro NS, escriba el `rm dns nsRec` comando, el nombre del dominio al que pertenece el registro NS y el nombre del servidor de nombres.

Crear un registro NS mediante la interfaz gráfica de usuario

Vaya a **Administración del tráfico > DNS > Registros > Registros del servidor de nombres** y cree un registro NS.

Crear registros CNAME para un subdominio

February 16, 2021

Un registro de nombre canónico (registro CNAME) es un alias para un nombre DNS. Estos registros son útiles cuando varios servicios consultan el servidor DNS. El host que tiene un registro de dirección (A) no puede tener un registro CNAME.

A veces, un dispositivo Citrix ADC en modo proxy solicita un registro de direcciones desde la caché en lugar del servidor.

Agregar un registro CNAME mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para crear un registro CNAME y compruebe la configuración:

```
-  add dns cnameRec <aliasName> <canonicalName> [-TTL <secs>]
-  show dns cnameRec <aliasName>
<!--NeedCopy-->
```

Ejemplo:

```
> add dns cnameRec www.example.com www.examplenw.com
 Done
> show dns cnameRec www.example.com
```



```
4          Alias Name      Canonical Name  TTL
5 1)       www.example.com        www.examplenw.com       5 secs
6  Done
7 <!--NeedCopy-->
```

Para quitar un registro CNAME de un dominio determinado, escriba el `rm dns cnameRec` comando y el alias del nombre de dominio.

Agregar un registro CNAME mediante la interfaz gráfica de usuario

Vaya a **Administración de Tráfico > DNS > Registros > Registros Canónicos** y cree un registro CNAME.

Caché registros CNAME

Cuando se implementa en modo proxy, el dispositivo ADC no siempre envía la consulta para un registro de direcciones al servidor back-end. Este comportamiento se produce cuando para una respuesta a una consulta para un registro de direcciones, una cadena CNAME parcial está presente en la caché. Hay pocas condiciones en las que ADC almacena en caché el registro CNAME parcial y sirve la consulta desde la caché. Las siguientes son las condiciones:

- Citrix ADC debe implementarse en modo proxy.
- La respuesta del servidor back-end debe tener una cadena CNAME, para la cual el tipo de registro de la última entrada en la sección de respuesta debe ser CNAME y el tipo de pregunta no CNAME.
- La respuesta del servidor back-end no puede ser un dominio sin datos o NX.
- La respuesta del servidor back-end tiene que ser una respuesta autorizada.

Crear registros NAPTR para el dominio de telecomunicaciones

February 16, 2021

NAPTR (Naming Address Pointer) es uno de los registros DNS más utilizados en el dominio de telecomunicaciones. Los registros NAPTR asignan el espacio de direcciones de telefonía de Internet al espacio de direcciones de Internet. Por lo tanto, permiten que un dispositivo móvil envíe una solicitud al servidor correcto. La combinación de registros NAPTR con registros de servicio (SRV) permite encadenar varios registros para formar reglas de reescritura complejas que producen nuevas etiquetas de dominio o identificadores de recursos uniformes (URI). El código DNS para NAPTR es 35.

Los ADC de Citrix admiten NAPTR en dos modos: Modo ADNS y modo proxy. En el modo proxy, el ADC almacena en caché la respuesta de los servidores y utiliza los registros almacenados en caché para las

consultas futuras del servidor. Se puede agregar un máximo de 20 registros NAPTR para un dominio concreto en Citrix ADC. Citrix ADC almacena en caché la respuesta a una consulta de registro NAPTR DNS. Cualquier solicitud posterior para el registro NAPTR se sirve desde la caché.

Crear un registro NAPTR mediante CLI

En el símbolo del sistema, escriba los siguientes comandos para agregar un registro NAPTR y verificar la configuración:

```
add dns naptrRec <order> <preference>[flags<string>][services<string>](
regexp<expressions>|-replacement<string>)[-TTL<secs>]
```

Quitar un registro NAPTR mediante CLU

```
rm dns naptrRec<domain> (<order> <preference> [-flags <string>] [-services
 <string>] (-regexp <expression> | -replacement <string>))| -recordId <
positive_integer>@)
```

Configurar un registro NAPTR mediante GUI

Vaya a **Administración del Tráfico > DNS > Registros > Registros NAPTR** y cree un registro NAPTR.

Crear registros PTR para direcciones IPv4 e IPv6

February 16, 2021

Un registro de puntero (PTR) traduce una dirección IP a su nombre de dominio. Los registros PTR IPv4 están representados por los octetos de una dirección IP en orden inverso con la cadena “in-addr.arpa.” anexado al final. Por ejemplo, el registro PTR para la dirección IP 1.2.3.4 es 4.3.2.1.in-addr.arpa.

Las direcciones IPv6 se asignan de forma inversa bajo el dominio IP6.ARPA. Los mapas inversos de IPv6 utilizan una secuencia de mordiscos separados por puntos con el sufijo “.IP6.ARPA” tal como se define en RFC 3596. Por ejemplo, el nombre de dominio de búsqueda inversa correspondiente a la dirección, 4321:0:1:2:3:4:567:89ab sería b.a.9.8.7.6.5.0.4.0.0.0.3.0.0.0.2.0.0.0.1.0.0.0.0.0.0.0.1.2.3.4.IP6.ARPA.

Agregar un registro PTR mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para agregar un registro PTR y verificar la configuración:


```
1 -  add dns ptrRec <reverseDomain> <domain> [-TTL <secs>]
2 -  show dns ptrRec <reverseDomain>
3 <!--NeedCopy-->
```

Ejemplo:

```
1 > add dns ptrRec 0.2.0.192.in-addr.arpa example.com
2  Done
3 > show dns ptrRec 0.2.0.192.in-addr.arpa
4 1)      Reverse Domain Name : 0.2.0.192.in-addr.arpa
5         Domain Name : example.com              TTL : 3600 secs
6  Done
7 <!--NeedCopy-->
```

Para quitar un registro PTR, escriba el `rm dns ptrRec` comando y el nombre de dominio inverso asociado al registro PTR

Agregar un registro PTR mediante la interfaz gráfica de usuario

Vaya a **Administración de Tráfico > DNS > Registros > Registros PTR** y cree un registro PTR.

Crear registros SOA para información autorizada

February 16, 2021

Un registro de inicio de autoridad (SOA) solo se crea en el vértice de la zona y contiene información sobre la zona. El registro incluye, entre otros parámetros, el servidor de nombres principal, la información de contacto (correo electrónico) y los valores predeterminados (mínimo) de tiempo de vida (TTL) para los registros.

Crear un registro SOA mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para agregar un registro SOA y verificar la configuración:

```
1 -  add dns soaRec <domain> -originServer <originServerName> -contact <
     contactName>
2 -  sh dns soaRec <do main>
```



```
<!--NeedCopy-->
```

Ejemplo:

```
> add dns soaRec example.com -originServer nameserver1.example.com -
   contact admin.example.com
 Done
> show dns soaRec example.com
1)      Domain Name : example.com
        Origin Server : nameserver1.example.com
        Contact : admin.example.com
        Serial No. : 100        Refresh : 3600 secs     Retry : 3 secs
        Expire : 3600 secs      Minimum : 5 secs        TTL : 3600 secs
 Done
<!--NeedCopy-->
```

Modificar o quitar un registro SOA mediante la CLI

- Para modificar un registro SOA, escriba el comando `set dns soaRec`, el nombre del dominio para el que está configurado el registro y los parámetros que se van a cambiar, con sus nuevos valores.
- Para quitar un registro SOA, escriba el comando `rm dns soaRec` y el nombre del dominio para el que está configurado el registro.

Configurar un registro SOA mediante la interfaz gráfica de usuario

Vaya a **Administración del tráfico > DNS > Registros > Registros SOA** y cree un registro SOA.

Crear registros TXT para contener texto descriptivo

February 16, 2021

Los hosts de dominio almacenan registros TXT con fines informativos. El componente RDATA de un registro TXT, que consiste en una o más cadenas de caracteres de longitud variable, puede almacenar prácticamente cualquier información que un destinatario pueda necesitar saber sobre el dominio. También puede incluir información sobre el proveedor de servicios, la persona de contacto, las direcciones de correo electrónico y los detalles asociados. La protección SPF (Sender Policy Framework) ha sido el caso de uso más destacado para el registro TXT.

Todos los tipos de configuración (DNS autoritario, proxy DNS, solucionador final y reenviador) del dispositivo Citrix ADC admiten registros TXT. Puede agregar un máximo de 20 registros de recursos TXT a un dominio. Cada registro de recurso se almacena con un identificador de registro único generado internamente. Puede ver el ID de un registro y utilizarlo para eliminarlo. Sin embargo, no puede modificar un registro de recursos TXT.

Crear un registro de recursos TXT mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para crear un registro de recursos TXT y compruebe la configuración:

```
1 -  add dns txtRec <domain> <string> ... [-TTL <secs>]
2 -  show dns txtRec [<domain> | -type <type>]
3 <!--NeedCopy-->
```

Ejemplo:

```
1 > add dns txtRec www.example.com "Contact: Mark" "Email: mark@example.
     com" -TTL 36000
2  Done
3 > show dns txtRec www.example.com
4 1)  Domain : www.example.com    Record id: 13783       TTL : 36000 secs
      Record Type : ADNS
5         "Contact: Mark"
6         "Email: mark@example.com"
7  Done
8 <!--NeedCopy-->
```

Quitar un registro de recursos TXT mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para quitar un registro de recursos TXT y verificar la configuración:

```
1 -  rm dns txtRec <domain> (<string> ... | -recordId <positive_integer>)
2 -  show dns txtRec [<domain> | -type <type>]
3 <!--NeedCopy-->
```


Ejemplo:
Puede utilizar el `show dns txtRec` comando primero para ver el Id. de registro del registro de recursos TXT que desea quitar, como se muestra:

```
> show dns txtRec www.example.com
1)  Domain : www.example.com    Record id: 36865       TTL : 36000 secs
     Record Type : ADNS
         ”Contact: Evan”
         ”Email: evan@example.com”
2)  Domain : www.example.com    Record id: 14373       TTL : 36000 secs
     Record Type : ADNS
         ”Contact: Mark”
         ”Email: mark1@example.com”
 Done
<!--NeedCopy-->
```

El método más simple de eliminar un registro TXT es usar el ID de registro. Si quiere proporcionar las cadenas, introdúzcalas en el orden en que se almacenan en el registro. En el ejemplo siguiente, el registro TXT se elimina mediante su ID de registro.

```
>rm dns txtRec www.example.com -recordID 36865
 Done
> show dns txtRec www.example.com
1)  Domain : www.example.com    Record id: 14373       TTL : 36000 secs
     Record Type : ADNS
         ”Contact: Mark”
         ”Email: mark1@example.com”
 Done
<!--NeedCopy-->
```

Configurar un registro TXT mediante la interfaz gráfica de usuario

Vaya a **Administración de tráfico > DNS > Registros > Registros TXT** y cree un registro TXT.

Crear registros de la CAA para un nombre de dominio

June 22, 2022

La autorización de la entidad de certificación (CAA) es un tipo de registro DNS que permite a los propietarios del dominio especificar qué entidad de certificación (CA) puede emitir certificados SSL para el dominio.

Una conexión segura a un servicio requiere certificados SSL/TLS para garantizar la identidad del host y establecer un canal seguro. No tener registros de la CAA puede provocar un riesgo de seguridad, ya que cualquiera puede generar una solicitud de firma de certificado (CSR) para el dominio y obtener la firma del certificado por cualquier CA.

Los registros de la CAA proporcionan una capa adicional de protección a su presencia en la web al permitir que el propietario del dominio declare qué entidades de certificación están autorizadas a emitir un certificado para el dominio. Si hay una solicitud de certificado de una CA no autorizada, el registro de la CAA notifica al propietario del dominio al respecto. Si un registro de la CAA no está presente para un dominio, cualquier CA puede emitir el certificado para ese dominio.

El dispositivo Citrix ADC admite registros CAA de DNS en los siguientes modos:

- **Proxy**: el dispositivo almacena en caché la respuesta de registro de la CAA de los servidores back-end y responde a consultas adicionales del mismo tipo desde la caché.
- **ADNS**: el dispositivo responde a las consultas DNS de tipo de registro de la CAA de los registros DNS configurados.

Nota:

> - Puede agregar un máximo de 20 registros de la CAA por nombre de dominio.
> - No se admiten los modos de resolución recursiva y reenviador.

Agregar un registro de CAA mediante la CLI

En el símbolo del sistema, escriba el siguiente comando:

```
1 add dns caaRec <domain> <issuer-string> -tag <tag-string> -flag [None|
     Critical] [-TTL <secs>]
2 <!--NeedCopy-->
```

Ejemplo:

```
1 > add dns caaRec newdomain string1 -tag Issue -flag None [-TTL 3600]
2 <!--NeedCopy-->
```

Mostrar detalles del comando


```
> show dns caaRec

1)  Domain : newdomain  ECS Subnet : None      Record id: 39423 TTL : 3600 secs Record Type : ADNS

Value: string1

Tag: issue

Flag: NONE

2)  Domain : test.com  ECS Subnet : None      Record id: 2572   TTL : 5 secs    Record Type : ADNS

Value: ca1.test.com

Tag: issue

Flag: NONE
<!--NeedCopy-->
```

Para eliminar un registro CAA, escriba el siguiente comando en el símbolo del sistema:

```
rm dns caaRec <domain> <issuer-string> -tag <tag-string> | -recordId <positive_integer>@)
<!--NeedCopy-->
```

Ejemplo:

```
rm dns caaRec newdomain -recordId 39423
<!--NeedCopy-->
```

> **Nota:**
>
> - ID de registro @ no se admite en un clúster.

Agregar un registro de CAA mediante la interfaz gráfica de usuario

Vaya a **Administración del tráfico > DNS > Registros > Registros de la CAA** y cree un registro de direcciones.

Ver estadísticas de DNS

February 16, 2021

Puede ver las estadísticas DNS generadas por el dispositivo Citrix ADC. Las estadísticas DNS incluyen estadísticas de tiempo de ejecución, configuración y error.

Ver estadísticas de registros DNS mediante la CLI

En el símbolo del sistema, escriba:

```
stat dns
```

Ejemplo:

```
> stat dns
DNS Statistics

Runtime Statistics
Dns queries                             21
NS queries                               8
SOA queries                             18
.
.
.
Configuration Statistics
AAAA records                            17
A records                               36
MX records                               9
.
.
.
Error Statistics
Nonexistent domain                      17
No AAAA records                          0
No A records                            13
.
.
.
Done
<!--NeedCopy-->
```


Ver estadísticas de registros DNS mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > DNS**.
2. En el panel de detalles, haga clic en **Estadísticas**.

Configurar una zona DNS

August 20, 2021

Una entidad de zona DNS en el dispositivo Citrix ADC facilita la propiedad de un dominio en el dispositivo. Una zona del dispositivo también permite implementar Extensiones de seguridad DNS (DNSSEC) para la zona o descargar las operaciones DNSSEC de la zona desde los servidores DNS al dispositivo. Las operaciones de firma DNSSEC se realizan en todos los registros de recursos de una zona DNS. Por lo tanto, si quiere firmar una zona o si quiere descargar operaciones DNSSEC para una zona, primero debe crear la zona en el dispositivo Citrix ADC.

Cree una zona DNS en el dispositivo en los siguientes casos:

- El dispositivo Citrix ADC posee todos los registros de una zona, es decir, el dispositivo funciona como servidor DNS autorizado para la zona. La zona debe crearse con el parámetro ProxyMode establecido en NO.
- El dispositivo Citrix ADC solo posee un subconjunto de los registros de una zona. Todos los demás registros de recursos de la zona están alojados en un conjunto de servidores de nombres back-end. El dispositivo está configurado como servidor proxy DNS para estos servidores back-end. Una configuración típica en la que el dispositivo Citrix ADC posee solo un subconjunto de registros de recursos en la zona es una configuración global de equilibrio de carga del servidor (GSLB). El dispositivo Citrix ADC solo posee los nombres de dominio GSLB, mientras que los servidores de nombres back-end poseen todos los demás registros. La zona debe crearse con el parámetro ProxyMode establecido en YES.
- Quiere descargar operaciones DNSSEC para una zona desde los servidores DNS autorizados al dispositivo. La zona debe crearse con el parámetro ProxyMode establecido en YES. Es posible que tenga que configurar más opciones para la zona.

El tema actual describe cómo crear una zona para los dos primeros casos. Para obtener más información sobre cómo configurar una zona para descargar operaciones DNSSEC en el dispositivo, consulte Descarga de operaciones DNSSEC al dispositivo Citrix ADC.

> **Nota**
>
> Si el dispositivo ADC funciona como servidor DNS autorizado para una zona, debe crear los registros de inicio de autoridad (SOA) y servidor de nombres (NS) para la zona antes de crear la zona. Si Citrix ADC funciona como servidor proxy DNS para una zona, los registros SOA y NS no deben

> crearse en el dispositivo Citrix ADC. Para obtener más información sobre la creación de registros SOA y NS, consulte Configurar registros de recursos DNS.

Al crear una zona, todos los nombres de dominio y registros de recursos existentes que terminan con el nombre de la zona se tratan automáticamente como parte de la zona. Además, todos los nuevos registros de recursos creados con un sufijo que coincida con el nombre de la zona se incluyen implícitamente en la zona.

Cree una zona DNS en el dispositivo Citrix ADC mediante la CLI

En el símbolo del sistema, escriba el comando siguiente para agregar una zona DNS al dispositivo Citrix ADC y compruebe la configuración:

```
-  add dns zone <zoneName> -proxyMode ( YES | NO )
-  show dns zone [<zoneName> | -type <type>]
<!--NeedCopy-->
```

Ejemplo:

```
> add dns zone example.com -proxyMode Yes
 Done
> show dns zone example.com
          Zone Name : example.com
          Proxy Mode : YES
Done
<!--NeedCopy-->
```

Modificar o quitar una zona DNS mediante la CLI

- Para modificar una zona DNS, escriba el comando `set dns zone`, el nombre de la zona DNS y los parámetros que se van a cambiar, con sus nuevos valores.
- Para quitar una zona DNS, escriba el `rm dns zone` comando y el nombre de la zona DNS.

Configurar una zona DNS mediante la interfaz gráfica de usuario

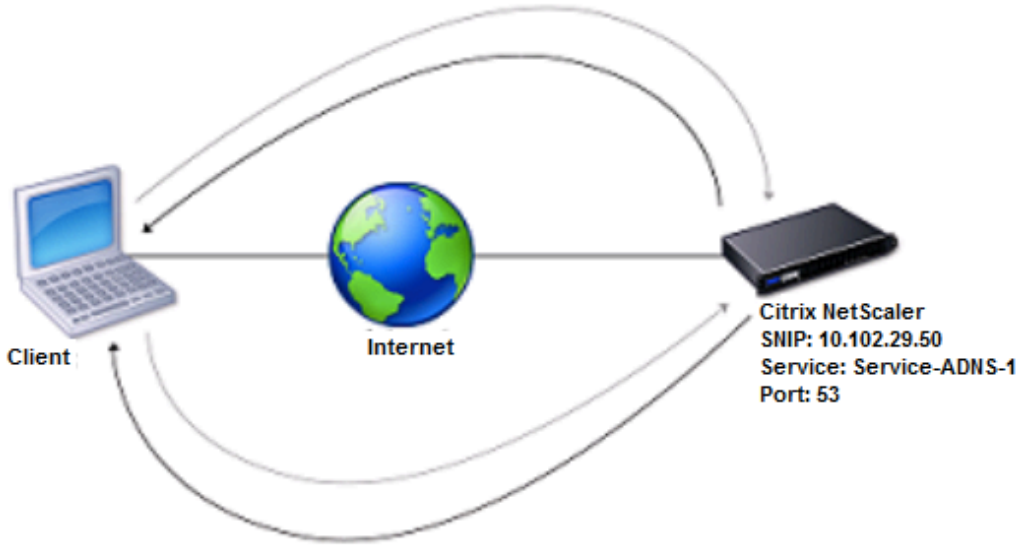
Vaya a **Administración de tráfico > DNS > Zonas** y cree una zona DNS.

Configurar Citrix ADC como un servidor ADNS

August 20, 2021

Puede configurar el dispositivo ADC para que funcione como un servidor de nombres de dominio autorizado (ADNS) para un dominio. Como servidor ADNS para un dominio, Citrix ADC resuelve las solicitudes DNS para todos los tipos de registros DNS que pertenecen al dominio. Para configurar Citrix ADC para que funcione como un servidor ADNS para un dominio, debe crear un servicio ADNS y configurar los registros NS y Address para el dominio en Citrix ADC. El servicio ADNS se puede configurar mediante la dirección IP de subred (SNIP) o una dirección IP independiente. El siguiente diagrama de topología muestra una configuración de ejemplo y el flujo de solicitudes y respuestas.

Ilustración 1. Citrix ADC como ADNS



En la tabla siguiente se muestran los parámetros configurados para el servicio ADNS ilustrados en el diagrama de topología anterior.

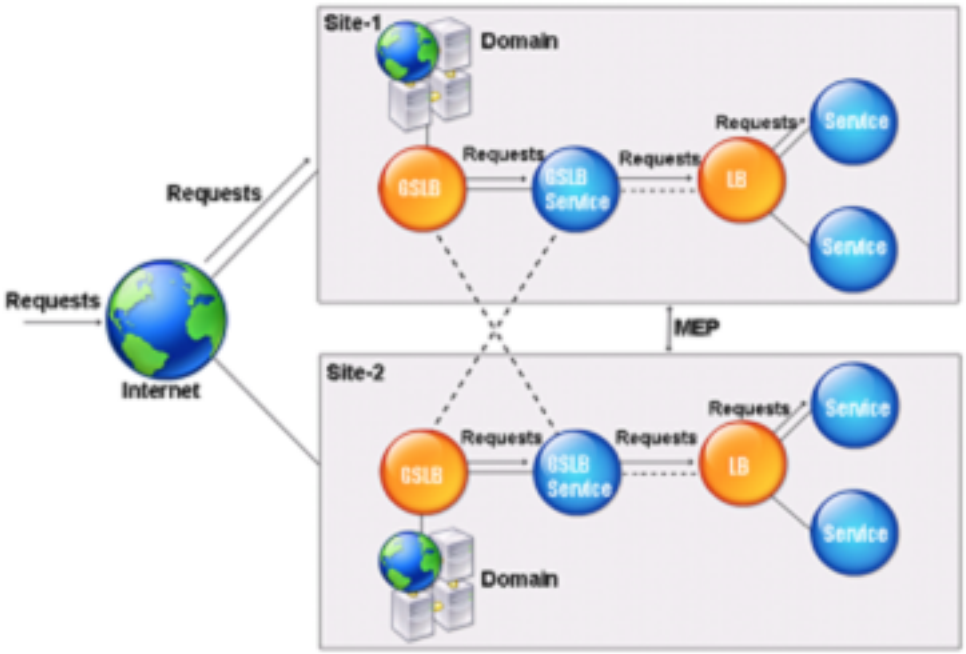
Tipo de entidad	Nombre	Dirección IP	Tipo	Port
Servicio ADNS	Service-ADNS-1	10.102.29.51	ADNS	53

Cuadro 1 Ejemplo de configuración del servicio ADNS

Para configurar una configuración de ADNS, debe configurar el servicio de ADNS. Para obtener instrucciones sobre cómo configurar el servicio ADNS, consulte Equilibrio de carga.

Durante la resolución de DNS, el servidor ADNS dirige al proxy DNS o al servidor DNS local para que consulten a Citrix ADC la dirección IP del dominio. Dado que Citrix ADC es autoritativo para el dominio, envía la dirección IP al proxy DNS o al servidor DNS local. El siguiente diagrama describe la ubicación y el rol del servidor ADNS en una configuración GSLB.

Ilustración 2. Modelo de entidad GSLB



Nota: En modo ADNS, si elimina registros SOA y ADNS, los siguientes elementos no funcionan para el dominio alojado por Citrix ADC: CUALQUIER consulta (para obtener más información sobre la consulta ANY, consulte consulta DNSANY) y respuestas negativas, como NODATA y NXDOMAIN.

Crear un servicio de ADNS

Un servicio ADNS se utiliza para el equilibrio de carga de servicio global. Para obtener más información sobre cómo crear una configuración de GSLB, consulte Equilibrio de carga global del servidor. Puede agregar, modificar, habilitar, inhabilitar y quitar un servicio ADNS. Para obtener instrucciones sobre cómo crear un servicio ADNS, consulte Configurar servicios.

Nota: Puede configurar el servicio ADNS para que utilice SNIP o cualquier dirección IP nueva.

Al crear un servicio ADNS, Citrix ADC responde a las consultas DNS en el puerto y la IP del servicio ADNS configurados.

Puede verificar la configuración viendo las propiedades del servicio ADNS. Puede ver propiedades como nombre, estado, dirección IP, puerto, protocolo y conexiones de cliente máximas.

Configurar la configuración de ADNS para utilizar TCP

De forma predeterminada, algunos clientes utilizan el Protocolo de datagramas de usuario (UDP) para DNS, que especifica un límite de 512 bytes para la longitud de carga útil de los paquetes UDP. Para manejar cargas útiles que superan los 512 bytes de tamaño, el cliente debe usar TCP. Para habilitar las comunicaciones DNS a través de TCP, debe configurar el dispositivo Citrix ADC para que use el protocolo TCP para DNS. A continuación, Citrix ADC establece el bit de truncamiento en los paquetes de respuestas DNS. El bit de truncamiento especifica que la respuesta es demasiado grande para UDP y que el cliente debe enviar la solicitud a través de una conexión TCP. A continuación, el cliente utiliza el protocolo TCP en el puerto 53 y abre una nueva conexión con Citrix ADC. Citrix ADC escucha en el puerto 53 con la dirección IP del servicio ADNS para aceptar las nuevas conexiones TCP del cliente.

Para configurar Citrix ADC para que use el protocolo TCP, debe configurar un servicio ADNS_TCP. Para obtener instrucciones sobre cómo crear un servicio ADNS_TCP, consulte Equilibrio de cargas.

> **Importante**
>
> Para configurar Citrix ADC para que use UDP para DNS y utilice TCP solo cuando la longitud de carga útil de UDP supere los 512 bytes, debe configurar los servicios ADNS y ADNS_TCP. La dirección IP del servicio ADNS_TCP debe ser la misma que la dirección IP del servicio ADNS.

Agregar registros de recursos DNS

Después de crear un servicio ADNS, puede agregar registros DNS. Para obtener instrucciones sobre cómo agregar registros DNS, consulte Configurar registros de recursos DNS.

Eliminar servicios de ADNS

Para obtener instrucciones sobre cómo quitar servicios, consulte Equilibrio de carga

Configurar delegación de dominio

La delegación de dominio es el proceso de asignar la responsabilidad de una parte del espacio de dominio a otro servidor de nombres. Por lo tanto, durante la delegación de dominio, la responsabilidad de responder a la consulta se delega en otro servidor DNS. La delegación utiliza registros NS.

En el siguiente ejemplo, sub1.abc.com es el subdominio de abc.com. El procedimiento describe los pasos para delegar el subdominio en el servidor de nombres ns2.sub1.abc.com y agregar un registro de dirección para ns2.sub1.abc.com.

Para configurar la delegación de dominio, debe realizar las siguientes tareas, que se describen en las siguientes secciones:

1. Crear un registro SOA para un dominio.
2. Cree un registro NS para agregar un servidor de nombres para el dominio.
3. Cree un registro de dirección para el servidor de nombres.
4. Cree un registro NS para delegar el subdominio.
5. Cree un registro de pegamento para el servidor de nombres.

Crear un registro SOA

Para obtener instrucciones sobre cómo configurar registros SOA, consulte Crear registros SOA para obtener información autorizada.

Crear un registro NS para un servidor de nombres

Para obtener instrucciones sobre cómo configurar un registro NS, consulte Crear registros NS para un servidor autorizado. En la lista **Servidor de nombres**, seleccione el servidor de nombres autorizado principal, por ejemplo, ns1.abc.com.

Crear un registro de direcciones

Para obtener instrucciones sobre cómo configurar registros de direcciones, consulte Crear registros de direcciones para un nombre de dominio. En los cuadros de texto Nombre de host y Dirección IP, escriba el nombre de dominio para el registro de dirección DNS y la dirección IP, por ejemplo, ns1.abc.com y 10.102.11.135, respectivamente.

Crear un registro NS para la delegación de dominio

Para obtener instrucciones sobre cómo configurar registros NS, consulte Crear registros NS para un servidor autorizado. En la lista **Servidor de nombres**, seleccione el servidor de nombres autorizado principal, por ejemplo ns2.sub1.abc.com.

Crear un registro de pegamento

Los registros NS normalmente se definen inmediatamente después del registro SOA (no una restricción). Un dominio debe tener al menos dos registros NS. Si un registro NS se define dentro de un

dominio, debe tener un registro de dirección coincidente. Este registro de dirección se conoce como un registro de pegamento. Los registros de pegamento aceleran las consultas DNS.

Para obtener instrucciones sobre cómo agregar registros de pegamento para un subdominio, consulte el procedimiento para agregar un registro de dirección (A), Configurar registros de recursos DNS.

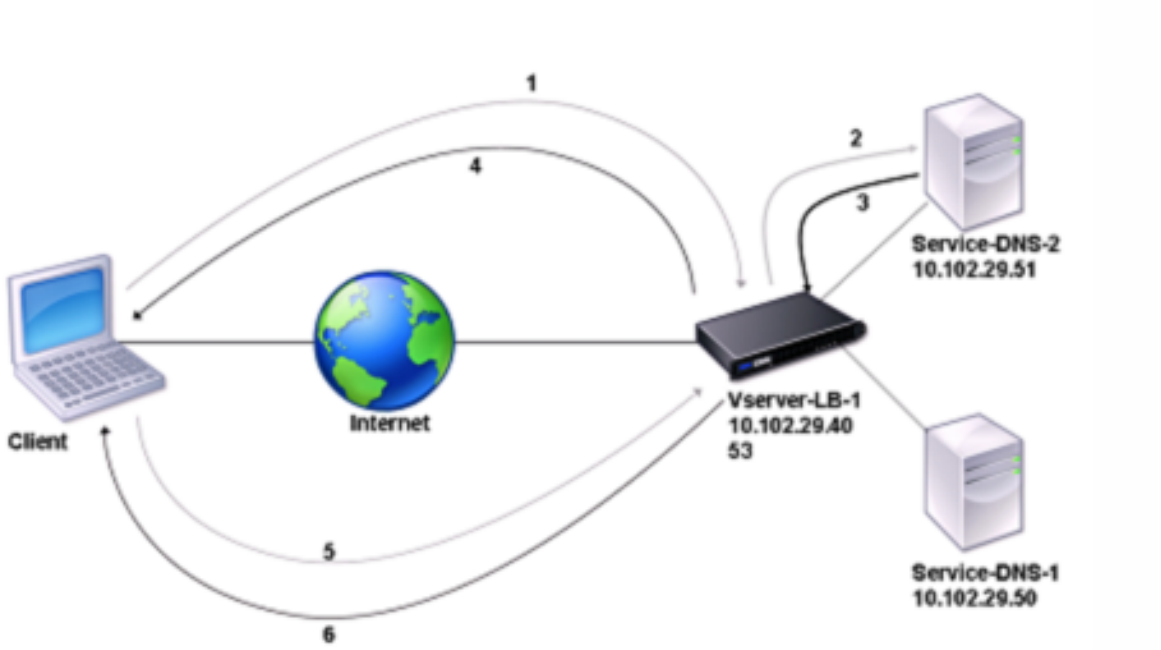
Para obtener instrucciones sobre cómo configurar registros de direcciones, consulte Crear registros de direcciones para un nombre de dominio. En los cuadros de texto Nombre de host y dirección IP, escriba el nombre de dominio para el registro de dirección DNS y la dirección IP, por ejemplo, ns2.sub1.abc.com y 10.102.12.135, respectivamente.

Configurar el dispositivo Citrix ADC como un servidor proxy DNS

August 20, 2021

Como servidor proxy DNS, el dispositivo ADC puede funcionar como proxy para un único servidor DNS o un grupo de servidores DNS. El flujo de solicitudes y respuestas se ilustra en el siguiente diagrama de topología de ejemplo.

Ilustración 1. Citrix ADC como proxy DNS



De forma predeterminada, el dispositivo Citrix ADC almacena en caché las respuestas de los servidores de nombres DNS. Cuando el dispositivo recibe una consulta DNS, comprueba el dominio consultado en su caché. Si la dirección del dominio consultado está presente en su caché, Citrix ADC devuelve la dirección correspondiente al cliente. De lo contrario, reenvía la consulta a un servidor de

nombres DNS que comprueba la disponibilidad de la dirección y la devuelve al Citrix ADC. A continuación, Citrix ADC devuelve la dirección al cliente.

Para las solicitudes de un dominio que se ha almacenado en caché anteriormente, Citrix ADC sirve el registro de direcciones del dominio desde la caché sin consultar el servidor DNS configurado.

El dispositivo descarta un registro almacenado en su caché cuando el valor de tiempo de vida (TTL) del registro alcanza el valor configurado. Un cliente que solicita un registro caducado tiene que esperar hasta que Citrix ADC recupere el registro del servidor y actualice su caché. Para evitar este retraso, Citrix ADC actualiza proactivamente la caché recuperando el registro del servidor antes de que caduque.

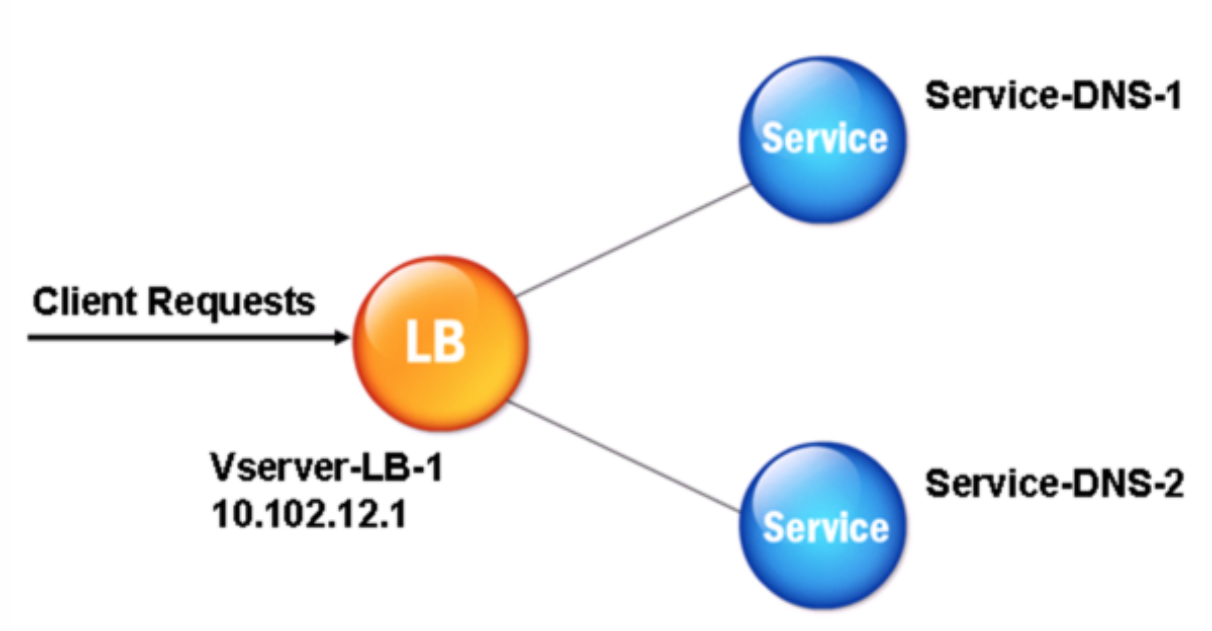
En la siguiente tabla se enumeran los nombres de ejemplo y los valores de las entidades que se deben configurar en Citrix ADC.

Cuadro 1 Ejemplo de configuración de entidad proxy DNS

Tipo de entidad	Nombre	Dirección IP	Tipo	Port
Servidor virtual LB	Vserver-DNS-1	10.102.29.40	DNS	53
Servicios	Service-DNS-1	10.102.29.50	DNS	53
Servicios	Service-DNS-2	10.102.29.51	DNS	53

El siguiente diagrama muestra las entidades de un proxy DNS y los valores de los parámetros que se configurarán en Citrix ADC.

Ilustración 2. Modelo de entidad proxy DNS



> **Nota**
>
> Para configurar la función de proxy DNS, necesita saber cómo configurar los servicios de equilibrio de carga y los servidores virtuales.

Crear un servidor virtual de equilibrio de carga

Para configurar un proxy DNS en Citrix ADC, configure un servidor virtual de equilibrio de carga de tipo DNS. Para configurar un servidor virtual DNS para equilibrar la carga de un conjunto de servidores DNS que admiten consultas recursivas, debe establecer la opción Recursión disponible. Con esta opción, el bit RA se establece en ON en las respuestas DNS del servidor virtual DNS.

Para obtener instrucciones sobre cómo crear un servidor virtual de equilibrio de carga, consulte Equilibrio de carga.

Crear servicios DNS

Después de crear un servidor virtual de equilibrio de carga de tipo DNS, debe crear servicios DNS. Puede agregar, modificar, habilitar, inhabilitar y quitar un servicio DNS. Para obtener instrucciones sobre cómo crear un servicio DNS, consulte Equilibrio de carga.

Enlazar un servidor virtual de equilibrio de carga a servicios DNS

Para completar la configuración del proxy DNS, debe vincular los servicios DNS al servidor virtual de equilibrio de carga. Para obtener instrucciones sobre cómo vincular un servicio a un servidor virtual de equilibrio de carga, consulte Equilibrio de carga.

Configurar la configuración del proxy DNS para usar TCP

Algunos clientes utilizan el Protocolo de datagramas de usuario (UDP) para las comunicaciones DNS. Sin embargo, UDP especifica un tamaño máximo de paquete de 512 bytes. Cuando las longitudes de carga útil superan los 512 bytes, el cliente debe usar TCP. Cuando un cliente envía al dispositivo Citrix ADC una consulta DNS, el dispositivo reenvía la consulta a uno de los servidores de nombres. Si la respuesta es demasiado grande para un paquete UDP, el servidor de nombres establece el bit de truncamiento en su respuesta al Citrix ADC. El bit de truncamiento indica que la respuesta es demasiado grande para UDP y que el cliente debe enviar la consulta a través de una conexión TCP. El dispositivo ADC transmite la respuesta al cliente con el bit de truncamiento intacto. Espera a que el cliente inicie una conexión TCP con la dirección IP del servidor virtual de equilibrio de carga DNS, en el puerto 53. El cliente envía la solicitud a través de una conexión TCP. A continuación, el dispositivo Citrix ADC reenvía la solicitud al servidor de nombres y transmite la respuesta al cliente.

Para configurar Citrix ADC para utilizar el protocolo TCP para DNS, debe configurar un servidor virtual de equilibrio de carga y servicios, ambos de tipo DNS_TCP. Puede configurar monitores de tipo DNS_TCP para comprobar el estado de los servicios. Para obtener instrucciones sobre cómo crear servidores virtuales, servicios y monitores DNS_TCP, consulte Equilibrio de carga.

Para actualizar los registros de forma proactiva, Citrix ADC utiliza una conexión TCP al servidor para recuperar los registros.

> **Importante**
>
> Para configurar Citrix ADC para que use UDP para DNS y utilice TCP solo cuando la longitud de carga útil de UDP supere los 512 bytes, debe configurar los servicios DNS y DNS_TCP. La dirección IP del servicio DNS_TCP debe ser la misma que la dirección IP del servicio DNS.

Configurar valores de tiempo de vida para entradas DNS

El TTL es el mismo para todos los registros DNS con el mismo nombre de dominio y tipo de registro. Si se cambia el valor TTL para uno de los registros, el nuevo valor se refleja en todos los registros del mismo nombre de dominio y tipo. El valor TTL predeterminado es 3600 segundos. El mínimo es 0 y el máximo es 604800. Si una entrada DNS tiene un valor TTL menor que el mínimo o mayor que el máximo, se guarda como valor TTL mínimo o máximo, respectivamente.

Especificar el TTL mínimo y máximo mediante la CLI

En el símbolo del sistema de Citrix ADC, escriba los siguientes comandos para especificar el TTL mínimo y máximo y verificar la configuración:

```
-  set dns parameter [-minTTL <secs>] [-maxTTL <secs>]
-  show dns parameter
<!--NeedCopy-->
```

Ejemplo:

```
> set dns parameter -minTTL 1200 -maxTTL 1800
 Done
> show dns parameter
        DNS parameters:
        DNS retries: 5
        Minimum TTL: 1200               Maximum TTL: 1800
            .
            .
```



```
9                .
10  Done
11 >
12 <!--NeedCopy-->
```

Especificar el TTL mínimo y máximo mediante la GUI

1. Vaya a **Administración del tráfico > DNS**.
2. En el panel de detalles, en Configuración, haga clic en Cambiar configuración de DNS.
3. En el cuadro de diálogo Configurar parámetros DNS, en TTL, en los cuadros de texto Mínimo y Máximo, escriba el tiempo mínimo y máximo de vida (en segundos) respectivamente y, a continuación, haga clic en Aceptar.

Nota: Cuando caduca el TTL, el registro se elimina de la caché. Citrix ADC se pone en contacto proactivamente con los servidores y obtiene el registro DNS justo antes de que caduque el registro DNS.

Vaciar registros DNS

Puede eliminar todos los registros DNS presentes en la caché. Por ejemplo, es posible que quiera vaciar los registros DNS cuando se reinicie un servidor después de realizar las modificaciones.

Eliminar todos los registros proxy mediante la CLI

En el símbolo del sistema de Citrix ADC, escriba:

```
flush dns proxyRecords
```

Eliminar todos los registros proxy mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > DNS > Registros**.
2. En el panel de detalles, haga clic en Vacar registros proxy.

Agregar registros de recursos DNS

Puede agregar registros DNS a un dominio para el que el dispositivo Citrix ADC esté configurado como servidor proxy DNS. Para obtener información sobre cómo agregar registros DNS, consulte Configuración de registros de recursos DNS.

Quitar un servidor virtual DNS de equilibrio de carga

Para obtener información sobre cómo quitar un servidor virtual de equilibrio de carga, consulte Equilibrio de carga.

Limitar el número de solicitudes DNS simultáneas en una conexión de cliente

Puede limitar el número de solicitudes DNS simultáneas en una única conexión de cliente, que es identificada por la <clientip:port>-<vserver ip:port> tupla. Las solicitudes DNS simultáneas son aquellas solicitudes que el dispositivo Citrix ADC ha reenviado a los servidores de nombres y para las que el dispositivo está esperando respuestas. Limitar el número de solicitudes simultáneas en una conexión de cliente permite proteger los servidores de nombres cuando un cliente hostil intenta un ataque de denegación de servicio distribuida (DDoS) enviando un flujo de solicitudes DNS. Cuando se alcanza el límite para una conexión de cliente, las solicitudes DNS posteriores en la conexión se eliminan hasta que el recuento de solicitudes pendientes vaya por debajo del límite. Este límite no se aplica a las solicitudes que el dispositivo Citrix ADC sirve fuera de su caché.

El valor predeterminado de este parámetro es 255. Este valor predeterminado es suficiente en la mayoría de los casos. Si los servidores de nombres atienden muchas solicitudes DNS simultáneas en condiciones normales de funcionamiento, puede especificar un valor grande o un valor de cero (0). Un valor de 0 inhabilita esta función y especifica que no hay límite para el número de solicitudes DNS permitidas en una única conexión de cliente. Este parámetro es un parámetro global y se aplica a todos los servidores virtuales DNS configurados en el dispositivo Citrix ADC.
El valor predeterminado de este parámetro es 255. Este valor predeterminado es suficiente en la mayoría de los casos. Si los servidores de nombres atienden muchas solicitudes DNS simultáneas en condiciones normales de funcionamiento, puede especificar un valor grande o un valor de cero (0). Un valor de 0 inhabilita esta función y especifica que no hay límite para el número de solicitudes DNS permitidas en una única conexión de cliente. Este parámetro es un parámetro global y se aplica a todos los servidores virtuales DNS configurados en el dispositivo Citrix ADC.
El valor predeterminado de este parámetro es 255. Este valor predeterminado es suficiente en la mayoría de los casos. Si los servidores de nombres atienden muchas solicitudes DNS simultáneas en condiciones normales de funcionamiento, puede especificar un valor grande o un valor de cero (0). Un valor de 0 inhabilita esta función y especifica que no hay límite para el número de solicitudes DNS permitidas en una única conexión de cliente. Este parámetro es un parámetro global y se aplica a todos los servidores virtuales DNS configurados en el dispositivo Citrix ADC.

Especifique el número máximo de solicitudes DNS simultáneas permitidas en una única conexión de cliente mediante la CLI

En el símbolo del sistema, escriba los comandos siguientes para especificar el número máximo de solicitudes DNS simultáneas permitidas en una única conexión de cliente y compruebe la configuración:

```
1 -  set dns parameter -maxPipeline <positive_integer>
2 -  show dns parameter
3 <!--NeedCopy-->
```


Ejemplo:

```
> set dns parameter -maxPipeline 1000
 Done
> show dns parameter
        DNS parameters:
        DNS retries: 5
        .
        .
        .
        Max DNS Pipeline Requests: 1000
 Done
<!--NeedCopy-->
```

Especifique el número máximo de solicitudes DNS simultáneas permitidas en una única conexión de cliente mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > DNS**.
2. En el panel de detalles, haga clic en Cambiar configuración DNS.
3. En el cuadro de diálogo Configurar parámetros DNS, especifique un valor para Máximo de solicitudes de proceso DNS.
4. Haga clic en Aceptar.

Configurar Citrix ADC como solución final

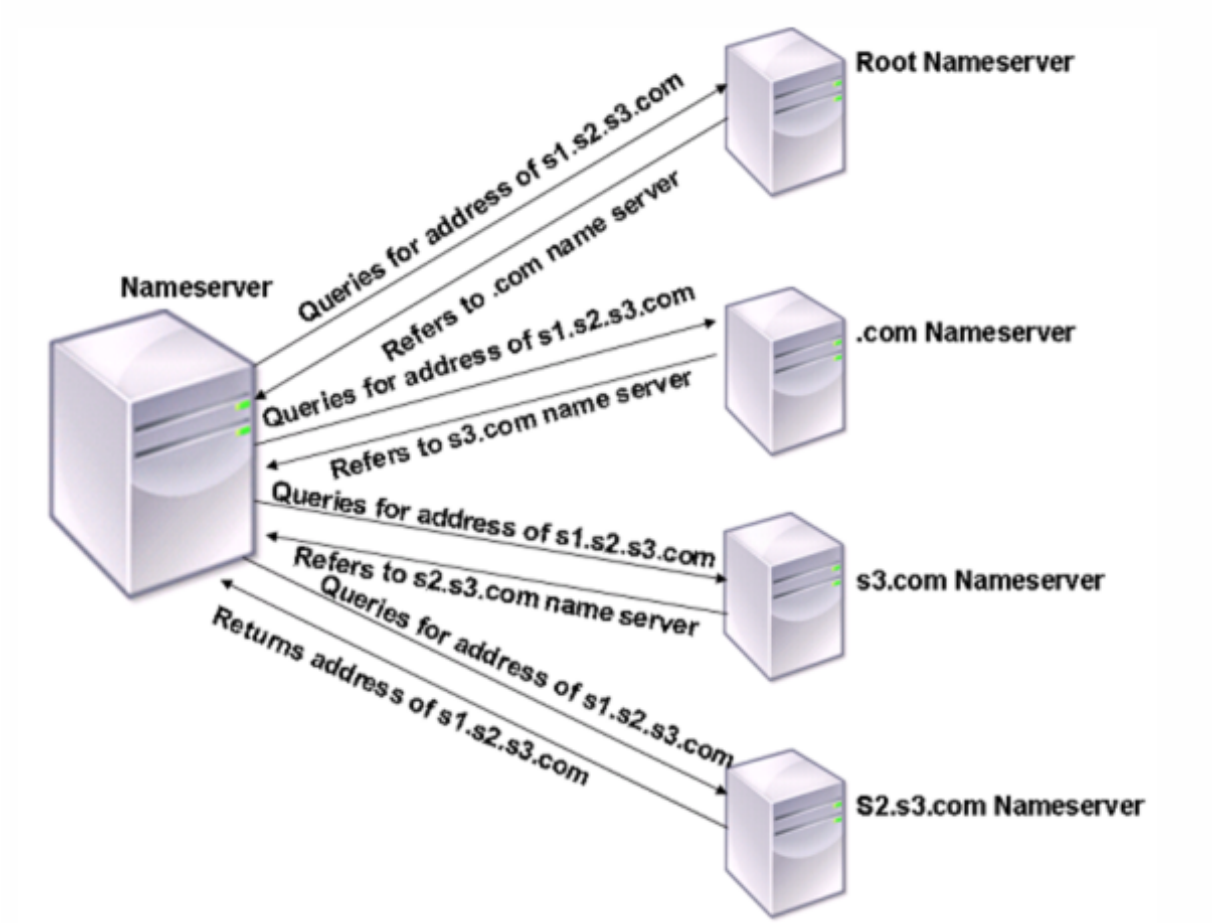
February 16, 2021

Un solucionador es un procedimiento invocado por un programa de aplicación que traduce un nombre de dominio/host a su registro de recursos. El solucionador interactúa con el LDNS, que busca el nombre de dominio para obtener su dirección IP. Citrix ADC puede proporcionar una resolución de extremo a extremo para las consultas DNS.

En la resolución recursiva, el dispositivo Citrix ADC consulta recursivamente diferentes servidores de nombres para acceder a la dirección IP de un dominio. Cuando Citrix ADC recibe una solicitud DNS, comprueba en su caché el registro DNS. Si el registro no está presente en la caché, consulta los servidores raíz configurados en el archivo ns.conf. El servidor de nombres raíz informa con la dirección de un servidor DNS que tiene información detallada sobre el dominio de segundo nivel. El proceso se repite hasta que se encuentra el registro requerido.

Al iniciar el dispositivo Citrix ADC por primera vez, se agregan 13 servidores de nombres raíz al archivo ns.conf. También se agregan los registros NS y Address para los 13 servidores raíz. Puede modificar el archivo ns.conf, pero Citrix ADC no permite eliminar los 13 registros. Se requiere al menos una entrada de servidor de nombres para que el dispositivo pueda realizar la resolución de nombres. El siguiente diagrama ilustra el proceso de resolución de nombres.

Ilustración 1. Resolución recursiva



En el proceso que se muestra en el diagrama, cuando el servidor de nombres recibe una consulta para la dirección de s1.s2.s3.com, primero comprueba los servidores de nombres raíz para s1.s2.s3.com. Un servidor de nombres raíz informa con la dirección del servidor de nombres .com. Si la dirección de s1.s2.s3.com se encuentra en el servidor de nombres, responde con una dirección IP adecuada. De lo contrario, consulta otros servidores de nombres para s3.com, luego para s2.s3.com para recuperar la dirección de s1.s2.s3.com. De esta manera, la resolución siempre comienza desde servidores de nombres raíz y termina con el servidor de nombres autorizado del dominio.

Nota: Para la funcionalidad de resolución recursiva, el almacenamiento en caché debe estar habilitado.

Habilitar resolución recursiva

Para configurar el dispositivo Citrix ADC para que funcione como resolución final, debe habilitar la resolución recursiva en el dispositivo.

Habilitar la resolución recursiva mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para habilitar la resolución recursiva y verificar la configuración:

```
-  set dns parameter -recursion ENABLED
-  show dns parameter
<!--NeedCopy-->
```

Ejemplo:

```
> set dns parameter -recursion ENABLED
 Done
> show dns parameter
        DNS parameters:
            .
            .
            .
        Recursive Resolution : ENABLED
            .
            .
            .
 Done
<!--NeedCopy-->
```

Habilitar la resolución recursiva mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > DNS**.
2. En el panel de detalles, en Configuración, haga clic en Cambiar configuración de DNS.
3. En el cuadro de diálogo Configurar parámetros DNS, active la casilla de verificación Habilitar recursión y, a continuación, haga clic en Aceptar.

Establecer el número de reintentos

Configure el dispositivo ADC para realizar un número preconfigurado de intentos (denominado reintentos DNS) cuando no reciba una respuesta del servidor al que envía una consulta. De forma predeterminada, el número de reintentos DNS se establece en 5.

Establecer el número de reintentos DNS mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para establecer el número de reintentos y verificar la configuración:

```
-  set dns parameter -retries <positive_integer>
-  show dns parameter
<!--NeedCopy-->
```

Ejemplo:

```
> set DNS parameter -retries 3
 Done
> show dns parameter
        DNS parameters:
        DNS retries: 3
            .
            .
            .
 Done
<!--NeedCopy-->
```

Establecer el número de reintentos mediante el uso de la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > DNS**.
2. En el panel de detalles, en Configuración, haga clic en Cambiar configuración de DNS.
3. En el cuadro de diálogo Configurar parámetros DNS, en el cuadro de texto Reintentos DNS, escriba el recuento de reintentos de solicitudes de resolución DNS y, a continuación, haga clic en Aceptar.

Configurar el dispositivo Citrix ADC como reenviador

June 2, 2022

Un reenviador es un servidor que reenvía consultas DNS a servidores DNS que están fuera de la red del servidor del reenviador. Las consultas que no se pueden resolver localmente se reenvían a otros servidores DNS. Un reenviador acumula información de DNS externa en su caché a medida que resuelve las consultas de DNS. Para configurar el dispositivo Citrix ADC como reenviador, debe agregar un servidor de nombres externo.

El dispositivo Citrix ADC le permite agregar servidores de nombres externos a los que puede reenviar las consultas de resolución de nombres que no se pueden resolver localmente. Para configurar el dispositivo Citrix ADC como reenviador, debe agregar los servidores de nombres a los que debe reenviar las consultas de resolución de nombres. Puede especificar la prioridad de búsqueda para especificar el servicio de nombres que el dispositivo Citrix ADC debe usar para la resolución de nombres.

Para obtener información sobre cómo configurar el dispositivo Citrix ADC como reenviador, consulte Agregar un servidor de nombres (cuando el dispositivo Citrix ADC actúa como reenviador) mediante la CLI.

> **Nota:**
>
> El dispositivo Citrix ADC en modo reenviador admite servidores de nombres TCP, UDP y UDP-TCP.
>
> - Si ha configurado un servidor de nombres TCP, el dispositivo Citrix ADC envía la solicitud de DNS a través de TCP.
> - Si ha configurado un servidor de nombres UDP, el dispositivo Citrix ADC envía la solicitud de DNS a través de UDP.
> - Si ha configurado un servidor de nombres UDP-TCP, el dispositivo Citrix ADC envía la solicitud de DNS a través de UDP. Sin embargo, si el bit truncado se establece en la respuesta DNS, el dispositivo envía dichas solicitudes DNS a través de TCP.

Agregar un servidor de nombres

August 20, 2021

Puede crear un servidor de nombres especificando su dirección IP o configurando un servidor virtual existente como servidor de nombres.

- Servidor de**nombres basado en direcciones IP: Servidor** de nombres externo al que ponerse en contacto para la resolución de nombres de dominio. Si en el dispositivo se configuran varios servidores de nombres basados en direcciones IP y el parámetro local no está establecido en

ninguno de ellos, las consultas DNS entrantes se equilibran la carga en todos los servidores de nombres, de forma round robin.

- **Servidor de nombres basado en servidor** virtual: Servidor virtual DNS configurado en Citrix ADC. Para obtener un control más detallado sobre cómo se equilibran la carga los servidores de nombres DNS externos (por ejemplo, si desea un método de equilibrio de carga que no sea round robin), haga lo siguiente:
- Configurar un servidor virtual DNS en el dispositivo
- Vincular los servidores de nombres externos como sus servicios
- Especifique el nombre del servidor virtual en este comando.

Para verificar la configuración, puede usar el comando `show dns nameServer`.

Para quitar un servidor de nombres, en la CLI de Citrix ADC, escriba el comando `rm dns nameServer` seguido de la dirección IP del servidor de nombres.

Para ver los detalles del servidor de nombres DNS, en la CLI de Citrix ADC, escriba el `show dns nameServer` comando seguido de la dirección IP del servidor de nombres.

Agregue un servidor de nombres (cuando el dispositivo Citrix ADC actúa como reenviador) mediante la CLI

En el símbolo del sistema, escriba;

```
add dns nameServer ((<IP>) | <dnsVserverName>)
<!--NeedCopy-->
```

O

```
add dns nameServer ((<IP> | <dnsVserverName>) [-type <type>]
<!--NeedCopy-->
```

Ejemplos:

```
add dns nameServer dnsVirtualNS

add dns nameServer 192.0.2.11 -type TCP

add dns nameServer 192.0.2.12 -type UDP_TCP


```



```
add dns nameServer 192.0.2.10
show dns nameServer 192.0.2.10

1) 192.0.2.10  -  State: UP  Protocol: UDP
Done
<!--NeedCopy-->
```

> **Nota:**
>
> Si no se especifica el tipo de servidor de nombres, se crea un servidor de nombres UDP de forma predeterminada. Para crear un servidor de nombres de tipo TCP o UDP_TCP, debe especificar el tipo.
>
> Cuando especifica el tipo como UDP_TCP, se crean dos servidores de nombres (un servidor de nombres UDP y un servidor de nombres TCP) para la dirección IP dada.

Agregue un servidor de nombres (cuando el dispositivo Citrix ADC actúa como solucionador) mediante la CLI

En el símbolo del sistema, escriba:

```
add dns nameServer ((<IP> [-local]) | <dnsVserverName>)
<!--NeedCopy-->
```

Ejemplo:

```
add dns nameServer 10.102.9.19 -local
show dns nameServer
1)  10.102.9.19 LOCAL -  State: UP  Protocol: UDP
Done
<!--NeedCopy-->
```

Local: Marque la dirección IP como una que pertenece a un servidor DNS recursivo local en el dispositivo Citrix ADC. El dispositivo resuelve recursivamente las consultas recibidas en una dirección IP marcada como local.
Para que la resolución recursiva funcione, también se debe establecer el parámetro DNS global, `recursion`.
Si no se marca ningún servidor de nombres como local, el dispositivo funciona como un solucionador de código auxiliar y equilibra la carga de los servidores de nombres.

Agregar un servidor de nombres mediante la interfaz gráfica de usuario

Vaya a **Administración del tráfico** > **DNS** > **Servidores de nombres** y cree un servidor de nombres.

Establecer prioridad de búsqueda DNS

January 12, 2021

Puede establecer la prioridad de búsqueda en DNS o WINS. Esta opción se utiliza en el modo de operación SSL VPN.

Establezca la prioridad de búsqueda en DNS mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para establecer la prioridad de búsqueda en DNS y verificar la configuración:

```
-  set dns parameter -nameLookupPriority (DNS | WINS)
-  show dns parameter
<!--NeedCopy-->
```

Ejemplo:

```
> set dns parameter -nameLookupPriority DNS
 Done
> show dns parameter
             .
             .
             .
         Name lookup priority : DNS
             .
             .
             .
 Done
<!--NeedCopy-->
```

Establecer la prioridad de búsqueda en DNS mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > DNS**.
2. En el panel de detalles, en **Configuración**, haga clic en Cambiar configuración de DNS.

3. En el cuadro de diálogo **Configurar parámetros DNS**, en **Prioridad de búsqueda de nombres**, seleccione DNS o WINS y, a continuación, haga clic en Aceptar.

> **Nota**
>
> Si el servidor virtual DNS que ha configurado es DOWN y si establece el `-nameLookupPriority` como DNS, Citrix ADC no intenta la búsqueda WINS. Por lo tanto, si un servidor virtual DNS no está configurado o está inhabilitado, establezca el `-nameLookupPriority` en WINS.

Inhabilitar y habilitar servidores de nombres

February 16, 2021

El procedimiento siguiente describe los pasos para habilitar o inhabilitar un servidor de nombres existente.

Habilitar o inhabilitar un servidor de nombres mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para habilitar o inhabilitar un servidor de nombres y verificar la configuración:

```
1 -  (enable | disable) dns nameServer <IPAddress>
2 -  show dns nameServer <IPAddress>
3 <!--NeedCopy-->
```

Ejemplo:

```
1 > disable dns nameServer 10.102.9.19
2  Done
3 > show dns nameServer 10.102.9.19
4 1)       10.102.9.19: LOCAL  -  State: OUT OF SERVICE
5  Done
6 <!--NeedCopy-->
```

Habilitar o inhabilitar un servidor de nombres mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > DNS > Servidores de nombres**.
2. En el panel de detalles, seleccione el servidor de nombres que quiere habilitar o inhabilitar.

3. Haga clic en Habilitar o Desactivar. Si se habilita un servidor de nombres, la opción Inhabilitar está disponible. Si un servidor de nombres está inhabilitado, la opción Habilitar está disponible.

Configurar Citrix ADC como un solucionador de stub-aware no validador de seguridad

February 16, 2021

A partir de Citrix ADC 12.1 compilación 49.xx, Citrix ADC actúa como un solucionador de seguridad que no valida la seguridad. Para habilitar este soporte, el bit AD se establece en el encabezado DNS y el bit DO se desestablece en el encabezado OPT. Cuando se establece el bit AD y el bit DO está desestablecido, el solucionador recursivo ascendente valida la respuesta DNSSEC. Si la validación es correcta, el solucionador recursivo responde sin RRs DNSSEC. Si falla la validación DNSSEC, el solucionador recursivo regresa con una respuesta SERVFAIL.

> **Importante:**
>
> El bit AD se establece de forma predeterminada en el reenviador ADC. El bit AD no está configurado para las consultas iniciadas por DBS.

Soporte de tramas jumbo para DNS para manejar respuestas de tamaños grandes

February 16, 2021

A partir de Citrix ADC 12.1, compilación 49.xx, DNS admite tramas jumbo para manejar respuestas UDP superiores a 1.280 bytes. Anteriormente, el dispositivo Citrix ADC solo admitía un tamaño de paquete UDP de hasta 1.280 bytes.

Puede establecer el tamaño máximo de paquete UDP que el dispositivo puede manejar en los modos proxy, ADNS y reenviador configurando el valor del parámetro Tamaño máximo de paquete UDP. Por ejemplo, si el valor del parámetro Tamaño máximo de paquete UDP se establece en 4096, el dispositivo puede gestionar una respuesta DNS de tamaño 4.096 bytes.

> **Importante**
>
> - En el modo proxy, el menor tamaño entre el tamaño de carga útil OPT de solicitud de cliente y el valor de tamaño máximo de paquete UDP se considera para enviar consultas DNS al back-end. Por ejemplo, si el tamaño de carga de OPT de solicitud del cliente es 3000 y el valor de tamaño máximo de paquete UDP es 4096, se envían consultas DNS de 3.000 bytes

> al back-end.
>
> Además, desde el back-end, el dispositivo puede recibir respuestas de tamaños grandes y procesar respuestas de tamaños grandes.
>
> - En el modo de reenvío, el dispositivo establece el tamaño de carga de OPT igual al valor del parámetro de tamaño de paquete UDP.
> - Si los registros DNS son locales en el dispositivo, el dispositivo puede componer tamaños de respuesta tan grandes como el valor del parámetro Tamaño máximo de paquete UDP. Esta configuración es aplicable a los solucionadores de ADN, proxy y recursivos.

Para configurar el tamaño máximo de paquete UDP mediante la CLI

En el símbolo del sistema, escriba:

```
set dns parameter [-maxUDPPacketSize <positive_integer>]
<!--NeedCopy-->
```

Ejemplo:

```
set dns parameter -maxUDPPacketSize 10000
<!--NeedCopy-->
```

> **Nota**: El valor mínimo y máximo que puede establecer para el parámetro Tamaño máximo de paquete UDP es 512 y 16384 respectivamente. El valor predeterminado es 1280.

Para configurar el tamaño máximo de paquete UDP mediante la CLI

1. Vaya a **Administración del tráfico** > **DNS**.
2. En el panel de detalles, haga clic en **Cambiar configuración DNS**.
3. En Tamaño máximo de paquete UDP, especifique el tamaño máximo de paquete UDP.
4. Haga clic en **Aceptar**.

Configurar el registro DNS

January 21, 2022

Puede configurar el dispositivo Citrix ADC para que registre las solicitudes y respuestas DNS que gestiona. El dispositivo registra las solicitudes y respuestas DNS en formato SYSLOG. Puede elegir registrar solicitudes DNS o respuestas DNS, o ambas, y enviar los mensajes de syslog a un servidor de registro remoto. Los mensajes de registro se pueden utilizar para:

- Auditar las respuestas DNS al cliente
- Auditoría de clientes DNS
- Detecte y evite ataques DNS
- Solución de problemas

Un dispositivo Citrix ADC puede registrar las siguientes secciones de la solicitud o respuesta DNS, según su configuración:

- Sección de encabezado
- Sección de preguntas
- Sección de respuestas
- Sección de autoridad
- Sección **adicional**

Perfiles DNS

Puede utilizar un perfil DNS para configurar los distintos parámetros DNS que quiere que el extremo DNS aplique al tráfico DNS. En el perfil, puede habilitar el registro, el almacenamiento en caché y el almacenamiento en caché negativo.

Importante: Desde la versión de NetScaler 11.0, la habilitación del almacenamiento en caché de DNS mediante parámetros DNS globales ha quedado obsoleta. Puede habilitar o inhabilitar el almacenamiento en caché de DNS mediante perfiles DNS. Ahora puede habilitar el almacenamiento en caché DNS para un servidor virtual individual habilitando el almacenamiento en caché DNS en un perfil DNS y configurando el perfil DNS en el servidor virtual individual.

Los perfiles DNS admiten los siguientes tipos de registro DNS:

- Registro de consultas DNS
- Registro de la sección de respuestas DNS
- Registro extendido de DNS
- Registro de errores DNS

Registro de consultas DNS

Puede configurar un dispositivo Citrix ADC para que registre únicamente las consultas DNS que reciben los puntos de enlace DNS del dispositivo.

Nota: Si se producen errores durante el procesamiento de una consulta, se registran si esta opción está establecida en el perfil DNS.

A continuación se muestra un ejemplo de mensaje de registro de consultas:

```
DNS DNS_QUERY 143 0 :  U:10.102.27.70#61297:10.102.27.73#53/22142/Q/
(RD)/NO/1/0/0/0#test.com./1#
<!--NeedCopy-->
```

Registro de la sección de respuestas DNS

Puede configurar un dispositivo Citrix ADC para que registre todas las secciones de **respuestas** de las respuestas DNS que el dispositivo envía al cliente. El registro de la sección de respuestas DNS resulta útil cuando Citrix ADC está configurado como solucionador de DNS o en casos de uso de GLSB.

A continuación se muestra un ejemplo de registro de la sección de respuestas DNS:

```
DNS DNS_RESPONSE 6678 0 :  U:100.100.100.210#32776:100.100.100.10#
53/61373/Q/(RD,AA,RA,R)/NO/1/1/2/4#n1.citrix.com1./
28#ANS#AAAA/120/1111:2345:6789:ffab:abcd:effa:1234:3212##
<!--NeedCopy-->
```

Registro extendido de DNS

Para configurar un dispositivo Citrix ADC para que registre las secciones Autoridad y **Adicional** en las respuestas DNS, habilite el registro extendido con el registro de la sección de respuestas.

Nota: Si se producen errores durante el procesamiento de consultas o respuestas, los errores se registran si esta opción se establece en el perfil DNS.

A continuación se muestra un ejemplo de un mensaje registrado cuando se completa la búsqueda de caché y la respuesta está incrustada en el paquete:

```
DNS DNS_RESPONSE 2252 0 :  T:100.100.100.118#21411:100.100.100.10
#53/48537/Q/(RD,AA,CD,RA,R)/NO/1/1/2/6#a1.citrix.com1./1#ANS#A/
120/1.1.1.1##AUTH#citrix.com1/NS/120/n2.citrix.com1#n1.citrix.com1##ADD
   #n1.citrix.com1
/A/120/1.1.1.1#1.1.1.2##n1.citrix.com1/AAAA/120/
1111:2345:6789:ffab:abcd:effa:1234:3212##n2.citrix.com1/A/120/2.1.1.2
##n2.citrix.com1/AAAA/120/2222:faff:3212:8976:123:1241:64:ff9b##OPT
   /0/1280/DO##
<!--NeedCopy-->
```


Registro de errores DNS

Puede configurar un dispositivo Citrix ADC para registrar los errores o errores que se producen cuando procesa una consulta o respuesta DNS. Para estos errores, el dispositivo registra el encabezado DNS, las secciones de **preguntas** y los registros OPT.

A continuación se muestra un ejemplo de mensaje registrado cuando se produce un error durante el procesamiento de una solicitud o respuesta DNS:

```
DNS DNS_ERROR 149 0 :  U:10.102.27.70#27832:10.102.27.73#53/61153/Q/
(RD)/NO/1/0/0/0#test.com./1140#Packet Dropped
<!--NeedCopy-->
```

Registro basado en directivas

Puede configurar el registro personalizado basado en expresiones DNS configurando las directivas LogAction on DNS, Rewrite o Responder. Puede especificar que el registro solo se produce cuando una directiva DNS determinada se evalúa como true. Para obtener más información, consulte Configurar el registro basado en directivas para DNS.

Comprender el formato de mensaje de registro de syslog de Citrix ADC

El dispositivo Citrix ADC registra las solicitudes y respuestas DNS en el siguiente formato Syslog:

```
<transport> :<client IP>#<client ephemeral port>:<DNS endpoint IP>#<
   port>
 : <query id> /opcode/header flags/rcode/question section count/answer
    section count
/ auth section count / additional section count #<queried domain name>
/<queried type>#...
<!--NeedCopy-->
```

- **<transport>:**
  - T = TCP
  - U = UDP
- **<client IP>#< client ephemeral port >:** Dirección IP y número de puerto del cliente DNS
- **<DNS endpoint IP>#<port>:** Dirección IP y número de puerto del dispositivo de punto final DNS de Citrix ADC

- **<query id>:**
  ID de consulta
- **<opcode>:** Código de operación. Valores admitidos:
  - Q: Consulta
  - I: Consulta inversa
  - S: Estado
  - X0: Sin asignar
  - N: Notificar
  - U: Actualización
  - X1-10: Valores sin asignar
- **<header flags>:** Marcas. Valores admitidos:
  - RD: Recursión deseada
  - TC: Truncado
  - AA: Respuesta autorizada
  - CD: Comprobación desactivada
  - AD: Datos autenticados
  - Z: Sin asignar
  - RA: Recursión disponible
  - R: Respuesta
- **<rcode>:** Código de respuesta. Valores admitidos:
  - NO: No hay error
  - F: Error de formato
  - S: Error del servidor
  - NX: Dominio inexistente
  - NI: No implementado
  - R: Consulta rechazada
  - YX: El nombre existe cuando no debe
  - YXR: El conjunto de RR existe cuando no debe
  - NXR: El conjunto de RR que debe existir no
  - NAS: Servidor no autorizado para zona
  - NA: No autorizado
  - NZ: Nombre no incluido en la zona
  - X1-5: Sin asignar
- **/question section count/answer section count/auth section count/additional section count:** Sección de preguntas, recuento de secciones de autoridad y recuento de secciones **adicionales** en la solicitud DNS

- **<queried domain name>/<queried type>:** Dominio consultado y tipo consultado en la solicitud DNS
- **#ANS#<record type>/<ttl>/.. #AUTH#<domain name>/<record type>/<ttl>.. #ADD#<domain name>/<record type>/<ttl>...:**

  En las respuestas DNS:

  La sección de respuestas se registra si el registro de la sección de respuestas está habilitado en el perfil DNS. Las secciones Autoridad y **Adicional** se registran si el registro extendido está habilitado en el perfil DNS. El formato del registro variaría según el tipo de registro. Para obtener más información, consulte Descripción del formato de registro de registros.

  - ANS: Sección de respuestas
  - AUTH: Autoridad
  - ADD: Sección **adicional**
- **OPT/<edns version>/UDP max payload size/DO:** Formato de registro OPT en el registro DNS
- **OPT/<EDNS version>/<UDP payload size>/<"DO"or empty based on whether DNSSEC OK bit is set or not>/<value of RDLEN>/ECS/<Q/R>/<option length>/<Family>/<Source Prefix-Length>/<Scope Prefix-Length>/<ECS Address>:**

  Si la consulta o respuesta DNS incluye la opción Subred cliente EDNS (ECS), también se registra en el formato de registro OPT del archivo de registros DNS.

  Cuando se envía una consulta DNS con una opción ECS que incluye una dirección IPv4 o IPv6, la opción ECS se registra con cualquiera de las opciones siguientes:

  - "ECS/Q" que indica que los valores en el registro provienen de la consulta
  - "ECS/R" que indica que los valores del registro provienen de la respuesta.

  El valor de Scope Prefix-Length también se establece correctamente. En la consulta DNS, se establece en cero y, para la respuesta, se establece en el valor calculado.

  En la tabla siguiente se describen los detalles registrados en varios casos:

Caso	Opción ECS establecida en la consulta DNS	Opción ECS establecida en la respuesta DNS	Detalles registrados
Se han habilitado tanto el registro de consultas como el registro extendido	Sí	Sí	La opción ECS se registra con la cadena "ECS/R/" y la longitud del prefijo de ámbito se establece en el valor calculado.

Caso	Opción ECS establecida en la consulta DNS	Opción ECS establecida en la respuesta DNS	Detalles registrados
Se han habilitado tanto el registro de consultas como el registro extendido	Sí	No	La opción ECS se registra con la cadena “ECS/Q” y la longitud del prefijo de ámbito se establece en cero.
El registro de consultas está habilitado, pero el registro ampliado no está habilitado	Sí	Sí	La opción ECS se registra con la cadena “ECS/Q/” y la longitud del prefijo de ámbito se establece en cero.
El registro de consultas y el registro extendido no están habilitados	Sí	Sí	La opción ECS no se registra.
El registro de consultas está habilitado, pero el registro ampliado no está habilitado	Sí	No	La opción ECS se registra con la cadena “ECS/Q/” y la longitud del prefijo de ámbito se establece en cero.
El registro de consultas no está habilitado, pero el registro ampliado está habilitado	Sí	Sí	La opción ECS se registra con la cadena “ECS/R/” y la longitud del prefijo de ámbito se establece en el valor calculado.
El registro de consultas no está habilitado, pero el registro ampliado está habilitado	Sí	No	La opción ECS no se registra.

Comprender el formato de registro de registros

A continuación se muestra un ejemplo del formato de registro de registros de un mensaje de Syslog:


```
<domainname>/<record type>/ <record ttl> / <resource record data>#<
   resource record data>#......##
<!--NeedCopy-->
```

Donde:

Tipo de registro	Formato de muestra	Datos de registro de recursos/formato
Registro de direcciones (A)	A/5/1.1.1.1#1.1.1.2#1.1.1.3##	Dirección IPv4
Registro AAAA	AAAA/5/1::1#1::2#1::3##	Dirección IPv6
Registro SOA	SOA/3600/ns1.dnslogging.test./	Servidor de Origin, contacto y otros detalles. El formato de registro de recursos es: <originServer>/<contact>/<serial number>/<refresh rate>/<retry>/<expire>/<minimum>##
NS record	NS/5/ns1.dnslogging.test	Nombre de host del servidor de nombres.
Récord MX	#MX/5/10/host1.dnslogging.test	Preferencia seguida del nombre de host del servidor de intercambio de correo
Registro de registros CNAME	CNAME/5/host1.dnslogging.test.##	Nombre canónico
Registro SRV	SRV/5/1/2/3/host1.dnslogging.te	Formato de registro de recursos: <priority>/<weight>/<port>/<target>#
Registro TXT	TXT/5/dns+logging##	Los datos comprenden todos los textos.
Registro NAPTR	NAPTR/5/10/11////dnslogging#2	Formato de registro de recursos: <order>/<preference>/<flags>/<services>/<re expression>/<replacement string>#
Registro DNSKEY	DNSKEY/5/1/3/5/AwEAAanP0K+i5	Formato de registro de recursos: <flags>/<protocol>/<algorithm>/<public key in base64 encoding>#

Tipo de registro	Formato de muestra	Datos de registro de recursos/formato
Registro PTR	PTR/3600/test.com.#test4.com	Nombre del dominio

Limitaciones del registro DNS

El registro DNS tiene las siguientes limitaciones:

- Si el registro de respuestas está habilitado, solo se registran los siguientes tipos de registro:
  - Registro de direcciones (A)
  - Registro AAAA
  - Registro SOA
  - Registro NS
  - Registro MX
  - Registro CNAME
  - Registro SRV
  - Registro TXT
  - Registro NAPTR
  - Registro DNSKEY
  - Registro PTR

  Para todos los demás tipos de registro, solo se registran los parámetros L3/L4, Encabezado DNS y sección Pregunta.
- Los registros RRSIG no se registran aunque el registro de respuestas esté habilitado.
- DNS64 no es compatible.
- Las solicitudes o respuestas de actualización proactiva de DNS se registran según la configuración del perfil predeterminado.
- En el servidor virtual, si está habilitado el registro de respuestas y opciones sin sesión, se registran los parámetros L3/L4, Encabezado DNS y la sección Pregunta DNS en lugar de la respuesta.
- El tamaño máximo del mensaje syslog es de 1024 bytes.
- Si ha establecido un perfil DNS para una directiva DNS con el tipo de acción Respuesta de reescritura, el dispositivo Citrix ADC no registra la consulta ni las respuestas manipuladas. Para registrar la información necesaria, debe utilizar una acción de mensaje de auditoría en la directiva DNS.
- Las transacciones DNS que se deben al tráfico de supervisión de DNS no se registran.

Configuración del registro DNS

A continuación se presenta una descripción general de la configuración del registro DNS:

1. Cree una acción Syslog y habilite DNS en la acción.
2. Cree una directiva Syslog y especifique la acción Syslog en la directiva.
3. Enlace globalmente la directiva Syslog para habilitar el registro de todos los sucesos del sistema Citrix ADC. O bien vincule la directiva Syslog a un servidor virtual de equilibrio de carga específico.
4. Cree un perfil DNS y defina cualquiera de los siguientes tipos de registro que quiera habilitar:
   - Registro de consultas DNS
   - Registro de la sección de respuestas DNS
   - Registro extendido de DNS
   - Registro de errores DNS
5. Configure cualquiera de las siguientes opciones según sus necesidades:
   - Servicio DNS y servidor virtual para DNS
   - Servicio ADNS
   - Citrix ADC como reenviador
   - Citrix ADC como solucionador
6. Defina el perfil DNS creado en una de las entidades DNS.

Configurar el registro DNS para Citrix ADC configurado como proxy DNS mediante la CLI

1. Agregue una acción syslog y habilite DNS en la acción. En el símbolo del sistema, escriba:

```
add audit syslogAction <name> (<serverIP> | -lbVserverName <string
    >) [-serverPort <port>] -logLevel <logLevel> ... [-dateFormat <
    dateFormat>] [-logFacility <logFacility>] [-tcp ( NONE | ALL )]
     [-acl ( ENABLED | DISABLED )] [-timeZone ( GMT_TIME |
    LOCAL_TIME )] [-userDefinedAuditlog ( YES | NO )] [-
    appflowExport ( ENABLED |DISABLED )] [-lsn ( ENABLED | DISABLED
     )] [-alg ( ENABLED | DISABLED )] [-transport ( TCP | UDP )] [-
    tcpProfileName <string>] [-maxLogDataSizeToHold <
    positive_integer>] [-dns ( ENABLED | DISABLED)]
<!--NeedCopy-->
```

Ejemplo:

```
add audit syslogAction nssyslogact1 10.102.151.136 -logLevel CRITICAL
ERROR WARNING NOTICE INFORMATIONAL DEBUG -logFacility LOCAL4 -timeZone
LOCAL_TIME -dns ENABLED
```


2. Cree una directiva syslog y especifique la acción syslog creada en la directiva. En el símbolo del sistema, escriba:

   ```
   add audit syslogPolicy <name> <rule> <action>
   ```

   Ejemplo:

   ```
   add audit syslogPolicy syslogpol1 ns_true nssyslogact1
   ```

3. Enlazar la directiva syslog globalmente. En el símbolo del sistema, escriba:

   ```
   bind system global [<policyName> [-priority <positive_integer>]]
   ```

   Ejemplo:

   ```
   bind system global syslogpol1
   ```

4. Cree un perfil DNS y habilite cualquiera de los siguientes tipos de registros que quiera configurar:

   - Registro de consultas DNS
   - Registro de la sección de respuestas DNS
   - Registro extendido de DNS
   - Registro de errores DNS

   En el símbolo del sistema, escriba:

   ```
   add dns profile <dnsProfileName> [-dnsQueryLogging ( ENABLED | DISABLED
    )] [-dnsAnswerSecLogging ( ENABLED | DISABLED )] [-dnsExtendedLogging
    (ENABLED | DISABLED )] [-dnsErrorLogging ( ENABLED | DISABLED )] [-
   cacheRecords ( ENABLED | DISABLED )] [-cacheNegativeResponses ( ENABLED
    | DISABLED )]
   ```

   Ejemplo:

   ```
   add dns profile dnsprofile1 -dnsQueryLogging ENABLED
   ```

5. Configure el servicio de tipo DNS. En el símbolo del sistema, escriba:

   ```
   add service <name> <serverName> <serviceType> <port>
   ```

   Ejemplo:

   ```
   add service svc1 10.102.84.140 dns 53
   ```

6. Configure un servidor virtual de equilibrio de carga de tipo de servicio DNS.

   ```
   add lb vserver <name> <serviceType> <ip> <port>
   ```

   Ejemplo:

   ```
   add lb vserver lb1 dns 100.100.100.10 53
   ```


7. Enlace el servicio al servidor virtual. En el símbolo del sistema, escriba:

   ```
   bind lb vserver <name> <serviceName>
   ```

   Ejemplo:

   ```
   bind lb vserver lb1 svc1
   ```

8. Defina el perfil DNS creado en el servidor virtual. En el símbolo del sistema, escriba:

   ```
   set lb vserver <name> [ - dnsProfileName <string>]
   ```

   Ejemplo:

   ```
   set lb vserver lb1 -dnsProfileName dnsprofile1
   ```

Configuración de registro DNS de ejemplo para el dispositivo Citrix ADC configurado como proxy DNS

```
1  > add audit syslogAction nssyslogact1 10.102.151.136 -logLevel
2  CRITICAL ERROR WARNING NOTICE INFORMATIONAL DEBUG -logFacility LOCAL4 -
       timeZone
3  LOCAL_TIME -dns ENABLED
4  Done
5  > add audit syslogPolicy syslogpol1 ns_true nssyslogact1
6  Done
7  > bind system global syslogpol1
8  Done
9  > add dns profile dnsprofile1 -dnsqueryLogging ENABLED
10 Done
11 > add lb vserver lb1 dns 100.100.100.10 53  - dnsProfileName dnsprofile1
12 Done
13 > add service svc1 10.102.84.140 dns 53
14 Done
15 > bind lb vserver lb1 svc1
16 Done
17 <!--NeedCopy-->
```

Configuración de registro DNS de ejemplo para el dispositivo Citrix ADC configurado como ADNS

```
1  > add audit syslogAction nssyslogact1 10.102.151.136 -logLevel CRITICAL
2  ERROR WARNING NOTICE INFORMATIONAL DEBUG -logFacility LOCAL4 -timeZone
       LOCAL_TIME
3  -dns ENABLED
```



```
Done
> add audit syslogPolicy syslogpol1 ns_true nssyslogact1
Done
> bind system global syslogpol1
Done
> add dns profile dnsprofile1 -dnsqueryLogging ENABLED
Done
> add lb vserver lb1 dns 100.100.100.10 53  - dnsProfileName dnsprofile1
Done
> add service svc1 10.102.84.140 dns 53
Done
> bind lb vserver lb1 svc1
Done
<!--NeedCopy-->
```

Configuración de registro DNS de ejemplo para el dispositivo Citrix ADC configurado como reenviador

```
> add audit syslogAction nssyslogact1 10.102.151.136 -logLevel CRITICAL
ERROR WARNING NOTICE INFORMATIONAL DEBUG -logFacility LOCAL4 -timeZone
    LOCAL_TIME
-dns ENABLED
Done
> add audit syslogPolicy syslogpol1 ns_true nssyslogact1
Done
> bind system global syslogpol1
Done
> add dns profile dnsprofile1 -dnsqueryLogging ENABLED
Done
> add dns nameserver 8.8.8.8  - dnsProfileName dnsprofile1
Done
<!--NeedCopy-->
```

Configuración de registro DNS de ejemplo para un dispositivo Citrix ADC configurado como resolución

```
> add audit syslogAction nssyslogact1 10.102.151.136
-logLevel CRITICAL ERROR WARNING NOTICE INFORMATIONAL DEBUG -
    logFacility LOCAL4
-timeZone LOCAL_TIME -dns ENABLED
Done
```



```
> add audit syslogPolicy syslogpol1 ns_true nssyslogact1
Done
> bind system global syslogpol1
Done
> add dns profile dnsprofile1 -dnsqueryLogging ENABLED
Done
> set dns parameter -recursion enABLED
Done
> add nameserver 1.1.1.100 -local dnsProfileName dnsprofile1
Done
<!--NeedCopy-->
```

Configurar el registro basado en directivas para DNS

El registro basado en directivas permite especificar un formato para los mensajes de registro. El contenido de un mensaje de registro se define mediante una expresión de directiva avanzada. Cuando se realiza la acción de mensaje especificada en la directiva, el dispositivo Citrix ADC construye el mensaje de registro a partir de la expresión y escribe el mensaje en el archivo de registros. Puede configurar el dispositivo para que registre únicamente cuando una directiva DNS concreta se evalúe como True.

> **Nota**
>
> Si ha establecido una directiva DNS con un perfil DNS para el lado de la solicitud, el dispositivo Citrix ADC registra únicamente la consulta.

Para configurar el registro basado en directivas para una directiva DNS, primero debe configurar una acción de mensaje de auditoría. Para obtener más información sobre la configuración de una acción de mensaje de auditoría, consulte Configurar el dispositivo NetScaler para el registro de auditoría. Después de configurar la acción de mensaje de auditoría, especifique la acción de mensaje en una directiva DNS.

Configurar el registro basado en directivas para una directiva DNS mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para configurar el registro basado en directivas para una directiva DNS y compruebe la configuración:

```
1 - add dns action <actionName> <actionType> [-IPAddress <ip_addr|
    ipv6_addr> ... | -viewName <string> | -preferredLocList <string>
    ...] [-TTL <secs>] [-dnsProfileName <string>]
2 - set dns policy <name> [<rule>] [-actionName <string>] [-logAction <
    string>]
3 - show dns policy [<name>]
```



```
<!--NeedCopy-->
```

Ejemplo 1:

En una implementación de GSLB, si quiere responder con direcciones IP diferentes a las solicitudes de cliente procedentes de una subred concreta, en lugar de responder con direcciones IP utilizadas con fines generales (como las direcciones IP de los usuarios internos), puede configurar una directiva DNS con el tipo de acción como vista DNS. En este caso, puede configurar el registro DNS en la acción DNS especificada de forma que pueda registrar las respuestas específicas.

```
> add dns profile dns_prof1 -dnsqueryLogging enABLED -
   dnsanswerSecLogging enABLED
 Done
> add dns view dns_view1
 Done
> add dns action dns_act1 viewName -view dns_view1  - dnsprofilename
   dns_prof1
 Done
> add dns policy dns_pol1 "CLIENT.IP.SRC.APPLY_MASK(255.255.255.0).EQ
   (100.100.100.0)"
dns_act1
 Done
> bind dns global dns_pol1 100 -gotoPriorityExpression END -type
   REQ_DEFAULT
 Done
> bind gslb service site_1_svc -viewName dns_view1 123.1.1.1
 Done
> bind gslb service site_5_svc -view dns_view1 132.1.1.1
 Done
<!--NeedCopy-->
```

Nota: En la configuración anterior, si consulta el dominio configurado en un servidor virtual GSLB, por ejemplo, *sampletest.com*, todos los usuarios internos de la subred 100.100.100.0/24 reciben las direcciones IP de la vista DNS y se registran las respuestas. Las solicitudes de los clientes de otras subredes no se registran.

Ejemplo 2:

Si quiere registrar únicamente las consultas del dominio *ejemplo.com*, puede crear un perfil DNS con el registro de consultas habilitado y establecer el perfil DNS en una acción DNS con el tipo de acción **NOOP**y, a continuación, crear una directiva DNS y establecer la acción DNS. Por ejemplo:


```
>add dns profile query_logging -dnsqueryLogging ENABLED
Done
>add dns action dns_act1 NOOP -dnsprofileName query_logging
Done
>add dns policy dns_pol1 DNS.REQ.QUESTION.DOMAIN.EQ("example.com")
   dns_act1
Done
<!--NeedCopy-->
```

Configurar la acción de registro para que la directiva DNS registre la dirección IP del cliente

La acción de registro se puede usar para registrar las IP de origen para las consultas de DNS mediante la siguiente expresión y usarla como parte de la acción de registro en la directiva de DNS.

```
> add audit messageaction log_act_custom INFORMATIONAL ""ClientIP:"
   CLIENT.IP.SRC" ECS IP:"+((DNS.REQ.OPT.ECS.IP).typecast_text_t ALT "
   NONE")"
Done
<!--NeedCopy-->
```

La expresión anterior captura tanto la IP de origen como en el encabezado IP y la IP de ECS de la opción DNS ECS, y cualquiera de ellas se puede excluir según sea necesario.

Configuración de registro DNS de ejemplo para que un dispositivo Citrix ADC registre la dirección IP del cliente

Si quiere tomar una muestra del registro de las consultas DNS, puede hacerlo mediante la siguiente expresión. Esto cerrará una de cada 10 consultas.

```
> add audit messageaction log_action_srcip_1of10 INFORMATIONAL ""
   OneOf10: Source IP : "+client.ip.src"
Done
> add responder policy logsrcip_1of10 "sys.random.mul(10).lt(1)" NOOP -
   logAction log_action_srcip_1of10
Done
<!--NeedCopy-->
```


Configuración de sufijos DNS

February 16, 2021

Puede configurar sufijos DNS que permitan al dispositivo Citrix ADC completar nombres de dominio no completos durante la resolución de nombres. Por ejemplo, al resolver un nombre de dominio abc no completo, si se configura un sufijo DNS example.com, el dispositivo anexa el sufijo al nombre de dominio. A continuación, resuelve el nombre de dominio. En este caso, resolvería abc.example.com. Si los sufijos DNS no están configurados, el dispositivo anexa un punto a los nombres de dominio no completos y resuelve el nombre de dominio.

Crear sufijos DNS

Los sufijos DNS tienen importancia y solo son válidos cuando Citrix ADC está configurado como un solucionador final o reenviador. Puede especificar un sufijo de hasta 127 caracteres.

Nota: El orden de los sufijos DNS es importante. El dispositivo ADC intenta los sufijos configurados en un orden serie y se detiene cuando obtiene una respuesta correcta para un sufijo.

Crear sufijos DNS mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para crear un sufijo DNS y verificar la configuración:

```
-  add dns suffix <dnsSuffix>
-  show dns suffix <dnsSuffix>
<!--NeedCopy-->
```

Ejemplo:

```
> add dns suffix example.com
 Done
> show dns suffix example.com
1)      Suffix: example.com
Done

<!--NeedCopy-->
```

Para quitar un sufijo DNS mediante la línea de comandos de Citrix ADC, en el símbolo del sistema, escriba el `rm dns suffix` comando y el nombre del sufijo DNS.

Crear sufijos DNS mediante la interfaz gráfica de usuario

Vaya a **Administración del tráfico > DNS > Sufijo DNS** y cree sufijos DNS.

Consulta DNS ANY

February 16, 2021

Una consulta CUALQUIER es un tipo de consulta DNS que recupera todos los registros disponibles para un nombre de dominio. La consulta CUALQUIER debe enviarse a un servidor de nombres autorizado para un dominio.

Comportamiento en modo ADNS

En el modo ADNS, el dispositivo Citrix ADC devuelve los registros almacenados en su caché local. Si no hay registros en la caché, el dispositivo devuelve la respuesta NXDOMAIN (negativa).

Si Citrix ADC puede coincidir con los registros de delegación de dominio, devuelve los registros NS. De lo contrario, devuelve los registros NS del dominio raíz.

Comportamiento en modo proxy DNS

En el modo proxy, el dispositivo Citrix ADC comprueba su caché local. Si no hay registros en la caché, el dispositivo pasa la consulta al servidor.

Comportamiento para dominios de Equilibrio de carga de servidor global (GSLB)

Si se configura un dominio GSLB en el dispositivo ADC y se envía una consulta ANY para el dominio GSLB (sitio), el dispositivo devuelve la dirección IP del servicio GSLB. Selecciona este servicio a través de una decisión de equilibrio de carga. Si la opción de respuesta IP múltiple (MIR) está habilitada, se envían las direcciones IP de todos los servicios GSLB.

Para que Citrix ADC devuelva estos registros cuando responda a la consulta ANY, todos los registros correspondientes a un dominio GSLB deben configurarse en Citrix ADC.

> **Nota**
>
> Si los registros de un dominio se distribuyen entre Citrix ADC y un servidor, solo se devuelven los registros configurados en Citrix ADC.

Citrix ADC proporciona la opción de configurar las vistas DNS y las directivas DNS. Estas vistas y directivas se utilizan para realizar el equilibrio de carga del servidor global. Para obtener más información, consulte Equilibrio de carga global del servidor.

Configurar el almacenamiento en caché negativo de registros DNS

August 20, 2021

El dispositivo Citrix ADC admite el almacenamiento en caché de respuestas negativas para un dominio. Una respuesta negativa indica que no existe información sobre un dominio solicitado o que el servidor no puede proporcionar una respuesta para la consulta. El almacenamiento de esta información se denomina almacenamiento en caché negativo. El almacenamiento en caché negativo ayuda a acelerar las respuestas a las consultas sobre un dominio.

> **Nota:**
>
> El almacenamiento en caché negativo solo se admite cuando el servidor back-end está configurado como un servidor DNS autoritario (ADNS) para el dominio consultado.

Una respuesta negativa puede ser una de las siguientes:

- Mensaje de error NXDOMAIN: Los servidores DNS autorizados responden con el mensaje de error NXDOMAIN cuando el nombre de dominio consultado no tiene ningún registro configurado en el servidor. Este mensaje implica que el dominio consultado es un nombre de dominio no válido o inexistente.
- Mensaje de error NODATA: Si el nombre de dominio de la consulta es válido pero los registros del tipo dado no están disponibles, el dispositivo envía un mensaje de error NODATA.

Cuando se habilita el almacenamiento en caché negativo, el dispositivo almacena en caché la respuesta negativa del servidor DNS y solo sirve las solicitudes futuras de la caché. Esta acción ayuda a acelerar las respuestas a las consultas y también a reducir el tráfico DNS de back-end. El almacenamiento en caché negativo se puede utilizar en todas las implementaciones, es decir, cuando un dispositivo Citrix ADC funciona como proxy, como solución final o como reenviador.

Puede habilitar o inhabilitar el almacenamiento en caché negativo mediante un perfil DNS. Para obtener más información, consulte Perfiles DNS. De forma predeterminada, el almacenamiento en caché negativo está habilitado en el perfil DNS predeterminado (**default**-dns-profile) que está enlazado de forma predeterminada a un servidor virtual DNS o en el perfil DNS recién creado.

Habilitar o inhabilitar el almacenamiento en caché negativo mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para habilitar o inhabilitar el almacenamiento en caché negativo y verificar la configuración:

```
1 - add dns profile <dnsProfileName> [-cacheRecords ( ENABLED | DISABLED
    )] [-cacheNegativeResponses (ENABLED | DISABLED )]
2 - show dns profile [<dnsProfileName>]
```



```
<!--NeedCopy-->
```

Ejemplo de un perfil DNS predeterminado:

```
> sh dns profile default-dns-profile
    1)   default-dns-profile
        Query logging : DISABLED        Answer section logging :
           DISABLED
        Extended logging : DISABLED     Error logging : DISABLED
        Cache Records : ENABLED     Cache Negative Responses: ENABLED
Done
<!--NeedCopy-->
```

Ejemplo de un perfil DNS recién creado:

```
> add dnsprofile dns_profile1 -cacheRecords ENABLED -
   cacheNegativeResponses ENABLED
Done
> show dns profile dns_profile1
    1)   dns_profile1
        Query logging : DISABLED        Answer section logging :
           DISABLED
        Extended logging : DISABLED     Error logging : DISABLED
        Cache Records : ENABLED     Cache Negative Responses: ENABLED
Done
<!--NeedCopy-->
```

Especificar los parámetros DNS de nivel de servidor virtual o de servicio mediante la CLI

En el símbolo del sistema, realice lo siguiente:

1. Configure el perfil DNS.

   ```
   add dns profile <dnsProfileName> [-cacheRecords ( ENABLED | DISABLED )]
    [-cacheNegativeResponses (ENABLED | DISABLED )]
   ```

2. Enlace el perfil DNS al servicio o servidor virtual.

   Para enlazar el perfil DNS al servicio:

   ```
   set service <name> [-dnsProfileName <string>]
   ```


Ejemplo:

```
>set service service1 -dnsProfileName dns_profile1
Done
<!--NeedCopy-->
```

Para enlazar el perfil DNS al servidor virtual:

```
set lb vserver <name> [-dnsProfileName <string>]
```

Ejemplo:

```
>set lb vserver lbvserver1 -dnsProfileName dns_profile1
Done
<!--NeedCopy-->
```

Especificar los parámetros DNS de nivel de servidor virtual o de servicio mediante la interfaz gráfica de usuario

1. Configure el perfil HTTP.

   Vaya a **Sistema** > **Perfiles** > **Perfil DNS** y cree el perfil DNS.

2. Enlace el perfil HTTP al servicio o servidor virtual.

   Vaya a **Administración del tráfico** > **Equilibrio de carga**> **Servicios/Servidores virtuales** y cree el perfil DNS, que debe estar enlazado al servicio o al servidor virtual.

Respuesta negativa limitante de velocidad atendida por el dispositivo

Puede establecer un umbral para las respuestas negativas que envía el dispositivo Citrix ADC desde la caché. Cuando se establece el umbral, el dispositivo sirve la respuesta desde la caché hasta que se alcanza el umbral. Una vez alcanzado el umbral, el dispositivo elimina las solicitudes en lugar de responder con una respuesta NXDOMAIN.

Establecer un límite de velocidad para las respuestas negativas tiene las siguientes ventajas.

- Guarde los recursos en el dispositivo Citrix ADC.
- Evite cualquier consulta maliciosa para nombres de dominio inexistentes.

> **Nota:** Puede establecer un umbral para las respuestas negativas solo para los dominios para los que el dispositivo ADC está configurado como servidor de nombres de dominio autorizado. No puede establecer un umbral para los registros almacenados en caché recibidos de los servidores

> de nombres back-end autorizados.

Rate limitando la respuesta negativa servida por la caché mediante el uso de la CLI

En el símbolo del sistema, escriba:

```
set dns parameter -NXDOMainRateLimitThreshold <positive-integer>
<!--NeedCopy-->
```

Ejemplo:

```
set dns parameter -NXDOMainRateLimitThreshold 1000
<!--NeedCopy-->
```

NxDomainRateLimitThreshold: Cuando este parámetro se establece en un valor entero positivo, las respuestas se sirven desde la caché hasta que se alcanza este umbral (en segundos). Una vez que el umbral supera, las solicitudes se eliminan. El umbral configurado es por motor de paquetes.

Rate limitando la respuesta negativa servida por la caché mediante el uso de la GUI

1. Vaya a **Administración del tráfico > DNS** y haga clic en **Cambiar configuración de DNS**.
2. En la página **Configurar parámetros DNS**, en el campo **Umbral de límite de velocidad de NXDOMAIN**, introduzca el valor de umbral hasta el que se deben servir las respuestas desde la caché.

Nota: El valor del **umbral cruzado de NXDOMAIN** muestra el número de veces que se eliminan las solicitudes después de alcanzar el umbral.

Caché de datos de subred del cliente EDNS0 cuando el dispositivo Citrix ADC está en modo proxy

February 16, 2021

En el modo Citrix ADC Proxy, si un servidor back-end que admite una subred de cliente (ECS) EDNS0 envía una respuesta que contiene la opción ECS, el dispositivo Citrix ADC realiza lo siguiente:

- Reenvía la respuesta tal cual al cliente y
- Almacena la respuesta en la caché, junto con la información de subred del cliente.

Las solicitudes DNS que provienen de la misma subred del mismo dominio, y para las que el servidor enviaría la misma respuesta, se sirven luego desde la caché.

Nota:

- El almacenamiento en caché de ECS está inhabilitado de forma predeterminada. Habilite el almacenamiento en caché de datos de subred cliente EDNS0 en el perfil DNS asociado.
- El número de subredes que puede almacenar en caché para un dominio está limitado a los ID de subred disponibles, es decir, 1270 en el dispositivo Citrix ADC. Opcionalmente, puede establecer el límite en un número inferior (valor mínimo: 1 ipv4/ipv6).

Habilitar el almacenamiento en caché de las respuestas de ECS mediante la CLI

En el símbolo del sistema, escriba:

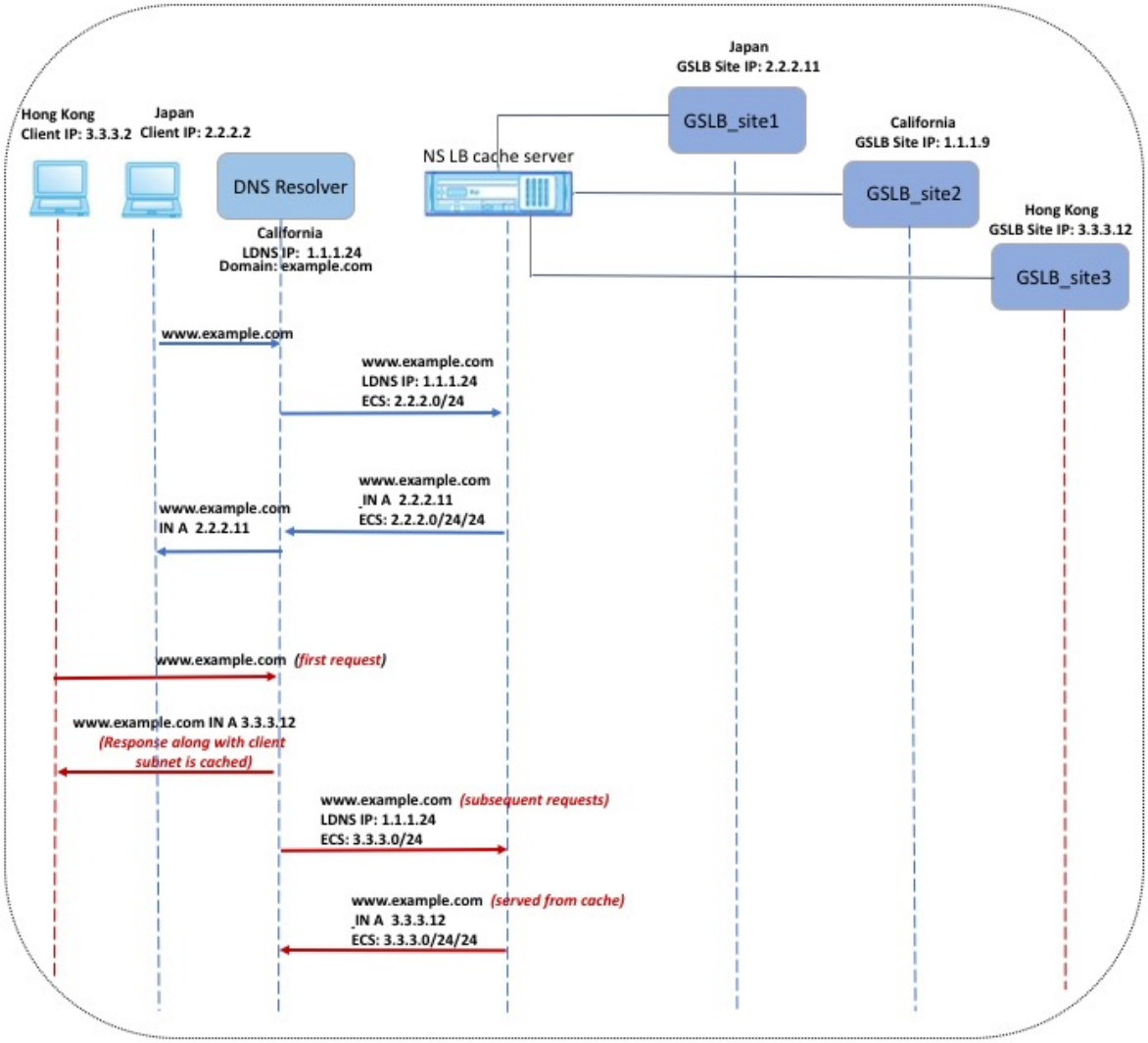
```
set dns profile <dnsProfileName> -cacheECSSubnet ( ENABLED | DISABLED )
```

Limite el número de subredes que se pueden almacenar en caché por dominio mediante la CLI

En el símbolo del sistema, escriba:

```
set dns profile <dnsProfileName> -maxSubnetsPerDomain <positive_integer>
```

Ejemplo:



En el ejemplo que se muestra en la ilustración anterior, el cliente en la dirección IP 2.2.2.2 envía una consulta para www.example.com al solucionador DNS. El solucionador DNS envía la siguiente respuesta:

www.example.com EN A, IP es 2.2.2.11 y ECS 2.2.2.0/24/24

En este punto, la respuesta y el identificador de subred del cliente (2.2.2.0/24) se almacenan en caché. Otras solicitudes de la misma subred y dominio se sirven desde la caché.

Por ejemplo, si la dirección IP del cliente es 2.2.2.100 y la consulta es para www.example.com, la consulta se sirve desde la caché en lugar de enviarse al servidor back-end.

Extensiones de seguridad del sistema de nombres de dominio

August 20, 2021

DNS Security Extensions (DNSSEC) es un estándar de Internet Engineering Task Force (IETF). Su objetivo es proporcionar integridad de los datos y autenticación del origen de los datos en las comunicaciones entre servidores de nombres y clientes, al mismo tiempo que transmite respuestas UDP en texto claro. DNSSEC especifica un mecanismo que utiliza criptografía de clave asimétrica y un conjunto de nuevos registros de recursos específicos para su implementación.

La especificación DNSSEC se describe en:

- RFC 4033, "Introducción y requisitos de seguridad DNS"
- RFC 4034, "Registros de recursos para las extensiones de seguridad DNS"
- RFC 4035, "Modificaciones de protocolo para las extensiones de seguridad DNS"

Los aspectos operacionales de la implementación de DNSSEC dentro de DNS se discuten en RFC 4641, "Prácticas operacionales de DNSSEC".

Puede configurar DNSSEC en Citrix ADC. Puede generar e importar claves para firmar zonas DNS. Puede configurar DNSSEC para zonas para las que Citrix ADC tiene autoridad. Puede configurar el ADC como un servidor proxy DNS para zonas firmadas alojadas en una comunidad de servidores de nombres back-end. Si el ADC tiene autoridad para un subconjunto de registros pertenecientes a una zona para la que el ADC está configurado como servidor proxy DNS, puede incluir el subconjunto de registros en la implementación DNSSEC.

Configurar DNSSEC

August 20, 2021

Realice los siguientes pasos para configurar DNSSEC:

1. Habilite DNSSEC en el dispositivo Citrix ADC.
2. Cree una clave de firma de zona y una clave de firma de clave para la zona.
3. Agregue las dos teclas a la zona.
4. Firma la zona con las llaves.

El dispositivo Citrix ADC no actúa como un solucionador DNSSEC. DNSSEC en ADC solo se admite en los siguientes casos de implementación:

1. ADNs: Citrix ADC es el ADNS y genera las firmas en sí.
2. Proxy: Citrix ADC actúa como proxy DNSSEC. Se supone que Citrix ADC se coloca frente a los servidores ADNS/LDNS en un modo de confianza. El ADC actúa solo como una entidad de almacenamiento en caché de proxy y no valida ninguna firma.

Habilitar e inhabilitar DNSSEC

Habilite las DNSSEC en Citrix ADC para que el ADC responda a clientes con DNSSEC. De forma predeterminada, DNSSEC está habilitado.

Puede inhabilitar la función DNSSEC si no quiere que Citrix ADC responda a los clientes con información específica de DNSSEC.

Habilitar o inhabilitar DNSSEC mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para habilitar o inhabilitar DNSSEC y verificar la configuración:

```
-  set dns parameter -dnssec ( ENABLED | DISABLED )
-  show dns parameter
<!--NeedCopy-->
```

Ejemplo:

```
> set dns parameter -dnssec ENABLED
 Done
> show dns parameter
        DNS parameters:
        DNS retries: 5
         .
         .
         .
         DNSEC Extension: ENABLED
        Max DNS Pipeline Requests: 255
 Done

<!--NeedCopy-->
```

Habilitar o inhabilitar DNSSEC mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > DNS**.
2. En el panel de detalles, haga clic en Cambiar configuración DNS.
3. En el cuadro de diálogo **Configurar parámetros DNS**, active o desactive la casilla de verificación **Habilitar extensión DNSSEC**.

Crear claves DNS para una zona

Para cada zona DNS que quiera firmar, debe crear dos pares de claves asimétricas. Un par, denominado clave de firma de zona (ZSK), se utiliza para firmar todos los conjuntos de registros de recursos de la zona. El segundo par se denomina clave de firma de claves (KSK) y se utiliza para firmar solo los registros de recursos DNSKEY en la zona.

Cuando se crean el ZSK y el KSK, el `suffix.key` se anexa a los nombres de los componentes públicos de las claves. El`suffix.private` se anexa a los nombres de sus componentes privados. El anexamiento ocurre automáticamente.

Citrix ADC también crea un registro de Delegación Signer (DS) y agrega el sufijo .ds al nombre del registro. Si la zona principal es una zona firmada, debe publicar el registro DS en la zona principal para establecer la cadena de confianza.

Al crear una clave, la clave se almacena en el `/nsconfig/dns/` directorio, pero no se publica automáticamente en la zona. Después de crear una clave mediante el `create dns key` comando, debe publicar explícitamente la clave en la zona mediante el `add dns key` comando. El proceso de generación de una clave es independiente del proceso de publicación de la clave en una zona para permitirle utilizar medios alternativos para generar claves. Por ejemplo, puede importar claves generadas por otros programas de generación de claves (como`bind-keygen`) mediante Secure FTP (SFTP) y, a continuación, publicar las claves en la zona. Para obtener más información sobre cómo publicar una clave en una zona, consulte Publicar una clave DNS en una zona.

Realice los pasos descritos en este tema para crear una clave de firma de zona y, a continuación, repita los pasos para crear una clave de firma de clave. El ejemplo que sigue a la sintaxis del comando crea primero un par de claves de firma de zona para la zona example.com. A continuación, el ejemplo utiliza el comando para crear un par de claves de firma de claves para la zona.

Desde la versión 13.0 compilación 61.x, el dispositivo Citrix ADC ahora admite algoritmos criptográficos más sólidos, como RSASHA256 y RSASHA512, para autenticar una zona DNS. Anteriormente, solo se soportaba el algoritmo RSASHA1.

Crear una clave DNS mediante la CLI

En el símbolo del sistema, escriba:

```
create dns key -zoneName <string> -keyType <keyType> -algorithm <algorithm>
 -keySize <positive_integer> -fileNamePrefix <string>
```

Ejemplo:

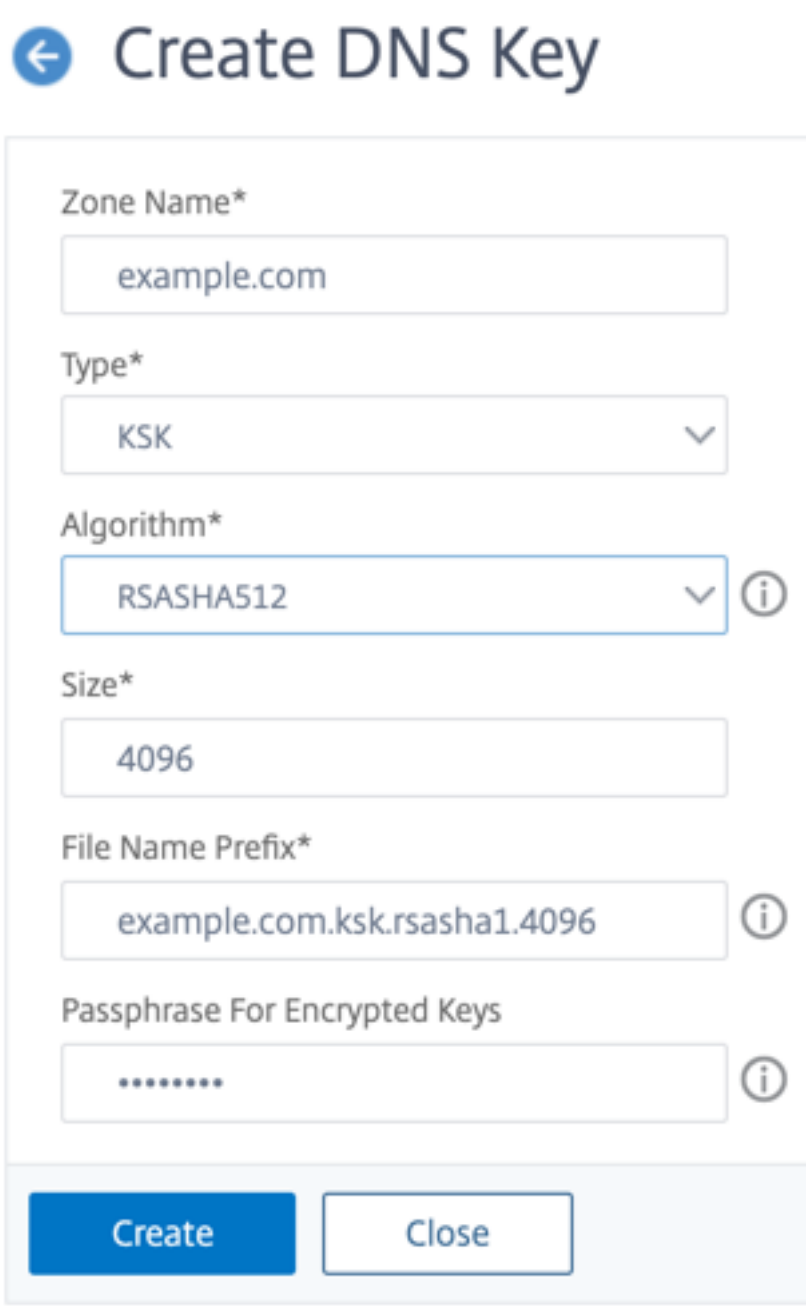
```
1 > create dns key -zoneName example.com -keyType zsk -algorithm
      RSASHA256 -keySize 1024 -fileNamePrefix example.com.zsk.rsasha1.1024
```



```
2 File Name: /nsconfig/dns/example.com.zsk.rsasha1.1024.key (public); /
     nsconfig/dns/example.com.zsk.rsasha1.1024.private (private); /
     nsconfig/dns/example.com.zsk.rsasha1.1024.ds (ds)
3 This operation may take some time, Please wait...
4  Done
5 > create dns key -zoneName example.com -keyType ksk -algorithm
     RSASHA512 -keySize 4096 -fileNamePrefix example.com.ksk.rsasha1.4096
6 File Name: /nsconfig/dns/example.com.ksk.rsasha1.4096.key (public); /
     nsconfig/dns/example.com.ksk.rsasha1.4096.private (private); /
     nsconfig/dns/example.com.ksk.rsasha1.4096.ds (ds)
7 This operation may take some time, Please wait...
8  Done
9 <!--NeedCopy-->
```

Crear una clave DNS mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > DNS**.
2. En el área de detalles, haga clic en **Crear clave DNS**.
3. Introduzca valores para los diferentes parámetros y haga clic en **Crear**.



Nota: Para modificar el prefijo de nombre de archivo de una clave existente:

- Haga clic en la flecha situada junto al botón **Examinar**.
- Haga clic en **Local** o **Appliance** (en función de si la clave existente está almacenada en el equipo local o en el `/nsconfig/dns/` directorio del dispositivo)
- Busque la ubicación de la clave y, a continuación, haga doble clic en ella.
  El cuadro **Prefijo de nombre de archivo** se rellena únicamente con el prefijo de la clave existente. Modifique el prefijo en consecuencia.

Publicar una clave DNS en una zona

Una clave (clave de firma de zona o clave de firma de clave) se publica en una zona agregando la clave al dispositivo ADC. Una clave debe publicarse en una zona antes de firmar la zona.

Antes de publicar una clave en una zona, la clave debe estar disponible en el directorio **/nsconfig/dns/**. Si creó la clave DNS en otro equipo (por ejemplo, mediante el programa `bind-keygen`), asegúrese de que la clave se agrega al directorio `/nsconfig/dns/`. A continuación, publique la clave en la zona. Utilice la GUI de ADC para agregar la clave al directorio `/nsconfig/dns/`. O bien, utilice algún otro programa para importar la clave al directorio, como Secure FTP (SFTP).

Utilice el `add dns key` comando para cada par de claves público-privadas que quiera publicar en una zona determinada. Si ha creado un par ZSK y un par KSK para una zona, utilice el `add dns key` comando para publicar primero uno de los pares de claves de la zona. Repita el comando para publicar el otro par de claves. Para cada clave que publique en una zona, se crea un registro de recursos DNSKEY en la zona.

El ejemplo que sigue a la sintaxis del comando publica primero el par de claves de firma de zona (creado para la zona example.com) en la zona. A continuación, el ejemplo utiliza el comando para publicar el par de claves de firma de claves en la zona.

Publicar una clave en una zona mediante la CLI

En el símbolo del sistema, escriba el siguiente comando para publicar una clave en una zona y verificar la configuración:

```
1 -  add dns key <keyName> <publickey> <privatekey> [-expires <
    positive_integer> [<units>]] [-notificationPeriod <positive_integer>
     [<units>]] [-TTL <secs>]
2 -  show dns zone [<zoneName> | -type <type>]
3 <!--NeedCopy-->
```

Ejemplo:

```
1 > add dns key example.com.zsk example.com.zsk.rsasha1.1024.key example.
    com.zsk.rsasha1.1024.private
2  Done
3 > add dns key example.com.ksk example.com.ksk.rsasha1.4096.key example.
    com.ksk.rsasha1.4096.private
4  Done
5 > show dns zone example.com
6          Zone Name : example.com
```



```
7           Proxy Mode : NO
8           Domain Name : example.com
9                   Record Types : NS SOA DNSKEY
10          Domain Name : ns1.example.com
11                  Record Types : A
12          Domain Name : ns2.example.com
13                  Record Types : A
14  Done
15 <!--NeedCopy-->
```

Publicar una clave en una zona DNS mediante la interfaz gráfica de usuario

Vaya a **Administración del tráfico > DNS > Claves**.

Nota: Para Clave pública y Clave privada, para agregar una clave almacenada en el equipo local, haga clic en la flecha situada junto al botón **Examinar**, haga clic en **Local**, busque la ubicación de la clave y, a continuación, haga doble clic en la clave.

Configurar una clave DNS

Puede configurar los parámetros de una clave publicada en una zona. Puede modificar los parámetros de tiempo de caducidad, período de notificación y tiempo de vida (TTL) de la clave. Si cambia el período de expiración de una clave, el dispositivo vuelve a firmar automáticamente todos los registros de recursos de la zona con la clave. La refirma ocurre si la zona está firmada con la clave en particular.

Configurar una clave mediante la CLI

En el símbolo del sistema, escriba el siguiente comando para configurar una clave y verificar la configuración:

```
1 -  set dns key <keyName> [-expires <positive_integer> [<units>]] [-
     notificationPeriod <positive_integer> [<units>]] [-TTL <secs>]
2 -  show dns key [<keyName>]
3 <!--NeedCopy-->
```

Ejemplo:

```
1 > set dns key example.com.ksk -expires 30 DAYS -notificationPeriod 3
     DAYS -TTL 3600
2  Done
```



```
> show dns key example.com.ksk
1)      Key Name: example.com.ksk
        Expires: 30 DAYS        Notification: 3 DAYS    TTL: 3600
        Public Key File: example.com.ksk.rsasha1.4096.key
        Private Key File: example.com.ksk.rsasha1.4096.private
 Done
<!--NeedCopy-->
```

Configurar una clave mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > DNS > Claves**.
2. En el panel de detalles, haga clic en la clave que quiere configurar y, a continuación, haga clic en Abrir.
3. En el cuadro de diálogo Configurar clave DNS, modifique los valores de los siguientes parámetros como se muestra:
   - Caduca: Caduca
   - Notification Period—notificationPeriod
   - TTL—TTL
4. Haga clic en Aceptar.

Firmar y anular la firma de una zona DNS

Para proteger una zona DNS, debe firmar la zona con las claves que se han publicado en la zona. Al firmar una zona, Citrix ADC crea un registro de recursos Next Secure (NSEC) para cada nombre de propietario. A continuación, utiliza la clave de firma de clave para firmar el conjunto de registros de recursos DNSKEY. Por último, utiliza ZSK para firmar todos los conjuntos de registros de recursos de la zona, incluidos los conjuntos de registros de recursos DNSKEY y los conjuntos de registros de recursos NSEC. Cada operación de signo da como resultado una firma para los conjuntos de registros de recursos en la zona. La firma se captura en un nuevo registro de recursos denominado registro de recursos RRSIG.

Después de firmar una zona, guarde la configuración.

Firmar una zona mediante la CLI

En el símbolo del sistema, escriba el siguiente comando para firmar una zona y verificar la configuración:


```
-  sign dns zone <zoneName> [-keyName <string> ...]
-  show dns zone [<zoneName> | -type (ADNS | PROXY | ALL)]
-  save config
<!--NeedCopy-->
```

Ejemplo:

```
> sign dns zone example.com -keyName example.com.zsk example.com.ksk
 Done
> show dns zone example.com
         Zone Name : example.com
         Proxy Mode : NO
         Domain Name : example.com
                 Record Types : NS SOA DNSKEY RRSIG NSEC
         Domain Name : ns1.example.com
                 Record Types : A RRSIG NSEC
         Domain Name : ns2.example.com
                 Record Types : A RRSIG
         Domain Name : ns2.example.com
                 Record Types : RRSIG NSEC
Done
> save config
 Done
<!--NeedCopy-->
```

Anular la firma de una zona mediante la CLI

En el símbolo del sistema, escriba el siguiente comando para anular la firma de una zona y verificar la configuración:

```
-  unsign dns zone <zoneName> [-keyName <string> ...]
-  show dns zone [<zoneName> | -type (ADNS | PROXY | ALL)]
<!--NeedCopy-->
```

Ejemplo:

```
> unsign dns zone example.com -keyName example.com.zsk example.com.ksk
 Done
> show dns zone example.com
```



```
4           Zone Name : example.com
5           Proxy Mode : NO
6           Domain Name : example.com
7                   Record Types : NS SOA DNSKEY
8           Domain Name : ns1.example.com
9                   Record Types : A
10          Domain Name : ns2.example.com
11                  Record Types : A
12  Done
13 <!--NeedCopy-->
```

Firmar o anular la firma de una zona mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > DNS > Zonas**.
2. En el panel de detalles, haga clic en la zona que quiere firmar y, a continuación, haga clic en Firmar/Anular firma.
3. En el cuadro de diálogo Firmar/Anular firma de la zona DNS, realice una de las acciones siguientes:
   - Para firmar la zona, active las casillas de verificación de las claves (clave de firma de zona y clave de firma de clave) con las que quiere firmar la zona.
     Puede firmar la zona con más de una clave de firma de zona o un par de claves de firma de clave.
   - Para anular la firma de la zona, desactive las casillas de verificación de las claves (clave de firma de zona y clave de firma de clave) con las que quiere anular la firma de la zona.
     Puede anular la firma de la zona con más de una clave de firma de zona o un par de claves de firma de clave.
4. Haga clic en Aceptar.

Ver los registros NSEC de un registro dado en una zona

Puede ver los registros NSEC que Citrix ADC crea automáticamente para cada nombre de propietario en la zona.

Ver el registro NSEC de un registro dado en una zona mediante la CLI

En el símbolo del sistema, escriba el comando siguiente para ver el registro NSEC de un registro dado en una zona:

```
show dns nsecRec [<hostName> | -type (ADNS | PROXY | ALL)]
```

Ejemplo:


```
> show dns nsecRec example.com
1)      Domain Name : example.com
        Next Nsec Name: ns1.example.com
        Record Types : NS SOA DNSKEY RRSIG NSEC
 Done
<!--NeedCopy-->
```

Ver el registro NSEC de un registro dado en una zona mediante la GUI

1. Vaya a **Administración del tráfico > DNS > Registros > Siguiente registros seguros**.
2. En el panel de detalles, haga clic en el nombre del registro para el que quiere ver el registro NSEC. El registro NSEC del registro seleccionado se muestra en el área Detalles.

Quitar una clave DNS

Elimine una clave de la zona en la que se publica cuando la clave ha caducado o si la clave ha sido comprometida. Cuando quita una clave de la zona, la zona se desfirma automáticamente con la clave. Al quitar la clave con este comando no se eliminan los archivos de clave presentes en el directorio /nsconfig/dns/. Si los archivos clave ya no son necesarios, deben eliminarse explícitamente del directorio.

Quitar una clave del Citrix ADC mediante la CLI

En el símbolo del sistema, escriba el siguiente comando para quitar una clave y verificar la configuración:

```
-  rm dns key <keyName>
-  show dns key <keyName>
<!--NeedCopy-->
```

Ejemplo:

```
> rm dns key example.com.zsk
 Done
> show dns key example.com.zsk
ERROR: No such resource [keyName, example.com.zsk]

<!--NeedCopy-->
```


Elimine una clave del Citrix ADC mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > DNS > Claves**.
2. En el panel de detalles, haga clic en el nombre de la clave que quiere quitar del ADC y, a continuación, haga clic en Quitar.

Configurar DNSSEC cuando Citrix ADC tiene autoridad para una zona

August 20, 2021

Cuando Citrix ADC tiene autoridad para una zona determinada, todos los registros de recursos de la zona se configuran en el ADC. Para firmar la zona autorizada, debe crear la firma de zona y las claves de firma de clave para la zona, agregar las claves al ADC y, a continuación, firmar la zona. Para obtener más información, consulte:

- Crear claves DNS para una zona
- Publicar una clave DNS en una zona
- Firmar y anular la firma de una zona DNS.

Si algún dominio GSLB configurado en el ADC pertenece a la zona que se está firmando, los nombres de dominio GSLB se firman junto con los demás registros que pertenecen a la zona.

Después de firmar una zona, las respuestas a las solicitudes de clientes compatibles con DNSSEC incluyen los registros de recursos RRSIG junto con los registros de recursos solicitados. DNSSEC debe estar habilitado en el ADC. Para obtener más información sobre cómo habilitar DNSSEC, consulte Habilitar y inhabilitar DNSSEC.

Por último, después de configurar DNSSEC para la zona autorizada, debe guardar la configuración de Citrix ADC.

Configurar DNSSEC para una zona para la que Citrix ADC es un servidor proxy DNS

August 20, 2021

El procedimiento para firmar una zona para la que Citrix ADC está configurado como servidor proxy DNS depende de si el ADC posee un subconjunto de la información de zona propiedad de los servidores de nombres back-end. Si lo hace, la configuración se considera una configuración de propiedad de zona parcial. Si el ADC no posee un subconjunto de la información de zona, la configuración de Citrix ADC para administrar los servidores back-end se considera una configuración de servidor proxy DNS sin zona. Las tareas básicas de configuración DNSSEC para ambas configuraciones de Citrix ADC

son las mismas. Sin embargo, la firma de la zona parcial en Citrix ADC requiere algunos pasos de configuración adicionales.

Nota: Los términos configuración del servidor proxy sin zona y zona parcial solo se utilizan en el contexto del dispositivo Citrix ADC.

Importante: Cuando se configura en modo proxy, el ADC no realiza la verificación de firma en las respuestas DNSSEC antes de actualizar la caché.

Si configura el ADC como un proxy DNS para equilibrar la carga de resolvers (servidores) conscientes de DNSSEC, debe establecer la opción Recursión disponible mientras configura el servidor virtual DNS. Si una consulta DNSSEC llega con el bit Checking Disabled (CD) establecido, la consulta se pasa al servidor con el bit de CD conservado. La respuesta del servidor no se almacena en caché.

Configurar DNSSEC para una configuración de servidor proxy DNS sin zonas

Para una configuración de servidor proxy DNS sin zona, la firma de zona debe realizarse en los servidores de nombres back-end. En Citrix ADC, configure el ADC como un servidor proxy DNS para la zona. Cree un servidor virtual de equilibrio de carga de tipo de protocolo DNS. Configure los servicios en el ADC para representar los servidores de nombres. A continuación, vincule los servicios al servidor virtual de equilibrio de carga. Para obtener más información sobre estas tareas de configuración, consulte Configurar NetScaler como servidor proxy DNS.

Cuando un cliente envía al ADC una solicitud DNS con el bit DNSSEC Aceptar (DO) configurado, el ADC comprueba su caché para la información solicitada. Si los registros de recursos no están disponibles en su caché, el ADC reenvía la solicitud a uno de los servidores de nombres DNS. A continuación, retransmite la respuesta del servidor de nombres al cliente. Además, el ADC almacena en caché los registros de recursos RRSIG junto con la respuesta del servidor de nombres. Las solicitudes posteriores de clientes compatibles con DNSsec se sirven desde la caché (incluidos los registros de recursos RRSIG), sujeto al parámetro de tiempo de vida (TTL). Si un cliente envía una solicitud DNS sin establecer el bit DO, el ADC responde solo con los registros de recursos solicitados. No incluye los registros de recursos RRSIG específicos de DNSSEC.

Configurar DNSSEC para una configuración de propiedad de zona parcial

En algunas configuraciones de ADC, aunque la autoridad para una zona recae en los servidores de nombres back-end, un subconjunto de los registros de recursos pertenecientes a la zona podría configurarse en el ADC. El ADC solo posee (o tiene autoridad para) este subconjunto de registros. Este subconjunto de registros puede considerarse como una *zona parcial* en el ADC. El ADC posee la zona parcial. Todos los demás registros son propiedad de los servidores de nombres back-end.

Una configuración típica de zona parcial en el Citrix ADC se ve cuando:

- Los dominios de equilibrio de carga global del servidor (GSLB) se configuran en el ADC

- Los dominios GSLB forman parte de una zona para la que los servidores de nombres back-end son autoritativos.

Firmar una zona que incluya solo una zona parcial en el ADC implica:

- Inclusión de la información de zona parcial en los archivos de zona del servidor de nombres back-end
- Firma de la zona en los servidores de nombres back-end
- Firma de la zona parcial en el ADC.

Se debe usar el mismo conjunto de claves para firmar la zona en los servidores de nombres y la zona parcial en el ADC.

Firmar la zona en los servidores de nombres back-end

1. Incluya los registros de recursos contenidos en la zona parcial, en los archivos de zona de los servidores de nombres.
2. Cree claves y utilice las claves para firmar la zona en los servidores de nombres back-end.

Firmar la zona parcial en el Citrix ADC

1. Cree una zona con el nombre de la zona propiedad de los servidores de nombres back-end. Al configurar la zona parcial, establezca el parámetro ProxyMode en YES. Esta zona es la zona parcial que contiene los registros de recursos propiedad del ADC.

   Por ejemplo, si el nombre de la zona configurada en los servidores de nombres back-end es example.com, debe crear una zona denominada example.com en el ADC. Establezca el parámetro ProxyMode en YES. Para obtener más información sobre cómo agregar una zona, consulte Configurar una zona DNS.

   > **Nota**
   >
   > No agregue registros SOA y NS para la zona. Estos registros deben existir en el ADC para una zona para la que el ADC sea autorizado.

2. Importe las claves (desde uno de los servidores de nombres back-end) al ADC y, a continuación, agréguelas al directorio /nsconfig/dns/. Para obtener más información sobre cómo importar una clave y agregarla al ADC, consulte Publicar una clave DNS en una zona.
3. Firme la zona parcial con las claves importadas. Al firmar la zona parcial con las claves, el ADC genera registros RRSIG y NSEC para los conjuntos de registros de recursos y registros de recursos individuales en la zona parcial, respectivamente. Para obtener más información sobre cómo firmar una zona, consulte Firmar y anular la firma de una zona DNS.

Configurar DNSSEC para nombres de dominio de equilibrio de carga de servidor global (GSLB)

August 20, 2021

Si GSLB está configurado en Citrix ADC y el ADC tiene autoridad para la zona a la que pertenecen los nombres de dominio GSLB, todos los nombres de dominio GLSB se firman cuando se firma la zona. Para obtener más información sobre la firma de una zona para la que el ADC tiene autoridad, consulte Configurar DNSSEC cuando el dispositivo Citrix ADC tiene autoridad para una zona.

Si los dominios GSLB pertenecen a una zona para la que los servidores de nombres back-end tienen autoridad, debe:

- Primero firme la zona en los servidores de nombres.
- A continuación, firme la zona parcial en el ADC para completar la configuración de DNSSEC para la zona.

Para obtener más información, consulte Configurar DNSSEC para una configuración de propiedad parcial de zona.

Mantenimiento de zonas

August 20, 2021

Desde la perspectiva de DNSSEC, el mantenimiento de la zona implica pasar por las claves de firma de zona y las claves de firma de claves cuando la expiración de la clave es inminente. Estas tareas de mantenimiento de zonas deben realizarse manualmente. La zona se vuelve a firmar automáticamente y no requiere ninguna intervención manual.

Volver a firmar una zona actualizada

Cuando se actualiza una zona (agregar un registro o modificar un registro existente), el dispositivo vuelve a firmar automáticamente el nuevo registro (o modificado). Si una zona contiene varias claves de firma de zona, el dispositivo vuelve a firmar el nuevo registro (o modificado) con la clave utilizada para firmar la zona.

Roll over keys DNSSEC

Nota: Pase manualmente las claves DNSSEC (KSK, ZSK) antes de que caduquen.

En Citrix ADC, puede utilizar los métodos de prepublicación y doble firma para realizar un rollover de la clave de firma de zona y la clave de firma de claves. Más información acerca de estos dos métodos de rollover está disponible en RFC 4641, “Prácticas operacionales DNSSEC”.

Los temas siguientes asignan comandos del ADC a los pasos de los procedimientos de rollover descritos en RFC 4641.

La notificación de caducidad de la clave se envía a través de una captura SNMP llamada dnskeyExpiry. Se envían tres variables MIB, DNSKeyName, DNSKeyTimeToExpirate y DNSKeyUnitsSofExpirate junto con la captura SNMP de DNSKeyExpirate. Para obtener más información, consulte Referencia de OID *SNMP de Citrix NetScaler en Referencia de OID*SNMP de NetScaler 12.0.

Prepublicar el rollover de claves

RFC 4641, “Prácticas operativas de DNSSEC” define cuatro etapas para el método de conversión de clave previa a la publicación: inicial, nuevo DNSKEY, RRSIGs nuevos y eliminación de DNSKEY. Cada etapa está asociada a un conjunto de tareas que debe realizar en el ADC. A continuación se presentan las descripciones de cada etapa y las tareas que debe realizar. El procedimiento de rollover descrito aquí se puede utilizar tanto para las claves de firma de claves como para las claves de firma de zona.

- **Etapa 1: Inicial.** La zona contiene solo los conjuntos de claves con los que se ha firmado la zona actualmente. El estado de la zona en la etapa inicial es el estado de la zona justo antes de comenzar el proceso de rollover de claves.

  Ejemplo:

  Considere la clave, example.com.zsk1, con la que está firmada la zona example.com. La zona contiene solo los RRSIGs generados por la clave example.com.zsk1, que debe caducar. La clave de firma de claves es example.com.ksk1.

- **Etapa 2: Nuevo DNSKEY.** Se crea y publica una nueva clave en la zona. Es decir, la clave se agrega al ADC, pero la zona no se firma con la nueva clave hasta que se complete la fase de pre-roll. En esta etapa, la zona contiene la clave antigua, la clave nueva y los RRSIGs generados por la clave anterior. La publicación de la nueva clave durante la duración completa de la fase de pre-roll proporciona al registro de recursos DNSKEY correspondiente al nuevo tiempo de clave para propagarse a los servidores de nombres secundarios.

  Ejemplo:

  Se agrega una nueva clave example.com.zsk2 a la zona example.com. La zona no está firmada con example.com.zsk2 hasta que se complete la fase de pre-roll. La zona example.com contiene registros de recursos DNSKEY para example.com.zsk1 y example.com.zsk2.

  Comandos Citrix ADC:

  Realice las siguientes tareas en el ADC:

- Cree una clave DNS mediante el comando `create dns key`.

  Para obtener más información sobre cómo crear una clave DNS, incluido un ejemplo, consulte Crear claves DNS para una zona.

- Publique la nueva clave DNS en la zona mediante el comando `add dns key`.

  Para obtener más información sobre cómo publicar la clave en la zona, incluido un ejemplo, consulte Publicar una clave DNS en una zona.

- **Etapa 3: Nuevos RRSIG.** La zona se firma con la nueva clave DNS y, a continuación, se desfirma con la clave DNS antigua. La clave DNS antigua no se quita de la zona y permanece publicada hasta que caduquen los RRSIGs generados por la clave anterior.

  Ejemplo:

  La zona está firmada con example.com.zsk2 y, a continuación, sin firmar con example.com.zsk1. La zona continúa publicando example.com.zsk1 hasta que caduquen los RRSIGs generados por example.com.zsk1.

  Comandos Citrix ADC:

  Realice las siguientes tareas en el ADC:

  - Firme la zona con la nueva clave DNS mediante el comando `sign dns zone`.
  - Anule la firma de la zona con la clave DNS antigua mediante el comando `unsign dns zone`.

  Para obtener más información sobre cómo firmar y anular la firma de una zona, incluidos ejemplos, consulte Firmar y anular la firma de una zona DNS.

- **Etapa 4: Eliminación de DNSKEY.** Cuando caducan los RRSIGs generados por la clave DNS antigua, la clave DNS antigua se quita de la zona.

  Ejemplo:

  La clave DNS antigua example.com.zsk1 se elimina de la zona example.com.

  Comandos Citrix ADC

  En el ADC, quite la clave DNS antigua mediante el comando `rm dns key`. Para obtener más información sobre cómo quitar una clave de una zona, incluido un ejemplo, consulte Eliminar una clave DNS.

Rollover de clave de firma doble

RFC 4641, "Prácticas operativas de DNSSEC" define tres etapas para el rollover de clave de firma doble: Inicial, nuevo DNSKEY y eliminación de DNSKEY. Cada etapa está asociada a un conjunto de tareas que debe realizar en el ADC. A continuación se presentan las descripciones de cada etapa y las tareas que

debe realizar. El procedimiento de rollover descrito aquí se puede utilizar tanto para las claves de firma de claves como para las claves de firma de zona.

- **Etapa 1: Inicial.** La zona contiene solo los conjuntos de claves con los que se ha firmado la zona actualmente. El estado de la zona en la etapa inicial es el estado de la zona justo antes de comenzar el proceso de rollover de claves.

  Ejemplo:

  Considere la clave, example.com.zsk1, con la que está firmada la zona example.com. La zona contiene solo los RRSIGs generados por la clave example.com.zsk1, que debe caducar. La clave de firma de claves es example.com.ksk1.

- **Etapa 2: Nuevo DNSKEY.** La nueva clave se publica en la zona y la zona se firma con la nueva clave. La zona contiene los RRSIGs generados por las claves antiguas y nuevas. La duración mínima para la que la zona debe contener ambos conjuntos de RRSIGs es el tiempo necesario para que todos los RRSIGs caduquen.

  Ejemplo:

  Se agrega una nueva clave example.com.zsk2 a la zona example.com. La zona está firmada con example.com.zsk2. La zona example.com ahora contiene los RRSIGs generados a partir de ambas claves.

  Comandos Citrix ADC

  Realice las siguientes tareas en el ADC:

  - Cree una clave DNS mediante el comando `create dns key`.

    Para obtener más información sobre cómo crear una clave DNS, incluido un ejemplo, consulte Crear claves DNS para una zona.

  - Publique la nueva clave en la zona mediante el comando `add dns key`.

    Para obtener más información sobre cómo publicar la clave en la zona, incluido un ejemplo, consulte Publicar una clave DNS en una zona.

  - Firme la zona con la nueva clave mediante el comando `sign dns zone`.

    Para obtener más información sobre cómo firmar una zona, incluidos ejemplos, consulte Firmar y anular la firma de una zona DNS.

- **Etapa 3: Eliminación de DNSKEY.** Cuando caducan los RRSIGs generados por la clave DNS antigua, la clave DNS antigua se quita de la zona.

  Ejemplo:

  La clave DNS antigua example.com.zsk1 se elimina de la zona example.com.

  Comandos Citrix ADC:

En el ADC, quite la clave DNS antigua mediante el comando `rm dns key`.

Para obtener más información sobre cómo quitar una clave de una zona, incluido un ejemplo, consulte Eliminar una clave DNS.

Descarga las operaciones DNSSEC al Citrix ADC

August 20, 2021

En las zonas DNS para las que los servidores DNS tienen autoridad, las operaciones DNSSEC se pueden descargar en el dispositivo ADC. En una implementación de descarga DNSSEC, un servidor DNS envía respuestas sin firmar. El ADC firma la respuesta dinámicamente antes de retransmitir al cliente. El ADC también almacena en caché la respuesta firmada. Además de reducir la carga en los servidores DNS, la descarga de operaciones DNSSEC al ADC ofrece las siguientes ventajas:

- Puede firmar registros que los servidores DNS generan mediante programación. Dichos registros no se pueden firmar mediante operaciones rutinarias de firma de zona realizadas en los servidores DNS.
- Puede proporcionar respuestas firmadas a los clientes incluso si no ha implementado DNSSEC en sus servidores.

Para configurar la descarga de DNSSEC, debe configurar un servidor virtual de equilibrio de carga DNS, configurar los servicios que representan los servidores DNS y, a continuación, enlazar los servicios al servidor virtual. Para obtener información sobre cómo configurar un servidor virtual de equilibrio de carga DNS, configurar servicios y vincular los servicios al servidor virtual, consulte Configurar una zona DNS.

Cree una entidad de zona en el ADC para cada zona DNS cuyas operaciones DNSSEC desee descargar. Para cada zona DNS, debe habilitar los parámetros Modo proxy y Descarga DNSSEC. Opcionalmente, puede configurar la generación de registros NSEC para una zona de descarga. Para crear una entidad de zona DNS para la descarga de DNSSEC, siga las instrucciones de este tema.

Para completar la configuración, debe generar claves DNS para la zona, agregar las claves a la zona y, a continuación, firmar la zona con las claves. Este proceso es el mismo que para DNSSEC normal. Para obtener información sobre cómo crear claves, agregar claves a una zona y firmar la zona, consulte Extensiones de seguridad del sistema de nombres de dominio.

Después de configurar la descarga de DNS, debe vaciar la caché DNS en Citrix ADC. Al vaciar la caché DNS se asegura de que todos los registros sin firmar en la caché se eliminan y, a continuación, se reemplazan por registros firmados. Para obtener información sobre cómo vaciar la caché DNS, consulte Vaciar registros DNS.

Habilitar la descarga de DNSSEC para una zona mediante la CLI

En la línea de comandos, escriba los siguientes comandos para habilitar la descarga de DNSSEC para una zona y compruebe la configuración:

```
1 -  add dns zone <zoneName> -proxyMode YES -dnssecOffload ENABLED [-nsec
     ( ENABLED | DISABLED )
2 -  show dns zone
3 <!--NeedCopy-->
```

Ejemplo:

```
1 > add dns zone example.com -proxyMode YES -dnssecOffload ENABLED nsec
    ENABLED
2  Done
3 > show dns zone example.com
4      Zone Name : example.com
5      Proxy Mode : YES
6      DNSSEC Offload: ENABLED    NSEC: ENABLED
7  Done
8 <!--NeedCopy-->
```

Habilitar la descarga de DNSSEC para una zona mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > DNS > Zonas**.
2. En el panel de detalles, realice una de las acciones siguientes:
   - Para crear una zona en Citrix ADC, haga clic en Agregar.
   - Para configurar la descarga de DNSSEC para una zona existente, haga doble clic en la zona.
3. En el cuadro de diálogo Crear zona DNS o Configurar zona DNS, active las casillas de verificación Modo proxy y Descarga DNSSEC.
4. Si quiere que Citrix ADC genere registros NSEC para la zona, active la casilla de verificación NSEC.

Soporte de partición de administración para DNSSEC

February 16, 2021

En un dispositivo Citrix ADC con particiones, las claves DNS que se generan se almacenan en las siguientes ubicaciones:

- Partición predeterminada: /nsconfig/dns/
- Partición no predeterminada: /nsconfig/partitions/ <partitionname> /dns/

Ahora puede agregar una contraseña a la clave DNS. Para agregar una contraseña a la clave DNS, primero debe agregar la contraseña en el `create dns key` comando. A continuación, proporcione la misma contraseña en el `add dns key` comando al agregar la clave DNS al dispositivo ADC. Por ejemplo:

```
create dns key -zoneName com -keytype ksK -algorithm rsASHA1 -keysize 4096
- fileNamePrefix com.ksk.rsasha1.4096 -password 1jsfd3Wa

add dns key com.zsk.4096 /nsconfig/dns/com.zsk.rsasha1.4096.private -
password 1jsfd3Wa
```

Nota:

- Para un entorno con particiones predeterminado, las claves se leen desde la ubicación predeterminada/nsconfig/dns/. Sin embargo, si las claves se almacenan en una ubicación diferente, el nombre de la ruta debe proporcionarse en el `add dns key -private` comando. Por ejemplo: `add dns key -private <path name>`.
- Para un entorno con particiones no predeterminado, las claves se leen desde la ubicación predeterminada `/nsconfig/partitions/<partitionname>/dns/`.

Compatibilidad con dominios DNS comodín

August 20, 2021

Los dominios DNS comodín se utilizan para gestionar solicitudes de dominios y subdominios inexistentes. En una zona, utilice dominios comodín para redirigir consultas de todos los dominios o subdominios inexistentes a un servidor determinado, en lugar de crear un registro de recursos (RR) independiente para cada dominio. El uso más común de un dominio DNS comodín es crear una zona que se pueda utilizar para reenviar correo desde Internet a otro sistema de correo.

En la resolución DNS, los RR comodín admiten el dominio comodín. Los RR comodín se utilizan para sintetizar las respuestas a las consultas de un nombre de dominio inexistente. Por ejemplo, si ha consultado `http://image.example.com`y el subdominio "imagen" no existe, es posible que se le redirija a example.com.

Un registro comodín tiene un carácter de asterisco (*) como etiqueta situada más a la izquierda de un nombre de dominio. Por ejemplo, `*.example.com`. Un asterisco en cualquier otro lugar del nombre de dominio significa un registro DNS comodín. Por ejemplo, no **new**`.*.example.com` es un registro DNS comodín válido.

> **Nota**
>
> - El dominio comodín solo se admite cuando el dispositivo Citrix ADC tiene autoridad para la zona y está configurado como un servidor proxy DNS o ADNS.
> - El dominio comodín no es compatible con los registros NS y SOA.
> - El dominio comodín no se puede aplicar cuando la consulta está en otra zona.
> - El dominio comodín no se puede aplicar cuando se sabe que existe el QNAME o un nombre entre el dominio comodín y el QNAME.

Ejemplo de configuración

```
add dns soaRec example.com -originServer n1.example.com -contact admin.
   example.com

add dns nsRec example.com n1.example.com

add dns nsRec example.com n2.example.com

add dns zone example.com  -proxyMode no

add dns addrec www.example.com 2.2.2.2

add dns addrec *.example.com 10.10.10.10

add dns addrec *.example.com 10.10.10.11

add dns aaaarec *.example.com 2001::1
<!--NeedCopy-->
```

En el ejemplo, se agrega un nombre de dominio comodín para un registro A y AAAA.

Cuando se recibe una consulta para un nombre de dominio que existe en la zona, el dispositivo Citrix ADC responde con la respuesta correspondiente. Por ejemplo, para `www.example.com`, el dispositivo responde con 2.2.2.2 en el ejemplo.

Para un nombre de dominio inexistente que coincida con un tipo de comodín, se entrega una respuesta sintetizada.

En el ejemplo, el dispositivo Citrix ADC responde con 10.10.10.10 y 10.10.10.11 para un nombre de dominio que no existe.example.com o xyz.example.com.

La síntesis comodín no es aplicable a un nombre de dominio que existe en la zona.

Por ejemplo, para la consulta `www.example.com` y el tipo AAAA, el dispositivo Citrix ADC no sintetiza con comodín, ya que `www.example.com` existe con el tipo A. En el ejemplo, el dispositivo Citrix ADC

responde con una respuesta NODATA.

Para una consulta, digamos abc.example.com y escriba AAAA, el dispositivo Citrix ADC responde con una respuesta sintetizada. Por ejemplo, para `www.example.com`, el dispositivo responde con 2001:DB8::1 en el ejemplo.

Mitigar ataques DDoS DNS

August 20, 2021

Los servidores DNS son uno de los componentes más críticos de una red y deben ser defendidos contra ataques. Uno de los tipos más básicos de ataques DNS es el ataque DDoS. Los ataques de este tipo están en aumento y pueden ser destructivos. Puede hacer lo siguiente para mitigar los ataques DDoS:

- Vacar registros negativos.
- Restringir el tiempo de vida (TTL) de los registros negativos.
- Conserve la memoria de Citrix ADC limitando la memoria consumida por la caché DNS.
- Conservar los registros DNS en la caché.
- Habilitar la omisión de caché DNS.

Vaciar registros negativos

Un ataque DNS llena la caché con registros negativos (NXDOMAIN y NODATA). Como resultado, las respuestas a solicitudes legítimas no se almacenan en caché, por lo que las nuevas solicitudes se envían a un servidor back-end para su resolución DNS. Por lo tanto, las respuestas se retrasan.

Ahora puede vaciar los registros DNS negativos de la caché DNS del dispositivo Citrix ADC.

Vacíe los registros de caché negativos mediante la CLI

En el símbolo del sistema, escriba:

```
flush dns proxyrecords -type (dnsRecordType | negRecType)NXDOMAIN | NODATA
```

Ejemplo:

```
flush dns proxyrecords -negRecType NODATA
```

Descarga de registros de caché negativos mediante la interfaz gráfica de usuario

1. Vaya a **Configuración** > **Administración del tráfico** > **DNS** > **Registros**.
2. En el panel de detalles, haga clic en **Vacar registros proxy**.
3. En el cuadro **Tipo de vaciado**, seleccione **Registros negativos**.

4. En el cuadro **Tipo de registros negativos**, seleccione **NXDOMAIN** o **NODATA**.

Protección contra ataques aleatorios de subdominios y NXDOMAIN

Para evitar ataques aleatorios de subdominio y NXDOMAIN, puede restringir la memoria caché DNS y ajustar los valores TTL para los registros negativos.

Para limitar la cantidad de memoria consumida por la caché DNS, especifique el tamaño máximo de caché (en MB) y también el tamaño de caché (en MB) para almacenar las respuestas negativas. Cuando se alcanza cualquiera de los límites, no se agregan más entradas a la caché. Además, se registran mensajes syslog y, si ha configurado capturas SNMP, se generan capturas SNMP. Si no se establecen estos límites, el almacenamiento en caché continúa hasta que se agota la memoria del sistema.

Un valor TTL más alto para los registros negativos puede dar como resultado el almacenamiento de registros que no son valiosos durante mucho tiempo. Un valor TTL más bajo da como resultado el envío de más solicitudes al servidor back-end.

El TTL del registro negativo se establece en un valor que puede ser el menor del valor TTL o el valor" Caduca" del registro SOA.

Nota:

- Esta limitación se agrega por motor de paquetes. Por ejemplo, si MaxCacheSize se establece en 5 MB y el dispositivo tiene 3 motores de paquetes, el tamaño total de la caché es de 15 MB.
- El tamaño de la caché para los registros negativos debe ser menor o igual al tamaño máximo de la caché.
- Si reduce el límite de memoria caché DNS a un valor inferior a la cantidad de datos ya almacenados en caché, el tamaño de la caché permanece por encima del límite hasta que los datos se agotan. Es decir, excede su TTL0 o se vacía (`flush dns proxyrecords` comando o Vacío de registros proxy en la GUI de Citrix ADC).
- Para configurar capturas SNMP, consulte Configuración de NetScaler para generar capturas SNMP.

Limite la memoria consumida por la caché DNS mediante la CLI

En el símbolo del sistema, escriba:

```
set dns parameter -maxCacheSize <MBytes> -maxNegativeCacheSize <MBytes>
```

Ejemplo:

```
set dns parameter - maxCacheSize 100 -maxNegativeCacheSize 25
```


Limite la memoria consumida por la caché DNS mediante la interfaz gráfica de usuario

Vaya a **Configuración** > **Administración del tráfico** > **DNS**, haga clic en **Cambiar configuración de DNS** y establezca los siguientes parámetros:

- Tamaño máximo de caché en MB
- Tamaño máximo de caché negativo en MB

Restringir el TTL de registros negativos mediante la CLI

En el símbolo del sistema, escriba:

```
set dns parameter -maxnegcacheTTL <secs>
```

Ejemplo:

```
set dns parameter -maxnegcacheTTL 360
```

Restringir el TTL de los registros negativos mediante la GUI

1. Vaya a **Configuración** > **Administración del tráfico** > **DNS**.
2. Haga clic en **Cambiar configuración DNS** y establezca el parámetro **TTL de caché negativa máxima en segundos**.

Conservar registros DNS en la caché

Un ataque puede inundar la caché DNS con entradas no importantes, pero puede provocar el vaciado de los registros legítimos ya almacenados en caché para dar espacio a las nuevas entradas. Para evitar que los ataques llenen la caché con datos no válidos, puede conservar los registros legítimos incluso después de que superen sus valores TTL.

Si habilita el parámetro cacheNoExpire, los registros actualmente en la caché se conservan hasta que inhabilite el parámetro.

Nota:

- Esta opción solo se puede utilizar cuando se especifica el tamaño máximo de la caché (parámetro MaxCacheSize).
- Si MaxNegcachettl está configurado y CachenoExpire está habilitado, CachenoExpire toma prioridad.

Conservar registros DNS en la caché mediante la CLI

En el símbolo del sistema, escriba:

```
set dns parameter -cacheNoExpire ( ENABLED | DISABLED)
```


Ejemplo:

```
set dns parameter -cacheNoExpire ENABLED
```

Conservar registros DNS en la caché mediante la interfaz gráfica de usuario

1. Vaya a **Configuración** > **Administración del tráfico** > **DNS** y haga clic en **Cambiar configuración de DNS**.
2. Seleccione **Caché Sin caducar**.

Habilitar omisión de caché DNS

Para una mayor visibilidad y control de las solicitudes DNS, establezca el parámetro CacheHitBypass para reenviar todas las solicitudes a los servidores back-end y permitir que la caché se construya pero no se utilice. Después de generar la caché, puede inhabilitar el parámetro para que las solicitudes se sirvan desde la caché.

Habilitar la omisión de caché DNS mediante la CLI

En el símbolo del sistema, escriba:

```
set dns parameter -cacheHitBypass ( ENABLED | DISABLED )
```

Ejemplo:

```
set dns parameter -cacheHitBypass ENABLED
```

Habilitar la omisión de caché DNS mediante la interfaz gráfica de usuario

1. Vaya a **Configuración** > **Administración del tráfico** > **DNS** y haga clic en **Cambiar configuración de DNS**.
2. Seleccione **Bypass de aciertos de caché**.

Prevenir el `Slowloris` ataque

Una consulta DNS que abarca varios paquetes presenta la amenaza potencial de un `Slowloris` ataque. El dispositivo Citrix ADC puede eliminar de forma silenciosa las consultas DNS que se dividen en varios paquetes.

Puede establecer el `splitPktQueryProcessing` parámetro en ALLOW o DROP una consulta DNS si la consulta está dividida en varios paquetes.

Nota: Esta configuración solo es aplicable para DNS TCP.

Limite las consultas DNS a un solo paquete mediante la CLI

En el símbolo del sistema, escriba:

```
set dns parameter -splitPktQueryProcessing ( ALLOW | DROP )
```

Ejemplo:

```
set dns parameter -splitPktQueryProcessing DROP
```

Limite las consultas DNS a un solo paquete mediante la interfaz gráfica de usuario

1. Vaya a **Configuración** > **Administración del tráfico** > **DNS** y haga clic en **Cambiar configuración de DNS**.
2. En el cuadro **Procesamiento de consultas de paquetes divididos**, elija **Permitir** o **DROP**.

Recopilar estadísticas de las respuestas DNS servidas desde la caché

Puede recopilar estadísticas de las respuestas DNS servidas desde la caché. A continuación, utilice estas estadísticas para crear un umbral más allá del cual se elimina más tráfico DNS y aplique este umbral con una directiva basada en ancho de banda. Anteriormente, el cálculo del ancho de banda para un servidor virtual de equilibrio de carga DNS no era preciso, porque no se notificaba el número de solicitudes servidas desde la caché.

En modo proxy, las estadísticas de bytes de solicitud, bytes de respuesta, Total de paquetes recibidos y Total de paquetes enviados se actualizan continuamente. Anteriormente, estas estadísticas no siempre se actualizaban, especialmente para un servidor virtual de equilibrio de carga DNS.

El modo proxy también ahora le permite determinar el número de respuestas DNS servidas desde la caché. Para recopilar estas estadísticas, se han agregado las siguientes opciones al `stat lb vserver <DNSvirtualServerName>` comando:

- **Solicitudes**: Número total de solicitudes recibidas por el servidor virtual DNS o DNS_TCP. Incluye las solicitudes reenviadas al back-end y las solicitudes respondidas desde la caché.
- **Visitas de vserver**: Número total de solicitudes reenviadas al back-end. El número de solicitudes servidas desde la caché es la diferencia entre el número total de solicitudes y el número de solicitudes servidas desde el servidor virtual.
- **Respuestas**: Número total de respuestas enviadas por este servidor virtual. Por ejemplo, si un servidor virtual LB de DNS recibió 5 solicitudes DNS, reenvió 3 de ellas al back-end y sirvió 2 de ellas desde la caché, el valor correspondiente de cada una de estas estadísticas sería el siguiente:
  - **Hits de vserver**: 3
  - **Solicitudes**: 5
  - **Respuestas**: 5

Equilibrio de carga del firewall

August 20, 2021

El equilibrio de carga del firewall distribuye el tráfico a través de varios firewalls, lo que proporciona tolerancia a fallos y un mayor rendimiento. El equilibrio de carga del firewall protege su red mediante:

- Dividir la carga entre los firewalls, lo que elimina un solo punto de falla y permite que la red escale.
- Aumento de la alta disponibilidad.

La configuración de un dispositivo Citrix ADC para el equilibrio de carga del firewall es similar a la configuración del equilibrio de carga, con la excepción de que el tipo de servicio recomendado es ANY, el tipo de monitor recomendado es PING y el modo de servidor virtual de equilibrio de carga está configurado en MAC.

Puede configurar el equilibrio de carga del firewall en una configuración de entorno sándwich, empresarial o de múltiples servidores de seguridad. El entorno sándwich se utiliza para equilibrar la carga del tráfico que entra en la red desde el exterior y el tráfico que sale de la red a Internet, e implica la configuración de dos dispositivos Citrix ADC, uno a cada lado de un conjunto de firewalls. Configurar un entorno empresarial para el tráfico de equilibrio de carga que sale de la red a Internet. El entorno empresarial implica la configuración de un único dispositivo Citrix ADC entre la red interna y los firewalls que proporcionan acceso a Internet. El entorno de firewall múltiple se utiliza para el tráfico de equilibrio de carga procedente de otro firewall. Tener habilitado el equilibrio de carga del firewall en ambos lados del dispositivo Citrix ADC mejora el flujo de tráfico tanto en la dirección de salida como de entrada, y garantiza un procesamiento más rápido del tráfico. El entorno de firewall múltiple implica la configuración de un dispositivo Citrix ADC intercalado entre dos firewalls.

Importante: Si configura rutas estáticas en el dispositivo Citrix ADC para la dirección IP de destino y habilita el modo L3, el dispositivo Citrix ADC utiliza su tabla de redirección para enrutar el tráfico en lugar de enviar el tráfico al servidor vserver de equilibrio de carga.

Nota: Para que FTP funcione, se debe configurar un servidor o servicio virtual adicional en el dispositivo Citrix ADC con dirección IP y puerto como* y 21 respectivamente, y el tipo de servicio especificado como FTP. En este caso, el dispositivo Citrix ADC administra el protocolo FTP aceptando la conexión de control FTP, modificando la carga útil y administrando la conexión de datos, todo ello a través del mismo firewall.

El equilibrio de carga del firewall solo admite algunos de los métodos de equilibrio de carga admitidos en el dispositivo Citrix ADC. Además, puede configurar solo algunos tipos de persistencia y monitores.

Métodos de equilibrio de carga del firewall

Los siguientes métodos de equilibrio de carga son compatibles con el equilibrio de carga del firewall.

- Menos conexiones
- Round Robin
- Menos paquetes
- Ancho de banda mínimo
- Hash IP de origen
- Hash IP de destino
- Hash IP de destino de IP de origen
- Hash del puerto de origen IP de origen
- Método de tiempo de respuesta mínimo (LRTM)
- Carga personalizada

Persistencia del firewall

Solo se admite la persistencia basada en SOURCEIP, DESTIP y SOURCEIPDESTIP para el equilibrio de carga del firewall.

Supervisión del servidor de firewall

Solo se admiten monitores PING y transparentes en el equilibrio de carga del firewall. Puede enlazar un monitor PING (predeterminado) al servicio back-end que representa el firewall. Si un firewall está configurado para no responder a los paquetes de ping, puede configurar monitores transparentes para supervisar los hosts del lado de confianza a través de firewalls individuales.

Entorno Sandwich

August 20, 2021

Una implementación de Citrix ADC en modo sandwich puede equilibrar la carga del tráfico de red a través de firewalls en ambas direcciones: entrada (tráfico que entra en la red desde el exterior, como Internet) y salida (tráfico que sale de la red a Internet).

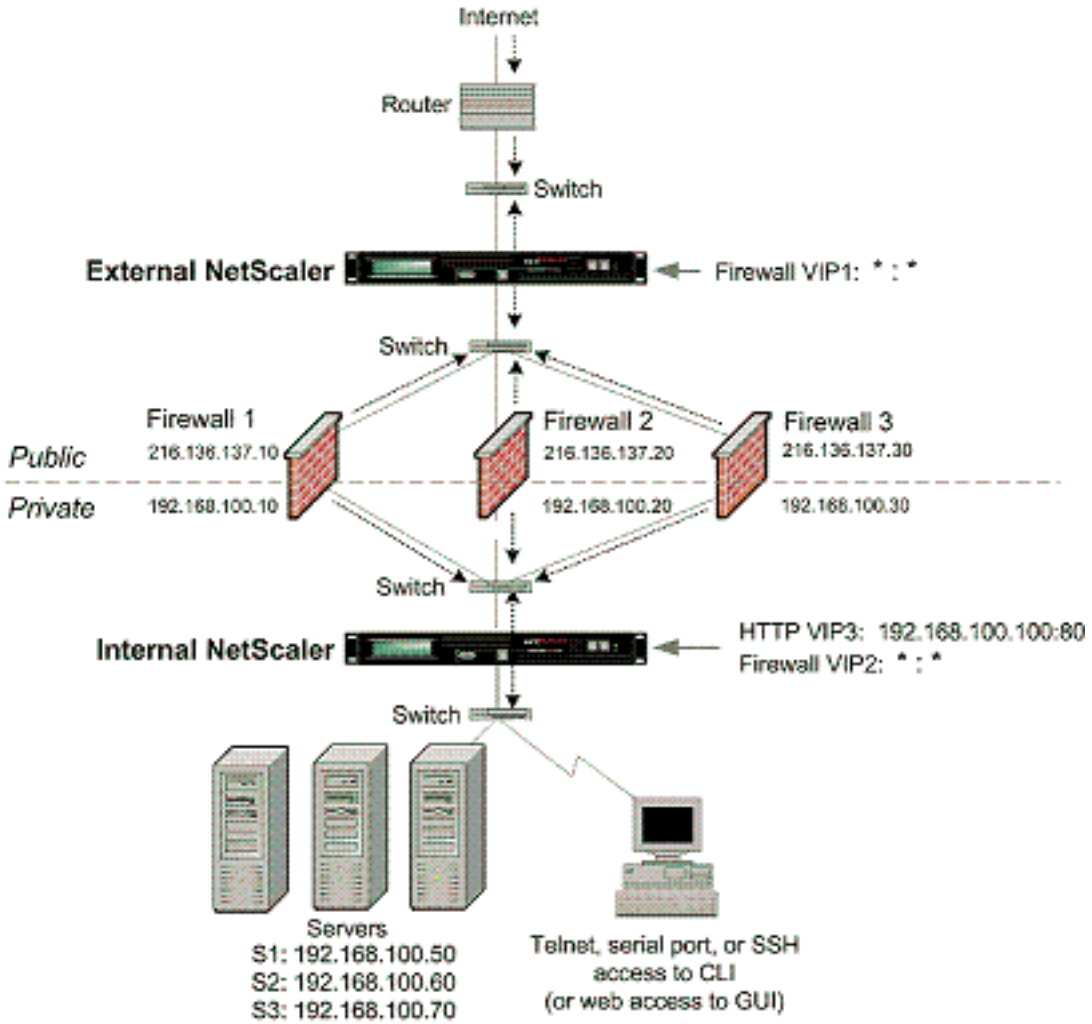
En esta configuración, un dispositivo Citrix ADC se encuentra a cada lado de un conjunto de firewalls. El Citrix ADC situado entre los firewalls e Internet, denominado dispositivo Citrix ADC externo que gestiona el tráfico de entrada, selecciona el mejor firewall, según el método configurado. El Citrix ADC entre los firewalls y la red privada, denominado dispositivo Citrix ADC interno, realiza un seguimiento del firewall desde el que se recibe el paquete inicial de una sesión. A continuación, se asegura de que todos los paquetes subsiguientes para esa sesión se envían al mismo firewall.

El dispositivo Citrix ADC interno se puede configurar como un administrador de tráfico normal para equilibrar la carga del tráfico en los servidores de red privados. Esta configuración también permite

equilibrar la carga del tráfico procedente de la red privada (salida) a través de los firewalls.

El siguiente diagrama muestra el entorno de equilibrio de carga del firewall sándwich.

Ilustración 1. Equilibrio de carga del firewall (sándwich)



El tipo de servicio ANY configura Citrix ADC para aceptar todo el tráfico.

Para aprovechar los beneficios relacionados con HTTP y TCP, configure el servicio y el servidor virtual con el tipo HTTP o TCP. Para que FTP funcione, configure el servicio con el tipo FTP.

Configuración del dispositivo Citrix ADC externo en un entorno sándwich

Realice las siguientes tareas para configurar el dispositivo Citrix ADC externo en un entorno sándwich

- Habilite la función de equilibrio de carga.
- Configure un servicio comodín para cada firewall.
- Configure un monitor para cada servicio comodín.
- Configure un servidor virtual comodín para el tráfico procedente de Internet.

- Configure el servidor virtual en el modo de reescritura MAC.
- Enlazar servicios al servidor virtual comodín.
- Guarde y verifique la configuración.

Habilitar la función de equilibrio de carga

Para habilitar el equilibrio de carga mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba el siguiente comando para habilitar el equilibrio de carga y verificar la configuración:

```
enable ns feature LB
show ns feature
<!--NeedCopy-->
```

Ejemplo:

```
> enable ns feature LoadBalancing
 Done
> show ns feature

        Feature                         Acronym              Status
        -------                         -------              ------
 1)     Web Logging                     WL                   OFF
 2)     Surge Protection                SP                   ON
 3)     Load Balancing                  LB                   ON
 .
 .
 .
 24)    NetScaler Push                  push                 OFF
 Done
<!--NeedCopy-->
```

Para habilitar el equilibrio de carga mediante la utilidad de configuración

Vaya a **Sistema > Configuración** y, en **Configurar funciones básicas**, seleccione **Equilibrio de carga**.

Configurar un servicio comodín para cada firewall

Para configurar un servicio comodín para cada firewall mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
add service <name> <serverName> ANY *
<!--NeedCopy-->
```

Ejemplo:

```
add service Service-HTTP-1 10.102.29.5 ANY *
<!--NeedCopy-->
```

Para configurar un servicio comodín para cada firewall mediante la utilidad de configuración

Vaya a **Administración del tráfico > Equilibrio de carga > Servicios** y agregue un servicio. Especifique **ANY** en el campo **Protocolo** y * en el campo Puerto.

Configurar un monitor para cada servicio comodín

Un monitor PING está enlazado de forma predeterminada al servicio. Debe configurar un monitor transparente para supervisar los hosts en el lado de confianza a través de firewalls individuales. A continuación, puede enlazar el monitor transparente a los servicios. El monitor PING predeterminado supervisa la conectividad solo entre el dispositivo Citrix ADC y el dispositivo ascendente. El monitor transparente supervisa todos los dispositivos existentes en la ruta de acceso desde el dispositivo al dispositivo que posee la dirección IP de destino especificada en el monitor. Si no se configura un monitor transparente y el estado del firewall es UP, pero uno de los dispositivos de salto siguiente de ese firewall está inactivado, el dispositivo incluye el firewall mientras realiza el equilibrio de carga y reenvía el paquete al firewall. Sin embargo, el paquete no se entrega al destino final porque uno de los dispositivos de salto siguiente está caído. Al vincular un monitor transparente, si alguno de los dispositivos (incluido el firewall) está inactivo, el servicio se marca como DOWN y el firewall no se incluye cuando el dispositivo realiza el equilibrio de carga del firewall.

El enlace de un monitor transparente anula el monitor PING. Para configurar un monitor PING además de un monitor transparente, después de crear y enlazar un monitor transparente, debe enlazar un monitor PING al servicio.

Para configurar un monitor transparente mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para configurar un monitor transparente y verificar la configuración:


```
add lb monitor <monitorName> <type> [-destIP <ip_addr|ipv6_addr|*>] [-
    transparent (YES | NO )]
bind lb monitor <monitorName> <serviceName>
<!--NeedCopy-->
```

Ejemplo:

```
add monitor monitor-HTTP-1 HTTP -destip 10.10.10.11 -transparent YES
bind monitor monitor-HTTP-1 fw-svc1
To bind a PING monitor, type the following command:
bind monitor PING fw-svc1
<!--NeedCopy-->
```

Para crear y enlazar un monitor transparente mediante la utilidad de configuración

Vaya a **Administración del tráfico > Equilibrio de carga > Monitores**y, a continuación, cree y enlaque un monitor transparente.

Configurar un servidor virtual comodín para el tráfico procedente de Internet

Para configurar un servidor virtual comodín para el tráfico procedente de Internet mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
add lb vserver <name> ANY * *
<!--NeedCopy-->
```

Ejemplo:

```
add lb vserver Vserver-LB-1 ANY * *
<!--NeedCopy-->
```

Para configurar un servidor virtual comodín para el tráfico procedente de Internet mediante la utilidad de configuración

Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales** y cree un servidor virtual comodín. Especifique **ANY** en el campo **Protocolo** y * en el campo Puerto.

Configurar el servidor virtual en el modo de reescritura MAC

Para configurar el servidor virtual en el modo de reescritura MAC mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
set lb vserver <name>@ -m <RedirectionMode>
<!--NeedCopy-->
```

Ejemplo:

```
set lb vserver Vserver-LB-1 -m MAC
<!--NeedCopy-->
```

Para configurar el servidor virtual en el modo de reescritura MAC mediante la utilidad de configuración

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**y seleccione el servidor virtual para el que quiere configurar el modo de redirección (por ejemplo, vServer-LB-1).
2. Modifique la sección **Configuración básica** y haga clic en **más**.
3. En la lista desplegable **Modo de redirección**, seleccione **Basado en MAC**.

Vincular servicios al servidor virtual comodín

Para enlazar un servicio al servidor virtual comodín mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Ejemplo:

```
bind lb vserver Vserver-LB-1 Service-HTTP-1
<!--NeedCopy-->
```


Para enlazar un servicio al servidor virtual comodín mediante la utilidad de configuración

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales** y seleccione el servidor virtual para el que quiere enlazar el servicio.
2. Haga clic en la sección **Servicios** y seleccione un servicio para enlazar.

Guardar y verificar la configuración

Cuando haya terminado las tareas de configuración, asegúrese de guardar la configuración. Asegúrese de que la configuración sea correcta.

Para guardar y verificar la configuración mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para configurar un monitor transparente y verificar la configuración:

```
save ns config
show vserver
<!--NeedCopy-->
```

Ejemplo:

```
save config
sh lb vserver FWLBVIP1
FWLBVIP1 (\*:\*) - ANY    Type: ADDRESS
        State: UP
        Last state change was at Mon Jun 14 06:40:14 2010
        Time since last state change: 0 days, 00:00:11.240
        Effective State: UP  ARP:DISABLED
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  2 (Total)       2 (Active)
        Configured Method: SRCIPDESTIPHASH
        Mode: MAC
        Persistence: NONE
        Connection Failover: DISABLED

1) fw_svc_1 (10.102.29.251: *) - ANY State: UP  Weight: 1
2) fw_svc_2 (10.102.29.18: \*) - ANY State: UP   Weight: 1
 Done
```



```
show service fw-svc1
        fw-svc1 (10.102.29.251:\*) - ANY
        State: DOWN
        Last state change was at Thu Jul  8 10:04:50 2010
        Time since last state change: 0 days, 00:00:38.120
        Server Name: 10.102.29.251
        Server ID : 0   Monitor Threshold : 0
        Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
        Use Source IP: NO
        Client Keepalive(CKA): NO
        Access Down Service: NO
        TCP Buffering(TCPB): YES
        HTTP Compression(CMP): NO
        Idle timeout: Client: 120 sec   Server: 120 sec
        Client IP: DISABLED
        Cacheable: NO
        SC: OFF
        SP: OFF
        Down state flush: ENABLED

1)      Monitor Name: monitor-HTTP-1
                State: DOWN     Weight: 1
                Probes: 5       Failed [Total: 5 Current: 5]
                Last response: Failure - Time out during TCP connection
                    establishment stage
                Response Time: 2000.0 millisec
2)      Monitor Name: ping
                State: UP       Weight: 1
                Probes: 3       Failed [Total: 0 Current: 0]
                Last response: Success - ICMP echo reply received.
                Response Time: 1.415 millisec
 Done
<!--NeedCopy-->
```

Configuración del dispositivo Citrix ADC interno en un entorno sándwich

Realice las siguientes tareas para configurar el dispositivo Citrix ADC interno en un entorno sándwich

Para el tráfico desde el servidor (salida)

- Habilite la función de equilibrio de carga.
- Configure un servicio comodín para cada firewall.
- Configure un monitor para cada servicio comodín.
- Configure un servidor virtual comodín para equilibrar la carga del tráfico enviado a los firewalls.

- Configure el servidor virtual en el modo de reescritura MAC.
- Enlazar servicios de firewall al servidor virtual comodín.

Para el tráfico a través de servidores de red privados

- Configure un servicio para cada servidor virtual.
- Configure un monitor para cada servicio.
- Configure un servidor virtual HTTP para equilibrar el tráfico enviado a los servidores.
- Enlazar servicios HTTP al servidor virtual HTTP.
- Guarde y verifique la configuración.

Habilitar la función de equilibrio de carga

Puede configurar entidades de equilibrio de carga como servicios y servidores virtuales cuando la función de equilibrio de carga está inhabilitada. Pero no funcionarán hasta que habilite la función.

Para habilitar el equilibrio de carga mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba el siguiente comando para habilitar el equilibrio de carga y verificar la configuración:

```
enable ns feature LB
show ns feature
<!--NeedCopy-->
```

Ejemplo:

```
> enable ns feature LoadBalancing
 Done
> show ns feature

        Feature                         Acronym             Status
        -------                         -------             ------
 1)     Web Logging                     WL                  OFF
 2)     Surge Protection                SP                  ON
 3)     Load Balancing                  LB                  ON
 .
 .
 .
 24)    NetScaler Push                  push                OFF
 Done
<!--NeedCopy-->
```


Para habilitar el equilibrio de carga mediante la utilidad de configuración

Vaya a **Sistema > Configuración** y, en Configurar funciones básicas, seleccione **Equilibrio de carga**.

Configurar un servicio comodín para cada firewall

Para configurar un servicio comodín para cada firewall mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
add service <name> <serverName> ANY *
<!--NeedCopy-->
```

Ejemplo:

```
add service Service-HTTP-1 10.102.29.5 ANY *
<!--NeedCopy-->
```

Para configurar un servicio comodín para cada firewall mediante la utilidad de configuración

Vaya a **Administración del tráfico > Equilibrio de carga > Servicios** y agregue un servicio. Especifique **ANY** en el campo **Protocolo** y * en el campo Puerto.

Configurar un monitor para cada servicio comodín

Un monitor PING está enlazado de forma predeterminada al servicio. Debe configurar un monitor transparente para supervisar los hosts en el lado de confianza a través de firewalls individuales. A continuación, puede enlazar el monitor transparente a los servicios. El monitor PING predeterminado supervisa la conectividad solo entre el dispositivo Citrix ADC y el dispositivo ascendente. El monitor transparente supervisa todos los dispositivos existentes en la ruta de acceso desde el dispositivo al dispositivo que posee la dirección IP de destino especificada en el monitor. Si no se configura un monitor transparente y el estado del firewall es UP, pero uno de los dispositivos de salto siguiente de ese firewall está inactivado, el dispositivo incluye el firewall mientras realiza el equilibrio de carga y reenvía el paquete al firewall. Sin embargo, el paquete no se entrega al destino final porque uno de los dispositivos de salto siguiente está caído. Al vincular un monitor transparente, si alguno de los dispositivos (incluido el firewall) está inactivo, el servicio se marca como DOWN y el firewall no se incluye cuando el dispositivo realiza el equilibrio de carga del firewall.

El enlace de un monitor transparente anula el monitor PING. Para configurar un monitor PING además de un monitor transparente, después de crear y enlazar un monitor transparente, debe enlazar un monitor PING al servicio.

Para configurar un monitor transparente mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para configurar un monitor transparente y verificar la configuración:

```
add lb monitor <monitorName> <type> [-destIP <ip_addr|ipv6_addr|*>] [-
   transparent (YES | NO )]
bind lb monitor <monitorName> <serviceName>
<!--NeedCopy-->
```

Ejemplo:

```
add monitor monitor-HTTP-1 HTTP -destip 10.10.10.11 -transparent YES
bind monitor monitor-HTTP-1 fw-svc1
<!--NeedCopy-->
```

Para crear y enlazar un monitor transparente mediante la utilidad de configuración

1. Vaya a **Administración del tráfico > Equilibrio de carga > Monitores** y cree un monitor.
2. En el cuadro de diálogo **Crear monitor**, introduzca los parámetros necesarios y seleccione **Transparente**.

Configurar un servidor virtual comodín para equilibrar la carga del tráfico enviado a los firewalls

Para configurar un servidor virtual comodín para equilibrar la carga del tráfico enviado a los firewalls mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
add lb vserver <name> ANY * *
<!--NeedCopy-->
```

Ejemplo:


```
add lb vserver Vserver-LB-1 ANY * *
<!--NeedCopy-->
```

Para configurar un servidor virtual comodín para el tráfico procedente de Internet mediante la utilidad de configuración

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales** y cree un servidor virtual comodín.
2. Especifique **CUALQUIERA** en el campo Protocolo y ***** en el campo Puerto.

Para configurar un servidor virtual comodín para equilibrar la carga del tráfico enviado a los firewalls mediante la utilidad de configuración

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. En el panel de detalles, haga clic en Agregar.
3. En el cuadro de diálogo Crear servidor virtual (equilibrio de carga), especifique valores para los siguientes parámetros como se muestra:
   - Nombre: Name
4. En Protocolo, seleccione CUALQUIERA y, en Dirección IP y Puerto, seleccione *.
5. Haga clic en Crear y, a continuación, en Cerrar. El servidor virtual creado aparece en el panel Servidores virtuales de equilibrio de carga.

Configurar el servidor virtual en el modo de reescritura MAC

Para configurar el servidor virtual en el modo de reescritura MAC mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
set lb vserver <name>@ -m <RedirectionMode>
<!--NeedCopy-->
```

Ejemplo:

```
set lb vserver Vserver-LB-1 -m MAC
<!--NeedCopy-->
```


Para configurar el servidor virtual en el modo de reescritura MAC mediante la utilidad de configuración

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**y seleccione el servidor virtual para el que quiere configurar el modo de redirección (por ejemplo, vServer-LB-1).
2. Modifique la sección **Configuración básica** y haga clic en **más**.
3. En la lista desplegable **Modo de redirección**, seleccione **Basado en MAC**.

Vincular servicios de firewall al servidor virtual comodín

Para enlazar servicios de firewall al servidor virtual comodín mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Ejemplo:

```
bind lb vserver Vserver-LB-1 Service-HTTP-1
<!--NeedCopy-->
```

Para enlazar servicios de firewall al servidor virtual comodín mediante la utilidad de configuración

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**y seleccione un servidor virtual.
2. Haga clic en la sección Servicio y seleccione un servicio para enlazar.

Nota: Puede enlazar un servicio a varios servidores virtuales.

Configurar un servicio para cada servidor virtual

Para configurar un servicio para cada servidor virtual mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:


```
add service <name> <serverName> HTTP <port>
<!--NeedCopy-->
```

Ejemplo:

```
add service Service-HTTP-1 10.102.29.5 HTTP 80
<!--NeedCopy-->
```

Para configurar un servicio para cada servidor virtual mediante la utilidad de configuración

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servicios**y configure un servicio para cada servidor virtual.
2. Especifique **HTTP** en el campo **Protocolo** y seleccione **HTTP** en **Monitores disponibles**.

Para configurar un servicio para cada servidor virtual mediante la utilidad de configuración

1. Vaya a **Administración de Tráfico > Equilibrio de carga > Servicios**.
2. En el panel de detalles, haga clic en Agregar.
3. En el cuadro de diálogo Crear servicio, especifique valores para los siguientes parámetros como se muestra:
   - Nombre del servicio: Nombre
   - Servidor: NombreServidor
   - Puerto: Puerto
4. En Protocolo, especifique HTTP. En Monitores disponibles, seleccione HTTP.
5. Haga clic en Crear y, a continuación, en Cerrar. El servicio creado aparece en el panel Servicios.

Configurar un monitor para cada servicio

Para enlazar un monitor a un servicio mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
bind lb monitor <monitorName> <ServiceName>
<!--NeedCopy-->
```

Ejemplo:


```
bind mon monitor-HTTP-1 Service-HTTP-1
<!--NeedCopy-->
```

Para enlazar un monitor a un servicio mediante la utilidad de configuración

Vaya a **Administración del tráfico > Equilibrio de carga > Servicios**, haga doble clic en un servicio y agregue un monitor.

Configurar un servidor virtual HTTP para equilibrar el tráfico enviado a los servidores

Para configurar un servidor virtual HTTP para equilibrar el tráfico enviado a los servidores mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
add lb vserver <name> HTTP <ip> <port>
<!--NeedCopy-->
```

Ejemplo:

```
add lb vserver Vserver-LB-1 HTTP 10.102.29.60 80
<!--NeedCopy-->
```

Para configurar un servidor virtual HTTP para equilibrar el tráfico enviado a los servidores mediante la utilidad de configuración

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servicios virtuales**y configure un servidor virtual HTTP.
2. Especifique **HTTP** en el campo **Protocolo**.

Para configurar un servidor virtual HTTP para equilibrar el tráfico enviado a los servidores mediante la utilidad de configuración

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. En el panel de detalles, haga clic en Agregar.
3. En el cuadro de diálogo Crear servidor virtual (equilibrio de carga), especifique valores para los siguientes parámetros como se muestra:
    - Nombre: Name

- Dirección IP: Dirección IP
  Nota: si el servidor virtual utiliza IPv6, active la casilla de verificación IPv6 e introduzca la dirección en formato IPv6 (por ejemplo, **1000:0000:0000:0000:0005:0600:700 a:888b**).
- Puerto: Puerto

4. En Protocolo, seleccione HTTP.
5. Haga clic en Crear y, a continuación, en Cerrar. El servidor virtual creado aparece en el panel Servidores virtuales de equilibrio de carga.

Guardar y verificar la configuración

Cuando haya terminado las tareas de configuración, asegúrese de guardar la configuración. También debe verificar para asegurarse de que la configuración sea correcta.

Para guardar y verificar la configuración mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para configurar un monitor transparente y verificar la configuración:

- `save ns config`
- `show vserver`

Ejemplo:

```
save config
show lb vserver FWLBVIP2
        FWLBVIP2 (\*:\*) - ANY    Type: ADDRESS
        State: UP
        Last state change was at Mon Jun 14 07:22:54 2010
        Time since last state change: 0 days, 00:00:32.760
        Effective State: UP
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  2 (Total)       2 (Active)
        Configured Method: LEASTCONNECTION
        Current Method: Round Robin, Reason: A new service is bound
        Mode: MAC
        Persistence: NONE
        Connection Failover: DISABLED

1) fw-int-svc1 (10.102.29.5: *) - ANY State: UP Weight: 1
```



```
2) fw-int-svc2 (10.102.29.9: \*) - ANY State: UP Weight: 1
 Done
show service fw-int-svc1
        fw-int-svc1 (10.102.29.5:\*) - ANY
        State: DOWN
        Last state change was at Thu Jul  8 14:44:51 2010
        Time since last state change: 0 days, 00:01:50.240
        Server Name: 10.102.29.5
        Server ID : 0   Monitor Threshold : 0
        Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
        Use Source IP: NO
        Client Keepalive(CKA): NO
        Access Down Service: NO
        TCP Buffering(TCPB): NO
        HTTP Compression(CMP): NO
        Idle timeout: Client: 120 sec   Server: 120 sec
        Client IP: DISABLED
        Cacheable: NO
        SC: OFF
        SP: OFF
        Down state flush: ENABLED

1)      Monitor Name: monitor-HTTP-1
                State: DOWN     Weight: 1
                Probes: 9       Failed [Total: 9 Current: 9]
                Last response: Failure - Time out during TCP connection
                    establishment stage
                Response Time: 2000.0 millisec
2)      Monitor Name: ping
                State: UP       Weight: 1
                Probes: 3       Failed [Total: 0 Current: 0]
                Last response: Success - ICMP echo reply received.
                Response Time: 1.275 millisec
 Done
<!--NeedCopy-->
```

Para guardar y verificar la configuración mediante la utilidad de configuración

1. En el panel **Detalles**, haga clic en **Guardar**.
2. En el cuadro de diálogo **Guardar configuración**, haga clic en **Sí**.
3. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
4. En el panel **Detalles**, seleccione el servidor virtual que creó en el paso 5.
5. Compruebe que la configuración mostrada en el panel **Detalles** sea correcta.

6. Vaya a **Administración de Tráfico > Equilibrio de carga > Servicios**.
7. En el panel **Detalles**, seleccione los servicios que creó en el paso 5.
8. Compruebe que la configuración mostrada en el panel **Detalles** sea correcta.

Supervisión de una configuración de equilibrio de carga de firewall en un entorno sandwich

Después de que la configuración esté activa y en ejecución, debe ver las estadísticas de cada servicio y servidor virtual para comprobar si hay posibles problemas.

Visualización de las estadísticas de un servidor virtual

Para evaluar el rendimiento de los servidores virtuales o solucionar problemas, puede mostrar detalles de los servidores virtuales configurados en el dispositivo Citrix ADC. Puede mostrar un resumen de estadísticas para todos los servidores virtuales o puede especificar el nombre de un servidor virtual para mostrar las estadísticas solo para ese servidor virtual. Puede mostrar los siguientes detalles:

- Nombre
- Dirección IP
- Port
- Protocolo
- Estado del servidor virtual
- Tasa de solicitudes recibidas
- Tasa de visitas

Para mostrar las estadísticas del servidor virtual mediante la interfaz de línea de comandos

Para mostrar un resumen de las estadísticas de todos los servidores virtuales configurados actualmente en Citrix ADC, o de un único servidor virtual, en el símbolo del sistema, escriba:

```
stat lb vserver [-detail] [<name>]
<!--NeedCopy-->
```

Ejemplo:

```
>stat lb vserver -detail
Virtual Server(s) Summary
                      vsvrIP  port     Protocol        State    Req/s
                           Hits/s
```



```
4  One                          *    80          HTTP            UP       5/s
           0/s
5  Two                          *     0           TCP          DOWN       0/s
           0/s
6  Three                        *  2598           TCP          DOWN       0/s
           0/s
7  dnsVirtualNS    10.102.29.90    53           DNS          DOWN       0/s
           0/s
8  BRVSERV            10.10.1.1    80          HTTP          DOWN       0/s
           0/s
9  LBVIP           10.102.29.66    80          HTTP            UP       0/s
           0/s
10  Done
11
12 <!--NeedCopy-->
```

Para mostrar las estadísticas del servidor virtual mediante la utilidad de configuración

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales > Estadísticas**.
2. Si desea mostrar las estadísticas de un solo servidor virtual, en el panel de detalles, seleccione el servidor virtual y haga clic en **Estadísticas**.

Visualización de las estadísticas de un servicio

Puede ver la tasa de solicitudes, respuestas, bytes de solicitud, bytes de respuesta, conexiones de cliente actuales, solicitudes en cola de sobretensiones, conexiones de servidor actuales, etc. mediante las estadísticas de servicio.

Para ver las estadísticas de un servicio mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
1 stat service <name>
2 <!--NeedCopy-->
```

Ejemplo:

```
1 stat service Service-HTTP-1
2 <!--NeedCopy-->
```


Para ver las estadísticas de un servicio mediante la utilidad de configuración

1. Vaya a **Administración del Tráfico > Equilibrio de carga > Servicios > Estadísticas**.
2. Si quiere mostrar las estadísticas de un solo servicio, seleccione el servicio y haga clic en **Estadísticas**.

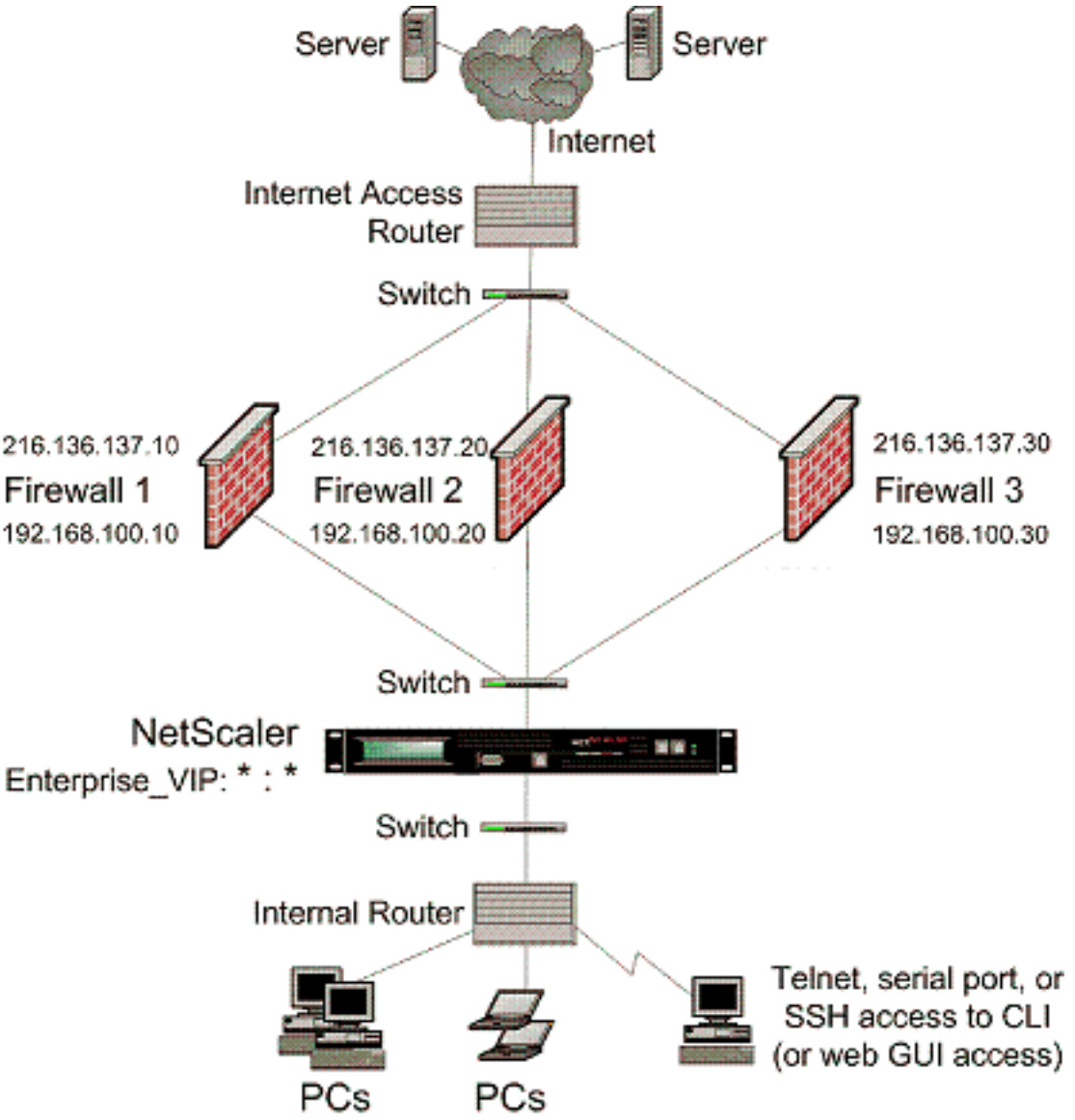
Entorno empresarial

June 22, 2022

En la configuración empresarial, el Citrix ADC se coloca entre los firewalls que se conectan a Internet pública y la red privada interna y maneja el tráfico de salida. El Citrix ADC selecciona el mejor firewall en función de la directiva de equilibrio de carga configurada.

El siguiente diagrama muestra el entorno de equilibrio de carga del firewall empresarial

Ilustración 1. Equilibrio de carga de los firewalls



El tipo de servicio ANY configura Citrix ADC para que acepte todo el tráfico.

Para aprovechar los beneficios relacionados con HTTP y TCP, configure el servicio y el vserver con el tipo HTTP o TCP. Para que funcione FTP, configure el servicio con el tipo FTP.

Configuración de Citrix ADC en un entorno empresarial

Realice las siguientes tareas para configurar un Citrix ADC en un entorno empresarial.

Para el tráfico del servidor (salida)

- Habilite la función de equilibrio de carga.
- Configure un servicio comodín para cada firewall.
- Configure un monitor para cada servicio comodín.

- Configure un servidor virtual comodín para equilibrar la carga del tráfico enviado a los firewalls.
- Configure el servidor virtual en modo de reescritura MAC.
- Enlazar los servicios de firewall al servidor virtual comodín.

Para tráfico a través de servidores de redes privadas

- Configure un servicio para cada servidor virtual.
- Configure un monitor para cada servicio.
- Configure un servidor virtual HTTP para equilibrar el tráfico enviado a los servidores.
- Enlazar los servicios HTTP al servidor virtual HTTP.
- Guarde y verifique la configuración.

En este ejemplo de configuración, se considera uno de los servidores de firewall que se muestra en el diagrama de topología de red (ilustración 1).

Habilitar la función de equilibrio de carga

Puede configurar entidades de equilibrio de carga, como servicios y servidores virtuales, cuando la función de equilibrio de carga está inhabilitada, pero no funcionarán hasta que habilite la función.

Para habilitar el equilibrio de carga mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba el siguiente comando para habilitar el equilibrio de carga y verificar la configuración:

- habilitar la función NS LB
- función show ns

Ejemplo:

```
> enable ns feature LoadBalancing
 Done
> show ns feature

        Feature                         Acronym             Status
        -------                         -------             ------
 1)     Web Logging                     WL                  OFF
 2)     Surge Protection                SP                  ON
 3)     Load Balancing                  LB                  ON
 .
 .
 .
 24)    NetScaler Push                  push                OFF
 Done
```



```
<!--NeedCopy-->
```

Para habilitar el equilibrio de carga mediante la utilidad de configuración

Vaya a Sistema > Configuración y, en Configurar funciones básicas, seleccione Equilibrio de carga.

Configurar un servicio comodín para cada firewall

Para configurar un servicio comodín para cada firewall mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
add service <name> <serverName> ANY *
<!--NeedCopy-->
```

Ejemplo:

```
add service Service-HTTP-1 192.168.100.10 ANY *
<!--NeedCopy-->
```

Para configurar un servicio comodín para cada firewall mediante la utilidad de configuración

1. Vaya a Administración del tráfico > Equilibrio de carga > Servicios.
2. En el panel de detalles, haga clic en Agregar.
3. En el cuadro de diálogo Crear servicio, especifique valores para los siguientes parámetros, como se muestra a continuación:
   - Nombre del servicio: nombre
   - server—nombreDeServidor
4. En Protocolo, seleccione CUALQUIERA y, en Puerto, seleccione *.
5. Haga clic en Crear y, a continuación, en Cerrar. El servicio que creó aparece en el panel Servicios.

Configurar un monitor para cada servicio comodín

Un monitor PING está enlazado de forma predeterminada al servicio. Deberá configurar un monitor transparente para monitorear los hosts en el lado de confianza a través de firewalls individuales. A continuación, puede vincular el monitor transparente a los servicios. El monitor PING predeterminado supervisa la conectividad solo entre el dispositivo Citrix ADC y el dispositivo ascendente. El

monitor transparente supervisa todos los dispositivos existentes en la ruta desde el dispositivo hasta el dispositivo que posee la dirección IP de destino especificada en el monitor. Si no se configura un monitor transparente y el estado del firewall es ACTIVO, pero uno de los dispositivos de siguiente salto de ese firewall está inactivo, el dispositivo incluye el firewall mientras realiza el equilibrio de carga y reenvía el paquete al firewall. Sin embargo, el paquete no se entrega al destino final porque uno de los dispositivos del siguiente salto está inactivo. Al vincular un monitor transparente, si alguno de los dispositivos (incluido el firewall) está inactivo, el servicio se marca como INACTIVO y el firewall no se incluye cuando el dispositivo realiza el equilibrio de carga del firewall.

La vinculación de un monitor transparente anulará el monitor PING. Para configurar un monitor PING además de un monitor transparente, después de crear y vincular un monitor transparente, debe vincular un monitor PING al servicio.

Para configurar un monitor transparente mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para configurar un monitor transparente y verificar la configuración:

```
add lb monitor <monitorName> <type> [-destIP <ip_addr|ipv6_addr|*>] [-
    transparent (YES | NO )]
bind lb monitor <monitorName> <serviceName>
<!--NeedCopy-->
```

Ejemplo:

```
add monitor monitor-HTTP-1 HTTP -destip 10.10.10.11 -destport 80 -
    transparent YES
bind monitor monitor-HTTP-1 fw-svc1
<!--NeedCopy-->
```

Para crear y vincular un monitor transparente mediante la utilidad de configuración

1. Vaya a Administración del tráfico > Equilibrio de carga > Monitores.
2. En el panel de detalles, haga clic en Agregar.
3. En el cuadro de diálogo Crear monitor, especifique los valores como se muestra:
   - Nombre*
   - Tipo*: tipo
   - IP de destino

- Transparente

-* Un parámetro obligatorio

4. Haga clic en Crear y, a continuación, en Cerrar. En el panel Monitores, seleccione el monitor que acaba de configurar y compruebe que la configuración que se muestra en la parte inferior de la pantalla es correcta.

Configurar un servidor virtual comodín para equilibrar la carga del tráfico enviado a los firewalls

El tráfico que pasa a través de los firewalls está destinado a diferentes proxies o servidores que se colocan detrás de los firewalls. Estos servidores proxy o servidores pueden tener diferentes direcciones IP y puertos. Para que el tráfico pase de forma transparente a través de los firewalls, la dirección IP y el puerto del servidor virtual que equilibra la carga de los firewalls deben configurarse como * para aceptar el tráfico de cualquier dirección IP y puerto.

Para configurar un servidor virtual comodín para equilibrar la carga del tráfico enviado a los firewalls mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
add lb vserver <name> ANY * *
<!--NeedCopy-->
```

Ejemplo:

```
add lb vserver Vserver-LB-1 ANY * *
<!--NeedCopy-->
```

Para configurar un servidor virtual comodín para equilibrar la carga del tráfico enviado a los firewalls mediante la utilidad de configuración

1. Vaya a Administración del tráfico > Equilibrio de carga > Servidores virtuales.
2. En el panel de detalles, haga clic en Agregar.
3. En el cuadro de diálogo Crear servidor virtual (equilibrio de carga), especifique valores para los siguientes parámetros, como se muestra a continuación:
   - Nombre: nombre
4. En Protocolo, seleccione CUALQUIERA y, en Dirección IP y puerto, seleccione *.

5. Haga clic en Crear y, a continuación, en Cerrar. El servidor virtual que creó aparece en el panel Servidores virtuales de equilibrio de carga.

Configurar el servidor virtual en modo de reescritura MAC

Para configurar el servidor virtual en modo de reescritura de MAC mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
set lb vserver <name>@ -m <RedirectionMode>
<!--NeedCopy-->
```

Ejemplo:

```
set lb vserver Vserver-LB-1 -m MAC
<!--NeedCopy-->
```

Para configurar el servidor virtual en modo de reescritura de MAC mediante la utilidad de configuración

1. Vaya a Administración del tráfico > Equilibrio de carga > Servidores virtuales.
2. En el panel de detalles, seleccione el servidor virtual para el que desea configurar el modo de redirección (por ejemplo, vServer-LB-1) y, a continuación, haga clic en Abrir.
3. En la ficha Avanzado, en Modo de redirección, haga clic en Basado en Mac.
4. Haga clic en Aceptar.

Enlazar los servicios de firewall al servidor virtual comodín

Para vincular los servicios de firewall al servidor virtual comodín mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Ejemplo:


```
bind lb vserver Vserver-LB-1 Service-HTTP-1
<!--NeedCopy-->
```

Para vincular los servicios de firewall al servidor virtual comodín mediante la utilidad de configuración

1. Vaya a Administración del tráfico > Equilibrio de carga > Servidores virtualesy seleccione un servidor virtual.
2. Haga clic en la sección Servicio y seleccione un servicio para vincular.

Nota: Puede vincular un servicio a varios servidores virtuales.

Configurar un servicio para cada servidor virtual

Para configurar un servicio para cada servidor virtual mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
add service <name> <serverName> HTTP <port>
<!--NeedCopy-->
```

Ejemplo:

```
add service Service-HTTP-1 192.168.100.10 HTTP 80
<!--NeedCopy-->
```

Para configurar un servicio para cada servidor virtual mediante la utilidad de configuración

1. Vaya a Administración del tráfico > Equilibrio de carga > Servicios.
2. En el panel de detalles, haga clic en Agregar.
3. En el cuadro de diálogo Crear servicio, especifique valores para los siguientes parámetros, como se muestra a continuación:
   - Nombre del servicio: nombre
   - server—nombreDeServidor
   - Puerto—puerto
4. En Protocolo, especifique HTTP. En Monitores disponibles, selecciona HTTP.
5. Haga clic en Crear y, a continuación, en Cerrar. El servicio que creó aparece en el panel Servicios.

Configurar un monitor para cada servicio

Para vincular un monitor a un servicio mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
bind lb monitor <monitorName> <ServiceName>
<!--NeedCopy-->
```

Ejemplo:

```
bind mon monitor-HTTP-1 Service-HTTP-1
<!--NeedCopy-->
```

Para vincular un monitor a un servicio mediante la utilidad de configuración

1. Vaya a Administración del tráfico > Equilibrio de carga > Servicios.
2. Abra el servicio y agregue un monitor.

Configurar un servidor virtual HTTP para equilibrar el tráfico enviado a los servidores

Para configurar un servidor virtual HTTP para equilibrar el tráfico enviado a los servidores mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
add lb vserver <name> HTTP <ip> <port>
<!--NeedCopy-->
```

Ejemplo:

```
add lb vserver Vserver-LB-1 HTTP 10.102.29.60 80
<!--NeedCopy-->
```

Para configurar un servidor virtual HTTP para equilibrar el tráfico enviado a los servidores mediante la utilidad de configuración

1. Vaya a Administración del tráfico > Equilibrio de carga > Servidores virtuales.

2. En el panel de detalles, haga clic en Agregar.
3. En el cuadro de diálogo Crear servidor virtual (equilibrio de carga), especifique valores para los siguientes parámetros, como se muestra a continuación:
   - Nombre: nombre
   - Dirección IP: dirección IP
     Nota: Si el servidor virtual utiliza IPv6, active la casilla de verificación IPv6 e introduzca la dirección en formato IPv6 (por ejemplo, **1000:0000:0000:0000:0005:0600:700 a:888b**).
   - Puerto—puerto
4. En Protocolo, selecciona HTTP.
5. Haga clic en Crear y, a continuación, en Cerrar. El servidor virtual que creó aparece en el panel Servidores virtuales de equilibrio de carga.

Enlazar servicios HTTP al servidor virtual HTTP

Para vincular los servicios HTTP al servidor virtual comodín mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Ejemplo:

```
bind lb vserver Vserver-LB-1 Service-HTTP-1
<!--NeedCopy-->
```

Para vincular los servicios HTTP al servidor virtual comodín mediante la utilidad de configuración

1. Vaya a Administración del tráfico > Equilibrio de carga > Servidores virtualesy seleccione un servidor virtual.
2. Haga clic en la sección Servicio y seleccione un servicio para vincular.

Nota: Puede vincular un servicio a varios servidores virtuales.

Guardar y verificar la configuración

Cuando haya terminado las tareas de configuración, asegúrese de guardar la configuración. También debe comprobar que la configuración es correcta.

Para guardar y verificar la configuración mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para configurar un monitor transparente y verificar la configuración:

- guardar configuración ns
- mostrar vserver

Ejemplo:

```
save config
show lb vserver FWLBVIP2
        FWLBVIP2 (\*:\*) - ANY    Type: ADDRESS
        State: UP
        Last state change was at Mon Jun 14 07:22:54 2010
        Time since last state change: 0 days, 00:00:32.760
        Effective State: UP
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  2 (Total)       2 (Active)
        Configured Method: LEASTCONNECTION
        Current Method: Round Robin, Reason: A new service is bound
        Mode: MAC
        Persistence: NONE
        Connection Failover: DISABLED

1) fw-int-svc1 (192.168.100.10: \*) - ANY State: UP Weight: 1
 Done
show service fw-int-svc1
        fw-int-svc1 (192.168.100.10:\*) - ANY
        State: UP
        Last state change was at Thu Jul  8 14:44:51 2010
        Time since last state change: 0 days, 00:01:50.240
        Server Name: 192.168.100.10
        Server ID : 0   Monitor Threshold : 0
        Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
        Use Source IP: NO
        Client Keepalive(CKA): NO
```



```
30          Access Down Service: NO
31          TCP Buffering(TCPB): NO
32          HTTP Compression(CMP): NO
33          Idle timeout: Client: 120 sec   Server: 120 sec
34          Client IP: DISABLED
35          Cacheable: NO
36          SC: OFF
37          SP: OFF
38          Down state flush: ENABLED
39
40  1)      Monitor Name: monitor-HTTP-1
41                  State: UP     Weight: 1
42                  Probes: 9       Failed [Total: 0 Current: 0]
43                  Last response: Success - HTTP response code 200
          received
44                  Response Time: 100.0 millisec
45  2)      Monitor Name: ping
46                  State: UP       Weight: 1
47                  Probes: 3       Failed [Total: 0 Current: 0]
48                  Last response: Success - ICMP echo reply received.
49                  Response Time: 1.275 millisec
50   Done
51  <!--NeedCopy-->
```

Para guardar y verificar la configuración mediante la utilidad de configuración

1. En el panel de detalles, haga clic en Guardar.
2. En el cuadro de diálogo Guardar configuración, haga clic en Sí.
3. Vaya a Administración del tráfico > Equilibrio de carga > Servidores virtuales.
4. En el panel de detalles, seleccione el servidor virtual que creó en el paso 5 y compruebe que la configuración que se muestra en el panel Detalles es correcta.
5. Vaya a Administración del tráfico > Equilibrio de carga > Servicios.
6. En el panel de detalles, seleccione el servicio que creó en el paso 5 y compruebe que la configuración que se muestra en el panel Detalles es correcta.

Supervisión de una configuración de equilibrio de carga de firewall en un entorno empresarial

Una vez que la configuración esté en funcionamiento, debe ver las estadísticas de cada servicio y servidor virtual para comprobar si hay posibles problemas.

Visualización de las estadísticas de un servidor virtual

Para evaluar el rendimiento de los servidores virtuales o solucionar problemas, puede mostrar detalles de los servidores virtuales configurados en el dispositivo Citrix ADC. Puede mostrar un resumen de las estadísticas de todos los servidores virtuales o puede especificar el nombre de un servidor virtual para mostrar las estadísticas solo de ese servidor virtual. Puede mostrar los siguientes detalles:

- Nombre
- Dirección IP
- Port
- Protocolo
- Estado del servidor virtual
- Tasa de solicitudes recibidas
- Tasa de aciertos

Para mostrar las estadísticas del servidor virtual mediante la interfaz de línea de comandos

Para mostrar un resumen de las estadísticas de todos los servidores virtuales actualmente configurados en el dispositivo Citrix ADC, o de un solo servidor virtual, en el símbolo del sistema, escriba:

```
stat lb vserver [-detail] [<name>]
<!--NeedCopy-->
```

Ejemplo:

```
>stat lb vserver -detail
Virtual Server(s) Summary
                       vsvrIP  port     Protocol        State    Req/s
                            Hits/s
One                         *    80         HTTP           UP      5/s
        0/s
Two                         *     0          TCP         DOWN      0/s
        0/s
Three                       *  2598          TCP         DOWN      0/s
        0/s
dnsVirtualNS    10.102.29.90    53          DNS         DOWN      0/s
        0/s
BRVSERV            10.10.1.1    80         HTTP         DOWN      0/s
        0/s
LBVIP           10.102.29.66    80         HTTP           UP      0/s
        0/s
```



```
10   Done
11
12
13 <!--NeedCopy-->
```

Para mostrar las estadísticas del servidor virtual mediante la utilidad de configuración

1. Vaya a Administración del tráfico > Equilibrio de carga > Servidores virtuales > Estadísticas.
2. Si desea mostrar las estadísticas de un solo servidor virtual, en el panel de detalles, seleccione el servidor virtual y haga clic en Estadísticas.

Visualización de las estadísticas de un servicio

Actualizado: 2013-08-28

Puede ver la tasa de solicitudes, respuestas, bytes de solicitud, bytes de respuesta, conexiones de clientes actuales, solicitudes en cola de sobretensión, conexiones de servidor actuales, etc. mediante las estadísticas de servicio.

Para ver las estadísticas de un servicio mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
1 stat service <name>
2 <!--NeedCopy-->
```

Ejemplo:

```
1 stat service Service-HTTP-1
2 <!--NeedCopy-->
```

Para ver las estadísticas de un servicio mediante la utilidad de configuración

1. Vaya a Administración del tráfico > Equilibrio de carga > Servicios > Estadísticas.
2. Si desea mostrar las estadísticas de un solo servicio, selecciónelo y haga clic en Estadísticas.

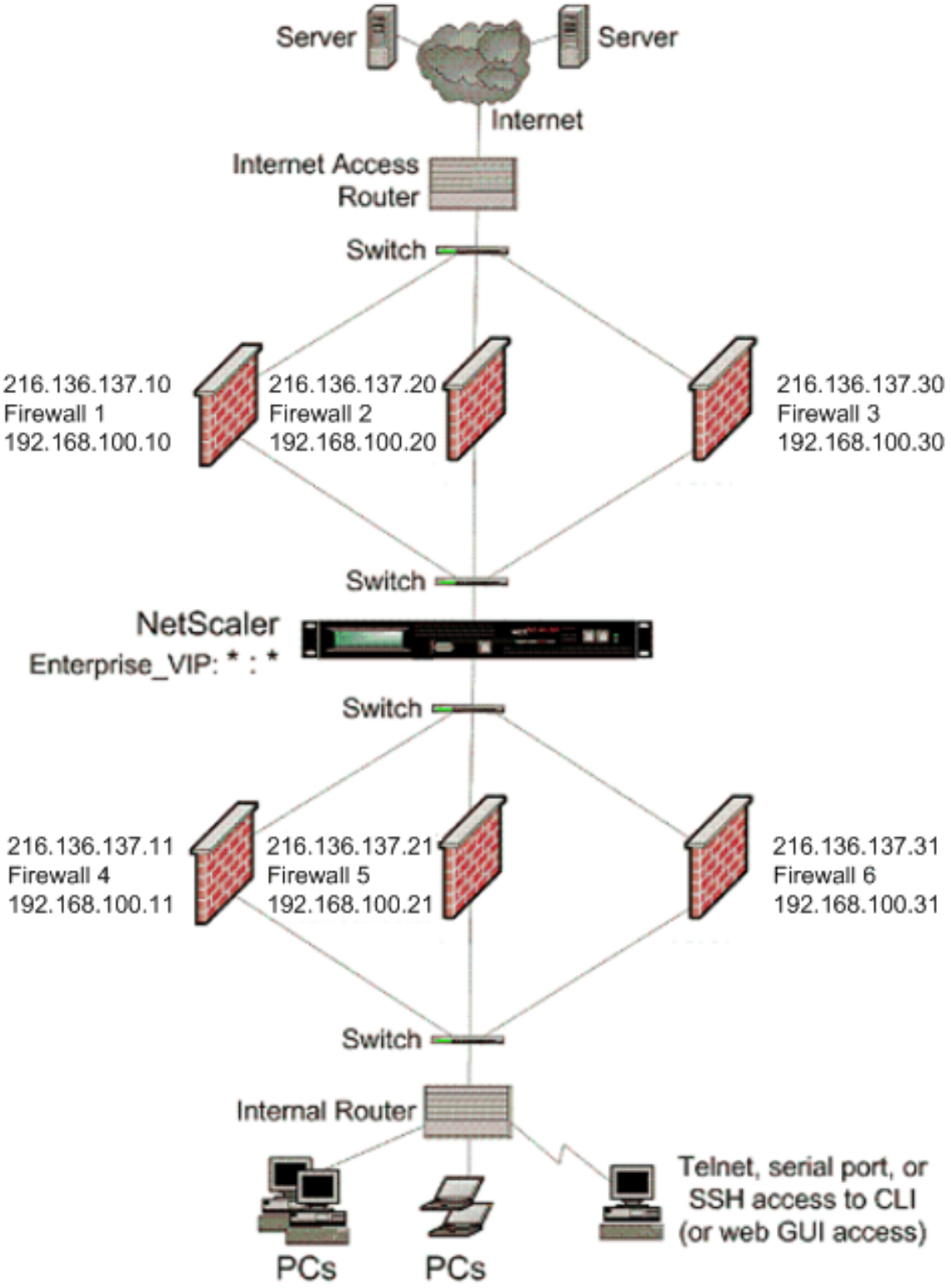
Entorno de varios firewall

August 20, 2021

En un entorno de varios firewall, el dispositivo Citrix ADC se coloca entre dos conjuntos de firewalls, el conjunto externo que se conecta a Internet público y el conjunto interno que se conecta a la red privada interna. El conjunto externo normalmente maneja el tráfico de salida. Estos firewalls implementan principalmente listas de control de acceso para permitir o denegar el acceso a recursos externos. El conjunto interno normalmente maneja el tráfico de entrada. Estos firewalls implementan la seguridad para proteger la intranet de ataques maliciosos, además de equilibrar la carga del tráfico de entrada. El entorno de firewall múltiple le permite equilibrar la carga del tráfico procedente de otro firewall. De forma predeterminada, el tráfico procedente de un firewall no está equilibrado de carga en el otro firewall en un dispositivo Citrix ADC. Tener habilitado el equilibrio de carga del firewall en ambos lados de Citrix ADC mejora el flujo de tráfico en la dirección de salida y entrada y garantiza un procesamiento más rápido del tráfico.

La siguiente ilustración muestra un entorno de equilibrio de carga de varios firewall

Ilustración 1. Equilibrio de carga del firewall (firewall múltiple)



Con una configuración como la que se muestra en la Ilustración 1, puede configurar Citrix ADC para equilibrar la carga del tráfico a través de un firewall interno, incluso si la carga está balanceada por

un firewall externo. Por ejemplo, con esta función configurada, el tráfico procedente de los firewalls externos (firewalls 1, 2 y 3) se equilibra la carga en los firewalls internos (firewalls 4, 5 y 6) y viceversa.

El equilibrio de carga del firewall solo es compatible con el servidor virtual LB en modo MAC.

El tipo de servicio ANY configura Citrix ADC para aceptar todo el tráfico.

Para aprovechar los beneficios relacionados con HTTP y TCP, configure el servicio y el servidor virtual con el tipo HTTP o TCP. Para que FTP funcione, configure el servicio con el tipo FTP.

Configuración del Citrix ADC en un entorno de múltiples firewall

Para configurar un dispositivo Citrix ADC en un entorno de varios firewall, debe habilitar la función de equilibrio de carga, configurar un servidor virtual para equilibrar la carga del tráfico de salida a través de los firewalls externos, configurar un servidor virtual para equilibrar la carga del tráfico de entrada a través de los firewalls internos y habilite el equilibrio de carga del firewall en el dispositivo Citrix ADC. Para configurar un servidor virtual para equilibrar la carga del tráfico a través de un firewall en el entorno de varios firewall, debe:

1. Configurar un servicio comodín para cada firewall
2. Configurar un monitor para cada servicio comodín
3. Configurar un servidor virtual comodín para equilibrar la carga del tráfico enviado a los firewalls
4. Configurar el servidor virtual en el modo de reescritura MAC
5. Vincular servicios de firewall al servidor virtual comodín

Activación de la función de equilibrio de carga

Para configurar e implementar entidades de equilibrio de carga como servicios y servidores virtuales, debe habilitar la función de equilibrio de carga en el dispositivo Citrix ADC.

Para habilitar el equilibrio de carga mediante la CLI:

En el símbolo del sistema, escriba el siguiente comando para habilitar el equilibrio de carga y verificar la configuración:

```
enable ns feature <featureName>
show ns feature
<!--NeedCopy-->
```

Ejemplo:

```
enable ns feature LoadBalancing
```



```
Done
show ns feature
Feature Acronym Status
------- ------- ------
1) Web Logging WL OFF
2) Surge Protection SP ON
3) Load Balancing LB ON
.
.
.
24) NetScaler Push push OFF
Done
<!--NeedCopy-->
```

Para habilitar el equilibrio de carga mediante la GUI:

1. En el panel de navegación, expanda Sistemay, a continuación, haga clic en Configuración.
2. En el panel Configuración, en Modos y funciones, haga clic en Cambiar funciones básicas.
3. En el cuadro de diálogo Configurar funciones básicas, active la casilla Equilibrio de carga y, a continuación, haga clic en Aceptar.

Configuración de un servicio comodín para cada firewall

Para aceptar el tráfico de todos los protocolos, debe configurar el servicio comodín para cada firewall especificando compatibilidad con todos los protocolos y puertos.

Para configurar un servicio comodín para cada firewall mediante la CLI:

En el símbolo del sistema, escriba el siguiente comando para configurar la compatibilidad con todos los protocolos y puertos:

```
add service <name>@ <serverName> <serviceType> <port_number>
<!--NeedCopy-->
```

Ejemplo:

```
add service fw-svc1 10.102.29.5 ANY *
<!--NeedCopy-->
```

Para configurar un servicio comodín para cada firewall mediante la GUI:

1. Vaya a Administración de Tráfico > Equilibrio de carga > Servicios.

2. En el panel de detalles, haga clic en Agregar.
3. En el cuadro de diálogo Crear servicios, especifique valores para los siguientes parámetros como se muestra:
   - Nombre del servicio: Nombre
   - Servidor: NombreServidor

   -* Un parámetro requerido
4. En Protocolo, seleccione Cualquiera y, en Puerto, seleccione *.
5. Haga clic en Crear y, a continuación, en Cerrar. El servicio creado aparece en el panel Servicios.

Configuración de un monitor para cada servicio

Un monitor PING está enlazado de forma predeterminada al servicio. Deberá configurar un monitor transparente para supervisar los hosts del lado de confianza a través de firewalls individuales. A continuación, puede enlazar el monitor transparente a los servicios. El monitor PING predeterminado supervisa la conectividad solo entre el dispositivo Citrix ADC y el dispositivo ascendente. El monitor transparente supervisa todos los dispositivos existentes en la ruta de acceso desde el dispositivo al dispositivo que posee la dirección IP de destino especificada en el monitor. Si no se configura un monitor transparente y el estado del firewall es UP, pero uno de los dispositivos de salto siguiente de ese firewall está inactivado, el dispositivo incluye el firewall mientras realiza el equilibrio de carga y reenvía el paquete al firewall. Sin embargo, el paquete no se entrega al destino final porque uno de los dispositivos de salto siguiente está caído. Al vincular un monitor transparente, si alguno de los dispositivos (incluido el firewall) está inactivo, el servicio se marca como DOWN y el firewall no se incluye cuando el dispositivo realiza el equilibrio de carga del firewall.

Enlazar un monitor transparente anulará el monitor PING. Para configurar un monitor PING además de un monitor transparente, después de crear y enlazar un monitor transparente, debe enlazar un monitor PING al servicio.

Para configurar un monitor transparente mediante la CLI:

En el símbolo del sistema, escriba los siguientes comandos para configurar un monitor transparente y verificar la configuración:

```
1 add lb monitor <monitorName> <type> [-destIP <ip_addr|ipv6_addr|*>] [-
     transparent (YES | NO )]
2 bind lb monitor <monitorName> <serviceName>
3 <!--NeedCopy-->
```

Ejemplo:


```
add monitor monitor-HTTP-1 HTTP -destip 10.10.10.11 -transparent YES
bind monitor monitor-HTTP-1 fw-svc1
<!--NeedCopy-->
```

El dispositivo Citrix ADC aprende los parámetros L2 del servidor desde el monitor enlazado al servicio. Para los monitores UDP-ECV, configure una cadena de recepción para permitir que el dispositivo aprenda los parámetros L2 del servidor. Si la cadena de recepción no está configurada y el servidor no responde, el dispositivo no aprende los parámetros L2, pero el servicio está configurado en UP. El tráfico de este servicio está bloqueado.

Para configurar una cadena de recepción mediante la CLI:

En el símbolo del sistema, escriba el siguiente comando:

```
add lb monitor <monitorName> <type> [-destIP <ip_addr|ipv6_addr|*>] [-
    transparent (YES | NO )] [-send <string>] [-recv <string>]
<!--NeedCopy-->
```

Ejemplo:

```
add lb monitor monitor-udp-1 udp-ecv -destip 10.10.10.11 -transparent
    YES  - send "test message"  - recv "site_is_up"
<!--NeedCopy-->
```

Para crear y enlazar un monitor transparente mediante la interfaz gráfica de usuario:

1. Vaya a Administración del Tráfico > Equilibrio de carga > Monitores.
2. En el panel de detalles, haga clic en Agregar.
3. En el cuadro de diálogo Crear monitor, especifique valores para los siguientes parámetros como se muestra:
   - Nombre*
   - tipo*: Tipo
   - IP de destino
   - Transparencia

   -* Un parámetro requerido
4. Haga clic en Crear y, a continuación, en Cerrar. En el panel Monitores, seleccione el monitor que acaba de configurar y compruebe que la configuración mostrada en la parte inferior de la pantalla sea correcta.

Configurar un servidor virtual para equilibrar la carga del tráfico enviado a los firewalls

Para equilibrar la carga cualquier tipo de tráfico, debe configurar un servidor virtual comodín especificando el protocolo y el puerto como cualquier valor.

Para configurar un servidor virtual para equilibrar la carga del tráfico enviado a los firewalls mediante la CLI:

En el símbolo del sistema, escriba el siguiente comando:

```
add lb vserver <name>@ <serviceType> <IPAddress> <port_number>
<!--NeedCopy-->
```

Ejemplo:

```
add lb vserver Vserver-LB-1 ANY * *
<!--NeedCopy-->
```

Para configurar un servidor virtual para equilibrar la carga del tráfico enviado a los firewalls mediante la GUI:

1. Vaya a Administración del tráfico > Equilibrio de carga > Servidores virtuales.
2. En el panel de detalles, haga clic en Agregar.
3. En Protocolo, seleccione Cualquiera y, en Dirección IP y Puerto, seleccione *.
4. Haga clic en Crear y, a continuación, en Cerrar. El servidor virtual creado aparece en el panel Servidores virtuales de equilibrio de carga.

Configuración del servidor virtual en el modo de reescritura MAC

Para configurar el servidor virtual para que use la dirección MAC para reenviar el tráfico entrante, debe habilitar el modo de reescritura MAC.

Para configurar el servidor virtual en el modo de reescritura MAC mediante la CLI:

En el símbolo del sistema, escriba el siguiente comando:

```
set lb vserver <name>@ -m <RedirectionMode>
<!--NeedCopy-->
```

Ejemplo:


```
set lb vserver Vserver-LB-1 -m MAC
<!--NeedCopy-->
```

Para configurar el servidor virtual en el modo de reescritura MAC mediante la GUI:

1. Vaya a Administración del tráfico > Equilibrio de carga > Servidores virtuales.
2. En el panel de detalles, seleccione el servidor virtual para el que quiere configurar el modo de redirección (por ejemplo, VServer-LB1) y, a continuación, haga clic en Abrir.
3. En la ficha Avanzadas, en el modo Modo de redirección, haga clic en Abrir.
4. Haga clic en Aceptar.

Enlace de servicios de firewall al servidor virtual

Para acceder a un servicio en el dispositivo Citrix ADC, debe vincularlo a un servidor virtual comodín.

Para enlazar servicios de firewall al servidor virtual mediante la CLI:

En el símbolo del sistema, escriba el siguiente comando:

```
bind lb vserver <name>@ <serviceName>
<!--NeedCopy-->
```

Ejemplo:

```
bind lb vserver Vserver-LB-1 Service-HTTP-1
<!--NeedCopy-->
```

Para enlazar servicios de firewall al servidor virtual mediante la GUI:

1. Vaya a Administración del tráfico > Equilibrio de carga > Servidores virtuales.
2. En el panel de detalles, seleccione el servidor virtual para el que quiere configurar el modo de redirección (por ejemplo, VServer-LB1) y, a continuación, haga clic en Abrir.
3. En el cuadro de diálogo Configurar servidor virtual (equilibrio de carga), en la ficha Servicios, active la casilla de verificación Activo junto al servicio que quiere enlazar al servidor virtual (por ejemplo, Service-HTTP-1).
4. Haga clic en Aceptar.

Configuración del equilibrio de carga de varios firewall en el dispositivo Citrix ADC

Para equilibrar la carga del tráfico en ambos lados de un dispositivo Citrix ADC mediante el equilibrio de carga del firewall, debe habilitar el equilibrio de carga entre varios firewall mediante el parámetro

vServerSpecificMac.

Para configurar el equilibrio de carga de varios firewall mediante la CLI:

En el símbolo del sistema, escriba el siguiente comando:

```
set lb parameter -vServerSpecificMac <status>
<!--NeedCopy-->
```

Ejemplo:

```
set lb parameter -vServerSpecificMac ENABLED
<!--NeedCopy-->
```

Para configurar el equilibrio de carga de varios firewall mediante la interfaz gráfica de usuario:

1. Vaya a Administración del tráfico > Equilibrio de carga > Servidores virtuales.
2. En el panel de detalles, seleccione el servidor virtual para el que quiere configurar el modo de redirección (por ejemplo, Configurar parámetros de equilibrio de carga).
3. En el cuadro de diálogo Establecer parámetros de equilibrio de carga, active la casilla de verificación MAC específico del servidor virtual.
4. Haga clic en Aceptar.

Guardar y verificar la configuración

Cuando haya terminado las tareas de configuración, asegúrese de guardar la configuración. También debe verificar para asegurarse de que la configuración sea correcta.

Para guardar y verificar la configuración mediante la CLI:

En el símbolo del sistema, escriba los siguientes comandos para configurar un monitor transparente y verificar la configuración:

- save ns config
- show vserver

Ejemplo:

```
save config
show lb vserver FWLBVIP2
        FWLBVIP2 (\*:\*) - ANY    Type: ADDRESS
        State: UP
```



```
        Last state change was at Mon Jun 14 07:22:54 2010
        Time since last state change: 0 days, 00:00:32.760
        Effective State: UP
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  2 (Total)       2 (Active)
        Configured Method: LEASTCONNECTION
        Current Method: Round Robin, Reason: A new service is bound
        Mode: MAC
        Persistence: NONE
        Connection Failover: DISABLED

1) fw-int-svc1 (10.102.29.5: *) - ANY State: UP Weight: 1
2) fw-int-svc2 (10.102.29.9: \*) - ANY State: UP Weight: 1
 Done
show service fw-int-svc1
        fw-int-svc1 (10.102.29.5:\*) - ANY
        State: DOWN
        Last state change was at Thu Jul  8 14:44:51 2010
        Time since last state change: 0 days, 00:01:50.240
        Server Name: 10.102.29.5
        Server ID : 0   Monitor Threshold : 0
        Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
        Use Source IP: NO
        Client Keepalive(CKA): NO
        Access Down Service: NO
        TCP Buffering(TCPB): NO
        HTTP Compression(CMP): NO
        Idle timeout: Client: 120 sec   Server: 120 sec
        Client IP: DISABLED
        Cacheable: NO
        SC: OFF
        SP: OFF
        Down state flush: ENABLED

1)      Monitor Name: monitor-HTTP-1
                State: DOWN     Weight: 1
                Probes: 9       Failed [Total: 9 Current: 9]
                Last response: Failure - Time out during TCP connection
                    establishment stage
                Response Time: 2000.0 millisec
2)      Monitor Name: ping
                State: UP       Weight: 1
                Probes: 3       Failed [Total: 0 Current: 0]
```



```
                Last response: Success - ICMP echo reply received.
                Response Time: 1.275 millisec
 Done
<!--NeedCopy-->
```

Para guardar y verificar la configuración mediante la interfaz gráfica de usuario:

1. En el panel de detalles, haga clic en Guardar.
2. En el cuadro de diálogo Guardar configuración, haga clic en Sí.
3. Vaya a Administración del tráfico > Equilibrio de carga > Servidores virtuales.
4. En el panel de detalles, seleccione el servidor virtual que creó en el paso 5 y compruebe que la configuración mostrada en el panel Detalles es correcta.
5. Vaya a Administración de Tráfico > Equilibrio de carga > Servicios.
6. En el panel de detalles, seleccione el servicio que creó en el paso 5 y compruebe que la configuración mostrada en el panel Detalles es correcta.

Supervisión de una configuración de equilibrio de carga de firewall en un entorno de varios firewall

Después de que la configuración esté activa y en ejecución, debe ver las estadísticas de cada servicio y servidor virtual para comprobar si hay posibles problemas.

Visualización de las estadísticas de un servidor virtual

Para evaluar el rendimiento de los servidores virtuales o solucionar problemas, puede mostrar detalles de los servidores virtuales configurados en el dispositivo Citrix ADC. Puede mostrar un resumen de estadísticas para todos los servidores virtuales o puede especificar el nombre de un servidor virtual para mostrar las estadísticas solo para ese servidor virtual. Puede mostrar los siguientes detalles:

- Nombre
- Dirección IP
- Port
- Protocolo
- Estado del servidor virtual
- Tasa de solicitudes recibidas
- Tasa de visitas

Para mostrar las estadísticas del servidor virtual mediante la interfaz de línea de comandos

Para mostrar un resumen de las estadísticas de todos los servidores virtuales configurados actualmente en el dispositivo Citrix ADC, o de un único servidor virtual, en el símbolo del sistema, escriba:


```
stat lb vserver [-detail] [<name>]
<!--NeedCopy-->
```

Ejemplo:

```
>stat lb vserver -detail
Virtual Server(s) Summary
                        vsvrIP  port     Protocol        State    Req/s
                             Hits/s
One                          *    80         HTTP           UP      5/s
        0/s
Two                          *     0          TCP         DOWN      0/s
        0/s
Three                        *  2598          TCP         DOWN      0/s
        0/s
dnsVirtualNS    10.102.29.90    53          DNS         DOWN      0/s
        0/s
BRVSERV            10.10.1.1    80         HTTP         DOWN      0/s
        0/s
LBVIP           10.102.29.66    80         HTTP           UP      0/s
        0/s
 Done


<!--NeedCopy-->
```

Para mostrar las estadísticas del servidor virtual mediante la GUI:

1. Vaya a Administración del tráfico > Equilibrio de carga > Servidores virtuales > Estadísticas.
2. Si quiere mostrar las estadísticas de un solo servidor virtual, en el panel de detalles seleccione el servidor virtual y haga clic en Estadísticas.

Visualización de las estadísticas de un servicio

Puede ver la tasa de solicitudes, respuestas, bytes de solicitud, bytes de respuesta, conexiones de cliente actuales, solicitudes en cola de sobretensiones, conexiones de servidor actuales, etc. mediante las estadísticas de servicio.

Para ver las estadísticas de un servicio mediante la CLI:

En el símbolo del sistema, escriba:


```
stat service <name>
<!--NeedCopy-->
```

Ejemplo:

```
stat service Service-HTTP-1
<!--NeedCopy-->
```

Para ver las estadísticas de un servicio mediante la GUI:

1. Vaya a Administración del Tráfico > Equilibrio de carga > Servicios > Estadísticas.
2. Si quiere mostrar las estadísticas de un solo servicio, seleccione el servicio y haga clic en Estadísticas.

Equilibrio de carga global del servidor

February 16, 2021

> **Notas:**
>
> - Desde la versión 13.0 compilación 41.x, las implementaciones de equilibrio de carga de servidor global (GSLB) que utilizan el dispositivo Citrix ADC cumplen totalmente con el día del indicador DNS 2019.
> - La función GSLB se incluye con las licencias de Citrix ADC Advance y Premium Edition. La licencia de opción de Citrix ADC es compatible con la edición Standard.

Los dispositivos Citrix ADC configurados para GSLB proporcionan recuperación ante desastres y garantizan la disponibilidad continua de las aplicaciones al protegerse contra puntos de falla en una WAN. GSLB equilibra la carga entre los centros de datos dirigiendo las solicitudes del cliente al centro de datos más cercano o con el mejor rendimiento, o a los centros de datos que sobreviven si hay una interrupción.

En una configuración típica, un servidor DNS local envía solicitudes de cliente a un servidor virtual GSLB, al que están vinculados servicios GSLB. Un servicio GSLB identifica un servidor virtual de equilibrio de carga o cambio de contenido, que puede estar en el sitio local o en un sitio remoto. Si el servidor virtual GSLB selecciona un servidor virtual de equilibrio de carga o cambio de contenido en un sitio remoto, envía la dirección IP del servidor virtual al servidor DNS. El servidor DNS lo envía al cliente. A continuación, el cliente vuelve a enviar la solicitud al nuevo servidor virtual en la nueva IP.

Las entidades GSLB que debe configurar son los sitios GSLB, los servicios GSLB, los servidores virtuales GSLB, los servidores virtuales de equilibrio de carga o cambio de contenido, y los servicios

DNS autoritativos (ADNS). También debe configurar MEP. También puede configurar vistas DNS para exponer diferentes partes de la red a los clientes que acceden a la red desde diferentes ubicaciones.

> **Nota:**
>
> Para aprovechar al máximo las funciones de GSLB, utilice dispositivos ADC para el equilibrio de carga o la cambio de contenido en cada centro de datos, de modo que la configuración de GSLB pueda utilizar el MEP propietario para intercambiar métricas de sitio.

Cómo funciona GSLB

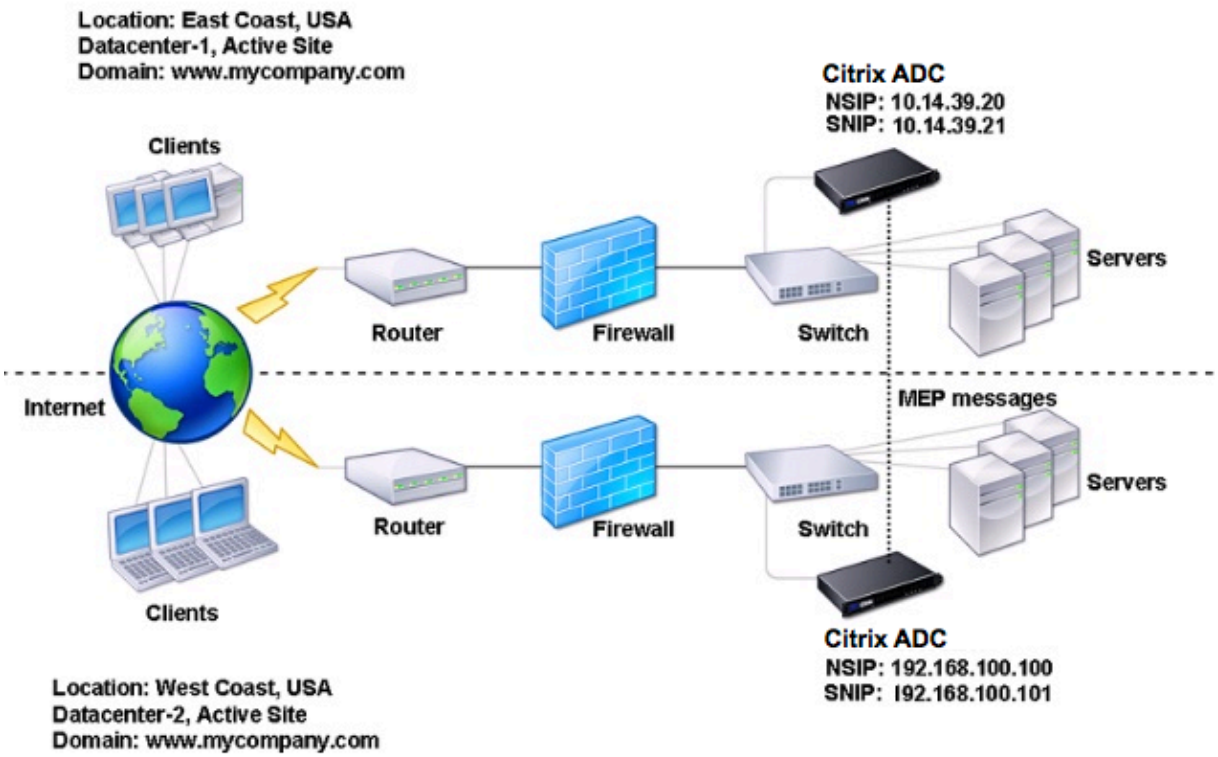
Con DNS ordinario, cuando un cliente envía una solicitud de sistema de nombres de dominio (DNS), recibe una lista de direcciones IP del dominio o servicio. Generalmente, el cliente elige la primera dirección IP de la lista e inicia una conexión con ese servidor. El servidor DNS utiliza una técnica llamada DNS round robin para rotar a través de las direcciones IP de la lista. Envía la primera dirección IP al final de la lista y promueve los demás después de responder a cada solicitud DNS. Esta técnica garantiza la distribución equitativa de la carga, pero no admite recuperación ante desastres, equilibrio de carga basado en la carga o la proximidad de los servidores, ni persistencia.

Cuando configura GSLB en dispositivos ADC y habilita MEP, la infraestructura DNS se utiliza para conectar el cliente al centro de datos que mejor cumpla los criterios establecidos. Los criterios pueden designar lo siguiente:

- Centro de datos menos cargado
- Centro de datos más cercano
- Centro de datos que responde más rápidamente a las solicitudes desde la ubicación del cliente
- Una combinación de esas métricas y métricas SNMP.

Un dispositivo realiza un seguimiento de la ubicación, el rendimiento, la carga y la disponibilidad de cada centro de datos. Utiliza estos factores para seleccionar el centro de datos para enviar la solicitud del cliente.

La siguiente ilustración ilustra una topología GSLB básica.



Una configuración de GSLB consta de un grupo de entidades GSLB en cada dispositivo de la configuración. Estas entidades incluyen sitios GSLB, servicios GSLB, grupos de servicios GSLB, servidores virtuales GSLB, servidores de equilibrio de carga, servidores de cambio de contenido y servicios ADNS.

Tipos de implementación de GSLB

January 19, 2021

Los dispositivos Citrix ADC configurados para el equilibrio de carga global de servidores (GSLB) proporcionan recuperación ante desastres y garantizan la disponibilidad continua de las aplicaciones al protegerse contra puntos de falla en una red de área extensa (WAN). GSLB puede equilibrar la carga entre los centros de datos dirigiendo las solicitudes del cliente al centro de datos más cercano o de mejor rendimiento, o a centros de datos que sobreviven en caso de interrupción.

Los siguientes son algunos de los tipos de implementación típicos de GSLB:

- Implementación de sitio activo-activo
- Implementación de sitio activo-pasivo
- Implementación de topología principal-secundario

Implementación de sitio activo-activo

August 20, 2021

Un sitio activo-activo consta de varios centros de datos activos. Las solicitudes de los clientes se equilibran la carga entre los centros de datos activos. Este tipo de implementación se puede utilizar cuando se necesita una distribución global del tráfico en un entorno distribuido.

Todos los sitios de una implementación activo-activa están activos y todos los servicios de una aplicación/dominio en particular están enlazados al mismo servidor virtual GSLB. Los sitios intercambian métricas a través del Protocolo de intercambio de métricas (MEP). Las métricas de sitio intercambiadas entre los sitios incluyen el estado de cada servidor virtual de equilibrio de carga y conmutación de contenido, el número actual de conexiones, la velocidad de paquetes actual y el uso actual del ancho de banda. El dispositivo Citrix ADC necesita esta información para realizar el equilibrio de carga en todos los sitios.

Una implementación activa-activa puede incluir un máximo de 32 sitios GSLB, porque MEP no puede sincronizar más de 32 sitios. No hay sitios de copia de seguridad configurados en este tipo de implementación.

El dispositivo Citrix ADC envía solicitudes de cliente al sitio GSLB apropiado según lo determinado por el método GSLB especificado en la configuración de GSLB.

Para una implementación activa-activa, puede configurar los siguientes métodos GSLB.

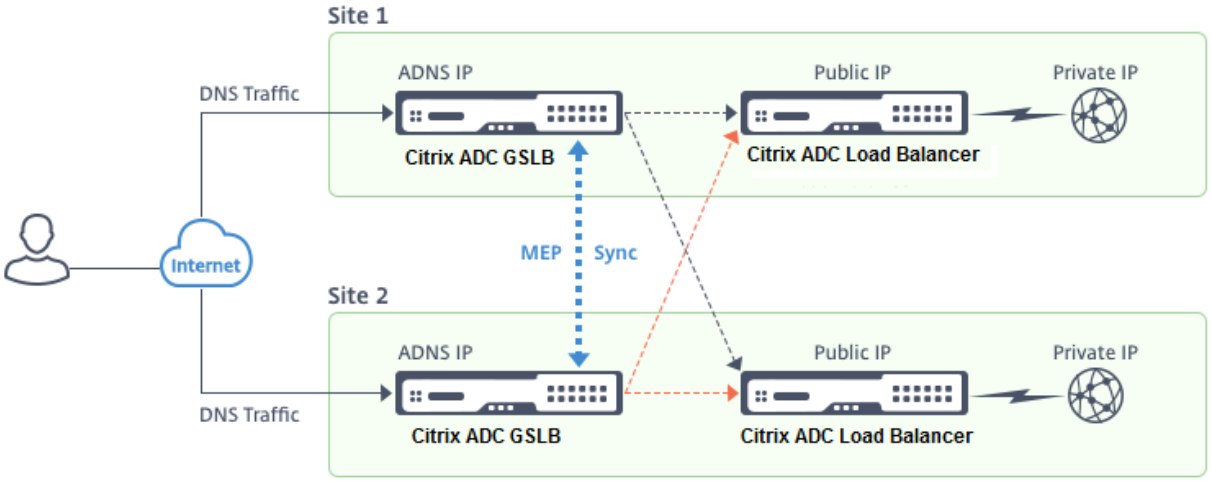
- Round Robin
- Menos conexiones
- Tiempo de respuesta mínimo
- Ancho de banda mínimo
- Menos paquetes
- Hash IP de origen
- Carga personalizada
- Tiempo de ida y vuelta (RTT)
- Proximidad estática

> Nota:
>
> - Si el MEP está inhabilitado, los siguientes métodos GSLB son por defecto el método Round Robin.
>   - RTT
>   - Menos conexiones
>   - Menos ancho de banda
>   - Menos paquetes

  - Menos tiempo de respuesta
- En el método GLSB de proximidad estática, el dispositivo envía la solicitud a la dirección IP del sitio que mejor coincide con los criterios de proximidad.
- En el método de tiempo de ida y vuelta, los valores de tiempo de ida y vuelta dinámico (RTT) son para seleccionar la dirección IP del sitio con mejor rendimiento. RTT es una medida del retraso en la red entre el servidor DNS local del cliente y un recurso de datos.

Topología de centro de datos activo-activo GSLB

En el diagrama, el sitio 1 y el sitio 2 son sitios GLSB activos.



Cuando el cliente envía una solicitud DNS, aterriza en uno de los sitios activos.

Si el sitio 1 recibe la solicitud del cliente, el servidor virtual GSLB del sitio 1 selecciona un servidor virtual de equilibrio de carga o cambio de contenido y envía la dirección IP del servidor virtual al servidor DNS, que la envía al cliente. A continuación, el cliente vuelve a enviar la solicitud al nuevo servidor virtual en la nueva dirección IP.

Como ambos sitios están activos, el algoritmo GSLB evalúa los servicios en ambos sitios al realizar una selección según lo determinado por el método GSLB configurado.

Implementación de sitio activo-pasivo

January 12, 2021

Un sitio activo-pasivo consiste en un centro de datos activo y un centro de datos pasivo. Este tipo de implementación es ideal para la recuperación ante desastres.

En este tipo de implementación, algunos de los sitios (sitios remotos) están reservados solo para la recuperación ante desastres. Estos sitios no participan en ninguna toma de decisiones hasta que to-

dos los sitios activos estén DOWN. Un sitio pasivo no entra en funcionamiento a menos que un evento de desastre desencadena una conmutación por error.

Una vez configurado el centro de datos principal, replicar la configuración del centro de datos de copia de seguridad y designarlo como el sitio GSLB pasivo designando un servidor virtual GSLB en ese sitio como servidor virtual de copia de seguridad.

Una implementación activo-pasiva puede incluir un máximo de 32 sitios GSLB, porque MEP no puede sincronizar más de 32 sitios.

Para una implementación activo-pasiva, puede configurar los siguientes métodos GSLB.

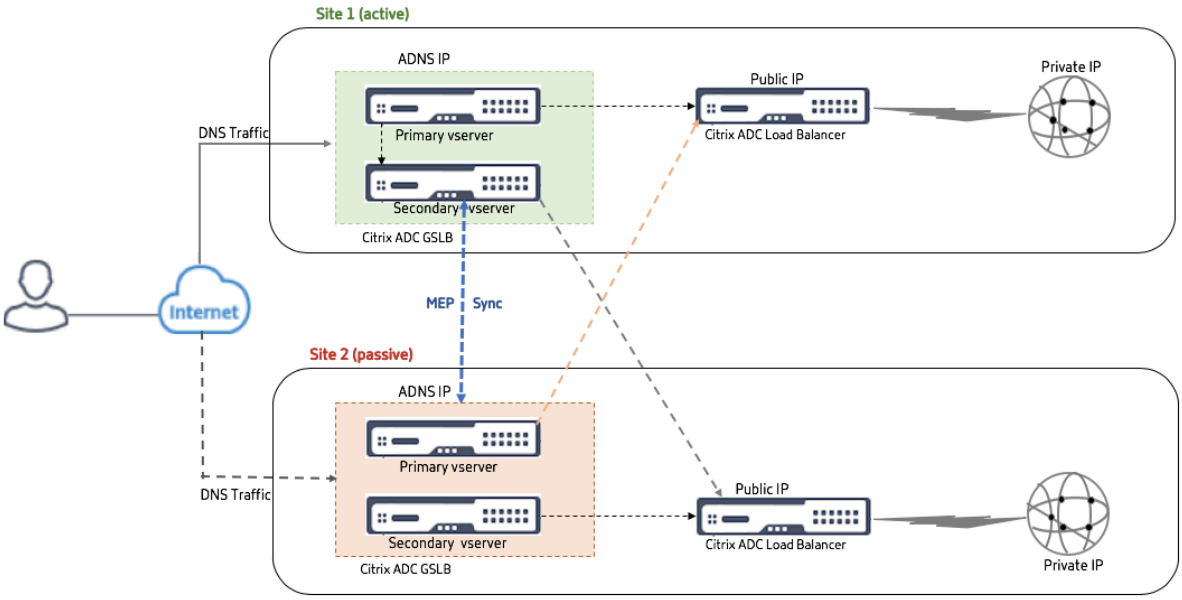
- Round Robin
- Menos conexiones
- Tiempo de respuesta mínimo
- Ancho de banda mínimo
- Menos paquetes
- Hash IP de origen
- Carga personalizada
- Tiempo de ida y vuelta (RTT)
- Proximidad estática

Nota:

- Si MEP está inhabilitado, los métodos de algoritmo siguientes son Round Robin por defecto.
  - RTT
  - Menos conexiones
  - Ancho de banda mínimo
  - Menos paquetes
  - Tiempo de respuesta mínimo
- En el método GLSB de proximidad estática, el dispositivo envía la solicitud a la dirección IP del sitio que mejor coincide con los criterios de proximidad.
- En el método de tiempo de ida y vuelta, los valores de tiempo de ida y vuelta dinámico (RTT) son para seleccionar la dirección IP del sitio con mejor rendimiento. RTT es una medida del retraso en la red entre el servidor DNS local del cliente y un recurso de datos.

Topología del centro de datos activo-pasivo de GSLB

En el diagrama, el sitio 1 es un sitio activo y el sitio 2 es un sitio pasivo, que tiene la misma configuración que la del sitio 1.



Si el sitio 1 cae hacia abajo, el sitio 2 entra en funcionamiento.

Cuando el cliente envía una solicitud DNS, la solicitud puede aterrizar en cualquiera de los sitios. Sin embargo, los servicios solo se seleccionan desde el sitio activo (Site1) siempre y cuando esté UP.

Los servicios del sitio pasivo (Sitio 2) solo se seleccionan si el sitio activo (Sitio 1) está DOWN.

Implementación de topología principal-secundaria mediante el protocolo MEP

March 9, 2022

Citrix ADC GSLB proporciona equilibrio de carga global del servidor y recuperación ante desastres mediante la creación de conexiones en malla entre todos los sitios involucrados y la toma de decisiones inteligentes sobre el equilibrio de carga. Cada sitio se comunica con los demás para intercambiar métricas de servidor y red a través del Protocolo de intercambio de métricas (MEP), a intervalos regulares. Sin embargo, con el aumento en el número de sitios homólogos, el volumen de tráfico de MEP aumenta exponencialmente debido a la topología de malla. Para superar esto, puede utilizar una topología principal-secundario. La topología principal-secundario también admite implementaciones más grandes. Además de los 32 sitios principales, puede configurar 1024 sitios secundarios.

La topología principal-secundario de GSLB es un diseño jerárquico de dos niveles con las siguientes características:

- En el nivel superior están los sitios para principales, que tienen relaciones con otros principales.

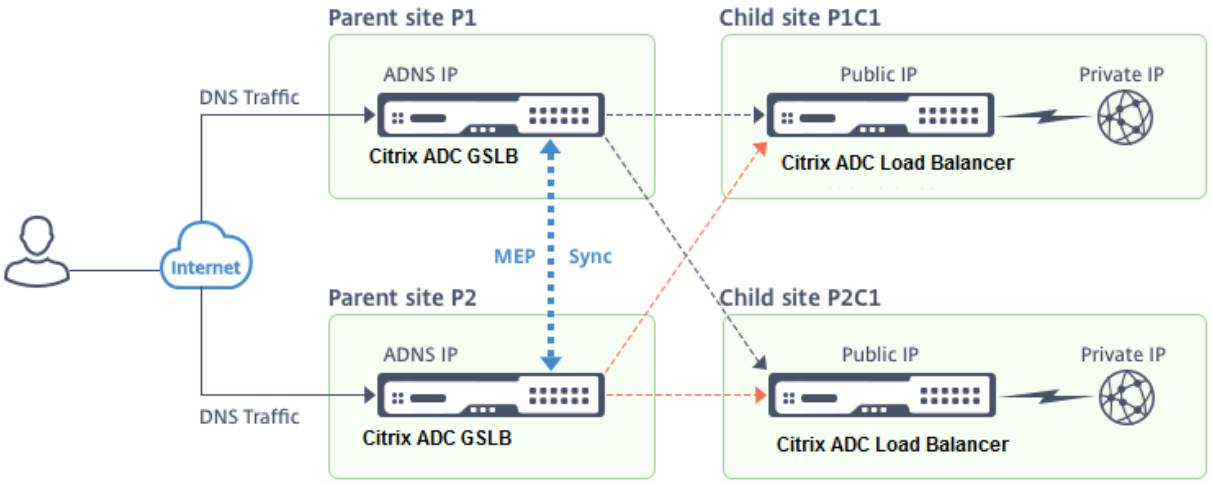
- Cada principal puede tener varios sitios secundarios.
- Cada sitio principal intercambia información de salud con sus sitios secundarios y con otros sitios principales.
- Un sitio secundario solo se comunica con su sitio principal.
- En una relación principal-secundario para GSLB, solo el sitio principal responde a las consultas de ADNS. Los sitios secundarios actúan como sitios de equilibrio de carga normales.
- Configure un servicio ADNS o un servidor virtual de equilibrio de carga DNS solo en el sitio principal.
- Un sitio principal puede tener una configuración GSLB normal, es decir, servicios de sitios locales y todos los sitios remotos, pero un sitio secundario solo puede tener servicios locales. Además, solo los sitios principales tienen servidores virtuales GSLB configurados.

> **Nota**
>
> - En una topología principal-secundario, el intercambio de métricas del sitio se inicia desde la más baja de las dos direcciones IP. Sin embargo, a partir de la versión 11.1 compilación 51.x de Citrix ADC, los sitios principales inician conexiones a los sitios secundarios, y no al revés. Porque los sitios principales tienen información sobre todos los sitios secundarios en la configuración de GSLB.

- En una conexión entre principales y principales, el intercambio de métricas del sitio aún se inicia desde la IP inferior de dos direcciones IP.
- En una topología principal-secundaria, los servicios GSLB no siempre deben configurarse en un sitio secundario. Sin embargo, si tiene más configuraciones, como autenticación de clientes, inserción de direcciones IP de clientes u otros requisitos específicos de SSL, debe agregar un servicio GSLB explícito en el sitio secundario y configurarlo en consecuencia.
- En una topología principal-secundario, el sitio principal y el sitio secundario pueden estar en diferentes versiones del software Citrix ADC. Sin embargo, para usar la opción GSLB AutomaticConfigSync para sincronizar la configuración en los sitios principales, todos los sitios principales deben estar en las versiones del software SameCitrix ADC. Si no está usando la opción AutomaticConfigSync, el sitio primario y el sitio secundario pueden estar en diferentes versiones de software Citrix ADC, pero asegúrese de que no está usando ninguna de las nuevas funciones de la versión más reciente. Esto también se aplica, en general, a dos nodos Citrix ADC que participan en GSLB.

Topología básica principal-secundario

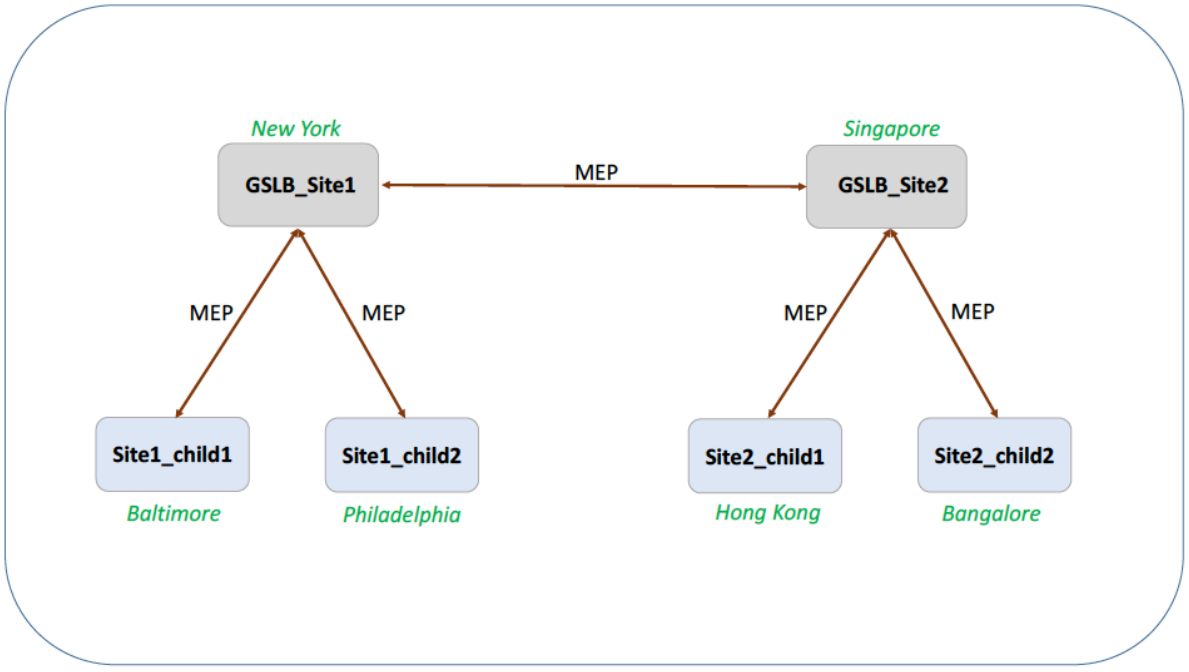
En el diagrama, SiteP1 y SiteP2 son sitios principales en una relación de pares. Los sitios P1C1 y P2C1 son los sitios secundarios de P1 y P2, respectivamente.



Configuración de una configuración principal-secundario para GSLB

Si tiene un firewall configurado en un sitio GSLB, asegúrese de que el puerto 3011 esté abierto.

En el siguiente diagrama se muestra un ejemplo de configuración principal-secundario.



- La configuración de un sitio secundario incluye el sitio secundario y su sitio principal, pero no otros sitios principales o secundarios.
- Las métricas de red, como el RTT y la información de sesión de persistencia, se sincronizan solo en los sitios principales. Por lo tanto, los parámetros como nwMetricExchange y sessionExchange están inhabilitados de forma predeterminada en todos los sitios secundarios.
- Para verificar la configuración principal-secundario correcta, verifique los estados de todos los servicios GSLB enlazados a los sitios principales.

Para configurar una configuración principal-secundario para GSLB mediante la CLI:

1. En cada sitio principal, configure todos sus sitios secundarios, los sitios principales del mismo nivel y los sitios secundarios asociados a los sitios del mismo nivel:

   Use el siguiente comando al agregar un sitio principal:

```
add gslb site <siteName> <siteIPAddress> [-publicIP <ip_addr|
   ipv6_addr|*>]
<!--NeedCopy-->
```

   Use el siguiente comando al agregar un sitio secundario:

```
add gslb site <siteName> <siteIPAddress> [-publicIP <ip_addr|
   ipv6_addr|*>] [-parentSite <string>]
<!--NeedCopy-->
```

2. En los sitios secundarios, configure el sitio secundario y asocie también el sitio secundario con su sitio principal:

   > **Nota:**
   >
   > Configure correctamente la asociación entre el sitio principal y el sitio secundario. Por ejemplo, debe configurar Site1_child1 con GSLB_Site1. No puede configurar Site1_child1 con GSLB_Site2.

   Use el siguiente comando para configurar el sitio principal con el que está asociado el sitio secundario:

```
add gslb site <siteName> <siteIPAddress> [-publicIP <ip_addr|
   ipv6_addr|*>]
<!--NeedCopy-->
```

   Use el siguiente comando para agregar un sitio secundario y asociarlo a su sitio principal:

```
add gslb site <siteName> <siteIPAddress> [-publicIP <ip_addr|
   ipv6_addr|*>] [-parentSite <string>]
<!--NeedCopy-->
```


Para obtener un ejemplo completo de una configuración principal-secundario, mediante la interfaz de línea de comandos, consulte Ejemplo de una configuración principal-secundario completa, mediante la CLI.

> **Nota**
>
> Si la dirección IP del servidor virtual de equilibrio de carga es una dirección IP privada y la dirección IP pública es diferente de esta dirección IP, debe configurar un servicio GSLB para el servidor virtual de equilibrio de carga local en el sitio secundario. Esto es necesario para la recopilación de estadísticas entre el sitio principal y el secundario.
>
> En el sitio secundario, en el símbolo del sistema, escriba:
>
> ```
> add gslb service <name> <private IP/lb vserver IP> http 80 -sitename <
> childsite name> -publicip <public IP of LB vserver>
> ```
>
> **Ejemplo:**
>
> ```
> add gslb service Service-GSLB 192.168.1.3 http 80 -GSLB_Site11 site 11
> _lb1 172.16.1.1
> ```
>
> Donde 192.168.1.3 es una dirección IP privada del servidor virtual de equilibrio de carga y 172.16.1.1 es una dirección IP pública del servidor virtual de equilibrio de carga.

Hacer una copia de seguridad del sitio principal

Nota: Esta función se introdujo en Citrix ADC versión 11.1 compilación 51.x. Para utilizar la topología del sitio principal de copia de seguridad, asegúrese de que el sitio principal y los sitios secundarios estén en Citrix ADC 11.1 compilación 51.x y posteriores.

La topología del sitio principal de copia de seguridad es útil en escenarios en los que muchos sitios secundarios están asociados a un sitio principal. Si este sitio principal deja de funcionar, todos sus sitios secundarios dejan de estar disponibles. Para evitarlo, ahora puede configurar un sitio principal de respaldo al que los sitios secundarios puedan conectarse si el sitio principal original está INACTIVO. El sitio principal envía la lista principal de respaldo a los sitios secundarios a través de los mensajes MEP.

Cuando un sitio principal está INACTIVO, los otros sitios principales en el GSLB se enteran de que un sitio principal en particular está DOWN a través de MEP porque el MEP de ese sitio principal está DOWN. Los otros sitios principales en la configuración de GSLB buscan la cadena de respaldo del principal homólogo. El sitio principal con la mayor preferencia adopta los sitios secundarios del principal que bajó. A continuación, el nuevo principal inicia una conexión con el sitio secundario. Un sitio secundario puede aceptar o rechazar la conexión después de evaluar sus conexiones existentes y la información de la lista de copias de seguridad. El principal de respaldo tarda unos segundos en adoptar los sitios secundarios.

Cuando se realiza una copia de seguridad del sitio principal original, intenta establecer conexiones con los sitios secundarios que han migrado a un sitio principal diferente. Cuando un intento de conexión tiene éxito, el sitio secundario se reasigna a su sitio principal original.

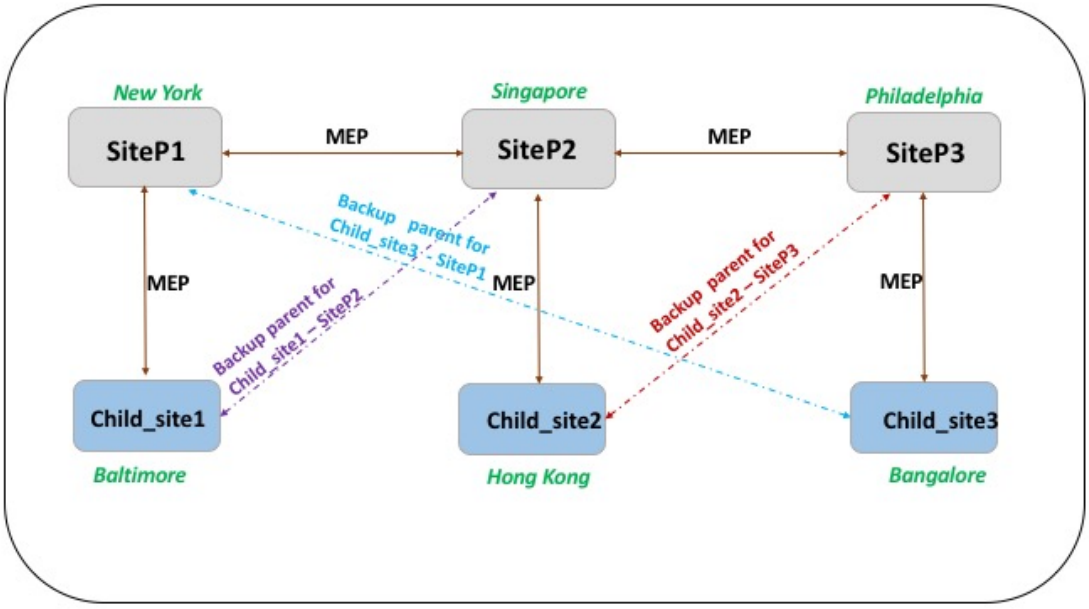
Nota:

- Solo los sitios principales se pueden configurar como copias de seguridad, y esta configuración solo se puede realizar en el sitio principal.
- Todos los sitios secundarios usan el conjunto principal de respaldo.
- La sincronización se realiza solo en los sitios principales. La configuración de los sitios secundarios de GSLB no se ve afectada por la sincronización. Esto se debe a que las configuraciones del sitio primario y del sitio secundario no son idénticas. La configuración de sitios secundarios se compone únicamente de los detalles propios y de su sitio principal. Además, no siempre se requiere que los servicios GSLB se configuren en los sitios secundarios.

Considere la configuración que se muestra en la siguiente ilustración, en la que:

- SiteP1, SiteP2 y SiteP3 son los sitios principales.
- child_site1, child_site2 y child_site3 son los sitios secundarios de SiteP1, SiteP2 y SiteP3, respectivamente.
- Sitios principales de reserva;
  - Principales de reserva de SiteP1: SiteP2 (mayor preferencia) y SiteP3
  - Principales de reserva de SiteP2: SiteP3 (mayor preferencia) y SiteP1
  - Principales de reserva de SiteP3: SiteP1 (mayor preferencia) y SiteP2

Nota: A título ilustrativo, la ilustración muestra solo un principal de copia de seguridad para cada sitio principal.



La siguiente lista resume el comportamiento de los sitios principales y secundarios en varios escenarios:

- Escenario 1: el SiteP1 deja de funcionar.
  - El SiteP2 y el SiteP3 detectan que la conexión MEP del SiteP1 está INACTIVA. SiteP2 ocupa un lugar más alto en la lista de preferencias de principales de reserva para SiteP1, por lo que intenta iniciar una conexión con child_Site1. SiteP3 supone que child_Site1 es ahora el sitio secundario del SiteP2 principal.
  - SiteP2 envía a Child_Site1 la lista de principales de reserva del SiteP1 (SiteP2 y SiteP3) a child_Site1. Child_site1 usa la lista para decidir si acepta o rechaza la conexión desde SiteP2. Acepta la conexión y se convierte en hijo del SiteP2.
  - Cuando SiteP1 está en funcionamiento de nuevo, envía a child_Site1 una solicitud de conexión. La nueva solicitud tiene prioridad y child_site 1 migra a SiteP1.
- Escenario 2: Solo la conexión MEP entre el SiteP1 y el SiteP2 ha caído. Child_site1 rechaza la solicitud de conexión del SiteP2, porque su principal, SiteP1, sigue ACTIVO.
- Escenario 3: el SiteP3 y Child_Site1 detectan que el SiteP1 está INACTIVO y la conexión MEP entre el SiteP3 y el SiteP2 también está INACTIVA. Sin embargo, el SiteP2 detecta que el SiteP1 está UP y que la conexión MEP entre el SiteP1 y el SiteP2 está UP.
  - SiteP2 no lleva a cabo ninguna acción.
  - SiteP3 comprueba la lista de copias de seguridad del SiteP1 y descubre que SiteP2 tiene una preferencia mayor que SiteP3. Pero SiteP2 está DOWN, por lo que SiteP3 intenta establecer una conexión con child_Site1. child_site1 ha detectado que SiteP1 está INACTIVO, por lo que acepta la solicitud de conexión del SiteP3.
  - Ahora la conexión entre el SiteP1 y el SiteP2 se reduce. SiteP2 comprueba la lista de copias de seguridad del SiteP1 y se encuentra como la copia de seguridad más preferida, por lo que intenta conectarse a child_Site1. child_Site1 evalúa la nueva solicitud de conexión en función de la lista del SiteP1 y encuentra a SiteP2 como la copia de seguridad más preferida, por lo que migra a SiteP2 desde SiteP3.

Para configurar un sitio principal de copia de seguridad mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
set gslb site <sitename> -backupParentlist <bkp_site1> <bkp_site2> ... <
   bkp_site5>
<!--NeedCopy-->
```


<sitename> es el sitio principal actual.

Ejemplo:

Para el sitio principal (SiteP1), los sitios (SiteP2 y SiteP3) se configuran como sitios principales de reserva.

```
set gslb site SiteP1 -backupParentlist SiteP2 SiteP3
<!--NeedCopy-->
```

Nota:

- No puede agregar un sitio nuevo como principal de respaldo. Primero debe agregar todos los sitios y, a continuación, configurar el sitio como principal de respaldo.
- Para eliminar una copia de seguridad principal, debe usar el comando unset, que anula todos los sitios que se configuraron anteriormente como sitios principales de copia de seguridad.

Para configurar un sitio principal de copia de seguridad mediante la interfaz gráfica de usuario

1. Vaya a **Configuración** > **Administración del tráfico** > **GSLB** > **Sitios**.
2. Agregue un sitio nuevo o seleccione un sitio existente.
3. Elija la opción **Backup Parent Sites** al crear o configurar el sitio GSLB.

Entidades de configuración de GSLB

August 20, 2021

Una configuración de GSLB consta de un grupo de entidades GSLB en cada dispositivo de la configuración. Estas entidades son las siguientes:

- Sitios GSLB
- Servicios GSLB
- Servidores virtuales GSLB
- Servidores virtuales de equilibrio de carga o conmutación de contenido
- Servicios ADNS
- VIP DNS

Sitios GSLB

Una configuración típica de GSLB consiste en centros de datos, cada uno de los cuales tiene varios dispositivos de red que pueden o no ser dispositivos Citrix ADC. Los centros de datos se denominan sitios GSLB. Cada sitio de GSLB es administrado por un dispositivo Citrix ADC que es local en ese sitio. Cada uno de estos dispositivos trata su propio sitio como el sitio local y todos los demás sitios, administrados por otros dispositivos, como sitios remotos.

Si el dispositivo que administra un sitio es el único dispositivo Citrix ADC en ese centro de datos, el sitio GSLB alojado en ese dispositivo actúa como marcador de posición de contabilidad para fines de auditoría, ya que no se pueden recopilar métricas. Normalmente, esto ocurre cuando el dispositivo se utiliza solo para GSLB y otros productos del centro de datos se utilizan para el equilibrio de carga o la conmutación de contenido.

Relaciones entre sitios de GSLB

El concepto de sitios es fundamental para las implementaciones de Citrix ADC GSLB. A menos que se especifique lo contrario, los sitios forman una relación de pares entre ellos. Esta relación se utiliza primero para intercambiar información de salud y, a continuación, para distribuir la carga según lo determinado por el algoritmo seleccionado. En muchas situaciones, sin embargo, una relación entre pares entre todos los sitios GSLB no es deseable. Las razones para no tener una aplicación de todos los pares podrían ser;

- Para separar claramente los sitios GSLB. Por ejemplo, para separar los sitios que participan en la resolución de consultas DNS de los sitios de administración de tráfico.
- Reducir el volumen de tráfico del Protocolo de intercambio métrico (MEP), que aumenta exponencialmente con un número creciente de sitios del mismo nivel.

Estos objetivos se pueden lograr mediante el uso de sitios GSLB primarios y secundarios.

Servicios GSLB

Un servicio GSLB suele ser una representación de un servidor virtual de equilibrio de carga o cambio de contenido, aunque puede representar cualquier tipo de servidor virtual. El servicio GSLB identifica la dirección IP, el número de puerto y el tipo de servicio del servidor virtual. Los servicios GSLB están enlazados a servidores virtuales GSLB en los dispositivos Citrix ADC que administran los sitios GSLB. Un servicio GSLB vinculado a un servidor virtual GSLB en el mismo centro de datos es local para el servidor virtual GSLB. Un servicio GSLB vinculado a un servidor virtual GSLB en un centro de datos diferente es remoto de ese servidor virtual GSLB.

> **Nota**
>
> Los sitios y servicios están intrínsecamente vinculados para indicar la proximidad entre ambos.

> Es decir, todos los servicios deben pertenecer a un sitio, y se supone que están en la misma ubicación que el sitio GSLB para fines de proximidad. Del mismo modo, los servicios y los servidores virtuales están vinculados, de modo que la lógica se vincula a los recursos disponibles.

Servidores virtuales GSLB

Un servidor virtual GSLB tiene uno o más servicios GSLB vinculados a él, y la carga equilibra el tráfico entre esos servicios. Evalúa los métodos GSLB configurados (algoritmos) para seleccionar el servicio apropiado al que enviar una solicitud de cliente. Dado que los servicios GSLB pueden representar servidores locales o remotos, la selección del servicio GSLB óptimo para una solicitud tiene el efecto de seleccionar el centro de datos que debe servir la solicitud del cliente.

El dominio para el que se configura el equilibrio de carga del servidor global debe estar enlazado al servidor virtual GSLB, ya que uno o más servicios vinculados al servidor virtual atenderán las solicitudes realizadas para ese dominio.

A diferencia de otros servidores virtuales configurados en un dispositivo Citrix ADC, un servidor virtual GSLB no tiene su propia dirección IP virtual (VIP).

Servidores virtuales de equilibrio de carga o conmutación de contenido

Un servidor virtual de equilibrio de carga o cambio de contenido representa uno o varios servidores físicos en la red local. Los clientes envían sus solicitudes a la dirección IP virtual (VIP) del servidor virtual de equilibrio de carga o conmutación de contenido, y el servidor virtual equilibra la carga entre los servidores físicos. Después de que un servidor virtual GSLB selecciona un servicio GSLB que representa un servidor virtual de equilibrio de carga local o remoto o de conmutación de contenido, el cliente envía la solicitud a la dirección VIP de ese servidor virtual.

Para obtener más información sobre los servidores y servicios virtuales de equilibrio de carga o de conmutación de contenido, consulte Equilibrio de carga o Content Switching.

Servicios ADNS

Un servicio ADNS es un tipo especial de servicio que responde solo a solicitudes DNS para dominios para los que el dispositivo Citrix ADC tiene autoridad. Cuando se configura un servicio ADNS, el dispositivo posee esa dirección IP y la anuncia. Al recibir una solicitud DNS por un servicio ADNS, el dispositivo comprueba si hay un servidor virtual GSLB enlazado a ese dominio. Si un servidor virtual GSLB está enlazado al dominio, se consulta la mejor dirección IP a la que enviar la respuesta DNS.

VIP DNS

Una IP virtual DNS es una dirección IP virtual (VIP) que representa un servidor virtual DNS de equilibrio de carga en el dispositivo Citrix ADC. Las solicitudes DNS para dominios para los que el dispositivo Citrix ADC tiene autoridad se pueden enviar a un VIP DNS.

Métodos GSLB

August 20, 2021

A diferencia de los servidores DNS tradicionales que simplemente responden con las direcciones IP de los servidores configurados, un dispositivo Citrix ADC configurado para GSLB responde con las direcciones IP de los servicios, según lo determinado por el método GSLB configurado. De forma predeterminada, el servidor virtual GSLB se establece en el método de menor conexión. Si todos los servicios GSLB están inactivados, el dispositivo responde con las direcciones IP de todos los servicios GSLB configurados.

Los métodos GSLB son algoritmos que el servidor virtual GSLB utiliza para seleccionar el servicio GSLB de mejor rendimiento. Una vez resuelto el nombre de host en la dirección web, el cliente envía tráfico directamente a la dirección IP del servicio resuelto.

El dispositivo Citrix ADC proporciona los siguientes métodos GSLB:

- Round Robin
- Menos conexiones
- Tiempo de respuesta mínimo
- Ancho de banda mínimo
- Menos paquetes
- Hash IP de origen
- Carga personalizada
- Tiempo de ida y vuelta (RTT)
- Proximidad estática

Para que los métodos GSLB funcionen con un sitio remoto, MEP debe estar habilitado o monitores explícitos deben estar enlazados a los servicios remotos. Si MEP está inhabilitado, los métodos RTT, Menos conexiones, Menos ancho de banda, Menos paquetes y Menos tiempo de respuesta por defecto son Round Robin.

Los métodos de equilibrio de carga de proximidad estática y RTT son específicos de GSLB.

Especificar un método GSLB distinto de la proximidad estática o RTT dinámico

Para obtener información sobre Round Robin, Menos conexiones, Menor tiempo de respuesta, Menor ancho de banda, Menos paquetes, Hash IP de origen o método de carga personalizada, consulte Equilibrio de carga.

Para cambiar el método GSLB mediante la CLI

En el símbolo del sistema, escriba:

```
set gslb vserver <name> -lbMethod GSLBMethod
<!--NeedCopy-->
```

Ejemplo:

```
set gslb vserver Vserver-GSLB-1 -lbMethod ROUNDROBIN
<!--NeedCopy-->
```

Para cambiar el método GSLB mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico** > **GSLB** > **Servidores virtuales**.
2. En el panel de detalles, seleccione un servidor virtual GSLB y haga clic en **Abrir**.
3. En el cuadro de diálogo Configurar servidor virtual GSLB, en la ficha Método y persistencia, en Método, seleccione un método de la lista Elegir método.
4. Haga clic en **Aceptar** y compruebe que el método seleccionado aparece en Detalles en la parte inferior de la pantalla.

Algoritmos GSLB

August 20, 2021

El siguiente algoritmo es compatible con GSLB.

- **Round Robin**: Cuando un servidor virtual GSLB está configurado para utilizar el método round robin, gira continuamente una lista de los servicios que están enlazados a él. Cuando el servidor virtual recibe una solicitud, asigna la conexión al primer servicio de la lista y, a continuación, mueve ese servicio al final de la lista.

- **Tiempo de respuesta mínimo**: Cuando el servidor virtual GSLB está configurado para utilizar el método de menor tiempo de respuesta, selecciona el servicio con el valor más bajo. Donde valor más bajo = conexiones activas actuales X tiempo medio de respuesta.

  Puede configurar este método solo para los servicios HTTP y Secure Sockets Layer (SSL). El tiempo de respuesta (también llamado Time to First Byte, o TTFB) es el intervalo de tiempo entre el envío de un paquete de solicitud a un servicio y la recepción del primer paquete de respuesta del servicio. El dispositivo NetScaler utiliza el código de respuesta 200 para calcular TTFB.

- **Conexiones mínimas**: Cuando un servidor virtual GSLB está configurado para utilizar el algoritmo GSLB de menor conexión (o método), selecciona el servicio con menor número de conexiones activas. Este es el método predeterminado, porque, en la mayoría de las circunstancias, proporciona el mejor rendimiento.

- **Ancho de banda mínimo**: Un servidor virtual GSLB configurado para utilizar el método de menor ancho de banda selecciona el servicio que actualmente está sirviendo la menor cantidad de tráfico, medido en megabits por segundo (Mbps).

- **Menos paquetes**: Un servidor virtual GSLB configurado para utilizar el método de menos paquetes selecciona el servicio que ha recibido el menor número de paquetes en los últimos 14 segundos.

- **Hash IP de origen**: Un servidor virtual GSLB configurado para utilizar el método hash IP de origen utiliza el valor hash de la dirección IPv4 o IPv6 del cliente para seleccionar un servicio. Para dirigir todas las solicitudes de direcciones IP de origen que pertenecen a una red determinada a un servidor de destino específico, debe enmascarar la dirección IP de origen. Para direcciones IPv4, utilice el parámetro NetMask. Para direcciones IPv6, utilice el parámetro V6NetMaskLength.

- **Carga personalizada**: El equilibrio de carga personalizado se realiza en parámetros del servidor como el uso de CPU, la memoria y el tiempo de respuesta. Cuando se utiliza el método de carga personalizado, el dispositivo Citrix ADC suele seleccionar un servicio que no gestiona transacciones activas. Si todos los servicios de la configuración de GSLB gestionan transacciones activas, el dispositivo selecciona el servicio con la carga más pequeña. Un tipo especial de monitor, conocido como monitor de carga, calcula la carga en cada servicio de la red. Los monitores de carga no marcan el estado de un servicio, pero sí quitan los servicios de la decisión de GSLB cuando esos servicios no están UP.

Para obtener más información, consulte Equilibrio de carga.

Proximidad estática

August 20, 2021

El método de proximidad estática para GSLB utiliza una base de datos de proximidad estática basada en direcciones IP para determinar la proximidad entre el servidor DNS local del cliente y los sitios GSLB. El dispositivo Citrix ADC responde con la dirección IP de un sitio que mejor se ajusta a los criterios de proximidad.

Si dos o más sitios GSLB en ubicaciones geográficas diferentes ofrecen el mismo contenido, el dispositivo Citrix ADC mantiene una base de datos de rangos de direcciones IP y utiliza la base de datos para tomar decisiones sobre los sitios GSLB a los que dirigir las solicitudes de clientes entrantes.

Para que funcione el método de proximidad estática, debe configurar el dispositivo Citrix ADC para que utilice una base de datos de proximidad estática existente rellenada a través de un archivo de ubicación o agregar entradas personalizadas a la base de datos de proximidad estática. Después de agregar entradas personalizadas, puede establecer sus calificadores de ubicación. Después de configurar la base de datos, está listo para especificar la proximidad estática como método GSLB.

Para obtener más información sobre cómo configurar la proximidad estática, consulte Configuración de la proximidad estática.

Método dinámico de tiempo de ida y vuelta

January 12, 2021

El tiempo dinámico de ida y vuelta (RTT) es una medida de tiempo o retraso en la red entre el servidor DNS local del cliente y un recurso de datos. Para medir RTT dinámico, el dispositivo Citrix ADC explora el servidor DNS local del cliente y recopila información de métrica RTT. A continuación, el dispositivo utiliza esta métrica para tomar su decisión de equilibrio de carga. El equilibrio de carga global del servidor supervisa el estado en tiempo real de la red y dirige dinámicamente la solicitud del cliente al centro de datos con el valor RTT más bajo.

Cuando la solicitud DNS de un cliente para un dominio llega al dispositivo Citrix ADC configurado como DNS autorizado para ese dominio, el dispositivo utiliza el valor RTT para seleccionar la dirección IP del sitio con mejor rendimiento para enviarlo como respuesta a la solicitud DNS.

El dispositivo Citrix ADC utiliza diferentes mecanismos, como la solicitud o respuesta de eco ICMP (PING), UDP y TCP para recopilar las métricas de RTT para las conexiones entre el servidor DNS local y los sitios participantes. El dispositivo envía primero un sondeo de ping para determinar el RTT. Si el sondeo ping falla, se utiliza un sondeo DNS UDP. Si el sondeo también falla, el dispositivo utiliza un sondeo TCP DNS.

Estos mecanismos se representan en el dispositivo Citrix ADC como monitores de equilibrio de carga y se identifican fácilmente debido al uso del prefijo “ldns”. Los tres monitores, en su orden predeterminado, son:

- `ldns-ping`
- `ldns-dns`
- `ldns-tcp`

Estos monitores están integrados en el dispositivo y están configurados en valores predeterminados seguros. Pero son personalizables como cualquier otro monitor del dispositivo.

Puede cambiar el orden predeterminado configurándolo explícitamente como parámetro GSLB. Por ejemplo, para establecer el orden para que sea la consulta UDP DNS seguida de PING y, a continuación, TCP, escriba el comando siguiente:

```
1 set gslb parameter -ldnsprobeOrder DNS PING TCP
2 <!--NeedCopy-->
```

A menos que se hayan personalizado, el dispositivo Citrix ADC realiza sondeos UDP y TCP en el puerto 53; sin embargo, a diferencia de los monitores de equilibrio de carga regulares, los sondeos no necesitan tener éxito para proporcionar información RTT válida. Los mensajes no disponibles del puerto ICMP, los Restablecer TCP y las respuestas de error DNS, que normalmente constituirían un error, son aceptables para calcular el valor RTT.

Una vez compilados los datos RTT, el dispositivo utiliza el protocolo de intercambio de métricas (MEP) propietario para intercambiar valores RTT entre los sitios participantes. Después de calcular las métricas RTT, el dispositivo ordena los valores RTT para identificar el centro de datos con la mejor métrica RTT (más pequeña).”

Si la información RTT no está disponible (por ejemplo, cuando el servidor DNS local de un cliente accede al sitio por primera vez), el dispositivo Citrix ADC selecciona un sitio mediante el método round robin y dirige al cliente al sitio.

Para configurar el método dinámico, configure el servidor virtual GSLB del sitio para RTT dinámico. También puede establecer el intervalo en el que se sondean los servidores DNS locales en un valor distinto del predeterminado.

Configurar un servidor virtual GSLB para RTT dinámico

Para configurar un servidor virtual GSLB para RTT dinámico, especifique el método de equilibrio de carga RTT.

El dispositivo Citrix ADC valida regularmente la información de temporización para un servidor local determinado. Si un cambio en la latencia supera el factor de tolerancia configurado, el dispositivo

actualiza su base de datos con la nueva información de temporización y envía el nuevo valor a otros sitios GSLB realizando un intercambio MEP. El factor de tolerancia predeterminado es 5 milisegundos (ms).

El factor de tolerancia RTT debe ser el mismo en todo el dominio GSLB. Si lo cambia para un sitio, debe configurar factores de tolerancia RTT idénticos en todos los dispositivos Citrix ADC implementados en el dominio GSLB.

Para configurar un servidor virtual GSLB para RTT dinámico mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
set gslb vserver <name> -lbMethod RTT -tolerance <value>
<!--NeedCopy-->
```

Ejemplo:

```
set gslb vserver Vserver-GSLB-1 -lbMethod RTT -tolerance 10
<!--NeedCopy-->
```

Para configurar un servidor virtual GSLB para RTT dinámico mediante la utilidad de configuración

Vaya a **Administración del tráfico** > **GSLB** > **Servidores virtuales** y haga doble clic en el servidor virtual.

Establecer el intervalo de sondeo de los servidores DNS locales

El dispositivo Citrix ADC utiliza diferentes mecanismos, como la solicitud o respuesta de eco ICMP (PING), TCP y UDP para obtener métricas de RTT para las conexiones entre el servidor DNS local y los sitios GSLB participantes. De forma predeterminada, el dispositivo utiliza un monitor de ping y sondea el servidor DNS local cada 5 segundos. A continuación, el dispositivo espera 2 segundos a la respuesta. Si no se recibe una respuesta en ese tiempo, utiliza el monitor DNS TCP para sondear.

Sin embargo, puede modificar el intervalo de tiempo para sondear el servidor DNS local para adaptarse a la configuración.

Para modificar el intervalo de sondeo mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
set lb monitor <monitorName> <type> -interval <integer> <units> -
   resptimeout <integer> <units>
<!--NeedCopy-->
```

Ejemplo:

```
set lb monitor ldns-tcp LDNS-TCP -interval 10 sec -resptimeout 5 sec
<!--NeedCopy-->
```

Para modificar el intervalo de sondeo mediante la utilidad de configuración

Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Monitores** y haga doble clic en el monitor que quiere modificar (por ejemplo, ping).

Método de API

January 19, 2021

Puede utilizar el método de API para determinar el servicio GSLB de mejor rendimiento. El método de API para GSLB utiliza una API REST para determinar el servicio GSLB de mejor rendimiento.

En el método de API, cuando GSLB recibe una solicitud DNS de un cliente, evalúa la solicitud con respecto a la regla especificada. Si GSLB encuentra la expresión de llamada HTTP, SYS.HTTP_CALLOUT (<name>), invoca una solicitud de API REST a un agente de llamada HTTP. GSLB utiliza la respuesta del agente de llamada HTTP para decidir el servicio de mejor rendimiento. En la respuesta DNS, GSLB devuelve la dirección IP del servicio de mejor rendimiento, de vuelta al cliente.

Para configurar un método de API GSLB mediante la CLI

Realice lo siguiente para configurar el método de API GSLB:

1. Configure una llamada HTTP.

   Para obtener más información, consulte Configuración de una llamada HTTP.

   En el símbolo del sistema, escriba:


```
add policy httpCallout <name> [-IPAddress <ip_addr|ipv6_addr>] [-
    port <port>] [-vServer <string>] [-returnType <returnType>] [-
    httpMethod (GET | POST)] [-hostExpr <string>] [-urlStemExpr <
    string>] [-headers <name(value)> ...] [-parameters <name(value)
    > ...] [-bodyExpr <string>] [-fullReqExpr <string>] [-scheme (
    http | https)] [-resultExpr <string>] [-cacheForSecs <secs>] [-
    comment <string>]
<!--NeedCopy-->
```

Ejemplo:

```
add policy httpCallout GSLB_Method_API -IPAddress 208.111.39.237 -
    port 443 -returnType TEXT -hostExpr  "\" hopx.gslb.com\ ""  -
    urlStemExpr  "\" /zones/1/customers/92395/apps/6/decision\ ""
    -headers Authorization( "Basic 19fbe6db-4332-4e3f-a8bc-
    ee47bdc726f8") -parameters ip(DNS.REQ.OPT.ECS.IP.
    TYPECAST_TEXT_T ALT CLIENT.IP.SRC.TYPECAST_TEXT_T) -scheme
    https -resultExpr  "HTTP.RES.BODY(HTTP.RES.CONTENT_LENGTH).
    XPATH_JSON(xp%/providers/Val[1]/provider%)"  -cacheForSecs 30
<!--NeedCopy-->
```

2. Especifique el método de API para el equilibrio de carga. GSLB evalúa la solicitud DNS con respecto a la regla especificada.

   En el símbolo del sistema, escriba:

```
add gslb vserver <name> <serviceType>  [-lbMethod <lbMethod>] [-
    backupLBMethod <backupLBMethod>] -rule <expression>
<!--NeedCopy-->
```

Ejemplo:

```
add gslb vserver vs1 HTTP -lbMethod API -backupLBMethod ROUNDROBIN
     -rule  "sys.http_callout(GSLB_Method_API)"
<!--NeedCopy-->
```


Configuración de ejemplo para integrar GSLB e ITM mediante API como método LB

Esta configuración permite a GSLB utilizar los aspectos de visibilidad de Internet de Citrix Intelligent Traffic Management (ITM) para determinar el mejor rendimiento del servicio GSLB.

```
/* Enable ns features */

enable ns feature lb gslb cs

/* This is a named expression that is used in the HTTP callout, used
   for result expression. */

add policy expression exp1 "HTTP.RES.BODY(HTTP.RES.CONTENT_LENGTH).
   XPATH_JSON(xp%/providers/Val[1]/provider%)"

/* This is a named expression that is used in HTTP callout, used for
   host expression. */

add policy expression exp2 ""hopx.cedexis.com""

/* This is the HTTP callout configured to request the ITM for the GSLB
   decision. */

add policy httpCallout ITM_OpenMix_API -IPAddress 208.111.39.237 -port
   80 -returnType TEXT -hostExpr exp2 -urlStemExpr ""/zones/1/customers
   /61770/apps/3/decision"" -headers Authorization("Basic a310697a-1d69
   -48bf-8f36-55742a8e894e") -parameters ip(DNS.REQ.OPT.ECS.IP.
   TYPECAST_TEXT_T ALT CLIENT.IP.SRC.TYPECAST_TEXT_T) -scheme http -
   resultExpr exp1 -cacheForSecs 30

/* Add service 1 */
add service sg1 98.136.103.24 HTTP 80 -gslb NONE -maxClient 0 -maxReq 0
    -cip DISABLED -usip NO -useproxyport YES -sp OFF -cltTimeout 180 -
   svrTimeout 360 -CKA NO -TCPB NO -CMP NO

/* Add service 2 */
add service sg2 172.217.194.113 HTTP 80 -gslb NONE -maxClient 0 -maxReq
    0 -cip DISABLED -usip NO -useproxyport YES -sp OFF -cltTimeout 180
   -svrTimeout 360 -CKA NO -TCPB NO -CMP NO

/* Add ADNS service */

add service adns1 10.102.217.106 ADNS 53 -gslb NONE -maxClient 0 -
   maxReq 0 -cip DISABLED -usip NO -useproxyport NO -sp OFF -cltTimeout
```



```
      120 -svrTimeout 120 -CKA NO -TCPB NO -CMP NO
26
27 /* Add lb vserver 1 for service 1 */
28 add lb vserver lbvs1 HTTP 10.102.217.116 80 -persistenceType NONE -
      cltTimeout 180
29
30 /* Add lb vserver 2 for service 2 */
31 add lb vserver lbvs2 HTTP 10.102.217.117 80 -persistenceType NONE -
      cltTimeout 180
32
33 /* Bind service 1 to lb vserver 1 */
34
35 bind lb vserver lbvs1 sg1
36
37 /* Bind service 2 to lb vserver 2 */
38
39 bind lb vserver lbvs2 sg2
40
41 /* Configure API GSLB method on GSLB virtual server to call the HTTP
      callout. This HTTP callout requests the ITM for the GSLB decision
      and returns GSLB service name, which should serve the request. */
42
43 add gslb vserver vs1 HTTP -lbMethod API -backupLBMethod ROUNDROBIN -
      rule "sys.http_callout(ITM_OpenMix_API)" -tolerance 0
44
45 /* Add GSLB site */
46
47 add gslb site site1 10.102.217.106 -publicIP 10.102.217.106
48
49 /* Add GSLB service 1 */
50
51 add gslb service aws_ec2_ap_south_1_asia_pacific_mumbai_1
      10.102.217.116 HTTP 80 -publicIP 10.102.217.116 -publicPort 80 -
      maxClient 0 -siteName site1 -sitePersistence HTTPRedirect -
      sitePrefix gs2. -cltTimeout 180 -svrTimeout 360 -downStateFlush
      ENABLED
52
53 /* Add GSLB service 2 */
54
55 add gslb service aws_ec2_ap_south_1_asia_pacific_mumbai 10.102.217.117
      HTTP 80 -publicIP 10.102.217.117 -publicPort 80 -maxClient 0 -
      siteName site1 -sitePersistence HTTPRedirect -sitePrefix gs1. -
      cltTimeout 180 -svrTimeout 360 -downStateFlush ENABLED
56
57 /* Bind the GSLB service 1 to GSLB server 1 */
```



```
bind gslb vserver vs1 -serviceName
    aws_ec2_ap_south_1_asia_pacific_mumbai_1

/* Bind the GSLB service 2 to GSLB server 2 */
bind gslb vserver vs1 -serviceName
    aws_ec2_ap_south_1_asia_pacific_mumbai

/* Bind a domain name to the GSLB virtual server */
bind gslb vserver vs1 -domainName testruchit104.com -TTL 5

<!--NeedCopy-->
```

Configurar proximidad estática

January 19, 2021

Para que funcione el método de proximidad estática, debe configurar el dispositivo Citrix ADC para que utilice una base de datos de proximidad estática existente rellenada a través de un archivo de ubicación o agregar entradas personalizadas a la base de datos de proximidad estática. Después de agregar entradas personalizadas, puede establecer sus calificadores de ubicación. Después de configurar la base de datos, está listo para especificar la proximidad estática como método GSLB.

Este documento incluye la siguiente información:

- Adición de un archivo de ubicación para crear una base de datos de proximidad estática
- Adición de Entradas Personalizadas a una Base de Datos de Proximidad Estática
- Configuración de los calificadores de ubicación
- Especificación del método de proximidad
- Sincronización de Base de Datos de Proximidad Estática GSLB

Agregar un archivo de ubicación para crear una base de datos de proximidad estática

July 27, 2022

Una base de datos de proximidad estática es un archivo ASCII basado en UNIX. Las entradas agregadas a esta base de datos desde un archivo de ubicación se denominan entradas estáticas. Solo se puede

cargar un archivo de ubicación en un dispositivo Citrix ADC. La adición de un nuevo archivo de ubicación anula el archivo existente. La cantidad de entradas en la base de datos de proximidad estática está limitada por la memoria configurada en el dispositivo Citrix ADC.

La base de datos de proximidad estática se puede crear en el formato predeterminado o en un formato derivado de bases de datos de terceros configuradas comercialmente (como www.maxmind.com y www.ip2location.com).

El dispositivo Citrix ADC incluye los dos archivos de base de datos de geolocalización de IP siguientes. Se trata de archivos GeoLite2, publicados por MaxMind.

- Citrix_Netscaler_InBuilt_GeoIP_DB_IPv4
- Citrix_Netscaler_InBuilt_GeoIP_DB_IPv6

Estos archivos de base de datos están disponibles en un formato compatible con el dispositivo Citrix ADC en el directorio /var/netscaler/inbuilt_db.

Puede utilizar estas bases de datos de geolocalización IP como archivo de ubicación para el método GSLB basado en proximidad estática o en directivas basadas en ubicación.

Estas bases de datos varían en los detalles que proporcionan. No hay una aplicación estricta del formato de archivo de base de datos, excepto que el archivo predeterminado tiene etiquetas de formato. Los archivos de base de datos son archivos ASCII que utilizan una coma como delimitador de campo. Existen diferencias en la estructura de los campos y la representación de las direcciones IP en las ubicaciones.

El parámetro format describe la estructura del archivo para el dispositivo Citrix ADC. Si se especifica un valor incorrecto para la opción de formato, se pueden dañar los datos internos.

> **Nota**
>
> - Después de una actualización, si el directorio /var/netscaler/inbuilt_db/ contiene el archivo de base de datos (Citrix_Netscaler_InBuilt_GeoIP_DB.csv) de las versiones anteriores del software Citrix ADC, el archivo se conserva.
> - La ubicación predeterminada del archivo de base de datos es /var/netscaler/locdb, y en una configuración de alta disponibilidad (HA), debe haber una copia idéntica del archivo en la misma ubicación en ambos dispositivos Citrix ADC.
> - Si el archivo de ubicaciones se almacena en una ubicación que no sea la predeterminada, especifique la ruta del archivo de ubicaciones.
> - Para particiones de administración, la ruta predeterminada es: /var/partitions/<`partitionName`>/netscaler/locdb.
> - Algunas bases de datos proporcionan nombres cortos de países de acuerdo con la norma ISO-3166 y también nombres de países largos. Citrix ADC utiliza nombres cortos al almacenar y hacer coincidir los calificadores.
> - Para crear una base de datos de proximidad estática, inicie sesión en el shell de UNIX del

dispositivo Citrix ADC y use un editor para crear un archivo con los detalles de la ubicación en uno de los formatos compatibles con Citrix ADC.

- El dispositivo Citrix ADC se entrega con la base de datos GeoLite2 (IPv4 e IPv6), pero Citrix no mantiene ni actualiza la base de datos GeoLite2 de MaxMind con regularidad. Si es necesario, puede obtener la base de datos GeoLite2 de www.maxmind.com y convertirla al formato de base de datos Citrix ADC. Para obtener más información, consulte Script para convertir el formato de base de datos de MaxMind GeoLite2 al formato de base de datos Citrix ADC.

Para agregar un archivo de ubicación estática mediante la CLI

En el símbolo del sistema, escriba:

```
add locationFile <locationFile> [-format <format>]
-  show locationFile
<!--NeedCopy-->
```

Ejemplo:

```
add locationFile /var/netscaler/locdb/nsgeo1.0 -format netscaler
Done

show locationFile
Location File: /var/netscaler/locdb/nsgeo1.0
Format: netscaler
 Done
>
<!--NeedCopy-->
```

Ejemplo:

```
add locationFile /var/netscaler/inbuilt_db/
   Citrix_Netscaler_InBuilt_GeoIP_DB_IPv4 -format netscaler

add locationFile6 /var/netscaler/inbuilt_db/
   Citrix_Netscaler_InBuilt_GeoIP_DB_IPv6 -format netscaler
<!--NeedCopy-->
```

Para agregar un archivo de ubicación estática mediante la GUI:

1. Vaya a **AppExpert** > **Ubicación**, haga clic en la ficha **Base de datos estática**.
2. Haga clic en **Agregar** para agregar un archivo de ubicación estática.

Puede ver una base de datos de archivos de ubicación importada mediante el cuadro de diálogo **Ver base** de datos en la utilidad de configuración. No hay un equivalente en CLI.

Para ver un archivo de ubicación estática mediante la GUI:

1. Vaya a **AppExpert** > **Ubicación**, haga clic en la ficha **Base de datos estática**.
2. Seleccione un archivo de ubicación estática y, en la lista **Acción**, haga clic en **Ver base de datos**.

Para convertir un archivo de ubicación al formato Citrix ADC:

De forma predeterminada, cuando agrega un archivo de ubicación, se guarda en el formato Citrix ADC. Puede convertir un archivo de ubicación de otros formatos al formato Citrix ADC.

> **Nota**: Solo se puede acceder a la opción `nsmap` desde la interfaz de línea de comandos. La conversión solo es posible en el formato Citrix ADC.

Para convertir el formato de base de datos estática, en el indicador de la CLI, escriba el siguiente comando:

```
nsmap -f <inputFileFormat> -o <outputFileName> <inputFileName>
<!--NeedCopy-->
```

Ejemplo:

```
 nsmap -f ip-country-region-city -o nsfile.ns ip-country-region-city.
    csv
<!--NeedCopy-->
```

Script para convertir el formato de base de datos MaxMind GeoLite2 al formato de base de datos Citrix ADC

La base de datos GeoIP de MaxMind no se puede usar directamente en Citrix ADC. La base de datos GeoIP de MaxMind debe convertirse al formato Citrix ADC y, a continuación, cargarse para la detección de ubicación IP en el método de proximidad estática GSLB y otras funciones, como directivas.

Puede utilizar un script para convertir el formato de base de datos GeoLite2 al formato de base de datos de Citrix ADC. Este script se puede utilizar para convertir archivos IPv4 e IPv6.

El guion está disponible en la ubicación: https://github.com/citrix/MaxMind-GeoIP-Database-Conversion-Citrix-ADC-Format

Pasos para convertir la base de datos GeoIP2 al formato Citrix ADC

1. Descargue la base de datos GeoLite2 City o GeoLite2 Country en formato CSV desde https://dev.maxmind.com/geoip/geoip2/geolite2/.
2. Copie el archivo en un directorio Citrix ADC (por ejemplo, /var). Descomprima el archivo con el siguiente comando de shell, que crearía un directorio con el mismo nombre.

   ```
   tar -xf <filename>
   ```

3. Descargue el script Convert_GeoIPDB_To_Netscaler_Format.pl de https://github.com/citrix/MaxMind-GeoIP-Database-Conversion-Citrix-ADC-Format y cópielo en el directorio creado en el paso 2.
4. Para comprobar las opciones aceptables para la ejecución del script, ejecute el siguiente comando:

   ```
   perl Convert_GeoIPDB_To_Netscaler_Format.pl -help
   ```

   Diversas opciones disponibles son:

   - `<filename>` Archivo de salida IPv4. Nombre de archivo de salida predeterminado: Netscaler_Maxmind_GeoIP_DB_IPv4.csv
   - `-p <filename>` archivo de salida IPv6. Nombre de archivo de salida predeterminado: Netscaler_Maxmind_GeoIP_DB_IPv6.csv
   - `-logfile <filename>` Archivo que contiene una lista de eventos/mensajes
   - `-debug` Imprime todos los mensajes en STDOUT

5. Ejecute el siguiente comando para convertir el formato de base de datos GeoLite2 al formato de base de datos Citrix ADC.

   ```
   perl Convert_GeoIPDB_To_Netscaler_Format.pl
   ```

   > **Nota:** La operación puede tardar hasta 5 minutos.

   Los nombres de archivo predeterminados utilizados en el script son los de la base de datos basada en MaxMind GeoLite2 City. Si ha descargado la base de datos GeoLite2 Country, debe proporcionar los nombres de los archivos de entrada en consecuencia tal como se enumeran.

   - `-b <filename>` nombre del archivo de bloque IPv4 que se va a convertir. Nombre de archivo por defecto: GeoLite2-City-Blocks-IPv4.csv
   - `-i <filename>` nombre del archivo de bloque IPv6 que se va a convertir. Nombre de archivo por defecto: GeoLite2-City-Blocks-IPv6.csv
   - `-l <filename>` nombre del archivo de ubicación que se va a convertir. Nombre de archivo por defecto: GeoLite2-City-Locations-en.csv

   Ejemplo:


```
perl Convert_GeoIPDB_To_Netscaler_Format.pl -b GeoLite2-Country-
   Blocks-IPv4.csv -i GeoLite2-Country-Blocks-IPv6.csv -l
   GeoLite2-Country-Locations-en.csv
<!--NeedCopy-->
```

A continuación se muestran los archivos de salida generados después de ejecutar el script.

- Netscaler_Maxmind_GeoIP_DB_IPv4.csv
- Netscaler_Maxmind_GeoIP_DB_IPv6.csv

6. Una vez que se complete la conversión de la base de datos al formato Citrix ADC, use el siguiente comando para comenzar a usarla.

   ```
   add locationFile <locationFile>
   ```

Agregar un archivo de base de datos estática de terceros en un dispositivo Citrix ADC

Realice los siguientes pasos para agregar un archivo de base de datos estática de terceros en un dispositivo Citrix ADC.

1. Obtenga el archivo de base de datos de ubicaciones de un proveedor externo, como www.maxmind.com.

   > **Nota:**
   >
   > Si descarga el archivo de base de datos de ubicaciones de www.maxmind.com, puede usar el script disponible para convertirlo al formato de base de datos Citrix ADC. Para obtener información sobre el uso del script, consulte Script para convertir el formato de base de datos MaxMind GeoLite2 al formato de base de datos Citrix ADC.
   >
   > Para las bases de datos de ubicación descargadas de otros proveedores de terceros, debe convertirlas al formato de base de datos Citrix ADC antes de agregarlas a un dispositivo Citrix ADC.

2. Ejecute este comando para agregar un archivo de ubicación estática:

```
add location file <locationfile Name>
<!--NeedCopy-->
```

> **Nota:**
>
> - Si el archivo de base de datos de ubicaciones no se coloca en la ubicación predeterminada **/var/netscaler/locdb**, `<locationfile Name>` debe contener la ubicación del

archivo junto con el nombre del archivo.
- Antes de ejecutar el comando `add location file <locationfile Name>`:
  - Make sure that the location database file is present in one of the directories of the Citrix ADC appliance.
  - Run the `sync HA files` command on the high availability setup and the `sync cluster files` command in a cluster setup. These commands ensure that the location database file is copied to the secondary appliance of the high availability pair and peer nodes of the cluster.

3. Ejecute el siguiente comando para asegurarse de que se carga la base de datos de ubicaciones:

```
show location parameter
<!--NeedCopy-->
```

Este comando muestra los parámetros, como el número de entradas estáticas. Si la base de datos no se carga correctamente, este comando también muestra un mensaje de error. Se puede cargar un máximo de 3 M-1 (3 millones menos uno) de entradas.

4. Ejecute el siguiente comando para ver la ubicación del sitio GSLB:

```
show gslb service
<!--NeedCopy-->
```

Nota

- Si la base de datos se carga correctamente, la ubicación de los sitios GSLB se rellena automáticamente en la base de datos.
- Solo puede especificar un archivo de ubicación en la configuración del dispositivo.
- Si no se encuentra ninguna coincidencia para una dirección IP entrante, la solicitud se procesa mediante el método Round Robin.

5. Ejecute el siguiente comando para configurar el método GSLB en el dispositivo:

```
set gslb vserver GSLBVserverName -lbMethod MethodType
<!--NeedCopy-->
```


Agregar entradas personalizadas a una base de datos de proximidad estática

January 12, 2021

Las entradas personalizadas tienen prioridad sobre las entradas estáticas en la base de datos de proximidad. Puede agregar un máximo de 500 entradas personalizadas. Para una entrada personalizada, indique todos los calificadores omitidos con un asterisco (*) y, si los calificadores tienen un punto o espacio en el nombre, escriba el parámetro entre comillas dobles. Los primeros 31 caracteres se evalúan para cada calificador. También puede proporcionar la longitud y latitud de la ubicación geográfica del rango de direcciones IP para seleccionar un servicio con el método GSLB de proximidad estática.

Para agregar entradas personalizadas mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para agregar una entrada personalizada a la base de datos de proximidad estática y compruebe la configuración:

```
add location < IPfrom> < IPto> <preferredLocation> [-longitude <integer
   >[-latitude <integer>]]
show location
<!--NeedCopy-->
```

Ejemplo:

```
>add location 192.168.100.1 192.168.100.100 *.us.ca.mycity
<!--NeedCopy-->
```

```
>show location
<!--NeedCopy-->
```

Parámetros para agregar entradas personalizadas

- IPFrom

  Primera dirección IP del rango, en notación decimal punteada. Este es un argumento obligatorio.

- IPA

  Última dirección IP del rango, en notación decimal con puntos. Este es un argumento obligatorio.

- preferredLocation

  Cadena de calificadores, en notación punteada, que describe la ubicación geográfica del rango de direcciones IP. Cada calificador es más específico que el que lo precede, como en continent.country.region.city.isp.organization. Por ejemplo, “na.us.ca.san Jose.att.Citrix”.

  Nota: Un calificador que incluya un punto (.) o un espacio () debe estar entre comillas dobles.

  Este es un argumento obligatorio. Longitud máxima: 197

- longitude

  Valor numérico, en grados, que especifica la longitud de la ubicación geográfica del rango de direcciones IP.

  Nota: Los parámetros de longitud y latitud se utilizan para seleccionar un servicio con el método GSLB de proximidad estática. Si no se especifican, la selección se basa en los calificadores especificados para la ubicación.

  Valor máximo: 180

- latitude

  Valor numérico, en grados, que especifica la latitud de la ubicación geográfica del rango de direcciones IP.

  Nota: Los parámetros de longitud y latitud se utilizan para seleccionar un servicio con el método GSLB de proximidad estática. Si no se especifican, la selección se basa en los calificadores especificados para la ubicación.

  Valor máximo: 180

Para agregar entradas personalizadas mediante la utilidad de configuración

Vaya a **AppExpert** > **Ubicación**, haga clic en la ficha **Entradas personalizadas** y agregue las entradas personalizadas.

Establecer calificadores de ubicación

April 21, 2022

La base de datos utilizada para implementar la proximidad estática tiene la ubicación de los sitios GSLB. Cada ubicación tiene un rango de direcciones IP y hasta seis calificadores para ese rango. Los calificadores son cadenas literales y se comparan en un orden prescrito en tiempo de ejecución. Cada ubicación debe tener al menos un calificador. Las etiquetas de calificadores definen el significado de los calificadores (contexto), definidos por el usuario. Citrix ADC tiene dos contextos integrados:

Contexto geográfico, que tiene las siguientes etiquetas calificadoras:

- Clasificatorio 1 — "Continente"
- Clasificatoria 2 — "País"
- Clasificatorio 3 — "Estado"
- Clasificatorio 4 — "Ciudad"
- Clasificatorio 5: "ISP"
- Clasificatoria 6 — "Organización"

Entradas personalizadas, que tienen las siguientes etiquetas calificadoras:

- Clasificatorio 1: "Clasificatorio 1"
- Clasificatorio 2: "Clasificatorio 2"
- Clasificatorio 3: "Clasificatorio 3"
- Clasificatorio 4: "Clasificatorio 4"
- Clasificatorio 5: "Clasificatorio 5"
- Clasificatorio 6 — "Clasificatorio 6"

Si el contexto geográfico se establece sin calificador Continent, Continent se deriva de Country. Incluso las etiquetas calificadoras integradas se basan en el contexto y las etiquetas se pueden cambiar. Estas etiquetas calificadoras especifican las ubicaciones asignadas con las direcciones IP utilizadas para tomar decisiones de proximidad estáticas.

Para tomar una decisión estática basada en la proximidad, el dispositivo Citrix ADC compara los atributos de ubicación (calificadores) derivados de la dirección IP del solucionador del servidor DNS local con los atributos de ubicación de los sitios participantes. Si solo coincide un sitio, el dispositivo devuelve la dirección IP de ese sitio. Si hay varias coincidencias, el sitio seleccionado es el resultado de un round robin en los sitios GSLB coincidentes. Si no hay coincidencia, el sitio seleccionado es el resultado de un round robin en todos los sitios configurados. Un sitio que no tiene calificadores se considera una coincidencia.

Las reglas GEO para la expresión de directivas basadas en la ubicación permiten comprobar las coincidencias de caracteres comodín. Esta función comprueba si los calificadores comodín coinciden con cualquier otro calificador, incluidos los que no sean comodines o no. La coincidencia de caracteres comodín se realiza mediante el atributo `matchWildcardtoany` que se agrega al comando `set locationParameter`.

El atributo `matchWildcardtoany` se puede establecer en los siguientes valores:

- **Sí:** los clasificatorios comodín coinciden con cualquier otro clasificatorio.

- **No:** los calificadores comodín no coinciden con los calificadores que no sean comodines, sino que coinciden con otros calificadores comodín. La opción predeterminada es **No**.
- **Expresión:** los calificadores comodín de una expresión coinciden con cualquier calificador de una ubicación LDNS, pero los calificadores comodín de la ubicación LDNS no coinciden con los calificadores que no sean comodines de una expresión.

Ejemplo:

```
add dns policy1 ”CLIENT.IP.SRC.MATCHES_LOCATION(”Continent.country
    \*.\*.\*.\* \ “)”  <action>
<!--NeedCopy-->
```

Para establecer los parámetros de ubicación mediante la CLI

En el símbolo del sistema, escriba:

```
set locationparameter -context <context> -q1label <string> [-q2label <
    string>] [-q3label <string>] [-q4label <string>] [-q5label <string>]
     [-q6label <string>] -matchWildcardtoany [Yes | No | Expression]
<!--NeedCopy-->
```

Ejemplo:

```
set locationparameter -context custom -q1label asia -matchWildcardtoany
    Yes
<!--NeedCopy-->
```

Para establecer los parámetros de ubicación mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > GSLB > Base de datos y entradas**.
2. En **Configuración**, haga clic en **Cambiar parámetros de ubicación**.
3. En la página **Configurar parámetros de ubicación**, defina los parámetros de ubicación.

Ejemplo de configuración (mediante CLI)

Tenga en cuenta la siguiente configuración de red:

- Nombre del servidor virtual GSLB: gv1

- Dirección IP del servidor virtual GSLB: 1.1.1.2
- Servicio GSLB: gsvc1 enlazado a gv1
- Nombre de archivo DB de ubicación: sample.csv
- Calificadores de geolocalización: se configuran los calificadores 1 y 2. El resto se establece para que coincida con el comodín.
  - Clasificatoria 1: Asia
  - Clasificatorio 2—IR
  - Clasificatorio 3-*
  - Clasificatorio 4-*
  - Clasificatorio 5-*
  - Clasificatorio 6-*
- Directiva de DNS: la directiva, pol1, está configurada para eliminar los paquetes si hay una coincidencia.

Establezca el parámetro location y configure la directiva de DNS de la siguiente manera:

```
set locationParameter -q2label Country_Code -q3label Subdivision_1_Name
    -q4label Subdivision_2_Name -q5label City

add locationFile "/var/netscaler/inbuilt_db/sample.csv"

add gslb vserver gv1 HTTP -backupLBMethod ROUNDROBIN -tolerance 0

add dns policy pol1 "CLIENT.IP.SRC.MATCHES_LOCATION("Asia.IR
   .\*.\*.\*.\*")||CLIENT.IP.SRC.MATCHES_LOCATION("Asia.SY.\*.\*.\*.\*"
   )||CLIENT.IP.SRC.MATCHES_LOCATION("Asia.SD.\*.\*.\*.\*")||CLIENT.IP.
   SRC.MATCHES_LOCATION("Asia.KP.\*.\*.\*.\*")||CLIENT.IP.SRC.
   MATCHES_LOCATION("North America.CU.\*.\*.\*.\*")||CLIENT.IP.SRC.
   MATCHES_LOCATION("Europe.UA.Crimea.\*.\*.\*.\*")"
   dns_default_act_Drop

bind dns global pol1 1 -gotoPriorityExpression 65535 -type REQ_DEFAULT

add gslb service gsvc1 1.1.1.2 HTTP 80 -publicIP 1.1.1.2 -publicPort 80
    -maxClient 0 -healthMonitor NO -siteName s1 -cltTimeout 180 -
   svrTimeout 360 -downStateFlush ENABLED

bind gslb vserver gv1 -serviceName gsvc1

bind gslb vserver gv1 -domainName www.gslbnew.com -TTL 5
<!--NeedCopy-->
```


Agregue las siguientes entradas de cliente en el archivo de base de datos de ubicaciones. En este ejemplo, el nombre del archivo de base de datos de ubicación es sample.csv:

```
10.106.24.170,10.106.24.190,,,,,,,8.0000,47.0000

10.102.82.170,10.102.82.190,Asia,,,,,,-73.9924,40.7553

10.106.24.140,10.106.24.150,,IR,,,,,51.4231,35.6961
<!--NeedCopy-->
```

Según la configuración anterior, los clientes entre 10.106.24.170 y 10.106.24.190 no tienen ningún calificador comodín definido. Los clientes entre 10.106.24.140 y 10.106.24.150 tienen el calificador 2 como IR.

Establezca el calificador comodín de coincidencia en NO:

```
set locationparameter -matchWildcardtoany no
<!--NeedCopy-->
```

Cuando el calificador de comodín de coincidencia se establece en NO, los calificadores de comodín solo coinciden con los calificadores de comodín definidos. No coincide con ningún otro calificador que no sea comodín.

- Las consultas DNS que llegan a 10.106.24.147 coinciden con el calificador comodín definido (calificador 2 = IR). Por lo tanto, la directiva de DNS entra en vigor y elimina las consultas.

  Al ejecutar el comando `dig @10.102.82.13 www.gslbnew.com` en el cliente 10.106.24.147, el resultado muestra que los servidores no eran accesibles.

  ```
  root@ns#  dig @10.102.82.13 www.gslbnew.com

  ; <<>> DiG 9.11.23 <<>> @10.102.82.13 www.gslbnew.com
  ; (1 server found)
  ;; global options: +cmd
  ;; connection timed out; no servers could be reached
  <!--NeedCopy-->
  ```

- Las consultas DNS procedentes de 10.106.24.180 no coinciden con los calificadores definidos. La directiva de DNS no entra en vigor y las consultas se procesan.

  Ejecute el comando `dig @10.102.82.13 www.gslbnew.com` en el cliente 10.106.24.180. El resultado muestra la dirección IP del servidor virtual GSLB.


```
root@ns# dig @10.102.82.13 www.gslbnew.com

; <<>> DiG 9.11.23 <<>> @10.102.82.13 www.gslbnew.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64265
;; flags: qr aa rd ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0,
   ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;www.gslbnew.com. IN    A

;; ANSWER SECTION:
www.gslbnew.com.    5   IN  A   1.1.1.2

;; Query time: 12 msec
;; SERVER: 10.102.82.13#53(10.102.82.13)
;; WHEN: Tue Mar 29 22:46:40 UTC 2022
;; MSG SIZE  rcvd: 60
<!--NeedCopy-->
```

Establezca el calificador comodín de coincidencia en Sí:

```
set locationparameter -matchWildcardtoany yes
<!--NeedCopy-->
```

Cuando el calificador de comodín de coincidencia se establece en sí, los calificadores de comodín coinciden con cualquier calificador de comodín (calificador definido y no comodín).

- Las consultas DNS que llegan 10.106.24.147 coinciden con el calificador definido (calificador 2 = IR). Por lo tanto, la directiva de DNS entra en vigor y elimina las consultas.

  Ejecute el comando `dig @10.102.82.13 www.gslbnew.com` en el cliente 10.106.24.147. El resultado muestra que no se podía acceder a los servidores.

```
root@ns#  dig @10.102.82.13 www.gslbnew.com

```



```
3   ; <<>> DiG 9.11.23 <<>> @10.102.82.13 www.gslbnew.com
4   ; (1 server found)
5   ;; global options: +cmd
6   ;; connection timed out; no servers could be reached
7   <!--NeedCopy-->
```

- Las consultas procedentes de 10.106.24.180 coinciden con los calificadores no comodín. Por lo tanto, la directiva de DNS entra en vigor y elimina las consultas.

  Ejecute el comando `dig @10.102.82.13 www.gslbnew.com` en el cliente 10.106.24.180. El resultado muestra que no se podía acceder a los servidores.

```
1   root@ns# dig @10.102.82.13 www.gslbnew.com
2
3   ; <<>> DiG 9.11.23 <<>> @10.102.82.13 www.gslbnew.com
4   ; (1 server found)
5   ;; global options: +cmd
6   ;; connection timed out; no servers could be reached
7   <!--NeedCopy-->
```

Establezca el calificador comodín de coincidencia en Expresión:

```
1 set locationparameter -matchWildcardtoany expression
2 <!--NeedCopy-->
```

Cuando el calificador de comodín de coincidencia se establece en expresión, los calificadores de comodín coinciden con el calificador disponible en la directiva de DNS o con los calificadores disponibles en el archivo de base de datos de ubicaciones.

- Las consultas DNS que llegan a 10.106.24.147 coinciden con los calificadores comodín definidos en la directiva de DNS. Por lo tanto, la directiva de DNS entra en vigor y elimina las consultas.

  Ejecute el comando `dig @10.102.82.13 www.gslbnew.com` en el cliente 10.106.24.147. El resultado muestra que no se podía acceder a los servidores.

```
1   root@ns#  dig @10.102.82.13 www.gslbnew.com
2
3   ; <<>> DiG 9.11.23 <<>> @10.102.82.13 www.gslbnew.com
4   ; (1 server found)
5   ;; global options: +cmd
6   ;; connection timed out; no servers could be reached
```



```
<!--NeedCopy-->
```

- Las consultas procedentes de 10.106.24.180 no coinciden con los calificadores de la directiva de DNS. Por lo tanto, la directiva de DNS no entra en vigor y las consultas se procesan.

  Ejecute el comando `dig @10.102.82.13 www.gslbnew.com` en el cliente 10.106.24.180. El resultado muestra la dirección IP del servidor virtual GSLB.

```
root@ns# dig @10.102.82.13 www.gslbnew.com

; <<>> DiG 9.11.23 <<>> @10.102.82.13 www.gslbnew.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64265
;; flags: qr aa rd ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0,
   ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;www.gslbnew.com.  IN   A

;; ANSWER SECTION:
www.gslbnew.com.    5   IN  A   1.1.1.2

;; Query time: 12 msec
;; SERVER: 10.102.82.13#53(10.102.82.13)
;; WHEN: Tue Mar 29 22:46:40 UTC 2022
;; MSG SIZE  rcvd: 60
<!--NeedCopy-->
```

Especificar método de proximidad

January 12, 2021

Cuando haya configurado la base de datos de proximidad estática, estará listo para especificar la proximidad estática como método GLSB.

Para especificar la proximidad estática mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para configurar la proximidad estática y verificar la configuración:

```
set gslb vserver <name> -lbMethod STATICPROXIMITY
show gslb vserver <name>
<!--NeedCopy-->
```

Ejemplo:

```
set gslb vserver Vserver-GSLB-1 -lbMethod STATICPROXIMITY
show gslb vserver
<!--NeedCopy-->
```

Para especificar la proximidad estática mediante la utilidad de configuración

1. Vaya a Administración del tráfico > GSLB > Servidores virtuales y haga doble clic en el servidor virtual.
2. Haga clic en la sección **Método** y, en la lista desplegable **Elegir método**, seleccione **STATICProximity**.

Sincronizar la base de datos de proximidad estática GSLB

January 12, 2021

La sincronización de una base de datos de proximidad estática de equilibrio de carga de servidor global (GSLB) requiere que uno de los sitios se identifique como nodo principal GSLB. Cualquier sitio de la topología se puede designar como nodo maestro. El resto de los nodos GSLB se designan automáticamente como nodos esclavos.

La sincronización de bases de datos estáticas de proximidad GSLB sincroniza los archivos en el directorio /var/netscaler/locdb a través de los nodos esclavos. Durante el proceso de sincronización, el nodo maestro obtiene la configuración en ejecución de cada uno de los nodos esclavos y la compara con la configuración del nodo maestro. El nodo principal GSLB utiliza el programa rsync para sincronizar la base de datos de proximidad estática a través de los nodos esclavos. Para acelerar el proceso de sincronización, el programa rsync solo realiza cambios suficientes para eliminar las diferencias entre los dos archivos. El proceso de sincronización no se puede revertir.

En el ejemplo siguiente se sincroniza Site2, que es un sitio esclavo, con el sitio maestro Site1. El administrador introducirá el comando **sync gslb config** en Site1:

```
sync gslb config -nowarn
Sync Time: Feb 24 2014 14:56:16
Retrieving local site info: ok
Retrieving all participating gslb sites info:
0 bytes in 0 blocks
ok
site1[Master]:
        Getting Config: ok
site2[Slave]:
        Syncing gslb static proximity database: ok
        Getting Config: ok
        Comparing config: ok
        Applying changes: ok
 Done
<!--NeedCopy-->
```

Configurar la comunicación de sitio a sitio

January 12, 2021

La comunicación de sitio a sitio de GSLB es entre los nodos de llamada a procedimiento remoto (RPC) asociados con los sitios de comunicación. Un sitio principal de GSLB establece conexiones con sitios esclavos para sincronizar la información de configuración de GSLB e intercambiar métricas de sitio.

Un nodo RPC se crea automáticamente cuando se crea un sitio GSLB y se le asigna un nombre de usuario y una contraseña generados internamente. El dispositivo Citrix ADC utiliza este nombre de usuario y contraseña para autenticarse en sitios GSLB remotos durante el establecimiento de la conexión. No son necesarios pasos de configuración para un nodo RPC, pero puede especificar una contraseña de su elección, mejorar la seguridad cifrando la información que intercambian los sitios GSLB y especificar una dirección IP de origen para el nodo RPC.

El dispositivo necesita una dirección IP propiedad de Citrix ADC para utilizarla como dirección IP de origen al comunicarse con otros sitios GSLB. De forma predeterminada, los nodos RPC utilizan una dirección IP de subred (SNIP), pero es posible que quiera especificar una dirección IP de su elección.

En los temas siguientes se describe el comportamiento y la configuración de los nodos RPC en el dispositivo Citrix ADC:

Cambiar la contraseña de un nodo RPC

Citrix recomienda proteger la comunicación entre sitios en la configuración de GSLB cambiando la contraseña de cada nodo RPC. Después de cambiar la contraseña del nodo RPC del sitio local, debe propagar manualmente el cambio al nodo RPC en cada uno de los sitios remotos.

La contraseña se almacena en forma cifrada. Puede comprobar que la contraseña ha cambiado mediante el comando show RpcNode para comparar la forma cifrada de la contraseña antes y después del cambio.

> **Nota:** GSLB utiliza una cuenta de usuario interna. Para mejorar la seguridad, Citrix recomienda cambiar también la contraseña de la cuenta de usuario interna. La contraseña de la cuenta de usuario interna se cambia a través de la contraseña del nodo RPC.

Para cambiar la contraseña de un nodo RPC mediante la interfaz de línea de comandos

En la línea de comandos, escriba los siguientes comandos para cambiar la contraseña de un nodo RPC:

```
set ns rpcNode <IPAddress> {
 -password }

show ns rpcNode
<!--NeedCopy-->
```

Ejemplo:

```
> set rpcNode 192.0.2.4 -password mypassword
 Done
> show rpcNode
.
.
.
2)  IPAddress:  192.0.2.4 Password:  d336004164d4352ce39e
    SrcIP:  *               Secure:  OFF
Done
>

<!--NeedCopy-->
```


Para anular la contraseña de un nodo RPC mediante la interfaz de línea de comandos

Para anular la configuración de la contraseña de un nodo RPC mediante la CLI, escriba el comando unset RpcNode, la dirección IP del nodo RPC y el parámetro password, sin ningún valor.

Para cambiar la contraseña de un nodo RPC mediante la utilidad de configuración

Vaya a Sistema > Red > RPC, seleccione el nodo RPC y cambie la contraseña.

Cifrar el intercambio de métricas del sitio

Puede proteger la información que se intercambia entre sitios GSLB estableciendo la opción segura para los nodos RPC en la configuración de GSLB. Con la opción segura establecida, el dispositivo Citrix ADC cifra todas las comunicaciones enviadas desde el nodo a otros nodos RPC.

Para cifrar el intercambio de métricas de sitio mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para cifrar el intercambio de métricas del sitio y verificar la configuración:

```
set ns rpcNode <IPAddress> [-secure ( YES | NO )]
show rpcNode
<!--NeedCopy-->
```

Ejemplo:

```
> set rpcNode 192.0.2.4 -secure YES
 Done
>
> show rpcNode
.
.
.
3)  IPAddress:  192.0.2.4 Password:  d336004164d4352ce39e SrcIP:
    192.0.2.3     Secure:  ON
 Done
>
<!--NeedCopy-->
```


Para anular la configuración del parámetro seguro mediante la interfaz de línea de comandos

Para desestablecer el parámetro secure mediante la CLI, escriba el comando unset RpcNode, la dirección IP del nodo RPC y el parámetro secure, sin ningún valor.

Para cifrar el intercambio de métricas de sitio mediante la utilidad de configuración de Citrix ADC

1. Vaya a Sistema > Red > RPC y haga doble clic en un nodo RPC.
2. Seleccione la opción **Secure** y haga clic en **Aceptar**.

Configurar la dirección IP de origen para un nodo RPC

De forma predeterminada, el dispositivo Citrix ADC utiliza una dirección IP de subred (SNIP) propiedad de Citrix ADC como dirección IP de origen para un nodo RPC, pero puede configurar el dispositivo para que utilice una dirección SNIP específica. Si una dirección SNIP no está disponible, el sitio GSLB no puede comunicarse con otros sitios. En tal caso, debe configurar la dirección NSIP o una dirección IP virtual (VIP) como la dirección IP de origen para un nodo RPC. Una dirección VIP se puede utilizar como dirección IP de origen de un nodo RPC solo si el nodo RPC es un nodo remoto. Si configura una dirección VIP como dirección IP de origen y quita la dirección VIP, el dispositivo utiliza una dirección SNIP.

> **Nota**
>
> A partir de la versión 11.0.64.x de NetScaler, puede configurar el dispositivo para que utilice la dirección IP del sitio GSLB como dirección IP de origen para un nodo RPC.

Para especificar una dirección IP de origen para un nodo RPC mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para cambiar la dirección IP de origen de un nodo RPC y compruebe la configuración:

```
set ns rpcNode <IPAddress> [-srcIP <ip_addr|ipv6_addr|*>]
show ns rpcNode
<!--NeedCopy-->
```

Ejemplo:

```
set rpcNode 192.0.2.4 -srcIP 192.0.2.3
```



```
2 Done
3 show rpcNode
4 <!--NeedCopy-->
```

```
1 IPAddress: 192.0.2.4 Password: d336004164d4352ce39e SrcIP: 192.0.2.3
     Secure: OFF
2 Done
3 <!--NeedCopy-->
```

Para anular la configuración del parámetro de dirección IP de origen mediante la interfaz de línea de comandos

Para desestablecer el parámetro de dirección IP de origen mediante la CLI, escriba RpcNodeCommand unset, la dirección IP del nodo RPC y el parámetro SRCIP, sin ningún valor.

Para especificar una dirección IP de origen para un nodo RPC mediante la utilidad de configuración de Citrix ADC

1. Vaya a Sistema > Red > RPC y haga doble clic en un nodo RPC.
2. En el campo Dirección IP de origen, escriba la dirección IP que quiere que el nodo RPC utilice como dirección IP de origen y haga clic en Aceptar.

> **Importante**
>
> La dirección IP de origen no se puede sincronizar entre los sitios que participan en GSLB porque la dirección IP de origen de un nodo RPC es específica de cada dispositivo Citrix ADC. Por lo tanto, después de forzar una sincronización (mediante el comando sync gslb config —ForceSync o seleccionando la opción ForceSync en la GUI), debe cambiar manualmente las direcciones IP de origen en los demás dispositivos Citrix ADC.

Configurar el protocolo de intercambio de métricas

August 20, 2021

Los centros de datos de una configuración de GSLB intercambian métricas entre sí a través del protocolo de intercambio de métricas (MEP), que es un protocolo propietario para el dispositivo Citrix ADC. El intercambio de la información de métrica comienza cuando se crea un sitio GSLB. Estas métricas incluyen información de carga, red y persistencia.

El MEP es necesario para el chequeo de estado de los centros de datos a fin de garantizar su disponibilidad. Una conexión para el intercambio de métricas de red (tiempo de ida y vuelta) puede ser iniciada por cualquiera de los centros de datos involucrados en el intercambio, pero una conexión para el intercambio de métricas de sitio siempre es iniciada por el centro de datos con la dirección IP inferior. De forma predeterminada, el centro de datos utiliza una dirección IP de subred (SNIP) para establecer una conexión con la dirección IP de un centro de datos diferente. Sin embargo, puede configurar un SNIP específico, una dirección IP virtual (VIP) o la dirección NSIP, como dirección IP de origen para el intercambio de métricas. El proceso de comunicación entre sitios GSLB utiliza el puerto TCP 3011 o 3009, por lo que este puerto debe estar abierto en firewalls que se encuentran entre los dispositivos Citrix ADC.

Nota: Puede configurar una dirección IP de sitio SNIP o GSLB como dirección IP de origen para el intercambio de métricas. Para obtener más información, consulte Configurar la dirección IP de origen para un nodo RPC.

Si los sitios de origen y destino (el sitio que inicia una conexión MEP y el sitio que recibe la solicitud de conexión, respectivamente) tienen configuradas direcciones IP privadas y públicas, los sitios intercambian información MEP mediante las direcciones IP públicas.

También puede enlazar monitores para comprobar el estado de los servicios remotos como se describe en "Supervisión de los servicios GSLB. " Cuando los monitores están enlazados, el intercambio de métricas no controla el estado del servicio remoto. Si un monitor está enlazado a un servicio remoto y el intercambio de métricas está habilitado, el monitor controla el estado de mantenimiento. La vinculación de los monitores al servicio remoto permite que el dispositivo Citrix ADC interactúe con un dispositivo de equilibrio de carga que no sea de Citrix ADC. El dispositivo Citrix ADC puede supervisar dispositivos ADC que no son de Citrix, pero no puede realizar el equilibrio de carga en ellos a menos que los monitores estén vinculados a todos los servicios GSLB y solo se utilicen métodos estáticos de equilibrio de carga (como el round robin, la proximidad estática o los métodos basados en hash).

Con NetScaler versión 11.1.51.x o posterior, para evitar interrupciones innecesarias de los servicios, puede establecer un retraso de tiempo para marcar los servicios GSLB como DOWN cuando una conexión MEP se desactiva.

Estado MEP en una configuración de alta disponibilidad

En una configuración de alta disponibilidad, el nodo principal establece conexiones con los sitios remotos y el estado MEP no se sincroniza desde el nodo principal con los nodos secundarios. Por lo tanto, el estado MEP en el nodo secundario permanece ABAJO. Cuando el nodo secundario se convierte en primario, establece conexiones MEP con el nuevo sitio GSLB y actualiza el estado MEP en consecuencia.

Habilitar el intercambio de métricas de sitio

Las métricas de sitio intercambiadas entre los sitios de GSLB incluyen el estado de cada servidor virtual de equilibrio de carga o de conmutación de contenido, el número actual de conexiones, la velocidad de paquetes actual y la información de uso del ancho de banda actual.

El dispositivo Citrix ADC necesita esta información para realizar el equilibrio de carga entre los sitios. El intervalo de intercambio métrico del sitio es de 1 segundo. Un servicio GSLB remoto debe estar enlazado a un servidor virtual GSLB local para permitir el intercambio de métricas de sitio con el servicio remoto.

Para habilitar o inhabilitar el intercambio de métricas de sitio mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para habilitar o inhabilitar el intercambio de métricas de sitio y verificar la configuración:

```
set gslb site <siteName> -metricExchange (ENABLED|DISABLED)
show gslb site** <siteName>
<!--NeedCopy-->
```

Ejemplo:

```
set gslb site Site-GSLB-East-Coast -metricExchange ENABLED
set gslb site Site-GSLB-East-Coast -metricExchange DISABLED
show gslb site Site-GSLB-East-Coast
<!--NeedCopy-->
```

Para habilitar o inhabilitar el intercambio de métricas de sitio mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico** > **GSLB** > **Sitios** y seleccione el sitio.
2. En el cuadro de diálogo **Configurar sitio GSLB**, seleccione la opción **Intercambio de métricas**.

Habilitar el intercambio de métricas de red

Si sus sitios GSLB utilizan el método de equilibrio de carga de tiempo de ida y vuelta (RTT), puede habilitar o inhabilitar el intercambio de información RTT sobre el servicio DNS local del cliente. Esta información se intercambia cada 5 segundos.

Para obtener más información sobre cómo cambiar el método GSLB a un método basado en RTT, consulte Métodos GSLB.

Para habilitar o inhabilitar el intercambio de información de métricas de red mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para habilitar o inhabilitar el intercambio de información de métricas de red y verificar la configuración:

```
set gslb site <siteName> -nwmetricExchange (ENABLED|DISABLED)
show gslb site <<siteName>
<!--NeedCopy-->
```

Ejemplo:

```
set gslb site Site-GSLB-East-Coast -nwmetricExchange ENABLED
set gslb site Site-GSLB-East-Coast -nwmetricExchange DISABLED
show gslb site Site-GSLB-East-Coast
<!--NeedCopy-->
```

Para habilitar o inhabilitar el intercambio de información de métricas de red mediante la interfaz gráfica de usuario

1. Desplácese hasta **Administración del tráfico** > **GSLB** > **Sitios**.
2. En el cuadro de diálogo **Configurar sitio GSLB**, seleccione la opción **Intercambio de métricas de red**.

Configuración de un retardo de tiempo para que los servicios GSLB se marquen como DOWN cuando una conexión MEP se desactiva

Si el estado de una conexión MEP a un sitio remoto cambia a DOWN, el estado de todos los servicios GSLB de ese sitio remoto se marca como DOWN, aunque es posible que el sitio no sea DOWN.

Ahora puede establecer un retraso para permitir un tiempo para restablecer la conexión MEP antes de que el sitio se marque como DOWN. Si se realiza una copia de seguridad de la conexión MEP antes de que expire el retraso, los servicios no se verán afectados.

Por ejemplo, si establece el retraso 10, los servicios GSLB se marcarán como DOWN hasta que la conexión MEP haya estado DOWN durante 10 segundos. Si la conexión MEP vuelve a estar UP en 10 segundos, los servicios GSLB permanecen en estado ACTIVO.

Nota: Este retraso solo se aplica a los servicios no vinculados a un monitor. El retraso no afecta a los monitores de disparo.

Para establecer un retardo de tiempo mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba el siguiente comando:

```
set gslb parameter** - GSLBSvcStateDelayTime <sec>
<!--NeedCopy-->
```

Ejemplo:

set gslb parámetro: GslbsvcStateDelayTime 10

> **Nota**
>
> En una implementación jerárquica (topología principal-secundario), si configura el servicio GSLB tanto en los sitios primario como secundario, establezca el parámetro GSLB tanto en los sitios primario como secundario. Si no configura el servicio GSLB en el sitio secundario, establezca el parámetro GSLB solo en el sitio primario.

Para establecer un retardo de tiempo mediante la interfaz gráfica de usuario

1. Vaya a **Configuración** > **Administración del tráfico** > **GSLB** > **Cambiar configuración de GSLB**.
2. En el cuadro **Tiempo de demora de estado de servicio GSLB (segundos)**, escriba el retardo de tiempo en segundos.

Configurar un tiempo de aprendizaje para los servicios GSLB cuando aparezca el estado de la conexión MEP para evitar fallas en los servicios GSLB

Cuando se reinicia un nodo o durante la conmutación por error de alta disponibilidad, el sistema se inicializa. A continuación, el nodo debe obtener información actual sobre los servicios locales y secundarios configurados para comunicar el estado del servicio a los nodos remotos a través de MEP. El nodo tarda algún tiempo en obtener la información correcta. Mientras tanto, si un nodo de pares se conecta a este nodo y solicita una actualización, el nodo podría enviar estadísticas y estado de servicio incorrectos. Esta información incorrecta podría provocar fallas de servicio y otros problemas relacionados con la funcionalidad en los nodos de pares remotos. Para evitar este caso, ahora puede establecer una hora de aprendizaje para el servicio GSLB local y secundario.

Cuando se configura un tiempo de espera de aprendizaje, el sitio de GSLB obtiene cierto tiempo de búfer (tiempo de espera de aprendizaje) para obtener las estadísticas correctas sobre sus servicios locales y secundarios. Cuando un servicio se encuentra en fase de aprendizaje, el sitio GSLB remoto

obtiene esta información en la actualización de MEP y no respeta el estado principal del sitio y las estadísticas recibidas a través de MEP para ese servicio.

Los servicios GSLB entran en la fase de aprendizaje en cualquiera de los siguientes casos.

- Se reinicia el dispositivo Citrix ADC
- Se ha producido conmutación por error de alta disponibilidad
- Se ha cambiado el nodo propietario de una configuración de GSLB de clúster
- MEP está habilitado en un nodo local
- El sitio GSLB sale del caso de la isla. Un sitio GSLB se convierte en isla cuando no está conectado a ningún otro sitio.

En una implementación principal-secundario, el principal de respaldo (si está configurado) mueve selectivamente los servicios GSLB del sitio secundario adoptado a la fase de aprendizaje cuando el principal principal se desactiva.

Para establecer un tiempo de aprendizaje del estado de servicio mediante la CLI

En el símbolo del sistema, escriba el siguiente comando:

```
set gslb parameter - SvcStateLearningTime <sec>
<!--NeedCopy-->
```

Puede configurar “SVCStateleLearningTime” en segundos. El valor predeterminado es 0 y el valor máximo es 3600. Este parámetro solo se aplica si los monitores no están vinculados a los servicios GSLB.

Ejemplo:

```
set gslb parameter - SvcStateLearningTime 10
<!--NeedCopy-->
```

Para configurar el tiempo de aprendizaje del estado del servicio mediante la GUI

1. Vaya a **Configuración > Administración del tráfico > GSLB > Panel > Cambiar la configuración de GSLB**.

   Aparecerá la página **Establecer parámetros GSLB** .

2. En el campo **Tiempo de aprendizaje del estado del servicio (segundos) de GSLB**, escriba el tiempo de aprendizaje en segundos.

Habilitar el intercambio de información de persistencia

Puede configurar el dispositivo Citrix ADC para proporcionar conexiones persistentes, de modo que una transmisión de cliente a cualquier servidor virtual de un grupo se pueda dirigir a un servidor que haya recibido transmisiones anteriores del mismo cliente.

Puede habilitar o inhabilitar el intercambio de información de persistencia en cada sitio. Esta información se intercambia una vez cada 5 segundos entre los dispositivos Citrix ADC que participan en GSLB.

Para obtener más información sobre la configuración de la persistencia, consulte Configuración de conexiones persistentes.

Para habilitar o inhabilitar el intercambio de información de persistencia mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para habilitar o inhabilitar el intercambio de información de persistencia y verificar la configuración:

```
set gslb site <siteName> -sessionExchange (ENABLED|DISABLED)
show gslb site** <siteName>
<!--NeedCopy-->
```

Ejemplo:

```
set gslb site Site-GSLB-East-Coast -sessionExchange  ENABLED
set gslb site Site-GSLB-East-Coast -sessionExchange  DISABLED
show gslb site Site-GSLB-East-Coast
<!--NeedCopy-->
```

Para habilitar o inhabilitar el intercambio de información de persistencia mediante la interfaz gráfica de usuario

1. Desplácese hasta **Administración del tráfico** > **GSLB** > **Sitios** y haga doble clic en el sitio.
2. En el cuadro de diálogo **Configurar sitio GSLB**, active o desactive la casilla de verificación **Intercambio de entrada de sesión de persistencia**.

Configurar GSLB mediante un asistente

January 19, 2021

Ahora puede utilizar un asistente para configurar los tipos de implementación de GSLB: Activo-activo, activo-pasivo y principal-secundario.

Este asistente está disponible en la GUI. Para acceder al asistente, vaya a **Configuración** > **Administración del tráfico** > **GSLB** y haga clic en **Introducción**.

También puede acceder a este asistente desde el panel GSLB. Vaya a **Configuración** > **Administración del tráfico** > **GSLB** > **Panel de control** y haga clic en **Configurar GSLB**.

Nota: También puede configurar las entidades GSLB individualmente.

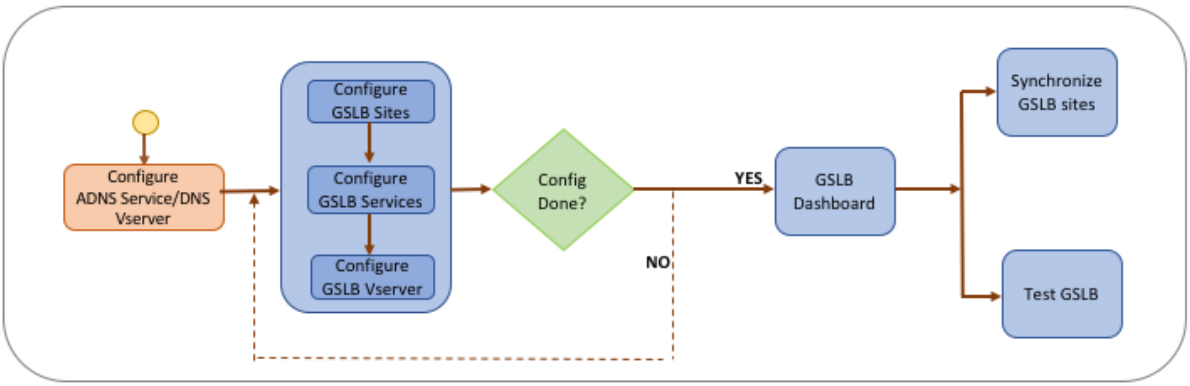
- Configuración del sitio activo-activo
- Configuración del sitio activo-pasivo
- Configuración de topología principal-secundario

> **Importante**
>
> Esta función se admite en la implementación de alta disponibilidad y no en las implementaciones de clúster y partición de administración.

Configurar sitio activo-activo

August 20, 2021

En la siguiente ilustración se muestra el flujo de trabajo implicado en una configuración de sitio activo-activo de GSLB.



Antes de comenzar a configurar un sitio activo-activo, asegúrese de haber configurado una configuración de equilibrio de carga estándar para cada conjunto de servidores o centro de datos.

Además, para sincronizar la configuración de GSLB en los sitios de GSLB en la implementación, asegúrese de que:

- Los sitios GLSB locales se configuran en todos los dispositivos de la configuración GSLB.
- Ha habilitado el acceso de administración en todos los Sitios GSLB en la configuración.
- Ha configurado el firewall para aceptar la sincronización automática y las conexiones MEP.
- Los dispositivos Citrix ADC maestros y esclavos ejecutan las mismas versiones de software Citrix ADC.
- Todos los dispositivos Citrix ADC que participan como sitios deben tener la misma versión de software Citrix ADC (los sitios no están en una relación maestro-esclavo).
- La contraseña del nodo RPC es la misma en todos los sitios de GSLB en la configuración de GSLB.

Para configurar un sitio activo-activo mediante el asistente

En la ficha Configuración, haga lo siguiente:

1. Vaya a **Administración del tráfico** > **GSLB** y, a continuación, haga clic en **Introducción**.
2. Si no ha configurado un servicio ADNS o un servidor virtual DNS para el sitio, puede hacerlo ahora.
   a) Haga clic en **Ver** y, a continuación, haga clic en **Agregar**.
   b) Introduzca el nombre del servicio, la dirección IP y seleccione el protocolo (ADNS/ADNS_TCP) a través del cual se intercambian los datos con el servicio.
3. Seleccione Sitio **activo-activo**.
4. Introduzca el nombre de dominio completo y especifique el período de tiempo para el que los proxies DNS deben almacenar en caché el registro.
5. Configure los sitios GSLB. Cada sitio debe configurarse con un sitio GSLB local, y la configuración de cada sitio debe incluir todos los demás sitios como sitios GSLB remotos. Solo puede haber un sitio local y todos los demás sitios son sitios remotos.
   a) Introduzca los detalles del sitio, como el nombre del sitio y la dirección IP del sitio.
   b) Seleccione el tipo de sitio REMOTE o LOCAL.
   c) Opcionalmente, cambie la contraseña de RPC y, si es necesario, asegúrela.
   d) Si se va a vincular un monitor al servicio GSLB, seleccione la condición bajo la que el monitor va a supervisar el servicio. Esto será efectivo solo después de que un monitor esté vinculado a los servicios. Las condiciones posibles son:
      - **ALWAYS**. Supervisar el servicio GSLB en todo momento.
      - **MEP Fails**. Supervisar el servicio GSLB solo cuando se produce un error en el intercambio de métricas a través de MEP.
      - **Error MEP y ID de servicio caído**. El intercambio de métricas a través de MEP está habilitado, pero el estado del servicio, actualizado a través del intercambio de métricas, es DOWN.

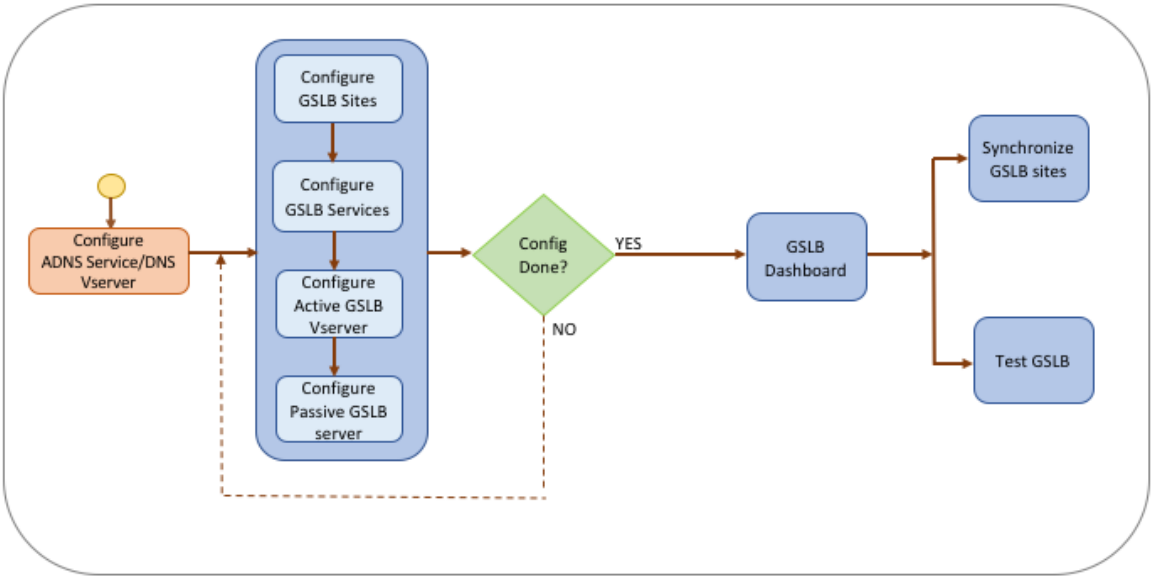
6. Configure los servicios GSLB. Para crear un sitio activo-activo, debe agregar al menos dos servicios GSLB.
   a) Introduzca los detalles del servicio, como el nombre del servicio, el tipo de servicio y el número de puerto.
   b) Asocie el servicio a un sitio (local o remoto) seleccionando el sitio GSLB al que pertenece el servicio GSLB.
   c) Seleccione el monitor que debe vincularse al servicio cuando MEP falla, si es necesario. El servicio puede ser un servidor existente o puede crear un nuevo servidor o un servidor virtual.
   d) Para asociar un servidor existente, seleccione el nombre del servidor. La dirección IP del servicio se rellena automáticamente.
      - Si la dirección IP pública es diferente de la IP del servidor, lo que puede ocurrir en un entorno NAT, introduzca la dirección IP pública y el número de puerto del puerto público.
      - Para asociar un nuevo servidor, cree un servidor introduciendo los detalles de IP del servidor y su dirección IP pública y el número de puerto público.
      - Para asociar un servidor virtual, seleccione un servidor virtual ya existente o haga clic en + y agregue un nuevo servidor virtual. Este servidor vserver es el servidor vserver de equilibrio de carga con el que se asociará este servicio GSLB.
7. Configure los servidores virtuales GSLB.
   a) Introduzca el nombre del servidor virtual GSLB y seleccione el tipo de registro DNS.
   b) Haga clic en **>** en el cuadro **Seleccionar servicio** y elija los servicios GSLB que se vincularán al servidor virtual GSLB.
   c) Haga clic en **>** en el cuadro **Enlace de dominio** para seleccionar el dominio que se enlazará a este servidor virtual GSLB.
   d) Elija el método GSLB para seleccionar el servicio GSLB de mejor rendimiento. Los valores predeterminados para el método GSLB, el método de copia de seguridad y el peso dinámico se rellenan automáticamente, de forma predeterminada. Puede cambiarlos si es necesario.
      - Si elige el método **basado en algoritmo**, seleccione los métodos principal y de copia de seguridad y especifique también la opción de peso dinámico.
      - Si elige el método de **proximidad estática**, seleccione el método de copia de seguridad y el método de peso dinámico. Además, proporcione la ubicación del archivo de base de datos haciendo clic en el icono > o agregue una nueva ubicación haciendo clic en **+** en el cuadro Seleccionar una base de datos de ubicación.
      - Si elige el método de **proximidad dinámica (RTT)**, seleccione el método de copia de seguridad y especifique la opción de peso dinámico y el valor de tiempo de ida y vuelta en función del cual debe seleccionarse el servicio de mejor rendimiento.
8. Haga clic en **Listo** si la configuración está completa. Aparecerá el panel de control GSLB.

9. Si ha modificado la configuración del sitio GSLB, haga clic en **Sincronizar automáticamente GSLB** en el panel para sincronizar la configuración con otros sitios de la configuración de GSLB.
   - Antes de la sincronización, asegúrese de que la configuración del sitio local incluye información sobre los sitios remotos. Además, para que la sincronización sea correcta, el sitio local debe configurarse en los demás dispositivos Citrix ADC.
   - Si la sincronización en tiempo real está habilitada, no es necesario que haga clic en **Sincronizar automáticamente GSLB**. La sincronización ocurre automáticamente. Para habilitar la sincronización en tiempo real, haga lo siguiente:
     a) Vaya a **Administración del tráfico** > **GSLB** > **Panel** y haga clic en **Cambiar configuración de GSLB**.
     b) Active la casilla de verificación **Sincronización automática de configuración**.
10. Haga clic en **Probar instalación de GSLB** para asegurarse de que los servicios ADNS o los servidores DNS están respondiendo con la dirección IP correcta para el nombre de dominio que está configurado en la instalación de GSLB.

Configurar sitio activo-pasivo

August 20, 2021

En la siguiente ilustración se muestra el flujo de trabajo implicado en la configuración del sitio activo-pasivo.



Antes de comenzar a configurar un sitio activo-pasivo, asegúrese de haber configurado una configuración de equilibrio de carga estándar para cada conjunto de servidores o centro de datos.

Además, para sincronizar la configuración de GSLB en los sitios de GSLB en la implementación, asegúrese de que:

- Los sitios GLSB locales se configuran en todos los dispositivos de la configuración GSLB.
- Ha habilitado el acceso de administración en todos los Sitios GSLB en la configuración.
- Ha configurado el firewall para aceptar la sincronización automática y las conexiones MEP.
- Los dispositivos Citrix ADC maestros y esclavos ejecutan las mismas versiones de software Citrix ADC.
- Todos los dispositivos Citrix ADC que participan como sitios deben tener la misma versión de software Citrix ADC (los sitios no están en una relación maestro-esclavo).
- La contraseña del nodo RPC es la misma en todos los sitios de GSLB en la configuración de GSLB.

Para configurar un sitio activo-pasivo mediante el asistente

En la ficha Configuración, haga lo siguiente:

1. Vaya a **Administración del tráfico** > **GSLB** y, a continuación, haga clic en **Introducción**.
2. Si no ha configurado un servicio ADNS o un servidor virtual DNS para el sitio, puede hacerlo ahora.
   a) Haga clic en **Ver** y, a continuación, haga clic en **Agregar**.
   b) Introduzca el nombre del servicio, la dirección IP y seleccione el protocolo (ADNS/ADNS_TCP) a través del cual se intercambian los datos con el servicio.
3. Seleccione **Sitio activo-pasivo**.
4. Introduzca el nombre de dominio completo y especifique el período de tiempo para el que los proxies DNS deben almacenar en caché el registro.
5. Configure los sitios GSLB. Cada sitio debe configurarse con un sitio GSLB local, y la configuración de cada sitio debe incluir todos los demás sitios como sitios GSLB remotos. Solo puede haber un sitio local y todos los demás sitios son sitios remotos.
   a) Introduzca los detalles del sitio, como el nombre del sitio y la dirección IP del sitio.
   b) Seleccione el tipo de sitio REMOTE o LOCAL.
   c) Opcionalmente, cambie la contraseña de RPC y, si es necesario, asegúrela.
   d) Si se va a vincular un monitor al servicio GSLB, seleccione la condición bajo la que el monitor va a supervisar el servicio. Esto será efectivo solo después de que un monitor esté vinculado a los servicios. Las condiciones posibles son:
      - **ALWAYS**. Supervisar el servicio GSLB en todo momento.
      - **MEP Fails**. Supervisar el servicio GSLB solo cuando se produce un error en el intercambio de métricas a través de MEP.
      - **Error MEP y ID de servicio caído**. El intercambio de métricas a través de MEP está habilitado, pero el estado del servicio, actualizado a través del intercambio de métricas, es DOWN.
6. Configure los servicios GSLB.

a) Introduzca los detalles del servicio, como el nombre del servicio, el tipo de servicio y el número de puerto.
b) Asocie el servicio a un sitio (local o remoto) seleccionando el sitio GSLB al que pertenece el servicio GSLB.
c) Seleccione el monitor que debe vincularse al servicio cuando MEP falla, si es necesario. El servicio puede ser un servidor existente o puede crear un nuevo servidor o un servidor virtual.
d) Para asociar un servidor existente, seleccione el nombre del servidor. La dirección IP del servicio se rellena automáticamente.
   - Si la dirección IP pública es diferente de la IP del servidor, lo que puede ocurrir en un entorno NAT, introduzca la dirección IP pública y el número de puerto del puerto público.
   - Para asociar un nuevo servidor, cree un servidor introduciendo los detalles de IP del servidor y su dirección IP pública y el número de puerto público.
   - Para asociar un servidor virtual, seleccione un servidor virtual ya existente o haga clic en **+** y agregue un nuevo servidor virtual. Este servidor vserver es el servidor vserver de equilibrio de carga con el que se asociará este servicio GSLB.

7. Configure los servidores virtuales de copia de seguridad de GSLB. Los servidores virtuales de copia de seguridad de GSLB solo funcionan cuando los servidores virtuales de GSLB primarios son inaccesibles o están marcados hacia abajo por cualquier motivo.
   a) Introduzca el nombre del servidor virtual GSLB y seleccione el tipo de registro DNS.
   b) Haga clic en **>** en **Enlace de servicios** y elija los servicios GSLB que deben estar enlazados al servidor virtual GSLB.
   c) Elija el método GSLB para seleccionar el servicio GSLB de mejor rendimiento. Los valores predeterminados para el método GSLB, el método de copia de seguridad y el peso dinámico se rellenan automáticamente, de forma predeterminada. Puede cambiarlos si es necesario.
      - Si elige el método **basado en algoritmo**, seleccione los métodos principal y de copia de seguridad.
      - Si elige el método de **proximidad estática**, seleccione el método de copia de seguridad y proporcione la ubicación del archivo de base de datos.
      - Si elige el método de **proximidad dinámica (RTT)**, seleccione el método de copia de seguridad y especifique el peso del servicio y el valor RTT en función del cual se seleccionará el servicio de mejor rendimiento.
8. Configure los servidores virtuales GSLB.
   a) Introduzca el nombre del servidor virtual GSLB y seleccione el tipo de registro DNS.
   b) Haga clic en **>** en el cuadro **Seleccionar servicio** y elija los servicios GSLB que se vincularán al servidor virtual GSLB.
   c) Haga clic en **>** en el cuadro **Enlace de dominio** para seleccionar el dominio que se enlazará

a este servidor virtual GSLB.

d) Elija el método GSLB para seleccionar el servicio GSLB de mejor rendimiento. Los valores predeterminados para el método GSLB, el método de copia de seguridad y el peso dinámico se rellenan automáticamente, de forma predeterminada. Puede cambiarlos si es necesario.

- Si elige el método **basado en algoritmo**, seleccione los métodos principal y de copia de seguridad y especifique también la opción de peso dinámico.
- Si elige el método de **proximidad estática**, seleccione el método de copia de seguridad y el método de peso dinámico. Además, proporcione la ubicación del archivo de base de datos haciendo clic en el icono **** o agregue una nueva ubicación haciendo clic en **+** en el cuadro Seleccionar una base de datos de ubicación.
- Si elige el método de **proximidad dinámica (RTT)**, seleccione el método de copia de seguridad y especifique la opción de peso dinámico y el valor de tiempo de ida y vuelta en función del cual debe seleccionarse el servicio de mejor rendimiento.

9. Haga clic en **Listo** si la configuración está completa. Aparecerá el panel de control GSLB.
10. Si ha modificado la configuración del sitio GSLB, haga clic en **Sincronizar automáticamente GSLB** en el panel para sincronizar la configuración con otros sitios de la configuración de GSLB.
    - Antes de la sincronización, asegúrese de que la configuración del sitio local incluye información sobre los sitios remotos. Además, para que la sincronización sea correcta, el sitio local debe configurarse en los demás dispositivos Citrix ADC.
    - Si la sincronización en tiempo real está habilitada, no es necesario que haga clic en **Sincronizar automáticamente GSLB**. La sincronización ocurre automáticamente. Para habilitar la sincronización en tiempo real, haga lo siguiente:
        a) Vaya a **Administración del tráfico** > **GSLB** > **Panel** y haga clic en **Cambiar configuración de GSLB**.
        b) Active la casilla de verificación **Sincronización automática de configuración**.
11. Haga clic en **Probar instalación de GSLB** para asegurarse de que los servicios ADNS o los servidores DNS están respondiendo con la dirección IP correcta para el nombre de dominio que está configurado en la instalación de GSLB.

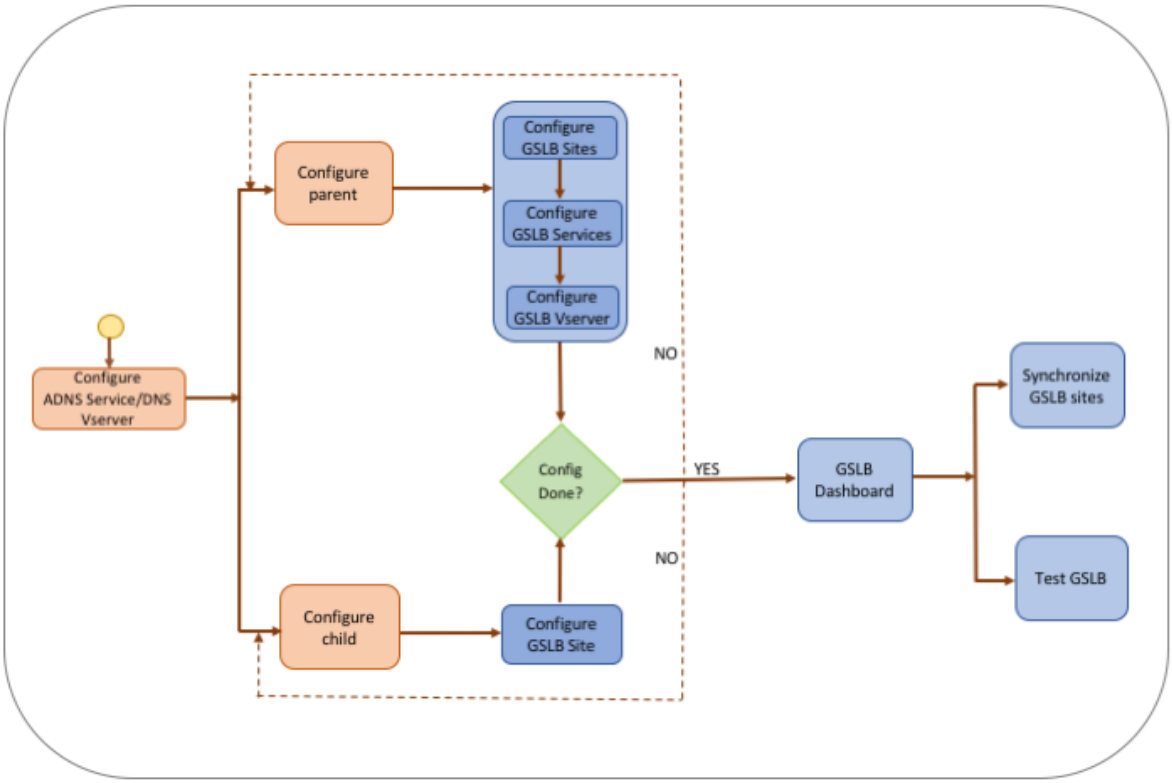
> **Nota**
>
> Para obtener más información sobre la configuración de entidades GSLB de una configuración GSLB pasiva activa para recuperación ante desastres, consulte Configuración de GSLB para recuperación ante desastres.

Configurar topología principal-secundario

February 16, 2021

En una topología principal-secundario, en el nivel superior se encuentran los sitios principales, que tienen relaciones de pares con otros sitios principales. Cada principal puede tener varios sitios secundarios y cada sitio primario intercambia información de estado con sus sitios secundarios y con otros sitios principales. Sin embargo, un sitio secundario solo se comunica con su sitio primario.

En la siguiente ilustración se muestra el flujo de trabajo implicado en una configuración de topología principal-secundario de GSLB.



Antes de comenzar a configurar la implementación de topología principal-secundario, asegúrese de haber configurado una configuración de equilibrio de carga estándar para cada conjunto de servidores o centro de datos.

Además, para sincronizar la configuración de GSLB en los sitios de GSLB en la implementación, asegúrese de que:

- Los sitios GLSB locales se configuran en todos los dispositivos de la configuración GSLB.
- Ha habilitado el acceso de administración en todos los Sitios GSLB en la configuración.
- Ha configurado el firewall para aceptar la sincronización automática y las conexiones MEP.
- Todos los dispositivos Citrix ADC que participan como sitios deben tener la misma versión de software Citrix ADC (los sitios no están en una relación maestro-esclavo).
- La contraseña del nodo RPC es la misma en todos los sitios de GSLB en la configuración de GSLB.

Para configurar una implementación principal-secundario mediante el asistente

En la ficha Configuración, haga lo siguiente:

1. Vaya a **Administración del tráfico** > **GSLB** y, a continuación, haga clic en **Introducción**.
2. Si no ha configurado un servidor ADNS o un servidor virtual DNS para el sitio, puede hacerlo ahora.
   a) Haga clic en **Ver** y, a continuación, haga clic en **Agregar**.
   b) Introduzca el nombre del servicio, la dirección IP y seleccione el protocolo (ADNS/ADNS_TCP) a través del cual se intercambian los datos con el servicio.
3. Seleccione **Topología Parent-Child**.
4. En el campo Seleccione el tipo de sitio, elija;
   - **Principal**: al configurar el sitio primario, debe configurar sus sitios secundarios asociados y también configurar los otros sitios principales en la configuración de GSLB.
   - **Secundario**: al configurar el sitio secundario, debe configurar solo el sitio secundario y su sitio primario.

Para configurar un sitio primario

1. Introduzca el nombre de dominio completo y especifique el período de tiempo para el que los proxies DNS deben almacenar en caché el registro.
2. Configure los sitios GSLB. Cada sitio debe configurarse con un sitio GSLB local, y la configuración de cada sitio debe incluir todos los demás sitios como sitios GSLB remotos. Solo puede haber un sitio local. Todos los demás sitios son sitios remotos. Si la dirección IP del sitio especificada es propiedad del dispositivo (por ejemplo, una dirección MIP o una dirección SNIP), el sitio es un sitio local. De lo contrario, es un sitio remoto.
3. Introduzca los detalles del sitio, como el nombre del sitio y la dirección IP del sitio.
   a) Seleccione el tipo de sitio.
   b) Opcionalmente, cambie la contraseña de RPC y, si es necesario, asegúrela.
   c) Si se va a vincular un monitor al servicio GSLB, seleccione la condición bajo la que el monitor va a supervisar el servicio. Esto será efectivo solo después de que un monitor esté vinculado a los servicios. Las condiciones posibles son:
      - **Always**. Supervisar el servicio GSLB en todo momento.
      - **MEP Fails**. Supervisar el servicio GSLB solo cuando se produce un error en el intercambio de métricas a través de MEP.
      - **El MEP falla y el servicio está DOWN**. El intercambio de métricas a través de MEP está habilitado, pero el estado del servicio, actualizado a través del intercambio de métricas, es DOWN.
4. Configure los servicios GSLB.
   a) Introduzca los detalles del servicio, como el nombre del servicio, el tipo de servicio y el número de puerto.

b) Asocie el servicio a un sitio (local o remoto) seleccionando el sitio GSLB al que pertenece el servicio GSLB.
c) Seleccione el monitor que debe vincularse al servicio cuando MEP falla, si es necesario. El servicio puede ser un servidor existente o puede crear un nuevo servidor o un servidor virtual.
   - Para asociar un servidor existente, seleccione el nombre del servidor. La dirección IP del servicio se rellena automáticamente.
   - Para asociar un nuevo servidor, cree un servidor introduciendo los detalles de IP del servidor y su dirección IP pública y el número de puerto público.
   - Para asociar un servidor virtual, seleccione un servidor virtual ya existente o haga clic en **+** y agregue un nuevo servidor virtual. Este servidor vserver es el servidor vserver de equilibrio de carga al que se asociará este servicio GSLB. Si la dirección IP pública es diferente de la IP del servidor, lo que puede ocurrir en un entorno NAT, introduzca la dirección IP pública y el número de puerto público.

5. Configure los servidores virtuales GSLB.
   a) Introduzca el nombre del servidor virtual GSLB y seleccione el tipo de registro DNS.
   b) Haga clic en **>** en el cuadro **Seleccionar servicio** y elija los servicios GSLB que se vincularán al servidor virtual GSLB.
   c) Haga clic en **>** en el cuadro **Enlace** de dominio para ver el nombre de dominio enlazado al servidor virtual GSLB.
   d) Elija el método GSLB para seleccionar el servicio GSLB de mejor rendimiento. Los valores predeterminados para el método GSLB, el método de copia de seguridad y el peso dinámico se rellenan automáticamente de forma predeterminada. Puede cambiarlos si es necesario.
      - Si elige el método **basado en algoritmo**, seleccione los métodos principal y de copia de seguridad y especifique también la opción de peso dinámico.
      - Si elige el método de **proximidad estática**, seleccione el método de copia de seguridad y el método de peso dinámico. Además, proporcione la ubicación del archivo de base de datos haciendo clic en el icono **** o agregue una nueva ubicación haciendo clic en **+** en el cuadro Seleccionar una base de datos de ubicación.
      - Si elige el método de **proximidad dinámica (RTT)**, seleccione el método de copia de seguridad y especifique el peso del servicio y el valor RTT en función del cual se seleccionará el servicio de mejor rendimiento.
6. Haga clic en **Listo** si la configuración está completa. Aparecerá el panel de control GSLB.
7. Si ha modificado la configuración del sitio principal de GSLB, haga clic en **Sincronizar automáticamente GSLB** para sincronizar la configuración con los otros sitios primarios de la configuración de GSLB. En una topología principal-secundario, se omite la sincronización de los sitios secundarios.
   - Antes de la sincronización, asegúrese de que la configuración del sitio local incluye infor-

mación sobre los sitios remotos.

- Si la sincronización en tiempo real está habilitada, no es necesario que haga clic en **Sincronizar automáticamente GSLB**. La sincronización ocurre automáticamente. Para habilitar la sincronización en tiempo real, haga lo siguiente:
  a) Vaya a **Administración del tráfico** > **GSLB** > **Panel** y haga clic en **Cambiar configuración de GSLB**.
  b) Active la casilla de verificación **Sincronización automática de configuración**.

8. Haga clic en **Probar instalación de GSLB** para asegurarse de que los servicios ADNS o los servidores DNS están respondiendo con la dirección IP correcta para el nombre de dominio que está configurado en la instalación de GSLB.

Para configurar un sitio secundario

1. Configure los sitios GSLB.
   a) Introduzca los detalles del sitio, como el nombre del sitio y la dirección IP del sitio.
   b) Seleccione el tipo de sitio.
   c) Opcionalmente, cambie la contraseña de RPC y, si es necesario, asegúrela. 4. Si un monitor está enlazado al servicio GSLB, seleccione la condición bajo la que el monitor debe supervisar el servicio. Las condiciones posibles son:
      - **Always**. Supervisar el servicio GSLB en todo momento.
      - **MEP Fails**. Supervisar el servicio GSLB solo cuando se produce un error en el intercambio de métricas a través de MEP.
      - **El MEP falla y el servicio está DOWN**. El intercambio de métricas a través de MEP está habilitado, pero el estado del servicio, actualizado a través del intercambio de métricas, es DOWN.
2. Haga clic en **Listo** si la configuración está completa. Aparecerá el panel de control GSLB.
3. Haga clic en **Probar instalación de GSLB** para asegurarse de que los servicios ADNS o los servidores DNS están respondiendo con la dirección IP correcta para el nombre de dominio que está configurado en la instalación de GSLB.

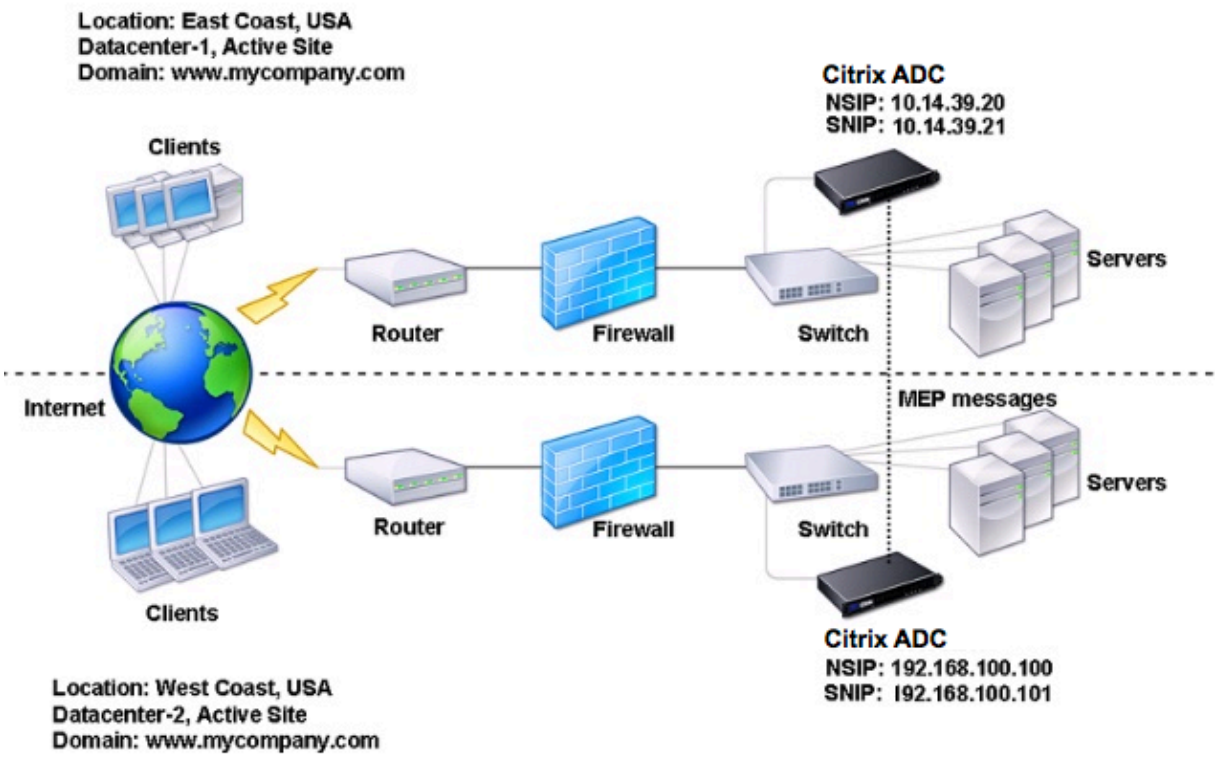
Configurar entidades GSLB individualmente

August 20, 2021

El equilibrio de carga del servidor global se utiliza para administrar el flujo de tráfico a un sitio web alojado en dos comunidades de servidores independientes que, idealmente, se encuentran en ubicaciones geográficas diferentes. Por ejemplo, considere un sitio web, www.mycompany.com, que está alojado en dos conjuntos de servidores o centros de datos separados geográficamente. Ambas

comunidades de servidores utilizan dispositivos Citrix ADC. Los dispositivos Citrix ADC de estas comunidades de servidores se configuran en modo de un brazo y funcionan como servidores DNS autorizados para el dominio www.mycompany.com. La siguiente ilustración ilustra esta configuración.

Ilustración 1. Topología básica de GSLB



Para configurar dicha configuración de GSLB, primero debe configurar una configuración de equilibrio de carga estándar para cada conjunto de servidores o centro de datos. Esto le permite equilibrar la carga entre los diferentes servidores de cada comunidad de servidores. A continuación, configure ambos dispositivos Citrix ADC como servidores DNS autorizados (ADNS). A continuación, cree un sitio GSLB para cada comunidad de servidores, configure los servidores virtuales GSLB para cada sitio, cree servicios GLSB y vincule los servicios GSLB a los servidores virtuales GSLB. Finalmente, vincule el dominio a los servidores virtuales GSLB. Las configuraciones de GSLB en los dos dispositivos en los dos sitios diferentes son idénticas, aunque las configuraciones de equilibrio de carga para cada sitio son específicas de ese sitio.

Nota: Para configurar un sitio GSLB en una configuración de clúster de Citrix ADC, consulte Configuración de GSLB en un clúster.

Configuración de una configuración de equilibrio de carga estándar

Un servidor virtual de equilibrio de carga equilibra la carga entre diferentes servidores físicos del centro de datos. Estos servidores se representan como servicios en el dispositivo Citrix ADC y los servicios están enlazados al servidor virtual de equilibrio de carga.

Para obtener más información sobre cómo configurar una configuración básica de equilibrio de cargas, consulte Equilibrio de carga.

Configurar un servicio DNS autorizado

August 20, 2021

Cuando configura el dispositivo Citrix ADC como un servidor DNS autorizado, acepta solicitudes DNS del cliente y responde con la dirección IP del centro de datos al que el cliente debe enviar solicitudes.

Nota: Para que el dispositivo Citrix ADC sea autoritario, también debe crear registros SOA y NS. Para obtener más información sobre los registros SOA y NS, consulte Sistema de nombres de dominio.

Para crear un servicio ADNS mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para crear un servicio ADNS y compruebe la configuración:

```
add service <name> <IP>@ ADNS <port>

show service <name>
<!--NeedCopy-->
```

Ejemplo:

```
add service Service-ADNS-1 10.14.39.21 ADNS 53

show service Service-ADNS-1
<!--NeedCopy-->
```

Para modificar un servicio ADNS mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba el siguiente comando:


```
set service <name> <IPAddress> ADNS <port>
<!--NeedCopy-->
```

Ejemplo:

```
set service Service-ADNS-1 10.14.39.21 ADNS 53
<!--NeedCopy-->
```

Para quitar un servicio ADNS mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba el siguiente comando:

```
rm service <name>
<!--NeedCopy-->
```

Ejemplo:

```
rm service Service-ADNS-1
<!--NeedCopy-->
```

Para configurar un servicio ADNS mediante la utilidad de configuración

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servicios**.
2. Agregue un nuevo servicio ADNS o seleccione un servicio existente y modifique su configuración.

Configurar un sitio GSLB básico

January 12, 2021

Un sitio GSLB es una representación de un centro de datos de la red y es una agrupación lógica de servidores virtuales GSLB, servicios y otras entidades de red. Normalmente, en una configuración de GSLB, hay muchos sitios GSLB que están equipados para servir el mismo contenido a un cliente. Estos suelen estar separados geográficamente para garantizar que el dominio esté activo incluso si un sitio

se desactiva por completo. Todos los sitios de la configuración de GSLB deben configurarse en todos los dispositivos Citrix ADC que alojan un sitio de GSLB. En otras palabras, en cada sitio, se configura el sitio GSLB local y cada sitio GSLB remoto.

Una vez creados los sitios GSLB para un dominio, el dispositivo Citrix ADC envía las solicitudes de cliente al sitio GSLB apropiado según lo determinado por los algoritmos GSLB configurados.

Para crear un sitio GSLB mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para crear un sitio GSLB y compruebe la configuración:

```
add gslb site <siteName> <siteIPAddress>
show gslb site <siteName>
<!--NeedCopy-->
```

Ejemplo:

```
add gslb site Site-GSLB-East-Coast 10.14.39.21
show glsb site Site-GSLB-East-Coast
<!--NeedCopy-->
```

Para modificar o quitar un sitio GSLB mediante la interfaz de línea de comandos

- Para modificar un sitio GSLB, utilice el comando set gslb site, que es igual que el comando add gslb site, excepto que escriba el nombre de un sitio GSLB existente.
- Para desestablecer un parámetro de sitio, utilice el comando unset gslb site, seguido del valor SiteName y el nombre del parámetro que se restablecerá a su valor predeterminado.
- Para eliminar un sitio GSLB, utilice el comando rm gslb site, que solo acepta el argumento <name>.

Para configurar un sitio GSLB básico mediante la utilidad de configuración

1. Desplácese hasta **Administración del tráfico** > **GSLB** > **Sitios**.
2. Agregue un nuevo sitio GSLB o seleccione un sitio GSLB existente y modifique su configuración.

Para ver las estadísticas de un sitio GSLB mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:


```
stat gslb site <siteName>
<!--NeedCopy-->
```

Ejemplo:

```
stat gslb site Site-GSLB-East-Coast
<!--NeedCopy-->
```

Para ver las estadísticas de un sitio GSLB mediante la utilidad de configuración

1. Desplácese hasta **Administración del tráfico** > **GSLB** > **Sitios**.
2. Seleccione el sitio GSLB y haga clic en **Estadísticas**.

Configurar un servicio GSLB

January 12, 2021

Un servicio GSLB es una representación de un servidor virtual de equilibrio de carga o conmutación de contenido. Un servicio GSLB local representa un servidor virtual de equilibrio de carga local o cambio de contenido. Un servicio GSLB remoto representa un servidor virtual de equilibrio de carga o conmutación de contenido configurado en uno de los otros sitios de la instalación de GSLB. En cada sitio de la configuración de GSLB, puede crear un servicio GSLB local y cualquier número de servicios GSLB remotos.

> **Importante**
>
> Si el servidor virtual de equilibrio de carga está en un nodo GSLB o está en un nodo secundario (en la implementación principal-secundario) y no hay monitores enlazados al servicio GSLB, asegúrese de que lo siguiente:
>
> La dirección IP del servicio GLSB, el número de puerto y el protocolo coinciden con la servidor virtual que representa el servicio. De lo contrario, el estado del servicio se marca como DOWN.

Para crear un servicio GSLB mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para crear un servicio GSLB y compruebe la configuración:


```
add gslb service <serviceName> <serverName | IP> <serviceType> <port>-
    siteName <string>
show gslb service <serviceName>
<!--NeedCopy-->
```

Ejemplo:

```
add gslb service Service-GSLB-1 10.14.39.14 HTTP 80  -siteName Site-
    GSLB-East-Coast
show gslb service Service-GSLB-1
<!--NeedCopy-->
```

Para modificar o quitar un servicio GSLB mediante la interfaz de línea de comandos

- Para modificar un servicio GSLB, utilice el comando set gslb service <serviceName>. Para este comando, especifique el nombre del servicio GSLB cuya configuración quiere modificar. Puede cambiar los valores existentes de los parámetros especificados por usted o definidos por defecto. Puede cambiar el valor de más de un parámetro en el mismo comando. Consulte el comando add gslb service para obtener detalles sobre los parámetros. Ejemplo

```
> set gslb service SKP_GSLB_NOTCNAME_SVC2 -maxBandWidth 25 -
    maxClient 8
Done
> sh gslb service SKP_GSLB_NOTCNAME_SVC2
SKP_GSLB_NOTCNAME_SVC2 (21.211.21.21: 80)- HTTP
...
Max Conn: 8  Max Bandwidth: 25 kbits
<!--NeedCopy-->
```

- Para restablecer un parámetro a su valor predeterminado, puede utilizar el comando unset gslb service <serviceName> y los parámetros que se van a desestablecer. Ejemplo

```
> unset gslb service SKP_GSLB_NOTCNAME_SVC2 maxBandWidth
Done
> sh gslb service SKP_GSLB_NOTCNAME_SVC2
SKP_GSLB_NOTCNAME_SVC2 (21.211.21.21: 80)- HTTP
...
Max Conn: 8  Max Bandwidth: 0 kbits
```



```
7   <!--NeedCopy-->
```

- Para quitar un servicio GSLB, utilice el comando rm gslb service <serviceName>.

Para crear un servicio GSLB mediante la utilidad de configuración

1. Vaya a **Administración de Tráfico** > **GSLB** > **Servicios**.
2. Agregue un nuevo servicio GSLB o seleccione un servicio existente y modifique su configuración.

Para ver las estadísticas de un servicio GSLB mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
1 stat gslb service <serviceName>
2 <!--NeedCopy-->
```

Ejemplo:

```
1 stat gslb service Service-GSLB-1
2 <!--NeedCopy-->
```

Para ver las estadísticas de un servicio GSLB mediante la utilidad de configuración

1. Vaya a **Administración de Tráfico** > **GSLB** > **Servicios**.
2. Seleccione el Servicio GSLB y haga clic en **Estadísticas**.

Configurar un grupo de servicios GSLB

March 9, 2022

El grupo de servicios le permite administrar un grupo de servicios con la misma facilidad que un solo servicio. Si habilita o inhabilita cualquier opción para un grupo de servicios, la opción se habilita o inhabilita para todos los miembros del grupo de servicios. Por ejemplo, puede aplicar esta función a opciones como Compresión, Supervisión del estado y apagado correcto.

Después de crear un grupo de servicios, puede realizar cualquiera de las siguientes acciones:

- Enlazar el grupo de servicios a un servidor virtual.

- Agregue servicios al grupo de servicios.
- Enlazar los monitores a los grupos de servicios.

> **Importante**
>
> Si el servidor virtual de equilibrio de carga está en un nodo GSLB o en un nodo secundario (en la implementación principal-secundario) y ningún monitor está enlazado al servicio GSLB, asegúrese de lo siguiente: La dirección IP,
>
> el número de puerto y el protocolo del grupo de servicios GLSB coinciden con el servidor virtual en el que está el servicio representando. De lo contrario, el estado del servicio se marca como DOWN.

Citrix ADC admite los siguientes tipos de grupos de servicios GSLB.

- Grupos de servicios basados en direcciones IP
- Grupos de servicios basados en nombres de dominio
- Grupos de servicios de escalabilidad automática basados en nombres de

Grupos de servicios de escala automática basados en nombres de dominio GSLB

La solución de equilibrio de carga de servidor global (GSLB) híbrido y multinube de Citrix ADC permite a los clientes distribuir el tráfico de aplicaciones en varios centros de datos en nubes híbridas, nubes múltiples y locales. La solución Citrix ADC GSLB admite varias soluciones de equilibrio de carga, como el equilibrador de carga Citrix ADC, Elastic Load Balancing (ELB) para AWS y otros equilibradores de carga de terceros. Además, la solución GSLB realiza el equilibrio de carga global incluso si las capas de equilibrio de carga y GSLB se administran de forma independiente.

En las implementaciones en la nube, los usuarios reciben un nombre de dominio como referencia cuando acceden a la solución de equilibrio de carga con fines de administración. Se recomienda que las entidades externas no utilicen las direcciones IP a las que se resuelven estos nombres de dominio. Además, las capas de equilibrio de carga se escalan hacia arriba o hacia abajo en función de la carga y no se garantiza que las direcciones IP sean estáticas. Por lo tanto, se recomienda utilizar el nombre de dominio para hacer referencia a los dispositivos de punto final de equilibrio de carga en lugar de a las direcciones IP. Esto requiere que se haga referencia a los servicios GSLB con el nombre de dominio en lugar de las direcciones IP y debe consumir todas las direcciones IP devueltas para el nombre de dominio de la capa de equilibrio de carga y tener una representación para el mismo en GSLB.

Para usar nombres de dominio en lugar de direcciones IP al hacer referencia a los dispositivos de punto final de equilibrio de carga, puede usar los grupos de servicios basados en nombres de dominio para GSLB.

Supervisar grupos de servicios basados en nombres de dominio GSLB

El dispositivo Citrix ADC tiene dos monitores integrados que monitorean las aplicaciones basadas en TCP; `tcp-default` y `ping-default`. El monitor `tcp-default` está vinculado a todos los servicios TCP y el monitor `ping-default` está vinculado a todos los servicios que no son TCP. Los monitores integrados están enlazados de forma predeterminada a los grupos de servicios GSLB. Sin embargo, se recomienda vincular un monitor específico de la aplicación a los grupos de servicios GSLB.

Recomendación para configurar la opción de monitores desencadenantes en MEPDOWN

La opción Monitores desencadenantes se puede utilizar para indicar si el sitio GSLB debe utilizar los monitores siempre, o utilizar monitores cuando el protocolo de intercambio de métricas (MEP) está DOWN.

La opción Monitores desencadenantes está establecida en SIEMPRE de forma predeterminada.

Cuando la opción Monitores desencadenantes está establecida en SIEMPRE, cada nodo GSLB activa los monitores de forma independiente. Si cada nodo GSLB activa los monitores de forma independiente, entonces cada nodo GSLB podría funcionar en un conjunto diferente de servicios GSLB. Esto puede provocar discrepancias en las respuestas de DNS para las solicitudes de DNS que llegan a estos nodos GSLB. Además, si cada nodo GSLB supervisa de forma independiente, aumenta el número de sondeos de monitorización que llegan a la entidad del equilibrador de carga. Las entradas de persistencia también se vuelven incompatibles en los nodos GSLB.

Por lo tanto, se recomienda que la opción Trigger Monitors en la entidad del sitio GSLB esté establecida en MEPDOWN. Cuando la opción Monitores desencadenantes está establecida en MEPDOWN, la resolución del dominio de equilibrio de carga y la propiedad de supervisión recae en el nodo GSLB local. Cuando la opción Trigger Monitors se establece en MEPDOWN, el nodo GSLB local de un grupo de servicios GSLB local de un grupo de servicios GSLB realiza la resolución del dominio de equilibrio de carga y la supervisión posterior. Los resultados se propagan a todos los demás nodos que participan en GSLB mediante el protocolo de intercambio de métricas (MEP).

Además, cada vez que se actualiza el conjunto de direcciones IP asociadas a un dominio de equilibrio de carga, se notifica a través de MEP.

Limitaciones de los grupos de servicios GSLB

- Para un dominio de equilibrio de carga, la dirección IP que se devuelve en la respuesta de DNS suele ser la dirección IP pública. La dirección IP privada no se puede aplicar de forma dinámica cuando se resuelve el dominio de equilibrio de carga. Por lo tanto, el puerto IP público y el puerto IP privado para los enlaces de puertos IP de los grupos de servicios de escalabilidad automática basados en nombres de dominio GSLB son los mismos. Estos parámetros no se

pueden establecer explícitamente para los grupos de servicios de escalabilidad automática basados en nombres de dominio.

- La persistencia del sitio, las vistas de DNS y la agrupación en clústeres no son compatibles con los grupos de servicios GSLB.

Configurar y administrar grupos de servicios GSLB mediante la CLI

Para agregar un grupo de servicios GSLB:

```
1 add gslb serviceGroup <serviceGroupName>@ <serviceType> [-autoScale (
     DISABLED | DNS )] -siteName <string>
2 <!--NeedCopy-->
```

Ejemplo:

```
1 add gslb serviceGroup Service-Group-1 http -autoScale DNS -siteName
     Site1
2 <!--NeedCopy-->
```

Para enlazar un grupo de servicios GSLB a un servidor virtual:

```
1 bind gslb serviceGroup <serviceGroupName> ((<IP>@ <port>) | <serverName
     >@ | (-monitorName <string>@))
2 <!--NeedCopy-->
```

Ejemplo:

```
1 bind gslb serviceGroup Service-Group-1 203.0.113.2
2 bind gslb serviceGroup Service-Group-1 S1 80
3 bind gslb serviceGroup** Service-Group-1 -monitorName Mon1
4 <!--NeedCopy-->
```

Para desvincular un grupo de servicios GSLB a un servidor virtual:

```
1 unbind gslb serviceGroup <serviceGroupName> ((<IP>@ <port>) | <
     serverName>@ | -monitorName <string>@)
2 <!--NeedCopy-->
```


Ejemplo:

```
unbind gslb serviceGroup Service-Group-1 -monitorName Mon1
<!--NeedCopy-->
```

Para establecer los parámetros de un grupo de servicios GSLB:

```
set gslb serviceGroup <serviceGroupName>@ [(<serverName>@ <port> [-
    weight <positive_integer>] [-hashId <positive_integer>] [-publicIP <
    ip_addr|ipv6_addr|*>] [-publicPort <port>]) | -maxClient <
    positive_integer> | -cip ( ENABLED | DISABLED ) | <cipHeader> | -
    cltTimeout <secs> | -svrTimeout <secs> | -maxBandwidth <
    positive_integer> | -monThreshold <positive_integer> | -
    downStateFlush ( ENABLED | DISABLED )] [-monitorName <string> -
    weight <positive_integer>] [-healthMonitor ( YES | NO )] [-comment <
    string>] [-appflowLog ( ENABLED | DISABLED )]
<!--NeedCopy-->
```

Para anular la configuración de los parámetros de un grupo de servicios GSLB:

```
unset gslb serviceGroup <serviceGroupName>@ [<serverName>@ <port> [-
    weight] [-hashId] [-publicIP] [-publicPort]] [-maxClient] [-cip] [-
    cltTimeout] [-svrTimeout] [-maxBandwidth] [-monThreshold] [-
    appflowLog] [-monitorName] [-weight] [-healthMonitor] [-cipHeader]
    [-downStateFlush] [-comment]
<!--NeedCopy-->
```

Para habilitar un grupo de servicios GSLB

```
enable gslb serviceGroup <serviceGroupName>@ [<serverName>@ <port>]
<!--NeedCopy-->
```

Ejemplo:

```
enable gslb serviceGroup SG1 S1 80
<!--NeedCopy-->
```

Para inhabilitar un grupo de servicios GSLB


```
disable gslb serviceGroup <serviceGroupName>@ [<serverName>@ <port>] [-
    delay <secs>] [-graceFul ( YES /| NO )]
<!--NeedCopy-->
```

Ejemplo:

```
disable gslb serviceGroup SRG2 S1 80
<!--NeedCopy-->
```

> **Nota:**
>
> El grupo de servicios que debe inhabilitarse debe ser un grupo de servicios de DBS y no un grupo de servicios de escalabilidad automática.

Para eliminar un grupo de servicios GSLB:

```
rm gslb serviceGroup <serviceGroupName>
<!--NeedCopy-->
```

Ejemplo:

```
rm gslb serviceGroup Service-Group-1
<!--NeedCopy-->
```

Para ver las estadísticas de un grupo de servicios GSLB:

```
stat gslb serviceGroup [<serviceGroupName>]
<!--NeedCopy-->
```

Ejemplo:

```
stat gslb serviceGroup Service-Group-1
<!--NeedCopy-->
```

Para ver las propiedades de un grupo de servicios GSLB:


```
show gslb serviceGroup [<serviceGroupName>  -includeMembers]
<!--NeedCopy-->
```

Ejemplo:

```
show gslb serviceGroup SG1
show gslb serviceGroup -includeMembers
<!--NeedCopy-->
```

Habilitar o inhabilitar miembros de grupos de servicios GSLB

Puede habilitar o inhabilitar selectivamente un miembro individual de un grupo de servicios GSLB (basado en DNS) en lugar de habilitar o inhabilitar todo el grupo de servicios. Esta función está disponible tanto en grupos de servicios de escalabilidad automática como en grupos de servicios sin escalabilidad automática. Por lo tanto, la administración de un grupo de servicios GSLB es más fácil.

Por ejemplo, tiene el requisito de evitar el tráfico a un servidor en particular en un sitio GSLB. Digamos que 10 servicios o servidores GSLB (S1 a S10) están enlazados a un grupo de servicios (SG1). Desea inhabilitar solo el servicio 5 (S5), es decir, evitar el tráfico al servidor 5. Sin esta función, debe vincular por separado los servicios S1 a S4 y los servicios S6 a S10. Este proceso se vuelve tedioso en un grupo de servicios GSLB grande en el que tiene que inhabilitar o habilitar una gran cantidad de servicios. Con esta función, puede inhabilitar directamente el servicio 5 (S5) sin afectar a otros servicios del grupo de servicios.

Para habilitar un miembro del grupo de servicios GSLB mediante la CLI:

```
enable gslb serviceGroup <serviceGroupName>@ [<serverName>@ <port>]
<!--NeedCopy-->
```

> **Nota:**
>
> Para habilitar un grupo de servicios GSLB, proporcione solo el nombre del grupo de servicios. Para habilitar a un miembro de un grupo de servicios, además del nombre del grupo de servicios GSLB, proporcione el nombre del servidor que aloja el servicio y el número de puerto del servicio.

Ejemplo:

```
enable gslb serviceGroup http_svc_group 10.102.27.153 80
<!--NeedCopy-->
```


Para inhabilitar un grupo de servicios GSLB o un miembro del grupo de servicios GSLB mediante la CLI:

```
disable gslb serviceGroup <serviceGroupName>@ [<serverName>@ <port>]
<!--NeedCopy-->
```

Ejemplo:

```
disable gslb serviceGroup http_svc_group 10.102.27.153 80
<!--NeedCopy-->
```

> **Nota:**
>
> Para inhabilitar un grupo de servicios GSLB, proporcione solo el nombre del grupo de servicios. Para inhabilitar a un miembro de un grupo de servicios, además del nombre del grupo de servicios GSLB, proporcione el nombre del servidor que aloja el servicio y el número de puerto del servicio.

Cambios en los comandos GSLB CLI existentes

Los siguientes son los cambios que se realizan en los comandos de GSLB existentes después de la introducción de los grupos de servicios de GSLB:

- `bind gslb vserver` - El nombre del grupo de servicios se agrega al comando bind.

  Ejemplo:

  ```
  bind gslb vserver <name> ((-serviceName <string> [-weight <
     positive_integer>] ) | <serviceGroupName>@ | | (-domainName <
     string> [-TTL <secs>] [-backupIP<ip_addr|ipv6_addr|*>] [-
     cookieDomain <string>] [-cookieTimeout <mins>][-sitedomainTTL
     <secs>]) | (-policyName <string>@ [-priority<positive_integer
     >] [-gotoPriorityExpression <expression>] [-type REQUEST |
     RESPONSE )]))
  <!--NeedCopy-->
  ```

- `unbind gslb vserver` - El grupo de servicios se agrega al comando unbind.

  Ejemplo:


```
unbind gslb vserver <name> (-serviceName <string> <
    serviceGroupName> @ /(-domainName <string> [-backupIP] [-
    cookieDomain]) | -policyName <string>@)
<!--NeedCopy-->
```

- `show gslb site` - Cuando se ejecuta este comando, también se muestran los grupos de servicios GSLB.
- `show gslb vs` - Cuando se ejecuta este comando, se muestran los grupos de servicios GSLB.
- `stat gslb vs` - Cuando se ejecuta este comando, también se muestran las estadísticas de los grupos de servicios GSLB.
- `show lb monitor bindings` - Cuando se ejecuta este comando, también se muestran los enlaces del grupo de servicios GSLB.

Configurar grupos de servicios GSLB mediante la interfaz gráfica de usuario

1. Vaya a **Gestión de tráfico** > **GSLB** > **Grupos de servicio**.
2. Cree un grupo de servicios y establezca el modo AutoScale en DNS.

Configurar la persistencia del sitio para los grupos de servicios GSLB

Puede configurar la persistencia del sitio para los grupos de servicios basados en direcciones IP y nombres de dominio. La persistencia del sitio no se admite para grupos de servicios de escalabilidad automática basados en nombres de dominio.

Para configurar la persistencia del sitio en función de las cookies HTTP mediante la CLI

- Para la persistencia del proxy de conexión, no tiene que establecer el prefijo del sitio.

  En el símbolo del sistema, escriba:

```
set gslb service group <serviceGroupName> [-sitePersistence <
    sitePersistence>]
<!--NeedCopy-->
```

- Para la persistencia de redirección HTTP, primero debe establecer el prefijo de sitio para un miembro del grupo de servicios y, a continuación, establecer el parámetro de persistencia `HTTPRedirect` para el grupo de servicios.

  En el símbolo del sistema, escriba:


```
set gslb servicegroup <serviceGroupName>  <serviceGroup member
   name|Ip> <port>  [-sitePrefix <string>]

set gslb servicegroup <serviceGroupName> [-sitePersistence <
   sitePersistence>]
<!--NeedCopy-->
```

Ejemplos:

- Persistencia del proxy de conexión

```
set gslbservicegroup sg1 -sitePersistence connectionProxy
<!--NeedCopy-->
```

- Persistencia de redirección HTTP

```
set gslb servicegroup sg2 test1 80 -sitePrefix vserver-GSLB-1

set gslb servicegroup sg2 -sitePersistence HTTPRedirect
<!--NeedCopy-->
```

Para establecer la persistencia del sitio basado en cookies mediante el uso de la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico** > **GSLB** > **Grupos de servicios** y seleccione el grupo de servicios que quiere configurar para la persistencia del sitio (por ejemplo, ServiceGroup-GSLB-1).
2. Haga clic en la sección **Persistencia del sitio** y establezca la persistencia que cumpla con sus requisitos.

> **Sugerencia**
>
> Para ver el escenario de implementación y la configuración de ejemplo de los grupos de servicios GSLB, consulte los siguientes temas:
>
> - Caso de uso: implementación del grupo de servicios de escalabilidad automática basada en nombres de dominio
> - Caso de uso: implementación del grupo de servicios de escalabilidad automática basada en direcciones IP

Configurar un servidor virtual GSLB

January 12, 2021

Un servidor virtual GSLB es una entidad que representa uno o más servicios GSLB y equilibra el tráfico entre ellos. Evalúa los métodos o algoritmos GSLB configurados para seleccionar un servicio GSLB al que enviar la solicitud del cliente.

> **Nota**
>
> Un requisito de protocolo de servidor virtual GSLB consiste principalmente en crear una relación entre el servidor virtual y los servicios que están vinculados al servidor virtual. Esto también mantiene la consistencia de CLI/API para otros tipos de servidores virtuales. El parámetro Tipo de servicio en un servicio o un servidor virtual no se utiliza al servir las solicitudes DNS. En su lugar, se hace referencia durante la persistencia del sitio, el supervisión y para hacer búsquedas a través de MEP.

Para crear un servidor virtual GSLB mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para agregar un servidor virtual GSLB y verificar la configuración:

```
1 -  add gslb vserver <name> <serviceType> -ipType (IPv4 | IPv6)
2 -  show gslb vserver <name>
3 <!--NeedCopy-->
```

Ejemplo:

```
1 add gslb vserver Vserver-GSLB-1 HTTP -ipType IPv4
2 add gslb vserver Vserver-GSLB-2 HTTP -ipType IPv6
3 show gslb vserver Vserver-GSLB-1
4 show gslb vserver Vserver-GSLB-2
5 <!--NeedCopy-->
```

Para modificar o quitar un servidor virtual GSLB mediante la interfaz de línea de comandos

- Para modificar un servidor virtual GSLB, utilice el comando `set gslb vserver`. Este comando funciona de forma similar al comando `add gslb vserver`, excepto que se escribe el nombre de un servidor virtual GSLB existente.

- Para restablecer un parámetro a su valor predeterminado, puede utilizar el comando `unset gslb vserver` seguido del valor VServerName y el nombre del parámetro que se va a desestablecer.
- Para quitar un servidor virtual GSLB, utilice el comando `rm gslb vserver`, que acepta solo el argumento name.

Para configurar un servidor virtual GSLB mediante la utilidad de configuración

1. Vaya a **Administración del tráfico** > **GSLB** > **Servidores virtuales**.
2. Agregue un nuevo servidor virtual GSLB o seleccione un servidor virtual GSLB existente y modifique su configuración.

Para ver las estadísticas de un servidor virtual GSLB mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
stat gslb vserver <name>
<!--NeedCopy-->
```

Ejemplo:

```
stat gslb vserver Vserver-GSLB-1
<!--NeedCopy-->
```

Para ver las estadísticas de un servidor virtual GSLB mediante la utilidad de configuración

Vaya a **Administración del tráfico** > **GSLB** > **Servidores virtuales**, seleccione el servidor virtual y haga clic en **Estadísticas**.

Estadísticas del servidor virtual GSLB

A partir de Citrix ADC versión 12.1 build 51.xx y versiones posteriores, las estadísticas del servidor virtual GSLB también muestran la siguiente información además de detalles como; hits de vserver, sesión de persistencia actual, bytes de solicitud, bytes de respuesta, umbral de desbordamiento, hits de desbordamiento, cliente actual establecido conexiones y vserver abajo visitas de copia de seguridad.

- **Fallos del método LB primario**: Número de veces que el método GSLB principal ha fallado.
- **Errores del método LB de copia**de seguridad: Número de veces que el método GSLB de copia de seguridad ha fallado.

- **Conciertos de persistencia de servidor virtual**: El número de veces que se sirve la solicitud a través de las sesiones de persistencia.

Las estadísticas del servidor virtual GSLB también muestran las estadísticas de los miembros del grupo de servicios vinculados al servidor virtual.

> **Nota:**
> El método primario o de copia de seguridad puede fallar cuando el método primario es proximidad estática y el método de copia de seguridad es RTT. En este caso, si no hay ninguna ubicación correspondiente a LDNS IP, la proximidad estática falla y se intenta el método de copia de seguridad. Las estadísticas se actualizan sobre la base de lo siguiente:
>
> - Si el método de copia de seguridad es correcto, solo se incrementan las estadísticas de error del método principal.
> - Si el cálculo RTT no es correcto, entonces el método de copia de seguridad también falla. En este caso, se incrementan las estadísticas de error del método primario y de copia de seguridad.
>
> Cuando el método de copia de seguridad falla, se utiliza el método de último recurso de round robin.

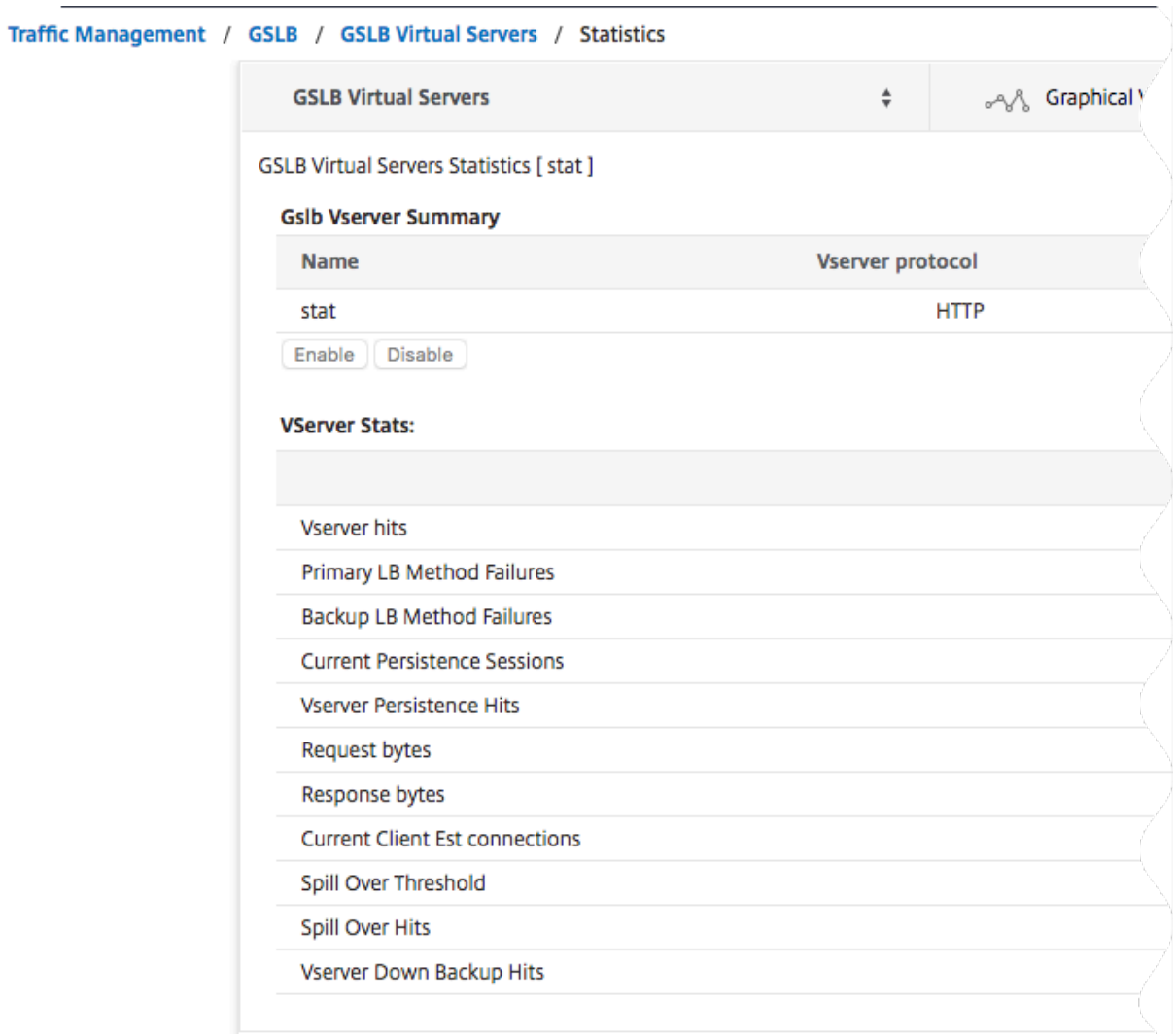
La siguiente imagen es un ejemplo de las estadísticas del servidor virtual GSLB de CLI.

```
Gslb Vserver Summary
                Protocol        State   Health  actSvcs inactSvc
gslbvip             HTTP         DOWN        0        0        0

VServer Stats:
                                        Rate (/s)               Total
Vserver hits                                 0                      0
Primary LB Method Failures                  --                      0
Backup LB Method Failures                   --                      0
Current Persistence Sessions                --                      0
Vserver Persistence Hits                    --                      0
Request bytes                                0                      0
Response bytes                               0                      0
Current Client Est connections              --                      0
Spill Over Threshold                        --                      0
Spill Over Hits                             --                      0
Vserver Down Backup Hits                    --                      0

Note: The above counters are the sum of all bound GSLB services
 Done
```

La siguiente imagen es un ejemplo de las estadísticas del servidor virtual GSLB de GUI.



Estadísticas de servicios GSLB

Cuando ejecuta el comando stat gslb service desde la línea de comandos o haga clic en el **enlace Estadísticas** de la utilidad de configuración, se muestran los siguientes detalles del servicio:

- **Bytes de solicitud.** Número total de bytes de solicitud recibidos en este servicio o servidor virtual.
- **Bytes de respuesta.** Número de bytes de respuesta recibidos por este servicio o servidor virtual.
- **Conexiones establecidas por el cliente actual.** Número de conexiones de cliente en estado ESTABLECIDO.
- **Carga actual en el servicio.** Carga en el servicio (calculada a partir del monitor de carga vinculado al servicio).

Es posible que no se muestren los datos del número de solicitudes y respuestas, así como el número

de conexiones actuales de cliente y servidor o que no se sincronicen con los datos del servidor virtual de equilibrio de carga correspondiente.

Borrar las estadísticas del servidor virtual o del servicio GSLB

Nota: Esta función está disponible en NetScaler versión 10.5.e.

Ahora puede borrar las estadísticas de un servidor virtual y servicio GSLB. Citrix ADC proporciona las dos opciones siguientes para borrar las estadísticas:

- **Básico**: Borra las estadísticas específicas del servidor virtual pero conserva las estadísticas aportadas por el servicio GLSB enlazado.
- **Completo**: Borra tanto el servidor virtual como las estadísticas del servicio GSLB enlazadas.

Para borrar las estadísticas de un servidor virtual GSLB mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
stat gslb vserver <name> -clearstats <basic | full>
<!--NeedCopy-->
```

Ejemplo:

```
stat gslb vserver Vserver-GSLB-1  - clearstats basic
<!--NeedCopy-->
```

Para borrar las estadísticas de un servicio GSLB mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
stat gslb service <name> -clearstats <basic | full>
<!--NeedCopy-->
```

Ejemplo:

```
stat gslb service service-GSLB-1  - clearstats basic
<!--NeedCopy-->
```


Para borrar las estadísticas de un servidor virtual GSLB mediante la utilidad de configuración

1. Vaya a **Administración del tráfico** > **GSLB** > **Servidores virtuales**.
2. Seleccione el servidor virtual GSLB y, a continuación, haga clic en **Estadísticas** y, a continuación, haga clic en **Borrar**.
3. En la lista desplegable **Borrar**, seleccione **Básico** o **Completo** y, a continuación, haga clic en **Aceptar**.

Para borrar las estadísticas de un servicio GSLB mediante la utilidad de configuración

1. Vaya a **Administración de Tráfico** > **GSLB** > **Servicios**.
2. Seleccione el servicio GSLB y, a continuación, haga clic en **Estadísticas** y, a continuación, haga clic en **Borrar**.
3. En la lista desplegable **Borrar**, seleccione **Básico** o **Completo** y, a continuación, haga clic en **Aceptar**.

Habilitación y desactivación de servidores virtuales GSLB

Cuando se crea un servidor virtual GSLB, se habilita de forma predeterminada. Si inhabilita el servidor virtual GSLB, al recibir una solicitud DNS, el dispositivo Citrix ADC no toma ninguna decisión GSLB basada en el método GSLB configurado. En su lugar, la respuesta a la consulta DNS contiene las direcciones IP de todos los servicios vinculados al servidor virtual.

Para habilitar o inhabilitar un servidor virtual GSLB mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba uno de los siguientes comandos:

```
enable gslb vserver <name>@

disable gslb vserver <name>@
<!--NeedCopy-->
```

Ejemplo:

```
enable gslb vserver Vserver-GSLB-1
disable gslb vserver Vserver-GSLB-1
<!--NeedCopy-->
```


Para habilitar o inhabilitar un servidor virtual GSLB mediante la utilidad de configuración

1. Vaya a **Administración del tráfico** > **GSLB** > **Servidores virtuales**.
2. Seleccione un servidor virtual y, en la lista **Acción**, seleccione **Activar** o **desactivar**.

Vincular servicios GSLB a un servidor virtual GSLB

January 12, 2021

Una vez configurados los servicios GSLB y el servidor virtual, los servicios GSLB pertinentes deben vincularse al servidor virtual GSLB para activar la configuración.

Para enlazar un servicio GSLB a un servidor virtual GSLB mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para enlazar un servicio GSLB a un servidor virtual GSLB y compruebe la configuración:

```
bind gslb vserver <name> -serviceName <string>

show gslb vserver <name>
<!--NeedCopy-->
```

Ejemplo:

```
bind gslb vserver Vserver-GSLB-1 -serviceName Service-GSLB-1
show gslb vserver Vserver-GSLB-1
<!--NeedCopy-->
```

Para desenlazar un servicio GSLB de un servidor virtual GSLB mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
unbind gslb vserver <name> -serviceName <string>
<!--NeedCopy-->
```


Para enlazar servicios GSLB mediante la utilidad de configuración

1. Vaya a **Administración del tráfico** > **GSLB** > **Servidores virtuales** y haga doble clic en un servidor virtual.
2. Haga clic en la sección **Dominios**, configure un dominio y vincule el dominio.

Enlazar un dominio a un servidor virtual GSLB

August 20, 2021

Para que un dispositivo Citrix ADC sea el servidor DNS autorizado de un dominio, debe enlazar el dominio al servidor virtual GSLB. Cuando vincula un dominio a un servidor virtual GSLB, el dispositivo Citrix ADC agrega un registro de direcciones para el dominio, que contiene el nombre del servidor virtual GSLB. Los registros de inicio de autoridad (SOA) y servidor de nombres (NS) para el dominio GSLB deben agregarse manualmente.

Para obtener información detallada sobre la configuración de registros SOA y NS, consulte Sistema de nombres de dominio.

Para enlazar un dominio a un servidor virtual GSLB mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para enlazar un dominio a un servidor virtual GSLB y compruebe la configuración:

```
bind gslb vserver <name> -domainName <string>
show gslb vserver <name>
<!--NeedCopy-->
```

Ejemplo:

```
bind gslb vserver Vserver-GSLB-1 -domainName www.mycompany.com
show gslb vserver Vserver-GSLB-1
<!--NeedCopy-->
```

Para desenlazar un dominio GSLB de un servidor virtual GSLB mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:


```
unbind gslb vserver <name> -domainName <string>
<!--NeedCopy-->
```

Para enlazar un dominio a un servidor virtual GSLB mediante la utilidad de configuración

1. Vaya a **Administración del tráfico** > **GSLB** > **Servidores virtuales**.
2. En el panel Servidores virtuales GSLB, seleccione el servidor virtual GSLB al que quiere enlazar el dominio (por ejemplo, VServer-GSLB-1) y haga clic en Abrir.
3. En el cuadro de diálogo Configurar servidor virtual GSLB, en la ficha Dominios, realice una de las acciones siguientes:
   - Para crear un nuevo dominio, haga clic en **Agregar**.
   - Para modificar un dominio existente, seleccione el dominio y, a continuación, haga clic en **Abrir**.
4. En el cuadro de diálogo Crear dominio GSLB o Configurar dominio GSLB, especifique valores para los siguientes parámetros como se muestra:
   - Nombre de dominio*: NombreDeDominio (por ejemplo, www.miempresa.com)

   *Un parámetro requerido
5. Haga clic en Crear.
6. Haga clic en Aceptar.

Para ver las estadísticas de un dominio mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
stat gslb domain <name>
<!--NeedCopy-->
```

Ejemplo:

```
stat gslb domain www.mycompany.com
<!--NeedCopy-->
```


Nota: Para ver las estadísticas de un dominio GSLB determinado, introduzca el nombre del dominio exactamente como se agregó al dispositivo Citrix ADC. Si no especifica el nombre de dominio, o si especifica un nombre de dominio incorrecto, se muestran las estadísticas de todos los dominios GSLB configurados.

Para ver las estadísticas de un dominio mediante la utilidad de configuración

1. Vaya a **Administración del tráfico** > **GSLB** > **Servidores virtuales**.
2. En el panel Servidores virtuales GSLB, seleccione el Servidor virtual GSLB (por ejemplo, VServer-GSLB-1) y haga clic en Abrir.
3. En el cuadro de diálogo Configurar servidor virtual GSLB, en la ficha Dominios, seleccione el dominio y, a continuación, haga clic en **Estadísticas**.

Para ver los detalles de configuración de las entidades enlazadas a un dominio GSLB mediante la línea de comandos

Nota: Esta función está disponible en NetScaler versión 10.5.e.

En el símbolo del sistema, escriba:

```
show gslb domain <name>
<!--NeedCopy-->
```

Ejemplo:

```
show gslb domain gslb1.com
       gslb1.com
       gvs1 - HTTP    state: DOWN
       DNS Record Type: A
       Configured Method: LEASTCONNECTION
       Backup Method: ROUNDROBIN
       Persistence Type: NONE
       Empty Down Response: DISABLED
       Multi IP Response: DISABLED
       Dynamic Weights: DISABLED

       gsvc1 (10.102.239.165: 80)- HTTP State: DOWN    Weight: 1
              Dynamic Weight: 0    Cumulative Weight: 1
              Effective State: DOWN
              Threshold : BELOW

```



```
17                Monitor Name : http
18                       State: DOWN   Weight: 1
19                       Probes: 144   Failed [Total: 144 Current: 144]
20                       Last response: Failure - TCP syn sent, reset
                            received.
21                       Response Time: 2000 millisec
22
23          gsvc2 (10.102.239.179: 80)- HTTP State: DOWN    Weight: 1
24                 Dynamic Weight: 0    Cumulative Weight: 1
25                 Effective State: DOWN
26                 Threshold : BELOW
27
28                 Monitor Name : http-ecv
29                       State: DOWN   Weight: 1
30                       Probes: 141   Failed [Total: 141 Current: 141]
31                       Last response: Failure - TCP syn sent, reset
                            received.
32                       Response Time: 2000 millisec
33  Done
34  <!--NeedCopy-->
```

Para ver los detalles de configuración de las entidades enlazadas a un dominio GSLB mediante la utilidad de configuración

Nota: Esta función está disponible en NetScaler versión 10.5.e.

1. Vaya a **Administración del tráfico** > **GSLB** > **Servidores virtuales** y haga doble clic en un servidor virtual.
2. Haga clic en el campo situado debajo del panel **Dominios**.
3. En el cuadro de diálogo **Enlace de dominio de servidor virtual GSLB**, seleccione un dominio y, a continuación, haga clic en **Mostrar enlaces**.

Ejemplo de configuración y configuración de GSLB

January 12, 2021

Una organización tiene una red geográficamente dispersa y cuenta con tres centros de datos ubicados en Estados Unidos, México y Colombia. En la configuración relacionada con estas ubicaciones, estas se denominan US, MX y CO respectivamente. En cada ubicación, la empresa tiene una comunidad de servidores, que proporciona el mismo contenido y la configuración funciona como se esperaba. El

dispositivo Citrix ADC en cada ubicación se configura a través de un servidor virtual con el protocolo HTTP en el puerto 80.

La organización ha implementado la configuración de GSLB agregando un identificador de sitio en cada sitio. El identificador del sitio incluye un nombre de sitio y una dirección IP propiedad del dispositivo Citrix ADC y se utiliza para las comunicaciones GSLB.
Cada sitio tiene un sitio local para el dispositivo. Además, cada sitio tiene dos sitios remotos al dispositivo local. En cada sitio, se crea un servidor virtual GSLB con el mismo nombre. Este servidor virtual identifica el sitio web de la organización globalmente y no tiene ninguna dirección IP asociada a él.
La instalación también tiene servicios GSLB configurados que apuntan a los servidores virtuales de equilibrio de carga configurados en cada sitio GSLB especificando la dirección IP, el protocolo y el número de puerto del servidor virtual respectivo. Estos servicios están enlazados al servidor virtual GSLB.

Nota: En el procedimiento siguiente, los comandos utilizan direcciones IP privadas para los sitios GSLB. Para sitios públicos y servicios GSLB, asegúrese de utilizar direcciones IP públicas para estos sitios.

En la siguiente tabla se enumeran las direcciones IP y las ubicaciones utilizadas en el ejemplo:

Dirección IP	Ubicación
10.3.1.101	IP del sitio del dispositivo Citrix ADC local.
172.16.1.101	Sitio IP de ubicación remota Site-MX.
192.168.1.101	Sitio IP de ubicación remota Site-Co.
172.16.1.100	IP de servicio de ubicación remota Site-MX.
10.3.1.100	IP de servicio de Citrix ADC local.
192.168.1.100	IP de servicio de ubicación remota Site-Co.

Al agregar un sitio GSLB, si el sitio solo se comunica a través de Internet, utilice el campo “IP pública”. Por ejemplo, cuando no hay conectividad VPN de sitio a sitio entre los sitios GSLB.

Para configurar la configuración de GSLB con dispositivos Citrix ADC mediante los comandos de CLI

1. Habilite la función GSLB, si aún no lo ha hecho.

```
enable ns feature gslb
<!--NeedCopy-->
```


2. Identificar un SNIP que para agregar sitio GSLB local.
3. Agregue el sitio GSLB para el dispositivo Citrix ADC local.

```
add gslb site site-US 10.3.1.101
<!--NeedCopy-->
```

4. Agregue los sitios GSLB para los dispositivos Citrix ADC remotos.

```
add gslb site site-MX 172.16.1.101
add gslb site site-CO 192.168.1.101
<!--NeedCopy-->
```

5. Agregue el servidor virtual GSLB que hace referencia a un servicio que se está usando en la configuración de GSLB:

```
add gslb vserver gslb-lb HTTP
<!--NeedCopy-->
```

6. Agregue los servicios de GSLB para cada sitio que participe en la configuración de GSLB:

```
add gslb service gslb_SVC30 172.16.1.100 HTTP 80 -siteName site-MX
add gslb service gslb_SVC10 10.3.1.100 HTTP 80 -siteName site-US
add gslb service gslb_SVC20 192.168.1.100 HTTP 80 -siteName site-
   CO
<!--NeedCopy-->
```

7. Enlazar los servicios de GSLB al servidor virtual de GSLB:

```
bind gslb vserver gslb-lb -serviceName gslb_SVC10
bind gslb vserver gslb-lb -serviceName gslb_SVC20
bind gslb vserver gslb-lb -serviceName gslb_SVC30
<!--NeedCopy-->
```

8. Enlazar el dominio al servidor virtual GSLB.


```
bind gslb vserver gslb-lb -domainName www.mycompany.com -TTL 30
<!--NeedCopy-->
```

9. Agregue un servicio ADNS que escuche las consultas DNS.

```
set service Service-ADNS-1 10.14.39.21 ADNS 53
<!--NeedCopy-->
```

Sincronizar la configuración en una configuración de GSLB

August 20, 2021

Normalmente, una configuración de GSLB tiene unos pocos centros de datos con un sitio GSLB configurado para cada centro de datos. En cada Citrix ADC, participando en GSLB, configure un sitio de GSLB como sitio local y los demás como sitios remotos. Cuando agrega otro sitio GSLB en un punto posterior, debe asegurarse de que la configuración en todos los sitios GSLB es idéntica. Puede utilizar la opción de sincronización de configuración GSLB de Citrix ADC para sincronizar la configuración en los sitios GSLB.

El dispositivo Citrix ADC desde el que utiliza la opción de sincronización se denomina “sitio principal” y sitios GSLB en los que se copia la configuración como “sitios subordinados”. Cuando sincroniza una configuración GSLB, las configuraciones de todos los sitios GSLB que participan en la configuración de GSLB se hacen similares a la configuración del sitio principal.

La sincronización se realiza solo en los sitios principales. La sincronización no afecta a la configuración de los sitios secundarios de GSLB. Esto se debe a que las configuraciones del sitio primario y del sitio secundario no son idénticas. La configuración de sitios secundarios se compone únicamente de los detalles propios y de su sitio principal. Además, no siempre se requiere que los servicios GSLB se configuren en los sitios secundarios.

- El nodo principal encuentra las diferencias entre la configuración del nodo principal y el nodo subordinado y cambia la configuración del nodo subordinado para hacerlo similar al nodo principal.

  Si forzas una sincronización (usa la opción “forzar sincronización”), el dispositivo elimina la configuración GSLB del nodo subordinado y, a continuación, configura al subordinado para que sea similar al nodo principal.

- Durante la sincronización, si falla un comando, la sincronización no se cancela y el mensaje de error se registra en un **archivo.err** del directorio **/var/netscaler/gslb**.

- La sincronización se realiza solo en los sitios principales. La sincronización no afecta a la configuración de los sitios secundarios de GSLB. Esto se debe a que las configuraciones del sitio primario y del sitio secundario no son idénticas. La configuración de sitios secundarios se compone únicamente de los detalles propios y de su sitio principal. Además, no siempre se requiere que los servicios GSLB se configuren en los sitios secundarios.
- Si inhabilita el inicio de sesión interno del usuario, la sincronización automática de GSLB utiliza las claves SSH para sincronizar la configuración. Sin embargo, para utilizar la sincronización automática de GSLB en el entorno de particiones, debe habilitar el inicio de sesión interno del usuario y asegurarse de que el nombre de usuario de la partición en los sitios GSLB locales y remotos sea el mismo.

> **Nota**
>
> - En el nodo RPC del sitio GSLB remoto, configure el firewall para que acepte conexiones de sincronización automática especificando la IP del sitio remoto (dirección IP del clúster para la configuración del clúster) y el puerto (3010 para RPC y 3008 para RPC seguro). Si la ruta predeterminada para llegar a los sitios remotos se encuentra en la subred de administración, como en la mayoría de los casos, NSIP se utiliza como dirección IP de origen.
>
> Para configurar una dirección IP de origen diferente, debe tener la dirección IP del sitio GSLB y el SNIP en una subred diferente. Además, debe tener definida una ruta explícita para la dirección IP del sitio remoto a través de una subred IP de sitio GSLB.
>
> Para mejorar la seguridad, Citrix recomienda cambiar la cuenta de usuario interna y las contraseñas de nodo RPC. La contraseña de la cuenta de usuario interna se cambia a través de la contraseña del nodo RPC. Para obtener más información, consulte Cambiar la contraseña de un nodo RPC.

Si utiliza la opción saveconfig, los sitios que participan en el proceso de sincronización guardan automáticamente su configuración, de la siguiente manera:

En el nodo RPC del sitio GSLB remoto, configure el firewall para que acepte conexiones de sincronización automática especificando la IP del sitio remoto (dirección IP del clúster para la configuración del clúster) y el puerto (3010 para RPC y 3008 para RPC seguro). Si la ruta predeterminada para llegar a los sitios remotos se encuentra en una subred de administración, como en la mayoría de los casos, NSIP se utiliza como dirección IP de origen.

Para configurar una dirección IP de origen diferente, debe tener la dirección IP del sitio GSLB y el SNIP en una subred diferente. Además, debe tener una ruta explícita definida para la dirección IP del sitio remoto a través de la subred IP del sitio GSLB. La dirección IP de origen no se puede sincronizar entre los sitios que participan en GSLB porque la dirección IP de origen de un nodo RPC es específica de cada dispositivo Citrix ADC. Por lo tanto, después de forzar una sincronización (mediante el comando sync gslb config -ForceSync o seleccionando la opción ForceSync en la GUI), debe cambiar manualmente las direcciones IP de origen en los demás dispositivos Citrix ADC. El puerto 22 también es necesario

para sincronizar los archivos de base de datos con el sitio remoto.

Para mejorar el tiempo que lleva la sincronización de la configuración en todos los sitios GSLB

Configure la configuración del perfil TCP en el símbolo del sistema de la siguiente manera:

```
set tcpprofile nstcp_internal_apps -bufferSize 4194304 -sendBuffsize
    4194304 -tcpmode ENDPOINT
<!--NeedCopy-->
```

Limitaciones de sincronización

- En el sitio principal, los nombres de los sitios GSLB remotos deben ser idénticos a los nombres de los sitios configurados en los dispositivos Citrix ADC que alojan esos sitios.
- Durante la sincronización, pueden producirse interrupciones del tráfico.
- Citrix ADC se ha probado para sincronizar hasta 200.000 líneas de la configuración.
- La sincronización puede fallar:
  - Si el método de derrame se cambia de CONNECTION a DYNAMIC CONNECTION.
  - Si intercambia el prefijo de sitio de los servicios GSLB enlazados a un servidor virtual GSLB en el nodo principal y, a continuación, intenta sincronizar.
  - Si las contraseñas del nodo RPC son diferentes para NSIP y la dirección IP de bucle invertido.
  - Si realiza la sincronización en sitios GSLB configurados en particiones diferentes del mismo dispositivo Citrix ADC.
- Si ha configurado los sitios GSLB como pares de alta disponibilidad (HA), las contraseñas de los nodos RPC de los nodos principal y secundario deben ser las mismas.
- Si cambia el nombre de cualquier entidad GLSB que forma parte de la configuración de GSLB (utilice el comando “show gslb runningConfig” para mostrar la configuración de GSLB). Debe utilizar la opción Forzar sincronización para sincronizar la configuración con otros sitios GSLB.

> **Nota:**
>
> - En la sincronización incremental, no es necesario utilizar la opción Forzar sincronización para sincronizar la configuración con otros sitios GSLB. Esto se aplica a partir de Citrix ADC versión 13.0 compilación 79.x en adelante.

Nota: Para superar las limitaciones debidas a algunos ajustes en la configuración de GSLB, puede usar la opción Forzar sincronización. Sin embargo, si utiliza la opción de sincronización forzada, las entidades GSLB se eliminan y se leen a la configuración y las estadísticas GSLB se restablecen a cero. Por lo tanto, el tráfico se interrumpe durante el cambio de configuración.

Puntos a tener en cuenta antes de iniciar la sincronización de una configuración de GSLB

Antes de iniciar la sincronización de una configuración de GSLB, asegúrese de que:

- En todos los sitios de GSLB, incluido el sitio principal, el acceso de administración y SSH deben estar habilitados para la dirección IP del sitio GSLB correspondiente. La dirección IP de un sitio GSLB debe ser una dirección IP propiedad del dispositivo Citrix ADC. Para obtener más información sobre cómo agregar las direcciones IP del sitio GSLB y habilitar el acceso de administración, consulte "Configuración de un sitio GSLB básico".
- La configuración de GSLB del dispositivo Citrix ADC que se considera el sitio principal está completa y es adecuada para copiarse en todos los sitios.
- Si está sincronizando la configuración de GSLB por primera vez, todos los sitios que participan en GSLB deben tener la entidad de sitio GSLB de sus respectivos sitios locales.
- No está sincronizando sitios que, por diseño, no tienen la misma configuración.
- El sitio principal y los sitios subordinados ejecutan las mismas versiones de Citrix ADC. A partir de la versión 12.1, compilación 50.x, el dispositivo comprueba la versión del firmware en los sitios principales y subordinados antes de iniciar la sincronización. Si el sitio principal y el subordinado ejecutan versiones diferentes, la sincronización se anulará para ese sitio remoto para evitar introducir cambios incompatibles en las versiones. Además, aparece un mensaje de error que muestra los detalles del sitio en el que se anuló la sincronización.

  Las siguientes ilustraciones muestran mensajes de error de ejemplo de la CLI y la GUI.

```
> sh gslb syncStatus -summary
Displaying the status summary of the manual GSLB configuration synchronization:

-------------------------------------------------------------------------------------------------------------
        Site Name               Status      Reason
-------------------------------------------------------------------------------------------------------------
        s2                      Failure     Error: Different netscaler release on the remote site. Local Site: 13.0, Remote Site: 12.1
        s1                      Success     All Done
        s3                      Success     All Done
Done
>
```

```
> sh gslb syncStatus -summary
Displaying the status summary of the manual GSLB configuration synchronization:

-------------------------------------------------------------------------------------------------------------
        Site Name               Status      Reason
-------------------------------------------------------------------------------------------------------------
        s2                      Failure     Error: Different netscaler release on the remote site. Local Site: 13.0, Remote Site: 12.1
        s1                      Success     All Done
        s3                      Success     All Done
Done
>
```


> **Importante**
>
> Los siguientes directorios se sincronizan como parte de la sincronización de configuración de GSLB.
>
> - /var/netscaler/locdb/
> - /var/netscaler/ssl/
> - /var/netscaler/inbuilt_db/

Sincronización manual entre los sitios que participan en GSLB

August 20, 2021

La sincronización manual de la configuración de GSLB en la ubicación maestra y las ubicaciones esclavas se realiza de la siguiente manera:

- La ubicación maestra detecta las diferencias entre la configuración de su propio sitio y el sitio esclavo.
- La ubicación maestra aplica la diferencia de configuración al sitio esclavo.
- La ubicación maestra realiza la sincronización de configuración con todas las ubicaciones esclavas de la configuración de GSLB y completa el proceso de sincronización.

Importante: Después de sincronizar una configuración GSLB, la configuración no se puede revertir en ninguno de los sitios GSLB. Realice la sincronización solo si está seguro de que el proceso de sincronización no sobrescribe la configuración en el sitio remoto. La sincronización de sitios no es deseable cuando los sitios locales y remotos tienen diferentes configuraciones por diseño, lo que provoca una interrupción del sitio. Si algunos comandos fallan y algunos tienen éxito, los comandos correctos no se deshacen.

Puntos a tener en cuenta

- Si fuerza una sincronización (utilice la opción “forzar sincronización”), el dispositivo Citrix ADC elimina la configuración de GSLB del sitio esclavo. A continuación, el sitio maestro configura el sitio esclavo para que sea similar a su propio sitio.
- Durante la sincronización, si un comando falla, la sincronización no se anula. Los mensajes de error se registran en un archivo.err del directorio /var/netscaler/gslb.
- Si utiliza la `saveconfig` opción, los sitios que participan en el proceso de sincronización guardan automáticamente su configuración, de la siguiente manera:
  - La ubicación maestra guarda su configuración inmediatamente antes de iniciar el proceso de sincronización.

- Los sitios esclavos guardan su configuración una vez finalizado el proceso de sincronización. Un sitio esclavo guarda su configuración solo si la diferencia de configuración se aplicó correctamente en él. Si la sincronización falla en un sitio esclavo, debe investigar manualmente la causa del error y realizar acciones correctivas.

Para sincronizar una configuración de GSLB mediante la CLI:

En el símbolo del sistema, escriba los siguientes comandos para sincronizar sitios GSLB y verificar la configuración:

```
sync gslb config [-preview | -forceSync <string> | -nowarn | -
   saveconfig] [-debug]
show gslb syncStatus
<!--NeedCopy-->
```

Ejemplo:

```
sync gslb config

[WARNING]: Syncing config may cause configuration loss on other site.

Please confirm whether you want to sync-config (Y/N)? [N]:y

Sync Time: Dec 9 2011 10:56:9

Retrieving local site info: ok

Retrieving all participating gslb sites info: ok

Gslb_site1[Master]:

Getting Config: ok

Gslb_site2[Slave]:

Getting Config: ok

Comparing config: ok

Applying changes: ok

Done
<!--NeedCopy-->
```


Para sincronizar una configuración de GSLB mediante la GUI:

1. Vaya a **Gestión del tráfico > GSLB > Panel de control**.
2. Haga clic en **Sincronización automática GSLB** y seleccione **ForceSyn**.
3. En **Nombre de sitio de GSLB**, seleccione los sitios de GSLB que se van a sincronizar con la configuración del nodo maestro.

Vista previa de la sincronización GSLB

Al previsualizar la operación de sincronización GSLB, puede ver las diferencias entre el nodo maestro y cada nodo esclavo. Si hay discrepancias, puede solucionar problemas antes de sincronizar la configuración de GSLB.

Para obtener una vista previa de la salida de sincronización GSLB mediante la CLI:

En el símbolo del sistema, escriba el siguiente comando:

```
sync gslb config -preview
<!--NeedCopy-->
```

Para obtener una vista previa de la salida de sincronización GSLB mediante la GUI:

1. Vaya a **Configuración** > **Administración del tráfico** > **GSLB** > **Panel**de control.
2. Haga clic en **Sincronización automática GSLB** y seleccione **Vista previa**.
3. Haga clic en **Ejecutar**.
   Una ventana de progreso muestra cualquier discrepancia en la configuración.

Depuración de los comandos activados durante el proceso de sincronización

Puede ver el estado (éxito o error) de cada comando desencadenado durante el proceso de sincronización y solucionar los problemas correspondientes.

Para depurar los comandos de sincronización GSLB mediante la CLI:

En el símbolo del sistema, escriba el siguiente comando:

```
sync gslb config -debug
<!--NeedCopy-->
```

Para depurar los comandos de sincronización GSLB mediante la GUI:

1. Vaya a **Configuración** > **Administración del tráfico** > **GSLB** > **Panel de control**.
2. Haga clic en **Sincronización automática GSLB** y seleccione **Depurar**.
3. Haga clic en **Ejecutar**. Una ventana de progreso muestra el estado de cada comando desencadenado durante la sincronización.

Sincronización en tiempo real entre sitios que participan en GSLB

October 5, 2021

Puede utilizar el parámetro `AutomaticConfigSync` para sincronizar automáticamente la configuración GSLB en tiempo real del sitio principal con todos los sitios subordinados. No es necesario activar manualmente la opción AutoSync para sincronizar la configuración.

Puede sincronizar automáticamente la configuración de GSLB del sitio principal con todos los sitios subordinados mediante sincronización incremental o sincronización completa. El parámetro `GSLBSyncMode` permite elegir el modo de sincronización.

> Nota:
>
> A partir de Citrix ADC versión 13.0 compilación 79.x, se admite la sincronización incremental de la sincronización GSLB. De forma predeterminada, la sincronización se realiza mediante sincronización incremental. La sincronización incremental se puede realizar activando el parámetro `IncrementalSync`. Para obtener más información, consulte Sincronización incremental de la configuración de GSLB.

Prácticas recomendadas para utilizar la función de sincronización en tiempo real

- Se recomienda que todos los dispositivos Citrix ADC que participan como sitios tengan la misma versión de software Citrix ADC.
- Para cambiar la contraseña del nodo RPC, cambie primero la contraseña en el sitio subordinado y, a continuación, en el sitio principal.
- Configure los sitios GSLB locales en cada sitio que participe en GSLB.
- Habilite AutomaticConfigSync en uno de los sitios en los que se realiza la configuración. Con el tiempo, este sitio se sincroniza con otros sitios GSLB.
- Si hay una nueva configuración o se han realizado cambios en la configuración existente, asegúrese de comprobar el estado mediante el comando `show gslb syncStatus` para confirmar si los cambios están sincronizados en todos los sitios o si se ha producido algún error.
- La supervisión de puertos RSYNC debe estar habilitada.

Para habilitar la sincronización en tiempo real mediante la CLI

En el símbolo del sistema, escriba:

```
set gslb parameter [ - automaticConfigSync (ENABLED | DISABLED)] [-
    MEPKeepAliveTimeout <secs>]  [-GSLBSyncMode ( IncrementalSync |
    FullSync )] [-GSLBSyncLocFiles ( ENABLED | DISABLED)] [-
    GslbConfigSyncMonitor ( ENABLED | DISABLED )] [-GSLBSyncInterval <
    secs>] [-GSLBSyncSaveConfigCommand ( ENABLED | DISABLED )]
<!--NeedCopy-->
```

Ejemplo:

```
set gslb parameter  - automaticConfigSync ENABLED
<!--NeedCopy-->
```

La sincronización en tiempo real proporciona los siguientes parámetros configurables:

- **GSLBSyncMode**: modo en el que la configuración se sincroniza desde el sitio principal a los sitios remotos.
  - Valores posibles: incrementalSync, FullSync
  - Valor predeterminado: IncrementalSync
- **GSLBSynclocFiles**: durante la sincronización de configuración de GSLB, de forma predeterminada, los cambios en los archivos de base de datos de ubicación se detectan y sincronizan automáticamente. Dado que los directorios de base de datos de ubicación no cambian con frecuencia, los administradores pueden inhabilitar la sincronización automática de los archivos de base de datos de ubicación. En su lugar, los administradores deben copiar manualmente los archivos de base de datos de ubicación en los sitios subordinados de GSLB. La sincronización de archivos de base de datos de ubicación lleva mucho tiempo. Por lo tanto, evitarlo reduce el tiempo de sincronización general.

  Ejemplo para inhabilitar la sincronización automática de los archivos de base de datos de ubicación:

  ```
  set gslb parameter -GSLBSyncMode IncrementalSync -
      GSLBSyncLocFiles DISABLED
  <!--NeedCopy-->
  ```

- **gslbConfigSyncMonitor**: habilite el parámetro GSLB Config Sync Monitor para supervisar el estado del puerto RSYNC de los sitios subordinados, que es el puerto SSH 22 en la dirección IP

del sitio GSLB remoto. Si el monitor muestra el estado del sitio subordinado como DOWN, se omite la operación RSYNC en ese sitio. Esto reduce los retrasos en la sincronización causados por intentar conectarse a los sitios remotos que están DESACTIVADOS.

Ejemplo para habilitar la supervisión de puertos RSYNC en la CLI:

```
set gslb parameter -GSLBSyncMode IncrementalSync -
   GslbConfigSyncMonitor ENABLED
<!--NeedCopy-->
```

- **GSLBSyncInterval**: establece el intervalo de tiempo (en segundos) en el que se produce la sincronización de configuración de GSLB. De forma predeterminada, la función de sincronización de configuración automática de GSLB sincroniza la configuración de GSLB automáticamente cada 10 segundos. Puede cambiar el intervalo de tiempo a cualquier valor deseado. Absténgase de establecer esto en un valor inferior, por ejemplo, no inferior a 5 segundos. Porque la sincronización frecuente puede aumentar el consumo de CPU de administración.

  > Nota:
  >
  > En una configuración de partición de administrador, el intervalo de tiempo solo se puede establecer en la partición predeterminada porque es un parámetro global.

  Ejemplo para establecer el intervalo de sincronización:

```
set gslb parameter -AutomaticConfigSync ENABLED -GSLBSyncMode
   IncrementalSync -GSLBSyncInterval 7
<!--NeedCopy-->
```

- **GSLBSyncSaveConfigCommand**: Habilite este parámetro para sincronizar el comando `save ns config` con sitios subordinados, si la opción `AutomaticConfigSync` está activada.

  Ejemplo para habilitar la sincronización del comando 'Save Config':

```
set gslb parameter -AutomaticConfigSync ENABLED -
   GSLBSyncSaveConfigCommand ENABLED
<!--NeedCopy-->
```

  El comando `save ns config` no se sincroniza con sitios subordinados en determinados casos de la siguiente manera:

  - El sitio subordinado está caído o no se puede acceder a él cuando la configuración se guarda en el sitio principal.

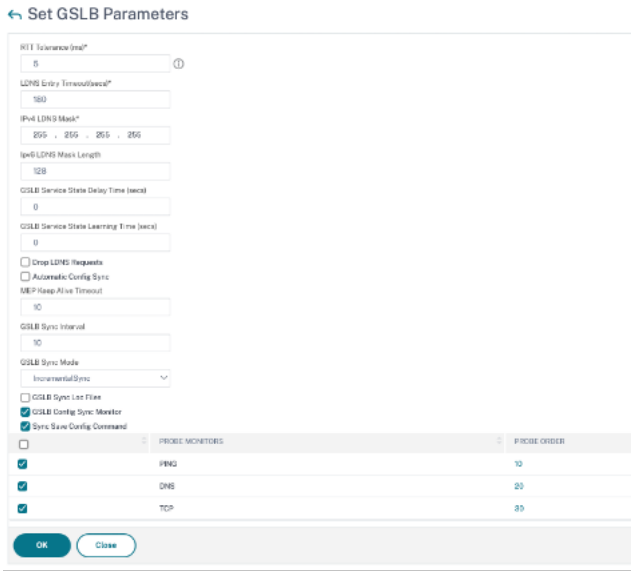
- La configuración ha fallado en un sitio subordinado.

Para habilitar la sincronización en tiempo real mediante la interfaz gráfica de usuario

1. Vaya a **Configuración** > **Administración del tráfico** > **GSLB** > **Cambiar configuración de GSLB**.
2. En la página **Establecer parámetros de GSLB**, puede realizar lo siguiente:
   - Para sincronizar automáticamente la configuración de GSLB en tiempo real, seleccione **ConfigSync automático**.

   Nota: Esta opción debe estar habilitada solo en el sitio donde se realiza la configuración.

   - Para establecer el intervalo de sincronización de configuración automática de GSLB, introduzca el tiempo en segundos en el campo **Intervalo de sincronización GSLB** .
   - Para habilitar la supervisión de puertos RSYNC, active la casilla **GSLB Config Sync Monitor** .
   - Para inhabilitar la sincronización automática de los archivos de base de datos de ubicación, desactive la casilla de verificación **GSLB Sync Loc Files** .
   - Para habilitar la sincronización del comando `save ns config` con los sitios subordinados, seleccione la casilla **Sincronizar comando Guardar configuración**.



Para obtener información sobre los siguientes temas, consulte Sincronización manual entre sitios que participan en GSLB.

- Vista previa de la sincronización GSLB
- Depuración de los comandos activados durante el proceso de sincronización

Puntos a tener en cuenta

- El archivo de registro consolidado relacionado con la sincronización en tiempo real se almacena en el directorio /var/netscaler/gslb/periodic_sync.log.
- El archivo de configuración predeterminado se almacena en el directorio /var/netscaler/gslb_sync/.
- El sitio principal utiliza la siguiente estructura de directorios:
  - El sitio principal almacena todos sus archivos en el directorio /var/netscaler/gslb_sync/master.
  - El sitio principal almacena su archivo de configuración que debe sincronizarse con los sitios subordinados, en el directorio /var/netscaler/gslb_sync/master/gslbconf/.
  - Los archivos de estado extraídos de todos los sitios subordinados se almacenan en el directorio /var/netscaler/gslb_sync/master/slavestatus/.
- El sitio subordinado utiliza la siguiente estructura de directorios:
  - El sitio subordinado recoge el último archivo de configuración que se va a aplicar del directorio /var/netscaler/gslb_sync/slave/gslbconf.
  - El sitio subordinado almacena su archivo de estado en el directorio /var/netscaler/gslb_sync/slave/gslb
- En una configuración de partición de administrador, se mantiene la misma estructura de directorios en la ubicación: /var/partitions/`partition name`/netscaler/gslb_sync.
- Los relojes de todos los sitios deben configurarse con precisión en un estándar en tiempo real, como la hora universal coordinada (UTC).

Sincronización incremental de la configuración GSLB

La función de sincronización de configuración automática de GSLB comprueba los cambios de configuración en el sitio principal cada 10 segundos y realiza una sincronización. Este valor de intervalo de sincronización se puede configurar.

En la sincronización incremental, solo las configuraciones que han cambiado en el sitio principal entre la última sincronización y el siguiente intervalo de sincronización (10 segundos) se sincronizan en todos los sitios subordinados. La sincronización incremental es el comportamiento predeterminado. Al pulsar solo las configuraciones incrementales se reduce considerablemente el tamaño del archivo de configuración y, por lo tanto, el tiempo de sincronización. Si falla una sincronización incremental, el sistema realiza automáticamente una sincronización de configuración completa.

La sincronización incremental se realiza de la siguiente manera:

- El sitio principal envía el archivo de configuración que incluye solo sus últimos cambios en todos los sitios subordinados. El último cambio hace referencia a las configuraciones que han cambiado entre la última sincronización y el siguiente intervalo de sincronización (10 segundos).
- Cada sitio subordinado aplica el último cambio a su propio sitio.
- La sincronización incremental no se ha intentado en los sitios subordinados, que están en estado DOWN. Cuando el sitio vuelve a UP, se vuelve a realizar la sincronización.

- El sitio subordinado genera registros de estado en cada paso y los copia en un archivo en una ubicación específica.
- El sitio principal extrae los archivos de registro de estado de la ubicación especificada.
- El sitio principal prepara un archivo de registro con registros combinados de todos los sitios subordinados.
- Este archivo de registro combinado se almacena en el archivo "/var/netscaler/gslb/periodic_sync.log".

Para obtener más información sobre los directorios en los que se almacenan los archivos de configuración, consulte la sección Puntos a tener en cuenta .

Para habilitar la sincronización incremental de la configuración de GSLB mediante la CLI

```
set gslb parameter -AutomaticConfigSync (ENABLED | DISABLED) -
    GSLBSyncMode (IncrementalSync | FullSync) -GslbConfigSyncMonitor (
    ENABLED | DISABLED) -GSLBSyncInterval <secs> -GSLBSyncLocFiles (
    ENABLED | DISABLED)
<!--NeedCopy-->
```

Ejemplo:

```
set gslb parameter -AutomaticConfigSync ENABLED -GSLBSyncMode
    IncrementalSync
<!--NeedCopy-->
```

Para habilitar la sincronización incremental de GSLB mediante la GUI

1. Vaya a **Administración del tráfico > GSLB > Panel de control > Cambiar configuración de GSLB**.
2. En la página **Definir parámetros de GSLB**, seleccione **IncrementalSync** en el menú desplegable **Modo de sincronización de GSLB** .

Sincronización completa de la configuración de GSLB

Cada vez que se produce un cambio de configuración en el sitio principal, la configuración completa que ejecuta GSLB en el sitio principal se envía a todos los sitios subordinados.
Incluso si se configura la sincronización incremental, se realiza una sincronización completa cuando el sitio principal no conoce el estado de configuración del sitio subordinado. Algunos de estos casos son los siguientes:

- Habilite la función de sincronización de configuración automática de GSLB por primera vez.
- Reinicie el dispositivo Citrix ADC.
- La implementación de GSLB tiene varios sitios principales y otro sitio principal se convierte en el sitio principal activo.
- Agregue un nuevo sitio subordinado a la implementación de GSLB.

La sincronización completa de la configuración de GSLB se realiza de la siguiente manera:

- El sitio principal envía su último archivo de configuración a todos los sitios subordinados.
- Cada sitio subordinado compara su propia configuración con el último archivo de configuración enviado por el sitio principal. El sitio subordinado identifica la diferencia de configuración y aplica la configuración delta para su propio sitio.
- El sitio subordinado genera registros de estado en cada paso y los copia en un archivo en una ubicación específica.
- El sitio principal extrae los archivos de registro de estado de la ubicación especificada.
- El sitio principal prepara un archivo de registro con registros combinados de todos los sitios subordinados.
- Este archivo de registro combinado se almacena en el archivo "/var/netscaler/gslb/periodic_sync.log".

Si intenta sincronizar manualmente (con el comando `sync gslb config`) un sitio mientras se está sincronizando automáticamente, aparece el mensaje de error "Sincronización en curso". La sincronización automática no se puede activar para un sitio que está en proceso de sincronizarse manualmente.

> **Atención:**
>
> A partir de Citrix ADC 12.1 compilación 49.37, se generan capturas SNMP al sincronizar la configuración de GSLB. En la sincronización en tiempo real, el estado de sincronización en la primera captura SNMP se captura como error. Puede ignorar este estado porque se genera automáticamente una segunda captura SNMP inmediatamente después de la primera captura con el estado de sincronización real. Sin embargo, si la sincronización también falló en el segundo intento, la captura SNMP no se genera porque el estado de sincronización no ha cambiado con respecto al estado de sincronización anterior.

Para obtener más información sobre la configuración del dispositivo Citrix ADC para generar capturas, consulte Configuración de Citrix ADC para generar capturas SNMP.

Para habilitar la sincronización completa de GSLB mediante la CLI

```
set gslb parameter -GSLBSyncMode (IncrementalSync | FullSync)
<!--NeedCopy-->
```


Ejemplo:

```
set gslb parameter -GSLBSyncMode FullSync
<!--NeedCopy-->
```

Para habilitar la sincronización incremental de GSLB mediante la GUI:

1. Vaya a **Administración del tráfico > GSLB > Panel > Cambiar la configuración de GSLB**.
2. En la página **Establecer parámetros de GSLB**, seleccione **FullSync** en el menú desplegable **Modo de sincronización de GSLB** .

Varios sitios principales en una implementación de GSLB

El dispositivo Citrix ADC admite varios sitios principales en una implementación activa pasiva. Se recomienda tener dos sitios principales en una implementación de GSLB para hacer frente al fallo del sitio principal de GSLB. Tener dos sitios principales puede evitar un único punto de falla en la sincronización de la configuración de GSLB. En cualquier momento, solo un sitio principal puede procesar activamente la configuración de GSLB del usuario. Si los cambios de configuración se realizan simultáneamente en más de un sitio principal, podría provocar incoherencia en la configuración o pérdidas de configuración. Por lo tanto, se recomienda realizar cambios de configuración desde un solo sitio principal a la vez y utilizar el otro sitio principal como copia de seguridad cuando falla el sitio principal activo.

> Nota:
>
> Cuando se utilizan varios sitios principales en una implementación de GSLB, la supervisión de RSYNC debe estar habilitada.

Para convertir un nodo GSLB como uno de los principales sitios para la sincronización de la configuración de GSLB, ejecute el siguiente comando:

```
set gslb parameter -automaticConfigSync Enabled
<!--NeedCopy-->
```

Ver el estado y el resumen de sincronización de GSLB

August 20, 2021

Después de sincronizar la configuración de GSLB en los sitios de GSLB, puede ver el estado detallado y el resumen de la última operación de sincronización de GSLB. Esto es aplicable a la sincronización GSLB manual y en tiempo real.

Para ver el estado o el resumen de sincronización de GSLB mediante la CLI

En el símbolo del sistema, escriba:

```
1 show gslb sync status
2 <!--NeedCopy-->
```

O bien:

```
1 show gslb syncStatus -summary
2 <!--NeedCopy-->
```

Ejemplo de salida de configuración para la sincronización manual GSLB

El siguiente resultado muestra el estado de la sincronización manual de configuración de GSLB.


```
> sh gslb syncStatus
Displaying the status of the manual GSLB configuration synchronization:

gslb_site1[Master]:
        Getting Config:  ok
gslb_site2[Slave]:
        Syncing gslb static proximity database:  ok
        Syncing inbuilt gslb static proximity database : ok
        Getting Config:  ok
        Comparing config:  ok
        Applying changes:  ok
gslb_natsite1[Slave]:
        Syncing gslb static proximity database:  ok
        Syncing inbuilt gslb static proximity database : ok
        Getting Config:  ok
        Comparing config:  ok
        Applying changes:  ok
 Done
>
```

El siguiente resultado muestra el resumen de estado de la sincronización manual de configuración de GSLB.

```
> sh gslb syncStatus -summary
Displaying the status summary of the manual GSLB configuration synchronization:

-------------------------------------------------------------------------------------------------------------
        Site Name                Status          Reason
-------------------------------------------------------------------------------------------------------------
        gslb_site1               Success         All Done
        gslb_site2               Failure         Error executing command on gslb site...ERROR: Connection failed
        gslb_natsite1            Success         All Done
Done
>
```

Ejemplo de salida de configuración para sincronización GSLB en tiempo real

El siguiente resultado muestra el estado de la sincronización de configuración GSLB en tiempo real para la ubicación maestra:


```
> sh gslb syncStatus
Displaying the status of the real time GSLB configuration
    synchronization as master node:

site2[Master]:
                New GSLB configuration detected at Fri Jan 23 20:54:24
                    2020
                Fetching current configuration: Done
                Updating default.conf file: Done
site1[Slave]:
                Syncing gslb static proximity database to node site1:
                    Done
                Syncing inbuilt GSLB static proximity database to node
                    site1: Done
                Syncing ssl certificates, keys and CRLS to node site1:
                    Done
                Syncing current configuration to site1: Done
                Pulling status files from site1: Status file not
                    available yet(Sync in progress)
                Pulling status files from site1: Done
                site1 received new configuration from 10.102.217.205 in
                     file 2JNSzClRHK5+pdek6szQ3g-default-10.102.217.210.
                    conf
                Firing set gslb parameter -startConfigSync ENABLED
                    command: Done
                Fetching running GSLB Config: Done
                Comparing config: Done
                Applying changes: Done
                Firing set gslb parameter -startConfigSync DISABLED
                    command: Done
                Updating default.conf file: Done
Done
<!--NeedCopy-->
```

El siguiente resultado muestra el estado de la sincronización de configuración GSLB en tiempo real para el sitio esclavo:

```
> sh gslb syncStatus
Displaying the status of the real time GSLB configuration
    synchronization as slave node:

                site1 received new configuration from 10.102.217.205 in
                     file 2JNSzClRHK5+pdek6szQ3g-default-10.102.217.210.
```



```
                    conf
5                 Firing set gslb parameter -startConfigSync ENABLED
                    command: Done
6                 Fetching running GSLB Config: Done
7                 Comparing config: Done
8                 Applying changes: Done
9                 Firing set gslb parameter -startConfigSync DISABLED
                    command: Done
10                Updating default.conf file: Done
11 Done
12 <!--NeedCopy-->
```

El siguiente resultado muestra el resumen de estado de la sincronización de configuración de GSLB en tiempo real para la ubicación maestra:

```
1  > sh gslb syncStatus -summary
2  Displaying the status summary of the real time GSLB configuration
       synchronization as master node:
3
4  ------------------------------------------------------------------------------

5                 Site Name                                   Status
                                Reason
6  ------------------------------------------------------------------------------

7                 site2                                       Success
                              All Done
8                 site1                                       Success
                              All Done
9
10 Done
11 <!--NeedCopy-->
```

El siguiente resultado muestra el resumen de estado de la sincronización de configuración de GSLB en tiempo real para el sitio esclavo:

```
1  > sh gslb syncStatus  - summary
2  Displaying the status summary of the real time GSLB configuration
       synchronization as slave node:
3
4  ------------------------------------------------------------------------------
```



```
                Site Name                                       Status
                                    Reason
------------------------------------------------------------------------------

                site1                                           Success
                                   All Done

Done
<!--NeedCopy-->
```

Para ver el estado o resumen de sincronización de GSLB mediante la interfaz gráfica de usuario

1. Vaya a **Configuración** > **Administración del tráfico** > **GSLB** > **Panel**de control.
2. Haga clic en **Ver resumen de sincronización** o **Ver estado de sincronización**, según sea necesario.

Trampas SNMP para sincronización de configuración GSLB

August 20, 2021

A partir de Citrix ADC 12.1 compilación 49.xx, el dispositivo Citrix ADC genera capturas SNMP para sitios locales y remotos al sincronizar la configuración de GSLB. Las capturas SNMP se generan tanto para la sincronización manual como para la sincronización en tiempo real.

Cuando sincroniza la configuración de GSLB por primera vez, se generan capturas SNMP. En los intentos de sincronización posteriores, las capturas SNMP solo se generan si hay un cambio en el estado de sincronización con respecto al estado de sincronización anterior. Además, las capturas SNMP se generan solo para sitios para los que el estado de sincronización cambió con respecto al estado anterior.

Por ejemplo, considere que la primera sincronización de configuración de GSLB es correcta. Cuando sincroniza la configuración por segunda vez y si la sincronización vuelve a tener éxito, las capturas SNMP no se generan porque el estado no se cambia. Sin embargo, en el tercer intento, si se produce un error en la sincronización para uno de los sitios, se genera una captura SNMP solo para ese sitio.

En una alta disponibilidad y una configuración de clúster, el dispositivo genera las capturas SNMP cuando sincroniza la configuración de GSLB desde el nuevo nodo, independientemente del estado de sincronización anterior. Además, si la opción de captura SNMP se inhabilitó previamente y luego se habilitó, las capturas SNMP se generan a partir de ese punto en adelante, independientemente del estado de sincronización anterior.

Las capturas SNMP de la sincronización de configuración de GSLB proporcionan los siguientes detalles:

- Nombre del sitio GSLB para el que se envía la captura SNMP.
- Estado de sincronización de la configuración de GSLB: correcta o fallo.
- Modo de sincronización de configuración GSLB: Sincronización incremental o Sincronización completa.
- (Opcional) Información detallada sobre las capturas SNMP.

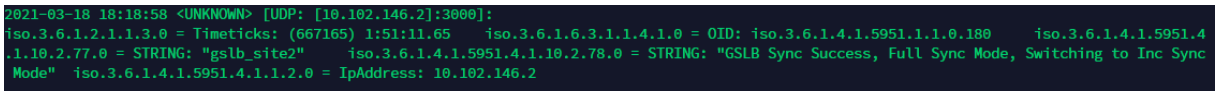
Las capturas SNMP se generan en los siguientes casos:

- El estado de sincronización de GSLB para un sitio GSLB cambia de Success to Failure y, por el contrario.
- El modo de sincronización GSLB cambia de sincronización incremental a sincronización completa y, por el contrario.

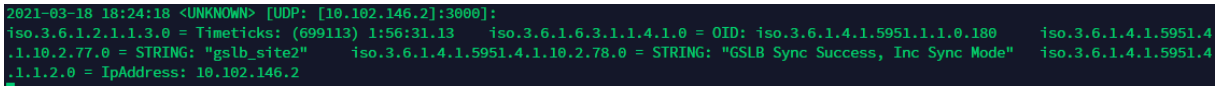
> Nota:
>
> Incluso cuando la sincronización incremental está habilitada, si se realiza la sincronización completa en un sitio GSLB por algún motivo, el motivo de la sincronización completa se menciona en la sección “Información detallada” del mensaje de trampa. Por ejemplo, cuando se agrega un nuevo sitio GSLB a la configuración de GSLB.

Mensajes de captura SNMP de ejemplo

En la siguiente ilustración se muestra una captura SNMP de ejemplo para gslb_site2, en la que la sincronización de configuración de GSLB se realiza correctamente mediante el modo Sincronización completa.



En la siguiente ilustración se muestra una captura SNMP de ejemplo para gslb_site2, en la que la sincronización de la configuración de GSLB se realiza correctamente mediante el modo de sincronización incremental.



En la siguiente ilustración se muestra una captura SNMP de ejemplo para gslb_site2, en la que se ha producido un error en la sincronización de configuración de GSLB mediante el modo de sincronización incremental. El mensaje de error indica que debe corregir manualmente los errores para completar la sincronización.


```
2021-03-18 18:17:34 <UNKNOWN> [UDP: [10.102.146.2]:3000]:
iso.3.6.1.2.1.1.3.0 = Timeticks: (658753) 1:49:47.53    iso.3.6.1.6.3.1.1.4.1.0 = OID: iso.3.6.1.4.1.5951.1.1.0.180     iso.3.6.1.4.1.5951.4
.1.10.2.77.0 = STRING: "gslb_site2"     iso.3.6.1.4.1.5951.4.1.10.2.78.0 = STRING: "GSLB Sync Failure, Inc Sync Mode, Site is not in sync, I
ncremental config application has failed, Switching to Full Sync Mode." iso.3.6.1.4.1.5951.4.1.1.2.0 = IpAddress: 10.102.146.2
2021-03-18 18:17:49 <UNKNOWN> [UDP: [10.102.146.2]:3000]:
iso.3.6.1.2.1.1.3.0 = Timeticks: (660256) 1:50:02.56    iso.3.6.1.6.3.1.1.4.1.0 = OID: iso.3.6.1.4.1.5951.1.1.0.180     iso.3.6.1.4.1.5951.4
.1.10.2.77.0 = STRING: "gslb_site2"     iso.3.6.1.4.1.5951.4.1.10.2.78.0 = STRING: "GSLB Sync Failure,Full Sync Mode, Site is not in sync, F
ull sync config application has failed, Please fix the errors." iso.3.6.1.4.1.5951.4.1.1.2.0 = IpAddress: 10.102.146.2
```

En la siguiente ilustración se muestra una captura SNMP de ejemplo para gslb_site2, en la que se ha producido un error en la sincronización de configuración de GSLB mediante el modo de sincronización incremental. También indica el motivo del error de sincronización, es decir, el monitor del sitio está DESACTIVADO.

```
2021-03-18 18:21:39 <UNKNOWN> [UDP: [10.102.146.2]:3000]:
iso.3.6.1.2.1.1.3.0 = Timeticks: (683289) 1:53:52.89    iso.3.6.1.6.3.1.1.4.1.0 = OID: iso.3.6.1.4.1.5951.1.1.0.180     iso.3.6.1.4.1.5951.4
.1.10.2.77.0 = STRING: "gslb_site2"     iso.3.6.1.4.1.5951.4.1.10.2.78.0 = STRING: "GSLB Sync Failure, Inc Sync Mode, Syncing current config
uration to gslb_site2: Skipped, Site Monitor is down"    iso.3.6.1.4.1.5951.4.1.1.2.0 = IpAddress: 10.102.146.2
```

Panel de control GSLB

January 12, 2021

Puede ver el estado general de los sitios de GSLB que participan en GSLB en el panel de GSLB.

Puede acceder a la configuración de GSLB desde el panel. También puede iniciar el asistente de configuración de GSLB desde el panel. Además, puede realizar la sincronización y probar la configuración de GSLB desde el panel.

Para acceder al panel de GSLB, vaya a **Configuración** > **Gestión del tráfico** > **GSLB** > **Panel de control**.

Supervisar los servicios de GSLB

August 20, 2021

Cuando vincula un servicio remoto a un servidor virtual GSLB, los sitios GSLB intercambian información de métrica, incluida la información de métrica de red, que es la información de tiempo de ida y vuelta y la información de persistencia.

Si se pierde momentáneamente una conexión de intercambio de métricas entre cualquiera de los sitios participantes, el sitio remoto se marca como DOWN y el equilibrio de carga se realiza en los sitios restantes que están UP. Cuando el intercambio de métricas para un sitio es DOWN, los servicios remotos que pertenecen al sitio también se marcan DOWN.

El dispositivo Citrix ADC evalúa periódicamente el estado de los servicios GSLB remotos mediante MEP o monitores vinculados explícitamente a los servicios remotos. No es necesario vincular monitores explícitos a servicios locales, ya que el estado del servicio GSLB local se actualiza de forma predeterminada mediante el MEP. Sin embargo, puede vincular monitores explícitos a un servicio remoto.

Cuando los monitores están vinculados explícitamente, el estado del servicio remoto no se controla mediante el intercambio de métricas.

De forma predeterminada, cuando se vincula un monitor a un servicio GSLB remoto, el dispositivo Citrix ADC utiliza el estado del servicio notificado por el monitor. Sin embargo, puede configurar el dispositivo Citrix ADC para que utilice monitores para evaluar servicios en las siguientes situaciones:

- Utilice siempre monitores (configuración predeterminada).
- Utilice monitores cuando MEP esté DOWN.
- Utilice monitores cuando los servicios remotos y MEP estén DOWN.

La segunda y tercera de las configuraciones anteriores permiten que el dispositivo deje de supervisar cuando MEP está UP. Por ejemplo, en una configuración jerárquica de GSLB, un sitio de GSLB proporciona la información MEP acerca de sus sitios secundarios a su sitio principal. Este sitio intermedio puede evaluar el estado del sitio secundario como DOWN debido a problemas de red, aunque el estado real del sitio es UP. En este caso, puede vincular monitores a los servicios del sitio principal e inhabilitar MEP para determinar el estado real del servicio remoto. Esta opción le permite controlar la forma en que se determinan los estados de los servicios remotos.

Para utilizar monitores, primero crearlos y, a continuación, vincularlos a los servicios GSLB.

Configurar desencadenador de monitor

Puede configurar un sitio GSLB para que utilice siempre monitores (el valor predeterminado), use monitores cuando MEP está inactivo o use monitores cuando el servicio remoto y MEP están inactivo. En los dos últimos casos, el dispositivo Citrix ADC deja de supervisar cuando MEP vuelve al estado ACTIVO.

Para configurar la activación del monitor mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
set gslb site <siteName> -triggerMonitor (ALWAYS | MEPDOWN |
    MEPDOWN_SVCDOWN)
<!--NeedCopy-->
```

Ejemplo:

```
set gslb site Site-GSLB-North-America -triggerMonitor Always
<!--NeedCopy-->
```


Para configurar la activación del monitor mediante la utilidad de configuración

1. Desplácese hasta **Administración del tráfico** > **GSLB** > **Sitios** y haga doble clic en el sitio.
2. En la lista desplegable **Monitores de disparo**, seleccione una opción para cuándo activar la supervisión.

Agregar o quitar monitores

Para agregar un monitor, especifique el tipo y el puerto. No se puede quitar un monitor enlazado a un servicio. Primero debe desvincular el monitor del servicio.

Para agregar un monitor mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para crear un monitor y verificar la configuración:

```
add lb monitor <monitorName> -type <monitorType> -destPort <portNumber>

show lb monitor <monitorName>
<!--NeedCopy-->
```

Ejemplo:

```
add lb monitor monitor-HTTP-1 -type HTTP -destPort 80
show lb monitor monitor-HTTP-1
<!--NeedCopy-->
```

Para quitar un monitor mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
rm lb monitor <monitorName>
<!--NeedCopy-->
```

Para agregar un monitor mediante la utilidad de configuración

Vaya a Administración
del tráfico > Equilibrio de carga > Monitores y agregue o elimine un monitor.

Vincular monitores a un servicio GSLB

Una vez que cree monitores, debe vincularlos a los servicios GSLB. Al vincular monitores a los servicios, puede especificar un peso para el monitor. Después de vincular uno o más monitores ponderados, puede configurar un umbral de monitor para el servicio. Este umbral baja el servicio si la suma de los pesos del monitor enlazado cae por debajo del valor del umbral.

Nota: En la utilidad de configuración, puede establecer tanto el peso como el umbral de supervisión al mismo tiempo que vincula el monitor. Al utilizar la línea de comandos, debe emitir un comando independiente para establecer el umbral de supervisión del servicio.

Para enlazar el monitor al servicio GSLB mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
bind monitor <name> <serviceName> [ -state (Enabled | Disabled) ] -
   weight <positiveInteger>
<!--NeedCopy-->
```

Ejemplo:

```
bind monitor monitor-HTTP-1 service-GSLB-1 -state enabled -weight 2
<!--NeedCopy-->
```

Para establecer el umbral de supervisión para un servicio GSLB mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
set gslb service <ServiceName> -monThreshold <PositiveInteger>
<!--NeedCopy-->
```

Ejemplo:

```
set gslb service service-GSLB-1 -monThreshold 9
<!--NeedCopy-->
```


Para enlazar el monitor al servicio GSLB mediante la utilidad de configuración

1. Vaya a Administración de Tráfico > GSLB > Servicios.
2. Haga clic en la sección **Monitor** y enlaza el monitor al servicio GSLB.

Para establecer el umbral de supervisión para un servicio GSLB mediante la utilidad de configuración

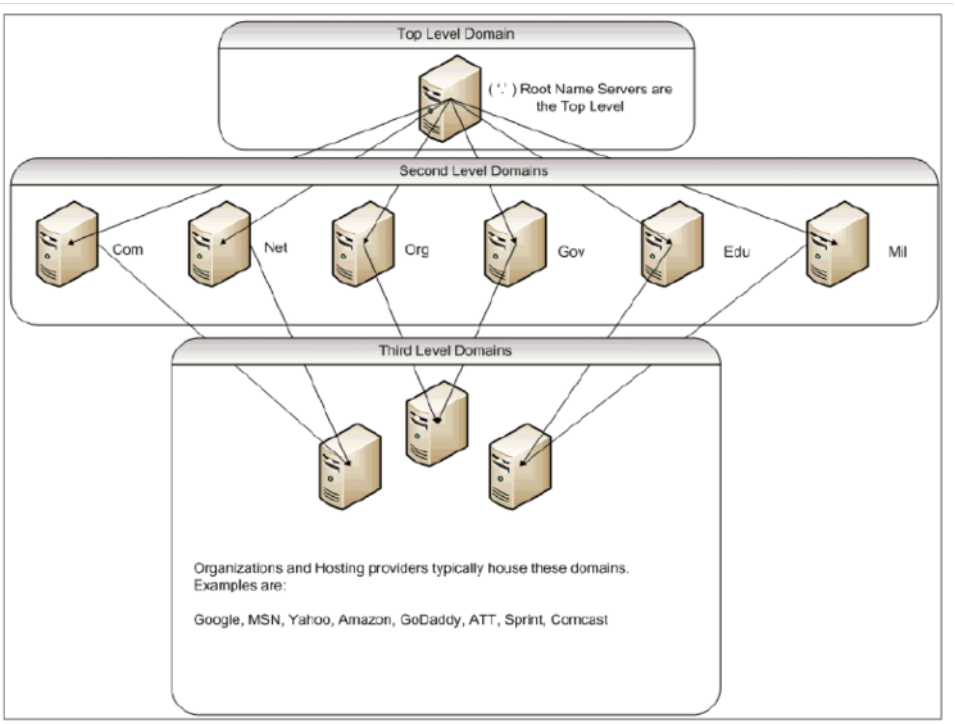
1. Vaya a Administración de Tráfico > GSLB > Servicios.
2. Haga clic en la sección **Supervisar Umbral** e introduzca un valor de umbral.

Cómo admite el sistema de nombres de dominio GSLB

October 5, 2021

El sistema de nombres de dominio (DNS) se considera una base de datos distribuida, que utiliza la arquitectura cliente/servidor. Los servidores de nombres son los servidores de la arquitectura y los solucionadores son los clientes que son rutinas de biblioteca instaladas en un sistema operativo que crean y envían consultas a través de la red.

La jerarquía lógica del DNS se muestra en el siguiente diagrama:



> Nota:
>
> Los servidores raíz de segundo nivel son responsables de mantener las asignaciones de servidor de nombres a direcciones para delegaciones de servidores de nombres dentro de los dominios .com, .net, .org, .gov, etc. Cada dominio de los dominios de segundo nivel es responsable de mantener las asignaciones de servidor de nombres a direcciones para los dominios organizativos de nivel inferior. A nivel de la organización, las direcciones de host individuales se resuelven para www, FTP y otros hosts que proporcionan servicios.

Delegación

El objetivo principal de la topología DNS actual es aliviar la carga de mantener todos los registros de direcciones en una sola autoridad. Esto permite la delegación de un espacio de nombres de organización a esa organización en particular. La organización puede delegar aún más su espacio en subdominios de la organización. Por ejemplo, en citrix.com puede crear subdominios llamados `sales.citrix.comeducation.citrix.com`, y `support.citrix.com`. Los departamentos correspondientes pueden mantener su propio conjunto de servidores de nombres autorizados para su subdominio y, a continuación, mantener su propio conjunto de asignaciones de nombres de host a direcciones. Ningún departamento es responsable de mantener todos los registros de direcciones de Citrix. Cada departamento puede cambiar direcciones y modificar topologías, y no imponer más trabajo en el dominio u organización de nivel superior.

Beneficios de la topología jerárquica

Algunas de las ventajas de la topología jerárquica incluyen:

- Escalabilidad
- Agregar funcionalidad de almacenamiento en caché a los servidores de nombres de cada nivel, donde un host atiende una solicitud DNS que no tiene autoridad para un dominio determinado pero puede contribuir a la respuesta a la consulta y reducir la congestión y el tiempo de respuesta.
- El almacenamiento en caché también crea redundancia y resiliencia ante fallos del servidor. Si falla un servidor de nombres, es posible que los registros se puedan entregar desde otros servidores que tienen copias recientes en caché de los mismos registros.

Resolvers

Los solucionadores son el componente cliente del sistema DNS. Los programas que se ejecutan en un host que necesitan información del espacio de nombres de dominio utilizan el solucionador. El solucionador se ocupa de:

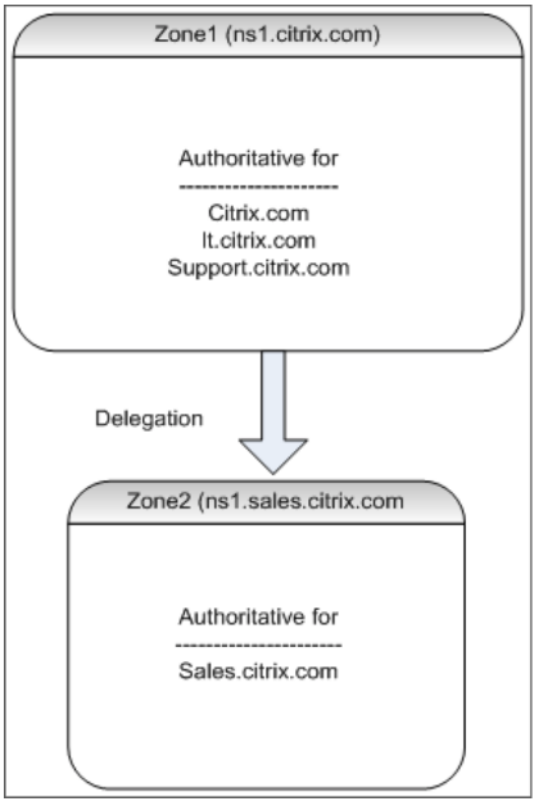
- Consulta de un servidor de nombres.
- Interpretación de respuestas (que pueden ser registros de recursos o un error).
- Devolver la información a los programas que la solicitaron.

El solucionador es un conjunto de rutinas de biblioteca que se compilan en programas como telnet, FTP y ping. No son procesos separados. Los solucionadores pueden crear una consulta, enviarla y esperar una respuesta. Y envíelo de nuevo (posiblemente a un servidor de nombres secundario) si no se responde dentro de un tiempo determinado. Este tipo de solucionadores se conocen como solucionadores de código auxiliar. Algunos solucionadores tienen la funcionalidad agregada a los registros en caché y respetan el tiempo de vida (TTL). En Windows, esta funcionalidad está disponible a través del servicio cliente DNS; se puede ver a través de la consola "services.msc".

Servidores de nombres

En general, los servidores de nombres almacenan información completa sobre una parte determinada de un espacio de nombres de dominio (denominado zona). A continuación, se dice que el servidor de nombres tiene autoridad para esa zona. También pueden ser autorizados para varias zonas.

La diferencia entre un dominio y una zona es sutil. Un dominio es el conjunto completo de entidades, incluidos sus subdominios, mientras que una zona es solo la información de un dominio que no se delega en otro servidor de nombres. Un ejemplo de zona es `citrix.com`, mientras que `sales.citrix.com` es una zona separada si esa zona se delega en otro servidor de nombres dentro del subdominio. En este caso, la zona Citrix principal puede incluir `citrix.comit.citrix.com`, y `support.citrix.com`. Dado que `sales.citrix.com` está delegado, no forma parte de la zona sobre la que el servidor de nombres `citrix.com` tiene autoridad. En el siguiente diagrama se muestran las dos zonas.

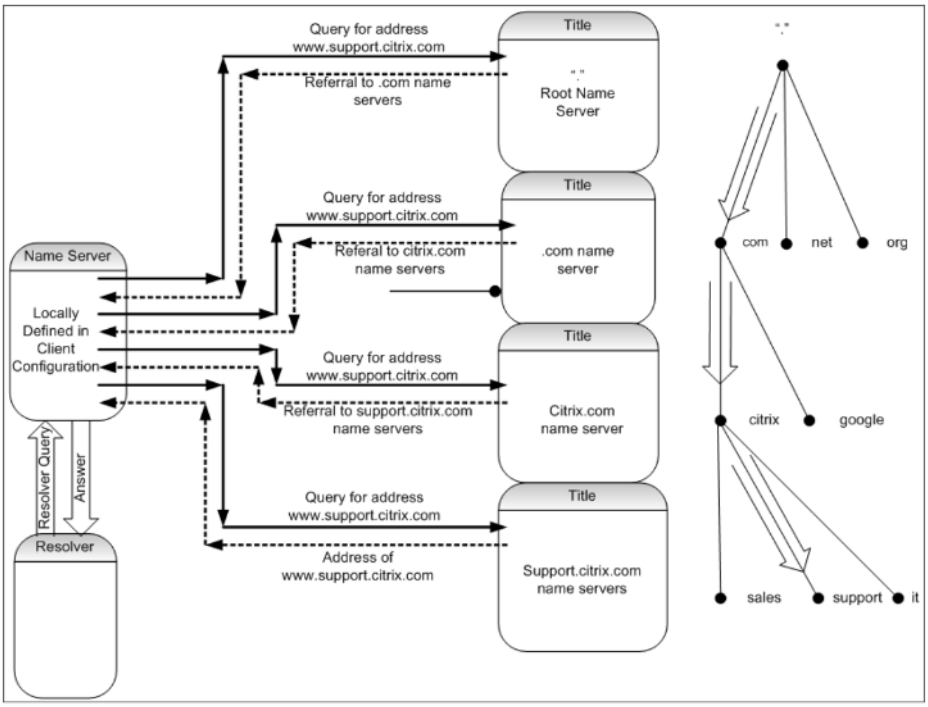


Para delegar correctamente un subdominio, debe asignar autoridad para el subdominio a distintos servidores de nombres. En el ejemplo anterior, `ns1.citrix.com` no contiene información sobre el subdominio `sales.citrix.com`. En su lugar, contiene punteros a los servidores de nombres autorizados para el subdominio `ns1.sales.citrix.com`.

Servidores de nombres raíz y resolución de consultas

Los servidores de nombres raíz conocen las direcciones IP de todos los servidores de nombres autorizados para los dominios de segundo nivel. Si un servidor de nombres no tiene información sobre un dominio determinado en sus propios archivos de datos, solo necesita ponerse en contacto con un servidor raíz para comenzar a atravesar la rama adecuada de la estructura de árbol **DNS** para llegar finalmente al dominio dado. Esto implica una serie de solicitudes a varios servidores de nombres para ayudar con el recorrido del árbol y encontrar el siguiente servidor de nombres autorizado, con el que debe contactarse para obtener más resolución.

En el siguiente diagrama se muestra una solicitud DNS típica, suponiendo que no haya ningún registro almacenado en caché para el nombre solicitado durante la transversal. En el siguiente ejemplo se utiliza una simulación del dominio Citrix.



Consultas recursivas y no recursivas

En el ejemplo anterior se muestran los dos tipos de consultas que pueden producirse.

- Consulta recursiva: La consulta entre el solucionador y el servidor de nombres configurado localmente es recursiva. Esto significa que el servidor de nombres recibe la consulta y no responde al solucionador hasta que se responde completamente a la consulta o se devuelve un error. Si el servidor de nombres recibe una referencia a la consulta, el servidor de nombres sigue la referencia hasta que el servidor de nombres finalmente recibe la respuesta (dirección IP) devuelta.
- Consulta no recursiva: La consulta que el servidor de nombres configurado localmente realiza en el servidor de nombres de nivel de dominio autorizado posterior no es recursiva (o iterativa). Cada solicitud se responde inmediatamente con una referencia a un servidor autorizado de nivel inferior o la respuesta a la consulta, si el servidor de nombres consultado contiene la respuesta en sus archivos de datos o en su caché.

Almacenamiento en caché

Aunque el proceso de resolución está involucrado y podría requerir pequeñas solicitudes a varios hosts, es rápido. Uno de los factores que aumenta la velocidad de la resolución DNS es el almacenamiento en caché. Cada vez que un servidor de nombres recibe una consulta recursiva, es posible que tenga que comunicarse con otros servidores para llegar al servidor autorizado adecuado para la

solicitud específica. Almacena toda la información que recibe para referencia futura. Cuando el siguiente cliente realiza una solicitud similar, como un host diferente pero en el mismo dominio, ya conoce el servidor de nombres autorizado para ese dominio y puede enviar una solicitud directamente allí en lugar de iniciarse en el servidor de nombres raíz.

También se puede almacenar en caché para respuestas negativas, como las consultas de hosts que no existen. En este caso, el servidor no debe consultar al servidor de nombres autorizado del dominio solicitado para averiguar que el host no existe. Para ahorrar tiempo, el servidor de nombres simplemente comprueba la memoria caché y responde con el registro negativo.

Los servidores de nombres no almacenan en caché los registros indefinidamente o, de lo contrario, nunca podrá actualizar las direcciones IP. Para evitar problemas de sincronización, las respuestas DNS contienen un tiempo de vida (TTL). Este campo describe el intervalo de tiempo para el que la caché puede almacenar un registro antes de descartarlo y comprobar con el servidor de nombres autorizado los registros actualizados. Si los registros no han cambiado, el uso de TTL también permite respuestas dinámicas rápidas desde dispositivos que realizan GSLB.

Tipos de registros de recursos

Varios RFC proporcionan una lista completa de los tipos de registros de recursos DNS y su descripción. En la tabla siguiente se enumeran los tipos de registros de recursos comunes.

Tipo de registro de recursos	Descripción	RFC
A	Dirección de host	RFC 1035
N	Un servidor de nombres autoritativo	RFC 1035
MD	Un destino de correo (Obsoleto - usar MX)	RFC 1035
MF	Un reenviador de correo (Obsoleto - usar MX)	RFC 1035
CNAME	El nombre canónico de un alias	RFC 1035
JABONERA	Marca el inicio de una zona de autoridad	RFC 1035
SEMANAS	Descripción de un servicio bien conocida	RFC 1035
PTR	Un puntero de nombre de dominio	RFC 1035
HINFO	Información del host	RFC 1035

Tipo de registro de recursos	Descripción	RFC
MINFO	Información sobre buzones de correo o listas de correo	RFC 1035
MX	Intercambio de correo	RFC 1035
TXT	Cadenas de texto	RFC 1035
AAAA	Dirección IP6	RFC 3596
SRV	Selección de servidores	RFC 2782]

Cómo admite GSLB DNS

GSLB utiliza algoritmos y protocolos que deciden qué dirección IP debe enviarse para una consulta DNS. Los sitios GSLB se distribuyen geográficamente y hay un servidor de nombres autorizado de DNS en cada sitio que se ejecuta como servicio en el dispositivo Citrix ADC. Todos los servidores de nombres de los distintos sitios implicados tienen autoridad para el mismo dominio. Cada uno de los dominios GSLB es un subdominio para el que se configura una delegación. Por lo tanto, los servidores de nombres GSLB son autorizados y pueden utilizar uno de los diversos algoritmos de equilibrio de carga para decidir qué dirección IP devolver.

Se crea una delegación agregando un registro del servidor de nombres para el dominio GSLB en los archivos de base de datos de dominio principal y un registro de direcciones posterior para los servidores de nombres que se utilizan para la delegación. Por ejemplo, si quiere utilizar GSLB para `www.citrix.com`, se puede utilizar el siguiente archivo SOA de enlace para delegar solicitudes en servidores de nombres: Netscaler1 y Netscaler2. `www.citrix.com`

```
###########################################################################

@ IN SOA citrix.com. hostmaster.citrix.com. (
1 ; serial
3h ; refresh
1h ; retry
1w ; expire
1h ) ; negative caching TTL
IN NS ns1
IN NS ns2
IN MX 10 mail

ns1   IN A 10.10.10.10
ns2   IN A 10.10.10.20
```



```
mail  IN A 10.20.20.50

### Old Configuration if www was not delegated to a GSLB name server
www IN A 10.20.20.50

### Updated Configuration
Netscaler1 IN A xxx.xxx.xxx.xxx
Netscaler2 IN A yyy.yyy.yyy.yyy
www IN NS Netscaler1.citrix.com.
www IN NS Netscaler2.citrix.com.
###
IN MX 20 mail2
mail2 IN A 10.50.50.20
################################################################################


<!--NeedCopy-->
```

Entender BIND no es un requisito para configurar DNS. Todas las implementaciones de servidores DNS compatibles tienen un método para crear la delegación equivalente. Los servidores DNS de Microsoft se pueden configurar para la delegación siguiendo las instrucciones de Crear una delegación de zona).

Lo que diferencia a GSLB en el dispositivo Citrix ADC del uso del servicio DNS estándar para distribuir el tráfico es que los sitios GSLB de Citrix ADC intercambian datos mediante un protocolo propietario denominado Metric Exchange Protocol (MEP). Con MEP, los sitios de la GSLB pueden mantener información sobre todos los demás sitios. Cuando se recibe una solicitud DNS, el MEP considera las métricas de GSLB para determinar información como la siguiente:

- Sitio con el menor número de conexiones actuales
- Sitio más cercano al servidor LDNS, que envió la solicitud en función de los tiempos de ida y vuelta (RTT).

Hay varios algoritmos de equilibrio de carga que se pueden utilizar, pero GSLB es un DNS con el cerebro debajo que indica al servidor de nombres (alojado en el dispositivo Citrix ADC) qué dirección debe enviarse según las métricas de los sitios participantes.

Otros beneficios que ofrece GSLB son la capacidad de mantener la persistencia (o afinidad del sitio). Las respuestas a las consultas DNS entrantes se pueden comparar con la dirección IP de origen para determinar si esa dirección se dirigió a un sitio concreto en el pasado reciente. Si es así, se envía la misma dirección en la respuesta DNS para garantizar que se mantenga la sesión del cliente.

Otra forma de persistencia se obtiene a nivel de sitio mediante redireccionamientos HTTP o proxying HTTP. Estas formas de persistencia ocurren después de que se produce la respuesta DNS. Por lo tanto, si recibe una solicitud HTTP en un sitio que contiene una cookie para dirigir la solicitud a otro sitio participante, puede responder con una redirección o enviar la solicitud al sitio correspondiente.

Protocolo de intercambio de métricas

Metric Exchange Protocol (MEP) se utiliza para compartir los datos utilizados en los cálculos de GSLB entre sitios. Mediante conexiones MEP, se intercambian tres tipos de datos. Estas conexiones no tienen por qué estar seguras a través del puerto TCP 3011 o pueden ser seguras mediante SSL a través del puerto TCP 3009.

Se intercambian los tres tipos de datos siguientes y tienen sus propios intervalos y métodos de intercambio.

- **Intercambio de métricas del sitio:** Este es un modelo de intercambio de encuestas. Por ejemplo, si site1 tiene una configuración para los servicios site2, cada segundo sitio1 solicita al sitio2 el estado de los servicios GSLB. Site2 responde con el estado y otros detalles de carga.
- **Intercambio de métricas de red:** Este es el intercambio de información RTT de LDNS, que se utiliza en el algoritmo de equilibrio de carga dinámico de proximidad. Este es un modelo de intercambio push. Cada cinco segundos, cada sitio envía sus datos a otros sitios participantes.
- **Intercambio de persistencia:** es para el intercambio de persistencia SOURCEIP. Este es también un modelo de intercambio push. Cada cinco segundos, cada sitio envía sus datos a otros sitios participantes.

De forma predeterminada, los servicios del sitio se supervisan a través de MEP basándose únicamente en la información de las encuestas. Si vincula monitores en función del intervalo de monitor, el estado se actualiza y puede controlar la frecuencia de las actualizaciones estableciendo el intervalo de supervisión en consecuencia.

Orden de prioridad para los servicios de GSLB

January 21, 2022

La función de orden de prioridad para los servicios le permite priorizar el orden de los servicios o grupos de servicios en función de las preferencias de selección de equilibrio de carga. Puede configurar el orden de prioridad si hace lo siguiente:

- Enlaza un servicio a un servidor virtual GSLB.
- Enlazar un grupo de servicios a un servidor virtual GSLB.
- Enlazar un miembro del grupo de servicios al grupo de servicios GSLB.

Actualmente, puede configurar el orden de prioridad de los servicios mediante los siguientes enfoques. Sin embargo, estos enfoques tienen las siguientes limitaciones:

- Configuración de una cadena de servidores virtuales de reserva: El número de líneas de configuración es alto y debe ejecutar el comando `show` varias veces para conocer el estado de todos los servicios GSLB para cada servidor virtual.
- Configuración de la ubicación preferida: debe crear entradas de ubicación para todos los puntos finales de la aplicación.

La función de orden de prioridad para los servicios aborda las limitaciones anteriores con menos comandos de configuración y le ayuda a realizar la configuración de ubicación preferida sin la necesidad de representar la ubicación de todas las direcciones IP de los servicios GSLB.

Configurar el orden de prioridad para los servicios GSLB

Para configurar el orden de prioridad de los servicios GSLB, el`-order <number>`parámetro se agrega a los comandos bind.

> **Nota:**
>
> El número de pedido más bajo tiene la prioridad más alta.

Comando:

```
bind gslb vserver <vservername> -servicename/servicegroupname <servicename/
servicegroupname> -order <number>
```

Por ejemplo, considere un conjunto de servicios que están enlazados a un servidor virtual GSLB (gv1). Con el
`- order <number>`parámetro, puede priorizar el orden de selección de los servicios de la siguiente manera:

- Conjunto 1 (s1, s2) vinculado a gv1 — orden 1
- Conjunto 2 (s3, s4) vinculado a gv1 — orden 2
- Conjunto 3 (s5, s6) vinculado a gv1 — orden 3

Después de vincular los servicios a gv1 y cuando gv1 recibe el tráfico del cliente, el orden de selección de los servicios es el siguiente:

- El servidor virtual (gv1) selecciona los servicios del conjunto 1 (s1 y s2) con el número de pedido 1, porque a este conjunto se le asigna el número de pedido más bajo. De forma predeterminada, el número de pedido más bajo tiene la prioridad más alta.
- Si todos los servicios del conjunto 1 están ABAJO, gv1 selecciona el conjunto 2 (s3 y s4) con el número de pedido 2.
- Si todos los servicios del conjunto 1 y el conjunto 2 están inactivos, gv1 selecciona el conjunto 3 (s5 y s6) con el número de pedido 3.

Configurar el orden de prioridad para los servicios GSLB mediante la CLI

Para configurar el orden de prioridad de los servicios GSLB, escriba los siguientes comandos en el símbolo del sistema:

1. Agregue sitios GSLB.

```
add gslb site site1 1.1.1.1
add gslb site site2 1.1.1.2
```

2. Agregue un servidor virtual GSLB.

```
add gslb vserver gv1 HTTP
```

3. Agregue los servicios de GSLB.

```
add gslb service gsvc1 1.1.1.3 http 80 -sitename site1
add gslb service gsvc2 1.1.1.4 http 80 -sitename site2
add gslb service gsvc3 1.1.1.5 http 80 -sitename site1
add gslb service gsvc4 1.1.1.6 http 80 -sitename site2
add gslb service gsvc5 1.1.1.7 http 80 -sitename site1
add gslb service gsvc6 1.1.1.8 http 80 -sitename site2
```

4. Establezca el número de pedido y vincule los servicios al servidor virtual GSLB.

```
bind gslb vserver gv1 gsvc1 -order 1
bind gslb vserver gv1 gsvc2 -order 1
bind gslb vserver gv1 gsvc3 -order 2
bind gslb vserver gv1 gsvc4 -order 2
bind gslb vserver gv1 gsvc5 -order 3
bind gslb vserver gv1 gsvc6 -order 3
```

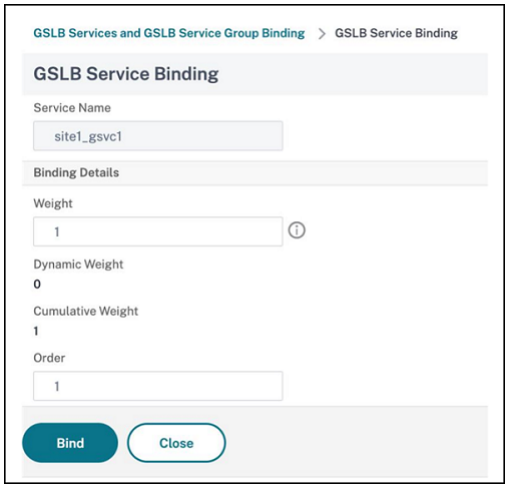
Configurar el orden de prioridad para los servicios GSLB mediante la interfaz gráfica de usuario

Requisitos previos:

- Ha creado sitios GSLB.
- Ha creado un servidor virtual GSLB.
- Ha creado servicios GSLB.

Para configurar el orden de prioridad de los servicios GSLB y vincularlos al servidor virtual GSLB, haga lo siguiente:

1. Vaya a**Administración del tráfico > GSLB > Servidores virtuales**y haga doble clic en el servidor virtual GSLB.
2. En **Servidor virtual GSLB**, en la sección Servicios**GSLB y enlace de grupos de servicios GSLB**, haga clic en **Enlaces de servidor virtual GSLB a servicios**GSLB.
3. En el cuadro de diálogo**Servicios GSLB y enlace de grupos de servicios GSLB**, haga clic en**Agregar enlace**.
4. En el cuadro de diálogo**Enlace de servicios GSLB**, seleccione un servicio.
5. Escriba un número en el campo**Pedido**para establecer el orden de prioridad del servicio.



6. Haga clic en **Vincular**
7. Repita los pasos del 1 al 6 para configurar un número de orden de prioridad diferente para diferentes servicios.

Configurar el orden de prioridad para los servicios GSLB mediante comandos de directiva LB

De forma predeterminada, el número de pedido más bajo tiene la prioridad más alta. Sin embargo, puede diferir este comportamiento predeterminado mediante los nuevos comandos de acción y directiva de LB. Puede configurar el orden de selección de servicios en función del tráfico de clientes entrantes o los datos de los clientes.

Por ejemplo, considere un conjunto de servicios que están enlazados a un servidor virtual GSLB (gv1). Con el- `order <number>`parámetro, ha configurado el orden de prioridad para los servicios de la siguiente manera:

- Conjunto 1 (s1, s2) vinculado a gv1 — orden 1
- Conjunto 2 (s3, s4) vinculado a gv1 — orden 2
- Conjunto 3 (s5, s6) vinculado a gv1 — orden 3

De forma predeterminada, el número de pedido más bajo tiene la prioridad más alta. Por lo tanto, el orden de prioridad predeterminado es 1, 2 y 3 para los servicios del conjunto 1, conjunto 2 y conjunto 3, respectivamente. Sin embargo, para un tráfico de clientes específico, quiere cambiar el orden de prioridad a 3, 1 y 2. Para lograr esto, puede agregar una directiva LB y vincularla a gv1.

Un comando de directiva de LB consta de dos elementos: una regla y una acción. La regla se asocia a una acción, que se lleva a cabo si una solicitud coincide con la regla.

> **Nota:**
>
> Los comandos de directiva LB son comunes para la configuración LB y GSLB y se aplican a las solicitudes administradas por el dispositivo Citrix ADC.

Acción LB

Expresión:

```
add lb action <name> <type> <string>
```

Ejemplo:

```
add lb action act1 -type SELECTIONORDER -value 3 2 1
```

Parámetros:

- `name`: Nombre de la acción.
- `type`: Tipo de acción.
- `string`: valor de la acción especificada.

Directiva de LB

Expresión:

```
add lb policy <name> <rule> <action> <undefaction>
```

Ejemplo:

```
add lb policy pol1 -rule CLIENT.IP.SRC.EQ(8.8.8.8)-action act1
```

Parámetros:

- `name`: Nombre de la directiva.
- `rule`: Una regla se compone de una o más expresiones. La regla se asocia a una acción, que se lleva a cabo si la solicitud coincide con la regla.
- `action`: Se admiten DROP, NOLBACTION y RESET.

- `undefaction`: El dispositivo Citrix ADC genera un evento indefinido (evento UNDEF) cuando una solicitud no coincide con una directiva. Puede usar el `set lb param -undefAction <action>`comando para establecer la acción indefinida. Puede asignar estas acciones a un evento indefinido: DROP, NOLBACTION y RESET.

Consideremos un ejemplo en el que agrega una acción LB, una directiva LB y vincula la directiva a un servidor virtual GSLB (gv1) de la siguiente manera:

```
add lb action act1 -type SELECTIONORDER -value 3 1 2

add lb policy pol1 -rule CLIENT.IP.SRC.EQ(8.8.8.8)-action act1

bind gslb vserver gv1 -policyName pol1 -priority 20 - gotoPriorityExpression
 END -type REQUEST
```

La regla selecciona el tráfico del cliente que coincide con la dirección IP y envía ese tráfico a gv1. `8.8.8.8` El tipo de acción LB (`SELECTIONORDER`) define el orden de selección de servicios. Después de vincular la directiva LB a gv1, y cuando gv1 recibe el tráfico del cliente desde la dirección IP`8.8.8.8`, los servicios se seleccionan en el siguiente orden:

1. El servidor virtual (gv1) selecciona los servicios en el conjunto 3 (s5 y s6) con el orden de prioridad 3.
2. Si todos los servicios del conjunto 3 están ABAJO, gv1 selecciona el conjunto 1 (s1 y s2) con el orden de prioridad 2.
3. Si todos los servicios del conjunto 3 y el conjunto 2 están inactivos, el gv1 selecciona el conjunto 1 (s1 y s2) con el pedido 1.

Configurar el orden de prioridad para los servicios GSLB con comandos de directiva LB mediante la CLI

Para configurar el orden de prioridad de los servicios GSLB mediante comandos de directiva LB, escriba los siguientes comandos en el símbolo del sistema:

1. Agregue una acción LB.

   ```
   add lb action act1 -type SELECTIONORDER -value 3 1 2
   ```

2. Agregue una directiva de LB.

   ```
   add lb policy pol1 -rule CLIENT.IP.SRC.EQ(8.8.8.8)-action act1
   ```

3. Agregue sitios GSLB.

   ```
   add gslb site site1 1.1.1.1

   add gslb site site2 1.1.1.2
   ```


4. Agregue un servidor virtual GSLB.

```
add gslb vserver gv1 HTTP
```

5. Enlazar la directiva LB al servidor virtual GSLB.

```
bind gslb vserver gv1 -policyName pol1 -priority 20 - gotoPriorityExpression
 END -type REQUEST
```

6. Agregue los servicios de GSLB.

```
add gslb service gsvc1 1.1.1.3 http 80 -sitename site1

add gslb service gsvc2 1.1.1.4 http 80 -sitename site2

add gslb service gsvc3 1.1.1.5 http 80 -sitename site1

add gslb service gsvc4 1.1.1.6 http 80 -sitename site2

add gslb service gsvc5 1.1.1.7 http 80 -sitename site1

add gslb service gsvc6 1.1.1.8 http 80 -sitename site2
```

7. Establezca el orden y vincule los servicios al servidor virtual GSLB.

```
bind gslb vserver gv1 gsvc1 -order 1

bind gslb vserver gv1 gsvc2 -order 1

bind gslb vserver gv1 gsvc3 -order 2

bind gslb vserver gv1 gsvc4 -order 2

bind gslb vserver gv1 gsvc5 -order 3

bind gslb vserver gv1 gsvc6 -order 3
```

Configurar el orden de prioridad para los servicios GSLB con los comandos de directiva LB mediante la interfaz gráfica de usuario

Requisitos previos:

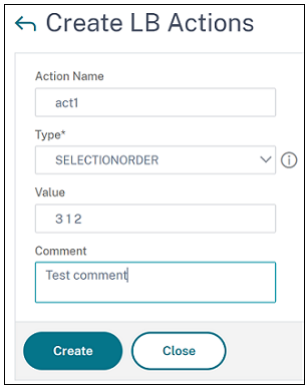
- Ha creado sitios GSLB.
- Ha creado un servidor virtual GSLB.
- Ha creado servicios.

Paso 1: crear una acción LB:

1. Vaya a **AppExpert > LB > Acciones**.
2. En**LB Actions**, haga clic en**Agregar**.
3. En el cuadro de diálogo**Crear acciones LB**, especifique los valores para los siguientes parámetros:

- **Nombre de acción**: act1
- **Tipo**: SELECTIONORDER
- **Valor**: 3 1 2

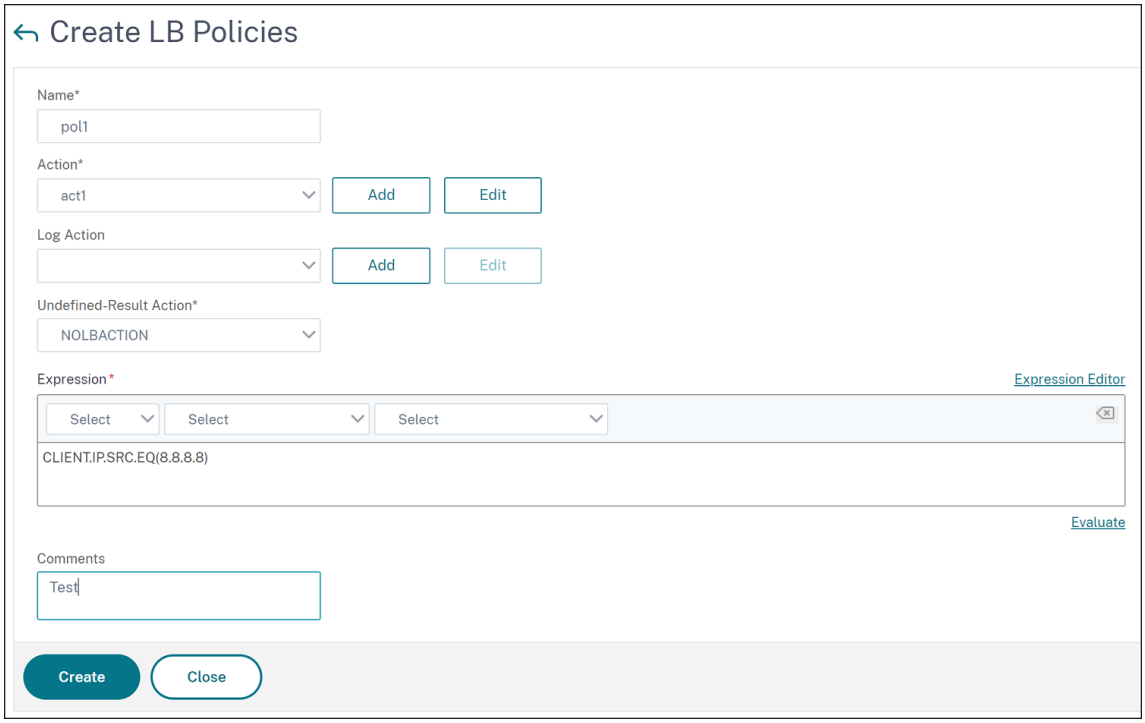
> **Nota:**
>
> Los números del campo **Valor**están separados por un espacio.



4. Haga clic en **Crear**.

Paso 2: Cree una directiva de LB:

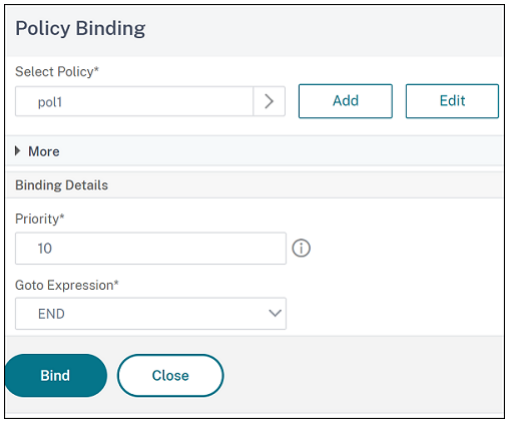
1. Vaya a **AppExpert > LB > Directivas**.
2. En**Directivas de LB**, haga clic en**Agregar**.
3. En el cuadro de diálogo**Crear directivas LB**, especifique los valores para los siguientes parámetros:
   - **Nombre**: pol1
   - **Acción**: act1
   - **Acción de resultado indefinido**: NOLBACTION
   - **Expresión**: CLIENT.IP.SRC.EQ (8.8.8.8)



4. Haga clic en**Crear**.

Paso 3: Enlazar la directiva LB al servidor virtual GSLB:

1. Vaya a**Administración del tráfico > GSLB > Servidores virtuales**y haga doble clic en el servidor virtual GSLB.
2. En **Servidor virtual GSLB**, en la sección **Configuración avanzada**, haga clic en**Directivas**.
3. En la sección**Directivas**, haga clic en **Enlace de directivas LB de servidor virtual GSLB**.
4. En el cuadro de diálogo **Enlace de directivas**, especifique los valores para los siguientes parámetros:
   - **Seleccione la directiva**: pol 1
   - **Prioridad**: 10
   - **Expresión de Goto**: END



5. Haga clic en **Bind**.

Paso 4: Configurar el orden de prioridad para los servicios GSLB:

Para configurar el orden de prioridad para GSLB, consulte el procedimiento **Configurar el orden de prioridad para los servicios GSLB mediante la interfaz gráfica** de usuario.

Configuración de persistencia para los servicios

Si la persistencia está configurada para un servicio, siempre se da preferencia a la persistencia, de forma predeterminada.

Por ejemplo, considere un servicio con persistencia configurada y orden de prioridad 1. Si un servicio con orden de prioridad 0 está ACTIVO, entonces siempre se da preferencia al servicio con orden de prioridad 1.

Sin embargo, puede anular este comportamiento predeterminado con el siguiente comando de la CLI:

```
set gslb param -overridePersistencyforOrder<YES/NO>
```

Consideremos el siguiente ejemplo:

Un conjunto de servicios se enlaza a un servidor virtual GSLB (gv1) con el siguiente orden de prioridad:

- Conjunto 1 (s1, s2) vinculado a gv1 — orden 1
- Conjunto 2 (s3, s4) vinculado a gv1 — orden 2

Escriba el siguiente comando en el símbolo del sistema para anular la persistencia:

```
set gslb parameter -overridePersistencyforOrder YES
```

Si el conjunto 1 (los servicios con persistencia están configurados) está ABAJO, los servicios establecidos 2 gestionan todas las solicitudes hasta que los servicios del conjunto 1 estén ACTIVOS. Se crea una entrada de persistencia para la prioridad 2.

Supongamos que después de algún tiempo, los servicios del conjunto 1 están ACTIVOS. Ahora, los servicios set 1 y set 2 están ARRIBA para gestionar las solicitudes. En este caso, se toman nuevas deci-

siones de equilibrio de carga a medida que los servicios de orden superior están ACTIVOS. La entrada de persistencia se anula con una nueva entrada de equilibrio de carga.

Alternar prioridad

Con la función de alternancia de prioridad, puede alternar todo el tráfico a un servicio de baja prioridad durante la actualización de la versión para un servicio con un orden de prioridad más alto. Puede usar los siguientes comandos para alternar la prioridad:

- `set gslb vserver -toggleorder <Ascending/Descending>`
- `set gslb vserver v1 –orderthreshold 80`

Por ejemplo, consideremos que hay dos servicios con las siguientes prioridades:

- Service 1- order 0
- Servicio 2 — pedido 1

De forma predeterminada, el servicio 1 gestiona todo el tráfico. Si el servicio 1 necesita actualizarse, entonces el tráfico debe reencaminarse al servicio 2.

En el símbolo del sistema, escriba los siguientes comandos para alternar la prioridad:

```
set gslb vserver -toggleorder Descending
```

De forma predeterminada, 0 tiene una prioridad más alta. Sin embargo, después de la conmutación de prioridades, 1 se considera una prioridad más alta. Si la entrada de persistencia está presente para el servicio, el comportamiento de preferencia de persistencia es el que se explica en la sección **Configuración de persistencia para los servicios**.

Recomendaciones de actualización para la implementación de GSLB

October 5, 2021

En esta sección se proporcionan recomendaciones sobre la secuencia en la que los nodos GSLB deben actualizarse en varias configuraciones de GSLB. También aborda algunas preguntas frecuentes.

Nota: El dispositivo Citrix ADC desde el que se inicia la sincronización GSLB se denomina “sitio principal” y los sitios GSLB en los que se copia la configuración como “sitios subordinados”.

Antes de iniciar el proceso de actualización, lea los requisitos previos mencionados en los temas siguientes:

- Antes de comenzar
- Actualice un par de alta disponibilidad.
- Actualizar un clúster.

Puntos a tener en cuenta al actualizar las configuraciones de GSLB

- En una configuración de alta disponibilidad, primero actualice los sitios subordinados y, a continuación, el sitio principal.
- En una configuración de alta disponibilidad, es posible que los estados de servicio no se propaguen de un nodo principal de compilación anterior a un nodo secundario de compilación más reciente. Sin embargo, si las compilaciones son de versiones diferentes, pero tienen la misma versión de alta disponibilidad, es posible que el estado del servicio siga propagándose.
- Si GSLB está configurado dentro de un clúster, primero actualice los nodos no propietarios y, a continuación, actualice el nodo propietario. Si hay un sitio o varios sitios en un clúster, siga la misma secuencia de actualización en cada uno de los sitios.
- Habilite las nuevas funciones de GSLB solo después de actualizar todos los nodos a una versión más reciente.
- Actualiza todos los nodos GSLB a la última versión. No hay ningún impacto funcional en las funciones disponibles cuando algunos de los nodos GSLB utilizan una versión anterior y algunos de los nodos GSLB se actualizan a una versión más reciente.

Preguntas frecuentes

- **¿Se propagan los estados del servicio GSLB cuando las instancias ejecutan versiones de software diferentes?**

  GSLB MEP funciona cuando las instancias se ejecutan en diferentes versiones y los estados de servicio de GSLB se propagan en los sitios de GSLB. No hay ningún impacto en la comunicación MEP cuando las instancias ejecutan versiones diferentes tras una actualización.

- **¿Se recomienda realizar cambios de configuración durante una actualización?**

  In a GSLB setup, when a main site is being upgraded, it is not recommended to do configuration changes on any other GSLB nodes.

Recursos conexos

Los siguientes recursos proporcionan información sobre la actualización de una instancia de Citrix ADC mediante Citrix ADM:

- 10 formas en que el servicio Citrix ADM admite actualizaciones más sencillas de Citrix ADC
- Usar el servicio Citrix ADM para actualizar instancias de Citrix ADC
- Utilice el software Citrix ADM para actualizar las instancias de Citrix ADC

Caso de uso: Implementación de un grupo de servicios de escala automática basado en nombres de dominio

August 20, 2021

> **Sugerencia**
>
> Para obtener información sobre los grupos de servicios GSLB, consulte Configuración de un grupo de servicios GSLB.

Caso de implementación

Dos centros de datos se implementan en dos regiones de AWS, uno en Sydney y otro en Virginia del Norte. Otro centro de datos se implementa en Azure. Se utiliza un ELB de AWS en cada región de AWS para equilibrar la carga de los servidores de aplicaciones. ALB se utiliza para Azure para equilibrar la carga del servidor de aplicaciones. Los dispositivos Citrix ADC se configuran para GSLB para los ELB y ALB mediante el grupo de servicios de escalado automático basado en nombres de dominio GSLB.

> **Importante**
>
> Debe configurar los grupos de seguridad necesarios en AWS y adjuntarlos a la instancia de GSLB. El puerto 53 debe estar permitido en las reglas de entrada y salida del grupo de seguridad. Además, los puertos (3009 o 3011 dependiendo de la configuración MEP segura) para la comunicación MEP deben estar abiertos. Para la supervisión de aplicaciones, se deben permitir los puertos correspondientes en las reglas de salida del grupo de seguridad.

Los pasos de configuración para el caso de implementación anterior y los comandos CLI correspondientes son los siguientes:

1. Crear centros de datos (representados por sitios GSLB).

   ```
   add gslb site aws-sydney 192.0.2.2

   add gslb site aws-nvirginia 198.51.100.111

   add gslb site alb-southindia 203.0.113.6
   ```

2. Agregue un servidor de nombres con la dirección IP de la Gateway DNS donde se agrega el nodo GSLB. Esto debe hacerse en todos los centros de datos.

   ```
   add dns nameServer 8.8.8.8
   ```

3. Agregar servidores para ELB y ALB.

   ```
   add server aws-sydney_server lb-sydney-1052691850.ap-southeast-2.elb.
   amazonaws.com
   ```



```
add server aws-nvirginia_server LB-nvirginia-860559595.us-east-1.elb.
amazonaws.com

add server alb-southindia_server alb.southindia.cloudapp.azure.com
```

4. Agregue grupos de servicios de escalado automático de GSLB para cada ELB y ALB y vincule cada servidor al grupo de servicios respectivo.

```
add gslb serviceGroup aws-nvirginia_sg HTTP -autoScale DNS -siteName
aws-nvirginia

add gslb serviceGroup aws-sydney_sg HTTP -autoScale DNS -siteName aws-
sydney

add gslb serviceGroup alb-southindia_sg HTTP -autoScale DNS -siteName
alb-southindia

bind gslb serviceGroup aws-nvirginia_sg aws-nvirginia_server 80

bind gslb serviceGroup aws-sydney_sg aws-sydney_server 80

bind gslb serviceGroup alb-southindia_sg alb-southindia_server 80
```

5. Agregue un servidor virtual GSLB y vincule el dominio de la aplicación y los grupos de servicios a este servidor virtual.

```
add gslb vserver gv1 HTTP

bind gslb vserver gv1 -serviceGroupName aws-nvirginia_sg

bind gslb vserver gv1 -serviceGroupName aws-sydney_sg

bind gslb vserver gv1 -serviceGroupName alb-southindia_sg
```

Caso de uso: Implementación del grupo de servicios GSLB basado en direcciones IP

August 20, 2021

> **Sugerencia**
>
> Para obtener información sobre los grupos de servicios GSLB, consulte Configuración de un grupo de servicios GSLB.

Caso de implementación

Si hay varias aplicaciones alojadas en el mismo servidor de aplicaciones, el GSLB debe sondear estas aplicaciones para ver si las aplicaciones responden o no. Si una aplicación no responde, se debe dirigir

al usuario al servidor en el que está UP la aplicación. Además, si una de las aplicaciones es DOWN, entonces el servidor no debe estar marcado como DOWN, porque las otras aplicaciones están UP.

En el siguiente ejemplo, varias aplicaciones (HTTPS) están alojadas en un servidor en cada sitio GSLB y, por lo tanto, todas estas aplicaciones se resuelven en una dirección IP del sitio respectivo.

Con los grupos de servicios GSLB, puede tener el mismo servidor con una dirección IP y un puerto enlazados a varios grupos de servicios donde cada grupo de servicios representa una aplicación diferente.

Un monitor específico de la aplicación está enlazado a los grupos de servicios que marcan el grupo de servicios como DOWN si la aplicación está DOWN. Por lo tanto, cada vez que una aplicación está DOWN, solo esa aplicación se saca de la configuración y no del servidor.

```
```
add gslb serviceGroup app1_site1 HTTP -maxClient 0 -cip DISABLED -
    cltTimeout 180 -svrTimeout 360 -siteName s1

add gslb serviceGroup app2_site1 HTTP -maxClient 0 -cip DISABLED -
    cltTimeout 180 -svrTimeout 360 -siteName s1

add gslb serviceGroup app1_site2 HTTP -maxClient 0 -cip DISABLED -
    cltTimeout 180 -svrTimeout 360 -siteName s2

add gslb serviceGroup app2_site2 HTTP -maxClient 0 -cip DISABLED -
    cltTimeout 180 -svrTimeout 360 -siteName s2

add lb monitor http_app2 HTTP -respCode 200 -httpRequest "GET /testsite
    /app2.html"

add lb monitor http_app1 HTTP -respCode 200 -httpRequest "GET /testsite
    /app1.html"

bind gslb serviceGroup app1_site1 192.0.2.140 80

bind gslb serviceGroup app1_site1 -monitorName http_app1

bind gslb serviceGroup app2_site1 192.0.2.140 80

bind gslb serviceGroup app2_site1 -monitorName http_app2

bind gslb serviceGroup app1_site2 192.0.2.142 80

bind gslb serviceGroup app1_site2 -monitorName http_app1
```

 
```

```
25
26 bind gslb serviceGroup app2_site2 192.0.2.142 80
27
28 bind gslb serviceGroup app2_site2 -monitorName http_app2
29 <!--NeedCopy--> ```
```

Artículos de procedimientos

January 19, 2021

Los artículos de procedimientos de GSLB contienen información sobre algunas de las configuraciones importantes de GSLB, como personalizar la configuración de GSLB, configurar conexiones persistentes, recuperación ante desastres, etc.

Personalización de la configuración de GSLB

Configuración de Conexiones Persistentes

Administración de conexiones de cliente

Configurar GSLB para la proximidad

Protección de la configuración de GSLB contra fallos

Configuración de GSLB para recuperación ante desastres

Anulado del comportamiento de proximidad estática mediante la configuración de ubicaciones preferidas

Configuración de la selección de servicios GSLB mediante Content Switching

Configuración del equilibrio de carga global del servidor para consultas DNS con registros NAPTR

Uso de la opción de subred cliente EDNS0 para el equilibrio de carga global del servidor

Ejemplo de una configuración principal-secundario completa mediante el protocolo de intercambio de métricas

Personalizar la configuración de GSLB

August 20, 2021

Una vez que la configuración básica de GSLB esté operativa, puede personalizarla modificando el ancho de banda de un servicio GSLB, configurando servicios GSLB basados en CNAME, proximidad

estática, RTT dinámico, conexiones persistentes o pesos dinámicos para servicios, o cambiando el método GSLB.

También puede configurar la supervisión de los servicios GSLB para determinar sus estados.

Esta configuración depende de la implementación de la red y de los tipos de clientes que espera conectarse a los servidores.

Modificar las conexiones máximas o el ancho de banda máximo para un servicio GSLB

Puede restringir el número de clientes nuevos que pueden conectarse simultáneamente a un servidor virtual de equilibrio de carga o de cambio de contenido configurando el número máximo de clientes y/o el ancho de banda máximo para el servicio GSLB que representa el servidor virtual.

Para modificar el máximo de clientes o ancho de banda de un servicio GSLB mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba el comando siguiente para modificar el número máximo de conexiones de cliente o el ancho de banda máximo de un servicio GSLB y compruebe la configuración:

```
set gslb service <serviceName> [-maxClients <positive_integer>] [-
   maxBandwidth <positive_integer>]
show gslb service <serviceName>
<!--NeedCopy-->
```

Ejemplo:

```
set glsb service Service-GSLB-1 -maxBandwidth 100 -maxClients 100
show gslb service Service-GSLB-1
<!--NeedCopy-->
```

Para modificar el máximo de clientes o ancho de banda de un servicio GSLB mediante la utilidad de configuración

1. Vaya a **Administración del tráfico** > **GSLB** > **Servicios**y haga doble clic en un servicio.
2. Haga clic en la sección **Otros ajustes** y defina los siguientes parámetros:
   - Máximo de clientes: MaxClients
   - Ancho de banda máximo: Ancho de banda máximo

Crear servicios GSLB basados en CNAME

Para configurar un servicio GSLB, puede utilizar la dirección IP del servidor o un nombre canónico del servidor. Si quiere ejecutar varios servicios (como un servidor FTP y un servidor web, cada uno en puertos diferentes) desde una única dirección IP o ejecutar varios servicios HTTP en el mismo puerto, con nombres diferentes, en el mismo host físico, puede utilizar nombres canónicos (CNAMES) para los servicios.

Por ejemplo, puede tener dos entradas en DNS como ftp.example.com y www.example.com para servicios FTP y servicios HTTP en el mismo dominio, example.com. Los servicios GSLB basados en CName son útiles en una configuración de resolución de dominios multinivel o en el equilibrio de carga de dominios multinivel. La configuración de un servicio GSLB basado en CNAME también puede ayudar si es probable que cambie la dirección IP del servidor físico.

Si configura servicios GSLB basados en CNAME para un dominio GSLB, cuando se envía una consulta para el dominio GSLB, el dispositivo Citrix ADC proporciona un CNAME en lugar de una dirección IP. Si el registro A para este registro CNAME no está configurado, el cliente debe consultar el dominio CNAME para obtener la dirección IP. Si se configura el registro A para este registro CNAME, el dispositivo Citrix ADC proporciona al CNAME el registro A correspondiente (dirección IP). El dispositivo Citrix ADC controla la resolución final de la consulta DNS, según lo determinado por el método GSLB. Los registros CNAME se pueden mantener en un dispositivo Citrix ADC diferente o en un sistema de terceros.

En un servicio GSLB basado en direcciones IP, el estado de un servicio viene determinado por el estado del servidor que representa. Sin embargo, un servicio GSLB basado en CNAME tiene su estado establecido en UP de forma predeterminada; la dirección IP (VIP) del servidor virtual o el protocolo de intercambio de métricas (MEP) no se utilizan para determinar su estado. Si un monitor basado en escritorio está enlazado a un servicio GSLB basado en CName, el estado del servicio se determina de acuerdo con el resultado de los sondeos del monitor.

Puede enlazar un servicio GSLB basado en CNAME solo a un servidor virtual GSLB que tenga el tipo de registro DNS como CNAME. Además, un dispositivo Citrix ADC puede contener como máximo un servicio GSLB con una entrada CNAME determinada.

Las siguientes son algunas de las funciones admitidas para un servicio GSLB basado en CName:

- Se admite la afinidad de sitio basada en directivas GSLB, con CNAME como ubicación preferida.
- Se admite la persistencia de IP de origen. La entrada de persistencia contiene la información CNAME en lugar de la dirección IP y el puerto del servicio seleccionado.

Las siguientes son las limitaciones de los servicios GSLB basados en CName:

- No se admite la persistencia del sitio, ya que el servicio al que hace referencia un CNAME puede estar presente en cualquier ubicación de terceros.
- No se admite la respuesta de varias direcciones IP porque un dominio no puede tener varias entradas CNAME.

- Hash IP de origen y Round Robin son los únicos métodos de equilibrio de carga admitidos. No se admite el método de proximidad estática porque un CNAME no está asociado a una dirección IP y la proximidad estática solo se puede mantener de acuerdo con las direcciones IP.

Nota: La función Vacy-Down-Response debe habilitar en el servidor virtual GSLB al que vincula el servicio GSLB basado en CName. Si habilita la función de respuesta vaciada, cuando un servidor virtual GSLB está DOWN o inhabilitado, la respuesta a una consulta DNS, para los dominios vinculados a este servidor virtual, contiene un registro vacío sin ninguna dirección IP, en lugar de un código de error.

Para crear un servicio GSLB basado en CNAME mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
1 add gslb service <serviceName> -cnameEntry <string> -siteName <string>
2 <!--NeedCopy-->
```

Ejemplo:

```
1 add gslb service Service-GSLB-1 -cnameEntry transport.mycompany.com -
     siteName Site-GSLB-East-Coast
2 add gslb service Service-GSLB-2 -cnameEntry finance.mycompany.com -
     siteName Site-GSLB-West-Coast
3 <!--NeedCopy-->
```

Para crear un servicio GSLB basado en CName mediante la utilidad de configuración

1. Vaya a **Administración de Tráfico** > **GSLB** > **Servicios**.
2. Cree un servicio y establezca **Tipo en Base de nombre canónico**.

Configurar el estado fuera de servicio de transición (TROFS) en GSLB

Cuando configura la persistencia en un servidor virtual GSLB al que está enlazado un servicio, el servicio continúa atendiendo las solicitudes del cliente incluso después de inhabilitarlo, aceptando nuevas solicitudes o conexiones solo para respetar la persistencia. Después de un período de tiempo configurado, conocido como período de apagado estable, no se dirigen nuevas solicitudes o conexiones al servicio y se cierran todas las conexiones existentes.

Al inhabilitar un servicio, puede especificar un período de apagado estable, en segundos, mediante el argumento delay. Durante el período de apagado estable, si el servicio está enlazado a un servidor virtual, su estado aparece como Fuera de servicio.

Configurar pesos dinámicos para servicios

En una red típica, hay servidores que tienen una mayor capacidad de tráfico que otros. Sin embargo, con una configuración de equilibrio de carga regular, la carga se distribuye uniformemente entre todos los servicios, aunque los diferentes servicios representan servidores con capacidades diferentes.

Para optimizar los recursos de GSLB, puede configurar pesos dinámicos en un servidor virtual de GSLB. Los pesos dinámicos pueden basarse en el número total de servicios enlazados al servidor virtual o en la suma de los pesos de los servicios individuales enlazados al servidor virtual. La distribución del tráfico se basa entonces en los pesos configurados para los servicios.

Cuando se configuran pesos dinámicos en el servidor virtual GSLB, las solicitudes se distribuyen según el método de equilibrio de carga, el peso del servicio GSLB y el peso dinámico. El producto del peso del servicio GSLB y el peso dinámico se conoce como el peso acumulado. Por lo tanto, cuando se configura el peso dinámico en el servidor virtual GSLB, las solicitudes se distribuyen sobre la base del método de equilibrio de carga y el peso acumulado.

Cuando el peso dinámico de un servidor virtual está inhabilitado, el valor numérico se establece en 1. Esto garantiza que el peso acumulado sea un entero distinto de cero en todo momento.

El peso dinámico puede basarse en el número total de servicios activos enlazados a servidores virtuales de equilibrio de carga o en los pesos asignados a los servicios.

Considere una configuración con dos sitios GSLB configurados para un dominio y cada sitio tiene dos servicios que pueden servir al cliente. Si un servicio en cualquiera de los sitios falla, el otro servidor de ese sitio tiene que manejar el doble de tráfico que un servicio en el otro sitio. Si el peso dinámico se basa en el número de servicios activos, el sitio con ambos servicios activos tiene el doble de peso que el sitio con un servicio caído y, por lo tanto, recibe el doble de tráfico.

Alternativamente, considere una configuración en la que los servicios del primer sitio representen servidores que son dos veces más potentes que los servidores del segundo sitio. Si el peso dinámico se basa en los pesos asignados a los servicios, se puede enviar el doble de tráfico al primer sitio que al segundo.

Nota: Para obtener más información sobre la asignación de ponderaciones a servicios de equilibrio de cargas, consulte Asignación de ponderaciones a servicios.

Como ejemplo de cómo se calcula el peso dinámico, considere un servidor virtual GSLB que tiene un servicio GSLB vinculado a él. El servicio GSLB representa un servidor virtual de equilibrio de carga que a su vez tiene dos servicios vinculados a él. El peso asignado al servicio GSLB es 3. Los pesos asignados a los dos servicios son 1 y 2 respectivamente. En este ejemplo, cuando el peso dinámico se establece en:

- **Inhabilitado: El**peso acumulado del servidor virtual GSLB es el producto del peso dinámico (inhabilitado = 1) y el peso del servicio GSLB (3), por lo que el peso acumulado es 3.

- **SERVICECOUNT**: El recuento es la suma del número de servicios vinculados a los servidores virtuales de equilibrio de carga correspondientes al servicio GSLB (2), y el peso acumulado es el producto del peso dinámico (2) y el peso del servicio GSLB (3), que es 6.
- **SERVICEWEIGHT**: El peso dinámico es la suma de los pesos de los servicios vinculados a los servidores virtuales de equilibrio de carga correspondientes al servicio GSLB (3), y el peso acumulado es el producto del peso dinámico (3) y el peso del servicio GSLB (3), que es 9.

Nota: Los pesos dinámicos no son aplicables cuando se configuran servidores virtuales de cambio de contenido.

Para configurar un servidor virtual GSLB para que utilice pesos dinámicos mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
set gslb vserver <name> -dynamicWeight SERVICECOUNT | SERVICEWEIGHT
<!--NeedCopy-->
```

Ejemplo:

```
set gslb vserver vserver-GSLB-1 -dynamicWeight SERVICECOUNT
<!--NeedCopy-->
```

Para configurar el servidor virtual GSLB para que utilice pesos dinámicos mediante la utilidad de configuración

1. Vaya a Administración del tráfico > GSLB > Servidores virtuales, haga doble clic en el servidor virtual GSLB cuyo método quiere cambiar (por ejemplo, VServer-GSLB-1).
2. Haga clic en la sección **Método** y, en la lista desplegable **Peso dinámico**, seleccione **SERVICECOUNT** o **SERVICEWEIGHT**.

Cómo configurar la persistencia en GSLB

August 20, 2021

La persistencia garantiza que una serie de solicitudes de cliente para un nombre de dominio determinado se envíe al mismo centro de datos en lugar de equilibrarse la carga. Si la persistencia está config-

urada para un dominio determinado, tiene prioridad sobre el método GSLB configurado. Puede utilizar la persistencia para implementaciones en las que una información relacionada con una transacción de cliente se almacena localmente en una instancia, que ha servido las solicitudes iniciales. Por ejemplo, las implementaciones para comercio electrónico que utiliza un carrito de compras, donde el servidor necesita mantener el estado de la conexión para realizar el seguimiento de la transacción. El dispositivo Citrix ADC selecciona un centro de datos para procesar una solicitud de cliente. Con la persistencia habilitada, reenvía la misma dirección IP del centro de datos seleccionado para todas las solicitudes posteriores del Sistema de nombres de dominio (DNS). Si una sesión de persistencia apunta a un centro de datos que está DESACTIVADO, el dispositivo Citrix ADC utiliza el método GSLB configurado para seleccionar un nuevo centro de datos. A continuación, se vuelve persistente para solicitudes posteriores del cliente.
Para la persistencia en GSLB, se debe configurar el mismo conjunto de identificadores de persistencia (PersisID) en los servidores virtuales GSLB en todos los centros de datos. El módulo GSLB utiliza el identificador de persistencia para identificar de forma única un servidor virtual GSLB. Cuando la persistencia de IP de origen está habilitada en el servidor virtual GSLB, las sesiones de persistencia también se intercambian como parte del intercambio de métricas. Para que el dispositivo Citrix ADC admita la persistencia entre sitios, la configuración relacionada con la persistencia debe realizarse en todos los sitios GSLB participantes. Citrix recomienda la persistencia en GSLB para aplicaciones con estado, lo que requiere que los clientes se reconecten a la misma instancia de aplicación para las solicitudes posteriores.

Puede lograr la persistencia en GSLB de las siguientes maneras:

- Persistencia en el servidor virtual GSLB
- Persistencia del sitio en los servicios GSLB

Persistencia en el servidor virtual GSLB

La persistencia en el servidor virtual GSLB se utiliza durante las solicitudes DNS. La dirección IP de origen de la solicitud DNS se utiliza para crear una sesión de persistencia entre el cliente y el centro de datos. Los clientes DNS son generalmente el DNS local (LDNS) o las puertas de enlace DNS que sirven como proxy de un conjunto de clientes que están detrás de ellos (en ISP). La persistencia en un servidor virtual GSLB es independiente del protocolo de aplicación.
En general, se configuran varias puertas de enlace DNS o Servidores de nombres de dominio local (LDNS) en la red cliente. Citrix recomienda configurar una máscara de persistencia adecuada porque para las solicitudes DNS posteriores, independientemente de los dispositivos LDNS ascendentes utilizados para conectarse al dispositivo ADC, el cliente puede persistir en el mismo centro de datos, que había servido las solicitudes anteriores. Después de crear la sesión de persistencia para una dirección IP LDNS, todos los clientes finales que se conectan con ese LDLN reciben la misma dirección IP del centro de datos.

Persistencia del sitio en los servicios GSLB

La persistencia del sitio se hace efectiva mientras se procesan las solicitudes de aplicación. La persistencia del sitio solo funciona para el tráfico HTTP y HTTPS porque la persistencia se logra mediante la cookie HTTP. Como las cookies se mantienen en clientes HTTP (exploradores web), da visibilidad a los clientes que se encuentran detrás de las puertas de enlace DNS. Cuando utiliza cookies para lograr la persistencia de los clientes, no se consumen recursos en el dispositivo ADC para cada cliente entrante. Cuando introduce un servicio GSLB DOWN con un tiempo de demora, el servicio entra en la transición al estado fuera de servicio (TROFS). La persistencia se admite siempre y cuando el servicio esté en estado ACTIVO o TROFS. Es decir, si el mismo cliente envía una solicitud para el mismo servicio dentro del tiempo de demora especificado después de que un servicio se marca TROFS, el mismo sitio GSLB (centro de datos) presta servicios a la solicitud.

Si accede a una aplicación a través de un alias, asegúrese de que el registro CNAME también está configurado en el dispositivo Citrix ADC. En una topología principal-secundario, la persistencia del sitio no funciona cuando se accede a una aplicación a través de un alias.

> Nota
>
> Si el proxy de conexión se especifica como método de persistencia del sitio y también quiere configurar la persistencia en servidores virtuales LB, no se recomienda la persistencia de IP de origen. Cuando se realiza el proxy de la conexión, se utiliza una dirección IP propiedad del dispositivo ADC, y no la dirección IP real del cliente.
> Configure una persistencia adecuada, que no utilice la IP de origen de la solicitud HTTP (S) para identificar al cliente, por ejemplo, la persistencia de cookies o la persistencia basada en reglas.

Configurar la persistencia en función de la dirección IP de origen

Si la persistencia IP de origen está configurada en el servidor virtual GSLB, se crean sesiones de persistencia para la dirección IP de origen de la solicitud DNS. Dependiendo de la función Subred de cliente extendido (ECS), la dirección IP de origen de la solicitud DNS se toma de cualquiera de las siguientes opciones:

- La IP de origen en el encabezado IP del paquete de solicitud DNS entrante
- La opción ECS de la solicitud DNS Para obtener más información sobre ECS, consulte Utilizar la opción de subred cliente EDNS0 para el equilibrio de carga global del servidor.

Las sesiones de persistencia de un cliente duran hasta el tiempo de espera de persistencia. Una vez expirado el período de tiempo de espera, se borran las sesiones de persistencia existentes. Para solicitudes posteriores, se toma una nueva decisión GSLB y se puede seleccionar una dirección IP de servicio GSLB diferente.
La persistencia de IP de origen en el servidor virtual GSLB y la persistencia del sitio en el servicio GSLB se complementa entre sí. Si la persistencia de IP de origen está inhabilitada en el servidor virtual

GSLB, ese servidor elige un servicio GSLB diferente cada vez que el DNS intenta hacer la resolución. El cliente también se conecta a un servicio GSLB diferente y al centro de datos que recibe la solicitud de aplicación proxy la conexión al centro de datos que sirvió primero al cliente. Esto podría agregar algo de latencia. Por lo tanto, al habilitar la persistencia IP de origen en el servidor virtual GSLB puede evitar frecuentes tales saltos múltiples para solicitudes de aplicaciones. Si la sesión de persistencia de IP de origen ha caducado y el cliente se vuelve a conectar después de eso, la persistencia del sitio conecta al cliente de nuevo al centro de datos, que había servido al cliente inicialmente. Además, si el cliente se conecta de nuevo a través de una puerta de enlace DNS, que no está dentro del rango de máscara de persistencia configurado, la persistencia del sitio también ayuda a los clientes a adherirse al centro de datos que sirvió la primera solicitud.

Para configurar la persistencia basada en la dirección IP de origen mediante la CLI

En el símbolo del sistema, escriba:

```
set gslb vserver <name> -persistenceType (SOURCEIP|NONE) -persistenceId
    <positive_integer> [-persistMask <netmask>] - [timeout <mins>]
<!--NeedCopy-->
```

Ejemplo:

```
set gslb vserver vserver-GSLB-1 -persistenceType SOURCEIP -
   persistenceId 23 -persistMask 255.255.255.255 - timeout 2
<!--NeedCopy-->
```

Para configurar la persistencia basada en la dirección IP de origen mediante la GUI

1. Vaya a **Administración de tráfico** > **GSLB** > **Servidores virtuales** y haga doble clic en el servidor virtual GSLB cuyo método desea cambiar (por ejemplo, vServer-GSLB-1).
2. Haga clic en la sección **Persistencia** y, en la lista desplegable **Persistencia**, seleccione **SOURCEIP** y establezca los siguientes parámetros:
   - ID de persistencia: ID de persistencia
   - Tiempo de espera: Tiempo de espera
   - Máscara de red IPv4 o longitud de máscara IPv6: Máscara persistente

Configurar la persistencia del sitio basado en cookies HTTP

La persistencia del sitio se logra mediante cookies HTTP (conocidas como “cookie del sitio”) para volver a conectar el cliente al mismo servidor. Cuando el dispositivo GSLB responde a una solicitud

DNS de cliente enviando la dirección IP del sitio GSLB seleccionado, el cliente envía una solicitud HTTP a ese sitio GSLB. El extremo de la aplicación en ese sitio GSLB agrega una cookie de sitio al encabezado HTTP y la persistencia del sitio está en vigor.
Si el cliente envía una consulta DNS después de que caduque la caché del cliente, la solicitud DNS puede dirigirse a un sitio GSLB diferente. El nuevo sitio GSLB utiliza la cookie del sitio presente en el encabezado de solicitud del cliente para implementar la persistencia. La función de persistencia del sitio se activa en las siguientes condiciones:

- Cuando el nombre de dominio en el encabezado de host coincide con uno de los dominios GSLB
- Cuando se habilita la persistencia del sitio en el servicio GSLB que representa el servidor virtual que recibe el tráfico de la aplicación.

La cookie del sitio contiene información sobre el servicio GSLB seleccionado en el que el cliente tiene una conexión persistente. Si el servicio GSLB apuntado por la cookie está DOWN o se elimina de la configuración GLSB, el servidor virtual que recibe el tráfico continuará procesando el tráfico. La caducidad de las cookies se basa en el tiempo de espera de las cookies configurado en el dispositivo Citrix ADC. Si los nombres de servidor virtual no son idénticos en todos los sitios, debe utilizar el identificador de persistencia. Las cookies insertadas cumplen con RFC 2109.

Citrix ADC admite dos tipos de persistencia del sitio:

- Proxy de conexión
- redirección HTTP

Proxy de conexión

En el modo Proxy de conexión de persistencia del sitio, el centro de datos que recibe la solicitud de aplicación posterior realiza las siguientes tareas para establecer una conexión:

1. Crea una conexión con el sitio GSLB que insertó la cookie del sitio.
2. Proxies la solicitud del cliente al sitio original.

> **Nota:**
>
> El servidor proxy establece la conexión con el sitio original mediante los siguientes detalles:
>
> ```
> 1 -  El SNIP del nuevo sitio es la dirección IP de origen.
> ```
>
> - La dirección IP pública del servicio GSLB del sitio original es la dirección IP de destino.
> - Un puerto efímero es el puerto de origen y el puerto de servicio GSLB es el puerto de destino.

- Utiliza protocolos HTTP o HTTPS dependiendo del tipo de servicio GSLB.

3. Recibe una respuesta del sitio GSLB original.
4. Retransmite esa respuesta al cliente.
5. Cierra la conexión.

redirección HTTP

Si la configuración de GSLB utiliza persistencia de redireccionamiento HTTP, el nuevo sitio redirige la solicitud al sitio que insertó originalmente la cookie. El nombre de dominio en la URL de redirección es el dominio del sitio. Asegúrese de que tanto las cookies como los certificados SSL sean aplicables tanto al dominio GSLB como al dominio del sitio. Para aplicar cookies tanto para GSLB como para el dominio del sitio, el dominio de cookies debe ser el sitio al dominio GSLB. Para aplicar certificados SSL tanto a GSLB como al dominio de sitio, el certificado enlazado al servidor virtual SSL debe ser un certificado comodín.

El proxy de conexión se produce cuando se cumplen las siguientes condiciones:

- Las solicitudes se envían para un dominio que participa en GSLB. El dominio se obtiene del encabezado URL/host.
- El servicio GSLB local tiene habilitado el proxy de conexión.
- La solicitud incluye una cookie válida que contiene la dirección IP de un servicio GSLB remoto activo.

> **Nota**
>
> En una configuración principal-secundario de GSLB, el proxy de conexión funciona como se pretende incluso cuando un servicio GSLB no está configurado en un sitio secundario. Sin embargo, si tiene configuración adicional, como autenticación de cliente, inserción de direcciones IP de cliente u otro requisito específico de SSL, debe agregar un servicio GSLB explícito en el sitio y configurarlo en consecuencia.
>
> Para obtener más información sobre la topología principal-secundario, consulte Implementación de topología principal-secundario mediante el protocolo MEP.

Para establecer la persistencia basada en cookies HTTP mediante el uso de la CLI

En el símbolo del sistema, escriba:

```
set gslb service <serviceName> -sitePersistence (ConnectionProxy [-
    sitePrefix <prefix>] | HTTPredirect -sitePrefix <prefix>)
<!--NeedCopy-->
```


Ejemplo:

```
set gslb service service-GSLB-1 -sitePersistence ConnectionProxy
set gslb service service-GSLB-1 -sitePersistence HTTPRedirect -
   sitePrefix vserver-GSLB-1
<!--NeedCopy-->
```

Para establecer la persistencia basada en cookies mediante el uso de la GUI

1. Vaya a **Administración de tráfico** > **GSLB** > **Servicios** y seleccione el servicio que desea configurar para la persistencia del sitio (por ejemplo, Service-GSLB-1).
2. Haga clic en la sección **Persistencia del sitio** y establezca la persistencia en función de las cookies.

Administrar conexiones de clientes

October 5, 2021

Para facilitar la administración de las conexiones de los clientes, puede habilitar la limpieza retardada de las conexiones al servidor virtual. A continuación, puede administrar el tráfico DNS local mediante la configuración de directivas DNS.

Habilitar la limpieza retrasada de las conexiones del servidor virtual

El estado de un servidor virtual depende de los estados de los servicios vinculados a él y el estado de cada servicio depende de los monitores vinculados a él. Si un servidor es lento o está inactivo, el tiempo de espera de los sondeos de supervisión y el servicio que representa al servidor se marca como DOWN. Un servidor virtual se marca como DOWN solo cuando todos los servicios vinculados a él están marcados como DOWN. Puede configurar los servicios y los servidores virtuales para que terminen todas las conexiones cuando se caigan o para permitir que las conexiones se lleven a cabo. Este último ajuste es para situaciones en las que un servicio está marcado como DOWN debido a la lentitud del servidor.

Al configurar la opción de vaciado de estado inactivo, el dispositivo Citrix ADC realiza una limpieza retrasada de las conexiones a un servicio GSLB que está inactivo.

Para habilitar la limpieza retrasada de las conexiones del servidor virtual mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para configurar la limpieza de la conexión retrasada y compruebe la configuración:

```
set gslb service <name> -downStateFlush (ENABLED | DISABLED)
show gslb service <name>
<!--NeedCopy-->
```

Ejemplo:

```
set gslb service Service-GSLB-1 -downStateFlush ENABLED
Done

show gslb service Service-GSLB-1
Done
<!--NeedCopy-->
```

Para habilitar la limpieza retrasada de las conexiones del servidor virtual mediante la utilidad de configuración

1. Vaya a **Administración del tráfico** > **GSLB** > **Servicios** y haga doble clic en el servicio.
2. Haga clic en la sección **Otros ajustes** y seleccione la opción **Down State Flush** .

Administrar el tráfico DNS local mediante directivas DNS

Puede utilizar directivas DNS para implementar la afinidad de sitios dirigiendo el tráfico desde la dirección IP de un solucionador o red DNS local a un sitio GSLB de destino predefinido. Esto se configura creando directivas DNS con expresiones DNS y vinculando las directivas de forma global en el dispositivo Citrix ADC.

expresiones DNS

El dispositivo Citrix ADC proporciona ciertas expresiones DNS predefinidas que se pueden utilizar para configurar acciones específicas de un dominio. Estas acciones pueden, por ejemplo, eliminar determinadas solicitudes, seleccionar una vista específica para un dominio específico o redirigir determinadas solicitudes a una ubicación específica.

Estas expresiones DNS (también denominadas *reglas*) se combinan para crear directivas DNS que luego se enlazan globalmente en el dispositivo Citrix ADC.

A continuación se muestra la lista de calificadores DNS predefinidos disponibles en el dispositivo Citrix ADC:

- CLIENT.UDP.DNS.DOMAIN.EQ("domainname")
- CLIENT.UDP.DNS.IS_AREC
- CLIENT.UDP.DNS.IS_AAAAREC
- CLIENT.UDP.DNS.IS_SRVREC
- CLIENT.UDP.DNS.IS_MXREC
- CLIENT.UDP.DNS.IS_SOAREC
- CLIENT.UDP.DNS.IS_PTRREC
- CLIENT.UDP.DNS.IS_CNAME
- CLIENT.UDP.DNS.IS_NSREC
- CLIENT.UDP.DNS.IS_ANYREC

La expresión DNS CLIENT.UDP.DNS.DOMAIN se puede utilizar con expresiones de cadena. Si utiliza nombres de dominio como parte de la expresión, deben terminar con un punto (.). Por ejemplo, CLIENT.UDP.DNS.DOMAIN.ENDSWITH("abc.com.")

Para crear una expresión mediante la utilidad de configuración

1. Haga clic en el icono situado junto al cuadro de texto Expresión. Haga clic en Add. (Deje vacíos los cuadros de lista desplegable Tipo de flujo y protocolo). Sigue estos pasos para crear una regla.
2. En el cuadro Calificador, seleccione un calificador (por ejemplo, UBICACIÓN).
3. En el cuadro Operador, seleccione un operador (por ejemplo, ==).
4. En el cuadro Valor, escriba un valor (por ejemplo, Asia, Japón…).
5. Haga clic en OK. Haga clic en Crear y haga clic en Cerrar. Se crea la regla.
6. Haga clic en OK.

Configurar acciones DNS

Una directiva DNS incluye el nombre de una acción DNS que se va a realizar cuando la regla de directiva se evalúa como TRUE. Una acción DNS puede realizar una de las siguientes acciones:

- Envíe al cliente una dirección IP para la que haya configurado una vista DNS. Para obtener más información sobre las vistas DNS, consulte Adición de vistas DNS.
- Envíe al cliente la dirección IP de un servicio GSLB después de hacer referencia a una lista de ubicaciones preferidas que anula el comportamiento de proximidad estático. Para obtener más información sobre las ubicaciones preferidas, consulte Modificación del comportamiento de proximidad estática mediante la configuración de ubicaciones preferidas.

- Enviar al cliente una dirección IP específica determinada por la evaluación de la consulta o respuesta DNS (reescritura de respuesta DNS).
- Reenvía una solicitud al servidor de nombres sin realizar una búsqueda en la caché DNS del dispositivo.
- Deja una solicitud.

No se puede crear una acción DNS para eliminar una solicitud DNS o para omitir la caché DNS del dispositivo. Si quieres eliminar una solicitud DNS, usa la acción integrada, DNS_default_act_drop. Si quieres omitir la caché DNS, usa la acción integrada, DNS_default_act_cacheBypass. Ambas acciones están disponibles junto con acciones personalizadas en los cuadros de diálogo Crear directiva DNS y Configurar directiva DNS. Estas acciones integradas no se pueden modificar ni quitar.

Para configurar una acción DNS mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para configurar una acción DNS y verificar la configuración:

```
add dns action <actionName> <actionType> (-IPAddress <ip_addr |
    ipv6_addr> ... | -viewName <string> | -preferredLocList <string>
    ...) [-TTL <secs>]

show dns action [<actionName>]
<!--NeedCopy-->
```

Ejemplos

Ejemplo 1: Configuración de la reescritura de respuestas DNS. La siguiente acción DNS envía al cliente una dirección IP preconfigurada cuando la directiva a la que está vinculada la acción se evalúa como verdadera:

```
add dns action dns_act_response_rewrite Rewrite_Response -IPAddress
    192.0.2.20 192.0.2.56 198.51.100.10
 Done

show dns action dns_act_response_rewrite
1)  ActionName:  dns_act_response_rewrite ActionType:  Rewrite_Response
     TTL:  3600              IPAddress:  192.0.2.20 192.0.2.56
    198.51.100.10
 Done
<!--NeedCopy-->
```


Ejemplo 2: Configuración de una respuesta basada en vista DNS. La siguiente acción DNS envía al cliente una dirección IP para la que ha configurado una vista DNS:

```
add dns action send_ip_from_view_internal_ip ViewName -viewName
   view_internal_ip
Done

show dns action send_ip_from_view_internal_ip
1)  ActionName:  send_ip_from_view_internal_ip ActionType:  ViewName
      ViewName:  view_internal_ip
 Done
<!--NeedCopy-->
```

Ejemplo 3: Configuración de una respuesta basada en una lista de ubicaciones preferidas. La siguiente acción DNS envía al cliente la dirección IP correspondiente a la ubicación preferida que selecciona de la lista de ubicaciones especificada:

```
add dns action send_preferred_location GslbPrefLoc -preferredLocList NA
   .tx.ns1.\*.\*.* NA.tx.ns2.\*.\*.* NA.tx.ns3.\*.\*.*
Done

show dns action  send_preferred_location
1)  ActionName:  send_preferred_location ActionType:  GslbPrefLoc
   PreferredLocList:  "NA.tx.ns1.\*.\*.\*" "NA.tx.ns2.\*.\*.\*" "NA.tx.
   ns3.\*.\*.*"
 Done
<!--NeedCopy-->
```

Para configurar una acción DNS mediante la utilidad de configuración de Citrix ADC

1. Vaya a Administración del tráfico > DNS > Acciones, cree o modifique una acción DNS.
2. En el cuadro de diálogo Crear acción DNS o Configurar acción DNS, defina los siguientes parámetros:
   - Nombre de acción (no se puede cambiar para una acción DNS existente)
   - Tipo (no se puede cambiar para una acción DNS existente)
     Para establecer el parámetro
     Type, realice una de las siguientes acciones:
     - Para crear una acción DNS asociada a una vista DNS, seleccione Nombre de vista. A continuación, en la lista Nombre de vista, seleccione la vista DNS que quiera utilizar en la acción.

  - Para crear una acción DNS con una lista de ubicaciones preferidas, seleccione Lista de ubicaciones preferidas. En Ubicación preferida, introduzca una ubicación y, a continuación, haga clic en Agregar. Agrega tantas ubicaciones DNS como quieras.
  - Para configurar una acción DNS para volver a escribir una respuesta DNS sobre la base de la evaluación de directivas, seleccione Reescribir respuesta. En Dirección IP, introduzca una dirección IP y, a continuación, haga clic en Agregar. Agrega tantas direcciones IP como quieras.
- TTL (aplicable solo al tipo de acción Reescribir respuesta)

Configurar directivas DNS

Las directivas DNS funcionan en una base de datos de ubicaciones que utiliza direcciones IP estáticas y personalizadas. Los atributos de la solicitud DNS local entrante se definen como parte de una expresión y el sitio de destino se define como parte de una directiva DNS. Al definir acciones y expresiones, puede utilizar un par de comillas simples (‘’) como calificador comodín para especificar más de una ubicación. Cuando se configura una directiva DNS y se recibe una solicitud GSLB, primero se consulta en la base de datos de direcciones IP personalizadas una entrada que define los atributos de ubicación del origen:

- Cuando una consulta DNS proviene de un LDNS, las funciones del LDNS se evalúan con respecto a las directivas configuradas. Si coinciden, se ejecuta una acción adecuada (afinidad del sitio). Si las funciones de LDNS coinciden con más de un sitio, la solicitud tiene un equilibrio de carga entre los sitios que coinciden con las funciones de LDNS.
- Si la entrada no se encuentra en la base de datos personalizada, se consulta una entrada en la base de datos de direcciones IP estáticas y, si hay una coincidencia, se repite la evaluación de directivas anterior.
- Si la entrada no se encuentra en las bases de datos estáticas o personalizadas, se selecciona el mejor sitio y se envía en la respuesta DNS según el método de equilibrio de carga configurado.

Las siguientes restricciones se aplican a las directivas DNS creadas en el dispositivo Citrix ADC.

- Se admite un máximo de 64 directivas.
- Las directivas DNS son globales para el dispositivo Citrix ADC y no se pueden aplicar a un servidor virtual o dominio específicos.
- No se admite la vinculación de directivas específica de dominio o servidor virtual.

Puede utilizar directivas DNS para dirigir a los clientes que coinciden con un determinado rango de direcciones IP a un sitio específico. Por ejemplo, si tiene una configuración de GSLB con varios sitios GSLB separados geográficamente, puede dirigir a todos los clientes cuya dirección IP se encuentre dentro de un rango específico a un centro de datos concreto.

Se puede evaluar el tráfico DNS tanto basado en TCP como en UDP. Las expresiones de directiva están

disponibles para el tráfico DNS basado en UDP en el servidor y para el tráfico DNS basado en UDP y el tráfico DNS basado en TCP del lado del cliente. Además, puede configurar expresiones para evaluar consultas y respuestas que solo implican los siguientes tipos de preguntas DNS (o valores QTYPE):

- A
- AAAA
- N
- SRV
- PTR
- CNAME
- JABONERA
- MX
- CUALQUIERA

También se admiten los siguientes códigos de respuesta (valores RCODE):

- NOERROR - Sin error
- FORMERR - Error de formato
- SERVFAIL - Fallo del servidor
- NXDOMAIN - Dominio inexistente
- NOTIMP - Tipo de consulta no implementado
- RECHAZADO - Consulta rechaz

Puede configurar expresiones para evaluar el tráfico DNS. Una expresión DNS comienza con los prefijos DNS.REQ o DNS.RES. Las funciones están disponibles para evaluar el dominio consultado, el tipo de consulta y el protocolo portadora. Para obtener más información sobre las expresiones DNS, consulte “Expresiones para evaluar un mensaje DNS e identificar su protocolo portador” en “Configuración y referencia de directivas”.

Para agregar una directiva DNS mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para crear una directiva DNS y verificar la configuración:

```
add dns policy <name> <rule> <actionName>
show dns policy <name>
<!--NeedCopy-->
```

Ejemplo:


```
> add dns policy-GSLB-1 'CLIENT.UDP.DNS.DOMAIN.EQ(”domainname”)'
   my_dns_action
 Done
> show dns policy-GSLB-1
    Name: policy-GSLB-1
    Rule: CLIENT.UDP.DNS.DOMAIN.EQ(”domainname”)
    Action Name: my_dns_action
    Hits: 0
    Undef Hits: 0

 Done
<!--NeedCopy-->
```

Para quitar una directiva DNS configurada mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
rm dns policy <name>
<!--NeedCopy-->
```

Para configurar una directiva DNS mediante la utilidad de configuración de Citrix ADC

1. Vaya a Administración del tráfico > DNS > Directivas y cree una directiva DNS.
2. En el cuadro de diálogo Crear directiva DNS o Configurar directiva DNS, defina los siguientes parámetros:
   - Nombre de la directiva (no se puede cambiar para una directiva existente)
   - Acción
   - Expresión

     Para especificar una expresión, haga lo siguiente:

     a) Haga clic en Agregar y, a continuación, en el cuadro desplegable que aparece, seleccione el elemento de expresión con el que quiere comenzar la expresión. Aparecerá una segunda lista. La lista contiene un conjunto de elementos de expresión que se pueden utilizar inmediatamente después del primer elemento expression.

     b) En la segunda lista, seleccione el elemento de expresión que quiera y, a continuación, introduzca un punto.

     c) Después de cada selección, si introduce un punto, el siguiente conjunto de elementos de expresión válidos aparece en una lista. Seleccione elementos de expresión y rellene los argumentos de las funciones hasta que tenga la expresión que quiera.
3. Haga clic en Crear o Aceptary, a continuación, en Cerrar.

Enlazar directivas DNS

Las directivas DNS están enlazadas globalmente en el dispositivo Citrix ADC y están disponibles para todos los servidores virtuales GSLB configurados. Aunque las directivas DNS están vinculadas globalmente, la ejecución de directivas se puede limitar a un servidor virtual GSLB específico especificando el dominio en la expresión.

Nota: Aunque el comando bind dns global acepta REQ_OVERRIDE y RES_OVERRIDE como puntos de enlace válidos, esos puntos de enlace son redundantes, porque las directivas DNS solo pueden enlazarse globalmente. Enlaza tus directivas DNS solo a los puntos de enlace REQ_DEFAULT y RES_DEFAULT.

Para enlazar una directiva DNS de forma global mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para enlazar una directiva DNS de forma global y compruebe la configuración:

```
bind dns global <policyName> <priority> [-gotoPriorityExpression <
    string>] [-type <type>]
show dns global -type <type>
<!--NeedCopy-->
```

Ejemplo:

```
bind dns global policy-GSLB-1 10 -gotoPriorityExpression END
 Done
show dns global -type REQ_DEFAULT
1)  Policy Name: policy-GSLB-1
    Priority: 10
    GotoPriorityExpression: END
 Done
<!--NeedCopy-->
```

Para enlazar una directiva DNS de forma global mediante la utilidad de configuración

1. Vaya a Administración del tráfico > DNS > Directivas.
2. En el panel de detalles, haga clic en Vinculaciones globales.
3. En el cuadro de diálogo Vincular o desvincular directivas DNS a Global, haga clic en Insertar directiva.

4. En la columna Nombre de la directiva, seleccione en la lista la directiva que quiere vincular. Como alternativa, en la lista, haga clic en Nueva directiva y, a continuación, cree una directiva DNS estableciendo parámetros en el cuadro de diálogo Crear directiva DNS.
5. Para modificar una directiva que ya está vinculada globalmente, haga clic en el nombre de la directiva y, a continuación, haga clic en Modificar directiva. A continuación, en el cuadro de diálogo Configurar directiva DNS, modifique la directiva y, a continuación, haga clic en Aceptar.
6. Para desvincular una directiva, haga clic en el nombre de la directiva y, a continuación, haga clic en Desvincular directiva.
7. Para modificar la prioridad asignada a una directiva, haga doble clic en el valor de prioridad y, a continuación, introduzca un nuevo valor.
8. Para regenerar prioridades asignadas, haga clic en Regenerar prioridades. Los valores de prioridad se modifican para empezar en 100, con incrementos de 10, sin afectar el orden de evaluación.
9. Haga clic en OK.

Para ver los enlaces globales de una directiva DNS mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
show dns global
```

Para ver los enlaces globales de una directiva DNS mediante la utilidad de configuración

1. Vaya a **Administración del tráfico** > **DNS** > **Directivas**.
2. En el panel de detalles, haga clic en **Enlaces globales**. Los enlaces globales de todas las directivas DNS aparecen en este cuadro de diálogo.

Adición de vistas DNS

Puede configurar vistas DNS para identificar varios tipos de clientes y proporcionar una dirección IP adecuada a un grupo de clientes que consultan el mismo dominio GSLB. Las vistas DNS se configuran mediante directivas DNS que seleccionan las direcciones IP devueltas al cliente.

Por ejemplo, si ha configurado GSLB para el dominio de su empresa y tiene el servidor alojado en la red de su empresa, a los clientes que consultan el dominio desde la red interna de su empresa se les puede proporcionar la dirección IP interna del servidor en lugar de la dirección IP pública. Por otro lado, a los clientes que consultan DNS para el dominio desde Internet se les puede proporcionar la dirección IP pública del dominio.

Para agregar una vista DNS, asigne un nombre de hasta 31 caracteres. El carácter principal debe ser un número o una letra. También se permiten los siguientes caracteres: @ _ -. (punto): (dos puntos) # y espacio(). Después de agregar la vista, configura una directiva para asociarla a los clientes y a

una parte de la red, y la vincula globalmente. Para configurar y enlazar una directiva DNS, consulte **Administración del tráfico DNS local mediante directivas DNS**.

Para agregar una vista DNS mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para crear una vista DNS y verificar la configuración:

```
add dns view <viewName>
show dns view <viewName>
<!--NeedCopy-->
```

Ejemplo:

```
add dns view PrivateSubnet
show dns view PrivateSubnet
<!--NeedCopy-->
```

Para quitar una vista DNS mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
rm dns view <viewName>
<!--NeedCopy-->
```

Para agregar una vista DNS mediante la utilidad de configuración

Vaya a Administración del tráfico > DNS > Vistas y agregue una vista DNS.

Para obtener más información sobre cómo crear una directiva DNS y cómo enlazar directivas DNS de forma global, consulte **Administrar el tráfico DNS local mediante directivas DNS**.

Configurar GSLB para proximidad

August 20, 2021

Cuando configura GSLB para la proximidad, las solicitudes de cliente se reenvían al centro de datos más cercano. El principal beneficio del método GSLB basado en proximidad son los tiempos de respuesta más rápidos resultantes de la selección del centro de datos más cercano disponible. Tal implementación es fundamental para aplicaciones que requieren un acceso rápido a grandes volúmenes de datos.

Puede configurar GSLB para la proximidad en función del tiempo de ida y vuelta (RTT), la proximidad estática o una combinación de ambos.

Método de configuración del tiempo dinámico de ida y vuelta (RTT)

El tiempo dinámico de ida y vuelta (RTT) es una medida de tiempo o retraso en la red entre el servidor DNS local del cliente y un recurso de datos. Para medir RTT dinámico, el dispositivo Citrix ADC explora el servidor DNS local del cliente y recopila información de métrica RTT. A continuación, el dispositivo utiliza esta métrica para tomar su decisión de equilibrio de carga. El equilibrio de carga global del servidor supervisa el estado en tiempo real de la red y dirige dinámicamente la solicitud del cliente al centro de datos con el valor RTT más bajo

Para configurar GSLB para la proximidad con el método dinámico, primero debe configurar la configuración básica de GSLB y, a continuación, configurar RTT dinámico.

Primero cree dos sitios GSLB, locales y remotos. A continuación, para el sitio local, cree un servidor virtual GSLB y servicios GSLB y vincule los servicios al servidor virtual. A continuación, cree servicios ADNS y vincule el dominio para el que está configurando GSLB al servidor virtual GSLB en el sitio local. Por último, cree un servidor virtual de equilibrio de carga con la misma dirección IP del servidor virtual que el servicio GSLB.

Para obtener más información sobre cómo configurar una configuración GSLB básica, consulte Configuración de entidades GSLB individualmente.

Una vez que haya configurado una configuración básica de GSLB, configure el método RTT dinámico.

Para obtener más información sobre cómo configurar el servidor virtual GSLB para utilizar el método RTT dinámico para equilibrar la carga, consulte Configuración de RTT dinámico.

Configurar proximidad estática

El método de proximidad estática para GSLB utiliza una base de datos de proximidad estática basada en direcciones IP para determinar la proximidad entre el servidor DNS local del cliente y los sitios GSLB. El dispositivo Citrix ADC responde con la dirección IP de un sitio que mejor se ajusta a los criterios de proximidad.

Si dos o más sitios GSLB en ubicaciones geográficas diferentes ofrecen el mismo contenido, el dispositivo Citrix ADC mantiene una base de datos de rangos de direcciones IP y utiliza la base de datos para tomar decisiones sobre los sitios GSLB a los que dirigir las solicitudes de clientes entrantes.

Para configurar GSLB para proximidad con proximidad estática, primero debe configurar la configuración básica de GSLB y, a continuación, configurar la proximidad estática.

Primero cree dos sitios GSLB, locales y remotos. A continuación, para el sitio local, cree un servidor virtual GSLB y servicios GSLB y vincule los servicios al servidor virtual. A continuación, cree servicios ADNS y vincule el dominio para el que está configurando GSLB al servidor virtual GSLB en el sitio local. Por último, cree un servidor virtual de equilibrio de carga con la misma dirección IP del servidor virtual que el servicio GSLB.

Para obtener más información sobre cómo configurar una configuración GSLB básica, consulte Configuración de entidades GSLB individualmente.

Una vez que haya configurado una configuración básica de GSLB, configure la proximidad estática.

Para obtener más información sobre cómo configurar el servidor virtual GSLB para utilizar la proximidad estática para el equilibrio de carga, consulte Configuración de la proximidad estática.

Configurar proximidad estática y RTT dinámico

Puede configurar el servidor virtual GSLB para utilizar una combinación de proximidad estática y RTT dinámico cuando tenga algunos clientes procedentes de una red interna como una sucursal. Puede configurar GSLB de modo que los clientes procedentes de la sucursal o de cualquier otra red interna se dirijan a un sitio GSLB determinado que esté geográficamente cerca de la red cliente. Para todas las demás solicitudes, puede usar RTT dinámico.

Primero cree dos sitios GSLB, locales y remotos. A continuación, para el sitio local, cree un servidor virtual GSLB y servicios GSLB y vincule los servicios al servidor virtual. A continuación, cree servicios ADNS y vincule el dominio para el que está configurando GSLB al servidor virtual GSLB en el sitio local. Por último, cree un servidor virtual de equilibrio de carga con la misma dirección IP del servidor virtual que el servicio GSLB.

Para obtener más información sobre cómo configurar una configuración GSLB básica, consulte Configuración de entidades GSLB individualmente.

Una vez que haya configurado una configuración básica de GSLB, configure el servidor virtual de GSLB para que utilice la proximidad estática para todo el tráfico que se origina desde una red interna y, a continuación, utilice RTT dinámico para el resto del tráfico.

Para obtener más información sobre cómo configurar la proximidad estática, consulte Configuración de la proximidad estática y para obtener más información sobre cómo configurar RTT dinámico, consulte Configuración de RTT dinámico.

Proteger la configuración de GSLB contra fallos

August 20, 2021

Puede proteger la configuración de GSLB contra fallos de un sitio GSLB o de un servidor virtual GSLB configurando lo siguiente:

- Un servidor virtual GSLB de respaldo
- Un dispositivo Citrix ADC para responder con varias direcciones IP
- Dirección IP de copia de seguridad para un dominio GSLB

También puede desviar el exceso de tráfico a un servidor virtual de copia de seguridad mediante el uso de spillover.

Configurar un servidor virtual GSLB de copia de seguridad

La configuración de una entidad de copia de seguridad para un servidor virtual GSLB garantiza que el tráfico DNS a un sitio no se interrumpa si el servidor virtual GSLB se apaga. La entidad de copia de seguridad puede ser otro servidor virtual GSLB, o puede ser una dirección IP de copia de seguridad. Con una entidad de copia de seguridad configurada, si el servidor virtual GSLB principal falla, la entidad de copia de seguridad maneja las solicitudes DNS. Para especificar qué debe ocurrir cuando vuelva a aparecer el servidor virtual GSLB principal, puede configurar la entidad de copia de seguridad para que continúe manejando el tráfico hasta que habilite manualmente el servidor virtual principal para que se haga cargo (mediante la opción DisablePrimaryOnDown).

Nota: Puede configurar una única entidad de copia de seguridad como copia de seguridad para varios servidores virtuales GSLB.

Para configurar un servidor virtual GSLB de copia de seguridad mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para configurar un servidor virtual GSLB como servidor virtual de copia de seguridad y verificar la configuración:

```
set gslb vserver <name> -backupVServer <name> [-disablePrimaryOnDown (
    ENABLED | DISABLED)]

show gslb vserver <name>
<!--NeedCopy-->
```

Ejemplo:


```
set gslb vserver vserver-GSLB-1 -backupVServer vserver-GSLB-2 -
   disablePrimaryOnDown ENABLED
show gslb vserver vserver-GSLB-1
<!--NeedCopy-->
```

Para establecer el servidor virtual GSLB como servidor virtual de copia de seguridad mediante la utilidad de configuración

1. Vaya a **Administración del tráfico** > **GSLB** > **Servidores virtuales** y haga doble clic en el servidor virtual GSLB.
2. Seleccione la sección **Servidor virtual de copia** de seguridad y elija el servidor virtual de copia de seguridad.

Configurar una configuración de GSLB para responder con varias direcciones IP

Una respuesta DNS típica contiene la dirección IP del servicio GSLB de mejor rendimiento. Sin embargo, si habilita varias respuestas IP (MIR), el dispositivo Citrix ADC envía el mejor servicio GSLB como primer registro de la respuesta y agrega los servicios activos restantes como registros adicionales. Si MIR está inhabilitado (predeterminado), el dispositivo Citrix ADC envía el mejor servicio como único registro en respuesta.

Para configurar un servidor virtual GSLB para varias respuestas IP mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para configurar un servidor virtual GSLB para varias respuestas IP y compruebe la configuración:

```
set gslb vserver<name> -MIR (ENABLED | DISABLED)
-  show gslb vserver <name>
<!--NeedCopy-->
```

Ejemplo:

```
set gslb vserver vserver-GSLB-1 -MIR ENABLED
 show gslb vserver <vserverName>
<!--NeedCopy-->
```


Para establecer un servidor virtual GSLB para varias respuestas IP mediante la utilidad de configuración

1. Vaya a **Administración del tráfico** > **GSLB** > **Servidores virtuales** y haga doble clic en el servidor virtual GSLB para el que quiere configurar un servidor virtual de copia de seguridad (por ejemplo, VServer-GSLB-1).
2. En la ficha **Avanzado**, en Cuando este servidor virtual está "ARRIBA", active la casilla de verificación Enviar todas las IP de servicio "activas" en respuesta (MIR) y seleccione **Aceptar**.

Configuración de un servidor virtual GSLB para que responda con un registro de direcciones vacío cuando está en estado de baja

Una respuesta DNS puede contener la dirección IP del dominio solicitado o una respuesta que indique que el servidor DNS no conoce la dirección IP del dominio, en cuyo caso la consulta se reenvía a otro servidor de nombres. Estas son las únicas respuestas posibles a una consulta DNS.

Cuando un servidor virtual GSLB está inhabilitado o en estado DOWN, la respuesta a una consulta DNS para el dominio GSLB enlazado a ese servidor virtual contiene las direcciones IP de todos los servicios enlazados al servidor virtual. Sin embargo, puede configurar el servidor virtual GSLB para que, en este caso, envíe una respuesta vacía (EDR). Cuando se establece esta opción, una respuesta DNS de un servidor virtual GSLB que está en estado DOWN no contiene registros de direcciones IP, pero el código de respuesta es correcto. Esto impide que los clientes intenten conectarse a sitios GSLB que están inconectados.

Nota: Debe configurar esta configuración para cada servidor virtual al que quiere que se aplique.

Para configurar un servidor virtual GSLB para respuestas vacías mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
set gslb vserver<name> -EDR (ENABLED | DISABLED)
<!--NeedCopy-->
```

Ejemplo:

```
> set gslb vserver vserver-GSLB-1 -EDR ENABLED
 Done
<!--NeedCopy-->
```


Para establecer un servidor virtual GSLB para respuestas vacías mediante la utilidad de configuración

1. Vaya a **Administración del tráfico** > **GSLB** > **Servidores virtuales** y haga doble clic en el servidor virtual GSLB para el que quiere configurar un servidor virtual de copia de seguridad (por ejemplo, VServer-GSLB-1).
2. En la ficha Avanzado, en Cuando este servidor virtual está "Inactivo", active la casilla de verificación No enviar la dirección IP de ningún servicio en respuesta (EDR).
3. Haga clic en **Aceptar**.

Configurar una dirección IP de copia de seguridad para un dominio GSLB

Puede configurar un sitio de copia de seguridad para su configuración GSLB. Con esta configuración, si todos los sitios principales caen, la dirección IP del sitio de copia de seguridad se proporciona en la respuesta DNS.

Normalmente, si un servidor virtual GSLB está activo, ese servidor virtual envía una respuesta DNS con una de las direcciones IP del sitio activo seleccionadas por el método GSLB configurado. Si todos los sitios principales configurados del servidor virtual GSLB están inactivos (en estado DOWN), el servidor del sistema de nombres de dominio autorizado (ADNS) o el servidor DNS envía una respuesta DNS con la dirección IP del sitio de copia de seguridad.

Nota: Cuando se envía una dirección IP de copia de seguridad, no se respeta la persistencia.

Para establecer una dirección IP de copia de seguridad para un dominio mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para establecer una dirección IP de copia de seguridad y verificar la configuración:

```
set gslb vserver <name> -domainName <string> -backupIP <IPAddress>
show gslb vserver <name>
<!--NeedCopy-->
```

Ejemplo:

```
set gslb vserver vserver-GSLB-1 -domainName www.abc.com -backupIP
   10.102.29.66
show gslb vserver vserver-GSLB-1
<!--NeedCopy-->
```


Para establecer una dirección IP de copia de seguridad para un dominio mediante la utilidad de configuración

1. Vaya a **Administración del tráfico** > **GSLB** > **Servidores virtuales** y haga doble clic en el servidor virtual GSLB al que quiere enlazar el dominio de copia de seguridad (por ejemplo, VServer-GSLB-1).
2. Haga clic en la sección **Dominios**, configure el dominio GSLB y especifique la dirección IP del dominio de copia de seguridad en el campo **IP de copia** de seguridad.

Desviar el exceso de tráfico a un servidor virtual de backup

Una vez que el número de conexiones a un servidor virtual GSLB primario supera el valor de umbral configurado, puede utilizar la opción de desbordamiento para desviar nuevas conexiones a un servidor virtual GSLB de copia de seguridad. Este valor de umbral se puede calcular dinámicamente o establecer manualmente. Una vez que el número de conexiones al servidor virtual principal cae por debajo del umbral, el servidor virtual GSLB principal reanuda el servicio de las solicitudes del cliente.

Puede configurar la persistencia con spillover. Cuando se configura la persistencia, los nuevos clientes se desvían al servidor virtual de copia de seguridad si ese cliente aún no está conectado a un servidor virtual principal. Cuando se configura la persistencia, las conexiones que se desviaron al servidor virtual de copia de seguridad no se vuelven a mover al servidor virtual principal después de que el número de conexiones al servidor virtual principal descienda por debajo del umbral. En su lugar, el servidor virtual de copia de seguridad continúa procesando esas conexiones hasta que el usuario las finalice. Mientras tanto, el servidor virtual principal acepta nuevos clientes.

El umbral se puede medir por el número de conexiones, ancho de banda y estado de los servicios.

Si el servidor virtual de copia de seguridad alcanza el umbral configurado y no puede asumir ninguna carga adicional, el servidor virtual principal desvía todas las solicitudes a la dirección URL de redirección designada. Si no se configura una dirección URL de redirección en el servidor virtual principal, se eliminan las solicitudes posteriores.

La función de desbordamiento impide que el servicio GSLB de copia de seguridad remota (sitio GSLB de copia de seguridad) se vea inundado de solicitudes de cliente cuando falla el servidor virtual GSLB principal. Esto ocurre cuando un monitor está enlazado a un servicio GSLB remoto y el servicio experimenta un error que hace que su estado baje hacia abajo. Sin embargo, el monitor sigue manteniendo el estado del servicio GSLB remoto UP, debido a la función de desbordamiento.

Como parte de la resolución de este problema, se mantienen dos estados para un servicio GSLB, el estado primario y el estado efectivo. El estado primario es el estado del servidor virtual primario y el estado efectivo es el estado acumulativo de los servidores virtuales (cadena primaria y de copia de seguridad). El estado efectivo se establece en UP si alguno de los servidores virtuales de la cadena de servidores virtuales es UP. También se proporciona un indicador que indica que el VIP principal ha alcanzado el umbral. El umbral se puede medir por el número de conexiones o por el ancho de banda.

Un servicio se considera para GSLB solo si su estado primario es UP. El tráfico se dirige al servicio GSLB de copia de seguridad solo cuando todos los servidores virtuales principales están DOWN. Normalmente, estas implementaciones tienen solo un servicio GSLB de respaldo.

Agregar estados primarios y efectivos a un servicio GSLB tiene los siguientes efectos:

- Cuando se configura la persistencia de IP de origen, el DNS local se dirige al sitio seleccionado anteriormente solo si el servidor virtual principal del sitio seleccionado está UP y por debajo del umbral. La persistencia se puede ignorar en el modo round robin.
- Si se configura la persistencia basada en cookies, las solicitudes de cliente se redirigen solo cuando el servidor virtual principal del sitio seleccionado está UP.
- Si el servidor virtual principal ha alcanzado su saturación y los VIP de backup están ausentes o están inactivas, el estado efectivo se establece en DOWN.
- Si los monitores externos están enlazados a un servidor virtual HTTP-HTTPS, el monitor decide el estado principal.
- Si no hay ningún servidor virtual de copia de seguridad en el servidor virtual principal y el servidor virtual principal ha alcanzado su umbral, el estado efectivo se establece en DOWN.

Para configurar el servidor virtual GSLB de copia de seguridad mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para configurar el servidor virtual GSLB de copia de seguridad y verificar la configuración:

```
set gslb vserver <name> -soMethod <method> -soThreshold <threshold> -
    soPersistence ( \*\*ENABLED\*\* | \*\*DISABLED\*\* ) -
    soPersistenceTimeout <timeout>
show gslb vserver <name>
<!--NeedCopy-->
```

Ejemplo:

```
set gslb vserver Vserver-GSLB-1 -soMethod CONNECTION -soThreshold 1000
    -soPersistence ENABLED -soPersistenceTimeout 2
show gslb vserver Vserver-GSLB-1
<!--NeedCopy-->
```


Para configurar el servidor virtual GSLB de copia de seguridad mediante la utilidad de configuración

1. Vaya a **Administración del tráfico** > **GSLB** > **Servidores virtuales** y haga doble clic en el servidor virtual que desea configurar como copia de seguridad (por ejemplo, vServer-LB-1).
2. Haga clic en la sección **SpilLover** y defina los siguientes parámetros:
   - Método: Somethod
   - Umbral: SoThreshold
   - Tiempo de espera de persistencia (min): SoPersistenceTimeout
3. Seleccione la opción Persistencia y haga clic en **Aceptar**.

Configurar GSLB para recuperación ante desastres

August 20, 2021

La capacidad de recuperación ante desastres es crítica, ya que el tiempo de inactividad es costoso. Un dispositivo Citrix ADC configurado para GSLB reenvía el tráfico al centro de datos menos cargado o al mejor rendimiento. Esta configuración, denominada configuración activa-activa, no solo mejora el rendimiento, sino que también proporciona recuperación ante desastres inmediata al enrutar el tráfico a otros centros de datos si un centro de datos que forma parte de la instalación falla. Alternativamente, puede configurar una configuración de GSLB activa en espera solo para recuperación ante desastres.

Configurar GSLB para recuperación ante desastres en una configuración de centro de datos activo en espera

Una configuración convencional de recuperación ante desastres incluye un centro de datos activo y un centro de datos en espera. El centro de datos en espera es un sitio remoto. Cuando se produce una conmutación por error como resultado de un evento de desastre que hace que el centro de datos activo principal esté inactivo, el centro de datos en espera entra en funcionamiento.

La configuración de la recuperación ante desastres en una configuración de centro de datos activo en espera consiste en las siguientes tareas.

- Cree el centro de datos activo.
  - Agregue un sitio GSLB local.
  - Agregue un vserver GSLB, que representa el centro de datos activo.
  - Enlazar el dominio al servidor virtual GSLB.
  - Agregue servicios gslb y vincule los servicios al servidor virtual GSLB activo.
- Cree el centro de datos en espera.
  - Agregue un sitio gslb remoto.

- Agregue un vserver gslb, que representa el centro de datos en espera.
- Agregue servicios gslb que representan el centro de datos en espera y vincule los servicios al servidor vserver gslb en espera.
- Designe el centro de datos en espera configurando el servidor virtual GSLB en espera como servidor virtual de copia de seguridad para el servidor virtual GSLB activo.

Una vez configurado el centro de datos principal, replicar la configuración del centro de datos de copia de seguridad y designarlo como el sitio GSLB en espera designando un servidor virtual GSLB en ese sitio como servidor virtual de copia de seguridad.

Para obtener más información sobre cómo configurar una configuración GSLB básica, consulte Configuración de entidades GSLB individualmente.

Para designar el sitio GSLB en espera mediante la interfaz de línea de comandos

Tanto en el sitio activo como en el sitio remoto, en el símbolo del sistema, escriba:

```
set gslb vserver <name> -backupVserver <string>
<!--NeedCopy-->
```

Ejemplo:

```
set gslb vserver vserver-GSLB-1 -backupVServer vserver-GSLB-2
<!--NeedCopy-->
```

Para configurar el sitio en espera mediante la utilidad de configuración

1. Vaya a Administración del tráfico > GSLB > Servidores virtuales y haga doble clic en el servidor virtual GSLB del sitio principal.
2. Haga clic en la sección **Servidor virtual de copia** de seguridad y seleccione un servidor virtual de copia de seguridad.

De forma predeterminada, una vez que el servidor virtual principal se activa, comienza a recibir tráfico. Sin embargo, si quiere que el tráfico se dirija al servidor virtual de copia de seguridad incluso después de que el servidor virtual principal se active, utilice la opción
'inhabilitar primario al activo'.

Configurar para recuperación ante desastres en una configuración de centro de datos activo-activo

Una implementación activa de GSLB, en la que ambos sitios de GSLB están activos, elimina cualquier riesgo que pueda surgir al tener un centro de datos en espera. Con tal configuración, el contenido web o de la aplicación se puede reflejar en ubicaciones geográficamente separadas. Esto garantiza que los datos estén siempre disponibles en cada centro de datos distribuido.

Para configurar GSLB para recuperación ante desastres en una configuración de centro de datos activo-activo, primero debe configurar la configuración básica de GSLB en el primer centro de datos y, a continuación, configurar todos los demás centros de datos.

Primero cree al menos dos sitios GSLB. A continuación, para el sitio local, cree un servidor virtual GSLB y servicios GSLB y vincule los servicios al servidor virtual. A continuación, cree servicios ADNS y vincule el dominio para el que está configurando GSLB al servidor virtual GSLB en el sitio local. Finalmente, en el sitio local, cree un servidor virtual de equilibrio de carga con la misma dirección IP del servidor virtual que el servicio GSLB.

Una vez que haya configurado el primer centro de datos, duplique la configuración para otros centros de datos que forman parte de la configuración.

Para obtener más información sobre cómo configurar una configuración GSLB básica, consulte Configuración de entidades GSLB individualmente.

Configuración de la recuperación ante desastres con Round Robin ponderado

Cuando configura GSLB para que utilice el método round robin ponderado, los pesos se agregan a los servicios GSLB y el porcentaje configurado de tráfico entrante se envía a cada sitio GSLB. Por ejemplo, puede configurar la configuración de GSLB para reenviar el 80 por ciento del tráfico a un sitio y el 20 por ciento del tráfico a otro. Después de hacerlo, el dispositivo Citrix ADC enviará cuatro solicitudes al primer sitio por cada solicitud que envíe al segundo.

Para configurar el método round robin ponderado, primero cree dos sitios GSLB, locales y remotos. A continuación, para el sitio local, cree un servidor virtual GSLB y servicios GSLB, y vincule los servicios al servidor virtual. Configure el método GSLB como round robin. A continuación, cree servicios ADNS y vincule el dominio para el que está configurando GSLB al servidor virtual GSLB. Por último, cree un servidor virtual de equilibrio de carga con la misma dirección IP del servidor virtual que el servicio GSLB.

Cada servicio que representa un servidor físico de la red tiene pesos asociados. Por lo tanto, al servicio GSLB se le asigna un peso dinámico que es la suma de pesos de todos los servicios vinculados a él. El tráfico se divide entonces entre los servicios de GSLB en función de la relación entre el peso dinámico del servicio en particular y el peso total. También puede configurar pesos individuales para cada servicio GSLB en lugar del peso dinámico.

Si los servicios no tienen pesos asociados a ellos, puede configurar el servidor virtual GSLB para que utilice el número de servicios enlazados a él para calcular el peso dinámicamente.

Para obtener más información sobre cómo configurar una configuración GSLB básica, consulte Configuración de entidades GSLB individualmente.

Una vez que configure una configuración básica de GSLB, debe configurar el método de round robin ponderado de modo que el tráfico se divida entre los sitios GSLB configurados de acuerdo con los pesos configurados para los servicios individuales.

Para configurar un servidor virtual para asignar pesos a los servicios mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba uno de los siguientes comandos, dependiendo de si quiere crear un nuevo servidor virtual de equilibrio de carga o configurar uno existente:

```
add lb vserver <name>@ -weight <WeightValue> <ServiceName>
set lb vserver <name>@ -weight <WeightValue> <ServiceName>
<!--NeedCopy-->
```

Ejemplo:

```
add lb vserver Vserver-LB-1 -weight 4 Service-HTTP-1
set lb vserver Vserver-LB-1 -weight 4 Service-HTTP-1
<!--NeedCopy-->
```

Para establecer el peso dinámico mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
set gslb vserver <name> -dynamicWeight DynamicWeightType
<!--NeedCopy-->
```

Ejemplo:

```
set gslb vserver Vserver-GSLB-1 -dynamicWeight ServiceWeight
<!--NeedCopy-->
```


Para agregar pesos a los servicios GSLB mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
set gslb vserver <name> -serviceName GSLBServiceName -weight
   WeightValue
<!--NeedCopy-->
```

Ejemplo:

```
set gslb vserver Vserver-GSLB-1 -serviceName Service-GSLB-1 -weight 1
<!--NeedCopy-->
```

Para configurar un servidor virtual para asignar pesos a los servicios mediante la utilidad de configuración

1. Vaya a Administración del tráfico > Equilibrio de carga > Servidores virtuales y haga doble clic en el servidor virtual (por ejemplo, VServer-LB-1).
2. Haga clic en la sección Servicios y establezca el peso de un servicio.

Para agregar pesos a los servicios GSLB mediante la utilidad de configuración

1. Vaya a Administración del tráfico > GSLB > Servidores virtuales y haga doble clic en el servidor virtual (por ejemplo, VServer-GSLB-1)
2. Haga clic en la sección Servicios y establezca el peso del servicio en el campo Peso.

Para establecer el peso dinámico mediante la utilidad de configuración

1. Vaya a Administración del tráfico > GSLB > Servidores virtuales y haga doble clic en el servidor virtual (por ejemplo, VServer-GSLB-1).
2. Haga clic en la sección **Método** y, en la lista desplegable **Peso dinámico**, seleccione **SERVICEWEIGHT**.

Configuración de la recuperación ante desastres con persistencia del centro de datos

La persistencia del centro de datos es necesaria para las aplicaciones web que requieren mantener una conexión con el mismo servidor en lugar de equilibrar la carga de las solicitudes. Por ejemplo, en

un portal de comercio electrónico, mantener una conexión entre el cliente y el mismo servidor es fundamental. Para tales aplicaciones, la persistencia de redireccionamiento HTTP se puede configurar en una configuración activa-activa.

Para configurar GSLB para recuperación ante desastres con persistencia del centro de datos, primero debe configurar la configuración básica de GSLB y, a continuación, configurar la persistencia de redireccionamiento HTTP.

Primero cree dos sitios GSLB, locales y remotos. A continuación, para el sitio local, cree un servidor virtual GSLB y servicios GSLB y vincule los servicios al servidor virtual. A continuación, cree servicios ADNS y vincule el dominio para el que está configurando GSLB al servidor virtual GSLB en el sitio local. A continuación, cree un servidor virtual de equilibrio de carga con la misma dirección IP del servidor virtual que el servicio GSLB. Por último, duplique los pasos anteriores para la configuración remota o configure el dispositivo Citrix ADC para que sincronice automáticamente la configuración de GSLB.

Para obtener más información sobre cómo configurar una configuración GSLB básica, consulte Configuración de entidades GSLB individualmente.

Una vez que haya configurado una configuración básica de GSLB, configure la precedencia de redirección HTTP para habilitar la persistencia del centro de datos.

Para configurar la redirección HTTP mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para configurar la redirección HTTP y verificar la configuración:

```
set gslb service <serviceName> -sitePersistence <sitePersistence> -
   sitePrefix <string>
show gslb service <serviceName>
<!--NeedCopy-->
```

Ejemplo:

```
set gslb service Service-GSLB-1 -sitePersistence HTTPRedirect -
   sitePrefix vserver-GSLB-1
show gslb service Service-GSLB-1
<!--NeedCopy-->
```


Para configurar la redirección HTTP mediante la utilidad de configuración

1. Vaya a Administración del tráfico > GSLB > Servicios y haga doble clic en el servicio GSLB que quiera configurar.
2. Haga clic en la sección **Persistencia del sitio**, seleccione la opción **HttpRedirect** y, en el cuadro de texto **Prefijo** del sitio, escriba el prefijo del sitio (por ejemplo, VServer-GSLB-1).

> **Nota**
>
> Cuando la persistencia del sitio no está configurada y si un servidor virtual de equilibrio de carga configurado como un servicio GSLB local está DOWN, las solicitudes HTTP se redirigen a otros sitios GSLB sanos mediante una redirección 302.

Anular el comportamiento de proximidad estática mediante la configuración de ubicaciones preferidas

August 20, 2021

Es posible que quiera dirigir el tráfico desde un servidor o red DNS local (LDNS) a un servicio GSLB distinto del servicio GSLB que el método de proximidad estática selecciona para ese tráfico. Es decir, usted tiene una
ubicación preferida para ese tráfico. Para anular el método de proximidad estática con ubicaciones preferidas, puede hacer lo siguiente:

1. Configure una acción DNS que consta de una lista de ubicaciones preferidas. Para obtener más información sobre la configuración de una acción DNS, consulte Configuración de una acción DNS.
2. Configure una directiva DNS para identificar el tráfico que llega desde el servidor o red LDNS para el que quiere anular la proximidad estática, y aplique la acción en la directiva.
3. Enlazar la directiva al punto de enlace de solicitud global.

En la acción DNS, puede configurar una lista de hasta 8 ubicaciones preferidas. Las ubicaciones deben proporcionarse en la notación de calificador punteado, que es la notación en la que se agregan ubicaciones personalizadas a la base de datos de proximidad estática. Las ubicaciones pueden incluir comodines para los calificadores que quiere omitir. Para obtener información sobre la notación de calificador punteado para ubicaciones, consulte Adición de entradas personalizadas a una base de datos de proximidad estática. Al introducir las ubicaciones preferidas, debe introducirlas en el orden descendente de prioridad.

Cuando una directiva se evalúa como
TRUE, el dispositivo Citrix ADC hace coincidir las ubicaciones preferidas, en orden de prioridad, con las ubicaciones de los servicios GSLB. Las coincidencias son de los dos tipos siguientes:

- Si todos los calificadores no comodín en una ubicación preferida coinciden con los calificadores correspondientes en la ubicación de un servicio GSLB, la coincidencia se considera una coincidencia perfecta. Por ejemplo, una ubicación de servicio GSLB de *.UK.*.* o Europe.uk.*.* es una combinación perfecta para la ubicación preferida *.UK.*.*.
- Si solo coincide un subconjunto de los calificadores no comodín, la coincidencia se considera una coincidencia parcial. Por ejemplo, una ubicación de servicio GSLB de Europe.eg es una coincidencia parcial para la ubicación preferida Europe.uk.

Cuando una directiva DNS se evalúa como
TRUE, se utiliza el siguiente algoritmo para seleccionar un servicio GSLB:

1. El dispositivo evalúa la ubicación preferida que tiene la prioridad más alta y desplaza hacia abajo el orden de prioridad hasta que se encuentra una coincidencia perfecta entre una ubicación preferida y la ubicación de un servicio GSLB.

   Si se encuentra una coincidencia perfecta, el dispositivo comprueba si el servicio GSLB correspondiente está activo. Si está activo, devuelve la dirección IP del servicio GSLB en la respuesta DNS. Si se encuentran varias coincidencias perfectas (lo que puede ocurrir cuando se usan uno o más comodines en una ubicación preferida), el dispositivo comprueba el estado de cada uno de los servicios GSLB correspondientes y equilibra la carga los servicios GSLB que están activos.

2. Si no se encuentra una coincidencia perfecta para ninguna de las ubicaciones preferidas, el dispositivo vuelve a la ubicación preferida que tiene la prioridad más alta y baja el orden de prioridad hasta que se encuentre una coincidencia parcial entre una ubicación preferida y la ubicación de un servicio GSLB.

   Si se encuentra una coincidencia parcial, el dispositivo comprueba si el servicio GSLB correspondiente está activo. Si está activo, devuelve la dirección IP del servicio GSLB en la respuesta DNS. Si se encuentran varias coincidencias parciales, el dispositivo comprueba el estado de cada uno de los servicios GSLB correspondientes y equilibra la carga los servicios GSLB que están activos.

3. Si ninguna de las coincidencias perfectas y parciales está disponible, la carga del dispositivo equilibra todos los demás servicios GSLB disponibles.

   De este modo, el dispositivo implementa un tipo de afinidad de sitio por el tráfico que coincide con la directiva DNS.

Ejemplo

Considere una configuración de GSLB que consta de los siguientes ocho servicios de GSLB:

- Asia.in
- Asia.JPN
- Asia.hk
- Europa.UK

- Europe.ru
- Europa.EG
- África.SD
- África.ZMB

Considere la siguiente acción DNS y configuración de directivas:

```
1 > add dns action prefLoc11 GslbPrefLoc -preferredLocList ”Asia.HK” ”
     Europe.UK”
2  Done
3 > add dns policy dnsPolPrefLoc ”CLIENT.IP.SRC.MATCHES_LOCATION(”\*.ZMB
     .\*.*”)” prefLoc11
4  Done
5 <!--NeedCopy-->
```

Cuando el dispositivo recibe una solicitud de la *ubicación.ZMB..**, las ubicaciones preferidas se evalúan de la siguiente manera:

1. El dispositivo intenta encontrar un servicio GSLB cuya ubicación coincide perfectamente con Asia.hk, que es la ubicación preferida que tiene la máxima prioridad. Encuentre que el servicio GSLB en Asia.hk es una combinación perfecta. Si el servicio GSLB está activo, envía al cliente la dirección IP del servicio GSLB.
2. Si el servicio GSLB en Asia.hk está inactivo, el dispositivo intenta encontrar una coincidencia perfecta para la segunda ubicación preferida, Europe.uk. Considera que el servicio GSLB en Europe.uk es una combinación perfecta. Si el servicio GSLB está activo, envía al cliente la dirección IP del servicio.
3. Si el servicio GSLB en Europe.uk está caído, vuelve a la ubicación preferida que tiene la prioridad más alta, Asia.hk, y busca coincidencias parciales. Para Asia.hk, encuentra que Asia.in y Asia.jpn son coincidencias parciales. Si solo uno de los servicios GSLB correspondientes está activo, envía al cliente la dirección IP del servicio. Si ambas ubicaciones están activas, equilibra la carga los dos servicios.
4. Si todas las coincidencias parciales para Asia.hk están inactivas, el dispositivo busca coincidencias parciales para Europe.uk. Encuentre que Europe.ru y Europe.eg son coincidencias parciales para la ubicación preferida. Si solo uno de los servicios GSLB correspondientes está activo, envía al cliente la dirección IP del servicio. Si ambas ubicaciones están activas, equilibra la carga los dos servicios.
5. Si todas las coincidencias parciales para Europe.uk están inactivas, la carga del dispositivo equilibra todos los demás servicios GSLB disponibles. En el ejemplo actual, la carga del dispositivo equilibra Africa.sd y Africa.zmb porque se ha comprobado que los seis servicios GSLB restantes están inactivos.

Configurar la selección de servicios GSLB mediante la conmutación de contenido

August 20, 2021

En una implementación típica de GSLB, puede priorizar la selección de un conjunto de servicios de GSLB enlazados a un servidor virtual de GSLB, pero no puede hacer lo siguiente:

- Restringir la selección de un servicio GSLB de un subconjunto de servicios GSLB enlazados a un servidor virtual GSLB para el dominio dado.
- Aplicar diferentes métodos de equilibrio de carga en los diferentes subconjuntos de servicios GSLB en la implementación.
- Aplique directivas de desbordamiento en un subconjunto de servicios GSLB y no puede tener una copia de seguridad para un subconjunto de servicios GSLB.
- Configure un subconjunto de servicios GSLB para servir contenido diferente. Es decir, no puede cambiar de contenido entre servidores en diferentes sitios GSLB. La configuración de GSLB asume que los servidores contienen el mismo contenido.
- Defina un servicio GSLB de subconjunto con diferentes prioridades y especifique un orden en el que los servicios del subconjunto se aplican a una solicitud.

Ahora puede configurar una directiva de conmutación de contenido (CS) para personalizar la implementación de GSLB. Primero configure un conjunto de servicios GSLB y lo vincule a un servidor virtual GSLB. A continuación, configure un servidor virtual CS de tipo GSLB de destino, defina una directiva CS y una acción con el servidor virtual GSLB como servidor virtual de destino y vincule la directiva CS al servidor virtual CS.

> **Importante**
>
> - Solo las directivas CS con expresiones basadas en DNS se pueden enlazar a un servidor virtual CS del tipo GSLB de destino.
> - Si un servicio GLSB está enlazado a un servidor virtual CS a través de un servidor virtual GSLB, no puede enlazar otro servidor virtual GSLB vinculado con el mismo servicio GSLB al servidor virtual CS.

Ejemplo

Considere una implementación GLSB que incluya dos sitios GSLB. En cada sitio, cuatro servicios GSLB (S-1, S-2, S-3 y S-4) están enlazados al servidor virtual VS-1 de GSLB. Puede configurar un servidor virtual de conmutación de contenido (CS) de tipo GSLB de destino y definir una directiva de CS y una acción con VS-1 como servidor virtual de destino, de modo que las solicitudes de contenido en inglés solo sean atendidas por S-1 y S-2, y las solicitudes de contenido en el idioma local solo se sirven por S-3 y S-4.

Puede dar prioridad a S-1 configurando un servidor virtual de copia de seguridad en VS-1 y vinculando

S-2 al servidor virtual de copia de seguridad. S-1 atiende las solicitudes del cliente. Si el servidor S-1 representa se apaga, S-2 sirve las solicitudes. Si tanto S-1 como S-2 están inactivas, los clientes reciben una respuesta vacía.

Para configurar la selección de servicios GSLB mediante Content Switching:

1. Configurar GSLB. Para obtener instrucciones, consulte Configuración del equilibrio de carga global del servidor.
2. Configure un servidor virtual de Content Switching (CS) del tipo de destino GSLB. Para obtener más información, consulte Creación de servidores virtuales de conmutación de contenido.
3. Configurar directivas de Content Switching (CS). Para obtener más información, consulte Configuración de directivas de conmutación de contenido.
4. Configure acciones CS que designen un servidor virtual GSLB como servidor virtual de destino. Para obtener más información, consulte Configuración de una acción de conmutación de contenido.
5. Enlazar las directivas CS al servidor virtual CS. Para obtener más información, consulte Vinculación de directivas a un servidor virtual de conmutación de contenido.
6. Enlazar el dominio al servidor virtual CS en lugar del servidor virtual GSLB.

Configuración de ejemplo

La siguiente configuración de ejemplo envía solicitudes desde el cliente con la dirección IP 5.5.5.5 a SERVICE_GSLB1 y SERVICE_GSLB2. SERVICE_GSLB1 tiene una prioridad más alta que SERVICE_GSLB2, y SERVICE_GSLB2 atiende las solicitudes del cliente solo cuando SERVICE_GSLB1 está inactiva. Si tanto SERVICE_GSLB1 como SERVICE_GSLB2 están inactivas, SERVICE_GSLB3 y Service-GSLB4 no se consideran, y se envía una respuesta en blanco al cliente.

```
add cs vs CSVSERVER_GSLB http  -targettype GSLB
Done
add gslb vs VSERVER_GSLB1 http
Done
add gslb vs VSERVER_GSLB2 http
Done
add gslb vs VSERVER_GSLB_BACKUP1 http
Done
set gslb vs VSERVER_GSLB1 -backupvserver VSERVER_GSLB_BACKUP1
Done
add gslb service SERVICE_GSLB1 1.1.1.1 HTTP 80 -sitename site1
Done
add gslb service SERVICE_GSLB2 1.1.1.2 HTTP 80 -sitename site1
Done
add gslb service SERVICE_GSLB3 1.1.1.3 HTTP 80 -sitename site2
```



```
Done
add gslb service SERVICE_GSLB4 1.1.1.4 HTTP 80 -sitename site2
Done
bind gslb vs VSERVER_GSLB1 -servicename SERVICE_GSLB1
Done
bind gslb vs VSERVER_GSLB_BACKUP1 -servicename SERVICE_GSLB2
Done
bind gslb vs VSERVER_GSLB2 -servicename SERVICE_GSLB3
Done
bind gslb vs VSERVER_GSLB2 -servicename SERVICE_GSLB4
Done
add cs action a1 -targetvserver VSERVER_GSLB1
Done
add cs policy p1 -rule "CLIENT.IP.SRC.EQ(5.5.5.5)" -action a1
Done
bind cs vs CSVSERVER_GSLB -domainName www.abc.com
Done
bind cs vs CSVSERVER_GSLB -policyname p1 -priority 1
Done
add cs action a2 -targetvserver VSERVER_GSLB2
Done
add cs policy p2 -rule "CLIENT.IP.SRC.EQ(6.6.6.6)" -action a2
Done
bind cs vs CSVSERVER_GSLB -policyname p2 -priority 2
Done
<!--NeedCopy-->
```

Asociar una expresión de servidor virtual de destino a una acción de conmutación de contenido GSLB

Ahora puede asociar una expresión de servidor virtual de destino a una acción de conmutación de contenido GSLB. Esto permite que el servidor virtual de conmutación de contenido GSLB utilice expresiones de directiva para componer el nombre del servidor virtual GSLB de destino mientras se procesan las solicitudes DNS.

Para configurar una acción de conmutación de contenido que especifique una expresión mediante la CLI

En el símbolo del sistema, escriba el comando siguiente para configurar la acción de conmutación de contenido para recuperar la respuesta de llamada HTTP.


```
add cs action <name> -targetVserverExpr <expression>
<!--NeedCopy-->
```

Ejemplo:

```
add cs action csact_GSLB_VServer -targetVserverExpr "SYS.HTTP_CALLOUT(
   GSLB_Method_API)"
<!--NeedCopy-->
```

Para configurar una acción de cambio de contenido que especifique una expresión mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Cambio de contenido > Acciones**.
2. Configure una acción de conmutación de contenido y especifique una **expresión** que calcule dinámicamente el nombre del servidor virtual de equilibrio de carga de destino.

Configurar GSLB para consultas DNS con registros NAPTR

August 20, 2021

En una implementación típica de Global Server Load Balancing (GSLB), el dispositivo Citrix ADC recibe consultas DNS para registros A/AAAA, selecciona el servicio GSLB más adecuado según el método de equilibrio de carga configurado y devuelve la dirección IP del servicio como respuesta a la consulta DNS. Ahora puede configurar el dispositivo para que reciba consultas DNS para registros NAPTR y responda con la lista de servicios configurados para un dominio. El dispositivo también supervisa el estado de los servicios y, en la respuesta, proporciona una lista de solo los servicios que están en funcionamiento.

Ejemplo:

En las implementaciones de telecomunicaciones, puede configurar un dispositivo Citrix ADC para que reciba consultas DNS con registros NAPTR de clientes como las entidades de administración móvil (MME), que desempeñan el papel de un solucionador DNS para descubrir todos los servicios que ofrece el nombre de dominio. El dispositivo responde a la consulta con registros NAPTR para todos los servicios que están en funcionamiento. El MME puede utilizar esta respuesta NAPTR para ejecutar el procedimiento S-NAPTR para seleccionar los nodos en función del servicio ofrecido, la coubicación, la cercanía topológica, etc.

Si se seleccionan varios nodos, el MME puede utilizar el campo de preferencia del registro NAPTR del dispositivo Citrix ADC para determinar el nodo.

Formato de registro NAPTR

Mientras responde a una consulta DNS con registro NAPTR, un dispositivo Citrix ADC construye un registro NAPTR de respuesta para cada servicio GSLB.

En la tabla siguiente se enumeran los archivos del registro NAPTR:

Campo	
Dominio	El dominio GSLB
TTL	Cantidad de tiempo durante el cual se puede almacenar en caché el registro NAPTR.
Class	La clase del registro. De forma predeterminada, este valor se establece en IN.
Tipo	El tipo de registro DNS.
Pedido	Especifica el orden en que DEBE procesarse el registro NAPTR. Puede especificar el orden en el servicio GSLB. De lo contrario, se establece en 1.
Preferencia	Especifica el orden en el que se deben procesar los registros NAPTR con valores iguales de “orden”, y los números bajos se procesan antes que los números altos. Si el orden no se especifica en el servicio GSLB, se establece en 1.
Marcas	Controla los aspectos de la reescritura e interpretación de los campos en el registro. El dispositivo Citrix ADC establece este valor en A.
Servicio	Especifica los servicios disponibles.
Expresión regular	Las expresiones regulares no son compatibles, por lo que este valor se establece en NULL.
Sustitución	El nombre de dominio del nodo que aloja los servicios.

Procedimiento de configuración

Para obtener instrucciones detalladas de configuración de GSLB, consulte Configuración del equilibrio de carga global del servidor (GSLB). Asegúrese de hacer lo siguiente:

- Establezca los siguientes parámetros al agregar el servidor virtual GSLB:
  - ServiceType: CUALQUIERA
  - DNSRecordType: NAPTR
  - LBMétodo: CUSTOMLOAD

Ejemplo:

```
add gslb vserver gslb_vs ANY -dnsRecordType NAPTR -lbMethod CUSTOMLOAD
<!--NeedCopy-->
```

- Al agregar un sitio GSLB, establezca el parámetro *NAPTRReplacementSuffix* en el nombre de dominio que quiere incrustar en los registros NAPTR.

Ejemplo:

```
add gslb site site1 10.102.218.200  -naptrReplacementSuffix example.com
<!--NeedCopy-->
```

- Defina los siguientes parámetros al agregar el servicio GSLB:
  - reemplazo de la siesta
  - Orden NAPTROrder
  - Servicios NAPTRs
  - NAPTRDomainttl
  - Preferencia NAPTRs

Configuración de ejemplo

```
add gslb vserver gslb_vs ANY -dnsRecordType NAPTR -lbMethod CUSTOMLOAD

Done

add gslb site site1 10.102.218.200  -naptrReplacementSuffix example.com

Done

add gslb service sgw1 3.3.3.13 ANY *  -siteName site1 -naptrreplacement
    sgw1.site1. -naptrOrder 2 -naptrServices x-3gpp-sgw:x-s5-gtp -
   naptrDomainTTL 20 -naptrPreference   200

Done

```



```
13 add gslb service sgw2 3.3.3.11 ANY *  -siteName site1 -naptrreplacement
       sgw2.site1. -naptrOrder 5 -naptrServices x-3gpp-sgw:x-s5-gtp  -
      naptrDomainTTL 20  naptrPreference  100
14
15 Done
16
17 add gslb service sgw3 3.3.3.12 ANY *  -siteName site2 -naptrreplacement
       sgw3.site1. -naptrOrder 10 -naptrServices x-3gpp-sgw:x-s5-gtp  -
      naptrDomainTTL 20 naptrPreference   300
18
19 bind gslb vserver gslb_vs -serviceName sgw1
20
21 Done
22
23 bind gslb vserver gslb_vs -serviceName sgw2
24
25 Done
26
27 bind gslb vserver gslb_vs -serviceName sgw3
28
29 Done
30
31 bind gslb service sgw1 -monitorName ping
32
33 Done
34
35 bind gslb service sgw2 -monitorName ping
36
37 Done
38
39 bind gslb service sgw3 -monitorName ping
40
41 Done
42
43 bind gslb vserver gslb_vs -domainName gslb.com -TTL 5
44
45 Done
46 <!--NeedCopy-->
```

> **Nota**
>
> Las consultas DNS con registros NAPTR no se admiten en la configuración principal-secundario.

Configurar GSLB para dominio comodín

July 8, 2022

Puede vincular un dominio DNS comodín a un servidor virtual GSLB. Los usuarios que acceden a las aplicaciones detrás de un dominio comodín se dirigen al mejor centro de datos óptimo, que aloja esas aplicaciones. El dominio comodín gestiona las solicitudes de dominios y subdominios inexistentes. Para obtener más información sobre los dominios comodín, consulte Compatibilidad con dominios DNS comodín. Para obtener información sobre las zonas DNS, consulte Configurar una zona DNS.

Para configurar GSLB para un dominio comodín, primero debe configurar la configuración básica de GSLB. Para obtener más información sobre cómo configurar una configuración GSLB básica, consulte Configuración de entidades GSLB individualmente.

Para configurar una configuración de GSLB para un dominio comodín mediante la CLI

Siga pasos para configurar una configuración de GSLB para el dominio comodín:

1. Cree los sitios de GSLB.

```
add gslb site site1 10.0.1.10
add gslb site site2 20.0.1.10
<!--NeedCopy-->
```

2. Agregue los servicios GSLB para cada sitio que participe en la configuración de GSLB.

```
add gslb service svc1 -sitename site1 10.0.1.10  http 80
add gslb service svc2 -sitename site1 10.0.1.10  http 80
add gslb service svc3 -sitename site2 20.0.1.10  http 80
add gslb service svc4 -sitename site2 20.0.1.10  http 80
<!--NeedCopy-->
```

3. Agregue el servidor virtual GSLB que hace referencia a un servicio que se está usando en la configuración de GSLB.

```
add gslb vserver gslb_vs http
<!--NeedCopy-->
```

4. Agregue un servicio ADNS que escuche las consultas de DNS.


```
add service adns_udp 10.14.39.21 ADNS 53
<!--NeedCopy-->
```

5. Enlazar los servicios GSLB al servidor virtual GSLB.

```
bind gslb vserver gslb_vs -service svc1
bind gslb vserver gslb_vs -service svc2
bind gslb vserver gslb_vs -service svc3
bind gslb vserver gslb_vs -service svc4
<!--NeedCopy-->
```

6. Cree una zona.

```
add dns soaRec test.com -originServer n1.test.com -contact n1.test
    .com
add dns nsrec test.com n1.test.com
add dns nsrec test.com n2.test.com
add dns zone test.com -proxymode no
<!--NeedCopy-->
```

7. Enlazar el nombre de dominio al servidor virtual GSLB.

```
bind gslb vserver gslb_vs -domainName *.test.com
<!--NeedCopy-->
```

Utilice la opción de subred cliente EDNS0 para Equilibrio de carga de servidor global

January 12, 2021

La subred de cliente de EDNS (ECS) es una extensión de encabezado de Servidor de nombres de dominio (DNS) que proporciona los detalles de la subred del cliente. Puede utilizar estos detalles para mejorar la precisión de Citrix ADC Global Server Load Balancing (GSLB) mediante la ubicación de red del cliente en lugar de la ubicación de resolución DNS para determinar la cercanía topológica del cliente.

> **Nota**
>
> Citrix ADC solo admite EDNS0.

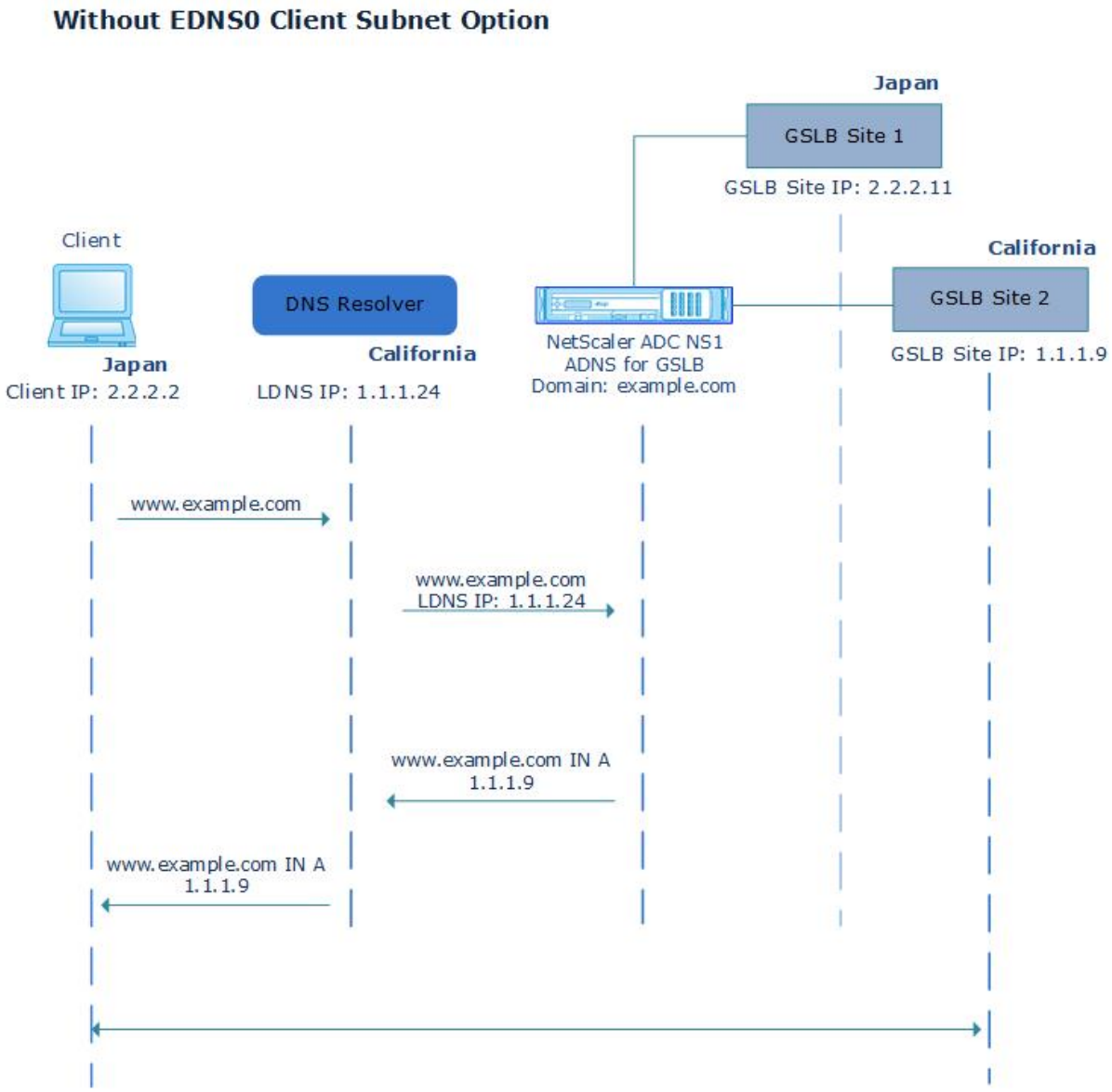
Importante:

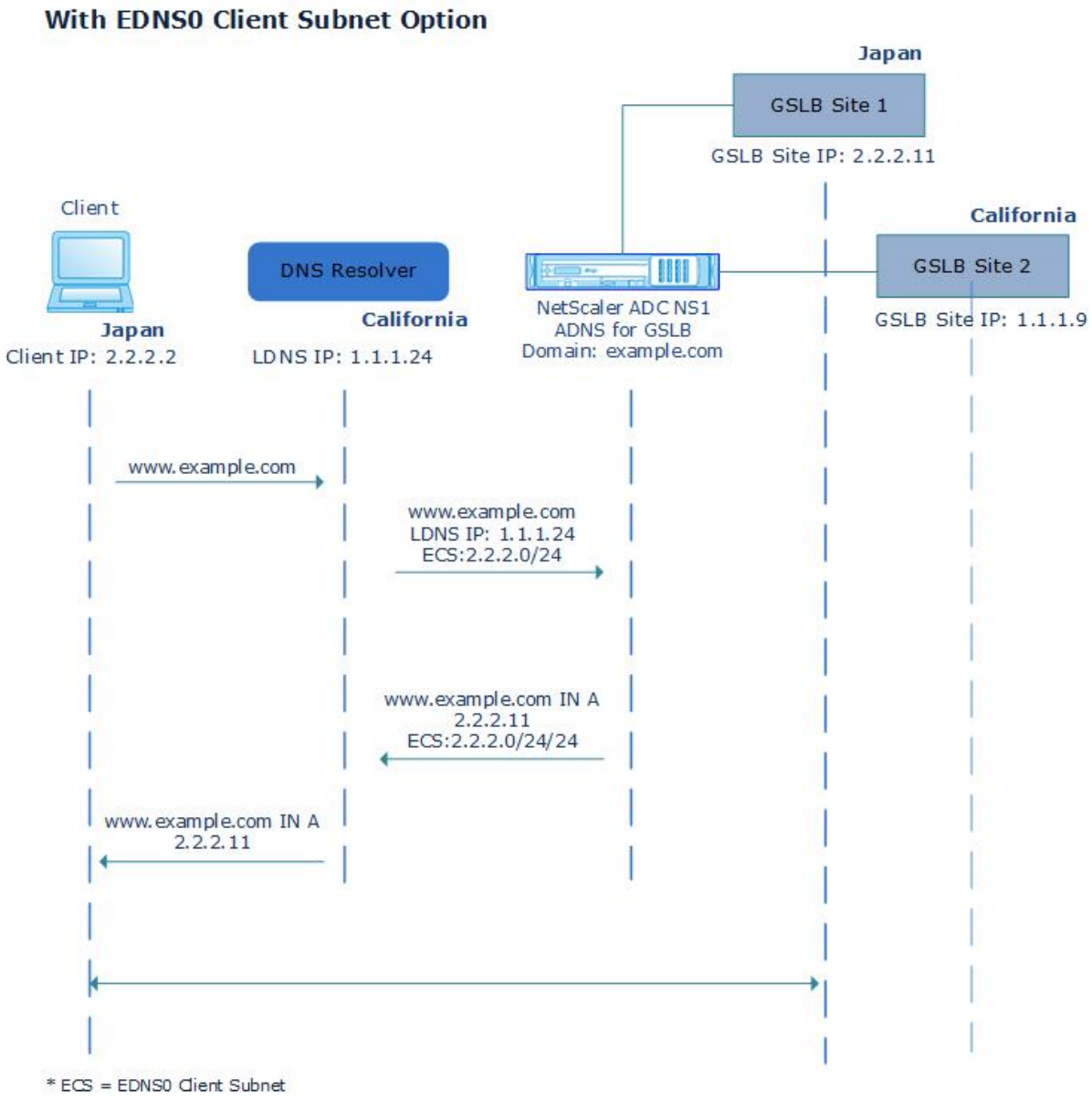
> Asegúrese de que el Servidor de nombres de dominio local (LDNS) de la implementación admite la subred cliente EDNS0, de modo que las consultas DNS entrantes contengan la opción Subred de cliente EDNS0 y el dispositivo Citrix ADC utilice la dirección ECS mientras procesa la consulta DNS.

El dispositivo Citrix ADC utiliza la dirección IP LTNS para determinar la cercanía topológica del cliente y realiza GSLB de este modo cuando se utilizan métodos de equilibrio de carga basados en proximidad, como proximidad estática o tiempo dinámico de ida y vuelta (RTT). Sucede en una implementación GSLB típica. Sin embargo, cuando un solucionador DNS centralizado, como Google DNS u OpenDNS, está involucrado en la implementación, el dispositivo Citrix ADC envía la solicitud DNS a un centro de datos cercano a la resolución DNS centralizada, que puede no estar cerca del cliente. Por ejemplo, en una implementación típica de Citrix ADC GSLB que utiliza el método de equilibrio de carga de proximidad estática, se envía una solicitud de usuario final de Japón a un centro de datos de Japón y una solicitud de usuario final de California se envía a un centro de datos de California. Pero si se trata de un solucionador DNS centralizado, el dispositivo Citrix ADC podría enviar una solicitud desde Japón a un centro de datos de California.

Puede utilizar la opción ECS en implementaciones que incluyen el dispositivo Citrix ADC configurado como servidor DNS autoritativo (ADNS) para un dominio GSLB. Si utiliza proximidad estática como método de equilibrio de carga, puede utilizar la subred IP en el encabezado EDNS en lugar de la dirección IP LDNS. Esto ayuda a determinar la proximidad geográfica del cliente. En la implementación en modo proxy, el dispositivo Citrix ADC reenvía una consulta DNS habilitada para ECS tal como está a los servidores back-end. El dispositivo no almacena en caché las respuestas DNS habilitadas para ECS.

> **Nota**
>
> La opción ECS no es aplicable a todos los demás modos de implementación, como el modo ADNS para dominios que no son GSLB, el modo de resolución y el modo de reenvío. El dispositivo Citrix ADC omite la opción ECS en los modos mencionados anteriormente. Además, de forma predeterminada, ECS está inhabilitado para la implementación de GSLB.





Para habilitar la opción Subred Cliente EDNS0 mediante la interfaz de línea de comandos:

En el símbolo del sistema, escriba:

```
set gslb vserver <vserver_name> **-ECS ENABLED

set gslb vserver vserver-GSLB-1 -ECS ENABLED
<!--NeedCopy-->
```


Validación de direcciones

Puede configurar un servidor virtual GSLB para comprobar que la dirección devuelta por la opción EDNS0 Client Subnet (ECS) de la consulta DNS no es una dirección IP privada o no enrutable. Con la validación de direcciones habilitada, el dispositivo Citrix ADC omite la dirección ECS en la consulta DNS si aparece en la tabla siguiente y, en su lugar, utiliza la dirección IP LDNS para el equilibrio de carga global del servidor.

> **Nota**
>
> De forma predeterminada, la validación de direcciones está inhabilitada.

Tipo de dirección	Dirección	Descripción
IPV4	10.0.0.0/8	Para uso privado.
	172.16.0.0/12	Para uso privado.
	192.168.0.0/16	Para uso privado.
	0.0.0.0/8	Hace referencia al host de la red
	100.64.0.0/10	Espacio de direcciones compartido
	127.0.0.0/8	Dirección de bucle invertido
	169.254.0.0/16	Enlace a la dirección IPv4 local tal como se define en RFC 3927
	192.0.0.0/24	Se utiliza para asignaciones de protocolo IETF, incluye el espacio privado 192.168.0.0/16
	192.0.2.0/24	Utilizado con fines de documentación
	192.88.99.0/24	Utilizado para 6to4 Relay Anycast
	198.18.0.0/15	Utilizado en pruebas de referencia de dispositivos
	198.51.100,0/24	Utilizado con fines de documentación
	203.0.113.0/24	Utilizado con fines de documentación

Tipo de dirección	Dirección	Descripción
	240.0.0.0/4	Utilizado como reservado
	255,255,255,255/32	Utilizado para la difusión
IPv6	::1/128	dirección de bucle invertido
	::/128	dirección no especificada
	::ffff:0:0/96	Dirección asignada a IPv4
	100::/64	bloque de direcciones de solo descarte
	2001::/23	Utilizado para asignaciones de protocolo IETF
	2001::/32	TEREDO
	2001:2::/48	Utilizado para la evaluación comparativa
	2001:db8::/32	Utilizado con fines de documentación
	2001:10::/28	ORQUÍDEA
	2002::/16	Utilizado para 6to4 Relay Anycast
	fc00::/7	Único-local
	fe80::/10	Direcciones de unidifusión locales de vínculo

Para habilitar la validación de direcciones mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
set gslb vserver <vserver_name> -ecsAddrValidation ENABLED

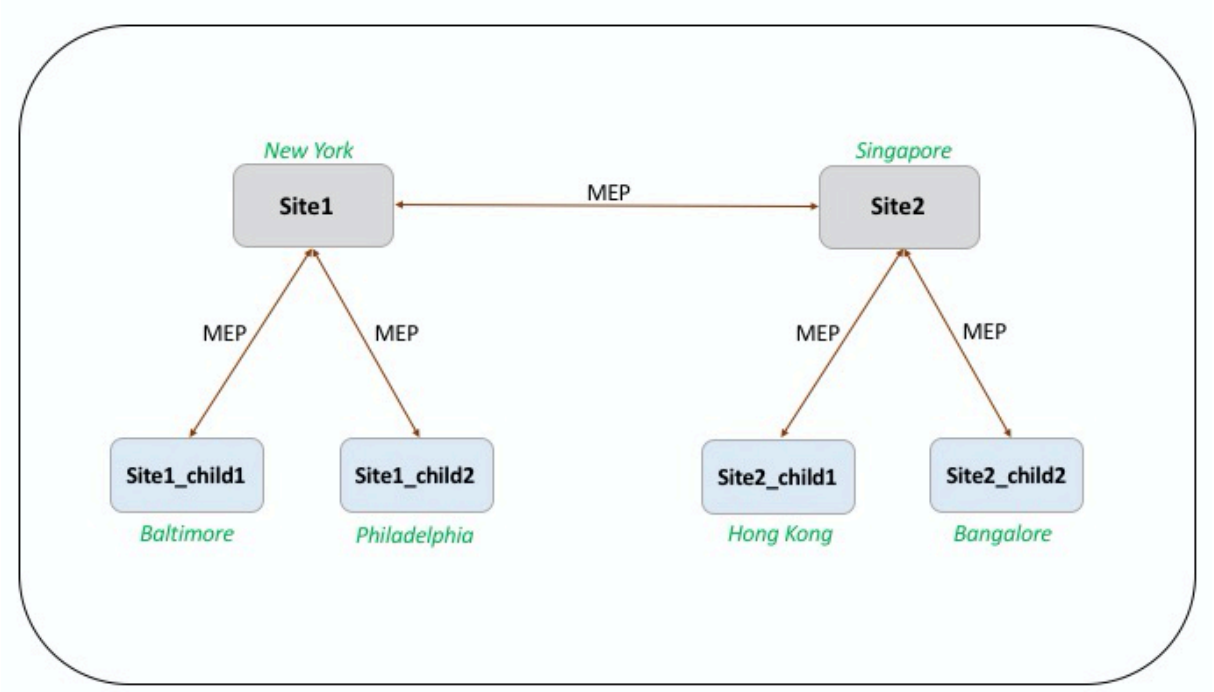
set gslb vserver vserver-GSLB-1 -ecsAddrValidation ENABLED
<!--NeedCopy-->
```


Ejemplo de una configuración principal-secundario completa mediante el protocolo de intercambio de métricas

August 20, 2021

Considere la siguiente topología principal-secundario en la que los sitios GSLB se distribuyen globalmente.

- Site1 y Site2 son los sitios principales.
- Site1_Child1 y Site1_Child2 son los sitios secundarios del Site1.
- Site2_Child1 y Site2_Child2 son los sitios secundarios del Site2.



Los siguientes comandos ilustran la configuración completa de la topología principal-secundario.

site1

```
1 add gslb site site1 10.102.82.164 -publicIP 10.102.82.164
2
3 add gslb site site2 10.106.24.164 -publicIP 10.106.24.164
4
5 add gslb site site1_child1 10.102.82.131 -publicIP 10.102.82.131 -
     nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
     site1
6
```



```
7  add gslb site site1_child2 10.102.82.67 -publicIP 10.102.82.67 -
       nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
       site1
8
9  add gslb site site2_child1 10.106.24.132 -publicIP 10.106.24.132 -
       nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
       site2
10
11 add gslb site site2_child2 10.106.24.67 -publicIP 10.106.24.67 -
       nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
       site2
12
13 add gslb service site1_child1_http_gsvc1 10.102.82.132 HTTP 80 -
       publicIP 10.102.82.132 -publicPort 80 -maxClient 0 -siteName
       site1_child1 -cltTimeout 180 -svrTimeout 360 -downStateFlush ENABLED
14
15 add gslb service site1_child2_http_gsvc1 10.102.82.68 HTTP 80 -publicIP
        10.102.82.68 -publicPort 80 -maxClient 0 -siteName site1_child2 -
       cltTimeout 180 -svrTimeout 360 -downStateFlush ENABLED
16
17 add gslb service site2_child1_http_gsvc1 10.106.24.134 HTTP 80 -
       publicIP 10.106.24.134 -publicPort 80 -maxClient 0 -siteName
       site2_child1 -cltTimeout 180 -svrTimeout 360 -downStateFlush ENABLED
18
19 add gslb service site2_child2_http_gsvc1 10.106.24.68 HTTP 80 -publicIP
        10.106.24.68 -publicPort 80 -maxClient 0 -siteName site2_child2 -
       cltTimeout 180 -svrTimeout 360 -downStateFlush ENABLED
20
21 add gslb vserver gv1 HTTP -backupLBMethod ROUNDROBIN -tolerance 0 -
       appflowLog DISABLED
22
23 bind gslb vserver gv1 -serviceName site1_child1_http_gsvc1
24
25 bind gslb vserver gv1 -serviceName site1_child2_http_gsvc1
26
27 bind gslb vserver gv1 -serviceName site2_child2_http_gsvc1
28
29 bind gslb vserver gv1 -serviceName site2_child1_http_gsvc1
30
31 bind gslb vserver gv1 -domainName www.gslb.com -TTL 5
32 <!--NeedCopy-->
```

site1_child1


```
add gslb site site1 10.102.82.164 -publicIP 10.102.82.164

add gslb site site1_child1 10.102.82.131 -publicIP 10.102.82.131 -
    nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
    site1
<!--NeedCopy-->
```

Puede agregar los siguientes comandos para la configuración de equilibrio de carga:

```
add service svc1 10.102.82.25 HTTP 80 -gslb NONE -maxClient 0 -maxReq 0
     -cip DISABLED -usip NO -useproxyport YES -sp ON -cltTimeout 180 -
    svrTimeout 360 -CKA NO -TCPB NO -CMP NO

add lb vserver lb1 HTTP 10.102.82.132 80 -persistenceType NONE -
    cltTimeout 180

bind lb vserver lb1 svc1
<!--NeedCopy-->
```

site1_child2

```
add gslb site site1 10.102.82.164 -publicIP 10.102.82.164

add gslb site site1_child2 10.102.82.67 -publicIP 10.102.82.67 -
    nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
    site1

You can add the following commands for load balancing configuration:

add service svc1 10.102.82.25 HTTP 80 -gslb NONE -maxClient 0 -maxReq 0
     -cip DISABLED -usip NO -useproxyport YES -sp OFF -cltTimeout 180 -
    svrTimeout 360 -CKA NO -TCPB NO -CMP NO

add lb vserver lb1 HTTP 10.102.82.68 80 -persistenceType NONE -
    cltTimeout 180

bind lb vserver lb1 svc1
<!--NeedCopy-->
```


site2

```
add gslb site site1 10.102.82.164 -publicIP 10.102.82.164

add gslb site site2 10.106.24.164 -publicIP 10.106.24.164

add gslb site site1_child1 10.102.82.131 -publicIP 10.102.82.131 -
    nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
    site1

add gslb site site1_child2 10.102.82.67 -publicIP 10.102.82.67 -
    nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
    site1

add gslb site site2_child1 10.106.24.132 -publicIP 10.106.24.132 -
    nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
    site2

add gslb site site2_child2 10.106.24.67 -publicIP 10.106.24.67 -
    nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
    site2

add gslb service site1_child1_http_gsvc1 10.102.82.132 HTTP 80 -
    publicIP 10.102.82.132 -publicPort 80 -maxClient 0 -siteName
    site1_child1 -cltTimeout 180 -svrTimeout 360 -downStateFlush ENABLED

add gslb service site1_child2_http_gsvc1 10.102.82.68 HTTP 80 -publicIP
     10.102.82.68 -publicPort 80 -maxClient 0 -siteName site1_child2 -
    cltTimeout 180 -svrTimeout 360 -downStateFlush ENABLED

add gslb service site2_child1_http_gsvc1 10.106.24.134 HTTP 80 -
    publicIP 10.106.24.134 -publicPort 80 -maxClient 0 -siteName
    site2_child1 -cltTimeout 180 -svrTimeout 360 -downStateFlush ENABLED

add gslb service site2_child2_http_gsvc1 10.106.24.68 HTTP 80 -publicIP
     10.106.24.68 -publicPort 80 -maxClient 0 -siteName site2_child2 -
    cltTimeout 180 -svrTimeout 360 -downStateFlush ENABLED

add gslb vserver gv1 HTTP -backupLBMethod ROUNDROBIN -tolerance 0 -
    appflowLog DISABLED

bind gslb vserver gv1 -serviceName site1_child1_http_gsvc1

bind gslb vserver gv1 -serviceName site1_child2_http_gsvc1
```



```
26
27 bind gslb vserver gv1 -serviceName site2_child2_http_gsvc1
28
29 bind gslb vserver gv1 -serviceName site2_child1_http_gsvc1
30
31 bind gslb vserver gv1 -domainName www.gslb.com -TTL 5
32 <!--NeedCopy-->
```

site2_child1

```
1 add gslb site site2 10.106.24.164 -publicIP 10.106.24.164
2
3 add gslb site site2_child1 10.106.24.132 -publicIP 10.106.24.132 -
     nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
     site2
4 <!--NeedCopy-->
```

You can add the following commands for load balancing configuration:

```
1 add service svc1 10.102.82.25 HTTP 80 -gslb NONE -maxClient 0 -maxReq 0
      -cip DISABLED -usip NO -useproxyport YES -sp ON -cltTimeout 180 -
     svrTimeout 360 -CKA NO -TCPB NO -CMP NO
2
3 add lb vserver lb1 HTTP 10.106.24.134 80 -PersistenceType NONE -
     CLTTimeout 180
4
5 enlace lb vserver lb1 svc1
6 <!--NeedCopy-->
```

site2_child2

```
1 add gslb site site2 10.106.24.164 -publicIP 10.106.24.164
2
3 add gslb site site2_child2 10.106.24.67 -publicIP 10.106.24.67 -
     nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
     site2
4 <!--NeedCopy-->
```

You can add the following commands for load balancing configuration:


```
add service svc1 10.102.82.25 HTTP 80 -gslb NONE -maxClient 0 -maxReq 0
     -cip DISABLED -usip NO -useproxyport YES -sp ON -cltTimeout 180 -
    svrTimeout 360 -CKA NO -TCPB NO -CMP NO

add lb vserver lb1 HTTP 10.106.24.68 80 -PersistenceType NONE -
    CLTTimeout 180

bind lb vserver lb1 svc1
\`\`\`
<!--NeedCopy-->
```

Equilibrio de carga de enlaces

February 16, 2021

El equilibrio de carga de enlace (LLB) equilibra el tráfico saliente a través de varias conexiones de Internet proporcionadas por diferentes proveedores de servicios. LLB permite que el dispositivo Citrix ADC supervise y controle el tráfico para que los paquetes se transmitan sin problemas a través del mejor enlace posible. A diferencia del equilibrio de carga del servidor, donde un servicio representa un servidor, con LLB, un servicio representa un enrutador o el salto siguiente. Un vínculo es una conexión entre el dispositivo Citrix ADC y el enrutador.

Para configurar el equilibrio de carga de vínculos, muchos usuarios comienzan por configurar una configuración básica con valores predeterminados. Una configuración básica incluye servicios, servidores virtuales, monitores, rutas, un método LLB y persistencia (opcional). Una vez que una configuración básica esté operativa, puede personalizarla para su entorno.

Los métodos de equilibrio de carga aplicables a LLB son round robin, hash IP de destino, menos ancho de banda y menos paquetes. Opcionalmente, puede configurar la persistencia para que las conexiones se mantengan en un vínculo específico. Los tipos de persistencia disponibles están basados en dirección IP de origen, dirección IP de destino y dirección IP de origen y dirección IP de destino. PING es el monitor predeterminado, pero se recomienda configurar un monitor transparente.

Puede personalizar la configuración configurando NAT inversa (RNAT) y enlaces de copia de seguridad.

Configuración de una Configuración Básica de LLB

August 20, 2021

Para configurar LLB, primero debe crear servicios que representen cada enrutador a los proveedores de servicios de Internet (ISP). Un monitor PING está enlazado de forma predeterminada a cada servicio. Encuadernar un monitor transparente es opcional, pero se recomienda. A continuación, crea un servidor virtual, vincula los servicios al servidor virtual y configura una ruta para el servidor virtual. La ruta identifica el servidor virtual como la Gateway a los enrutadores físicos representados por los servicios. El servidor virtual selecciona un enrutador mediante el método de equilibrio de carga que especifique. Opcionalmente, puede configurar la persistencia para asegurarse de que todo el tráfico de una sesión determinada se envía a través de un vínculo específico.

Para configurar una configuración básica de LLB, haga lo siguiente:

- Configurar servicios
- Configurar un servidor virtual LLB y vincular un servicio
- Configurar el método LLB y la persistencia
- Configurar una ruta LLB
- Crear y enlazar un monitor transparente

Configurar servicios

Un monitor predeterminado (PING) se enlaza automáticamente a un tipo de servicio ANY cuando se crea el servicio, pero puede reemplazar el monitor predeterminado por un monitor transparente, como se describe en Creación y vinculación de un monitor transparente.

Para crear un servicio mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
add service <name> <IP> <serviceType> <port>

show service <name>
<!--NeedCopy-->
```

Ejemplo:

```
add service ISP1R_svc_any 10.10.10.254 any *
show service ISP1R_svc_any
        ISP1R_svc_any (10.10.10.254:*) - ANY
        State: DOWN
        Last state change was at Tue Aug 31 04:31:13 2010
```



```
        Time since last state change: 2 days, 05:34:18.600
        Server Name: 10.10.10.254
        Server ID : 0   Monitor Threshold : 0
        Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
        Use Source IP: NO
        Client Keepalive(CKA): NO
        Access Down Service: NO
        TCP Buffering(TCPB): YES
        HTTP Compression(CMP): NO
        Idle timeout: Client: 120 sec   Server: 120 sec
        Client IP: DISABLED
        Cacheable: NO
        SC: OFF
        SP: OFF
        Down state flush: ENABLED

1)      Monitor Name: ping
                State: UP       Weight: 1
                Probes: 244705  Failed [Total: 0 Current: 0]
                Last response: Success - ICMP echo reply received.
                Response Time: 1.322 millisec
 Done
<!--NeedCopy-->
```

Para crear servicios mediante la utilidad de configuración

Vaya a Administración del tráfico > Equilibrio de carga > Serviciosy cree un servicio.

Para crear servicios mediante la utilidad de configuración

1. Vaya a Administración de Tráfico > Equilibrio de carga > Servicios.
2. En el panel de detalles, haga clic en Agregar.
3. En el cuadro de diálogo Crear servicio, especifique valores para los siguientes parámetros:
   - Nombre del servicio*: Nombre
   - Servidor: IP
   - Protocolo*: ServiceType (Seleccione ANY en la lista desplegable).
   - puerto*: Puerto

Un parámetro requerido

1. Haga clic en Crear.
2. Repita los pasos 2-4 para crear otro servicio.

3. Haga clic en Cerrar.
4. En el panel Servicios, seleccione los servicios que acaba de configurar y compruebe que la configuración mostrada en la parte inferior de la pantalla sea correcta.

Configurar un servidor virtual LLB y enlazar un servicio

Después de crear un servicio, cree un servidor virtual y vincule servicios al servidor virtual. El método LB predeterminado de las conexiones mínimas no se admite en LLB. Para obtener información sobre cómo cambiar el método LB, consulte Configuración del método LLB y la persistencia.

Para crear un servidor virtual de equilibrio de carga de vínculos y enlazar un servicio mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
add lb vserver <name> <serviceType>

bind lb vserver < name> <serviceName>

show lb vserver < name>
<!--NeedCopy-->
```

Ejemplo:

```
add lb vserver LLB-vip any
bind lb vserver LLB-vip ISP1R_svc_any
sh lb vserver LLB-vip
        LLB-vip (0.0.0.0:0) - ANY    Type: ADDRESS
        State: DOWN
        Last state change was at Thu Sep  2 10:51:32 2010
        Time since last state change: 0 days, 17:51:46.770
        Effective State: DOWN
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  1 (Total)       0 (Active)
        Configured Method: ROUNDROBIN
        Mode: IP
        Persistence: NONE
        Connection Failover: DISABLED
```



```
17
18 1) ISP1R_svc_any (10.10.10.254: *) - ANY State: DOWN    Weight: 1
19  Done
20 <!--NeedCopy-->
```

Para crear un servidor virtual de equilibrio de carga de vínculos y enlazar un servicio mediante la utilidad de configuración

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales** y cree un servidor virtual para el equilibrio de carga de vínculos. Especifique **CUALQUIERA** en el campo **Protocolo**.
2. En la lista desplegable **Tipo de dirección IP**, seleccione la opción deseada. Seleccione **No direccionable** para crear un servidor virtual al que no se pueda acceder directamente.
3. En la ficha **Servicios**, en la columna **Activo**, active la casilla de verificación del servicio que quiere enlazar al servidor virtual.

Configurar el método LLB y la persistencia

De forma predeterminada, el dispositivo Citrix ADC utiliza el método de menos conexiones para seleccionar el servicio para redirigir cada solicitud de cliente, pero debe establecer el método LLB en uno de los métodos admitidos. También puede configurar la persistencia para que diferentes transmisiones del mismo cliente se dirijan al mismo servidor.

Para configurar el método LLB y/o la persistencia mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba el siguiente comando:

```
1 set lb vserver <name> -lbMethod <lbMethod> -persistenceType <
     persistenceType>
2
3 show lb vserver <name>
4 <!--NeedCopy-->
```

Ejemplo:

```
1 set lb vserver LLB-vip -lbmethod ROUNDROBIN -persistencetype SOURCEIP
2
3 show lb vserver LLB-vip
4         LLB-vip (0.0.0.0:0) - ANY    Type: ADDRESS
```



```
5          State: DOWN
6          Last state change was at Fri Sep  3 04:46:48 2010
7          Time since last state change: 0 days, 00:52:21.200
8          Effective State: DOWN
9          Client Idle Timeout: 120 sec
10         Down state flush: ENABLED
11         Disable Primary Vserver On Down : DISABLED
12         No. of Bound Services :  0 (Total)       0 (Active)
13         Configured Method: ROUNDROBIN
14         Mode: IP
15         Persistence: SOURCEIP
16       Persistence Mask: 255.255.255.255       Persistence v6MaskLength:
             128   Persistence Timeout: 2 min
17         Connection Failover: DISABLED
18 <!--NeedCopy-->
```

Para configurar el método de equilibrio de carga de vínculos y/o la persistencia mediante la utilidad de configuración

1. Vaya a Administración del tráfico > Equilibrio de carga > Servidores virtuales y seleccione el servidor virtual para el que quiere configurar el método de equilibrio de carga y/o la configuración de persistencia.
2. En la sección **Configuración avanzada**, seleccione Método y configure el método de equilibrio de carga.
3. En la sección **Configuración avanzada**, seleccione **Persistencia** y configure los parámetros de persistencia.

Configurar una ruta LLB

Después de configurar los servicios IPv4 o IPv6, los servidores virtuales, los métodos LLB y la persistencia, configure una ruta LLB IPv4 o IPv6 para la red que especifica el servidor virtual LLB como Gateway. Una ruta es una colección de vínculos que están equilibrados de carga. Las solicitudes se envían a la dirección IP del servidor virtual LLB que actúa como Gateway para todo el tráfico saliente y selecciona el enrutador según el método LLB configurado.

Para configurar una ruta IPv4 LLB mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
1 add lb route <network> <netmask> <gatewayName>
```



```
2
3 show lb route [<network> <netmask>]
4 <!--NeedCopy-->
```

Ejemplo:

```
1 add lb route 0.0.0.0 0.0.0.0 LLB-vip
2 show lb route 0.0.0.0 0.0.0.0
3        Network          Netmask        Gateway/VIP              Flags
4      -----------      -------------   --------------          --------
5 1)     0.0.0.0          0.0.0.0        LLB-vip                UP
6 <!--NeedCopy-->
```

Para configurar una ruta IPv6 LLB mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
1 add lb route6 <network> <gatewayName>
2
3 show lb route6
4 <!--NeedCopy-->
```

Ejemplo:

```
1 add lb route6 ::/0 llb6_vs show lb route6 Network VIP Flags -----------
      --------- -------- 1) ::/0 llb6_vs UP
2 <!--NeedCopy-->
```

Para configurar una ruta LLB mediante la utilidad de configuración

Vaya a Sistema > Red > Rutas, seleccione **LLB** y configure la ruta LLB.

Nota: Seleccione LLBV6 para configurar una ruta IPV6.

Para configurar una ruta LLB mediante la utilidad de configuración

1. Vaya a Sistema > Red > Rutas.
2. En el panel de detalles, seleccione una de las opciones siguientes:

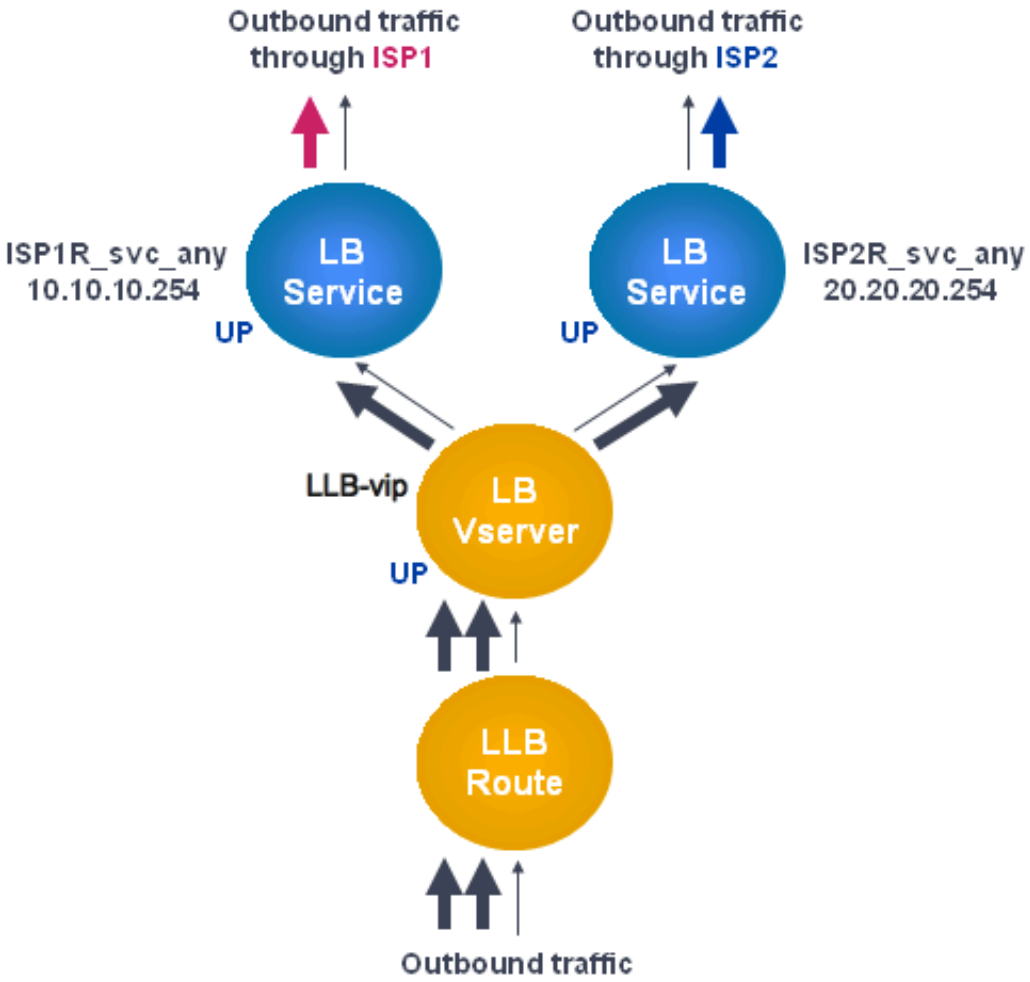
- Haga clic en LLB para configurar una ruta IPv4.
- Haga clic en LLBV6 para configurar una ruta IPv4.

3. En el cuadro de diálogo Crear ruta LB o Crear ruta IPv6 LB, defina los siguientes parámetros:
   - Red*
   - Netmask*: Necesario para rutas IPv4.
   - Nombre de puerta de enlace *: NombreDeAcceso

     *Un parámetro requerido
4. Haga clic en Crear y, a continuación, en Cerrar. La ruta que acaba de crear aparece en la ficha LLB o LLB6 del panel Rutas.

El siguiente diagrama muestra una configuración básica de LLB. Se configura un servicio para cada uno de los dos vínculos (ISP) y los monitores PING están enlazados de forma predeterminada a estos servicios. Se selecciona un vínculo basado en el método LLB configurado.

Ilustración 1. Configuración básica de LLB



> **Nota**
>
> Si su proveedor de servicios de Internet ha proporcionado una dirección IPv6, reemplace el servicio IPv4 por un servicio IPv6 en la ilustración anterior.

Crear y enlazar un monitor transparente

Cree un monitor transparente para supervisar el estado de los dispositivos ascendentes, como los enrutadores. A continuación, puede enlazar el monitor transparente a los servicios. El monitor PING predeterminado supervisa la conectividad solo entre el dispositivo Citrix ADC y el dispositivo ascendente. El monitor transparente supervisa todos los dispositivos existentes en la ruta de acceso desde el dispositivo al dispositivo que posee la dirección IP de destino especificada en el monitor. Si no se configura un monitor transparente y el estado del router es UP pero uno de los dispositivos de salto siguiente de ese router está inactivo, el dispositivo incluye el router mientras realiza el equilibrio de carga y reenvía el paquete al router. Sin embargo, el paquete no se entrega al destino final porque

uno de los dispositivos de salto siguiente está caído. Al vincular un monitor transparente, si alguno de los dispositivos (incluido el router) está inactivo, el servicio se marca como DOWN y el router no se incluye cuando el dispositivo realiza el equilibrio de carga de enlace.

Para crear un monitor transparente mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
add lb monitor <monitorName> <type> -destIP <ip_addr|*> -transparent
    YES

show lb monitor [<monitorName>]
<!--NeedCopy-->
```

Ejemplo:

```
add lb monitor monitor-1 PING -destIP 10.10.10.11 -transparent YES
> show lb monitor monitor-1
1)   Name.......: monitor-1  Type......:      PING   State....:
    ENABLED
Standard parameters:
  Interval.........:           5 sec   Retries...........:
                    3
  Response timeout.:           2 sec   Down time.........:
     30 sec
  Reverse..........:              NO   Transparent.......:
                  YES
  Secure...........:              NO   LRTM..............:
     ENABLED
  Action...........:   Not applicable   Deviation.........:
     0 sec
  Destination IP...:      10.10.10.11
  Destination port.:    Bound service
  Iptunnel.........:              NO
  TOS..............:              NO   TOS ID............:
                    0
  SNMP Alert Retries:               0     Success Retries..:
                    1
  Failure Retries..:                0
<!--NeedCopy-->
```


Para crear un monitor transparente mediante la utilidad de configuración

Vaya a Administración del tráfico > Equilibrio de carga > Monitores y configure un monitor transparente.

Para crear un monitor transparente mediante la utilidad de configuración

1. Vaya a Administración del Tráfico > Equilibrio de carga > Monitores.
2. En el panel Monitores, haga clic en Agregar.
3. En el cuadro de diálogo Crear monitor, defina los siguientes parámetros:
   - Nombre*
   - Tipo*
   - IP de destino
   - Transparencia

   *Un parámetro requerido
4. Haga clic en Crear y, a continuación, en Cerrar.
5. En el panel Monitores, seleccione el monitor que acaba de configurar y compruebe que la configuración mostrada en el panel Detalles sea correcta.

Para enlazar un monitor a un servicio mediante la utilidad de configuración

1. Vaya a Administración de Tráfico > Equilibrio de carga > Servicios.
2. En la ficha **Monitores**, en **Disponible**, seleccione el monitor que quiere vincular al servicio y, a continuación, haga clic en **Agregar**.

Para enlazar un monitor a un servicio mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
bind lb monitor <monitorName> <serviceName>

show service <name>
<!--NeedCopy-->
```

Ejemplo:


```
bind lb monitor monitor-HTTP-1 ISP1R_svc_any
 Done
> show service ISP1R_svc_any
        ISP1R_svc_any (10.10.10.254:*) - ANY
        State: UP
        Last state change was at Thu Sep  2 10:51:07 2010
        Time since last state change: 0 days, 18:41:55.130
        Server Name: 10.10.10.254
        Server ID : 0   Monitor Threshold : 0
        Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
        Use Source IP: NO
        Client Keepalive(CKA): NO
        Access Down Service: NO
        TCP Buffering(TCPB): YES
        HTTP Compression(CMP): NO
        Idle timeout: Client: 120 sec   Server: 120 sec
        Client IP: DISABLED
        Cacheable: NO
        SC: OFF
        SP: OFF
        Down state flush: ENABLED

1)      Monitor Name: monitor-HTTP-1
                State: UP  Weight: 1
                Probes: 1256       Failed [Total: 0 Current: 0]
                Last response: Success - ICMP echo reply received.
                Response Time: 1.322 millisec
 Done
<!--NeedCopy-->
```

Para enlazar un monitor a un servicio mediante la utilidad de configuración

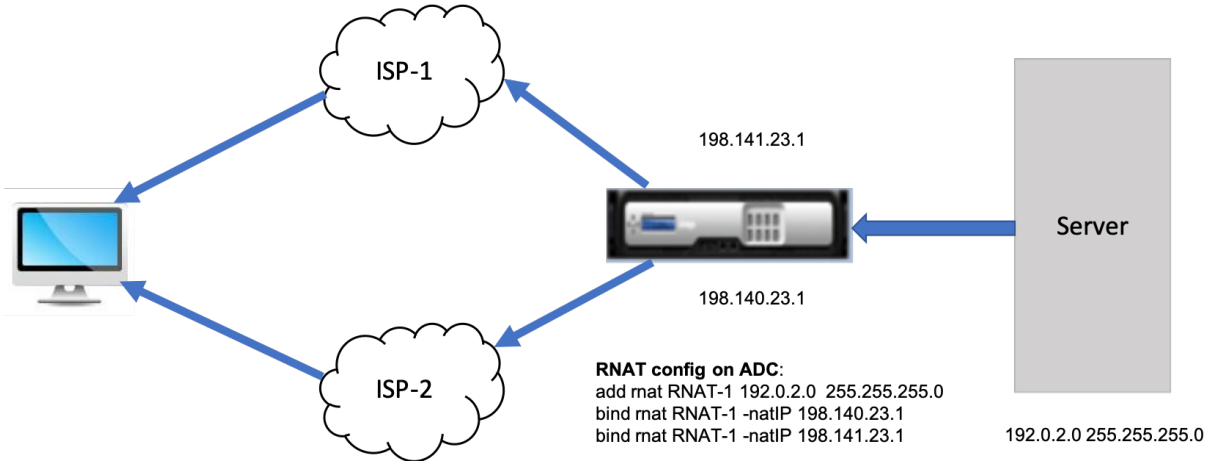
1. Vaya a Administración de Tráfico > Equilibrio de carga > Servicios.
2. En el panel de detalles, seleccione un servicio al que quiera enlazar un monitor y, a continuación, haga clic en Abrir.
3. En el cuadro de diálogo Configurar servicio, en la ficha Monitores, en Disponible, seleccione el monitor que quiere enlazar al servicio y, a continuación, haga clic en Agregar.
4. Haga clic en Aceptar.
5. En el panel Servicios, seleccione el servicio que acaba de configurar y compruebe que la configuración mostrada en el panel Detalles sea correcta.

Configurar RNAT con LLB

August 20, 2021

Puede configurar una configuración LLB para la traducción inversa de direcciones de red (RNAT) para el tráfico saliente. Garantiza que el tráfico de red de retorno para un flujo específico se enrute a través de la misma ruta. En primer lugar, configure LLB básico, como se describe en Configuración de una configuración de LLB básicay, a continuación, configure RNAT como se describe en Configurar RNAT. A continuación, habilite el modo "usar IP de subred (USNIP)".

En el diagrama siguiente, el dispositivo Citrix ADC utiliza LLB para enrutar el tráfico saliente a diferentes vínculos. Durante la operación RNAT, el dispositivo ADC reemplaza las direcciones IP de origen del tráfico saliente por la dirección IP NAT pública (198.141.23.1) para enrutar el tráfico a través de ISP-1. Del mismo modo, el dispositivo ADC reemplaza las direcciones IP de origen por 198.140.23.1 para enrutar el tráfico a través de ISP-2.



Para agregar SNIP para enrutadores ISP mediante la CLI

En el símbolo del sistema, escriba:

```
add NS IP <subnet of first ISP in the IP router> <subnet mask> -type
   SNIP

add NS IP <subnet of second ISP in the IP router> <subnet mask> -type
   SNIP
<!--NeedCopy-->
```

Ejemplo:


```
add ns ip 198.140.23.1 255.255.255.0 -type snip

add ns ip 198.141.23.1 255.255.255.0 -type snip
<!--NeedCopy-->
```

Para configurar RNAT mediante la CLI

En el símbolo del sistema, escriba:

```
add rnat <name> (<network> | (<aclname> [-redirectPort <port>]))

bind rnat <name> <natIP>@ ...

show rnat <name>
<!--NeedCopy-->
```

Ejemplo:

```
add rnat RNAT-1 192.0.2.0 255.255.255.0
bind rnat RNAT-1 -natIP 198.140.23.1
bind rnat RNAT-1 -natIP 198.141.23.1

> show rnat RNAT-1
    1) RNAT Name: RNAT-1     Network: 192.0.2.0      Netmask:
       255.255.255.0     Traffic Domain: 0
        UseProxyPort: ENABLED

        NatIP: 198.140.23.1
        NatIP: 198.141.23.1
<!--NeedCopy-->
```

Para configurar RNAT mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **Red** > **NAT**.
2. En la ficha **RNAT**, haga clic en **Configurar RNAT**.
3. Especifique la red en la que quiere realizar RNAT.

> **Nota**
>
> También puede configurar RNAT mediante Listas de control de acceso (ACL). Consulte Configuración de RNAT para obtener más información.

Para habilitar el modo Usar IP de subred mediante la CLI

En el símbolo del sistema, escriba:

```
enable ns mode USNIP

show ns mode
<!--NeedCopy-->
```

Ejemplo:

```
enable ns mode USNIP

show ns mode
        Mode                            Acronym             Status
        -------                         -------             ------
 1)     Fast Ramp                       FR                  ON
 2)     … .
 8)     Use Subnet IP                   USNIP               ON
 9)     …
<!--NeedCopy-->
```

Para habilitar el modo Usar IP de subred mediante la GUI

1. Desplácese hasta **Sistema** > **Configuración** y, en **Modos y funciones**, haga clic en **Configurar modos**.
2. En el cuadro de diálogo **Configurar modos**, seleccione **Usar IP de subred** y, a continuación, haga clic en **Aceptar**.

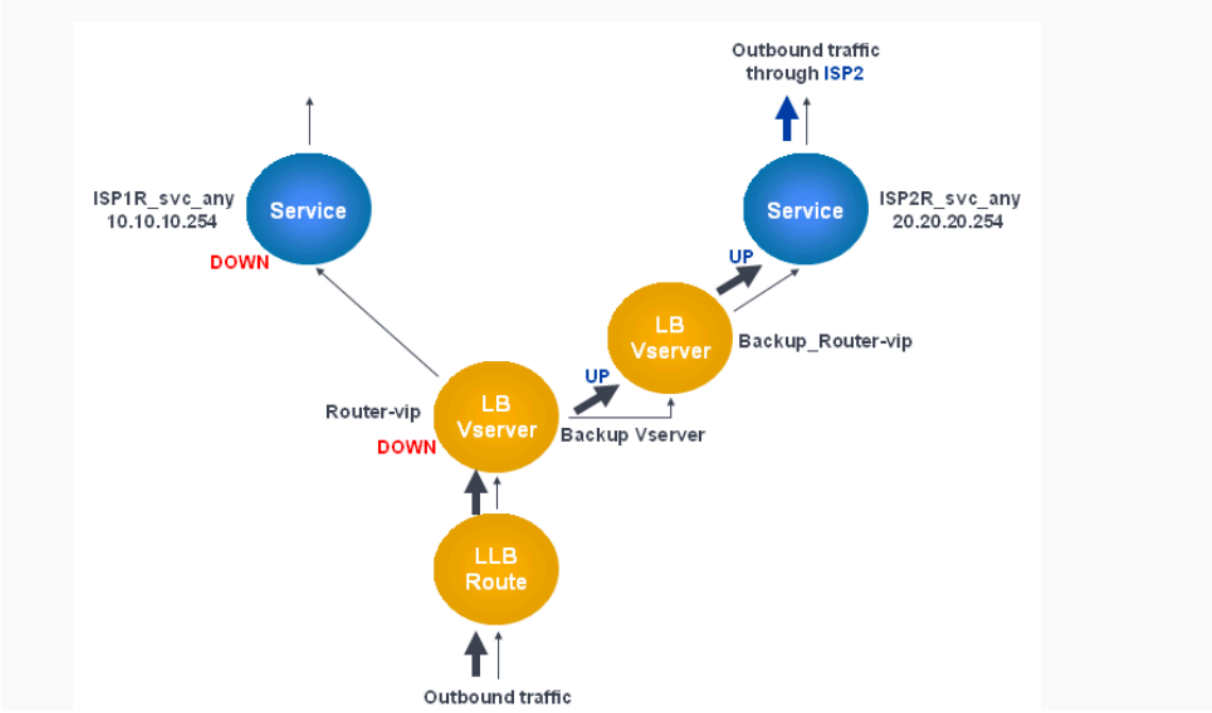
Configurar una ruta de copia de seguridad

August 20, 2021

Para evitar interrupciones en los servicios cuando la ruta principal está inactiva, puede configurar una ruta de copia de seguridad. Una vez configurada la ruta de copia de seguridad, el dispositivo Citrix ADC la utiliza automáticamente cuando falla la ruta principal. En primer lugar, cree un servidor virtual principal como se describe en Configuración de un servidor virtual LLB y Vinculación de un servicio. Para configurar una ruta de copia de seguridad, cree un servidor virtual secundario similar al servidor virtual principal y, a continuación, designe este servidor virtual como servidor virtual de copia de seguridad (ruta).

En el siguiente diagrama, **Router-VIP** es el servidor virtual principal y **Backup_Router-VIP** es el servidor virtual secundario designado como servidor virtual de copia de seguridad.

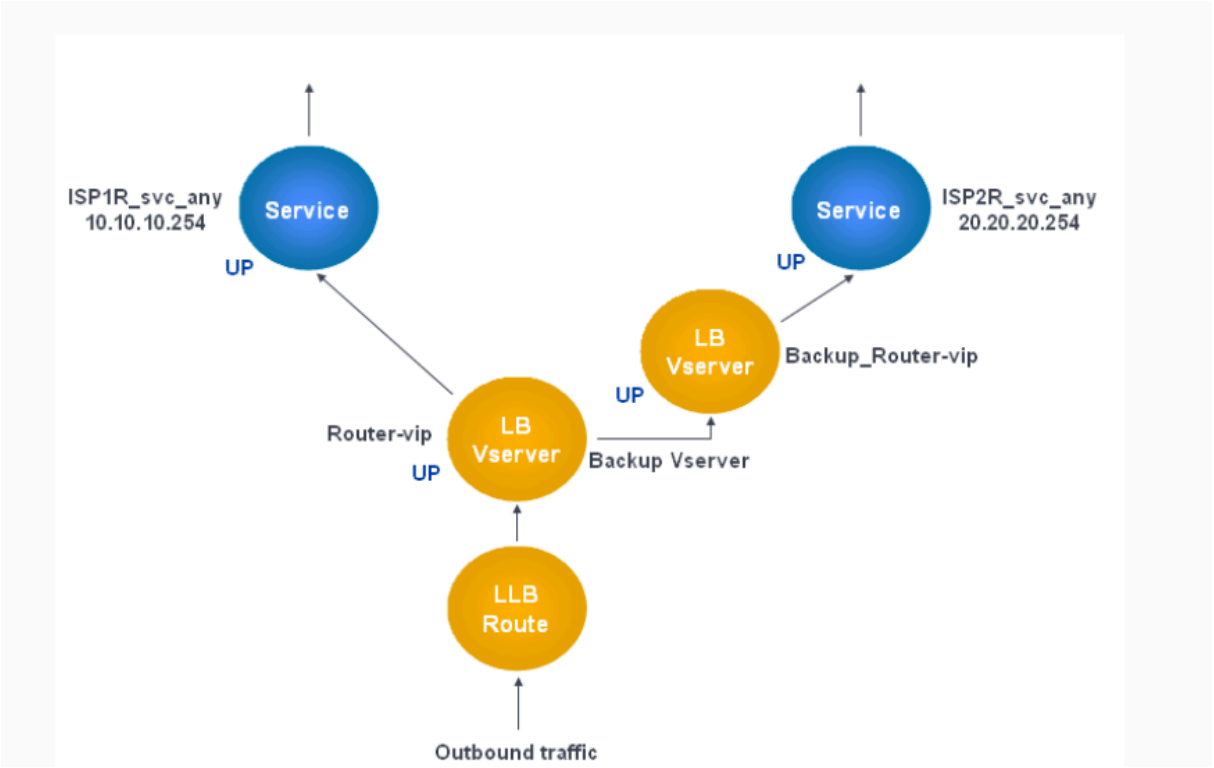
Ilustración 1. Configuración de ruta de copia de seguridad



Nota: Si su ISP ha proporcionado una dirección IPv6, reemplace el servicio IPv4 por un servicio IPv6 en la ilustración anterior.

De forma predeterminada, todo el tráfico se envía a través de la ruta principal. Sin embargo, cuando falla la ruta principal, todo el tráfico se desvía a la ruta de copia de seguridad como se muestra en el siguiente diagrama.

Ilustración 2. Realización de copias de seguridad de redirección



Nota: Si su ISP ha proporcionado una dirección IPv6, reemplace el servicio IPv4 por un servicio IPv6 en la ilustración anterior.

Para establecer el servidor virtual secundario como servidor virtual de copia de seguridad mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
set lb vserver <name> -backupVserver <string>
<!--NeedCopy-->
```

Ejemplo:

```
set lb vserver Router-vip -backupVServer Backup_Router-vip
> show lb vserver Router-vip
        Router-vip (0.0.0.0:0) - ANY    Type: ADDRESS
        State: UP
        Last state change was at Fri Sep  3 04:46:48 2010
        Time since last state change: 0 days, 03:09:45.600
        Effective State: UP
        Client Idle Timeout: 120 sec
```



```
9          Down state flush: ENABLED
10         Disable Primary Vserver On Down : DISABLED
11         No. of Bound Services :  1 (Total)       1 (Active)
12         Configured Method: ROUNDROBIN
13         Mode: IP
14         Persistence: DESTIP     Persistence Mask: 255.255.255.255
                     Persistence v6MaskLength: 128   Persistence Timeout: 2
               min
15         Backup: Router2-vip
16         Connection Failover: DISABLED
17  Done
18 <!--NeedCopy-->
```

Para establecer el servidor virtual secundario como servidor virtual de copia de seguridad mediante la utilidad de configuración

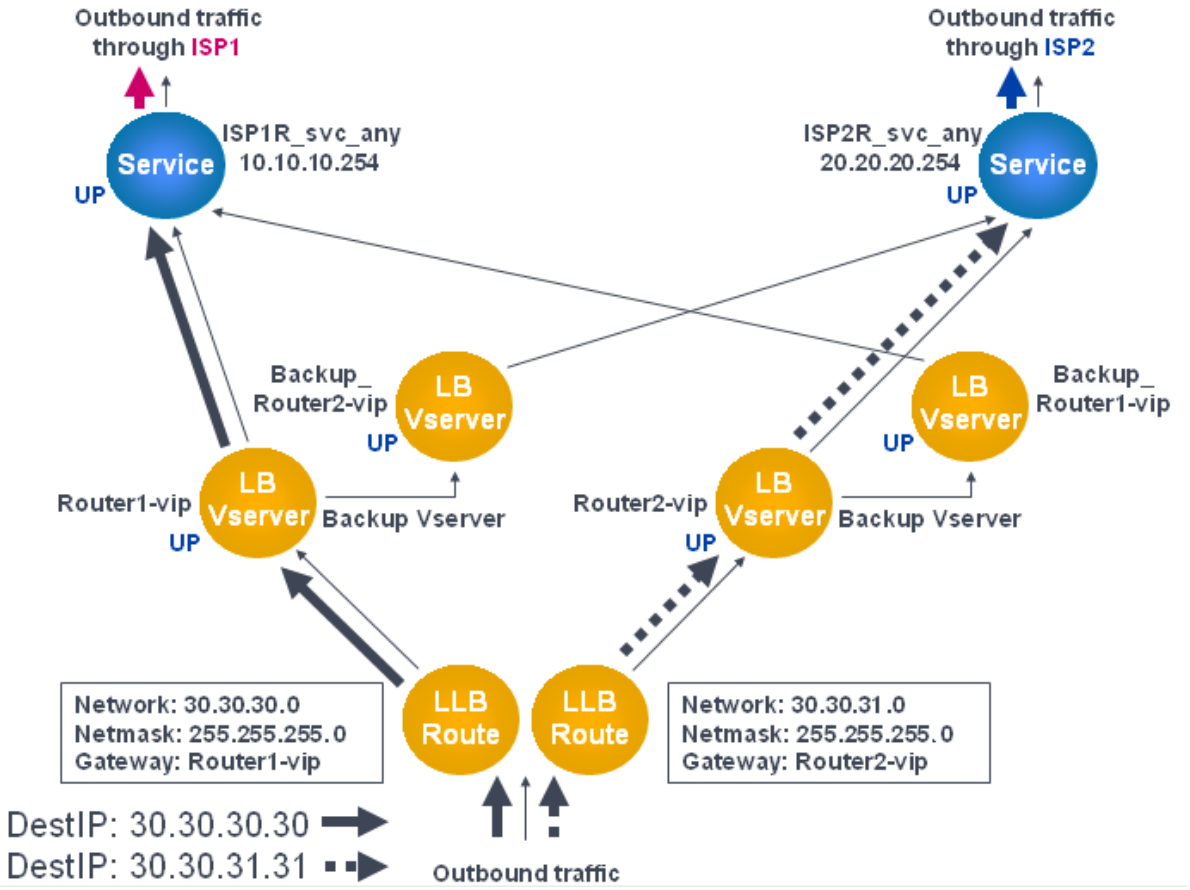
1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales** y seleccione el servidor virtual secundario para el que desea configurar el servidor virtual de copia de seguridad.
2. En el cuadro de diálogo **Servidor virtual de equilibrio de carga**, en **Avanzadas**, seleccione **Protección**.
3. En la lista desplegable **Servidor virtual de copia** de seguridad, seleccione el servidor virtual de copia de seguridad secundario y, a continuación, haga clic en **Aceptar**.

Caso de implementación de LLB resiliente

February 16, 2021

En el siguiente diagrama, hay dos redes: 30.30.30.0 y 30.30.31.0. El equilibrio de carga de enlace se configura en función de la dirección IP de destino. Dos rutas se configuran con puertas de enlace **Router1-VIP** y **Router2-VIP**, respectivamente. **Router1-VIP** se configura como una copia de seguridad para **Router2-VIP** y de la manera opuesta. Todo el tráfico con la IP de destino especificada como 30.30.30.30 se envía a través del **Router1-VIP** y el tráfico con la IP de destino especificada como 30.30.31.31 se envía a través del **Router2-VIP**.

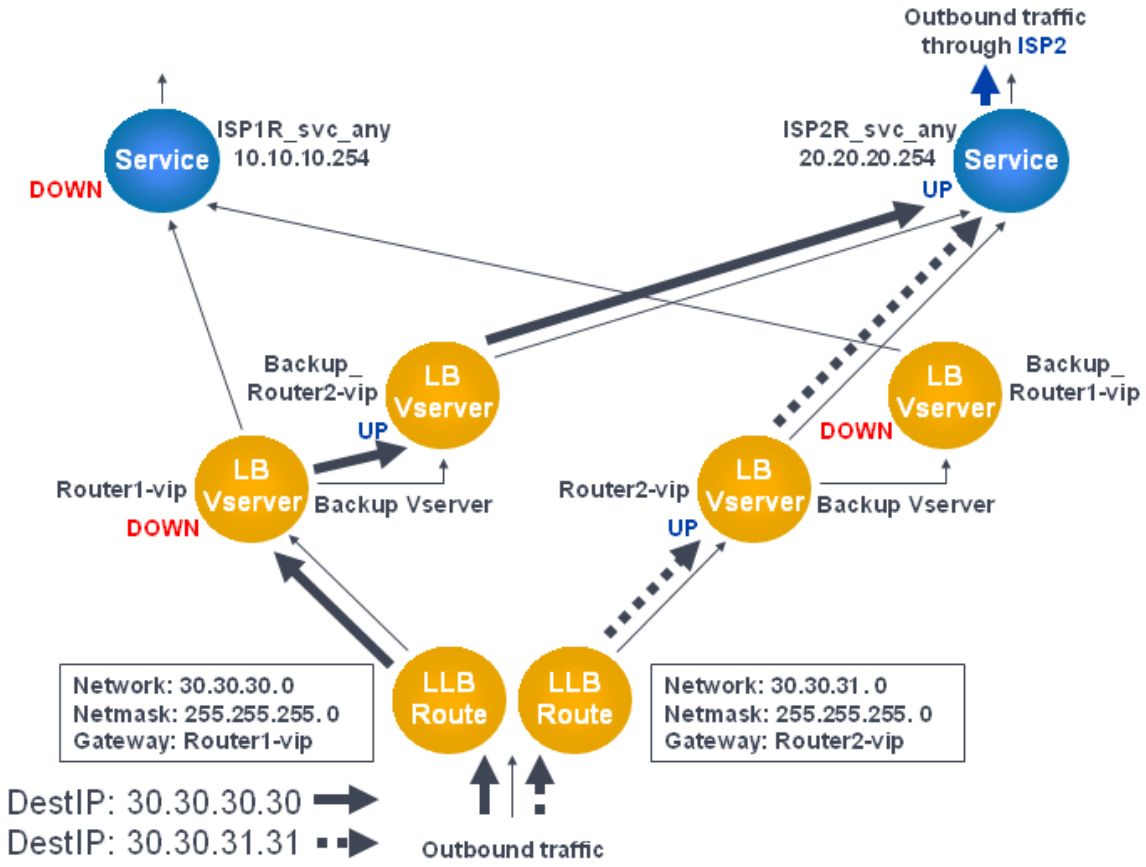
Ilustración 1. Configuración de implementación de LLB resiliente



Nota: Si su ISP ha proporcionado una dirección IPv6, reemplace el servicio IPv4 por un servicio IPv6 en la ilustración anterior.

Sin embargo, si alguna de las puertas de enlace (**Router1-VIP** o **Router2-VIP**) está DESACTIVADO, el tráfico se enruta a través del enrutador de reserva. En el siguiente diagrama, **Router1-VIP** para ISP1 está DOWN, por lo que todo el tráfico con la IP de destino especificada como 30.30.30.30 también se envía a través de ISP2.

Ilustración 2. Caso de implementación de LLB resiliente



Nota: Si su ISP ha proporcionado una dirección IPv6, reemplace el servicio IPv4 por un servicio IPv6 en la ilustración anterior.

Supervisar una configuración de LLB

August 20, 2021

Una vez que la configuración esté en funcionamiento, puede ver las estadísticas de cada servicio y servidor virtual para comprobar si hay posibles problemas.

Ver las estadísticas de un servidor virtual

Para evaluar el rendimiento de los servidores virtuales o solucionar problemas, puede mostrar detalles de los servidores virtuales configurados en el dispositivo Citrix ADC. Puede mostrar un resumen de las estadísticas de todos los servidores virtuales. También puede especificar el nombre de un servidor virtual para mostrar las estadísticas solo para ese servidor virtual. Puede mostrar los siguientes detalles:

- Nombre
- Dirección IP
- Port
- Protocolo
- Estado del servidor virtual
- Tasa de solicitudes recibidas
- `Rate of hits`

Mostrar estadísticas del servidor virtual mediante la CLI

Para mostrar un resumen de las estadísticas de todos los servidores virtuales configurados actualmente en Citrix ADC, o de un único servidor virtual, en el símbolo del sistema, escriba:

```
stat lb vserver -detail] [<name>]
<!--NeedCopy-->
```

Ejemplo:

```
stat lb vserver -detail
Virtual Server(s) Summary
                        vsvrIP  port     Protocol        State    Req/s
                             Hits/s
One                          *    80         HTTP           UP      5/s
        0/s
Two                          *     0          TCP         DOWN      0/s
        0/s
Three                        *  2598          TCP         DOWN      0/s
        0/s
dnsVirtualNS    10.102.29.90    53          DNS         DOWN      0/s
        0/s
BRVSERV            10.10.1.1    80         HTTP         DOWN      0/s
        0/s
LBVIP           10.102.29.66    80         HTTP           UP      0/s
        0/s
 Done
<!--NeedCopy-->
```

Mostrar estadísticas del servidor virtual mediante la GUI

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales > Estadísticas**.

2. Si quiere mostrar las estadísticas de un solo servidor virtual, en el panel de detalles seleccione el servidor virtual y haga clic en Estadísticas.

Ver las estadísticas de un servicio

Puede ver la tasa de solicitudes, respuestas, bytes de solicitud, bytes de respuesta, conexiones de cliente actuales, solicitudes en la cola de sobretensión, conexiones de servidor actuales, etc. mediante las estadísticas del servicio.

Ver las estadísticas de un servicio mediante la CLI

En el símbolo del sistema, escriba:

```
stat service <name>
<!--NeedCopy-->
```

Ejemplo:

```
stat service Service-HTTP-1
<!--NeedCopy-->
```

Ver las estadísticas de un servicio mediante la GUI

1. Vaya a **Administración del Tráfico > Equilibrio de carga > Servicios > Estadísticas**.
2. Si quiere mostrar las estadísticas de un solo servicio, seleccione el servicio y haga clic en Estadísticas.

Equilibrio de carga

August 20, 2021

La función de equilibrio de carga distribuye las solicitudes de los usuarios de páginas web y otras aplicaciones protegidas en varios servidores que alojan (o reflejan) el mismo contenido. El equilibrio de carga se utiliza principalmente para administrar las solicitudes de los usuarios a aplicaciones muy utilizadas, lo que evita el rendimiento deficiente y las interrupciones y garantiza que los usuarios

puedan acceder a las aplicaciones protegidas. El equilibrio de carga también proporciona tolerancia a errores. Cuando un servidor que aloja una aplicación protegida no está disponible, la función distribuye las solicitudes de los usuarios a los demás servidores que alojan la misma aplicación.

Puede configurar la función de equilibrio de carga en;

- Distribuya todas las solicitudes de un sitio web protegido específico, aplicación o recurso entre dos o más servidores configurados de forma idéntica.
- Utilice cualquiera de los varios algoritmos diferentes para determinar qué servidor debe recibir cada solicitud de usuario entrante, basando la decisión en distintos factores, como qué servidor tiene menos conexiones de usuario actuales o qué servidor tiene la carga más ligera.

La función de equilibrio de carga es una función principal del dispositivo Citrix ADC. La mayoría de los usuarios configuran primero una configuración básica en funcionamiento y, a continuación, personalizan varias configuraciones, incluida la persistencia de conexiones. Además, puede configurar funciones para proteger la configuración contra fallos, administrar el tráfico de clientes, administrar y supervisar servidores y administrar una implementación a gran escala.

Cómo funciona el equilibrio de carga

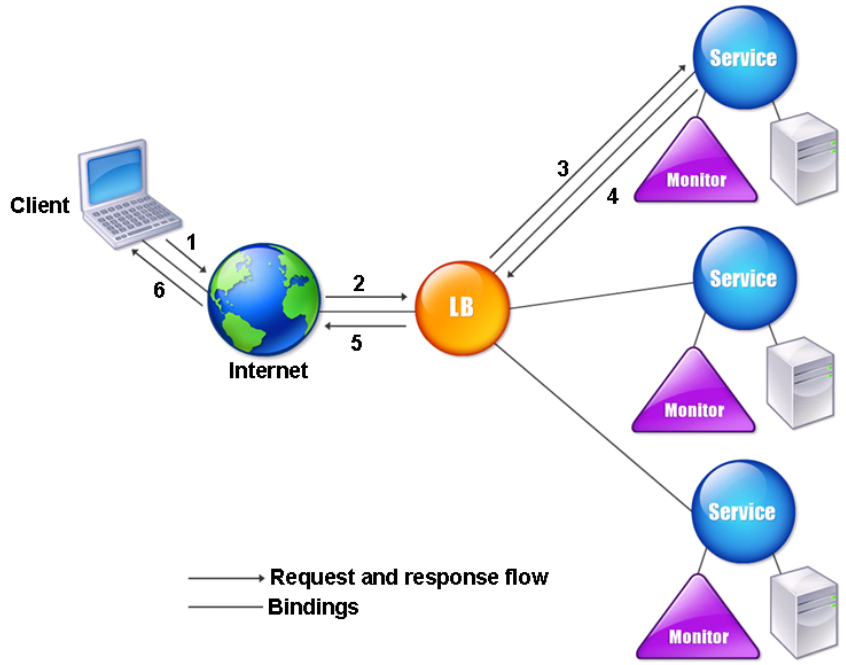
August 20, 2021

En una configuración básica de equilibrio de carga, los clientes envían sus solicitudes a la dirección IP de un servidor virtual configurado en el dispositivo Citrix ADC. El servidor virtual los distribuye a los servidores de aplicaciones con equilibrio de carga según un patrón preestablecido, denominado algoritmo de equilibrio de carga. A veces, puede que desee asignar al servidor virtual de equilibrio de carga una dirección comodín en lugar de una dirección IP específica. Para obtener instrucciones acerca de cómo especificar un puerto HTTP global en el dispositivo, consulte **Puertos HTTP globales**.

Conceptos básicos del equilibrio de carga

Una configuración de equilibrio de carga incluye un servidor virtual de equilibrio de carga y varios servidores de aplicaciones con equilibrio de carga. El servidor virtual recibe solicitudes de cliente entrantes, utiliza el algoritmo de equilibrio de carga para seleccionar un servidor de aplicaciones y reenvía las solicitudes al servidor de aplicaciones seleccionado. El siguiente dibujo conceptual ilustra una implementación típica de equilibrio de carga. Otra variación implica asignar un puerto HTTP global.

Ilustración 1. Arquitectura de equilibrio de carga



El servidor virtual de equilibrio de carga puede utilizar varios algoritmos (o métodos) para determinar cómo distribuir la carga entre los servidores equilibrados de carga que administra. El método de equilibrio de carga predeterminado es el método de menor conexión, en el que el dispositivo Citrix ADC reenvía cada conexión de cliente entrante al servidor de aplicaciones con equilibrio de carga que tenga actualmente menos conexiones de usuario activas.

Las entidades que configura en una configuración típica de equilibrio de carga de Citrix ADC son:

- **Servidor virtual de equilibrio de carga.** La combinación de dirección IP, puerto y protocolo a la que un cliente envía solicitudes de conexión para un sitio web o aplicación con equilibrio de carga determinado. Si la aplicación es accesible desde Internet, la dirección IP del servidor virtual (VIP) es una dirección IP pública. Si solo se puede acceder a la aplicación desde la LAN o la WAN, el VIP suele ser una dirección IP privada (ICANN no enrutable).
- **Servicio.** La combinación de direcciones IP, puerto y protocolo utilizada para enrutar las solicitudes a un servidor de aplicaciones con equilibrio de carga específico. Un servicio puede ser una representación lógica del propio servidor de aplicaciones o de una aplicación que se ejecuta en un servidor que hospeda varias aplicaciones. Después de crear un servicio, lo vincula a un servidor virtual de equilibrio de carga.
- **Objeto servidor.** Entidad virtual que permite asignar un nombre a un servidor físico en lugar de identificarlo por su dirección IP. Si crea un objeto de servidor, puede especificar su nombre

en lugar de la dirección IP del servidor al crear un servicio. De lo contrario, debe especificar la dirección IP del servidor al crear un servicio y la dirección IP se convierte en el nombre del servidor.

- **monitor.** Entidad del dispositivo Citrix ADC que realiza un seguimiento de un servicio y garantiza que funciona correctamente. El monitor sondea periódicamente (o realiza una comprobación de estado) cada servicio al que se asigna. Si el servicio no responde dentro del tiempo especificado por el tiempo de espera y se produce un error en un número especificado de comprobaciones de estado, ese servicio se marca como DOWN. A continuación, el dispositivo Citrix ADC omite ese servicio al realizar el equilibrio de carga, hasta que se corrigen los problemas que causaron que el servicio dejara de responder.

El servidor virtual, los servicios y los servidores de aplicaciones con equilibrio de carga en una configuración de equilibrio de carga pueden utilizar direcciones IP de Protocolo de Internet versión 4 (IPv4) o Protocolo de Internet versión 6 (IPv6). Puede mezclar direcciones IPv4 e IPv6 en una configuración de equilibrio de carga única.

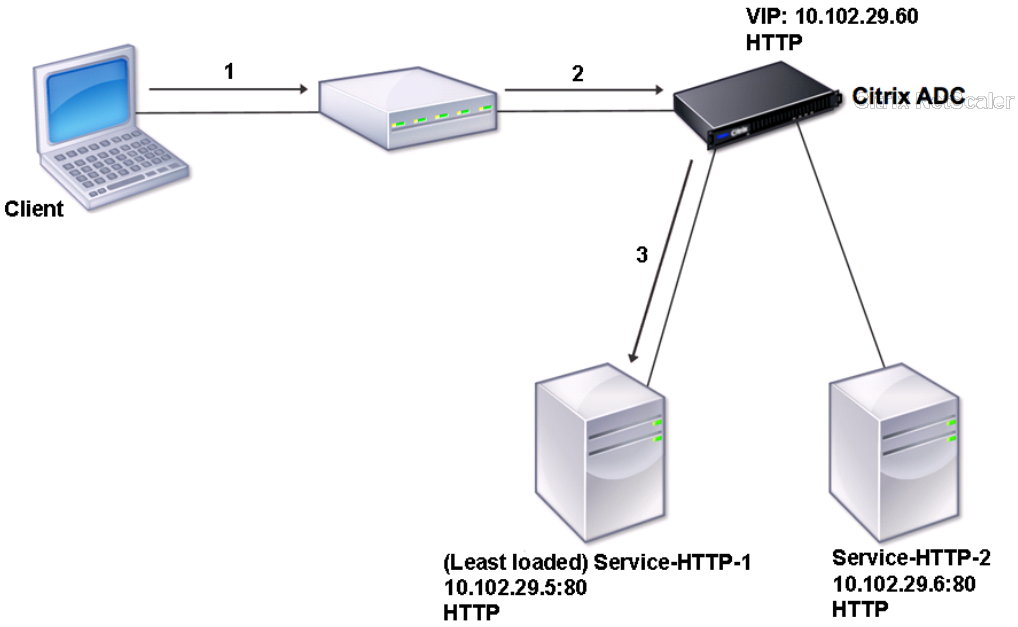
Para ver variaciones en la configuración de equilibrio de carga, consulte los siguientes casos de uso:

- Configuración del equilibrio de carga en el modo de retorno directo del servidor
- Configuración de servidores LINUX en modo DSR
- Configuración del modo DSR al utilizar TOS
- Configuración del equilibrio de carga en modo DSR mediante IP sobre IP
- Configuración del equilibrio de carga en el modo de un brazo
- Configuración del equilibrio de carga en el modo en línea
- Equilibrio de carga de servidores del sistema de detección de intrusiones
- Servidores de protocolo de escritorio remoto de equilibrio de carga

Descripción de la topología

En una configuración de equilibrio de carga, el servidor de equilibrio de carga se encuentra lógicamente entre el cliente y la comunidad de servidores, y administra el flujo de tráfico a los servidores de la comunidad de servidores. En el dispositivo Citrix ADC, los servidores de aplicaciones están representados por entidades virtuales denominadas servicios. El siguiente diagrama muestra la topología de una configuración básica de equilibrio de carga.

Ilustración 2. Topología básica de equilibrio de carga

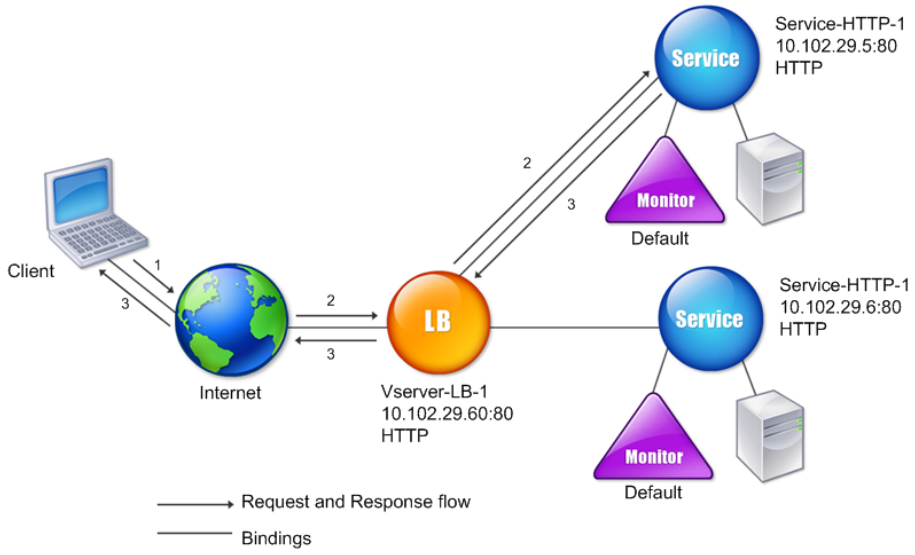


En el diagrama, el equilibrio de carga se utiliza para administrar el flujo de tráfico a los servidores. El servidor virtual selecciona el servicio y lo asigna para atender las solicitudes del cliente. Considere un caso en el que los servicios Service-HTTP-1 y Service-HTTP-2 se crean y vinculan al servidor virtual denominado VServer-LB-1. VServer-LB-1 reenvía la solicitud del cliente a Service-HTTP-1 o Servicio-HTTP-2. El dispositivo Citrix ADC utiliza el método de equilibrio de carga de conexión mínimo para seleccionar el servicio para cada solicitud. En la tabla siguiente se enumeran los nombres y valores de las entidades básicas que se deben configurar en el dispositivo.

Entidad	Nombre	Dirección IP	Port	Protocolo
Servidor virtual	Vserver-LB-1	10.102.29.60	80	HTTP
Servicios	Service-HTTP-1	10.102.29.5	80	HTTP
	Service-HTTP-2	10.102.29.6	80	HTTP
Monitores	Valor predeterminado	Ninguno	Ninguno	Ninguno

El siguiente diagrama muestra los valores de muestra de equilibrio de carga y los parámetros obligatorios que se describen en la tabla anterior.

Ilustración 3. Modelo de entidad de equilibrio de carga



Uso de comodines en lugar de direcciones IP y puertos

En ocasiones, es posible que tenga que utilizar un comodín para la dirección IP o el puerto de un servidor virtual o para el puerto de un servicio. Los casos siguientes podrían requerir el uso de un comodín:

- Si el dispositivo Citrix ADC está configurado como un paso transparente, el cual debe aceptar todo el tráfico que se le envíe independientemente de la IP o el puerto al que se envíe.
- Si uno o más servicios escuchan en puertos que no son bien conocidos.
- Si uno o más servicios, con el tiempo, cambie los puertos en los que escuchan.
- Si alcanza el límite para el número de direcciones IP y puertos que puede configurar en un único dispositivo Citrix ADC.
- Si quiere crear servidores virtuales que escuchen todo el tráfico en una LAN virtual específica.

Cuando un servidor virtual o servicio configurado con comodín recibe tráfico, el dispositivo Citrix ADC determina la dirección IP o el puerto reales y crea registros para el servicio y el servidor de aplicaciones equilibrado de carga asociado. Estos registros creados dinámicamente se denominan registros de servidor y servicio aprendidos dinámicamente.

Por ejemplo, una configuración de equilibrio de carga del firewall puede utilizar comodines tanto para la dirección IP como para el puerto. Si vincula un servicio TCP comodín a este tipo de servidor virtual de equilibrio de carga, el servidor virtual recibe y procesa todo el tráfico TCP que no coincide con ningún otro servicio o servidor virtual.

En la tabla siguiente se describen algunos de los distintos tipos de configuraciones comodín y cuándo debe utilizarse cada una.

IP	Port	Protocolo	Descripción
*	*	TCP	Servidor virtual de comodín general que acepta el tráfico enviado a cualquier dirección IP y puerto del dispositivo Citrix ADC. Al utilizar un servidor virtual comodín, el dispositivo aprende dinámicamente la IP y el puerto de cada servicio y crea los registros necesarios a medida que procesa el tráfico.
*	*	TCP	Un servidor virtual de equilibrio de carga de firewall. Puede enlazar servicios de firewall a este servidor virtual y el dispositivo Citrix ADC pasa el tráfico a través del firewall al destino.

IP	Port	Protocolo	Descripción
Dirección IP	*	TCP, UDP y ANY	Servidor virtual que acepta todo el tráfico que se envía a la dirección IP especificada, independientemente del puerto. Debe vincular explícitamente a este tipo de servidor virtual los servicios a los que redirigirá el tráfico. No los aprende dinámicamente. **Nota**: No se configuran servicios o servidores virtuales para un puerto HTTP global. En este caso, configure un puerto específico como un puerto HTTP global (por ejemplo, configure ns param -HttpPort 80). A continuación, el dispositivo acepta todo el tráfico que coincide con el número de puerto y lo procesa como tráfico HTTP. El dispositivo aprende dinámicamente y crea servicios para este tráfico.

IP	Port	Protocolo	Descripción
*	puerto	SSL, SSL_TCP	Servidor virtual que acepta todo el tráfico enviado a cualquier dirección IP en un puerto específico. Se utiliza para la descarga de SSL transparente global. Todo el procesamiento SSL, HTTP y TCP que normalmente se realiza para un servicio del mismo tipo de protocolo se aplica al tráfico que se dirige a este puerto específico. El dispositivo utiliza el puerto para conocer dinámicamente la IP del servicio que debe utilizar. Si no se especifica —cleartext, el dispositivo Citrix ADC utiliza SSL de extremo a extremo.
*	puerto	No corresponde	Todos los demás servidores virtuales que pueden aceptar tráfico al puerto. No vincula servicios a estos servidores virtuales. El dispositivo Citrix ADC los aprende dinámicamente.

Nota: Si ha configurado el dispositivo Citrix ADC como un paso transparente que utiliza puertos globales (comodín), puede que desee activar el modo Edge.
Para obtener más información, consulte "Configuración del modo perimetral. "

El dispositivo Citrix ADC intenta localizar servidores y servicios virtuales al intentar primero una coincidencia exacta. Si no se encuentra ninguno, continúa buscando una coincidencia basada en comodines, en el siguiente orden:

1. Dirección IP específica y número de puerto específico
2. Dirección IP específica y puerto * (comodín)
3. • (comodín) dirección IP y un puerto específico
4. • (comodín) dirección IP y un puerto * (comodín)

Si el dispositivo no puede seleccionar un servidor virtual por dirección IP o número de puerto, busca un servidor virtual según el protocolo utilizado en la solicitud, en el siguiente orden:

1. HTTP
2. TCP
3. CUALQUIERA

Configuración de puertos HTTP globales

No se configuran servicios o servidores virtuales para un puerto HTTP global. En su lugar, se configura un puerto específico mediante el comando set ns param. Después de configurar este puerto, el dispositivo Citrix ADC acepta todo el tráfico que coincida con el número de puerto y lo procesa como tráfico HTTP, aprendiendo dinámicamente y creando servicios para ese tráfico.

Puede configurar más de un número de puerto como puerto HTTP global. Si especifica más de un número de puerto en un solo comando set ns param, separe los números de puerto por un solo espacio en blanco. Si ya se han especificado uno o más puertos como puertos HTTP globales y quiere agregar uno o más puertos sin quitar los puertos que están configurados actualmente, debe especificar todos los números de puerto, actuales y nuevos, en el comando. Antes de agregar números de puerto, utilice el comando show ns param para ver los puertos que están configurados actualmente.

Para configurar un puerto HTTP global mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para configurar un puerto HTTP global y compruebe la configuración:

```
set ns param -httpPort <port>

```



```
show ns param
<!--NeedCopy-->
```

Ejemplo 1: Configuración de un puerto como puerto HTTP global

En este ejemplo, el puerto 80 está configurado como un puerto HTTP global.

```
set ns param -httpPort 80
Done
show ns param
         Global configuration settings:
                            HTTP port(s): 80
                        Max connections: 0
           Max requests per connection: 0
                   Client IP insertion: DISABLED
                        Cookie version: 0
         Persistence Cookie Secure Flag: ENABLED
         ...
         ...
<!--NeedCopy-->
```

Ejemplo 2: Agregar puertos cuando uno o más puertos HTTP globales ya están configurados

En este ejemplo, el puerto 8888 se agrega a la lista global de puertos HTTP. El puerto 80 ya está configurado como un puerto HTTP global.

```
> show ns param
        Global configuration settings:
                            HTTP port(s): 80
                        Max connections: 0
           Max requests per connection: 0
                   Client IP insertion: DISABLED
                        Cookie version: 0
        Persistence Cookie Secure Flag: ENABLED
                            Min Path MTU: 576
        ...
        ...
 Done
> set ns param -httpPort 80 8888
 Done
```



```
>  show ns param

        Global configuration settings:
                            HTTP port(s): 80,8888
                         Max connections: 0
            Max requests per connection: 0
                    Client IP insertion: DISABLED
                         Cookie version: 0
        Persistence Cookie Secure Flag: ENABLED
                            Min Path MTU: 576

        ...
        ...
 Done
>
<!--NeedCopy-->
```

Para configurar un puerto HTTP global mediante la utilidad de configuración

1. Vaya a **Sistema > Configuración > Cambiar parámetros HTTP**y, a continuación, agregue un número de puerto HTTP.

Configurar el equilibrio de carga básico

August 20, 2021

Antes de configurar la configuración inicial de equilibrio de carga, habilite la función de equilibrio de carga. A continuación, comience creando al menos un servicio para cada servidor en el grupo de equilibrio de carga. Con los servicios configurados, está listo para crear un servidor virtual de equilibrio de carga y enlazar cada servicio con el servidor virtual. Eso completa la configuración inicial. Antes de continuar con la configuración, verifique la configuración para asegurarse de que cada elemento se configuró correctamente y funciona como se esperaba.

Activación del equilibrio de carga

Puede configurar entidades de equilibrio de carga como servicios y servidores virtuales cuando la función de equilibrio de carga está inhabilitada, pero no funcionarán hasta que la habilite.

Para habilitar el equilibrio de carga mediante la CLI

En el símbolo del sistema, escriba el siguiente comando para habilitar el equilibrio de carga y verificar la configuración:

- habilitar la función ns LB
- show ns feature

Ejemplo

```
1     > enable ns feature LoadBalancing
2
3      Done
4
5     > show ns feature
6
7
8
9             Feature                         Acronym              Status
10
11            -------                         -------              ------
12
13     1)     Web Logging                     WL                   OFF
14
15     2)     Surge Protection                SP                   ON
16
17     3) Load Balancing LB ON
18
19     .
20
21     .
22
23     .
24
25     24)    NetScaler Push                  push                 OFF
26
27     Done
28 <!--NeedCopy-->
```

Para habilitar el equilibrio de carga mediante la interfaz gráfica de usuario

Vaya a **Sistema** > **Configuración** y, en **Configurar funciones básicas**, seleccione **Equilibrio de carga**.

Configuración de un objeto de servidor

Cree una entrada para su servidor en el dispositivo Citrix ADC. El dispositivo Citrix ADC admite servidores basados en direcciones IP y servidores basados en dominios. Si crea un servidor basado en direcciones IP, puede especificar el nombre del servidor en lugar de su dirección IP al crear un servicio. Para obtener información sobre cómo configurar DNS para un servidor basado en dominio, consulte Sistema de nombres de dominio.

Para crear un objeto de servidor mediante la CLI

En el símbolo del sistema, escriba:

```
add server `<name>`@ `<IPAddress>`@ | `<domain>`
<!--NeedCopy-->
```

Ejemplo para agregar un servidor de nombres basado en direcciones IP:

```
add server web_serv 10.102.27.150
<!--NeedCopy-->
```

Ejemplo para agregar un servidor basado en dominio:

```
add server web_serv test.com
<!--NeedCopy-->
```

Para crear un objeto de servidor mediante la interfaz gráfica de usuario

Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores** y agregue un objeto de servidor.

Configuración de servicios

Después de habilitar la función de equilibrio de carga, debe crear al menos un servicio para cada servidor de aplicaciones que se va a incluir en la configuración de equilibrio de carga. Los servicios que configura proporcionan las conexiones entre el dispositivo Citrix ADC y los servidores con equilibrio de carga. Cada servicio tiene un nombre y especifica una dirección IP, un puerto y el tipo de datos que se sirven.

Si crea un servicio sin crear primero un objeto de servidor, la dirección IP del servicio es también el nombre del servidor que hospeda el servicio. Si prefiere identificar servidores por nombre en lugar

de por dirección IP, puede crear objetos de servidor y, a continuación, especificar el nombre de un servidor en lugar de su dirección IP al crear un servicio.

Cuando se crea un servicio que utiliza UDP como protocolo de capa de transporte, un monitor de ping se vincula automáticamente al servicio. Un monitor ping es el más básico de los monitores integrados. Cuando se crea un servicio que utiliza TCP como protocolo de capa de transporte, un monitor TCP_Default se vincula automáticamente al servicio. Al desarrollar una estrategia para administrar la configuración de equilibrio de carga, puede decidir vincular un tipo diferente de monitor, o varios monitores, al servicio.

Creación de un servicio

Antes de crear un servicio, debe comprender los diferentes tipos de servicio y cómo se usa cada uno. En la lista siguiente se describen los tipos de servicios admitidos en el dispositivo Citrix ADC.

HTTP

Se utiliza para servidores con equilibrio de carga que aceptan tráfico HTTP, como sitios web estándar y aplicaciones web. El tipo de servicio HTTP permite al dispositivo Citrix ADC proporcionar compatibilidad con compresión, filtrado de contenido, almacenamiento en caché y mantenimiento de clientes para los servidores web de capa 7. Este tipo de servicio también admite la inserción de puertos IP de servidor virtual, la reescritura de puertos de redirección, Web 2.0 Push y el soporte de redirección de URL.

Dado que HTTP es un protocolo de aplicación basado en TCP, también puede utilizar el tipo de servicio TCP para servidores web. Sin embargo, si lo hace, el dispositivo Citrix ADC solo puede realizar el equilibrio de carga de la capa 4. No puede proporcionar ninguno de los soportes de Capa 7 descritos anteriormente.

SSL

Se utiliza para servidores que aceptan tráfico HTTPS, como sitios web de comercio electrónico y aplicaciones de carrito de compras. El tipo de servicio SSL permite al dispositivo Citrix ADC cifrar y descifrar el tráfico SSL (realizar la descarga SSL) para sus aplicaciones web seguras. También es compatible con persistencia HTTP, cambio de contenido, reescritura, inserción de puertos IP de servidor virtual, inserción web 2.0 y redirección de URL.

También puede utilizar los tipos de servicio SSL_BRIDGE, SSL_TCP o TCP. Sin embargo, si lo hace, el dispositivo solo realiza el equilibrio de carga de la capa 4. No puede proporcionar descarga SSL ni ninguno de los soportes de Capa 7 descritos.

FTP

Se utiliza para servidores que aceptan tráfico FTP. El tipo de servicio FTP permite que el dispositivo Citrix ADC admita detalles específicos del protocolo FTP.

También puede utilizar tipos de servicio TCP o CUALQUIERA para servidores FTP.

TCP

Se utiliza para servidores que aceptan muchos tipos diferentes de tráfico TCP o que aceptan un tipo de tráfico TCP para el que un tipo de servicio más específico no está disponible.

También puede utilizar el tipo de servicio CUALQUIERA para estos servidores.

SSL_TCP

Se utiliza para servidores que aceptan tráfico SSL no basado en HTTP, para admitir la descarga SSL.

También puede utilizar el tipo de servicio TCP para estos servicios. Si lo hace, el dispositivo Citrix ADC realiza el equilibrio de carga de la capa 4 y la descarga SSL.

UDP

Se utiliza para servidores que aceptan tráfico UDP. También puede utilizar el tipo de servicio CUALQUIERA.

PUENTE SSL_BRIDGE

Se utiliza para servidores que aceptan tráfico SSL cuando no quiere que el dispositivo Citrix ADC realice la descarga SSL. También puede utilizar el tipo de servicio SSL_TCP.

NNTP

Se utiliza para servidores que aceptan tráfico de Network News Transfer Protocol (NNTP), normalmente sitios de Usenet.

DNS

Se utiliza para servidores que aceptan tráfico DNS, normalmente servidores de nombres. Con el tipo de servicio DNS, el dispositivo Citrix ADC valida el formato de paquete de cada solicitud y respuesta DNS. También puede almacenar en caché las respuestas DNS. Puede aplicar directivas DNS a los servicios DNS.

También puede utilizar el tipo de servicio UDP para estos servicios. Sin embargo, si lo hace, el dispositivo Citrix ADC solo puede realizar el equilibrio de carga de la capa 4. No puede proporcionar soporte para funciones específicas de DNS.

CUALQUIERA

Se utiliza para servidores que aceptan cualquier tipo de tráfico TCP, UDP o ICMP. El parámetro ANY se utiliza principalmente con el equilibrio de carga de firewall y el equilibrio de carga de enlace.

SIP-UDP

Se utiliza para servidores que aceptan tráfico de Protocolo de inicio de sesión (SIP) basado en UDP. SIP inicia, administra y termina sesiones de comunicaciones multimedia, y ha surgido como el estándar para la telefonía por Internet (VoIP).

También puede utilizar el tipo de servicio UDP para estos servicios. Sin embargo, si lo hace, el dispositivo Citrix ADC solo realiza el equilibrio de carga de la capa 4. No puede proporcionar soporte para funciones específicas de SIP.

DNS-TCP

Se utiliza para servidores que aceptan tráfico DNS, donde el dispositivo Citrix ADC actúa como proxy para el tráfico TCP enviado a servidores DNS. Con servicios del tipo de servicio DNS-TCP, el dispositivo Citrix ADC valida el formato de paquete de cada solicitud y respuesta DNS y puede almacenar en caché las respuestas DNS, como ocurre con el tipo de servicio DNS.

También puede utilizar el tipo de servicio TCP para estos servicios. Sin embargo, si lo hace, el dispositivo Citrix ADC solo realiza el equilibrio de carga de la capa 4 de los servidores de nombres DNS externos. No puede proporcionar soporte para ninguna función específica de DNS.

RTSP

Se utiliza para servidores que aceptan tráfico de Protocolo de transmisión en tiempo real (RTSP). RTSP proporciona la entrega de multimedia y otros datos de streaming. Seleccione este tipo para admitir audio, vídeo y otros tipos de medios transmitidos.

También puede utilizar el tipo de servicio TCP para estos servicios. Sin embargo, si lo hace, el dispositivo Citrix ADC solo realiza el equilibrio de carga de la capa 4. No puede analizar el flujo RTSP ni proporcionar soporte para la persistencia RTSPID o NAT RTSP.

DHCPRA

Se utiliza para servidores que aceptan tráfico DHCP. El tipo de servicio DHCPRA se puede utilizar para retransmitir solicitudes DHCP y respuestas entre VLAN.

diameter

Se utiliza para equilibrar la carga del tráfico de diameter entre varios servidores de diameter. Diameter utiliza el equilibrio de carga basado en mensajes.

DIÁMETRO DE SSL_

Se utiliza para equilibrar la carga de tráfico de diameter a través de SSL.

Los servicios se designan como DISABLED hasta que el dispositivo Citrix ADC se conecte al servidor con equilibrio de carga asociado y compruebe que está operativo. En ese momento, el servicio se designa como ENABLED. A partir de entonces, el dispositivo Citrix ADC supervisa periódicamente el estado de los servidores y vuelve a colocar los que no respondan a los sondeos de supervisión (denominados comprobaciones de estado) en el estado DISABLED hasta que respondan.

Nota: Puede crear un rango de servicios a partir de un solo comando CLI o del mismo cuadro de diálogo. Los nombres del rango varían según un número utilizado como sufijo/prefijo. Por ejemplo, service1, service2, etc. Desde la utilidad de configuración, puede especificar un rango solo en el último octeto de la dirección IP, que es el cuarto en caso de una dirección IPv4 y el octavo en una dirección IPv6. Desde la línea de comandos, puede especificar el rango en cualquier octeto de la dirección IP.

QUIC

Utilizado por servidores de equilibrio de carga que aceptan tráfico de vídeo QUIC basado en UDP. El servicio permite que el dispositivo Citrix ADC optimice el tráfico de vídeo ABR cifrado a través del protocolo UDP.

Para crear un servicio mediante la CLI

En el símbolo del sistema, escriba:

```
add service <name> <serverName> <serviceType> <port>

add service Service-HTTP-1 192.0.2.5 HTTP 80
<!--NeedCopy-->
```


Para crear un servicio mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico**> **Equilibrio de carga**> **Servicios**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En el cuadro de diálogo Crear servicio, especifique valores para los siguientes parámetros:
   - Nombre del servicio: Nombre
   - Servidor: NombreServidor
   - Protocolo—ServiceType
   - Puerto: Puerto
4. Haga clic en **Crear** y, a continuación, en **Cerrar**. El servicio creado aparece en el panel Servicios.

Creación de un servidor virtual

Después de crear los servicios, debe crear un servidor virtual para aceptar tráfico para los sitios web, aplicaciones o servidores con equilibrio de carga. Una vez configurado el equilibrio de carga, los usuarios se conectan al sitio web, la aplicación o el servidor con equilibrio de carga a través de la dirección IP o el FQDN del servidor virtual.

Nota:

- Los nombres de servidores virtuales con el prefijo “app_” no aparecen en la GUI aunque están presentes en el archivo ns.conf y se muestran al ejecutar el comando show. Sin embargo, los nombres de servidores virtuales con el prefijo “app” se muestran en la GUI.
- El servidor virtual se designa como DOWN hasta que vincule los servicios que creó a él y hasta que el dispositivo Citrix ADC se conecte a esos servicios y compruebe que están operativos. Solo entonces se designará el servidor virtual como UP.

Para crear un servidor virtual mediante la CLI

En el símbolo del sistema, escriba:

```
add lb vserver <name> <serviceType> <ip> <port>

add lb vserver Vserver-LB-1 HTTP 10.102.29.60 80
<!--NeedCopy-->
```

Para crear un servidor virtual mediante la interfaz gráfica de usuario

Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**y, a continuación, cree un servidor virtual.

Servicios de enlace con el servidor virtual

Nota: Un servicio puede vincularse a un máximo de 500 servidores virtuales.

Después de crear servicios y un servidor virtual, debe vincular los servicios al servidor virtual. Normalmente, los servicios están enlazados a servidores virtuales del mismo tipo, pero puede enlazar ciertos tipos de servicios a ciertos tipos diferentes de servidores virtuales, como se muestra a continuación.

Tipo de servidor virtual	Tipo de servicio	Comentario
HTTP	SSL	Normalmente, enlazaría un servicio SSL a un servidor virtual HTTP para hacer cifrado.
SSL	HTTP	Normalmente, enlazaría un servicio HTTP a un servidor virtual SSL para realizar la descarga SSL.
SSL_TCP	TCP	Normalmente, enlazaría un servicio TCP a un servidor virtual SSL_TCP para realizar la descarga SSL para otro TCP (descifrado SSL sin conocimiento de contenido).

El estado de los servicios enlazados a un servidor virtual determina el estado del servidor virtual: Si todos los servicios enlazados están DOWN, el servidor virtual se marca DOWN y si alguno de los servicios enlazados es UP o OUT OWN OWN SERVICE, el estado del servidor virtual es UP.

Para enlazar un servicio a un servidor virtual de equilibrio de carga mediante la CLI

En el símbolo del sistema, escriba:

```
bind lb vserver <name> <serviceName>

bind lb vserver Vserver-LB-1 Service-HTTP-1
<!--NeedCopy-->
```


Para enlazar un servicio a un servidor virtual de equilibrio de carga mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico**> **Equilibrio de carga**> **Servidores virtuales** y seleccione un servidor virtual.
2. Haga clic en la sección **Servicio** y seleccione un servicio para enlazar.

Nota: Puede enlazar un servicio a varios servidores virtuales.

Verificación de la configuración

Una vez finalizada la configuración básica, puede ver las propiedades de cada servicio y del servidor virtual de equilibrio de carga en la configuración de equilibrio de carga para comprobar que cada uno está configurado correctamente. Una vez que la configuración esté activa y en ejecución, puede ver las estadísticas de cada servicio y del servidor virtual de equilibrio de carga para comprobar si hay posibles problemas.

Visualización de las propiedades de un objeto de servidor

Puede ver propiedades como el nombre, el estado y la dirección IP de cualquier objeto de servidor en la configuración del dispositivo Citrix ADC.

Para ver las propiedades de los objetos de servidor mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
show server <serverName>

show server server-1
<!--NeedCopy-->
```

Para ver las propiedades de los objetos de servidor mediante la utilidad de configuración

Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores**. Los valores de los parámetros de los servidores disponibles aparecen en el panel de detalles.

Visualización de las propiedades de un servidor virtual

Puede ver propiedades como el nombre, el estado, el estado efectivo, la dirección IP, el puerto, el protocolo, el método y el número de servicios enlazados para los servidores virtuales. Si ha configurado

más que la configuración básica de equilibrio de carga, puede ver la configuración de persistencia de los servidores virtuales, cualquier directiva que esté vinculada a ellos y cualquier redirección de caché y servidor virtual de cambio de contenido enlazado a los servidores virtuales.

Para ver las propiedades de un servidor virtual de equilibrio de carga mediante la CLI

En el símbolo del sistema, escriba:

```
show lb vserver <name>

show lb vserver Vserver-LB-1
<!--NeedCopy-->
```

Para ver las propiedades de un servidor virtual de equilibrio de carga mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**.
2. En el panel de detalles, haga clic en un servidor virtual para mostrar sus propiedades en la parte inferior del panel de detalles.
3. Para ver los servidores virtuales de redirección de caché y conmutación de contenido enlazados a este servidor virtual, haga clic en **Mostrar enlaces CS/CR**.

Visualización de las propiedades de un servicio

Puede ver el nombre, el estado, la dirección IP, el puerto, el protocolo, la conexión máxima del cliente, el número máximo de solicitudes por conexión y el tipo de servidor de los servicios configurados, y utilizar esta información para solucionar cualquier error en la configuración del servicio.

Para ver las propiedades de los servicios mediante la CLI

En el símbolo del sistema, escriba:

```
show service <name>

show service Service-HTTP-1
<!--NeedCopy-->
```


Para ver las propiedades de los servicios mediante la interfaz gráfica de usuario

Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servicios**. Los detalles de los servicios disponibles aparecen en el panel Servicios.

Visualización de los enlaces de un servicio

Puede ver la lista de servidores virtuales a los que está enlazado el servicio. La información de enlace también proporciona el nombre, la dirección IP, el puerto y el estado de los servidores virtuales a los que están vinculados los servicios. Puede utilizar la información de enlace para solucionar cualquier problema relacionado con la vinculación de los servicios a servidores virtuales.

Para ver los enlaces de un servicio mediante la CLI

En el símbolo del sistema, escriba:

```
show service bindings <name>

show service bindings Service-HTTP-1
<!--NeedCopy-->
```

Para ver los enlaces de un servicio mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servicios**.
2. En el panel de detalles, seleccione el servicio cuya información de enlace quiere ver.
3. En la ficha **Acción**, haga clic en **Mostrar enlaces**.

Visualización de las estadísticas de un servidor virtual

Para evaluar el rendimiento de los servidores virtuales o solucionar problemas, puede mostrar detalles de los servidores virtuales configurados en el dispositivo Citrix ADC. Puede mostrar un resumen de estadísticas para todos los servidores virtuales o puede especificar el nombre de un servidor virtual para mostrar las estadísticas solo para ese servidor virtual. Puede mostrar los siguientes detalles:

- Nombre
- Dirección IP
- Port
- Protocolo
- Estado del servidor virtual
- Tasa de solicitudes recibidas

- Tasa de visitas

Para mostrar las estadísticas del servidor virtual mediante la CLI

Para mostrar un resumen de las estadísticas de todos los servidores virtuales configurados actualmente en el dispositivo o de un único servidor virtual, escriba en el símbolo del sistema:

```
stat lb vserver [`<name>`]
<!--NeedCopy-->
```

Ejemplo:

```
stat lb vserver server-1
<!--NeedCopy-->
```

En la siguiente ilustración se muestra una estadística de ejemplo.


```
> stat lbvserver
[
Virtual Server(s) Summary
                        vsvrIP  port     Protocol        State    Req/s
vserver1        10.102.20.200    80          SSL         DOWN      0/s

lb1               203.1.113.5   443         DTLS         DOWN      0/s

vicap                       *     0          TCP         DOWN      0/s

lbicap                2.2.3.4  1344          TCP         DOWN      0/s

app_...stest          0.0.0.0     0         HTTP         DOWN      0/s

app_...ttest          0.0.0.0     0         HTTP         DOWN      0/s

app_...fault          0.0.0.0     0         HTTP         DOWN      0/s

app_...test1          0.0.0.0     0         HTTP         DOWN      0/s

app_...1test          0.0.0.0     0         HTTP         DOWN      0/s

app_...fault          0.0.0.0     0         HTTP         DOWN      0/s

app_...est12          0.0.0.0     0         HTTP         DOWN      0/s

app_...sting          0.0.0.0     0         HTTP         DOWN      0/s

test                  2.2.2.2    80         HTTP         DOWN      0/s

shar...lt-lb          0.0.0.0     0         HTTP         DOWN      0/s

shar...es-lb          0.0.0.0     0         HTTP           UP      0/s

shar...es-lb          0.0.0.0     0         HTTP           UP      0/s

shar...nt-lb          0.0.0.0     0         HTTP           UP      0/s

shar...nt-lb          0.0.0.0     0         HTTP           UP      0/s

shar...nt-lb          0.0.0.0     0         HTTP           UP      0/s

shar...nt-lb          0.0.0.0     0         HTTP           UP      0/s

shar...nt-lb          0.0.0.0     0         HTTP           UP      0/s

shar...nt-lb          0.0.0.0     0         HTTP           UP      0/s

shar...nt-lb          0.0.0.0     0         HTTP           UP      0/s

shar...ts-lb          0.0.0.0     0         HTTP           UP      0/s

shar...ns-lb          0.0.0.0     0         HTTP           UP      0/s

shar...as-lb          0.0.0.0     0         HTTP           UP      0/s

forward-vs            0.0.0.0     0          TCP         DOWN      0/s

tcpcs                 0.0.0.0     0          TCP         DOWN      0/s

test124               0.0.0.0     0          SSL         DOWN      0/s

testssl               0.0.0.0     0          SSL         DOWN      0/s
```


Para mostrar las estadísticas del servidor virtual mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**.
2. Si quiere mostrar las estadísticas de un solo servidor virtual, en el panel de detalles, seleccione el servidor virtual cuyas estadísticas quiere mostrar.
3. En el panel de detalles, haga clic en **Estadísticas**.

Visualización de las estadísticas de un servicio

Puede ver la tasa de solicitudes, respuestas, bytes de solicitud, bytes de respuesta, conexiones de cliente actuales, solicitudes en la cola de sobretensión, conexiones de servidor actuales, etc. mediante las estadísticas del servicio.

Para ver las estadísticas de un servicio mediante la CLI

En el símbolo del sistema, escriba:

```
stat service <name>
<!--NeedCopy-->
```

Ejemplo:

```
stat service Service-HTTP-1
<!--NeedCopy-->
```

Para ver las estadísticas de un servicio mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servicios**.
2. En el panel de detalles, seleccione el servicio cuyas estadísticas quiere ver (por ejemplo, Service-HTTP-1).
3. Haga clic en **Estadísticas**. Las estadísticas aparecen en una nueva ventana.

Estado de servicio y servidor virtual de equilibrio de carga

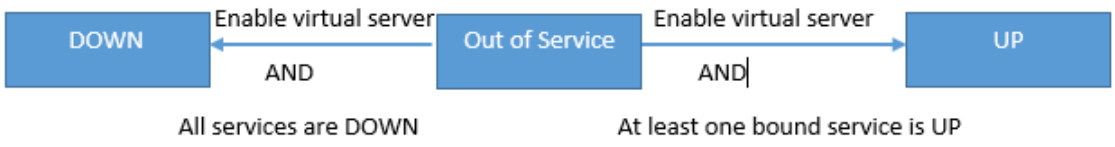
August 20, 2021

Un servidor virtual de equilibrio de carga que no tiene un servidor virtual de copia de seguridad puede tomar los siguientes estados, según los estados de los servicios vinculados a él y si está inhabilitado administrativamente:

- **UP**: Al menos uno de los servicios vinculados al servidor virtual está UP.
- **DOWN**: Todos los servicios enlazados al servidor virtual están DOWN o la función de equilibrio de carga no está habilitada.
- **Fuera de servicio (OFS)**: Si inhabilita administrativamente el servidor virtual, éste entra en el estado OFS pero su estado efectivo es DOWN. El administrador puede controlar la transición al estado OFS desde el estado DOWN o UP, o al estado DOWN o UP desde el estado OFS.

El estado y el estado efectivo de un servidor virtual son los mismos si no se configura un servidor virtual de copia de seguridad. Sin embargo, si se configura un servidor virtual de respaldo o una cadena de servidores virtuales de backup, el estado efectivo se deriva de los estados de los servicios vinculados al servidor virtual principal y a los servidores virtuales de respaldo. Si alguno de los servidores virtuales de copia de seguridad de la cadena es UP, el estado efectivo del servidor virtual principal es UP, incluso si todos los servicios vinculados al servidor virtual primario están DOWN.

Los diagramas siguientes muestran las condiciones en las que un servidor virtual pasa de un estado a otro.



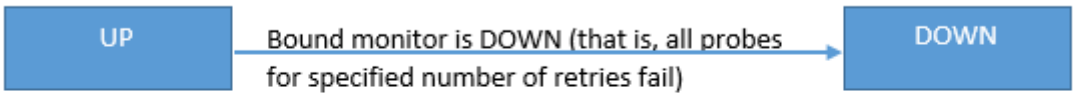
Un servicio puede tener los siguientes estados:

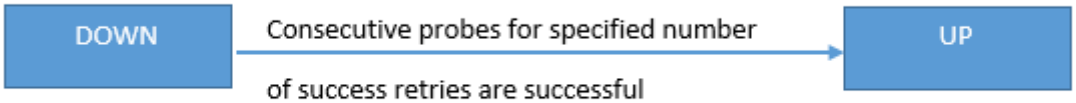
- **UP:** Si los sondeos de todos los monitores vinculados al servicio son correctos.
- **DOWN**: Si los sondeos de supervisión para el servicio no se responden dentro del límite de tiempo configurado.
- **Fuera de servicio**: Si inhabilita administrativamente el servicio, o si cierra el servicio correctamente y no hay transacciones activas en el servicio
- **DESCUENTA DE SERVICIO (TROFS)**: Si inhabilita administrativamente el servicio con retraso, o cierra el servicio con gracia y hay transacciones activas en el servicio. Para obtener más información, consulte Cierre de servicios de forma grácil.
- **APAGADA AL SALIR DE SERVICIO (TROFS_DOWN)[]** Un sondeo de supervisión falla mientras el servicio está en estado GOING OUT OF SERVICE.

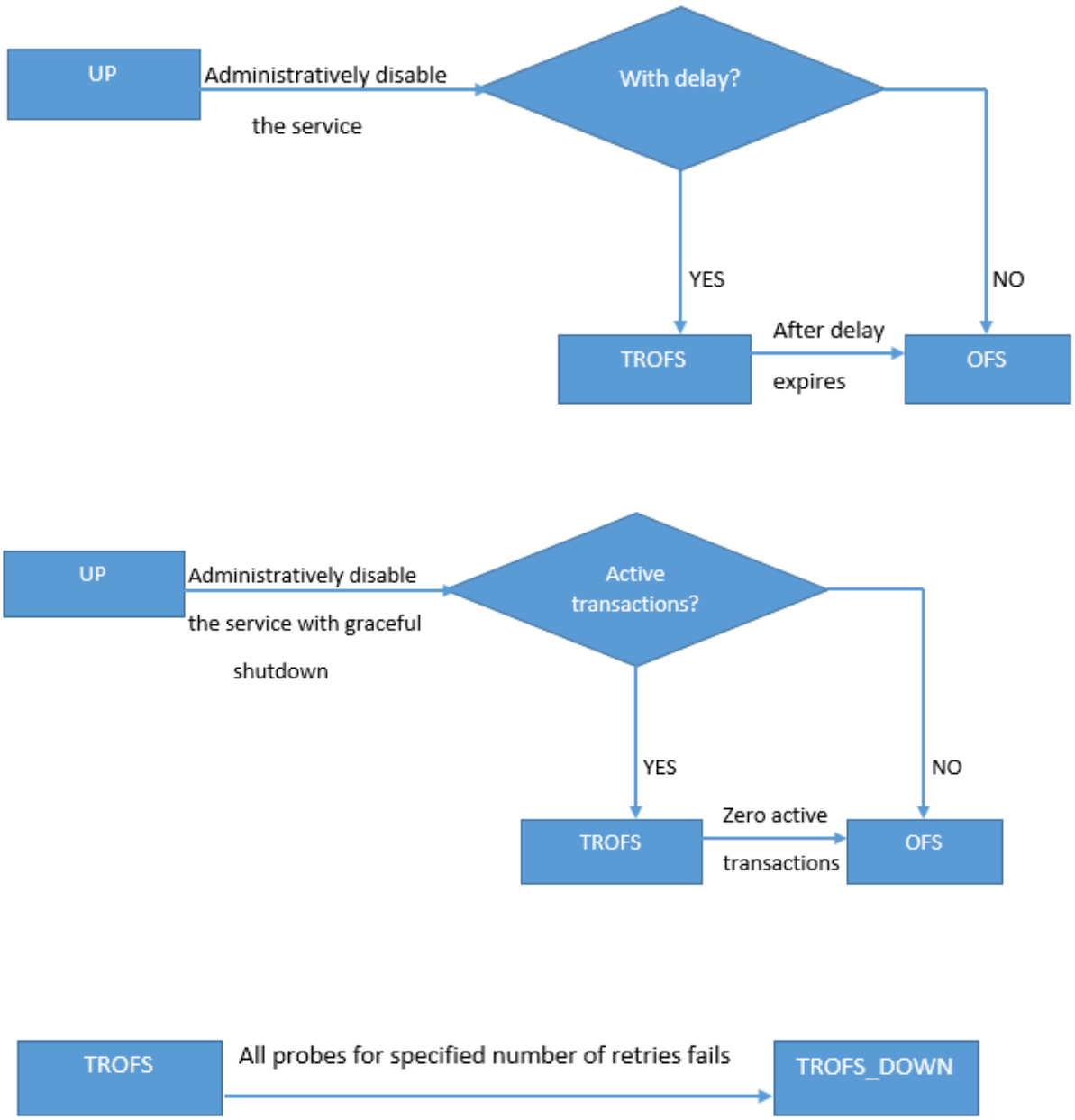
Un servicio en el proceso de transición de UP a OFS está en el estado de salida del servicio. Un servicio que pasa de DOWN a OFS se encuentra en el estado DOWN WHEN GOING OUT OF SERVICE. Por ejemplo, si un servicio está DOWN y lo inhabilita con retraso, el servicio pasa a DOWN When DOWN WHEN GOING OUT OF SERVICE y, a continuación, al estado OUT OF SERVICE. Si un servicio está UP y lo inhabilita con retraso, el servicio pasa a DESACTIVAR DE SERVICIO. Durante este tiempo, si se produce un error en un sondeo de supervisión al servidor, el servicio pasa a DOWN WHEN GOING OUT OF SERVICE y, después de que expire el tiempo de demora, entra en el estado OFS.

> **Nota**
>
> Puede configurar el desbordamiento en un servidor virtual de copia de seguridad estableciendo el parámetro “HealthThreshold” en un valor positivo distinto de cero. A continuación, si un único servicio vinculado al servidor virtual principal pasa al estado DOWN WHEN GOING OUT OF SERVICE y no se alcanza el umbral de mantenimiento, el servidor virtual principal se marca como DOWN y las nuevas conexiones se dirigen al servidor virtual de copia de seguridad.

Los diagramas siguientes muestran las condiciones en las que un servicio pasa de un estado a otro.







Soporte para perfil de equilibrio de carga

August 20, 2021

Una configuración de equilibrio de carga tiene muchos parámetros, por lo que configurar los mismos parámetros en varios servidores virtuales puede resultar tedioso. A partir de la versión 11.1, un perfil de

equilibrio de carga (LB) facilita esta tarea. Ahora puede establecer parámetros de equilibrio de carga en un perfil y asociar este perfil con servidores virtuales, en lugar de establecer estos parámetros en cada servidor virtual.

Los siguientes parámetros se admiten actualmente en un perfil LB:

- `HTTPonlyflag`: incluye el atributo HttpOnly en las cookies de persistencia. El atributo HttpOnly limita el ámbito de una cookie a las solicitudes HTTP y ayuda a mitigar el riesgo de ataques de scripts entre sitios.
- useSecurredPersistenceCookie: cifra los valores de las cookie de persistencia mediante el algoritmo hash SHA2.
- `Cookiepassphrase`: especifique la frase de contraseña utilizada para generar un valor de cookie de persistencia segura.
- DBS_LB: Habilite el equilibrio de carga específico de la base de datos para los tipos de servicio MySQL y MSSQL.
- CL_PROCESS_LOCAL: Los paquetes destinados a un servidor virtual en un clúster no se dirigen. Active la opción para el modo de respuesta de solicitud de paquete único o cuando el dispositivo ascendente está realizando un RSS adecuado para la distribución basada en conexión.
- lbhashAlgorithm: especifique el algoritmo de hash que se utilizará para los siguientes métodos de equilibrio de carga basados en hash:
  - Método hash de URL
  - Método hash de dominio
  - Método hash IP de destino
  - Método hash IP de origen
  - Método hash IP de destino IP de origen
  - Método hash del puerto de origen IP de origen
  - Método hash ID de llamada
  - Método Token

  Valores posibles: DEFAULT, PRAC, JARH Valor
  predeterminado: DEFAULT
- LBHashFingers: especifique el número de huellas que se utilizarán en los algoritmos PRAC y JARH para los métodos LB basados en hash. El aumento del número de huellas proporciona una mejor distribución del tráfico a expensas de la memoria adicional.

Valor predeterminado: 256 Valor
mínimo: 1 Valor
máximo: 1024

> **Nota**
>
> Puede establecer los parámetros DBS_LB y CL_Process_Local en un servidor virtual y en el perfil. Si habilita estos parámetros en un servidor virtual y, a continuación, establece un perfil en este servidor virtual, los parámetros aparecen como inhabilitados en la salida del "`show lb vserver`" comando para ese servidor virtual. Compruebe el perfil para ver el estado real de estos parámetros. Además, si establece y desestablece un perfil en un servidor virtual, los parámetros se establecen con valores predeterminados para ese servidor virtual.

Para crear un perfil LB mediante la CLI

En el símbolo del sistema, escriba:

```
add lb profile <lbprofilename> -dbsLb ( ENABLED | DISABLED ) -
    processLocal ( ENABLED | DISABLED ) -httpOnlyCookieFlag ( ENABLED |
    DISABLED ) -cookiePassphrase -useSecuredPersistenceCookie ( ENABLED
    | DISABLED ) -lbHashAlgorithm <lbHashAlgorithm> -lbHashFingers <
    positive_integer>
<!--NeedCopy-->
```

Ejemplo:

```
> sh lb profile p1
LB Profile name:  p1
DBS LB : DISABLED   Process Local: DISABLED
Persistence Cookie HttpOnly Flag: ENABLED
Use Encrypted Persistence Cookie: DISABLED
No of vservers bound: 0
Store MQTT clientid and username in transactional logs: NO
Hash LB algorithm used in LB decision: DEFAULT
Number of fingers for Hash LB algorithm: 256
Done

<!--NeedCopy-->
```

Para crear un perfil LB mediante la interfaz gráfica de usuario

Vaya a **Sistema** > **Perfiles** > **Perfil LB** y agregue un perfil.

Para asociar un perfil LB con un servidor virtual LB mediante la CLI

En el símbolo del sistema, escriba:

```
set lb vserver <name> -lbprofilename <string>
<!--NeedCopy-->
```

Ejemplo

```
set lbvserver lbvip1 -lbprofile p1

Done

sh lb vserver lbvip1

lbvip1 (203.0.113.1:80) - HTTP       Type: ADDRESS
State: UP
Last state change was at Wed May 25 12:36:20 2016
Time since last state change: 0 days, 00:01:26.140
Effective State: UP  ARP:DISABLED
Client Idle Timeout: 180 sec
Down state flush: ENABLED
Disable Primary Vserver On Down : DISABLED
Appflow logging: ENABLED
Port Rewrite : DISABLED
No. of Bound Services :  2 (Total)       2 (Active)
Configured Method: LEASTCONNECTION      BackupMethod: ROUNDROBIN
Mode: IP
Persistence: NONE
Vserver IP and Port insertion: OFF
Push: DISABLED  Push VServer:
Push Multi Clients: NO
Push Label Rule: none
L2Conn: OFF
Skip Persistency: None
Listen Policy: NONE
IcmpResponse: PASSIVE
RHIstate: PASSIVE
New Service Startup Request Rate: 0 PER_SECOND, Increment Interval: 0
Mac mode Retain Vlan: DISABLED
DBS_LB: DISABLED
Process Local: DISABLED
Traffic Domain: 0
```



```
LB Profile: p1
Done
<!--NeedCopy-->
```

Para asociar un perfil LB con un servidor virtual LB mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**.
2. Seleccione un servidor virtual y haga clic en **Modificar**.
3. En **Configuración avanzada**, haga clic en **Perfiles**.
4. En la lista **Perfil LB**, seleccione el perfil que quiere asociar con este servidor virtual.

Algoritmos de equilibrio de carga

August 20, 2021

El algoritmo de equilibrio de carga define los criterios que utiliza el dispositivo Citrix ADC para seleccionar el servicio al que redirigir cada solicitud de cliente. Los diferentes algoritmos de equilibrio de carga utilizan criterios diferentes. Por ejemplo, el algoritmo de menor conexión selecciona el servicio con menor número de conexiones activas, mientras que el algoritmo de round robin mantiene una cola en ejecución de servicios activos, distribuye cada conexión al siguiente servicio de la cola y, a continuación, envía ese servicio al final de la cola.

Algunos algoritmos de equilibrio de carga son los más adecuados para manejar el tráfico en sitios web, otros para administrar el tráfico a servidores DNS y otros para manejar aplicaciones web complejas utilizadas en comercio electrónico o en LAN o WAN de la empresa. En la siguiente tabla se enumeran cada algoritmo de equilibrio de carga compatible con el dispositivo Citrix ADC, con una breve descripción de cómo funciona cada uno de ellos.

Nombre	Selección del servidor basada en
MENOS CONEXIÓN	Qué servicio tiene actualmente el menor número de conexiones de cliente. Este es el algoritmo de equilibrio de carga predeterminado.
ROUNDROBIN	Qué servicio está en la parte superior de una lista de servicios. Después de seleccionar ese servicio para una conexión, se mueve al final de la lista.

Nombre	Selección del servidor basada en
MENOS TIEMPO DE RESPUESTA	Qué servidor equilibrado de carga tiene actualmente el tiempo de respuesta más rápido.
URLHASH	Un hash de la URL de destino.
DOMINIO HASH	Un hash del dominio de destino.
DESTINATIONIFASH	Un hash de la dirección IP de destino.
SOURCEIPHASH	Un hash de la dirección IP de origen.
SRCIPDESTIPHASH	Un hash de las direcciones IP de origen y destino.
CALIDHASH	Un hash del ID de llamada en el encabezado SIP.
SRCIPSRCPORTHASH	Un hash de la dirección IP y el puerto del cliente.
LEASTBANDWIDTH	Qué servicio tiene actualmente menos restricciones de ancho de banda.
LEASTPACKETS	Qué servicio recibe actualmente el menor número de paquetes.
CUSTOMLOAD	Datos de un monitor de carga.
TOKEN	El token configurado.
LRTM	Menor número de conexiones activas y el menor tiempo de respuesta promedio.

Dependiendo del protocolo del servicio que esté equilibrando la carga, el dispositivo Citrix ADC configura cada conexión entre el cliente y el servidor para que dure un intervalo de tiempo diferente. Esto se denomina granularidad de equilibrio de carga, de los cuales son tres tipos: Granularidad basada en solicitudes, basada en conexiones y granularidad basada en tiempo. La tabla siguiente describe cada tipo de granularidad y cuándo se utiliza cada uno.

Granularidad	Tipos de servicio balanceado de carga	Especifica
Basado en solicitudes	HTTP o HTTPS	Se elige un nuevo servicio para cada solicitud HTTP, independientemente de las conexiones TCP. Al igual que con todas las solicitudes HTTP, una vez que el servidor web cumple la solicitud, la conexión se cierra.
Basado en conexión	Protocolos TCP y basados en TCP distintos de HTTP	Se elige un servicio para cada nueva conexión TCP. La conexión persiste hasta que el servicio o el cliente la terminen.
Basado en el tiempo	UDP y otros protocolos IP	Se elige un nuevo servicio para cada paquete UDP. Tras la selección de un servicio, se crea una sesión entre el servicio y un cliente durante un período determinado. Cuando expira el tiempo, se elimina la sesión y se elige un nuevo servicio para cualquier paquete adicional, incluso si esos paquetes provienen del mismo cliente.

Durante el inicio de un servidor virtual, o siempre que cambie el estado de un servidor virtual, el servidor virtual puede utilizar inicialmente el método round robin para distribuir las solicitudes del cliente entre los servidores físicos. Este tipo de distribución, denominado *round robin de inicio,* ayuda a evitar la carga innecesaria en un único servidor a medida que se sirven las solicitudes iniciales. Después de utilizar el método round robin en el inicio, el servidor virtual cambia al método de equilibrio de carga especificado en el servidor virtual.

El factor RR de inicio funciona de la siguiente manera:

- Si el factor RR de inicio se establece en cero, el dispositivo cambia al método de equilibrio de carga especificado en función de la velocidad de solicitud.

- Si el factor RR de inicio es cualquier número que no sea cero, el dispositivo utiliza el método round robin para el número especificado de solicitudes antes de cambiar al método de equilibrio de carga especificado.
- De forma predeterminada, el factor RR de inicio se establece en cero.

Nota: No puede establecer el factor RR de inicio para un servidor virtual individual. El valor especificado se aplica a todos los servidores virtuales del dispositivo Citrix ADC.

Para establecer el factor de inicio round robin mediante la CLI

En el símbolo del sistema, escriba:

```
set lb parameter -startupRRFactor <positive_integer>
```

Ejemplo

```
set lb parameter -startupRRFactor 25000
```

Para establecer el factor de inicio round robin mediante el uso de la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Configurar parámetros de equilibrio**de carga y establezca el factor RR de inicio.

Método de conexión mínimo

August 20, 2021

Cuando un servidor virtual está configurado para utilizar el algoritmo de equilibrio de carga de conexión mínimo (o método), selecciona el servicio con el menor número de conexiones activas. Este es el método predeterminado, porque, en la mayoría de las circunstancias, proporciona el mejor rendimiento.

Para los servicios TCP, HTTP, HTTPS y SSL_TCP, el dispositivo Citrix ADC incluye los siguientes tipos de conexión en su lista de conexiones existentes:

- **Conexiones activas a un servicio.** Conexiones que representan las solicitudes que un cliente ha enviado al servidor virtual y que el servidor virtual ha reenviado a un servicio. Para los servicios HTTP y HTTPS, las conexiones activas representan solo aquellas solicitudes HTTP o HTTPS que aún no han recibido respuesta.
- **Esperando conexiones en la cola de sobretensiones.** Cualquier conexión al servidor virtual que esté esperando en una cola de sobretensión y que aún no se haya reenviado a un servicio.

Las conexiones pueden acumularse en la cola de sobretensiones en cualquier momento, por cualquiera de las siguientes razones:

- Sus servicios tienen límites de conexión y todos los servicios de su configuración de equilibrio de carga están en ese límite.
- La función de protección contra sobretensiones está configurada y ha sido activada por una sobretensión en las solicitudes al servidor virtual.
- El servidor con equilibrio de carga ha alcanzado un límite interno y, por lo tanto, no abre nuevas conexiones. (Por ejemplo, se alcanza el límite de conexión de un servidor Apache).

Cuando un servidor virtual utiliza el método de menor conexión, considera que las conexiones en espera pertenecen al servicio específico. Por lo tanto, no abre nuevas conexiones a esos servicios.

Para los servicios UDP, las conexiones que considera el algoritmo de menor conexión incluyen todas las sesiones entre el cliente y un servicio. Estas sesiones son entidades lógicas basadas en el tiempo. Cuando llega el primer paquete UDP de una sesión, el dispositivo Citrix ADC crea una sesión entre la dirección IP y el puerto de origen y la dirección IP y el puerto de destino.

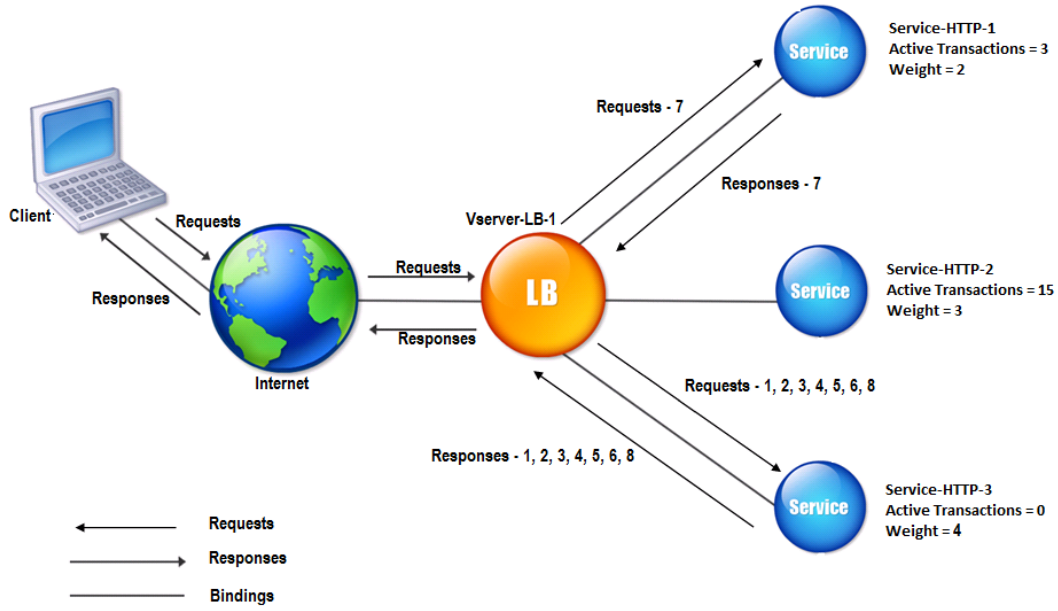
Para las conexiones de Protocolo de transmisión en tiempo real (RTSP), el dispositivo Citrix ADC utiliza el número de conexiones de control activas para determinar el menor número de conexiones a un servicio RTSP.

En el ejemplo siguiente se muestra cómo un servidor virtual selecciona un servicio para el equilibrio de carga mediante el método de menor conexión. Considere los tres servicios siguientes:

- Service-HTTP-1 está manejando 3 transacciones activas.
- Service-HTTP-2 está manejando 15 transacciones activas.
- Service-HTTP-3 no está manejando ninguna transacción activa.

En el siguiente diagrama se muestra cómo el dispositivo Citrix ADC reenvía las solicitudes entrantes cuando se utiliza el método de menor conexión.

Ilustración 1. Mecanismo del método de equilibrio de carga de menos conexiones



En este diagrama, el servidor virtual selecciona el servicio para cada conexión entrante eligiendo el servidor con el menor número de transacciones activas.

Las conexiones se reenvían de la siguiente manera:

- Service-HTTP-3 recibe la primera solicitud, ya que no está manejando ninguna transacción activa.

  Nota: El servicio sin transacción activa se selecciona primero.

- Service-HTTP-3 recibe la segunda y tercera solicitudes porque el servicio tiene el siguiente menor número de transacciones activas.
- Service-HTTP-1 recibe la cuarta solicitud porque Service-HTTP-1 y Service-HTTP-3 tienen el mismo número de transacciones activas, el servidor virtual utiliza el método round robin para elegir entre ellas.
- Service-http-3 recibe la quinta solicitud.
- Service-HTTP-1 recibe la sexta solicitud, y así sucesivamente, hasta que Service-HTTP-1 y Service-HTTP-3 manejan el mismo número de solicitudes que Service-HTTP-2. A continuación, el dispositivo Citrix ADC comienza a reenviar solicitudes a Service-HTTP-2 cuando es el servicio menos cargado o aparece su turno en la cola de round robin.

  Nota: Si las conexiones a Service-HTTP-2 se cierran, podría obtener nuevas conexiones antes de que cada uno de los otros dos servicios tenga 15 transacciones activas.

En la tabla siguiente se explica cómo se distribuyen las conexiones en la configuración de equilibrio de carga de tres servicios descrita anteriormente.

Conexión entrante	Servicio seleccionado	Número actual de conexiones activas	Observaciones
Request-1	Service-HTTP-3; (N = 0)	1	Service-HTTP-3 tiene el menor número de conexiones activas.
Request-2	Service-HTTP-3; (N = 1)	2	Service-HTTP-3 tiene el menor número de conexiones activas.
Request-3	Service-HTTP-3; (N = 2)	3	-
Request-4	Servicio-HTTP-1; (N = 3)	4	Service-HTTP-1 y Service-HTTP-3 tienen el mismo número de conexiones activas.
Request-5	Service-HTTP-3; (N = 3)	4	Service-HTTP-1 y Service-HTTP-3 tienen el mismo número de conexiones activas.
Request-6	Service-HTTP-1;(N = 4)	5	-
Request-7	Service-HTTP-3; (N = 4)	5	-
Request-8	Servicio-HTTP-1; (N = 5)	6	-

Service-HTTP-2 se selecciona para el equilibrio de carga cuando completa sus transacciones activas y se cierran las conexiones actuales, o cuando los otros servicios (Service-HTTP-1 y Servicio-HTTP-3) tienen 15 o más conexiones cada uno.

El dispositivo Citrix ADC también puede utilizar el método de menor conexión cuando se asignan pesos a los servicios. Se selecciona un servicio mediante el valor (Nw) de la siguiente expresión:

Nw = (Número de transacciones activas) * (10000/peso)

En el ejemplo siguiente se muestra cómo el dispositivo Citrix ADC selecciona un servicio para el equilibrio de carga mediante el método de menor conexión cuando se asignan pesos a los servicios. En el ejemplo anterior, supongamos que a Service-HTTP-1 se le asigna un peso de 2, Service-HTTP-2 se le asigna un peso de 3 y Service-HTTP-3 se le asigna un peso de 4. Las conexiones se reenvían de la siguiente manera:

- Service-HTTP-3 recibe el primero porque el servicio no está manejando ninguna transacción activa.

  Nota: Si los servicios no gestionan ninguna transacción activa, el dispositivo Citrix ADC utiliza el método round robin independientemente de las ponderaciones asignadas a cada uno de los servicios.

- Service-HTTP-3 recibe la segunda, tercera, cuarta, quinta, sexta y séptima solicitudes porque el servicio tiene el valor Nw más bajo.
- Service-HTTP-1 recibe la octava solicitud. Dado que Service-HTTP-1 y Service-HTTP-3 ahora tienen el mismo valor Nw, el dispositivo realiza el equilibrio de carga de forma redonda. Por lo tanto, Service-HTTP-3 recibe la novena solicitud.

En la tabla siguiente se explica cómo se distribuyen las conexiones en la configuración de equilibrio de carga de tres servicios descrita anteriormente.

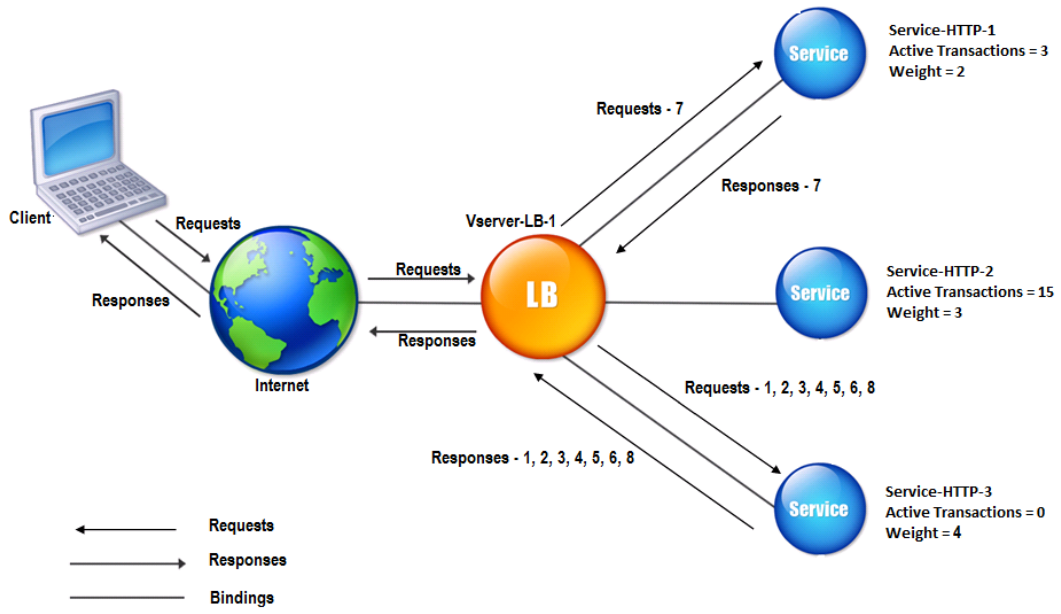
Solicitud recibida	Servicio seleccionado	Valor Nw actual (Número de transacciones activas) * (10000/peso)	Observaciones
Request-1	Servicio-HTTP-3; (Nw = 0)	Nw = 2500	Service-HTTP-3 tiene el valor Nw más bajo.
Request-2	Servicio-HTTP-3; (Nw = 2500)	Nw = 5000	
Request-3	Servicio-HTTP-3; (Nw = 5000)	Nw = 7500	
Request-4	Servicio-HTTP-3; (Nw = 7500)	Nw = 10000	
Request-5	Servicio-HTTP-3; (Nw = 10000)	Nw = 12500	
Request-6	Servicio-HTTP-3; (Nw = 12500)	Nw = 15000	

Solicitud recibida	Servicio seleccionado	Valor Nw actual (Número de transacciones activas) * (10000/peso)	Observaciones
Request-7	Servicio-HTTP-1; (Nw = 15000)	Nw = 20000	Service-HTTP-1 y Service-HTTP-3 tienen los mismos valores Nw
Request-8	Servicio-HTTP-3; (Nw = 15000)	Nw = 17500	

Service-HTTP-2 se selecciona para el equilibrio de carga cuando finaliza sus transacciones activas o cuando el valor Nw de otros servicios (Service-HTTP-1 y Servicio-HTTP-3) es igual a 50000.

En el siguiente diagrama se muestra cómo el dispositivo Citrix ADC utiliza el método de menor conexión cuando se asignan pesos a los servicios.

Ilustración 2. Mecanismo del método de equilibrio de carga de las conexiones mínimas cuando se asignan pesos



Para configurar el método de menor conexión, consulte Configuración de un método de equilibrio de carga que no incluye una directiva.

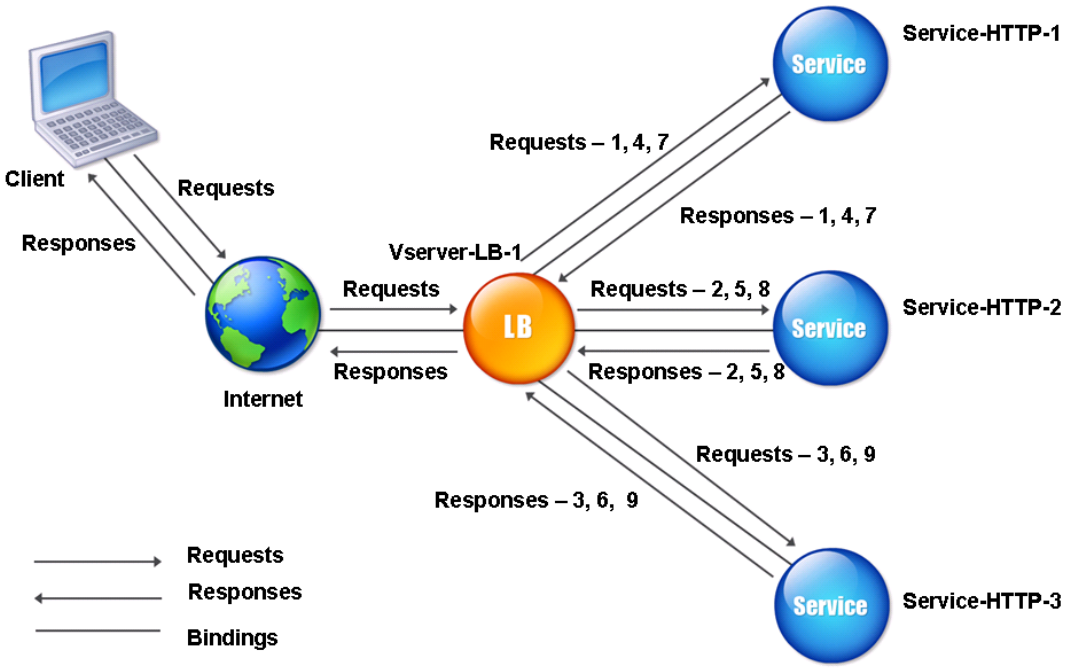
Método Round robin

August 20, 2021

Cuando se configura un servidor virtual de equilibrio de carga para utilizar el método round robin, gira continuamente una lista de los servicios que están enlazados a él. Cuando el servidor virtual recibe una solicitud, asigna la conexión al primer servicio de la lista y, a continuación, mueve ese servicio al final de la lista.

En el siguiente diagrama se muestra cómo el dispositivo Citrix ADC utiliza el método round robin con una configuración de equilibrio de carga que contiene tres servidores con equilibrio de carga y sus servicios asociados.

Ilustración 1. Cómo funciona el método de equilibrio de carga Round Robin



Si asigna un peso diferente a cada servicio, el dispositivo Citrix ADC realiza la distribución de round robin ponderada de las conexiones entrantes. Lo hace omitiendo los servicios de menor ponderación

a intervalos apropiados.

Por ejemplo, suponga que tiene una configuración de equilibrio de carga con tres servicios. Establezca Service-HTTP-1 en un peso de 2, Servicio-HTTP-2 en un peso de 3 y Servicio-HTTP-3 en un peso de 4. Los servicios están enlazados a VServer-LB-1, que está configurado para utilizar el método round robin. Con esta configuración, las solicitudes entrantes se entregan de la siguiente manera:

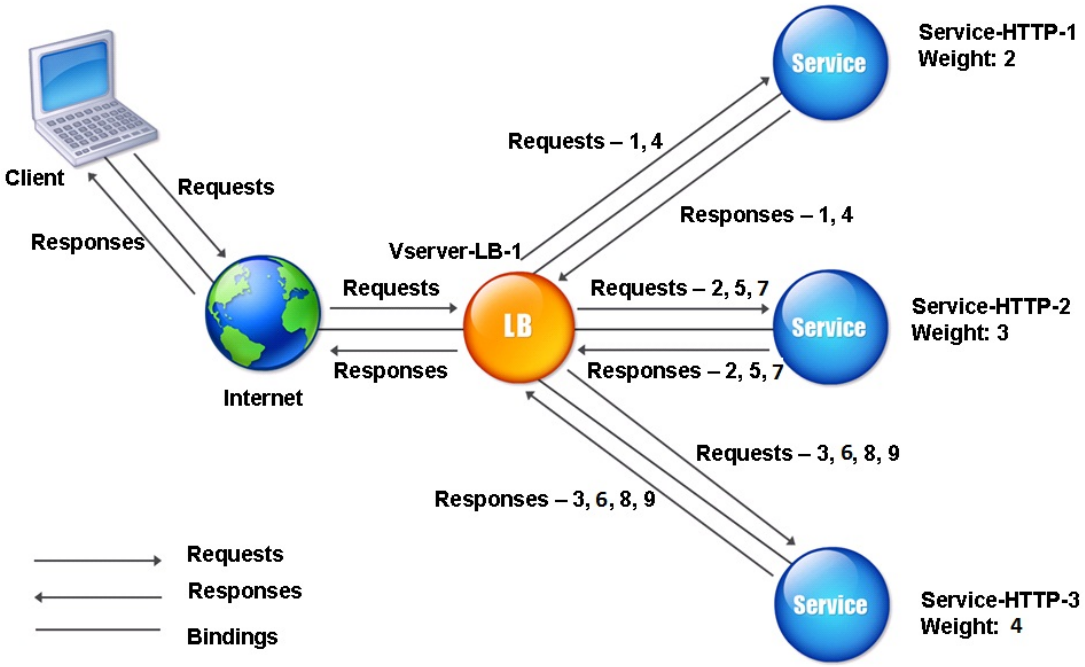
- Service-HTTP-1 recibe la primera solicitud.
- Service-http-2 recibe la segunda solicitud.
- Service-HTTP-3 recibe la tercera solicitud.
- Service-HTTP-1 recibe la cuarta solicitud.
- Service-http-2 recibe la quinta solicitud.
- Service-http-3 recibe la sexta solicitud.
- Service-http-2 recibe la séptima solicitud.
- Service-HTTP-3 recibe tanto la octava como la novena solicitud.

Nota: También puede configurar pesos en los servicios para evitar que varios servicios utilicen el mismo servidor y sobrecarguen el servidor.

A continuación, comienza un nuevo ciclo, mediante el mismo patrón.

El siguiente diagrama ilustra el método de round robin ponderado.

Ilustración 2. Cómo admite el método de equilibrio de carga Round Robin



Para configurar el método de round robin, consulte Configuración de un método de equilibrio de carga que no incluye una directiva.

Método de tiempo de respuesta mínimo

August 20, 2021

Cuando el servidor virtual de equilibrio de carga está configurado para utilizar el método de menor tiempo de respuesta, selecciona el servicio con menos conexiones activas y el tiempo medio de respuesta más bajo. Puede configurar este método solo para servidores virtuales de equilibrio de carga HTTP y Secure Sockets Layer (SSL). El tiempo de respuesta (también llamado Time to First Byte, o TTFB) es el intervalo de tiempo entre el envío de un paquete de solicitud a un servicio y la recepción del primer paquete de respuesta del servicio. El dispositivo Citrix ADC utiliza el código de respuesta 200 para calcular TTFB.

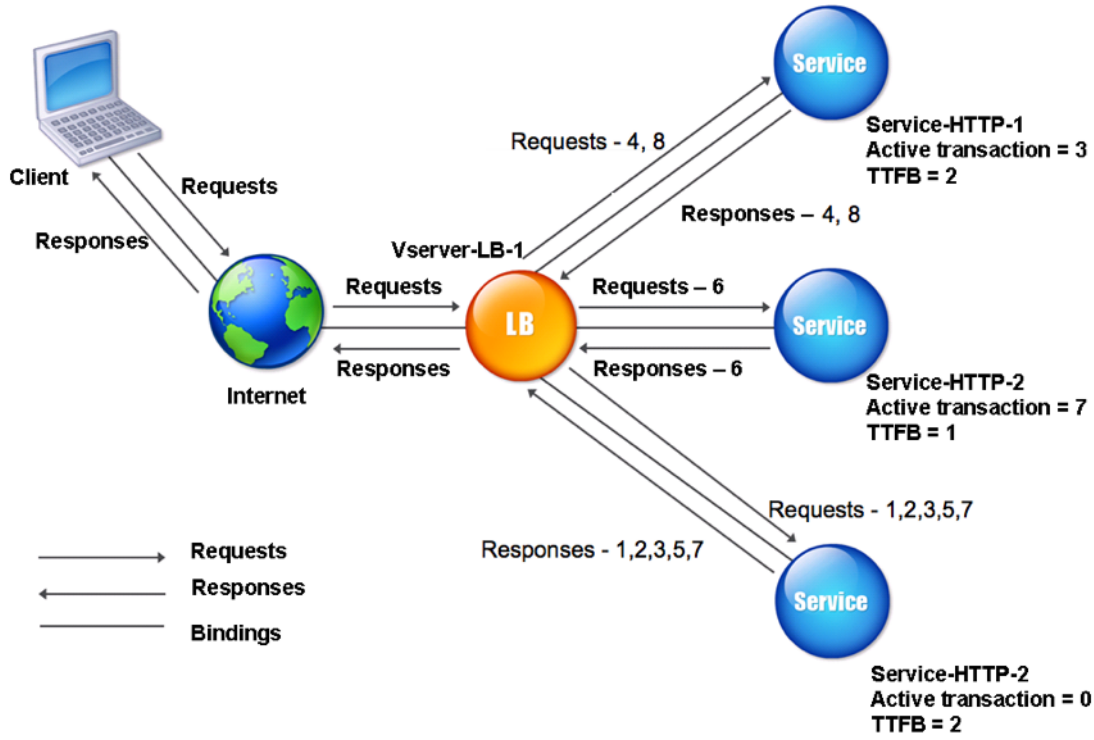
En el ejemplo siguiente se muestra cómo un servidor virtual selecciona un servicio para el equilibrio de carga mediante el método de menor tiempo de respuesta. Considere los tres servicios siguientes:

- Service-HTTP-1 está manejando tres transacciones activas y TTFB es de dos segundos.

- Service-HTTP-2 está manejando siete transacciones activas y TTFB es un segundo.
- Service-HTTP-3 no está manejando ninguna transacción activa y TTFB es de dos segundos.

En el siguiente diagrama se muestra cómo el dispositivo Citrix ADC utiliza el método de menor tiempo de respuesta para reenviar las conexiones.

Ilustración 1. Cómo funciona el método de equilibrio de carga de tiempo de respuesta mínimo



El servidor virtual selecciona un servicio multiplicando el número de transacciones activas por el TTFB para cada servicio y, a continuación, seleccionando el servicio con el resultado más bajo. Para el ejemplo mostrado anteriormente, el servidor virtual reenvía las solicitudes de la siguiente manera:

- Service-HTTP-3 recibe la primera solicitud, porque el servicio no está manejando ninguna transacción activa.
- Service-HTTP-3 también recibe la segunda y la tercera solicitudes, porque el resultado es el más bajo de los tres servicios.
- Service-HTTP-1 recibe la cuarta solicitud. Dado que Service-HTTP-1 y Service-HTTP-3 tienen el mismo resultado, el dispositivo Citrix ADC elige entre ellos aplicando el método Round Robin.
- Service-http-3 recibe la quinta solicitud.
- Service-http-2 recibe la sexta solicitud, porque en este punto tiene el resultado más bajo.
- Dado que Service-HTTP-1, Service-HTTP-2 y Service-HTTP-3 todos tienen el mismo resultado en este momento, el dispositivo cambia al método round robin y continúa distribuyendo conex-

iones mediante ese método.

En la tabla siguiente se explica cómo se distribuyen las conexiones en la configuración de equilibrio de carga de tres servicios descrita anteriormente.

Solicitud recibida	Servicio seleccionado	Valor N Actual (Número de Transacciones Activas * TTFB)	Observaciones
Request-1	Service-HTTP-3;(N = 0)	N = 2	Service-HTTP-3 tiene el valor N más bajo.
Request-2	Service-HTTP-3; (N = 2)	N = 4	Service-HTTP-3 tiene el valor N más bajo.
Request-3	Service-HTTP-3; (N = 4)	N = 6	Service-HTTP-3 tiene el valor N más bajo.
Request-4	Servicio-HTTP-1; (N = 6)	N = 8	Service-HTTP-1 y Service-HTTP-3 tienen los mismos valores N. El dispositivo utiliza el método round robin para distribuir las solicitudes.
Request-5	Service-HTTP-3; (N = 6)	N = 8	Service-HTTP-1 y Service-HTTP-3 tienen los mismos valores N.
Request-6	Service-HTTP-2; (N = 7)	N = 8	Service-HTTP-2 tiene el valor N más bajo.
Request-7	Service-HTTP-3; (N = 8)	N = 10	Service-HTTP-1, Service-HTTP-2 y Service-HTTP-3 tienen los mismos valores N. El dispositivo Citrix ADC utiliza el método round robin para distribuir las solicitudes.

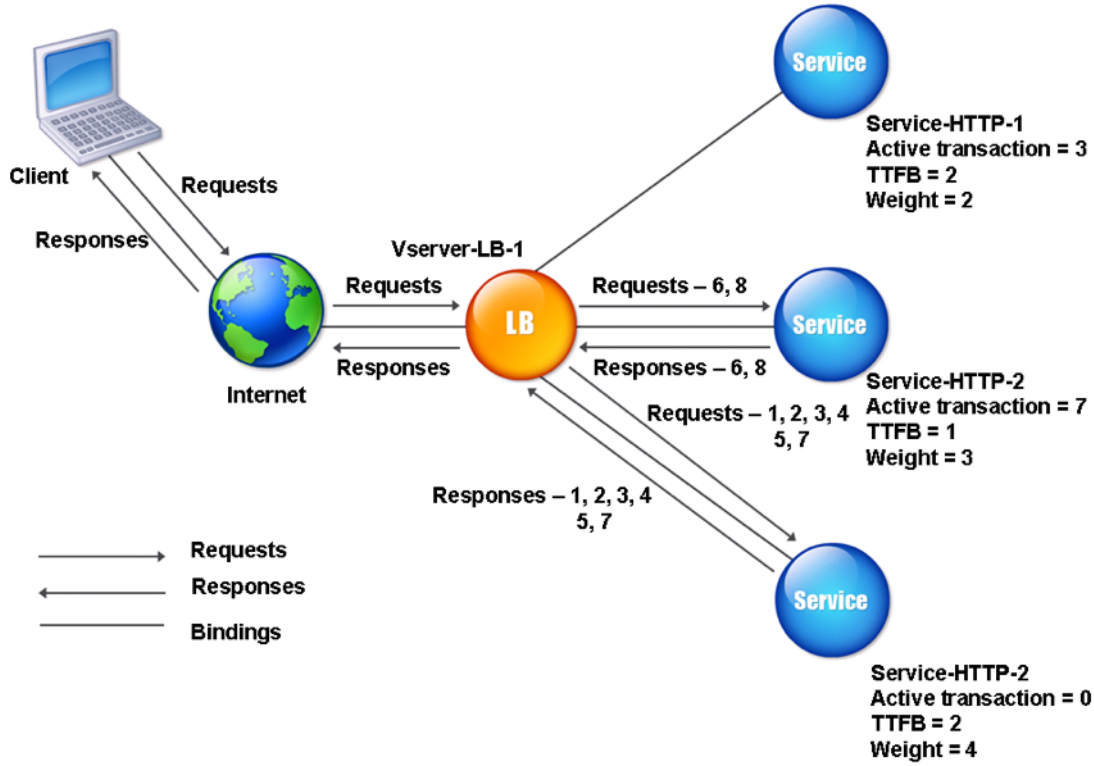
Solicitud recibida	Servicio seleccionado	Valor N Actual (Número de Transacciones Activas * TTFB)	Observaciones
Request-8	Servicio-HTTP-1; (N = 8)	N = 10	Service-HTTP-1 y Service-HTTP-2 tienen los mismos valores N; el dispositivo utiliza el método round robin para distribuir las solicitudes.

Service-HTTP-1 se vuelve a seleccionar para el equilibrio de carga cuando finaliza sus transacciones activas o cuando su valor N es menor que los otros servicios (Service-HTTP-2 y Service-HTTP-3).

Selección de servicios cuando se asignan pesos

En el siguiente diagrama se muestra cómo el dispositivo Citrix ADC utiliza el método de menor tiempo de respuesta cuando se asignan pesos.

Ilustración 2. Cómo funciona el método de equilibrio de carga de tiempo de respuesta mínimo cuando se asignan pesos



El servidor virtual selecciona un servicio mediante el valor (Nw) en la siguiente expresión:

Nw = (N) ⋆ (10000/peso), donde N = (número de transacciones activas ⋆ TTFB)

Supongamos que a Service-HTTP-1 se le asigna un peso de 2, Servicio-HTTP-2 se le asigna un peso de 3 y Servicio-HTTP-3 se le asigna un peso de 4.

El dispositivo Citrix ADC distribuye las solicitudes de la siguiente manera:

- Service-HTTP-3 recibe la primera solicitud, ya que no está manejando ninguna transacción activa.

  Si los servicios no gestionan ninguna transacción activa, el dispositivo las selecciona independientemente de las ponderaciones asignadas a ellos.
- Service-HTTP-3 recibe la segunda, tercera, cuarta y quinta solicitudes, porque este servicio tiene el valor Nw más bajo.
- Service-HTTP-2 recibe la sexta solicitud, porque este servicio tiene el valor Nw más bajo.
- Service-HTTP-3 recibe la séptima solicitud, porque este servicio tiene el valor Nw más bajo.
- Service-HTTP-2 recibe la octava solicitud, porque este servicio tiene el valor Nw más bajo.

Service-HTTP-1 tiene el peso más bajo y, por lo tanto, el valor Nw más alto, por lo que el servidor virtual no lo selecciona para el equilibrio de carga.

En la tabla siguiente se explica cómo se distribuyen las conexiones en la configuración de equilibrio de carga de tres servicios descrita anteriormente.

Solicitud recibida	Servicio seleccionado	Valor Nw actual = (N) * (10000/Peso)	Observaciones
Request-1	Servicio-HTTP-3; (Nw = 0)	Nw = 5000	Service-HTTP-3 tiene el valor Nw más bajo.
Request-2	Service-HTTP-3; (Nw = 5000	Nw = 10000	Service-HTTP-3 tiene el valor Nw más bajo.
Request-3	Servicio-HTTP-3; (Nw = 10000)	Nw = 15000	Service-HTTP-3 tiene el valor Nw más bajo.
Request-4	Servicio-HTTP-3; (Nw = 15000)	Nw = 20000	Service-HTTP-3 tiene el valor Nw más bajo.
Request-5	Servicio-HTTP-3; (Nw = 20000)	Nw = 25000	Service-HTTP-3 tiene el valor Nw más bajo.
Request-6	Servicio-HTTP-2; (Nw = 23333,34)	Nw = 26666,67	Service-http-2 tiene el valor Nw más bajo.
Request-7	Servicio-HTTP-3; (Nw = 25000)	Nw= 30000	Service-HTTP-3 tiene el valor Nw más bajo.
Request-8	Servicio-HTTP-2; (Nw = 26666,67)	Nw = 30000	Service-http-2 tiene el valor Nw más bajo.

Service-HTTP-1 se selecciona para el equilibrio de carga cuando completa sus transacciones activas o cuando su valor Nw es menor que otros servicios (Service-HTTP-2 y Service-HTTP-3).

Para configurar el método de equilibrio de carga de menor tiempo de respuesta mediante la CLI

En el símbolo del sistema, escriba;

```
set lb vserver <name> -lbMethod LEASTRESPONSETIME
<!--NeedCopy-->
```

Ejemplo:

```
set lb vserver Vserver-LB-1 -lbMethod LEASTRESPONSETIME
<!--NeedCopy-->
```


Para configurar el método de equilibrio de carga de menor tiempo de respuesta mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**y abra un servidor virtual.
2. En Configuración avanzada, seleccione **LEASRESPONSETIME**.

Para obtener más información sobre la configuración de monitores, consulte Configuración de monitores en una configuración de equilibrio de carga.

Método LRTM

August 20, 2021

Nota: LRTM significa Método de tiempo de respuesta mínimo mediante monitores (LRTM).

Cuando se configura un servidor virtual de equilibrio de carga para utilizar el método LRTM, utiliza la infraestructura de supervisión existente para obtener el tiempo de respuesta más rápido. A continuación, el servidor virtual de equilibrio de carga selecciona el servicio con el menor número de transacciones activas y el menor tiempo de respuesta. Antes de utilizar el método LRTM, debe vincular monitores específicos de la aplicación a cada servicio y habilitar el modo LRTM en estos monitores. A continuación, el dispositivo Citrix ADC toma decisiones de equilibrio de carga en función de los tiempos de respuesta que calcula a partir de sondeos de supervisión.

Puede utilizar el método LRTM para equilibrar la carga de servicios no HTTP y no HTTPS también. También puede utilizar este método cuando varios monitores están enlazados a un servicio. Cada monitor determina el tiempo de respuesta mediante el protocolo que mide para el servicio al que está enlazado. A continuación, el servidor virtual calcula un tiempo de respuesta medio para ese servicio promediando los resultados.

En la tabla siguiente se resume cómo se calculan los tiempos de respuesta para los distintos monitores.

Supervisar	Cálculo del tiempo de respuesta
PING	Diferencia horaria entre la solicitud ICMP ECHO y la respuesta ICMP ECHO.
TCP	Diferencia horaria entre la solicitud SYN y la respuesta SYN+ACK.
HTTP	Diferencia horaria entre la solicitud HTTP (después de establecer la conexión TCP) y la respuesta HTTP.

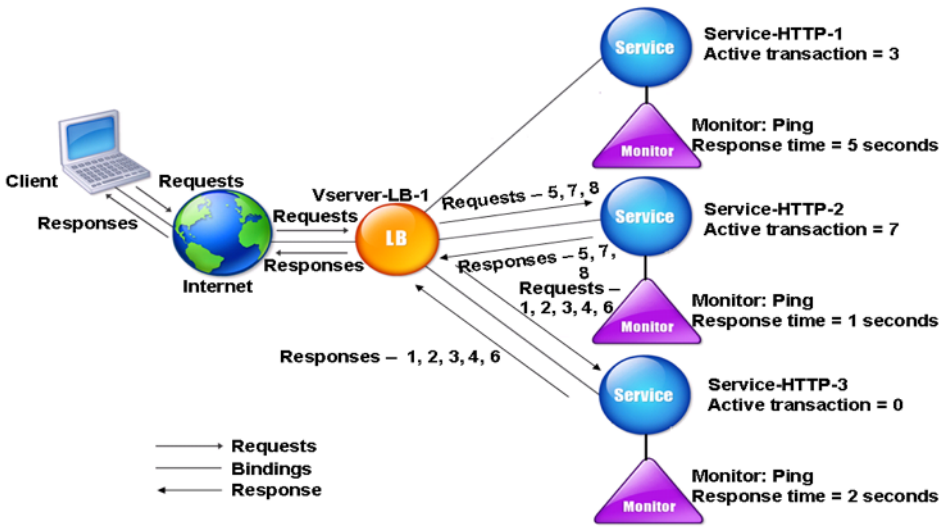
Supervisar	Cálculo del tiempo de respuesta
TCP-ECV	Diferencia horaria entre el momento en que se envía la cadena de envío de datos y la cadena de recepción de datos se devuelve. Se considera que un monitor TCP-ECV sin cadenas de envío y recepción tiene una configuración incorrecta.
HTTP-ECV	Diferencia horaria entre la solicitud HTTP y la respuesta HTTP.
UDP-ECV	Diferencia horaria entre la cadena de envío del UDP y la cadena de recepción. Se considera que un monitor UDP-ECV sin la cadena de recepción tiene una configuración incorrecta.
DNS	Diferencia horaria entre una consulta DNS y la respuesta DNS.
TCPS	Diferencia horaria entre una solicitud SYN y la finalización del protocolo de enlace SSL.
FTP	Diferencia horaria entre el envío del nombre de usuario y la finalización de la autenticación de usuario.
HTTPS (supervisa las solicitudes HTTPS)	La diferencia horaria es la misma que para el monitor HTTP.
HTTS-ECV (supervisa las solicitudes HTTPS)	La diferencia horaria es la misma que para el monitor HTTP-ECV
USER	Diferencia horaria entre la hora en que se envía una solicitud al despachador y la hora en que se recibe la respuesta del despachador.

En el ejemplo siguiente se muestra cómo el dispositivo Citrix ADC selecciona un servicio para el equilibrio de carga mediante el método LRTM. Considere los tres servicios siguientes:

- Service-HTTP-1 está manejando 3 transacciones activas y el tiempo de respuesta es de cinco segundos.
- Service-HTTP-2 está manejando 7 transacciones activas y el tiempo de respuesta es de un segundo.
- Service-HTTP-3 no está manejando ninguna transacción activa y el tiempo de respuesta es de dos segundos.

El siguiente diagrama ilustra el proceso que sigue el dispositivo Citrix ADC cuando reenvía solicitudes.

Ilustración 1. Cómo funciona el método LRTM



El servidor virtual selecciona un servicio mediante el valor (N) en la siguiente expresión:

N = (Número de transacciones activas* Tiempo de respuesta determinado por el monitor)

El servidor virtual entrega las solicitudes de la siguiente manera:

- Service-HTTP-3 recibe la primera solicitud, porque este servicio no está manejando ninguna transacción activa.
- Service-HTTP-3 recibe la segunda, tercera y cuarta solicitudes, porque este servicio tiene el valor N más bajo.
- Service-HTTP-2 recibe la quinta solicitud, porque este servicio tiene el valor N más bajo.
- Dado que tanto Service-HTTP-2 como Service-HTTP-3 tienen actualmente el mismo valor N, el dispositivo Citrix ADC cambia al método round robin. Por lo tanto, Service-HTTP-3 recibe la sexta solicitud.
- Service-HTTP-2 recibe las solicitudes séptima y octava, porque este servicio tiene el valor N más bajo.

Service-HTTP-1 no se considera para el equilibrio de carga, ya que está más cargado (tiene el valor N más alto) en comparación con los otros dos servicios. Sin embargo, si Service-HTTP-1 completa sus transacciones activas, el dispositivo Citrix ADC vuelve a considerar ese servicio para el equilibrio de carga.

En la siguiente tabla se resume cómo se calcula N para los servicios.

Solicitud recibida	Servicio seleccionado	Valor N Actual (Número de Transacciones Activas * TTFB)	Observaciones
Request-1	Service-HTTP-3;(N = 0)	N = 2	Service-HTTP-3 tiene el valor N más bajo.
Request-2	Service-HTTP-3; (N = 2)	N = 4	Service-HTTP-3 tiene el valor N más bajo.
Request-3	Service-HTTP-3; (N = 4)	N = 6	Service-HTTP-3 tiene el valor N más bajo.
Request-4	Service-HTTP-3; (N = 6)	N = 8	Service-HTTP-3 tiene el valor N más bajo.
Request-5	Service-HTTP-2; (N = 7)	N = 8	Service-HTTP-2 tiene el valor N más bajo.
Request-6	Service-HTTP-3; (N = 8)	N = 10	Service-HTTP-2 y Service-HTTP-3 tienen los mismos valores N. El dispositivo Citrix ADC cambia al método round robin y selecciona Service-HTTP-3
Request-7	Service-HTTP-2; (N = 8)	N = 9	Service-HTTP-2 tiene el valor N más bajo.
Request-8	Service-HTTP-2; (N = 9)	N = 10	Service-HTTP-2 tiene el valor N más bajo.

Service-HTTP-1 se vuelve a seleccionar para el equilibrio de carga cuando finaliza sus transacciones activas o cuando su valor N es menor que los otros servicios (Service-HTTP-2 y Service-HTTP-3).

Selección de servicios cuando se asignan pesos

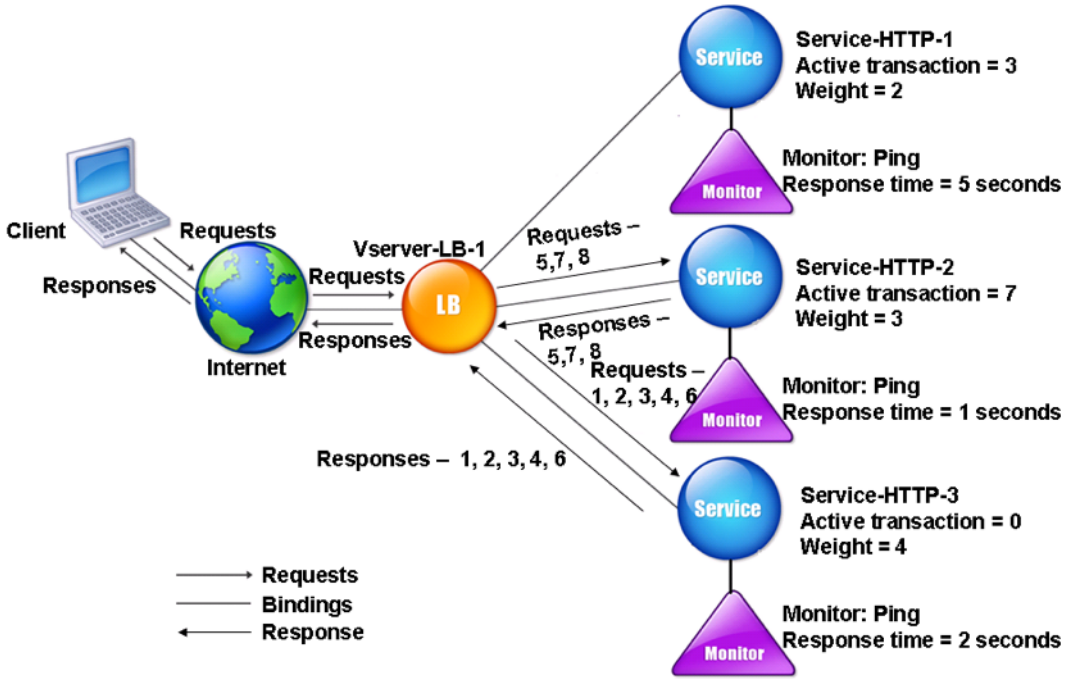
El dispositivo Citrix ADC también realiza el equilibrio de carga mediante el número de transacciones activas, el tiempo de respuesta y los pesos si se asignan diferentes pesos a los servicios. El dispositivo Citrix ADC selecciona el servicio mediante el valor (Nw) en la siguiente expresión:

Nw = (N) * (10000/peso)

Donde N = (Número de transacciones activas* Tiempo de respuesta determinado por el monitor)

El siguiente diagrama ilustra cómo el servidor virtual utiliza el método LRTM cuando se asignan pesos.

Ilustración 2. Cómo funciona el método de equilibrio de carga de tiempo de respuesta mínimo cuando se asignan pesos



En este ejemplo, supongamos que a Service-HTTP-1 se le asigna un peso de 2, Service-HTTP-2 se le asigna un peso de 3 y Service-HTTP-3 se le asigna un peso de 4.

El dispositivo Citrix ADC entrega las solicitudes de la siguiente manera:

- Service-HTTP-3 recibe la primera solicitud, ya que no está manejando ninguna transacción activa.
- Service-HTTP-3 recibe la segunda, tercera, cuarta y quinta solicitudes, porque este servicio tiene el valor Nw más bajo.
- Service-HTTP-2 recibe la sexta solicitud, porque este servicio tiene el valor Nw más bajo.
- Service-HTTP-3 recibe la séptima solicitud, porque este servicio tiene el valor Nw más bajo.
- Service-HTTP-2 recibe las octava solicitudes, porque este servicio tiene el valor Nw más bajo.

Service-HTTP-1 tiene el peso más bajo y el valor Nw más alto, por lo que el dispositivo Citrix ADC no lo selecciona para el equilibrio de carga.

La siguiente tabla resume cómo se calcula Nw para varios monitores.

Solicitud recibida	Servicio seleccionado	Valor Nw actual (N) * (10000/Peso)	Observaciones
Request-1	Servicio-HTTP-3; (Nw = 0)	Nw = 5000	Service-HTTP-3 tiene el valor Nw más bajo.
Request-2	Service-HTTP-3; (Nw = 5000	Nw = 10000	Service-HTTP-3 tiene el valor Nw más bajo.
Request-3	Servicio-HTTP-3; (Nw = 10000)	Nw = 15000	Service-HTTP-3 tiene el valor Nw más bajo.
Request-4	Servicio-HTTP-3; (Nw = 15000)	Nw = 20000	Service-HTTP-3 tiene el valor Nw más bajo.
Request-5	Servicio-HTTP-3; (Nw = 20000)	Nw = 25000	Service-HTTP-3 tiene el valor Nw más bajo.
Request-6	Servicio-HTTP-2; (Nw = 23333,34)	Nw = 26666,67	Service-http-2 tiene el valor Nw más bajo.
Request-7	Servicio-HTTP-3; (Nw = 25000)	Nw= 30000	Service-HTTP-3 tiene el valor Nw más bajo.
Request-8	Servicio-HTTP-2; (Nw = 26666,67)	Nw = 30000	Service-http-2 tiene el valor Nw más bajo.

Service-HTTP-1 se selecciona para el equilibrio de carga cuando completa sus transacciones activas o cuando su valor Nw es menor que otros servicios (Service-HTTP-2 y Service-HTTP-3).

Para configurar el método de equilibrio de carga LRTM mediante la CLI

En el símbolo del sistema, escriba;

```
set lb vserver <name> [-lbMethod <lbMethod>]
<!--NeedCopy-->
```

Ejemplo:

```
set lb vserver Vserver-LB-1 -lbMethod LRTM
<!--NeedCopy-->
```


Para configurar el método de equilibrio de carga LRTM mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**y abra un servidor virtual.
2. En Configuración avanzada, seleccione **LRTM**.

Para habilitar la opción LRTM en monitores mediante la CLI

En el símbolo del sistema, escriba;

```
set lb monitor <monitorName> <type> [-LRTM ( ENABLED | DISABLED )]
<!--NeedCopy-->
```

Ejemplo:

```
set lb monitor monitor-HTTP-1 HTTP -LRTM ENABLED
<!--NeedCopy-->
```

Para habilitar la opción LRTM en monitores mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Monitores** y abra un monitor.
2. En Parámetros avanzados, seleccione **LRTM (Tiempo de respuesta mínimo mediante supervisión)**.

Para obtener más información sobre la configuración de monitores, consulte Configuración de monitores en una configuración de equilibrio de carga.

Métodos de hash

August 20, 2021

Los métodos de equilibrio de carga basados en hash de cierta información de conexión o información de encabezado constituyen la mayoría de los métodos de equilibrio de carga del dispositivo Citrix ADC. Los hash son más cortos y más fáciles de usar que la información en la que se basan, al tiempo que conservan suficiente información para garantizar que no hay dos partes diferentes de información generan el mismo hash y, por lo tanto, se confunden entre sí.

Puede utilizar los métodos de equilibrio de carga de hash en un entorno donde una caché sirve una amplia gama de contenido de Internet o servidores de origen especificados. Las solicitudes de almacenamiento en caché reducen la latencia de solicitudes y respuestas y garantizan una mejor utilización de los recursos (CPU), lo que hace que el almacenamiento en caché sea popular en sitios web y servidores de aplicaciones muy utilizados. Dado que estos sitios también se benefician del equilibrio de carga, los métodos de equilibrio de carga hash son ampliamente útiles.

El dispositivo Citrix ADC proporciona los siguientes métodos de hash:

- Método hash de URL
- Método hash de dominio
- Método hash IP de destino
- Método hash IP de origen
- Método hash IP de destino IP de origen
- Método hash del puerto de origen IP de origen
- Método hash ID de llamada
- Método Token

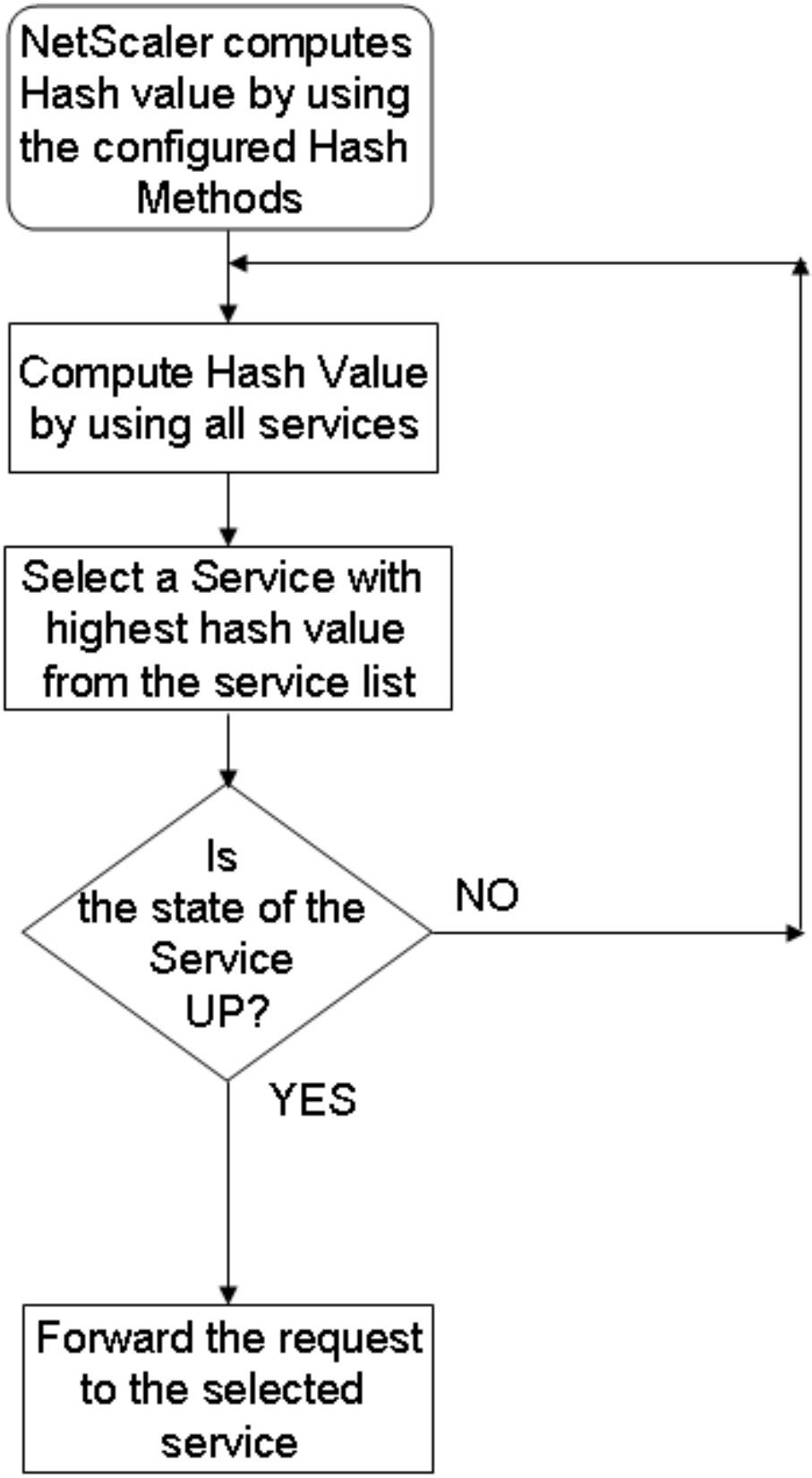
La mayoría de los algoritmos hash calculan dos valores hash:

- Un hash de la dirección IP y el puerto del servicio.
- Un hash de la dirección URL entrante, el nombre de dominio, la dirección IP de origen, la dirección IP de destino o las direcciones IP de origen y destino, dependiendo del método hash configurado.

A continuación, el dispositivo Citrix ADC genera un nuevo valor hash mediante el uso de ambos valores hash. Por último, reenvía la solicitud al servicio con el mayor valor hash. A medida que el dispositivo calcula un valor hash para cada solicitud y selecciona el servicio que procesa la solicitud, rellena una caché. Las solicitudes posteriores con el mismo valor hash se envían al mismo servicio. El siguiente diagrama de flujo ilustra este proceso.

> Nota
>
> A partir de Citrix ADC versión 13.0 compilación 79.x, se admiten los algoritmos hash consistentes de Ring asistido (JARH) de Prime Re-Shuffled Assisted Ring Hash (JARH) y Jump table. Los algoritmos de hash coherentes garantizan una interrupción mínima cuando se agregan o eliminan servicios de la configuración del equilibrio de carga, o durante un evento de fallo de servicio en la configuración del equilibrio de carga. Para obtener más información, consulte Algoritmos hash coherentes.

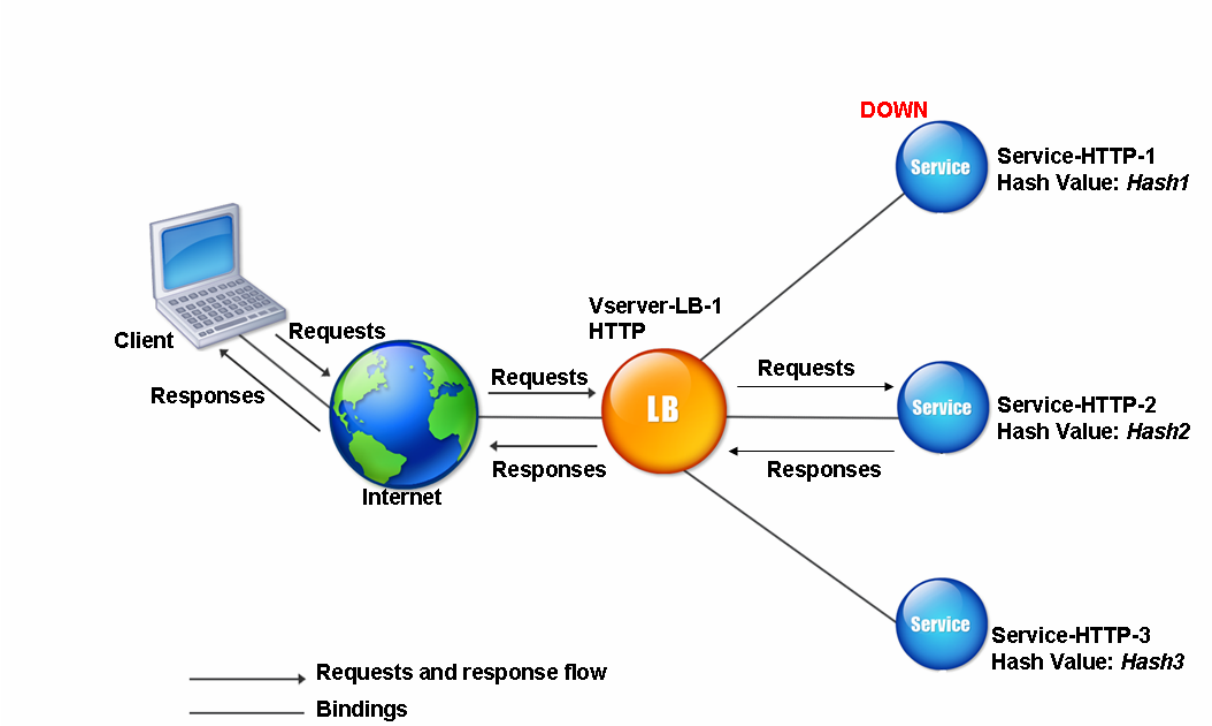
Ilustración 1. Cómo distribuyen las solicitudes los métodos de hash



Los métodos de hash se pueden aplicar a direcciones IPv4 e IPv6.

Considere un caso en el que tres servicios (Service-HTTP-1, Servicio-HTTP-2 y Servicio-HTTP-3) están enlazados a un servidor virtual, cualquier método hash está configurado y el valor hash es Hash1. Cuando los servicios configurados están UP, la solicitud se envía a Service-HTTP-1. Si Service-HTTP-1 está inactivado, el dispositivo Citrix ADC calcula el valor hash del último registro del número de servicios. A continuación, el dispositivo selecciona el servicio con el valor hash más alto, como Service-HTTP-2. El siguiente diagrama ilustra este proceso.

Ilustración 2. Modelo de entidad para métodos de hash



> Nota
>
> Si el dispositivo Citrix ADC no selecciona un servicio mediante un método de hash, se establece por defecto el método de menor conexión para seleccionar un servicio para la solicitud entrante. Ajuste los grupos de servidores eliminando servicios durante períodos de poco tráfico para permitir que las memorias caché se rellenen sin afectar al rendimiento de la configuración del equilibrio de carga.

Algoritmos hash coherentes

Los algoritmos hash consistentes se utilizan para lograr una persistencia sin estado. Los métodos LB basados en hash utilizan uno de los tres algoritmos hash consistentes siguientes:

- **Protocolo de redirección de arreglos de caché (CARP)**

El algoritmo CARP se utiliza en las solicitudes HTTP de equilibrio de carga en varios servidores de caché proxy. Este algoritmo está habilitado de forma predeterminada.

- **CARP asistida de rebarajado Prime (PRAC)**

  El dispositivo Citrix ADC utiliza el algoritmo PRAC patentado para proporcionar una distribución uniforme del tráfico.

- **Mesa de salto Hash de anillo asistido (JARH)**

  El dispositivo Citrix ADC utiliza el algoritmo JARH patentado para proporcionar coherencia y distribución uniforme del tráfico. Este algoritmo utiliza huellas hash. Un mayor número de huellas proporciona una mejor distribución del tráfico. Sin embargo, aumentar el número de huellas también aumenta el uso de la memoria.

Para elegir el algoritmo de hash coherente mediante CLI

```
set lb parameter [-lbHashAlgorithm [DEFAULT|JARH|PRAC] [-lbHashFingers
    <positive_integer>]
<!--NeedCopy-->
```

Ejemplo:

```
set lb parameter -lbHashAlgorithm JARH -lbHashFingers 10
<!--NeedCopy-->
```

ARGUMENTOS:

- **LBHashAlgorithm**: especifique el algoritmo de hash que se utilizará para los siguientes métodos de equilibrio de carga basados en hash:
  - Método hash de URL
  - Método hash de dominio
  - Método hash IP de destino
  - Método hash IP de origen
  - Método hash IP de destino IP de origen
  - Método hash del puerto de origen IP de origen
  - Método hash ID de llamada
  - Método Token

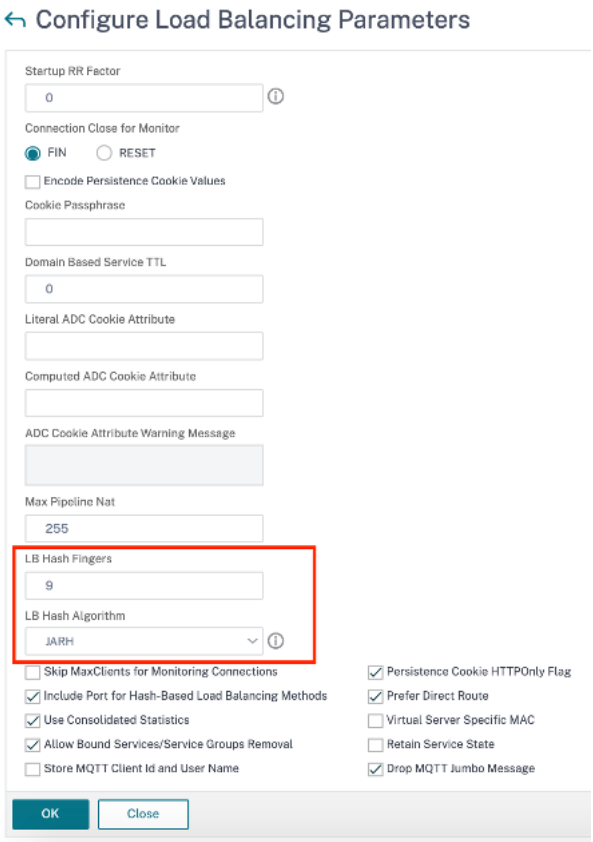
  Valores posibles: DEFAULT, PRAC, JARH Valor predeterminado: DEFAULT

- **lbHashFingers**: Especifique el número de huellas que se utilizarán en los algoritmos PRAC y JARH para métodos LB basados en hash. El aumento del número de huellas proporciona una mejor distribución del tráfico a expensas de la memoria adicional.

  Valor predeterminado: 256
  Valor mínimo: 1
  Valor máximo: 1024

Para elegir el algoritmo de hash coherente mediante GUI

1. Vaya a **Gestión de tráfico > Equilibrio de carga > Cambiar parámetros de Equilibrio de carga**.
2. En el panel **Configurar parámetros de equilibrio de carga**, introduzca los valores adecuados para los siguientes campos en función de sus requisitos:
   - Huellas hash LB
   - En el campo **Algoritmo hash LB**, elija el algoritmo hash coherente en el menú desplegable.



El método hash de URL

Cuando configura el dispositivo Citrix ADC para que utilice el método hash de URL para equilibrar la carga de los servicios, para seleccionar un servicio, el dispositivo genera un valor hash de la URL HTTP

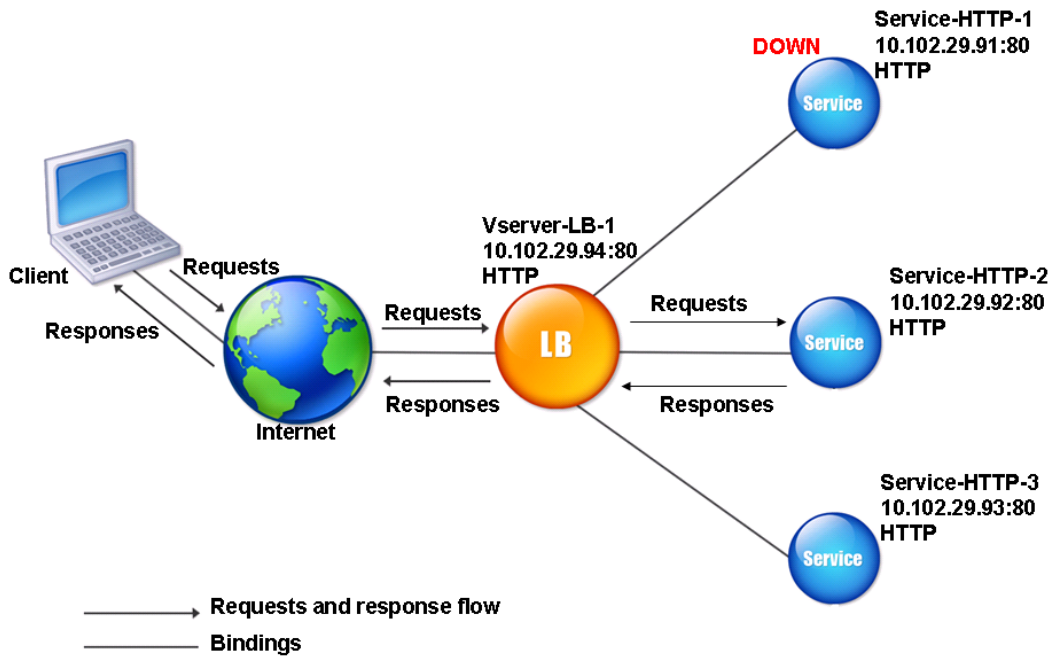
presente en la solicitud entrante. Si el servicio seleccionado por el valor hash es DOWN, el algoritmo tiene un método para seleccionar otro servicio de la lista de servicios activos. El dispositivo almacena en caché el valor hash de la dirección URL y, cuando recibe solicitudes posteriores que utilizan la misma dirección URL, las reenvía al mismo servicio. Si el dispositivo no puede analizar una solicitud entrante, utiliza el método round robin para el equilibrio de carga en lugar del método hash URL.

Para generar el valor hash, el dispositivo utiliza un algoritmo específico y considera una parte de la URL. De forma predeterminada, el dispositivo considera los primeros 80 bytes de la dirección URL. Si la URL es inferior a 80 bytes, se utiliza la URL completa. Puede especificar una longitud diferente. La longitud del hash puede ser de 1 byte a 4096 bytes. En general, si se utilizan URL largas donde solo unos pocos caracteres son diferentes, es recomendable que la longitud del hash sea lo más alta posible para intentar garantizar una distribución de carga más uniforme.

Considere un caso en el que tres servicios, Service-HTTP-1, Service-HTTP-2 y Service-HTTP-3, están enlazados a un servidor virtual, y el método de equilibrio de carga configurado en el servidor virtual es el método hash de URL. El servidor virtual recibe una solicitud y el valor hash de la URL es U1. El dispositivo selecciona Service-HTTP-1. Si Service-HTTP-1 está DOWN, el dispositivo selecciona Service-HTTP-2.

El siguiente diagrama ilustra este proceso.

Ilustración 3. Cómo funciona el hash de URL



Si tanto Service-HTTP-1 como Service-HTTP-2 están CAÍDOS, el dispositivo envía solicitudes con valor hash U1 a Service-HTTP-3.

Si Service-HTTP-1 y Service-HTTP-2 están inactivas, las solicitudes que generan la URL hash se envían a Service-HTTP-3. Si estos servicios están en UP, las solicitudes que generan la URL hash 1 se distribuyen de la siguiente manera:

- Si Service-HTTP-2 está activado, la solicitud se envía a Service-HTTP-2.
- Si el Service-HTTP-1 está activado, la solicitud se envía a Service-HTTP-1.
- Si Service-HTTP-1 y Service-HTTP-2 están activas al mismo tiempo, la solicitud se envía a Service-HTTP-1.

Para configurar el método hash de URL, consulte Configuración de un método de equilibrio de carga que no incluye una directiva. Seleccione el método de equilibrio de carga como URL Hash y establezca la longitud del hash en el número de bytes que se utilizarán para generar el valor hash.

El método hash de dominio

Un servidor virtual de equilibrio de carga configurado para utilizar el método hash de dominio utiliza el valor hash del nombre de dominio en la solicitud HTTP para seleccionar un servicio. El nombre de dominio se toma de la dirección URL entrante o del encabezado Host de la solicitud HTTP. Si el nombre de dominio aparece tanto en la dirección URL como en el encabezado Host, el dispositivo da preferencia a la dirección URL.

Si configura el hash de nombres de dominio y una solicitud HTTP entrante no contiene un nombre de dominio, el dispositivo Citrix ADC utilizará de forma predeterminada el método round robin para esa solicitud.

El cálculo de valor hash utiliza la longitud del nombre o el valor de longitud hash, lo que sea más pequeño. De forma predeterminada, el dispositivo Citrix ADC calcula el valor hash a partir de los primeros 80 bytes del nombre de dominio. Para especificar un número diferente de bytes en el nombre de dominio al calcular el valor hash, puede establecer el parámetro hashLength (Hash Length en la utilidad de configuración) en un valor de 1 a 4096 (bytes).

Para configurar el método hash de dominio, consulte Configuración de un método de equilibrio de carga que no incluye una directiva.

Método Hash IP de destino

Un servidor virtual de equilibrio de carga configurado para utilizar el método hash IP de destino utiliza el valor hash de la dirección IP de destino para seleccionar un servidor. Puede enmascarar la dirección IP de destino para especificar qué parte de ella se va a utilizar en el cálculo del valor hash, de modo que las solicitudes procedentes de redes diferentes pero destinadas a la misma subred se dirijan al mismo servidor. Este método admite servidores de destino basados en IPv4 e IPv6.

Este método de equilibrio de carga es apropiado para su uso con la función de redirección de caché.

Para configurar el método hash IP de destino para un servidor de destino IPv4, establezca el parámetro NetMask. Para configurar este método para un servidor de destino IPv6, utilice el parámetro V6NetMasklen. En la utilidad de configuración, los cuadros de texto para configurar estos parámetros aparecen al seleccionar el **método Hash IP de destino**.

Para configurar el método hash IP de destino, consulte Configuración de un método de equilibrio de carga que no incluye una directiva.

Método Hash IP de origen

Un servidor virtual de equilibrio de carga configurado para utilizar el método hash IP de origen utiliza el valor hash de la dirección IPv4 o IPv6 del cliente para seleccionar un servicio. Para dirigir todas las solicitudes de direcciones IP de origen que pertenecen a una red determinada a un servidor de destino específico, debe enmascarar la dirección IP de origen. Para direcciones IPv4, utilice el parámetro NetMask. Para direcciones IPv6, utilice el parámetro V6NetMaskLength.

Para configurar el método hash IP de origen, consulte Configuración de un método de equilibrio de carga que no incluye una directiva.

Método Hash IP de destino IP de origen

Un servidor virtual de equilibrio de carga configurado para utilizar el método hash IP de destino IP de origen utiliza el valor hash de las direcciones IP de origen y destino (IPv4 o IPv6) para seleccionar un servicio. El hash es simétrico. El valor hash es el mismo independientemente del orden de las IP de origen y de destino. Esto garantiza que todos los paquetes que fluyen desde un cliente concreto al mismo destino se dirijan al mismo servidor.

Para dirigir todas las solicitudes que pertenecen a una red determinada a un servidor de destino específico, debe enmascarar la dirección IP de origen. Para direcciones IPv4, utilice el parámetro NetMask. Para direcciones IPv6, utilice el parámetro V6NetMaskLength.

Para configurar el método hash IP de destino de IP de origen, consulte Configuración de un método de equilibrio de carga que no incluye una directiva.

Método Hash del puerto de origen IP de origen

Un servidor virtual de equilibrio de carga configurado para utilizar el método hash del puerto de origen IP de origen utiliza el valor hash de la IP de origen (IPv4 o IPv6) y el puerto de origen para seleccionar un servicio. Esto garantiza que todos los paquetes de una conexión determinada se dirijan al mismo servicio.

Este método se utiliza en la duplicación de conexiones y el equilibrio de carga del firewall. Para obtener más información sobre el reflejo de conexiones, consulte Conmutación por error de conexión.

Para dirigir todas las solicitudes que pertenecen a una red determinada a un servidor de destino específico, debe enmascarar la dirección IP de origen. Para direcciones IPv4, utilice el parámetro NetMask. Para direcciones IPv6, utilice el parámetro V6NetMaskLength.

Para configurar el método hash del puerto de origen IP de origen, consulte Configuración de un método de equilibrio de carga que no incluye una directiva.

El método Hash ID de llamada

Un servidor virtual de equilibrio de carga configurado para utilizar el método hash ID de llamada utiliza el valor hash del ID de llamada en el encabezado SIP para seleccionar un servicio. Por lo tanto, los paquetes para una sesión SIP determinada siempre se dirigen al mismo servidor proxy.

Este método es aplicable al equilibrio de carga SIP. Para obtener más información sobre el equilibrio de carga SIP, consulte Supervisión de los servicios SIP.

Para configurar el método hash de ID de llamada, consulte Configuración de un método de equilibrio de carga que no incluye una directiva.

Método de ancho de banda mínimo

August 20, 2021

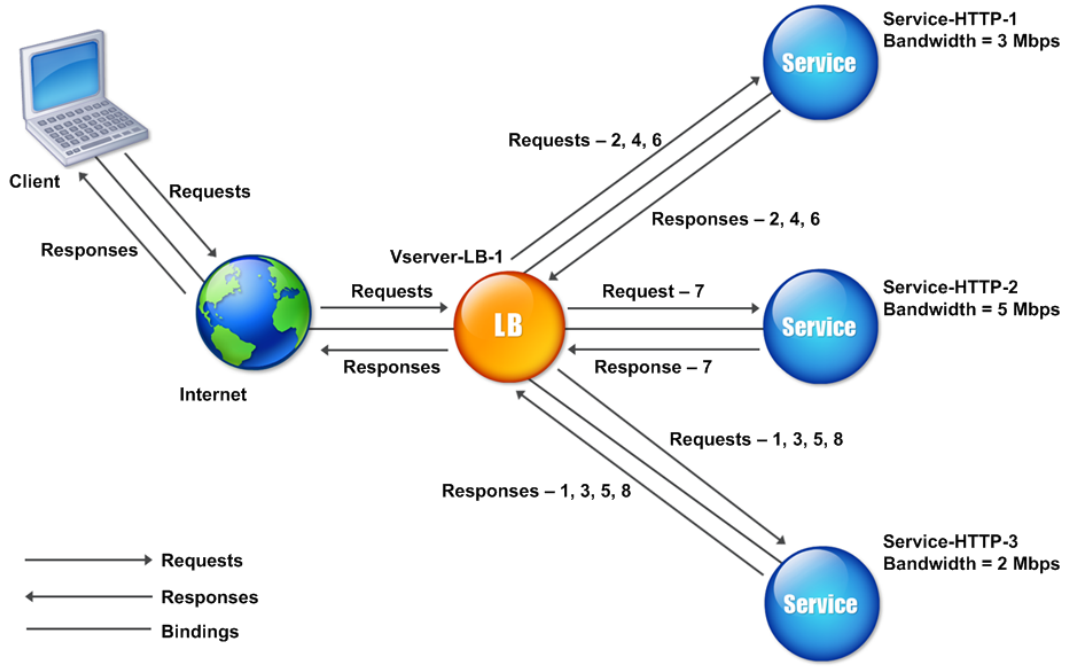
Un servidor virtual de equilibrio de carga configurado para utilizar el método de menor ancho de banda selecciona el servicio que actualmente atiende la menor cantidad de tráfico, medido en megabits por segundo (Mbps). En el ejemplo siguiente se muestra cómo el servidor virtual selecciona un servicio para el equilibrio de carga mediante el método de menor ancho de banda.

Considere tres servicios, Service-HTTP-1, Servicio-HTTP-2 y Servicio-HTTP-3.

- Service-HTTP-1 tiene un ancho de banda de 3 Mbps.
- Service-HTTP-2 tiene un ancho de banda de 5 Mbps.
- Service-HTTP-3 tiene un ancho de banda de 2 Mbps.

El siguiente diagrama ilustra cómo el servidor virtual utiliza el método de menor ancho de banda para reenviar solicitudes a los tres servicios.

Ilustración 1. Cómo funciona el método de equilibrio de carga de menor ancho de banda



El servidor virtual selecciona el servicio mediante el valor de ancho de banda (N), que es la suma del número de bytes transmitidos y recibidos durante los 14 segundos anteriores. Si cada solicitud requiere un ancho de banda de 1 Mbps, el dispositivo Citrix ADC entrega las solicitudes de la siguiente manera:

- Service-HTTP-3 recibe la primera solicitud, porque este servicio tiene el valor N más bajo.
- Dado que Service-HTTP-1 y Service-HTTP-3 ahora tienen el mismo valor N, el servidor virtual cambia al método round robin para estos servidores, alternando entre ellos. Service-HTTP-1 recibe la segunda solicitud, Servicio-HTTP-3 recibe la tercera solicitud, Servicio-HTTP-1 recibe la cuarta solicitud, Servicio-HTTP-3 recibe la quinta solicitud y Servicio-HTTP-1 recibe la sexta solicitud.
- Dado que Service-HTTP-1, Service-HTTP-2 y Service-HTTP-3 ahora tienen el mismo valor N, el servidor virtual incluye Service-HTTP-2 en la lista de round robin. Por lo tanto, Service-HTTP-2 recibe la séptima solicitud, Service-HTTP-3 recibe la octava solicitud, y así sucesivamente.

En la siguiente tabla se resume cómo se calcula N.

Solicitud recibida	Servicio seleccionado	Valor N actual	Observaciones

Solicitud recibida	Servicio seleccionado	Valor N actual	Observaciones
Request-1	Service-HTTP-3; (N = 2)	N = 3	Service-HTTP-3 tiene el valor N más bajo.
Request-2	Servicio-HTTP-1; (N = 3)	N = 4	Service-HTTP-1 y Service-HTTP-3 tienen los mismos valores N.
Request-3	Service-HTTP-3;(N = 3)	N = 4	Service-HTTP-1 y Service-HTTP-3 tienen los mismos valores N.
Request-4	Servicio-HTTP-1; (N = 4)	N = 5	-
Request-5	Service-HTTP-3; (N = 4)	N = 5	-
Request-6	Servicio-HTTP-1; (N = 5)	N = 6	Service-HTTP-1, Service-HTTP-2 y Service-HTTP-3 tienen los mismos valores N.
Request-7	Service-HTTP-2; (N = 5)	N = 6	Service-HTTP-1, Service-HTTP-2 y Service-HTTP-3 tienen los mismos valores N.
Request-8	Service-HTTP-3; (N = 5)	N = 6	-

Nota: Si habilita la opción RTSP NAT en el servidor virtual, el dispositivo Citrix ADC utiliza el número de bytes de datos y control intercambiados para determinar el uso del ancho de banda para los servicios RTSP. Para obtener más información sobre la opción NAT de RTSP, consulte Administración de conexiones RTSP.

El dispositivo Citrix ADC también realiza el equilibrio de carga mediante el ancho de banda y los pesos si se asignan diferentes pesos a los servicios. Se selecciona un servicio mediante el valor (Nw) en la

siguiente expresión:

Nw = (N) * (10000/peso)

Como en el ejemplo anterior, supongamos que a Service-HTTP-1 se le asigna un peso de 2, Service-HTTP-2 se le asigna un peso de 3 y Service-HTTP-3 se le asigna un peso de 4. El dispositivo Citrix ADC entrega las solicitudes de la siguiente manera:

- Service-HTTP-3 recibe la primera segunda, tercera, cuarta y quinta solicitudes, porque este servicio tiene el valor Nw más bajo.
- Service-HTTP-1 recibe la sexta solicitud, porque este servicio tiene el valor Nw más bajo.
- Service-HTTP-3 recibe la séptima solicitud, porque este servicio tiene el valor Nw más bajo.
- Service-HTTP-2 recibe la octava solicitud, porque este servicio tiene el valor Nw más bajo.

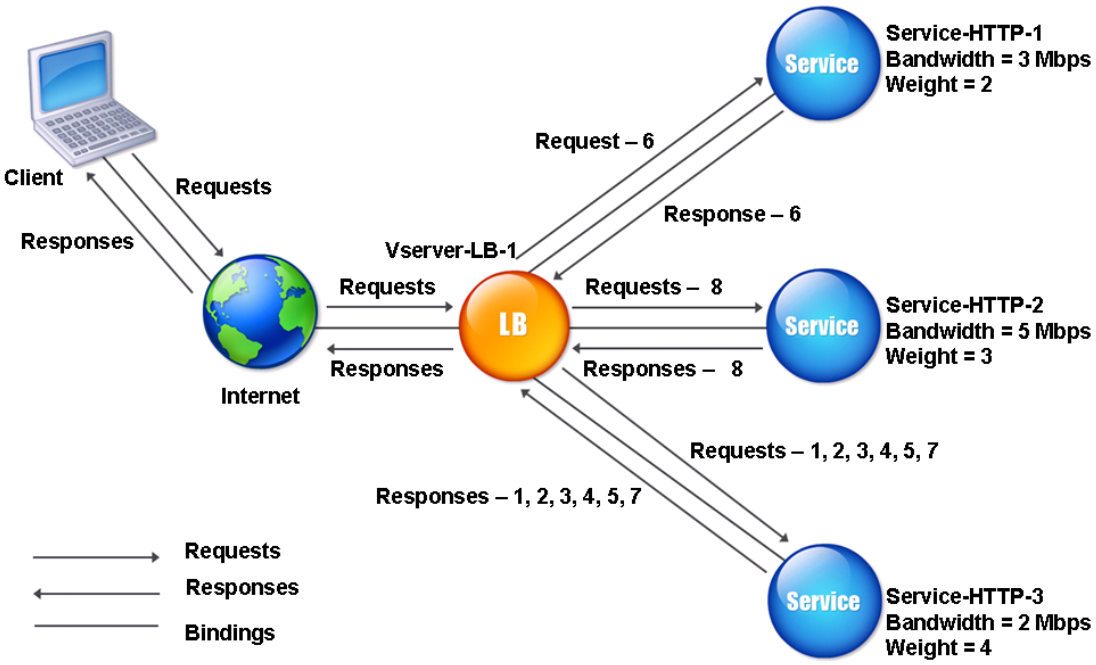
La siguiente tabla resume cómo se calcula Nw.

Solicitud recibida	Servicio seleccionado	Valor Nw actual (Número de transacciones activas) * (10000/Peso)	Observaciones
Request-1	Servicio-HTTP-3; (Nw = 5000)	Nw = 5000	Service-HTTP-3 tiene el valor Nw más bajo.
Request-2	Servicio-HTTP-3; (Nw = 5000)	Nw = 7500	-
Request-3	Servicio-HTTP-3; (Nw = 7500)	Nw = 10000	-
Request-4	Servicio-HTTP-3; (Nw = 10000)	Nw = 12500	-
Request-5	Servicio-HTTP-3; (Nw = 12500)	Nw = 15000	-
Request-6	Servicio-HTTP-1; (Nw = 15000)	Nw = 20000	Service-HTTP-1 y Service-HTTP-3 tienen el mismo valor Nw.
Request-7	Servicio-HTTP-3; (Nw = 15000)	Nw = 17500	Service-HTTP-1 y Service-HTTP-3 tienen el mismo valor Nw.

Solicitud recibida	Servicio seleccionado	Valor Nw actual (Número de transacciones activas) * (10000/Peso)	Observaciones
Request-8	Servicio-HTTP-2; (Nw = 16666,67)	Nw = 20000	Service-http-2 tiene el valor Nw más bajo.

El siguiente diagrama ilustra cómo el servidor virtual utiliza el método de menor ancho de banda cuando se asignan pesos a los servicios.

Ilustración 2. Cómo funciona el método de equilibrio de carga de menor ancho de banda cuando se asignan pesos



Para configurar el método de menor ancho de banda, consulte Configuración de un método de equilibrio de carga que no incluye una directiva.

Método de paquetes mínimos

August 20, 2021

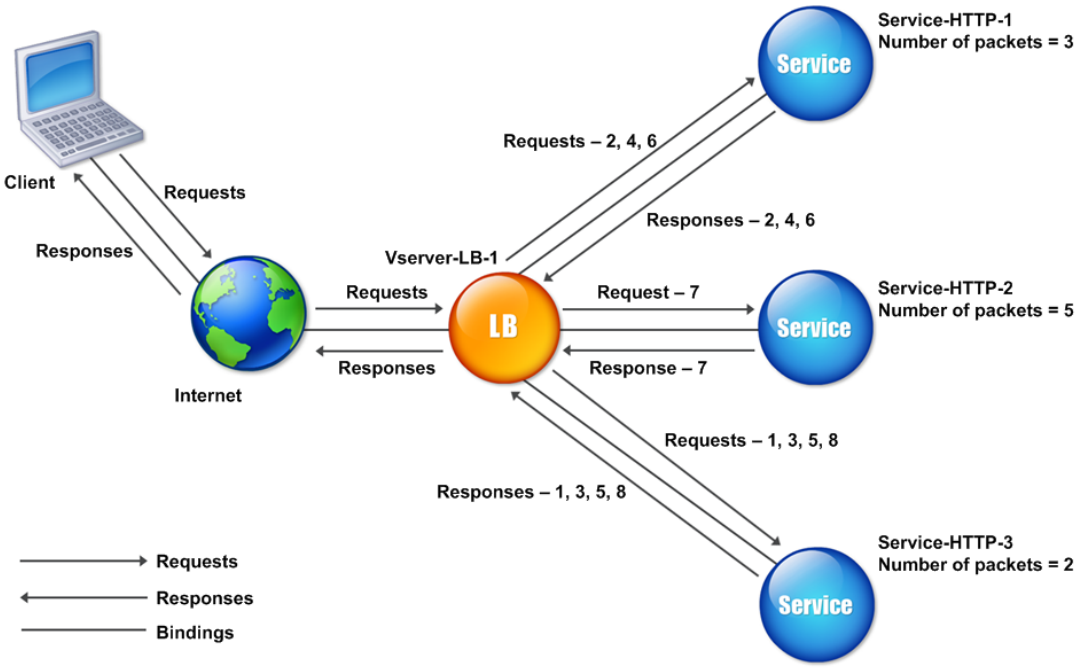
Un servidor virtual de equilibrio de carga configurado para utilizar el método de menos paquetes selecciona el servicio que ha recibido el menor número de paquetes en los últimos 14 segundos.

Por ejemplo, considere tres servicios, Service-HTTP-1, Service-HTTP-2 y Service-HTTP-3.

- Service-HTTP-1 ha manejado tres paquetes en los últimos 14 segundos.
- Service-HTTP-2 ha manejado cinco paquetes en los últimos 14 segundos.
- Service-HTTP-3 ha manejado dos paquetes en los últimos 14 segundos.

En el siguiente diagrama se muestra cómo el dispositivo Citrix ADC utiliza el método de menos paquetes para elegir un servicio para cada solicitud que recibe.

Ilustración 1. Cómo funciona el método de equilibrio de carga de paquetes mínimos



El dispositivo Citrix ADC selecciona un servicio mediante el número de paquetes (N) transmitidos y recibidos por cada servicio en los últimos 14 segundos. Mediante este método, entrega las solicitudes de la siguiente manera:

- Service-HTTP-3 recibe la primera solicitud, porque este servicio tiene el valor N más bajo.

- Dado que Service-HTTP-1 y Service-HTTP-3 ahora tienen el mismo valor N, el servidor virtual cambia al método round robin. Service-HTTP-1 recibe la segunda solicitud, Service-HTTP-3 recibe la tercera solicitud, Servicio-HTTP-1 recibe la cuarta solicitud, Servicio-HTTP-3 recibe la quinta solicitud y Servicio-HTTP-1 recibe la sexta solicitud.
- Dado que Service-HTTP-1, Service-HTTP-2 y Service-HTTP-3 ahora tienen el mismo valor N, el servidor virtual cambia también al método round robin para Service-HTTP-2, incluido en la lista de round robin. Por lo tanto, Service-HTTP-2 recibe la séptima solicitud, Service-HTTP-3 recibe la octava solicitud, y así sucesivamente.

En la siguiente tabla se resume cómo se calcula N.

Solicitud recibida	Servicio seleccionado	Valor N actual	Observaciones
Request-1	Service-HTTP-3; (N = 2)	N = 3	Service-HTTP-3 tiene el valor N más bajo.
Request-2	Servicio-HTTP-1; (N = 3)	N = 4	Service-HTTP-1 y Service-HTTP-3 tienen los mismos valores N.
Request-3	Service-HTTP-3; (N = 3)	N = 4	Service-HTTP-1 y Service-HTTP-3 tienen los mismos valores N.
Request-4	Servicio-HTTP-1; (N = 4)	N = 5	-
Request-5	Service-HTTP-3; (N = 4)	N = 5	-
Request-6	Servicio-HTTP-1; (N = 5)	N = 6	Service-HTTP-1, Service-HTTP-2 y Service-HTTP-3 tienen los mismos valores N.
Request-7	Service-HTTP-2; (N = 5)	N = 6	Service-HTTP-1, Service-HTTP-2 y Service-HTTP-3 tienen los mismos valores N.
Request-8	Service-HTTP-3; (N = 5)	N = 6	-

Nota: Si habilita la opción NAT RTSP en el servidor virtual, el dispositivo utiliza el número de paquetes de datos y control para calcular el número de paquetes para los servicios RTSP. Para obtener más información sobre la opción NAT de RTSP, consulte Administración de conexiones RTSP.

El dispositivo Citrix ADC también realiza el equilibrio de carga mediante el uso del número de paquetes y pesos cuando se asigna un peso diferente a cada servicio. Se selecciona un servicio mediante el valor (Nw) en la siguiente expresión:

Nw = (N) * (10000/peso)

Como en el ejemplo anterior, supongamos que a Service-HTTP-1 se le asigna un peso de 2, Service-HTTP-2 se le asigna un peso de 3 y Service-HTTP-3 se le asigna un peso de 4. El dispositivo Citrix ADC entrega las solicitudes de la siguiente manera:

- Service-HTTP-3 recibe la primera segunda, tercera, cuarta y quinta solicitudes, porque este servicio tiene el valor Nw más bajo.
- Service-HTTP-1 recibe la sexta solicitud, porque este servicio tiene el valor Nw más bajo.
- Service-HTTP-3 recibe la séptima solicitud, porque este servicio tiene el valor Nw más bajo.
- Service-HTTP-2 recibe la octava solicitud, porque este servicio tiene el valor Nw más bajo.

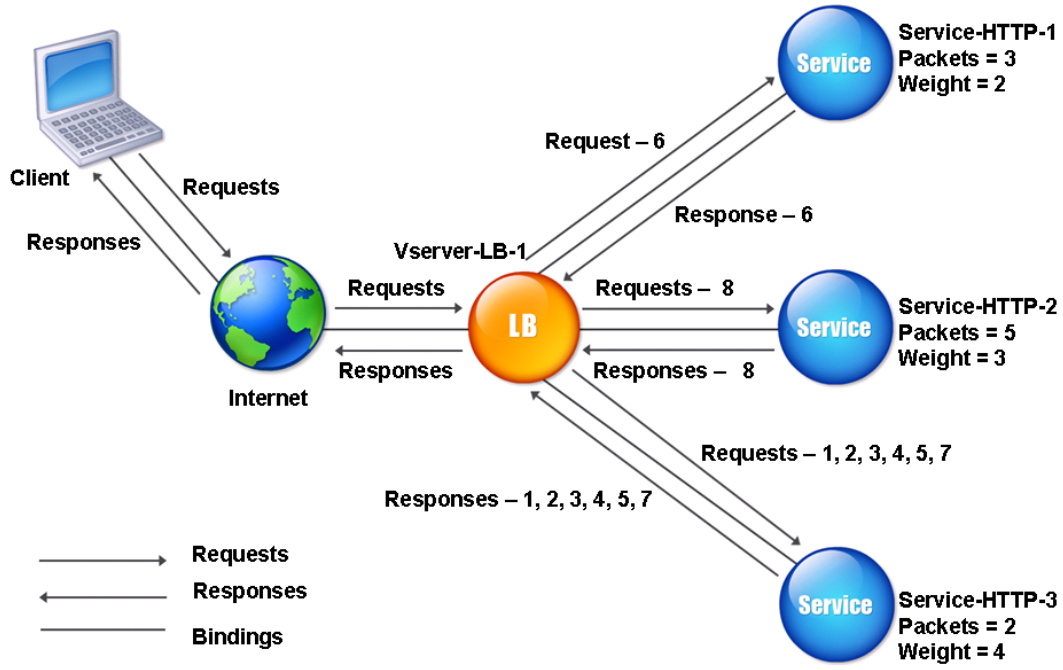
La siguiente tabla resume cómo se calcula Nw.

Solicitud recibida	Servicio seleccionado	Valor Nw actual (número de transacciones activas) * (10000/peso)	Observaciones
Request-1	Servicio-HTTP-3; (Nw = 5000)	Nw = 5000	Service-HTTP-3 tiene el valor Nw más bajo.
Request-2	Servicio-HTTP-3; (Nw = 5000)	Nw = 7500	-
Request-3	Servicio-HTTP-3; (Nw = 7500)	Nw = 10000	-
Request-4	Servicio-HTTP-3; (Nw = 10000)	Nw = 12500	-
Request-5	Servicio-HTTP-3; (Nw = 12500)	Nw = 15000	-
Request-6	Servicio-HTTP-1; (Nw = 15000)	Nw = 20000	Service-HTTP-1 y Service-HTTP-3 tienen el mismo valor Nw.

Solicitud recibida	Servicio seleccionado	Valor Nw actual (número de transacciones activas) * (10000/peso)	Observaciones
Request-7	Servicio-HTTP-3; (Nw = 15000)	Nw = 17500	Service-HTTP-1 y Service-HTTP-3 tienen el mismo valor Nw.
Request-8	Servicio-HTTP-2; (Nw = 16666,67)	Nw = 20000	Service-http-2 tiene el valor Nw más bajo.

El siguiente diagrama ilustra cómo el servidor virtual utiliza el método de menos paquetes cuando se asignan pesos.

Ilustración 2. Cómo funciona el método de menos paquetes cuando se asignan pesos



Para configurar el método de menor cantidad de paquetes, consulte Configuración de un método de equilibrio de carga que no incluye una directiva.

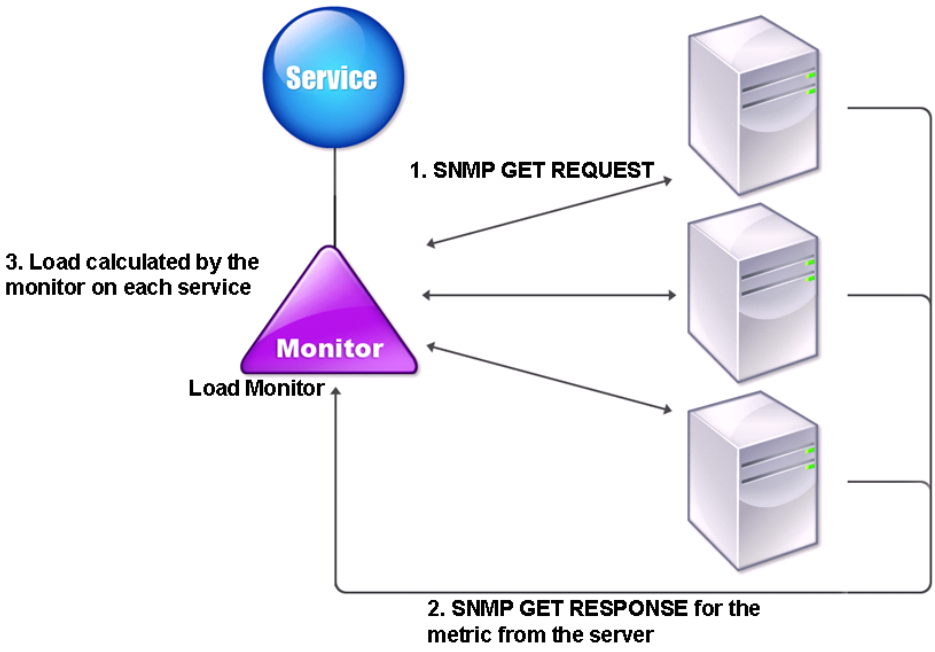
Método de carga personalizado

October 5, 2021

El equilibrio de carga personalizado se realiza en parámetros del servidor como el uso de CPU, la memoria y el tiempo de respuesta. Cuando se utiliza el método de carga personalizado, el dispositivo Citrix ADC suele seleccionar un servicio que no gestiona transacciones activas. Si todos los servicios de la configuración de equilibrio de carga gestionan transacciones activas, el dispositivo selecciona el servicio con la menor carga. Un tipo especial de monitor, conocido como monitor de carga, calcula la carga en cada servicio de la red. Los monitores de carga no marcan el estado de un servicio, pero sí quitan los servicios de la decisión de equilibrio de carga cuando esos servicios no están UP.

Para obtener más información sobre los monitores de carga, consulte Descripción de los monitores de carga. El siguiente diagrama ilustra cómo funciona un monitor de carga.

Ilustración 1. Funcionamiento de los monitores de carga



El monitor de carga utiliza sondeos SNMP para calcular la carga de cada servicio mediante el envío de una solicitud SNMP GET al servicio. Esta solicitud contiene uno o más ID de objeto (OID). El servicio responde con una respuesta SNMP GET, con métricas correspondientes a los OID SNMP. El monitor de carga utiliza las métricas de respuesta para calcular la carga del servicio.

El monitor de carga calcula la carga en un servicio mediante los siguientes parámetros:

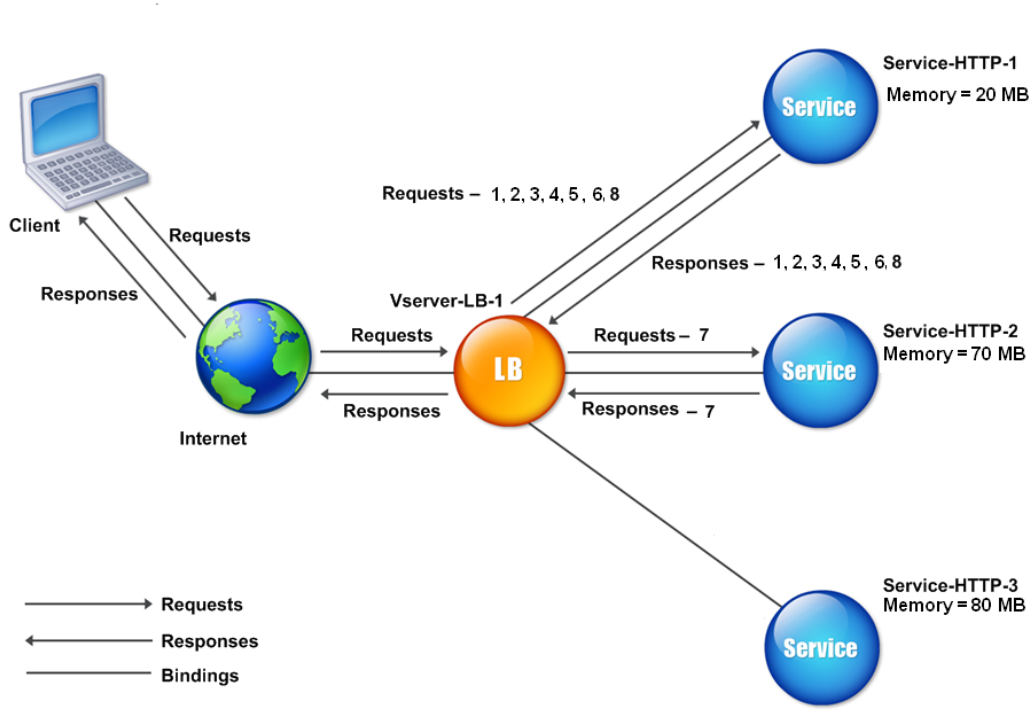
- Valores de métricas recuperados mediante sondeos SNMP que existen como tablas en el dispositivo Citrix ADC.
- Valor de umbral establecido para cada métrica.
- Peso asignado a cada métrica.

Por ejemplo, considere tres servicios, Service-HTTP-1, Service-HTTP-2 y Service-HTTP-3.

- Service-HTTP-1 utiliza 20 MB de memoria.
- Servicio-HTTP-2 está usando 70 MB de memoria.
- Service-HTTP-3 está usando 80 MB de memoria.

Los servidores con equilibrio de carga pueden exportar métricas como CPU y uso de memoria a los servicios, lo que a su vez puede proporcionarlas al monitor de carga. El monitor de carga envía una solicitud SNMP GET que contiene los OID 1.3.6.1.4.1.5951.4.1.1.41.1.5, 1.3.6.1.4.1.5951.4.1.1.41.1.4 y 1.3.6.1.4.1.5951.4.1.1.41.1.3 a los servicios. No se admiten los OID SNMP de tipo STRING, porque no se puede calcular la carga mediante un OID STRING. Las cargas se pueden calcular mediante otros tipos de datos, como INT y gauge32. Los tres servicios responden a la solicitud. El dispositivo Citrix ADC compara las métricas exportadas y, a continuación, selecciona Service-HTTP-1 porque tiene más memoria disponible. El siguiente diagrama ilustra este proceso.

Ilustración 2. Cómo funciona el método de carga personalizada



Si cada solicitud utiliza 10 MB de memoria, el dispositivo Citrix ADC entrega las solicitudes de la siguiente manera:

- Service-HTTP-1 recibe la primera, segunda, tercera, cuarta y quinta solicitudes, porque este servicio tiene el valor N más bajo.
- Service-HTTP-1 y Service-HTTP-2 ahora tienen la misma carga, por lo que el servidor virtual vuelve al método round robin para estos servidores. Por lo tanto, Service-HTTP-2 recibe la sexta solicitud y Service-HTTP-1 recibe la séptima solicitud.
- Dado que Service-HTTP-1, Service-HTTP-2 y Service-HTTP-3 ahora tienen la misma carga, el servidor virtual vuelve al método round robin para Service-HTTP-3 también. Por lo tanto, Service-HTTP-3 recibe la octava solicitud.

En la siguiente tabla se resume cómo se calcula N.

Solicitud recibida	Servicio seleccionado	Valor N Actual (Número de Transacciones Activas)	Observaciones
Request-1	Servicio-HTTP-1; (N = 20)	N = 30	Service-HTTP-3 tiene el valor N más bajo.

Solicitud recibida	Servicio seleccionado	Valor N Actual (Número de Transacciones Activas)	Observaciones
Request-2	Servicio-HTTP-1; (N = 30)	N = 40	-
Request-3	Servicio-HTTP-1; (N = 40)	N = 50	-
Request-4	Servicio-HTTP-1; (N = 50)	N = 60	-
Request-5	Servicio-HTTP-1; (N = 60)	N = 70	-
Request-6	Servicio-HTTP-1; (N = 70)	N = 80	Service-HTTP-2 y Service-HTTP-3 tienen los mismos valores N.
Request-7	Service-HTTP-2; (N = 70)	N = 80	Service-HTTP-3 tiene los mismos valores N.
Request-8	Servicio-HTTP-1; (N = 80)	N = 90	Service-HTTP-1, Service-HTTP-2 y Service-HTTP-3 tienen los mismos valores N.

Si se asignan diferentes pesos a los servicios, el algoritmo de carga personalizado considera tanto la carga de cada servicio como el peso asignado a cada servicio. Se selecciona un servicio mediante el valor (Nw) en la siguiente expresión:

Nw = (N) * (10000/peso)

Como en el ejemplo anterior, supongamos que a Service-HTTP-1 se le asigna un peso de 4, Service-HTTP-2 se le asigna un peso de 3 y Service-HTTP-3 se le asigna un peso de 2. Si cada solicitud utiliza 10 MB de memoria, el dispositivo Citrix ADC entrega las solicitudes de la siguiente manera:

- Service-HTTP-1 recibe la primera, segunda, tercera, cuarta, quinta, sexta, séptima y octava solicitudes, porque este servicio tiene el valor Nw más bajo.
- Service-HTTP-2 recibe la novena solicitud, porque este servicio tiene el valor Nw más bajo.

Service-HTTP-3 tiene el valor Nw más alto y, por lo tanto, no se considera para el equilibrio de carga.

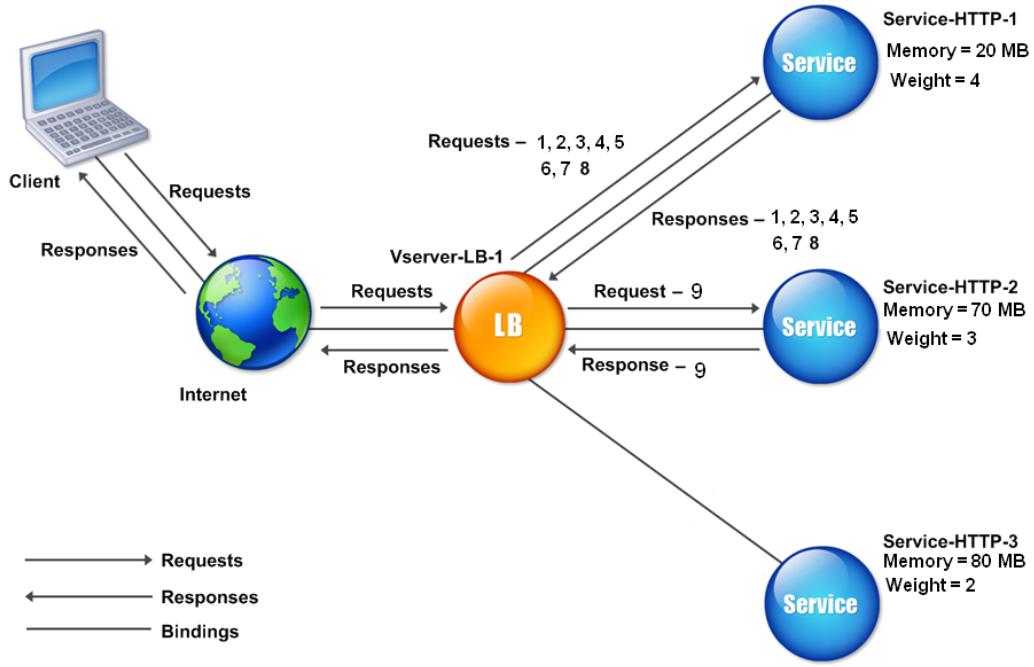
La siguiente tabla resume cómo se calcula Nw.

Solicitud recibida	Servicio seleccionado	Valor Nw actual (Número de transacciones activas) * (10000/Peso)	Observaciones
Request-1	Service-HTTP-1; (Nw = 50000)	Nw = 75000	Service-HTTP-1 tiene el valor Nw más bajo.
Request-2	Servicio-HTTP-1; (Nw = 5000)	Nw = 100000	-
Request-3	Servicio-HTTP-1; (Nw = 15000)	Nw = 125000	-
Request-4	Servicio-HTTP-1; (Nw = 20000)	Nw = 150000	-
Request-5	Servicio-HTTP-1; (Nw = 23333,34)	Nw = 175000	-
Request-6	Servicio-HTTP-1; (Nw = 25000)	Nw = 200000	-
Request-7	Servicio-HTTP-1; (Nw = 23333,34)	Nw = 225000	-
Request-8	Servicio-HTTP-1; (Nw = 25000)	Nw = 250000	-
Request-9	Servicio-HTTP-2; (Nw = 233333.34)	Nw = 266666.67	Servicio-HTTP-2 tiene el valor Nw más bajo.

Service-HTTP-1 se selecciona para el equilibrio de carga cuando finaliza sus transacciones activas o cuando el valor Nw de otros servicios (Service-HTTP-2 y Service-HTTP-3) es igual a 400.000.

En el siguiente diagrama se muestra cómo el dispositivo Citrix ADC utiliza el método de carga personalizado cuando se asignan pesos.

Ilustración 3. Cómo funciona el método de carga personalizada cuando se asignan pesos



Para configurar el método de carga personalizado, consulte Configuración de un método de equilibrio de carga que no incluye una directiva.

Método de proximidad estático

January 19, 2021

Cuando un servidor virtual está configurado para utilizar el método de proximidad estática, selecciona el servicio que mejor se ajusta a los criterios de proximidad.

Para que funcione el método de proximidad estática, debe configurar el dispositivo Citrix ADC para que utilice una base de datos de proximidad estática existente rellenada a través de un archivo de ubicación o agregar entradas personalizadas a la base de datos de proximidad estática. Después de agregar entradas personalizadas, puede establecer sus calificadores de ubicación. Después de configurar la base de datos, está listo para especificar la proximidad estática como método de equilibrio de carga.

Para obtener más información, consulte los temas siguientes.

- Adición de un archivo de ubicación para crear una base de datos de proximidad estática

- Adición de Entradas Personalizadas a una Base de Datos de Proximidad Estática
- Configuración de los calificadores de ubicación
- Especificación del método de proximidad estática

Especificación del método de proximidad

Cuando haya configurado la base de datos de proximidad estática, estará listo para especificar la proximidad estática como método GLSB.

Para especificar la proximidad estática mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para configurar la proximidad estática y verificar la configuración:

```
set lb vserver <name> -lbMethod STATICPROXIMITY

show lb vserver <name>
<!--NeedCopy-->
```

Ejemplo:

```
set lb vserver Vserver-LB-1 -lbMethod STATICPROXIMITY

show lb vserver
<!--NeedCopy-->
```

Para especificar la proximidad estática mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales** y seleccione el servidor virtual.
2. Haga clic en **Modificar** y expanda la sección **Método**.
3. En la lista **Método de equilibrio de carga**, seleccione **STATICProximity**.

Método Token

August 20, 2021

Un servidor virtual de equilibrio de carga configurado para utilizar el método token basa su selección de un servicio en el valor de un segmento de datos extraído de la solicitud del cliente. El segmento de datos se denomina token. Configurar la ubicación y el tamaño del token. Para las solicitudes posteriores con el mismo token, el servidor virtual elige el mismo servicio que manejó la solicitud inicial.

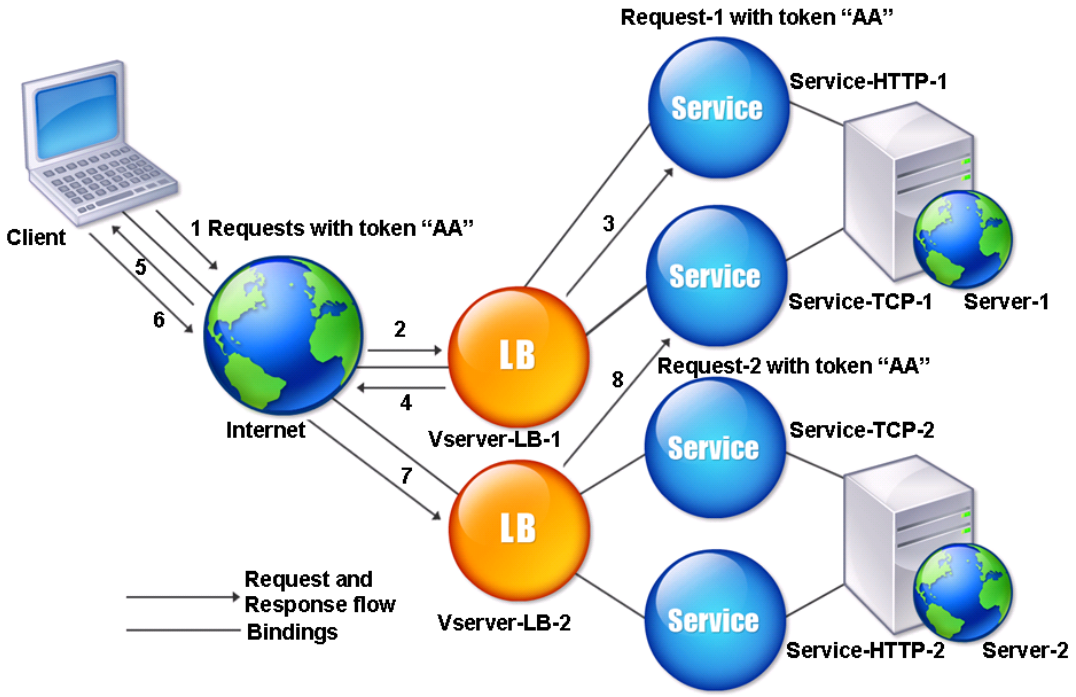
Este método es consciente del contenido. Funciona de forma diferente para conexiones TCP, HTTP y HTTPS. Para los servicios HTTP o HTTPS, el token se encuentra en los encabezados HTTP, la URL o el BODY. Para localizar el token, especifique o cree una expresión clásica o avanzada. Para obtener más información sobre expresiones clásicas o avanzadas, consulte Configuración y referencia de directivas.

Para los servicios HTTP, el servidor virtual busca el token configurado en los primeros 24 kilobytes (KB) de la carga útil TCP. Para servicios no HTTP (TCP, SSL y SSL_TCP), el servidor virtual busca el token configurado en los primeros 16 paquetes si el tamaño total de los 16 paquetes es inferior a 24 KB. Pero si el tamaño total de los 16 paquetes es mayor que 24 KB, el dispositivo busca el token en los primeros 24 KB de carga útil. Puede utilizar este método de equilibrio de carga en servidores virtuales de diferentes tipos para asegurarse de que las solicitudes que presentan el mismo token se dirigen a los servicios apropiados, independientemente del protocolo utilizado.

Por ejemplo, considere una configuración de equilibrio de carga compuesta por servidores que contengan contenido web. Quiere configurar el dispositivo Citrix ADC para que busque una cadena específica (el token) dentro de la parte de consulta de URL de la solicitud. Server-1 tiene dos servicios, Service-HTTP-1 y Servicio-TCP-1, y Server-2 tiene dos servicios, Servicio-HTTP-2 y Servicio-TCP-2. Los servicios TCP están enlazados a VServer-lb-2 y los servicios HTTP están enlazados a VServer-lb-1.

Si VServer-LB-1 recibe una solicitud con el token AA, selecciona el servicio Service-HTTP-1 (vinculado al servidor-1) para procesar la solicitud. Si VServer-LB-2 recibe una solicitud diferente con el mismo token (AA), dirige esta solicitud al servicio Service-TCP-1. El siguiente diagrama ilustra este proceso.

Ilustración 1. Cómo funciona el método Token



Para configurar el método de equilibrio de carga de Token mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para configurar el método de equilibrio de carga del token y verificar la configuración:

```
set lb vserver <name> -lbMethod TOKEN -rule <rule> -datalength <length>
    -dataoffset <offset>

show lb vserver <name>
<!--NeedCopy-->
```

Ejemplo:

```
set lb vserver LB-VServer-1 -lbMethod TOKEN -rule 'AA' -datalength 2 -
   dataoffset 25

```



```
show lb vserver LB-VServer-1
<!--NeedCopy-->
```

Para configurar el método de equilibrio de carga del token mediante la utilidad de configuración

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**y abra un servidor virtual.
2. En Configuración avanzada, haga clic en Método
3. En la lista Método de equilibrio de carga, seleccione Token y especifique una expresión.

Configurar un método de equilibrio de carga que no incluya una directiva

January 19, 2021

Después de seleccionar un algoritmo de equilibrio de carga para la configuración de equilibrio de carga, debe configurar el dispositivo Citrix ADC para que utilice ese algoritmo. Puede configurarlo mediante la CLI o mediante la utilidad de configuración.

Nota:

El método token está basado en directivas y requiere más configuración de la que se describe aquí. Para configurar el método token, consulte Método Token.

Para algunos métodos basados en hash, puede enmascarar una dirección IP para dirigir las solicitudes que pertenecen a la misma subred al mismo servidor. Para obtener más información, consulte Métodos de hash.

Para establecer el método de equilibrio de carga mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
set lb vserver <name> -lbMethod <method>
<!--NeedCopy-->
```

Ejemplo:


```
set lb vserver Vserver-LB-1 -lbMethod LeastConnection
<!--NeedCopy-->
```

Para establecer el método de equilibrio de carga mediante la utilidad de configuración

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**y abra un servidor virtual.
2. En Configuración avanzada, haga clic en **Método** y, en la lista Método de equilibrio de carga, seleccione un método.

Persistencia y conexiones persistentes

August 20, 2021

Un protocolo sin estado de equilibrio de carga, como HTTP, interrumpe el mantenimiento de la información de estado sobre las conexiones de clientes si no se configura la persistencia. Es posible que las transmisiones distintas del mismo cliente se dirijan a distintos servidores, aunque todas las transmisiones formen parte de la misma sesión. Puede configurar la persistencia en un servidor virtual de equilibrio de carga que gestiona ciertos tipos de aplicaciones web, como las aplicaciones de carrito de compras.

Antes de configurar la persistencia, debe comprender los diferentes tipos de persistencia, cómo se usan y cuáles son las implicaciones de cada tipo. A continuación, debe configurar el dispositivo Citrix ADC para proporcionar conexiones persistentes para los sitios web y las aplicaciones web que los requieren.

También puede configurar la persistencia de la copia de seguridad, que surte efecto si falla el tipo principal de persistencia configurado para un servidor virtual de equilibrio de carga. Puede configurar grupos de persistencia para que una transmisión de cliente a cualquier servidor virtual de un grupo se pueda dirigir a un servidor que haya recibido transmisiones anteriores del mismo cliente.

Para obtener información sobre la persistencia con equilibrio de cargas RADIUS, consulte Configuración del equilibrio de cargas RADIUS con persistencia.

Acerca de la persistencia

August 20, 2021

Puede elegir entre varios tipos de persistencia para un servidor virtual de equilibrio de carga determinado, que luego dirige al mismo servicio todas las conexiones del mismo usuario a su aplicación de carrito de compras, correo electrónico basado en web u otra aplicación de red. La sesión de persistencia permanece vigente durante el tiempo que especifique.

Si un servidor que participa en una sesión de persistencia baja, el servidor virtual de equilibrio de carga utiliza el método de equilibrio de carga configurado para seleccionar un nuevo servicio y establece una nueva sesión de persistencia con el servidor representado por ese servicio. Si el servidor sale DE SERVICIO, continúa procesando las sesiones de persistencia existentes, pero el servidor virtual no dirige ningún tráfico nuevo a él. Una vez transcurrido el período de apagado, el servidor virtual deja de dirigir las conexiones de los clientes existentes al servicio, cierra las conexiones existentes y redirige esos clientes a nuevos servicios si es necesario.

Dependiendo del tipo de persistencia que configure, el dispositivo Citrix ADC podría examinar las direcciones IP de origen, las direcciones IP de destino, los identificadores de sesión SSL, los encabezados de host o URL, o alguna combinación de estos elementos para colocar cada conexión en la sesión de persistencia adecuada. También puede basar la persistencia en una cookie emitida por el servidor web, en un token asignado arbitrariamente o en una regla lógica. Casi cualquier cosa que permita que el dispositivo coincida con las conexiones con la sesión de persistencia adecuada y se utiliza como base para la persistencia.

En la siguiente tabla se resumen los tipos de persistencia disponibles en el dispositivo Citrix ADC.

Tipo de persistencia	Descripción
IP de origen	SOURCEIP. Las conexiones desde la misma dirección IP del cliente forman parte de la misma sesión de persistencia.
Cookie HTTP	COOKIEINSERT. Las conexiones que tienen el mismo encabezado HTTP Cookie son partes de la misma sesión de persistencia.
ID de sesión SSL	SSLSESSION. Las conexiones que tienen el mismo ID de sesión SSL son parte de la misma sesión de persistencia.
URL Pasiva	URLPASIVO. Las conexiones a la misma dirección URL se tratan como partes de la misma sesión de persistencia.
ID de servidor personalizado	CUSTOMSERVERID. Las conexiones con el mismo encabezado HOST HTTP se tratan como partes de la misma sesión de persistencia.

Tipo de persistencia	Descripción
IP de destino	DESTIPÓN. Las conexiones a la misma IP de destino se tratan como partes de la misma sesión de persistencia.
IP de origen y destino	SRCIPDESTIP. Las conexiones que son de la misma IP de origen y de la misma IP de destino se tratan como partes de la misma sesión de persistencia.
ID de llamada SIP	CALLID. Las conexiones que tienen el mismo ID de llamada en el encabezado SIP se tratan como partes de la misma sesión de persistencia.
ID de sesión RTSP	RTSPSID. Las conexiones que tienen el mismo identificador de sesión RTSP se tratan como partes de la misma sesión de persistencia.
Regla definida por el usuario	REGLA. Las conexiones que coinciden con una regla definida por el usuario se tratan como partes de la misma sesión de persistencia.

Cuadro 1 Tipos de persistencia

Dependiendo del tipo de persistencia que haya configurado, el servidor virtual puede admitir 250.000 conexiones persistentes simultáneas o cualquier número de conexiones persistentes hasta los límites impuestos por la cantidad de RAM del dispositivo Citrix ADC. La siguiente tabla muestra qué tipos de persistencia pertenecen a cada categoría.

Tipo de persistencia	Número de conexiones persistentes simultáneas admitidas
IP de origen, ID de sesión SSL, regla, IP de destino, IP de origen/IP de destino, ID de llamada SIP, ID de sesión RTSP	250 K
Cookie, ID de servidor de URL, ID de servidor personalizado	Límite de memoria. En CookieInsert, si el tiempo de espera no es 0, el número de conexiones está limitado por la memoria.

Tabla 2. Tipos de persistencia y números de conexiones simultáneas admitidas

Algunos tipos de persistencia son específicos de determinados tipos de servidor virtual. La tabla siguiente muestra cada tipo de persistencia e indica qué tipos de persistencia se admiten en qué tipos de servidor virtual.

Tipo de persistencia	HTTP	HTTPS	TCP	UDP/IP	Puente SSL_Bridge	SSL_TCP	RTSP	SIP_UDP
SOURCEI	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	NO	NO
COOKIEINSÉRT	SÍ	NO	NO	NO	NO	NO	NO	NO
SSLSESS	NO	SÍ	NO	NO	SÍ	SÍ	NO	NO
URLPASIVAS	SÍ	SÍ	NO	NO	NO	NO	NO	NO
IDENTIFI DE CLIENTE	SÍ	SÍ	NO	NO	NO	NO	NO	NO
REGLA	SÍ	SÍ	SÍ	NO	NO		NO	NO
SRCIPDE	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	NO	NO
DESTIP	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	NO	NO
CALLID	NO	NO	NO	NO	NO	NO	NO	SÍ
IDRTSPID	NO	NO	NO	NO	NO	NO	SÍ	NO

Tabla 3. Relación del tipo de persistencia con el tipo de servidor virtual

Persistencia de la dirección IP de origen

August 20, 2021

Cuando se configura la persistencia de IP de origen, el servidor virtual de equilibrio de carga utiliza el método de equilibrio de carga configurado para seleccionar un servicio para la solicitud inicial y, a continuación, utiliza la dirección IP de origen (dirección IP del cliente) para identificar las solicitudes posteriores de ese cliente y enviarlas al mismo servicio. Puede establecer un valor de tiempo de espera, que especifica el período máximo de inactividad para la sesión. Cuando caduca el valor de tiempo de espera, se descarta la sesión y se utiliza el algoritmo de equilibrio de carga configurado para seleccionar un nuevo servidor.

Precaución: En algunas circunstancias, el uso de persistencia basada en la dirección IP de origen puede sobrecargar los servidores. Todas las solicitudes a un único sitio web o aplicación se enrutan

a través de la puerta de enlace única al dispositivo Citrix ADC, aunque luego se redirijan a varias ubicaciones. En varios entornos proxy, las solicitudes de cliente suelen tener direcciones IP de origen diferentes, incluso cuando se envían desde el mismo cliente, lo que da como resultado una rápida multiplicación de las sesiones de persistencia en las que se debe crear una sola sesión. Este problema se llama el "problema de Mega Proxy". Puede utilizar la persistencia basada en cookies HTTP en lugar de la persistencia basada en IP de origen para evitar que esto suceda.

Para configurar la persistencia basada en la dirección IP de origen, consulte Configuración de tipos de persistencia que no requieren una regla.

Nota: Si todo el tráfico entrante viene de detrás de un dispositivo o proxy de traducción de direcciones de red (NAT), el tráfico parece que el dispositivo Citrix ADC procede de una única dirección IP de origen. Esto impide que la persistencia de IP de origen funcione correctamente. En este caso, debe seleccionar un tipo de persistencia diferente.

persistencia de cookies HTTP

August 20, 2021

Cuando se configura la persistencia de cookies HTTP, el dispositivo Citrix ADC establece una cookie en los encabezados HTTP de la solicitud inicial del cliente. La cookie contiene la dirección IP y el puerto del servicio seleccionado por el algoritmo de equilibrio de carga. Al igual que con cualquier conexión HTTP, el cliente incluye esa cookie con cualquier solicitud posterior.

Cuando el dispositivo Citrix ADC detecta la cookie, reenvía la solicitud a la IP del servicio y al puerto de la cookie, manteniendo la persistencia de la conexión. Puede utilizar este tipo de persistencia con servidores virtuales de tipo HTTP o HTTPS. Este tipo de persistencia no consume recursos de dispositivo y, por lo tanto, puede acomodar un número ilimitado de clientes persistentes.

Nota: Si el explorador web del cliente está configurado para rechazar las cookies, la persistencia basada en cookies HTTP no funciona. Puede ser aconsejable configurar una comprobación de cookie en el sitio web y advertir a los clientes que parecen no almacenar cookies correctamente que necesitan habilitar las cookies para el sitio web si desean utilizarlo.

El formato de la cookie que inserta el dispositivo Citrix ADC es:

```
NSC_XXXX=<ServiceIP ><ServicePort>
```

Donde:

- NSC_XXXX es el ID del servidor virtual que se deriva del nombre del servidor virtual.
- ServiceIP y ServicePort son representaciones codificadas de la dirección IP del servicio y el puerto de servicio, respectivamente. La dirección IP y el puerto se codifican por separado.

Puede establecer un valor de tiempo de espera para este tipo de persistencia para especificar un período de inactividad para la sesión. Cuando la conexión ha estado inactiva durante el período especificado, el dispositivo Citrix ADC descarta la sesión de persistencia. Cualquier conexión posterior del mismo cliente hace que se seleccione un nuevo servidor basado en el método de equilibrio de carga configurado y se establezca una nueva sesión de persistencia.

Nota: Si establece el valor de tiempo de espera en 0, el dispositivo Citrix ADC no especifica un tiempo de caducidad, sino que establece una cookie de sesión que no se guarda cuando se cierra el explorador del cliente.

De forma predeterminada, el dispositivo Citrix ADC establece las cookies HTTP versión 0 para obtener la máxima compatibilidad con los exploradores cliente. (Solo ciertos proxies HTTP entienden las cookies de la versión 1; los exploradores más utilizados no.) Puede configurar el dispositivo para que establezca cookies HTTP versión 1, para cumplir con RFC2109. Para las cookies de la versión 0 de HTTP, el dispositivo inserta la fecha y hora de caducidad de la cookie como una hora universal coordinada (GMT) absoluta. Calcula este valor como la suma de la hora GMT actual en el dispositivo y el valor de tiempo de espera. Para las cookies HTTP versión 1, el dispositivo inserta un tiempo de caducidad relativo estableciendo el atributo "Max-Age" de la cookie HTTP. En este caso, el explorador del cliente calcula el tiempo de caducidad real.

Para configurar la persistencia basada en una cookie insertada por el dispositivo, consulte Configuración de tipos de persistencia que no requieren una regla.

En la cookie HTTP, el dispositivo establece de forma predeterminada el `HTTPOnly` indicador para indicar que la cookie no se puede escribir en scripts y no debe revelarse a la aplicación cliente. Por lo tanto, un script del lado del cliente no puede acceder a la cookie, y el cliente no es susceptible a scripts entre sitios.

Sin embargo, algunos exploradores no admiten el `HTTPOnly` indicador y, por lo tanto, es posible que no devuelvan la cookie. Como resultado, la persistencia se rompe. En el caso de los exploradores que no admiten el indicador, puede omitir el `HTTPOnly` indicador en la cookie de persistencia.

Para cambiar la configuración de la `HTTPOnly` marca mediante la CLI

En el símbolo del sistema, escriba:

```
set lb parameter -httpOnlyCookieFlag (ENABLED|DISABLED)
<!--NeedCopy-->
```

Ejemplo:


```
> set lb parameter -httpOnlyCookieFlag disabled
  Done
> show lb parameter
  Global LB parameters:
       Persistence Cookie HttpOnly Flag: DISABLED
       Use port for hash LB: YES
 Done
<!--NeedCopy-->
```

Para cambiar la configuración de la HTTPOnly marca mediante la GUI

1. Vaya a **Administración del tráfico > Equilibrio de carga > Configurar parámetros de equilibrio de carga**y seleccione o desactive la marca **Cookie de persistencia HttpOnly** .

Cifrado de la cookie

A partir de la versión 10.5 build 55.8, puede cifrar la cookie además de cualquier cifrado SSL.

Para cifrar la cookie mediante la interfaz de línea de comandos, en el símbolo del sistema, escriba

```
set lb parameter -UseEncryptedPersistenceCookie ENABLED -
   cookiePassphrase test
<!--NeedCopy-->
```

Para cifrar la cookie mediante la utilidad de configuración

1. Vaya a **Gestión del tráfico** > **Cambiar parámetros de equilibrio de carga** y seleccione **Codificar valores de cookies de persistencia** e introduzca una frase de contraseña en la **frase de contraseña de Cookie**.

Persistencia de ID de sesión SSL

August 20, 2021

Cuando se configura la persistencia de ID de sesión SSL, el dispositivo Citrix ADC utiliza el ID de sesión SSL, que forma parte del proceso de enlace SSL, para crear una sesión de persistencia antes de que la solicitud inicial se dirija a un servicio. El servidor virtual de equilibrio de carga dirige las solicitudes

posteriores que tienen el mismo ID de sesión SSL al mismo servicio. Este tipo de persistencia se utiliza para los servicios de puente SSL.

Nota:

Hay dos problemas que los usuarios deben tener en cuenta antes de elegir este tipo de persistencia. En primer lugar, este tipo de persistencia consume recursos en el dispositivo Citrix ADC, lo que limita el número de sesiones de persistencia simultáneas que puede admitir. Si espera admitir varias sesiones de persistencia, puede que desee elegir otro tipo de persistencia.

En segundo lugar, si el cliente y el servidor equilibrado de carga deben renegociar el ID de sesión durante sus transacciones, la persistencia no se mantiene y se crea una nueva sesión de persistencia cuando se recibe la próxima solicitud del cliente. Esto podría provocar la interrupción de la actividad del cliente en el sitio web y se le podría pedir al cliente que vuelva a autenticar o reiniciar la sesión. También podría dar lugar a un gran número de sesiones abandonadas si el tiempo de espera se establece en un valor demasiado grande.

Para configurar la persistencia basada en el ID de sesión SSL, consulte Configuración de tipos de persistencia que no requieren una regla.

> **Nota**
>
> La persistencia de ID de sesión SSL no es compatible con los tíquets de sesión.

Compatibilidad con la persistencia de copia de seguridad para ID de sesión SSL

Desde la versión 12.0 de NetScaler, versión 56.20, se admite la persistencia de IP de origen como un tipo de persistencia de copia de seguridad para la persistencia de ID de sesión SSL. Si el cliente y el servidor con equilibrio de carga renegocian la sesión y la persistencia de IP de origen se configura como persistencia de copia de seguridad, las solicitudes de cliente se reenvían al mismo servidor.

Para admitir la persistencia de copias de seguridad para el ID de sesión SSL, el dispositivo Citrix ADC crea entradas de sesión tanto para la IP de origen como para el ID de sesión SSL cuando se recibe una solicitud de cliente por primera vez. Para las solicitudes posteriores que contienen el mismo ID de sesión, se utiliza el ID de sesión SSL. Sin embargo, cuando el cliente y el servidor balanceado de carga renegocian la sesión, la solicitud de cliente se reenvía al mismo servidor mediante la persistencia IP de origen y se crea una nueva entrada de persistencia de ID de sesión SSL.

Para obtener información sobre cómo configurar la persistencia de la copia de seguridad, consulte Configuración de la persistencia de respaldo.

Persistencia del número AVP de diameter

January 12, 2021

Puede utilizar la persistencia basada en el número de par atributo-valor (AVP) de un mensaje Diameter para crear sesiones de diameter persistentes. Cuando el dispositivo Citrix ADC encuentra el AVP en el mensaje Diameter, crea una sesión de persistencia basada en el valor del AVP. Todos los mensajes posteriores que coincidan con el valor del AVP se dirigen al servidor seleccionado previamente. Si el valor del AVP no coincide con la sesión de persistencia, se crea una nueva sesión para el nuevo valor.

Nota: Si el número AVP no está definido en el protocolo base de diámetro RFC 6733, y si el número está anidado dentro de un AVP agrupado, debe definir una secuencia de números AVP (máximo de 3) en orden principal a secundario. Por ejemplo, si el número AVP persistente X está anidado dentro de AVP Y, que está anidado en Z, defina la lista como Z Y X.

Para configurar la persistencia basada en diameter en un servidor virtual mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba el siguiente comando:

```
set lb vserver <name> -PersistenceType <type-> persistAVPno <
   positive_integer>
<!--NeedCopy-->
```

Ejemplo:

```
set lb vserver diameter_vs -persistenceType DIAMETER -persistAVPno 263
<!--NeedCopy-->
```

Persistencia de ID de servidor personalizada

August 20, 2021

En el método de persistencia de ID de servidor personalizado, el ID de servidor especificado en la solicitud de cliente se utiliza para mantener la persistencia. Para que este tipo de persistencia funcione, primero debe establecer un ID de servidor en los servicios. El dispositivo Citrix ADC comprueba la dirección URL de la solicitud de cliente y se conecta al servidor asociado con el ID de servidor especificado. El proveedor de servicios debe asegurarse de que los usuarios conozcan los ID de servidor que se deben proporcionar en sus solicitudes de servicios específicos.

Por ejemplo, si el sitio proporciona diferentes tipos de datos, como imágenes, texto y multimedia, de distintos servidores, puede asignar a cada servidor un ID de servidor. En el dispositivo Citrix ADC,

especifique esos ID de servidor para los servicios correspondientes y configure la persistencia de ID de servidor personalizada en el servidor virtual de equilibrio de carga correspondiente. Al enviar una solicitud, el cliente inserta el ID del servidor en la URL que indica el tipo de datos requerido.

Para configurar la persistencia de ID de servidor personalizada:

- En la configuración de equilibrio de carga, asigne un Id. de servidor a cada servicio para el que quiera utilizar el Id. de servidor definido por el usuario para mantener la persistencia. Se permiten identificadores de servidor alfanuméricos.
- Especifique reglas, en el lenguaje de expresión de sintaxis predeterminada, para examinar las consultas de URL para el ID del servidor y reenviar el tráfico al servidor correspondiente.
- Configure la persistencia de ID de servidor personalizada.

Nota: El valor de tiempo de espera de persistencia no afecta al tipo de persistencia de ID de servidor personalizado. No hay límite en el número máximo de clientes persistentes porque este tipo de persistencia no almacena ninguna información de cliente.

Ejemplo:

En una configuración de equilibrio de carga con dos servicios, asigne el ID de servidor 2345-photo-56789 a Service-1 y el ID de servidor 2345-drawing-abb123 a Service-2. Enlazar estos servicios a un servidor virtual denominado web11.

```
1 set service Service-1 10.102.29.5 -CustomServerID 2345-photo-56789
2
3 set service Service-2 10.102.29.6 -CustomServerID 2345-drawing-abb123
4 <!--NeedCopy-->
```

En el servidor virtual Web11, habilite la persistencia de ID de servidor personalizado.

Cree la siguiente expresión para que se examinen todas las consultas de URL que contengan la cadena “sid=”.

HTTP.REQ.URL.AFTER_STR (“sid=”)

Ejemplo:

```
1 set lb vserver Web11 -persistenceType customserverID -rule ”HTTP.REQ.
     URL.AFTER_STR(”sid=”)”
2
3 bind lb vserver Web11 Service-[1-2]
4 <!--NeedCopy-->
```


Cuando un cliente envía una solicitud con la siguiente dirección URL a la dirección IP de Web11, el dispositivo dirige la solicitud a Service-2 y respeta la persistencia.

Ejemplo:

```
http://www.example.com/index.asp?&sid=2345-drawing-abb123
```

Para obtener más información sobre las expresiones de directiva de sintaxis por defecto, consulte Configuración y referencia de directivas.

Para configurar la persistencia de ID de servidor personalizada mediante la utilidad de configuración

1. Vaya a **Administración de Tráfico > Equilibrio de carga > Servicios**.
2. Abra el servicio y establezca un ID de servidor.
3. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**y abra el servidor virtual.
4. En Configuración avanzada, seleccione Persistencia.
5. Seleccione CUSTOMERVERID y especifique una expresión.

Persistencia de direcciones IP

August 20, 2021

Puede basar la persistencia en direcciones IP de destino o en direcciones IP de origen y direcciones IP de destino.

Persistencia basada en direcciones IP de destino

Con persistencia basada en direcciones IP de destino, cuando el dispositivo Citrix ADC recibe una solicitud de un nuevo cliente, crea una sesión de persistencia basada en la dirección IP del servicio seleccionado por el servidor virtual (la dirección IP de destino). Posteriormente, dirige las solicitudes a la misma IP de destino al mismo servicio. Este tipo de persistencia se utiliza con el equilibrio de carga de enlace. Para obtener más información sobre el equilibrio de carga de vínculos, consulte Equilibrio de cargade vínculos.

El valor de tiempo de espera de la persistencia IP de destino es el mismo que para la persistencia IP de origen, descrito en Persistencia basada en la dirección IP de origen.

Para configurar la persistencia en función de la dirección IP de destino, consulte Configuración de tipos de persistencia que no requieren una regla.

Persistencia basada en direcciones IP de origen y destino

Con persistencia basada en direcciones IP de origen y destino, cuando el dispositivo Citrix ADC recibe una solicitud, crea una sesión de persistencia basada tanto en la dirección IP del cliente (la dirección IP de origen) como en la dirección IP del servicio seleccionado por el servidor virtual (la dirección IP de destino). Posteriormente, dirige las solicitudes desde la misma IP de origen y hacia la misma IP de destino al mismo servicio.

El valor de tiempo de espera de la persistencia IP de destino es el mismo que para la persistencia IP de origen, descrito en Persistencia basada en la dirección IP de origen.

Para configurar la persistencia en función de las direcciones IP de origen y de destino, consulte Configuración de tipos de persistencia que no requieren una regla.

Persistencia del ID de llamada SIP

August 20, 2021

Con la persistencia de ID de llamada SIP, el dispositivo Citrix ADC elige un servicio basado en el ID de llamada del encabezado SIP. Esto le permite dirigir paquetes para una sesión SIP particular al mismo servicio y, por lo tanto, al mismo servidor equilibrado de carga. Este tipo de persistencia es aplicable específicamente al equilibrio de carga SIP. Para obtener más información sobre el equilibrio de carga SIP, consulte Supervisión de los servicios SIP.

Para configurar la persistencia basada en el identificador de llamada SIP, consulte Configuración de tipos de persistencia que no requieren una regla.

Persistencia de ID de sesión RTSP

August 20, 2021

Con la persistencia de ID de sesión de RTSP, cuando el dispositivo Citrix ADC recibe una solicitud de un nuevo cliente, crea una sesión de persistencia basada en el ID de sesión del protocolo de transmisión en tiempo real (RTSP) en el encabezado del paquete RTSP y, a continuación, dirige la solicitud al servicio RTSP seleccionado por el equilibrio de carga configurado método. Dirige las solicitudes posteriores que contienen el mismo ID de sesión al mismo servicio. Este tipo de persistencia es aplicable específicamente al equilibrio de carga SIP. Para obtener más información sobre el equilibrio de carga SIP, consulte Supervisión de los servicios SIP.

Nota: La persistencia de ID de sesión RTSP está configurada de forma predeterminada en servidores virtuales RTSP y no puede modificar esa configuración.

A veces, diferentes servidores RTSP emiten los mismos ID de sesión. Cuando esto sucede, no se pueden crear sesiones únicas entre el cliente y el servidor RTSP mediante solo el ID de sesión RTSP. Si tiene varios servidores RTSP que pueden emitir los mismos ID de sesión, puede configurar el dispositivo para que agregue la dirección IP del servidor y el puerto al ID de sesión, creando un token único que se puede utilizar para establecer la persistencia. Esto se denomina asignación de ID de sesión.

Para configurar la persistencia basada en ID de sesión de RTSP, consulte Configuración de tipos de persistencia que no requieren una regla.

Importante: Si necesita utilizar la asignación de ID de sesión, debe establecer el siguiente parámetro al configurar cada servicio dentro de la configuración de equilibrio de carga. Además, asegúrese de que no se enrutan conexiones no persistentes a través del servidor virtual RTSP.

Configurar persistencia pasiva de URL

August 20, 2021

Con persistencia pasiva de URL, cuando el dispositivo Citrix ADC recibe una solicitud de un cliente, extrae la información del puerto de dirección IP del servidor (expresada como un único número hexadecimal) de la solicitud del cliente.

La persistencia pasiva de URL requiere configurar una expresión avanzada que especifique el elemento de consulta que contiene la información del puerto de dirección IP del servidor. Para obtener más información sobre las expresiones de directivas clásicas y avanzadas, consulte Directivas y expresiones.

La siguiente expresión configura el dispositivo para examinar las solicitudes de consultas de URL que contienen la cadena “urlp=”, extraer la información del puerto de dirección IP del servidor, convertirla de una cadena hexadecimal a una IP y un número de puerto y reenviar la solicitud al servicio configurado con esta dirección IP y número de puerto.

HTTP.REQ.URL.AFTER_STR (“urlp=”)

Si la persistencia pasiva de URL está habilitada y se configura la expresión anterior, se dirige una solicitud con la siguiente URL y cadena de puerto de dirección IP del servidor a 10.102.29. 10:80.

```
http://www.example.com/index.asp?&urlp=0A661D0A0050
```

El valor de tiempo de espera de persistencia no afecta a este tipo de persistencia. La persistencia se mantiene siempre que la información del puerto de dirección IP del servidor se pueda extraer de las solicitudes del cliente. Este tipo de persistencia no consume recursos de dispositivo, por lo que puede acomodar un número ilimitado de clientes persistentes.

Para configurar la persistencia pasiva de URL, primero configure la persistencia como se describe en Configuración de tipos de persistencia que no requieren una regla. Establecer el tipo de persistencia en URLPASSIVE. A continuación, realiza los siguientes procedimientos.

Para configurar la persistencia pasiva de URL mediante la CLI

En el símbolo del sistema, escriba:

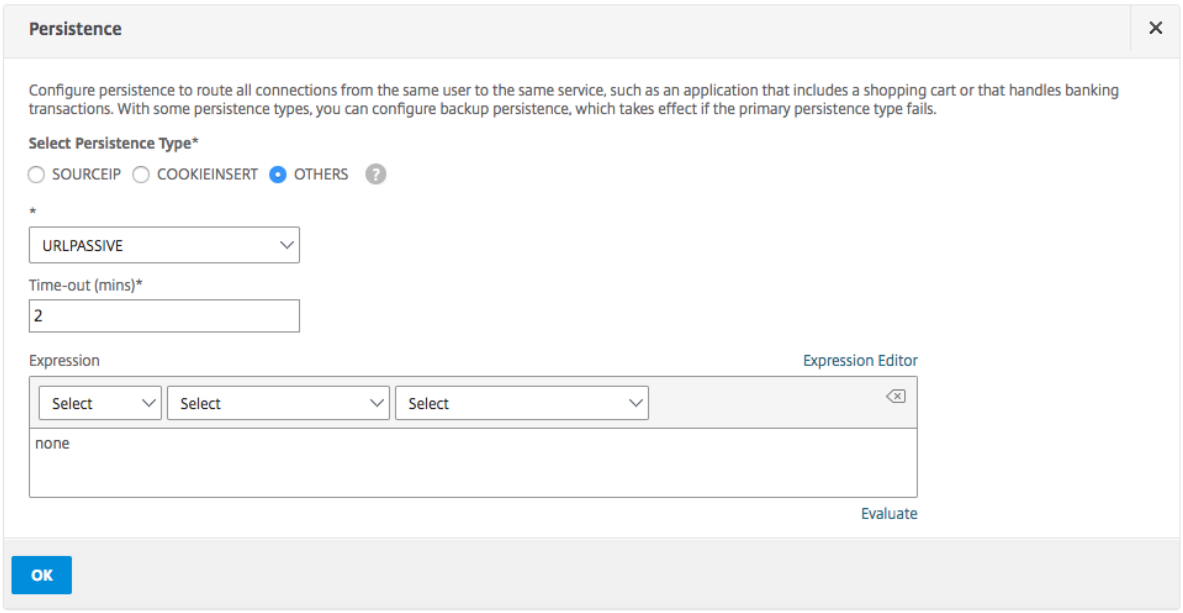
```
set lb vserver <vserverName>  [-persistenceType <persistenceType>]  [-
    rule <expression>]
<!--NeedCopy-->
```

Ejemplo:

```
set lb vserver LB-VServer-1 -persistenceType URLPASSIVE  -rule HTTP.REQ
    .URL.AFTER_STR( "urlp=" )
<!--NeedCopy-->
```

Para configurar la persistencia en un servidor virtual mediante la interfaz gráfica de usuario

1. Vaya a **Administracióndel tráfico**>**Equilibrio**de**carga**>**Servidoresvirtuales**y abra el servidor virtual.
2. En la sección Persistencia, elija el tipo de persistencia que cumpla con sus requisitos. El tipo de persistencia más adecuado para el servidor virtual está disponible como botones de opción. Se pueden seleccionar otros tipos de persistencia aplicables al tipo de servidor virtual específico en la lista Otros.



> **Nota:**
>
> Antes de NetScaler versión 12.0 compilación 56.20, todos los tipos de persistencia están disponibles en una sola lista desplegable Persistencia sin botones de opción.

Configurar la persistencia según las reglas definidas por el usuario

October 5, 2021

> **Advertencia:**
>
> Se ha eliminado el uso de expresiones clásicas para la regla de persistencia en la función de equilibrio de carga y ya no está disponible para la regla de filtro en la versión 13.1 del dispositivo Citrix ADC en adelante. Citrix recomienda no utilizar estas expresiones de directiva a través de la interfaz de línea de comandos de Citrix ADC, la GUI de Citrix ADC o la automatización de Nitro. Para obtener más información, consulte la tabla 1 y la tabla 2 de la página de preguntas frecuentes sobre el desuso de directivas clásicas .

Cuando se configura la persistencia basada en reglas, el dispositivo Citrix ADC crea una sesión de persistencia basada en el contenido de la regla coincidente antes de dirigir la solicitud al servicio seleccionado por el método de equilibrio de carga configurado. Posteriormente, dirige todas las solicitudes que coinciden con la regla al mismo servicio. Puede configurar la persistencia basada en reglas para servicios de tipo HTTP, SSL, RADIUS, ANY, TCP y SSL_TCP.

La persistencia basada en reglas requiere una expresión de directiva clásica o avanzada. Puede utilizar una expresión clásica para evaluar los encabezados de solicitud o una expresión de directiva avanzada para evaluar los encabezados de solicitud, los datos de formularios web de una solicitud,

los encabezados de respuesta o los cuerpos de respuesta. Por ejemplo, puede utilizar una expresión clásica para configurar la persistencia basada en el contenido del encabezado de host HTTP. También puede utilizar una expresión de directiva avanzada para configurar la persistencia en función de la información de sesión de la aplicación en una cookie de respuesta o en un encabezado personalizado. Para obtener más información sobre la creación y el uso de expresiones de directiva clásicas y avanzadas, consulte Directivas y expresiones.

Las expresiones que puede configurar dependen del tipo de servicio para el que está configurando la persistencia basada en reglas. Por ejemplo, determinadas expresiones específicas de RADIUS no están permitidas para protocolos distintos de RADIUS, y las expresiones basadas en opciones TCP no están permitidas para tipos de servicio distintos del tipo CUALQUIERA. Para los tipos de servicio TCP y SSL_TCP, puede utilizar expresiones que evalúen datos de protocolo TCP/IP, datos de capa 2, opciones TCP y cargas útiles TCP.

Nota: Para un caso de uso que implica configurar la persistencia basada en reglas basada en datos del protocolo Financial Information Exchange ("FIX") transmitidos a través de TCP, consulte Configuración de la persistencia basada en reglas basada en un par nombre-valor en un flujo de bytes TCP.

La persistencia basada en reglas se puede utilizar para mantener la persistencia con entidades como dispositivos Citrix SD-WAN, complementos Citrix SD-WAN, servidores de caché y servidores de aplicaciones.

Nota: En un servidor virtual CUALQUIERA, no puede configurar la persistencia basada en reglas para las respuestas.

Para configurar la persistencia basada en una regla definida por el usuario, primero configure la persistencia como se describe en Configuración de tipos de persistencia que no requieren una reglay establezca el tipo de persistencia en RULE. A continuación, puede llevar a cabo los siguientes procedimientos. Puede configurar la persistencia basada en reglas mediante la utilidad de configuración o la CLI.

Para configurar la persistencia según reglas definidas por el usuario mediante la CLI

En el símbolo del sistema, escriba:

```
set lb vserver <vserverName> [-rule <expression>][-resRule <expression
    >]
<!--NeedCopy-->
```

Ejemplo:

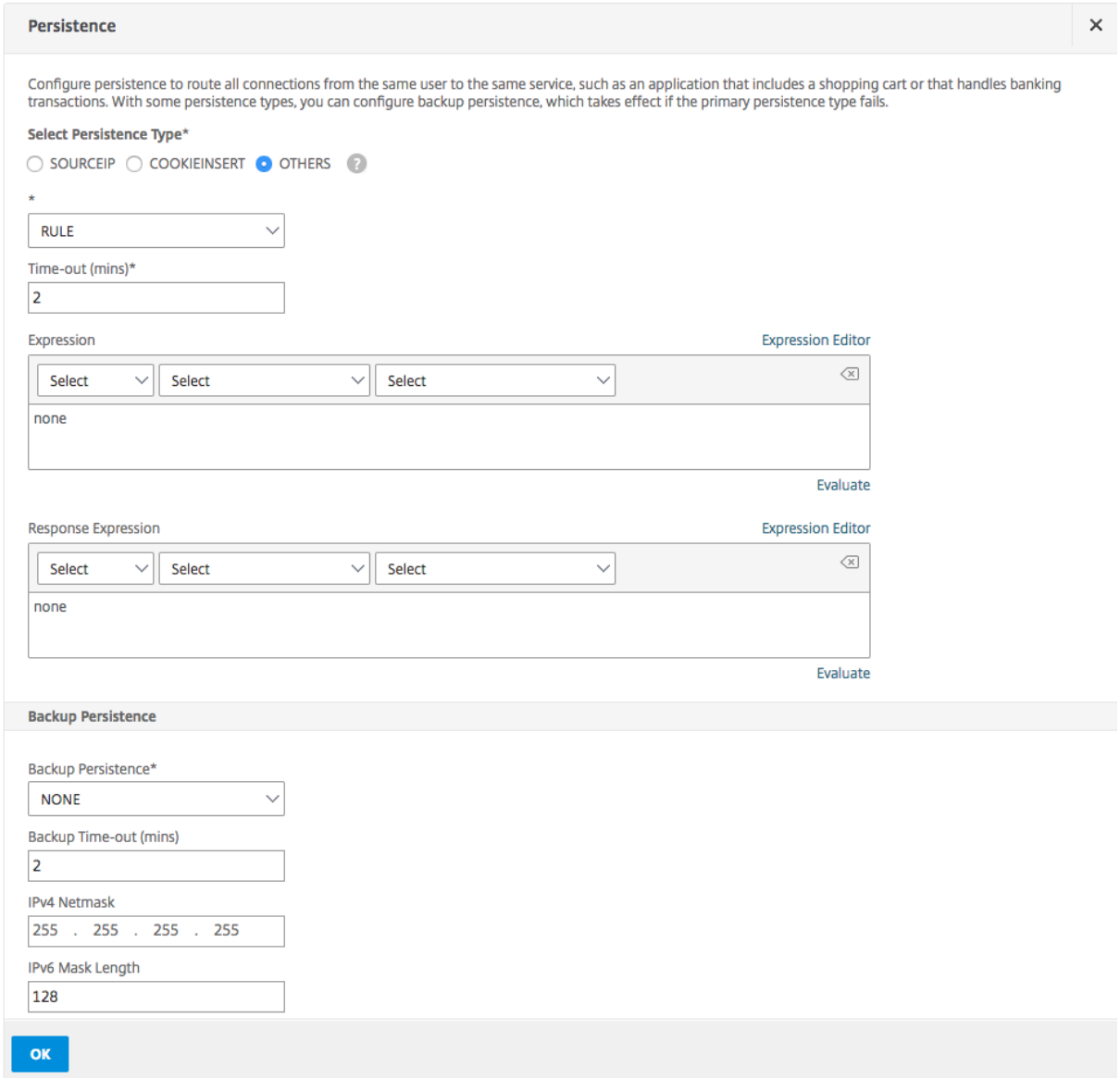

```
set lb vserver vsvr_name -rule http.req.header(”cookie”).value(0).
    typecast_nvlist_t('=',';').value(”server”)

set lb vserver vsvr_name -resrule http.res.header(”set-cookie”).value
    (0).typecast_nvlist_t('=',';').value(”server”)

<!--NeedCopy-->
```

Para configurar la persistencia en función de reglas definidas por el usuario mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**y abra el servidor virtual.
2. En la sección Persistencia, elige el tipo de persistencia que cumpla tus requisitos. El tipo de persistencia más adecuado para el servidor virtual está disponible como botones de opción. Se pueden seleccionar otros tipos de persistencia aplicables al tipo de servidor virtual específico en la lista Otros.



> **Nota**
>
> Antes de NetScaler versión 12.0 compilación 56.20, todos los tipos de persistencia están disponibles en una sola lista desplegable Persistencia sin botones de opción.

Ejemplo: expresión clásica para una carga útil de solicitud

La siguiente expresión clásica crea una sesión de persistencia basada en la presencia de un encabezado HTTP User-Agent que contiene la cadena “MyBrowser” y dirige cualquier solicitud de cliente posterior que contenga este encabezado y cadena al mismo servidor que se seleccionó para la solicitud inicial.


```
http header User-Agent contains MyBrowser
<!--NeedCopy-->
```

Ejemplo: expresión de directiva avanzada para un encabezado de solicitud

La siguiente expresión de directiva avanzada hace lo mismo que la expresión clásica anterior.

HTTP.REQ.HEADER(“User-Agent”).CONTAINS (“MyBrowser”)

Ejemplo: Expresión de directiva avanzada para una cookie de respuesta

La siguiente expresión examina las respuestas de las cookies de “servidor” y, a continuación, dirige cualquier solicitud que contenga esa cookie al mismo servidor que se seleccionó para la solicitud inicial.

HTTP.RES.HEADER(“SET-COOKIE”).VALUE(0).TYPECAST_NVLIST_T(‘=’,’;’).VALUE(“server”)

Configurar tipos de persistencia que no requieren una regla

January 19, 2021

Para configurar la persistencia, primero debe configurar un servidor virtual de equilibrio de carga, como se describe en Configuración del equilibrio de carga básico. A continuación, configure la persistencia en el servidor virtual.

Para configurar la persistencia en un servidor virtual mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para configurar la persistencia y verificar la configuración:

```
set lb vserver <name> -PersistenceType <type> [-timeout <integer>]

show lb vserver
<!--NeedCopy-->
```

Ejemplo:


```
set lb vserver Vserver-LB-1 -persistenceType SOURCEIP -timeout 60

show lb vserver
<!--NeedCopy-->
```

Tiempo de espera es el período de tiempo para el que está en vigor una sesión de persistencia. Los valores predeterminados y mínimos de tiempo de espera (en minutos) varían según el tipo de persistencia que se muestra en la tabla siguiente.

tipo de persistencia	Valor predeterminado	Valor mínimo	Valor máximo
Inserción de galletas/inserción de galleta de grupo	2	0	1440
Otros tipos de persistencia	2	2	1440

> **Nota**
>
> - El tipo de persistencia de inserción de cookie de grupo se puede establecer en el grupo de equilibrio de carga.
> - Para la persistencia basada en IP, también puede establecer el parámetro PersistMask.
> - El tipo de persistencia de forma predeterminada se establece en NONE.

Para configurar la persistencia en un servidor virtual mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**y abra el servidor virtual.
2. En la sección Persistencia, elija el tipo de persistencia que cumpla con sus requisitos. El tipo de persistencia más adecuado para el servidor virtual está disponible como botones de opción. Se pueden seleccionar otros tipos de persistencia aplicables al tipo de servidor virtual específico en la lista **Otros**.

> **Nota** Antes de la versión 12.0 de Citrix ADC versión 56.20, todos los tipos de persistencia están disponibles en una sola lista desplegable Persistencia sin botones de opción.

Configurar la persistencia de copias de seguridad

August 20, 2021

Puede configurar un servidor virtual para que use el tipo de persistencia IP de origen cuando falla el tipo de persistencia principal.

En la tabla siguiente se describen las combinaciones de tipos de persistencia de copia de seguridad primaria y secundaria y las condiciones en las que se utiliza la persistencia de copia de seguridad.

Persistencia primaria	Persistencia de backup	Cuando falla la búsqueda de persistencia principal…
Inserción de cookies	IP de origen	El dispositivo vuelve a la persistencia basada en IP de origen solo cuando el explorador cliente no devuelve ninguna cookie en la solicitud. Sin embargo, si el explorador devuelve una cookie (no necesariamente la cookie de persistencia), se supone que el explorador admite cookies y, por lo tanto, la persistencia de la copia de seguridad no se activa.
Regla	IP de origen	El dispositivo utiliza persistencia basada en IP de origen cuando falta el parámetro especificado en la regla en la solicitud entrante.

Nota

- Si el tipo de persistencia principal es la persistencia basada en cookies HTTP y el tipo de persistencia de copia de seguridad está basado en IP de origen, puede establecer un valor de tiempo de espera para la persistencia de la copia de seguridad. Para obtener instrucciones, consulte Configuración de un valor de tiempo de espera para las conexiones de clientes inactivas.
- No se puede establecer un valor de tiempo de espera para la persistencia de copia de se-

> guridad cuando la persistencia principal se basa en reglas, porque en ese caso el valor de tiempo de espera para la persistencia secundaria debe ser el mismo que para la persistencia primaria. Por lo tanto, el primario y el secundario caducan al mismo tiempo.

Para establecer la persistencia de copia de seguridad para un servidor virtual mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
set lb vserver <name> -persistenceType <PersistenceType> -
    persistenceBackup <BackupPersistenceType>
<!--NeedCopy-->
```

Ejemplo:

```
set lb vserver Vserver-LB-1 -persistenceType CookieInsert -
    persistenceBackup SourceIP

set lb vserver Vserver-LB-1 -persistenceType sslsession -
    persistenceBackup SourceIP

set lb vserver Vserver-LB-1  - persistenceType RULE  - rule http.req.
    header("User-Agent").value(0).contains("MyBrowser")  -
    persistenceBackup SOURCEIP

set lb vserver Vserver-LB-1 -persistenceType sslsession -
    persistenceBackup SourceIP
<!--NeedCopy-->
```

Para establecer la persistencia de copias de seguridad para un servidor virtual mediante la utilidad de configuración

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**y abra el servidor virtual.
2. En **Configuración avanzada**, seleccione **Persistencia** y especifique un tipo de persistencia de copia de seguridad.

Nota: La persistencia principal debe establecerse en COOKIEINSERT, RULE o SSLSESSION.

Configurar grupos de persistencia

January 19, 2021

Cuando tiene servidores con equilibrio de carga que manejan varios tipos diferentes de conexiones (como servidores web que alojan multimedia), puede configurar un grupo de servidores virtuales para controlar estas conexiones. Para crear un grupo de servidores virtuales, se vinculan diferentes tipos de servidores virtuales, uno para cada tipo de conexión que los servidores con equilibrio de carga aceptan, en un solo grupo. A continuación, configure un tipo de persistencia para todo el grupo.

Puede configurar la persistencia basada en IP de origen o la persistencia basada en cookies HTTP para grupos de persistencia. Después de establecer la persistencia para todo el grupo, no puede cambiarla para los servidores virtuales individuales del grupo. Si configura la persistencia en un grupo y, a continuación, agrega un nuevo servidor virtual al grupo, la persistencia del nuevo servidor virtual se cambia para que coincida con la configuración de persistencia del grupo.

Cuando se configura la persistencia en un grupo de servidores virtuales, las sesiones de persistencia se crean para las solicitudes iniciales y las solicitudes posteriores se dirigen al mismo servicio que la solicitud inicial, independientemente del servidor virtual del grupo que recibe cada solicitud de cliente.

Cuando agrega un servidor virtual que tiene sesiones de persistencia a un grupo de equilibrio de carga con un tipo de persistencia diferente, se eliminan las sesiones persistentes existentes específicas de un tipo de persistencia antiguo. Las sesiones persistentes deciden si el tráfico debe ir al mismo servidor virtual o a otro servidor. Por lo tanto, las conexiones establecidas existentes no se ven afectadas.

El tipo de persistencia de un grupo de equilibrio de carga se aplica a todos los servidores virtuales enlazados a ese grupo, independientemente del tipo de protocolo de los servidores virtuales. Un grupo de equilibrio de carga admite los siguientes tipos de persistencia:

- SourceIP
- CookieInsert
- Regla

Algunos servidores virtuales admiten solo ciertos tipos de persistencia. Por ejemplo, un servidor virtual de tipo SSL_BRIDGE solo puede utilizar el tipo de persistencia de SourceIP para un grupo LB.

Si configura la persistencia basada en cookies HTTP, se establece el atributo de dominio de la cookie HTTP. Esta configuración hace que el software cliente agregue la cookie HTTP en las solicitudes de cliente si diferentes servidores virtuales tienen nombres de host públicos diferentes. Para obtener más información sobre el tipo de persistencia CookieInsert, consulte Persistencia basada en cookies HTTP.

Para crear un grupo de persistencia de servidores virtuales mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
bind lb group <vServerGroupName> <vServerName> -persistenceType <
    PersistenceType>
<!--NeedCopy-->
```

Ejemplo:

```
bind lb group Vserver-Group-1 Vserver-LB-1 -persistenceType
    CookieInsert
<!--NeedCopy-->
```

Para modificar un grupo de servidores virtuales mediante la utilidad de configuración

1. Vaya a **Administración del tráfico > Equilibrio de carga > Grupos de persistencia**, cree un grupo de persistencia y especifique los servidores virtuales que deben formar parte de este grupo.

Para modificar un grupo de servidores virtuales mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
set lb group <vServerGroupName> -PersistenceBackup <
    BackupPersistenceType> -persistMask <SubnetMaskAddress>
<!--NeedCopy-->
```

Ejemplo:

```
set lb group vserver-Group-1 -PersistenceBackup SourceIP -persistMask
    255.255.255.255
<!--NeedCopy-->
```


Compartir sesiones persistentes entre servidores virtuales

August 20, 2021

En algunos entornos de clientes (telecomunicaciones e ISP), un único servidor maneja tanto el control como el tráfico de datos. Para una dirección IP de cliente determinada, tanto el control como el tráfico de datos deben dirigirse al mismo servidor back-end. Para ello, se requiere un servidor virtual para manejar el tráfico de autenticación de cliente y, por lo general, la persistencia basada en reglas se configura en él. Por ejemplo, Radius.req.avp (8) .value.typecast_text_t'. El segundo servidor virtual para gestionar el tráfico de datos. Por lo general, la persistencia de SourceIP se configura en él.

Anteriormente, las entradas de persistencia eran locales en el servidor virtual. Si tenía que aplicar persistencia en varios servidores virtuales, tenía que agregar el servidor virtual a un grupo de equilibrio de carga y, a continuación, aplicar un tipo de persistencia común al grupo. Este requisito no se puede lograr porque todos los servidores virtuales enlazados a un grupo de equilibrio de carga heredaron la persistencia configurada en el grupo.

Con la función de compartir persistencia entre servidores virtuales, puede establecer el nuevo `useVserverPersistency` parámetro para un grupo de equilibrio de carga para permitir que el servidor virtual del grupo utilice sus propios parámetros de persistencia en lugar de heredarlos de la configuración del grupo. Puede configurar una persistencia basada en reglas por separado en cada servidor virtual.

Opcionalmente, también puede designar uno de los servidores virtuales del grupo como servidor virtual principal. Cuando un servidor virtual se designa como servidor virtual principal, solo ese servidor virtual crea las entradas de persistencia, que utilizan todo el servidor virtual del grupo. Si el servidor virtual principal está inactivo, el dispositivo Citrix ADC no crea ninguna entrada de persistencia.

Nota: El uso compartido de persistencia en los servidores virtuales solo se admite para métodos de persistencia basados en reglas. Configure parámetros de persistencia basados en reglas compatibles en los servidores virtuales miembros.

Ejemplo:

Supongamos que v1 y v2 están enlazados a un grupo de equilibrio de carga, v1 es un servidor virtual de tipo RADIUS y v2 es un servidor virtual de tipo HTTP. La persistencia de 'Radius.req.avp (8) .value.typecast_text_t' está configurada en v1 y 'client.ip.src' está configurada en v2.

Cuando el tráfico fluye a través del servidor virtual RADIUS v1, crea una entrada persistente basada en la cadena de reglas evaluada. Posteriormente, cuando el tráfico llega al servidor virtual de tipo HTTP v2, v2 comprueba las entradas de persistencia en el grupo de equilibrio de carga y utiliza la misma sesión de persistencia para dirigir el tráfico al mismo servidor back-end.

Configuración del uso compartido de sesiones persistentes

Para compartir parámetros de persistencia en todo el servidor virtual de un grupo de equilibrio de carga, primero debe habilitar el parámetro UsevServerPersistency y, a continuación, designar uno de los servidores virtuales del grupo como servidor principal.

Para habilitar el parámetro UseVServerPersistency mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
set lb group <name> -useVserverPersistency ( ENABLED)
<!--NeedCopy-->
```

Ejemplo:

```
set lb group lb_grp1 -useVserverPersistency ENABLED
<!--NeedCopy-->
```

Para habilitar el parámetro UseVServerPersistency mediante la interfaz gráfica de usuario

1. Vaya a **Configuración** > **Administración del tráfico** > **Equilibrio de carga** > **Grupos de persistencia**.
2. Haga clic en **Agregar** para agregar un nuevo grupo o seleccione uno existente y haga clic en **Modificar**.
3. Seleccione **Usar persistencia de servidor virtual**.

Para designar un servidor virtual como servidor virtual principal mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
set lb group <name> -useVserverPersistency ( ENABLED ) -masterVserver <
    string>
<!--NeedCopy-->
```


Ejemplo:

```
set lb group lb_grp1 -useVserverPersistency ENABLED - masterVserver vs1
<!--NeedCopy-->
```

Para designar un servidor virtual como servidor virtual principal mediante la GUI

1. Vaya a **Configuración** > **Administración del tráfico** > **Equilibrio de carga** > **Grupos de persistencia**.
2. Haga clic en **Agregar** para agregar un nuevo grupo o seleccione uno existente y haga clic en **Modificar**.
3. Seleccione **Usar persistencia de servidor virtual**.
4. En el cuadro **Nombre del servidor virtual**, haga clic en **+** para agregar el servidor virtual al grupo. Puede seleccionar el servidor virtual disponible o crear un servidor virtual.
5. Haga clic en **Crear** si va a agregar un nuevo grupo o en **Cerrar** si está modificando un grupo existente.
6. Seleccione el grupo para el que ha habilitado el parámetro UseVServerPersistency y haga clic en **Modificar** para establecer un servidor virtual como principal para crear entradas de persistencia.
7. En la lista **Servidor virtual principal**, seleccione el servidor virtual que debe designarse como servidor virtual principal.

Argumentos

UseVServerPersistency

Permitir que los servidores virtuales de un grupo utilicen sus propios parámetros de persistencia para crear sesiones persistentes, en lugar de heredar la configuración de persistencia de la configuración de grupo. Cuando este parámetro está habilitado, la persistencia no se puede establecer en el grupo de equilibrio de carga.

Cuando este parámetro está inhabilitado, los servidores virtuales del grupo heredan los parámetros de persistencia de la configuración del grupo.

Cuando se activa este parámetro en el grupo de equilibrio de carga, el dispositivo Citrix ADC vacía todas las entradas de persistencia correspondientes del grupo y los servidores virtuales miembros.

Valores posibles: ENABLED, DISABLED

Predeterminado: DISABLED

Ejemplo:


```
set lb group lb_grp1 -useVserverPersistency ENABLED
<!--NeedCopy-->
```

Servidor MasterVServer

Designe un servidor virtual como servidor virtual principal en su grupo de equilibrio de carga. Una vez designado, solo el servidor virtual principal puede crear las entradas persistentes utilizadas por el grupo.

Nota: Este parámetro solo se puede establecer si el parámetro UseVServerPersistency está habilitado.

Ejemplo:

```
set lb group lb_grp1 -masterVserver vs1
<!--NeedCopy-->
```

Ejemplo de configuración de uso compartido de sesiones persistentes mediante la interfaz de línea de comandos

Se crean los servidores virtuales

```
add lb vs vs1 http 10.1.10.11 80 -persistence rule -rule 'client.ip.
    src'

add lb vs vs2 radius 10.2.2.2 1812 -persistenceType rule -rule '
    Radius.req.avp(8).value.typecast_text_t'
<!--NeedCopy-->
```

Se crean los grupos.

```
add lb group lb_grp1 -persistenceType NONE -useVserverPersistency
    ENABLED
<!--NeedCopy-->
```

Un servidor virtual de un grupo se designa como servidor virtual principal.


```
set lb group lb_grp1  -masterVserver vs1
<!--NeedCopy-->
```

Los servidores virtuales están enlazados al grupo.

```
bind lb group lb_grp1 vs1
bind lb group lb_grp1 vs2
<!--NeedCopy-->
```

Para obtener más información, consulte Configuración del equilibrio de carga básico y configuración de grupos de persistencia.

Configurar el equilibrio de carga RADIUS con persistencia

August 20, 2021

El complejo entorno de red actual a menudo requiere coordinar una configuración de equilibrio de carga de gran volumen y gran capacidad con autenticación y autorización sólidas. Los usuarios de aplicaciones pueden conectarse a una VPN a través de puntos de acceso móviles, como conexiones DSL o por cable de nivel de consumidor, WiFi o incluso nodos de acceso telefónico. Esas conexiones suelen utilizar IP dinámicas, que pueden cambiar durante la conexión.

Si configura el equilibrio de carga RADIUS en el dispositivo Citrix ADC para admitir conexiones de cliente persistentes a los servidores de autenticación RADIUS, el dispositivo utiliza el inicio de sesión de usuario o el atributo RADIUS especificado en lugar de la IP del cliente como ID de sesión, dirigiendo todas las conexiones y registros asociados a esa en el mismo servidor RADIUS. Por lo tanto, los usuarios pueden iniciar sesión en su VPN desde ubicaciones de acceso móvil sin experimentar desconexiones cuando cambia la IP del cliente o el punto de acceso WiFi.

Para configurar el equilibrio de carga RADIUS con persistencia, primero debe configurar la autenticación RADIUS para su VPN. Para obtener información e instrucciones, consulte el capítulo Autenticación, Autorización, Auditoría (AAA) en Tráfico de aplicaciones AAA. Elija también la función Equilibrio de carga o Content Switching como base para la configuración y asegúrese de que la función elegida esté habilitada. El proceso de configuración con cualquiera de las funciones es casi el mismo.

A continuación, configure dos servidores virtuales de equilibrio de carga o dos servidores virtuales de conmutación de contenido, uno para controlar el tráfico de autenticación RADIUS y el otro para controlar el tráfico de cuentas RADIUS. A continuación, configure dos servicios, uno para cada servidor virtual de equilibrio de carga y vincule cada servidor virtual de equilibrio de carga a su servicio. Por

último, se crea un grupo de persistencia de equilibrio de carga y se establece el tipo de persistencia en regla.

Activación de la función Equilibrio de carga o Content Switching

Para utilizar la función Equilibrio de carga o Content Switching, primero debe asegurarse de que la función está habilitada. Si está configurando un nuevo dispositivo Citrix ADC que no se haya configurado previamente, ambas funciones ya están habilitadas, por lo que puede pasar a la sección siguiente. Si está configurando un dispositivo Citrix ADC con una configuración anterior en él y no está seguro de que la función que utiliza esté habilitada, debe hacerlo ahora.

- Para obtener instrucciones sobre cómo habilitar la función de equilibrio de carga, consulte Habilitación del equilibrio de carga.
- Para obtener instrucciones sobre cómo habilitar la función de cambio de contenido, consulte Habilitación de la conmutación

Configuración de Servidores Virtuales

Después de habilitar la función de equilibrio de carga o conmutación de contenido, debe configurar dos servidores virtuales para admitir la autenticación RADIUS:

- **Servidor virtual de autenticación RADIUS.** Este servidor virtual y su servicio asociado gestiona el tráfico de autenticación hacia el servidor RADIUS. El tráfico de autenticación consiste en conexiones asociadas con los usuarios que inician sesión en su aplicación protegida o red privada virtual (VPN).
- **Servidor virtual de cuentas RADIUS.** Este servidor virtual y su servicio asociado gestiona las conexiones contables al servidor RADIUS. El tráfico de cuentas consiste en conexiones que realizan un seguimiento de las actividades de un usuario autenticado en su aplicación protegida o VPN.

Importante: Debe crear un par de servidores virtuales de equilibrio de carga o un par de servidores virtuales de conmutación de contenido para utilizarlos en la configuración de persistencia RADIUS. No se pueden mezclar tipos de servidores virtuales.

Para configurar un servidor virtual de equilibrio de carga mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para crear un servidor virtual de equilibrio de carga y verificar la configuración:


```
add lb vserver <name> RADIUS <IP address> <port> -lbmethod TOKEN -rule
    <rule>

show lb vserver <name>
<!--NeedCopy-->
```

Para configurar un servidor virtual de equilibrio de carga existente, sustituya el `add lb virtual server` comando anterior por el `set lb vserver` comando, que toma los mismos argumentos.

Para configurar un servidor virtual de conmutación de contenido mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para crear un servidor virtual de conmutación de contenido y verificar la configuración:

```
add cs vserver <name> RADIUS <IP address> <port> -lbmethod TOKEN -rule
    <rule>

show cs vserver <name>
<!--NeedCopy-->
```

Para configurar un servidor virtual de conmutación de contenido existente, sustituya el `add cs vserver` comando anterior por el `set cs vserver` comando, que toma los mismos argumentos.

Ejemplo:

```
add lb vserver radius_auth_vs1 RADIUS 192.168.46.33 1812 -lbmethod
    TOKEN -rule CLIENT.UDP.RADIUS.USERNAME

add lb vserver radius_acct_vs1 RADIUS 192.168.46.34 1813 -lbmethod
    TOKEN -rule CLIENT.UDP.RADIUS.USERNAME

set lb vserver radius_auth_vs1 RADIUS 192.168.46.33 1812 -lbmethod
    TOKEN -rule CLIENT.UDP.RADIUS.USERNAME

set lb vserver radius_auth_vs1 RADIUS 192.168.46.34 1813 -lbmethod
    TOKEN -rule CLIENT.UDP.RADIUS.USERNAME
<!--NeedCopy-->
```


Para configurar un servidor virtual de equilibrio de carga o conmutación de contenido mediante la utilidad de configuración

Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales** o vaya a **Administración del tráfico > Cambio de contenido > Servidores virtuales>**y configure un servidor virtual.

Configuración de servicios

Después de configurar los servidores virtuales, debe configurar dos servicios, uno para cada uno de los servidores virtuales creados.

Nota: Una vez configurados, estos servicios se encuentran en el estado DISABLED hasta que el dispositivo Citrix ADC pueda conectarse a las direcciones IP de cuentas y autenticación del servidor RADIUS y supervisar su estado. Para obtener instrucciones, consulte Configuración de servicios.

Vinculación de servidores virtuales a servicios

Después de configurar los servicios, debe enlazar a continuación cada uno de los servidores virtuales que creó al servicio apropiado.Para obtener instrucciones, consulte Vinculación de servicios al servidor virtual.

Configuración de un grupo de persistencia para Radius

Después de vincular los servidores virtuales de equilibrio de carga a los servicios correspondientes, debe configurar la configuración de equilibrio de carga RADIUS para admitir la persistencia. Para ello, configure un grupo de persistencia de equilibrio de carga que contenga los servidores y servicios virtuales de equilibrio de carga RADIUS, y configure ese grupo de persistencia de equilibrio de carga para utilizar la persistencia basada en reglas. Se requiere un grupo de persistencia porque los servidores virtuales de autenticación y contabilidad son diferentes y el mensaje de autenticación y contabilidad para un solo usuario debe llegar al mismo servidor RADIUS. El grupo de persistencia permite utilizar la misma sesión para ambos servidores virtuales. Para obtener instrucciones, consulte Configuración de grupos de persistencia.

Configuración de RADIUS Shared Secret

A partir de la versión 12.0, un dispositivo Citrix ADC admite el secreto compartido RADIUS. Un cliente y un servidor RADIUS se comunican entre sí mediante un secreto compartido configurado en el cliente y en el servidor. Las transacciones entre un cliente RADIUS y un servidor se autentican mediante un secreto compartido. Este secreto también se utiliza para cifrar parte de la información del paquete RADIUS.

Casos de validación de clave secreta compartida RADIUS

La validación de la clave **secreta compartida RADIUS** se produce en los siguientes casos:

- **La clave secreta compartida RADIUS está configurada tanto para el cliente radius como para el servidor radius:** el dispositivo Citrix ADC utiliza la clave secreta RADIUS tanto para el lado cliente como para el servidor. Si la verificación se realiza correctamente, el dispositivo permite que el mensaje RADIUS pase. De lo contrario, descarta el mensaje RADIUS.
- **La clave secreta compartida RADIUS no está configurada para el cliente radius ni para el servidor radius:** el dispositivo Citrix ADC elimina el mensaje RADIUS, ya que la validación de clave secreta compartida no se puede realizar en un nodo que no tiene configurado radkey.
- **La clave secreta compartida RADIUS no está configurada tanto para el cliente RADIUS como para el servidor RADIUS:** el dispositivo Citrix ADC omite la validación de la clave secreta RADIUS y permite que los mensajes RADIUS pasen.

Puede configurar un secreto compartido RADIUS predeterminado o configurarlo por cliente o por subred. Se recomienda agregar una clave secreta compartida RADIUS para todas las implementaciones con directiva RADIUS configurada. El dispositivo utiliza la dirección IP de origen del paquete RADIUS para decidir qué secreto compartido utilizar. Puede configurar un cliente y un servidor RADIUS y el secreto compartido correspondiente de la siguiente manera:

En el símbolo del CLI, escriba:

```
1 add radiusNode <clientPrefix/Subnet> -radKey <Shared_secret_key>
2 <!--NeedCopy-->
```

Argumentos

Dirección IP

Dirección IP o subred del cliente RADIUS en formato CIDR. El dispositivo utiliza la dirección IP de origen de un paquete de solicitud entrante para que coincida con la dirección IP del cliente. En lugar de configurar una dirección IP de cliente, puede configurar la dirección de red del cliente. El prefijo más largo se compara para identificar el secreto compartido para una solicitud de cliente entrante.

Radkey

Secreto compartido entre el cliente, el dispositivo Citrix ADC y el servidor. Longitud máxima: 31.

```
1 add lb vserver radius_auth_vs1 RADIUS 192.168.46.33 1812 -lbmethod
     TOKEN -rule CLIENT.UDP.RADIUS.USERNAME
```



```
2
3 add lb vserver radius_acct_vs1 RADIUS 192.168.46.34 1813 -lbmethod
     TOKEN -rule CLIENT.UDP.RADIUS.USERNAME
4
5 add service radius_auth_service1 192.168.41.68 RADIUS 1812
6
7 add service radius_acct_service1 192.168.41.70 RADIUS 1813
8
9 bind lb vserver radius_auth_vs1 radius_auth_service1
10
11 bind lb vserver radius_acct_vs1 radius_acct_service[1-3]
12
13 add radiusNode 192.168.41.0/24 -radKey  serverkey123
14
15 add radiusNode 203.0.113.0/24 -radkey clientkey123
16 <!--NeedCopy-->
```

Se debe configurar un secreto compartido tanto para un cliente RADIUS como para un servidor. El comando es el mismo. La subred determina si el secreto compartido es para un cliente o para un servidor.

Por ejemplo, si la subred especificada es una subred de cliente, el secreto compartido es para el cliente. Si la subred especificada es una subred de servidor (192.168.41.0/24 en el ejemplo anterior), el secreto compartido es para el servidor.

Una subred de 0.0.0.0/0 implica que es el secreto compartido predeterminado para todos los clientes y servidores.

> **Nota:**
>
> Solo los métodos de autenticación PAP y CHAP son compatibles con el secreto compartido RADIUS.

Ver sesiones de persistencia

August 20, 2021

Puede ver las diferentes sesiones de persistencia que están en vigor globalmente o para un servidor virtual concreto.

> **Nota**: Un dispositivo Citrix ADC nCore utiliza varios núcleos de CPU para la gestión de paquetes. El núcleo de la CPU es propietario de todas las sesiones del dispositivo. Si el dispositivo recibe una solicitud para la que no existe una sesión, se crea una sesión y uno de los núcleos se designa

> como propietario de esa sesión.
>
> Es posible que las solicitudes subsiguientes que pertenecen a esa sesión no siempre lleguen y sean manejadas por el núcleo del propietario. En ese caso, la mensajería intercore garantiza que la información de la sesión en el núcleo del propietario esté siempre actualizada.

Sin embargo, cuando un núcleo recibe una solicitud que pertenece a una sesión de persistencia propiedad de otro núcleo, la mensajería internúcleo no actualiza el valor de tiempo de espera para la sesión de persistencia.

Por lo tanto, en el resultado de los comandos show lb PersistentSessions ejecutados sucesivamente, que muestran valores de tiempo de espera únicamente de los núcleos del propietario, el valor de tiempo de espera de una sesión de persistencia podría disminuir a 0 (cero), incluso si la sesión de persistencia permanece activa.

Para ver las sesiones de persistencia mediante la interfaz de línea de comandos

En el símbolo del sistema, para ver las sesiones de persistencia relacionadas con todos los servidores virtuales, escriba:

```
show lb persistentSessions [<vServer>]
<!--NeedCopy-->
```

En el símbolo del sistema, para ver las sesiones de persistencia relacionadas con un servidor virtual, escriba:

```
show lb persistentSessions <vServername>
<!--NeedCopy-->
```

Ejemplo:

```
show lb persistentSessions myVserver
<!--NeedCopy-->
```

Para ver las sesiones de persistencia mediante la GUI

Vaya a **Administración del tráfico** > **Sesiones persistentes del servidor virtual**.

Sesiones de persistencia claras

August 20, 2021

Es posible que tenga que borrar las sesiones de persistencia del dispositivo Citrix ADC si no se agana el tiempo de espera de las sesiones. Puede realizar una de las siguientes acciones:

- Borre todas las sesiones de todos los servidores virtuales a la vez.
- Borre todas las sesiones de un servidor virtual determinado a la vez.
- Borre una sesión en particular asociada a un servidor virtual determinado.

Para borrar una sesión de persistencia mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para borrar las sesiones de persistencia y verificar la configuración:

```
clear lb persistentSessions [<vServer> [-persistenceParam <string>]]

show persistentSessions <vServer>
<!--NeedCopy-->
```

Ejemplos:

Ejemplo 1 borra todas las sesiones de persistencia para el equilibrio de carga del servidor virtual lbvip1.

El ejemplo 2 muestra primero las sesiones de persistencia para el servidor virtual de equilibrio de carga lbvip1, borra la sesión con el parámetro de persistencia xls y, a continuación, muestra las sesiones de persistencia para comprobar que la sesión se ha borrado.

Ejemplo 1:

```
> clear persistentSessions lbvip1
 Done
> show persistentSessions
 Done
>
<!--NeedCopy-->
```

Ejemplo 2:


```
> show persistentSessions lbvip1
Type        SRC-IP    ...    PERSISTENCE-PARAMETER
RULE        0.0.0.0   ...    xls
RULE        0.0.0.0   ...    txt
RULE        0.0.0.0   ...    html
 Done
> clear persistentSessions lbvip1 -persistenceParam xls
 Done
> show persistentSessions lbvip1
Type        SRC-IP    ...    PERSISTENCE-PARAMETER
RULE        0.0.0.0   ...    txt
RULE        0.0.0.0   ...    html
 Done
>
<!--NeedCopy-->
```

Para borrar sesiones de persistencia mediante la utilidad de configuración

1. Vaya a **Administración del tráfico > Borrar sesiones persistentes**.

Anular la configuración de persistencia para servicios sobrecargados

August 20, 2021

Cuando se carga un servicio o no está disponible de otro modo, el servicio a los clientes se degrada. En este caso, es posible que tenga que configurar el dispositivo Citrix ADC para que reenvíe temporalmente a otros servicios las solicitudes que de otro modo se incluirían en la sesión de persistencia asociada al servicio sobrecargado. En otras palabras, es posible que tenga que anular la configuración de persistencia que está configurada para el servidor virtual de equilibrio de carga. Puede lograr esta funcionalidad estableciendo el parámetro skippersistency. Cuando se establece este parámetro de persistencia de saltos y si el servidor virtual recibe nuevas conexiones para un servicio sobrecargado, ocurre lo siguiente.

- El servidor virtual no tiene en cuenta las sesiones de persistencia existentes asociadas a ese servicio, hasta que el servicio vuelve a un estado en el que puede aceptar solicitudes.
- Las sesiones de persistencia asociadas con otros servicios no se ven afectadas.

Esta funcionalidad está disponible solo para servidores virtuales cuyo tipo es ANY o UDP.

En las configuraciones de equilibrio de carga del repetidor de rama, también debe configurar un monitor de carga y vincularlo al servicio. El monitor elimina el servicio de las decisiones posteriores de

equilibrio de carga hasta que la carga en el servicio se sitúa por debajo del umbral configurado. Para obtener información sobre cómo configurar un monitor de carga para el servidor virtual, consulte Descripción de los monitores de carga.

Puede configurar el servidor virtual para que realice una de las acciones siguientes con las solicitudes que de otro modo formarían parte de la sesión de persistencia:

- **Enviar cada solicitud a uno de los otros servicios.** El servidor virtual toma una decisión de equilibrio de carga y envía cada solicitud a uno de los otros servicios según el método de equilibrio de carga. Si todos los servicios están sobrecargados, las solicitudes se descartan hasta que un servicio esté disponible.

  Los servidores virtuales basados en comodines y direcciones IP admiten esta opción. Esta acción es apropiada para todas las implementaciones, incluidas las implementaciones en las que el servidor virtual está equilibrando la carga de dispositivos o firewalls de Branch Repeater.

- **Omitir la configuración del servicio de servidor virtual.** El servidor virtual no toma una decisión de equilibrio de carga. En cambio, simplemente une cada solicitud a un servidor físico en función de la dirección IP de destino de la solicitud.

  Solo los servidores virtuales comodín de tipo CUALQUIERA y UDP admiten la opción de omisión. Los servidores virtuales comodín tienen una combinación *:* IP y puerto. Esta acción es apropiada para implementaciones en las que está usando el servidor virtual para equilibrar la carga de dispositivos o firewalls repetidores de rama. En estas implementaciones, el dispositivo Citrix ADC reenvía primero una solicitud a un dispositivo repetidor de rama o firewall y, a continuación, reenvía la respuesta procesada a un servidor físico. El servidor virtual envía solicitudes directamente a sus direcciones IP de destino en las siguientes condiciones.

  - Puede configurar el servidor virtual para omitir la configuración del servicio del servidor virtual para servicios sobrecargados.
  - El dispositivo repetidor de sucursales o el firewall se sobrecargan.

  El servidor virtual envía solicitudes directamente a sus direcciones IP de destino hasta que el dispositivo repetidor de sucursales o el firewall puedan aceptar solicitudes.

Para anular la configuración de persistencia de los servicios sobrecargados mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para anular la configuración de persistencia de los servicios sobrecargados y verificar la configuración:

```
set lb vserver <name> -skippersistency <skippersistency>

show lb vserver <name>
```



```
<!--NeedCopy-->
```

Ejemplo

```
> set lb vserver mylbvserver -skippersistency ReLb
 Done
> show lb vserver mylbvserver
    mylbvserver (\*:\*) - ANY Type: ADDRESS
      . . .
      . . .
 Skip Persistency: ReLb
      . . .
 Done
>
<!--NeedCopy-->
```

Para anular la configuración de persistencia de los servicios sobrecargados mediante la GUI

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales** y seleccione el servidor virtual de tipo UDP o ANY.
2. En el panel Configuración avanzada, seleccione Configuración de tráfico y especifique el tipo de Omitir persistencia.

Solucionar problemas

August 20, 2021

- **Las estadísticas del dispositivo Citrix ADC VPX indican que el dispositivo ha alcanzado el límite de persistencia de sesión. Como resultado, las sesiones de persistencia están fallando. ¿Es posible aumentar el límite de persistencia de sesión?**

  Causa: el dispositivo Citrix ADC tiene el límite del sistema de 250.000 sesiones de persistencia para un núcleo.

  Resolución: Para resolver este problema, puede realizar cualquiera de las siguientes tareas:

  - Reducir el valor de tiempo de espera de persistencia
  - Aumentar el número de núcleos del dispositivo

- **Después de configurar la persistencia de la inserción de cookies en el dispositivo Citrix ADC, los usuarios informan de que las conexiones funcionan bien durante algún tiempo, pero luego comienzan a desconectarse. ¿Qué prácticas recomendadas debo seguir al configurar la persistencia?**

  Causa: De forma predeterminada, el valor de tiempo de espera para la persistencia de la inserción de cookies es de 120 segundos.

  Resolución: Cuando configure la persistencia para aplicaciones para las que no se puede determinar el tiempo de inactividad, establezca el valor de tiempo de espera de persistencia de inserción de cookies en 0. Con esta configuración, la conexión no se agotará.

- **Después de configurar un servidor virtual HTTP en el dispositivo Citrix ADC, necesito asegurarme de que un usuario siempre se conecta al mismo servidor para el contenido solicitado, por lo que configuré la persistencia de SourceIP. Ahora, aumentar el valor de tiempo de espera para la persistencia introduce latencia. ¿Cómo puedo aumentar el valor de tiempo de espera sin afectar el rendimiento?**

  Resolución: Considere usar la persistencia de inserción de cookies con el valor de tiempo de espera establecido en 0. Esta configuración habilita la configuración de persistencia de larga duración, ya que el dispositivo no especifica una hora para caducar la cookie.

- **Después de configurar la persistencia de la inserción de cookies en el dispositivo Citrix ADC, funciona como se esperaba cuando los clientes de la misma zona horaria acceden al contenido. Sin embargo, cuando un cliente de otra zona horaria intenta conectarse, la conexión se agotará inmediatamente.**

  Causa: Lapersistencia de la inserción de cookies basada en el tiempo funciona como se esperaba cuando un cliente de la misma zona horaria realiza una conexión. Sin embargo, cuando el equipo cliente y el dispositivo Citrix ADC están en diferentes zonas horarias, la cookie no es válida. Por ejemplo, cuando un cliente de la zona horaria EST envía una cookie a las 11:00 AM EST a un dispositivo Citrix ADC de la zona horaria PST, el dispositivo recibe la cookie a las 14:00 PM PST. Como resultado de la diferencia de tiempo, la cookie no es válida, y la conexión es inmediatamente agotada.

  Resolución: Establezca el valor de tiempo de espera para la persistencia de la inserción de cookies en 0.

- **Un dispositivo Citrix ADC se utiliza para equilibrar la carga de servidores de aplicaciones, como el servidor Oracle Weblogic. Para asegurarse de que los clientes obtienen conexiones persistentes a estos servidores, se configura la persistencia de SourceIP. Funciona como se esperaba cuando se realiza una conexión desde un equipo. Sin embargo, cuando los clientes ligeros intentan una conexión a través de un servidor Terminal Server y, como resultado, el dispositivo recibe solicitudes de varios clientes desde la misma dirección IP (la dirección IP de Terminal Server). Por lo tanto, las conexiones de todos los clientes ligeros**

se dirigen al mismo servidor de aplicaciones. ¿Es posible configurar la persistencia de solicitudes de clientes ligeros individuales en función de la dirección IP del cliente?

Causa: El dispositivo Citrix ADC recibe solicitudes del servidor Terminal Server y la dirección IP de origen de la solicitud sigue siendo la misma. Como resultado, el dispositivo no puede distinguir entre las solicitudes recibidas de los clientes ligeros y proporcionar persistencia según las solicitudes de los clientes ligeros.

Resolución: Para evitar este problema, puede configurar la persistencia de reglas basándose en algún valor de parámetro único para cada cliente ligero.

- **El dispositivo Citrix ADC se utiliza para equilibrar la carga de los servidores de la Interfaz Web. Al acceder a los servidores, el usuario recibe el mensaje de error "Error de estado". Además, cuando uno de los servidores de Interfaz Web está apagado o no está disponible, algunos de los usuarios reciben un mensaje de error.**

  Causa: La falta de persistencia en los servidores de la Interfaz Web puede dar lugar a mensajes de error cuando un usuario intenta conectarse al servidor.

  Resolución: Citrix recomienda especificar el método de persistencia de inserción de cookies en el dispositivo Citrix ADC al equilibrar la carga de los servidores de Interfaz Web.

Insertar atributos de cookie a las cookies generadas por ADC

August 20, 2021

Los administradores web pueden insertar otros atributos de cookie en las cookies generadas por el dispositivo Citrix ADC. Estos atributos de cookies adicionales ayudan a aplicar las directivas requeridas para las cookies generadas por ADC en función del patrón de acceso a la aplicación.

Las siguientes funciones utilizan las cookies generadas por ADC para lograr la persistencia.

- Persistencia de cookies de equilibrio de carga
- Persistencia de cookies de grupo de equilibrio de carga
- Persistencia del sitio GSLB
- Persistencia de cookies de cambio de contenido

Puede insertar otros atributos de cookie en las cookies generadas por el ADC mediante los siguientes parámetros:

- **literalADCCookieAttribute:** Agregue otros atributos de cookie a la cookie generada por ADC, como cadena.
- **computedAdcCookieAttribute:** utilice una variable ADC ns para anexar condicionalmente atributos de cookie a la cookie generada por ADC, en función de los atributos de cliente o servidor, por ejemplo, la versión del agente de usuario.

> **Nota**
>
> No puede configurar tanto el atributo de cookie ADC literal como el atributo de cookie ADC computado, simultáneamente en el parámetro de equilibrio de carga o en un único perfil de equilibrio de carga.

Caso de uso: Configurar el atributo de cookie de SameSite

Cada cookie tiene un dominio asociado a ella. Cuando el dominio de una cookie coincide con el dominio del sitio web en la barra de direcciones del usuario, se considera un contexto del mismo sitio (o de primera parte). Si el dominio asociado a una cookie coincide con un servicio externo y no con el sitio web en la barra de direcciones del usuario, se considera un contexto entre sitios (o de terceros).

El atributo **SameSite** indica al explorador si la cookie se puede utilizar para el contexto entre sitios o solo para el contexto del mismo sitio. Además, si se pretende acceder a una aplicación en el contexto entre sitios, solo puede hacerlo a través de la conexión HTTPS. Para obtener más información, consulte RFC6265.

Hasta febrero de 2020, la propiedad **SameSite** no se estableció explícitamente en Citrix ADC. El explorador tomó el valor predeterminado None y no afectó a las implementaciones de Citrix ADC.

Sin embargo, con la actualización de ciertos exploradores, como Google Chrome 80, se produce un cambio en el comportamiento predeterminado entre dominios de las cookies. El atributo **SameSite** se puede establecer en uno de los siguientes valores. El valor predeterminado para Google Chrome se establece en Lax.

- **Ninguno:** indica que el explorador debe utilizar una cookie en contexto entre sitios solo en conexiones seguras.
- **Lax:** indica que el explorador debe utilizar una cookie para las solicitudes en el mismo contexto del sitio. En el contexto entre sitios, solo los métodos HTTP seguros como la solicitud GET pueden usar la cookie.
- **Estricta:** utilice la cookie solo en el contexto del mismo sitio.

Si no hay ningún atributo SameSite en la cookie, Google Chrome asume la funcionalidad de SameSite = Lax.

> **Nota**
>
> Para determinadas versiones de otros exploradores, el valor predeterminado del atributo SameSite podría establecerse en **Ninguno**. En algunas versiones del explorador, "SameSite = none" se puede tratar de manera diferente. Por ejemplo, los siguientes exploradores rechazan una cookie con "SameSite = none":

- Versiones de Chrome de Chrome 51 a Chrome 66 (incluido en ambos extremos)
- Versiones del explorador UC en Android anteriores a la versión 12.13.2

Configurar cookies generadas por ADC

Para configurar los atributos de cookies generados por ADC, debe realizar lo siguiente:

1. Crear un servidor virtual de equilibrio de carga
2. Establezca los atributos de Cookie ADC para el servidor virtual de equilibrio de carga, ya sea a través de parámetros LB o perfil LB.
3. Si utiliza un perfil LB, defina el perfil LB en un servidor virtual de equilibrio de carga.
4. Si decide utilizar el atributo de cookies ADC computado, configure la directiva de reescritura relacionada.

> **Nota**
>
> Si un perfil LB está enlazado a un servidor virtual LB, se tiene en cuenta la configuración del parámetro de perfil en lugar de la configuración global de parámetros LB.

Puede establecer los atributos de cookies generados por ADC mediante los siguientes métodos:

- Configuración de los atributos de cookie ADC en los parámetros de equilibrio de carga
- Configuración de los atributos de cookie ADC en el perfil de equilibrio de carga

Configuración de los atributos de cookie ADC en los parámetros de equilibrio de carga mediante la CLI

Para aplicar una directiva uniformemente a las cookies generadas por ADC de todas las aplicaciones configuradas en el dispositivo Citrix ADC, puede establecer el atributo cookie ADC en los parámetros LB globales.

La configuración **Literal ADC Cookie Atributo** le permite insertar incondicionalmente los atributos de cookie en la cookie generada por ADC.

En el símbolo del sistema, escriba:

```
set lb parameter -LiteralADCCookieAttribute <string>
<!--NeedCopy-->
```

Ejemplo:

```
set lb parameter -LiteralADCCookieAttribute SameSite=None
<!--NeedCopy-->
```


La configuración del **atributo de cookie ADC computado** le permite insertar condicionalmente los atributos de cookie, basados en los atributos del cliente o del servidor, en la cookie generada por ADC.

En el símbolo del sistema, escriba:

```
set lb parameter -ComputedADCCookieAttribute <ns variable>
<!--NeedCopy-->
```

Ejemplo:

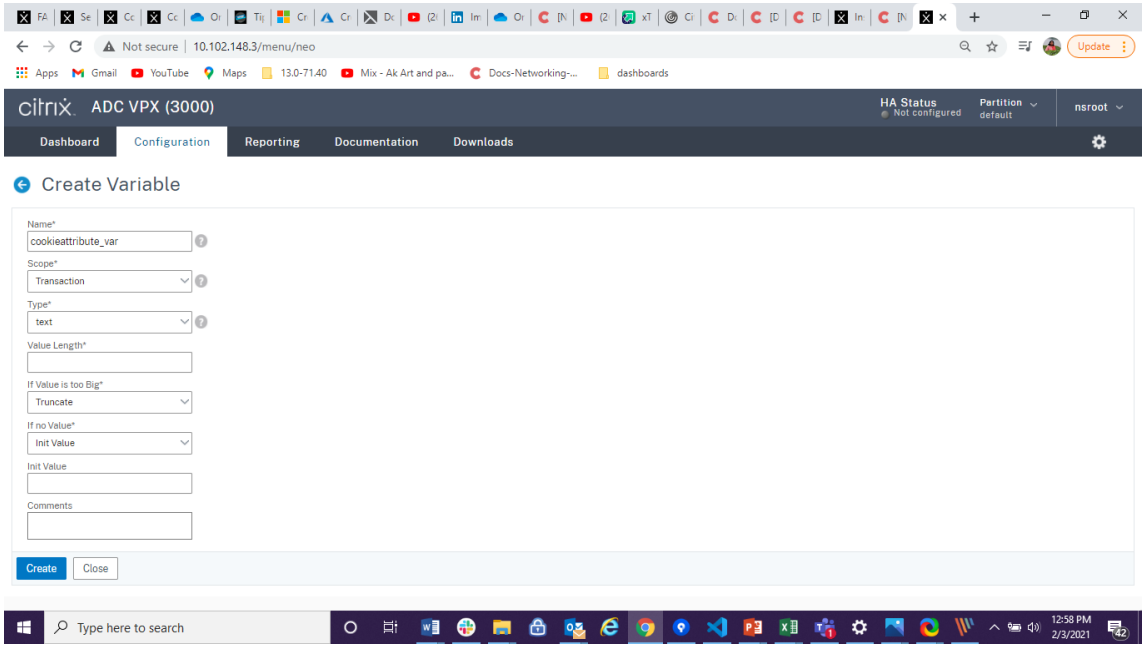
```
add ns variable cookieattribute_var -type "text(100)" -scope
    transaction
set lb parameter -ComputedADCCookieAttributE "$cookieattribute_var"
add ns assignment samesiteassign -variable "$cookieattribute_var" -set
    ""SameSite=None""

add policy expression pol_iphone "(HTTP.REQ.HEADER("User-Agent").
    CONTAINS("iP") && (HTTP.REQ.HEADER("User-Agent").REGEX_SELECT(re/OS
    \d+\\_/).REGEX_SELECT(re/\d+/).TYPECAST_NUM_T(DECIMAL).EQ(12).
    typecast_text_t ALT "false").eq("true"))"
add policy expression pol_chrome "(HTTP.REQ.HEADER("User-Agent").
    CONTAINS("Chrom") && (HTTP.REQ.HEADER("User-Agent").REGEX_SELECT(re/
    Chrom.*\d+./).REGEX_SELECT(re/\d+/).TYPECAST_NUM_T(DECIMAL).BETWEEN
    (51,66).typecast_text_t ALT "false").eq("true"))"
add rewrite policy exception_samesite_attribute "pol_iphone ||
    pol_chrome " NOREWRITE
add rewrite policy append_samesite_attribute true samesiteassign

bind rewrite global exception_samesite_attribute 90 110 -type
    RES_OVERRIDE
bind rewrite global append_samesite_attribute 100 110 -type
    RES_OVERRIDE
<!--NeedCopy-->
```

Configurar variables mediante la interfaz gráfica de usuario

1. Vaya a **AppExpert > Variables**y haga clic en **Agregar**.
2. En la página **Crear Variable**, seleccione **Ámbito** como **transacción** y **Tipo** como **texto** en el menú desplegable.

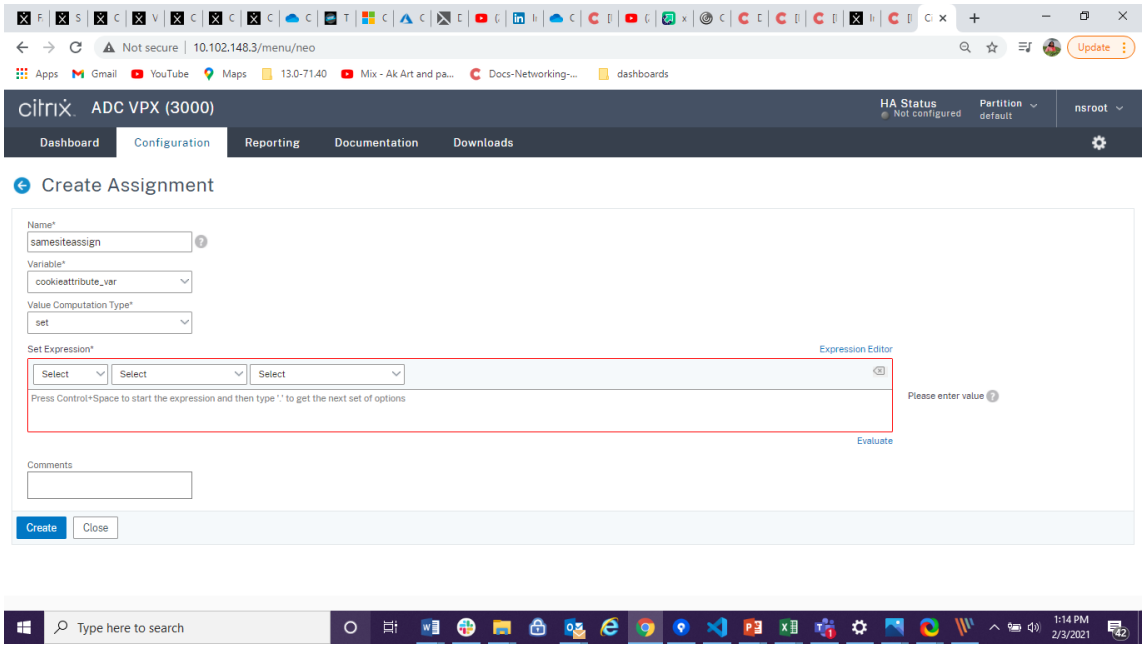


3. Introduzca otros detalles y haga clic en **Crear**.

Crear una asignación mediante la interfaz gráfica de usuario

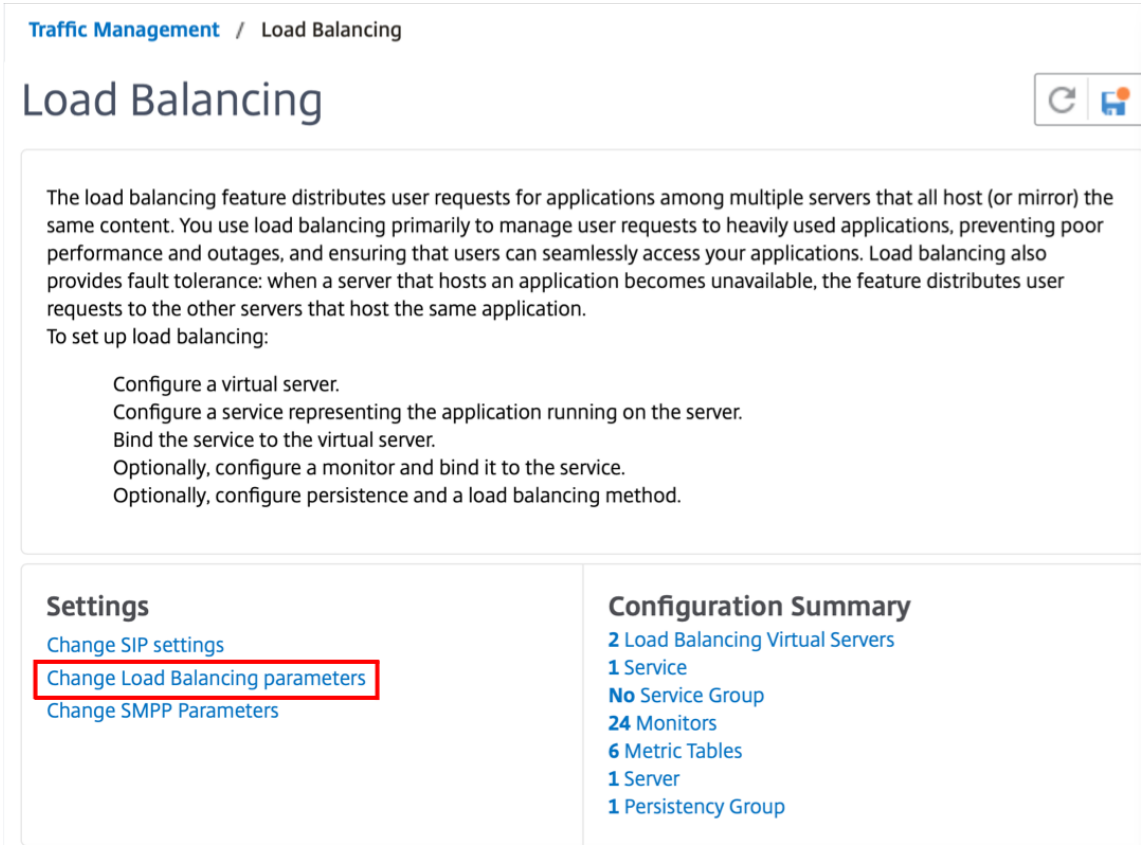
Después de configurar una variable, puede asignar un valor o especificar la operación que se va a realizar en la variable creando una asignación.

1. Vaya a **AppExpert > Asignaciones**y haga clic en **Agregar**.
2. En la página **Crear asignación**, introduzca los detalles y haga clic en **Crear**.



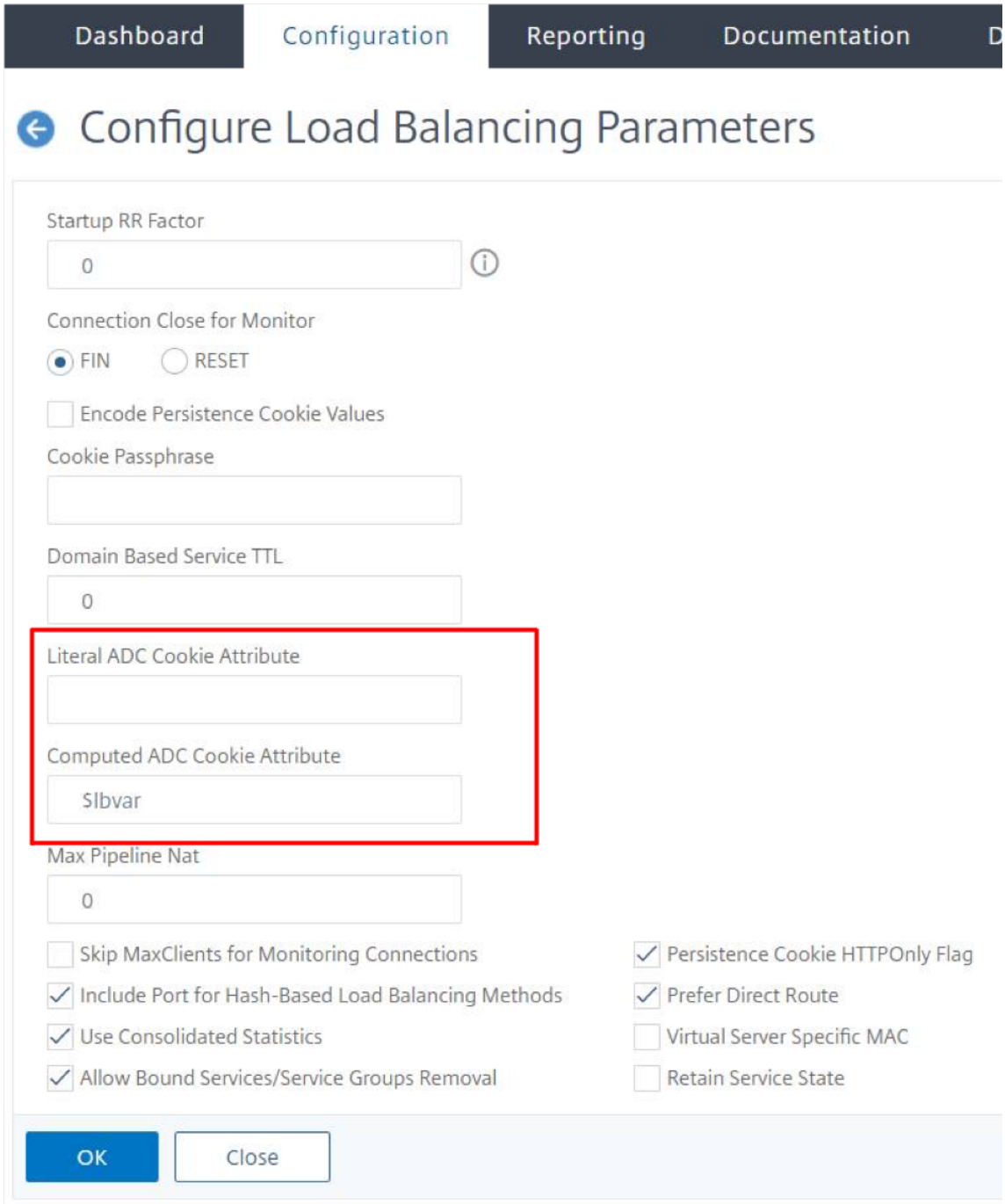
Configuración de los atributos de cookie ADC en los parámetros de equilibrio de carga mediante la GUI

1. Vaya a **Gestión de tráfico > Equilibrio de carga > Cambiar parámetros de Equilibrio de carga**.



2. En el panel **Configurar parámetros de equilibrio de carga**, introduzca los valores adecuados para cualquiera de los campos según su requisito:

   - **Atributo de cookie ADC literal**
   - **Atributo de cookie ADC calculado**



3. Haga clic en **Aceptar**.

Configuración de los atributos de cookie ADC en el perfil de equilibrio de carga mediante la CLI

Para aplicar una directiva para una aplicación específica configurada en el dispositivo Citrix ADC, puede establecer los parámetros de atributo de cookie en el perfil LB vinculado al servidor virtual LB específico de la aplicación.

La configuración **Literal ADC Cookie Atributo** en el perfil LB le permite insertar incondicionalmente los atributos de cookie en la cookie generada por ADC que es específica de un servidor virtual.

En el símbolo del sistema, escriba:

```
add lb profile <profile name> -LiteralADCCookieAttribute <string>
<!--NeedCopy-->
```

Ejemplo:

```
add lb profile LB-Vserver-Profile-1 -LiteralADCCookieAttribute SameSite
    =None
add lb vserver LB-VServer-1 SSL 10.102.148.37 443 -persistenceType
    COOKIEINSERT -lbprofilename LB-Vserver-Profile-1
<!--NeedCopy-->
```

La configuración del **atributo de cookie ADC computado** en el perfil LB le permite insertar condicionalmente los atributos de cookie basados en los atributos de cliente o servidor, en la cookie generada por ADC. A continuación, configure este perfil LB en un servidor virtual LB.

En el símbolo del sistema, escriba:

```
add lb profile <profile name> -ComputedADCCookieAttribute <ns variable>
<!--NeedCopy-->
```

Ejemplo:

```
add ns variable cookieattribute_var -type "text(100)" -scope
    transaction
add ns assignment samesiteassign -variable "$cookieattribute_var" -set
    ""SameSite=None""
add lb profile LB-Vserver-Profile-1 -ComputedADCCookieAttributE "
    $cookieattribute_var"

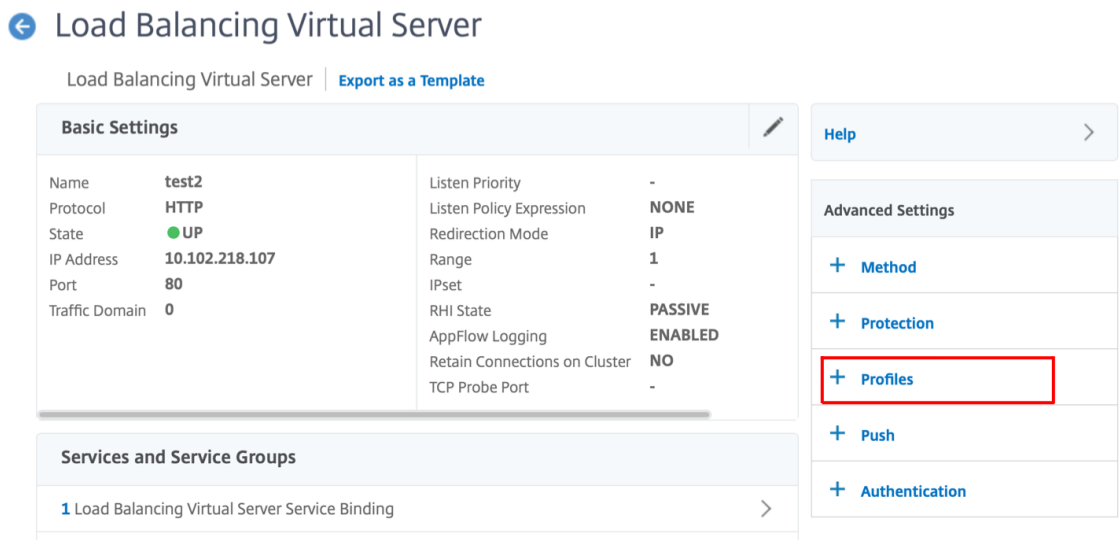
add policy expression pol_iphone "(HTTP.REQ.HEADER("User-Agent").
    CONTAINS("iP") && (HTTP.REQ.HEADER("User-Agent").REGEX_SELECT(re/OS
    \d+\\_/).REGEX_SELECT(re/\d+/).TYPECAST_NUM_T(DECIMAL).EQ(12).
    typecast_text_t ALT "false").eq("true"))"
add policy expression pol_chrome "(HTTP.REQ.HEADER("User-Agent").
    CONTAINS("Chrom") && (HTTP.REQ.HEADER("User-Agent").REGEX_SELECT(re/
```



```
    Chrom.*\d+./).REGEX_SELECT(re/\d+/).TYPECAST_NUM_T(DECIMAL).BETWEEN
    (51,66).typecast_text_t ALT "false").eq("true"))"
7 add rewrite policy exception_samesite_attribute "pol_iphone ||
    pol_chrome " NOREWRITE
8 add rewrite policy append_samesite_attribute true samesiteassign
9
10 add lb vserver LB-VServer-1 SSL 10.102.148.37 443 -persistenceType
    COOKIEINSERT -lbprofilename LB-Vserver-Profile-1
11 bind lb vserver LB-VServer-1 -policyName exception_samesite_attribute -
    priority 90 -gotoPriorityExpression 110 -type RESPONSE
12 bind lb vserver LB-VServer-1 -policyName append_samesite_attribute -
    priority 100 -gotoPriorityExpression 110 -type RESPONSE
13 <!--NeedCopy-->
```

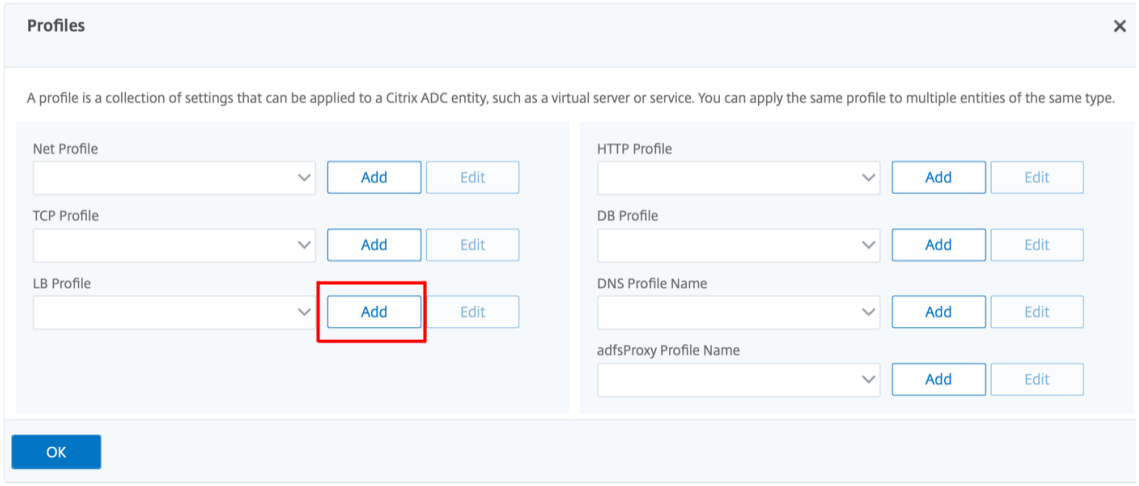
Configuración de los atributos Cookie ADC en el perfil de equilibrio de carga mediante la GUI

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. Seleccione un servidor virtual y haga clic en **Modificar**.
3. En la sección **Configuración avanzada**, haga clic en **Agregar perfiles**.



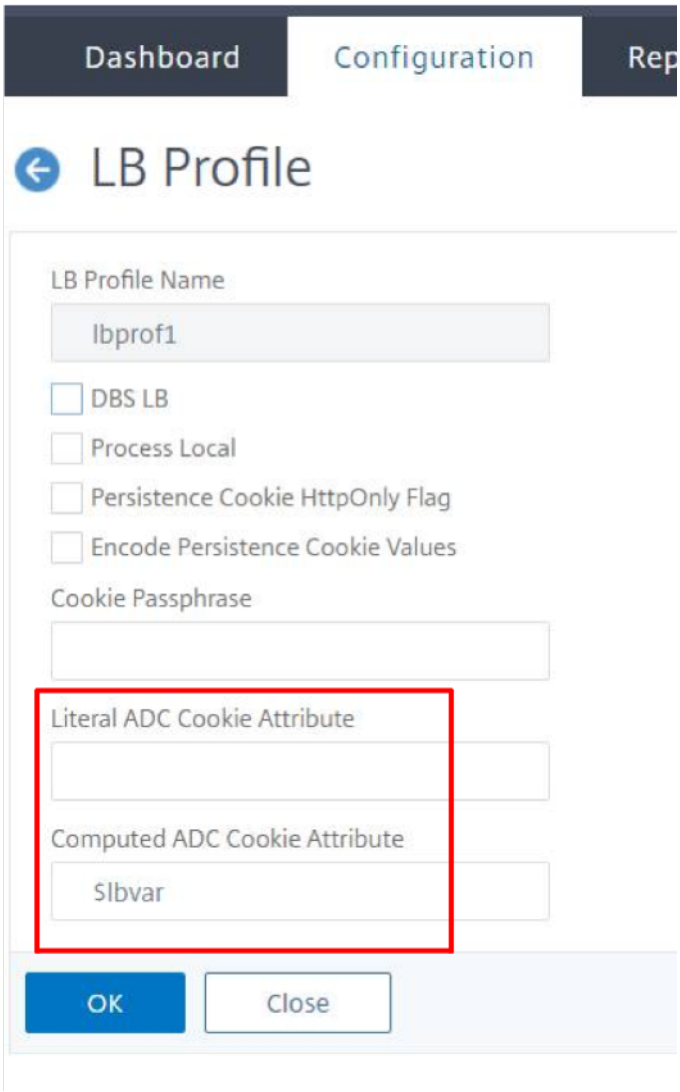
4. En la sección **Perfiles**, haga clic en **Agregar** para crear un perfil LB.

   Si ya ha creado un perfil, selecciónelo en el menú desplegable **Perfil de LB** .



5. En el panel **Perfil LB**, introduzca los valores adecuados para cualquiera de los campos según su requisito:

- **Atributo de cookie ADC literal**
- **Atributo de cookie ADC calculado**



1. Haga clic en **Aceptar**.
2. Establezca el perfil LB creado en el servidor virtual LB creado en el **paso 1**.

Verificar la configuración de la variable ns

Para comprobar que la variable ADC ns está configurada adecuadamente en parámetros LB o perfil LB, utilice los comandos show lb parámetro o show lb profile.

En la tabla siguiente se enumeran los diversos mensajes de advertencia y su causa, cuando la variable ns no está configurada correctamente.

Mensaje de advertencia	Razones
La variable NS no está configurada. Configúrelo con tipo text () y transacción de ámbito para la variable	La variable NS aún no está configurada.
El ámbito de la variable NS configurada no es transacción.	La variable está configurada, pero el ámbito no se establece en “transacción”.
El tipo de variable no es Text ().	La variable está configurada pero el tipo no se establece en “Texto”.
El valor máximo configurado para la variable NS es mayor que 255.	El valor configurado para la variable NS es superior a 255 caracteres. **Nota:** Se puede agregar una longitud máxima de 255 caracteres a una cookie generada por ADC. Los caracteres que superan la longitud máxima se truncan.

Salida de muestra

En el ejemplo siguiente, se muestra el mensaje de advertencia cuando la variable ns no está configurada.

```
set lb parameter -ComputedADCCookieAttribute ”$lbvar”

Warning: NS Variable is not configured. Please configure it with type
    text() and scope transaction
Done
<!--NeedCopy-->
```

El mensaje de advertencia se muestra en la siguiente salida del `show lb parameter` comando.

```
show lb parameter

Global LB parameters:
Persistence Cookie HttpOnly Flag: ENABLED
Use Encrypted Persistence Cookie: DISABLED
Use Port For Hash LB: YES
Prefer direct route: YES
Retain Service State: OFF
Start RR Factor: 0
```



```
Skip Maxclient for Monitoring: DISABLED
Monitor Connection Close: FIN
Use consolidated stats for LeastConnection: YES
Allow mac mode based vserver to pick thereturn traffic from services:
    DISABLED
Allow bound service removal: ENABLED
TTL for Domain Based Server: 0 secs

Citrix ADC Cookie Variable Name: $lbvar(NS Variable is not configured.
    Please configure it with type text() and scope transaction)

Done
<!--NeedCopy-->
```

Configuración de ejemplo para insertar atributos de cookies en la implementación de GSLB

La siguiente configuración de ejemplo se aplica a la persistencia del sitio configurada en los servicios GSLB correspondientes a un servidor virtual LB. Para agregar algunos atributos de cookies adicionales a las cookies GSLB, realice la siguiente configuración.

- Establezca los atributos de cookie ADC en el perfil LB (LB-Vserver-Profile-1).
- Establezca el valor del atributo de cookie de ADC literal, por ejemplo “SameSite=None”, en el perfil LB.
- Establezca el perfil LB en el servidor virtual de equilibrio de carga (LB-VServer-1), que representa el servicio GSLB.

```
add gslb vserver GSLB-VServer-1 SSL -backupLBMethod ROUNDROBIN -
    tolerance 0 -appflowLog DISABLED
add gslb site site1 10.102.148.4 -publicIP 10.102.148.4
add gslb service site1_gsvc1 10.102.148.35 SSL 443 -publicIP
    10.102.148.35 -publicPort 443 -maxClient 0 -siteName site1 -
    sitePersistence HTTPRedirect -sitePrefix ss1 -cltTimeout 180 -
    svrTimeout 360 -downStateFlush ENABLED

bind gslb vserver GSLB-VServer-1 -serviceName site1_gsvc1
bind gslb vserver GSLB-VServer-1 -domainName www.gslb.com -TTL 5

add service service-1 10.102.84.140 SSL 443

add lb profile LB-Vserver-Profile-1 -LiteralADCCookieAttribute SameSite
    =None
```



```
add lb vserver LB-VServer-1 SSL 10.102.148.37 443 -persistenceType
    COOKIEINSERT -lbprofilename LB-Vserver-Profile-1

bind lb vserver LB-VServer-1 service-1
<!--NeedCopy-->
```

> **Nota**
>
> También puede insertar condicionalmente los atributos de cookie mediante el atributo de cookie de ADC computado.

Configuración de ejemplo para insertar el atributo de cookie en la implementación de cambio de contenido

La siguiente configuración de ejemplo se aplica cuando se alojan varias aplicaciones detrás de un servidor virtual de cambio de contenido. Para aplicar la misma directiva a todas las aplicaciones, vincule las directivas de reescritura al servidor virtual de cambio de contenido en lugar del servidor virtual LB, de la siguiente manera:

- Establezca los atributos de cookie ADC en los parámetros LB.

  > **Nota:**
  >
  > También puede establecer los atributos de la cookie ADC en el perfil LB.

- Configure la variable ns (cookieattribute_var) de Tipo establecido en Texto y Ámbito establecido en Transacción.
- Establezca el atributo de cookie de ADC computado en los parámetros LB globales mediante la variable ns.
- Establezca las directivas de reescritura (exception_samesite_attribute y append_samesite_attribute) en los servidores virtuales de cambio de contenido para insertar los atributos de cookie.

```
add ns variable cookieattribute_var -type "text(100)" -scope
    transaction
set lb parameter -ComputedADCCookieAttributE "$cookieattribute_var"
add ns assignment samesiteassign -variable "$cookieattribute_var" -set
    ""SameSite=None""

add policy expression pol_iphone "(HTTP.REQ.HEADER("User-Agent").
    CONTAINS("iP") && (HTTP.REQ.HEADER("User-Agent").REGEX_SELECT(re/OS
    \d+\\_/).REGEX_SELECT(re/\d+/).TYPECAST_NUM_T(DECIMAL).EQ(12).
    typecast_text_t ALT "false").eq("true"))"
```



```
6  add policy expression pol_chrome "(HTTP.REQ.HEADER("User-Agent").
       CONTAINS("Chrom") && (HTTP.REQ.HEADER("User-Agent").REGEX_SELECT(re/
       Chrom.*\d+./).REGEX_SELECT(re/\d+/).TYPECAST_NUM_T(DECIMAL).BETWEEN
       (51,66).typecast_text_t ALT "false").eq("true"))"
7  add rewrite policy exception_samesite_attribute "pol_iphone ||
       pol_chrome " NOREWRITE
8  add rewrite policy append_samesite_attribute true samesiteassign
9
10 add lb vserver LB-VServer-1 SSL 10.102.148.35 443
11 add lb vserver LB-VServer-2 SSL 10.102.148.36 443
12
13 add cs vserver CS-VServer-1 SSL 10.102.148.42 443 -persistenceType
       COOKIEINSERT
14
15 add cs action act1 -targetLBVserver v1
16 add cs action act2 -targetLBVserver v2
17 add cs policy CS-policy-1 -rule "HTTP.REQ.URL.CONTAINS("file1.html")" -
       action act1
18 add cs policy CS-policy-2 -rule "HTTP.REQ.URL.CONTAINS("file2.html")" -
       action act2
19
20 bind cs vserver CS-VServer-1 -policyName CS-policy-1 -priority 1
21 bind cs vserver CS-VServer-1 -policyName CS-policy-2 -priority 2
22
23 bind cs vserver -policyname exception_samesite_attribute 90 110 -type
       RES_OVERRIDE
24 bind cs vserver -policyname append_samesite_attribute 100 110 -type
       RES_OVERRIDE
25 <!--NeedCopy-->
```

Personalizar una configuración de equilibrio de carga

August 20, 2021

Después de configurar una configuración básica de equilibrio de carga, puede realizar varias modificaciones para que distribuya la carga exactamente como sea necesario. La función de equilibrio de carga es compleja. Puede modificar los elementos básicos siguiendo uno o varios de los siguientes procedimientos:

- Cambio del algoritmo de equilibrio de carga
- Configuración de grupos de equilibrio de carga y uso de ellos para crear la configuración de equilibrio de carga

- Configuración de conexiones cliente-servidor persistentes
- Configuración del modo de redirección
- Asignación de pesos diferentes a distintos servicios que tienen capacidades diferentes.

El algoritmo de equilibrio de carga predeterminado del dispositivo Citrix ADC es el método de menor conexión. En el método de menor conexión, el dispositivo envía cada conexión entrante al servicio que actualmente gestiona el menor número de conexiones. Puede especificar diferentes algoritmos de equilibrio de carga, cada uno de los cuales se adapta a diferentes condiciones.

Para acomodar aplicaciones como carritos de compra, que requieren que todas las solicitudes del mismo usuario se dirijan al mismo servidor, puede configurar el dispositivo para mantener conexiones persistentes entre clientes y servidores. También puede especificar la persistencia para un grupo de servidores virtuales. La persistencia permite al dispositivo dirigir las solicitudes de cliente individuales al mismo servicio, independientemente del servidor virtual del grupo que reciba la solicitud del cliente.

Puede habilitar y configurar el modo de redirección que utiliza el dispositivo al redirigir las solicitudes de los usuarios, eligiendo entre el reenvío basado en IP y el reenvío basado en MAC. También puede asignar ponderaciones a distintos servicios, especificando qué porcentaje de carga entrante debe dirigirse a cada servicio. La asignación de pesos le permite incluir servidores con capacidades diferentes en la misma configuración de equilibrio de carga sin;

- sobrecargar los servidores de menor capacidad o
- lo que permite que los servidores de mayor capacidad permanezquen inactivos.

Personalizar el algoritmo hash para la persistencia en los servidores virtuales

August 20, 2021

El dispositivo Citrix ADC utiliza algoritmos basados en hash para mantener la persistencia en los servidores virtuales. De forma predeterminada, el método de equilibrio de carga basado en hash utiliza un valor hash de la dirección IP y el número de puerto del servicio. Si un servicio está disponible en diferentes puertos en el mismo servidor, el algoritmo genera diferentes valores hash. Por lo tanto, diferentes servidores virtuales de equilibrio de carga pueden enviar solicitudes para la misma aplicación a diferentes servicios, rompiendo la pseudo-persistencia.

Como alternativa al uso del número de puerto para generar el valor hash, puede especificar un identificador hash único para cada servicio. Para un servicio, se debe especificar el mismo valor de identificador de hash en todos los servidores virtuales. Si un servidor físico sirve más de un tipo de aplicación, cada tipo de aplicación debe tener un identificador hash único.

El algoritmo para calcular el valor hash para un servicio funciona de la siguiente manera:

- De forma predeterminada, una configuración global especifica el uso del número de puerto en un cálculo hash.
- Si configura un identificador hash para un servicio, se utiliza y el número de puerto no lo es, independientemente de la configuración global.
- Si no configura un identificador hash, pero cambia el valor predeterminado de la configuración global para que no especifique el uso del número de puerto, el valor hash se basa únicamente en la dirección IP del servicio.
- Si no configura un identificador hash o cambia el valor predeterminado de la configuración global para utilizar el número de puerto, el valor hash se basa en la dirección IP y el número de puerto del servicio.

También puede especificar identificadores hash cuando utilice la CLI para enlazar servicios a un grupo de servicios. En la utilidad de configuración, puede abrir un grupo de servicios y agregar identificadores hash en la ficha Miembros.

Para cambiar la configuración global use-port-number mediante la CLI

En el símbolo del sistema, escriba:

```
set lb parámetro -UsePortForHashLB (YES NO)
```

Ejemplo:

```
> set lb parameter -usePortForHashLb NO
 Done
>show lb parameter
Global LB parameters:
        Persistence Cookie HttpOnly Flag: DISABLED
        Use port for hash LB: NO
 Done
<!--NeedCopy-->
```

Para cambiar la configuración global use-port-number mediante la interfaz gráfica de usuario

1. Vaya a Administración del tráfico > Equilibrio de carga > Configurar parámetros de Equilibrio de carga.
2. Seleccione o desactive Usar puerto para métodos LB basados en hash.

Para crear un nuevo servicio y especificar un identificador hash para un servicio mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para establecer el ID de hash y verificar la configuración:

add service < name > (< ip >	< serverName > < positive_integer >) < serviceType > < port > -Hashid

```
show service <name>
<!--NeedCopy-->
```

Ejemplo:

```
> add service flbkng 10.101.10.1 http 80 -hashId 12345
 Done
>show service flbkng
        flbkng (10.101.10.1:80) - HTTP
        State: DOWN
        Last state change was at Thu Nov  4 10:14:52 2010
        Time since last state change: 0 days, 00:00:15.990
        Server Name: 10.101.10.1
        Server ID : 0   Monitor Threshold : 0

        Down state flush: ENABLED
        Hash Id: 12345

1)      Monitor Name: tcp-default
                State: DOWN     Weight: 1

 Done
<!--NeedCopy-->
```

Para especificar un identificador hash para un servicio existente mediante la CLI

Escriba el comando set service, el nombre del servicio y **-hashid** seguido del valor de ID.

Para especificar un identificador hash al agregar un miembro del grupo de servicios

Para especificar un identificador hash para cada miembro que se agregará al grupo y verificar la configuración, en el símbolo del sistema, escriba los comandos siguientes (Asegúrese de especificar un HaShid único para cada miembro.):

```
bind servicegroup <serviceGroupName> <memberName> <port> -hashId <
   positive_integer>

show servicegroup <serviceGroupName>
<!--NeedCopy-->
```

Ejemplo:

```
 bind servicegroup http_svc_group 10.102.27.153 80 -hashId 2222222

>show servicegroup SRV
        SRV - HTTP
        State: ENABLED  Monitor Threshold : 0
        ...

        1)          1.1.1.1:80   State: DOWN     Server Name: 1.1.1.1
              Server ID: 123  Weight: 1
        Hash Id: 32211

                Monitor Name: tcp-default       State: DOWN
        ...

        2)          2.2.2.2:80   State: DOWN     Server Name: 2.2.2.2
              Server ID: 123  Weight: 1
        Hash Id: 12345

                Monitor Name: tcp-default       State: DOWN
        ...
Done

<!--NeedCopy-->
```


Para especificar un identificador hash para un servicio mediante la interfaz gráfica de usuario

1. Vaya a Administración de Tráfico > Equilibrio de carga > Servicios.
2. Cree un nuevo servicio o abra un servicio existente y especifique el ID de hash.

Para especificar un identificador hash para un miembro del grupo de servicios ya configurado mediante la interfaz gráfica de usuario

1. Vaya a Administración del tráfico > Equilibrio de carga > Grupos de servicio.
2. Abra un miembro y escriba un ID de hash único.

Configurar el modo de redirección

October 5, 2021

El modo de redirección configura el método utilizado por un servidor virtual para determinar a dónde reenviar el tráfico entrante. El dispositivo Citrix ADC admite los siguientes modos de redirección. Antes de reenviar la solicitud a un servidor, los modos de redirección funcionan de la siguiente manera:

- Reenvío basado en IP (opción predeterminada): La dirección IP de destino se cambia a la dirección IP del servidor.
- Reenvío basado en MAC: La dirección MAC de destino se cambia a la dirección MAC del servidor. Sin embargo, la dirección IP de destino no cambia. El modo de redirección basado en Mac se utiliza principalmente en implementaciones de equilibrio de carga de firewall.
- Basado en IP TUNNEL: Se realiza una encapsulación IP en IP para los paquetes IP del cliente. En los encabezados IP externos, la dirección IP de destino se establece en la dirección IP del servidor y la dirección IP de origen se establece en la IP de subred (SNIP). Los paquetes IP del cliente no se modifican. Esto se aplica tanto a los paquetes IPv4 como a los IPv6.
- Basado en ID de TOS: El ID de TOS del servidor virtual está codificado en el campo TOS del encabezado IP.

Puede utilizar la opción IP TUNNEL o TOS para implementar Direct Server Return (DSR). Para obtener más información, consulte:

- Configurar el modo DSR al utilizar TOS
- Configurar el equilibrio de carga en modo DSR para redes IPv6 mediante el campo TOS
- Configurar el equilibrio de carga en modo DSR mediante IP sobre IP

Puede configurar el reenvío basado en MAC en redes que utilizan topología DSR, equilibrio de carga de vínculos o equilibrio de carga de firewall. Para obtener más información sobre el reenvío basado

en MAC para el equilibrio de carga, consulte Configurar MBF para la configuración del equilibrio de carga.

Para configurar el modo de redirección mediante la CLI

En el símbolo del sistema, escriba:

```
set lb vserver <name> -m <RedirectionMode>
<!--NeedCopy-->
```

Ejemplo:

```
set lb vserver Vserver-LB-1 -m MAC
<!--NeedCopy-->
```

> **Nota**
>
> En el caso de un servicio vinculado a un servidor virtual en el que está habilitada la opción `-m MAC`, debe vincular un monitor que no es usuario.

Para configurar el modo de redirección mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. Abra un servidor virtual y seleccione el modo de redirección.

Configurar servidores virtuales con comodines por VLAN

August 20, 2021

Si quiere configurar el equilibrio de carga para el tráfico en una red de área local virtual (VLAN) específica, puede crear un servidor virtual comodín con una directiva de escucha que lo restrinja al tráfico de procesamiento solo en la VLAN especificada.

Para configurar un servidor virtual comodín que escucha una VLAN específica mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para configurar un servidor virtual comodín que escuche una VLAN específica y verifique la configuración:


```
add lb vserver <name> <serviceType> IPAddress * Port * -listenpolicy <
    expression> [-listenpriority <positive_integer>]

show vserver
<!--NeedCopy-->
```

Ejemplo:

```
add lb vserver Vserver-LB-vlan1 ANY -listenpolicy "CLIENT.VLAN.ID.EQ(2)
    " -listenpriority 10

show vserver Vserver-LB-vlan1
<!--NeedCopy-->
```

Para configurar un servidor virtual con caracteres comodín que escucha una VLAN específica mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**.
2. Cree un nuevo servidor virtual o abra un servidor virtual existente.
3. Especifique una prioridad y una expresión de directiva de escucha.

Después de crear este servidor virtual, lo vincula a uno o varios servicios tal y como se describe en Configuración del equilibrio de carga básico.

Asignar pesos a los servicios

August 20, 2021

En una configuración de equilibrio de carga, asigne pesos a los servicios para indicar el porcentaje de tráfico que se debe enviar a cada servicio. Los servicios con pesos más altos pueden manejar más solicitudes; los servicios con pesos más bajos pueden manejar menos solicitudes. La asignación de pesos a los servicios permite al dispositivo Citrix ADC determinar la cantidad de tráfico que puede manejar cada servidor balanceado de carga y, por lo tanto, equilibrar la carga de manera más eficaz.

Nota: Si utiliza un método de equilibrio de carga que admite la ponderación de los servicios (por ejemplo, el método round robin), puede asignar un peso al servicio.

En la tabla siguiente se describen los métodos de equilibrio de carga que admiten la ponderación y se describe brevemente la forma en que la ponderación afecta a la forma en que se selecciona un

servicio para cada uno.

Métodos de equilibrio de carga	Selección de servicio con pesos
Round Robin	El servidor virtual prioriza la cola de servicios disponibles de manera que los servicios con los pesos más altos lleguen al frente de la cola con mayor frecuencia que aquellos con los pesos más bajos y reciban proporcionalmente más tráfico. Para obtener una descripción completa, consulte El método Round Robin.
Conexión mínima	El servidor virtual selecciona el servicio con la mejor combinación de menos transacciones activas y mayor peso. Para obtener una descripción completa, consulte El método de menos conexión.
Método de menor tiempo de respuesta y menor tiempo de respuesta mediante monitores	El servidor virtual selecciona el servicio con la mejor combinación de menos transacciones activas y el tiempo medio de respuesta más rápido. Para obtener una descripción completa, consulte El método de menor tiempo de respuesta.
Ancho de banda mínimo	El servidor virtual selecciona el servicio con la mejor combinación de menos tráfico y mayor ancho de banda. Para obtener una descripción completa, consulte El método de menos ancho de banda.
Menos paquetes	El servidor virtual selecciona el servicio con la mejor combinación de menos paquetes y mayor peso. Para obtener una descripción completa, consulte El método de menos paquetes.
Carga personalizada	El servidor virtual selecciona el servicio con la mejor combinación de carga más baja y peso más alto. Para obtener una descripción completa, consulte El método de carga personalizada.

Métodos de equilibrio de carga	Selección de servicio con pesos
Métodos de hash y método Token	Estos métodos de equilibrio de carga no admiten la ponderación.

Para configurar un servidor virtual para asignar pesos a los servicios mediante la CLI

En el símbolo del sistema, escriba:

```
set lb vserver <name> -weight <Value> <ServiceName>
<!--NeedCopy-->
```

Ejemplo:

```
set lb vserver Vserver-LB-1 -weight 10 Service-HTTP-1
<!--NeedCopy-->
```

Para configurar un servidor virtual para asignar pesos a los servicios mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**.
2. Abra el servidor virtual y, a continuación, haga clic en la sección **Servicios**.
3. En la columna de peso del servicio, asigne un peso al servicio.

Configurar la configuración de la versión de MySQL y Microsoft SQL Server

January 12, 2021

Puede especificar la versión de Microsoft® SQL Server® y el servidor MySQL para un servidor virtual de equilibrio de carga que sea de tipo MSSQL y MySQL respectivamente. Se recomienda la configuración de versión si espera que algunos clientes no ejecuten la misma versión que su producto MySQL o Microsoft SQL Server. La configuración de la versión proporciona compatibilidad entre las conexiones del lado del cliente y del lado del servidor al asegurarse de que todas las comunicaciones se ajustan a la versión del servidor.

Para establecer el parámetro de versión de Microsoft SQL Server mediante la CLI

En el símbolo del sistema, escriba los comandos siguientes para establecer el parámetro de versión de Microsoft SQL Server para un servidor virtual de equilibrio de carga y compruebe la configuración:

```
set lb vserver <name> -mssqlServerVersion <mssqlServerVersion>

show lb vserver <name>
<!--NeedCopy-->
```

Ejemplo

```
> set lb vserver myMSSQLvip -mssqlServerVersion 2008R2
 Done
> show lb vserver myMSSQLvip
    myMSSQLvip (190.0.2.12:1433) - MSSQL    Type: ADDRESS
 . . .
 . . .
    MSsql Server Version: 2008R2
    . . .
    . . .
 Done
>
<!--NeedCopy-->
```

Para establecer el parámetro de versión del servidor MySQL mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para establecer el parámetro de versión de MySQL Server para un servidor virtual de equilibrio de carga y verifique la configuración:

```
set lb vserver <name> -mysqlServerVersion <string>

show lb vserver <name>
<!--NeedCopy-->
```

Ejemplo


```
> set lb vserver mysqlsvr -mysqlserverversion 5.5.30
 Done
> sh lb vserver mysqlsvr
     mysqlsvr (2.22.2.222:3306) - MYSQL      Type: ADDRESS
 . . .
 . . .
     Mysql Server Version: 5.5.30
    . . .
    . . .
 Done
>
<!--NeedCopy-->
```

Para establecer el parámetro de versión de MySQL o Microsoft SQL Server mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**.
2. Abra un servidor virtual de tipo MySQL o MSSQL y configure la versión del servidor.

Servidores virtuales multi-IP

June 2, 2022

Citrix ADC admite la creación de un único servidor virtual de equilibrio de carga con varias direcciones IPv4 e IPv6 no consecutivas/consecutivas de tipo VIP. Cada dirección VIP enlazada a un servidor virtual se trata como un servidor virtual individual. Estos servidores virtuales tienen el mismo protocolo y otras configuraciones de nivel de servidor virtual. Un servidor virtual con varias direcciones VIP también se denomina servidor virtual multi-IP.

Las siguientes son algunas de las ventajas del uso de servidores virtuales multi-IP:

- Un servidor virtual multi-IP descarga el trabajo de crear muchos servidores virtuales con la misma configuración y enlaces de servicio.
- Los servidores virtuales multi-IP reducen eficazmente la posibilidad de alcanzar el límite máximo de las entidades de servidor virtual.
- Se puede usar un servidor virtual multi-IP para que los clientes de diferentes subredes se conecten al mismo conjunto de servidores.
- Solo se puede usar un servidor virtual de IP múltiple para que los clientes IPv6 e IPv4 se conecten al mismo conjunto de servidores.

Configurar un servidor virtual multi-IP

La configuración de un servidor virtual multi-IP consiste en las siguientes tareas:

- Cree un IPset y vincule varias direcciones IP a él.
- Enlazar el IPset a servidores virtuales de equilibrio de carga.

Tenga en cuenta los siguientes puntos relacionados con la configuración de IPset:

- Un IPset puede tener:
  - direcciones IPv4 y direcciones IPv6 no consecutivas/consecutivas
  - combinaciones de direcciones IPv4 e IPv6.
- Todas las direcciones IPv4/IPv6 que se asocien a servidores virtuales mediante IPset deben ser del tipo VIP.
- Un único conjunto de IP se puede vincular a varios servidores virtuales.
- Las direcciones IPv4/IPv6 se pueden enlazar o desvincular a/desde IPset independientemente de cualquier enlace IPset existente a servidores virtuales.
- Debe anular la configuración del enlace de IPset a un servidor virtual antes de vincular un nuevo IPset al mismo.

Para agregar un IPset y vincular varias direcciones VIP a él mediante la CLI

En el símbolo del sistema, escriba:

```
add ipset <name>

bind ipset <name> <IPaddress1 ... >

bind ipset <name> <IPaddress2... >

show ipset <name>
<!--NeedCopy-->
```

Para vincular el IPset a un servidor virtual mediante la CLI

En el símbolo del sistema, escriba:

```
set lb vserver <name> -ipset <ipset name>

show lb vserver <name>
<!--NeedCopy-->
```


Para agregar un conjunto de IP y vincular varias direcciones VIP a él mediante la interfaz gráfica de usuario

Vaya a **Sistema** > **Red** > **IPsets** y cree un IPset con varias direcciones VIP.

Para vincular el IPset a un servidor virtual mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales** y abra un servidor virtual al que quiera vincular el IPset creado.
2. En **Configuración básica**, establezca el parámetro **IPset**en el nombre del IPset creado.

```
> add ipset IPSET-1


Done

> bind ipset IPSET-1 9.9.9.10


Done

> bind ipset IPSET-1 1000::20


Done

> add lb vserver LBVS-1 HTTP 8.8.8.10 80  -ipset IPSET-1


Done

> add service SVC-1 3.3.3.10 HTTP 80


Done

> add service SVC-2 3.3.3.100 HTTP 80


Done

> bind lb vserver LBVS-1 SVC-1

```



```
33
34 Done
35
36 > bind lb vserver LBVS-1 SVC-2
37
38
39 Done
```

Compatibilidad con GSLB para servidores virtuales multi-IP

Las direcciones IP flotantes son necesarias para las implementaciones de alta disponibilidad. Las implementaciones en la nube no admiten direcciones IP flotantes. Por lo tanto, la función de conjunto de IP lo ayuda a admitir una alta disponibilidad en las implementaciones en la nube. Con la función de conjunto de IP, puede asociar una dirección IP privada a cada una de las instancias principal y secundaria. Al crear el servidor virtual, se agrega una de las direcciones IP privadas. La otra dirección IP está enlazada a un conjunto de IP. A continuación, el conjunto de IP se asocia con el servidor virtual. Por lo general, una dirección IP pública se asigna a una de las direcciones IP privadas en función del dispositivo que recibe el tráfico. Durante la conmutación por error, esta asignación cambia dinámicamente para enrutar el tráfico al nuevo primario.

En las implementaciones de GSLB, el servicio GSLB representa el servidor virtual y requiere la dirección IP pública y privada del servidor virtual. En las implementaciones en la nube, hay varias direcciones IP privadas representadas como un conjunto de IP, pero el servicio GSLB solo puede aceptar una dirección IP privada. Por lo tanto, al configurar el servicio GSLB, se recomienda dar la dirección IP que se configura al agregar el servidor virtual o una de las direcciones IP en el conjunto de IP. No es necesario configurar la función de conjunto de IP en el servicio GSLB. El conjunto de IP configurado en el servidor virtual de equilibrio de carga asociado al servicio GSLB es suficiente.

En la topología principal-secundario de GSLB, los servidores virtuales de equilibrio de carga de los sitios secundarios pueden tener el conjunto de IP asociado a ellos. El servicio GSLB correspondiente a esta topología incluye la dirección IP pública y una de las direcciones IP privadas. La dirección IP privada puede ser una dirección IP del conjunto de IP o la que se configuró al agregar el servidor virtual en el sitio secundario. La comunicación entre los sitios principal y secundario siempre se realiza mediante la dirección IP pública y el puerto público del servicio GSLB.

Además, con la compatibilidad con conjuntos de IP, puede tener un único punto final de servidor virtual para el tráfico IPv4 e IPv6. Anteriormente, tenía que configurar diferentes servidores virtuales para el tráfico IPv4 e IPv6. Con la compatibilidad con conjuntos de IP, puede asociar direcciones IP IPv4 e IPv6 al mismo conjunto de IP. Puede agregar diferentes servicios GSLB que representen los puntos finales IPv4 e IPv6.

Limitar el número de solicitudes simultáneas en una conexión de cliente

January 12, 2021

Puede limitar el número de solicitudes simultáneas en una única conexión de cliente. Puede proteger los servidores de vulnerabilidades de seguridad limitando el número de solicitudes simultáneas. Cuando la conexión de cliente alcanza el límite máximo especificado, el dispositivo Citrix ADC descarta las solicitudes posteriores en la conexión hasta que el recuento de solicitudes pendientes sea inferior al límite.

Puede configurar el parámetro MaxPipelineNat para limitar el número de solicitudes simultáneas en una única conexión de cliente. Este parámetro solo es aplicable a los siguientes tipos de servicio y cuando "svrTimeout" se establece en cero:

- CUALQUIERA
- Todos los tipos de servicio UDP excepto DNS

El valor predeterminado del parámetro MaxPipelineNat es 255. Un valor de cero (0) no aplica ningún límite al número de solicitudes simultáneas. Cuando no se establece ningún límite, el dispositivo Citrix ADC ejecuta todas las solicitudes.

> **Nota**
>
> Si establece MaxPipelineNat en un valor más alto, entonces la probabilidad de ataque de suplantación puede ser mayor. Por lo tanto, se recomienda establecer MaxPipelineNat a un valor inferior.

Para limitar el número de conexiones simultáneas para un cliente mediante la CLI

En el símbolo del sistema, escriba:

```
set lb parameter -maxPipelineNat <positive_integer>
<!--NeedCopy-->
```

Ejemplo:

```
set lb parameter -maxPipelineNat 199
<!--NeedCopy-->
```


Para limitar el número de conexiones simultáneas para un cliente mediante la interfaz gráfica de usuario

Desplácese hasta **Administración del tráfico > Equilibrio de carga > Configurar parámetros de equilibrio**de carga, especifique un valor para solicitudes NAT de proceso máxima.

Configurar el equilibrio de carga de diameter

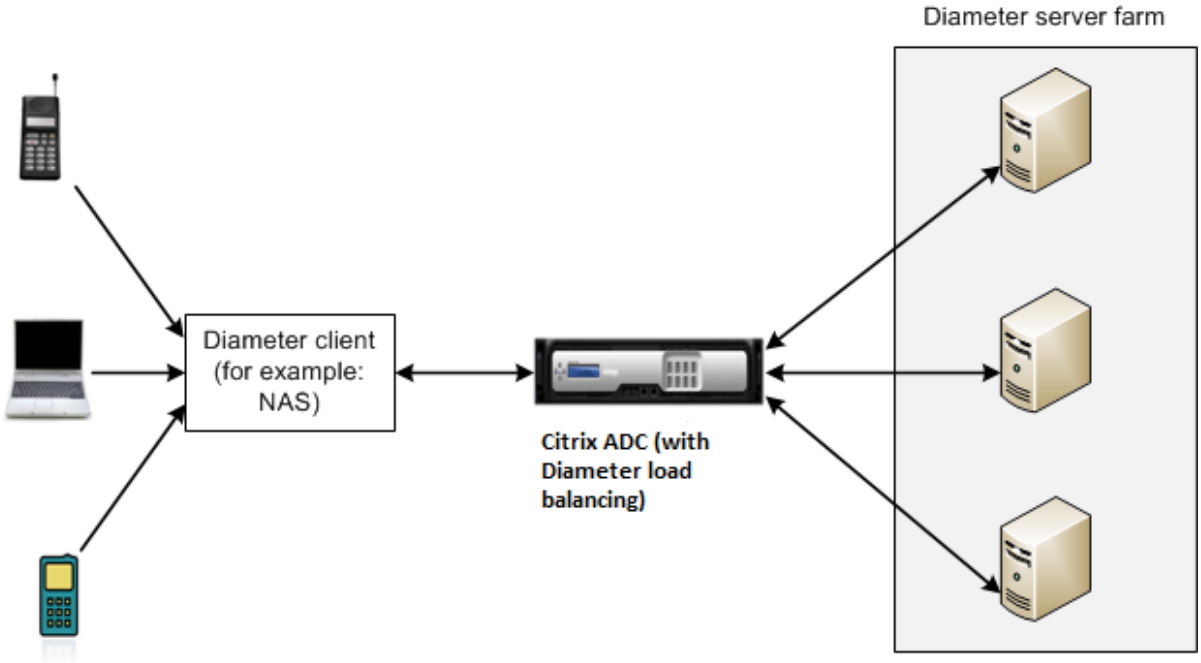
August 20, 2021

El protocolo Diameter es un protocolo de señalización AAA (Autenticación, Autorización y Contabilidad) de próxima generación utilizado principalmente en dispositivos móviles como equipos portátiles y teléfonos móviles. Es un protocolo peer-to-peer, a diferencia del modelo cliente-servidor tradicional utilizado por la mayoría de los otros protocolos. Sin embargo, en la mayoría de las implementaciones de Diameter, los clientes origina la solicitud y el servidor responde a la solicitud.

Cuando se intercambian mensajes de diameter, el servidor de diameter suele realizar mucho más procesamiento que el cliente de diameter. Con el aumento del volumen de señalización del plano de control, el servidor de diameter se convierte en un cuello de botella. Por lo tanto, los mensajes de diameter deben equilibrarse la carga en varios servidores. Un servidor virtual que realiza el equilibrio de carga de los mensajes de Diameter proporciona las siguientes ventajas:

- Carga más ligera en los servidores Diameter, lo que se traduce en un tiempo de respuesta más rápido para los usuarios finales.
- Supervisión del estado del servidor y mejores capacidades de conmutación por error.
- Mejor escalabilidad en términos de adición de servidores sin cambiar la configuración del cliente.
- Alta disponibilidad.
- Descarga de diameter SSL.

La siguiente ilustración muestra un sistema de diameter en una implementación de Citrix ADC:



Un sistema de diameter tiene los siguientes componentes:

- **Cliente Diameter.** Admite aplicaciones cliente Diameter además del protocolo base. Los clientes de Diameter a menudo se implementan en dispositivos situados en el borde de una red y proporcionan servicios de control de acceso para esa red. Ejemplos típicos de clientes Diameter son un servidor de acceso a la red (NAS) y el agente externo de IP móvil (FA).
- **Agente de diameter.** Proporciona servicios de retransmisión, proxy, redirección o traducción. El dispositivo Citrix ADC (configurado con un servidor virtual de equilibrio de carga de diameter) desempeña el papel de agente de diameter.
- **Servidor de diameter.** Maneja las solicitudes de autenticación, autorización y contabilidad para un dominio determinado. Un servidor Diameter debe admitir aplicaciones de servidor Diameter además del protocolo base.

En una topología típica de diameter, cuando un dispositivo de usuario final (como un teléfono móvil) necesita un servicio, envía una solicitud a un cliente de diameter. Cada cliente Diameter establece una única conexión (TCP Connection—SCTP aún no se admite) con un servidor Diameter como se especifica en el protocolo base Diameter RFC 6733. La conexión es de larga duración y todos los mensajes entre los dos nodos Diameter (cliente y servidor) se intercambian a través de esta conexión. Citrix ADC utiliza el equilibrio de carga basado en mensajes.

Ejemplo:

Un proveedor de servicios móviles utiliza Diameter para su sistema de facturación. Cuando un suscriptor utiliza un número de prepago, el cliente Diameter envía repetidamente solicitudes al servidor para comprobar el saldo disponible. El protocolo Diameter establece una conexión entre el cliente y el servidor, y todas las solicitudes se intercambian a través de esa conexión. El equilibrio de carga

basado en la conexión no tendría sentido, porque solo hay una conexión. Sin embargo, con la gran cantidad de mensajes en la conexión, el equilibrio de carga basado en mensajes acelera el proceso de facturación al suscriptor móvil prepago.

Cómo funciona el equilibrio de carga de diameter

Una solicitud de desconexión del mismo nivel (DPR) indica la intención del par de cerrar la conexión, con el motivo para cerrar la conexión. El par responde con un DPA (TCP siempre proporciona un DPA correcto).

- Cuando el dispositivo recibe un DPR del cliente, transmite el DPR a todos los servidores y responde inmediatamente con un DPA al cliente. Los servidores responden con DPA, pero el dispositivo los ignora. El cliente envía un FIN, que el dispositivo transmite a todos los servidores.
- Cuando el dispositivo recibe un DPR del servidor, responde solo con un DPA a ese servidor y no quita el servidor del grupo de reutilización. Cuando el servidor envía un FIN, el dispositivo responde con FIN/ACK y quita las conexiones del grupo de reutilización.
- Si el dispositivo recibe un FIN del cliente, envía al cliente un FIN/ACK, transmite el FIN y quita inmediatamente la conexión del servidor del grupo de reutilización.
- Si el dispositivo recibe un FIN del servidor, envía un FIN/ACK y lo elimina del grupo de reutilización. Cualquier mensaje nuevo para este servidor se envía en una nueva conexión.

Tráfico de diameter de equilibrio de carga

Cuando un cliente envía una solicitud al dispositivo Citrix ADC, el dispositivo analiza la solicitud y la carga contextualmente equilibra en un servidor Diameter basado en un AVP persistente. El dispositivo ha anunciado la identidad del cliente al servidor, por lo que no agrega entradas de ruta, ya que el servidor espera mensajes directamente del cliente.

Las solicitudes iniciadas por el servidor no son tan frecuentes como las solicitudes del cliente. Las solicitudes iniciadas por el servidor son similares a las solicitudes iniciadas por el cliente, excepto:

- Dado que los mensajes se reciben de varios servidores, el dispositivo mantiene el estado de la transacción agregando un número único de Hop by Hop (HByH) a cada mensaje de solicitud reenviada. Cuando llega la respuesta del mensaje (con el mismo número de HByH), el dispositivo traduce este número de HByH al número de HByH que se recibió en el servidor cuando llegó la solicitud.
- El dispositivo Citrix ADC agrega una entrada de ruta colocando su identidad, ya que el cliente ve el dispositivo como un agente de retransmisión.

Nota: Si un mensaje de Diámetro abarca más de un paquete, el dispositivo acumula los paquetes en una cola de encabezado incompleta y los reenvía al servidor cuando se acumula el mensaje completo. Del mismo modo, si un único paquete contiene más de un mensaje de Diameter, el dispositivo divide

el paquete y reenvía los mensajes a los servidores según determine el servidor virtual de equilibrio de carga.

Desconectar una sesión

Una solicitud de desconexión del mismo nivel (DPR) indica la intención del par de cerrar la conexión, con el motivo para cerrar la conexión. El par responde con un DPA (TCP siempre proporciona un DPA correcto).

- Cuando el dispositivo Citrix ADC recibe un DPR del cliente, transmite el DPR a todos los servidores y responde inmediatamente con un DPA al cliente. Los servidores responden con DPA, pero el dispositivo los ignora. El cliente envía un FIN, que el dispositivo transmite a todos los servidores.
- Cuando el dispositivo recibe un DPR del servidor, responde solo con un DPA a ese servidor y no quita el servidor del grupo de reutilización. Cuando el servidor envía un FIN, el dispositivo responde con FIN/ACK y quita las conexiones del grupo de reutilización.
- Si el dispositivo recibe un FIN del cliente, envía al cliente un FIN/ACK, transmite el FIN y quita inmediatamente la conexión del servidor del grupo de reutilización.
- Si el dispositivo recibe un FIN del servidor, envía un FIN/ACK y lo elimina del grupo de reutilización. Cualquier mensaje nuevo para este servidor se envía en una nueva conexión.

Configurar el equilibrio de carga para el tráfico de diameter

Para configurar el dispositivo Citrix ADC para equilibrar la carga del tráfico de diameter, primero debe establecer los parámetros de diameter en el dispositivo y, a continuación, agregar el monitor de diameter, agregar los servicios de diameter, enlazar los servicios al monitor, agregar el servidor virtual de equilibrio de carga de diameter y enlazar los servicios a la servidor.

Para configurar el equilibrio de carga para el tráfico de diameter mediante la interfaz de línea de comandos

Configure los parámetros de diameter.

```
1 set ns diameter -identity <string> -realm <string> -
     serverClosePropagation <YES|NO>
2 <!--NeedCopy-->
```

Ejemplo:


```
set ns diameter -identity mydomain.org -realm org -
    serverClosePropagation YES
<!--NeedCopy-->
```

Agregue un monitor de diameter.

```
add lb monitor <monitorName> DIAMETER -originHost <string> -originRealm
     <string>
<!--NeedCopy-->
```

Ejemplo:

```
add lb monitor diameter_mon DIAMETER -originHost mydomain.org -
    originRealm org
<!--NeedCopy-->
```

Cree los servicios de Diameter.

```
add service <name> <IP> DIAMETER <port>
<!--NeedCopy-->
```

Ejemplo:

```
add service diameter_svc0 10.102.82.86 DIAMETER 3868

add service diameter_svc1 10.102.82.87 DIAMETER 3868

add service diameter_svc2 10.102.82.88 DIAMETER 3868

add service diameter_svc3 10.102.82.89 DIAMETER 3868
<!--NeedCopy-->
```

Enlazar los servicios Diameter al monitor Diameter.

```
bind service <name>@ monitorName <monitorName>
<!--NeedCopy-->
```


Ejemplo:

```
bind service diameter_svc0 -monitorName diameter_mon

bind service diameter_svc1 -monitorName diameter_mon

bind service diameter_svc2 -monitorName diameter_mon

bind service diameter_svc3 -monitorName diameter_mon
<!--NeedCopy-->
```

Agregue un servidor virtual de equilibrio de carga de diameter con persistencia de diameter.

```
add lb vserver <name> DIAMETER <IPAddress> <port> -persistenceType
   DIAMETER -persistAVPno <positive_integer>
<!--NeedCopy-->
```

Ejemplo:

```
add lb vserver diameter_vs DIAMETER 10.102.112.152 3868 -
   persistenceType DIAMETER -persistAVPno 263
<!--NeedCopy-->
```

Enlazar los servicios de diameter al servidor virtual de equilibrio de carga de diameter.

```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Ejemplo:

```
bind lb vserver diameter_vs diameter_svc0

bind lb vserver diameter_vs diameter_svc1

bind lb vserver diameter_vs diameter_svc2

bind lb vserver diameter_vs diameter_svc3
<!--NeedCopy-->
```


Guarde la configuración.

```
save ns config
<!--NeedCopy-->
```

Nota: También puede configurar el equilibrio de carga del tráfico de diámetro a través de SSL mediante el tipo de servicio **SSL_DIAMETER**.

Para configurar el equilibrio de carga para el tráfico de diameter mediante la utilidad de configuración

1. Vaya a **Sistema** > **Configuración** > **Cambiar parámetros de diámetro** y defina los parámetros de diámetro.
2. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales** y cree un servidor virtual de equilibrio de carga del tipo Diámetro.
3. Cree un servicio de tipo Diameter.
4. Cree un monitor de tipo Diameter. En Parámetros especiales, defina el host de origen y el dominio de origen.
5. Enlazar el monitor al servicio y enlazar el servicio al servidor virtual Diameter.
6. En Configuración avanzada, haga clic en **Persistencia**, especifique el diámetro e introduzca un número AVP de persistencia.
7. Haga clic en **Guardar** y haga clic en **Listo**.

Configurar equilibrio de carga de FIX

August 20, 2021

El protocolo Financial Information Exchange (FIX) es un estándar de mensajes abiertos utilizado en el sector financiero para el intercambio electrónico de información relacionada con las transacciones de valores entre socios comerciales. El protocolo FIX/SSL_FIX es ampliamente utilizado por las empresas del lado de compra y venta, las plataformas comerciales y los reguladores para comunicar información comercial.

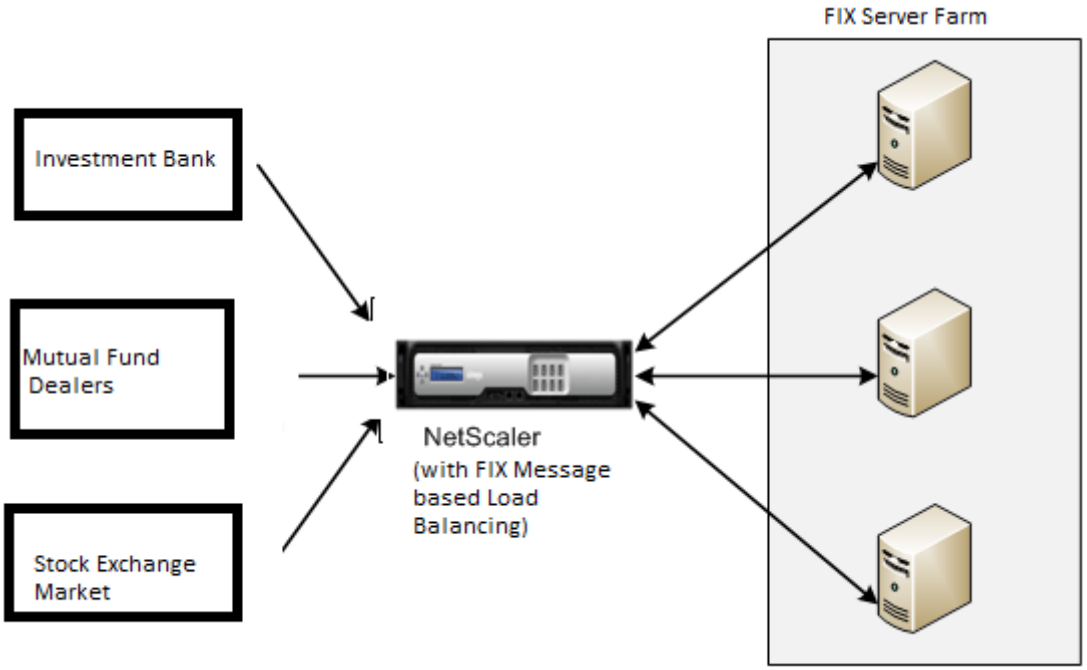
Esta función le permite configurar un servidor virtual de equilibrio de carga FIX o SSL_FIX para distribuir los mensajes FIX entrantes y proporcionar seguridad en los mensajes FIX. Citrix ADC admite el equilibrio de carga basado en mensajes FIX (MBLB) para las versiones FIX 4.1, FIX 4.2, FIX 4.3 y FIX 4.4.

FIX MBLB en un dispositivo Citrix ADC proporciona las siguientes ventajas:

1. Gestión eficiente de servidores FIX o SSL_FIX con alta disponibilidad y supervisión de estado superiores.
2. Protección SYN para todos los servidores FIX o SSL_FIX.
3. Permanencia de sesión de FIX.

Cómo funciona el equilibrio de carga de FIX

Una configuración de FIX MBLB incluye un servidor virtual de equilibrio de carga FIX y varios servidores FIX equilibrados de carga. El servidor virtual FIX recibe tráfico de cliente entrante, analiza el tráfico entrante en mensajes FIX, selecciona un servidor FIX para cada mensaje FIX y lo reenvía al servidor FIX seleccionado. El siguiente dibujo conceptual ilustra una configuración típica de equilibrio de carga FIX.



En una configuración básica de FIX MBLB, el servidor virtual FIX distribuye los mensajes FIX procedentes de clientes a los servidores FIX equilibrados de carga mediante el método de equilibrio de carga round robin. Con la persistencia del tipo FIXSESSION habilitada, el servidor virtual FIX selecciona el mismo servidor para diferentes mensajes FIX pertenecientes a la misma sesión FIX. La sesión FIX se determina en función de los valores de los campos **FIX** SenderCompid (etiqueta 49) y TargetCompid (etiqueta 56).

Configurar y supervisar el equilibrio de carga para el tráfico FIX

A continuación se presentan las configuraciones que debe hacer para equilibrar la carga del tráfico de mensajes FIX:

1. Configuración del servidor virtual de equilibrio de carga FIX
2. Configuración del servidor virtual de equilibrio de carga SSL_FIX
3. Configuración del servicio de equilibrio de carga FIX
4. Configuración del servicio de equilibrio de carga SSL_FIX
5. Configuración de la persistencia de FIXSESSION
6. Establecer el tiempo de espera de persistencia
7. Visualización de estadísticas FIX/SSL_FIX
8. Supervisión de sesiones persistentes FIX/SSL_FIX

Para configurar un servidor de equilibrio de carga de FIX mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
add lb vserver <name> FIX <IP> <PORT>
<!--NeedCopy-->
```

Ejemplo

```
add lb vserver vs1 FIX 10.102.82.86 3868
<!--NeedCopy-->
```

Para configurar un servidor virtual de equilibrio de carga SSL_FIX mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
add lb vserver <name> SSL_FIX <IP> <PORT>
<!--NeedCopy-->
```

Ejemplo

```
add lb vserver vs1 SSL_FIX 10.102.82.86 3868
<!--NeedCopy-->
```


Para configurar un servicio FIX mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
add service <name> <ip-addr> FIX <port>
<!--NeedCopy-->
```

Ejemplo

```
add service_svc1 10.102.82.86 FIX 3868
<!--NeedCopy-->
```

Para configurar un servicio SSL_FIX mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
add service <name> <ip-addr> SSL_FIX <port>
<!--NeedCopy-->
```

Ejemplo

```
add service svc1 10.102.82.86 SSL_FIX 3868
<!--NeedCopy-->
```

Para configurar la persistencia de FIXSESSION mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
set lb vserver <name> -persistenceType FIXSESSION
<!--NeedCopy-->
```

Ejemplo

```
set lb vserver vs1 -persistenceType FIXSESSION
<!--NeedCopy-->
```


Para establecer el tiempo de espera de persistencia mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
set lb vserver <name> -timeout <value>
<!--NeedCopy-->
```

Ejemplo

```
set lb vserver vs1  - timeout 2
<!--NeedCopy-->
```

Para mostrar las estadísticas de FIX mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
stat lb vserver <name>
<!--NeedCopy-->
```

Ejemplo

```
stat lb vserver_svc1
<!--NeedCopy-->
```

Para enlazar el servicio FIX al servidor virtual FIX mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
bind lb vserver <name> <service name>
<!--NeedCopy-->
```

Ejemplo

```
bind lb vserver vs1 svc1
<!--NeedCopy-->
```


Para mostrar las sesiones persistentes de FIX mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
show lb persistentSessions <name>
<!--NeedCopy-->
```

Ejemplo

```
show lb persistentSessions vs1
<!--NeedCopy-->
```

> **Nota**
>
> Nota: Ahora puede configurar el equilibrio de carga del tráfico FIX sobre SSL mediante el tipo de servicio SSL_FIX. Este servicio proporciona una comunicación segura para los mensajes FIX.

Para configurar el servidor virtual de equilibrio de carga FIX mediante la interfaz gráfica de usuario

1. Vaya a la página **Configuración** > **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales** y haga clic en **Agregar** para crear un servidor virtual de Equilibrio de carga de FIX.
2. En la página **Servidor virtual de equilibrio de carga**, establezca los parámetros del servidor:
   a) Nombre del servidor virtual
   b) Tipo de protocolo como “FIX”
   c) Tipo de dirección IP del servidor
   d) Dirección IP del servidor
   e) Número de puerto del servidor
3. Haga clic en **Aceptar** y en **Continuar** para establecer otros parámetros.
4. En la sección **Servicios**, seleccione o agregue un nuevo servicio virtual de equilibrio de carga de FIX y enlaza al servidor FIX.
5. En la sección **Persistencia**, establezca los siguientes parámetros:
   a) Tipo de persistencia como ‘FIXSESSION’
   b) Intervalo de tiempo de espera
6. Haga clic en **Aceptar** y, a continuación, **Listo**.

Para modificar un servidor virtual de equilibrio de carga FIX mediante la interfaz gráfica de usuario

Vaya a la página **Configuración** > **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**, seleccione un servidor FIX y haga clic en **Modificar**.

Para eliminar un servidor virtual de equilibrio de carga FIX mediante la interfaz gráfica de usuario

Vaya a **la página Configuración** > **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**, seleccione un servidor FIX y haga clic en **Eliminar**.

Para configurar el servicio virtual de equilibrio de carga de FIX mediante la interfaz gráfica de usuario

1. Vaya a **Configuración** > **Administración del tráfico** > **Equilibrio de carga** > **Servicios** y haga clic en **Agregar** para crear un servicio virtual de Equilibrio de carga de FIX.
2. En la página **Servicios**, establezca los siguientes parámetros. Puede hacer clic en la flecha "Más" para definir otros parámetros, como Dominio de tráfico, ID de hash, ID de servidor, Tipo de caché y Número de conexiones activas.
   a) Nombre de servicio: Nombre de servicio virtual de FIX
   b) Elija el tipo de servidor virtual como (nuevo o existente)
   c) Protocolo: Tipo de protocolo como 'FIX'
   d) Servidor: Dirección IP del servidor virtual
   e) Puerto: Número de puerto del servidor
3. Haga clic en **Aceptar** y **Continuar** para establecer otros parámetros como Monitores, Umbral y tiempo de espera, Perfiles y Directivas.
4. Haga clic en **Aceptar** y, a continuación, **Listo**.

Para modificar un servicio virtual de equilibrio de carga de FIX mediante la interfaz gráfica de usuario

Vaya a la página **Configuración** > **Administración del tráfico** > **Equilibrio de carga** > **Servicios**, seleccione un **servicio FIX** y haga clic en **Modificar**.

Para eliminar un servicio virtual de equilibrio de carga de FIX mediante la interfaz gráfica de usuario

Vaya a **la página Configuración** > **Administración del tráfico** > **Equilibrio de carga** > **Servicios**, seleccione un servicio FIX y haga clic en **Eliminar**.

Para mostrar las estadísticas del servidor de equilibrio de carga de FIX

Vaya a la página **Configuración** > **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales** y, a continuación, haga clic en **Estadísticas** para mostrar las estadísticas del servidor FIX.

Para mostrar sesiones persistentes para un servidor FIX mediante la interfaz gráfica de usuario

Vaya a la página **Configuración** > **Administración del Tráfico** y, en **Supervisión de Sesiones, haga clic en SesionesPersistentes del Servidor Virtual**.

Para borrar sesiones persistentes para un servidor FIX mediante la interfaz gráfica de usuario

1. Acceda a la página **Configuración** > **Administración del tráfico** y, en **Supervisión de Sesiones**, haga clic en **Borrar Sesiones Persistentes**.
2. En la página **Borrar Sesiones Persistentes**, establezca los siguientes parámetros:
   a) Servidor virtual: Elija un servidor virtual FIX
   b) Parámetro de persistencia: Elija un parámetro de persistencia FIX
3. Haga clic en **Aceptar**.

Equilibrio de carga MQTT

August 20, 2021

El transporte de telemetría de Message Queue Server (MQTT) es un protocolo de mensajería estándar de OASIS para Internet de las cosas (IoT). MQTT es una tecnología flexible y fácil de usar que proporciona una comunicación efectiva dentro de un sistema IoT. MQTT es un protocolo basado en intermediarios y es ampliamente utilizado para facilitar el intercambio de mensajes entre clientes y bróker.

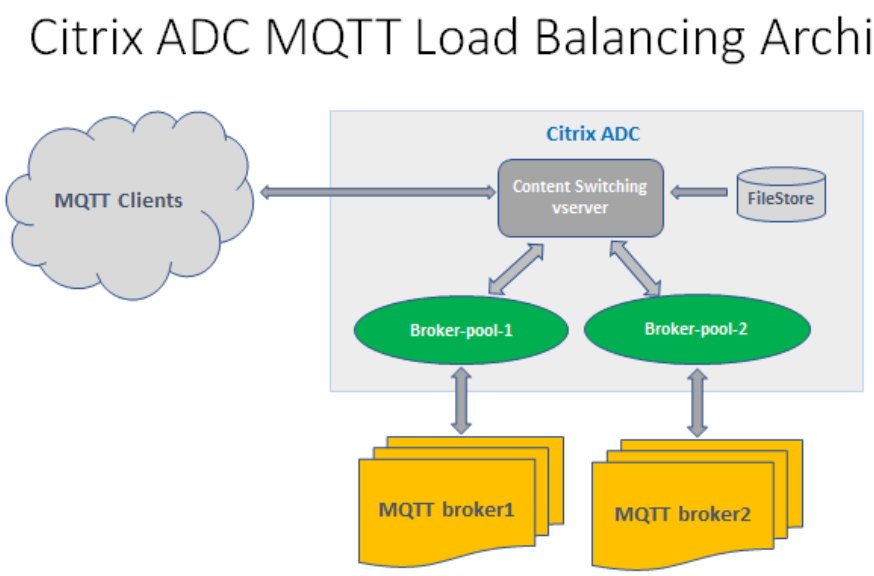
Las siguientes ventajas clave de MQTT lo convierten en una opción adecuada para su dispositivo IoT:

- Fiabilidad
- Tiempo de respuesta rápido
- Capacidad para admitir dispositivos ilimitados
- Publicar/suscribir mensajes que son perfectos para la comunicación de muchos a muchos

IoT es la red de dispositivos interconectados que están integrados con sensores, software, conectividad de red y electrónica necesaria. Los componentes integrados permiten a los dispositivos IoT recopilar e intercambiar datos. El aumento en el uso de dispositivos IoT trae consigo múltiples desafíos para la infraestructura de red, siendo Scale el más destacado. En una implementación a gran escala

de dispositivos IoT, los datos generados por cada dispositivo IoT deben analizarse rápidamente. Para lograr el requisito de escala y el uso eficiente de los recursos, la carga en el grupo de broker debe distribuirse de manera uniforme. Con la compatibilidad del protocolo MQTT, puede utilizar el dispositivo Citrix ADC en implementaciones de IoT para equilibrar la carga del tráfico MQTT.

En la siguiente ilustración se muestra la arquitectura MQTT que utiliza un dispositivo Citrix ADC para equilibrar la carga del tráfico de MQTT.



Una implementación de IoT con protocolo MQTT tiene los siguientes componentes:

- **Intermediario MQTT.** Servidor que recibe todos los mensajes de los clientes y, a continuación, los enruta a los clientes de destino apropiados. El intermediario es responsable de recibir todos los mensajes, filtrar los mensajes, determinar quién está suscrito a cada mensaje y enviar el mensaje a estos clientes suscritos. El intermediario es el centro central a través del cual debe pasar cada mensaje.
- **Cliente MQTT.** Cualquier dispositivo, desde un microcontrolador hasta un servidor completo, que ejecuta una biblioteca MQTT y se conecta a un broker de MQTT a través de una red. Tanto los editores como los suscriptores son clientes de MQTT. Las etiquetas de publicador y suscriptor hacen referencia a si el cliente está publicando mensajes o si está suscrito para recibir mensajes.
- **Equilibrador de carga MQTT.** El dispositivo Citrix ADC está configurado con un servidor virtual de equilibrio de carga MQTT para equilibrar la carga del tráfico de MQTT.

En una implementación típica de IoT, el agente (clúster de servidores) administra el grupo de dispositivos IoT (clientes de IoT). La carga del dispositivo Citrix ADC equilibra el tráfico de MQTT con los agentes en función de varios parámetros, como ID de cliente, tema y nombre de usuario.

Configurar el equilibrio de carga para el tráfico MQTT

Para que el dispositivo Citrix ADC pueda equilibrar la carga del tráfico de MQTT, realice las siguientes tareas de configuración:

1. Configure los servicios o grupos de servicios MQTT/MQTT_TLS.
2. Configure el servidor virtual de equilibrio de carga MQTT/MQTT_TLS.
3. Enlazar los servicios MQTT/MQTT_TLS al servidor virtual de equilibrio de carga MQTT/MQTT_TLS.
4. Configure el servidor virtual de conmutación de contenido MQTT/MQTT_TLS.
5. Configurar una acción de conmutación de contenido que especifique el servidor virtual de equilibrio de carga de destino
6. Configurar una directiva de conmutación de contenido.
7. Enlazar la directiva de conmutación de contenido a un servidor virtual de conmutación de contenido que ya está configurado para redirigir al servidor virtual de equilibrio de carga específico.
8. Guarde la configuración.

Para configurar el equilibrio de carga para el tráfico MQTT mediante la CLI

Configure los servicios o grupos de servicios MQTT/MQTT_TLS.

```
add service <name> <IP> <protocol> <port>
add servicegroup <ServiceGroupName> <Protocol>
bind servicegroup <serviceGroupName> <IP> <port>
<!--NeedCopy-->
```

Ejemplo:

```
add service srvc1 10.106.163.3 MQTT 1883
add servicegroup srvcg1 MQTT
bind servicegroup srvcg1 10.106.163.3 1883
<!--NeedCopy-->
```

Configure el servidor virtual de equilibrio de carga MQTT/MQTT_TLS.

```
add lb vserver <name> <protocol> <IPAddress> <port>
<!--NeedCopy-->
```

Ejemplo:


```
add lb vserver lb1 MQTT 10.106.163.9 1883
<!--NeedCopy-->
```

Enlazar los servicios o grupos de servicios MQTT/MQTT_TLS al servidor virtual de equilibrio de carga de MQTT.

```
bind lb vserver <name> <serviceName>
bind lb vserver <name> <servicegroupName>
<!--NeedCopy-->
```

Ejemplo:

```
bind lb vserver lb1 srvc1
bind lb vserver lb1 srvcg1
<!--NeedCopy-->
```

Configure el servidor virtual de conmutación de contenido MQTT/MQTT_TLS.

```
add cs vserver <name> <protocol> <IPAddress> <port>
<!--NeedCopy-->
```

Ejemplo:

```
add cs vserver cs1 MQTT 10.106.163.13 1883
<!--NeedCopy-->
```

Configure una acción de conmutación de contenido que especifique el servidor virtual de equilibrio de carga de destino.

```
add cs action <name> -targetLBVserver <string> [-comment <string>]
<!--NeedCopy-->
```

Ejemplo:


```
1 add cs action act1 -targetlbvserver lbv1
2 <!--NeedCopy-->
```

Configurar una directiva de conmutación de contenido.

```
1 add cs policy <policyName> [-url <string> | -rule <expression>] -
     action <actName>
2 <!--NeedCopy-->
```

Ejemplo:

```
1 add cs policy cspol1  -rule   "MQTT.COMMAND.EQ(CONNECT) && MQTT.CONNECT
     .FLAGS.QOS.eq(2)"  -action act1
2 <!--NeedCopy-->
```

Enlazar la directiva de conmutación de contenido a un servidor virtual de conmutación de contenido que ya está configurado para redirigir al servidor virtual de equilibrio de carga específico.

```
1 bind cs vserver <virtualServerName> -policyName <policyName> -priority
     <positiveInteger>
2 <!--NeedCopy-->
```

Ejemplo:

```
1 bind cs vserver cs1  - policyName cspol1 -priority 20
2 <!--NeedCopy-->
```

Guarde la configuración.

```
1 save ns config
2 <!--NeedCopy-->
```

Para configurar el equilibrio de carga para el tráfico MQTT mediante la GUI

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**y cree un servidor virtual de equilibrio de carga de tipo **MQTT** o **MQTT_TLS**.

2. Cree un servicio o grupo de servicios de tipo MQTT.
3. Enlazar el servicio al servidor virtual MQTT.
4. Haga clic en **Guardar**.

Límite de longitud de mensaje MQTT

El dispositivo Citrix ADC trata los mensajes con una longitud de mensaje superior a 65536 bytes como paquetes jumbo y los descarta de forma predeterminada. El parámetro `dropmqttjumbomessage` lb decide si se procesan los paquetes jumbo o no. Este parámetro se establece de forma predeterminada en **YES**, lo que implica que los paquetes MQTT jumbo se descartan de forma predeterminada. Si este parámetro se establece en **NO**, el dispositivo ADC maneja incluso los paquetes con una longitud de mensaje superior a 65536 bytes.

Para configurar el dispositivo ADC para que gestione paquetes jumbo mediante CLI:

```
Set lb parameter -dropMqttJumboMessage [YES | NO]
<!--NeedCopy-->
```

Ejemplo:

```
set lb parameter -dropMqttJumboMessage no
<!--NeedCopy-->
```

Proteger una configuración de equilibrio de carga contra fallos

August 20, 2021

Cuando se produce un error en un servidor virtual de equilibrio de carga o cuando el servidor virtual no puede controlar el tráfico excesivo, la configuración de equilibrio de carga puede fallar. Puede proteger la configuración del equilibrio de carga contra fallos mediante la configuración;

- el dispositivo Citrix ADC para redirigir el exceso de tráfico a una URL alternativa,
- un servidor virtual de equilibrio de carga de respaldo, y
- una conmutación por error de conexión con estado.

Redirigir las solicitudes de cliente a una URL alternativa

August 20, 2021

Puede redirigir solicitudes a una dirección URL alternativa mediante un redireccionamiento HTTP 302 si un servidor virtual de equilibrio de carga de tipo HTTP o HTTPS se desactiva o se inhabilita. La dirección URL alternativa puede proporcionar información sobre el estado del servidor. La URL de redirección configurada se especifica en el encabezado de ubicación de la respuesta HTTP. La dirección URL exacta especificada en la respuesta depende de las siguientes opciones de configuración:

- Si la dirección URL de redirección configurada contiene solo el nombre de dominio, por ejemplohttp://www.sample1.example.com, la dirección URL de redirección especificada en la respuesta HTTP anexa el identificador uniforme de recursos (URI). Se especifica en la solicitud HTTP al nombre de dominio configurado. Por ejemplo, si la solicitud contiene el http://www.sample2.example.com/images/site_nav.png encabezado GET, el encabezado de ubicación en la respuesta de redirección especifica el http://www.sample1.example.com/images/site_nav.png encabezado location:.

  > **Nota**
  >
  > Los nombres de dominio en la solicitud y la respuesta pueden diferir. En este tema, los dos dominios se denominan sample1.example.com y sample2.example.com para explicar el concepto.

- Si la URL de redirección configurada contiene una ruta completa, la respuesta de redirección especifica la URL configurada completa, independientemente del URI de la solicitud. Por ejemplo, las siguientes son las direcciones URL:
  - URL solicitada - http://www.redirect.com/en/index.html
  - URL de redirección - http://www.redirect.com/en/site_down.html

En la tabla siguiente se enumeran las opciones de configuración anteriores:

URL de redirección configurada	URL en solicitud HTTP	Encabezado en respuesta HTTP
http://www.sample1.example.com	http://www.sample2.example.com/en/index.html	http://www.sample1.example.com/en/index.html
http://www.sample1.example.com/en/error.html	http://www.sample2.example.com/en/index.html	http://www.sample1.example.com/en/error.html

Nota

- Al configurar una URL de redirección, la http://example.com URL no es la misma que la http://example.com/ URL, porque esta última contiene la ruta completa a la ruta de Webroot, /.
- Si un servidor virtual de equilibrio de carga está configurado tanto con un servidor virtual de copia de seguridad como con una URL de redirección, el servidor virtual de copia de seguridad tiene prioridad sobre la URL de redirección. Solo se utiliza una redirección cuando los servidores virtuales principales y de copia de seguridad están DOWN.

Para configurar un servidor virtual para redirigir la solicitud del cliente a una URL mediante la CLI

1. Cree un servidor virtual de equilibrio de carga.

   ```
   set lb vserver -redirect url
   ```

2. Compruebe que la opción URL de redirección funciona como se esperaba. Inhabilite el servidor virtual.

   ```
   disable vserver <vserver_name>
   ```

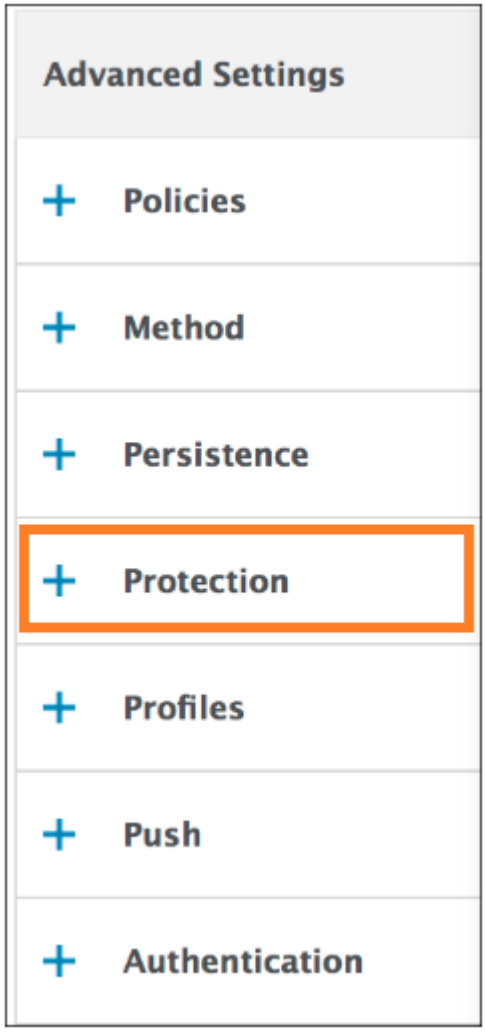
3. Acceda a la URL del sitio web desde un explorador web para verificar que la solicitud se redirige como se esperaba. Es posible que tenga que borrar la caché del explorador web y establecer una nueva conexión antes de acceder al sitio web.

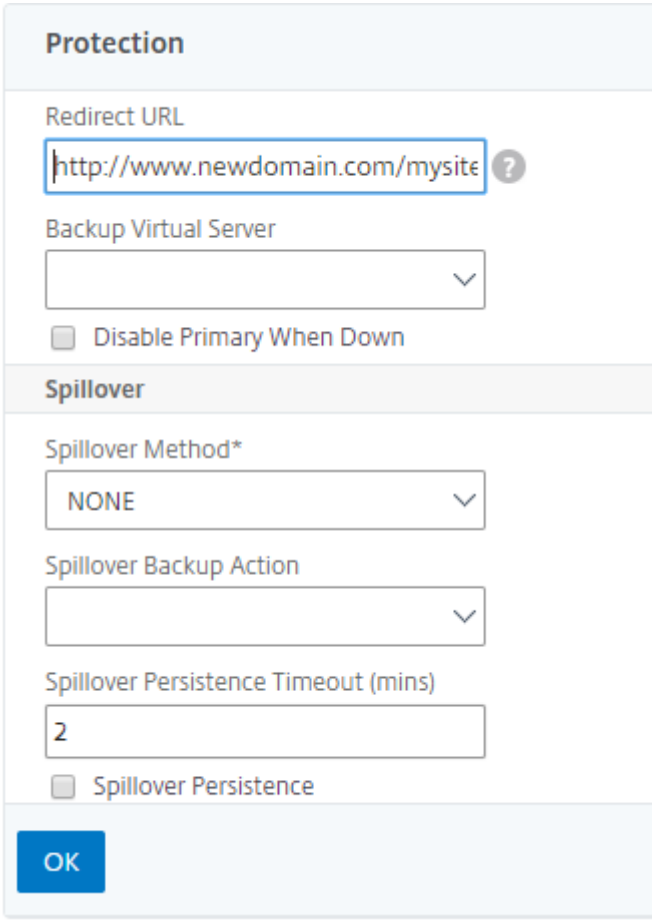
4. Habilite el servidor virtual.

   ```
   enable vserver <vserver_name>
   ```

Para configurar un servidor virtual para redirigir la solicitud del cliente a una URL mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. En el panel de detalles, para agregar un nuevo servidor virtual, haga clic en **Agregar**.
3. Para modificar un servidor virtual existente, seleccione el servidor virtual de la lista y haga clic en **Modificar**.
4. En la ficha **Configuración avanzada**, haga clic en **Protección**. En el campo **URL de redirección**, escriba la URL de redirección (por ejemplo, http://www.newdomain.com/mysite/maintenance).





5. Haga clic en **Aceptar**.

Configurar un servidor virtual de equilibrio de carga de copia de seguridad

August 20, 2021

Puede configurar el dispositivo Citrix ADC para dirigir las solicitudes a un servidor virtual de copia de seguridad cuando el servidor virtual de equilibrio de carga principal está INHABILITADO o no está disponible. El servidor virtual de copia de seguridad es un proxy y es transparente para el cliente. El dispositivo también puede enviar un mensaje de notificación al cliente en relación con la interrupción del sitio.

> Nota:
>
> El servidor virtual de copia de seguridad sigue manejando las conexiones existentes, incluso después de que se haya eliminado o inhabilitado el servidor virtual principal.

Puede configurar un servidor virtual de equilibrio de carga de copia de seguridad al crearlo, o puede cambiar los parámetros opcionales de un servidor virtual existente. También puede configurar un servidor virtual de copia de seguridad para un servidor virtual de copia de seguridad existente, creando así servidores virtuales de copia de seguridad en cascada. La profundidad máxima de los servidores virtuales de backup en cascada es 10.

Si tiene varios servidores virtuales que se conectan a dos servidores, puede elegir lo que sucede si el servidor virtual principal baja y vuelve a aparecer. El comportamiento predeterminado es que el servidor virtual principal reanude su función como principal. Sin embargo, puede configurar el servidor virtual de copia de seguridad para que mantenga el control cuando se haga cargo. Por ejemplo, puede sincronizar las actualizaciones del servidor virtual de copia de seguridad con el servidor virtual principal y, a continuación, forzar manualmente al servidor principal original a reanudar su función. En este caso, puede designar el servidor virtual de copia de seguridad para que mantenga el control cuando el servidor virtual principal se desactiva y vuelva a aparecer.

Puede configurar una dirección URL de redirección en el servidor virtual de equilibrio de carga principal como alternativa para cuando los servidores virtuales principal y de copia de seguridad estén DOWN o hayan alcanzado su umbral para gestionar solicitudes. Cuando los servicios enlazados a servidores virtuales están fuera de servicio, el dispositivo utiliza la dirección URL de redirección.

Nota: Si un servidor virtual de equilibrio de carga está configurado tanto con un servidor virtual de copia de seguridad como con una URL de redirección, el servidor virtual de copia de seguridad tiene prioridad sobre la URL de redirección. Una redirección se utiliza solo cuando los servidores virtuales principales y de copia de seguridad están inactivos.

Para establecer un servidor virtual de copia de seguridad mediante la CLI

En el símbolo del sistema, escriba:

```
set lb vserver <vServerName> -backupVserver <BackupVServerName> [-
   disablePrimaryOnDown]
<!--NeedCopy-->
```

Ejemplo:

```
set lb vserver Vserver-LB-1 -backupVserver Vserver-LB-2 -
   disablePrimaryOnDown
<!--NeedCopy-->
```


Para establecer un servidor virtual de copia de seguridad mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**y abra el servidor virtual.
2. En Configuración avanzada, haga clic en **Protección** y seleccione un servidor virtual de copia de seguridad.
3. Si quiere que el servidor virtual de copia de seguridad permanezca en control hasta que habilite manualmente el servidor virtual principal, incluso si el servidor virtual principal vuelve a activarse, seleccione **Inhabilitar primario cuando está desactivado**.

> **Nota:** A partir de Citrix ADC versión 12.1 build 51.xx, la GUI muestra el estado efectivo de ese servidor indicando si la copia de seguridad está activa o no.
>
> El estado efectivo del servidor actual puede ser uno de los siguientes:
>
> - **UP**: Indica que el servidor está UP
> - **DOWN**: Indica que el servidor está DOWN
> - **UP (Copia de seguridad activa)**: Indica que el servidor virtual principal o secundario está UP y el tráfico se dirige al servidor virtual de copia de seguridad.
> - **DOWN (Copia de seguridad activa)**: Indica que tanto los servidores virtuales principales como los de copia de seguridad están inactivos y el tráfico se enruta al servidor virtual de copia de seguridad.
>
> Cuando la opción **Inhabilitar primario cuando está desactivado** está habilitada en el servidor virtual principal y el servidor principal baja y vuelve a estar UP, el servidor virtual de copia de seguridad seguirá sirviendo el tráfico hasta que el servidor virtual principal se vuelva a habilitar explícitamente. Puede utilizar el comando `enable lb vserver <vserver_name>` para volver a habilitar el servidor virtual principal.

Configurar desbordamiento

August 20, 2021

Una configuración de desbordamiento en el dispositivo consiste en un servidor virtual principal configurado con un método de desbordamiento, un umbral de desbordamiento y un servidor virtual de copia de seguridad. Los servidores virtuales de copia de seguridad también se pueden configurar para el desbordamiento, creando una cadena de servidores virtuales de copia de seguridad.

El método spillover especifica la condición operativa en la que quiere basar la configuración de desbordamiento (por ejemplo, el número de conexiones establecidas, el ancho de banda o el estado combinado de la comunidad de servidores). Cuando llega una nueva conexión, el dispositivo com-

prueba que el servidor virtual principal está activo y compara la condición operativa con el umbral de desbordamiento configurado. Si se alcanza el umbral, la función de desbordamiento desvía nuevas conexiones al primer servidor virtual disponible en la cadena de copia de seguridad. El servidor virtual de copia de seguridad administra las conexiones que recibe hasta que la carga en el primario cae por debajo del umbral.

Si configura la persistencia de desbordamiento, el servidor virtual de copia de seguridad continúa procesando las conexiones recibidas, incluso después de que la carga en el primario caiga por debajo del umbral. Si configura la persistencia de spillover y un tiempo de espera de persistencia de spillover, el servidor virtual de copia de seguridad procesa las conexiones solo durante el período especificado después de que la carga en el primario caiga por debajo del umbral.

Nota: Normalmente, el derrame se activa si el valor asociado con el método de derrame excede el umbral (por ejemplo, número de conexiones). Sin embargo, con el método de derrame de mantenimiento del servidor, se desencadena si el estado de la comunidad de servidores cae por debajo del umbral.

Puede configurar spillover de una de las siguientes maneras:

- Especifique un método de difusión predefinido. Hay cuatro métodos predefinidos disponibles y cumplen con los requisitos comunes de propagación.
- Configurar el desbordamiento basado en directivas. En la extensión basada en directivas, se utiliza una regla de Citrix ADC para especificar las condiciones para que se produzca la propagación. Las reglas Citrix ADC le ofrecen la flexibilidad necesaria para configurar el desbordamiento para diversas condiciones operativas.

Utilice el desbordamiento basado en directivas si un método predefinido no satisface sus requisitos. Si configura ambos para un servidor virtual principal, la configuración de propagación basada en directivas tiene prioridad sobre el método predefinido.

En primer lugar, crea el servidor virtual principal y los servidores virtuales que necesita para la cadena de copia de seguridad. Para configurar la cadena de copia de seguridad, especifique un servidor virtual como copia de seguridad para el principal (es decir, crear un servidor virtual secundario), un servidor virtual como copia de seguridad para el secundario (es decir, crear un servidor virtual terciario), etc. A continuación, puede configurar el desbordamiento especificando un método de desbordamiento predefinido o creando y vinculando directivas de desbordamiento.

Para obtener instrucciones sobre cómo asignar un servidor virtual como copia de seguridad de otro servidor virtual, consulte Configuración de un servidor virtual de equilibrio de carga de respaldo.

Configurar un método de desbordamiento predefinido

Los métodos de desbordamiento predefinidos cumplen algunos de los requisitos de desbordamiento más comunes. Para utilizar uno de los métodos de desbordamiento predefinidos, configure los

parámetros de desbordamiento en el servidor virtual principal. Para crear una cadena de servidores virtuales de copia de seguridad, también puede configurar parámetros de desbordamiento en servidores virtuales de copia de seguridad.

Si los servidores virtuales de copia de seguridad alcanzan sus propios valores de umbral y el tipo de servicio es TCP, el dispositivo Citrix ADC envía a los clientes un restablecimiento de TCP. Para los tipos de servicio HTTP, SSL y RTSP, desvía nuevas solicitudes a la URL de redirección configurada para el servidor virtual principal. Solo se puede especificar una dirección URL de redirección para servidores virtuales HTTP, SSL y RTSP. Si no se configura una dirección URL de redirección, el dispositivo Citrix ADC envía a los clientes un restablecimiento de TCP (si el servidor virtual es de tipo TCP) o una respuesta HTTP 503 (si el servidor virtual es de tipo HTTP o SSL).

Nota: Con los servidores virtuales RTSP, el dispositivo Citrix ADC utiliza solo conexiones de datos para el desbordamiento. Si el servidor virtual RTSP de copia de seguridad no está disponible, las solicitudes se redirigen a una URL RTSP y se envía un mensaje de redirección RTSP al cliente.

Para configurar un método de desbordamiento predefinido para un servidor virtual mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
set lb vserver <vServerName> -soMethod <spillOverType> -soThreshold <
    positiveInteger> -soPersistence ENABLED -soPersistenceTimeout <
    positiveInteger>
<!--NeedCopy-->
```

Ejemplo

```
set lb vserver Vserver-LB-1 -soMethod Connection -soThreshold 1000 -
    soPersistence enabled -soPersistenceTimeout 2
<!--NeedCopy-->
```

Para configurar un método de desbordamiento predefinido para un servidor virtual mediante la utilidad de configuración

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**y abra el servidor virtual.
2. En Configuración avanzada, haga clic en **Protección** y establezca los parámetros de propagación.

Configurar el desbordamiento basado en directivas

Las directivas de desbordamiento, basadas en reglas (expresiones), permiten configurar el dispositivo para una gama más amplia de casos de desbordamiento. Por ejemplo, puede configurar el spillover en función del tiempo de respuesta del servidor virtual o en función del número de conexiones de la cola de sobretensiones del servidor virtual.

Para configurar el desbordamiento basado en directivas, primero cree una acción de desbordamiento. A continuación, seleccione la expresión que quiere utilizar en la directiva de desbordamiento, configure la directiva y asocie la acción a ella. Por último, vincula la directiva de desbordamiento a un servidor virtual de equilibrio de carga, conmutación de contenido o equilibrio de carga de servidor global. Puede enlazar varias directivas de desbordamiento a un servidor virtual, con números de prioridad. El dispositivo evalúa las directivas de desbordamiento en orden ascendente de números de prioridad y realiza la acción asociada a la última directiva que se va a evaluar como TRUE.

Un servidor virtual también puede tener una acción de copia de seguridad. La acción de copia de seguridad se realiza si el servidor virtual no tiene uno o más servidores virtuales de copia de seguridad, o si todos los servidores virtuales de copia de seguridad están ABAJOS, inhabilitados o han alcanzado sus propios límites de propagación.

Cuando una directiva de propagación da lugar a una condición de UNDEF (una excepción que se produce cuando el resultado de la evaluación de directivas no está definido), se realiza una acción del UNDEF. La acción UNDEF siempre es ACEPTAR. No puede especificar una acción UNDEF de su elección.

Configuración de una acción de desbordamiento

Una acción de desbordamiento se realiza cuando la directiva de desbordamiento con la que está asociada se evalúa como TRUE. Actualmente, SPILLOVER es la única acción de desbordamiento admitida.

Para configurar el desbordamiento basado en directivas mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para configurar una directiva de desbordamiento y compruebe la configuración:

```
add spillover action <name> -action SPILLOVER

show spillover action <name>
<!--NeedCopy-->
```


Ejemplo

```
add spillover action mySoAction -action SPILLOVER
Done
<!--NeedCopy-->
```

```
show spillover action mySoAction
1) Name: mySoAction Action: SPILLOVER
Done
<!--NeedCopy-->
```

Selección de una expresión para la directiva de desbordamiento

En la expresión de directiva, puede utilizar cualquier expresión basada en servidor virtual que devuelva un valor booleano. Por ejemplo, puede utilizar una de las siguientes expresiones:

```
SYS.VSERVER("vserver").RESPTIME.GT(<int>)
SYS.VSERVER("vserver").STATE.EQ( " <string>" ), and
SYS.VSERVER("vserver").THROUGHPUT.LT    (<int>)
<!--NeedCopy-->
```

Además de las funciones existentes, como RESPTIME, STATE y DREFACHORD, puede utilizar las siguientes funciones basadas en servidores virtuales que se han introducido con esta función:

`Averagesurgecount`

Devuelve el número medio de solicitudes en las colas de sobrecarga de servicios activos. Devuelve 0 (cero) si no hay servicios activos. Genera una condición UNDEF si se utiliza con un servidor virtual de equilibrio de carga de servidor global o conmutación de contenido.

`Activeservices`

Devuelve el número de servicios activos. Genera una condición UNDEF si se utiliza con un servidor virtual de equilibrio de carga de servidor global o conmutación de contenido.

`Activetransactions`

Devuelve el valor del contador de nivel de servidor virtual para las transacciones activas actuales.

is_dynamic_limit_alcanzado

Devuelve un valor Boolean TRUE si el número de conexiones que administra el servidor virtual es igual al umbral calculado dinámicamente. El umbral dinámico es la suma de la configuración máxima del cliente (Clientes máximos) de los servicios enlazados que son UP.

Puede utilizar una expresión de directiva para implementar cualquiera de los métodos de difusión predefinidos. La siguiente tabla asigna los métodos de difusión predefinidos a las expresiones que puede utilizar para implementarlos:

Cuadro 1 Conversión de métodos de difusión predefinidos en expresiones de directiva

Método de difusión predefinido	Expresión correspondiente
CONEXIÓN	SYS.VSERVER("<vserver-name>").CONNECTIONS, utilizado con la función aritmética GT(int).
ANCHO DE BANDA	SYS.VSERVER("<vserver-name>").THROUGHPUT, utilizado con la función aritmética GT(int).
SALUD	SYS.VSERVER("<vserver-name>").HEALTH, utilizado con la función aritmética LT(int).
CONEXIÓN DINÁMICA	SYS.VSERVER ("<vserver-name>").IS_DYNAMIC_LIMIT_REACHED **Nota**: Si implementa el spillover basado en directivas mediante la función IS_DYNAMIC_LIMIT_REACHED, también debe configurar el método DYNAMICCONNECTION predefinido para el servidor virtual, de modo que las estadísticas necesarias para que el spillover funcione se recogen.

Configuración de una directiva de desbordamiento

Una directiva de desbordamiento utiliza una expresión booleana como regla para especificar las condiciones que deben cumplirse para que se produzca el desbordamiento.

Para configurar una directiva de desbordamiento mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para configurar una directiva de desbordamiento y compruebe la configuración:


```
add spillover policy <name> -rule <expression> -action <string> [-
    comment <string>]

show spillover policy <name>
<!--NeedCopy-->
```

Ejemplo

```
> add spillover policy mySoPolicy -rule SYS.VSERVER("v1").RESPTIME.GT
    (50) -action mySoAction -comment "Triggers spillover when the
    vserver's response time is greater than 50 ms."
Done

> show spillover policy mySoPolicy

1)  Name: mySoPolicy Rule: "SYS.VSERVER("v1").RESPTIME.GT(50)" Action:
    mySoAction Hits: 0 ActivePolicy: 0
Comment: "Triggers spillover when the vserver's response time is
    greater than 50 ms."
Done
>
<!--NeedCopy-->
```

Vinculación de una directiva de desbordamiento a un servidor virtual

Puede vincular una directiva de desbordamiento a los servidores virtuales de equilibrio de carga, conmutación de contenido o equilibrio de carga de servidores globales). Puede enlazar varias directivas a un servidor virtual, con las expresiones Goto que controlan el flujo de evaluación.

Para enlazar una directiva de desbordamiento a un servidor virtual mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los comandos siguientes para enlazar una directiva de desbordamiento a un servidor virtual de equilibrio de carga, conmutación de contenido o equilibrio de carga de servidor global y compruebe la configuración:


```
bind (lb | cs | gslb) vserver <name> -policyName <string> -priority <
    positive_integer> [-gotoPriorityExpression <expression>]

show (lb | cs | gslb) vserver <name>
<!--NeedCopy-->
```

Ejemplo

```
> bind lb vserver vserver1 -policyName mySoPolicy -priority 5
Done
> show lb vserver vserver1
vserver1 (2.2.2.12:80) - HTTP Type: ADDRESS
. . .

1)  Spillover Policy Name: mySoPolicy Priority: 5
GotoPriority Expression: END
Flowtype: REQUEST
Done
>
<!--NeedCopy-->
```

Configuración de una acción de copia de seguridad para un evento de desbordamiento

Una acción de copia de seguridad especifica qué hacer cuando se alcanza el umbral de desbordamiento, pero uno o más servicios virtuales de copia de seguridad no están configurados o están inactivados, inhabilitados o han alcanzado sus propios umbrales.

Nota: Para los métodos de desbordamiento predefinidos que se configuran directamente en el servidor virtual (como valores del parámetro Método de desbordamiento), la acción de copia de seguridad no es configurable. De forma predeterminada, el dispositivo envía a los clientes un restablecimiento de TCP (si el servidor virtual es de tipo TCP) o una respuesta HTTP 503 (si el servidor virtual es de tipo HTTP o SSL).

La acción de copia de seguridad se configura en el servidor virtual. Puede configurar el servidor virtual para que acepte solicitudes (después de alcanzar el umbral especificado por la directiva), redirigir clientes a una URL o simplemente eliminar solicitudes incluso antes de establecer conexiones TCP o SSL hasta que el número de solicitudes caiga por debajo del umbral. Por lo tanto, se utilizan recursos de memoria menores a medida que las conexiones se restablecen incluso antes de asignar estructuras de datos.

Para configurar una acción de copia de seguridad para el desbordamiento mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para configurar una acción de copia de seguridad y verificar la configuración:

```
set lb vserver <name> -soBackupAction <soBackupAction>

show lb vserver <name>
<!--NeedCopy-->
```

Ejemplo:

```
set lb vserver vs1 -soBackupAction REDIRECT -redirectURL `http://www.
   mysite.com/maintenance`
Done
> show lb vserver vs1
vs1 (10.102.29.76:80) - HTTP Type: ADDRESS
State: UP
. . .
Redirect URL: `http://www.mysite.com/maintenance`
. . .
Done
<!--NeedCopy-->
```

Para configurar una acción de copia de seguridad para el desbordamiento mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**y abra el servidor virtual.
2. En Configuración avanzada, haga clic en **Protección** y, a continuación, especifique una acción de copia de seguridad de desbordamiento.

Failover de conexión

June 22, 2022

La conmutación por error de conexión ayuda a evitar la interrupción del acceso a las aplicaciones implementadas en un entorno distribuido. En una configuración de alta disponibilidad (HA) de Citrix

ADC, la *conmutación por error* de *conexión (o duplicación*de conexiones,*CM*) se refiere a mantener activa una conexión TCP o UDP establecida cuando se produce una conmutación por error. El nuevo dispositivo Citrix ADC principal tiene información sobre las conexiones establecidas antes de la conmutación por error y continúa sirviendo esas conexiones. Tras la conmutación por error, el cliente permanece conectado al mismo servidor físico. El nuevo dispositivo principal sincroniza la información con el nuevo dispositivo secundario. Si se establece el parámetro L2Conn, los parámetros de conexión de Capa 2 también se sincronizan con el secundario.

> Nota:
>
> Considere una configuración de alta disponibilidad, en la que un cliente establece una sesión con el nodo principal, que a su vez establece una sesión con el servidor back-end. Cuando se activa una conmutación por error en este estado, los paquetes recibidos en un nuevo primario de los nodos cliente y servidor existentes se tratan como paquetes obsoletos y se restablecen las conexiones cliente y servidor. Mientras que si la conmutación por error de conexión sin estado está habilitada (USIP está ACTIVADO), después de la conmutación por error, las conexiones no se restablecen cuando recibe paquetes de nodos cliente o servidor. En cambio, las conexiones de cliente y servidor se crean dinámicamente.

Puede configurar la conmutación por error de conexión en modo sin estado o con estado. En el modo de conmutación por error de conexión sin estado, los nodos HA no intercambian información sobre las conexiones que se conmutan por error. Este método no tiene sobrecarga de tiempo de ejecución.

En el modo de conmutación por error de conexión con estado, el dispositivo principal sincroniza los datos de las conexiones de conmutación por error con el nuevo dispositivo secundario.

La conmutación por error de conexión es útil si la implementación tiene conexiones de larga duración. Por ejemplo, si está descargando un archivo grande a través de FTP y se produce una conmutación por error durante la descarga, la conexión se interrumpe y se anula la descarga. Sin embargo, si configura la conmutación por error de conexión en modo con estado, la descarga continúa incluso después de la conmutación por error.

Cómo funciona la conmutación por error de conexión en dispositivos Citrix ADC

En una conmutación por error de conexión sin estado, el nuevo dispositivo principal intenta volver a crear el flujo de paquetes de acuerdo con la información contenida en los paquetes que recibe.

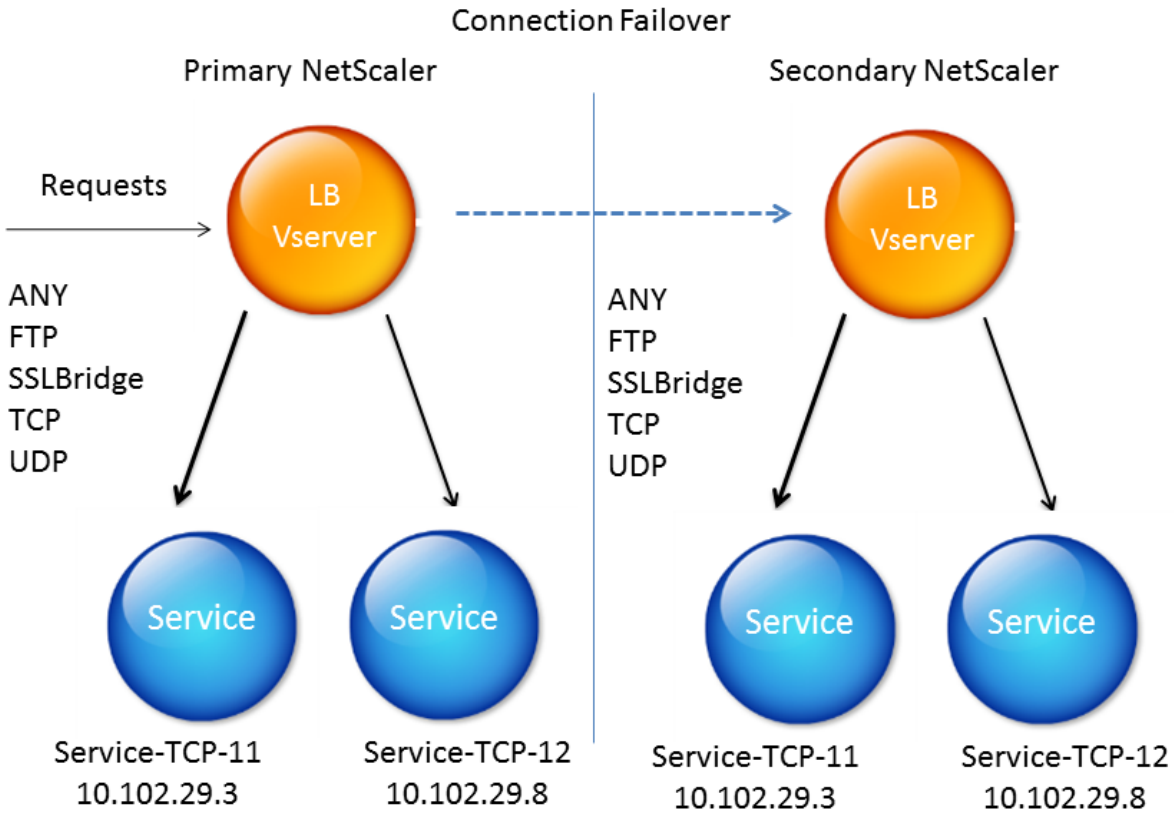
En caso de conmutación por error con estado, para mantener la información actual sobre las conexiones reflejadas, el dispositivo principal envía mensajes al dispositivo secundario. El dispositivo secundario mantiene los datos relacionados con los paquetes, pero solo los usa en caso de una conmutación por error. Si se produce una conmutación por error, el nuevo dispositivo principal (antiguo secundario) comienza a utilizar los datos almacenados sobre las conexiones reflejadas y aceptar tráfico. Durante el período de transición, el cliente y el servidor pueden experimentar una breve interrupción y retransmisiones.

Nota:

Compruebe que el dispositivo principal puede autorizarse en el dispositivo secundario. Para verificar la correcta configuración de las contraseñas, utilice el comando `rpcnode` show desde la línea de comandos o utilice la opción RPC del menú **Red** de la GUI.

Una configuración básica de alta disponibilidad con conmutación por error de conexión contiene las entidades que se muestran en la siguiente ilustración.

Ilustración 1. Diagrama de entidad de conmutación por error de conexión



Nota

La conmutación por error de conexión no se admite después de cualquiera de los siguientes eventos:

```
- An upgrade to a later release.
- An upgrade to a later build within the same release, if the new
    build uses a different HA version.
```


Configuración admitida

La conmutación por error de conexión solo se puede configurar en servidores virtuales de equilibrio de carga. No se puede configurar en servidores virtuales de conmutación de contenido. Si habilita la conmutación por error de conexión en los servidores virtuales de equilibrio de carga conectados a un servidor virtual de conmutación de contenido, la conmutación por error de conexión no funciona porque los servidores virtuales de equilibrio de carga no aceptan inicialmente el tráfico.

En la siguiente tabla se describe la configuración admitida para la conmutación por error de conexión.

Tabla 1. Conmutación por error de conexión: configuración compatible

Parámetro	apátridas	Con estado
Tipo de servicio	CUALQUIERA.	CUALQUIERA, UDP, TCP, FTP, SSL_BRIDGE.
Métodos de equilibrio de carga	Todos los métodos admitidos para el tipo de servicio ANY. Sin embargo, si no se establece la persistencia de IP de origen, se debe usar el método SRCIPSRCPORTHASH.	Todos los métodos aplicables a los tipos de servicios admitidos.
Tipos de persistencia	Persistencia de SOURCEIP.	Se admiten todos los tipos aplicables a los tipos de servicio admitidos.
USIP	Debe estar encendido.	Sin restricciones. Puede estar ENCENDIDO o APAGADO.
Fijaciones de servicio	El servicio solo se puede vincular a un servidor virtual.	El servicio se puede vincular a uno o más servidores virtuales.
Versiones de protocolo de Internet (IP)	IPv4 e IPv6	IPV4 e IPv6
Soporte de redundancia	Clústeres y alta disponibilidad	Alta disponibilidad
Modo INC	No se admite	Se admite cuando el tipo de servicio de servidor virtual es ANY, el modo es DSR (MAC, IPTUNNEL, TOS) y USIP está habilitado en los servicios enlazados al servidor virtual.

> **Nota:**
>
> La conmutación por error de conexión con estado solo se admite para los servicios de conmutación basados en conexión, por ejemplo, TCP. Dado que HTTP utiliza conmutación basada en solicitudes, no admite la conmutación por error de conexión. En SSL, las conexiones existentes se restablecen tras la conmutación por error.

Funciones afectadas por la conmutación por error de conexión

En la siguiente tabla se enumeran las funciones afectadas si se configura la conmutación por error de conexión.

Tabla 2. Cómo afecta la conmutación por error de conexión a las funciones Citrix ADC

Función	Impacto del failover de conexión
Protección SYN	Para cualquier conexión, si se produce una conmutación por error después de que el dispositivo emite SYN-ACK pero antes de recibir el ACK final, la conexión no es compatible con la conmutación por error de conexión. El cliente debe volver a emitir la solicitud para establecer la conexión.
Protección contra picos de tensión	Si la conmutación por error se produce antes de establecer una conexión con el servidor, el nuevo dispositivo principal intenta establecer la conexión con el servidor. También retransmite todos los paquetes que se mantienen durante la protección contra sobretensiones.
Acceso no disponible	Si está habilitada, la funcionalidad de acceso no disponible tiene prioridad sobre la conmutación por error de conexión.
Firewall de aplicaciones	No se admite la función de firewall de aplicaciones.

Función	Impacto del failover de conexión
INCLUYE	La configuración de red independiente (INC) solo se admite en el modo de alta disponibilidad cuando el tipo de servicio del servidor virtual es ANY, el modo es DSR (MAC, IPTUNNEL, TOS) y USIP está habilitado en los servicios enlazados al servidor virtual. En todos los demás casos, INC no es compatible.
Almacenamiento en búfer TCP	El almacenamiento en búfer TCP no es compatible con la duplicación de conexiones.
Cerrar en la respuesta	Tras la conmutación por error, es posible que los NATPCB no se cierren en respuesta.

Para configurar la conmutación por error de conexión mediante GUI

Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**. Abra el servidor virtual y, en **Configuración avanzada**, haga clic en **Protección**y seleccione **Conmutación por error de conexión como Conestado**.

Para configurar la conmutación por error de conexión mediante la CLI

En el símbolo del sistema:

```
set lb vserver <vServerName> -connFailover <Value>
show lb vserver <vServerName>
<!--NeedCopy-->
```

Ejemplo:

```
set lb vserver Vserver-LB-1 -connFailover stateful
Done
<!--NeedCopy-->
```

Cuando se inhabilita la conmutación por error de conexión en un servidor virtual, se liberan los recursos asignados al servidor virtual.

Para inhabilitar la conmutación por error de conexión mediante la CLI

En el símbolo del sistema:

```
set lb vserver <vServerName> -connFailover <Value>
show lb vserver <vServerName>
<!--NeedCopy-->
```

Ejemplo:

```
set lb vserver Vserver-LB-1 -connFailover disable
Done
<!--NeedCopy-->
```

Para inhabilitar la conmutación por error de conexión mediante GUI

Vaya a **Administración del tráfico**> **Equilibrio de carga**> **Servidores virtuales**. Abra el servidor virtual, en **Protección**, seleccione **Conmutación por error de conexión** como Desactivado.

Vacíe la cola de sobretensiones

August 20, 2021

Cuando un servidor físico recibe un aumento de solicitudes, se vuelve lento para responder a los clientes que están conectados actualmente a él, lo que deja a los usuarios insatisfechos y descontentos. A menudo, la sobrecarga también hace que los clientes reciban páginas de error. El dispositivo Citrix ADC proporciona funciones tales como protección contra sobretensiones, que controla la velocidad a la que se pueden establecer nuevas conexiones a un servicio y evitar así sobrecargas.

El dispositivo realiza multiplexación de conexión entre clientes y servidores físicos. Cuando recibe una solicitud de cliente para acceder a un servicio en un servidor, el dispositivo busca una conexión ya establecida con el servidor que sea gratuita. Si encuentra una conexión libre, utiliza esa conexión para establecer un vínculo virtual entre el cliente y el servidor. Si no encuentra una conexión libre existente, el dispositivo establece una nueva conexión con el servidor y establece un vínculo virtual entre el cliente y el servidor. Sin embargo, si el dispositivo no puede establecer una nueva conexión con el servidor, envía la solicitud del cliente a una cola de sobretensiones. Si todos los servidores físicos vinculados al servidor virtual de equilibrio de carga o de cambio de contenido alcanzan el límite superior de las conexiones de cliente (valor máximo del cliente, umbral de protección contra sobretensiones

o capacidad máxima del servicio), el dispositivo no podrá establecer una conexión con ningún servidor. La función de protección contra sobretensiones utiliza la cola de sobretensiones para regular la velocidad a la que se abren las conexiones con los servidores físicos. El dispositivo mantiene una cola de sobretensión diferente para cada servicio vinculado al servidor virtual.

La longitud de una cola de sobretensiones aumenta cada vez que recibe una solicitud para la que el dispositivo no puede establecer una conexión. La longitud de una cola de sobretensiones disminuye en cualquiera de las siguientes condiciones:

- Una solicitud de la cola se envía al servidor.
- Se agota el tiempo de espera de una solicitud y se elimina de la cola.

Si la cola de sobretensión de un servicio o grupo de servicios es demasiado larga, es posible que desee vaciarla. Puede vaciar la cola de sobretensiones de un servicio o grupo de servicios específico, o de todos los servicios y grupos de servicios vinculados a un servidor virtual de equilibrio de carga. El vaciado de una cola de sobretensión no afecta a las conexiones existentes. Solo se eliminan las solicitudes presentes en la cola de sobretensiones. Para esas solicitudes, el cliente tiene que hacer una nueva solicitud.

También puede vaciar la cola de sobretensiones de un servidor virtual de cambio de contenido. Si un servidor virtual de cambio de contenido reenvía algunas solicitudes a un servidor virtual de equilibrio de carga determinado y el servidor virtual de equilibrio de carga también recibe otras solicitudes, al vaciar la cola de sobretensión del servidor virtual de cambio de contenido, solo las solicitudes recibidas de esta cambio de contenido servidor virtual se vacían. Las demás solicitudes de la cola de sobretensión del servidor virtual de equilibrio de carga no se vacían.

Nota: No puede vaciar las colas de sobretensión de redirección de caché, autenticación, servidores virtuales VPN o GSLB o servicios GSLB.

Nota: No utilice la función Protección contra sobretensiones si está habilitada la opción Usar IP de origen (USIP).

Para vaciar una cola de sobretensiones mediante la CLI

El comando flush ns SurgeQ funciona de la siguiente manera:

- Puede especificar el nombre de un servicio, grupo de servicios o servidor virtual cuya cola de sobretensiones debe vaciarse.
- Si especifica un nombre mientras se ejecuta el comando, se vacía la cola de sobretensión de la entidad especificada. Si más de una entidad tiene el mismo nombre, el dispositivo vacía las colas de sobretensión de todas esas entidades.
- Si especifica el nombre de un grupo de servicios y un nombre de servidor y un puerto mientras ejecuta el comando, el dispositivo vacía la cola de sobretensión solo del miembro del grupo de servicio especificado.

- No puede especificar directamente un miembro del grupo de servicios (<serverName> y <port>) sin especificar el nombre del grupo de servicios (<name>) y no puede especificar <port> sin una<serverName>. Especifique <serverName> y <port> si quiere vaciar la cola de sobretensión para un miembro del grupo de servicios específico.
- Si ejecuta el comando sin especificar ningún nombre, el dispositivo vacía las colas de sobretensión de todas las entidades presentes en el dispositivo.
- Si un miembro del grupo de servicios se identifica con un nombre de servidor, debe especificar el nombre del servidor en este comando; no puede especificar su dirección IP.

En el símbolo del sistema, escriba:

```
flush ns surgeQ [-name <name>] [-serverName <serverName> <port>]
<!--NeedCopy-->
```

Ejemplos

```
flush ns surgeQ -name SVC1ANZGB -serverName 10.10.10.1 80
<!--NeedCopy-->
```

El comando anterior vacía la cola de sobretensiones del servicio o servidor virtual denominado SVC1ANZGB y tiene una dirección IP como 10.10.10.

```
flush ns surgeQ
<!--NeedCopy-->
```

El comando anterior vacía todas las colas de sobretensiones del dispositivo.

Para vaciar una cola de sobretensiones mediante la interfaz gráfica de usuario

Vaya a **Administración del tráfico** > **Cambio de contenido** > **Servidores virtuales**, seleccione un servidor virtual y, en la lista Acción, seleccione **Cola de sobretensiones de vaciado**.

Administrar una configuración de equilibrio de carga

August 20, 2021

Una configuración de equilibrio de carga existente no requiere mucho trabajo para mantener mientras no se modifique, pero la mayoría no permanece sin cambios durante mucho tiempo. El aumento de la

carga requiere nuevos servidores equilibrados de carga y, finalmente, nuevos dispositivos Citrix ADC, que deben configurarse y agregarse a la configuración existente. Los servidores antiguos se desgastan y deben reemplazarse, lo que requiere la eliminación de algunos servidores y la adición de otros. Las actualizaciones de los equipos de red o los cambios en la topología también pueden requerir modificaciones en la configuración del equilibrio de carga. Por lo tanto, debe realizar operaciones en objetos de servidor, servicios y servidores virtuales. El Visualizador puede mostrar la configuración gráficamente y puede realizar operaciones en las entidades de la visualización. También puede aprovechar otras funciones que facilitan la administración del tráfico mediante la configuración del equilibrio de carga.

Administrar objetos de servidor

August 20, 2021

Durante la configuración básica del equilibrio de carga, al crear un servicio, se crea un objeto de servidor con la dirección IP del servicio, si no existe uno. Si prefiere los objetos de servicio nombrados con nombres de dominio en lugar de direcciones IP, es posible que también haya creado uno o varios objetos de servidor manualmente. Puede habilitar, inhabilitar o quitar cualquier objeto de servidor.

Cuando habilita o inhabilita un objeto de servidor, habilita o inhabilita todos los servicios asociados al objeto de servidor. Cuando actualiza el dispositivo Citrix ADC después de inhabilitar un objeto de servidor, el estado de su servicio aparece como OUT ODE SERVICIO. Si especifica un tiempo de espera al inhabilitar un objeto de servidor, el objeto de servidor continúa manejando las conexiones establecidas durante el tiempo especificado, pero rechaza las nuevas conexiones. Si quita un objeto de servidor, también se elimina el servicio al que está vinculado.

Para habilitar un servidor mediante la CLI

En el símbolo del sistema, escriba:

```
enable server <name>
<!--NeedCopy-->
```

Ejemplo:

```
enable server 10.102.29.5
<!--NeedCopy-->
```


Para habilitar o inhabilitar un objeto de servidor mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores**.
2. Seleccione el servidor y, en la lista Acción, seleccione **Habilitar** o **Inhabilitar**.

Para inhabilitar un objeto de servidor mediante la CLI

En el símbolo del sistema, escriba:

```
disable server <name> <delay>
<!--NeedCopy-->
```

Ejemplo:

```
disable server 10.102.29.5 30
<!--NeedCopy-->
```

Para quitar un objeto de servidor mediante la CLI

En el símbolo del sistema, escriba:

```
rm server <name>
<!--NeedCopy-->
```

Ejemplo:

```
rm server 10.102.29.5
<!--NeedCopy-->
```

Para eliminar un objeto de servidor mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores**.
2. Seleccione un servidor y haga clic en **Quitar**.

Administrar servicios

August 20, 2021

Los servicios se habilitan de forma predeterminada al crearlos. Puede inhabilitar o habilitar cada servicio individualmente. Al inhabilitar un servicio, normalmente se especifica un tiempo de espera durante el cual el servicio continúa manejando las conexiones establecidas, pero rechaza las nuevas, antes de cerrarlas. Si no especifica un tiempo de espera, el servicio se apaga inmediatamente. Durante el tiempo de espera, el estado del servicio es fuera de servicio.

Puede eliminar un servicio cuando ya no se utilice. Cuando se quita un servicio, se desvincula de su servidor virtual y se elimina de la configuración de Citrix ADC.

Para habilitar o inhabilitar un servicio mediante la CLI

En el símbolo del sistema, escriba:

```
enable service <name>

disable service <name> <DelayInSeconds>
<!--NeedCopy-->
```

Ejemplos:

```
enable service Service-HTTP-1
disable service Service-HTTP-1 30
<!--NeedCopy-->
```

Para habilitar o inhabilitar un servicio mediante la interfaz gráfica de usuario

1. Vaya a **Administración de Tráfico > Equilibrio de carga > Servicios**.
2. Abra un servicio y, en la lista **Acción**, seleccione **Habilitar** o **Inhabilitar**.

Identifique la causa del estado del servicio marcado hacia abajo mediante la interfaz gráfica de usuario

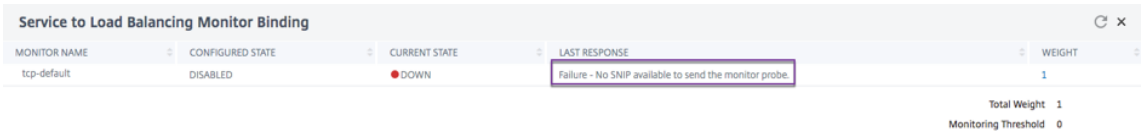
A partir de Citrix ADC versión 13.0 compilación 41.20, puede ver la información del sondeo del monitor en la GUI de los servicios que están DOWN sin desplazarse a la interfaz de enlace del monitor. Se puede

hacer clic en el valor de la columna **Estado del servidor** de la página Servicios. Puede hacer clic en **DOWN** para identificar la causa raíz por la cual el servicio está marcado como DOWN.

1. Vaya a **Administración de Tráfico > Equilibrio de carga > Servicios**.
2. Haga clic en **DOWN** en la columna **Estado del servidor** correspondiente al servicio que es DOWN.

Aparecerá la página Enlace del Monitor de Equilibrio de Servicio a Carga.

La columna **Última respuesta** muestra el motivo por el cual el servicio está marcado como DOWN.



Administrar un servidor virtual de equilibrio de carga

August 20, 2021

Los servidores virtuales se habilitan de forma predeterminada al crearlos. Puede inhabilitar y habilitar servidores virtuales manualmente. Si inhabilita un servidor virtual, el estado del servicio virtual aparece como OUT DE SERVICIO. Cuando esto sucede, el servidor virtual termina todas las conexiones, ya sea inmediatamente o después de permitir que se completen las conexiones existentes, dependiendo de la configuración del parámetro DownStateFlush. Si DownStateFLush está ENABLED (valor predeterminado), se vaciarán todas las conexiones. Si está inhabilitado, el servidor virtual continúa atendiendo solicitudes en conexiones existentes.

Quitar un servidor virtual solo cuando ya no necesite el servidor virtual. Antes de eliminarlo, debe desvincular todos los servicios de él.

Para habilitar o inhabilitar un servidor virtual mediante la CLI

En el símbolo del sistema, escriba:


```
enable lb vserver <name>
<!--NeedCopy-->
```

```
disable lb vserver <name>
<!--NeedCopy-->
```

Ejemplos:

```
enable lb vserver Vserver-LB-1
disable lb vserver Vserver-LB-1
<!--NeedCopy-->
```

Para habilitar o inhabilitar un servidor virtual mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. Seleccione un servidor virtual y, en la lista **Acción**, seleccione **Habilitar** o **Inhabilitar**.

Para desvincular un servicio de un servidor virtual mediante la CLI

En el símbolo del sistema, escriba:

```
unbind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Ejemplo:

```
unbind lb vserver Vserver-LB-1 Service-HTTP-1
<!--NeedCopy-->
```

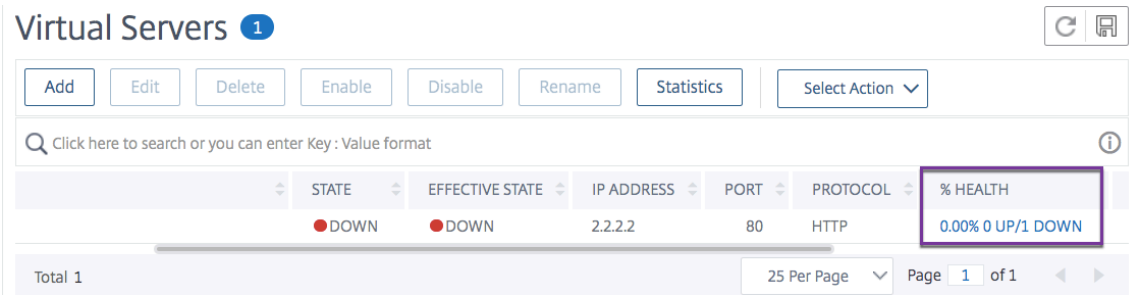
Para desvincular un servicio de un servidor virtual mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. Abra un servidor virtual y haga clic en la sección **Servicios**.
3. Seleccione un servicio y haga clic en **Desenlazar**.

Identifique la causa del estado del servidor virtual marcado hacia abajo mediante la interfaz gráfica de usuario

A partir de Citrix ADC versión 13.0 compilación 41.20, puede ver la información del sondeo del monitor en la GUI de los servidores virtuales que están CAÍDOS sin navegar a la interfaz de enlace de monitores. Se puede hacer clic en el valor de la **columna% HEALTH** de la página Servidor virtual. Puede hacer clic en el valor de la **columna% HEALTH** para identificar la causa raíz por la cual el servidor virtual está marcado como DOWN.

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. Haga clic en el valor de la **columna%** HEALTH correspondiente al servidor virtual que está inactivo.

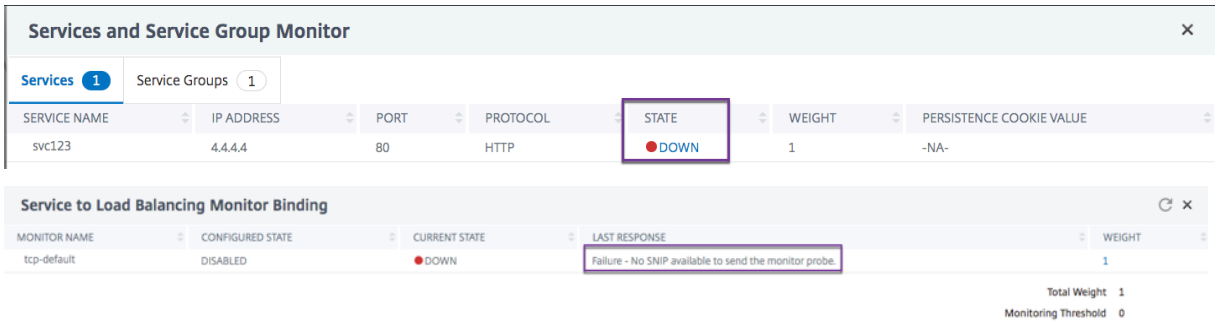


Aparecerá la página Monitor de Servicio y Grupo de Servicio. Los servicios y grupos de servicios enlazados a este servidor virtual se muestran en las fichas respectivas.

Si está usando servicios enlazados para el equilibrio de carga virtual, realice lo siguiente:

En la ficha **Servicios**, haga clic en **DOWN** correspondiente al servicio que está inactivo.

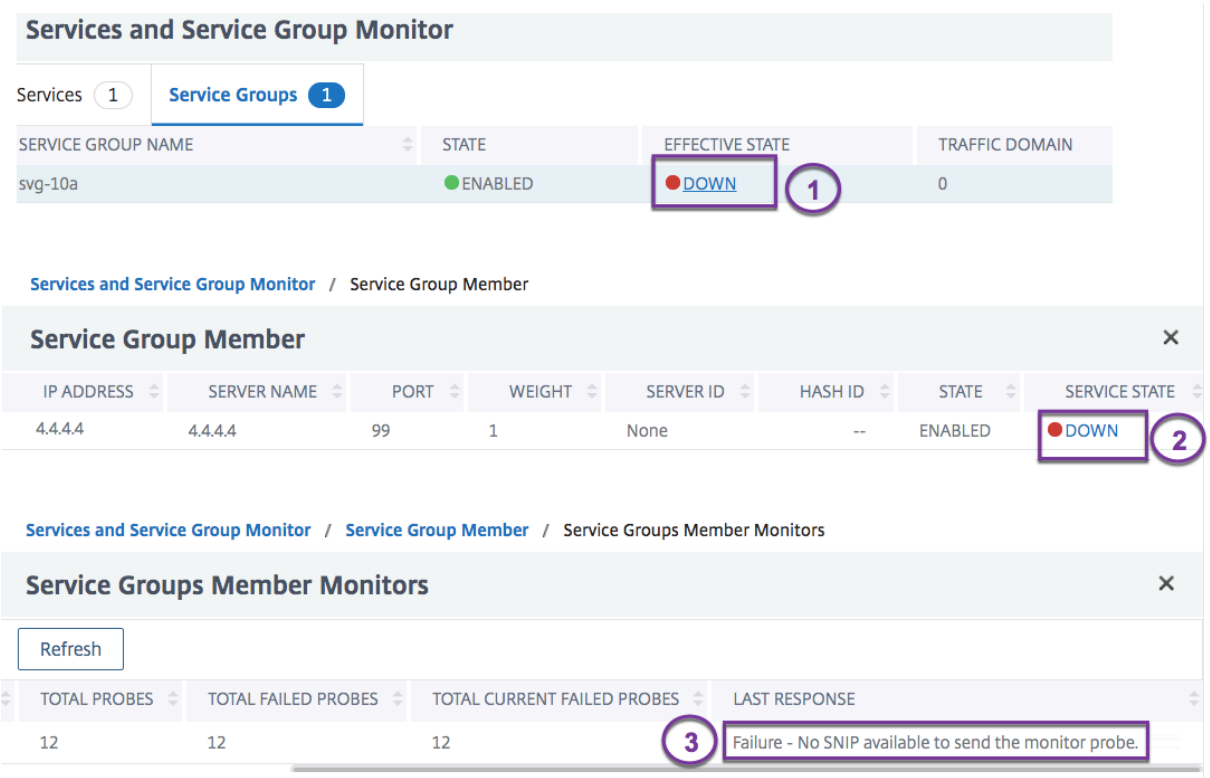
La columna **Última Respuesta** de la página Enlace del Monitor de Equilibrio de Servicio a Carga muestra el motivo por el cual el servidor virtual está marcado hacia abajo.



Si está usando grupos de servicios enlazados para el equilibrio de carga virtual, realice lo siguiente:

En la ficha **Grupos de servicios**, haga clic en **Abajo** en la página Servicios y Monitor de grupo de servicios y, a continuación, haga clic en **Abajo** en la página Miembro del grupo de servicios.

La columna **Última respuesta** de la página Grupos de servicio: Monitores de miembros muestra el motivo por el cual el servidor virtual está marcado hacia abajo.



Visualizador de equilibrio de carga

August 20, 2021

El Visualizador de equilibrio de carga es una herramienta que puede utilizar para ver y modificar la configuración de equilibrio de carga en un formato gráfico. A continuación se muestra un ejemplo de la visualización del visualizador.

Ilustración 1. Visualización del visualizador de equilibrio de carga

Puede utilizar el visualizador para ver lo siguiente:

- Los servicios y grupos de servicios que están enlazados a un servidor virtual.
- Los monitores que están vinculados a cada servicio.
- Las directivas que están enlazadas al servidor virtual.
- Las etiquetas de directiva, si están configuradas.
- Detalles de configuración de cualquier elemento mostrado.

También puede utilizar el Visualizador para agregar y enlazar objetos nuevos, modificar los existentes y habilitar o inhabilitar objetos. La mayoría de los elementos de configuración mostrados en el Visu-

alizador aparecen con los mismos nombres que en otras partes de la utilidad de configuración. Sin embargo, a diferencia del resto de la utilidad de configuración, el Visualizador agrupa los servicios que tienen los mismos detalles de configuración y los enlaces de supervisión en una entidad denominada contenedor de servicios.

Un contenedor de servicios es un conjunto de servicios y grupos de servicios similares que están enlazados a un único servidor virtual de equilibrio de carga. Los servicios del contenedor tienen las mismas propiedades, excepto el nombre, la dirección IP y el puerto, y sus enlaces de monitor deben tener el mismo peso y estado de enlace. Cuando vincula un nuevo servicio a un servidor virtual, se coloca en un contenedor existente si sus enlaces de configuración y monitorización coinciden con los de otros servicios. De lo contrario, se coloca en su propio contenedor.

En los siguientes procedimientos se proporcionan únicamente los pasos básicos para utilizar el visualizador. Dado que el Visualizador duplica la funcionalidad en otras áreas de la función Equilibrio de carga, se proporcionan otros métodos para ver o configurar todos los ajustes que se pueden configurar en el Visualizador en toda la documentación de Equilibrio de carga.

Nota: El Visualizador requiere una interfaz gráfica, por lo que solo está disponible a través de la utilidad de configuración.

Para ver las propiedades del servidor virtual de equilibrio de carga mediante el Visualizador

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. En el panel de detalles, seleccione el servidor virtual que desea ver y, a continuación, haga clic en **Visualizador**.

Para ver los detalles de configuración de servicios, grupos de servicios y monitores mediante el Visualizador

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. En el panel de detalles, seleccione el servidor virtual que desea ver y, a continuación, haga clic en **Visualizador**.
3. En el cuadro de diálogo Visualizador de equilibrio de carga, haga doble clic en la entidad para ver los detalles de configuración de la entidad enlazada a este servidor virtual, puede hacer lo siguiente:

Para ver los detalles de configuración de directivas y rótulos de directivas mediante el Visualizador en la utilidad de configuración

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.

2. En el panel de detalles, seleccione el servidor virtual que desea ver y, a continuación, haga clic en Visualizador.
3. En el cuadro de diálogo Visualizador de equilibrio de carga, haga doble clic en la entidad de directivas para ver las directivas vinculadas a este servidor virtual.

Para modificar un recurso en una configuración de equilibrio de carga mediante el visualizador

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. En el panel de detalles, seleccione el servidor virtual que quiere configurar y, a continuación, haga clic en Visualizador.
3. En el cuadro de diálogo Visualizador de equilibrio de carga, en la imagen del visualizador, haga doble clic en el recurso que quiere modificar.

Para agregar una configuración de equilibrio de carga mediante el Visualizador

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. En el panel de detalles, seleccione el servidor virtual que quiere configurar y, a continuación, haga clic en Visualizador.
3. En el cuadro de diálogo Visualizador de equilibrio de carga, haga clic en **+** para agregar el recurso.

Administrar el tráfico de clientes

October 5, 2021

Administrar correctamente las conexiones de cliente ayuda a garantizar que las aplicaciones permanezcan disponibles para los usuarios incluso cuando el dispositivo Citrix ADC experimente cargas elevadas. Se pueden integrar varias funciones de equilibrio de carga y otras funciones disponibles en el dispositivo en una configuración de equilibrio de carga para procesar la carga de forma más eficiente, desviarla cuando sea necesario y priorizar las tareas que debe realizar el dispositivo:

- **Equilibrio de carga sin sesión.** Puede configurar servidores virtuales de equilibrio de carga sin sesión y realizar el equilibrio de carga sin crear sesiones en configuraciones que utilizan DSR o sistemas de detección de intrusiones (IDS).
- **Almacenamiento en caché integrado.** Puede redirigir las solicitudes HTTP a una memoria caché.
- **Limpieza retrasada.** Puede configurar la limpieza retrasada de las conexiones del servidor virtual para evitar que el proceso de limpieza utilice ciclos de CPU durante los períodos en que el dispositivo Citrix ADC experimenta cargas elevadas.

- **Reescritura.** Puede utilizar la función Reescritura para modificar el puerto y el protocolo al realizar la redirección HTTP o insertar la dirección IP y el puerto del servidor virtual en un encabezado de solicitud personalizado.
- **RTSP NAT.**
- **Monitorización basada en tarifas.** Puede habilitar la supervisión basada en tarifas para desviar el tráfico excesivo.
- **Parámetros de capa 2.** Puede configurar un servidor virtual para que utilice los parámetros L2 para identificar una conexión.
- **Respuesta ICMP**. Puede configurar el dispositivo para que envíe respuestas ICMP a las solicitudes PING según su configuración. En la dirección IP correspondiente al servidor virtual, establezca ICMP RESPONSE en VSVR_CNTRLD y, en el servidor virtual, establezca el `ICMP VSERVER RESPONSE`.

  Se pueden realizar las siguientes configuraciones en un servidor virtual:
  - Cuando se establece `ICMP VSERVER RESPONSE` en PASIVO en todos los servidores virtuales, el dispositivo siempre responde.
  - Cuando se establece `ICMP VSERVER RESPONSE` en ACTIVE en todos los servidores virtuales, el dispositivo responde incluso si un servidor virtual está ACTIVO.
  - Cuando se establece `ICMP VSERVER RESPONSE` en ACTIVE en algunos y PASIVO en otros, el dispositivo responde incluso si un servidor virtual configurado en ACTIVE está ACTIVO.

Configurar servidores virtuales de equilibrio de carga sin sesión

August 20, 2021

Cuando el dispositivo Citrix ADC realiza el equilibrio de carga, crea y mantiene sesiones entre clientes y servidores. El mantenimiento de la información de sesión supone una carga significativa en los recursos del dispositivo y es posible que no se necesiten sesiones en casos como una configuración de retorno directo del servidor (DSR) y el equilibrio de carga de los sistemas de detección de intrusiones (IDS). Para evitar la creación de sesiones cuando no sean necesarias, puede configurar un servidor virtual en el dispositivo para el equilibrio de carga sin sesión. En el equilibrio de carga sin sesión, el dispositivo realiza el equilibrio de carga por paquete.

El equilibrio de carga sin sesión puede funcionar en el modo de reenvío basado en Mac o en el modo de reenvío basado en IP.

Para el reenvío basado en Mac, la dirección IP del servidor virtual sin sesión debe especificarse en todos los servidores físicos a los que se reenvía el tráfico.

Para el reenvío basado en IP en el equilibrio de carga sin sesión, no es necesario especificar la dirección IP y el puerto del servidor virtual en los servidores físicos, ya que esta información se incluye en los paquetes reenviados. Al reenviar un paquete desde el cliente al servidor físico, el dispositivo deja sin

cambios los detalles del cliente, como la dirección IP y el puerto, y agrega la dirección IP y el puerto del destino.

Configuración admitida

El equilibrio de carga sin sesión de Citrix ADC admite los siguientes tipos de servicio y métodos de equilibrio de carga:

Tipos de Servicio

- CUALQUIERA para redirección basada en Mac
- CUALQUIERA, DNS y UDP para redirección basada en IP

Métodos de equilibrio de carga

- Round Robin
- Ancho de banda mínimo
- LRTM (método de tiempo de respuesta mínimo)
- Hash IP de origen
- Hash IP de destino
- Hash IP de destino de IP de origen
- Hash del puerto de origen IP de origen
- Carga personalizada

Limitaciones

El equilibrio de carga sin sesión tiene las siguientes limitaciones:

- El dispositivo debe implementarse en modo de dos brazos.
- Un servicio debe estar enlazado a un solo servidor virtual.
- El equilibrio de carga sin sesión no es compatible con los grupos de servicios.
- El equilibrio de carga sin sesión no es compatible con los servicios basados en dominio (servicios DBS).
- El equilibrio de carga sin sesión en el modo IP no es compatible con un servidor virtual configurado como copia de seguridad en un servidor virtual principal.
- No se puede habilitar el modo de desbordamiento.
- Para todos los servicios enlazados a un servidor virtual de equilibrio de carga sin sesión, debe habilitarse la opción Usar IP de origen (USIP).
- En el caso de un servidor virtual comodín o servicio, la dirección IP de destino no se modifica.

Nota:

- Al configurar un servidor virtual para el equilibrio de carga sin sesión, especifique explícitamente un método de equilibrio de carga compatible. El método predeterminado, Least Connection, no se puede utilizar para el equilibrio de carga sin sesión.
- Para configurar el equilibrio de carga sin sesión en el modo de redirección basado en Mac en un servidor virtual, la opción de reenvío basado en Mac debe estar habilitada en el dispositivo Citrix ADC.

Para agregar un servidor virtual sin sesión mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para agregar un servidor virtual sin sesión y verificar la configuración:

```
add lb vserver <name>@ <serviceType> <IPAddress>@ <port> -m <
    redirectionMode> -sessionless <(ENABLED|DISABLED)> -lbMethod <
    load_balancing_method>

show lb vserver <name>
<!--NeedCopy-->
```

Ejemplo:

```
 add lb vserver sesslessv1 any 11.11.12.123 54 -sessionless ENABLED -
    lbMethod roundrobin -m ip
      Done
 show lb vserver sesslessv1
      sesslessv1 (11.11.12.123:54) - ANY Type: ADDRESS
      State: DOWN
      ...
      Effective State: DOWN
      Client Idle Timeout: 120 sec
      Down state flush: ENABLED
      ...
      Persistence: NONE
      Sessionless LB: ENABLED
      Connection Failover: DISABLED
      L2Conn: OFF
      1) Policy : cmp_text Priority:8680 Inherited
      2) Policy : cmp_nocmp_ie60 Priority:8690 Inherited
<!--NeedCopy-->
```


Para configurar el equilibrio de carga sin sesión en un servidor virtual existente

En el símbolo del sistema, escriba:

```
set lb vserver <name>@ -m <redirectionMode> -sessionless <(ENABLED|
    DISABLED)> -lbMethod <load_balancing_method>
<!--NeedCopy-->
```

Ejemplo

```
set lb vserver sesslessv1 -m mac -sessionless ENABLED -lbmethod lrtm
  Done
<!--NeedCopy-->
```

> **Nota**
>
> En el caso de un servicio vinculado a un servidor virtual en el que está habilitada la `-m MAC` opción, debe vincular un monitor que no es usuario.

Para configurar un servidor virtual sin sesión mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. Abra el servidor virtual y, en Configuración avanzada, haga clic en Configuración de tráfico y, a continuación, seleccione Equilibrio de carga sin sesión.

Redirigir solicitudes HTTP a una caché

August 20, 2021

La función de redirección de caché Citrix ADC redirige las solicitudes HTTP a una caché. Puede reducir significativamente el impacto de responder a las solicitudes HTTP y mejorar el rendimiento de su sitio web mediante la correcta implementación de la función de redirección de caché.

Una caché almacena el contenido HTTP solicitado con frecuencia. Al configurar la redirección de caché en un servidor virtual, el dispositivo Citrix ADC envía solicitudes HTTP que se pueden almacenar en caché a la caché y solicitudes HTTP que no se pueden almacenar en caché al servidor web de origen.

Para configurar la redirección de caché en un servidor virtual mediante la CLI

En el símbolo del sistema, escriba:

```
set lb vserver <name> -cacheable <Value>
<!--NeedCopy-->
```

Ejemplo:

```
set lb vserver Vserver-LB-1 -cacheable yes
<!--NeedCopy-->
```

Para configurar la redirección de caché en un servidor virtual mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**y abra el servidor virtual.
2. En Configuración avanzada, haga clic en Configuración de tráfico y seleccione Caché.

Habilitar la limpieza de conexiones de servidor virtual

August 20, 2021

En determinadas condiciones, puede configurar la configuración DownStateFlush para que termine inmediatamente las conexiones existentes cuando un servicio o un servidor virtual estén marcados como DESCONECTADAS. Terminar las conexiones existentes libera recursos y, en algunos casos, acelera la recuperación de configuraciones de equilibrio de carga sobrecargadas.

El estado de un servidor virtual depende de los estados de los servicios vinculados a él. El estado de cada servicio depende de las respuestas de los servidores con equilibrio de carga a los sondeos y comprobaciones de estado enviados por los monitores vinculados a ese servicio. A veces, los servidores con equilibrio de carga no responden. Si un servidor es lento u ocupado, los sondeos de supervisión pueden agotar el tiempo de espera. Si los sondeos de supervisión repetidos no se responden dentro del período de tiempo de espera configurado, el servicio se marca como DOWN.

Un servidor virtual se marca como DOWN solo cuando todos los servicios enlazados a él están marcados como DOWN. Cuando un servidor virtual baja, termina todas las conexiones, ya sea inmediatamente o después de permitir que se completen las conexiones existentes.

No active la configuración DownStateFlush en los servidores de aplicaciones que deben completar sus transacciones. Puede habilitar esta configuración en servidores web cuyas conexiones se pueden terminar de forma segura cuando marquen hacia abajo.

En la siguiente tabla se resume el efecto de esta configuración en una configuración de ejemplo que consta de un servidor virtual, VServer-LB-1, con un servicio vinculado a él, Service-TCP-1. En la tabla, E y D indican el estado de la configuración DownStateFlush: E significa Habilitado y D significa Inhabilitado.

Vserver-LB-1	Service-TCP-1	Estado de las conexiones
E	E	Se terminan las conexiones de cliente y servidor.
E	D	En algunos tipos de servicio, como TCP, para los que el dispositivo Citrix ADC no admite la reutilización de conexiones, se terminan las conexiones cliente y servidor. Para los tipos de servicio, como HTTP, para los que el dispositivo admite la reutilización de conexiones, las conexiones cliente y servidor solo se terminan si una transacción está activa en esas conexiones. Si una transacción no está activa, solo se terminan las conexiones de cliente.

Vserver-LB-1	Service-TCP-1	Estado de las conexiones
D	E	En algunos tipos de servicio, como TCP, para los que el dispositivo Citrix ADC no admite la reutilización de conexiones, se terminan las conexiones cliente y servidor. Para los tipos de servicio, como HTTP, para los que el dispositivo admite la reutilización de conexiones, las conexiones cliente y servidor solo se terminan si una transacción está activa en esas conexiones. Si una transacción no está activa, solo se finalizan las conexiones del servidor.
D	D	Ni las conexiones del cliente ni del servidor se terminan.

Si quiere inhabilitar un servicio solo cuando el servidor o el cliente cierran todas las conexiones establecidas, puede utilizar la opción de apagado estable. Para obtener información sobre el cierre correcto de un servicio, consulte Cierre de servicios de forma grácil.

Para configurar la configuración de vaciado de estado inactivo en un servidor virtual mediante la CLI

En el símbolo del sistema, escriba:

```
set lb vserver <name> -downStateFlush <Value>
<!--NeedCopy-->
```

Ejemplo:

```
set lb vserver Vserver-LB-1 -downStateFlush enabled
```



```
<!--NeedCopy-->
```

Para configurar la configuración de vaciado de estado inactivo en un servidor virtual mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**y abra el servidor virtual.
2. En Configuración avanzada, haga clic en Configuración de tráfico y seleccione Desactivar estado.

Reescritura de puertos y protocolos para la redirección HTTP

August 20, 2021

Los servidores virtuales y los servicios que están enlazados a ellos pueden utilizar puertos diferentes. Cuando un servicio responde a una conexión HTTP con una redirección, es posible que deba configurar el dispositivo Citrix ADC para modificar el puerto y el protocolo para asegurarse de que la redirección se realiza correctamente. Para ello, habilite y configure la opción RedirectPortRewrite.

Esta configuración solo afecta al tráfico HTTP y HTTPS. Si esta configuración está habilitada en un servidor virtual, el servidor virtual vuelve a escribir el puerto en redirecciones, reemplazando el puerto utilizado por el servicio por el puerto utilizado por el servidor virtual.

Si el servidor virtual o servicio es de tipo SSL, debe habilitar la redirección SSL en el servidor virtual o servicio. Si tanto el servidor virtual como el servicio son de tipo SSL, habilite la redirección SSL en el servidor virtual.

La configuración de RedirectPortRewrite se puede utilizar en los siguientes casos:

- El servidor virtual es de tipo HTTP y los servicios son de tipo SSL.
- El servidor virtual es de tipo SSL y los servicios son de tipo HTTP.
- El servidor virtual es de tipo HTTP y los servicios son de tipo HTTP.
- El servidor virtual es de tipo SSL y los servicios son de tipo SSL.

Caso 1: El servidor virtual es de tipo HTTP y los servicios son de tipo SSL. La redirección SSL y, opcionalmente, la reescritura de puertos, está habilitada en el servicio. Si la reescritura de puertos está habilitada, se reescribe el puerto de direcciones URL HTTPS. Las URL HTTP del servidor se envían tal cual al cliente.

Solo la redirección SSL está habilitada. El servidor virtual se puede configurar en cualquier puerto. Consulte la siguiente tabla:

Redirigir URL desde el servidor	URL de redirección enviada al cliente
http://domain.com/	http://domain.com/
http://domain.com:8080/	http://domain.com:8080/
https://domain.com/	https://domain.com/
https://domain.com:444/	https://domain.com:444/

La redirección SSL y la reescritura de puertos están habilitadas. El servidor virtual está configurado en el puerto 80. Consulte la siguiente tabla:

Redirigir URL desde el servidor	URL de redirección enviada al cliente
http://domain.com/	http://domain.com/
http://domain.com:8080/	http://domain.com:8080/
https://domain.com/	https://domain.com/
https://domain.com:444/	https://domain.com/

La redirección SSL y la reescritura de puertos están habilitadas. El servidor virtual está configurado en el puerto 8080. Consulte la siguiente tabla:

Redirigir URL desde el servidor	URL de redirección enviada al cliente
http://domain.com/	http://domain.com/
http://domain.com:8080/	http://domain.com:8080/
https://domain.com/	http://domain.com:8080/
https://domain.com:444/	http://domain.com:8080/

Caso 2: El servidor virtual es de tipo SSL y los servicios son de tipo HTTP. Si la reescritura de puertos está habilitada, solo se reescribe el puerto de direcciones URL HTTP. Las URL HTTPS del servidor se envían tal cual al cliente.

La redirección SSL está habilitada en el servidor virtual. El servidor virtual se puede configurar en cualquier puerto. Consulte la siguiente tabla.

Redirigir URL desde el servidor	URL de redirección enviada al cliente
http://domain.com/	https://domain.com/
http://domain.com:8080/	https://domain.com:8080/
https://domain.com/	https://domain.com/
https://domain.com:444/	https://domain.com:444/

La redirección SSL y la reescritura de puertos están habilitadas en el servidor virtual. El servidor virtual está configurado en el puerto 443. Consulte la siguiente tabla:

Redirigir URL desde el servidor	URL de redirección enviada al cliente
http://domain.com/	https://domain.com/
http://domain.com:8080/	https://domain.com/
https://domain.com/	https://domain.com/
https://domain.com:444/	https://domain.com:444/

La redirección SSL y la reescritura de puertos están habilitadas. El servidor virtual está configurado en el puerto 444. Consulte la siguiente tabla:

Redirigir URL desde el servidor	URL de redirección enviada al cliente
http://domain.com/	https://domain.com:444/
http://domain.com:8080/	https://domain.com:444/
https://domain.com/	https://domain.com/
https://domain.com:445/	https://domain.com:445/

Caso 3: El servidor virtual y el servicio son de tipo HTTP. La reescritura de puertos debe estar habilitada en el servidor virtual. Solo se reescribe el puerto de URL HTTP. Las URL HTTPS del servidor se envían tal cual al cliente.

El servidor virtual está configurado en el puerto 80. Consulte la siguiente tabla:

Redirigir URL desde el servidor	URL de redirección enviada al cliente
http://domain.com/	http://domain.com/

Redirigir URL desde el servidor	URL de redirección enviada al cliente
http://domain.com:8080/	http://domain.com/
https://domain.com/	https://domain.com/
https://domain.com:444/	https://domain.com:444/

El servidor virtual está configurado en el puerto 8080. Consulte la siguiente tabla:

Redirigir URL desde el servidor	URL de redirección enviada al cliente
http://domain.com/	http://domain.com:8080/
http://domain.com:8080/	http://domain.com:8080/
https://domain.com/	https://domain.com/
https://domain.com:445/	https://domain.com:445/

Caso 4: El servidor virtual y el servicio son de tipo SSL. Si la reescritura de puertos está habilitada, solo se reescribe el puerto de direcciones URL HTTPS. Las URL HTTP del servidor se envían tal cual al cliente.

La redirección SSL está habilitada en el servidor virtual. El servidor virtual se puede configurar en cualquier puerto. Consulte la siguiente tabla:

Redirigir URL desde el servidor	URL de redirección enviada al cliente
http://domain.com/	http://domain.com/
http://domain.com:8080/	http://domain.com:8080/
https://domain.com/	https://domain.com/
https://domain.com:444/	https://domain.com:444/

La redirección SSL y la reescritura de puertos están habilitadas en el servidor virtual. El servidor virtual está configurado en el puerto 443. Consulte la siguiente tabla:

Redirigir URL desde el servidor	URL de redirección enviada al cliente
http://domain.com/	http://domain.com/
http://domain.com:8080/	http://domain.com:8080/

Redirigir URL desde el servidor	URL de redirección enviada al cliente
https://domain.com/	https://domain.com/
https://domain.com:444/	https://domain.com/

La redirección SSL y la reescritura de puertos están habilitadas en el servidor virtual. El servidor virtual está configurado en el puerto 444. Consulte la siguiente tabla:

Redirigir URL desde el servidor	URL de redirección enviada al cliente
http://domain.com/	http://domain.com/
http://domain.com:8080/	http://domain.com:8080/
https://domain.com/	https://domain.com:444/
https://domain.com:445/	https://domain.com:444/

Para configurar la redirección HTTP en un servidor virtual mediante la CLI

En el símbolo del sistema, escriba:

```
set lb vserver <name> -redirectPortRewrite (ENABLED | DISABLED)
<!--NeedCopy-->
```

Ejemplo:

```
set lb vserver Vserver-LB-1 -redirectPortRewrite enabled
<!--NeedCopy-->
```

Para configurar la redirección HTTP en un servidor virtual mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. Abra el servidor virtual y, en el panel Configuración avanzada, haga clic en Configuración de tráfico y, a continuación, seleccione Volver a escribir.

Para configurar SSL Redirect en un servidor virtual SSL o servicio mediante la CLI

En el símbolo del sistema, escriba:

```
set ssl vserver <vServerName> - sslRedirect (ENABLED | DISABLED)

set ssl service <serviceName> - sslRedirect (ENABLED | DISABLED)
<!--NeedCopy-->
```

Ejemplo:

```
set ssl vserver Vserver-SSL-1 -sslRedirect enabled

set ssl service service-SSL-1 -sslRedirect enabled
<!--NeedCopy-->
```

Para configurar la redirección SSL y la reescritura del puerto SSL en un servidor virtual SSL o servicio mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**y abra el servidor virtual.
2. En Configuración avanzada, haga clic en Parámetros SSL y seleccione Redirigir SSL.

Insertar la dirección IP y el puerto de un servidor virtual en el encabezado de solicitud

August 20, 2021

Si tiene varios servidores virtuales que se comunican con distintas aplicaciones en el mismo servicio, debe hacer lo siguiente:

Configure el dispositivo Citrix ADC para agregar la dirección IP y el número de puerto del servidor virtual apropiado a las solicitudes HTTP que se envían a ese servicio. Esta configuración permite que las aplicaciones que se ejecutan en el servicio identifiquen el servidor virtual que envió la solicitud.

Si el servidor virtual principal está inactivo y el servidor virtual de copia de seguridad está activo, los valores de configuración del servidor virtual de copia de seguridad se agregan a las solicitudes del cliente. Si quiere agregar la misma etiqueta de encabezado, independientemente de si las solicitudes

proceden del servidor virtual principal o del servidor virtual de copia de seguridad, debe configurar la etiqueta de encabezado requerida en ambos servidores virtuales.

Nota: Esta opción no es compatible con los servidores virtuales de comodín o los servidores virtuales ficticios.

Para insertar la dirección IP y el puerto del servidor virtual en las solicitudes del cliente mediante la CLI

En el símbolo del sistema, escriba:

```
set lb vserver <name> -insertVserverIPPort <insertVserverIPPort> [<
   vipHeader>]
<!--NeedCopy-->
```

Ejemplo:

```
set lb vserver Vserver-LB-1 -insertVserverIPPort VipAddr
<!--NeedCopy-->
```

Para insertar la dirección IP y el puerto del servidor virtual en las solicitudes del cliente mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. Abra el servidor virtual y, en el panel Configuración avanzada, haga clic en **Configuración de tráfico**y, a continuación, seleccione Inserción de puertos IP del servidor virtual y especifique un encabezado de puerto IP del servidor virtual.

Utilizar una IP de origen especificada para la comunicación back-end

December 2, 2021

Para la comunicación con los servidores físicos u otros dispositivos del mismo nivel, el dispositivo Citrix ADC utiliza una dirección IP de su propiedad como dirección IP de origen. El dispositivo Citrix ADC mantiene un conjunto de sus direcciones IP y selecciona dinámicamente una dirección IP mientras se conecta con un servidor. En función de la subred en la que se coloque el servidor físico, el dispositivo decide qué dirección IP se va a utilizar. Este grupo de direcciones se utiliza para enviar sondeos de tráfico y monitorizar.

En muchas situaciones, es posible que desee que el dispositivo utilice una dirección IP específica o cualquier dirección IP de un conjunto específico de direcciones IP para comunicaciones de back-end. A continuación se presentan algunos ejemplos:

- Un servidor puede distinguir sondeos de monitor del tráfico si la dirección IP de origen utilizada para sondeos de monitor pertenece a un conjunto específico.
- Para mejorar la seguridad del servidor, se puede configurar un servidor para responder a las solicitudes de un conjunto específico de direcciones IP o, en ocasiones, de una única dirección IP específica. En tal caso, el dispositivo solo puede utilizar las direcciones IP aceptadas por el servidor como dirección IP de origen.
- El dispositivo puede administrar sus conexiones internas de manera eficiente si puede distribuir sus direcciones IP en conjuntos de IP y usar una dirección de un conjunto solo para conectarse a un servicio específico.

Para configurar el dispositivo para que utilice una dirección IP de origen especificada, cree perfiles de red (perfiles de red) y configure las entidades del dispositivo para que utilicen el perfil. Un perfil de red se puede enlazar a servidores virtuales de equilibrio de carga o conmutación de contenido, servidores virtuales VPN de Citrix Gateway, servicios, grupos de servicios o monitores. Un perfil de red tiene direcciones IP propiedad de Citrix ADC (SNIP y VIP) que se pueden utilizar como dirección IP de origen. Puede ser una única dirección IP o un conjunto de direcciones IP, denominadas conjunto de IP. Si un perfil de red tiene una IP establecida, el dispositivo selecciona dinámicamente una dirección IP del conjunto de IP en el momento de la conexión. Si un perfil tiene una sola dirección IP, se utiliza la misma dirección IP que la IP de origen.

Si un perfil de red está enlazado a un servidor virtual de equilibrio de carga o conmutación de contenido, el perfil se usa para enviar tráfico a todos los servicios vinculados a él. Si un perfil de red está enlazado a un grupo de servicios, el dispositivo utiliza el perfil para todos los miembros del grupo de servicio. Si un perfil de red está enlazado a un monitor, el dispositivo utiliza el perfil para todos los sondeos enviados desde el monitor.

> **Nota:**
>
> - Cuando un dispositivo Citrix ADC utiliza una dirección VIP para comunicarse con un servidor, utiliza entradas de sesión para identificar si el tráfico destinado a la dirección VIP es una respuesta de un servidor o una solicitud de un cliente.
> - Puede vincular un perfil de red a servidores virtuales VPN de Citrix Gateway. Sin embargo, debe tener en cuenta algunos puntos al vincular un perfil de red. Para obtener más información, consulte Puntos a tener en cuenta al vincular un perfil de red al servidor virtual VPN.
> - Las IP del perfil de red enlazadas a un servicio o grupo de servicios no solo se utilizan para enviar tráfico hacia los servidores back-end correspondientes, sino también para las solici-

> tudes DNS que se activan por cualquier FQDN back-end sin resolver.

Uso de un perfil de red para enviar tráfico

Si la opción Usar dirección IP de origen (USIP) está habilitada, el dispositivo utiliza la dirección IP del cliente e ignora todos los perfiles de red. Si la opción USIP no está habilitada, el dispositivo selecciona la IP de origen de la siguiente manera:

- Si no hay un perfil de red en el servidor virtual ni en el grupo de servicios/servicios, el dispositivo utiliza el método predeterminado.
- Si hay un perfil de red solo en el grupo de servicios/servicios, el dispositivo utiliza ese perfil de red.
- Si hay un perfil de red solo en el servidor virtual, el dispositivo utiliza el perfil de red.
- Si hay un perfil de red tanto en el servidor virtual como en el grupo de servicios/servicios, el dispositivo utiliza el perfil de red enlazado al grupo de servicios/servicios.

Uso de un perfil de red para enviar sondeos de monitor:

Para los sondeos de monitor, el dispositivo selecciona la IP de origen de la siguiente manera:

- Si hay un perfil de red enlazado al monitor, el dispositivo utiliza el perfil de red del monitor. Ignora los perfiles de red vinculados al servidor virtual o al grupo de servicios/servicios.
- Si no hay un perfil de red vinculado al monitor,
  - Si hay un perfil de red en el grupo de servicios/servicios, el dispositivo utiliza el perfil de red del grupo de servicios/servicios.
  - Si no hay un perfil de red ni siquiera en el grupo de servicios/servicios, el dispositivo utiliza el método predeterminado para seleccionar una IP de origen.

Nota: Si no hay un perfil de red vinculado a un servicio, el dispositivo busca un perfil de red en el grupo de servicios si el servicio está enlazado a un grupo de servicios.

Para usar una dirección IP de origen especificada para la comunicación, siga los siguientes pasos:

1. Cree conjuntos de IP a partir del grupo de SNIP y VIP propiedad del dispositivo Citrix ADC. Un conjunto de IP puede constar de direcciones SNIP y VIP. Para obtener instrucciones, consulte Creación de conjuntos de IP.
2. Crear perfiles de red. Para obtener instrucciones, consulte Creación de un perfil de red.
3. Enlazar los perfiles de red a las entidades del dispositivo. Para obtener instrucciones, consulte Vinculación de un perfil de red a una entidad Citrix ADC.

> **Nota:**
>
> - Un perfil de red solo puede tener las direcciones IP especificadas como SNIP y VIP en el

> dispositivo Citrix ADC.
>
> - La persistencia de IP de origen no se respeta para los paquetes iniciados por Citrix ADC.

Administrar perfiles de red

Un perfil de red (o perfil de red) contiene una dirección IP o un conjunto de IP. Durante la comunicación con servidores físicos o pares, el dispositivo Citrix ADC utiliza las direcciones especificadas en el perfil como dirección IP de origen.

- Para obtener instrucciones sobre cómo crear un perfil de red, consulte Creación de un perfil de red.
- Para obtener instrucciones sobre cómo vincular un perfil de red a una entidad Citrix ADC, consulte Vinculación de un perfil de red a una entidad Citrix ADC.

Crear un conjunto de IP

Un conjunto de IP es un conjunto de direcciones IP, que se configuran en el dispositivo Citrix ADC como direcciones IP de subred (SNIP) o direcciones IP virtuales (VIP). Un conjunto de IP se identifica con un nombre significativo que ayuda a identificar el uso de las direcciones IP contenidas en él. Para crear un conjunto de IP, agregue un conjunto de IP y vincule direcciones IP propiedad de Citrix ADC a él. Las direcciones SNIP y las direcciones VIP pueden estar presentes en el mismo conjunto de IP.

Para crear un conjunto de direcciones IP mediante la CLI

En el símbolo del sistema, escriba los comandos siguientes:

```
add ipset <name>

bind ipset <name> <IPAddress>
<!--NeedCopy-->
```

o

```
bind ipset <name> <IPAddress>

show ipset [<name>]
<!--NeedCopy-->
```

El comando anterior muestra los nombres de todos los conjuntos de IP del dispositivo si no pasa ningún nombre. Muestra las direcciones IP enlazadas al conjunto IP especificado si pasa un nombre.

Ejemplos

```
1.
> add ipset skpnwipset
 Done
> bind ipset skpnwipset 21.21.20.1
 Done

2.
 > add ipset testnwipset
 Done
> bind ipset testnwipset 21.21.21.[21-25]
 IPAddress ”21.21.21.21” bound
 IPAddress ”21.21.21.22” bound
 IPAddress ”21.21.21.23” bound
 IPAddress ”21.21.21.24” bound
 IPAddress ”21.21.21.25” bound
 Done

3.
 > bind ipset skpipset 11.11.11.101
 ERROR: Invalid IP address
[This IP address could not be added because this is not an IP address
   owned by the Citrix ADC appliance]
 > add ns ip 11.11.11.101 255.255.255.0 -type SNIP
 ip ”11.11.11.101” added
 Done
 > bind ipset skpipset 11.11.11.101
 IPAddress ”11.11.11.101” bound
 Done
4.
> sh ipset
1) Name: ipset-1
2) Name: ipset-2
3) Name: ipset-3
4) Name: skpnewipset
 Done

5.
> sh ipset skpnewipset
IP:21.21.21.21
IP:21.21.21.22
IP:21.21.21.23
```



```
IP:21.21.21.24
IP:21.21.21.25
 Done
<!--NeedCopy-->
```

Para crear un conjunto de direcciones IP mediante la interfaz gráfica de usuario

Vaya a **Sistema > Red > Conjuntos de IP**y cree un conjunto de IP.

Crear un perfil de red

Un perfil de red (perfil de red) consta de una o más direcciones SNIP
o VIP del dispositivo Citrix ADC.

Para crear un perfil de red mediante la CLI

En el símbolo del sistema, escriba:

```
add netprofile <name> [-srcIp <srcIpVal>]
<!--NeedCopy-->
```

Si el srciPval no se proporciona en este comando, se puede proporcionar más adelante mediante el comando `set netprofile`.

Ejemplos

```
add netprofile skpnetprofile1 -srcIp 21.21.20.1
Done

add netprofile baksnp -srcIp bakipset
Done

set netprofile yahnp -srcIp 12.12.23.1
Done

set netprofile citkbnp -srcIp citkbipset
Done
<!--NeedCopy-->
```


Enlace un perfil de red a una entidad Citrix ADC

Un perfil de red se puede enlazar a un servidor virtual, servicio, grupo de servicios o monitor de equilibrio de carga.

Nota: Puede enlazar un perfil de red en el momento de crear una entidad Citrix ADC o enlazarlo a una entidad existente.

Para enlazar un perfil de red a un servidor mediante la interfaz de línea de comandos

Puede vincular un perfil de red a los servidores virtuales de equilibrio de carga y a los servidores virtuales de conmutación de contenido. Especifique el servidor virtual apropiado.

En el símbolo del sistema, escriba:

```
set lb vserver <name> -netProfile <net_profile_name>
<!--NeedCopy-->
```

o

```
set cs vserver <name> -netProfile <net_profile_name>
<!--NeedCopy-->
```

Ejemplos

```
set lb vserver skpnwvs1 -netProfile gntnp
 Done
set cs vserver mmdcsv -netProfile mmdnp
 Done
<!--NeedCopy-->
```

Para enlazar un perfil de red a un servidor virtual mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**y abra el servidor virtual.
2. En Configuración avanzada, haga clic en **Perfiles**y establezca un perfil de red.

Para enlazar un perfil de red a un servicio mediante la CLI

En el símbolo del sistema, escriba:

```
set service <name> -netProfile <net_profile_name>
<!--NeedCopy-->
```

Ejemplo

```
set service brnssvc1 -netProfile brnsnp
 Done
<!--NeedCopy-->
```

Para enlazar un perfil de red a un servicio mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servicios**y abra un servicio.
2. En Configuración avanzada, haga clic en **Perfiles**y establezca un perfil de red.

Para enlazar un perfil de red a un grupo de servicios mediante la CLI

En el símbolo del sistema, escriba:

```
set servicegroup <serviceGroupName> -netProfile <net_profile_name>
<!--NeedCopy-->
```

Ejemplo

```
set servicegroup ndhsvcgrp -netProfile ndhnp
 Done
<!--NeedCopy-->
```

Para enlazar un perfil de red a un grupo de servicios mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Grupos de servicios**y abra un grupo de servicios.

2. En Configuración avanzada, haga clic en **Perfiles**y establezca un perfil de red.

Para enlazar un perfil de red a un monitor mediante la CLI

En el símbolo del sistema, escriba:

```
set monitor <monitor_name> -netProfile <net_profile_name>
```

Ejemplo

```
set monitor brnsecvmon1 -netProfile brnsmonnp
 Done
<!--NeedCopy-->
```

Para enlazar un perfil de red a un monitor mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Monitores**.
2. Abra un monitor y configure el perfil de red.

Establecer un valor de tiempo de espera para las conexiones de cliente inactivas

August 20, 2021

Puede configurar un servidor virtual para que finalice cualquier conexión de cliente inactiva después de que transcurra un período de tiempo de espera configurado (en segundos). Al configurar esta configuración, el dispositivo Citrix ADC espera el tiempo especificado y, si el cliente está inactivo después de ese tiempo, cierra la conexión del cliente. De forma predeterminada, el valor de tiempo de espera de inactividad del cliente se establece en 180 segundos.

Para establecer un valor de tiempo de espera para las conexiones de cliente inactivas mediante la CLI

En el símbolo del sistema, escriba:

```
set lb vserver <name> -cltTimeout <Value>
<!--NeedCopy-->
```


Ejemplo:

```
set lb vserver Vserver-LB-1 -cltTimeout 100
<!--NeedCopy-->
```

Para establecer un valor de tiempo de espera para las conexiones de cliente inactivas mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**y abra un servidor virtual.
2. En **Configuración avanzada,** haga clic en **Configuración de tráfico** y establezca el valor de tiempo de espera de inactividad del cliente en segundos.

Administrar conexiones RTSP

August 20, 2021

El dispositivo Citrix ADC puede utilizar dos topologías (modo NAT activado o modo NAT desactivado) para equilibrar la carga de los servidores RTSP. En el modo NAT activado, la traducción de direcciones de red (NAT) está habilitada y configurada en el dispositivo. Tanto las solicitudes como las respuestas RTSP pasan por el dispositivo. Por lo tanto, debe configurar el dispositivo para que realice la traducción de direcciones de red (NAT) para identificar la conexión de datos.

Para obtener más información sobre cómo habilitar y configurar NAT, consulte Direccionamiento IP.

En el modo NAT desactivado, NAT no está habilitado ni configurado. El dispositivo recibe solicitudes RTSP del cliente y las enruta al servicio que selecciona mediante el método de equilibrio de carga configurado. Los servidores RTSP equilibrados de carga envían sus respuestas directamente al cliente, evitando el dispositivo. Por lo tanto, debe configurar el dispositivo para que utilice el modo de retorno directo del servidor (DSR) y asignar FQDN de acceso público en DNS a los servidores RTSP equilibrados de carga.

Para obtener más información sobre cómo habilitar y configurar el modo DSR, consulte Configuración del equilibrio de carga en modo de retorno de Direct Server. Para obtener más información sobre la configuración de DNS, consulte Sistema de nombres de dominio. En cualquier caso, al configurar el equilibrio de carga RTSP, también debe configurar RTSPNat para que coincida con la topología de su configuración de equilibrio de carga.

Para configurar RTSP NAT mediante la CLI

En el símbolo del sistema, escriba:

```
set lb vserver <name>  -RTSPNAT <ValueOfRTSPNAT>
<!--NeedCopy-->
```

Ejemplo:

```
set lb vserver vserver-LB-1  -RTSPNAT ON
<!--NeedCopy-->
```

Para configurar RTSP NAT mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales** y abra un servidor virtual de tipo RTSP.
2. En Configuración avanzada, haga clic en **Configuración de tráfico** y seleccione **Natting RTSP**.

Administrar el tráfico de clientes según la velocidad de tráfico

August 20, 2021

Puede supervisar la velocidad de tráfico que fluye a través de los servidores virtuales de equilibrio de carga y controlar el comportamiento del dispositivo Citrix ADC en función de la velocidad de tráfico. Por ejemplo:

- Acelerar el flujo de tráfico si es demasiado alto.
- Información en caché basada en la velocidad de tráfico.
- Si la velocidad de tráfico es demasiado alta, redirija el exceso de tráfico a otro servidor virtual de equilibrio de carga diferente.
- Aplique la supervisión basada en la tasa a las solicitudes HTTP y del Sistema de Nombres de Dominio (DNS).

Para obtener más información sobre las directivas basadas en tarifas, consulte Limitación de tarifas.

Identificar una conexión con parámetros de capa 2

August 20, 2021

Por lo general, para identificar una conexión, el dispositivo Citrix ADC utiliza las cuatro tuplas de dirección IP del cliente, puerto del cliente, dirección IP de destino y puerto de destino. Al habilitar la opción Conexión L2, los parámetros de Capa 2 de la conexión (número de canal, dirección MAC e ID de VLAN) se utilizan además de las 4 tuplas normales.

Habilitar el parámetro L2Conn para un servidor virtual de equilibrio de carga permite múltiples conexiones TCP y no TCP con las mismas 4 tuplas (<source IP>:<source port>::<destination IP>:<destination port>) para que coexistan en el dispositivo Citrix ADC. El dispositivo utiliza los parámetros de 4 tuplas y de Capa 2 para identificar las conexiones TCP y no TCP.

Puede habilitar la opción L2Conn en los siguientes casos:

- Se configuran varias VLAN en el dispositivo Citrix ADC y se configura un firewall para cada VLAN.
- Quiere que el tráfico procedente de los servidores de una VLAN y enlazado a un servidor virtual de otra VLAN pase a través de los firewalls configurados para ambas VLAN.

Por lo tanto, cuando un dispositivo Citrix ADC de nCore en el que se establece el parámetro L2conn para uno o más servidores virtuales de equilibrio de carga se reduce a una versión clásica o a una compilación nCore que no admite el parámetro L2conn, las configuraciones de equilibrio de carga que utilizan el parámetro L2conn se vuelven ineficaces.

Para configurar la opción de conexión L2 mediante la CLI

En el símbolo del sistema, escriba:

```
add lb vserver <name> <serviceType> <IPAddress>@ <port> -l2Conn ON
<!--NeedCopy-->
```

Ejemplo

```
 add lb vserver LB-VIP1 HTTP 10.1.1.254 80 -l2Conn ON
<!--NeedCopy-->
```

Para configurar la opción de conexión L2 mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**y abra un servidor virtual.
2. En Configuración avanzada, seleccione Configuración de tráfico y seleccione Parámetros de capa 2.

Configurar la opción Preferir ruta directa

August 20, 2021

En un servidor virtual de equilibrio de carga comodín si configura explícitamente una ruta a un destino, de forma predeterminada, el dispositivo Citrix ADC reenvía el tráfico según la ruta configurada. Si quiere que el dispositivo no busque la ruta configurada, puede establecer la opción Preferir ruta directa en NO.

Si un dispositivo está conectado directamente a un dispositivo Citrix ADC, el dispositivo reenvía directamente el tráfico al dispositivo. Por ejemplo, si el destino de un paquete es un firewall, el paquete no necesita ser enrutado a través de otro firewall. Sin embargo, a veces, es posible que desee que el tráfico pase por el firewall incluso si el dispositivo está conectado directamente a él. En tales casos, puede establecer la opción Preferir ruta directa en NO.

Nota: La configuración PreferDirecTroute es aplicable a todos los servidores virtuales comodín del dispositivo Citrix ADC.

Para configurar la opción Preferir ruta directa mediante la CLI

En el símbolo del sistema, escriba:

```
set lb parameter -preferDirectRoute (YES | NO)
<!--NeedCopy-->
```

Ejemplo:

```
set lb parameter -preferDirectRoute YES
<!--NeedCopy-->
```

Para configurar la opción Preferir ruta directa mediante la GUI

1. Vaya a **Administración del tráfico > Equilibrio de carga > Configurar parámetros de equilibrio de carga**.
2. Seleccione Preferir ruta directa.

Utilizar un puerto de origen de un rango de puertos especificado para la comunicación back-end

August 20, 2021

De forma predeterminada, para configuraciones con la opción USIP inhabilitada o con USIP y utilizar opciones de puerto proxy habilitadas, el dispositivo Citrix ADC se comunica a los servidores desde un puerto de origen aleatorio (mayor que 1024).

El dispositivo admite el uso de un puerto de origen de un intervalo de puertos especificado para comunicarse con los servidores. Uno de los casos de uso de esta función es para servidores que están configurados para identificar el tráfico recibido perteneciente a un conjunto específico basado en el puerto de origen con fines de registro y supervisión. Por ejemplo, identificar el tráfico interno y externo para fines de registro.

La configuración del dispositivo Citrix ADC para que utilice un puerto de origen de un intervalo de puertos para comunicarse con los servidores consiste en las siguientes tareas:

- **Cree un perfil de red y defina el parámetro de rango de puertos de origen**. Un parámetro de rango de puertos de origen especifica uno o más rangos de puertos. El dispositivo selecciona aleatoriamente uno de los puertos libres de los intervalos de puertos especificados y lo utiliza como puerto de origen para cada conexión a servidores.
- **Enlazar el perfil de red a servidores virtuales de equilibrio de carga, servicios o grupos**de servicios: Un perfil de red con configuración de rango de puertos de origen puede enlazarse a un servidor virtual, servicio o grupo de servicios de una configuración de equilibrio de carga. Para una conexión a un servidor virtual, el dispositivo selecciona aleatoriamente uno de los puertos libres de los rangos de puertos especificados de un perfil de red y lo utiliza como puerto de origen para conectarse a uno de los servidores vinculados.

Para especificar un rango o rangos de puertos de origen mediante la CLI

En el símbolo del sistema, escriba:

```
bind netProfile <name> (-srcPortRange <int[-int]> ...)

show netprofile <name>
<!--NeedCopy-->
```


Para especificar un rango o rangos de puertos de origen mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **Red** > **Perfiles de red**.
2. Defina el parámetro **Rango de puerto de origen** al agregar o modificar NetProfiles.

Configuración de ejemplo

En la siguiente configuración de ejemplo, el perfil de red PARTIAL-NAT-1 tiene una configuración NAT parcial y está enlazado al servidor virtual de equilibrio de carga LBVS-1, que es de tipo ANY. Para los paquetes recibidos en LBVS-1 desde 192.0.0.0/8, el dispositivo Citrix ADC traduce el último octeto de la dirección IP de origen del paquete a 100. Por ejemplo, un paquete con dirección IP de origen 192.0.2.30 recibido en LBVS-1, el dispositivo Citrix ADC traduce la dirección IP de origen a 100.0.2.30 antes de enviarla uno de los servidores enlazados.

```
```
> add netprofile CUSTOM-SRCPORT-NP-1
Done
> bind netprofile CUSTOM-SRCPRT-NP-1 - srcportrange 2000-3000

Done
> bind netprofile CUSTOM-SRCPRT-NP-1 - srcportrange 5000-6000

Done
> add lb vserver LBVS-1 ANY 203.0.113. 61 * -netprofile PARTIAL-NAT-1

Done
<!--NeedCopy--> ```
```

## Configurar la persistencia IP de origen para la comunicación back-end

August 20, 2021

De forma predeterminada, para una configuración de equilibrio de carga con la opción USIP inhabilitada y un perfil de red enlazado a un servidor virtual o servicios o grupos de servicios, el dispositivo Citrix ADC utiliza el algoritmo round robin para seleccionar una dirección IP del perfil de red para comunicarse con los servidores. Debido a este método de selección, la dirección IP seleccionada puede ser diferente para diferentes sesiones de un cliente específico.

 
```

Algunas situaciones requieren que el dispositivo Citrix ADC enrute todo el tráfico de un cliente específico desde la misma dirección IP al enviar el tráfico a los servidores. Los servidores pueden entonces, por ejemplo, identificar el tráfico que pertenece a un conjunto específico para fines de registro y supervisión.

La opción de persistencia de IP de origen de un perfil de red permite que el dispositivo Citrix ADC utilice la misma dirección, especificada en el perfil de red, para comunicarse con los servidores acerca de todas las sesiones iniciadas desde un cliente específico a un servidor virtual.

Para habilitar la persistencia de IP de origen en un perfil de red mediante la CLI

Para habilitar la persistencia de IP de origen al agregar un perfil de red, en el símbolo del sistema, escriba:

```
add netProfile <name> -srcippersistency ( ENABLED | DISABLED )

show netprofile <name>
<!--NeedCopy-->
```

Para habilitar la persistencia de IP de origen en un perfil de red existente, en el símbolo del sistema, escriba:

```
set netProfile <name> -srcippersistency ( ENABLED | DISABLED )

show netprofile <name>
<!--NeedCopy-->
```

Para habilitar la persistencia de IP de origen en un perfil de red mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **Red** > **Perfiles de red**.
2. Seleccione **Persistencia IP de origen** mientras agrega o modifica un perfil de red.

Ejemplo

En la siguiente configuración de ejemplo, el perfil de red NETPROFILE-IPPRSTNCY-1 tiene habilitada la opción de persistencia IP de origen y está enlazado al servidor virtual de equilibrio de carga LBVS-1.

El dispositivo Citrix ADC siempre utiliza la misma dirección IP (en este ejemplo, 192.0.2.11) para comunicarse con los servidores enlazados a LBVS-1, para todas las sesiones iniciadas desde un cliente específico al servidor virtual.

```
```
> add ipset IPSET-1

Done
> bind ipset IPSET-1 192.0.2.[11-15]
 IPAddress ”192.0.2.11” bound
 IPAddress ”192.0.2.12” bound
 IPAddress ”192.0.2.13” bound
 IPAddress ”192.0.2.14” bound
 IPAddress ”192.0.2.15” bound
 Done
> add netprofile NETPROFILE-IPPRSTNCY-1 -srcIp IPSET-1 -
   srcippersistency ENABLED

Done
> set lb vserver LBVS-1 -netprofile NETPROFILE-IPPRSTNCY-1

 Done
<!--NeedCopy--> ```
```

## Utilizar direcciones locales de enlace IPv6 en el lado del servidor de una configuración de equilibrio de carga

August 20, 2021

La dirección local de enlace IPv6 se admite para servicios, grupos de servicios y servidores de una configuración de equilibrio de carga. Puede especificar una dirección IPv6 local de enlace junto con el ID de VLAN asociado en configuraciones de servicios, grupos de servicios y servidores. El dispositivo Citrix ADC utiliza la dirección SNIP6 local del enlace desde la misma VLAN especificada en las configuraciones de servicios, grupos de servicios y servidores para comunicarse con ellos.

Una dirección IPv6 local de enlace y el ID de VLAN asociado se especifican con el siguiente formato en configuraciones de servicios, grupos de servicios y servidores: `&lt;IPv6_Addrs&gt;%&lt;vlan_id&gt;`

Por ejemplo, `fe80:123:4567::a%2048:`, `fe80:123:4567::a` es la dirección local del vínculo Y 2048 es el ID de VLAN.

 
```

```
> add service SERVICE-1 fe80:123:4567::a%2048 HTTP 80

Done
> bind servicegroup SERVICE-GROUP-1 fe80::1%24 80

Done
> add server SERVER-1 fe80:b:c:d::e:f:a/64%1028

Done
```

Configuración avanzada de equilibrio de carga

January 19, 2021

Además de configurar servidores virtuales, puede configurar opciones avanzadas para los servicios.

Para configurar opciones avanzadas de equilibrio de carga, consulte las siguientes secciones:

- Aumente gradualmente la carga de un nuevo servicio con inicio lento a nivel de servidor virtual
- La opción sin monitor para los servicios
- Proteja las aplicaciones en servidores protegidos contra sobretensiones de tráfico
- Habilitar la limpieza de las conexiones de servidor virtual y servicio
- Apagado estable de los servicios
- Habilitar o inhabilitar la sesión de persistencia en los servicios TROFS
- Solicitudes directas a una página web personalizada
- Habilitar el acceso a los servicios cuando está inactivo
- Habilitar el almacenamiento en búfer TCP de respuestas
- Habilitar compresión
- Mantener la conexión de cliente para varias solicitudes de cliente
- Insertar la dirección IP del cliente en el encabezado de solicitud
- Recuperar detalles de ubicación de la dirección IP del usuario mediante la base de datos de geolocalización
- Usar la dirección IP de origen del cliente al conectarse al servidor
- Configurar el puerto de origen para las conexiones del lado del servidor
- Establecer un límite en el número de conexiones de cliente
- Establecer un límite en el número de solicitudes por conexión al servidor
- Establecer un valor de umbral para los monitores enlazados a un servicio
- Establecer un valor de tiempo de espera para las conexiones de cliente inactivas
- Establecer un valor de tiempo de espera para las conexiones de servidor inactivas

- Establecer un límite en el uso del ancho de banda por parte de los clientes
- Redirigir las solicitudes de cliente a una caché
- Conservar el identificador de VLAN para la transparencia de VLAN
- Configurar la transición de estado automática en función del porcentaje de estado de los servicios enlazados

Aumente gradualmente la carga de un nuevo servicio con inicio lento a nivel de servidor virtual

August 20, 2021

Puede configurar el dispositivo Citrix ADC para que aumente gradualmente la carga en un servicio (el número de solicitudes que el servicio recibe por segundo) inmediatamente después de que el servicio se haya agregado a una configuración de equilibrio de carga o haya cambiado de estado de ABAJO a ARRIBA (en este documento, el término "nuevo servicio" es utilizado para ambas situaciones). Puede aumentar la carga manualmente con los valores de carga e intervalos de su elección (inicio lento manual) o configurar el dispositivo para que aumente la carga en un intervalo especificado (inicio lento automático) hasta que el servicio reciba tantas solicitudes como los demás servicios de la configuración. Durante el período de aumento del servicio nuevo, el dispositivo utiliza el método de equilibrio de carga configurado.

Esta funcionalidad no está disponible globalmente. Debe configurarse para cada servidor virtual. La funcionalidad solo está disponible para servidores virtuales que utilizan uno de los siguientes métodos de equilibrio de carga:

- Round robin
- Conexión mínima
- Tiempo de respuesta mínimo
- Ancho de banda mínimo
- Menos paquetes
- LRTM (método de tiempo de respuesta mínimo)
- Carga personalizada

Para esta funcionalidad, debe establecer los siguientes parámetros:

- La nueva tasa de solicitudes de servicio, que es la cantidad en la que se aumenta el número o el porcentaje de solicitudes enviadas a un nuevo servicio cada vez que se incrementa la tasa. Es decir, se especifica el tamaño del incremento en términos del número de solicitudes por segundo o el porcentaje de la carga que soportan, en ese momento, los servicios existentes. Si este valor se establece en 0 (cero), no se realiza un inicio lento en los servicios nuevos.

Nota: En un modo de inicio lento automatizado, el incremento final es menor que el valor especificado si el valor especificado colocaría una carga más pesada en el nuevo servicio que en los demás servicios.

- El intervalo de incremento, en segundos. Si este valor se establece en 0 (cero), la carga no se incrementa automáticamente. Tienes que incrementarlo manualmente.

Con un inicio lento automatizado, un servicio sale de la fase de inicio lento cuando se aplica una de las siguientes condiciones:

- La tasa real de solicitudes es menor que la nueva tasa de solicitudes de servicio.
- El servicio no recibe tráfico durante tres intervalos sucesivos de incremento.
- La tasa de solicitud se ha incrementado 200 veces.
- El porcentaje de tráfico que debe recibir el nuevo servicio es mayor o igual a 100.

Con el inicio lento manual, el servicio permanece en la fase de inicio lento hasta que lo saque de esa fase.

Inicio lento manual

Si quiere aumentar manualmente la carga en un servicio nuevo, no especifique un intervalo de incremento para el servidor virtual de equilibrio de carga. Especifique solo la nueva tasa de solicitud de servicio y las unidades. Sin intervalo especificado, el dispositivo no incrementa la carga periódicamente. Mantiene la carga en el nuevo servicio en el valor especificado por la combinación de la nueva tasa de solicitud de servicio y unidades hasta que modifique manualmente cualquiera de los parámetros. Por ejemplo, si establece los nuevos parámetros de velocidad de solicitud de servicio y unidad en 25 y “por segundo”, respectivamente, el dispositivo mantiene la carga en el nuevo servicio en 25 solicitudes por segundo hasta que cambie cualquiera de los parámetros. Cuando quiera que el nuevo servicio salga del modo de inicio lento y reciba tantas solicitudes como los servicios existentes, establezca el nuevo parámetro de velocidad de solicitud de servicio en 0.

Como ejemplo, suponga que está usando un servidor virtual para equilibrar la carga de 2 servicios, Service1 y Service2, en modo round robin. Además, suponga que el servidor virtual está recibiendo 240 solicitudes por segundo y que está distribuyendo la carga de manera uniforme entre los servicios. Cuando se agrega un nuevo servicio, Service3, a la configuración, es posible que quiera aumentar la carga en él manualmente a través de valores de 10, 20 y 40 solicitudes por segundo antes de enviar su parte completa de la carga. En la tabla siguiente se muestran los valores en los que se establecen los tres parámetros.

Cuadro 1 Valores de parámetros

Parámetro	Valor
Intervalo en segundos	0

Parámetro	Valor
Nueva tarifa de solicitudes de servicio	10, 20, 40 y 0, a intervalos que elija
Unidades para la nueva tarifa de solicitud de servicio	Solicitudes por segundo

Cuando establece el nuevo parámetro de velocidad de solicitud de servicio en 0, Service3 ya no se considera un servicio nuevo y recibe su parte completa de la carga.

Suponga que agrega otro servicio, Service4, durante el período de aumento para Service3. En este ejemplo, Service4 se agrega cuando el nuevo parámetro de velocidad de solicitud de servicio se establece en 40. Por lo tanto, Service4 comienza a recibir 40 solicitudes por segundo.

La tabla siguiente muestra la distribución de carga en los servicios durante el período descrito en este ejemplo.

Tabla 2. Distribución de carga en servicios al aumentar manualmente la carga

	nueva tasa de solicitud de servicio = 10 req/seg (Service3Added)	nueva tasa de solicitud de servicio = 20 req/seg.	nueva tasa de solicitud de servicio = 40 req/seg (servicio4 agregado)	nueva tasa de solicitud de servicio = 0 req/seg (nuevos servicios salen del modo de inicio lento)
Service1	115	110	80	60
Service2	115	110	80	60
Service3	10	20	40	60
Service4	-	-	40	60
Total de repetido/s (carga en el servidor virtual)	240	240	240	240

Inicio lento automatizado

Si quiere que el dispositivo aumente automáticamente la carga en un servicio nuevo a intervalos especificados hasta que el servicio pueda considerarse capaz de manejar su parte completa de la carga, establezca el nuevo parámetro de velocidad de solicitud de servicio, el parámetro de unidades y el intervalo de incremento. Cuando todos los parámetros se establecen en valores distintos de 0, el dispositivo incrementa la carga de un nuevo servicio por el valor de la nueva velocidad de solicitud de servicio, en el intervalo especificado, hasta que el servicio recibe su parte completa de la carga.

Como ejemplo, supongamos que cuatro servicios, Service1, Service2, Service3 y Service4, están enlazados a un servidor virtual de equilibrio de carga, vserver1. Además, supongamos que vserver1 recibe 100 solicitudes por segundo y que distribuye la carga uniformemente entre los servicios (25 solicitudes por segundo por servicio). Al agregar un quinto servicio, Service5, a la configuración, es posible que quiera que el dispositivo envíe el nuevo servicio 4 solicitudes por segundo durante los primeros 10 segundos, 8 solicitudes por segundo durante los próximos 10 segundos, etc., hasta que reciba 20 solicitudes por segundo. Para este requisito, la tabla siguiente muestra los valores en los que se establecen los tres parámetros:

Tabla 3. Valores de parámetros

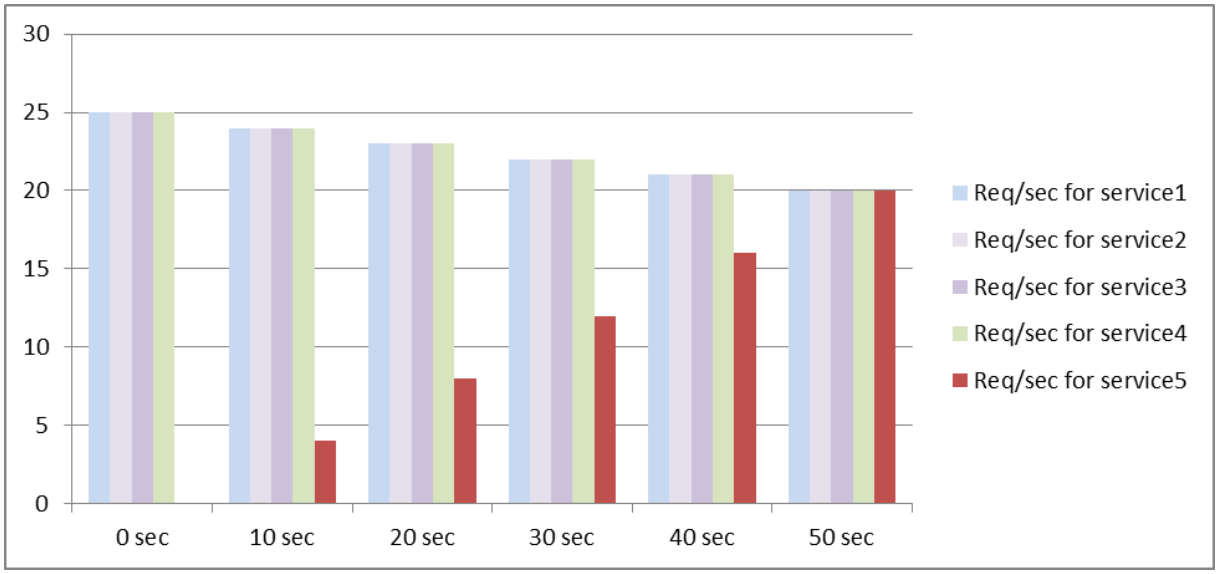
Parámetro	**Valor**
Intervalo en segundos	10
Valor de incremento	4
Unidades para la nueva tarifa de solicitud de servicio	Solicitudes por segundo

Con esta configuración, el nuevo servicio comienza a recibir tantas solicitudes como los servicios existentes 50 segundos después de que se agrega o su estado ha cambiado de DOWN a UP. Durante cada intervalo de este período, el dispositivo distribuye a los servidores existentes el exceso de solicitudes que se habrían enviado al nuevo servicio en ausencia de incrementos por etapas. Por ejemplo, en ausencia de incrementos escalonados, cada servicio, incluido Service5, habría recibido 20 solicitudes cada uno por segundo. Con incrementos escalonados, durante los primeros 10 segundos, cuando Service5 recibe solo 4 solicitudes por segundo, el dispositivo distribuye el exceso de 16 solicitudes por segundo a los servicios existentes, lo que da como resultado el patrón de distribución que se muestra en la siguiente tabla y ilustración durante el período de 50 segundos. Después del período de 50 segundos, Service5 ya no se considera un servicio nuevo y recibe su parte normal del tráfico.

Tabla 4. Patrón de distribución de carga en todos los servicios para el período de 50 segundos inmediatamente después de agregar Service5

	0 s	10 s	20 s	30 s	40 s	50 s
Req/seg para Service1	25	24	23	22	21	20
Req/seg para Service2	25	24	23	22	21	20
Req/seg para Service3	25	24	23	22	21	20
Req/seg para Service4	25	24	23	22	21	20
Req/seg para Service5	0	4	8	12	16	20
Total de repetido/s (carga en el servidor virtual)	100	100	100	100	100	100

Ilustración 1. Un gráfico del patrón de distribución de carga en todos los servicios para el período de 50 segundos inmediatamente después de agregar Service5



Un requisito alternativo podría ser que el dispositivo envíe Service5 el 25% de la carga de los servicios existentes en los primeros 5 segundos, el 50% en los siguientes 5 segundos, etc., hasta que reciba 20 solicitudes por segundo. Para este requisito, la tabla siguiente muestra los valores en los que se establecen los tres parámetros.

Tabla 5. Valores de parámetros

Parámetro	Valor
Intervalo en segundos	5
Valor de incremento	25
Unidades para la nueva tarifa de solicitud de servicio	Porcentaje

Con esta configuración, el servicio comienza a recibir tantas solicitudes como los servicios existentes 20 segundos después de que se agrega o su estado ha cambiado de DOWN a UP. La distribución del tráfico durante el período de aumento para el nuevo servicio es idéntica a la descrita anteriormente, donde la unidad para los incrementos de paso era “solicitudes por segundo”.

Establecer los parámetros de inicio lento

Los parámetros de inicio lento se establecen mediante el comando `set lb vserver` o el `add lb vserver` comando. El siguiente comando es para establecer parámetros de inicio lento al agregar un servidor virtual.

Para configurar incrementos de carga por etapas para un nuevo servicio mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para configurar incrementos paso a paso en la carga de un servicio y compruebe la configuración:

```
add lb vserver <name> <serviceType> <IPAddress> <port> [-
    newServiceRequest <positive_integer>] [<newServiceRequestUnit>] [-
    newServiceRequestIncrementInterval <positive_integer>]

show lb vserver <name>
<!--NeedCopy-->
```

Ejemplo

```
set lb vserver BR_LB -newServiceRequest 5 PER_SECOND -
    newServiceRequestIncrementInterval 10
Done

show lb vserver BR_LB
BR_LB (192.0.2.33:80) - HTTP Type: ADDRESS
State: UP
...
...
New Service Startup Request Rate: 5 PER_SECOND, Increment Interval: 10
...
...
Done
<!--NeedCopy-->
```

Para configurar incrementos de carga por etapas para un nuevo servicio mediante la utilidad de configuración

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**y abra un servidor virtual.
2. En Configuración avanzada, seleccione Método y establezca los siguientes parámetros de inicio lento:
   - Ratio de solicitudes de inicio de servicio nuevo.
   - Nueva Unidad de Solicitud de Servicio.

- Intervalo de incremento.

La opción sin monitor para los servicios

August 20, 2021

Si utiliza un sistema externo para realizar comprobaciones de estado de los servicios y no quiere que el dispositivo Citrix ADC supervise el estado de un servicio, puede establecer la opción sin monitor para el servicio. Si lo hace, el dispositivo no envía sondeos para comprobar el estado del servicio, sino que muestra el servicio como UP. Incluso si el servicio se apaga, el dispositivo continúa enviando tráfico desde el cliente al servicio según lo especificado por el método de equilibrio de carga.

El monitor puede estar en el estado ABLED o DISABLED cuando se establece la opción sin monitor, y cuando se quita la opción sin monitor, se reanuda el estado anterior del monitor.

Puede establecer la opción sin monitor para un servicio al crear el servicio. También puede configurar la opción sin monitor en un servicio existente.

Las siguientes son las consecuencias de establecer la opción sin monitor:

- Si se desactiva un servicio para el que ha habilitado la opción sin monitor, el dispositivo continúa mostrando el servicio como UP y continúa reenviando tráfico al servicio. Una conexión persistente con el servicio puede empeorar la situación. En ese caso, o si muchos servicios mostrados como UP son en realidad DOWN, el sistema puede fallar. Para evitar tal situación, cuando el mecanismo externo que supervisa los servicios informa de un servicio como DOWN, elimine el servicio de la configuración de Citrix ADC.
- Si configura la opción sin monitor en un servicio, no puede configurar el equilibrio de carga en el modo de retorno directo del servidor (DSR). Para un servicio existente, si establece la opción sin monitor, no puede configurar el modo DSR para el servicio.

Para establecer la opción sin monitor para un servicio nuevo mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para crear un servicio con la opción Monitor de estado y compruebe la configuración:

```
1 add service <serviceName> <IP | serverName> <serviceType> <port> -
     healthMonitor (YES|NO)
2 <!--NeedCopy-->
```

Ejemplo:


```
add service nomonsrvc 10.102.21.21 http 80 -healthMonitor no
Done

show service nomonsrvc
nomonsrvc (10.102.21.21:80) - HTTP
State: UP
Last state change was at Mon Nov 15 22:41:29 2010
Time since last state change: 0 days, 00:00:00.970
Server Name: 10.102.21.21
 Server ID : 0 Monitor Threshold : 0
...
Access Down Service: NO
...
Down state flush: ENABLED
Health monitoring: OFF

1 bound monitor:
1) Monitor Name: tcp-default
State: UNKNOWN Weight: 1
Probes: 3 Failed [Total: 3 Current: 3]
Last response: Probe skipped - Health monitoring is turned off.
Response Time: N/A
Done
<!--NeedCopy-->
```

Para establecer la opción sin monitor para un servicio existente mediante la CLI

En el símbolo del sistema, escriba el comando siguiente para establecer la opción del monitor de estado:

```
set service <name> -healthMonitor (YES|NO)
<!--NeedCopy-->
```

Ejemplo:

```
By default, the state of a service and the state of the corresponding
   monitor are UP.
 >show service LB-SVC1
LB-SVC1 (10.102.29.5:80) - HTTP
State: UP
```



```
5
6
7  1) Monitor Name: http-ecv
8   State: UP Weight: 1
9  Probes: 99992 Failed [Total: 0 Current: 0]
10 Last response: Success - Pattern found in response.
11 Response Time: 3.76 millisec
12 Done
13
14 When the no-monitor option is set on a service, the state of the
       monitor changes to UNKNOWN.
15 set service LB-SVC1 -healthMonitor NO
16 Done
17
18 show service LB-SVC1
19 LB-SVC1 (10.102.29.5:80) - HTTP
20 State: UP
21 Last state change was at Fri Dec 10 10:17:37 2010.
22 Time since last state change: 5 days, 18:55:48.710
23 Health monitoring: OFF
24
25 1) Monitor Name: http-ecv
26    State: UNKNOWN Weight: 1
27          Probes: 100028 Failed [Total: 0 Current: 0]
28    Last response: Probe skipped - Health monitoring is turned off.
29      Response Time: 0.0 millisec
30   Done
31 When the no-monitor option is removed, the earlier state of the monitor
       is resumed.
32 > set service LB-SVC1 -healthMonitor YES
33 Done
34 >show service LB-SVC1
35 LB-SVC1 (10.102.29.5:80) - HTTP
36 State: UP
37 Last state change was at Fri Dec 10 10:17:37 2010
38 Time since last state change: 5 days, 18:57:47.880
39 1) Monitor Name: http-ecv
40    State: UP Weight: 1
41    Probes: 100029 Failed [Total: 0 Current: 0]
42    Last response: Success - Pattern found in response.
43    Response Time: 5.690 millisec
44    Done
45 <!--NeedCopy-->
```


Para establecer la opción sin monitor para un servicio mediante la interfaz gráfica de usuario

1. Vaya a Administración de Tráfico > Equilibrio de carga > Servicios.
2. Abra el servicio y desactive Supervisión del estado.

Proteja las aplicaciones en servidores protegidos contra sobretensiones de tráfico

August 20, 2021

El dispositivo Citrix ADC proporciona la opción de protección contra sobretensiones para mantener la capacidad de un servidor o caché. El dispositivo regula el flujo de solicitudes de cliente a los servidores y controla el número de clientes que pueden acceder simultáneamente a los servidores. El dispositivo bloquea las sobretensiones pasadas al servidor, lo que evita la sobrecarga del servidor.

Para que la protección contra sobretensiones funcione correctamente, debe habilitarla globalmente. Para obtener más información sobre protección contra sobretensiones, consulte Protección contra sobretensiones.

Para establecer la protección contra sobretensiones en el servicio mediante la CLI

En el símbolo del sistema, escriba:

```
set service <name> -sp <Value>
<!--NeedCopy-->
```

Ejemplo:

```
set service Service-HTTP-1 -sp ON
<!--NeedCopy-->
```

Para establecer la protección contra sobretensiones en el servicio mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servicios**y abra un origen.
2. En Configuración avanzada, seleccione Configuración de **tráfico**y, a continuación, **Protección contra sobretensiones**.

Habilitar la limpieza de las conexiones de servidor virtual y servicio

August 20, 2021

El estado de un servidor virtual depende de los estados de los servicios vinculados a él. El estado de cada servicio depende de las respuestas de los servidores con equilibrio de carga a los sondeos o comprobaciones de estado enviados por los monitores vinculados a ese servicio. A veces, los servidores con equilibrio de carga no responden. Si un servidor es lento u ocupado, los sondeos de supervisión pueden agotar el tiempo de espera. Si los sondeos de supervisión repetidos no se responden dentro del período de tiempo de espera configurado, el servicio se marca como DOWN. Si un servicio o servidor virtual están marcados como INactivo, se deben vaciar las conexiones del lado del servidor y del cliente. Terminar las conexiones existentes libera recursos y, en algunos casos, acelera la recuperación de configuraciones de equilibrio de carga sobrecargadas.

En determinadas condiciones, puede configurar la configuración **DownStateFlush** para que termine inmediatamente las conexiones existentes cuando un servicio o un servidor virtual estén marcados como DESCONECTADAS. No active la configuración DownStateFlush en los servidores de aplicaciones que deben completar sus transacciones. Puede habilitar esta configuración en servidores web cuyas conexiones se pueden terminar de forma segura cuando marquen hacia abajo.

En la siguiente tabla se resume el efecto de esta configuración en una configuración de ejemplo que consta de un servidor virtual, VServer-LB-1, con un servicio vinculado a él, Service-1. En la tabla, E y D indican el estado de la configuración DownStateFlush: E significa Habilitado y D significa Inhabilitado.

Vserver-LB-1	Service-1	Estado de las conexiones
E	E	Se terminan las conexiones de cliente y servidor.

Vserver-LB-1	Service-1	Estado de las conexiones
E	D	En algunos tipos de servicio, como TCP, para los que el dispositivo Citrix ADC no admite la reutilización de conexiones, se terminan las conexiones cliente y servidor. Para los tipos de servicio, como HTTP, para los que el dispositivo admite la reutilización de conexiones, las conexiones cliente y servidor solo se terminan si una transacción está activa en esas conexiones. Si una transacción no está activa, solo se terminan las conexiones de cliente.
D	E	En algunos tipos de servicio, como TCP, para los que el dispositivo Citrix ADC no admite la reutilización de conexiones, se terminan las conexiones cliente y servidor. Para los tipos de servicio, como HTTP, para los que el dispositivo admite la reutilización de conexiones, las conexiones cliente y servidor solo se terminan si una transacción está activa en esas conexiones. Si una transacción no está activa, solo se finalizan las conexiones del servidor.
D	D	Ni las conexiones del cliente ni del servidor se terminan.

Si quiere inhabilitar un servicio solo cuando el servidor o el cliente cierran todas las conexiones establecidas, puede utilizar la opción de apagado estable. Para obtener información sobre el cierre correcto de un servicio, consulte Cierre de servicios de forma grácil.

Para establecer el estado de descarga en el servicio mediante la CLI

En el símbolo del sistema, escriba:

```
set service <name>  -downStateFlush (ENABLED | DISABLED )
<!--NeedCopy-->
```

Ejemplo:

```
set service Service-HTTP-1 -downStateFlush enabled
<!--NeedCopy-->
```

Para establecer el estado de descarga en el servicio mediante el uso de la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servicios**y abra un servicio.
2. En Configuración avanzada, seleccione Configuración de **tráfico**y, a continuación, **Vaciado de estado descendente**.

Para establecer el vaciado de estado en el servidor virtual mediante la CLI

En el símbolo del sistema, escriba:

```
set lb vserver <name>  -downStateFlush (ENABLED | DISABLED )
<!--NeedCopy-->
```

Ejemplo:

```
set lb vserver vsvr1 -downStateFlush enabled
<!--NeedCopy-->
```


Para establecer el estado de descarga en el servidor virtual mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**y abra un servidor virtual.
2. En Configuración avanzada, seleccione Configuración de **tráfico**y, a continuación, **Vaciado de estado descendente**.

Apagado estable de los servicios

August 20, 2021

Durante las interrupciones programadas de la red, como las actualizaciones del sistema o el mantenimiento del hardware, es posible que tenga que cerrar o inhabilitar algunos servicios. Más adelante, puede habilitar el servicio mediante el comando "enable service <name>.

Para evitar interrumpir las sesiones establecidas, puede colocar un servicio en el estado Transición Fuera del Servicio (TROFS) mediante una de las siguientes acciones:

- Agregar un código o una cadena TROFS al monitor: Configure el servidor para que envíe un código o una cadena específicos en respuesta a un sondeo de monitor.
- Inhabilite explícitamente el servicio y:
  - Establezca un retraso (en segundos).
  - Habilite el apagado correcto.

Adición de un código o cadena TROFS

Si vincula solo un monitor a un servicio y el monitor está habilitado para TROFS, puede colocar el servicio en el estado TROFS sobre la base de la respuesta del servidor a un sondeo de monitor. Esta respuesta se compara con el valor del parámetro TrofsCode para un monitor HTTP o el parámetro TrofsString para un monitor HTTP-ECV o TCP-ECV. Si el código coincide, el servicio se coloca en el estado TROFS. En este estado, continúa honrando las conexiones persistentes.

Si varios monitores están vinculados a un servicio, el estado efectivo del servicio se calcula sobre la base del estado de todos los monitores vinculados al servicio. Al recibir una respuesta TROFS, el estado del monitor habilitado para TRFS se considera UP a efectos de este cálculo. Para obtener más información sobre cómo un dispositivo Citrix ADC designa un servicio como UP, consulte Configuración de un valor umbral para los monitores enlazados a un servicio.

Importante:

- Puede enlazar varios monitores a un servicio, pero no debe habilitar trofs-más de uno de ellos.

- Puede convertir un monitor habilitado para TROFS en un monitor que no esté habilitado para TRFS, pero no viceversa.

Para configurar un código o una cadena TROFS en un monitor mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba uno de los siguientes comandos:

```
add lb monitor <monitor-name> HTTP -trofsCode <respcode>

add lb monitor <monitor-name> HTTP-ECV  -trofsString <resp string>

add lb monitor <monitor-name> TCP-ECV  -trofsString <resp string>
<!--NeedCopy-->
```

Para modificar el código o la cadena TROFS mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba uno de los siguientes comandos:

```
set lb monitor <trofs monitorname> HTTP -trofscode <newcode>

set lb monitor <trofs monitorname> HTTP-ECV -trofsstring <new string>

set lb monitor <trofs monitorname> TCP-ECV -trofsstring <new string>
<!--NeedCopy-->
```

Nota: Puede utilizar el comando set solo si se ha agregado anteriormente un monitor habilitado para TRFS. No puede utilizar este comando para establecer el código o la cadena TROFS para un monitor que no esté habilitado para TROFS.

Para configurar un código o una cadena TROFS en un monitor mediante la utilidad de configuración

1. Vaya a Administración del Tráfico > Equilibrio de carga > Monitores.
2. En el panel Monitores, haga clic en Agregar y realice una de las acciones siguientes:
   - Seleccione Tipo como HTTP y especifique un código TROFS.
   - Seleccione Tipo como HTTP-ECV o TCP-ECV y especifique una cadena TROFS.

Desactivación de un servicio

Sin embargo, a menudo no se puede estimar la cantidad de tiempo necesario para que todas las conexiones a un servicio completen las transacciones existentes. Si una transacción no está terminada cuando caduca el tiempo de espera, el cierre del servicio puede provocar la pérdida de datos. En este caso, puede especificar el apagado estable para el servicio, de modo que el servicio solo se inhabilite cuando el servidor o el cliente cierran todas las conexiones de cliente activas actuales. Consulte la tabla siguiente para ver el comportamiento si especifica un tiempo de espera además de un apagado estable.

La persistencia se mantiene de acuerdo con el método especificado incluso si habilita el apagado estable. El sistema continúa sirviendo a todos los clientes persistentes, incluidas las nuevas conexiones de los clientes, a menos que el servicio esté marcado como DOWN durante el estado de apagado estable como resultado de las comprobaciones realizadas por un monitor.

En la tabla siguiente se describen las opciones de apagado adecuadas.

State	Resultados
El apagado estable está habilitado y se especifica un tiempo de espera.	El servicio se cierra después de que se sirve la última de las conexiones de cliente activas actuales, incluso si el tiempo de espera no ha expirado. El dispositivo comprueba el estado de las conexiones una vez por segundo. Si el tiempo de espera expira, las sesiones abiertas se cerrarán.
El apagado estable está inhabilitado y se especifica un tiempo de espera.	El servicio se cierra solo después de que expire el tiempo de espera, incluso si todas las conexiones establecidas se sirven antes de la expiración.
El apagado estable está habilitado y no se especifica tiempo de espera.	El servicio se cierra solo después de que se sirve la última de las conexiones establecidas previamente, independientemente del tiempo que se tarda en servir a la última conexión.
El apagado estable está inhabilitado y no se especifica tiempo de espera.	No hay apagado estable. El servicio se apaga inmediatamente después de que se elige la opción disable o se emite el comando disable. (El tiempo de espera predeterminado es cero segundos).

Para terminar las conexiones existentes cuando un servicio o un servidor virtual está marcado como

DOWN, puede utilizar la opción Desactivar estado. Para obtener más información, consulte Habilitación de la limpieza de conexiones de servidores virtuales.

Para configurar el apagado estable para un servicio mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para cerrar un servicio correctamente y verificar la configuración:

```
disable service <name> [<delay>] [-graceFul (YES|NO)]

show service <name>
<!--NeedCopy-->
```

Ejemplo:

```
> disable service svc1 6000 -graceFul YES
Done
>show service svc1
svc1 (10.102.80.41:80) - HTTP
State: GOING OUT OF SERVICE (Graceful, Out Of Service in 5998 seconds)
Last state change was at Mon Nov 15 22:44:15 2010
Time since last state change: 0 days, 00:00:01.160
...
Down state flush: ENABLED

1 bound monitor:
1) Monitor Name: tcp-default
State: UP              Weight: 1
Probes: 13898    Failed [Total: 0 Current: 0]
Last response: Probe skipped - live traffic to service.
Response Time: N/A
Done

>show service svc1
svc1 (10.102.80.41:80) - HTTP
State: OUT OF SERVICE
Last state change was at Mon Nov 15 22:44:19 2010
Time since last state change: 0 days, 00:00:03.250
Down state flush: ENABLED

```



```
1 bound monitor:
1)  Monitor Name: tcp-default
State: UNKNOWN           Weight: 1
Probes: 13898    Failed [Total: 0 Current: 0]
Last response: Probe skipped - service state OFS.
Response Time: N/A
Done
<!--NeedCopy-->
```

Para configurar el apagado estable para un servicio mediante la utilidad de configuración

1. Vaya a Administración de Tráfico > Equilibrio de carga > Servicios.
2. Abra el servicio y, en la lista Acciones, haga clic en Inhabilitar. Introduzca un tiempo de espera y seleccione Agraciado.

Habilitar o inhabilitar la sesión de persistencia en los servicios TROFS

August 20, 2021

Puede establecer el indicador TROFSpersistence para especificar si un servicio en estado de transición fuera de servicio (TROFS) debe mantener sesiones persistentes. Cuando un monitor está habilitado TROFS, puede colocar un servicio en el estado TROFS sobre la base de la respuesta del servidor a un sondeo de monitor. Esta respuesta se compara con el valor del parámetro TrofsCode para un monitor HTTP o el parámetro TrofsString para un monitor HTTP-ECV o TCP-ECV. Si el código coincide, el servicio se coloca en el estado TROFS. En este estado, continúa honrando las conexiones de cliente activas. En algunos casos, las sesiones activas honradas podrían tener que incluir sesiones persistentes. Pero en otros casos, especialmente aquellos que implican sesiones de persistencia de larga duración o métodos de persistencia, como el ID de servidor personalizado, respetar las sesiones persistentes puede impedir que el servicio pase al estado fuera de servicio.

Si establece el indicador trofsPersistence en ENABLED, se respetan las sesiones persistentes. Si lo establece en DISABLED, no lo son.

Para establecer el indicador TrofsPersistence mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba uno de los siguientes comandos para establecer el indicador `trofsPersistence` de un nuevo servidor virtual o un servidor virtual existente, o para devolver la configuración a su valor predeterminado:


```
add lb vserver <name> [-trofsPersistence ( ENABLED | DISABLED )]

set lb vserver <name> [-trofsPersistence ( ENABLED | DISABLED )]

unset lb vserver <name> [-trofsPersistence]
<!--NeedCopy-->
```

Argumento

trofsPersistence. Respetar las conexiones actuales de cliente activo y las nuevas solicitudes en sesiones de persistencia cuando el servicio está en estado TROFS.

Valores posibles: ENABLED, DISABLED. Valor predeterminado: ENABLED.

Ejemplos:

```
add lb vserver v1 http 10.102.217.42 80 -persistencetype SOURCEIP -
    trofsPersistence ENABLED

set lb vserver v1 -trofsPersistence DISABLED

unset lb vserver v1 -trofsPersistence
<!--NeedCopy-->
```

Solicitudes directas a una página web personalizada

February 19, 2022

> **Advertencia**
>
> SureConnect (SC) ha quedado obsoleto de NetScaler 12.0 compilación 56.20 en adelante y, como alternativa, Citrix recomienda utilizar la función AppQOe. Para obtener más información, consulteAppQOE.

Para que SureConnect funcione correctamente, debe configurarlo globalmente. Citrix ADC proporciona la opción SureConnect para garantizar la respuesta de una aplicación.
Para obtener más información sobre la opción SureConnect, consulte Sure Connect.

Para configurar SureConnect en el servicio mediante la CLI

En el símbolo del sistema, escriba:

```
set service <name> -sc <Value>
<!--NeedCopy-->
```

Ejemplo:

```
set service Service-HTTP-1 -sc ON
<!--NeedCopy-->
```

Para configurar SureConnect en el servicio mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servicios**y abra un servicio.
2. En Configuración avanzada, selecciona Configuración de tráfico y selecciona **Sure Connect**.

Habilitar el acceso a los servicios cuando está inactivo

August 20, 2021

Puede habilitar el acceso a un servicio cuando está inhabilitado o en estado DOWN configurando el dispositivo Citrix ADC para que utilice el modo de capa 2 para conectar los paquetes enviados al servicio. Normalmente, cuando las solicitudes se reenvían a servicios que están DOWN, los paquetes de solicitud se descartan. Sin embargo, cuando habilita la configuración **Access Down**, estos paquetes de solicitud se envían directamente a los servidores con equilibrio de carga.

Para obtener más información sobre los modos de capa 2 y capa 3, consulte Direcciones IP.

Para que el dispositivo pueda conectar los paquetes enviados a los servicios DOWN, habilite el modo Capa 2 con el parámetro AccessDown.

Para habilitar el acceso hacia abajo en un servicio mediante la CLI

En el símbolo del sistema, escriba:

```
set service <name> -accessDown <Value>
<!--NeedCopy-->
```


Ejemplo:

```
set service Service-HTTP-1 -accessDown YES
<!--NeedCopy-->
```

Para habilitar el acceso hacia abajo en un servicio mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servicios**y abra un servicio.
2. En Configuración avanzada, selecciona **Configuración de tráfico**y selecciona **Acceso descendente**.

Habilitar el almacenamiento en búfer TCP de respuestas

August 20, 2021

El dispositivo Citrix ADC proporciona una opción de almacenamiento en búfer TCP que solo almacena en búfer las respuestas del servidor con equilibrio de carga. Esto permite que el dispositivo envíe respuestas de servidor al cliente a la velocidad máxima que el cliente puede aceptarlas. El dispositivo asigna de 0 a 4095 MB (MB) de memoria para almacenamiento en búfer TCP y de 4 a 20480 kilobytes (KB) de memoria por conexión.

Nota: El almacenamiento en búfer TCP establecido en el nivel de servicio tiene prioridad sobre la configuración global.
Para obtener más información sobre cómo configurar el buffering TCP globalmente, consulte Almacenamiento en búfer TCP.

Para habilitar el almacenamiento en búfer TCP en un servicio mediante la CLI

En el símbolo del sistema, escriba:

```
set service <name> -TCPB <Value>
<!--NeedCopy-->
```

Ejemplo:


```
set service Service-HTTP-1 -TCPB YES
<!--NeedCopy-->
```

Para habilitar el almacenamiento en búfer TCP en un servicio mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servicios**y abra un servicio.
2. En Configuración avanzada, seleccione **Configuración de tráfico**y seleccione **Almacenamiento en búfer TCP**.

Habilitar compresión

August 20, 2021

El dispositivo Citrix ADC proporciona una opción de compresión para comprimir archivos HTML y de texto de forma transparente mediante un conjunto de directivas de compresión integradas. La compresión reduce los requisitos de ancho de banda y puede mejorar significativamente la capacidad de respuesta del servidor en configuraciones con limitaciones de ancho de banda. Las directivas de compresión están asociadas con servicios vinculados al servidor virtual. Las directivas determinan si una respuesta se puede comprimir y enviar contenido comprimible al dispositivo, que lo comprime y lo envía al cliente.

Nota: Para que la compresión funcione correctamente, debe habilitarla globalmente. Para obtener más información sobre cómo configurar la compresión globalmente, consulte Compresión.

Para habilitar la compresión en un servicio mediante la CLI

En el símbolo del sistema, escriba:

```
set service <name> -CMP <YES | NO>
<!--NeedCopy-->
```

Ejemplo:

```
set service Service-HTTP-1 -CMP YES
<!--NeedCopy-->
```


Para habilitar la compresión en un servicio mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servicios**y abra un servicio.
2. En Configuración avanzada, selecciona **Configuración de tráfico**y, a continuación, **Compresión**.

Habilitar la comprobación externa del estado de TCP para servidores virtuales UDP

August 20, 2021

En las nubes públicas, puede utilizar el dispositivo Citrix ADC como equilibrador de carga de segundo nivel cuando se utiliza el equilibrador de carga nativo como primer nivel. El equilibrador de carga nativo puede ser un equilibrador de carga de aplicaciones (ALB) o un equilibrador de carga de red (NLB). La mayoría de las nubes públicas no admiten sondas de estado UDP en sus equilibradores de carga nativos. Para supervisar el estado de la aplicación UDP, las nubes públicas recomiendan agregar un extremo basado en TCP al servicio. El punto final refleja el estado de la aplicación UDP.

El dispositivo Citrix ADC admite la comprobación de estado basada en TCP externa para un servidor virtual UDP. Esta función introduce un detector TCP en el VIP del servidor virtual y el puerto configurado. El agente de escucha TCP refleja el estado del servidor virtual.

Para habilitar una comprobación de estado TCP externa para servidores virtuales UDP mediante CLI

En el símbolo del sistema, escriba el comando siguiente para habilitar una comprobación de estado TCP externa con la opción TcpProbeport:

```
1 add lb vserver <name> <serviceType> <IPAddress> <port> -tcpProbePort <
     tcpProbePort>
2 <!--NeedCopy-->
```

Ejemplo:

```
1 add lb vserver Vserver-UDP-1 UDP 10.102.29.60 80 tcpProbePort 5000
2 <!--NeedCopy-->
```


Para habilitar una comprobación de estado TCP externa para servidores virtuales UDP mediante GUI

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**y, a continuación, cree un servidor virtual.
2. Haga clic en **Agregar** para crear un servidor virtual.
3. En el panel **Configuración básica**, agregue el número de puerto en el campo **Puerto de sondeo TCP**.
4. Haga clic en **Aceptar**.

Mantener la conexión de cliente para varias solicitudes de cliente

August 20, 2021

Puede configurar el parámetro keep-alive del cliente para configurar un servicio HTTP o SSL para mantener abierta una conexión de cliente a un sitio web en varias solicitudes de cliente. Si el cliente keep-alive está habilitado, incluso cuando el servidor web con equilibrio de carga cierra una conexión, el dispositivo Citrix ADC mantiene abierta la conexión entre el cliente y él mismo. Esta configuración permite que los servicios atiendan varias solicitudes de cliente en una sola conexión de cliente.

Si no habilita esta configuración, el cliente abre una nueva conexión para cada solicitud que envía al sitio web. La configuración Keep-alive del cliente ahorra el tiempo de ida y vuelta del paquete necesario para establecer y cerrar conexiones. Esta configuración también reduce el tiempo necesario para completar cada transacción. El mantenimiento del cliente solo se puede habilitar en tipos de servicios HTTP o SSL.

El valor keep-alive del cliente en el nivel de servicio tiene prioridad sobre la configuración global keep-alive del cliente. Para obtener más información sobre el mantenimiento del cliente, consulte Client Keep-Alive.

Para habilitar el mantenimiento del cliente en un servicio mediante la CLI

En el símbolo del sistema, escriba:

```
set service <name> -CKA <Value>
<!--NeedCopy-->
```

Ejemplo:


```
set service Service-HTTP-1 -CKA YES
<!--NeedCopy-->
```

Para habilitar el cliente keep-alive en un servicio mediante la GUI

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servicios**y abra un servicio.
2. En Configuración avanzada, seleccione **Configuración de tráfico**y, a continuación, **Client Keep-Alive**.

Inserte la dirección IP del cliente en el encabezado de solicitud

August 20, 2021

Un Citrix ADC utiliza la dirección IP de subred (SNIP) para conectarse al servidor. El servidor no necesita ser consciente del cliente.

Sin embargo, en algunas situaciones, el servidor debe ser consciente del cliente al que tiene que servir. Cuando habilita la configuración de IP del cliente, el dispositivo inserta la dirección IPv4 o IPv6 del cliente mientras reenvía las solicitudes al servidor. El servidor inserta esta IP de cliente en el encabezado de las respuestas. Por lo tanto, el servidor es consciente del cliente.

> **Nota**: Para insertar varios encabezados, debe realizar una de las siguientes acciones:
>
> - Agregue directivas de reescritura para comprobar CLIENT.IS_SSL e inserte el encabezado apropiado.
> - Enlazar la directiva de reescritura adecuada para cada servidor virtual según el tipo.

Para insertar la dirección IP del cliente en la solicitud del cliente mediante la CLI

En el símbolo del sistema, escriba:

```
set service <name> -CIP <Value> <cipHeader>
<!--NeedCopy-->
```

Ejemplo:

```
set service Service-HTTP-1 -CIP enabled X-Forwarded-For
<!--NeedCopy-->
```


Para insertar la dirección IP del cliente en la solicitud del cliente mediante la GUI

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servicios** y modifique un servicio.
2. En el panel **Configuración del servicio**, haga clic en el **icono de edición**.
3. En el panel **Servicio de equilibrio de carga**, active la casilla de verificación **Insertar dirección IP del cliente**.

Recuperar detalles de ubicación de la dirección IP del usuario mediante la base de datos de geolocalización

October 5, 2021

> **Nota** Esta función está disponible en Citrix ADC versión 12.1 compilación 50.x y posteriores.

El dispositivo Citrix ADC puede obtener detalles de ubicación del usuario, como continente, condado y ciudad. Para cualquier dirección IP pública de una base de datos de geolocalización. Se realiza mediante la infraestructura de directivas avanzada. Los detalles de ubicación recuperados se utilizan en una acción de reescritura o en una acción de respuesta para realizar los siguientes casos de uso.

- Inserte un encabezado HTTP con los detalles de ubicación del usuario (como información de país o ciudad) al enviar la solicitud del cliente al servidor back-end.
- Agrega el nombre del país en la respuesta de la página HTML de un usuario no válido.

El dispositivo también puede registrar los detalles de ubicación mediante el mecanismo de registro de auditoría.

Obtener detalles de ubicación de usuario mediante funciones de geolocalización

Los componentes interactúan de la siguiente manera:

1. El usuario envía una solicitud de cliente desde una ubicación geográfica concreta.
2. El dispositivo Citrix ADC busca la dirección IP del usuario en la solicitud del cliente y recupera los detalles de la ubicación geográfica. Los detalles incluyen detalles del continente, el país, la región, la ciudad, el ISP, la organización o los detalles personalizados de una base de datos de geolocalización.
3. Una vez recuperados los detalles de la ubicación, el dispositivo utiliza una directiva de respuesta o una directiva de reescritura para evaluar la solicitud.
4. En una directiva de reescritura, el dispositivo agrega un encabezado con los detalles de ubicación geográfica y lo envía al servidor back-end. Por ejemplo, inserta un encabezado HTTP personalizado con información del país.

5. En una directiva de respuesta, el dispositivo evalúa la solicitud HTTP y, en función de la evaluación de la directiva, permite el acceso a los usuarios o redirige al usuario a una página de error. Indica que la región desde la que acceden a la aplicación no tiene acceso.

Configuración de base de datos de geolocalización

Como requisito previo, debe tener una base de datos de geolocalización para ejecutarse en el dispositivo Citrix ADC. Los archivos de base de datos de geolocalización están disponibles con el firmware Citrix ADC. Para descargar los archivos de la base de datos de un proveedor, conviértelo al formato Citrix ADC e impórtelo en el dispositivo.
Para obtener más información sobre la base de datos de geolocalización, consulte el tema Agregar un archivo de ubicación para crear una base de datos de proximidad estática .

Funciones de geolocalización

En la tabla siguiente se proporciona una lista de funciones de geolocalización que recuperan los detalles de ubicación de cualquier dirección IP pública. Estas funciones se pueden utilizar en directivas de reescritura o de respuesta.

Función de geolocalización	Ejemplo
CLIENT.IP.SRC.UBICACIÓN	Asia. En Karnataka. Bangalore
CLIENT.IP.SRC.LOCATION.GET (1) .LOCATION_LONG	India
CLIENT.IP.SRC.LOCATION (3)	Asia. En Karnataka
CLIENT.IP.SRC.LAT_LONG	12,77
CLIENT.IPV6.SRC.LOCATION	América del Norte.us.California.Santa Clara.Verizon.Citrix
CLIENT.IPV6.SRC.LOCATION(3)	Norteamérica.us.california
CLIENT.IPV6.SRC.LOCATION.GET (1) .LOCATION_LONG	Estados Unidos
CLIENT.IPV6.SRC.LOCATION.GET (3)	California
CLIENT.IPV6.SRC.LAT_LONG	36, -119

Configuración de funciones de geolocalización

Para configurar las funciones de geolocalización mediante una infraestructura de directivas avanzada, debe habilitar las funciones de equilibrio de carga, reescritura y respuesta y, a continuación, completar los siguientes casos de uso.

Habilitar funciones de equilibrio de carga, respuesta y reescritura

Si quiere que el dispositivo Citrix ADC autorice el acceso de los usuarios desde una ubicación geográfica concreta, debe habilitar las funciones de equilibrio de carga, reescritura y respuesta.

```
enable ns feature loadbalancing rewrite responder
<!--NeedCopy-->
```

Caso de uso 1: Configuración de la función de geolocalización para redirigir a usuarios no válidos fuera de la ubicación geográfica

Cuando un usuario de la India solicita acceso a una página web, bloquea la solicitud y responde con una página HTML con el nombre del país.

Los pasos siguientes le ayudarán a completar la configuración de este caso de uso.

- Agregar acción de respuesta
- Agregar directiva de Responder
- Vincular la directiva de respuesta al servidor de equilibrio de carga

Para obtener más información sobre los procedimientos de GUI para la acción de reescritura y la configuración de la directiva de reescritura, consulte el tema Responder .

Agregar acción de respuesta

Agrega una acción de respuesta para responder con una página HTML con el nombre del país.
En el símbolo del sistema, escriba:

```
add responder action <name> <type> (<target> | <htmlpage>) [-comment <
    string>] [-responseStatusCode <positive_integer>][-reasonPhrase <
    string>]
<!--NeedCopy-->
```

Ejemplo:


```
add responder action responder_act respondwith "HTTP.REQ.VERSION + "
    304 Requested Page not allowed in your country - " + CLIENT.IP.SRC.
    LOCATION.GET (1).LOCATION_LONG + "\r\n""
<!--NeedCopy-->
```

Agregar acción de mensaje de registro de auditoría

Puede configurar acciones de mensajes de auditoría para registrar mensajes en varios niveles de registro, ya sea solo en formato syslog o en formato syslog y en `newnslog` formatos. Las acciones de mensajes de auditoría utilizan expresiones para especificar el formato de los mensajes de auditoría. Para crear una acción de mensaje de auditoría mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
add audit messageaction <name> <logLevel> <stringBuilderExpr> [-logtoNewnslog
 (YES|NO)]
```

Ejemplo:

```
add audit messageaction msg1 DEBUG ""Request Location: "+CLIENT.IP.SRC.
    LOCATION"
<!--NeedCopy-->
```

Agregar directiva de Responder

Agregue una directiva de respuesta para identificar las solicitudes procedentes de la India y asociar la acción de respuesta a esta directiva.
En el símbolo del sistema, escriba:

```
add responder policy <name> <rule> <action> [<undefAction>] [-comment <
    string>] [-logAction <string>] [-appflowAction <string>]
<!--NeedCopy-->
```

Ejemplo:

```
add responder policy responder_pol CLIENT.IP.SRC.MATCHES_LOCATION("Asia
    .India.\*.\*.\*.\*") responder_act -logaction msg1
<!--NeedCopy-->
```


Vincular la directiva de respuesta al servidor de equilibrio de carga

Enlazar la directiva de respuesta a un servidor virtual de equilibrio de carga de tipo HTTP/SSL.
En el símbolo del sistema, escriba:

```
bind lb vserver <vserver name> -policyName < policy_name >  -priority
    <> -type <L7InlineREQUEST | L4Inline-REQUEST>
<!--NeedCopy-->
```

Ejemplo:

```
bind lb vserver http_vserver -policyName responder_pol -priority 100 -
    type REQUEST
<!--NeedCopy-->
```

Caso de uso 2: Configuración de la función de geolocalización para insertar un nuevo encabezado HTTP con detalles de ubicación para que el back-end responda

Considere un caso en el que un dispositivo Citrix ADC debe insertar la ubicación del usuario en el encabezado HTTP de una solicitud enviada al servidor de aplicaciones para que el servidor pueda utilizar la información para cierta lógica empresarial.
Los pasos siguientes le ayudarán a completar la configuración de este caso de uso.

- Agregar acción de reescritura
- Agregar directiva de reescritura
- Vincular la directiva de reescritura al equilibrio de carga

Para obtener más información sobre los procedimientos de la GUI para la acción de reescritura y la configuración de la directiva de reescritura, consulte el tema Responder .

Agregar acción de reescritura

Agregue una acción de reescritura para insertar un encabezado HTTP personalizado con detalles de geolocalización del usuario en la solicitud y enviarla a servidores back-end.
En el símbolo del sistema, escriba:

```
add rewrite action <name> <type> <target> [<stringBuilderExpr>] [-
    search <expression>] [-refineSearch <string>][-comment <string>]
<!--NeedCopy-->
```


Ejemplo:

```
add rewrite action rewrite_act insert_http_header "User_location"
   CLIENT.IP.SRC.LOCATION
<!--NeedCopy-->
```

Agregar directiva de reescritura

Agregue una directiva de reescritura para evaluar si se debe ejecutar la acción de reescritura. En este caso, todas las solicitudes que van al servidor de aplicaciones deben tener un encabezado HTTP personalizado, por lo que la regla puede ser "true".
En el símbolo del sistema, escriba:

```
add rewrite policy <name> <rule> <action> [<undefAction>] [-comment <
   string>] [-logAction <string>]
<!--NeedCopy-->
```

Ejemplo:

```
add rewrite policy rewrite_pol true rewrite_act -logaction log_act
<!--NeedCopy-->
```

Vincular la directiva de reescritura al equilibrio de carga

Enlazar la directiva de reescritura al servidor virtual de equilibrio de carga necesario de tipo HTTP/SSL.
En el símbolo del sistema, escriba:

```
bind lb vserver <vserver name> -policyName < policy_name >  -priority
   <> -type <L7InlineREQUEST | L4Inline-REQUEST>
<!--NeedCopy-->
```

Ejemplo:

```
bind lb vserver http_vserver -policyName rewrite_pol -priority 100 -
   type REQUEST
<!--NeedCopy-->
```


Compatibilidad con syslog para registrar detalles de geolocalización (opcional)

Si prefiere registrar los detalles de geolocalización del usuario, debe especificar la acción SYSLOG que se realizará cuando una solicitud coincida con la directiva. El dispositivo almacena los detalles como un mensaje de registro en el archivo ns.log.
Para obtener más información sobre las auditorías SYSLOG y NSLOG, consulte el tema Registro de auditoría .

Salida para detalles de geolocalización del usuario

La siguiente salida se registra en el dispositivo mediante SYSLOG o `newnslog` acción si intenta acceder a una aplicación desde la ubicación de Bangalore y si el dispositivo utiliza la función de geolocalización, “CLIENT.IP.SRC.LOCATION’.

```
Asia.India.Karnataka.Banglore
<!--NeedCopy-->
```

Ejemplo de registro de salida:

```
07/23/2018:19:03:54 GMT  Debug 0-PPE-0 : default REWRITE Message 22 0 :
     ”Request Location: asia.in.karnataka.bangalore.\*.\*”
07/23/2018:19:23:55 GMT  Debug 0-PPE-0 : default RESPONDER Message 32 0
Done
<!--NeedCopy-->
```

Usar la dirección IP de origen del cliente al conectarse al servidor

August 20, 2021

Puede configurar el dispositivo Citrix ADC para que reenvíe paquetes desde el cliente al servidor sin cambiar la dirección IP de origen. Esto resulta útil cuando no se puede insertar la dirección IP del cliente en un encabezado, como cuando se trabaja con servicios que no son HTTP.

Para obtener más información sobre cómo configurar USIP globalmente, consulte Habilitación del modo IP de origen de uso.

Para habilitar el modo USIP para un servicio mediante la CLI

En el símbolo del sistema, escriba:


```
set service <name> -usip (YES | NO)
<!--NeedCopy-->
```

Ejemplo:

```
set service Service-HTTP-1 -usip YES
<!--NeedCopy-->
```

Para habilitar el modo USIP para un servicio mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servicios**y abra un servicio.
2. En Configuración avanzada, en la sección Configuración del servicio, seleccione **Usar dirección IP de origen**.

Utilizar la dirección IP de origen del cliente para la comunicación backend en una configuración de equilibrio de carga v4-v6

August 20, 2021

En una configuración de equilibrio de carga de v4-a v6, para los servicios con USIP inhabilitado, el dispositivo Citrix ADC se comunica con los servidores relacionados desde una de las direcciones SNIP IPv6 (SNIP6) configuradas.

Para los servicios con USIP habilitado, debe establecer el parámetro de prefijo NAT de USIP global para que los servidores relacionados conozcan la dirección IP del cliente de los paquetes de solicitud. El prefijo USIP NAT es un prefijo IPv6 global de longitud 32/40/48/56/64/96 bits configurado en el dispositivo Citrix ADC.

Para un servicio de equilibrio de carga que tiene USIP habilitado, el dispositivo traduce el paquete de solicitud IPv4 a un paquete IPv6 y establece la dirección IP de origen del paquete IPv6 traducido en una concatenación de:

- el prefijo USIP NAT de longitud de 32/40/48/56/64/96 bits.
- ceros acolchados si la longitud del prefijo USIP NAT es inferior a 96 bits. Número de bits acolchados con ceros = 96-USIP NAT longitud del prefijo. Por ejemplo, si la longitud del prefijo USIP NAT es 64, entonces el número de bits acolchados con ceros = 96-64 = 32.

- la dirección de origen IPv4 de [32 bits] que se recibió en el paquete de solicitud. En otras palabras, los últimos 32 bits de la dirección IPv6 de origen se establecen en la dirección IPv4 del cliente.

Al recibir un paquete de respuesta IPv6 del servidor, el dispositivo Citrix ADC traduce el paquete IPv6 a un paquete IPv4 y establece la dirección IP de destino del paquete IPv4 traducido en los últimos 32 bits de la dirección IP de destino del paquete IPv6.

> **Nota**: Esta función no es compatible con la configuración de Citrix Gateway ni con configuraciones de equilibrio de carga de conmutación de contenido y redirección de caché.

Pasos de configuración

La configuración de USIP para una configuración de equilibrio de carga de v4-a v6 consta de las siguientes tareas:

- **Agregue el prefijo NAT USIP global**. Es un prefijo IPv6 global de longitud 32/40/48/56/64/96 bits que se configurará en el dispositivo.
- **Habilite el modo USIP global**. Para obtener más información, consulte Habilitar el modo IP de origen.
- **Habilite el modo USIP para los servicios de equilibrio de carga**. Para obtener más información, consulte Utilizar la dirección IP de origen del cliente al conectarse al servidor.

Para agregar un prefijo NAT USIP global mediante la CLI:

- `set ipv6 -usipnatprefix <prefix/prefix_length>`
- `show ipv6`

Para agregar un prefijo NAT USIP global mediante la GUI:

1. Vaya a **Sistema** > **Red** y haga clic en **Cambiar configuración de IPv6**.
2. En la pantalla **Configurar configuración para IPV6**, establezca el parámetro **USIP NAT Prefijo**.

Configuración de ejemplo

```
> set ipv6 -usipnatprefix 2001:DB8:90::/64
Done

> enable ns mode USIP
Done

> add lb vserver LBVS-1 HTTP 203.0.113.90 80
Done

> add service SVC-1 2001:DB8:5001::30 HTTP 80 -usip yes
```



```
Done

> add service SVC-2 2001:DB8:5001::60 HTTP 80 -usip yes
Done

> bind lb vserver LBVS-1 SVC-1
Done

> bind lb vserver LBVS-1 SVC-2
Done

<!--NeedCopy-->
```

Configurar el puerto de origen para las conexiones del lado del servidor

August 20, 2021

Cuando el dispositivo Citrix ADC se conecta a un servidor físico, puede utilizar el puerto de origen de la solicitud del cliente o puede utilizar un puerto proxy como puerto de origen de la conexión. Puede establecer el parámetro Usar puerto proxy en YES para manejar situaciones como el siguiente caso:

- El dispositivo Citrix ADC está configurado con dos servidores virtuales de equilibrio de carga, LBVS1 y LBVS2.
- Ambos servidores virtuales están enlazados al mismo servicio, S-any.
- El uso de la dirección IP de origen (USIP) del cliente está habilitado en el servicio.
- El cliente C1 envía dos solicitudes, Req1 y Req2, para el mismo servicio.
- LBVS1 recibe Req1 y LBVS2 recibe Req2.
- LBVS1 y LBVS2 reenvían la solicitud a S-ANY y cuando S-ANY envía la respuesta, LBVS1 y LBVS2 reenvían la respuesta al cliente.
- Considere dos casos:
  - Utilice el puerto del cliente. Cuando el dispositivo utiliza el puerto cliente, tanto los servidores virtuales utilizan la dirección IP del cliente (porque USIP está ON) como el puerto del cliente al conectarse al servidor. Por lo tanto, cuando el servicio envía la respuesta, el dispositivo no puede determinar qué servidor virtual debe recibir la respuesta.
  - Utilice el puerto proxy. Cuando el dispositivo utiliza un puerto proxy, los servidores virtuales utilizan la dirección IP del cliente (porque USIP está ON), pero puertos diferentes al conectarse al servidor. Por lo tanto, cuando el servicio envía la respuesta, el número de puerto identifica el servidor virtual que debe recibir la respuesta.

Sin embargo, si necesita una configuración totalmente transparente, como una configuración de redirección de caché totalmente transparente, debe inhabilitar la configuración Usar puerto proxy para

que el dispositivo Citrix ADC pueda utilizar el puerto de origen de la solicitud del cliente.

La opción Usar puerto proxy pasa a ser relevante si está habilitada la opción Usar IP de origen (USIP). Para tipos de servicio basados en TCP, como TCP, HTTP y SSL, la opción está habilitada de forma predeterminada. Para los tipos de servicio basados en UDP, como UDP y DNS, incluido CUALQUIERA, la opción está inhabilitada de forma predeterminada. Para obtener más información sobre la opción USIP, consulte "Habilitación del modo IP de origen de uso. "

Puede configurar la configuración **Usar puerto proxy** de forma global o en un servicio determinado.

Configurar la opción Usar puerto proxy en un servicio

Puede configurar la configuración **Usar ProxyPort** en el servicio si desea anular la configuración global.

Para configurar la opción Usar puerto proxy en un servicio mediante la CLI

En el símbolo del sistema, escriba:

```
set service <name> -useProxyPort (YES | NO)
<!--NeedCopy-->
```

Ejemplo:

```
set service svc1 -useproxyport YES
Done

show service svc1
svc1 (10.102.29.30:80) - HTTP
State: UP
. . .
Use Source IP: YES Use Proxy Port: YES
. . .
Done
<!--NeedCopy-->
```

Para configurar la opción Usar puerto proxy en un servicio mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servicios**y abra un servicio.

2. En Configuración avanzada, seleccione Configuración de tráfico y, a continuación, **Usar puerto proxy**.

Configurar globalmente la configuración del puerto proxy de uso

Puede configurar la configuración **Usar puerto proxy** de forma global si desea aplicar la configuración a todos los servicios del dispositivo Citrix ADC. La configuración **Usar puerto proxy** específica del servicio anula la configuración global.

Para configurar la configuración Usar puerto proxy globalmente mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para configurar la configuración **Usar puerto proxy** globalmente y verificar la configuración:

```
set ns param -useproxyport ( ENABLED | DISABLED )`
show ns param`
<!--NeedCopy-->
```

Ejemplo:

```
set ns param -useproxyport ENABLED

Done

show ns param
Global configuration settings:
. . .
Use Proxy Port: ENABLED
Done
<!--NeedCopy-->
```

Para configurar la configuración Usar puerto proxy globalmente mediante la interfaz gráfica de usuario

Vaya a **Sistema > Configuración > Cambiar la configuración global del sistema** y seleccione o desactive Usar puerto proxy.

Establecer un límite en el número de conexiones de cliente

August 20, 2021

Puede especificar un número máximo de conexiones de cliente que puede controlar cada servidor con equilibrio de carga. A continuación, el dispositivo Citrix ADC abre las conexiones de cliente a un servidor solo hasta que se alcance este límite. Cuando el servidor con equilibrio de carga alcanza su límite, se omiten los sondeos de monitor y el servidor no se utiliza para el equilibrio de carga hasta que haya terminado de procesar las conexiones existentes y libere capacidad.

Para obtener más información sobre la configuración **Máximo cliente**, consulte Servicios basados en nombres de dominio de equilibrio de carga.

Nota: Las conexiones que están en proceso de cierre no se consideran para este límite.

Para establecer un límite en el número de conexiones de cliente mediante la CLI

En el símbolo del sistema, escriba:

```
set service <name> -maxclient <Value>
<!--NeedCopy-->
```

Ejemplo:

```
set service Service-HTTP-1 -maxClient 1000
<!--NeedCopy-->
```

Para establecer un límite al número de conexiones de cliente mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servicios**y abra un servicio.
2. En Configuración avanzada, selecciona **Umbrales y tiempos de espera**y selecciona **Máximo de clientes**.

Establecer un límite en el número de solicitudes por conexión al servidor

August 20, 2021

El dispositivo Citrix ADC se puede configurar para reutilizar las conexiones a fin de mejorar el rendimiento. Sin embargo, en algunos casos, los servidores Web con equilibrio de carga pueden tener problemas cuando las conexiones se reutilizan para demasiadas solicitudes. Para los servicios HTTP o SSL, utilice la opción de solicitud máxima para limitar el número de solicitudes enviadas a través de una única conexión a un servidor web con equilibrio de carga.

Nota: Puede configurar la opción de solicitud máxima solo para servicios HTTP o SSL.

Para limitar el número de solicitudes de cliente por conexión mediante la CLI

En el símbolo del sistema, escriba:

```
set service <ServiceName> -maxReq <Value>
<!--NeedCopy-->
```

Ejemplo:

```
set service Service-HTTP-1 -maxReq 100
<!--NeedCopy-->
```

Para limitar el número de solicitudes de cliente por conexión mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servicios**y abra un servicio.
2. En Configuración avanzada, seleccione **Umbrales y tiempos de espera y**, a continuación, **Solicitudes máximas**.

Establecer un valor de umbral para los monitores enlazados a un servicio

August 20, 2021

El dispositivo Citrix ADC designa un servicio como UP solo cuando la suma de los pesos de todos los monitores enlazados a él y que son UP es igual o mayor que el valor de umbral configurado en el servicio. El peso de un monitor especifica cuánto contribuye a designar el servicio al que está vinculado como UP.

De forma predeterminada, el umbral del monitor se establece en 0 y los pesos del monitor se establecen en 1. Todos los monitores tienen el mismo peso y un servicio puede bajar cuando cualquiera de los monitores baja.

Por ejemplo, suponga que tres monitores, denominados Monitor-HTTP-1, Monitor-HTTP-2 y Monitor-HTTP-3 respectivamente, están enlazados a Service-HTTP-1 y que el umbral configurado en el servicio es tres. Supongamos que se asignan los siguientes pesos a cada monitor:

- El peso de Monitor-HTTP-1 es 1.
- El peso de Monitor-HTTP-2 es 3.
- El peso de Monitor-HTTP-3 es 1.

El servicio se marca como UP solo cuando se cumple una de las siguientes condiciones:

- El monitor HTTP-2 está UP.
- Monitor-HTTP-2 y Monitor-HTTP-1 o Monitor-HTTP-3 están UP
- Los tres monitores están UP.

Para establecer el valor de umbral del monitor en un servicio mediante la CLI

En el símbolo del sistema, escriba:

```
set service <name> -monThreshold <Value>
<!--NeedCopy-->
```

Ejemplo:

```
set service Service-HTTP-1 -monThreshold 100
<!--NeedCopy-->
```

Para establecer el valor del umbral del monitor en un servicio mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servicios**y abra un servicio.
2. En Configuración avanzada, selecciona **Umbrales y tiempos de espera**y selecciona **Supervisar umbral**.

Establecer un valor de tiempo de espera para las conexiones de cliente inactivas

August 20, 2021

Puede configurar el servicio con un valor de tiempo de espera para finalizar cualquier conexión de cliente inactiva cuando transcurra el tiempo configurado. Si el cliente está inactivo durante el tiempo configurado, el dispositivo Citrix ADC cierra la conexión del cliente.

Para establecer un valor de tiempo de espera para las conexiones de cliente inactivas mediante la CLI

En el símbolo del sistema, escriba:

```
set service <name> -cltTimeout <Value>
<!--NeedCopy-->
```

Ejemplo:

```
set service Service-HTTP-1 -cltTimeout 100
<!--NeedCopy-->
```

Para establecer un valor de tiempo de espera para las conexiones de cliente inactivas mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servicios**y abra un servicio.
2. En Configuración avanzada, seleccione **Umbrales y tiempos de espera y**, a continuación, Tiempo de **espera de inactividad del cliente**.

Establecer un valor de tiempo de espera para las conexiones de servidor inactivas

August 20, 2021

Puede configurar un servicio con un valor de tiempo de espera para finalizar las conexiones de servidor inactivas cuando transcurra el tiempo configurado (en segundos). Si el servidor está inactivo durante el tiempo configurado, el dispositivo Citrix ADC cierra la conexión al servidor.

Para establecer un valor de tiempo de espera para las conexiones de servidor inactivas mediante la CLI

En el símbolo del sistema, escriba:


```
set service <name> -svrTimeout <Value>
<!--NeedCopy-->
```

Ejemplo:

```
set service Service-HTTP-1 -svrTimeout 100
<!--NeedCopy-->
```

Para establecer un valor de tiempo de espera para las conexiones de servidor inactivas mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servicios**y abra un servicio.
2. En Configuración avanzada, seleccione **Umbrales y tiempos de espera y**, a continuación, Tiempo de **espera de inactividad del servidor**.

Establecer un límite en el uso del ancho de banda por parte de los clientes

August 20, 2021

En ocasiones, los servidores pueden tener un ancho de banda limitado para gestionar las solicitudes de los clientes y sobrecargarse. Para evitar la sobrecarga de un servidor, puede especificar un límite máximo en el ancho de banda, en Kbps, procesado por el servidor. El dispositivo Citrix ADC reenvía las solicitudes a un servidor con equilibrio de carga solo hasta que se alcance este límite.

Para establecer un límite máximo de ancho de banda en un servicio mediante la CLI

En el símbolo del sistema, escriba:

```
set service <name> -maxBandwidth <Value>
<!--NeedCopy-->
```

Ejemplo:


```
set service Service-HTTP-1 -maxBandwidth 100
<!--NeedCopy-->
```

Para establecer un límite máximo de ancho de banda en un servicio mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servicios**y abra un servicio.
2. En Configuración avanzada, seleccione **Umbrales y tiempos de espera y**, a continuación, Ancho de **banda máximo**.

Redirigir las solicitudes de cliente a una caché

August 20, 2021

Puede configurar un servicio para redirigir las solicitudes de cliente a una caché y reenviar las solicitudes que no se pueden almacenar en caché a un servicio elegido por el método de equilibrio de carga configurado.

Para establecer la redirección de caché en un servicio mediante la CLI

En el símbolo del sistema, escriba:

```
set service <name> -cacheable <Value>
<!--NeedCopy-->
```

Ejemplo:

```
set service Service-HTTP-1 -cacheable YES
<!--NeedCopy-->
```

Para establecer la redirección de caché en un servicio mediante la interfaz gráfica de usuario

1. Vaya a **Administración de Tráfico > Equilibrio de carga > Servicios**.
2. Abra un servicio y establezca el tipo de caché.

Conservar el identificador de VLAN para la transparencia de VLAN

August 20, 2021

Puede configurar un servidor virtual de equilibrio de carga para conservar el identificador de VLAN del cliente en paquetes que se van a reenviar a los servidores. El servidor virtual debe ser un servidor virtual comodín de tipo ANY y debe estar funcionando en modo MAC.

Para configurar un servidor virtual de equilibrio de carga para retener el ID de VLAN del cliente mediante la CLI

En el símbolo del sistema, escriba el siguiente comando para configurar un servidor virtual de equilibrio de carga para conservar el ID de VLAN del cliente y verificar la configuración:

```
set lb vserver <name> -m MAC -macmodeRetainvlan ENABLED

show lb vserver <name>
<!--NeedCopy-->
```

> **Nota**
>
> En el caso de un servicio vinculado a un servidor virtual en el que está habilitada la `-m MAC` opción, debe vincular un monitor que no es usuario.

Para configurar un servidor virtual de equilibrio de carga para conservar el ID de VLAN del cliente mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**y abra un servidor virtual.
2. En Configuración avanzada, seleccione **Configuración de tráfico**y, a continuación, **Retener ID de VLAN**.

Configurar la transición de estado automática en función del porcentaje de estado de los servicios enlazados

August 20, 2021

Puede configurar un servidor virtual de equilibrio de carga para que pase automáticamente del estado ACTIVO al estado ABAJO si el porcentaje de servicios activos cae por debajo de un umbral configurado.

Por ejemplo, si vincula 10 servicios a un servidor virtual de equilibrio de carga y configura un umbral del 50% para ese servidor virtual, pasa de arriba a abajo si seis o más servicios están abajo. Cuando el porcentaje de mantenimiento se eleva por encima del valor umbral, el servidor virtual vuelve al estado ACTIVO.

También puede habilitar una alarma SNMP denominada ENTITY-STATE si quiere que el dispositivo Citrix ADC le notifique cuándo el porcentaje de mantenimiento de servicios enlazados hace que un servidor virtual cambie de estado.

Para configurar la transición automática de estado basada en porcentajes mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para configurar una transición de estado automática para un servidor virtual y verificar la configuración:

```
set lb vserver <name> -healthThreshold <positive_integer>

show lb vserver <name>
<!--NeedCopy-->
```

Para configurar la transición automática de estado basada en porcentajes mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**y abra un servidor virtual.
2. En Configuración avanzada, selecciona **Configuración de tráfico**y establece un **umbral de mantenimiento**.

Para habilitar la alarma ENTITY-STATE mediante la CLI

En el símbolo del sistema, escriba los comandos siguientes para habilitar la alarma ENTITY-STATE SNMP y compruebe la configuración:

```
enable snmp alarm ENTITY-STATE

show snmp alarm
<!--NeedCopy-->
```


Para habilitar la alarma ENTITY-STATE mediante la interfaz gráfica de usuario

1. Vaya a **Sistema > SNMP > Alarmas**.
2. Seleccione **ENTITY-STATE** y, en la lista Acción, seleccione **Habilitar**.

Monitores integrados

August 20, 2021

El dispositivo Citrix ADC contiene varios monitores integrados que puede utilizar para supervisar sus servicios. Estos monitores integrados manejan la mayoría de los protocolos comunes. Proporcionan opciones para modificar algunos parámetros, como el intervalo, el tiempo de espera de respuesta para satisfacer sus requisitos. Sin embargo, no se puede modificar el nombre y el protocolo del monitor. Para obtener más información, consulte Modificación de monitores. También puede vincular un monitor integrado a un servicio y desvincularlo del servicio.

> **Nota**
>
> Puede crear un monitor personalizado basado en un monitor integrado. Para obtener información sobre cómo crear monitores personalizados, consulte Configuración de monitores en una configuración de equilibrio de carga.

Supervisión de aplicaciones basada en TCP

September 8, 2021

El dispositivo Citrix ADC tiene dos monitores integrados que supervisan las aplicaciones basadas en TCP: `tcp-default` y `ping-default`. Cuando crea un servicio, el monitor predeterminado apropiado se vincula automáticamente a él, de modo que el servicio se puede utilizar inmediatamente si está UP. El monitor tcp-default está enlazado a todos los servicios TCP. El monitor ping-default está enlazado a todos los servicios que no son TCP.

No se pueden eliminar ni modificar los monitores predeterminados. Cuando enlaza cualquier otro monitor a un servicio TCP, el monitor predeterminado no está vinculado del servicio. En la siguiente tabla se enumeran los tipos de monitor y los parámetros y procesos de supervisión asociados a cada tipo.

Tipo de monitor	Parámetros específicos	Process
tcp	No corresponde	El dispositivo Citrix ADC establece un apretón de manos de 3 vías con el destino del monitor y, a continuación, cierra la conexión. Si el dispositivo observa el tráfico TCP hacia el destino, no envía solicitudes de supervisión TCP. Esto ocurre si la LRTM está deshabilitada. De forma predeterminada, LRTM está deshabilitado en este monitor.
http	httprequest [«HEAD/»] - Solicitud HTTP que se envía al servicio. respcode [200] - Se espera un conjunto de códigos de respuesta HTTP del servicio.	El dispositivo Citrix ADC establece un protocolo de enlace de tres vías con el destino del monitor. Una vez establecida la conexión, el dispositivo envía solicitudes HTTP y, a continuación, compara el código de respuesta con el conjunto de códigos de respuesta configurado.

Tipo de monitor	Parámetros específicos	Process
tcp-ecv	send [””] - son los datos que se envían al servicio. La longitud máxima permitida de la cadena es de 512 bytes. recv [””] - respuesta esperada del servicio. La longitud máxima permitida de la cadena es de 128 bytes. El último carácter es la terminación NULL.	El dispositivo Citrix ADC establece un protocolo de enlace de tres vías con el destino del monitor. Cuando se establece la conexión, el dispositivo utiliza el parámetro send para enviar datos específicos al servicio y espera una respuesta específica a través del parámetro de recepción. Los distintos servidores envían segmentos de diferentes tamaños. Sin embargo, el patrón debe estar dentro de 16 segmentos TCP.
http-ecv	send [””]: Datos HTTP que se envían al servicio; recv [””]: Los datos de respuesta HTTP esperados del servicio	El dispositivo Citrix ADC establece un protocolo de enlace de tres vías con el destino del monitor. Cuando se establece la conexión, el dispositivo utiliza el parámetro send para enviar los datos HTTP al servicio y espera la respuesta HTTP especificada por el parámetro de recepción. (parte del cuerpo HTTP sin incluir encabezados HTTP). Los datos de respuesta vacíos coinciden con cualquier respuesta. Los datos esperados podrían estar en cualquier parte de los primeros 24 K bytes del cuerpo HTTP de la respuesta.

Tipo de monitor	Parámetros específicos	Process
ping	No corresponde	El dispositivo Citrix ADC envía una solicitud de eco ICMP al destino del monitor y espera una respuesta de eco ICMP.

Para configurar monitores integrados para aplicaciones basadas en TCP, consulte Configuración de monitores en una configuración de equilibrio de carga.

Para configurar monitores basados en TCP mediante CLI

Escriba el siguiente comando:

```
add lb monitor <monitorName> <type> -respCode <int[-int]> -httpRequest
    <string> -resptimeout <integer> [<units>] -retries <integer> -
    downTime <integer> [<units>] -action <action>
<!--NeedCopy-->
```

Ejemplo de tipo de monitor TCP:

```
add lb monitor Exch2010-RPC-AddressBook TCP -LRTM ENABLED -interval 10
    -resptimeout 5 -destPort 59601
<!--NeedCopy-->
```

Ejemplo de tipo de monitor HTTP:

```
add lb monitor Mon_S4B_FE_2 HTTP -respCode 200 -httpRequest "GET /
    Autodiscover/XFrame/XFrame.html" -LRTM ENABLED -retries 10 -secure
    YES
<!--NeedCopy-->
```

Ejemplo de tipo de monitor HTTP-ECV:

```
add lb monitor STM_EXC2016_SSLBridge_MON HTTP-ECV -send "GET /owa/
    healthcheck.htm" -recv "200 OK" -LRTM ENABLED -destPort 443 -secure
    YES
```



```
2 <!--NeedCopy-->
```

Ejemplo de tipo de monitor PING:

```
1 add lb monitor lbmon-localhost-ping PING -LRTM DISABLED -destIP
     127.0.0.1
2 <!--NeedCopy-->
```

Supervisión de servicios SSL

August 20, 2021

El dispositivo Citrix ADC tiene monitores seguros integrados, TCPS y HTTPS. Puede utilizar los monitores seguros para supervisar el tráfico HTTP y no HTTP. Para configurar un monitor HTTP seguro, seleccione el tipo de monitor como HTTP y, a continuación, establezca el indicador seguro. Para configurar un monitor TCP seguro, seleccione el tipo de monitor como TCP y, a continuación, establezca el indicador seguro. Los monitores seguros funcionan de la siguiente manera:

- **Supervisión TCP segura.** El dispositivo Citrix ADC establece una conexión TCP. Una vez establecida la conexión, el dispositivo realiza un protocolo de enlace SSL con el servidor. Una vez finalizado el apretón de manos, el dispositivo cierra la conexión.
- **Supervisión HTTP segura.** El dispositivo Citrix ADC establece una conexión TCP. Una vez establecida la conexión, el dispositivo realiza un protocolo de enlace SSL con el servidor. Cuando se establece la conexión SSL, el dispositivo envía solicitudes HTTP a través del canal cifrado y comprueba los códigos de respuesta.

En la siguiente tabla se describen los monitores integrados disponibles para supervisar los servicios SSL.

Tipo de monitor	Sonda	Criterios de éxito (condición directa)
TCP	conexión TCP; protocolo de enlace SSL	Conexión TCP correcta establecida y protocolo de enlace SSL correcto.

Tipo de monitor	Sonda	Criterios de éxito (condición directa)
HTTP	Conexión TCP; protocolo de enlace SSL; solicitud HTTP cifrada	Se establece una conexión TCP correcta, se realiza un protocolo de enlace SSL correcto y se cifra el código de respuesta HTTP esperado en la respuesta HTTP del servidor.
TCP-ECV	Conexión TCP. apretón de manos SSL (los datos enviados a un servidor están cifrados).	Se establece una conexión TCP correcta, se realiza un protocolo de enlace SSL correcto y se reciben los datos TCP esperados del servidor.
HTTP-ECV	Conexión TCP; protocolo de enlace SSL (solicitud HTTP cifrada)	Se establece una conexión TCP correcta, se realiza un protocolo de enlace SSL correcto y se reciben los datos HTTP esperados del servidor.

Configuración de ejemplo para el monitor de comprobación de estado HTTS-ECV

Los servicios HTTP tienen monitores predefinidos capaces de Verificación de contenido extendido (ECV).
Estos monitores se utilizan cuando se requiere una validación más allá de una conexión TCP correcta. Estos monitores validan el servicio como UP, cuando se cumplen todos los criterios siguientes:

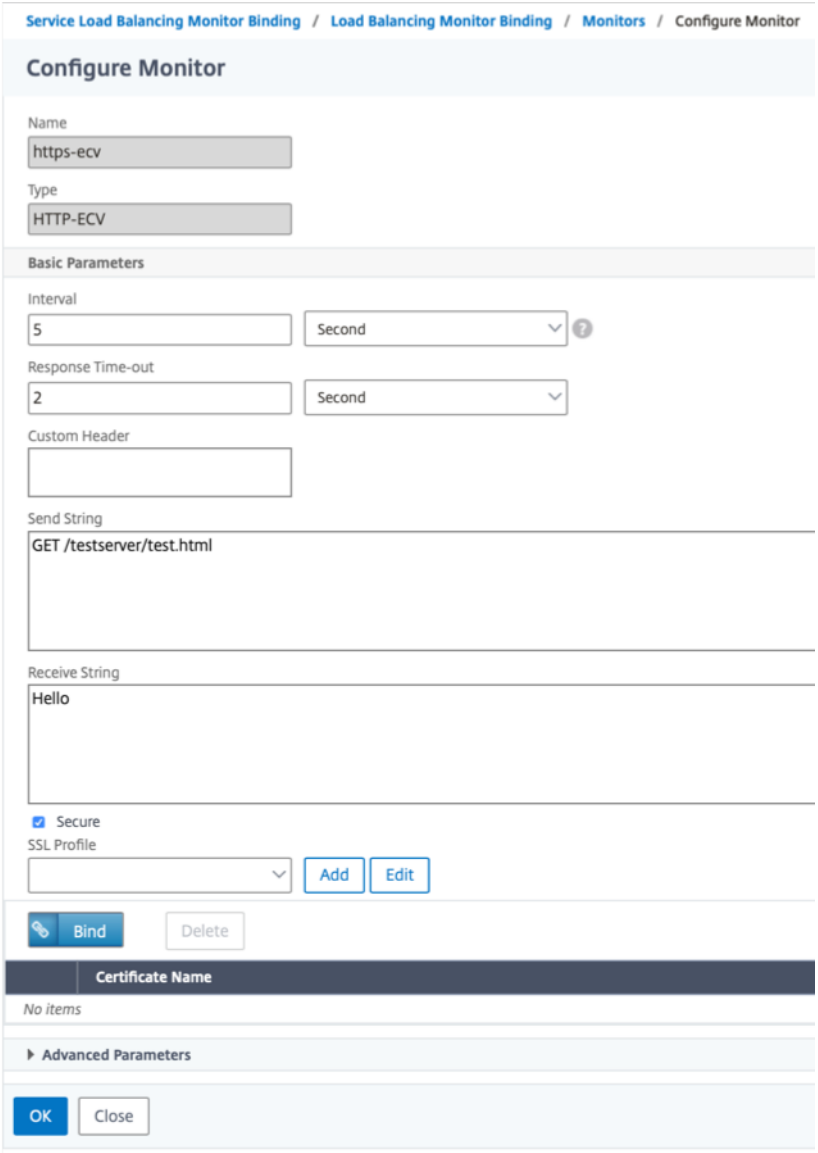
- Una conexión TCP correcta.
- Se debe generar un tipo particular de solicitud.
- Se espera un mensaje específico en respuesta de la **cadena de recepción**.

Para estos monitores, se configura una cadena de solicitud junto con una cadena de respuesta. Si la cadena de respuesta recibida por el monitor Citrix ADC coincide con la cadena configurada, el servicio se marca como UP.

Enlazar un monitor a un servicio mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servicios**, cree un servicio y especifique el protocolo como **SSL**. Haga clic en **Aceptar**.

2. Haga clic en el panel **Enlace de supervisión de equilibrio de servicio** y haga clic en **Agregar enlace**.
3. Elija el tipo de monitor como **HTTPS-ECV** y haga clic en **Modificar**.
4. En el panel **Configurar monitor** en la ficha **Parámetros básicos**, escriba valores para los siguientes parámetros:
   - **Cadena de envío**: Cadena que el monitor debe enviar al servicio.
   - Cadena de**recepción: Cadena** que el monitor debe recibir para marcar el servicio como UP.



5. Haga clic en **Aceptar** para completar la configuración del monitor.
6. Haga clic en **Select**.
7. Haga clic en Vincular para **vincular** el monitor **HTTS-ECV** al servicio.

8. Haga clic en **Cerrar**.

Enlazar un monitor a un servicio mediante la CLI

En el símbolo del sistema, escriba:

```
bind service <servicename> -monitorName https-ecv
<!--NeedCopy-->
```

Ejemplo:

```
bind services1 -monitorName https-ecv
<!--NeedCopy-->
```

Monitorización de servicios HTTP/2

August 20, 2021

El dispositivo Citrix ADC admite monitores HTTP/2 para supervisar el estado de mantenimiento de los servicios HTTP/2.

El monitor HTTP/2 se puede configurar de dos formas diferentes. Según el tipo de tráfico, puede configurar un monitor HTTP/2.

- **HTTP/2 Directo.** Puede configurar HTTP/2 Direct para supervisar los servicios HTTP/2 no seguros.
- **<HTTP://2> SSL.** Puede configurar HTTP/2 SSL para supervisar el tráfico seguro a través de SSL. Habilite el parámetro de marca segura en HTTP/2 para supervisar el tráfico SSL.

http2direct y http2ssl son los dos monitores integrados diferentes compatibles con el protocolo HTTP/2.

En la tabla siguiente se enumeran los tipos de configuración y los procesos de supervisión asociados a cada tipo.

Tipo de configuración	Sonda	Criterios éxito
HTTP/2 Directo	Conexión TCP; Prefacio de conexión HTTP2 y negociación de configuración; Solicitud HTTP2	El código de estado de respuesta HTTP/2 debe coincidir con el código de respuesta configurado.
<HTTP://2> SSL	Conexión TCP; apretón de manos SSL; Prefacio de conexión HTTP2 y negociación de configuración; Solicitud HTTP2	El servidor debe seleccionar siempre `ALPN` con el protocolo HTTP/2 y el código de estado de respuesta HTTP/2 debe coincidir con el código de respuesta configurado.

Vincular el monitor HTTP/2 a un servicio mediante la CLI

En el símbolo del sistema, escriba:

- `bind service <servicename> -monitorName <name>`
- `bind service <servicename> -monitorName <name>`

Ejemplo:

- `bind service s1 -monitorName http2direct`
- `bind service s2 -monitorName http2ssl`

Supervisión del servicio de protocolo proxy

August 20, 2021

El dispositivo Citrix ADC con protocolo proxy admite la comprobación de monitores. La comprobación del monitor garantiza que el servidor back-end también admita el protocolo proxy. El dispositivo Citrix ADC tiene cuatro tipos de monitores integrados para servicios relacionados con HTTP o TCP: HTTP, HTTPS, HTTP-ECV y TCP-ECV.

En la siguiente tabla se enumeran los tipos de monitor y los parámetros y procesos de supervisión asociados a cada tipo.

Tipo de configuración	Sonda	Criterios éxito
HTTP	`httprequest` [“HEAD/”]: Solicitud HTTP que se envía al servicio. `respcode` [200]: Se espera un conjunto de códigos de respuesta HTTP del servicio.	El dispositivo Citrix ADC establece un protocolo de enlace de tres vías con el destino del monitor. Una vez establecida la conexión, el dispositivo envía solicitudes HTTP y, a continuación, compara el código de respuesta con el conjunto de códigos de respuesta configurado.
HTTPS	`httprequest` [“HEAD/”] - Solicitud HTTPS que se envía al servicio. `respcode` [200] - Se espera un conjunto de códigos de respuesta HTTPS del servicio.	El dispositivo Citrix ADC establece un protocolo de enlace de tres vías con el destino del monitor. Una vez establecida la conexión, el dispositivo envía solicitudes HTTPS y, a continuación, compara el código de respuesta con el conjunto de códigos de respuesta configurado.

Tipo de configuración	Sonda	Criterios éxito
HTTP-ECV	send [””]: Datos HTTP que se envían al servicio. Received [””]: Los datos de respuesta HTTP esperados del servicio	El dispositivo Citrix ADC establece un protocolo de enlace de tres vías con el destino del monitor. Cuando se establece la conexión, el dispositivo utiliza el parámetro send para enviar los datos HTTP al servicio y espera la respuesta HTTP que especifica el parámetro receive. (parte del cuerpo HTTP sin incluir encabezados HTTP). Los datos de respuesta vacíos coinciden con cualquier respuesta. Los datos esperados podrían estar en cualquier parte de los primeros 24 K bytes del cuerpo HTTP de la respuesta.
TCP-ECV	send [””]: Son los datos que se envían al servicio. La longitud máxima permitida de la cadena es de 512 K bytes. recibida [””] - la respuesta esperada del servicio. La longitud máxima permitida de la cadena es de 128 K bytes.	El dispositivo Citrix ADC establece un protocolo de enlace de tres vías con el destino del monitor. Cuando se establece la conexión, el dispositivo utiliza el parámetro send para enviar datos específicos al servicio y espera una respuesta específica a través del parámetro receive. Los diferentes servidores envían diferentes tamaños de segmentos. Sin embargo, el patrón debe estar dentro de 16 segmentos TCP.

Puede configurar el monitor de protocolo proxy mediante `netprofile`.

Configurar el monitor de protocolo proxy mediante la CLI

En el símbolo del sistema, escriba:

1. Agregar perfil de red con el protocolo proxy habilitado

   ```
   add netprofile <name> -proxyProtocol ( ENABLED | DISABLED )
   ```

Ejemplo:

```
1 add netprofile profile1 - proxyProtocol ENABLED
```

1. Vincular el perfil de red a un servicio.

   ```
   set service <name> -netprofile <netprofile-name>
   ```

Ejemplo:

```
1 set service S1 - netprofile profile1
```

> **Nota**
>
> Puede ejecutar el comando anterior si desea que el perfil de red se vincula a un servicio.

1. Enlazar el perfil de red a un monitor.

   ```
   set lb monitor <monitor-name> <type> -netprofile <netprofile-name>
   ```

Ejemplo:

```
1 set lb monitor http1 HTTPS - netprofile profile1
```

> **Nota**
>
> - Puede ejecutar el comando anterior si desea que el perfil de red se enlace a un monitor.
> - Puede seleccionar el tipo de monitor de su elección. Puede ser HTTP, HTTPS, TCP-ECV o HTTP-ECV.
>
> **Importante**
>
> - En un caso general, se considera el perfil de red (protocolo proxy habilitado) vinculado a un servicio.
> - Si el perfil de red está vinculado tanto al monitor como al servicio, se considera el perfil de red vinculado al monitor. Se ignora el perfil de red vinculado al servicio.

Supervisión del servicio FTP

August 20, 2021

Para supervisar los servicios FTP, el dispositivo Citrix ADC abre dos conexiones al servidor FTP. Primero se conecta al puerto de control, que se utiliza para transferir comandos entre un cliente y un servidor FTP. Después de recibir la respuesta esperada, se conecta al puerto de datos, que se utiliza para transferir archivos entre un cliente y un servidor FTP. Solo cuando el servidor FTP responde como se esperaba, en ambas conexiones, se marca como UP.

Nota: Los sondeos del monitor se originan a partir de la dirección NSIP.

El dispositivo Citrix ADC tiene dos monitores integrados para los servicios FTP: El monitor FTP y el monitor FTP-EXTENDED. El monitor FTP-EXTENDED es un monitor con scripts. Utiliza el script nsftp.pl. El script de monitor FTP-EXTENDED se ha mejorado para enviar sondeos seguros a servicios FTP. Puede crear un monitor de tipo FTP-EXTENDED. El script nsftp.pl se toma automáticamente del directorio predeterminado.

Para enviar sondeos FTP seguros a servicios FTP mediante la CLI

En el símbolo del sistema, escriba:

```
1 add lb monitor <monitorName> <type> -username <string> -password <
     string> -filename <filename>
2 <!--NeedCopy-->
```

Ejemplo

```
1 add monitor mon1 FTP-EXTENDED -username root -password freebsd -
     filename fsdf
2 <!--NeedCopy-->
```

Para enviar sondeos FTP seguros a servicios FTP mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Monitores**.
2. Especifique el tipo de monitor como **FTP-EXTENDED** y defina los parámetros.
3. En **Parámetros especiales**, especifique un **nombre de archivo**, **nombre de usuario** y **contraseña**.

Para configurar monitores integrados para comprobar el estado de los servicios FTP, consulte Configuración de monitores en una configuración de equilibrio de carga.

Supervisión segura de servidores mediante SFTP

January 12, 2021

Se agrega un script de usuario 'nssftp.pl' para admitir la supervisión del protocolo de transferencia de archivos SSH (SFTP). Está disponible en la lista actual de monitores de usuario de Citrix ADC incorporados y se encuentra en el directorio /netscaler/monitors. El monitor SFTP utiliza el nombre de usuario y la contraseña especificados para comprobar si el archivo está presente en el servidor.

Para configurar la supervisión segura mediante SFTP mediante la CLI

En el símbolo del sistema, escriba:

```
1 add lb monitor <monitorName> <type> -scriptName <string> -scriptArgs <
     string> -secure ( YES | NO )
2 <!--NeedCopy-->
```

Ejemplo:

```
1 add monitor SFTP_MON USER -scriptname nssftp.pl -scriptargs "file=
     example.txt;user=sam;password=sam_passwd"
2 <!--NeedCopy-->
```

Para configurar la supervisión segura mediante SFTP mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Monitores** y en **Tipo** especifique **USUARIO**.
2. En **Parámetros especiales**, en **Nombre del script**, seleccione nssftp.pl.
3. Especifique los **argumentos del script**.

Establecer parámetros SSL en un monitor seguro

August 20, 2021

> **Importante**
>
> Esta función solo se admite en los nuevos perfiles predeterminados. Para obtener más información sobre estos perfiles, consulte Descripción general de la infraestructura de perfiles SSL mejorados.

Un monitor hereda la configuración global o la configuración del servicio al que está vinculado. Si un monitor está enlazado a un servicio que no sea SSL o no SSL_TCP, como SSL_BRIDGE, no puede configurarlo con valores SSL como la versión del protocolo o los cifrados que se van a utilizar. Por lo tanto, si la implementación requiere supervisión basada en SSL de los servidores back-end, la supervisión no es efectiva.

Puede tener más control sobre la supervisión basada en SSL de los servidores back-end, vinculando un perfil SSL a un monitor. Un perfil SSL contiene parámetros SSL, enlaces de cifrado y enlaces ECC. Por ejemplo, puede establecer la autenticación del servidor, los cifrados y la versión del protocolo en un perfil SSL y enlazar el perfil a un monitor. Para realizar la autenticación del servidor, también debe vincular un certificado de CA a un monitor. Para realizar la autenticación de cliente, debe vincular un certificado de cliente al monitor. Los nuevos parámetros para el comando “bind lb monitor” le permiten hacerlo.

> **Nota**
>
> La configuración de SSL solo surtirá efecto si agrega un monitor seguro. Además, el tipo de perfil SSL debe ser **BackEnd**.

Tipos de supervisión que admiten perfiles SSL

Los perfiles SSL se pueden enlazar a los siguientes tipos de monitor:

- HTTP
- HTTP-ECV
- TCP
- TCP-ECV
- HTTP-INLINE

Para especificar un perfil SSL al agregar un monitor mediante la línea de comandos

En el símbolo del sistema, escriba:


```
add lb monitor <monitorName> <type> -secure  YES   -sslprofile <string>

set lb monitor <monitorName> <type> -secure YES -sslprofile <string>
<!--NeedCopy-->
```

Ejemplo:

```
add ssl profile prof1 -sslProfileType  BackEnd

add lb monitor mon1 HTTP -secure  YES -sslprofile prof1
<!--NeedCopy-->
```

Para enlazar un par de claves de certificado a un monitor mediante la línea de comandos

En el símbolo del sistema, escriba:

```
bind monitor  <monitor name> -certkeyName <string>  [(-CA  [-crlCheck (
    Mandatory | Optional ) | -ocspCheck ( Mandatory | Optional )]
<!--NeedCopy-->
```

Supervisión de servicios SIP

August 20, 2021

Un Citrix ADC tiene dos monitores integrados que se pueden utilizar para supervisar los servicios SIP: Los monitores **SIP-UDP** y **SIP-TCP**. Un monitor SIP comprueba periódicamente el servicio SIP al que está vinculado el monitor SIP, enviando métodos de solicitud SIP al servicio SIP. Si el servicio SIP responde con un código de respuesta, el monitor marca el servicio como UP. Si el servicio SIP no responde o responde incorrectamente, se marca como DOWN.

Parámetro	Especifica
Sipuri	Esquema de direccionamiento SIP del servidor SIP.

Parámetro	Especifica
`sipmethod`	Tipo de solicitud SIP utilizada para sondear el servicio SIP. Especifique uno de los métodos siguientes: INVITE, OPTION (valor predeterminado), REGISTER
`respcode`	Código de respuesta SIP con el que el servicio SIP responde la solicitud de sondeo. Valor predeterminado: 200.

Supervisión de servicios RADIUS

August 20, 2021

El monitor RADIUS del dispositivo Citrix ADC comprueba periódicamente el estado del servicio RADIUS al que está vinculado enviando una solicitud de autenticación al servicio. El servidor RADIUS autentica el monitor RADIUS y envía una respuesta. De forma predeterminada, el monitor espera recibir un código de respuesta de 2, la respuesta de aceptación de acceso predeterminada, del servidor RADIUS. Siempre que el monitor reciba la respuesta adecuada, marca el servicio UP.

Nota: El monitor RADIUS solo admite autenticación de tipo PAP.

- Si el cliente se autenticó correctamente, el servidor RADIUS envía una respuesta de aceptación de acceso. El código de respuesta predeterminado de aceptación de acceso es 2 y éste es el código que utiliza el dispositivo.
- Si el cliente no puede autenticarse correctamente (por ejemplo, cuando hay una discrepancia en el nombre de usuario, la contraseña o la clave secreta), el servidor RADIUS envía una respuesta de Rechazo de acceso. El código de respuesta de rechazo de acceso predeterminado es 3 y éste es el código que utiliza el dispositivo.

Parámetro	Especifica
`userName`	Nombre de usuario en el servidor RADIUS/NNTP/FTP/FTP-EXTENDED/MYSQL/POP3. Este nombre de usuario se utiliza en el sondeo.
contraseña	Contraseña utilizada en la supervisión de servidores RADIUS/NNTP/FTP/FTP-EXTENDED/MYSQL/POP3/LDAP.

Parámetro	Especifica
Radkey	Valor de clave secreta compartida que utiliza el servidor RADIUS durante la autenticación del cliente.
RadNasid	NAS-ID que está encapsulado en la carga útil cuando se realiza una solicitud de acceso.
RadNasip	La dirección IP encapsulada en la carga útil cuando se realiza una solicitud de acceso. Cuando RadNasip no está configurado, el dispositivo Citrix ADC envía la dirección IP asignada (MIP) al servidor RADIUS como dirección IP del NAS.

Para supervisar un servicio RADIUS, debe configurar el servidor RADIUS al que está enlazado de la siguiente manera:

1. Agregue el nombre de usuario y la contraseña del cliente que utiliza el monitor para la autenticación a la base de datos de autenticación RADIUS.
2. Agregue la dirección IP y la clave secreta del cliente a la base de datos RADIUS apropiada.
3. Agregue las direcciones IP que utiliza el dispositivo para enviar paquetes RADIUS a la base de datos RADIUS. Si el dispositivo Citrix ADC tiene más de una dirección IP asignada o si se utiliza una dirección IP de subred (SNIP), debe agregar la misma clave secreta para todas las direcciones IP.

   Precaución: Si la dirección IP utilizada por el dispositivo no se agrega a la base de datos RADIUS, el servidor RADIUS descarta todos los paquetes.

Para configurar monitores integrados para comprobar el estado del servidor RADIUS, consulte Configuración de monitores en una configuración de equilibrio de carga.

Supervisar la entrega de información contable desde un servidor RADIUS

August 20, 2021

Puede configurar un monitor denominado monitor *contable RADIUS* para determinar si el servidor RADIUS utilizado para la autenticación, autorización y contabilidad (Citrix ADC AAA) proporciona información contable según lo esperado. El monitor es de tipo RADIUS_ACTAKING. El sondeo se genera

mediante un script Perl llamado nsbmradius.pl, que se encuentra en el directorio /nsconfig/monitors/. El script envía sondeos sucesivos de solicitudes de contabilidad al servidor RADIUS. El sondeo se considera correcto solo si el servidor de cuentas RADIUS responde con un paquete cuyo campo Código está establecido en 5, que, de acuerdo con RFC 2866, indica un paquete Accounting-Response.

Al configurar un monitor de cuentas RADIUS, debe especificar una clave secreta. Puede especificar parámetros opcionales, cada uno de los cuales representa un atributo RADIUS, como Acct-Status-Type y Framed-IP-Address. Para obtener información acerca de estos atributos, consulte RFC 2865, "Remote Authentication Dial In User Service (RADIUS)" y RFC 2866, "RADIUS Accounting."

Para configurar un monitor de cuentas RADIUS mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para configurar un monitor de cuentas RADIUS y compruebe la configuración:

```
add lb monitor <monitorName> RADIUS_ACCOUNTING [-userName <string>] {
 -password  }
  {
 -radKey  }
  [-radNASip <ip_addr>] [-radAccountType <positive_integer>] [-
     radFramedIP <ip_addr>] [-radAPN <string>] [-radMSISDN <string>] [-
     radAccountSession <string>]

show lb monitor <monitorName>
<!--NeedCopy-->
```

Ejemplo

```
add lb monitor radAccntMon RADIUS_ACCOUNTING -radKey "8d#>9jr4rV)L7%a2-
   zW13sM"
<!--NeedCopy-->
```

Supervisión de servicios DNS y DNS-TCP

August 20, 2021

El dispositivo Citrix ADC tiene dos monitores integrados que se pueden utilizar para supervisar servicios DNS: DNS y DNS-TCP. Cuando está enlazado a un servicio, el monitor comprueba periódicamente

el estado de ese servicio DNS enviándole una consulta DNS. La consulta se resuelve en una dirección IPv4 o IPv6. Esa dirección IP se compara con la lista de direcciones IP de prueba que configura. La lista puede contener hasta cinco direcciones IP. Si la dirección IP resuelta coincide con al menos una dirección IP de la lista, el servicio DNS se marca como activo. Si la IP resuelta no coincide con ninguna dirección IP de la lista, el servicio DNS se marca como caído.

Parámetro	Descripción
consulta	Consulta DNS (nombre de dominio) enviada al servicio DNS que se está supervisando. Valor predeterminado: "\ 007" Si la consulta DNS se ejecuta correctamente, el servicio se marca como UP. De lo contrario, se marca como ABAJO. Para un monitor inverso, si la consulta DNS se realiza correctamente, el servicio se marca como INCORRECTO. De lo contrario, se marca como UP. Si no se recibe respuesta, el servicio se marca como DOWN.
Tipo de consulta	El tipo de consulta DNS que se envía. Valores posibles: Dirección, Zona.
`IPAddress`	Lista de direcciones IP que se comprueban con la respuesta al sondeo de supervisión DNS.
IPv6	Active esta casilla de verificación si la dirección IP utiliza el formato IPv6.

Para configurar los monitores DNS o DNS-TCP integrados, consulte Configuración de monitores en una configuración de equilibrio de carga.

Supervisión de servicios LDAP

August 20, 2021

El dispositivo Citrix ADC tiene un monitor integrado que se puede utilizar para supervisar los servicios LDAP: El monitor LDAP. Comprueba periódicamente el servicio LDAP al que está vinculado mediante la autenticación y el envío de una consulta de búsqueda. Si la búsqueda se realiza correctamente, el servicio se marca como UP. Si el servidor LDAP no encuentra la entrada, se envía un mensaje de error al monitor LDAP y el servicio se marca como DOWN.

Configure el monitor LDAP para definir la búsqueda que debe realizar al enviar una consulta. Puede utilizar el parámetro DN base para especificar una ubicación en la jerarquía de directorios en la que el servidor LDAP debe iniciar la consulta de prueba. Puede utilizar el parámetro Attribute para especificar un atributo de la entidad de destino.

Nota: Los sondeos del monitor se originan a partir de la dirección NSIP.

Parámetro	Especifica
BaseDN	Nombre base para el monitor LDAP desde donde debe iniciarse la búsqueda LDAP. Si el servidor LDAP se ejecuta localmente, el valor predeterminado de base es dc=`netscaler`, dc=com.
BindDN	Nombre de BDN para el monitor LDAP.
filter	Filtro para el monitor LDAP. Utilice el parámetro filtro de una consulta para limitar el número de resultados. Si no especifica este parámetro en la consulta, el filtro se aplica a toda la clase de objeto, lo que podría ser una operación costosa, como un uso elevado de la CPU.
contraseña	Contraseña utilizada en la supervisión de servidores LDAP.
atributo	Atributo para el monitor LDAP.

Para configurar el monitor LDAP integrado, consulte Configuración de monitores en una configuración de equilibrio de carga.

Monitorización del servicio MySQL

August 20, 2021

El dispositivo Citrix ADC tiene un monitor integrado que se puede utilizar para supervisar los servicios de MySQL: El monitor MySQL. Comprueba periódicamente el servicio MySQL al que está vinculado enviando una consulta de búsqueda. Si la búsqueda se realiza correctamente, el servicio se marca como UP. Si el servidor MySQL no responde o la búsqueda falla, se envía un mensaje de error al monitor MySQL y el servicio está marcado como DOWN.

Nota: Los sondeos del monitor se originan a partir de la dirección NSIP.

Parámetro	Especifica
base de datos	Base de datos que se utiliza para el monitor MySQL.
SQLQuery	Consulta SQL que se utiliza para el monitor MySQL.

Para configurar un monitor MySQL integrado, consulte Configuración de monitores en una configuración de equilibrio de carga.

Para configurar monitores MySQL mediante CLI

Escriba el siguiente comando:

```
1 add lb monitor <monitorName> <type> -scriptName <string> -scriptArgs <
     string>
2 <!--NeedCopy-->
```

Ejemplo:

```
1 add lb monitor mysql1 USER -scriptName nsmysql.pl -scriptArgs ”database
     =cloud;user=cloud;password=password;query=show tables from cloud”
2 <!--NeedCopy-->
```

Supervisión de servicios SNMP

January 19, 2021

El dispositivo Citrix ADC tiene un monitor integrado que se puede utilizar para supervisar los servicios SMNP: El monitor SNMP. Comprueba periódicamente el agente SNMP en el servicio al que está vinculado enviando una consulta para el ID de identificación de empresa (OID) que configura para supervisar. Si la consulta se realiza correctamente, el servicio se marca como UP. Si el servicio SNMP encuentra el OID especificado, la consulta se realiza correctamente y el monitor SNMP marca el servicio UP. Si no encuentra el OID, la consulta falla y el monitor SNMP marca el servicio DOWN.

Nota: Los sondeos del monitor se originan a partir de la dirección NSIP.

Parámetro	Especifica
SNMPOID	OID que se utiliza para el monitor SNMP.
Comunidad SNMPs	Comunidad que se utiliza para el monitor SNMP.
Umbral SNMP	Umbral que se utiliza para el monitor SNMP.
Versión SNMPVersion	Versión SNMP que se utiliza para la supervisión de carga. Valores posibles: V1, V2.

Para configurar el monitor SNMP integrado, consulte Configuración de monitores en una configuración de equilibrio de carga.

Supervisión de servicios NNTP

August 20, 2021

El dispositivo Citrix ADC tiene un monitor integrado que se puede utilizar para supervisar los servicios NNTP: El monitor NNTP. Comprueba periódicamente el servicio NNTP al que está vinculado conectándose al servicio y comprobando la existencia del grupo de noticias que especifique. Si el grupo de noticias existe, la búsqueda se realiza correctamente y el servicio se marca como UP. Si el servicio NNTP no responde o la búsqueda falla, el servicio se marca como DOWN.

Nota: Los sondeos del monitor se originan a partir de la dirección NSIP.

El monitor NNTP se puede configurar opcionalmente para publicar un mensaje de prueba en el grupo de noticias también.

Parámetro	Especifica
`userName`	Nombre de usuario en el servidor RADIUS/NNTP/FTP/FTP-EXTENDED/MYSQL/POP3. Este nombre de usuario se utiliza en el sondeo.
contraseña	Contraseña utilizada en la supervisión de servidores RADIUS/NNTP/FTP/FTP-EXTENDED/MYSQL/POP3/LDAP.
grupo	Nombre del grupo que se va a consultar para el monitor NNTP.

Para configurar el monitor NNTP integrado, consulte Configuración de monitores en una configuración de equilibrio de carga.

Supervisión del servicio POP3

August 20, 2021

El dispositivo Citrix ADC tiene un monitor integrado que se puede utilizar para supervisar los servicios POP3: El monitor POP3. Comprueba periódicamente el servicio POP3 al que está vinculado abriendo una conexión con un servidor POP3. Si el servidor POP3 responde con los códigos de respuesta correctos dentro del período de tiempo configurado, marca el servicio UP. Si el servicio POP3 no responde o responde incorrectamente, marca el servicio DOWN.

Nota: Los sondeos del monitor se originan a partir de la dirección NSIP.

Parámetro	Especifica
Nombre de usuario	Servidor POP3 de nombre de usuario. Este nombre de usuario se utiliza en el sondeo.
contraseña	Contraseña utilizada en la supervisión de servidores POP3.
scriptName	Ruta de acceso y nombre del script que se va a ejecutar.
dispatcherIP	La dirección IP del despachador al que se envía el sondeo.
dispatcherPort	El puerto del despachador al que se envía el sondeo.

Para configurar el monitor POP3 integrado, consulte Configuración de monitores en una configuración de equilibrio de carga.

Para configurar monitores POP3 mediante CLI

Escriba el siguiente comando:

```
1 add lb monitor <monitorName> <type> -scriptName <string> -scriptArgs <
     string>
2 <!--NeedCopy-->
```


Ejemplo:

```
add lb monitor pop31 USER -scriptName nspop3.pl -scriptArgs ”user=
    test@lbmon1.net;password=Freebsd123”

<!--NeedCopy-->
```

Supervisión de servicios SMTP

August 20, 2021

El dispositivo Citrix ADC tiene un monitor integrado que se puede utilizar para supervisar los servicios SMTP: el monitor SMTP. El monitor comprueba el servicio SMTP al que está vinculado abriendo una conexión con él y realizando una serie de apretones de manos para garantizar que el servidor funcione correctamente. Si el servicio SMTP completa los apretones de manos correctamente, el monitor marca el servicio UP. De lo contrario, si el servicio SMTP no responde o responde incorrectamente, marca el servicio INCORRECTO.

Nota: Los sondeos del monitor se originan a partir de la dirección NSIP.

Parámetro	Especifica
scriptName	Ruta y nombre del script que se va a ejecutar.
dispatcherIP	La dirección IP del despachador al que se envía el sondeo.
dispatcherPort	El puerto del despachador al que se envía el sondeo.

Para configurar el monitor SMTP integrado, consulte Configuración de monitores en una configuración de equilibrio de carga.

Supervisión de servicios RTSP

August 20, 2021

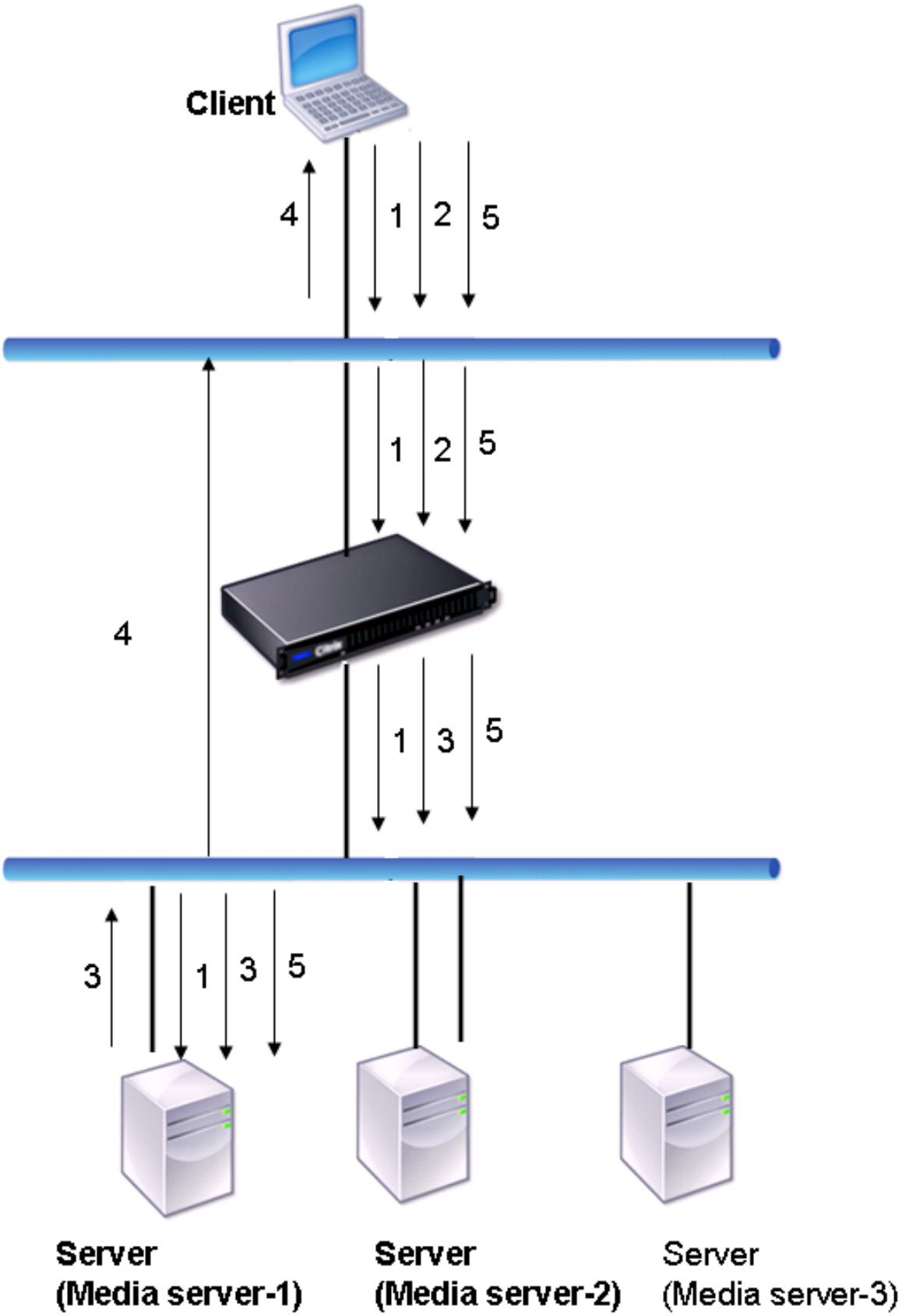
El dispositivo Citrix ADC tiene un monitor integrado que se puede utilizar para supervisar los servicios RTSP: El monitor RTSP. Comprueba periódicamente el servicio RTSP al que está vinculado abriendo

una conexión con el servidor RTSP equilibrado de carga. El tipo de conexión que abre y la respuesta que espera varían según la configuración de la red. Si el servicio RTSP responde como se esperaba dentro del período de tiempo configurado, marca el servicio UP. Si el servicio no responde o responde incorrectamente, marca el servicio DOWN.

El dispositivo Citrix ADC se puede configurar para equilibrar la carga de los servidores RTSP mediante dos topologías: NAT-off y NAT-on. Los servidores RTSP envían sus respuestas directamente al cliente, evitando el dispositivo. El dispositivo debe configurarse para supervisar los servicios RTSP de manera diferente en función de la topología que utilice la red. El dispositivo se puede implementar en modo en línea o no en modo en modo NAT desactivado y NAT activado.

En el modo Nat-off, el dispositivo funciona como un enrutador: Recibe solicitudes RTSP del cliente y las enruta al servicio que selecciona mediante el método de equilibrio de carga configurado. Si los servidores RTSP equilibrados de carga tienen asignados FQDN de acceso público en DNS, los servidores con equilibrio de carga envían sus respuestas directamente al cliente, sin pasar por el dispositivo. La siguiente ilustración muestra esta configuración.

Ilustración 1. RTSP en modo NAT desactivado



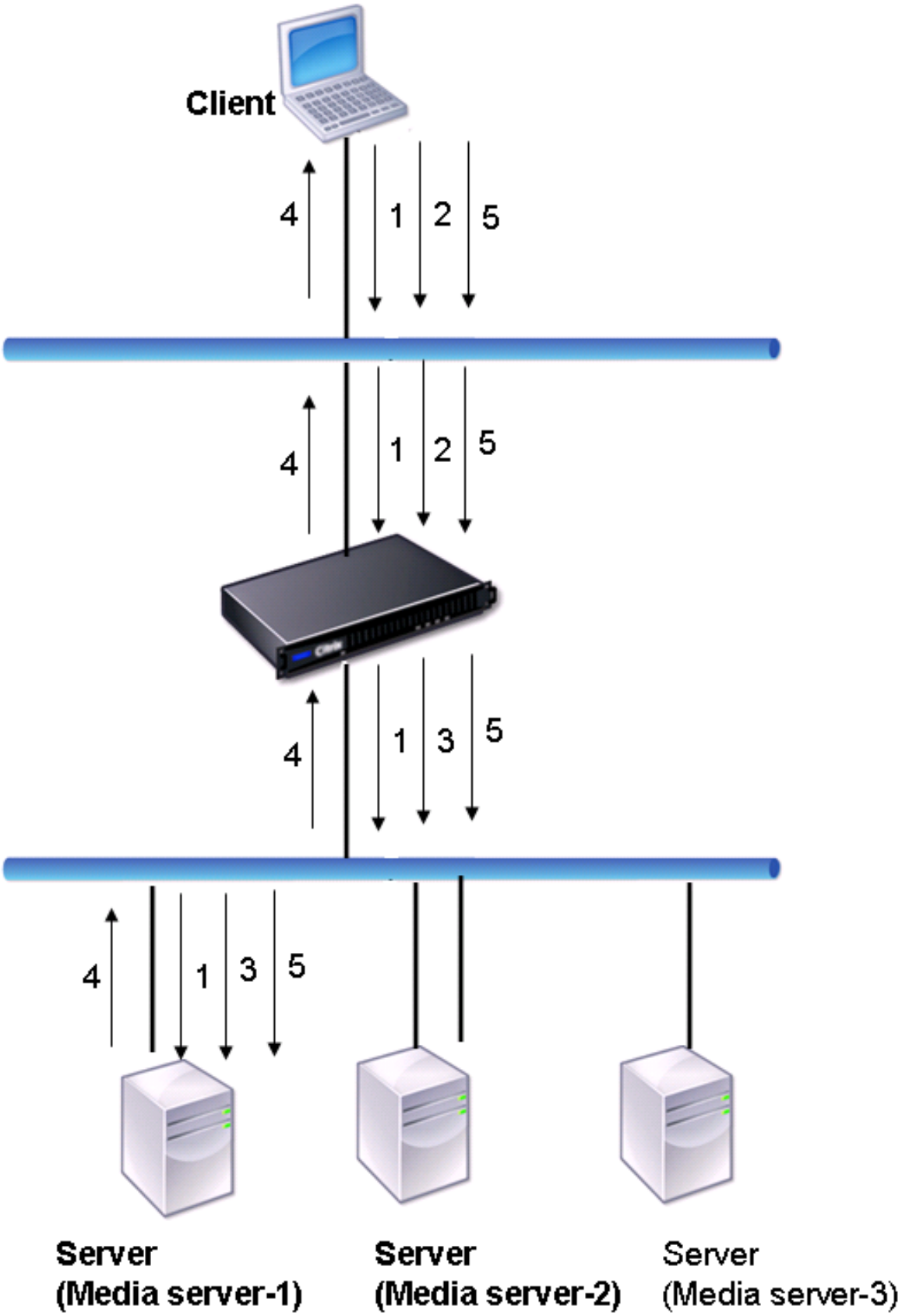
El flujo de solicitudes y respuestas en este caso es el siguiente:

1. El cliente envía una solicitud DESCRIBE al dispositivo. El dispositivo utiliza el método de equilibrio de carga configurado para elegir un servicio y enruta la solicitud a Media Server-1.
2. El cliente envía una solicitud SETUP al dispositivo. Si se intercambia el Id. de sesión RTSP en la solicitud DESCRIBE, el dispositivo, mediante la persistencia RTSPSID, enruta la solicitud al Servidor de medios 1. Si se intercambia el ID de sesión RTSP en la solicitud SETUP, el dispositivo realiza una de las acciones siguientes:
   - Si la solicitud RTSP viene en la misma conexión TCP, enruta la solicitud a Media Server-1, manteniendo la persistencia.
   - Si la solicitud llega a una conexión TCP diferente, utiliza el método de equilibrio de carga configurado para elegir un servicio y envía la solicitud a ese servicio, sin mantener la persistencia. Esto significa que la solicitud podría enviarse a otro servicio.
3. Media Server-1 recibe la solicitud SETUP del dispositivo, asigna recursos para procesar la solicitud RTSP y envía el ID de sesión apropiado al cliente.

   Nota: El dispositivo no realiza NAT para identificar la conexión RTSP, ya que las conexiones RTSP la omiten.
4. Para las solicitudes posteriores, el cliente utiliza el ID de sesión para identificar la sesión y enviar mensajes de control al servidor de medios. Media Server-1 realiza las acciones solicitadas, como reproducir, avanzar o rebobinar.

En el modo Nat-On, el dispositivo recibe solicitudes RTSP del cliente y las enruta al servidor de medios adecuado mediante el método de equilibrio de carga configurado. A continuación, el servidor de medios envía sus respuestas al cliente a través del dispositivo, como se muestra en el siguiente diagrama.

Ilustración 2. RTSP en modo Nat-On



El flujo de solicitudes y respuestas en este caso es el siguiente:

1. El cliente envía una solicitud DESCRIBE al dispositivo. El dispositivo utiliza el método de equilibrio de carga configurado para elegir un servicio y enruta la solicitud a Media Server-1.
2. El cliente envía una solicitud SETUP al dispositivo. Si se intercambia el Id. de sesión RTSP en la solicitud DESCRIBE, el dispositivo, mediante la persistencia RTSPSID, enruta la solicitud al Servidor de medios 1. Si se intercambia el ID de sesión RTSP en la solicitud SETUP, el dispositivo realiza una de las acciones siguientes:
   - Si la solicitud RTSP viene en la misma conexión TCP, enruta la solicitud a Media Server-1, manteniendo la persistencia.
   - Si la solicitud llega a una conexión TCP diferente, utiliza el método de equilibrio de carga configurado para elegir un servicio y envía la solicitud a ese servicio, sin mantener la persistencia. Esto significa que la solicitud podría enviarse a otro servicio.
3. Media Server-1 recibe la solicitud SETUP del dispositivo, asigna recursos para procesar la solicitud RTSP y envía el ID de sesión apropiado al cliente.
4. El dispositivo realiza NAT para identificar el cliente para las conexiones de datos RTSP, y las conexiones RTSP pasan a través del dispositivo y se enrutan al cliente correcto.
5. Para las solicitudes posteriores, el cliente utiliza el identificador de sesión para identificar la sesión y enviar mensajes de control al dispositivo. El dispositivo utiliza la persistencia RTSPSID para identificar el servicio adecuado y enruta la solicitud a Media Server-1. Media Server-1 realiza la acción solicitada, como reproducir, avanzar o rebobinar.

El monitor RTSP utiliza el protocolo RTSP para evaluar el estado de los servicios RTSP. El monitor RTSP se conecta al servidor RTSP y realiza una secuencia de apretones de manos para asegurarse de que el servidor funciona correctamente.

Parámetro	Especifica
Solicitud RTSPRequest	La cadena de solicitud RTSP que se envía al servidor RTSP (por ejemplo, OPTIONS *). El valor predeterminado es 07. La longitud de la solicitud no debe superar los 163 caracteres.
respCode	Conjunto de códigos de respuesta que se esperan del servicio.

Para obtener instrucciones sobre cómo configurar un monitor RTSP, consulte Configuración de monitores en una configuración de equilibrio de carga.

Supervisión de XML Broker Service

August 20, 2021

El dispositivo Citrix ADC tiene un tipo de monitor integrado, CITRIX-XML-SERVICE, con el que puede crear monitores para supervisar XML Broker Services. Citrix XenApp utiliza XML Broker Services. El monitor abre una conexión al servicio y examina periódicamente los servicios XML a los que está vinculado. Si el servidor responde como se esperaba dentro del período de tiempo configurado, el monitor marca el servicio UP. Si el servicio no responde o responde incorrectamente, el monitor marca el servicio DOWN.

Para configurar un monitor CITRIX-XML-SERVICE, debe especificar el nombre de la aplicación además de establecer los parámetros estándar. El nombre de la aplicación es el nombre de la aplicación que debe ejecutarse para supervisar el estado del servicio de agente XML. La aplicación predeterminada es Bloc de notas.

Para configurar monitores para XML Broker Services, consulte Configuración de monitores en una configuración de equilibrio de carga.

> **Nota**
>
> El parámetro “Nombre de aplicación” para el monitor de servicio Citrix-XML no es válido para XenApp y Citrix Virtual Desktops versiones 7 y posteriores. Se recomienda no utilizar este parámetro en XA/XD 7. En caso de configurar este parámetro, este parámetro no se utiliza internamente. El criterio de sondeo es diferente a partir de XA/XD 7. Sin embargo, puede utilizar los parámetros “Nombre de aplicación” en versiones anteriores a XA/XD 7.

Supervisión de solicitudes ARP

August 20, 2021

El dispositivo Citrix ADC tiene un monitor integrado que se puede utilizar para supervisar las solicitudes ARP: El monitor ARP. Este monitor envía periódicamente una solicitud ARP al servicio al que está vinculado y escucha la respuesta esperada. Si recibe la respuesta esperada, marca el servicio UP. Si no recibe respuesta o la respuesta incorrecta, marca el servicio DOWN.

ARP localiza una dirección de hardware para un servidor con equilibrio de carga cuando solo se conoce la dirección de la capa de red. ARP es compatible con IPv4 para traducir direcciones IP a direcciones MAC Ethernet. La supervisión ARP no es relevante para las redes IPv6 y, por lo tanto, no se admite en dichas redes.

No hay parámetros especiales para el monitor ARP.

Para obtener instrucciones sobre cómo configurar un monitor ARP, consulte Configuración de monitores en una configuración de equilibrio de carga.

Supervisión del servicio de Delivery Controller de XenDesktop

August 20, 2021

En la virtualización de escritorios, el dispositivo Citrix ADC se puede utilizar para equilibrar la carga de los servidores de interfaz web (WI) y los servidores de XenDesktop Delivery Controller implementados por el entorno Citrix XenDesktop. El dispositivo Citrix ADC proporciona un monitor integrado, `CITRIX-XD-DDC` un monitor que supervisa los servidores de XenDesktop Delivery Controller. Además de la comprobación de estado, también puede comprobar si el sondeo es enviado por un usuario válido del servidor de Delivery Controller de XenDesktop.

El monitor envía un sondeo al servidor de Delivery Controller de XenDesktop en forma de mensaje XML. Si el servidor responde al sondeo con la identidad del conjunto de servidores, se considera que el sondeo tiene éxito y el estado del servidor se marca como UP. Si la respuesta HTTP no tiene un código correcto o la identidad de la comunidad de servidores no está presente en la respuesta, se considera que el sondeo es un error y el estado del servidor se marca como DOWN.

La opción Validar credenciales determina el sondeo que debe enviar el monitor al servidor de Delivery Controller de XenDesktop, es decir, si quiere solicitar solo el nombre del servidor o validar también las credenciales de inicio de sesión.

Nota: Independientemente de si las credenciales de usuario (nombre de usuario, contraseña y dominio) se especifican en el
`CITRIX-XD-DDC` monitor, el servidor de XenDesktop Delivery Controller valida las credenciales de usuario solo si la opción de validar credenciales está habilitada en el monitor.

Si utiliza el asistente para configurar el equilibrio de carga de los servidores de XenDesktop, el `CITRIX-XD-DDC` monitor se crea automáticamente y se enlaza a los servicios de XenDesktop Delivery Controller.

Para agregar un monitor XD-DDC con la opción validar credenciales mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para agregar un monitor XD-DDC y verificar la configuración:

```
1 add lb monitor <monitorName> <monitorType> -userName <userName> -
    password <password> -domain <domain_name> -validateCred YES
```



```
2
3 show lb monitor <monitorName>
4 <!--NeedCopy-->
```

Ejemplo:

```
1  > add lb monitor xdddcmon Citrix-xd-ddc -userName Administrator -
      password E12Dc35450a1 -domain dhop -validateCred YES
2  Done
3 > show lb monitor xdddcmon
4 1) Name......:xdddcmon Type......:CITRIX-XD-DDC State......: ENABLED
5
6 Standard parameters:
7 Interval......:..5 sec...Retries......:..3
8 Response timeout......:..2 sec...Down time......:..30 sec
9 Reverse......:..NO...Transparent......:..NO
10 Secure......:..NO...LRTM......:..ENABLED
11 Action......:..Not applicable...Deviation......:..0 sec
12 Destination IP......:..Bound service
13 Destination port......:..Bound service
14 Iptunnel......:..NO
15 TOS......:..NO...TOS ID......:..0
16 SNMP Alert Retries......:..0...Success Retries......:..1
17 Failure Retries......:..0
18
19 Special parameters:
20 User Name..........:"Administrator"
21 Password..........:*****
22 DDC Domain.........: "dhop"
23 Done
24 <!--NeedCopy-->
```

Para especificar la opción de validación de credenciales en un monitor XD-DDC mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
1 set lb monitor <monitorName> <monitorType> -userName -password -domain
     <domain_name> -validateCred YES
2 <!--NeedCopy-->
```


Ejemplo:

```
1  set lb monitor XD_DDC_21.21.21.22_443_mn CITRIX-xd-ddc -userName
      Administrator -password D123S1R2A123 -domain dhop -validateCred YES
2 Done
3 <!--NeedCopy-->
```

Para configurar un monitor XD-DDC con la opción validar credenciales mediante la utilidad de configuración

Vaya a **Administración del tráfico > Equilibrio de carga > Monitores**y cree un monitor de tipo `Citrix-XD-DDC`.

Supervisión de almacenes de Citrix StoreFront

August 20, 2021

Puede configurar un monitor de usuario para un almacén Citrix StoreFront. El monitor determina el estado del almacén de StoreFront explorando sucesivamente el servicio de cuentas, el servicio de detección y el endpoint de autenticación (si Citrix StoreFront Store es un almacén autenticado). Si alguno de estos servicios no responde al sondeo, el sondeo del monitor falla y el almacén de StoreFront se marca como DOWN. El monitor envía sondeos a la dirección IP y al puerto del servicio vinculado. Para obtener más información, consulte API de servicios de almacén de Citrix StoreFront.

Nota: Los sondeos del monitor se originan a partir de la dirección NSIP. Sin embargo, si la subred de un servidor StoreFront es diferente de la del dispositivo, se utiliza la dirección IP de la subred (SNIP).

A partir de la versión 10.1 compilación 120.13, también puede enlazar un monitor de StoreFront a un grupo de servicios. Un monitor está enlazado a cada miembro del grupo de servicios y los sondeos se envían a la dirección IP y al puerto del miembro vinculado (servicio). Además, dado que cada miembro de un grupo de servicios se supervisa ahora mediante la dirección IP del miembro, ahora puede utilizar el monitor de StoreFront para supervisar los nodos del clúster de StoreFront que se agregan como miembros del grupo de servicios.

En versiones anteriores, el monitor de StoreFront intentó autenticar almacenes anónimos. Como resultado, un servicio se puede marcar como INactivo y no se puede iniciar XenApp o XenDesktop mediante la URL del servidor virtual de equilibrio de carga.

Desde la compilación 64.x, el orden del sondeo ha cambiado. Ahora, el monitor determina el estado del almacén de StoreFront probando sucesivamente el servicio de cuentas, el documento de detec-

ción y, a continuación, el servicio de autenticación, y omite la autenticación para almacenes anónimos.

El parámetro nombre de host de los monitores StoreFront está obsoleto. El parámetro seguro se utiliza ahora para determinar si se debe utilizar HTTP (el valor predeterminado) o HTTPS para enviar sondeos de monitor.

Para utilizar HTTPS, establezca la opción segura en Sí.

Para crear un monitor de StoreFront mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para configurar un monitor de StoreFront y verifique la configuración:

```
add lb monitor <monitorName> STOREFRONT <string> -storeName <string> [-
   storefrontacctservice ( YES | NO )] -secure ( YES | NO )

show lb monitor <monitorName>
<!--NeedCopy-->
```

Ejemplo

```
add lb monitor storefront_ssl STOREFRONT -storename myStore -
   storefrontacctservice YES -secure YES
<!--NeedCopy-->
```

Para crear un monitor de StoreFront mediante la utilidad de configuración

Vaya a **Administración del tráfico > Equilibrio de carga > Monitores**y cree un monitor de tipo **STOREFRONT**.

> **Nota**
>
> Para obtener más información sobre los monitores StoreFront, consulte la documentación de StoreFront.

Monitores personalizados

August 20, 2021

Además de los monitores integrados, puede usar monitores personalizados para verificar el estado de sus servicios. El dispositivo Citrix ADC proporciona varios tipos de monitores personalizados basados en scripts incluidos en el sistema operativo Citrix ADC. Los scripts se pueden utilizar para determinar el estado de los servicios en función de la carga del servicio o del tráfico de red enviado al servicio. Los monitores personalizados son monitores en línea, monitores de usuario y monitores de carga.

Con este tipo de monitores, puede utilizar la funcionalidad suministrada o crear sus propios scripts y utilizarlos para determinar el estado del servicio al que está enlazado el monitor.

Configurar monitores en línea HTTP

August 20, 2021

Los monitores en línea analizan y sondean las respuestas de los servicios a los que están enlazados solo cuando esos servicios reciben solicitudes de clientes. El monitor en línea es de tipo HTTP-INLINE y solo se puede configurar con los servicios HTTP y HTTPS. Un monitor en línea determina que el servicio al que está enlazado está UP comprobando sus respuestas a las solicitudes que se le envían. Cuando no se envían solicitudes de cliente al servicio, el monitor en línea sondea el servicio mediante la dirección URL configurada.

Nota: Los monitores en línea no se pueden enlazar a servicios locales o remotos HTTP o HTTPS Global Server Load Balancing (GSLB) porque estos servicios representan servidores virtuales en lugar de servidores web equilibrados de carga real.

Los monitores en línea tienen un valor de tiempo de espera y un recuento de reintentos cuando los sondeos fallan. Puede seleccionar cualquiera de los siguientes tipos de acción para que el dispositivo Citrix ADC realice cuando se produzca un error:

- **NINGUNO.** No se toman medidas explícitas. Puede ver el servicio y el monitor, y el monitor indica el número de respuestas de error contiguas actuales y respuestas acumulativas comprobadas.
- **LOG.** Registra el evento en ns/syslog y muestra los contadores.
- **DOWN.** Marca el servicio inactivo y no dirige ningún tráfico al servicio. Esta configuración interrumpe las conexiones persistentes con el servicio. Esta acción también registra el evento y muestra los contadores.

Una vez que el servicio está inactivo, el servicio permanece INactivo durante el tiempo de inactividad configurado. Una vez transcurrido el tiempo de inactividad, el monitor en línea utiliza la URL configurada para sondear el servicio y ver si está disponible de nuevo. Si el sondeo tiene éxito, el estado del servicio cambia a UP. El tráfico se dirige al servicio y la supervisión se reanuda como antes.

Para configurar monitores en línea, consulte Configuración de monitores en una configuración de equilibrio de carga.

Para configurar monitores en línea HTTP mediante CLI

Escriba el siguiente comando:

```
add lb monitor <monitorName> <type> -respCode <int[-int]> -httpRequest
    <string> -resptimeout <integer> [<units>] -retries <integer> -
    downTime <integer> [<units>] -action <action>
<!--NeedCopy-->
```

Ejemplo:

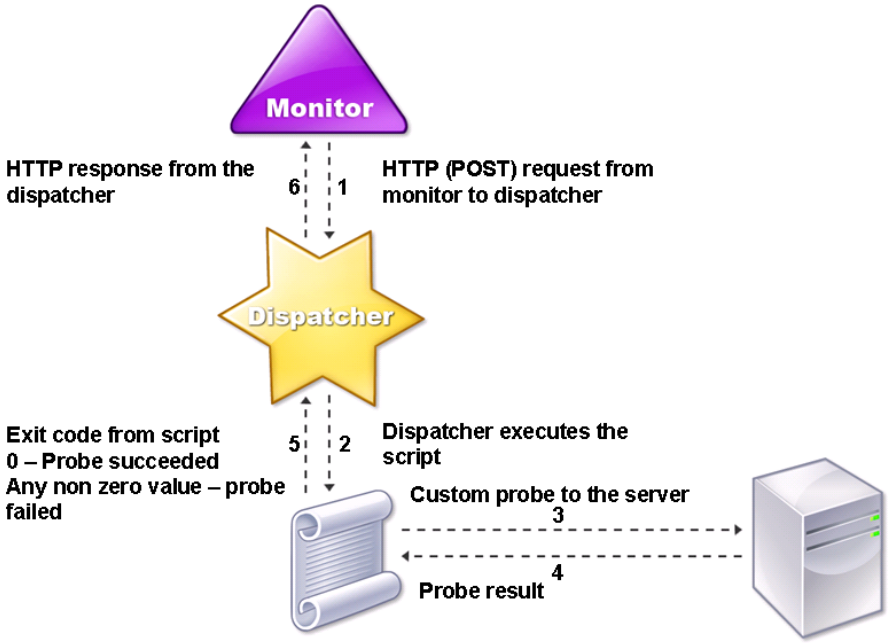
```
add lb monitor http_inline HTTP-INLINE -respCode 200 304 -httpRequest "
    HEAD /var/static/empty.htm" -resptimeout 4 -retries 1 -downTime 2 -
    action NONE
<!--NeedCopy-->
```

Comprender los monitores de

October 5, 2021

Los monitores de usuario amplían el alcance de los monitores personalizados. Puede crear monitores de usuario para realizar un seguimiento del estado de las aplicaciones y los protocolos personalizados que el dispositivo Citrix ADC no admite. El siguiente diagrama ilustra cómo funciona un monitor de usuario.

Ilustración 1. Monitores de usuario



Un monitor de usuario requiere los siguientes componentes.

Despachador. Proceso, en el dispositivo, que escucha las solicitudes de supervisión. Un despachador puede estar en la dirección IP de bucle de retorno (127.0.0.1) y en el puerto 3013. Los despachadores también se conocen como despachadores internos. Un despachador también puede ser un servidor web que admite la interfaz de puerta de enlace común (CGI). Dichos despachadores también se conocen como despachadores externos. Se utilizan para scripts personalizados que no se ejecutan en el entorno de FreeBSD, como guiones de .NET.

> Nota:
>
> Puede configurar el monitor y el despachador para que utilicen HTTPS en lugar de HTTP activando la opción “seguro” en el monitor y configurándolo como despachador externo. Sin embargo, un despachador interno solo entiende HTTP y no puede usar HTTPS.

En una configuración de alta disponibilidad, el despachador se ejecuta tanto en el dispositivo Citrix ADC principal como en el secundario. El despachador permanece inactivo en el dispositivo secundario.

Guión. El script es un programa que envía sondeos personalizados al servidor con equilibrio de carga y devuelve el código de respuesta al despachador. El script puede devolver cualquier valor al despachador, pero si un sondeo tiene éxito, el script debe devolver el valor cero (0). El despachador

considera que cualquier otro valor es un error de sondeo.

El dispositivo Citrix ADC incluye scripts de ejemplo para los protocolos de uso común. Los scripts existen en el directorio /nsconfig/monitors. Si quieres agregar un guión, añádelo allí. Para personalizar un script existente, cree una copia con un nombre nuevo y modifíquela.

Importante:

- A partir de Citrix ADC 13.0, compilación 41.20, puede utilizar el script `nsntlm-lwp.pl` para crear un monitor para supervisar un servidor NTLM seguro.
- A partir de la versión 10.1 build 122.17, los archivos de script para los monitores de usuario se encuentran en una nueva ubicación.

  Si actualiza un dispositivo virtual MPX o VPX a la versión 10.1 compilación 122.17 o posterior, los cambios son los siguientes:

  - Se crea un nuevo directorio denominado conflicts en /nsconfig/monitors/ y todas los scripts integradas de las compilaciones anteriores se trasladan a este directorio.
  - Todas las nuevas scripts integradas están disponibles en el directorio /netscaler/monitors/. Todas los scripts personalizadas están disponibles en el directorio /nsconfig/monitors/.
  - Guarde un nuevo script personalizado en el directorio /nsconfig/monitors/.
  - Una vez finalizada la actualización, si se crea un script personalizado y se guarda en el directorio /nsconfig/monitors/, con el mismo nombre que el script integrado, el script del directorio /netscaler/monitors/ tiene prioridad. El script personalizado no se ejecuta.

  Si aprovisione un dispositivo virtual con la versión 10.1 compilación 122.17 o posterior, los cambios son los siguientes:

  - Todas los scripts integradas están disponibles en el directorio /netscaler/monitors/.
  - El directorio /nsconfig/monitors/ está vacío.
  - Si crea un script personalizado, debe guardarlo en el directorio /nsconfig/monitors/.

Para que los scripts funcionen correctamente:

- El número máximo de caracteres del nombre del guión no debe exceder de 63.
- El número máximo de argumentos de script que se pueden proporcionar a un script no debe superar 512.
- El número máximo de caracteres que se pueden proporcionar en los argumentos de script de parámetros no debe exceder de 639.

Para depurar el script, debe ejecutarlo mediante el script nsumon-debug.pl de la CLI. El nombre del script (con sus argumentos), la dirección IP y el puerto se utilizan como argumentos del script nsumon-debug.pl. Los usuarios deben usar el nombre del script, la dirección IP, el puerto, el tiempo de espera y los argumentos del script nsumon-debug.pl.

En la CLI, escriba:

```
nsumon-debug.pl <scriptname> <IP> <port> <timeout> <partitionID> [
   scriptarguments][is_secure]
<!--NeedCopy-->
```

Importante: A partir de la versión 10.5 build 57.x y los archivos de script 11.0 para monitores de usuario admiten direcciones IPv6 e incluyen los siguientes cambios:

- Para los siguientes protocolos, se `pm files` han incluido nuevos para la compatibilidad con IPv6.
  - RADIUS
  - NNTP
  - POP3
  - SMTP
- Los siguientes scripts de ejemplo de /netscaler/monitors/ se han actualizado para admitir IPv6:
  - nsbmradius.pl
  - nsldap.pl
  - nsnntp.pl
  - nspop3 nssf.pl
  - nssnmp.pl
  - nswi.pl
  - nstftp.pl
  - nssmtp.pl
  - nsrdp.pl
  - nsntlm-lwp.pl
  - nsftp.pl
  - nsappc.pl

  Después de actualizar a la versión 10.5 compilación 57.x o 11.0, si quiere utilizar los scripts personalizados existentes con servicios IPv6, asegúrese de actualizar los scripts personalizados existentes con los cambios proporcionados en los scripts de ejemplo actualizados en /netscaler/monitors/.

  Nota: El script de ejemplo nsmysql.pl no admite la dirección IPv6. Si un servicio IPv6 está enlazado a un monitor de usuario que utiliza nsmysql.pl, se produce un error en el sondeo.

- Los siguientes tipos de monitores LB se han actualizado para admitir direcciones IPv6:
  - USER
  - SMTP
  - NNTP
  - LDAP
  - SNMP
  - POP3
  - FTP_EXTENDED
  - StoreFront
  - APPC
  - CITRIX_WI_EXTENDED

  Si va a crear un script personalizado que utiliza uno de estos tipos de monitores LB, asegúrese de incluir compatibilidad con IPv6 en el script personalizado. Consulte el script de ejemplo asociado en /netscaler/monitors/ para ver los cambios que debe realizar en el script personalizado para admitir IPv6.

Para realizar un seguimiento del estado del servidor, el monitor envía una solicitud HTTP POST al distribuidor configurado. Esta solicitud POST contiene la dirección IP y el puerto del servidor y el script que se debe ejecutar. El despachador ejecuta el script como un proceso secundario, con parámetros definidos por el usuario (si los hay). A continuación, el script envía un sondeo al servidor. El script envía el estado de la sonda (código de respuesta) al despachador. El despachador convierte el código de respuesta en una respuesta HTTP y lo envía al monitor. Según la respuesta HTTP, el monitor marca el servicio como activo o inactivo.

El dispositivo Citrix ADC registra los mensajes de error en el archivo /var/nslog/nsumond.log cuando los sondeos del monitor de usuario fallan. Estos mensajes de error detallados se muestran en la GUI y en la CLI de los comandos `show service`/`service group`.

En la siguiente tabla se enumeran los monitores de usuario y las posibles razones del error.

Tipo de monitor de usuario	Motivos de fallo de sonda
SMTP	El monitor no establece una conexión con el servidor.
NNTP	El monitor no establece una conexión con el servidor.

Tipo de monitor de usuario	Motivos de fallo de sonda
	Argumentos de script faltantes o no válidos, que pueden incluir un número de argumentos o un formato de argumentos no válidos.
	El monitor no encuentra el grupo NNTP.
LDAP	El monitor no establece una conexión con el servidor.
	Argumentos de script faltantes o no válidos, que pueden incluir un número de argumentos o un formato de argumentos no válidos.
	El monitor no se puede enlazar con el servidor LDAP.
	El monitor no encuentra ninguna entrada para la entidad de destino en el servidor LDAP.
FTP	Se agotó el tiempo de espera de la conexión con el servidor.
	Argumentos de script faltantes o no válidos, que pueden incluir un número de argumentos o un formato de argumentos no válidos.
	Error de inicio de sesión.
	El monitor no encuentra el archivo en el servidor.
POP3	El monitor no establece una conexión con la base de datos.
	Argumentos de script faltantes o no válidos, que pueden incluir un número de argumentos o un formato de argumentos no válidos.
	Error de inicio de sesión.
POP3	El monitor no establece una conexión con la base de datos.
	Argumentos de script faltantes o no válidos, que pueden incluir un número de argumentos o un formato de argumentos no válidos.
	Error de inicio de sesión.

Tipo de monitor de usuario	Motivos de fallo de sonda
	La preparación de la consulta SQL falla.
	Error en la ejecución de la consulta SQL.
SNMP	El monitor no establece una conexión con la base de datos.
	Argumentos de script faltantes o no válidos, que pueden incluir un número de argumentos o un formato de argumentos no válidos.
	Error de inicio de sesión.
	El monitor no crea la sesión SNMP.
	El monitor no encuentra el identificador del objeto.
	El valor del umbral del monitor es mayor o igual que el umbral real del monitor.
RDP (Windows Terminal Server)	Argumentos de script faltantes o no válidos, que pueden incluir un número de argumentos o un formato de argumentos no válidos.
	El monitor no crea un zócalo.
	La falta de coincidencia en las versiones.
	El monitor no confirma la conexión.

Puede ver el archivo de registro desde la CLI mediante los siguientes comandos, que abren un shell de BSD, muestran el archivo de registro en la pantalla y, a continuación, cierran el shell de BSD y lo devuelven a la CLI:

```
1 > shell
2 root@ns# cat /var/nslog/nsumond.log
3 root@ns# exit
4 >
5 <!--NeedCopy-->
```

Antes de la versión 13.0 compilación 52.X de Citrix ADC, el comando `show service/service group` mostraba un mensaje de error genérico que decía “error de sondeo” como causa del error del sondeo del monitor de usuario.

Ejemplo:


```
show service ftp

Monitor Name: mon2
State: UNKNOWN  Weight: 1   Passive: 0
Probes: 3    Failed [Total: 0 Current: 0]
Last response: Failure - Probe failed.
Response Time: 1071.838 millisec
<!--NeedCopy-->
```

A partir de la versión 13.0 compilación 52.X de Citrix ADC, el comando `show service/service group` muestra la causa real del error del sondeo del monitor de usuario.

Ejemplo:

```
show service ftp

Monitor Name: mon2
State: DOWN   Weight: 1   Passive: 0
Probes: 729   Failed [Total: 726 Current: 726]
Last response: Failure - Login failed.
Response Time: 8000.0 millisec
<!--NeedCopy-->
```

Los monitores de usuario también tienen un valor de tiempo de espera y un recuento de reintentos para los fallos de sondeo. Puede utilizar monitores de usuario con monitores que no sean usuarios. Durante un uso elevado de la CPU, un monitor que no es usuario permite detectar con mayor rapidez un fallo del servidor.

Si el sondeo del monitor de usuario se desactiva durante un uso elevado de la CPU, el estado del servicio permanece sin cambios.

Ejemplo 1:

```
add lb monitor <name> USER  -scriptname <script-name> -resptimeout 5
   seconds
<!--NeedCopy-->
```

> Nota
>
> Para los monitores con scripts, el tiempo de espera de respuesta debe configurarse en un valor igual al tiempo de espera esperado + 1 segundo. Por ejemplo, si espera que el tiempo de espera

> sea de 4 segundos, configure el tiempo de espera de respuesta como 5 segundos.

Ejemplo 2:

```
add lb monitor <name> USER -scriptname <script-name> -scriptargs <
    Arguments> -secureargs <Arguments>
<!--NeedCopy-->
```

> Nota
>
> Citrix recomienda utilizar el parámetro `secureargs` en lugar del parámetro `scriptargs` para cualquier dato confidencial relacionado con los scripts.

Cómo utilizar un monitor de usuario para revisar sitios web

August 20, 2021

Puede configurar un monitor de usuario para que compruebe si hay problemas específicos del sitio web de los que los servidores HTTP informan mediante códigos HTTP específicos. En la tabla siguiente se enumeran los códigos de respuesta HTTP que este monitor de usuario espera.

Código de respuesta HTTP	Significado
200: éxito	El éxito de la sonda.
503: Servicio no disponible	Fallo de la sonda.
404: No encontrado	No se ha encontrado el script o no se puede ejecutar.
500: Error interno del servidor	Restricciones internas de error/recursos en el despachador (memoria insuficiente, demasiadas conexiones, error inesperado del sistema o demasiados procesos). El servicio no está marcado como DOWN.
400: Solicitud incorrecta	Error al analizar la solicitud HTTP.
502: Gateway incorrecta	Error al decodificar la respuesta del script.

Configurar el monitor de usuario para HTTP mediante los siguientes parámetros.

Parámetro	Especifica
scriptName	Ruta y nombre del script que se va a ejecutar.
Scriptargs	Las cadenas que se agregan en los datos POST. Se copian a la solicitud textualmente.
dispatcherIP	La dirección IP del despachador al que se envía el sondeo.
dispatcherPort	El puerto del despachador al que se envía el sondeo.
LocalFileName	Nombre de un archivo de script de monitor en el sistema local.
DestPath	Una ubicación concreta en el dispositivo Citrix ADC donde se almacena el archivo local cargado.

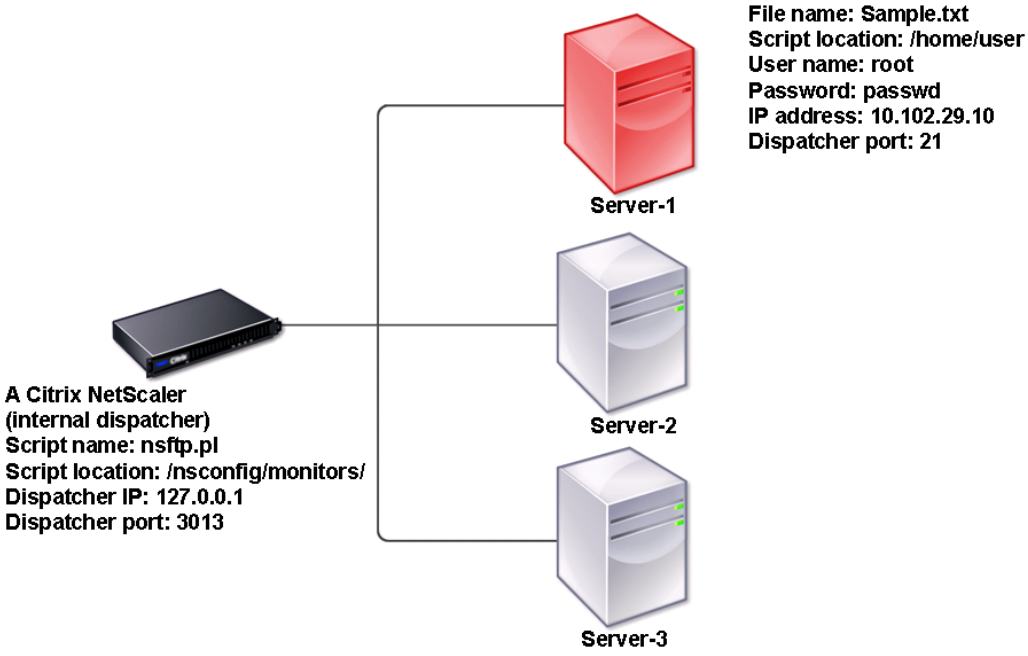
Para crear un monitor de usuario para supervisar HTTP, consulte Configuración de monitores en una configuración de equilibrio de carga.

Comprender el despachador interno

August 20, 2021

Puede utilizar un monitor de usuario personalizado con el distribuidor interno. Considere un caso en el que necesite realizar un seguimiento del estado de un servidor basado en la presencia de un archivo en el servidor. El siguiente diagrama ilustra este caso.

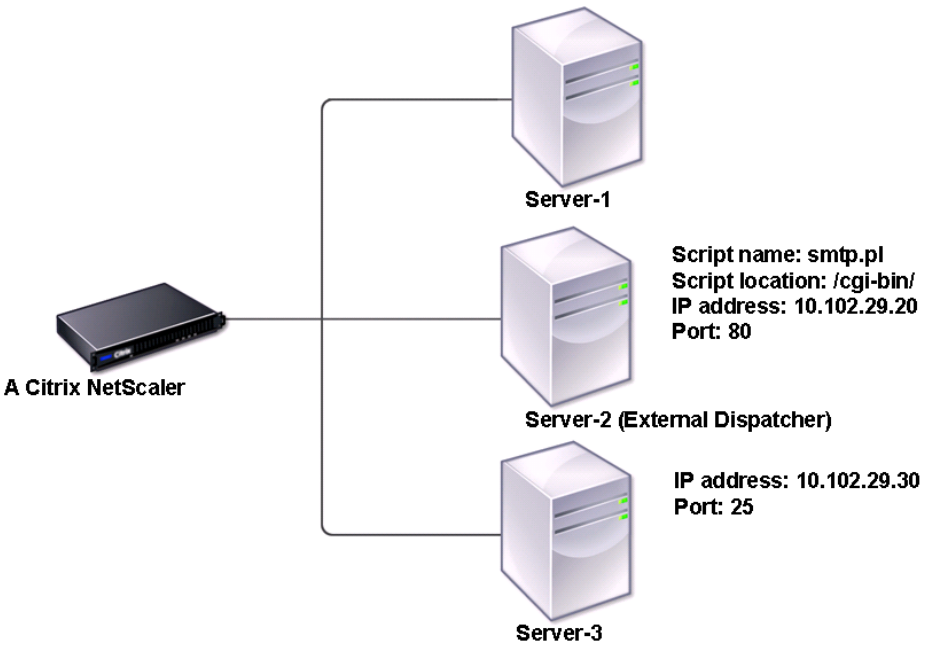
Ilustración 1. Uso de un monitor de usuario con el distribuidor interno



Una posible solución es utilizar un script Perl que inicia una sesión FTP con el servidor y comprueba la presencia del archivo. A continuación, puede crear un monitor de usuario que utilice el script Perl. El dispositivo Citrix ADC incluye un script Perl (nsftp.pl), en el directorio /nsconfig/monitors/.

Puede utilizar un monitor de usuario con un distribuidor externo. Considere un caso en el que debe realizar un seguimiento del estado de un servidor basado en el estado de un servicio SMTP en otro servidor. Este caso se ilustra en el siguiente diagrama.

Ilustración 2. Uso de un monitor de usuario con un distribuidor externo



Una posible solución sería crear un script Perl que compruebe el estado del servicio SMTP en el servidor. A continuación, puede crear un monitor de usuario que utilice el script Perl.

Configurar monitor de usuario

October 5, 2021

Los monitores de usuario realizan un seguimiento del estado de las aplicaciones y los protocolos personalizados que un dispositivo Citrix ADC no admite. Se trata de un ámbito ampliado de monitores personalizados. Para configurar un monitor de usuarios, debe realizar los siguientes pasos:

- Escriba un script que pueda supervisar los servicios vinculados a él.
- Cargue el script en el directorio `/nsconfig/monitors` del dispositivo Citrix ADC.
- Otorgue permiso de ejecutable al script.

Si el tipo de monitor es un protocolo que el dispositivo no admite, solo entonces deberá utilizar un monitor de tipo **USER**. Los monitores de usuario solo admiten scripts de tipo Perl y Bash. No admiten scripts de Python.

> **Nota**
>
> Los sondeos del monitor se originan a partir de la dirección NSIP. `scriptargs` configurado para el tipo de monitor **USER** se muestra en los archivos de configuración y ns.conf en ejecución.

Para obtener más información sobre los monitores, consulte Configurar monitores.

Para configurar un monitor de usuario mediante la CLI

En el símbolo del sistema, escriba:

```
add lb monitor <monitorName> USER -scriptname <NameOfScript> -
    scriptargs <Arguments> -secureargs <Arguments>
<!--NeedCopy-->
```

Ejemplo 1:

```
add monitor Monitor-User-1 USER -scriptname nsftp.pl -scriptargs "file
    =/home/user/
sample.txt;user=root;password=passwd"
<!--NeedCopy-->
```

Ejemplo 2:

```
add monitor Monitor-User-1 USER -scriptname nsftp.pl -scriptargs "file
    =/home/user/
sample.txt -secureargs "user=root;password=passwd"
<!--NeedCopy-->
```

> Nota
>
> El parámetro `secureargs` almacena los argumentos del script en un formato cifrado en lugar de en formato de texto sin formato. Citrix recomienda utilizar el parámetro `secureargs` en lugar del parámetro scriptargs para cualquier dato confidencial relacionado con los scripts, por ejemplo, nombre de usuario y contraseña. Si elige utilizar ambos parámetros a la vez, el script especificado en `-scriptname` debe aceptar los argumentos en el orden: `<scriptargs> <secureargs>`. Especifique los primeros argumentos del parámetro `<scriptargs>`; y el resto de los argumentos del parámetro `<secureargs>`. Es decir, mantener el orden definido para los argumentos. Los argumentos seguros solo se aplican al despachador interno. Si quiere utilizar

> un despachador externo, Citrix recomienda proteger los datos vulnerables de los scripts.

Ejemplo 3:

Supongamos que ya ha configurado el parámetro `scriptargs` con los argumentos: “a=b;c=d;e=f”.

```
add monitor mon1 USER -scriptargs ”a=b;c=d;e=f”
<!--NeedCopy-->
```

Si quiere utilizar el parámetro `secureargs` en lugar del parámetro `scriptargs`, haga lo siguiente:

- Anule el parámetro `scriptargs`.
- Proporciona todos los argumentos en `secureargs` parámetro.

```
set monitor mon1 USER -scriptargs ”” -secureargs ”a=b;c=d;e=f”
<!--NeedCopy-->
```

Para configurar un monitor de usuario mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Monitores y**haga clic en **Agregar**.
2. En la página **Crear monitor**, haga lo siguiente:
   - Seleccione el tipo de monitor como **USUARIO**.
   - Elija el guión del menú desplegable o cargue su propio guión.
   - Introduzca los valores apropiados para los campos **Argumentos de guión** y **Argumentos seguros** .
   - Haga clic en **Crear**.

   Se crea un monitor de usuario.

Comprender los monitores de carga

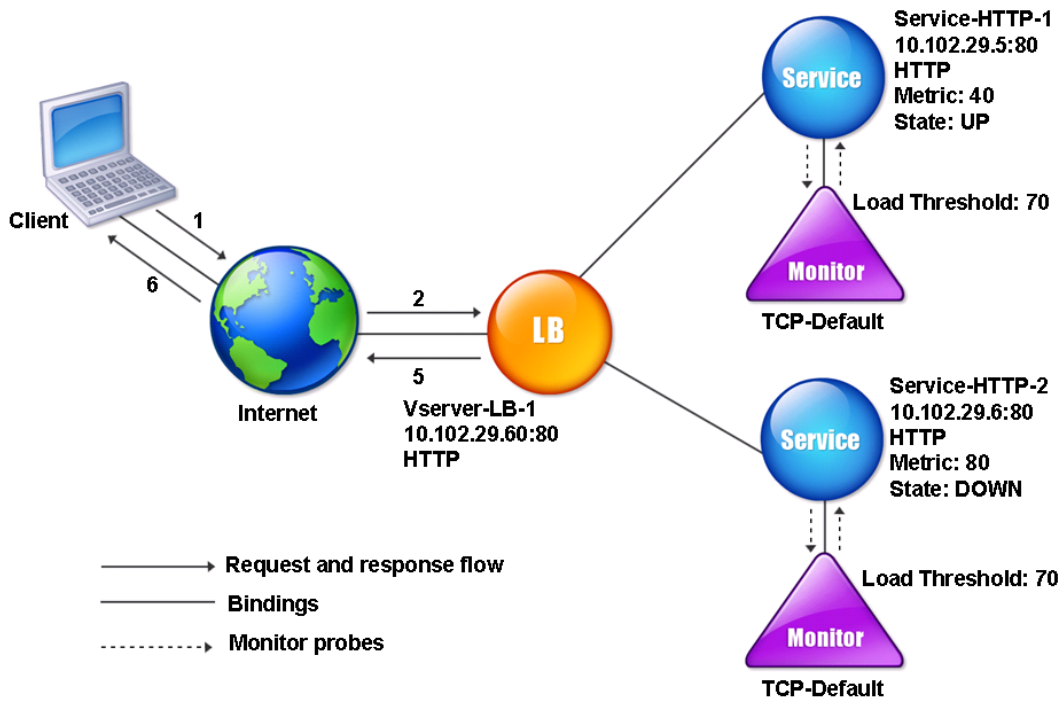
August 20, 2021

Los monitores de carga utilizan OID sondeados SNMP para calcular la carga. El monitor de carga utiliza la dirección IP del servicio al que está vinculado (la dirección IP de destino) para el sondeo. Envía una consulta SNMP al servicio, especificando el OID para una métrica. Las métricas pueden ser CPU, memoria o número de conexiones de servidor. El servidor responde a la consulta con un valor de métrica. El valor de métrica en la respuesta se compara con el valor de umbral. El dispositivo Citrix

ADC considera el servicio para el equilibrio de carga solo si la métrica es menor que el valor umbral. El servicio con el valor de carga más bajo se considera primero.

El siguiente diagrama ilustra un monitor de carga configurado para los servicios descritos en la configuración básica de equilibrio de carga descrita en Configuración del equilibrio de carga básico.

Ilustración 1. Funcionamiento de los monitores de carga



Nota: El monitor de carga no determina el estado del servicio. Solo permite que el dispositivo tenga en cuenta el servicio para el equilibrio de carga.

Después de configurar el monitor de carga, debe configurar las métricas que utilizará el monitor. Para la evaluación de la carga, el monitor de carga considera los parámetros del servidor conocidos como métricas, que se definen en las tablas de métricas de la configuración del dispositivo. Las tablas métricas pueden ser de dos tipos:

- **Locales.** De forma predeterminada, esta tabla existe en el dispositivo. Consta de cuatro métricas: Conexiones, paquetes, tiempo de respuesta y ancho de banda. El dispositivo especifica estas métricas para un servicio y las consultas SNMP no se originan para estos servicios. Estas métricas no se pueden cambiar.
- **Personalizado.** Tabla definida por el usuario. Cada métrica está asociada a un OID.

De forma predeterminada, el dispositivo genera las tablas siguientes:

- NetScaler
- RADWARE
- CISCO-CSS
- LOCAL
- FOUNDRY
- ALTEON

Puede agregar las tablas métricas generadas por el dispositivo o puede agregar tablas de su propia elección, como se muestra en la tabla siguiente. Los valores de la tabla de métricas se proporcionan solo como ejemplos. En un caso real, considere los valores reales de las métricas.

Nombre de la métrica	OID	Peso	Umbral
CPU	1.2.3.4	2	70
Memoria	4.5.6.7	3	80
Conexiones	5.6.7.8	4	90

Para calcular la carga de una o varias métricas, asigne un peso a cada métrica. El peso predeterminado es 1. El peso representa la prioridad dada a cada métrica. Si el peso es alto, la prioridad es alta. El dispositivo elige un servicio basado en el algoritmo hash SOURCEIPDESTIP.

También puede establecer el valor de umbral para cada métrica. El valor de umbral permite al dispositivo seleccionar un servicio para el equilibrio de carga si el valor de métrica para el servicio es menor que el valor de umbral. El valor de umbral también determina la carga en cada servicio.

Configurar monitores de carga

August 20, 2021

Para configurar un monitor de carga, primero cree el monitor de carga. Para obtener instrucciones sobre cómo crear un monitor, consulte Creación de monitores. A continuación, seleccione o cree la tabla de métricas para definir un conjunto de métricas que determinan el estado del servidor y (si crea una tabla de métricas) vincule cada métrica a la tabla de métricas.

Para crear una tabla de métricas mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos:


```
add lb metricTable <metricTableName>

bind lb metricTable <metricTableName> <metric> <SNMPOID>
<!--NeedCopy-->
```

Ejemplo:

```
add metricTable Table-Custom-1

bind metricTable Table-Custom-1 1.3.6.1.4.1.5951.4.1.1.41.1.5 11
<!--NeedCopy-->
```

Para crear una tabla de métricas y enlazar métricas con ella mediante la utilidad de configuración

1. Vaya a **Administración del tráfico > Equilibrio de carga > Tablas de métricas** y cree una tabla de métricas.
2. Para enlazar métricas, haga clic en **Enlazar** y especifique una métrica y un OID SNMP.

Desenlazar métricas de una tabla de métricas

January 12, 2021

Puede desvincular métricas de una tabla de métricas si es necesario cambiar las métricas o si quiere eliminar la tabla de métricas por completo.

Para desenlazar métricas de una tabla de métricas mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
unbind lb metricTable <metricTable> <metric>
<!--NeedCopy-->
```

Ejemplo:


```
unbind metricTable Table-Custom-1 1.3.6.1.4.1.5951.4.1.1.41.1.5
<!--NeedCopy-->
```

Para desvincular métricas de una tabla de métricas mediante la utilidad de configuración

1. Acceda a **Administración del tráfico** > **Equilibrio de carga** > **Tablas Métricas**.
2. Abra una tabla de métricas, seleccione una métrica y haga clic en **Suprimir**.

Puede ver el detalle de todas las tablas de métricas configuradas, como el nombre y el tipo, para determinar si la tabla de métricas es interna o si se ha creado y configurado.

Configurar la supervisión inversa para un servicio

August 20, 2021

Un monitor inverso marca un servicio como DOWN si se cumplen los criterios de sondeo y UP si no se cumplen. Por ejemplo, si quiere que un servicio de copia de seguridad reciba tráfico solo cuando el servicio principal está DOWN, puede enlazar un monitor inverso al servicio secundario pero configurarlo para sondear el servicio principal.

El dispositivo Citrix ADC admite los siguientes monitores inversos:

- HTTP
- ICMP
- TCP (de la versión 11.1 compilación 49.x)

Configuración de la supervisión inversa HTTP para un servicio

En la siguiente tabla se describen las condiciones de la supervisión directa e inversa HTTP para un servicio:

Condición	Directo	Reverso
Conexión no establecida.	Error	Error
El código de respuesta HTTP coincide con las especificaciones del sondeo.	Operación correctamente realizada.	Error

Condición	Directo	Reverso
El código de respuesta HTTP no coincide con las especificaciones del sondeo.	Error	Correcto
Se agotó el tiempo de espera de la sonda.	Error	Error

Para configurar la supervisión inversa HTTP para un servicio mediante la CLI

En el símbolo del sistema, escriba:

```
add lb monitor <Monitor_Name> HTTP -respCode 200 -httpRequest "HEAD /"
   -destIP <Primary_Service_IP_Address> -destPort 80 -reverse YES

bind service <Secondary_Service_Name> -monitorname <Monitor_Name>
<!--NeedCopy-->
```

Configuración de la supervisión inversa ICMP para un servicio

En la siguiente tabla se describen las condiciones de la supervisión directa e inversa de ICMP para un servicio:

Condición	Directo	Reverso
Se recibe la respuesta de eco ICMP.	Operación correctamente realizada.	Error
Se agotó el tiempo de espera de la sonda.	Error	Operación correctamente realizada.

Para configurar la supervisión inversa ICMP para un servicio mediante la CLI

En el símbolo del sistema, escriba:

```
add lb monitor <Monitor_Name> PING -destIP <Primary_Service_IP_Address>
    -reverse YES

```



```
3 bind service <Secondary_Service_Name> -monitorname <Monitor_Name>
4 <!--NeedCopy-->
```

Configuración de la supervisión inversa TCP para un servicio

Si un monitor TCP directo recibe un RESET en respuesta a un sondeo de monitor, el servicio se marca como DOWN. Sin embargo, si un monitor TCP inverso recibe una respuesta RESET, el sondeo se considera correcto y el servicio se marca como UP.

En la siguiente tabla se describen las condiciones de la supervisión inversa TCP para un servicio:

Condición	Directo	Reverso
Se establece la conexión TCP.	Operación correctamente realizada.	Error
Se agotó el tiempo de espera de la sonda.	Error	Error
La respuesta a la sonda es RESET.	Error	Operación correctamente realizada.

Para configurar la supervisión inversa TCP para un servicio mediante la CLI

En el símbolo del sistema, escriba:

```
1 add lb monitor <Monitor_Name> TCP  - destip <Primary_Service_IP_Address>
      -destport <primary_service_port>  - reverse YES
2
3 bind service <Secondary_Service_Name> -monitorname <Monitor_Name>
4 <!--NeedCopy-->
```

Para configurar la supervisión inversa mediante la interfaz gráfica de usuario

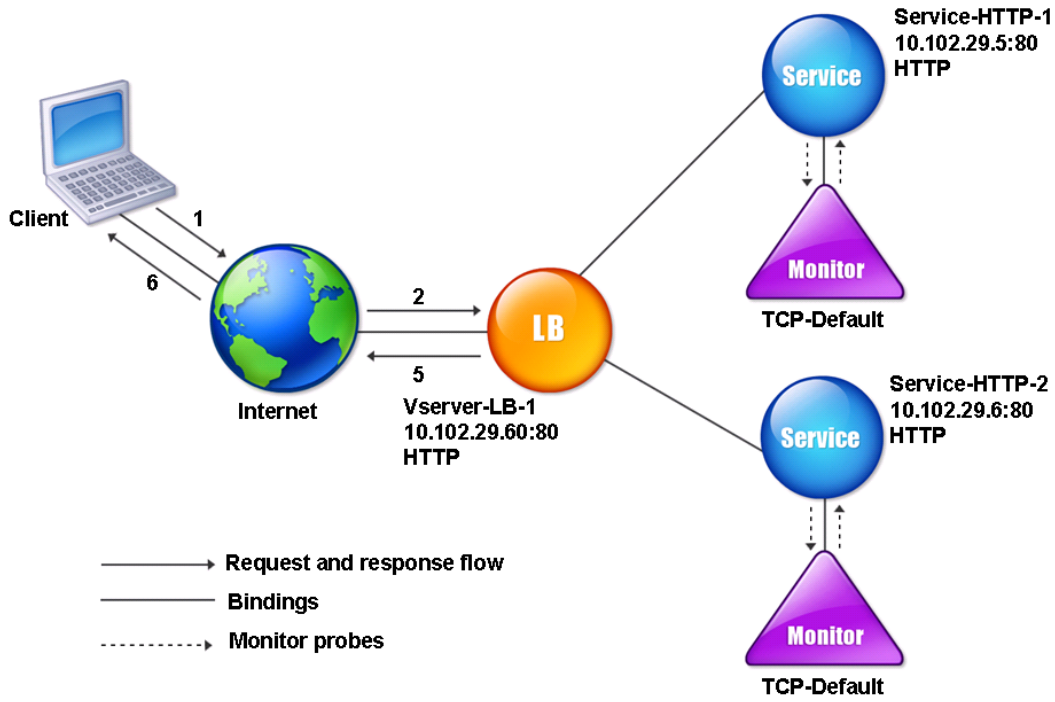
1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Monitores**.
2. Cree un monitor HTTP, ICMP o TCP y seleccione **Invertir**.

Configurar monitores en una configuración de equilibrio de carga

August 20, 2021

Para configurar monitores en un sitio web, primero decide si desea utilizar un monitor integrado o crear su propio monitor. Si crea un monitor, puede elegir entre crear un monitor basado en un monitor integrado o crear un monitor personalizado que utilice un script que escriba para supervisar el servicio. Para obtener más información sobre la creación de monitores personalizados, consulte Monitores personalizados. Una vez que haya elegido o creado un monitor, lo vinculará al servicio apropiado. Los nombres del monitor pueden tener hasta 255 caracteres de longitud. El siguiente diagrama conceptual ilustra una configuración básica de equilibrio de carga con monitores.

Ilustración 1. Funcionamiento de los monitores



Como se muestra, cada servicio tiene un monitor vinculado a él. El monitor sondea el servidor balanceado de carga a través de su servicio. Mientras el servidor balanceado de carga responda a los sondeos, el monitor lo marca UP. Si el servidor equilibrado de carga no responde al número designado de sondas dentro del período de tiempo designado, el monitor lo marca INactivo.

Esta sección incluye los siguientes detalles:

Crear monitores

August 20, 2021

El dispositivo Citrix ADC proporciona un conjunto de monitores integrados. También le permite crear monitores personalizados, ya sea basados en los monitores incorporados o desde cero.

Para crear un monitor mediante la CLI

En el símbolo del sistema, escriba:

```
add lb monitor <monitorName> <monitorType> [<interval>]

add lb mon monitor-HTTP-1 HTTP

add lb mon monitor-HTTP-2 TCP 2
<!--NeedCopy-->
```

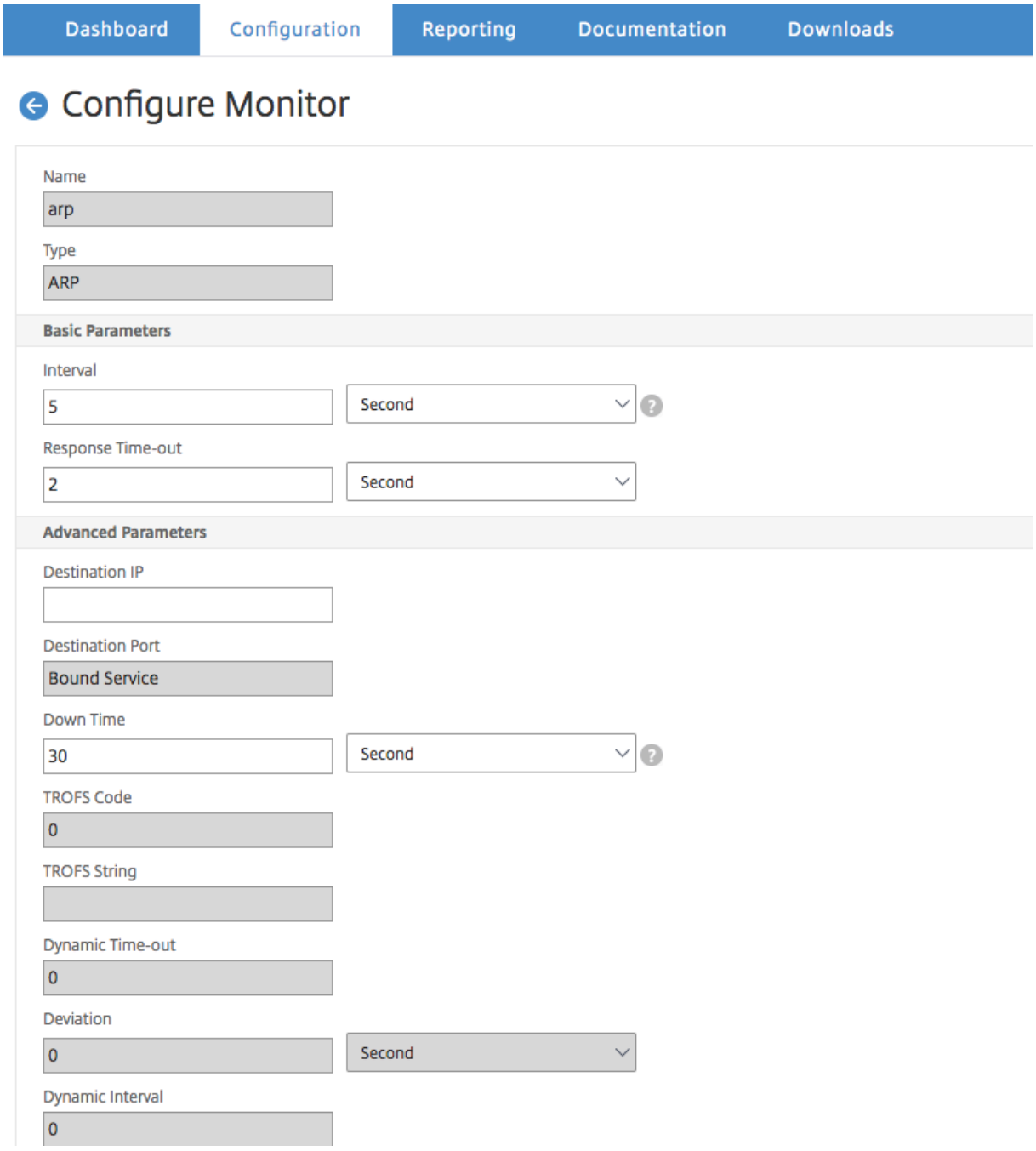
Para crear un monitor mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico**> **Equilibrio de carga**> **Monitores**.
2. Haga clic en **Agregar** y cree un tipo de monitor que cumpla con sus requisitos.

La pantalla Crear monitor contiene dos secciones, **Parámetros básicos** y **Parámetros avanzados**.

Dependiendo del tipo de monitor, la sección **Parámetros básicos** contiene los parámetros que se deben establecer para cada monitor. La sección **Parámetros avanzados** contiene los parámetros que se pueden utilizar en casos de uso avanzados.

La siguiente ilustración es un ejemplo de una página Crear Monitor del tipo de monitor ARP.



Nota

Antes de NetScaler versión 12.0 compilación 56.20, Parámetros Básicos y Parámetros Avanzados se denominan Parámetros Estándar y Parámetros Especiales respectivamente.

Configurar parámetros de monitor para determinar el estado del servicio

August 20, 2021

Puede configurar los siguientes parámetros de supervisión para marcar un servicio como DOWN en función de los sondeos de supervisión.

Reintentos

Número máximo de sondeos a enviar para establecer el estado de un servicio para el que falla un sondeo de supervisión.

Errores

Número de reintentos que deben fallar, fuera del número especificado para el parámetro Reintentos, para que un servicio se marque como DOWN. Por ejemplo, si el parámetro Retries se establece en 10 y el parámetro Reintentos de falla se establece en 6, de los 10 sondeos enviados, al menos seis sondeos deben fallar si el servicio se va a marcar como DOWN.

AlertRetries

Número de errores consecutivos de sondeo después de los cuales el dispositivo genera una captura SNMP llamada MonProbeFailed.

Configuración de alertIntenta un valor superior al valor Reintentos

El parámetro AlertRetries, que especifica el número máximo de errores consecutivos de sondeo de supervisión tras los cuales el dispositivo Citrix ADC genera una captura SNMP denominada Monprobe-Failed, ahora se puede establecer en un valor superior al valor de Retries (que especifica el número máximo de sondeos que se deben enviar para establecer la propiedad de un servicio para el que falló un sondeo de supervisión). Si el valor AlertRetries es mayor que el valor Retries, la captura SNMP no se envía hasta después de que el servicio esté DOWN.

Por ejemplo, si establece Reintentos en 3, Alertas en 12 y el intervalo de tiempo en 5 segundos, el servicio se marca como DOWN después de 15 segundos (3*5), pero no se genera ninguna alerta. Si los sondeos del monitor siguen fallando después de 60 segundos (12*5), el dispositivo Citrix ADC genera una captura MonProbeFailed. Si un sondeo tiene éxito en algún momento entre 15 y 60 segundos, el servicio se marca como UP y no se genera ninguna alerta.

Establecer el valor AlertRetries en un valor mayor que el valor Retries ayuda a generar solo alertas genuinas y a evitar falsos positivos durante los reinicios programados.

Para establecer el valor del parámetro AlertRetries en un valor mayor que el valor Retries mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
add lb monitor <monitorName> [-retries <integer>] [-alertRetries <
   integer>]
<!--NeedCopy-->
```

Ejemplo:

add lb monitor Monitor-HTTP-1 HTTP -retries 3 -AlertRetries 12

Para establecer el valor del parámetro AlertRetries en un valor mayor que el valor Retries mediante la interfaz gráfica de usuario

1. Vaya a **Configuración** > **Administración del tráfico** > **Equilibrio de carga** > **Monitores**.
2. Haga clic en **Agregar** para agregar un monitor nuevo o seleccione uno existente y haga clic en **Modificar**.
3. En el cuadro **Reintentos**, escriba el valor del parámetro Reintentos.
4. En el cuadro de **reintentos de alerta SNMP**, escriba el valor del parámetro `alertRetries`.

Vincular monitores a servicios

August 20, 2021

Después de crear un monitor, lo vincula a un servicio. Puede enlazar uno o varios monitores a un servicio. Si vincula un monitor a un servicio, ese monitor determina si el servicio está marcado hacia arriba o hacia abajo.

Si vincula varios monitores a un servicio, el dispositivo Citrix ADC comprueba el estado de todos los monitores y, a continuación, decide el estado del servicio. Puede configurar diferentes pesos en un monitor. El peso de un monitor especifica cuánto contribuye a designar el servicio como UP o DOWN. Un monitor con un mayor peso tiene una mayor preferencia al marcar el servicio UP o DOWN. El peso predeterminado es 1. Por lo tanto, incluso si uno de los monitores falla, el servicio se marca como DOWN. Para obtener más información, consulte Establecer un valor umbral para los monitores enlazados a un servicio.

Nota: La dirección IP de destino de un sondeo de monitor puede ser diferente de la dirección IP del servidor y el puerto.

Para enlazar un monitor a un servicio mediante la CLI

En el símbolo del sistema, escriba:

```
bind service <name> (-monitorName <string>)
<!--NeedCopy-->
```

Ejemplo:

```
bind service s1 -monitorName tcp
<!--NeedCopy-->
```

Para vincular un monitor a un servicio mediante la GUI

1. Vaya a **Administración de Tráfico > Equilibrio de carga > Servicios**.
2. Abra el servicio y agregue un monitor.

Modificar monitores

August 20, 2021

Puede modificar la configuración de cualquier monitor que haya creado.

Nota: Dos conjuntos de parámetros se aplican a los monitores: Los que se aplican a todos los monitores, independientemente del tipo, y los que son específicos de un tipo de monitor. Para obtener información sobre los parámetros de un tipo de monitor específico, consulte la descripción de ese tipo de monitor.

Para modificar un monitor existente mediante la CLI

En el símbolo del sistema, escriba:


```
set lb monitor <monitorName> <type> -interval <interval> -resptimeout <
    resptimeout>
<!--NeedCopy-->
```

Ejemplo:

```
set mon monitor-HTTP-1 HTTP -interval 50 milli
-resptimeout 20 milli
<!--NeedCopy-->
```

Para modificar un monitor existente mediante la GUI

Vaya a **Administración del tráfico > Equilibrio de carga > Monitores**y abra un monitor para modificarlo.

Habilitar e inhabilitar monitores

August 20, 2021

De forma predeterminada, los monitores enlazados a servicios y grupos de servicios están habilitados. Cuando habilita un monitor, el monitor comienza a sondear los servicios a los que está enlazado. Si inhabilita un monitor vinculado a un servicio, el estado en el que se determina el servicio mediante los otros monitores enlazados al servicio. Si el servicio está enlazado a un solo monitor y si inhabilita el monitor, el estado del servicio se determina mediante el monitor predeterminado.

Para habilitar un monitor mediante la CLI

En el símbolo del sistema, escriba:

```
enable lb monitor <monitorName>
<!--NeedCopy-->
```

Ejemplo:

```
enable lb mon monitor-HTTP-1
<!--NeedCopy-->
```


Para habilitar un monitor mediante la GUI

1. Vaya a **Administración del Tráfico > Equilibrio de carga > Monitores**.
2. Seleccione un monitor y, en la lista Acción, seleccione Activar o Desactivar.

Para inhabilitar un monitor mediante la CLI

En el símbolo del sistema, escriba:

```
disable lb monitor <monitorName>
<!--NeedCopy-->
```

Ejemplo:

```
disable lb mon monitor-HTTP-1
<!--NeedCopy-->
```

Desenlazar monitores

August 20, 2021

Puede desenlazar monitores de un servicio y un grupo de servicios. Cuando desvincula un monitor del grupo de servicios, los monitores se desvinculan de los servicios individuales que constituyen el grupo de servicios. Cuando desvincula un monitor de un servicio o un grupo de servicios, el monitor no sondea el servicio o el grupo de servicios.

Nota: Cuando desvincula todos los monitores configurados por el usuario de un servicio o un grupo de servicios, el monitor predeterminado está enlazado al servicio y al grupo de servicios. A continuación, los monitores predeterminados sondea el servicio o los grupos de servicios.

Para desenlazar un monitor de un servicio mediante la CLI

En el símbolo del sistema, escriba:

```
unbind lb monitor <monitorName>
<!--NeedCopy-->
```


Ejemplo:

```
unbind mon monitor-HTTP-1 Service-HTTP-1
<!--NeedCopy-->
```

Para desenlazar un monitor de un servicio mediante la GUI

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servicios**y abra un servicio para modificarlo.
2. Haga clic en la sección Monitores, seleccione un monitor y haga clic en **Desenlazar**.

Quitar monitores

August 20, 2021

Después de desenlazar un monitor creado de su servicio, puede quitarlo de la configuración de Citrix ADC. (Si un monitor está vinculado a un servicio, no se puede quitar).

Nota: Cuando quita monitores enlazados a un servicio, el monitor predeterminado está enlazado al servicio. No se pueden quitar los monitores predeterminados.

Para quitar un monitor mediante la CLI

En el símbolo del sistema, escriba:

```
rm lb monitor <monitorName> <type>
<!--NeedCopy-->
```

Ejemplo:

```
rm lb monitor monitor-HTTP-1 HTTP
<!--NeedCopy-->
```

Para quitar un monitor mediante la GUI

1. Vaya a **Administración del Tráfico > Equilibrio de carga > Monitores**.
2. Seleccione un monitor y haga clic en **Eliminar**.

Ver monitores

August 20, 2021

Puede ver los servicios y grupos de servicios enlazados a un monitor. Puede verificar la configuración de un monitor para solucionar problemas de la configuración de Citrix ADC. El procedimiento siguiente describe los pasos para ver los enlaces de un monitor a los servicios y grupos de servicios.

Para ver los enlaces de monitores mediante la CLI

En el símbolo del sistema, escriba:

```
show lb monbindings <MonitorName>
<!--NeedCopy-->
```

Ejemplo:

```
show lb monbindings monitor-HTTP-1
<!--NeedCopy-->
```

Para ver los enlaces de monitores mediante la GUI

1. Vaya a **Administración del Tráfico > Equilibrio de carga > Monitores**.
2. Seleccione un monitor y, en la lista Acción, haga clic en **Mostrar enlaces**.

Para ver monitores mediante la CLI

En el símbolo del sistema, escriba:

```
show lb monitor <monitorName>
<!--NeedCopy-->
```

Ejemplo:

```
show lb mon monitor-HTTP-1
<!--NeedCopy-->
```


Para ver monitores mediante la GUI

1. Vaya a **Administración del Tráfico > Equilibrio de carga > Monitores**. Los detalles de los monitores disponibles aparecen en el panel Monitores.

Cerrar conexiones de monitor

August 20, 2021

El dispositivo Citrix ADC envía sondeos a los servicios a través de los monitores enlazados a los servicios. De forma predeterminada, el monitor del dispositivo y el servidor físico siguen el procedimiento de enlace completo incluso para sondas de monitor. Sin embargo, este procedimiento agrega sobrecarga al proceso de supervisión y puede que no siempre sea necesario.

Para el monitor de tipo TCP, puede configurar el dispositivo para que cierre una conexión de sondeo de monitor después de recibir SYN-ACK del servicio. Para ello, establezca el valor del parámetro MonitorConnectionClose en RESET. Si quiere que la conexión del monitor y la sonda siga el procedimiento completo, establezca el valor en FIN.

Nota: La configuración MonitorConnectionClose es aplicable solo para monitores TCP y TCP predeterminados.

Para configurar el cierre de la conexión del monitor mediante la interfaz de línea de comandos:

En el símbolo del sistema, escriba:

```
set lb parameter -monitorConnectionClose <monitor_conn_close_option>
<!--NeedCopy-->
```

Ejemplo

```
set lb parameter -monitorConnectionClose RESET
<!--NeedCopy-->
```

Para configurar el cierre de la conexión del monitor mediante la utilidad de configuración:

1. Vaya a **Administración del tráfico > Equilibrio de carga > Configurar parámetros de equilibrio de carga**.
2. Seleccione **FIN** o **Restablecer**.

Cierre de conexiones de monitor en el nivel de servicio o grupo de servicios

También puede configurar el dispositivo para que cierre una conexión de sondeo de monitor en el nivel de servicio y grupo de servicios estableciendo el parámetro MonConnectionClose. Si no se establece este parámetro, la conexión del monitor se cierra mediante el valor establecido en los parámetros de equilibrio de carga global. Si este parámetro se establece en el nivel de servicio o grupo de servicios, la conexión del monitor se cierra enviando un mensaje de terminación de conexión, con el bit FIN o RESET establecido, al servicio o grupo de servicios.

Para configurar el cierre de la conexión del monitor en el nivel de servicio mediante la CLI

En el símbolo del sistema, escriba:

```
set service <service_name> -monConnectionClose ( RESET | FIN )
<!--NeedCopy-->
```

Para configurar el cierre de la conexión del monitor en el nivel de grupo de servicios mediante la CLI

En el símbolo del sistema, escriba:

```
 set serviceGroup <service_name> -monConnectionClose ( RESET | FIN )
<!--NeedCopy-->
```

Para configurar el cierre de la conexión del monitor en el nivel de servicio mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servicios**.
2. Agregue o modifique un servicio y, en **Configuración básica**, configure el **bit de cierre de conexión de supervisión**.

Para configurar el cierre de la conexión del monitor en el nivel de grupo de servicios mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Grupos de servicio**.
2. Agregue o modifique un grupo de servicios y, en **Configuración básica**, establezca el **bit de cierre de conexión de supervisión**.

> **Nota:** Para cerrar una conexión de monitor y sonda mediante parámetros de equilibrio de carga global, puede configurar MonitorConnectionClose en FIN o RESET. Al configurar el parámetro MonitorConnectionClose en;
>
> - FIN: El dispositivo realiza un protocolo de enlace TCP completo.
> - RESET: El dispositivo cierra la conexión después de recibir el SYN-ACK del servicio.
>
> En la versión más ligera de Citrix ADC CPX, el valor del parámetro MonitorConnectionClose se establece en RESET de forma predeterminada y no se puede cambiar a FIN a nivel global. Sin embargo, puede cambiar el parámetro MonitorConnectionClose a FIN en el nivel de servicio.

Ignorar el límite superior en las conexiones de cliente para sondeos de monitor

August 20, 2021

Dependiendo de consideraciones como la capacidad de un servidor físico, puede especificar un límite en el número máximo de conexiones de cliente realizadas a cualquier servicio. Si ha establecido dicho límite en un servicio, el dispositivo Citrix ADC deja de enviar solicitudes al servicio cuando se alcanza el umbral y reanuda el envío de conexiones al servicio después de que el número de conexiones existentes se encuentre dentro de los límites. Puede configurar el dispositivo para que omita esta comprobación cuando envía conexiones de sondeo de monitor a un servicio.

Nota: No puede omitir la comprobación de conexiones de cliente máximo para un servicio individual. Si especifica esta opción, se aplicará a todos los monitores enlazados a todos los servicios configurados en el dispositivo Citrix ADC.

Para configurar la opción Omitir MaxClients for Monitor Connections mediante la CLI

En el símbolo del sistema, escriba:

```
set lb parameter -monitorSkipMaxClient (ENABLED|DISABLED)
<!--NeedCopy-->
```

Ejemplo:

```
set lb parameter -monitorSkipMaxClient enabled
<!--NeedCopy-->
```


Para configurar la opción Omitir MaxClients for Monitor Connections mediante la GUI

1. Vaya a **Administración del tráfico > Equilibrio de carga > Configurar parámetros de equilibrio de carga**.
2. Seleccione **Omitir MaxClients para supervisar conexiones**.

Administrar una implementación a gran escala

August 20, 2021

El dispositivo Citrix ADC contiene varias funciones que resultan útiles cuando se configura una implementación de equilibrio de carga grande. En lugar de configurar servidores y servicios virtuales individualmente, puede crear grupos de servidores y servicios virtuales. También puede crear una variedad de servidores y servicios virtuales, y puede traducir o enmascarar direcciones IP de servidor virtual y servicio.

Puede establecer la persistencia para un grupo de servidores virtuales. Puede enlazar monitores a un grupo de servicios. La creación de una gama de servidores y servicios virtuales de idéntico tipo le permite configurar y configurar esos servidores en un solo procedimiento. Esto reduce significativamente el tiempo necesario para configurar esos servidores y servicios virtuales.

Al traducir o enmascarar direcciones IP, puede eliminar servidores y servicios virtuales. A continuación, puede realizar cambios en la infraestructura sin una reconfiguración exhaustiva de las definiciones de servicio y servidor virtual.

Rangos de servidores y servicios virtuales

August 20, 2021

Al configurar el equilibrio de carga, puede crear rangos de servidores y servicios virtuales, eliminando la necesidad de configurar servidores y servicios virtuales individualmente. Por ejemplo, puede utilizar un único procedimiento para crear tres servidores virtuales con tres direcciones IP correspondientes. Cuando más de un argumento utiliza un rango, los rangos deben ser del mismo tamaño.

Los siguientes son los tipos de rangos que puede especificar al agregar servicios y servidores virtuales a la configuración:

- **Rangos numéricos.** En lugar de escribir un solo número, puede especificar un rango de números consecutivos.

  Por ejemplo, puede crear un intervalo de servidores virtuales especificando una dirección IP inicial, como 10.102.29.30, y escribiendo un valor para el último byte que indique el rango, como

34. En este ejemplo, se crean cinco servidores virtuales con direcciones IP que oscilan entre 10.102.29.30 y 10.102.29.34.

    Nota: Las direcciones IP de los servidores y servicios virtuales deben ser consecutivas.

- **Rangos alfabéticos.** En lugar de escribir una letra literal, puede sustituir un rango por cualquier letra, por ejemplo, [C-G]. Esto da como resultado que se incluyan todas las letras del rango, en este caso C, D, E, F y G.

  Por ejemplo, si tiene tres servidores virtuales nombrados y `Vserver-xVserver-yVserver-z`, en lugar de configurarlos por separado, puede escribir `vserver [x-z]` para configurarlos todos.

Creación de una gama de servidores virtuales

Para crear una gama de servidores virtuales mediante la CLI

En el símbolo del sistema, escriba uno de los siguientes comandos:

```
add lb vserver <name>@ <protocol> -range <rangeValue> <IPAddress> [<port>]

add lb vserver <name>@[<rangeValue>]> <protocol> <IPAddress[<rangeValue>]> [<port>]
<!--NeedCopy-->
```

Ejemplo:

```
add lb vserver Vserver-LB-2 http -range 6 10.102.29.30 80
<!--NeedCopy-->
```

O BIEN

```
add lb vserver vserver[P-R] http 10.102.29.[26-28] 80

vserver ”vserverP” added

vserver ”vserverQ” added

vserver ”vserverR” added

```



```
9  Done
10 <!--NeedCopy-->
```

Para crear una gama de servidores virtuales mediante la CLI

En el símbolo del sistema, escriba uno de los siguientes comandos:

```
1 add lb vserver <name>@ <protocol> -range <rangeValue> <IPAddress> [<
     port>]
2
3 add lb vserver <name>@\*\*[\*\*<rangeValue>\*\*]\*\*> <protocol> <
     IPAddress[<rangeValue>]> [<port>]
4 <!--NeedCopy-->
```

Ejemplo:

```
1 add lb vserver Vserver-LB-2 http -range 6 10.102.29.30 80
2 <!--NeedCopy-->
```

O BIEN

```
1 add lb vserver vserver[P-R] http 10.102.29.[26-28] 80
2 vserver "vserverP" added
3 vserver "vserverQ" added
4 vserver "vserverR" added
5 Done
6 <!--NeedCopy-->
```

Para crear una gama de servidores virtuales mediante la GUI

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. Agregue un servidor virtual y especifique un rango.

Creación de una gama de servicios

Si especifica un rango para el nombre del servicio, especifique también un rango para la dirección IP.

Para crear una gama de servicios mediante la CLI

En el símbolo del sistema, escriba el comando:

```
add service <name>@ <IP>@ <protocol> <port>
<!--NeedCopy-->
```

Ejemplo:

```
> add service serv[1-3] 10.102.29.[102-104] http 80
service "serv1" added
service "serv2" added
service "serv3" added
 Done
<!--NeedCopy-->
```

Configurar grupos de servicios

August 20, 2021

La configuración de un grupo de servicios le permite administrar un grupo de servicios con la misma facilidad que un único servicio. Por ejemplo, si habilita o inhabilita cualquier opción, como compresión, supervisión de estado o apagado correcto, para un grupo de servicios, la opción se habilita para todos los miembros del grupo de servicios.

Después de crear un grupo de servicios, puede vincularlo a un servidor virtual y agregar servicios al grupo. También puede enlazar monitores a grupos de servicio.

Los miembros de un grupo de servicios se identifican por dirección IP o nombre de servidor.

El uso de miembros del grupo de servicios basados en nombres de dominio (DBS) es ventajoso porque no es necesario volver a configurar el miembro en el dispositivo Citrix ADC si cambia la dirección IP del miembro. El dispositivo detecta automáticamente dichos cambios a través del servidor de nombres configurado. Esta función resulta útil en casos de nube, en los que el proveedor de servicios puede cambiar un servidor físico o cambiar la dirección IP de un servicio. Si especifica un miembro del grupo DBS, el dispositivo aprende la dirección IP de forma dinámica.

Puede enlazar miembros basados en IP y DBS al mismo grupo de servicios.

Nota: Si utiliza miembros del grupo de servicios DBS, asegúrese de que se haya especificado un servidor de nombres o de que esté configurado un servidor DNS en el dispositivo Citrix ADC. Un nombre

de dominio se resuelve en una dirección IP solo si el registro de direcciones correspondiente está presente en el dispositivo o en el servidor de nombres.

Crear grupos de servicios

Puede configurar hasta 8192 grupos de servicios en el dispositivo Citrix ADC.

Para crear un grupo de servicios mediante la línea de comandos

En el símbolo del sistema, escriba:

```
add servicegroup <ServiceGroupName> <Protocol>
<!--NeedCopy-->
```

Ejemplo:

```
add servicegroup Service-Group-1 HTTP
<!--NeedCopy-->
```

Para crear un grupo de servicios mediante la utilidad de configuración

Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Grupos de servicio** y agregue un grupo de servicios.

Enlazar un grupo de servicios a un servidor virtual

Cuando vincula un grupo de servicios a un servidor virtual, los servicios miembros están enlazados al servidor virtual.

Para enlazar un grupo de servicios a un servidor virtual mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
bind lb vserver <name>@ <serviceGroupName>
<!--NeedCopy-->
```


Ejemplo:

```
bind lb vserver Vserver-LB-1 Service-Group-1
<!--NeedCopy-->
```

Para enlazar un grupo de servicios a un servidor virtual mediante la GUI

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**y abra un servidor virtual.
2. En Configuración avanzada, seleccione **Grupos de servicios**.

Vincular a un miembro a un grupo de servicios

Agregar servicios a un grupo de servicios permite que el grupo de servicios administre los servidores. Puede agregar los servidores a un grupo de servicios especificando las direcciones IP o los nombres de los servidores.

En la GUI, si desea agregar un miembro del grupo de servicios basado en nombres de dominio, seleccione **Basado en servidor**.

Con esta opción, puede agregar cualquier servidor al que se le haya asignado un nombre, independientemente de si el nombre es una dirección IP o un nombre asignado por el usuario.

Para agregar miembros a un grupo de servicios mediante la interfaz de línea de comandos

Para configurar un grupo de servicios, en el símbolo del sistema, escriba:

```
bind servicegroup <serviceGroupName> (<IP>@ | <serverName>) <port>
<!--NeedCopy-->
```

Ejemplos:

```
bind servicegroup Service-Group-1 10.102.29.30 80

bind servicegroup Service-Group-2 1000:0000:0000:0000:0005:0600:700a
    :888b 80

bind servicegroup CitrixEdu s1.citrite.net
<!--NeedCopy-->
```


Para agregar miembros a un grupo de servicios mediante la utilidad de configuración

1. Vaya a **Administración del tráfico > Equilibrio de carga > Grupos de servicios** y abra un grupo de servicios.
2. Haga clic en la sección Grupo de servicios y realice una de las acciones siguientes:
   - Para agregar un miembro del grupo de servicios basado en IP, seleccione Basado en IP.
   - Para agregar un miembro del grupo de servicios basado en nombre de servidor, seleccione Basado en servidor.

   Si quiere agregar un miembro del grupo de servicios basado en nombres de dominio, seleccione **Basado en servidor**. Con esta opción, puede agregar cualquier servidor al que se le haya asignado un nombre, independientemente de si el nombre es una dirección IP o un nombre asignado por el usuario.
3. Si agrega un nuevo miembro basado en IP, en el cuadro de texto Dirección IP, escriba la dirección IP. Si la dirección IP utiliza el formato IPv6, active la casilla de verificación IPv6 y, a continuación, escriba la dirección en el cuadro de texto Dirección IP

   Nota: Puede agregar un rango de direcciones IP. Las direcciones IP del intervalo deben ser consecutivas. Especifique el intervalo introduciendo la dirección IP inicial en el cuadro de texto Dirección IP (por ejemplo, 10.102.29.30). Especifique el byte final del intervalo de direcciones IP en el cuadro de texto bajo Rango (por ejemplo, 35). En el cuadro de texto Puerto, escriba el puerto (por ejemplo, 80) y, a continuación, haga clic en Agregar.
4. Haga clic en Crear.

Enlazar un monitor a un grupo de servicios

Al crear un grupo de servicios, el monitor predeterminado del tipo apropiado para el grupo se vincula automáticamente a él. Los monitores examinan periódicamente los servidores del grupo de servicios al que están enlazados y actualizan el estado de los grupos de servicios.

Puede vincular un monitor diferente de su propia elección al grupo de servicios.

Para enlazar un monitor a un grupo de servicios mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
bind serviceGroup <serviceGroupName> -monitorName <string> -monState (
    ENABLED | DISABLED)
<!--NeedCopy-->
```


Ejemplo:

```
bind serviceGroup Service-Group-1 -monitorName monitor-HTTP-1
<!--NeedCopy-->
```

Para un monitor de enlace a un grupo de servicios mediante la utilidad de configuración

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Grupos de servicio**.
2. Abra un grupo de servicios y, en Configuración avanzada, haga clic en **Monitores**.

Conservar el estado original de un miembro del grupo de servicios después de inhabilitar y habilitar un servidor virtual

Desde la compilación 64.x, una nueva opción global, —RetainDisableServer, le permite conservar el estado de un miembro del grupo de servicios cuando se inhabilita y vuelve a habilitar un servidor.

Anteriormente, el estado de un miembro cambiaba de DISABLED a ENABLED bajo el siguiente conjunto de condiciones:

- Dos aplicaciones se implementan en el mismo puerto en un servidor virtual.
- Dos grupos de servicios con un miembro común están enlazados a este servidor virtual, y el miembro común está habilitado en un grupo e inhabilitado en el otro.
- El servidor se inhabilita y, a continuación, se vuelve a habilitar.

En estas condiciones, inhabilitar el servidor inhabilita todos los miembros del grupo de servicios y volver a habilitar el servidor habilita a todos los miembros, de forma predeterminada, independientemente de sus estados anteriores. Para que los miembros vuelvan a los estados originales, debe inhabilitarlos manualmente en el grupo de servicios. Esta es una tarea engorrosa y propensa a errores.

Administrar grupos de servicios

October 5, 2021

Puede cambiar la configuración de los servicios de un grupo de servicios y realizar tareas como habilitar, inhabilitar y quitar grupos de servicios. También puede desvincular miembros de un grupo de servicios. Para obtener más información sobre los grupos de servicios, consulte Configurar grupos de servicios.

Modificar un grupo de servicios

Puede modificar los atributos de los miembros del grupo de servicios. Puede establecer varios atributos del grupo de servicios, como cliente máximo y compresión. Los atributos se establecen en los servidores individuales del grupo de servicios. No se pueden establecer parámetros en el grupo de servicios, como información de transporte (dirección IP y puerto), peso e ID de servidor.

Nota: Un parámetro configurado para un grupo de servicios se aplica a los servidores miembro del grupo, no a los servicios individuales.

Para modificar un grupo de servicios mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba el siguiente comando con uno o varios de los parámetros opcionales:

```
set servicegroup <serviceGroupName> [-type <type>] [-maxClient <
    maxClient>] [-maxReq <maxReq>] [-cacheable (YES|NO)] [-cip (ENABLED|
    DISABLED)] [-cipHeader <cipHeader>] [-usip (YES|NO)] [-sc (ON|OFF)]
    [-sp (ON|OFF)] [-cltTimeout <cltTimeout>] [-svrTimeout <svrTimeout>]
     [-cka (YES|NO)] [-TCPB (YES|NO)] [-CMP (\*\*YES\*\*|\*\*NO\*\*)] [-
    maxBandwidth <maxBandwidth>] [-maxThreshold <maxThreshold>] [-state
    (ENABLED|DISABLED)] [-downStateFlush (ENABLED|DISABLED)
<!--NeedCopy-->
```

Ejemplo:

```
set servicegroup Service-Group-1 -type TRANSPARENT

set servicegroup Service-Group-1 -maxClient 4096

set servicegroup Service-Group-1 -maxReq 16384

set servicegroup Service-Group-1 -cacheable YES
<!--NeedCopy-->
```

Para modificar un grupo de servicios mediante la utilidad de configuración

Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Grupos de servicios**y abra el grupo de servicios para modificarlo.

Eliminar un grupo de servicios

Al quitar un grupo de servicios, los servidores enlazados al grupo conservan su configuración individual y siguen existiendo en el dispositivo Citrix ADC.

Para quitar un grupo de servicios mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
rm servicegroup <ServiceGroupName>
<!--NeedCopy-->
```

Ejemplo:

```
rm servicegroup Service-Group-1
<!--NeedCopy-->
```

Para quitar un grupo de servicios mediante la utilidad de configuración

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Grupos de servicios**.
2. Seleccione un grupo de servicios y haga clic en **Eliminar**.

Desvincular a un miembro de un grupo de servicios

Al desvincular a un miembro del grupo de servicios, los atributos definidos en el grupo de servicios ya no se aplican al miembro que se ha desvinculado. Sin embargo, los servicios para miembros conservan su configuración individual y siguen existiendo en el dispositivo Citrix ADC.

Para desvincular miembros de un grupo de servicios mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
unbind servicegroup <serviceGroupName> <IP>@ [<port>]
<!--NeedCopy-->
```

Ejemplo:


```
unbind servicegroup Service-Group-1 10.102.29.30 80
<!--NeedCopy-->
```

Para desvincular miembros de un grupo de servicios mediante la utilidad de configuración

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Grupos de servicios**.
2. Abra un grupo de servicios y haga clic en la sección Miembros del grupo de servicios.
3. Seleccione un miembro del grupo de servicios y haga clic en **Desvincular**.

Desvincular un grupo de servicios de un servidor virtual

Al desenlazar un grupo de servicios de un servidor virtual, los servicios miembro no están vinculados al servidor virtual y siguen existiendo en el dispositivo Citrix ADC.

Para desenlazar un grupo de servicios de un servidor virtual mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
unbind lb vserver <name>@ <ServiceGroupName>
<!--NeedCopy-->
```

Ejemplo:

```
unbind lb vserver Vserver-LB-1 Service-Group-1
<!--NeedCopy-->
```

Para desenlazar un grupo de servicios de un servidor virtual mediante la utilidad de configuración

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**.
2. Abra el servidor virtual y haga clic en la sección Grupo de servicios.
3. Seleccione el grupo de servicios y haga clic en **Desvincular**.

Desvincular monitores de grupos de servicios

Al desvincular un monitor de un grupo de servicios, el monitor que se desvincula ya no supervisa los servicios individuales que constituyen el grupo.

Para desenlazar un monitor de un grupo de servicios mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
unbind serviceGroup <serviceGroupName> -monitorName <string>
<!--NeedCopy-->
```

Ejemplo:

```
unbind serviceGroup Service-Group-1 -monitorName monitor-HTTP-1
<!--NeedCopy-->
```

Para desenlazar un monitor de un grupo de servicios mediante la utilidad de configuración

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Grupos de servicios**.
2. Abra un grupo de servicios y haga clic en la sección Monitores.
3. Seleccione un monitor y haga clic en **Desenlazar**.

Habilitar o inhabilitar un grupo de servicios

Al habilitar un grupo de servicios y los servidores, se habilitan los servicios que pertenecen al grupo de servicios. Del mismo modo, cuando se habilita un servicio que pertenece a un grupo de servicios, el grupo de servicios y el servicio están habilitados. De forma predeterminada, los grupos de servicios están habilitados.

Después de inhabilitar un servicio habilitado, puede ver el servicio mediante la utilidad de configuración o la línea de comandos para ver el tiempo que queda antes de que el servicio se caiga.

Para inhabilitar un grupo de servicios mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
disable servicegroup <ServiceGroupName>
<!--NeedCopy-->
```

Ejemplo:


```
disable servicegroup Service-Group-1
<!--NeedCopy-->
```

Para inhabilitar un grupo de servicios mediante la utilidad de configuración

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Grupos de servicios**.
2. Seleccione un grupo de servicios y, en la lista Acción, haga clic en **Inhabilitar**.

Para habilitar un grupo de servicios mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
enable servicegroup <ServiceGroupName>
<!--NeedCopy-->
```

Ejemplo:

```
enable servicegroup Service-Group-1
<!--NeedCopy-->
```

Para habilitar un grupo de servicios mediante la utilidad de configuración

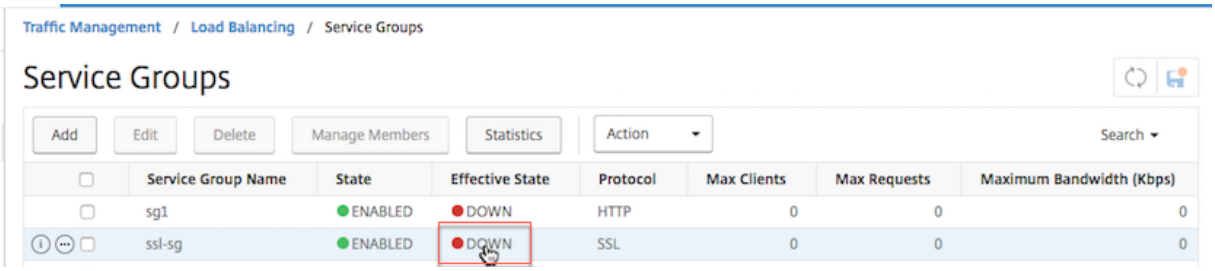
1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Grupos de servicios**.
2. Seleccione un grupo de servicios y, en la lista Acción, haga clic en **Habilitar**.

Ver el estado de los miembros de los grupos de servicios

Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Grupos de servicios**.

En la página Grupos de servicios, la columna **Estado efectivo** muestra el estado de los grupos de servicios. Se puede hacer clic en el **estado UP/DOWN de la columna Estado efectivo** . Puede hacer clic en el estado y obtener la lista de miembros junto con su estado en la misma vista. Seleccione un miembro y haga clic en el botón **Detalles del monitor** para ver el motivo por el que el estado está CAÍDA.

Nota: Antes de la versión 12.0 build 56.20 de NetScaler, no se podía hacer clic en el **estado de la columna Estado efectivo** .



Visualización de las propiedades de un grupo de servicios

Puede ver la siguiente configuración de los grupos de servicios configurados:

- Nombre
- Dirección IP
- State
- Protocolo
- Conexiones máximas de
- Número máximo de solicitudes por conexión
- Ancho de banda máximo
- Umbral de supervisión

Ver los detalles de la configuración puede ser útil para solucionar problemas de configuración.

Para ver las propiedades de un grupo de servicios mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba uno de los comandos siguientes para mostrar las propiedades del grupo o las propiedades y los miembros del grupo:

```
show servicegroup <ServiceGroupName>

show servicegroup <ServiceGroupName> -includemembers
<!--NeedCopy-->
```

Ejemplo:

```
show servicegroup Service-Group-1
<!--NeedCopy-->
```

Para ver las propiedades de un grupo de servicios mediante la utilidad de configuración

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Grupos de servicios**.

2. Haga clic en la flecha situada junto al grupo de servicios.

Visualización de las estadísticas de grupos

Puede ver datos estadísticos de grupos de servicios, como la tasa de solicitudes, respuestas, bytes de solicitud y bytes de respuesta. El dispositivo Citrix ADC utiliza las estadísticas de un grupo de servicios para equilibrar la carga de los servicios.

Para ver las estadísticas de un grupo de servicios mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
stat servicegroup <ServiceGroupName>
<!--NeedCopy-->
```

Ejemplo:

```
stat servicegroup Service-Group-1
<!--NeedCopy-->
```

Para ver las estadísticas de un grupo de servicios mediante la utilidad de configuración

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Grupos de servicios**.
2. Seleccione un grupo de servicios y haga clic en **Estadísticas**.

Servidores virtuales de equilibrio de carga enlazados a un grupo de servicios

En implementaciones a gran escala, el mismo grupo de servicios se puede enlazar a varios servidores virtuales de equilibrio de carga. En este caso, en lugar de ver cada servidor virtual para ver el grupo de servicios al que está enlazado, puede ver una lista de todos los servidores virtuales de equilibrio de carga enlazados a un grupo de servicios. Puede ver los siguientes detalles de cada servidor virtual:

- Nombre
- State
- Dirección IP
- Port

Para mostrar los servidores virtuales enlazados a un grupo de servicios mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba el siguiente comando para mostrar los servidores virtuales enlazados a un grupo de servicios:

```
show servicegroupbindings <serviceGroupName>
<!--NeedCopy-->
```

Ejemplo:

```
> show servicegroupbindings SVCGRPDTLS
SVCGRPDTLS - State :ENABLED
1) Test-pers (10.10.10.3:80) - State : DOWN
2) BRVSERV (10.10.1.1:80) - State : DOWN
3) OneMore (10.102.29.136:80) - State : DOWN
4) LBVIP1 (10.102.29.66:80) - State : UP
Done
>
<!--NeedCopy-->
```

Para mostrar los servidores virtuales enlazados a un grupo de servicios mediante la utilidad de configuración

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Grupos de servicios**.
2. Seleccione un grupo de servicios y, en la lista Acción, haga clic en **Mostrar enlaces**.

Configurar el conjunto deseado de miembros del grupo de servicios para un grupo de servicios en una llamada a la API de NITRO

April 21, 2022

Ahora se permite configurar un conjunto deseado de miembros de grupos de servicios para un grupo de servicios en una llamada a la API de NITRO. Se agrega una nueva API, la API de estado deseado, para admitir esta configuración. Con la API de estado deseado, puede:

- Proporcione una lista de los miembros del grupo de servicios en una sola solicitud PUT en el recurso “servicegroup_servicegroupmemberlist_binding”.

- Indique su peso y estado (opcional) en esa solicitud PUT.
- Sincronice eficazmente la configuración del dispositivo con los cambios de implementación en los servidores de aplicaciones.

El dispositivo Citrix ADC compara el conjunto de miembros deseado solicitado con el conjunto de miembros configurado. A continuación, vincula automáticamente a los nuevos miembros y desvincula a los miembros que no están presentes en la solicitud.

Nota:

- Esta función solo se admite para grupos de servicios de tipo `API`.
- Solo puede vincular servicios basados en direcciones IP mediante la API de estado deseado, no se permiten los servicios basados en nombres de dominio.
- Anteriormente, solo un miembro del grupo de servicios puede estar vinculado en una llamada NITRO.

> **Importante**
>
> La API de estado deseada para la membresía de ServiceGroup se admite en la implementación de clústeres Citrix ADC.

Caso de uso: sincronizar los cambios de implementación en el dispositivo Citrix ADC en implementaciones a gran escala, como Kubernetes

En implementaciones a gran escala y altamente dinámicas (por ejemplo, Kubernetes), el desafío es mantener la configuración del dispositivo actualizada con la velocidad de cambio de las implementaciones para atender con precisión el tráfico de las aplicaciones. En tales implementaciones, los controladores (Ingress o E-W Controller) son responsables de actualizar la configuración de ADC. Siempre que se produzcan cambios en la implementación, `kube-api server` envía el conjunto efectivo de puntos finales a través del "evento Endpoints" al controlador. El Controller utiliza el enfoque Read-Delta-Modify donde realiza lo siguiente:

- Obtiene el conjunto de puntos finales configurado actualmente (conjunto de miembros del grupo de servicios de un grupo de servicios) para el servicio desde el dispositivo ADC.
- Compara el conjunto de puntos finales configurados con el conjunto en el evento recibido.
- Enlaza los nuevos puntos finales (miembros del grupo de servicios) o desvincula los puntos finales eliminados.

Dado que la tasa de cambio y el tamaño de los servicios son altos en este entorno, este método de configuración no es eficiente y puede retrasar las actualizaciones de configuración.

La API de estado deseada resuelve el problema aceptando el conjunto de miembros previsto para un grupo de servicios en una única API y actualiza eficazmente la configuración.

Crear un grupo de servicios de tipo API mediante la CLI

En el símbolo del sistema, escriba;

```
add serviceGroup <serviceGroupName>@ <serviceType> [-autoScale <
    autoScale>]
```

Ejemplo:

```
add serviceGroup svg1 HTTP -autoScale API
```

Puede configurar los parámetros `autoDisablegraceful`, `autoDisabledelay` y `autoScale` mediante el comando add ServiceGroup o set ServiceGroup.

```
add serviceGroup <serviceGroupName>@ <serviceType> [-autoScale <
    autoScale>] [-autoDisablegraceful ( YES | NO)] [-autoDisabledelay <
    secs>]

add serviceGroup <serviceGroupName>@ <serviceType> [-autoScale (API |
    CLOUD | DISABLED| DNS |POLICY)]

set serviceGroup <serviceGroupName [-autoDisablegraceful ( YES | NO)]
    [-autoDisabledelay <secs>]

set serviceGroup <serviceGroupName [-autoScale (API |CLOUD | DISABLED|
    DNS |POLICY)]
```

Ejemplo:

```
add serviceGroup svg1 HTTP autoDisablegraceful YES -autoDisabledelay
    100

add serviceGroup svg1 HTTP -autoScale API

set serviceGroup svg1 -autoDisablegraceful  YES -autoDisabledelay 100

set serviceGroup svg1 -autoScale API
```


Argumentos

Desactivación automática de Graceful

Indica un cierre correcto del servicio. Si esta opción está habilitada, el dispositivo espera a que se cierren todas las conexiones pendientes a este servicio antes de eliminarlo. Para los clientes que ya tienen una sesión persistente en el sistema, se siguen enviando nuevas conexiones o solicitudes a este servicio. El miembro del servicio se elimina solo si no hay conexiones pendientes. Valor por defecto: NO

Retraso de desactivación automática

Indica el tiempo permitido (en segundos) para un apagado correcto. Durante este período, se siguen enviando nuevas conexiones o solicitudes a este servicio para los clientes que ya tienen una sesión persistente en el sistema. Las conexiones o solicitudes de nuevos clientes que no tienen sesiones persistentes en el sistema no se envían al servicio. En cambio, tienen equilibrio de carga entre otros servicios disponibles. Una vez transcurrido el tiempo de retraso, se elimina al miembro del servicio.

API de Autoscale

El argumento de la API de Autoscale permite usar la API de estado deseado para vincular el conjunto de miembros a un grupo de servicios deseado. Puede establecer el grupo de servicios de API de estado deseado que no sea de escalabilidad automática al tipo de escalabilidad automática, si todas las condiciones proporcionadas coinciden.

La API de estado deseada comprueba si la dirección IP del miembro del grupo de servicios está asociada a algún servidor existente. Si la dirección IP coincide con un servidor existente, la API reutiliza la dirección IP y el nombre del servidor existente. Si la dirección IP no coincide con ningún servidor existente, la API crea un servidor y asigna la dirección IP misma como el nombre del servidor.

Ejemplo:

Considere un servidor con dirección IP 2.2.2.2 y nombre como myserver que existe en un dispositivo Citrix ADC. Con la API de estado deseada, vincula un conjunto de miembros del grupo de servicios cuya dirección IP varía de 2.2.2.1 a 2.2.2.3.

Como la dirección IP 2.2.2.2 está asociada a un servidor existente, la API reutiliza la dirección IP y el nombre (2.2.2.2 y myserver). Como no hay servidores existentes con direcciones IP, 2.2.2.1, 2.2.2.3, la API crea servidores con estas direcciones IP. La API asigna la dirección IP en sí misma como el nombre del servidor.

Si la dirección IP proporcionada en el comando de estado deseado entra en conflicto con otras entidades de Citrix ADC, como el servidor virtual de CS, se produce un conflicto. Se muestra un mensaje de error que contiene el motivo del error. La dirección IP del primer miembro del grupo de servicios de la lista de miembros fallidos se muestra en el mensaje de error.

Ejemplo:

Considere un servidor con dirección IP 2.2.2.8 que se usa como servidor LB. Con la API de estado deseada, intenta vincular un conjunto de miembros del grupo de servicios cuya dirección IP varía entre 2.2.2.2 y 2.2.2.11.

Como 2.2.2.8 ya está en uso para el servicio LB, se produce un conflicto. Se muestra el siguiente mensaje de error que contiene el motivo del error y los enlaces de miembros fallidos:

```
{
  "errorcode": 304, "message": "Address already in use", "severity": "
     ERROR", "servicegroup_servicegroupmemberlist_binding": {
  "servicegroupname": "sg1", "failedmembers": [ {
  "ip": "2.2.2.8", "port": 80  }
 , {
  "ip": "2.2.2.9", "port": 80  }
  ]  }
   }

<!--NeedCopy-->
```

El código de error 304 muestra el primer miembro del grupo de servicios de la lista de miembros fallidos, que es 2.2.2.8.

El comando `set serviceGroup Autoscale` puede fallar si los enlaces de miembros existentes cumplen alguna de estas condiciones:

- Si el servidor enlazado al grupo de servicios es un servidor de nombres o un servidor basado en dominio.
- Si el nombre del servidor de bucle invertido no es 127.0.0.1 o 0000:0000:0000:0000:0000:0000:0000:0001.
- Si elige diferentes tipos de escalabilidad automática (nube, API, DNS y directiva) en un comando set ServiceGroup y agrega el comando ServiceGroup.

Importante:

- Los parámetros AutoDisableGraceful y AutoDisableDelay solo se aplican a los grupos de servicios de tipo Autoscale “API” y “CLOUD”.
- Si los parámetros AutoDisableGraceful o AutoDisableDelay no están configurados, los miembros del servicio se eliminan de inmediato.

Desvincular un miembro de un grupo de servicios correctamente

Si alguno de los miembros del grupo de servicios no se encuentra en la lista de estados deseada, esos miembros se desvinculan correctamente en función de la configuración de parámetros

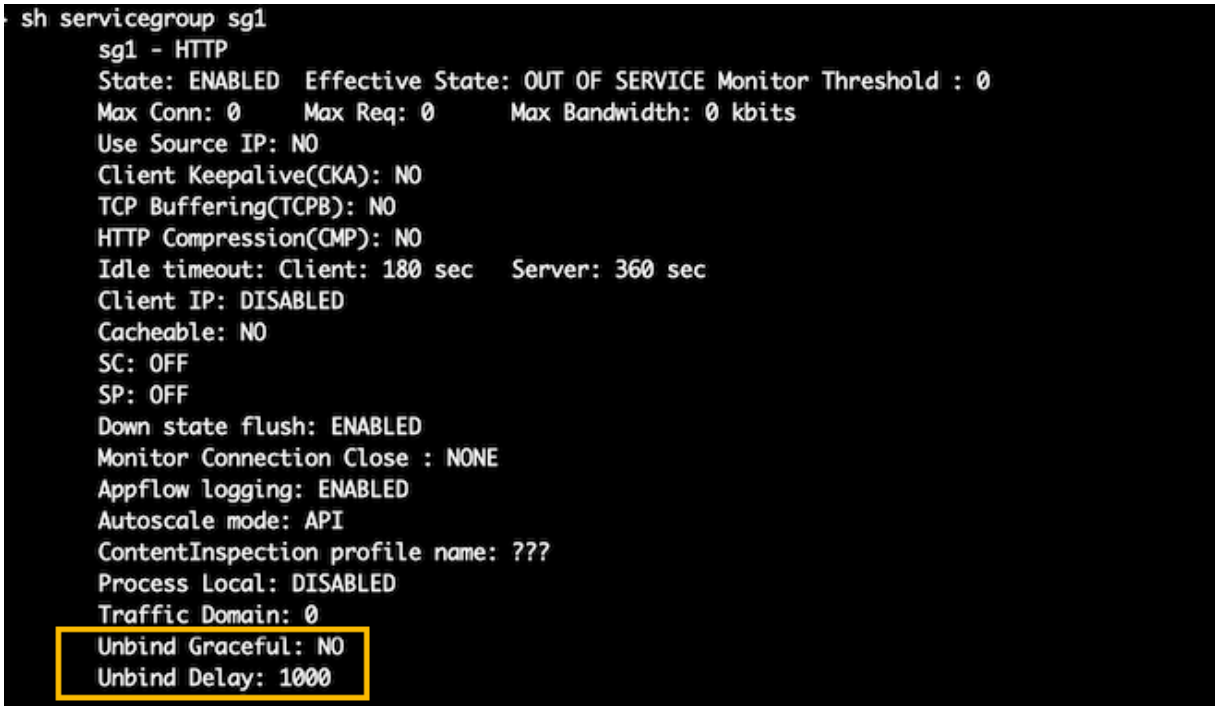
`autoDisablegraceful` o `autoDisabledelay`.

- Si se establece uno de estos parámetros, el miembro del grupo de servicios se desvincula correctamente.
- Si no se establece ninguno de estos parámetros, el miembro del grupo de servicios se desvincula inmediatamente.

Nota:

- Los miembros del grupo de servicios identificados para unbind graceful se muestran solo cuando se ejecuta el comando show service group.
- No puede realizar ninguna operación (como set, unset) en el miembro del grupo de servicios identificado para la desvinculación graciosa.

En la siguiente ilustración se muestra un ejemplo de comando show service group.

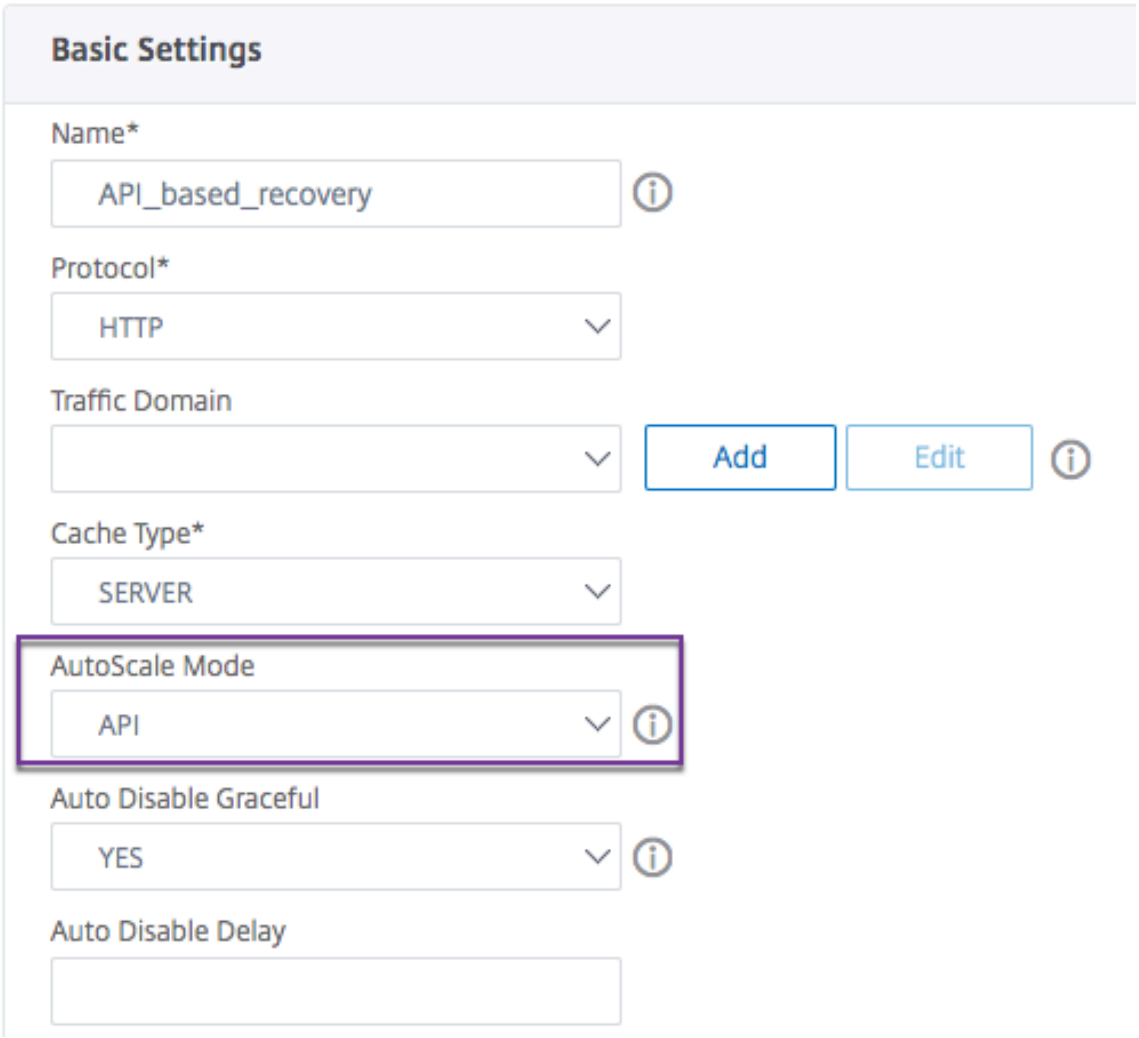


Crear un grupo de servicios de tipo API mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Grupos de servicios**y haga clic en **Agregar**.
2. En el **modo AutoScale**, seleccione **API**.

Configurar el apagado correcto o un retraso de tiempo para un grupo de servicios de tipo API mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Grupos de servicios**.



2. En el **modo AutoScale**, seleccione **API**.
3. En **Desactivación automática de Graceful**, seleccione **SÍ**.
4. En **Retraso de desactivación automática**, introduzca el tiempo de espera para un apagado correcto.

Nota: Los campos **Desactivación automática gradual** o **Retraso de visualización automática** solo están habilitados si selecciona **API** o **CLOUD** en el **modo AutoScale**.

Configurar el escalado automático de grupos de servicios basado en dominios

February 19, 2022

Un grupo de servicios basado en dominio consta de miembros cuyas direcciones IP se obtienen resolviendo los nombres de dominio de los servidores enlazados al grupo de servicios. Los nombres de dominio se resuelven mediante un servidor de nombres cuyos detalles se configuran en el dispositivo. Un grupo de servicios basado en dominios también puede incluir miembros basados en direcciones IP.

El proceso de resolución de nombres para un servidor basado en dominio puede devolver más de una dirección IP. El número de direcciones IP en la respuesta DNS viene determinado por el número de registros de direcciones (A) configurados para el nombre de dominio, en el servidor de nombres. Incluso si el proceso de resolución de nombres devuelve varias direcciones IP, solo una dirección IP está enlazada al grupo de servicios. Para ampliar o reducir la escala de un grupo de servicios, debe vincular y desvincular manualmente otros servidores basados en dominios hacia y desde el grupo de servicios, respectivamente.

Sin embargo, puede configurar un grupo de servicios basado en dominio para que escale automáticamente en función del conjunto completo de direcciones IP devueltas por un servidor de nombres DNS para un servidor basado en dominio. Para configurar el escalado automático, al vincular un servidor basado en dominio a un grupo de servicios, habilite la opción de escalado automático. Los siguientes son los pasos para configurar un grupo de servicios basado en dominio que escala automáticamente:

- Agregue un servidor de nombres para resolver nombres de dominio. Para obtener más información sobre la configuración de un servidor de nombres en el dispositivo, consulte Adición de un servidor de nombres.
- Agregue un servidor basado en dominio. Para obtener información sobre cómo agregar un servidor basado en dominio, consulte Configuración de un objeto de servidor.
- Agregue un grupo de servicios y asocie el servidor basado en dominio al grupo de servicios, con la opción Escalar automática establecida en DNS. Para obtener información sobre cómo agregar un grupo de servicios, consulte Configuración de grupos de servicios.

Cuando un servidor basado en dominio está enlazado a un grupo de servicios y la opción de escala automática se establece en el enlace, un monitor UDP y un monitor TCP se crean automáticamente y se vinculan al servidor basado en dominio. Los dos monitores funcionan como solucionadores. El monitor TCP está inhabilitado de forma predeterminada y el dispositivo utiliza el monitor UDP para enviar consultas DNS al servidor de nombres para resolver el nombre de dominio. Si la respuesta DNS se trunca (tiene el indicador TC establecido en 1), el dispositivo vuelve a TCP y utiliza el monitor TCP para enviar las consultas DNS a través de TCP. A partir de entonces, el dispositivo continúa mediante solo el monitor TCP.

La respuesta DNS del servidor de nombres puede contener varias direcciones IP para el nombre de dominio. Con la opción de escala automática establecida, el dispositivo sondea cada una de las direcciones IP mediante el monitor predeterminado y, a continuación, incluye en el grupo de servicios solo las direcciones IP que están activadas y disponibles. Después de que caduquen los registros de direcciones IP, según lo definido por sus valores de tiempo de vida (TTL), el monitor UDP (o el monitor

TCP, si el dispositivo ha vuelto a utilizar el monitor TCP) consulta al servidor de nombres para la resolución de dominio e incluye cualquier nueva dirección IP en el grupo de servicios. Si una dirección IP que forma parte del grupo de servicios no está presente en la respuesta DNS, el dispositivo quita esa dirección del grupo de servicios después de cerrar correctamente las conexiones existentes con el miembro del grupo, proceso durante el cual no permite establecer nuevas conexiones con el miembro. Si un nombre de dominio que se resolvió correctamente en el pasado da como resultado una respuesta NXDOMAIN, se quitan todos los miembros del grupo de servicios asociados a ese dominio.

Los miembros estáticos (basados en direcciones IP) y los miembros basados en dominios de escala dinámica pueden coexistir en un grupo de servicios. También puede enlazar miembros con diferentes nombres de dominio a un grupo de servicios con la opción de escala automática establecida. Sin embargo, cada nombre de dominio asociado a un grupo de servicios debe ser único dentro del grupo de servicios. Debe habilitar la opción de escala automática para cada servidor basado en dominio que quiera utilizar para escalar grupos de servicios automáticos. Si una dirección IP es común a uno o más dominios, la dirección IP se agrega al grupo de servicios solo una vez.

> **Importante**
>
> - La escala automática de DNS se admite en una implementación de clúster.
> - La supervisión de rutas para grupos de servicios de Escalado automático no se admite en la implementación de clústeres.

Para configurar un grupo de servicios para que escale automáticamente mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para configurar el grupo de servicios y verificar la configuración:

```
add serviceGroup <serviceGroupName> -autoScale (YES | NO)

show serviceGroup <serviceGroupName>
<!--NeedCopy-->
```

Ejemplo

En el ejemplo siguiente, server1 es un servidor basado en dominio. La respuesta DNS contiene varias direcciones IP. Cinco direcciones están disponibles y se agregan al grupo de servicios.

```
> add serviceGroup servGroup -autoScale YES
 Done
```



```
> sh servicegroup servGroup
        servGroup - HTTP
         State: ENABLED  Monitor Threshold : 0
               . . .
               . . .
         1)   192.0.2.31:80   State: UP       Server Name: server1 (Auto
              scale)    Server ID: None Weight: 1

                 Monitor Name: tcp-default       State: UP
                 Probes: 2       Failed [Total: 0 Current: 0]
                 Last response: Success - TCP syn+ack received.

         2)   192.0.2.32:80   State: UP       Server Name: server1 (Auto
              scale)    Server ID: None Weight: 1

                 Monitor Name: tcp-default       State: UP
                 Probes: 2       Failed [Total: 0 Current: 0]
                 Last response: Success - TCP syn+ack received.

         3)   192.0.2.36:80   State: UP       Server Name: server1 (Auto
              scale)    Server ID: None Weight: 1

                 Monitor Name: tcp-default       State: UP
                 Probes: 2       Failed [Total: 0 Current: 0]
                 Last response: Success - TCP syn+ack received.

         4)   192.0.2.55:80   State: UP       Server Name: server1 (Auto
              scale)    Server ID: None Weight: 1

                 Monitor Name: tcp-default       State: UP
                 Probes: 2       Failed [Total: 0 Current: 0]
                 Last response: Success - TCP syn+ack received.

         5)   192.0.2.80:80   State: UP       Server Name: server1 (Auto
              scale)    Server ID: None Weight: 1

                 Monitor Name: tcp-default       State: UP
                 Probes: 2       Failed [Total: 0 Current: 0]
                 Last response: Success - TCP syn+ack received.
 Done
<!--NeedCopy-->
```


Para configurar un grupo de servicios para que escale automáticamente mediante la utilidad de configuración

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Grupos de servicios**.
2. Cree un grupo de servicios y establezca el modo de escala automática en DNS.

Sobrescribir valores TTL

> **Nota:**
>
> Esta opción se admite en Citrix ADC 12.1 compilación 51.xx y posteriores.

El dispositivo Citrix ADC está configurado para consultar periódicamente al servidor DNS cualquier actualización del registro SRV asociado a la aplicación durante el inicio de la aplicación. De forma predeterminada, la periodicidad de esta consulta depende del TTL publicado en el registro SRV. En aplicaciones de microservicios o cloud world, las implementaciones cambian más dinámicamente. Como resultado, los proxies tienen que ser más rápidos en la absorción de cualquier cambio en la implementación de aplicaciones. Por lo tanto, se recomienda a los usuarios establecer explícitamente el parámetro TTL del servicio basado en dominio en un valor que sea menor que el TTL del registro SRV y que sea óptimo para su implementación. Puede sobrescribir el valor TTL por dos métodos:

- Al vincular a un miembro al grupo de servicios
- Establecer el valor TTL globalmente mediante el comando set lb parameter.

En caso de que el valor TTL esté configurado tanto al vincular al miembro del grupo de servicios como también a nivel global, prevalece el valor TTL especificado al vincular al miembro del grupo de servicios.
Si el valor TTL no se especifica mientras se vincula a un miembro del grupo de servicios o en el nivel global, el intervalo del monitor DBS se deriva del valor TTL en la respuesta DNS.

Sobrescribir los valores TTL mediante la CLI

- Para sobrescribir el valor TTL mientras se vincula, en el símbolo del sistema, escriba:

```
bind serviceGroup <serviceGroupName> (<serverName> [-dbsTTL <secs
   >])
<!--NeedCopy-->
```

Ejemplo:

```
bind servicegroup svc_grp_1 web_serv -dbsTTL 10
<!--NeedCopy-->
```


- Para sobrescribir el valor TTL globalmente, en el símbolo del sistema, escriba:

```
set lb parameter [-dbsTTL <secs>]
<!--NeedCopy-->
```

Ejemplo:

```
set lb parameter -dbsTTL 15
<!--NeedCopy-->
```

Sobrescribir los valores TTL mediante la GUI

Para sobrescribir el valor TTL mientras se vincula:

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Grupos de servicios**.
2. En la página **Grupos de servicios**, seleccione el grupo de servicios que ha creado y haga clic en **Modificar**.
3. En la página **Grupos de servicio de equilibrio de carga**, haga clic en **Miembros del grupo de servicios**.
4. En la página **Enlace de miembros del grupo de servicios**, seleccione el servidor que ha creado y haga clic en **Modificar**.
5. En **Domain Based Service TTL**, introduzca el valor TTL.

Para sobrescribir el valor TTL en el nivel global:

1. Acceda a **Administración del tráfico** > **Equilibrio de carga** > **Cambiar Parámetros de Equilibrio de carga**.
2. En **Domain Based Service TTL**, introduzca el valor TTL.

> **Nota:**
>
> Si el valor TTL del servidor basado en dominio se establece en 0, se utilizará el valor TTL del paquete de datos.

Especificar servidores de nombres diferentes para enlaces de nombres de dominio y grupos de servicios

> **Nota:**

> Esta opción se admite en Citrix ADC 12.1 compilación 51.xx y posteriores.

Puede configurar diferentes servidores de nombres para diferentes nombres de dominio en un grupo específico. Establecer el parámetro nameServer es opcional mientras se vincula un servidor DBS al grupo de servicios. Cuando no se especifica un servidor de nombres mientras se vincula a un miembro al grupo de servicios, se considera el servidor de nombres configurado globalmente.

Especificar servidores de nombres al vincular un servidor a grupos de servicios mediante la CLI

En el símbolo del sistema, escriba:

```
bind serviceGroup <serviceGroupName> (<serverName> [-nameServer <
    ip_addr>] [-dbsTTL <secs>])
<!--NeedCopy-->
```

Ejemplo:

```
bind servicegroup svc_grp_1 web_serv  -ns.nameserver.com 10.102.27.155
    -dbsTTL 10
<!--NeedCopy-->
```

Especificar servidores de nombres al enlazar un servidor a grupos de servicios mediante la GUI

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Grupos de servicios**.
2. En la página **Grupos de servicios**, seleccione el grupo de servicios que ha creado y haga clic en **Modificar**.
3. En la página **Grupos de servicio de equilibrio de carga**, haga clic en **Miembros del grupo de servicios**.
4. En la página **Enlace de miembros del grupo de servicios**, seleccione el servidor que ha creado y haga clic en **Modificar**.
5. En **Servidor**de nombres, especifique el nombre del servidor de nombres al que debe enviarse la consulta del dominio enlazado.

Detección de servicios mediante registros DNS SRV

August 20, 2021

Un registro SRV (registro de servicio) es una especificación de datos en el sistema de nombres de dominio que define la ubicación, es decir, el nombre de host y el número de puerto de los servidores para los servicios especificados. El registro también define el peso y la prioridad de cada servidor.

Ejemplo de registro SRV:

_http._tcp.example.com. 100 IN SRV 10 60 5060 a.example.com.

La siguiente tabla describe cada elemento de un registro SRV:

Service	Protocol	Name	TTL	Class	SRV	Priority	Weight	Port	Target
HTTP	TCP	example.com	100	IN	SRV	10	60	5060	a.example.com

Puede utilizar los registros SRV DNS para descubrir los extremos de servicio. El dispositivo Citrix ADC está configurado para consultar periódicamente los servidores DNS con el registro SRV asociado a un servicio. Al recibir el registro SRV, cada host de destino publicado en el registro SRV está enlazado a un grupo de servicios asociado al servicio. Cada uno de los enlaces hereda el puerto, la prioridad y el peso del registro SRV. Para cada implementación de servicio, el usuario debe configurar el dispositivo Citrix ADC una vez mientras lo levanta, lo que lo convierte en una implementación de un solo toque para las aplicaciones.

Importante: El peso de los miembros del grupo de servicios aprendidos dinámicamente no se puede modificar mediante la CLI o la GUI.

Caso de uso: Microservicios de equilibrio de carga

Las aplicaciones se están moviendo hacia la arquitectura de microservicios desde arquitecturas monolíticas. El movimiento hacia la arquitectura de microservicios junto con la solución de escala automática de servidores back-end hace que la implementación de aplicaciones sea más dinámica. Para admitir una implementación dinámica de este tipo, los proxies o el ADC deben poder detectar dinámicamente las instancias de servicio o aplicación back-end y absorberlas en la configuración del proxy.
La función de detección de servicios mediante registros SRV de DNS ayuda a configurar el dispositivo Citrix ADC en un caso de implementación dinámico de este tipo. Los desarrolladores de aplicaciones pueden utilizar algunas de las plataformas de orquestación para implementar la aplicación. Es posible que las plataformas de orquestación mientras se crean instancias de contenedores durante la implementación de aplicaciones no asignen el puerto estándar específico del protocolo para cada uno de estos contenedores. En tales situaciones, descubrir la información del puerto se convierte en la clave para configurar el dispositivo Citrix ADC. Los registros SRV son útiles en tal caso. Los

parámetros de registro SRV, como la prioridad y el peso, se pueden utilizar para un mejor equilibrio de carga de las aplicaciones.

- El parámetro Priority se puede utilizar para dictar la prioridad del grupo de servidores.
- El parámetro de peso se puede utilizar para dictar la capacidad de las instancias de servicio back-end y, por lo tanto, se puede utilizar para el equilibrio de carga ponderada.
- Cada vez que hay un cambio en el grupo de servidores back-end, por ejemplo, se quita una instancia back-end del grupo, la instancia se elimina gentilmente solo después de que se cumplan todas las conexiones de cliente existentes.

> **Nota:**
>
> - Una detección de servicio basada en registros A/AAAA, todas las direcciones IP resueltas tienen el mismo peso porque asigna el peso al dominio que se está resolviendo.
> - Si el peso en la respuesta SRV es mayor que 100, entonces los servicios no se crean.

Equilibrio de carga basado en prioridad mediante registros SRV

Puede utilizar registros SRV para realizar el equilibrio de carga basado en prioridades. El grupo de servidores basado en prioridades puede ser una alternativa para los servidores virtuales de backup. El archivo ns.conf requiere una configuración mínima en comparación con los servidores virtuales de backup.

En el equilibrio de carga basado en prioridades mediante registros SRV, se asigna un número de prioridad a cada uno de los servidores. El menor número tiene la prioridad más alta. Uno de los servidores del grupo de prioridad más alta se selecciona para el equilibrio de carga en función del estado y la disponibilidad del servidor. Si todos los servidores del grupo de servidores de prioridad más alta están inactivos, los servidores que tienen la siguiente prioridad más alta se seleccionan para el equilibrio de carga. Sin embargo, si los servidores del grupo de servidores de prioridad más alta están activos de nuevo, los servidores se seleccionan de nuevo del grupo de prioridad más alta.

El cambio de un grupo de servidores de prioridad a otro grupo de servidores se produce graciosamente al purgar las transacciones de cliente existentes. Por lo tanto, los clientes actuales no ven ninguna interrupción en el acceso a la aplicación.

Para habilitar la consulta de registros SRV mediante la CLI

Realice las siguientes tareas para habilitar la consulta de registros SRV:

1. Cree un servidor especificando el parámetro de tipo de consulta como SRV.

   En el símbolo del sistema, escriba:


```
add server <name> <domain> [-queryType <queryType>])
<!--NeedCopy-->
```

Ejemplo:

```
add server web_serv example.com -queryType SRV
<!--NeedCopy-->
```

Nota:

- De forma predeterminada, se envían consultas IPv4. Para enviar consultas IPv6, debe habilitar el dominio IPv6.
- El nombre de dominio de destino SRV no debe superar los 127 caracteres.

2. Cree un grupo de servicios con el modo de escala automática como DNS.

   En el símbolo del sistema, escriba:

```
add serviceGroup <serviceGroupName> <serviceType> [-autoScale <
    autoScale>]
<!--NeedCopy-->
```

Ejemplo:

```
add servicegroup svc_grp_1 http -autoscale dns
<!--NeedCopy-->
```

3. Enlazar el servidor creado en el paso 1 al grupo de servicios como miembro.

   En el símbolo del sistema, escriba:

```
bind serviceGroup <serviceGroupName> <serverName>
<!--NeedCopy-->
```

Ejemplo:

```
bind servicegroup svc_grp_1 web_serv
<!--NeedCopy-->
```

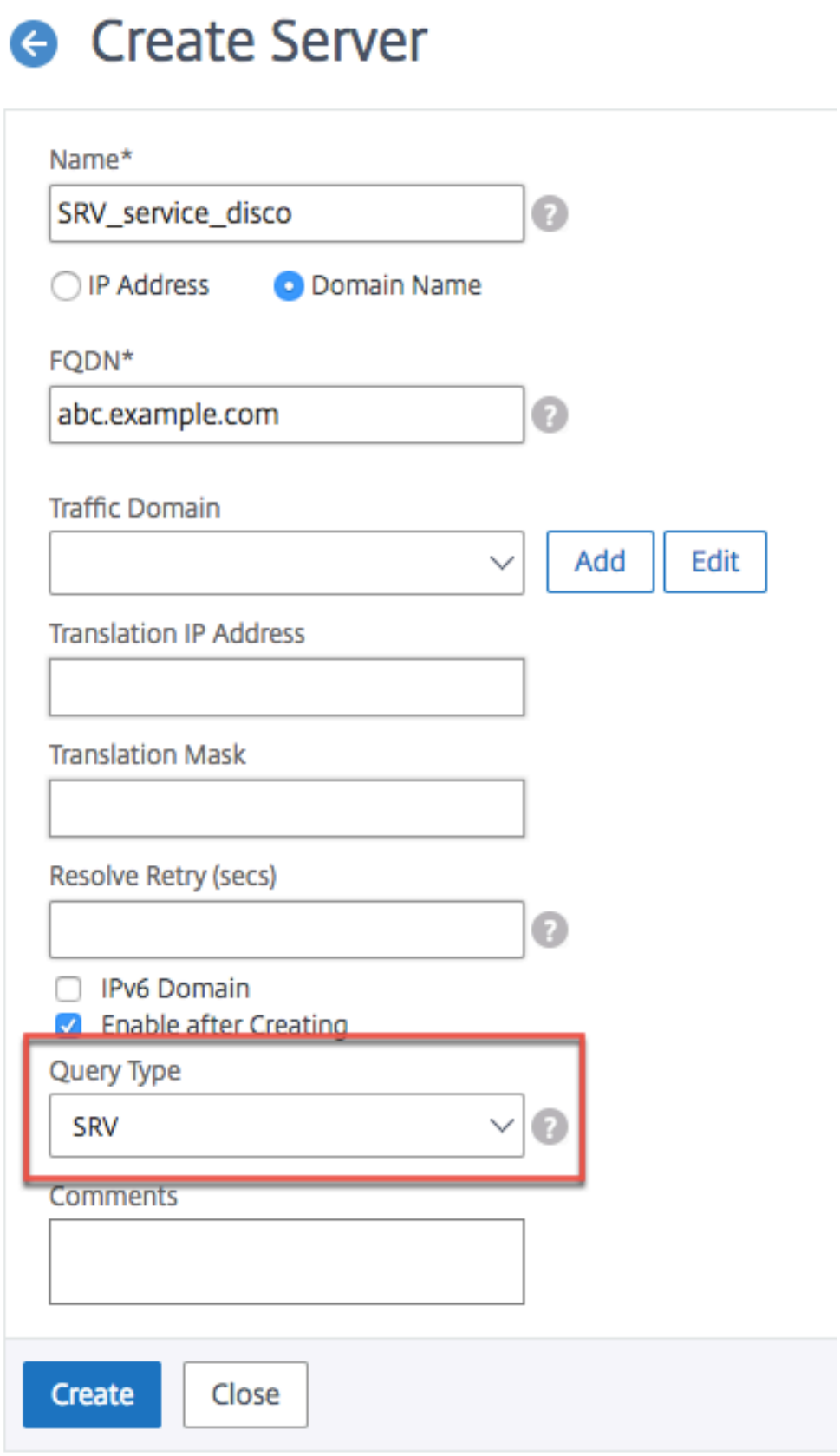

Nota:

- Al vincular servidores a miembros del grupo de servicios, no es necesario especificar el número de puerto para los tipos de servidor SRV. En caso de que especifique un número de puerto para el tipo de servidor SRV, aparecerá un mensaje de error.
- Opcionalmente, puede especificar un servidor de nombres y un valor TTL mientras se vincula un servidor al grupo de servicios.

Para habilitar la consulta de registros SRV mediante la interfaz gráfica de usuario

Crear un servidor

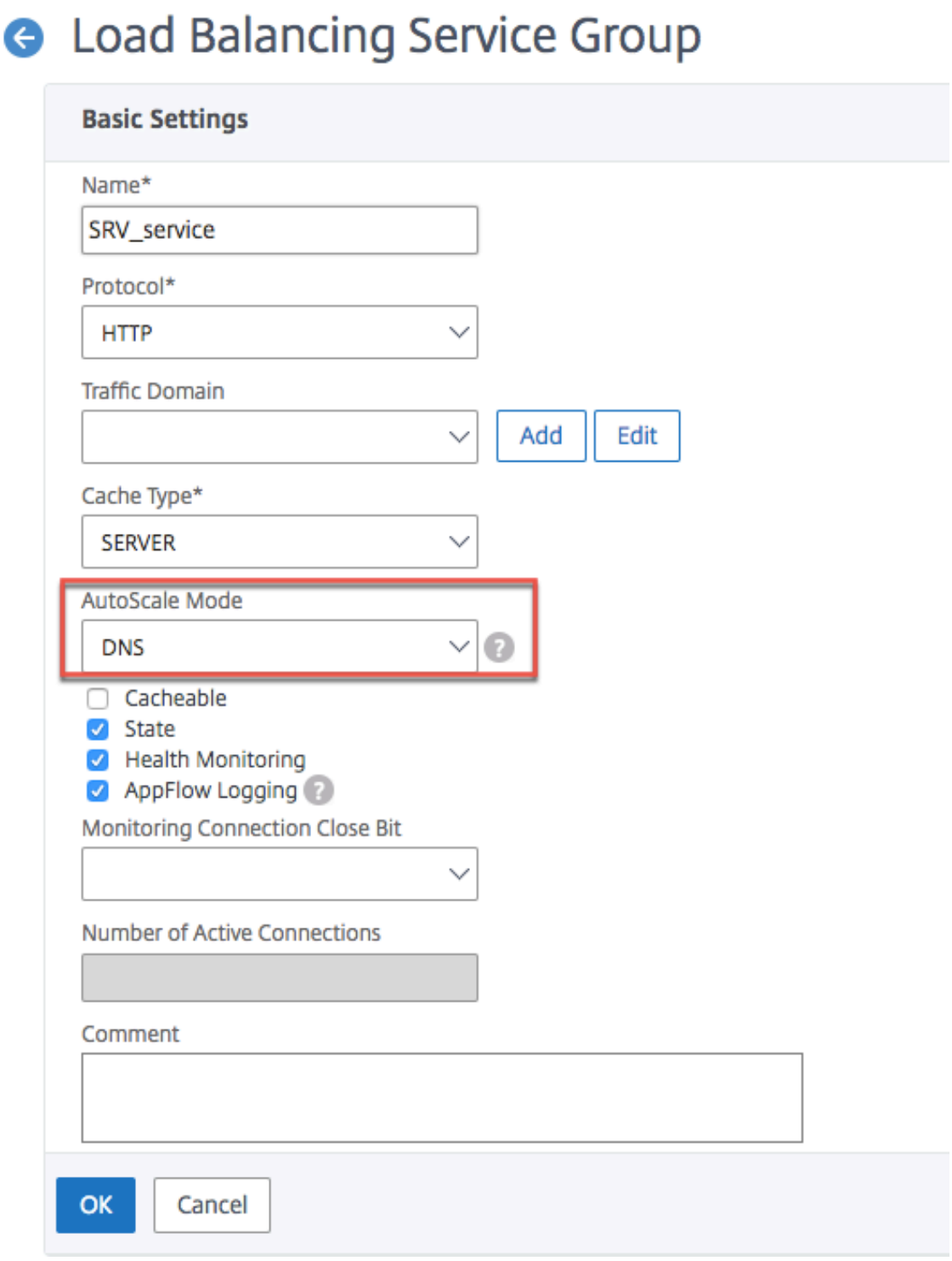
1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores** y haga clic en **Agregar**.



2. En la página **Crear servidor**, seleccione nombre de dominio.
3. Introduzca los detalles de todos los parámetros requeridos.
4. En **Tipo de consulta**, seleccione **SRV**.
5. Haga clic en **Crear**.

Crear un grupo de servicios con el modo de escala automática como DNS

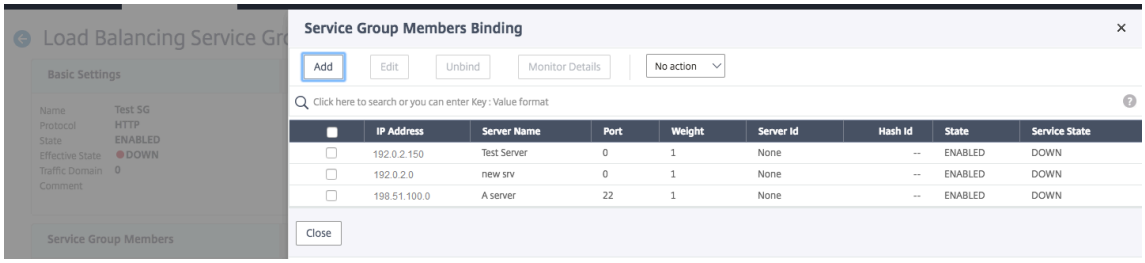
1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Grupos de servicio**.
2. En la página **Grupo de servicio de equilibrio de carga**, introduzca los detalles de todos los parámetros necesarios.
3. En **Modo de Autoscale**, seleccione **DNS**.



4. Haga clic en **Aceptar**.

Vincular el servidor al miembro del grupo de servicios

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Grupos de servicio**.
2. En la página **Grupos de servicios**, seleccione el grupo de servicios que ha creado y haga clic en **Modificar**.
3. En la página **Grupos de servicio de equilibrio de carga**, haga clic en **Miembros del grupo de servicios**.
4. En la página **Enlace de miembros del grupo de servicios**, seleccione el servidor que ha creado y haga clic en **Cerrar**.



Nota:

- Durante el enlace, no es necesario introducir el número de puerto para los tipos de servidor SRV. En caso de que introduzca un número de puerto para el tipo de servidor SRV, aparecerá un mensaje de error.
- Opcionalmente, puede especificar un servidor de nombres y un valor TTL mientras se vincula un servidor al grupo de servicios.

Sobrescribir valores TTL

El dispositivo Citrix ADC está configurado para consultar periódicamente al servidor DNS cualquier actualización del registro SRV asociado a la aplicación durante el inicio de la aplicación. De forma predeterminada, la periodicidad de esta consulta depende del TTL publicado en el registro SRV. En aplicaciones de microservicios o cloud world, las implementaciones cambian más dinámicamente. Como resultado, los proxies tienen que ser más rápidos en la absorción de cualquier cambio en la implementación de aplicaciones. Por lo tanto, se recomienda a los usuarios establecer explícitamente el parámetro TTL del servicio basado en dominio en un valor que sea menor que el TTL del registro SRV y que sea óptimo para su implementación. Puede sobrescribir el valor TTL por dos métodos:

- Al vincular a un miembro al grupo de servicios
- Establecer el valor TTL globalmente mediante el comando set lb parameter.

En caso de que el valor TTL esté configurado tanto al vincular al miembro del grupo de servicios como también a nivel global, prevalece el valor TTL especificado al vincular al miembro del grupo de servicios.
Si el valor TTL no se especifica mientras se vincula a un miembro del grupo de servicios o en el nivel global, el intervalo del monitor DBS se deriva del valor TTL en la respuesta DNS.

Sobrescribir los valores TTL mediante la CLI

- Para sobrescribir el valor TTL mientras se vincula, en el símbolo del sistema, escriba:

```
bind serviceGroup <serviceGroupName> (<serverName> [-dbsTTL <secs
    >])
<!--NeedCopy-->
```

Ejemplo:

```
bind servicegroup svc_grp_1 web_serv -dbsTTL 10
<!--NeedCopy-->
```

- Para sobrescribir el valor TTL globalmente, en el símbolo del sistema, escriba:

```
set lb parameter [-dbsTTL <secs>]
<!--NeedCopy-->
```

Ejemplo:

```
set lb parameter -dbsTTL 15
<!--NeedCopy-->
```

Sobrescribir los valores TTL mediante la GUI

Para sobrescribir el valor TTL mientras se vincula:

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Grupos de servicio**.
2. En la página **Grupos de servicios**, seleccione el grupo de servicios que ha creado y haga clic en **Modificar**.
3. En la página **Grupos de servicio de equilibrio de carga**, haga clic en **Miembros del grupo de servicios**.
4. En la página **Enlace de miembros del grupo de servicios**, seleccione el servidor que ha creado y haga clic en **Modificar**.
5. En **Domain Based Service TTL**, introduzca el valor TTL.

Para sobrescribir el valor TTL en el nivel global:

1. Acceda a **Administración del tráfico** > **Equilibrio de carga** > **Cambiar Parámetros de Equilibrio de carga**.
2. En **Domain Based Service TTL**, introduzca el valor TTL.

> **Nota**: Si el valor TTL del servidor basado en dominio se establece en 0, se utiliza el valor TTL del paquete de datos.

Especificar servidores de nombres diferentes para enlaces de nombres de dominio y grupos de servicios

Puede configurar diferentes servidores de nombres para diferentes nombres de dominio en un grupo específico. Establecer el parámetro NameServer es opcional mientras se vincula un servidor DBS al grupo de servicios. Cuando no se especifica un servidor de nombres mientras se vincula a un miembro al grupo de servicios, se considera el servidor de nombres configurado globalmente.

Especificar servidores de nombres al vincular un servidor a grupos de servicios mediante la CLI

En el símbolo del sistema, escriba:

```
bind serviceGroup <serviceGroupName> (<serverName> [-nameServer <
    ip_addr>] [-dbsTTL <secs>])
<!--NeedCopy-->
```

Ejemplo:

```
bind servicegroup svc_grp_1 web_serv  -ns.nameserver.com 10.102.27.155
    -dbsTTL 10
<!--NeedCopy-->
```

Especificar servidores de nombres al enlazar un servidor a grupos de servicios mediante la GUI

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Grupos de servicio**.
2. En la página **Grupos de servicios**, seleccione el grupo de servicios que ha creado y haga clic en **Modificar**.
3. En la página **Grupos de servicio de equilibrio de carga**, haga clic en **Miembros del grupo de servicios**.
4. En la página **Enlace de miembros del grupo de servicios**, seleccione el servidor que ha creado y haga clic en **Modificar**.

5. En **Servidor**de nombres, especifique el nombre del servidor de nombres al que debe enviarse la consulta del dominio enlazado.

Traducir la dirección IP de un servidor basado en dominio

August 20, 2021

Para simplificar el mantenimiento en el dispositivo Citrix ADC y en los servidores basados en dominios que están conectados a él, puede configurar máscaras de direcciones IP y direcciones IP de traducción. Estas funciones funcionan juntas para analizar los paquetes DNS entrantes y sustituir una nueva dirección IP por una dirección IP resuelta por DNS.

Cuando se configura para un servidor basado en dominio, la traducción de direcciones IP permite al dispositivo localizar una dirección IP de servidor alternativo cuando desactiva el servidor para su mantenimiento o si realiza cualquier otro cambio de infraestructura que afecte al servidor.

Al configurar la máscara, debe usar valores de máscara IP estándar (una potencia de dos, menos uno) y ceros, por ejemplo, 255.255.0.0. Los valores distintos de cero solo se permiten en los octetos iniciales.

Al configurar una dirección IP de traducción para un servidor, se crea una correspondencia 1:1 entre una dirección IP del servidor y un servidor alternativo que comparte octetos iniciales o finales en su dirección IP. La máscara bloquea octetos concretos en la dirección IP del servidor original. La dirección IP con resolución DNS se transforma en una nueva dirección IP aplicando la dirección IP de traducción y la máscara de traducción.

Por ejemplo, puede configurar una dirección IP de traducción 10.20.0.0 y una máscara de traducción 255.255.0.0. Si una dirección IP resuelta por DNS para un servidor es 40.50.27.3, esta dirección se transforma a 10.20.27.3. En este caso, la dirección IP de traducción proporciona los dos primeros octetos de la nueva dirección y la máscara pasa a través de los dos últimos octetos de la dirección IP original. Se pierde la referencia a la dirección IP original, según lo resuelto por DNS. Los monitores de todos los servicios a los que el servidor está vinculado también informan sobre la dirección IP transformada.

Al configurar una dirección IP de traducción para un servidor basado en dominio, especifique una máscara y una dirección IP a la que se va a traducir la dirección IP con resolución DNS.

Nota: La traducción de la dirección IP solo es posible para servidores basados en dominios. No puede utilizar esta función para servidores basados en IP. El patrón de direcciones puede basarse únicamente en direcciones IPv4.

Para configurar una dirección IP de traducción para un servidor mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:


```
add server <name>@ <serverDomainName> -translationIp <
    translationIPAddress> -translationMask <netMask> -state <ENABLED|
    DISABLED>
<!--NeedCopy-->
```

Ejemplo:

```
add server myMaskedServer www.example.com -translationIp 10.10.10.10 -
    translationMask
255.255.0.0 -state ENABLED
<!--NeedCopy-->
```

Para configurar una dirección IP de traducción para un servidor mediante la utilidad de configuración

Vaya a **Administración del tráfico > Equilibrio de carga > Servidores**, cree un servidor basado en dominio y especifique una dirección IP de traducción.

Enmascarar la dirección IP de un servidor virtual

October 5, 2021

Puede configurar una máscara y un patrón en lugar de una dirección IP fija para un servidor virtual. Esto permite que el tráfico que se dirige a cualquiera de las direcciones IP que coinciden con la máscara y el patrón se redirija a un servidor virtual concreto. Por ejemplo, puede configurar una máscara que permita que los tres primeros octetos de una dirección IP sean variables, de modo que el tráfico a 111.11.11.198, 22.22.22.198 y 33.33.33.198 se envíe al mismo servidor virtual.

Al configurar una máscara para una dirección IP de servidor virtual, puede evitar la reconfiguración de sus servidores virtuales debido a un cambio en la redirección u otro cambio en la infraestructura. La máscara permite que el tráfico continúe fluyendo sin una reconfiguración extensa de sus servidores virtuales.

La máscara de la dirección IP de un servidor virtual funciona de forma diferente a la definición de un patrón IP para un servidor descrito en Traducción de la dirección IP de un servidor basado en dominio. Para una máscara de dirección IP de servidor virtual, una máscara distinta de cero se interpreta como un octeto que se considera. Para un servicio, se bloquea el valor distinto de cero.

Además, para una máscara de dirección IP de servidor virtual, se pueden considerar valores iniciales o finales. Si la máscara de dirección IP del servidor virtual considera los valores de la izquierda de la dirección IP, se conoce como máscara de reenvío. Si la máscara considera los valores situados a la derecha de la dirección, esto se conoce como máscara inversa.

Nota: El dispositivo Citrix ADC evalúa todos los servidores virtuales de máscara directa antes de evaluar los servidores virtuales de máscara inversa.

Al enmascarar la dirección IP de un servidor virtual, también debe crear un patrón de dirección IP para hacer coincidir el tráfico entrante con el servidor virtual correcto. Cuando el dispositivo recibe un paquete IP entrante, hace coincidir la dirección IP de destino del paquete con los bits que se consideran en el patrón de dirección IP y, una vez que encuentra una coincidencia, aplica la máscara de dirección IP para construir la dirección IP de destino final.

Considere el siguiente ejemplo:

- Dirección IP de destino en el paquete entrante: 10.102.27.189
- Patrón de dirección IP: 10.102.0.0
- Máscara IP: 255.255.0.0
- Dirección IP de destino construida (final): 10.102.27.189.

En este caso, los primeros 16 bits de la dirección IP de destino original coinciden con el patrón de dirección IP de este servidor virtual, por lo que este paquete entrante se redirige a este servidor virtual.

Si una dirección IP de destino coincide con los patrones IP de más de un servidor virtual, prevalecerá la coincidencia más larga. Considere el siguiente ejemplo:

- Servidor virtual 1: patrón de IP 10.10.0.0, máscara IP 255.255.0.0
- Servidor virtual 2: patrón de IP 10.10.10.0, máscara IP 255.255.255.0
- Dirección IP de destino en el paquete: 10.10.10.45.
- Servidor virtual seleccionado: Servidor virtual 2.

El patrón asociado con Virtual Server 2 coincide con más bits que el asociado con Virtual Server 1, por lo que las IP que coinciden con él se envían al servidor virtual 2.

Nota: Los puertos también se consideran si se requiere un desempate.

Para configurar una máscara de dirección IP de servidor virtual mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
1 add lb vserver <name>@ http -ipPattern <ipAddressPattern> -ipMask <
     ipMask> <listenPort>
2 <!--NeedCopy-->
```


Ejemplo:

Coincidencia de patrones basada en octetos de prefijo:

```
add lb vserver myLBVserver http -ippattern 10.102.0.0 -ipmask
   255.255.0.0 80
<!--NeedCopy-->
```

Coincidencia de patrones basada en octetos finales:

```
add lb vserver myLBVserver1 http -ippattern 0.0.22.74 -ipmask
   0.0.255.255 80
<!--NeedCopy-->
```

Modificar un servidor virtual basado en patrones:

```
set lb vserver myLBVserver1 -ippattern 0.0.22.74 -ipmask 0.0.255.255
<!--NeedCopy-->
```

Si configura el servidor virtual 1 de la siguiente manera:

```
add lb vserver vs1 HTTP -ippattern 100.1.1.0 -ipmask 255.255.255.0 80
<!--NeedCopy-->
```

El dispositivo Citrix ADC no responderá a una solicitud ARP en todas las direcciones IP. Sin embargo, responde al tráfico del servidor virtual redirigido a todas las direcciones IP de ese patrón.

Para configurar una máscara de dirección IP de servidor virtual mediante la utilidad de configuración

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. En la lista Tipo de dirección, seleccione Patrón IP y especifique un patrón IP y una máscara IP.

Configurar el equilibrio de carga para los protocolos de uso común

August 20, 2021

Además de los sitios web y las aplicaciones basadas en web, otros tipos de aplicaciones implementadas en red que utilizan otros protocolos comunes suelen recibir grandes cantidades de tráfico y, por lo tanto, se benefician del equilibrio de carga. Varios de estos protocolos requieren configuraciones específicas para que el equilibrio de carga funcione correctamente. Entre ellos se encuentran FTP, DNS, SIP y RTSP.

Si configura el dispositivo Citrix ADC para que use nombres de dominio para sus servidores en lugar de IP, es posible que también tenga que configurar la traducción y el enmascaramiento de IP para esos servidores.

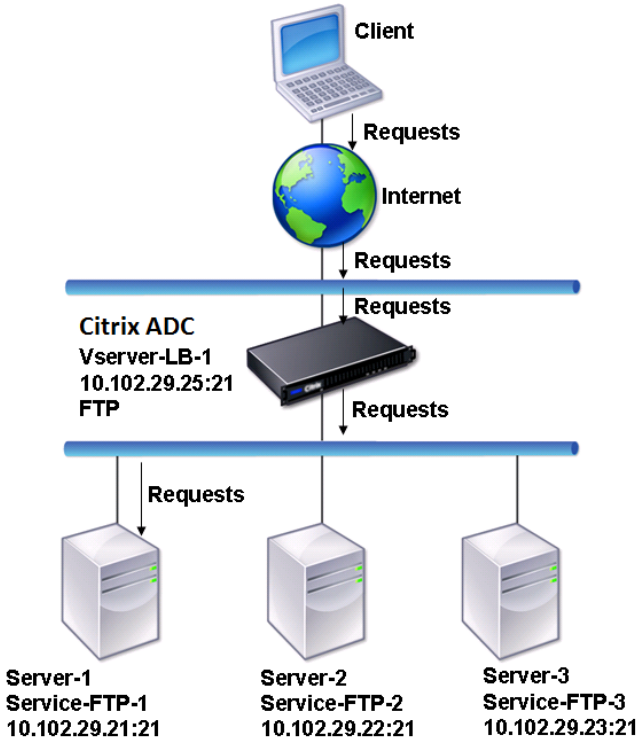
Equilibrio de carga de un grupo de servidores FTP

August 20, 2021

El dispositivo Citrix ADC se puede utilizar para equilibrar la carga de servidores FTP. FTP requiere que el usuario inicie dos conexiones en dos puertos diferentes al mismo servidor: La conexión de control, a través de la cual el cliente envía comandos al servidor, y la conexión de datos, a través de la cual el servidor envía datos al cliente. Cuando el cliente inicia una sesión FTP abriendo una conexión de control al servidor FTP, el dispositivo utiliza el método de equilibrio de carga configurado para seleccionar un servicio FTP y reenvía la conexión de control a él. A continuación, el servidor FTP equilibrado de carga abre una conexión de datos al cliente para el intercambio de información.

En el siguiente diagrama se describe la topología de una configuración de equilibrio de carga para un grupo de servidores FTP.

Ilustración 1. Topología básica de equilibrio de carga para servidores FTP



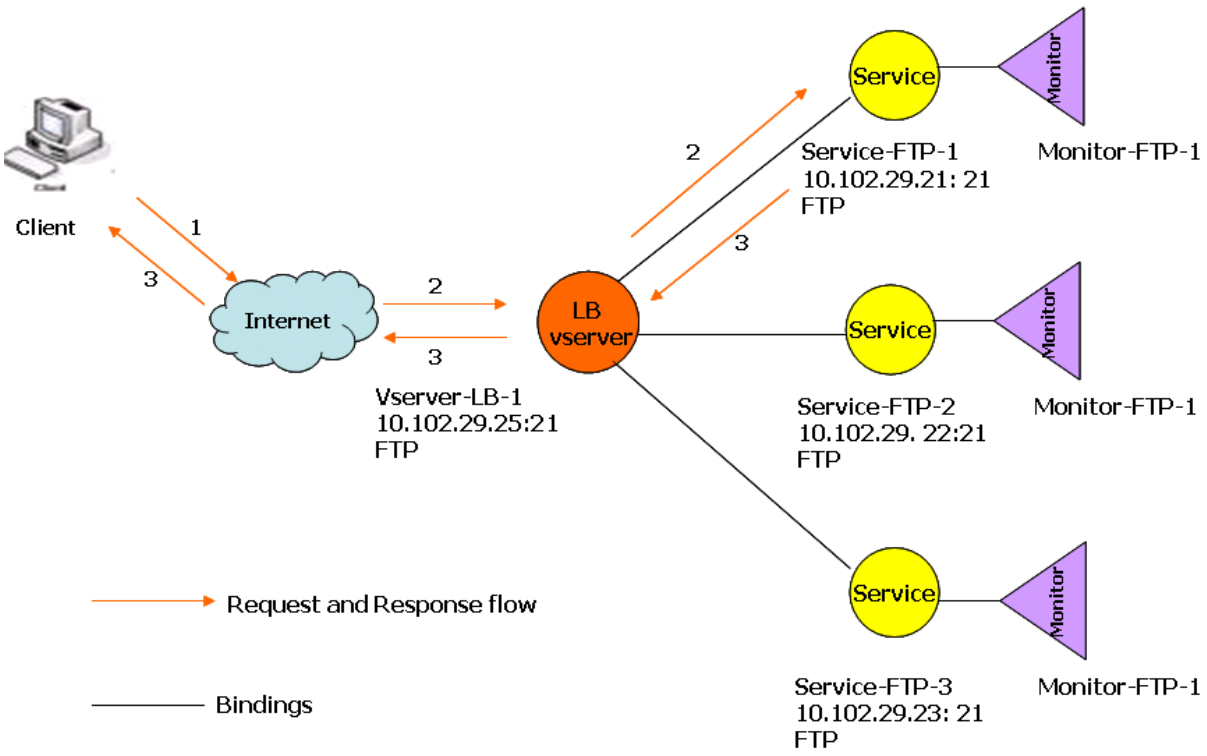
En el diagrama, los servicios Service-FTP-1, Service-FTP-2 y Service-FTP-3 están enlazados al servidor virtual VServer-LB-1. VServer-LB-1 reenvía la solicitud de conexión del cliente a uno de los servicios mediante el método de equilibrio de carga de conexión mínimo. Las solicitudes posteriores se reenvían al servicio que el dispositivo seleccionó inicialmente para el equilibrio de carga.

En la tabla siguiente se enumeran los nombres y valores de las entidades básicas configuradas en el dispositivo.

Tipo de entidad	Nombre	Dirección IP	Port	Protocolo
Vserver	Vserver-LB-1	10.102.29.25	21	FTP
Servicios	Service-FTP-1	10.102.29.21	21	FTP
	Service-FTP-2	10.102.29.22	21	FTP
	Service-FTP-3	10.102.29.23	21	FTP
Monitores	FTP	Ninguno	Ninguno	Ninguno

El siguiente diagrama muestra las entidades de equilibrio de carga y los valores de los parámetros que deben configurarse en el dispositivo.

Ilustración 2. Modelo de entidad de servidores FTP de equilibrio de carga



El dispositivo también puede proporcionar una opción FTP pasiva para acceder a servidores FTP desde fuera de un firewall. Cuando un cliente utiliza la opción FTP pasivo e inicia una conexión de control con el servidor FTP, el servidor FTP también inicia una conexión de control con el cliente. A continuación, inicia una conexión de datos para transferir un archivo a través del firewall.

Para crear servicios y servidores virtuales de tipo FTP, consulte Configuración del equilibrio de carga básico. Asigne un nombre a las entidades y establezca los parámetros en los valores descritos en las columnas de la tabla anterior. Cuando configura una configuración básica de equilibrio de carga, un monitor predeterminado está enlazado a los servicios.

A continuación, vincule el monitor FTP a los servicios siguiendo el procedimiento descrito en la sección Vinculación de monitores a servicios.

Para crear monitores FTP mediante la CLI

En el símbolo del sistema, escriba:

```
add lb monitor <MonitorName> FTP -interval <Interval> -userName <
    UserName> -password <Password>
<!--NeedCopy-->
```


Ejemplo:

```
add lb monitor monitor-FTP-1 FTP -interval 360 -userName User -password
    User
<!--NeedCopy-->
```

Para crear monitores FTP mediante la GUI

1. Vaya a **Administración del Tráfico > Equilibrio de carga > Monitores**.
2. Cree un monitor de tipo FTP y, en Parámetros especiales, especifique un nombre de usuario y una contraseña.

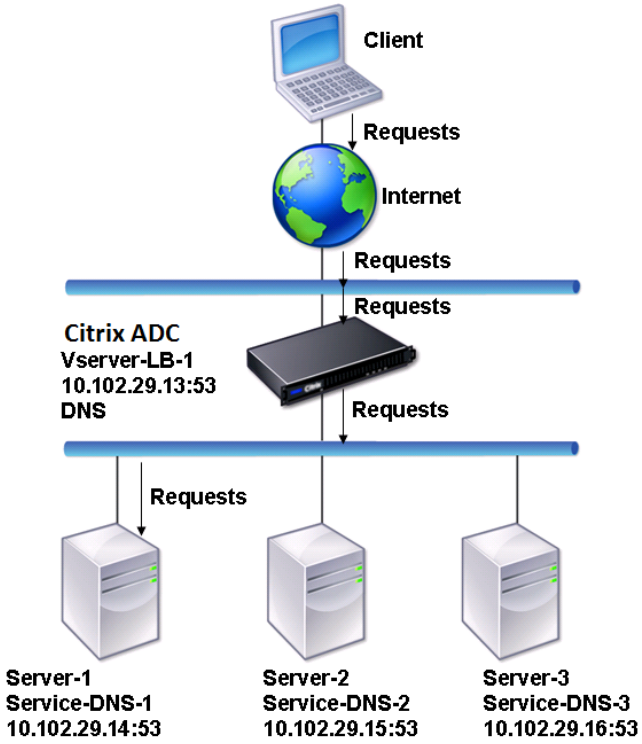
Servidores DNS de equilibrio de carga

August 20, 2021

Cuando solicita la resolución DNS de un nombre de dominio, el dispositivo Citrix ADC utiliza el método de equilibrio de carga configurado para seleccionar un servicio DNS. El servidor DNS al que está enlazado el servicio resuelve el nombre de dominio y devuelve la dirección IP como respuesta. El dispositivo también puede almacenar en caché las respuestas DNS y utilizar la información almacenada en caché para responder a futuras solicitudes de resolución del mismo nombre de dominio. Los servidores DNS de equilibrio de carga mejoran los tiempos de respuesta DNS.

En el siguiente diagrama se describe la topología de una configuración de equilibrio de carga que equilibra la carga un grupo de servicios DNS.

Ilustración 1. Topología básica de equilibrio de carga para servidores DNS

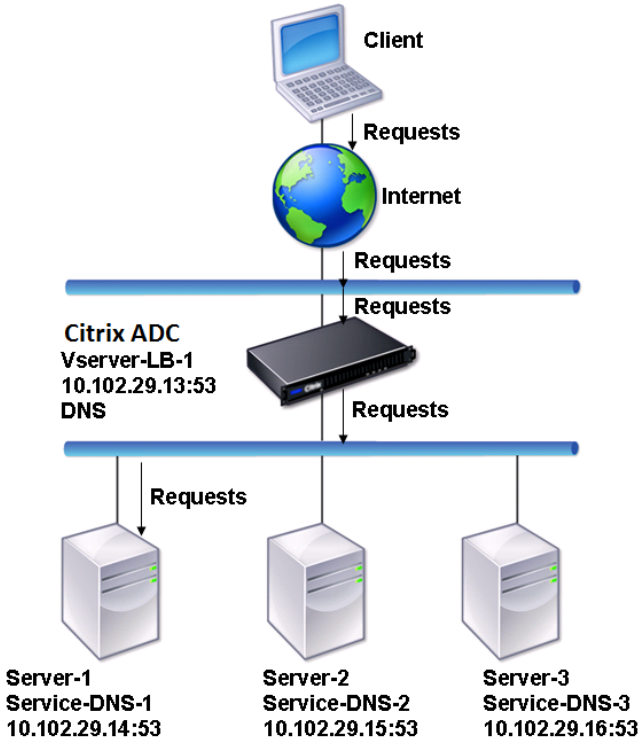


En el diagrama, los servicios Service-DNS-1, Servicio-DNS-2 y Servicio-DNS-3 están enlazados al servidor virtual VServer-LB-1. El servidor virtual VServer-LB-1 reenvía las solicitudes de cliente a un servicio mediante el método de equilibrio de carga de conexión mínimo. En la tabla siguiente se enumeran los nombres y valores de las entidades básicas configuradas en el dispositivo.

Tipo de entidad	Nombre	Dirección IP	Port	Protocolo
Servidor virtual	Vserver-LB-1	10.102.29.13	53	DNS
Servicios	Service-DNS-1	10.102.29.14	53	DNS
	Service-DNS-2	10.102.29.15	53	DNS
	Service-DNS-3	10.102.29.16	53	DNS
Monitores	monitor-DNS-1	Ninguno	Ninguno	Ninguno

El siguiente diagrama muestra las entidades de equilibrio de carga y los valores de los parámetros que deben configurarse en el dispositivo.

Ilustración 2. Modelo de entidad de servidores DNS de equilibrio de carga



Para configurar una configuración básica de equilibrio de cargas DNS, consulte Configuración del equilibrio de carga básico. Siga los procedimientos para crear servicios y servidores virtuales de tipo DNS, nombrando las entidades y estableciendo los parámetros mediante los valores descritos en la tabla anterior. Al configurar una configuración básica de equilibrio de carga, el monitor de ping predeterminado está enlazado a los servicios. Para obtener instrucciones sobre cómo vincular un monitor DNS a servicios DNS, también puede consultar Vinculación de monitores a servicios.
El procedimiento siguiente describe los pasos para crear un monitor que asigne un nombre de dominio a la dirección IP en función de una consulta.

Para configurar monitores DNS mediante la CLI

En el símbolo del sistema, escriba:

```
1 add lb monitor <monitorName> DNS -query <domainName> -queryType <
     Address|ZONE> -IPAddress <ipAddress>
2 <!--NeedCopy-->
```

Ejemplo:


```
1 add lb monitor monitor-DNS-1 DNS -query www.citrix.com -queryType
     Address -IPAddress 10.102.29.66
2
3 add lb monitor monitor-DNS-2 DNS -query www.citrix2.com -queryType
     Address -IPAddress
4 1000:0000:0000:0000:0005:0600:700a::888b-888d
5 <!--NeedCopy-->
```

Para configurar monitores DNS mediante la GUI

1. Vaya a **Administración del Tráfico > Equilibrio de carga > Monitores**.
2. Cree un monitor de tipo DNS y, en Parámetros especiales, especifique una consulta y un tipo de consulta.

Servicios basados en nombres de dominio de equilibrio de carga

August 20, 2021

Cuando crea un servicio para el equilibrio de carga, puede proporcionar una dirección IP. Alternativamente, puede crear un servidor mediante un nombre de dominio. El nombre del servidor (nombre de dominio) se puede resolver mediante un servidor de nombres IPv4 o IPv6, o agregando un registro DNS autorizado (Un registro para IPv4 o AAAA para IPv6) a la configuración de Citrix ADC.

Cuando configura servicios con nombres de dominio en lugar de direcciones IP, y si el servidor de nombres resuelve el nombre de dominio en una nueva dirección IP, el monitor vinculado al servicio ejecuta una comprobación de estado en la nueva dirección IP y actualiza la dirección IP del servicio solo cuando se encuentra que la dirección IP está en buen estado. El monitor puede ser el monitor predeterminado vinculado al servicio o puede enlazar cualquier otro monitor compatible. Sondea el servicio a intervalos regulares definidos en los parámetros del monitor. Si el nombre de dominio se resuelve en una nueva dirección IP, el monitor envía un nuevo sondeo para comprobar el estado del servicio. Todos los sondeos posteriores se encuentran en el intervalo predefinido.

Nota: Cuando cambia la dirección IP de un servidor, el servicio correspondiente se marca hacia abajo para la primera solicitud del cliente. El servidor de nombres resuelve la dirección IP del servicio en la dirección IP modificada para la siguiente solicitud y el servicio se marca como UP.

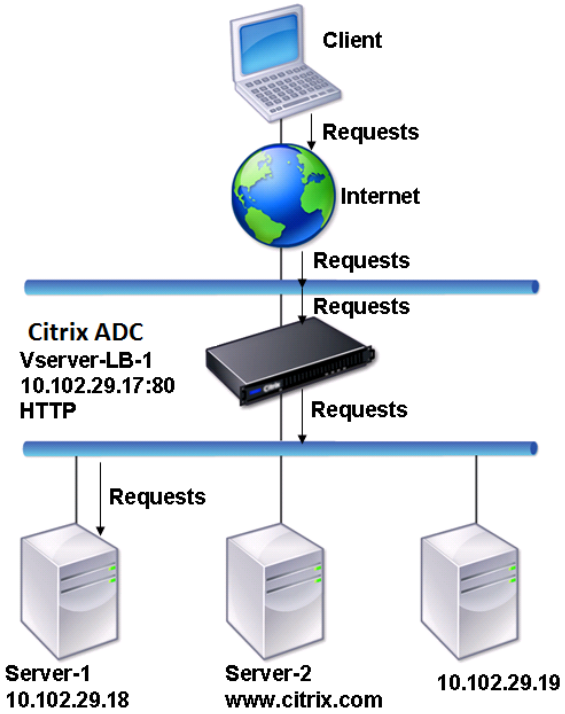
Los servicios basados en nombres de dominio tienen las siguientes restricciones:

- La longitud máxima del nombre de dominio es 255 caracteres.

- El parámetro Maximum Client se utiliza para configurar un servicio que representa el servidor basado en nombres de dominio. Por ejemplo, se establece un MaxClient de 1000 para los servicios enlazados a un servidor virtual. Cuando el recuento de conexiones en el servidor virtual alcanza 2000, el solucionador DNS cambia la dirección IP de los servicios. Sin embargo, dado que el contador de conexión del servicio no se restablece, el servidor virtual no puede tomar ninguna conexión nueva hasta que se cierren todas las conexiones antiguas.
- Cuando la dirección IP del servicio cambia, la persistencia es difícil de mantener.
- Si la resolución del nombre de dominio falla debido a un tiempo de espera, el dispositivo utiliza la información anterior (dirección IP).
- Cuando la supervisión detecta que un servicio está inactivo, el dispositivo realiza una resolución DNS en el servicio (que representa el servidor basado en nombres de dominio) para obtener una nueva dirección IP.
- Las estadísticas se recopilan en un servicio y no se restablecen cuando cambia la dirección IP.
- Si una resolución DNS devuelve un código de “error de nombre” (3), el dispositivo marca el servicio y cambia la dirección IP a cero.

Cuando el dispositivo recibe una solicitud de servicio, selecciona el servicio de destino. De este modo, el dispositivo equilibra la carga de los servicios. En el siguiente diagrama se describe la topología de una configuración de equilibrio de carga que equilibra la carga un grupo de servidores basados en nombres de dominio (DBS).

Ilustración 1. Topología básica de equilibrio de carga para servidores DBS



Los servicios Service-HTTP-1, Servicio-HTTP-2 y Servicio-HTTP-3 están enlazados al servidor virtual VServer-LB-1. El servidor virtual vServer-LB-1 utiliza el método de equilibrio de carga de menos conexión para elegir el servicio. La dirección IP del servicio se resuelve mediante el servidor de nombres VServer-lB-2.

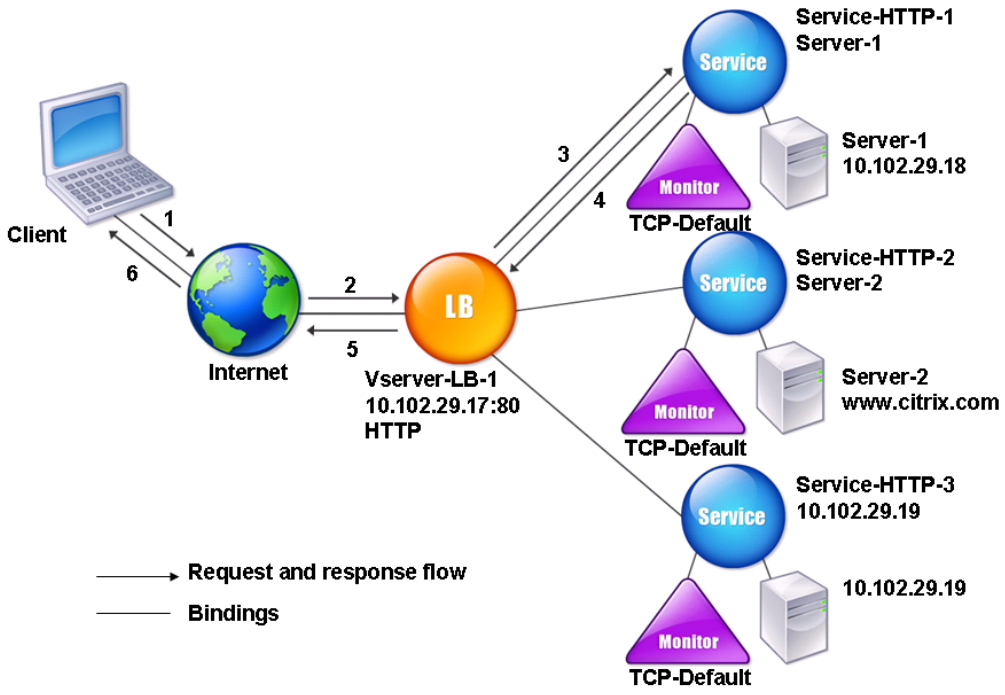
En la tabla siguiente se enumeran los nombres y valores de las entidades básicas configuradas en el dispositivo.

Tipo de entidad	Nombre	Dirección IP	Port	Protocolo
Servidor virtual	Vserver-LB-1	10.102.29.17	80	HTTP
	Vserver-LB-2	10.102.29.20	53	DNS
Servidores	server-1	10.102.29.18	80	HTTP
	server-2	www.citrix.com	80	HTTP
Servicios	Service-HTTP-1	server-1	80	HTTP
	Service-HTTP-2	server-2	80	HTTP
	Service-HTTP-2	10.102.29.19	80	HTTP

Tipo de entidad	Nombre	Dirección IP	Port	Protocolo
Monitores	Valor predeterminado	Ninguno	Ninguno	Ninguno
Servidor de nombres	Ninguno	10.102.29.19	Ninguno	Ninguno

El siguiente diagrama muestra las entidades de equilibrio de carga y los valores de los parámetros que deben configurarse en el dispositivo.

Ilustración 2. Modelo de entidad de servidores DBS de equilibrio de carga



Para configurar una configuración de equilibrio de carga básica, consulte Configuración del equilibrio de carga básico. Cree los servicios y servidores virtuales de tipo HTTP, asigne un nombre a las entidades y establezca los parámetros mediante los valores descritos en la tabla anterior.

Puede agregar, quitar, habilitar e inhabilitar servidores de nombres externos. Puede crear un servidor de nombres especificando su dirección IP o puede configurar un servidor virtual existente como servidor de nombres.

Para agregar un servidor de nombres mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
1 add dns nameServer <dnsVserverName>
2 <!--NeedCopy-->
```

Ejemplo:

```
1 add dns nameServer Vserver-LB-2
2 <!--NeedCopy-->
```

Para agregar un servidor de nombres mediante la utilidad de configuración

1. Vaya a **Administracióndel tráfico**>**DNS**>**Servidores de **nombres****.
2. Cree un servidor de nombres DNS de tipo Servidor virtual DNS y seleccione un servidor de la lista Servidor virtual DNS.

También puede agregar un servidor de nombres autorizado que resuelva el nombre de dominio a una dirección IP.

> **Nota**
>
> Puede agregar un servidor de nombres de tipo TCP, UDP o UDP_TCP para resolver sondeos DBS. Sin embargo, si los servidores de nombres TCP y UDP coexisten y un servidor de nombres UDP recibe una respuesta con el bit truncado, esta respuesta no se vuelve a intentar a través del servidor de nombres TCP.

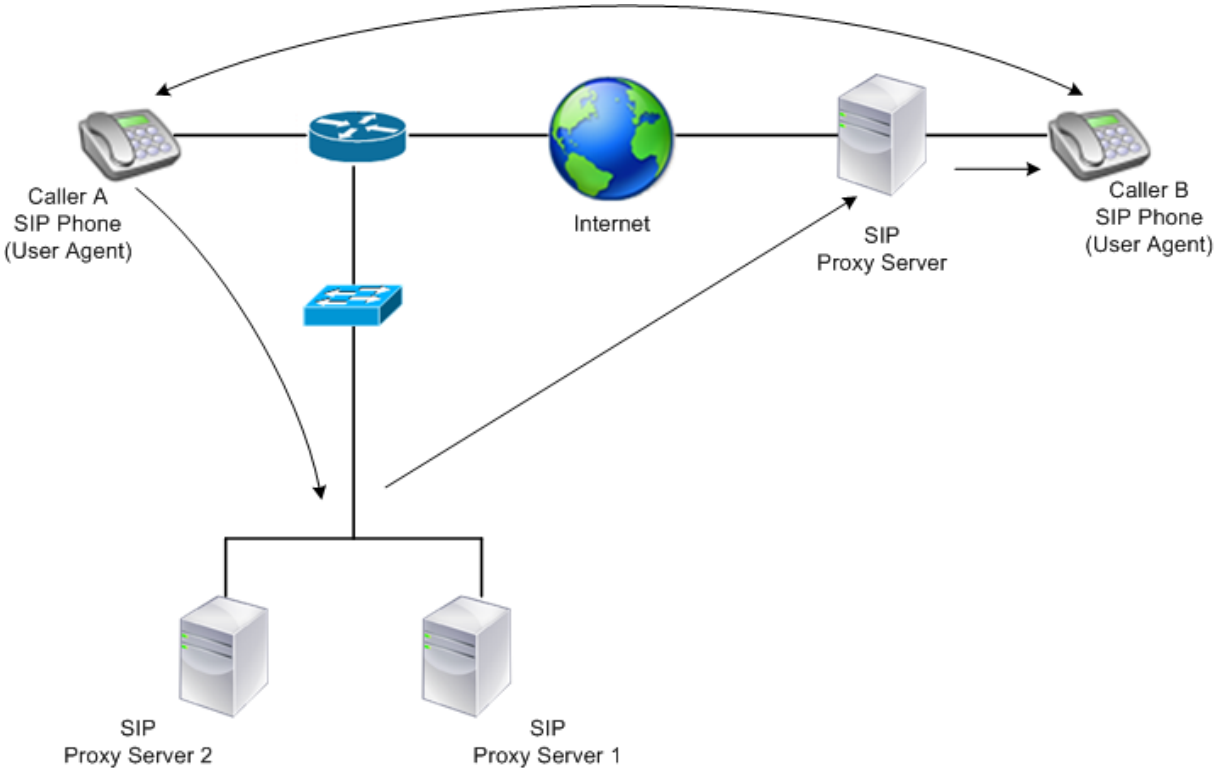
Equilibrio de carga de un grupo de servidores SIP

August 20, 2021

El Protocolo de Iniciación de Sesión (SIP) está diseñado para iniciar, administrar y terminar sesiones de comunicaciones multimedia. Ha surgido como el estándar para la telefonía por Internet (VoIP). Los mensajes SIP se pueden transmitir a través de TCP o UDP. Los mensajes SIP son de dos tipos: Mensajes de solicitud y mensajes de respuesta.

El tráfico en un sistema de comunicación basado en SIP se enruta a través de dispositivos y aplicaciones (entidades) dedicados. En una sesión de comunicación multimedia, estas entidades intercambian mensajes. La siguiente ilustración muestra un sistema básico de comunicación basado en SIP:

Ilustración 1. Sistema de comunicación basado en SIP



Un Citrix ADC le permite equilibrar la carga de mensajes SIP a través de UDP o a través de TCP (incluido TLS). Puede configurar Citrix ADC para equilibrar la carga de las solicitudes SIP en un grupo de servidores proxy SIP. Para ello, cree un servidor virtual de equilibrio de carga con el método de equilibrio de carga y el tipo de persistencia establecido en una de las siguientes combinaciones:

- Método de equilibrio de carga hash de ID de llamada sin configuración de persistencia
- Persistencia basada en ID de llamada con menos conexión o método de equilibrio de carga de round robin
- Persistencia basada en reglas con menos conexión o método de equilibrio de carga round robin

Además, de forma predeterminada, Citrix ADC agrega RPORT a través del encabezado de la solicitud SIP, de modo que el servidor devuelve la respuesta a la dirección IP de origen y al puerto desde el que se originó la solicitud.

Nota: Para que el equilibrio de carga funcione, debe configurar los proxies SIP para que no añadan direcciones IP privadas o dominios privados a la carga o cabecera SIP. Los proxies SIP deben agregar al encabezado SIP un nombre de dominio que se resuelva a la dirección IP del servidor virtual SIP. Además, los proxies SIP deben comunicarse con una base de datos común para compartir información de registro.

Tráfico iniciado por el servidor

Para el tráfico saliente iniciado por el servidor SIP, configure RNAT en Citrix ADC para que las direcciones IP privadas utilizadas por los clientes se traduzcan en direcciones IP públicas.

Si ha configurado parámetros SIP que incluyen el puerto de origen o destino RNAT, el dispositivo compara los valores de los puertos de origen y destino de los paquetes de solicitud con el puerto de origen RNAT y el puerto de destino RNAT. Si uno de los valores coincide, el dispositivo actualiza el encabezado VIA con RPORT. A continuación, la respuesta SIP del cliente atraviesa la misma ruta que la solicitud.

Para el tráfico SSL iniciado por el servidor, Citrix ADC utiliza un par integrado de claves de certificado. Si quiere utilizar un par de claves de certificado personalizado, vincule el par de claves de certificado personalizado al servicio interno de Citrix ADC denominado **nsrnatsip-127.0.0.0.1-5061**.

Compatibilidad con directivas y expresiones

El lenguaje de expresiones predeterminadas de Citrix ADC contiene varias expresiones que funcionan en conexiones de Session Initiation Protocol (SIP). Estas expresiones solo pueden vincularse a servidores virtuales basados en SIP (sip_udp, sip_tcp o sip_ssl) y a puntos de enlace globales. Puede utilizar estas expresiones en directivas de conmutación de contenido, limitación de velocidad, respuesta y reescritura.

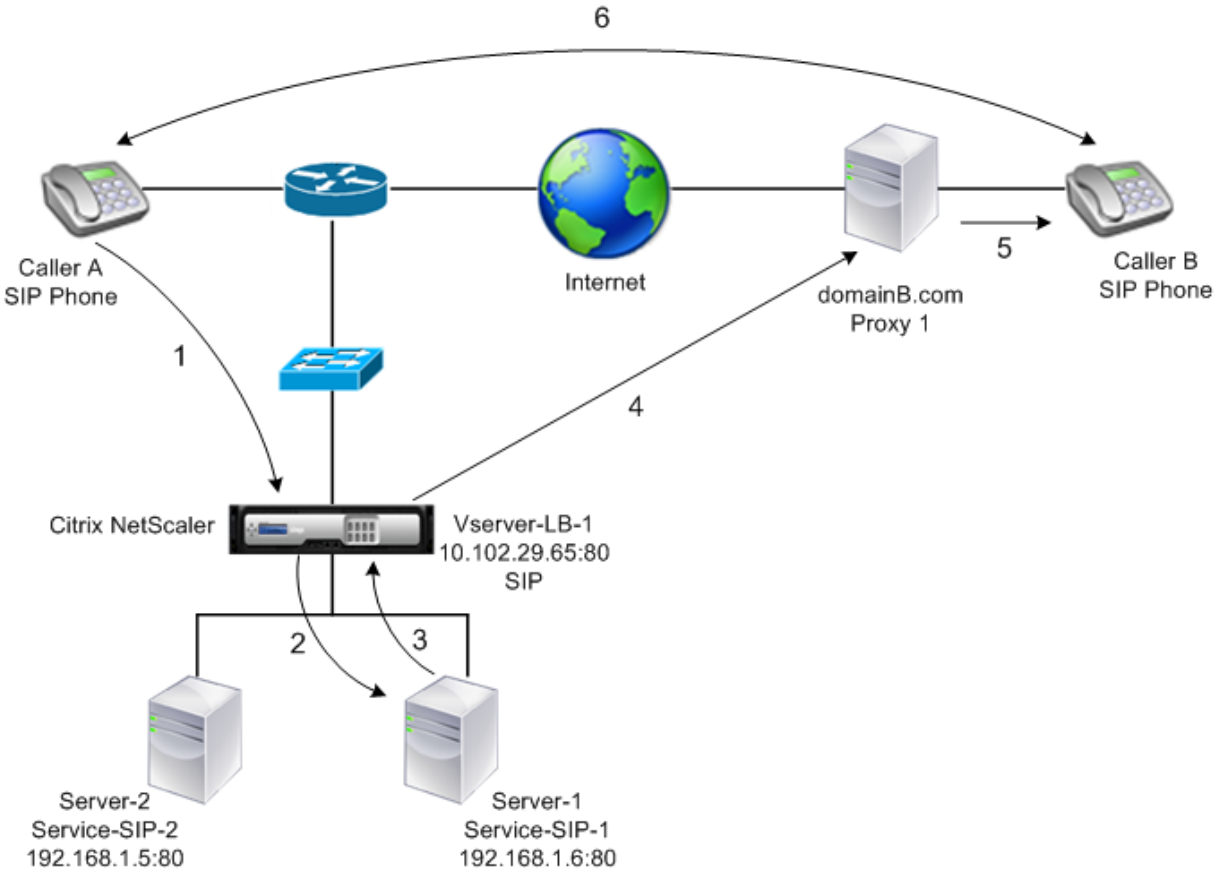
Configuración de Equilibrio de carga para Tráfico de Señalización SIP a través de TCP o UDP

Citrix ADC puede equilibrar la carga de servidores SIP que envían solicitudes a través de UDP o TCP, incluido el tráfico TCP protegido por TLS. El ADC proporciona los siguientes tipos de servicio para equilibrar la carga de los servidores SIP:

- SIP_UDP: Se utiliza cuando los servidores SIP envían mensajes SIP a través de UDP.
- SIP_TCP: Se utiliza cuando los servidores SIP envían mensajes SIP a través de TCP.
- SIP_SSL: Se utiliza para proteger el tráfico de señalización SIP a través de TCP mediante SSL o TLS. Citrix ADC admite los siguientes modos:
  - Conexión TLS de extremo a extremo entre el cliente, el ADC y el servidor SIP.
  - Conexión TLS entre el cliente y el ADC, y conexión TCP entre el ADC y el servidor SIP.
  - Conexión TCP entre el cliente y el ADC, y conexión TLS entre el ADC y el servidor SIP.

La siguiente ilustración muestra la topología de una instalación configurada para equilibrar la carga de un grupo de servidores SIP que envían mensajes SIP a través de TCP o UDP.

Ilustración 2. Topología de equilibrio de carga SIP



Tipo de entidad	Nombre	Dirección IP	Port	Tipo de servicio/Protocolo
Servidor virtual	Vserver-LB-1	10.102.29.65	80	SIP_UDP / SIP_TCP / SIP_SSL
Servicios	Service-SIP-1	192.168.1.6	80	SIP_UDP / SIP_TCP / SIP_SSL
	Service-SIP-2	192.168.1.5	80	SIP_UDP / SIP_TCP / SIP_SSL
Monitores	Valor predeterminado	Ninguno	80	SIP_UDP / SIP_TCP / SIP_SSL

A continuación se presenta una descripción general de la configuración del equilibrio de carga básico para el tráfico SIP:

1. Configure los servicios y configure un servidor virtual para cada tipo de tráfico SIP que quiera equilibrar la carga:

   - **SIP_UDP**: Si está equilibrando la carga del tráfico SIP a través de UDP.
   - **SIP_TCP**: Si está equilibrando la carga del tráfico SIP a través de TCP.
   - **SIP_SSL**: Si está equilibrando la carga y protegiendo el tráfico SIP a través de TCP.

   Nota: Si utiliza SIP_SSL, asegúrese de crear un par de claves de certificado SSL. Para obtener más información, consulte Adición de un par de claves de certificado.

2. Enlazar los servicios a los servidores virtuales.
3. Si quiere supervisar los estados de los servicios con un monitor distinto del predeterminado (**tcp-default**), cree un monitor personalizado y vincularlo a los servicios. Citrix ADC proporciona dos tipos de monitor personalizados, **SIP-UDP** y **SIP-TCP**, para supervisar los servicios SIP.
4. Si utiliza un servidor virtual SIP_SSL, vincule un par de certificados SSL con el servidor virtual.
5. Si utiliza Citrix ADC como Gateway para los servidores SIP de la implementación, configure RNAT.
6. Si quiere anexar RPORT a los mensajes SIP que se inician desde el servidor SIP, configure los parámetros SIP.

Para configurar una configuración básica de equilibrio de carga para el tráfico SIP mediante la interfaz de línea de comandos

Cree uno o más servicios. En el símbolo del sistema, escriba:

```
add service <name> <serverName> (SIP_UDP | SIP_TCP | SIP_SSL) <port>
<!--NeedCopy-->
```

Ejemplo:

```
add service Service-SIP-UDP-1 192.0.2.5 SIP_UDP 80
<!--NeedCopy-->
```

Cree tantos servidores virtuales como sea necesario para gestionar los servicios que ha creado. El tipo de servidor virtual debe coincidir con el tipo de servicios que le vincula. En el símbolo del sistema, escriba:


```
add lb vserver <name> <serverName> (SIP_UDP | SIP_TCP | SIP_SSL) <port>
<!--NeedCopy-->
```

Ejemplo:

```
add lb vserver Vserver-LB-1 SIP_UDP 10.102.29.60 80
<!--NeedCopy-->
```

Enlazar cada servicio a un servidor virtual. En el símbolo del sistema, escriba:

```
bind lb vserver <name> <serverName>
<!--NeedCopy-->
```

Ejemplo:

```
bind lb vserver Vserver-LB-1 Service-SIP-UDP-1
<!--NeedCopy-->
```

(Opcional) Cree un monitor personalizado de tipo SIP-UDP o SIP-TCP y vincule el monitor al servicio. En el símbolo del sistema, escriba:

```
add lb monitor <monitorName> <monitorType> [<interval>]

bind lb monitor <monitorName> <ServiceName>
<!--NeedCopy-->
```

Ejemplo:

```
add lb monitor mon1 sip-UDP -sipMethod REGISTER -sipuRI sip:mon@test.
   com -sipregURI sip:mon@test.com -respcode 200

bind monitor mon1 Service-SIP-UDP-1
<!--NeedCopy-->
```

Si ha creado un servidor virtual SIP_SSL, vincule un par de claves de certificado SSL al servidor virtual. En el símbolo del sistema, escriba: En el símbolo del sistema, escriba:


```
bind ssl vserver <vServerName> -certkeyName <certificate-KeyPairName> -
    CA  - skipCAName
<!--NeedCopy-->
```

Ejemplo:

```
bind ssl vserver Vserver-LB-1 -certkeyName CertKey-SSL-1
<!--NeedCopy-->
```

Configure RNAT según lo requiera su topología de red. En el símbolo del sistema, escriba uno de los siguientes comandos para crear, respectivamente, una entrada RNAT que utilice una dirección de red como condición y SNIP como dirección IP NAT, una entrada RNAT que utiliza una dirección de red como condición y una dirección IP única como la dirección IP NAT, una entrada RNAT que utiliza una ACL como la condición y un SNIP como la dirección IP NAT, o una entrada RNAT que utiliza una ACL como condición y una dirección IP única como la dirección IP NAT:

```
add rnat <name> (<network> | (<aclname> [-redirectPort <port>]))

bind rnat <name> <natIP>@ ...

show rnat
<!--NeedCopy-->
```

Ejemplo:

```
add rnat RNAT-1 192.168.1.0 255.255.255.0

bind rnat RNAT-1 -natip 10.102.29.50
<!--NeedCopy-->
```

Si quiere utilizar un par de claves de certificado personalizado, vincule el par de claves de certificado personalizado al servicio interno de Citrix ADC denominado nsrnatsip-127.0.0.0.1-5061.

```
add ssl certKey <certkeyName> -cert <string> [-key <string>]

bind ssl service <serviceName> -certkeyName <string>
<!--NeedCopy-->
```


Ejemplo:

```
add ssl certKey c1 -cert cert.epm -key key.ky

bind ssl service nsrnatsip-127.0.0.1-5061 -certkeyName c1
<!--NeedCopy-->
```

Si quiere anexar RPORT a los mensajes SIP que inicia el servidor SIP, escriba el comando siguiente en el símbolo del sistema:

```
set lb sipParameters -rnatSrcPort <rnatSrcPort> -rnatDstPort<
    rnatDstPort> -retryDur <integer> -addRportVip <addRportVip> -
    sip503RateThreshold <sip503_rate_threshold_value>
<!--NeedCopy-->
```

Ejemplo de configuración para equilibrar la carga del tráfico SIP a través de UDP

```
add service service-UDP-1 10.102.29.5 SIP_UDP 80

Done

add lb vserver vserver-LB-1 SIP_UDP 10.102.29.60 80

Done

bind lb vserver vserver-LB-1 service-UDP-1

Done

add lb mon mon1 sip-udp -sipMethod REGISTER -sipuRI sip:mon@test.com -
    sipregURI sip:mon@test.com -respcode 200

Done

bind mon mon1 service-UDP-1

Done

add rnat RNAT-1 192.168.1.0 255.255.255.0

```



```
23 Done
24
25 set lb sipParameters -rnatSrcPort 5060 -rnatDstPort 5060 -retryDur 1000
       -addRportVip ENABLED -sip503RateThreshold 1000
26
27 Done
28 <!--NeedCopy-->
```

Ejemplo de configuración para equilibrar la carga del tráfico SIP a través de TCP

```
1  add service service-TCP-1 10.102.29.5 SIP_TCP 80
2
3  Done
4
5  add lb vserver vserver-LB-1 SIP_TCP 10.102.29.60 80
6
7  Done
8
9  bind lb vserver vserver-LB-1 service-TCP-1
10
11 Done
12
13 add lb mon mon1 sip-tcp -sipMethod REGISTER -sipuRI sip:mon@test.com -
       sipregURI sip:mon@test.com -respcode 200
14
15 Done
16
17 bind mon mon1 service-TCP-1
18
19 Done
20
21 add rnat RNAT-1 192.168.1.0 255.255.255.0
22
23 Done
24
25 set lb sipParameters -rnatSrcPort 5060 -rnatDstPort 5060 -retryDur 1000
       -addRportVip ENABLED -sip503RateThreshold 1000
26
27 Done
28 <!--NeedCopy-->
```


Ejemplo de configuración para el equilibrio de carga y la protección del tráfico SIP a través de TCP

```
add service service-SIP-SSL-1 10.102.29.5 SIP_SSL 80

Done

add lb vserver vserver-LB-1 SIP_SSL 10.102.29.60 80

Done

bind lb vserver vserver-LB-1 service-SIP-SSL

Done

add lb mon mon1 sip-tCP -sipMethod REGISTER -sipuRI sip:mon@test.com -
    sipregURI sip:mon@test.com -respcode 200

Done

bind mon mon1 service-SIP-SSL

Done

bind ssl vserver Vserver-LB-1 -certkeyName CertKey-SSL-1

Done

add rnat RNAT-1 192.168.1.0 255.255.255.0

Done

set lb sipParameters -rnatSrcPort 5060 -rnatDstPort 5060 -retryDur 1000
     -addRportVip ENABLED -sip503RateThreshold 1000

Done
<!--NeedCopy-->
```

Para configurar una configuración básica de equilibrio de carga para el tráfico SIP mediante la GUI

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**y agregue un servidor virtual de tipo SIP_UDP, SIP_TCP o SIP_SSL.

2. Haga clic en la sección **Servicio** y agregue un servicio de tipo SIP_UDP, SIP_TCP o SIP_SSL.
3. (Opcional) Haga clic en la sección **Supervisar** y agregue un monitor del tipo: SIP-UDP o SIP-TCP.
4. Enlazar el monitor al servicio y enlazar el servicio al servidor virtual.
5. Si ha creado un servidor virtual SIP_SSL, vincule un par de claves de certificado SSL al servidor virtual. Haga clic en la sección Certificados y vincule un par de claves de certificado al servidor virtual.
6. Configure RNAT según lo requiera su topología de red. Para configurar RNAT:
   a) Vaya a **Sistema > Red > Rutas**.
   b) En la página Rutas, haga clic en la ficha **RNAT** .
   c) En el panel de detalles, haga clic en **Configurar RNAT**.
   d) En el cuadro de diálogo Configurar RNAT, realice una de las acciones siguientes:
      - Si desea utilizar la dirección de red como condición para crear una entrada RNAT, haga clic en **Red** y establezca los siguientes parámetros:
        - Red
        - Máscara de red
      - Si desea utilizar una ACL extendida como condición para crear una entrada RNAT, haga clic en **ACL** y establezca los siguientes parámetros:
        - Nombre de ACL
        - Puerto de redireccionamiento
   e) Para establecer una dirección SNIP como una dirección IP NAT, vaya al paso 7.
   f) Para establecer una dirección IP única como IP NAT, en la lista IP NAT disponible (s), seleccione la dirección IP que quiere establecer como IP NAT y, a continuación, haga clic en Agregar. La IP NAT que ha seleccionado aparece en la lista de IP NAT configuradas.
   g) Haga clic en Crear y, a continuación, en Cerrar.

   Si quiere utilizar un par de claves de certificado personalizado, vincule el par de claves de certificado personalizado al servicio interno de Citrix ADC denominado **nsrnatsip-127.0.0.0.1-5061**. Para enlazar el par:

   a) Vaya a **Administración del tráfico > Equilibrio de carga > Servicios** y haga clic en la ficha Servicios internos.
   b) Seleccione nsrnatsip-127.0.0.1-5061 y haga clic en **Modificar**.
   c) Haga clic en la sección **Certificados** y vincule un par de claves de certificado al servicio interno.
7. Si quiere anexar RPORT a los mensajes SIP que inicia el servidor SIP, configure los parámetros SIP. Vaya a **Administración del tráfico > Equilibrio de carga** y haga clic en Cambiar configuración de SIP, establezca los distintos parámetros SIP.

Ejemplo de directiva y expresión SIP: Compresión habilitada en solicitudes de cliente

Un Citrix ADC no puede procesar solicitudes SIP de cliente comprimido, por lo que se produce un error en la solicitud SIP de cliente.

Puede configurar una directiva de respuesta que intercepte el mensaje SIP NEGOCIE del cliente y busque el encabezado de compresión. Si el mensaje incluye un encabezado de compresión, la directiva responde con “400 Bad Request”, de modo que el cliente vuelva a enviar la solicitud sin comprimirla.

En el símbolo del sistema, escriba los siguientes comandos para crear la directiva de respuesta:

```
add responder action sipaction1 respondwith q{
 ”SIP/2.0 400 Bad Requestrnrn” }


Done

add responder policy sippol1

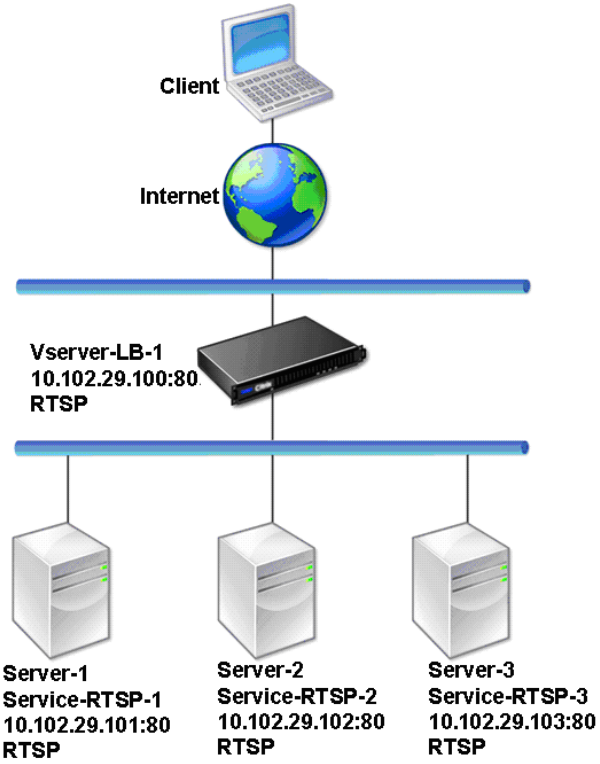
add responder policy sippol1 ”SIP.REQ.METHOD.EQ(”NEGOTIATE”)&&SIP.REQ.
   HEADER(”Compression”).EXISTS” sipaction1
<!--NeedCopy-->
```

Servidores RTSP de equilibrio de carga

August 20, 2021

El dispositivo Citrix ADC puede equilibrar la carga de los servidores RTSP para mejorar el rendimiento de las transmisiones de audio y vídeo a través de redes. En el siguiente diagrama se describe la topología de una configuración de equilibrio de carga configurada para equilibrar la carga de un grupo de servidores RTSP.

Ilustración 1. Topología de equilibrio de carga para RTSP

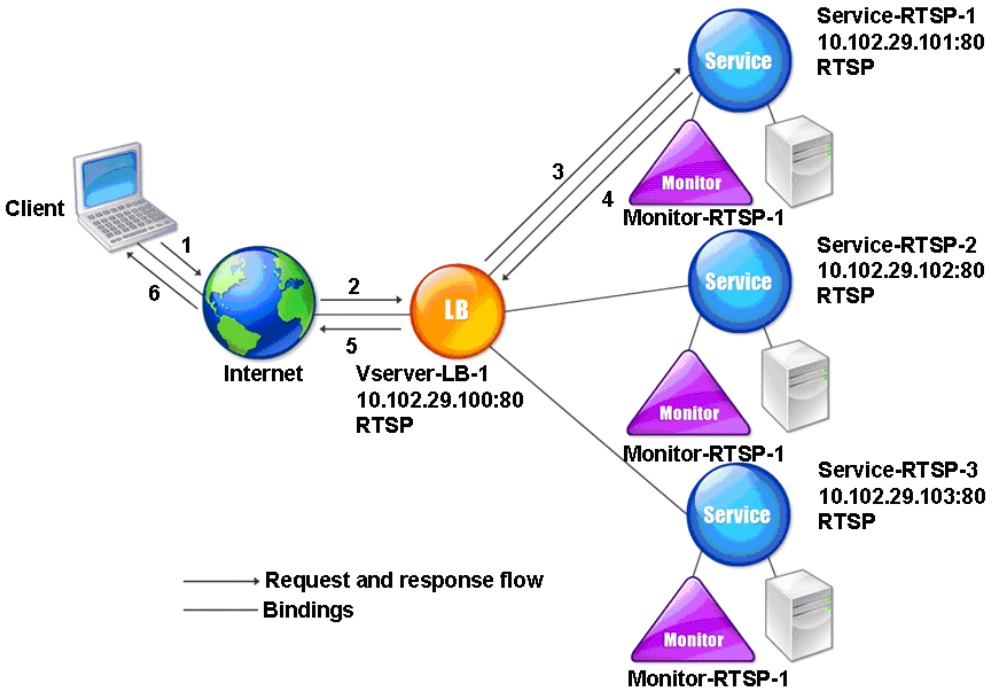


En el ejemplo, los servicios Service-RTSP-1, Service-RTSP-2 y Service-RTSP-3 están enlazados al servidor virtual VServer-LB-1. En la tabla siguiente se enumeran los nombres y valores de las entidades de ejemplo.

Tipo de entidad	Nombre	Dirección IP	Port	Protocolo
Servidor virtual	Vserver-LB-1	10.102.29.100	554	RTSP
Servicios	Service-RTSP-1	10.102.29.101	554	RTSP
	Service-RTSP-2	10.102.29.102	554	RTSP
	Service-RTSP-3	10.102.29.103	554	RTSP
Monitores	Monitor-RTSP-1	Ninguno	554	RTSP

En el siguiente diagrama se muestran las entidades de equilibrio de carga utilizadas en la configuración de RTSP.

Ilustración 2. Modelo de entidad de servidores RTSP de equilibrio de carga



Para configurar una configuración básica de equilibrio de carga para servidores RTSP, consulte Configuración del equilibrio de carga básico. Crear servicios y servidores virtuales de tipo RTSP. Cuando configura una configuración básica de equilibrio de carga, el monitor predeterminado de TCP está enlazado a los servicios. Para vincular un monitor RTSP a estos servicios, consulte Vinculación de monitores a servicios. El procedimiento siguiente describe cómo crear un monitor que comprueba los servidores RTSP.

Para configurar monitores RTSP mediante la CLI

En el símbolo del sistema, escriba:

```
add lb monitor <monitorName> <type>
<!--NeedCopy-->
```

Ejemplo:

```
add lb monitor Monitor-RTSP-1 RTSP
```



```
<!--NeedCopy-->
```

Para configurar monitores RTSP mediante la GUI

Vaya a Administración del tráfico > Equilibrio de carga > Monitores y cree un monitor de tipo RTSP.

Servidores de protocolo de escritorio remoto de equilibrio de carga

August 20, 2021

El protocolo de escritorio remoto (RDP) es un protocolo compatible con múltiples canales que permite canales virtuales separados para transportar datos de presentación, comunicación de dispositivos serie, información de licencias, datos altamente cifrados (actividad de teclado y ratón), etc.

RDP se utiliza para proporcionar una GUI a otro equipo de la red. RDP se utiliza con servidores terminales de Windows para proporcionar un acceso rápido con transmisión casi en tiempo real de movimientos del ratón y pulsaciones de teclas incluso a través de conexiones de bajo ancho de banda.

Cuando se implementan varios servidores Terminal Server para proporcionar servicios de escritorio remoto, el dispositivo Citrix ADC proporciona equilibrio de carga de los servidores Terminal Server (ediciones Windows 2003 y 2008 Server Enterprise). A veces, un usuario que está accediendo a una aplicación de forma remota puede desear dejar la aplicación ejecutándose en el equipo remoto pero apagar el equipo local. Por lo tanto, el usuario cierra la aplicación local sin cerrar la sesión de la aplicación remota. Después de volver a conectarse al equipo remoto, el usuario debe poder continuar con la aplicación remota. Para proporcionar esta funcionalidad, la implementación de Citrix ADC RDP respeta el token de redirección (cookie) establecido por el Directorio de sesión de Servicios de Terminal Server o Broker para que el cliente pueda volver a conectarse al mismo servidor Terminal Server al que estaba conectado anteriormente. El Directorio de sesiones, implementado en Windows 2003 Terminal Server, se conoce como Broker en Windows 2008 Terminal Server.

Cuando se establece una conexión TCP entre el cliente y el servidor virtual de equilibrio de carga, Citrix ADC aplica el método de equilibrio de carga especificado y reenvía la solicitud a uno de los servidores de Terminal Server. El servidor de Terminal Server comprueba el directorio de sesión para determinar si el cliente tiene una sesión ejecutándose en cualquier otro servidor de Terminal Server del dominio.

Si no hay ninguna sesión activa en ningún otro servidor de Terminal Server, el servidor de Terminal Server responde atendiendo la solicitud del cliente y el dispositivo Citrix ADC reenvía la respuesta al cliente.

Si hay una sesión activa en cualquier otro servidor de terminal, el servidor de terminal que recibe la solicitud inserta una cookie (denominada token de redirección) con los detalles de la sesión activa y

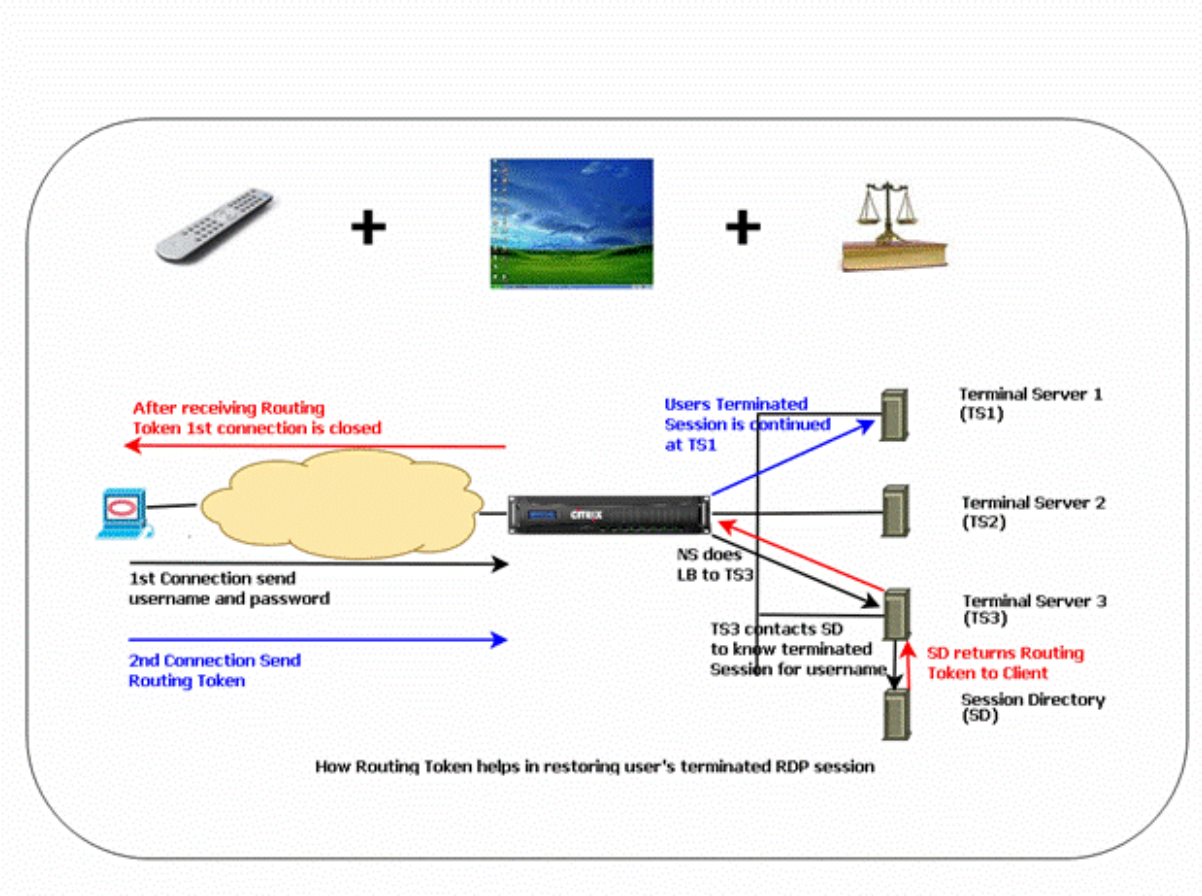
devuelve los paquetes al dispositivo Citrix ADC, que devuelve el paquete al cliente. El servidor cierra la conexión con el cliente. Cuando el cliente intenta conectarse, Citrix ADC lee la información de la cookie y reenvía el paquete al servidor Terminal Server en el que el cliente tiene una sesión activa.

El usuario en el equipo cliente experimenta una continuación del servicio y no tiene que realizar ninguna acción específica.

Nota: La función Directorio de sesiones de Windows requiere el cliente de Escritorio remoto que se lanzó por primera vez con Windows XP. Si se desconecta una sesión con un cliente Terminal Server de Windows 2000 o Windows NT 4.0 y el cliente se vuelve a conectar, el servidor con el que se establece la conexión se selecciona mediante el algoritmo de equilibrio de carga.

El siguiente diagrama describe el equilibrio de carga de RDP.

Ilustración 1. Topología de equilibrio de carga para RDP



Nota

- Cuando se configura un servicio RDP, la persistencia se mantiene automáticamente mediante un token de redirección. No es necesario habilitar la persistencia explícitamente.
- El dispositivo Citrix ADC admite únicamente cookies basadas en IP.

> • El script nsrdp.pl no es compatible con ninguna versión actual de servidores Windows.

Asegúrese de que las sesiones RDP desconectadas se borran en los servidores de Terminal Server en el back-end para evitar que entre dos servidores Terminal Server cuando se desconecte una sesión RDP sin cerrar sesión. Para obtener más información, consulte https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc758177(v=ws.10)##BKMK_2

Cuando agrega un servicio RDP, de forma predeterminada, Citrix ADC agrega un monitor del tipo TCP y lo vincula al servicio. El monitor predeterminado es un monitor TCP simple que comprueba si existe un proceso de escucha en el puerto 3389 del servidor especificado para el servicio RDP. Si hay un proceso de escucha en el 3389, Citrix ADC marca este servicio como UP y, si no hay un proceso de escucha, marca el servicio como DOWN.

Para una supervisión más eficiente de un servicio RDP, además del monitor predeterminado, puede configurar un monitor de script diseñado para el protocolo RDP. Al configurar el monitor de scripts, Citrix ADC abre una conexión TCP al servidor especificado y envía un paquete RDP. El monitor marca el servicio como UP solo si recibe una confirmación de la conexión del servidor físico. Por lo tanto, desde el monitor de scripts, Citrix ADC puede saber si el servicio RDP está listo para atender una solicitud.

El monitor es un monitor de tipo usuario y el script se encuentra en Citrix ADC en /nsconfig/monitors/nsrdp.pl. Al configurar el monitor de usuario, Citrix ADC ejecuta el script automáticamente. Para configurar el monitor de scripts, agregue el monitor y vincularlo al servicio RDP.

Para configurar el equilibrio de carga de RDP, cree servicios de tipo RDP y vincularlos a un servidor virtual RDP.

Para configurar los servicios de equilibrio de carga RDP mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para configurar una configuración de equilibrio de carga RDP y verifique la configuración:

```
add service <name>@ <serverName> <serviceType> <port>
<!--NeedCopy-->
```

Nota: Repita el comando anterior para agregar más servicios.

Ejemplo

```
> add service ser1 10.102.27.182 RDP 3389
Done
```



```
> add service ser2 10.102.27.183 RDP 3389
Done
>show service ser1
ser1 (10.102. 27.182:3389) - RDP
        State: UP
…
            Server Name: 10.102.27.182
            Server ID : 0           Monitor Threshold : 0
        Down state flush: ENABLED
…
1)      Monitor Name: tcp-default
                State: UP       Weight: 1
…
                Response Time: 4.152 millisec
 Done
<!--NeedCopy-->
```

Para configurar los servicios de equilibrio de carga RDP mediante la utilidad de configuración

Vaya a **Administración del tráfico > Equilibrio de carga > Servicios**y cree servicios de tipo RDP.

Para configurar un servidor virtual de equilibrio de carga RDP mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para configurar un servidor virtual de equilibrio de carga RDP y compruebe la configuración:

```
add lb vserver <name>@ <serviceType> <ipAddress> <port>

bind lb vserver <name>@ <serviceName>

Bind all the RDP services to be load balanced to the virtual server.
<!--NeedCopy-->
```

Ejemplo:

Este ejemplo tiene dos servicios RDP enlazados al servidor virtual RDP.

```
add lb vs v1 rdP 10.102.27.186 3389
Done
```



```
3
4  bind lb vs v1 ser1
5  service ”ser1” bound
6
7  bind lb vs v1 ser2
8  service ”ser2” bound
9  Done
10
11 sh lb vs v1
12 v1 (10.102.27.186:3389) - RDP   Type: ADDRESS
13 State: UP
14 …
15 No. of Bound Services :  2 (Total)       2 (Active)
16 Configured Method: LEASTCONNECTION
17   Current Method: Round Robin, Reason: A new service is bound
18 Mode: IP
19 Persistence: NONE
20   L2Conn: OFF
21
22 1) ser1 (10.102.27.182: 3389) - RDPState: UP   Weight: 1
23 2) ser2 (10.102.27.183: 3389) - RDPState: UP   Weight: 1
24 Done
25 <!--NeedCopy-->
```

Para configurar un servidor virtual de equilibrio de carga RDP mediante la utilidad de configuración

Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**, cree un servidor virtual de tipo RDP y vincule servicios RDP a este servidor virtual.

Para configurar un monitor de scripts para servicios RDP mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos:

```
1 add lb monitor <monitorName> USER -scriptName nsrdp.pl
2
3 bind lb monitor <monitorName> <rdpServiceName>
4 <!--NeedCopy-->
```

Ejemplo:


```
add service ser1 10.102.27.182 RDP 3389

add lb monitor RDP_MON USER -scriptName nsrdp.pl

bind lb monitor RDP_MON ser1

<!--NeedCopy-->
```

Para configurar un monitor de scripts para los servicios RDP mediante la utilidad de configuración

1. Vaya a **Administración del tráfico > Equilibrio de carga > Monitores**y cree un monitor de tipo USUARIO.
2. En Parámetros especiales, en la lista Nombre de script, seleccione nsrdp.pl y, a continuación, vincule este monitor a un servicio RDP.

Equilibrio de carga del servidor Microsoft Exchange

May 8, 2022

En este documento se proporcionan los ejemplos de configuración recomendados para el equilibrio de carga del servidor Microsoft Exchange mediante el dispositivo Citrix ADC.

Citrix ADM StyleBooks simplifica las configuraciones de equilibrio de carga de Citrix ADC para Exchange. Para obtener más información, consulte StyleBook de Microsoft Exchange.

> Nota:
>
> El equilibrio de carga de Microsoft Exchange no es posible mediante un único servidor virtual de equilibrio de carga. En su lugar, siga las configuraciones recomendadas que se proporcionan en este documento.

Diferencias en Microsoft Exchange 2016 y versiones posteriores

- No es necesario configurar puertos de llamada de procedimiento remoto (RPC) estáticos en Exchange 2016 porque no se utilizan puertos RPC.
- Todas las secciones denominadas “para versiones de Exchange inferiores a 2016” no son necesarias con Exchange 2016.

- Si ya ha configurado alguna de las versiones distintas a 2016 y migra a 2016, no tiene que eliminarlas. Porque incluso si existen, no hay problemas.

Puntos que tener en cuenta

- Para las llamadas a procedimientos remotos (RPC) con el servidor Exchange inferior a 2016, los servidores CAS de Exchange deben configurarse para asignaciones de puertos estáticos. Para obtener más información, consulte Servidor de acceso de cliente de Exchange 2010: Configuración de puertos RPC estáticos documentación de Microsoft.
- En esta configuración se supone que se utiliza el dispositivo Citrix ADC para descarga SSL. Para obtener más información, consulte Cómo configurar la descarga de SSL en Exchange 2010 o Configuración de la descarga SSL en Exchange 2013.
- Si no quiere utilizar la función Descarga SSL del dispositivo Citrix ADC, cambie el grupo de servicios `CAS_servicegroup_http` y los monitores por tipo `SSL` y sus enlaces al puerto `443`.
- La protección contra sobretensiones no es compatible con Microsoft Exchange. No lo habilite en ningún servicio o grupo de servicios relacionado con Microsoft Exchange. La habilitación de la protección contra sobretensiones provoca problemas de conectividad
- Sustituya las siguientes variables por la información adecuada:
  - {IP pública HTTP}: dirección IP para endpoint HTTP de Exchange público
  - {RPC Public IP} —Dirección IP para endpoint RPC de Exchange público (puede ser lo mismo que la IP pública HTTP)
  - {Timeout}: tiempo de espera deseado (en segundos). Se recomienda que sea el tiempo estándar de turno de trabajo (es decir, 8 horas)
  - {persTimeout}: tiempo de espera deseado (en minutos). Debe corresponder a la configuración de tiempo de espera anterior.
  - {AB Port} —Puerto TCP de libreta de direcciones RPC (normalmente 59601)
  - {CA Port} —Puerto TCP de acceso de cliente RPC (normalmente 59600)
  - {certKey} —Clave de certificado SSL
  - {CAS-1 Server}: dirección IP del servidor CAS
  - {CAS-2 Server}: dirección IP del servidor CAS

Ejemplos de configuración recomendados para todas las versiones de Microsoft Exchange server

Grupos de servicios:


```
add serviceGroup CAS_servicegroup_http HTTP -maxClient 0 -maxReq 0 -cip
    DISABLED -usip NO -SP OFF -useproxyport YES -cltTimeout {
 Timeout }
  -svrTimeout {
 Timeout }
  -CKA NO -TCPB NO -CMP YES
add serviceGroup CAS_servicegroup_rpc_epm TCP -maxClient 0 -maxReq 0 -
   cip DISABLED -usip NO -SP OFF -useproxyport YES -cltTimeout {
 Timeout }
  -svrTimeout {
 Timeout }
  -CKA NO -TCPB NO -CMP NO
bind serviceGroup CAS_servicegroup_http {
 CAS-1 Server }
  80 -CustomServerID ""None""
bind serviceGroup CAS_servicegroup_http {
 CAS-2 Server }
  80 -CustomServerID ""None""
bind serviceGroup CAS_servicegroup_rpc_epm {
 CAS-1 Server }
  135 -CustomServerID ""None""
bind serviceGroup CAS_servicegroup_rpc_epm {
 CAS-2 Server }
  135 -CustomServerID ""None""
<!--NeedCopy-->
```

Monitores:

```
add lb monitor CAS_monitor_rpc_epm TCP -LRTM ENABLED -destPort 135
add lb monitor mon_http_ecv HTTP-ECV -recv 403 -LRTM DISABLED
bind serviceGroup CAS_servicegroup_http -monitorName mon_http_ecv
bind serviceGroup CAS_servicegroup_rpc_epm -monitorName
   CAS_monitor_rpc_epm
<!--NeedCopy-->
```

Servidores virtuales de equilibrio de carga:

```
add lb vserver CAS_vserver_owa SSL 0.0.0.0 0 -persistenceType
   COOKIEINSERT -timeout {
 PersTimeout }
  -lbMethod LEASTCONNECTION -cltTimeout {
 Timeout }
```



```
5
6  add lb vserver CAS_vserver_as SSL 0.0.0.0 0 -persistenceType RULE -
       timeout {
7   PersTimeout }
8    -lbMethod LEASTCONNECTION -rule "HTTP.REQ.HEADER("Authorization")" -
         cltTimeout {
9   Timeout }
10
11 add lb vserver CAS_vserver_oa SSL 0.0.0.0 0 -timeout {
12  PersTimeout }
13   -lbMethod LEASTCONNECTION -cltTimeout {
14  Timeout }
15
16 add lb vserver CAS_vserver_ews SSL 0.0.0.0 0 -timeout {
17  PersTimeout }
18   -lbMethod LEASTCONNECTION -cltTimeout {
19  Timeout }
20
21 add lb vserver CAS_vserver_ad SSL 0.0.0.0 0 -timeout {
22  PersTimeout }
23   -lbMethod LEASTCONNECTION -cltTimeout {
24  Timeout }
25
26 add lb vserver CAS_vserver_oab SSL 0.0.0.0 0 -timeout {
27  PersTimeout }
28   -lbMethod LEASTCONNECTION -cltTimeout {
29  Timeout }
30
31 set ssl vserver CAS_vserver_owa -sslRedirect ENABLED
32 bind ssl vserver CAS_vserver_owa -certkeyName {
33  CertKey }
34
35 bind ssl vserver CAS_vserver_oab -certkeyName {
36  CertKey }
37
38 bind ssl vserver CAS_vserver_as -certkeyName {
39  CertKey }
40
41 bind ssl vserver CAS_vserver_oa -certkeyName {
42  CertKey }
43
44 bind ssl vserver CAS_vserver_ews -certkeyName {
45  CertKey }
46
47 bind ssl vserver CAS_vserver_ad -certkeyName {
```



```
 CertKey }

bind lb vserver CAS_vserver_owa CAS_servicegroup_http
bind lb vserver CAS_vserver_oab CAS_servicegroup_http
bind lb vserver CAS_vserver_as CAS_servicegroup_http
bind lb vserver CAS_vserver_oa CAS_servicegroup_http
bind lb vserver CAS_vserver_ews CAS_servicegroup_http
bind lb vserver CAS_vserver_ad CAS_servicegroup_http
add lb vserver CAS_vserver_rpc_epm TCP {
 RPC Public IP }
  135 -timeout {
 PersTimeout }
  -cltTimeout {
 Timeout }
  -comment "vserver for RPC End Point Mapper"
bind lb vserver CAS_vserver_rpc_epm CAS_servicegroup_rpc_epm
<!--NeedCopy-->
```

Grupo de persistencia:

```
add lb group CAS_persistency_group_sourceip
bind lb group CAS_persistency_group_sourceip CAS_vserver_oa
bind lb group CAS_persistency_group_sourceip CAS_vserver_oab
bind lb group CAS_persistency_group_sourceip CAS_vserver_ews
bind lb group CAS_persistency_group_sourceip CAS_vserver_ad
bind lb group CAS_persistency_group_sourceip CAS_vserver_rpc_epm
set lb group CAS_persistency_group_sourceip -persistenceType SOURCEIP -
    timeout {
 PersTimeout }

<!--NeedCopy-->
```

Cambio de contenido para servicios HTTP:

```
add cs vserver CAS_vserver_cs SSL {
 Public IP }
  443 -cltTimeout {
 Timeout }
  -caseSensitive OFF -comment "Exchange CS VServer"
bind ssl vserver CAS_vserver_cs -certkeyName {
 CertKey }

```



```
add cs action CAS_action_cs_owa -targetLBVserver CAS_vserver_owa
add cs action CAS_action_cs_oab -targetLBVserver CAS_vserver_oab
add cs action CAS_action_cs_as -targetLBVserver CAS_vserver_as
add cs action CAS_action_cs_oa -targetLBVserver CAS_vserver_oa
add cs action CAS_action_cs_ews -targetLBVserver CAS_vserver_ews
add cs action CAS_action_cs_autodiscover -targetLBVserver
    CAS_vserver_ad
add cs policy CAS_policy_cs_owa -rule "HTTP.REQ.URL.SET_TEXT_MODE(
    IGNORECASE).STARTSWITH("/owa")" -action CAS_action_cs_owa
add cs policy CAS_vserver_oab -rule "HTTP.REQ.URL.SET_TEXT_MODE (
    IGNORECASE).STARTSWITH("/OAB")"
add cs policy CAS_policy_cs_as -rule "HTTP.REQ.URL.SET_TEXT_MODE(
    IGNORECASE).STARTSWITH("/Microsoft-Server-ActiveSync")" -action
    CAS_action_cs_as
add cs policy CAS_policy_cs_autodiscover -rule "HTTP.REQ.URL.
    SET_TEXT_MODE(IGNORECASE).STARTSWITH("/Autodiscover")" -action
    CAS_action_cs_autodiscover
add cs policy CAS_policy_cs_oa -rule "HTTP.REQ.URL.SET_TEXT_MODE(
    IGNORECASE).STARTSWITH("/rpc")" -action CAS_action_cs_oa
add cs policy CAS_policy_cs_ews -rule "HTTP.REQ.URL.SET_TEXT_MODE(
    IGNORECASE).STARTSWITH("/EWS")" -action CAS_action_cs_ews

bind cs vserver CAS_vserver_cs -policyName CAS_policy_cs_oa -priority
    90
bind cs vserver CAS_vserver_cs -policyName CAS_policy_cs_owa -priority
    100
bind cs vserver CAS_vserver_cs -policyName CAS_policy_cs_oab -priority
    100
bind cs vserver CAS_vserver_cs -policyName CAS_policy_cs_as -priority
    110
bind cs vserver CAS_vserver_cs -policyName CAS_policy_cs_autodiscover -
    priority 120
bind cs vserver CAS_vserver_cs -policyName CAS_policy_cs_ews -priority
    130
bind cs vserver CAS_vserver_cs -lbvserver CAS_vserver_owa
<!--NeedCopy-->
```

Ejemplos de configuración recomendados para versiones de Microsoft Exchange server inferiores a 2016

Grupos de servicios adicionales:


```
add serviceGroup CAS_servicegroup_rpc_ca TCP -maxClient 0 -maxReq 0 -
    cip DISABLED -usip NO -SP OFF -useproxyport YES -cltTimeout {
 Timeout }
  -svrTimeout {
 Timeout }
  -CKA NO -TCPB NO -CMP NO
add serviceGroup CAS_servicegroup_rpc_ab TCP -maxClient 0 -maxReq 0 -
    cip DISABLED -usip NO -SP OFF -useproxyport YES -cltTimeout {
 Timeout }
  -svrTimeout {
 Timeout }
  -CKA NO -TCPB NO -CMP NO
bind serviceGroup CAS_servicegroup_rpc_ca {
 CAS-1 Server }
  {
 CA Port }
  -CustomServerID ""None""
bind serviceGroup CAS_servicegroup_rpc_ca {
 CAS-2 Server }
  {
 CA Port }
  -CustomServerID ""None""
bind serviceGroup CAS_servicegroup_rpc_ab {
 CAS-1 Server }
  {
 AB Port }
  -CustomServerID ""None""
bind serviceGroup CAS_servicegroup_rpc_ab {
 CAS-2 Server }
  {
 AB Port }
  -CustomServerID ""None""
<!--NeedCopy-->
```

Monitores adicionales:

```
add lb monitor CAS_monitor_rpc_ca TCP -LRTM ENABLED -destPort {
 CA Port }

add lb monitor CAS_monitor_rpc_ab TCP -LRTM ENABLED -destPort {
 AB Port }

bind serviceGroup CAS_servicegroup_rpc_ca -monitorName
```



```
    CAS_monitor_rpc_ca
bind serviceGroup CAS_servicegroup_rpc_ab -monitorName
    CAS_monitor_rpc_ab
<!--NeedCopy-->
```

Servidores virtuales de equilibrio de carga adicionales:

```
add lb vserver CAS_vserver_rpc_ab TCP {
 RPC Public IP }
  {
 AB Port }
  -timeout {
 PersTimeout }
  -cltTimeout {
 Timeout }
  -comment ”vserver for  RPC Address Book”
add lb vserver CAS_vserver_rpc_ca TCP {
 RPC Public IP }
  {
 CA Port }
  -timeout {
 PersTimeout }
  -cltTimeout {
 Timeout }
  -comment ”vserver for  RPC Client Access”
bind lb vserver CAS_vserver_rpc_ab CAS_servicegroup_rpc_ab
bind lb vserver CAS_vserver_rpc_ca CAS_servicegroup_rpc_ca
<!--NeedCopy-->
```

Grupo de persistencia adicional:

```
bind lb group CAS_persistency_group_sourceip CAS_vserver_rpc_ab
bind lb group CAS_persistency_group_sourceip CAS_vserver_rpc_ca
<!--NeedCopy-->
```

Ejemplos de configuración recomendados para versiones de Microsoft Exchange server 2016 y posteriores

Servidor virtual de equilibrio de carga adicional:


```
add lb vserver CAS_vserver_mapi SSL 0.0.0.0 0 -timeout {
 PersTimeout }
  -lbMethod LEASTCONNECTION -cltTimeout {
 Timeout }

bind ssl vserver CAS_vserver_mapi -certkeyName {
 CertKey }

bind lb vserver CAS_vserver_mapi CAS_servicegroup_http
<!--NeedCopy-->
```

Grupo de persistencia adicional:

```
bind lb group CAS_persistency_group_sourceip CAS_vserver_mapi
<!--NeedCopy-->
```

Cambio de contenido para servicios HTTP:

```
add cs action CAS_action_cs_mapi -targetLBVserver CAS_vserver_mapi
add cs policy CAS_policy_cs_mapi -rule "HTTP.REQ.URL.SET_TEXT_MODE(
    IGNORECASE).STARTSWITH("/mapi")" -action CAS_action_cs_mapi
bind cs vserver CAS_vserver_cs -policyName CAS_policy_cs_mapi -priority
     140
<!--NeedCopy-->
```

Configuraciones opcionales

Redirección HTTPS para Outlook Web App (OWA):

```
add lb vserver CAS_vserver_owa_http_redirect HTTP {
 HTTP Public IP }
  80 -persistenceType COOKIEINSERT -timeout {
 PersTimeout }
  -lbMethod ROUNDROBIN -redirectURL "https://mail.example.com/owa" -
      cltTimeout {
 Timeout }

<!--NeedCopy-->
```


NOTA: Reemplácelo por la URL de redirección HTTPS adecuada.

Directiva de reescritura /owa:

```
add rewrite action owa_rewrite replace http.REQ.URL ""/owa""
add rewrite policy owa_rewrite_policy "http.req.url.eq("/")"
   owa_rewrite
bind lb vserver CAS_vserver_owa -policyName owa_rewrite_policy -
   priority 100 -gotoPriorityExpression END -type REQUEST
add responder action action_responder_owa redirect ""https://www.
   example.com/owa""
add responder policy_responder_owa HTTP.REQ.IS_VALID
   action_responder_owa
set responder param -undefAction NOOP
bind lb vserver CAS_vserver_owa -policyName policy_responder_owa -
   priority 100 -gotoPriorityExpression END -type REQUEST
<!--NeedCopy-->
```

NOTA: Reemplácelo por la URL de redirección HTTPS adecuada.

Soporte para SMTP:

Para la siguiente configuración, USIP debe estar habilitado para que los servidores CAS puedan ver la dirección IP del servidor SMTP que envía para su validación. Esta configuración también requiere que la puerta de enlace predeterminada del servidor CAS esté configurada para apuntar a la dirección SNIP del dispositivo ADC.

```
add lb vserver CAS_vserver_smtp TCP {
 HTTP Public IP }
  25 -persistenceType SOURCEIP -timeout 60 -lbMethod LEASTCONNECTION -
     cltTimeout 30
add serviceGroup CAS_servicegroup_smtp TCP -maxClient 0 -maxReq 0 -cip
   DISABLED -usip YES -SP OFF -useproxyport YES -cltTimeout 30 -
   svrTimeout 30 -CKA NO -TCPB NO -CMP NO
bind serviceGroup CAS_servicegroup_smtp {
 CAS-1 Server }
  25 -CustomServerID ""None"" bind serviceGroup CAS_servicegroup_smtp {
 CAS-2 Server }
  25 -CustomServerID ""None""
bind lb vserver CAS_vserver_smtp CAS_servicegroup_smtp
<!--NeedCopy-->
```

Compatibilidad con el protocolo de correos versión 3 (POP3):


```
add lb vserver CAS_vserver_pop3 TCP {
 HTTP Public IP }
  110 -persistenceType SOURCEIP -timeout {
 PersTimeout }
  -lbMethod LEASTCONNECTION -cltTimeout {
 Timeout }

add serviceGroup CAS_servicegroup_pop3 TCP -maxClient 0 -maxReq 0 -cip
    DISABLED -usip NO -SP OFF -useproxyport YES -cltTimeout {
 Timeout }
  -svrTimeout {
 Timeout }
  -CKA NO -TCPB NO -CMP NO
bind serviceGroup CAS_servicegroup_pop3 {
 CAS-1 Server }
  110 -CustomServerID ""None"" bind serviceGroup CAS_servicegroup_pop3
      {
 CAS-2 Server }
  110 -CustomServerID ""None""
bind lb vserver CAS_vserver_pop3 CAS_servicegroup_pop3
<!--NeedCopy-->
```

> Nota:
>
> Puede realizar la configuración anterior para POP3 con cifrado SSL cambiando el puerto a 995 y los tipos de servidor/servicio virtual a SSL. También vincular un certificado SSL adecuado.

Soporte para IMAP:

```
add lb vserver CAS_vserver_imap TCP {
 HTTP Public IP }
  143 -persistenceType SOURCEIP -timeout {
 PersTimeout }
  -lbMethod LEASTCONNECTION -cltTimeout {
 Timeout }

add serviceGroup CAS_servicegroup_imap TCP -maxClient 0 -maxReq 0 -cip
    DISABLED -usip NO -SP OFF -useproxyport YES -cltTimeout {
 Timeout }
  -svrTimeout {
 Timeout }
  -CKA NO -TCPB NO -CMP NO
```



```
bind serviceGroup CAS_servicegroup_imap {
 CAS-1 Server }
  143 -CustomServerID ""None"" bind serviceGroup CAS_servicegroup_imap
     {
 CAS-2 Server }
  143 -CustomServerID ""None""
bind lb vserver CAS_vserver_imap CAS_servicegroup_imap
<!--NeedCopy-->
```

> Nota:
>
> Puede realizar la configuración anterior para IMAP cifrado SSL cambiando el puerto a 993 y los tipos de servidor/servicio virtual a SSL. También vincular un certificado SSL adecuado.

Otros recursos

- Configuración de servidores de equilibrio de carga para Microsoft Exchange con filtrado de seguridad de correo electrónico
- Implementación de NetScaler con Microsoft Exchange 2016

Orden de prioridad para servicios de equilibrio de carga

January 21, 2022

La función de orden de prioridad para los servicios le permite priorizar el orden de los servicios o grupos de servicios en función de las preferencias de selección de equilibrio de carga. Puede configurar el orden de prioridad si hace lo siguiente:

- Enlazar un servicio a un servidor virtual de equilibrio de carga.
- Enlazar un grupo de servicios a un servidor virtual de equilibrio de carga.
- Enlaza un miembro del grupo de servicios al grupo de servicios de equilibrio de carga.

Actualmente, puede configurar el orden de prioridad de los servicios mediante los siguientes enfoques. Sin embargo, estos enfoques tienen las siguientes limitaciones:

- Configuración de una cadena de servidores virtuales de reserva: El número de líneas de configuración es alto y debe ejecutar el comando `show` varias veces para conocer el estado de todos los servicios LB para cada servidor virtual.
- Configuración de la ubicación preferida: debe crear entradas de ubicación para todos los puntos finales de la aplicación.

La función de orden de prioridad para los servicios aborda las limitaciones anteriores con menos comandos de configuración y le ayuda a realizar la configuración de ubicación preferida sin la necesidad de representar la ubicación de todas las direcciones IP de los servicios de equilibrio de carga.

Configurar el orden de prioridad para los servicios de equilibrio de carga

Para configurar el orden de prioridad de los servicios de equilibrio de carga, el`-order <number>` parámetro se agrega a los comandos bind.

> **Nota:**
>
> El número de pedido más bajo tiene la prioridad más alta.

Comando:

```
bind lb vserver <vservername> <servicename/servicegroupname> -order <number
>
```

Por ejemplo, considere un conjunto de servicios que están enlazados a un servidor virtual de equilibrio de carga (vs1). Con el
`- order <number>`parámetro, puede priorizar el orden de selección de los servicios de la siguiente manera:

- Conjunto 1 (s1, s2) vinculado a vs1 — orden 1
- Conjunto 2 (s3, s4) vinculado a vs1 — orden 2
- Conjunto 3 (s5, s6) vinculado a vs1 — orden 3

Después de vincular los servicios a vs1 y cuando vs1 recibe el tráfico del cliente, el orden de selección de los servicios es el siguiente:

- El servidor virtual (vs1) selecciona primero los servicios del conjunto 1 (s1 y s2) con el número de pedido 1, porque a este conjunto se le asigna el número de pedido más bajo. De forma predeterminada, el número de pedido más bajo tiene la prioridad más alta.
- Si todos los servicios del conjunto 1 están DESACTIVADOS, vs1 selecciona el conjunto 2 (s3 y s4) con el número de pedido 2.
- Si todos los servicios en el conjunto 1 y el conjunto 2 están inactivos, vs1 selecciona el conjunto 3 (s5 y s6) con el número de pedido 3.

Configurar el orden de prioridad para los servicios de equilibrio de carga mediante la CL

Para configurar el orden de prioridad de los servicios de equilibrio de carga, escriba los siguientes comandos en el símbolo del sistema:

1. Agregue un servidor virtual LB.


```
add lb vserver vs1 HTTP 1.1.1.1 80
```

2. Agregue los servicios LB.

```
add service s[1-6] 2.2.2.[1-6] HTTP 80
```

3. Establezca el número de pedido y vincule los servicios al servidor virtual LB.

```
bind lb vserver vs1 s1 -order 1
bind lb vserver vs1 s2 -order 1
bind lb vserver vs1 s3 -order 2
bind lb vserver vs1 s4 -order 2
bind lb vserver vs1 s5 -order 3
bind lb vserver vs1 s6 -order 3
```

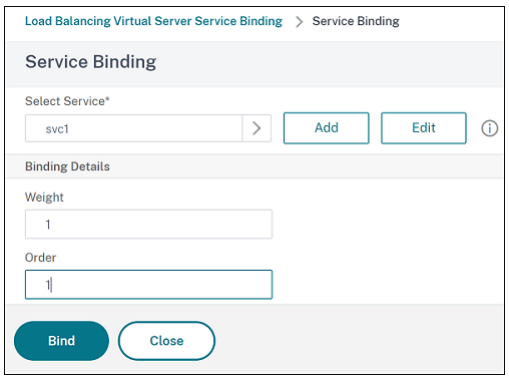
Configurar el orden de prioridad para los servicios de equilibrio de carga mediante la interfaz

Requisitos previos:

- Ha creado un servidor virtual de equilibrio de carga.
- Ha creado servicios.

Para configurar el orden de prioridad de los servicios de equilibrio de carga y vincularlos al servidor virtual, haga lo siguiente:

1. Vaya a**Administración del tráfico > Equilibrio de carga > Servidores virtuales**y haga doble clic en el servidor virtual de equilibrio de carga.
2. En **Servidor virtual de equilibrio de carga**, en la sección **Servicios y grupos de servicios**, haga clic en Enlace de **servicio de servidor virtual de equilibrio de carga**.
3. En el cuadro de diálogo**Enlace de servicio de servidor virtual de equilibrio de carga**, haga clic en**Agregar enlace**.
4. En el cuadro**de diálogo Enlace**de servicios, seleccione un servicio.
5. Escriba un número en el campo **Pedido**para establecer el orden de prioridad del servicio.



6. Haga clic en **Vincular**
7. Repita los pasos del 1 al 6 para configurar un número de orden de prioridad diferente para diferentes servicios.

Configurar el orden de prioridad para los servicios de equilibrio de carga mediante comandos de directiva LB

De forma predeterminada, el número de pedido más bajo tiene la prioridad más alta. Sin embargo, puede diferir este comportamiento predeterminado mediante los nuevos comandos de acción y directiva de LB. Puede configurar el orden de selección de servicios en función del tráfico de clientes entrantes o los datos de los clientes.

Por ejemplo, considere un conjunto de servicios que están enlazados a un servidor virtual (vs1). Con el- `order <number>`parámetro, ha configurado el orden de prioridad para los servicios de la siguiente manera:

- Conjunto 1 (s1, s2) vinculado a vs1 — orden 1
- Conjunto 2 (s3, s4) vinculado a vs1 — orden 2
- Conjunto 3 (s5, s6) vinculado a vs1 — orden 3

De forma predeterminada, el número de pedido más bajo tiene la prioridad más alta. Por lo tanto, el orden de prioridad predeterminado es 1, 2 y 3 para los servicios del conjunto 1, conjunto 2 y conjunto 3, respectivamente. Sin embargo, para un tráfico de clientes específico, quiere cambiar el orden de prioridad a 3, 1 y 2. Para lograr esto, puede agregar una directiva LB y vincularla a vs1.

Un comando de directiva de LB consta de dos elementos: una regla y una acción. La regla se asocia a una acción, que se lleva a cabo si una solicitud coincide con la regla.

> **Nota:**
>
> Los comandos de directiva LB son comunes para la configuración LB y GSLB y se aplican a las solicitudes administradas por el dispositivo Citrix ADC.

Acción LB

Expresión:

```
add lb action <name> <type> <string>
```

Ejemplo:

```
add lb action act1 -type SELECTIONORDER -value 3 2 1
```

Parámetros:

- `name`: Nombre de la acción.
- `type`: Tipo de acción.
- `string`: valor de la acción especificada.

Directiva de LB

Expresión:

```
add lb policy <name> <rule> <action> <undefaction>
```

Ejemplo:

```
add lb policy pol1 -rule CLIENT.IP.SRC.EQ(8.8.8.8)-action act1
```

Parámetros:

- `name`: Nombre de la directiva.
- `rule`: Una regla se compone de una o más expresiones. La regla se asocia a una acción, que se lleva a cabo si la solicitud coincide con la regla.
- `action`: Se admiten DROP, NOLBACTION y RESET.
- `undefaction`: El dispositivo Citrix ADC genera un evento indefinido (evento UNDEF) cuando una solicitud no coincide con una directiva. Puede usar el `set lb param -undefAction <action>`comando para establecer la acción indefinida. Puede asignar estas acciones a un evento indefinido: DROP, NOLBACTION y RESET.

Consideremos un ejemplo en el que agrega una acción LB, una directiva LB y vincula la directiva a un servidor virtual de equilibrio de carga (vs1) de la siguiente manera:

```
add lb action act1 -type SELECTIONORDER -value 3 1 2
```

```
add lb policy pol1 -rule CLIENT.IP.SRC.EQ(8.8.8.8)-action act1
```

```
bind lb vserver vs1 -policyName pol1 -priority 10
```

La regla selecciona el tráfico del cliente que coincide con la dirección IP y envía ese tráfico a vs1. `8.8.8.8` El tipo de acción LB (`SELECTIONORDER`) define el orden de selección de servicios. Después

de vincular la directiva LB a vs1 y cuando vs1 recibe el tráfico del cliente desde la dirección IP`8.8.8.8`, los servicios se seleccionan en el siguiente orden:

1. El servidor virtual (vs1) selecciona los servicios en el conjunto 3 (s5 y s6) con el orden de prioridad 3.
2. Si todos los servicios en el conjunto 3 están DESACTIVADOS, vs1 selecciona el conjunto 1 (s1 y s2) con el orden de prioridad 2.
3. Si todos los servicios en el conjunto 3 y el conjunto 2 están inactivos, vs1 selecciona el conjunto 1 (s1 y s2) con el orden 1.

Configurar el orden de prioridad para los servicios de equilibrio de carga con comandos de directiva LB mediante la CLI

Para configurar el orden de prioridad para los servicios de equilibrio de carga mediante los comandos de directiva LB, escriba los siguientes comandos en el símbolo del sistema:

1. Agregue una acción LB.

   ```
   add lb action act1 -type SELECTIONORDER -value 3 1 2
   ```

2. Agregue una directiva de LB.

   ```
   add lb policy pol1 -rule CLIENT.IP.SRC.EQ(8.8.8.8)-action act1
   ```

3. Agregue un servidor virtual LB.

   ```
   add lb vserver vs1 HTTP 1.1.1.1 80
   ```

4. Enlazar la directiva LB al servidor virtual LB.

   ```
   bind lb vs vs1 -policyName pol1 -priority 10
   ```

5. Agregue los servicios LB.

   ```
   add service s[1-6] 2.2.2.[1-6] HTTP 80
   ```

6. Establezca el orden y vincule los servicios al servidor virtual LB.

   ```
   bind lb vserver vs1 s1 -order 1

   bind lb vserver vs1 s2 -order 1

   bind lb vserver vs1 s3 -order 2

   bind lb vserver vs1 s4 -order 2

   bind lb vserver vs1 s5 -order 3

   bind lb vserver vs1 s6 -order 3
   ```


Configurar el orden de prioridad para los servicios de equilibrio de carga con los comandos de directiva LB mediante la GUI

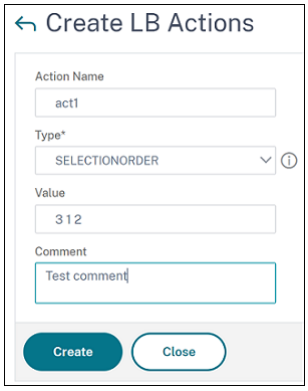
Requisitos previos:

- Ha creado un servidor virtual de equilibrio de carga.
- Ha creado servicios.

Paso 1: crear una acción LB:

1. Vaya a **AppExpert > LB > Acciones**.
2. En**LB Actions**, haga clic en**Agregar**.
3. En el cuadro de diálogo**Crear acciones LB**, especifique los valores para los siguientes parámetros:
   - **Nombre de acción**: act1
   - **Tipo**: SELECTIONORDER
   - **Valor**: 3 1 2

     > **Nota:**
     >
     > Los números del campo **Valor**están separados por un espacio.

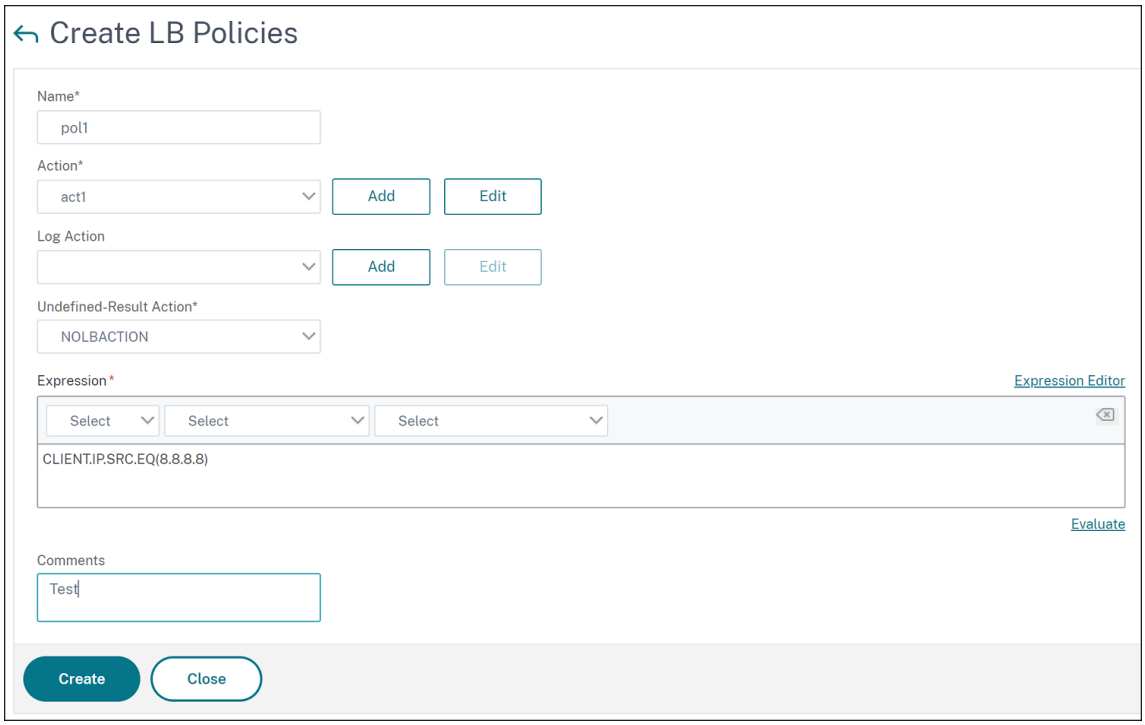


4. Haga clic en **Crear**.

Paso 2: Cree una directiva de LB:

1. Vaya a **AppExpert > LB > Directivas**.
2. En**Directivas de LB**, haga clic en**Agregar**.
3. En el cuadro de diálogo**Crear directivas LB**, especifique los valores para los siguientes parámetros:
   - **Nombre**: pol1
   - **Acción**: act1
   - **Acción de resultado indefinido**: NOLBACTION

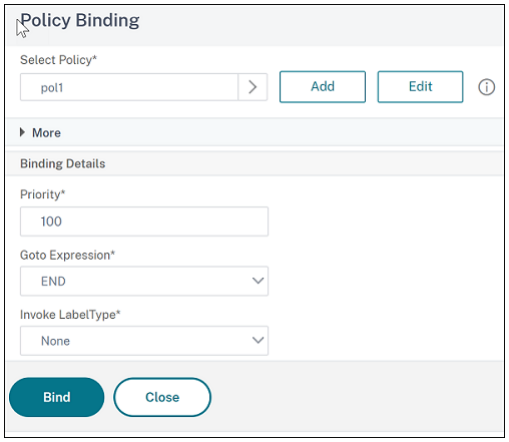
- **Expresión**: CLIENT.IP.SRC.EQ (8.8.8.8)



4. Haga clic en**Crear**.

Paso 3: Enlazar la directiva LB al servidor virtual LB:

1. Vaya a**Administración del tráfico > LB > Servidores virtuales**y haga doble clic en el servidor virtual.
2. En**Configuración avanzada**, haga clic en**Directivas**.
3. En la sección**Directivas**, haga clic en el icono más (+).
4. En el cuadro **de diálogo Elegir tipo**, especifique los valores de los siguientes parámetros:
   - **Seleccione una directiva**: LB
   - **Elija el tipo**: Solicitud
5. Haga clic en **Agregar enlace**.
6. En el cuadro de diálogo **Enlace de directivas**, especifique los valores para los siguientes parámetros:
   - **Seleccione la directiva**: pol 1
   - **Prioridad**: 10
   - **Expresión de Goto**: END
   - **Invoke LabelType**: Ninguno



7. Haga clic en **Bind**.

Paso 4: Configurar el orden de prioridad para los servicios de equilibrio de carga:

Para configurar el orden de prioridad para los servicios de equilibrio de carga, consulte el procedimiento **Configurar el orden de prioridad para los servicios de equilibrio de carga mediante la GUI**.

Configuración de persistencia para los servicios

Si la persistencia está configurada para un servicio, siempre se da preferencia a la persistencia, de forma predeterminada.

Por ejemplo, considere un servicio con persistencia configurada y orden de prioridad 1. Si un servicio con orden de prioridad 0 está ACTIVO, entonces siempre se da preferencia al servicio con orden de prioridad 1.

Sin embargo, puede anular este comportamiento predeterminado con el siguiente comando de la CLI:

```
set lb param -overridePersistencyforOrder <YES/NO>
```

Consideremos el siguiente ejemplo:

Un conjunto de servicios está enlazado a un servidor virtual (vs1) con el siguiente orden de prioridad:

- Conjunto 1 (s1, s2) vinculado a vs1 — orden 1
- Conjunto 2 (s3, s4) vinculado a vs1 — orden 2

Escriba el siguiente comando en el símbolo del sistema para anular la persistencia:

```
set lb parameter -overridePersistencyforOrder YES
```

Si el conjunto 1 (los servicios con persistencia están configurados) está ABAJO, los servicios establecidos 2 gestionan todas las solicitudes hasta que los servicios del conjunto 1 estén ACTIVOS. Se crea una entrada de persistencia para la prioridad 2.

Supongamos que después de algún tiempo, los servicios del conjunto 1 están ACTIVOS. Ahora, los servicios set 1 y set 2 están ARRIBA para gestionar las solicitudes. En este caso, se toman nuevas decisiones de equilibrio de carga a medida que los servicios de orden superior están ACTIVOS. La entrada de persistencia se anula con una nueva entrada de equilibrio de carga.

Alternar prioridad

Con la función de alternancia de prioridad, puede alternar todo el tráfico a un servicio de baja prioridad durante la actualización de la versión para un servicio con un orden de prioridad más alto. Puede usar los siguientes comandos para alternar la prioridad:

- `set lb vserver -toggleorder<Ascending/Descending>`
- `set lb vserver v1 -orderthreshold 80`

Por ejemplo, consideremos que hay dos servicios con las siguientes prioridades:

- Service 1- order 0
- Servicio 2 — pedido 1

De forma predeterminada, el servicio 1 gestiona todo el tráfico. Si el servicio 1 necesita actualizarse, entonces el tráfico debe reencaminarse al servicio 2.

En el símbolo del sistema, escriba los siguientes comandos para alternar la prioridad:

```
set lb vserver -toggleorder Descending
```

De forma predeterminada, 0 tiene una prioridad más alta. Sin embargo, después de la conmutación de prioridades, 1 se considera una prioridad más alta. Si la entrada de persistencia está presente para el servicio, el comportamiento de preferencia de persistencia es el que se explica en la sección **Configuración de persistencia para los servicios**.

Caso de uso 1: Equilibrio de carga SMPP

August 20, 2021

Millones de mensajes cortos se intercambian diariamente entre individuos y proveedores de servicios de valor agregado, como bancos, anunciantes y servicios de directorio, mediante el protocolo de mensajes cortos peer to peer (SMPP). A menudo, la entrega de mensajes se retrasa porque los servidores están sobrecargados y el tráfico no se distribuye de manera óptima entre los servidores. Citrix ADC admite el equilibrio de carga SMPP y proporciona una distribución óptima de mensajes entre los servidores, lo que evita un rendimiento deficiente y las interrupciones.

Citrix ADC realiza el equilibrio de carga en el lado del servidor cuando se reciben mensajes de clientes y en el lado del cliente cuando se reciben mensajes de servidores.

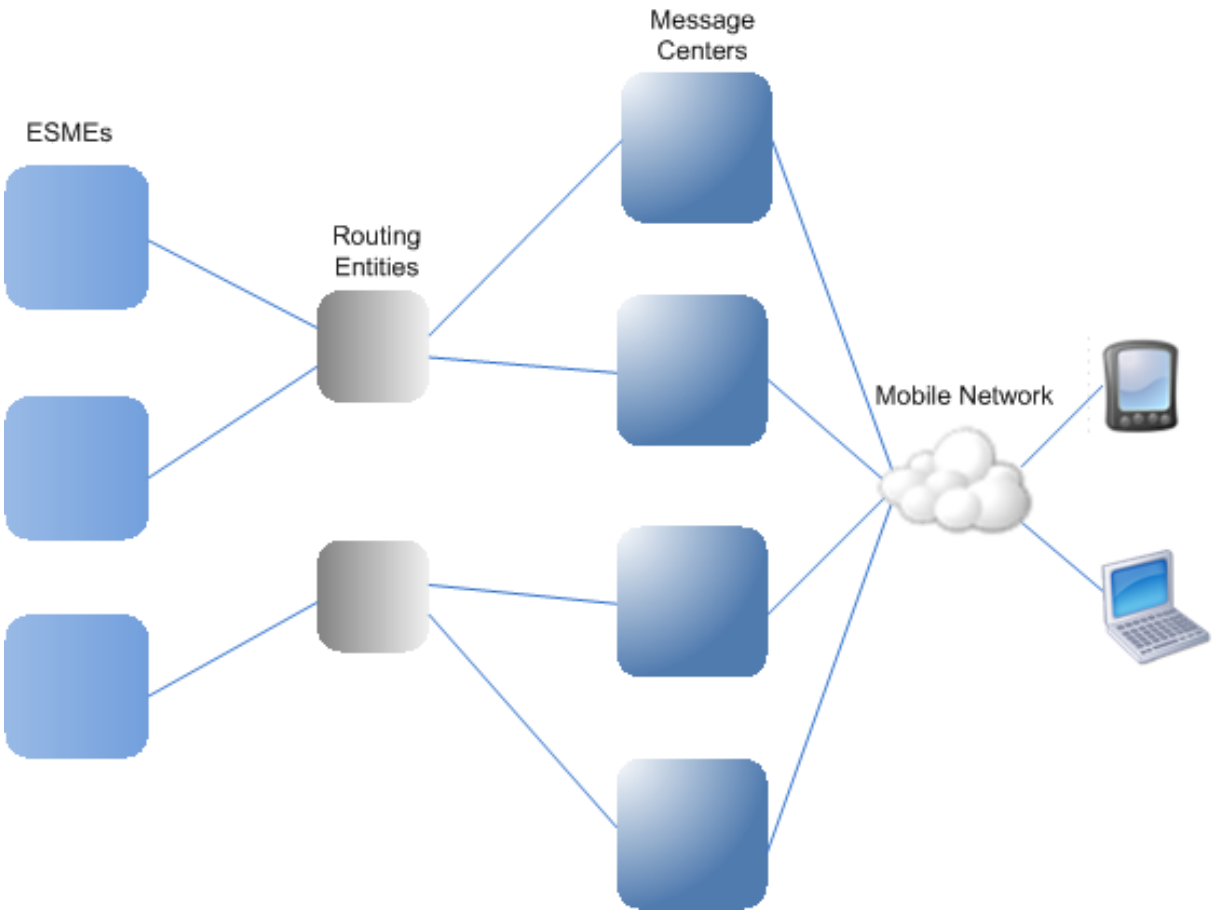
El equilibrio de carga de los mensajes SMPP por Citrix ADC proporciona las siguientes ventajas:

- Mejor distribución de la carga en los servidores, lo que se traduce en un tiempo de respuesta más rápido para los usuarios finales
- Supervisión del estado de los servidores y mejores capacidades de conmutación por error
- Adición rápida y sencilla de nuevos servidores (centros de mensajes) sin cambiar la configuración del cliente
- Alta disponibilidad

Introducción a SMPP

SMPP es un protocolo de capa de aplicación para la transferencia de mensajes cortos entre entidades externas de mensajes cortos (ESME), entidades de redirección (RE) y centros de mensajes (MC) a través de conexiones TCP de larga duración. Se utiliza para enviar mensajes de servicio de mensajes cortos (SMS) entre amigos, contactos y terceros como bancos (banca móvil), anunciantes (comercio móvil) y servicios de directorio. Los mensajes de una ESME (entidad no móvil) llegan al MC, que los distribuye a entidades de mensajes cortos (PYME), como teléfonos móviles. SMPP también es utilizado por las PYME para enviar mensajes cortos a terceros (por ejemplo, para la compra de productos, el pago de facturas y la transferencia de fondos). Estos mensajes llegan al MC y se reenvían al MC de destino o ESME.

El siguiente diagrama muestra las diferentes entidades SMPP: ESMES, Res y MCs, en una red móvil.



Descripción general de la arquitectura de las diferentes entidades SMPP en una red móvil

Nota: Los términos cliente y ESME se utilizan indistintamente en todo el documento.

Un ESME (cliente) abre una conexión al MC en uno de los tres modos: Como transmisor, receptor o transceptor. Como transmisor, solo puede enviar mensajes para su entrega. Como receptor, solo puede recibir mensajes. Como transceptor, el ESME puede enviar y recibir mensajes. El ESME envía al MC uno de los tres mensajes (también conocidos como PDU): Bind_transmitter, bind_receiver o bind_transceiver. El MC responde con bind_transmitter_resp, bind_receiver_resp o bind_transceiver_resp, según corresponda para la solicitud.

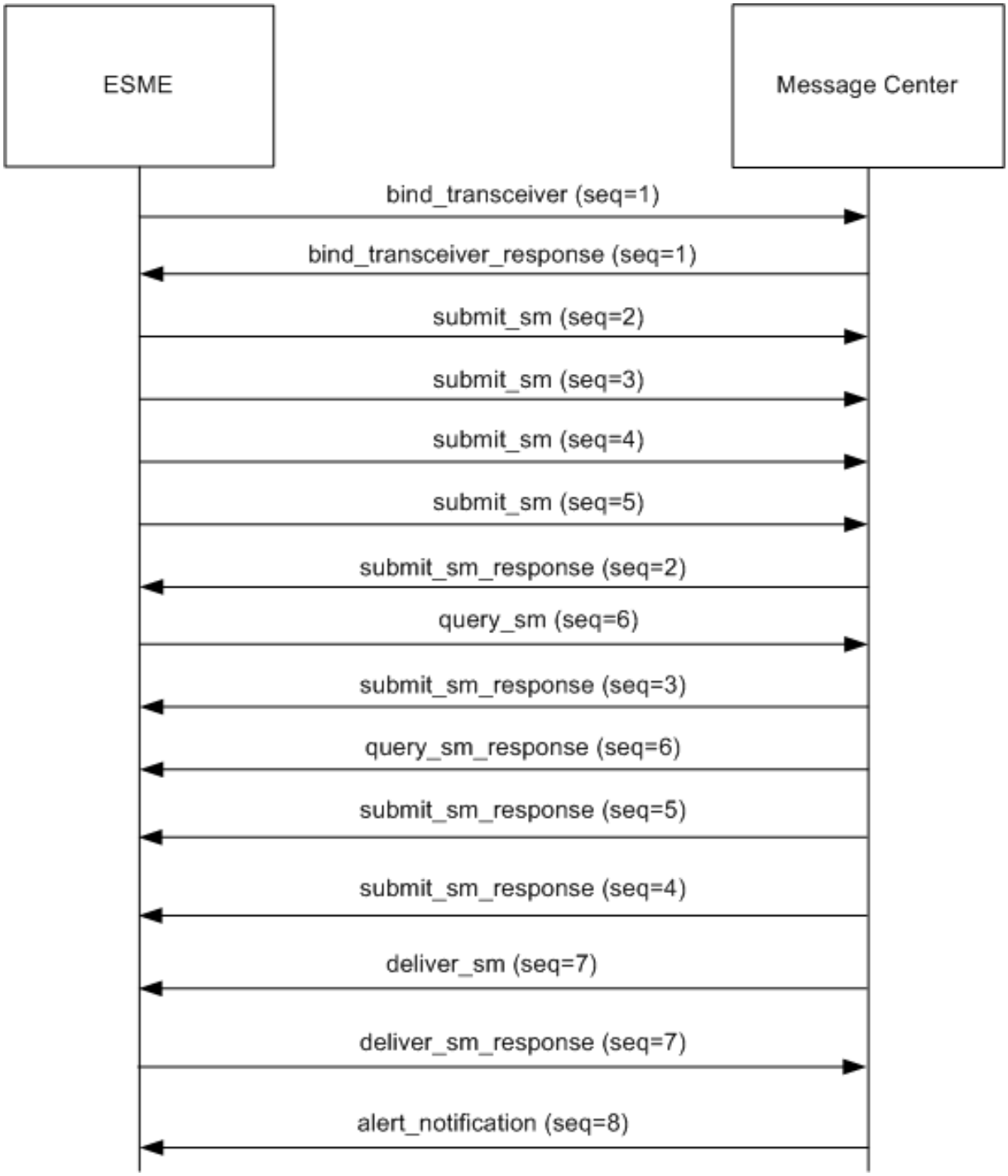
Una vez establecida la conexión, el ESME puede, dependiendo del modo en el que esté enlazado al MC, enviar un mensaje submit_sm o data_sm, recibir un mensaje deliver_sm o data_sm, o enviar y recibir cualquiera de estos tipos de mensajes. El ESME también puede enviar mensajes auxiliares, como query_sm, replace_sm y cancel_sm, para consultar el estado de una entrega de mensajes anterior, reemplazar un mensaje anterior por un mensaje nuevo o cancelar un mensaje no entregado.

Si no se entrega un mensaje porque un ESME no está disponible o un suscriptor móvil no está conec-

tado, el mensaje se pone en cola. Más tarde, cuando el MC detecta que el suscriptor móvil es ahora accesible, envía una PDU de notificación de alerta a la ESME a través de una sesión de receptor o transceptor, solicitando la entrega de cualquier mensaje en cola.

Cada PDU de solicitud tiene un número de secuencia único. La PDU de respuesta tiene el mismo número de secuencia que la solicitud original. Dado que el intercambio de mensajes a través de SMPP puede estar en modo asíncrono, un ESME o un MC pueden enviar varias solicitudes a la vez. El número de secuencia juega un papel crucial en la devolución de la respuesta en la misma sesión SMPP. En otras palabras, el número de secuencia hace posible la coincidencia de solicitudes y respuestas.

El siguiente diagrama muestra cómo el flujo de tráfico utiliza las distintas PDU cuando ESME se vincula como transceptor.



Limitación:

El dispositivo Citrix ADC no admite operaciones salientes. Es decir, un centro de mensajes no puede iniciar una sesión SMPP con un ESME a través del dispositivo Citrix ADC.

Cómo funciona el equilibrio de carga SMPP en Citrix ADC

Un ESME (cliente) envía un mensaje de enlace para abrir una conexión con Citrix ADC. El ADC autentica cada ESME y, si tiene éxito, responde con un mensaje apropiado. Citrix ADC establece una conexión con cada centro de mensajes y equilibra la carga todos los mensajes entre estos centros de mensajes. Cuando el ADC recibe un mensaje de un cliente, vuelve a utilizar una conexión abierta al centro de mensajes o envía una solicitud de enlace a un centro de mensajes si no hay disponible una conexión abierta.

El ADC puede equilibrar la carga mensajes procedentes de los clientes y de los servidores. Puede supervisar el estado de los centros de mensajes y manejar mensajes concatenados. También proporciona compatibilidad con el cambio de contenido para los centros de mensajes.

Mensajes que se originan desde los eMES

Cada ESME debe agregarse como usuario en Citrix ADC para la autenticación. El cliente establece una conexión TCP con un servidor virtual SMPP configurado en el ADC mediante el envío de una solicitud de enlace. El ADC autentica el cliente y, si tiene éxito, analiza el mensaje de enlace. A continuación, el ADC envía la solicitud al centro de mensajes seleccionado por el método de equilibrio de carga configurado. Si una conexión con el centro de mensajes no está disponible para su reutilización, el ADC abre una conexión TCP con el centro de mensajes enviando una nueva solicitud de enlace al centro de mensajes.

Antes de reenviar la respuesta (submit_sm_resp o data_sm_resp) desde el centro de mensajes al cliente, el ADC agrega un identificador de servidor personalizado al identificador del mensaje para identificar el centro de mensajes para operaciones auxiliares, como consultar, reemplazar o cancelar solicitudes de un mensaje, realizadas por el cliente. Las solicitudes de otros clientes se equilibran de la misma manera.

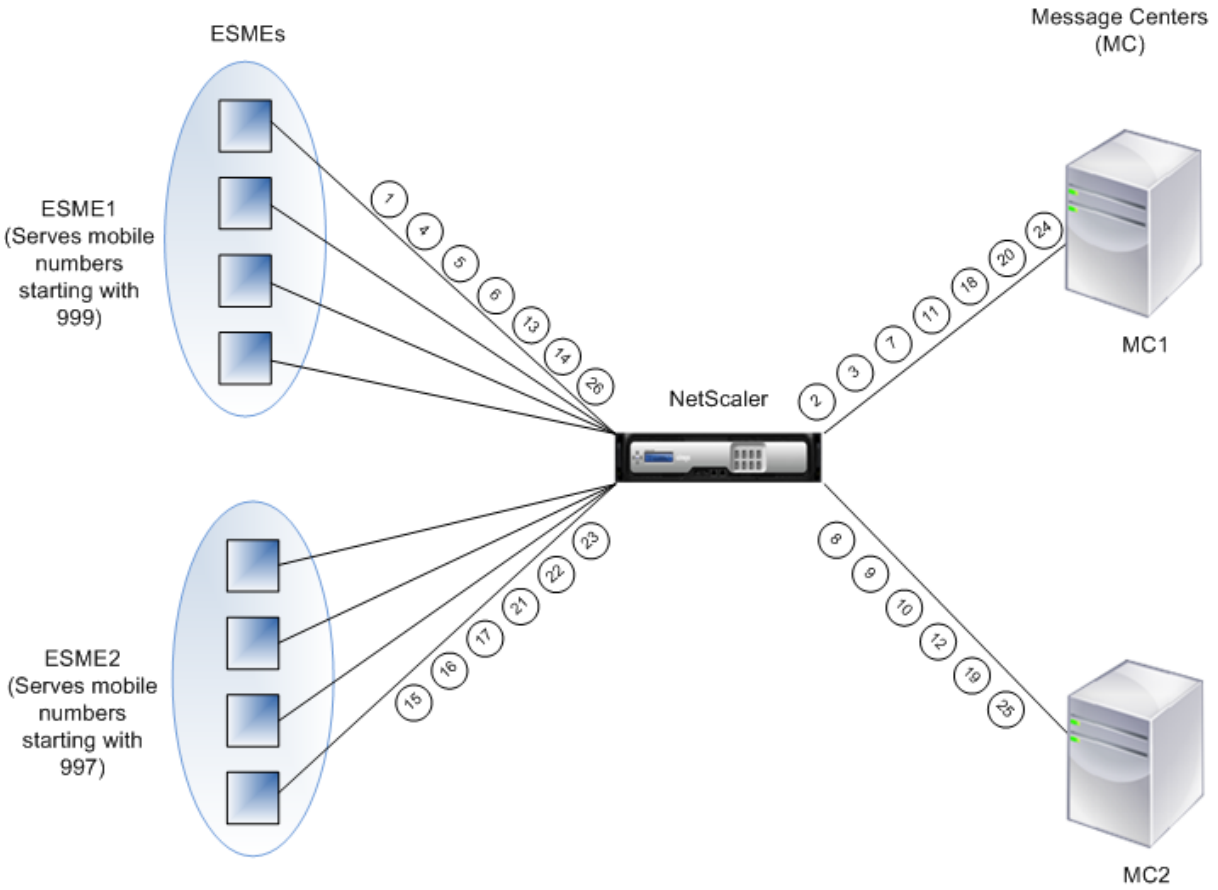
En la solicitud de enlace original, un cliente especifica el rango de direcciones que puede servir. Este intervalo se utiliza para reenviar mensajes deliver_sm o data_sm desde los centros de mensajes a los clientes.

Mensajes que se originan desde un centro de mensajes

Los ESME que pueden manejar un intervalo de direcciones específico se agrupan en un clúster. Todos los nodos de un clúster proporcionan las mismas credenciales. Dentro de un clúster, solo se utiliza el método round robin para el equilibrio de carga. Para entregar mensajes móviles originados (MO), el centro de mensajes envía un mensaje deliver_sm al Citrix ADC. Si un clúster que puede servir el intervalo de direcciones de destino (por ejemplo, números que comienzan por 998) está enlazado al ADC, selecciona ese clúster y, a continuación, equilibra la carga el mensaje entre los nodos ESME de ese clúster.

Si un ESME que puede servir mensajes deliver_sm para el intervalo de direcciones no está enlazado al ADC y la cola de mensajes está habilitada, el mensaje se pone en cola hasta que dicho cliente se vincule al ADC en un modo receptor o transceptor. Puede especificar el tamaño de la cola.

El siguiente diagrama ilustra el flujo interno de PDU entre ESMES, Citrix ADC y los centros de mensajes. Para simplificar, solo se muestran dos ESMES y dos centros de mensajes.



Flujo de mensajes (PDU):

1. ESME1 envía una solicitud de enlace a NetScaler
2. NetScaler envía una solicitud de enlace a MC1
3. MC1 envía una respuesta de enlace a NetScaler
4. NetScaler envía una respuesta de enlace a ESME1
5. ESME1 envía submit_sm (1) a NetScaler
6. ESME1 envía submit_sm (2) a NetScaler
7. NetScaler reenvía submit_sm (1) a MC1
8. NetScaler envía una solicitud de enlace a MC2
9. MC2 envía una respuesta de enlace a NetScaler
10. NetScaler reenvía submit_sm (2) a MC2
11. MC1 envía submit_sm_resp (1) a NetScaler
12. MC2 envía submit_sm_resp (2) a NetScaler

13. NetScaler reenvía submit_sm_resp (1) a ESME1
14. NetScaler reenvía submit_sm_resp (2) a ESME1
15. ESME2 envía una solicitud de enlace a NetScaler
16. NetScaler envía una respuesta de enlace a ESME2
17. ESME2 envía submit_sm (3) a NetScaler
18. NetScaler reenvía submit_sm (3) a MC1
19. MC2 envía deliver_sm a NetScaler (ESME2 sirve el intervalo de direcciones especificado en el mensaje)
20. MC1 envía submit_sm_resp (3) a NetScaler
21. NetScaler reenvía submit_sm_resp (3) a ESME2
22. NetScaler reenvía deliver_sm a ESME2
23. ESME2 envía deliver_sm_resp a NetScaler
24. MC1 envía alert_notification a NetScaler (ESME1 sirve el intervalo de direcciones especificado en el mensaje)
25. NetScaler reenvía deliver_sm_resp a MC2
26. NetScaler reenvía la alert_notification a ESME1

Supervisión de Salud de Centros de Mensajes

De forma predeterminada, un monitor TCP_Default está enlazado a un servicio SMPP, pero puede enlazar un monitor personalizado de tipo SMPP. El monitor personalizado abre una conexión TCP al centro de mensajes y envía un paquete enquire_link. En función del éxito o el fallo del sondeo, el servicio se marca hacia arriba o hacia abajo.

Cambio de contenido en centros de mensajes

Los centros de mensajes pueden aceptar varias conexiones (o enlazar solicitudes) de ESMES. Puede configurar Citrix ADC para cambiar contenido estas solicitudes en función de los parámetros de enlace de SMPP. A continuación se presentan algunas expresiones comunes para configurar métodos para seleccionar un centro de mensajes:

- Basado en el intervalo de direcciones: En la siguiente expresión de ejemplo, el ADC selecciona un centro de mensajes específico si el intervalo de direcciones comienza en 988.

Ejemplo:

SMPP.BINDINFO.ADDRESS_RANGE.CONTAINS(“^988”)

- Basado en el ID de ESME: En la siguiente expresión de ejemplo, el ADC selecciona un centro de mensajes específico si el ID de ESME es igual a ESME1.

Ejemplo:

SMPP.BINDINFO.SYSTEM_ID.EQ (“ESME1”)

- Basado en el tipo ESME: En la siguiente expresión de ejemplo, el ADC selecciona un centro de mensajes específico si el tipo ESME es VMS. VMS significa sistema de correo de voz.

Ejemplo:

SMPP.BINDINFO.SYSTEM_TYPE.EQ (“VMS”)

- Según el tipo de número (TON) de ESME: En la siguiente expresión de ejemplo, el ADC selecciona un centro de mensajes específico si TON es igual a 1 (1 significa un número internacional).

Ejemplo:

SMPP.BINDINFO.ADDR_TON.EQ (1)

- Basado en el indicador de plan numérico (NPI) de ESME: En la siguiente expresión de ejemplo, el ADC selecciona un centro de mensajes específico si NPI es igual a 0 (0 representa una conexión desconocida).

Ejemplo:

SMPP.BINDINFO.ADDR_NPI.EQ (0)

- Basado en el tipo de enlace: En la siguiente expresión de ejemplo, el ADC selecciona un centro de mensajes específico si el tipo de enlace es TRANSCEPTER. (Un transceptor puede enviar y recibir mensajes.)

Ejemplo:

SMPP.BINDINFO.TYPE.EQ (TRANSCEPTOR)

Manejo de mensajes concatenados

Un SMS puede contener un máximo de 140 bytes. Los mensajes más largos deben dividirse en partes más pequeñas. Si el móvil de destino es capaz, los mensajes se combinan y se entregan como un SMS largo. Citrix ADC reenvía los fragmentos de un mensaje al mismo centro de mensajes. Cada mensaje contiene un número de referencia, un número de secuencia y el número total de fragmentos. El número de referencia es el mismo para cada fragmento de un mensaje largo. El número de secuencia especifica la posición del fragmento en particular en el mensaje completo. Después de recibir todos los fragmentos, ESME combina los fragmentos en un mensaje largo y entrega el mensaje al suscriptor móvil.

Si un cliente se desconecta de una conexión activa, la conexión al centro de mensajes no se cierra. Se reutiliza para solicitudes de otros clientes.

Limitación

Los ID de mensaje, desde el centro de mensajes, no son compatibles con más de 59 bytes. Si la longitud del identificador del mensaje devuelto por el centro de mensajes es superior a 59 bytes, las

operaciones auxiliares fallan y Citrix ADC responde con un mensaje de error.

Configuración del equilibrio de carga SMPP en Citrix ADC

Realice las siguientes tareas para configurar el equilibrio de carga SMPP en el ADC:

1. Agregue un usuario SMPP. El ADC autentica al usuario antes de aceptar una solicitud de enlace del usuario. El usuario suele ser un ESME.
2. Agregue un servidor virtual de equilibrio de carga, especificando el protocolo como SMPP.
3. Agregue un servicio, especificando el protocolo como SMPP y un identificador de servidor personalizado que sea único para cada servidor. Enlace el servicio al servidor virtual de equilibrio de carga creado anteriormente.
4. Opcionalmente, cree un grupo de servicios y agregue servicios al grupo de servicios.
5. Opcionalmente, agregue un monitor de tipo SMPP-ECV y vincularlo al servicio. Un monitor TCP predeterminado está enlazado de forma predeterminada.
6. Establezca los parámetros SMPP, como el modo cliente y la cola de mensajes.

Para configurar el equilibrio de carga SMPP mediante la línea de comandos

En el símbolo del sistema, escriba:

```
add smpp user <username> -password <password>
add service <name> <IP> SMPP <port>  - customserverID <customserverID>
add lb vserver <name> <IP> SMPP <port>
bind lb vserver <name> <service name>
set smpp param
<!--NeedCopy-->
```

Ejemplo

```
add smpp user smppclient1 -password c03ebb540695b6110eb31172f32245a1 -
    encrypted -encryptmethod ENCMTHD_2
add smpp user smppclient2 -password c03ebb540695b6110eb31172f32245a1 -
    encrypted -encryptmethod ENCMTHD_2
add service smmpsvc 10.102.84.140 SMPP 2775 -gslb NONE -maxClient 0 -
    maxReq 0 -cip DISABLED -usip NO -useproxyport YES -sp ON -cltTimeout
     180 -svrTimeout 360 -CustomServerID ab -CKA NO -TCPB NO -CMP NO
add service smmpsvc2 10.102.81.175 SMPP 2775 -gslb NONE -maxClient 0 -
    maxReq 0 -cip DISABLED -usip NO -useproxyport YES -sp ON -cltTimeout
     180 -svrTimeout 360 -CustomServerID xy -CKA NO -TCPB NO -CMP NO
```



```
5 add lb vserver smppvs SMPP 10.102.239.179 2775 -persistenceType NONE -
     cltTimeout 180
6 bind lb vserver smppvs smmpsvc2
7 bind lb vserver smppvs smmpsvc
8 set smpp param -addrrange "d*"
9 <!--NeedCopy-->
```

Para configurar el equilibrio de carga SMPP mediante la utilidad de configuración

1. Vaya a **Sistema > Administración de usuarios > Usuarios de SMPP**y agregue un usuario SMPP.
2. Vaya a **Administración del tráfico > Equilibrio de carga > Configurar parámetros SMPP**y establezca los parámetros según lo requiera la implementación.
3. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**y agregue un servidor virtual de tipo SMPP.
4. Haga clic en la sección Servicio, agregue un servicio de tipo SMPP y especifique un ID de servidor.

Caso de uso 2: Configurar la persistencia basada en reglas basada en un par nombre-valor en una secuencia de bytes TCP

August 20, 2021

Algunos protocolos transmiten pares nombre-valor en una secuencia de bytes TCP. El protocolo de la secuencia de bytes TCP en este ejemplo es el protocolo Financial Information Exchange (FIX). En la implementación no XML, el protocolo FIX permite que dos hosts que se comunican a través de una red intercambien información empresarial o relacionada con el comercio como una lista de pares nombre-valor (denominados "campos FIX"). El formato del campo es <tag>=<value><delimiter>. Este formato tradicional de valor de etiqueta hace que el protocolo FIX sea ideal para el caso de uso.

La etiqueta de un campo FIX es un identificador numérico que indica el significado del campo. En el ejemplo;

- La etiqueta 35 indica el tipo de mensaje.
- El valor después del signo igual contiene un significado específico para la etiqueta dada y está asociado con un tipo de datos. El valor A para la etiqueta 35 indica que el mensaje es un mensaje de inicio de sesión.
- El delimitador es el carácter ASCII "Start of Header" (SOH) no imprimible (0x01), que es el símbolo de intercalación (^).
- A cada campo también se le asigna un nombre. El campo con etiqueta 35 es el campo MsgType.

A continuación se muestra un ejemplo de un mensaje de inicio de sesión.

8=FIX.4.1 9=61 35=A 49=INVMGR 56=BRKR 34=1 52=20000426-12:05:06 98=0 108=30 10=157

Su elección del tipo de persistencia para una lista de valores de etiqueta como la que se muestra arriba está determinada por las opciones disponibles para extraer una cadena determinada de la lista. Los métodos de persistencia basados en token requieren que especifique el desplazamiento y la longitud del token que quiere extraer de la carga útil. El protocolo FIX no permite hacerlo, porque el desplazamiento de un campo determinado y la longitud de su valor pueden variar de un mensaje a otro. Esta variación depende del tipo de mensaje, de los campos anteriores y de la longitud de los valores anteriores. También varía según la implementación de una a otra, en función de si se han definido campos personalizados. Tales variaciones hacen que sea imposible predecir el desplazamiento exacto de un campo dado o especificar la longitud del valor que se va a extraer como el token. En este caso, por lo tanto, la persistencia basada en reglas es el tipo de persistencia preferido.

Supongamos que un servidor virtual fixlb1 equilibra la carga de las conexiones TCP a un conjunto de servidores que aloja instancias de una aplicación habilitada para Fix. Desea configurar la persistencia para las conexiones sobre la base del valor del campo SenderCompid, que identifica a la empresa que envía el mensaje. La etiqueta de este campo FIX es 49 (se muestra en el ejemplo de mensaje de inicio de sesión anterior).

Para configurar la persistencia basada en reglas para el servidor virtual de equilibrio de carga, establezca el tipo de persistencia para el servidor virtual de equilibrio de carga en RULE y configure el parámetro de regla con una expresión. La expresión debe ser aquella que extraiga la parte de la carga útil TCP en la que se espera encontrar el campo SenderCompid, cree la cadena resultante en una lista nombre-valor basada en los delimitadores y, a continuación, extraiga el valor del campo SenderCompid (etiqueta 49), de la siguiente manera:

```
set lb vserver fixlb1 -persistenceType RULE -rule ”CLIENT.TCP.PAYLOAD(300).
TYPECAST_NVLIST_T('=','^').VALUE(”\49\”)”
```

Nota: Los caracteres de barra invertida se han utilizado en la expresión porque se trata de un comando CLI. Si está usando la utilidad de configuración, no introduzca los caracteres de barra invertida.

Si el cliente envía un mensaje FIX que contiene la lista nombre-valor en el ejemplo de mensaje de inicio de sesión anterior, la expresión extrae el valor INVMGR y el dispositivo Citrix ADC crea una sesión de persistencia basada en este valor.

El argumento de la función PAYLOAD () puede ser tan grande como considere necesario para incluir el campo SenderCompid en la cadena extraída por la función. Opcionalmente, puede utilizar la función SET_TEXT_MODE (IGNORECASE) si desea que el dispositivo ignore el caso al extraer el valor del campo y la función HASH para crear una sesión de persistencia basada en un hash del valor extraído. La siguiente expresión utiliza las funciones SET_TEXT_MODE (IGNORECASE) y HASH:

```
CLIENT.TCP.PAYLOAD(500).TYPECAST_NVLIST_T('=','^').SET_TEXT_MODE(IGNORECASE
).VALUE(”49”).HASH
```


A continuación se presentan más ejemplos de reglas que puede utilizar para configurar la persistencia de conexiones FIX (reemplace <tag> por la etiqueta del campo cuyo valor quiere extraer):

- Para extraer el valor de cualquier campo FIX en los primeros 300 bytes de la carga útil TCP, puede utilizar la expresión CLIENT.TCP.PAYLOAD(300).BEFORE_STR("^").AFTER_STR("<tag>=").
- Para extraer una cadena de 20 bytes de longitud en el desplazamiento 80, convertir la cadena en una lista nombre-valor y, a continuación, extraer el valor del campo que quiera, utilice la expresión CLIENT.TCP.PAYLOAD(100).SUBSTR(80,20).TYPECAST_NVLIST_T('=','^').VALUE("<tag>").
- Para extraer los primeros 100 bytes de la carga útil TCP, convertir la cadena en una lista nombre-valor y extraer el valor de la tercera aparición del campo que quiera, utilice la expresión CLIENT.TCP.PAYLOAD(100).TYPECAST_NVLIST_T('=','^').VALUE("<tag>",2).
  Nota: Si el segundo argumento que se pasa a la función
  VALUE() es
  n, el dispositivo extrae el valor de la instancia
  (n+1)
  th del campo porque el recuento comienza desde cero (
  0).

A continuación se presentan más ejemplos de reglas que puede utilizar para configurar la persistencia. Solo las expresiones basadas en la carga útil pueden evaluar los datos que se transmiten a través del protocolo FIX. Las otras expresiones son expresiones más generales para configurar la persistencia basada en protocolos de red más bajos.

- CLIENT.TCP.PAYLOAD (100)
- CLIENT.TCP.PAYLOAD (100) .HASH
- CLIENT.TCP.PAYLOAD (100) .SUBSTR (5,10)
- CLIENT.TCP.SRCPORT
- CLIENT.TCP.DSTPORT
- CLIENT.IP.SRC
- CLIENT.IP.DST
- CLIENT.IP.SRC.GET4
- CLIENT.IP.DST.GET4
- CLIENT.ETHER.SRCMAC.GET6
- CLIENT.ETHER.DSTMAC.GET5
- CLIENT.VLAN.ID

Caso de uso 3: Configurar el equilibrio de carga en el modo de retorno directo del servidor

August 20, 2021

El equilibrio de carga en modo de retorno directo del servidor (DSR) permite al servidor responder a los clientes directamente mediante una ruta de retorno que no fluye a través del dispositivo Citrix ADC. Sin embargo, en el modo DSR, el dispositivo puede continuar realizando comprobaciones de estado de los servicios. En un entorno de gran volumen de datos, el envío de tráfico del servidor directamente al cliente en modo DSR aumenta la capacidad general de gestión de paquetes del dispositivo porque los paquetes no fluyen a través del dispositivo.

El modo DSR tiene las siguientes funciones y limitaciones:

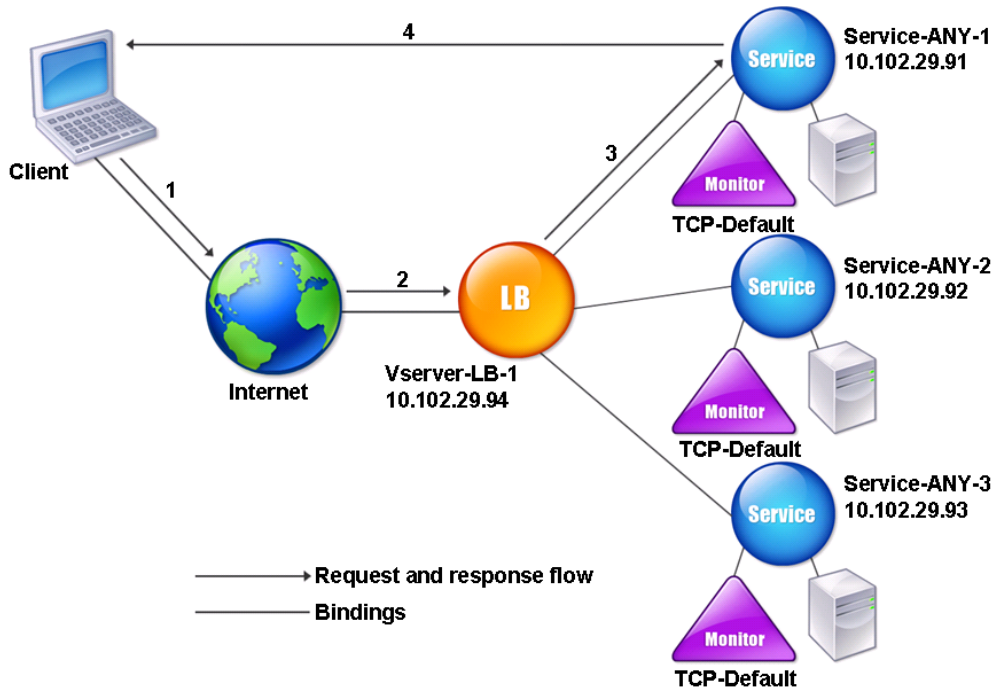
- Es compatible con el modo de un brazo y el modo en línea.
- El dispositivo agota las sesiones en función del tiempo de espera inactivo.
- Dado que el dispositivo no realiza un proxy de conexiones TCP (es decir, no envía SYN-ACK al cliente), no cierra los ataques SYN. Mediante el filtro de velocidad de paquetes SYN, puede controlar la velocidad de SYN al servidor. Para controlar la tasa de SYN, establezca un umbral para la tasa de SYN. Para obtener protección contra ataques SYN, debe configurar el dispositivo para proxy de conexiones TCP. Sin embargo, esto requiere que el tráfico inverso fluya a través del dispositivo.
- En una configuración DSR, el dispositivo Citrix ADC no reemplaza la dirección IP del servidor virtual de equilibrio de carga con la dirección IP del servidor de destino. En su lugar, reenvía paquetes a un servicio mediante la dirección MAC del servidor. El VIP debe estar configurado en el servidor y ARP debe estar inhabilitado para el VIP que está configurado en el servidor. Al hacerlo, se evita que la solicitud del cliente omite el dispositivo cuando se configura en modo de un brazo. Por ejemplo, un usuario debe configurar VIP en la interfaz de bucle inactivo y inhabilitar el ARP para el mismo VIP.
- El dispositivo obtiene la dirección MAC del servidor del monitor vinculado al servicio. Sin embargo, los monitores de usuario personalizados (monitores de tipo USER), que utilizan scripts almacenadas en el dispositivo Citrix ADC, no aprenden la dirección MAC de un servidor. Si solo utiliza monitores personalizados en una configuración DSR, para cada solicitud que reciba el servidor virtual, el dispositivo intentará resolver la dirección IP de destino en una dirección MAC (enviando solicitudes ARP). Dado que la dirección IP de destino es una dirección IP virtual propiedad del dispositivo Citrix ADC, las solicitudes ARP siempre se resuelven en la dirección MAC de la interfaz Citrix ADC. Por lo tanto, todo el tráfico recibido por el servidor virtual se devuelve al dispositivo. Si utiliza monitores de usuario en una configuración DSR, también debe configurar otro monitor de un tipo diferente (por ejemplo, un monitor PING) para los servicios, idealmente con un intervalo más largo entre sondeos, de modo que pueda aprenderse la dirección MAC de los servidores.
- El dispositivo Citrix ADC aprende los parámetros L2 del servidor desde el monitor enlazado al servicio. Para los monitores UDP-ECV, configure una cadena de recepción para permitir que el dispositivo aprenda los parámetros L2 del servidor. Si la cadena de recepción no está configurada y el servidor no responde, el dispositivo no aprende los parámetros L2, pero el servicio está configurado en UP. El tráfico de este servicio está bloqueado.

En el caso de ejemplo, los servicios Service-ANY-1, Servicio-ANY-2 y Servicio-ANY-3 se crean y vinculan al servidor virtual VServer-LB-1. La carga del servidor virtual equilibra la solicitud del cliente a un servicio y el servicio responde a los clientes directamente, sin pasar por alto el dispositivo Citrix ADC. En la siguiente tabla se enumeran los nombres y valores de las entidades configuradas en el dispositivo Citrix ADC en modo DSR.

Tipo de entidad	Nombre	Dirección IP	Protocolo
Servidor virtual	Vserver-LB-1	10.102.29.94	CUALQUIERA
Servicios	Service-ANY-1	10.102.29.91	CUALQUIERA
	Service-ANY-2	10.102.29.92	CUALQUIERA
	Service-ANY-3	10.102.29.93	CUALQUIERA
Monitores	TCP	Ninguno	Ninguno

El siguiente diagrama muestra las entidades de equilibrio de carga y los valores de los parámetros que se configurarán en el dispositivo.

Ilustración 1. Modelo de entidad para equilibrio de carga en el modelo DSR



Para que el dispositivo funcione correctamente en modo DSR, la dirección IP de destino en la solicitud del cliente debe no modificarse. En su lugar, el dispositivo cambia la MAC de destino por la del servidor seleccionado. Esta configuración permite al servidor determinar la dirección MAC del cliente para reenviar solicitudes al cliente mientras se omite el servidor.

A continuación, configura una configuración de equilibrio de carga básica como se describe en Configuración del equilibrio de carga básico, nombrando las entidades y configurando los parámetros mediante los valores descritos en la tabla anterior.

Después de configurar la configuración básica de equilibrio de carga, debe personalizarla para el modo DSR. Para ello, configure un método de equilibrio de carga compatible, como el método Hash IP de origen con un servidor virtual sin sesión. También debe establecer el modo de redirección para que el servidor pueda determinar la dirección MAC del cliente para reenviar las respuestas y omitir el dispositivo.

Después de configurar el método de equilibrio de carga y el modo de redirección, debe habilitar el modo USIP en cada servicio. A continuación, el servicio utiliza la dirección IP de origen al reenviar las respuestas.

Para configurar el método de equilibrio de carga y el modo de redirección para un servidor virtual sin sesión mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
1 set lb vserver <vServerName> -lbMethod <LBMethodOption> -m <
     RedirectionMode> -sessionless <Value>
2 <!--NeedCopy-->
```

Ejemplo

```
1 set lb vserver Vserver-LB-1 -lbMethod SourceIPHash -m MAC -sessionless
     enabled
2 <!--NeedCopy-->
```

> **Nota**
>
> Para un servicio enlazado a un servidor virtual en el que la opción MAC -m está habilitada, debe enlazar un monitor que no sea usuario.

Para configurar el método de equilibrio de carga y el modo de redirección para un servidor virtual sin sesión mediante la utilidad de configuración

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. Abra un servidor virtual, seleccione Modo de redirección como basado en MAC y método como SOURCEIPHASH.
3. En Configuración del tráfico, seleccione Equilibrio de carga sin sesión.

Para configurar un servicio para que utilice la dirección IP de origen mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
set service <ServiceName> -usip <Value>
<!--NeedCopy-->
```

Ejemplo:

```
set service Service-ANY-1 -usip yes
<!--NeedCopy-->
```

Para configurar un servicio para que utilice la dirección IP de origen mediante la utilidad de configuración

1. Vaya a **Administración de Tráfico > Equilibrio de carga > Servicios**.
2. Abra un servicio y, en Configuración de tráfico, seleccione **Usar dirección IP de origen**.

Se requieren algunos pasos adicionales en ciertas situaciones, que se describen en las secciones siguientes.

Caso de uso 4: Configurar servidores LINUX en modo DSR

August 20, 2021

El sistema operativo LINUX requiere que configure una interfaz de bucle invertido con la dirección IP virtual (VIP) del dispositivo Citrix ADC en cada servidor equilibrado de carga del clúster DSR.

Para configurar el servidor LINUX en modo DSR

Para crear una interfaz de bucle hacia atrás con el VIP del dispositivo Citrix ADC en cada servidor con equilibrio de carga, en el símbolo del sistema operativo Linux escriba los siguientes comandos:

```
ifconfig dummy0 up

ifconfig dummy0:0 inet <netscaler vip> netmask 255.255.255.255 up

echo 1 > /proc/sys/net/ipv4/conf/dummy0/arp_ignore

echo 2 > /proc/sys/net/ipv4/conf/dummy0/arp_announce
<!--NeedCopy-->
```

A continuación, ejecute el software que reasigna el ID de TOS a VIP.

Nota: Agregue las asignaciones correctas al software antes de ejecutarlo. En los comandos anteriores, el servidor LINUX utiliza dummy0 para conectarse a la red. Cuando utilice este comando, escriba el nombre de la interfaz que el servidor LINUX utiliza para conectarse a la red.

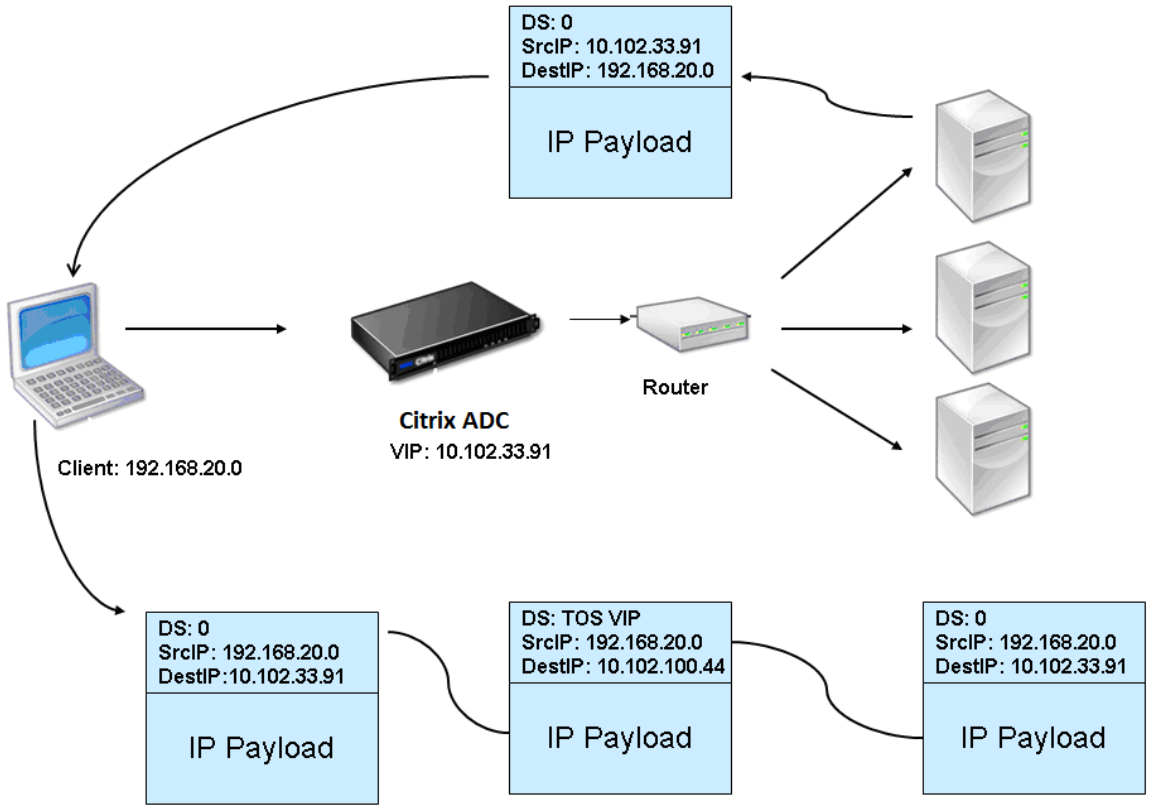
Caso de uso 5: Configure el modo DSR cuando use TOS

August 20, 2021

Servicios diferenciados (DS), también conocidos como TOS (Tipo de servicio), es un campo que forma parte del encabezado de paquete IPv4. El campo equivalente en el encabezado IPv6 es Clase de tráfico. TOS es utilizado por los protocolos de capa superior para optimizar la ruta de un paquete. La información TOS codifica la dirección IP virtual (VIP) del dispositivo Citrix ADC y los servidores con equilibrio de carga extraen el VIP.

En el caso siguiente, el dispositivo agrega el VIP al campo **TOS** del paquete y, a continuación, reenvía el paquete al servidor de carga equilibrada. A continuación, el servidor con equilibrio de carga responde directamente al cliente, omitiendo el dispositivo, como se ilustra en el siguiente diagrama.

Ilustración 1. El dispositivo Citrix ADC en modo DSR con TOS



La función TOS se personaliza para un entorno controlado de la siguiente manera:

- El entorno no debe tener ningún dispositivo con estado, como firewall con estado y puertas de enlace TCP, en la ruta entre el dispositivo y los servidores con equilibrio de carga.
- Los enrutadores de todos los puntos de entrada a la red deben quitar el campo TOS de todos los paquetes entrantes para asegurarse de que el servidor equilibrado de carga no confunde otro campo TOS con el agregado por el dispositivo.
- Cada servidor puede tener solo 63 VIP.
- El router intermedio no debe enviar mensajes de error ICMP con respecto a la fragmentación. El cliente no entiende el mensaje, ya que la dirección IP de origen es la dirección IP del servidor con equilibrio de carga y no el VIP de Citrix ADC.
- TOS es válido solo para servicios basados en IP. No puede utilizar servicios basados en nombres de dominio con TOS.

En el ejemplo, Service-Any-1 se crea y se vincula al servidor virtual VServer-lb-1. La carga del servidor virtual equilibra la solicitud del cliente al servicio y el servicio responde a los clientes directamente, sin pasar por el dispositivo. En la tabla siguiente se enumeran los nombres y valores de las entidades configuradas en el dispositivo en modo DSR.

Tipo de entidad	Nombre	Dirección IP	Protocolo
Servidor virtual	Vserver-LB-1	10.102.33.91	CUALQUIERA
Servicios	Service-ANY-1	10.102.100.44	CUALQUIERA
Monitores	PING	Ninguno	Ninguno

DSR con TOS requiere que el equilibrio de carga esté configurado en la capa 3. Para configurar una configuración básica de equilibrio de carga para la capa 3, consulte Configuración del equilibrio de carga básico. Asigne un nombre a las entidades y establezca los parámetros mediante los valores descritos en la tabla anterior.

Después de configurar la configuración de equilibrio de carga, debe personalizar la configuración de equilibrio de carga para el modo DSR configurando el modo de redirección para que el servidor pueda descapsular el paquete de datos y, a continuación, responder directamente al cliente y omitir el dispositivo.

Después de especificar el modo de redirección, puede habilitar opcionalmente el dispositivo para supervisar el servidor de forma transparente. Esto permite que el dispositivo supervise de forma transparente los servidores con equilibrio de carga.

Para configurar el modo de redirección para el servidor virtual mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
set lb vserver <vServerName> -m <Value> -tosId <Value>
<!--NeedCopy-->
```

Ejemplo:

```
set lb vserver Vserver-LB-1 -m TOS -tosId 3
<!--NeedCopy-->
```

Para configurar el modo de redirección para el servidor virtual mediante la utilidad de configuración

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. Abra un servidor virtual y, en Modo de redirección, seleccione ID de TOS.

Para configurar el monitor transparente para TOS mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
1 add monitor <MonitorName> <Type> -destip <DestinationIP> -tos <Value> -
     tosId <Value>
2 <!--NeedCopy-->
```

Ejemplo:

```
1 add monitor mon1 PING -destip 10.102.33.91 -tos Yes  -tosId 3
2 <!--NeedCopy-->
```

Para crear el monitor transparente para TOS mediante la utilidad de configuración

1. Vaya a **Administración del Tráfico > Equilibrio de carga > Monitores**.
2. Cree un monitor, seleccione TOS y escriba el ID de TOS que especificó para el servidor virtual.

Monitores TOS comodín

En una configuración de equilibrio de carga en modo DSR mediante el campo TOS, la supervisión de sus servicios requiere que se cree un monitor TOS y se vincula a estos servicios. Se requiere un monitor TOS independiente para cada configuración de equilibrio de carga en modo DSR mediante el campo TOS, porque un monitor TOS requiere la dirección VIP y el ID de TOS para crear un valor codificado de la dirección VIP. El monitor crea paquetes de sondeo en los que el campo **TOS** se establece en el valor codificado de la dirección VIP. A continuación, envía los paquetes de sondeo a los servidores representados por los servicios de una configuración de equilibrio de carga.

Con muchas configuraciones de equilibrio de carga, crear un monitor de TOS personalizado separado para cada configuración es una tarea importante y engorrosa. Administrar estos monitores de TOS también es una tarea importante. Ahora, puede crear monitores de TOS comodín. Cree solo un monitor de TOS comodín para todas las configuraciones de equilibrio de carga que utilicen el mismo protocolo (por ejemplo, TCP o UDP).

Un monitor de TOS comodín tiene las siguientes configuraciones obligatorias:

- Tipo = <protocol>
- TOS = Sí

Los siguientes parámetros se pueden establecer en un valor o se pueden dejar en blanco:

- IP de destino
- Puerto de destino
- ID DE TOS

Un monitor de TOS con comodín (con IP de destino, puerto de destino y ID de TOS no definidos) enlazado a un servicio DSR aprende automáticamente el ID de TOS y la dirección VIP del servidor virtual de equilibrio de carga. El monitor crea paquetes de sondeo con el campo TOS configurado en la dirección VIP codificada y, a continuación, envía los paquetes de sondeo al servidor representado por el servicio DSR.

Para crear un monitor de TOS comodín mediante la CLI

En el símbolo del sistema, escriba:

```
add lb monitor <monitorName> <Type> -tos YES

show lb monitor <monitorName>
<!--NeedCopy-->
```

Para enlazar un monitor de TOS comodín a un servicio mediante la CLI

En el símbolo del sistema, escriba:

```
bind lb monitor <monitorName> <serviceName>

show lb monitor <monitorName>
<!--NeedCopy-->
```

Para crear un monitor de TOS comodín mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Monitores**.
2. Agregue un monitor con los siguientes parámetros:
   - Tipo = <protocol>
   - TOS = SÍ

Para enlazar un monitor de TOS comodín a un servicio mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servicios**.

2. Abra un servicio y vincule un monitor de TOS comodín a él.

En la siguiente configuración de ejemplo, V1, V2 y V3 son servidores virtuales de equilibrio de carga de tipo ANY y tiene TOS ID establecido en 1, 2 y 3 respectivamente. S1, S2, S3, S4 y S5 son servicios de tipo CUALQUIERA. S1 y S2 están enlazados a V1 y V2. S3, S4 y S5 y enlazados a V1 y V3. WLCD-TOS-MON es un monitor de TOS comodín con tipo TCP y está enlazado a S1, S2, S3, S4 y S5.

WLCD-TOS-MON aprende automáticamente el ID TOD y la dirección VIP de los servidores virtuales enlazados a S1, S2, S3, S4 y S5.

Dado que S1 está enlazado a V1 y V2, WLCD-TOS-MON crea dos tipos de paquetes de sondeo para S1, uno con el campo **TOS** configurado en la dirección VIP codificada (203.0.113.1) de V1 y el otro con la dirección VIP (203.0.113.2) de V2. A continuación, Citrix ADC envía estos paquetes de sondeo al servidor representado por S1. Del mismo modo, WLCD-TOS-MON crea paquetes de sondeo para S2, S3, S4 y S5.

```
add lb monitor WLCD-TOS-MON  TCP -tos YES

Done

add lb vserver V1 ANY 203.0.113.1 * -m TOS  - tosID 1

Done

add lb vserver V2 ANY 203.0.113.2 * -m TOS  - tosID 2

Done

add lb vserver V3 ANY 203.0.113.3 * -m TOS  - tosID 3

Done

add service S1 198.51.100.1 ANY *

Done

add service S2 198.51.100.2 ANY *

Done

add service S3 198.51.100.3 ANY *

Done

```



```
add service S4 198.51.100.4 ANY *

Done

add service S5 198.51.100.5 ANY *

Done

bind lb monitor WLCD-TOS-MON S1

Done

bind lb monitor WLCD-TOS-MON S2

Done

bind lb monitor WLCD-TOS-MON S3

Done

bind lb monitor WLCD-TOS-MON S4

Done

bind lb monitor WLCD-TOS-MON S5

Done

bind lb vserver V1 S1, S2, S3, S4, S5

Done

bind lb vserver V2, S1, S2

Done

bind lb vserver V3 S3, S4, S5

Done
<!--NeedCopy-->
```


Caso de uso 6: Configurar el equilibrio de carga en modo DSR para redes IPv6 mediante el campo TOS

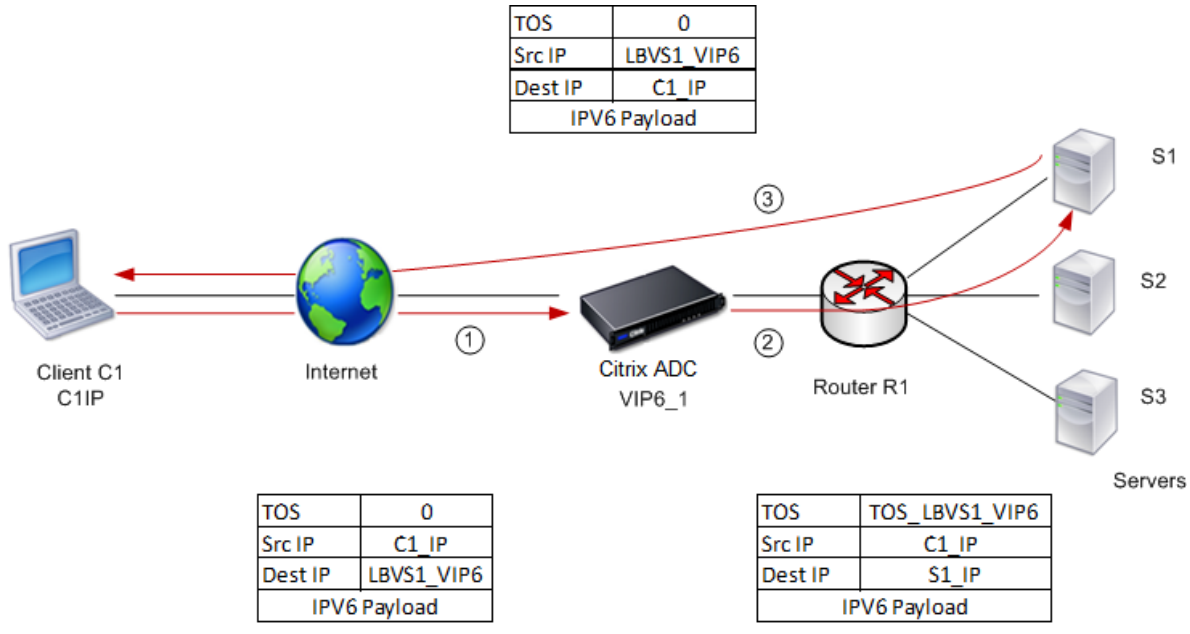
August 20, 2021

Puede configurar el equilibrio de carga en modo Direct Server Return (DSR) para redes IPv6 mediante el campo Tipo de servicio (TOS) cuando el dispositivo Citrix ADC y los servidores se encuentren en redes diferentes.

Nota: El campo TOS también se denomina campo Clase de tráfico.

En el modo DSR, cuando un cliente envía una solicitud a una dirección VIP6 en un dispositivo Citrix ADC, el dispositivo reenvía esta solicitud al servidor cambiando la dirección IPv6 de destino del paquete a la dirección IPv6 del servidor y establece un valor codificado de la dirección VIP6 en los TOS (también denominada clase de tráfico) del encabezado IPv6. Puede configurar el servidor para que utilice la información del campo TOS para derivar la dirección VIP6 del valor codificado, que luego se utiliza como dirección IP de origen en los paquetes de respuesta. El tráfico de respuesta va directamente al cliente, evitando el dispositivo.

Considere un ejemplo en el que un servidor virtual de equilibrio de carga LBVS1, configurado en un dispositivo Citrix ADC NS1, se utiliza para equilibrar la carga entre los servidores S1, S2 y S3. El dispositivo Citrix ADC NS1 y los servidores S1, S2 y S3 se encuentran en redes diferentes, por lo que el router R1 se implementa entre NS1 y los servidores.



En la tabla siguiente se enumeran los parámetros utilizados en este ejemplo.

Entidades	Nombre
Dirección IPv6 del cliente C1	C1_IP (solo para fines de referencia)
Servidor virtual de equilibrio de carga en NS1	LBVS1
Dirección IPv6 de LBVS1	LBVS1_VIP6 (solo para referencias)
Valor de TOS	TOS_LBVS1_VIP6 (solo para fines de referencia)
Servicio para el servidor S1 en NS1	SVC_S1
Dirección IPv6 para el servidor S1	S1_IP (solo para fines de referencia)
Servicio para el servidor S2 en NS1	SVC_S2
Dirección IPv6 para el servidor S1	S2_IP (solo para fines de referencia)
Servicio para el servidor S3 en NS1	SVC_S3
Dirección IPv6 para el servidor S1	S3_IP (solo para fines de referencia)

A continuación se presenta el flujo de tráfico en el caso de ejemplo:

1. El cliente C1 envía una solicitud al servidor virtual LBVS1.
2. El algoritmo de equilibrio de carga de LBVS1 selecciona el servidor S1 y el dispositivo abre una conexión a S1. NS1 envía la solicitud a S1 con:
   - Campo TOS establecido en TOS_LBVS1_VIP6.
   - Dirección IP de origen como C1_IP.
3. El servidor S1, al recibir la solicitud, utiliza la información del campo TOS para derivar la dirección LBVS1_VIP6, que es la dirección IP del servidor virtual LBVS1 en NS1. El servidor envía directamente la respuesta a C1, omitiendo el dispositivo, con:
   - Dirección IP de origen establecida en la dirección derivedLBVS1_VIP6 para que el cliente se comunique con el servidor virtual LBVS1 en NS1 y no con el servidor S1.

Para configurar el equilibrio de carga en modo DSR mediante TOS, lleve a cabo los siguientes pasos en el dispositivo

1. Habilite el modo USIP globalmente.
2. Agregue los servidores como servicios.
3. Configure un servidor virtual de equilibrio de carga con un valor TOS.
4. Enlazar los servicios al servidor virtual.

Para configurar el equilibrio de carga en modo DSR mediante TOS mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
enable ns mode USIP

add service <serviceName> <IP> <serviceType> <port>
<!--NeedCopy-->
```

Repita el comando anterior tantas veces como sea necesario para agregar cada servidor como servicio en el dispositivo Citrix ADC.

```
add lb vserver <name> <serviceType> <ip> <port> -m <redirectionMode> -
    tosId <positive_integer>

bind lb vserver <vserverName> <serviceName>
<!--NeedCopy-->
```

Para habilitar el modo USIP mediante la utilidad de configuración

Vaya a **Sistema > Configuración > Configurar modos**y seleccione **Usar dirección IP de origen**.

Para crear servicios mediante la utilidad de configuración

Vaya a **Administración del tráfico > Equilibrio de carga > Servicios**y cree un servicio.

Para crear un servidor virtual de equilibrio de carga y enlazar servicios mediante la utilidad de configuración

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**y cree un servidor virtual.
2. Haga clic en la sección Servicio para enlazar un servicio a este servidor virtual.

Caso de uso 7: Configurar el equilibrio de carga en modo DSR mediante IP sobre IP

January 21, 2022

Puede configurar un dispositivo Citrix ADC para utilizar el modo de Direct Server Return (DSR) en redes de capa 3 mediante túnel IP, también denominado configuración *IP sobre IP*. Al igual que con las configuraciones de equilibrio de carga estándar para el modo DSR, esto permite a los servidores responder directamente a los clientes en lugar de utilizar una ruta de retorno a través del dispositivo Citrix ADC. Esto mejora el tiempo de respuesta y el rendimiento. Al igual que con el modo DSR estándar, el dispositivo Citrix ADC supervisa los servidores y realiza comprobaciones de estado en los puertos de la aplicación.

Con la configuración de IP sobre IP, el dispositivo Citrix ADC y los servidores no necesitan estar en la misma subred de Capa 2. En cambio, el dispositivo Citrix ADC encapsula los paquetes antes de enviarlos al servidor de destino. Después de que el servidor de destino recibe los paquetes, descapsulará los paquetes y, a continuación, envía sus respuestas directamente al cliente. Esto se conoce a menudo como L3DSR.

Para configurar el modo L3-DSR en el dispositivo Citrix ADC:

- Cree un servidor virtual de equilibrio de carga. Establezca el modo en IPTUNNEL y habilite el seguimiento sin sesión.
- Cree servicios. Cree un servicio para cada aplicación de back-end y vincule los servicios al servidor virtual.
- Configurar para descapsulación. Configure un dispositivo Citrix ADC o un servidor back-end para que actúe como desencapsulador.

  > Nota:
  >
  > Cuando utiliza un dispositivo Citrix ADC, la configuración de descapsulación es un túnel IP entre los dispositivos ADC con el back-end que realiza L2DSR en los servidores reales.

Configurar un servidor virtual de equilibrio de carga

Configure un servidor virtual para gestionar las solicitudes a sus aplicaciones. Asigne el tipo de servicio que coincida con el servicio o utilice un tipo de ANY para varios servicios.
Establezca el método de reenvío en IPTUNNEL y permita que el servidor virtual funcione en modo sin sesión. Configure cualquier método de equilibrio de carga que quiera utilizar.

Para crear y configurar un servidor virtual de equilibrio de carga para IP sobre IP DSR mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba el siguiente comando para configurar un servidor virtual de equilibrio de carga para IP sobre IP DSR y verificar la configuración:


```
add lb vserver <name> serviceType <serviceType> IPAddress <ip> Port <
    port> -lbMethod <method> -m <ipTunnelTag> -sessionless [ENABLED |
    DISABLED]

show lb vserver <name>
<!--NeedCopy-->
```

Ejemplo:

En el siguiente ejemplo, seleccionamos el método de equilibrio de carga como sourceIPhash y configuramos el equilibrio de carga sin sesión.

```
add lb vserver Vserver-LB-1 ANY 1.1.1.80 * -lbMethod SourceIPHash -m
    IPTUNNEL -sessionless ENABLED
<!--NeedCopy-->
```

Para crear y configurar un servidor virtual de equilibrio de carga para IP sobre IP DSR mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. Cree un servidor virtual y especifique el modo de redirección como **basado en túnel IP**.

Configurar servicios para IP sobre IP DSR

Después de crear el servidor con equilibrio de carga, configure un servicio para cada una de las aplicaciones. El servicio controla el tráfico desde el dispositivo Citrix ADC a esas aplicaciones y permite que el dispositivo Citrix ADC supervise el estado de cada aplicación.

Asigne los servicios para utilizar el modo USIP y vincule un monitor de tipo IPTUNNEL al servicio para la supervisión basada en túneles.

Para crear y configurar un servicio para IP sobre IP DSR mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para crear un servicio y, opcionalmente, crear un monitor y vincularlo al servicio:

```
add service <serviceName> <serverName> <serviceType> <port> -usip <usip
    >
```



```
2
3 add monitor <monitorName> <monitorType> -destip <ip> -iptunnel <
     iptunnel>
4
5 bind service <serviceName> -monitorName <monitorName>
6 <!--NeedCopy-->
```

Ejemplo:

En el siguiente ejemplo, se crea un monitor de tipo IPTUNNEL.

```
1 add monitor mon_DSR PING -destip 1.1.1.80 -iptunnel yes
2 add service svc_DSR01 2.2.2.100 ANY * -usip yes
3 bind service svc_DSR01 -monitorName mon_DSR
4 <!--NeedCopy-->
```

Un enfoque alternativo para simplificar la redirección tanto en el servidor como en el dispositivo ADC es configurar el ADC y el servidor para que utilicen una IP desde la misma subred. Al hacerlo, se garantiza que cualquier tráfico con destino de un extremo de túnel se envíe a través del túnel. En el ejemplo, se utiliza 10.0.1.0/30.

> **Nota:**
>
> El objetivo del monitor es garantizar que el túnel esté activo alcanzando el bucle inactivo de cada servidor a través del túnel IP. Si el servicio no está activo, compruebe si la redirección IP externo entre ADC y el servidor es correcto. Compruebe también si se puede acceder a las direcciones IP internas a través del túnel IP. Es posible que se requieran rutas en el servidor o que se agregue PBR a ADC en función de la implementación elegida.

Ejemplo:

```
1 add ns ip 10.0.1.2 255.255.255.252 -vServer DISABLED
2 add netProfile netProfile_DSR -srcIP 10.0.1.2
3 add lb monitor mon_DSR PING -LRTM DISABLED -destIP 1.1.1.80 -ipTunnel
     YES -netProfile netProfile_DSR
4 <!--NeedCopy-->
```

Para configurar un monitor mediante la GUI

1. Vaya a **Administración del tráfico > Equilibrio de carga > Monitores**.
2. Cree un monitor y seleccione **IP Tunnel**.

Para crear y configurar un servicio para IP sobre IP DSR mediante la interfaz gráfica de usuario

1. Vaya a **Traffic Management > Load Balancing > Services**.
2. Cree un servicio y, en la ficha **Configuración**, seleccione **Usar dirección IP de origen**.

Para enlazar un servicio a un servidor virtual de equilibrio de carga mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba el siguiente comando:

```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Ejemplo:

```
bind lb vserver Vserver-LB-1 Service-DSR-1
<!--NeedCopy-->
```

Para enlazar un servicio a un servidor virtual de equilibrio de carga mediante la GUI

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. Abra un servidor virtual y haga clic en la sección **Servicios** para enlazar un servicio al servidor virtual.

Uso de la dirección IP del cliente en el encabezado externo de los paquetes de túnel

Citrix ADC admite el uso de la dirección IP de origen del cliente como dirección IP de origen en el encabezado externo de los paquetes de túnel relacionados con el modo de Direct Server Return mediante túnel IP. Esta función es compatible con DSR con IPv4 y DSR con modos de túnel IPv6. Para habilitar esta función, habilite el parámetro **use la dirección IP de origen del cliente** para IPv4 o IPv6. Esta configuración se aplica globalmente a todas las configuraciones DSR que utilizan túnel IP.

Para utilizar una dirección IP de origen cliente como dirección IP de origen mediante la CLI

En el símbolo del sistema, escriba:

- `set iptunnelparam -useclientsourceip [YES | NO]`
- `show iptunnelparam`

Para utilizar la dirección IP de origen del cliente como dirección IP de origen mediante la GUI

1. Vaya a **Sistema > Red**.
2. En **la ficha Configuración**, haga clic en **Configuración global del túnel IPv4**.
3. En la página **Configurar parámetros globales del túnel IPv4**, seleccione la casilla de verificación **Usar IP de origen del cliente**.
4. Haga clic en **OK**.

Para utilizar la dirección IP de origen del cliente como dirección IP de origen mediante la CLI

En el símbolo del sistema, escriba:

- `set ip6tunnelparam -useclientsourceip [YES | NO]`
- `show ip6tunnelparam`

Para utilizar la dirección IP de origen del cliente como dirección IP de origen mediante la GUI

1. Vaya a **Sistema > Red**.
2. En **la ficha Configuración**, haga clic en **Configuración global del túnel IPv6**.
3. En la página **Configurar parámetros globales del túnel IPv6**, seleccione la casilla de verificación **Usar IP de origen del cliente**.
4. Haga clic en **OK**.

Configuración de descapsulación

Puede configurar un dispositivo Citrix ADC o un servidor back-end como descapsulación.

Descapsulación Citrix ADC

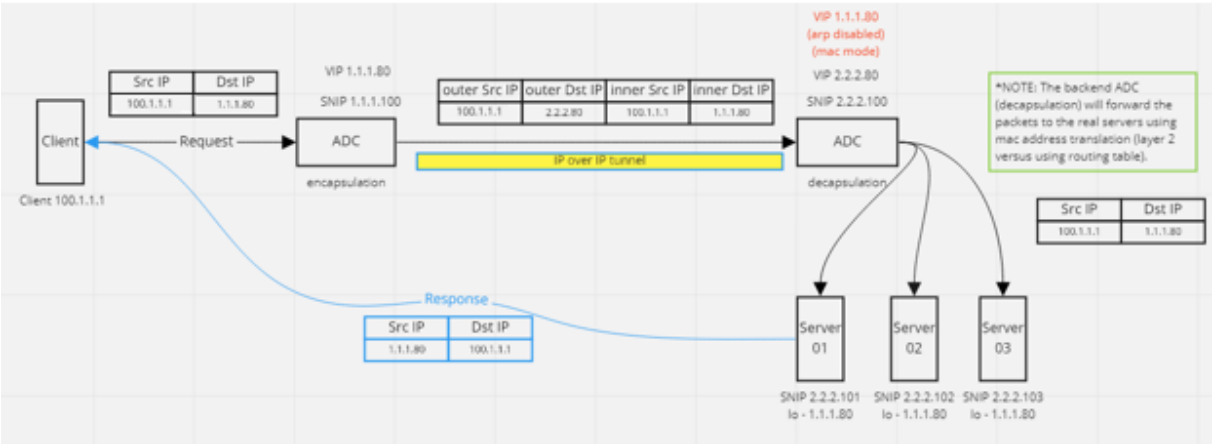
Cuando se utiliza un dispositivo Citrix ADC como descapsulación, se debe crear un túnel IP en el dispositivo Citrix ADC. Para obtener más información, consulte Configuración de túneles IP.

La configuración de descapsulación de Citrix ADC consta de los dos servidores virtuales siguientes:

- El primer servidor virtual recibe el paquete encapsulado y elimina la encapsulación IP externa.
- El segundo servidor virtual tiene la IP del servicio original en el ADC front-end y utiliza la traducción MAC para reenviar el paquete hacia el back-end mediante la dirección MAC de los servicios vinculados. Esta configuración se conoce normalmente como L2DSR. Asegúrese de inhabilitar ARP en este servidor virtual.

Configuración de ejemplo:

En la siguiente ilustración se muestra una configuración de descapsulación mediante los dispositivos ADC.



La configuración completa necesaria para la configuración es la siguiente.

Configuración ADC front-end:

```
add service svc_DSR01 2.2.2.80 ANY * -usip YES -useproxyport NO
add lb vserver vip_DSR_ENCAP ANY 1.1.1.80 * -lbMethod SOURCEIPHASH -m
    IPTUNNEL -sessionless ENABLED
bind lb vserver vip_DSR_ENCAP svc_DSR01
<!--NeedCopy-->
```

Configuración de ADC back-end:

```
add ipTunnel DSR-IPIP 1.1.1.100 255.255.255.255 *

add service svc_DSR01_01 2.2.2.101 ANY * -usip YES -useproxyport NO
add service svc_DSR01_02 2.2.2.102 ANY * -usip YES -useproxyport NO
add service svc_DSR01_03 2.2.2.103 ANY * -usip YES -useproxyport NO

add lb vserver vs_DSR_DECAP ANY 2.2.2.80 * -lbMethod SOURCEIPHASH -m
    IPTUNNEL -sessionless ENABLED -netProfile netProf_DSR_MBF_noIP

add ns ip 1.1.1.80 255.255.255.255 -type VIP -arp DISABLED -snmp
    DISABLED
add lb vserver vs_DSR_Relay ANY 1.1.1.80 * -lbMethod SOURCEIPHASH -m
    MAC -sessionless ENABLED

bind lb vserver vs_DSR_DECAP svc_DSR01_01
bind lb vserver vs_DSR_DECAP svc_DSR01_02
bind lb vserver vs_DSR_DECAP svc_DSR01_03

```



```
bind lb vserver vip_DSR_Relay svc_DSR01_01
bind lb vserver vip_DSR_Relay svc_DSR01_02
bind lb vserver vip_DSR_Relay svc_DSR01_03

add netProfile netProf_DSR_MBF_noIP -MBF ENABLED
add lb monitor mon_DSR_MAC PING -netProfile netProf_DSR_MBF_noIP
bind service svc_DSR01_01 -monitorName mon_DSR_MAC
bind service svc_DSR01_02 -monitorName mon_DSR_MAC
bind service svc_DSR01_03 -monitorName mon_DSR_MAC
<!--NeedCopy-->
```

En el ejemplo siguiente se muestra una configuración de pruebas mediante servidores de Ubuntu y Red Hat que ejecutan apache2. Estos comandos se configuran en cada servidor back-end.

```
sudo ip addr add 1.1.1.80 255.255.255.255 dev lo
sudo sysctl net.ipv4.conf.all.arp_ignore=1
sudo sysctl net.ipv4.conf.all.arp_announce=2
sudo sysctl net.ipv4.conf.eth4.rp_filter=2 (The interface has the
   external IP with route towards the ADC)
sudo sysctl net.ipv4.conf.all.forwarding=1
sudo ip link set dev lo arp on
<!--NeedCopy-->
```

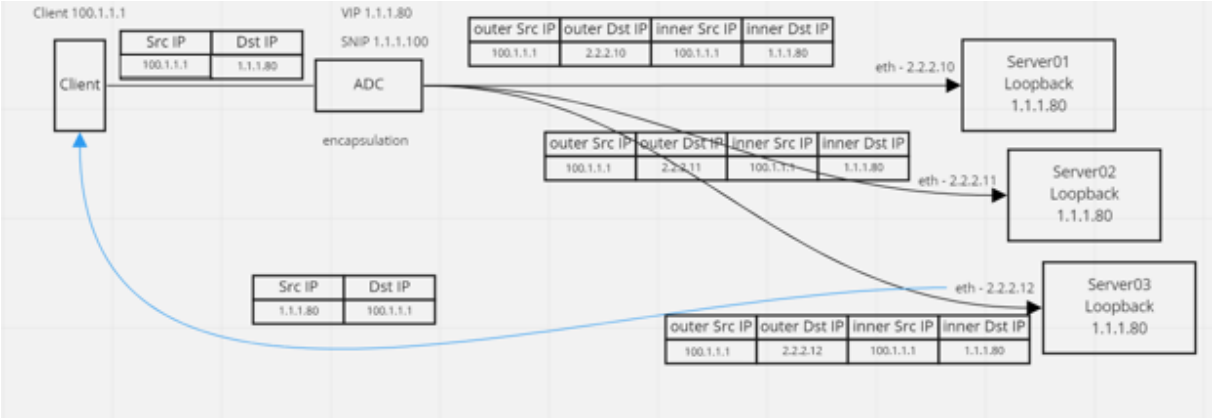
Descapsulación de servidores back-end

Cuando utiliza los servidores back-end como descapsulación, la configuración de back-end varía según el tipo de SO del servidor. Puede configurar un servidor back-end como descapsulación siguiendo estos pasos:

1. Configure una interfaz de bucle posterior con IP para IP de servicio.
2. Cree una interfaz de túnel.
3. Agregue una ruta a través de la interfaz del túnel.
4. Configure los ajustes de la interfaz según sea necesario para el tráfico.

> Nota:
>
> Los servidores del sistema operativo Windows no pueden realizar túneles IP de forma nativa, por lo que los comandos se proporcionan como ejemplos para sistemas basados en Linux. Sin embargo, los complementos de terceros están disponibles para los servidores del sistema operativo Windows, que están fuera del ámbito de este ejemplo.

En la siguiente ilustración se muestra una configuración de descapsulación mediante los servidores back-end.



Ejemplo de configuración:

En este ejemplo, 1.1.1.80 es la dirección IP virtual (VIP) de Citrix ADC y 2.2.2.10-2.2.2.12 son las direcciones IP del servidor back-end. La dirección VIP se configura en la interfaz de bucle inactivo y se agrega una ruta a través de la interfaz de túnel. Los monitores utilizan la IP del servidor y túnel los paquetes de supervisión sobre el túnel IP mediante los extremos del túnel.

La configuración completa necesaria para la configuración es la siguiente.

Configuración ADC front-end:

La siguiente configuración crea un monitor que utiliza el extremo del túnel como origen. A continuación, envíe pings a través del túnel a la dirección IP de servicio.

```
1 add ns ip 10.0.1.2 255.255.255.252 -vServer DISABLED
2 add netProfile netProfile_DSR -srcIP 10.0.1.2
3 add lb monitor mon_DSR PING -LRTM DISABLED -destIP 1.1.1.80 -ipTunnel
     YES -netProfile netProfile_DSR
4 <!--NeedCopy-->
```

La siguiente configuración crea un VIP para el servicio que utiliza la dirección IP de origen original. A continuación, reenvía el tráfico a través del túnel IP a los servidores back-end.

```
1 add service svc_DSR01 2.2.2.10 ANY * -usip YES -useproxyport NO
2 bind service svc_DSR01 -monitorName mon_DSR
3
4 add service svc_DSR02 2.2.2.11 ANY * -usip YES -useproxyport NO
5 bind service svc_DSR02 -monitorName mon_DSR
6
7 add service svc_DSR03 2.2.2.12 ANY * -usip YES -useproxyport NO
8 bind service svc_DSR03 -monitorName mon_DSR
9
```



```
add lb vserver vip_DSR_ENCAP ANY 1.1.1.80 * -lbMethod SOURCEIPHASH -m
    IPTUNNEL -sessionless ENABLED
bind lb vserver vip_DSR_ENCAP svc_DSR01
bind lb vserver vip_DSR_ENCAP svc_DSR02
bind lb vserver vip_DSR_ENCAP svc_DSR03
<!--NeedCopy-->
```

Configuración del servidor back-end de cada servidor:

Los siguientes comandos son necesarios para que el servidor back-end reciba el paquete IPIP, elimine la encapsulación externa y luego responda desde el bucle de retorno a la IP del cliente original. Al hacerlo, se garantiza que las direcciones IP del paquete recibido por el cliente coincidan con las direcciones IP de la solicitud original.

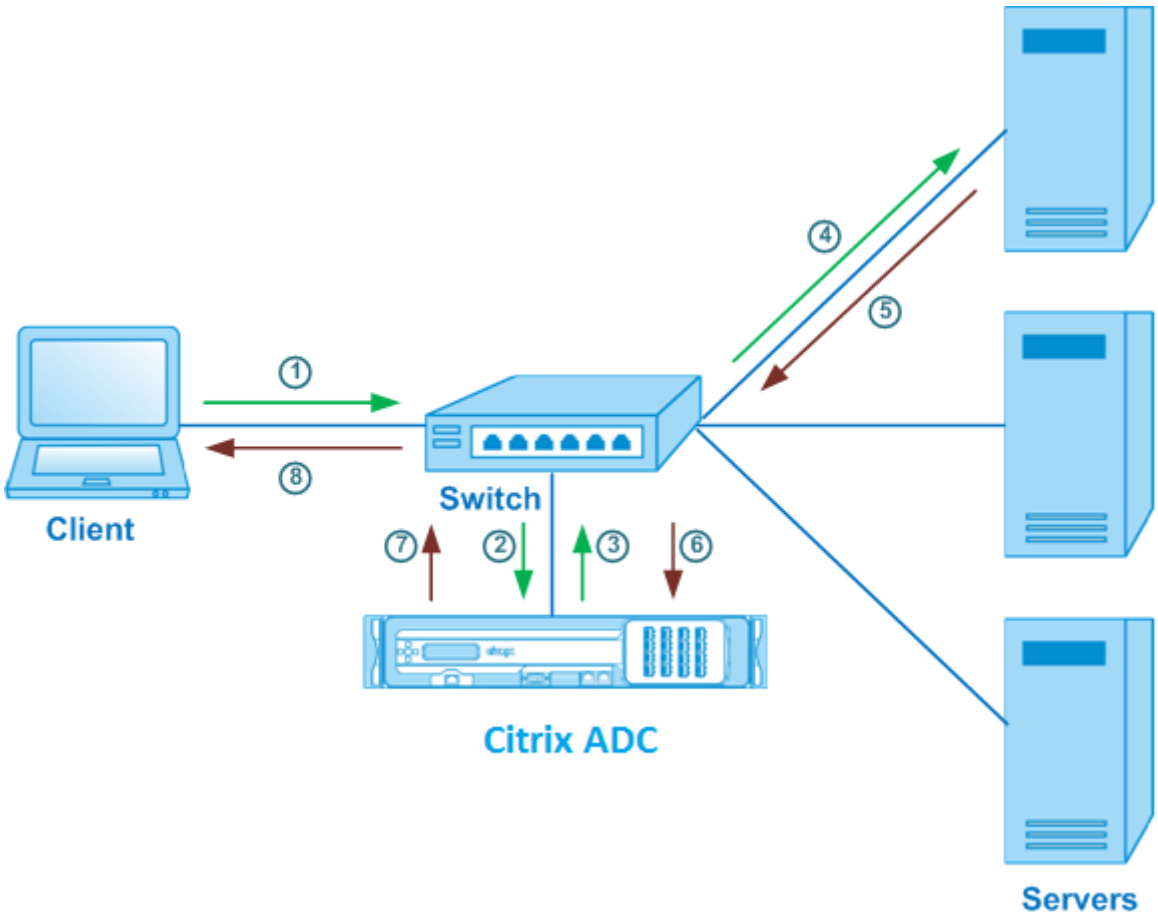
```
modprobe ipip
sudo ip addr add 1.1.1.80 255.255.255.255 dev lo
nmcli connection add type ip-tunnel ip-tunnel.mode ipip con-name tun0
ifname tun0 remote 198.51.100.5 local 203.0.113.10
nmcli connection modify tun0 ipv4.addresses '10.0.1.1/30'
nmcli connection up tun0
sudo sysctl net.ipv4.conf.all.arp_ignore=1
sudo sysctl net.ipv4.conf.all.arp_announce=2
sudo sysctl net.ipv4.conf.tun0.rp_filter=2
sudo sysctl net.ipv4.conf.all.forwarding=1
sudo ip link set dev lo arp off
<!--NeedCopy-->
```

Caso de uso 8: Configurar el equilibrio de carga en modo de un brazo

August 20, 2021

En una configuración de un solo brazo, se conecta el dispositivo Citrix ADC a la red a través de una única VLAN. El dispositivo recibe la solicitud del cliente en una única VLAN y la envía al servidor de la misma VLAN. Este es uno de los casos de implementación más simples, donde el enrutador, los servidores y el dispositivo están conectados al mismo conmutador. Las solicitudes de cliente del conmutador se reenvían al dispositivo y el dispositivo utiliza el método de equilibrio de carga configurado para seleccionar el servicio.

Ilustración 1. Equilibrio de carga en modo de un brazo



En el caso de ejemplo, los servicios Service-ANY-1, Servicio-ANY-2 y Servicio-ANY-3 se crean y vinculan al servidor virtual VServer-LB-1. La carga del servidor virtual equilibra la solicitud del cliente a un servicio. En la tabla siguiente se enumeran los nombres y valores de las entidades configuradas en el dispositivo en modo de un brazo.

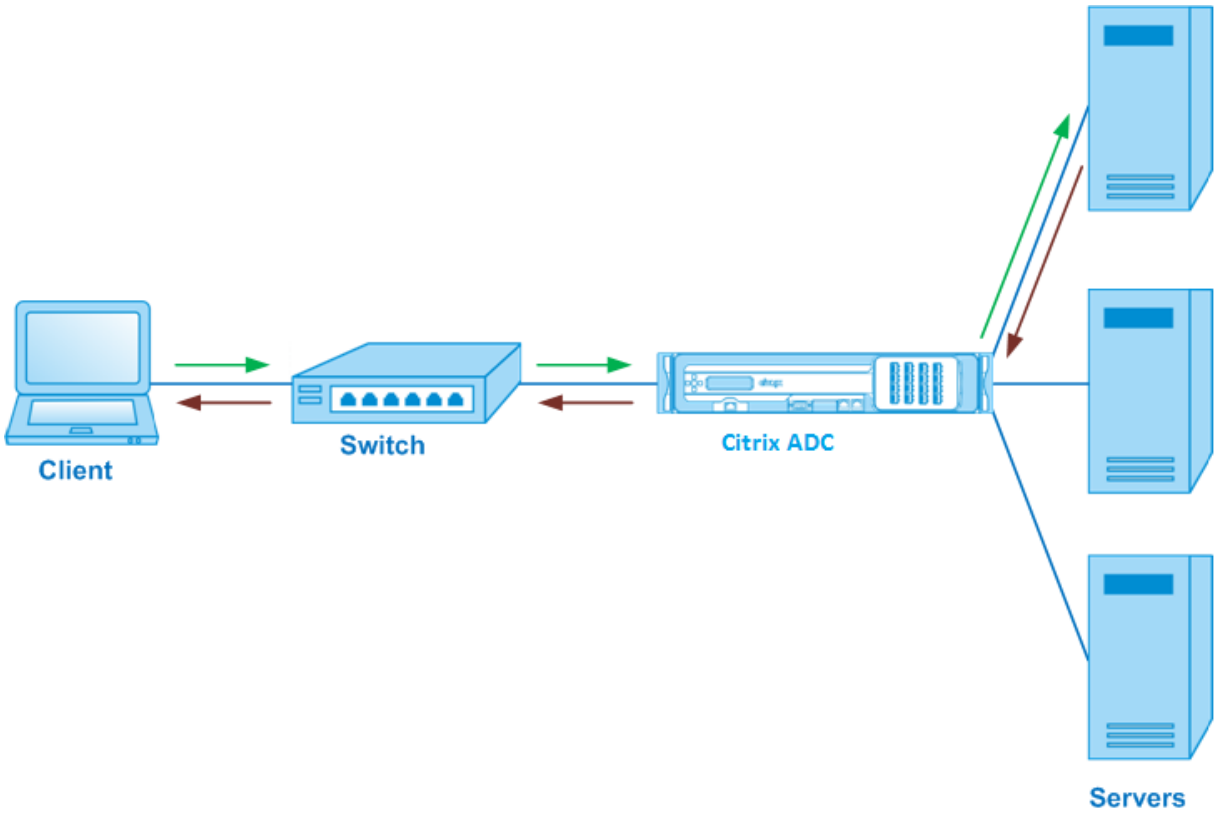
Tipo de entidad	Nombre	Dirección IP	Protocolo
Servidor virtual	Vserver-LB-1	10.102.29.94	CUALQUIERA
Servicios	Service-ANY-1	10.102.29.91	CUALQUIERA
	Service-ANY-2	10.102.29.92	CUALQUIERA
	Service-ANY-3	10.102.29.93	CUALQUIERA
Monitores	TCP	Ninguno	Ninguno

Para configurar una configuración de equilibrio de carga en modo de un brazo, consulte Configuración del equilibrio de carga básico.

Caso de uso 9: Configurar el equilibrio de carga en el modo en línea

August 20, 2021

En una configuración del modo en línea (también denominada modo de dos brazos), se conecta el dispositivo Citrix ADC a la red a través de varias VLAN. El dispositivo recibe la solicitud del cliente en una VLAN y la envía al servidor de otra VLAN. En la configuración de dos brazos, el dispositivo está conectado entre los servidores y el cliente. Las solicitudes de cliente del conmutador se reenvían al dispositivo y el dispositivo utiliza el método de equilibrio de carga configurado para seleccionar el servicio.



La configuración y el diagrama de entidad para el modo en línea son los mismos que se describen en Configuración del equilibrio de carga en modo de brazo único.

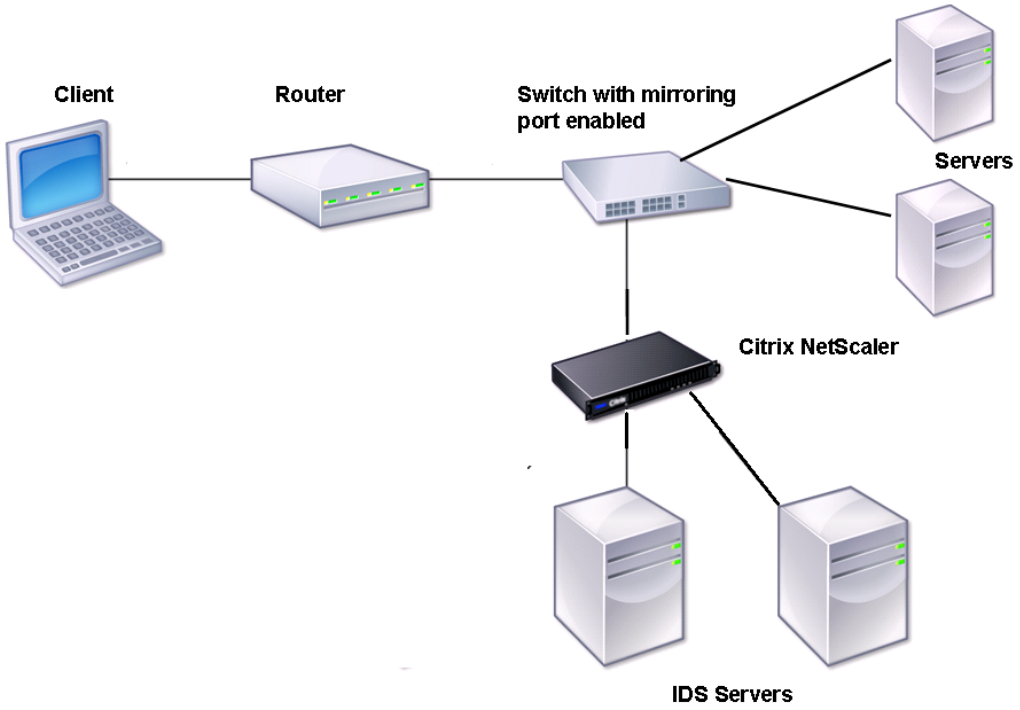
Caso de uso 10: Equilibrio de carga de servidores del sistema de detección de intrusiones

August 20, 2021

Para permitir que el dispositivo Citrix ADC admita el equilibrio de carga de los servidores del sistema

de detección de intrusiones (IDS), los servidores y los clientes IDS deben conectarse a través de un conmutador que tenga habilitada la duplicación de puertos. El cliente envía una solicitud al servidor. Dado que la duplicación de puertos está habilitada en el conmutador, los paquetes de solicitud se copian o envían al puerto del servidor virtual del dispositivo Citrix ADC. A continuación, el dispositivo utiliza el método de equilibrio de carga configurado para seleccionar un servidor IDS, como se muestra en el siguiente diagrama.

Ilustración 1. Topología de servidores IDS balanceados de carga



Nota: Actualmente, el dispositivo solo admite el equilibrio de carga de dispositivos IDS pasivos.

Como se ilustra en el diagrama anterior, la configuración de equilibrio de carga de IDS funciona de la siguiente manera:

1. La solicitud del cliente se envía al servidor IDS y un switch con un puerto de duplicación habilitado reenvía estos paquetes al servidor IDS. La dirección IP de origen es la dirección IP del cliente y la dirección IP de destino es la dirección IP del servidor. La dirección MAC de origen es la dirección MAC del enrutador y la dirección MAC de destino es la dirección MAC del servidor.
2. El tráfico que fluye a través del conmutador se refleja en el dispositivo. El dispositivo utiliza la información de capa 3 (dirección IP de origen y dirección IP de destino) para reenviar el paquete al servidor IDS seleccionado sin cambiar la dirección IP de origen o la dirección IP de destino.

Modifica la dirección MAC de origen y la dirección MAC de destino a la dirección MAC del servidor IDS seleccionado.

Nota: Cuando los servidores IDS de equilibrio de carga, puede configurar los métodos de equilibrio de carga SRCIPHASH, DESTIPHASH o SRCIPDESTIPHASH. Se recomienda el método SRCIPDESTIPHASH porque los paquetes que fluyen desde el cliente a un servicio del dispositivo deben enviarse a un único servidor IDS.

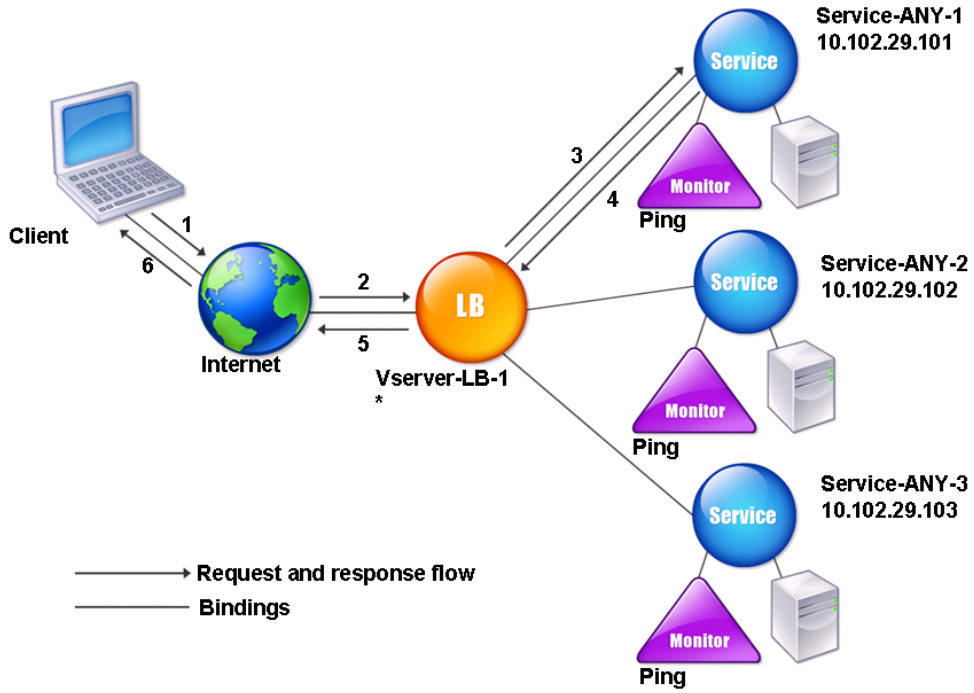
Supongamos que Service-ANY-1, Servicio-ANY-2 y Servicio-ANY-3 se crean y vinculan a VServer-LB-1. El servidor virtual equilibra la carga en los servicios. En la tabla siguiente se enumeran los nombres y valores de las entidades configuradas en el dispositivo.

Tipo de entidad	Nombre	Dirección IP	Port	Protocolo
Servidor virtual	Vserver-LB-1	*	*	CUALQUIERA
Servicios	Service-ANY-1	10.102.29.101	*	CUALQUIERA
	Service-ANY-2	10.102.29.102	*	CUALQUIERA
	Service-ANY-3	10.102.29.103	*	CUALQUIERA
Monitores	Ping	Ninguno	Ninguno	Ninguno

Nota: Puede utilizar el modo en línea o el modo de un brazo para una configuración de equilibrio de carga IDS.

El siguiente diagrama muestra las entidades de equilibrio de carga y los valores de los parámetros que se configurarán en el dispositivo.

Ilustración 2. Modelo de entidad para servidores IDS de equilibrio de carga



Para configurar una configuración de equilibrio de carga de IDS, primero debe habilitar el reenvío basado en Mac. Desactive también los modos de capa 2 y capa 3 en el dispositivo.

Para habilitar el reenvío basado en Mac mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
enable ns mode <ConfigureMode>
<!--NeedCopy-->
```

Ejemplo:

```
enable ns mode MAC
<!--NeedCopy-->
```


Para habilitar el reenvío basado en Mac mediante la utilidad de configuración

Vaya a **Sistema > Configuración > Configurar modos**y seleccione **Reenvío basado en MAC**.

A continuación, consulte "Configuración del equilibrio de carga básico", para configurar una configuración básica de equilibrio de carga.

Después de configurar la configuración básica de equilibrio de carga, debe personalizarla para IDS configurando un método de equilibrio de carga compatible (como el método Hash SRCIPDESTIP en un servidor virtual sin sesión) y habilitando el modo MAC. El dispositivo no mantiene el estado de la conexión y solo reenvía los paquetes a los servidores IDS sin procesarlos. La dirección IP de destino y el puerto permanecen sin cambios porque el servidor virtual está en modo MAC.

Para configurar un método de equilibrio de carga y un modo de redirección para un servidor virtual sin sesión mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
set lb vserver <vServerName> -lbMethod <LBMethodOption> -m <
   RedirectionMode> -sessionless <Value>
<!--NeedCopy-->
```

Ejemplo:

```
set lb vserver Vserver-LB-1 -lbMethod SourceIPDestIPHash -m MAC -
   sessionless enabled
<!--NeedCopy-->
```

> **Nota**
>
> Para un servicio enlazado a un servidor virtual en el que está habilitada la opción -m MAC, debe vincular un monitor que no sea usuario.

Para configurar un método de equilibrio de carga y un modo de redirección para un servidor virtual sin sesión mediante la utilidad de configuración

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. Abra un servidor virtual y, en Modo de redirección, seleccione Basado en MAC.
3. En Configuración avanzada, haga clic en Métodos y seleccione SRCIPDESTIPHASH. Haga clic en Configuración del tráfico y seleccione Equilibrio de carga sin sesión.

Para configurar un servicio para que utilice la dirección IP de origen mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
set service <ServiceName> -usip <Value>
<!--NeedCopy-->
```

Ejemplo:

```
set service Service-ANY-1 -usip yes
<!--NeedCopy-->
```

Para configurar un servicio de modo que utilice la dirección IP de origen mediante la utilidad de configuración

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servicios**.
2. Abra un servicio y, en Configuración, seleccione **Usar dirección IP de origen**.

Para que USIP funcione correctamente, debe configurarlo globalmente. Para obtener más información sobre la configuración de USIP en todo el mundo, consulte Direccionamiento IP.

Caso de uso 11: Aislamiento del tráfico de red mediante directivas de escucha

August 20, 2021

> **Nota**Ya no se recomienda
>
> la solución de aislamiento de tráfico que utiliza servidores virtuales instantáneas para simular el aislamiento de varios arrendatarios. Como alternativa, Citrix recomienda utilizar la función de partición de administración de Citrix ADC para dichas implementaciones. Para obtener más información, consulte Partición de administración.

Un requisito de seguridad común en un centro de datos es mantener el aislamiento de rutas de red entre el tráfico de varias aplicaciones o arrendatarios. El tráfico de una aplicación o de un arrendatario debe estar aislado del tráfico de otras aplicaciones o arrendatarios. Por ejemplo, una empresa de servicios financieros querría mantener el tráfico de las solicitudes de su departamento de seguros

separado del de sus aplicaciones de servicios financieros. En el pasado, esto se lograba fácilmente mediante la separación física de dispositivos de servicio de red como firewalls, balanceadores de carga e IdP, y supervisión de red y separación lógica en la estructura de conmutación.

A medida que las arquitecturas de centros de datos evolucionan hacia centros de datos virtualizados multiarrendatarios, los servicios de red en la capa de agregación de un centro de datos se están consolidando. Este desarrollo ha convertido el aislamiento de rutas de red en un componente crítico para los dispositivos de servicio de red y está impulsando el requisito de que los ADC puedan aislar el tráfico en los niveles de L4 a L7. Además, todo el tráfico de un arrendatario en particular debe pasar por un firewall antes de llegar a la capa de servicio.

Para resolver el requisito de aislar las rutas de red, un dispositivo Citrix ADC identifica los dominios de red y controla el tráfico entre los dominios. La solución Citrix ADC tiene dos componentes principales: Directivas de escucha y servidores virtuales de sombra.

A cada ruta de red que se va a aislar se le asigna un servidor virtual en el que se define una directiva de escucha para que el servidor virtual escuche el tráfico solo desde un dominio de red especificado.

Para aislar el tráfico, las directivas de escucha se pueden basar en varios parámetros de cliente o en sus combinaciones, y se pueden asignar prioridades a las directivas. En la tabla siguiente se enumeran los parámetros que se pueden utilizar en las directivas de escucha para identificar el tráfico.

Categoría	Parámetros
Protocolo Ethernet	Dirección MAC de origen, dirección MAC de destino
Interfaz de red	ID de red, rendimiento de recepción, rendimiento de envío, rendimiento de transmisión
Protocolo IP	Dirección IP de origen, dirección IP de destino
Protocolo IPv6	Dirección IPv6 de origen, dirección IPv6 de destino
Protocolo TCP	Puerto de origen, puerto de destino, tamaño máximo del segmento, carga útil y otras opciones
Protocolo UDP	Puerto de origen, puerto de destino
VLAN	ID

Cuadro 1 Parámetros de cliente utilizados para definir directivas de escucha

En el dispositivo Citrix ADC, se configura un servidor virtual para cada dominio, con una directiva de

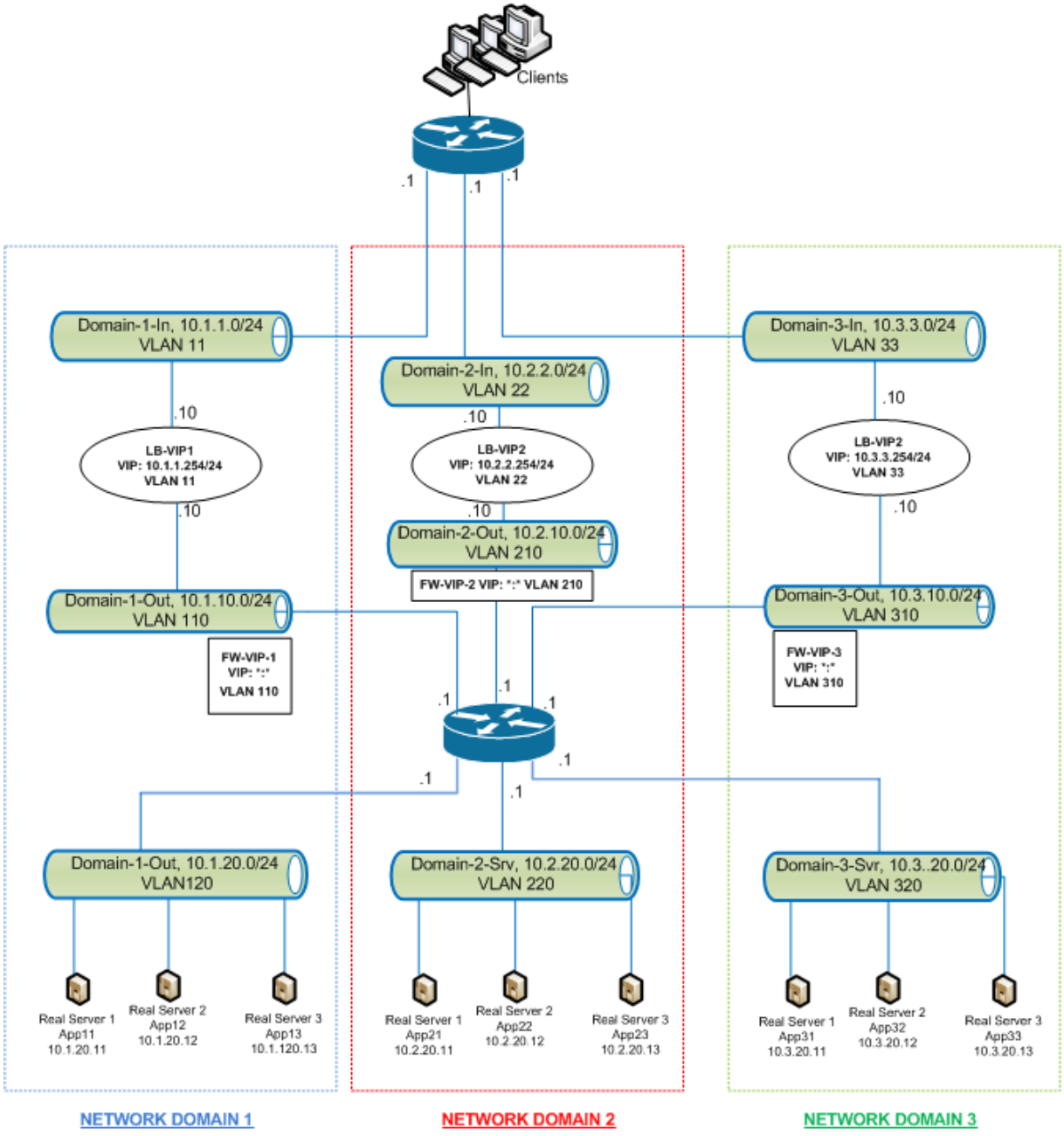
escucha que especifica que el servidor virtual debe escuchar solo el tráfico de ese dominio. También está configurado para cada dominio un servidor virtual de equilibrio de carga de sombra, que escucha el tráfico destinado a cualquier dominio. Cada uno de los servidores virtuales de equilibrio de carga de sombra tiene una dirección IP comodín (*) y un puerto, y su tipo de servicio se establece en CUALQUIERA.

En cada dominio, un firewall para el dominio está enlazado como servicio al servidor virtual de equilibrio de carga de sombra, que reenvía todo el tráfico a través del firewall. El tráfico local se reenvía a su destino y el tráfico destinado a otro dominio se reenvía al firewall de ese dominio. Los servidores virtuales de equilibrio de carga de sombra están configurados para la redirección del modo MAC.

Cómo se aíslan las rutas de red

La siguiente ilustración muestra un flujo de tráfico típico entre dominios. Considere el flujo de tráfico dentro del dominio de red 1 y entre el dominio de red 1 y el dominio de red 2.

Ilustración 1. Aislamiento de ruta de red



Tráfico dentro del dominio de red 1

El dominio de red 1 tiene tres VLAN: VLAN 11, VLAN110 y VLAN120. Los pasos siguientes describen el flujo de tráfico.

- Un cliente de VLAN 11 envía una solicitud de un servicio disponible desde el pool de servicios en VLAN 120.
- El servidor virtual de equilibrio de carga LB-VIP1, que está configurado para escuchar el tráfico de la VLAN 11, recibe la solicitud y la reenvía a la VLAN 110. El servidor virtual de la VLAN 110

reenvía la solicitud para el servidor virtual de equilibrio de carga de sombra FW-VIP-1.
- FW-VIP-1, que está configurado para escuchar el tráfico de la VLAN 110, recibe la solicitud y la reenvía a la VLAN 120.
- El servidor virtual de equilibrio de carga de la VLAN 120 equilibra la solicitud a uno de los servidores físicos, App11, App12 o App13.
- La respuesta enviada por el servidor físico devuelve por la misma ruta al cliente en VLAN 11.

Esta configuración garantiza que el tráfico siempre esté segregado dentro del Citrix ADC para todo el tráfico que se origina en un cliente.

Tráfico entre el dominio de red 1 y el dominio de red 2

El dominio de red 1 tiene tres VLAN: VLAN 11, VLAN 110 y VLAN 120. El dominio de red 2 también tiene tres VLAN: VLAN 22, VLAN 210 y VLAN 220. Los pasos siguientes describen el flujo de tráfico de VALN 11 a VLAN 22.

- Un cliente de VLAN 11, que pertenece al dominio de red 1, envía una solicitud de un servicio disponible desde el grupo de servicios en la VLAN 220, que pertenece al dominio de red 2.
- En el dominio de red 1, el servidor virtual de equilibrio de carga LB-VIP1, que está configurado para escuchar el tráfico de la VLAN 11, recibe la solicitud y la reenvía a la VLAN 110.
- El servidor virtual de equilibrio de carga de sombra FW-VIP-1, que está configurado para escuchar el tráfico VLAN 110 destinado a cualquier otro dominio, recibe la solicitud y la reenvía al servidor virtual de firewall FW-VIP-2 porque la solicitud está destinada a un servidor físico en el dominio de red 2.
- En Network Domain 2, FW-VIP-2 reenvía la solicitud a VLAN 220.
- El servidor virtual de equilibrio de carga de la VLAN 220 equilibra la solicitud a uno de los servidores físicos, App21, App22 o App23.
- La respuesta enviada por el servidor físico devuelve por la misma ruta a través del firewall en el dominio de red 2 y, a continuación, al dominio de red 1 para llegar al cliente en la VLAN 11.

Pasos de configuración

Para configurar el aislamiento de rutas de red mediante directivas de escucha, haga lo siguiente:

- Agregar expresiones de directiva de escucha. Cada expresión especifica un dominio al que está destinado el tráfico. Puede utilizar el ID de VLAN u otros parámetros para identificar el tráfico.
- Para cada dominio de red, configure dos servidores virtuales de la siguiente manera:
  - Cree un servidor virtual de equilibrio de carga para el que especifique una directiva de escucha que identifique el tráfico destinado a este dominio. Puede especificar el nombre de una expresión creada anteriormente o crear una expresión mientras crea el servidor virtual.

  - Cree otro servidor virtual de equilibrio de carga, denominado servidor virtual de sombra, para el que especifique una expresión de directiva de escucha que se aplique al tráfico destinado a cualquier dominio. En este servidor virtual, establezca el tipo de servicio en ANY y la dirección IP y el puerto en un asterisco (*). Habilite el reenvío basado en Mac en este servidor virtual.
  - Habilite la opción Conexión L2 en ambos servidores virtuales.
    Por lo general, para identificar una conexión, el dispositivo Citrix ADC utiliza las cuatro tuplas de dirección IP del cliente, puerto del cliente, dirección IP de destino y puerto de destino. Al habilitar la opción Conexión L2, los parámetros de Capa 2 de la conexión (número de canal, dirección MAC e ID de VLAN) se utilizan además de las 4 tuplas normales.
- Agregue servicios que representan los grupos de servidores en el dominio y vincularlos al servidor virtual.
- Configure el firewall para cada dominio como servicio y vincule todos los servicios de firewall al servidor virtual en la sombra.

Para aislar el tráfico de red mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos:

```
add policy expression <expressionName> <listenPolicyExpression>

add lb vserver <name> <serviceType> <ip> <port> -l2conn ON -
   listenPolicy <expressionName>
<!--NeedCopy-->
```

Agregue un servidor virtual de equilibrio de carga para cada dominio. Este servidor virtual es para el tráfico del mismo dominio.

```
add lb vserver <name> ANY * * -l2conn ON -m MAC -listenPolicy <
   expressionName>
<!--NeedCopy-->
```

Agregue un servidor virtual de equilibrio de carga de sombra para cada dominio. Este servidor virtual es para el tráfico de otros dominios.

Ejemplo:

```
add policy expression e110 client.vlan.id==110
add policy expression e210 client.vlan.id==210
```



```
add policy expression e310 client.vlan.id==310
add policy expression e11 client.vlan.id==11
add policy expression e22 client.vlan.id==22
add policy expression e33 client.vlan.id==33

add lb vserver LB-VIP1 HTTP 10.1.1.254 80 -persistenceType NONE -
    listenPolicy e11
-cltTimeout 180 -l2Conn ON

add lb vserver LB-VIP2 HTTP 10.2.2.254 80 -persistenceType NONE -
    listenPolicy e22
-cltTimeout 180 -l2Conn ON

add lb vserver LB-VIP3 HTTP 10.3.3.254 80 -persistenceType NONE -
    listenPolicy e33
-cltTimeout 180 -l2Conn ON


add lb vserver FW-VIP-1 ANY * * -persistenceType NONE -lbMethod
    ROUNDROBIN - listenPolicy e110 -Listenpriority 1 -m MAC -cltTimeout
    120

add lb vserver FW-VIP-2 ANY * * -persistenceType NONE -lbMethod
    ROUNDROBIN - listenPolicy e210 -Listenpriority 2 -m MAC -cltTimeout
    120

add lb vserver FW-VIP-3 ANY * * -persistenceType NONE -lbMethod
    ROUNDROBIN - listenPolicy e310 -Listenpriority 3 -m MAC -cltTimeout
    120


add service RD-1 10.1.1.1 ANY * -gslb NONE -maxClient 0 -maxReq 0 -cip
    DISABLED
-usip NO -useproxyport NO -sp ON -cltTimeout 120 -svrTimeout 120 -CKA
    NO -TCPB NO -CMP NO

add service RD-2 10.2.2.1 ANY * -gslb NONE -maxClient 0 -maxReq 0 -cip
    DISABLED
-usip NO -useproxyport NO -sp ON -cltTimeout 120 -svrTimeout 120 -CKA
    NO -TCPB NO -CMP NO

add service RD-3 10.3.3.1 ANY * -gslb NONE -maxClient 0 -maxReq 0 -cip
    DISABLED
-usip NO -useproxyport NO -sp ON -cltTimeout 120 -svrTimeout 120 -CKA
    NO -TCPB NO -CMP NO
```



```
33
34
35 bind lb vserver FW-VIP-1 RD-1
36
37 bind lb vserver FW-VIP-2 RD-2
38
39 bind lb vserver FW-VIP-3 RD-3
40 <!--NeedCopy-->
```

Para aislar el tráfico de red mediante la utilidad de configuración

1. Agregue servicios que representan los servidores, tal como se describe en Creación de un servicio.
2. Agregue cada firewall como servicio:
   a) Vaya a **Administración de Tráfico > Equilibrio de carga > Servicios**.
   b) Cree un servicio, especificando el protocolo como CUALQUIERA, servidor como dirección IP del firewall y puerto como 80.
3. Configure un servidor virtual de equilibrio de carga.
4. Configure el servidor virtual de equilibrio de carga de sombra.
5. Para cada dominio de red, repita los pasos 3 y 4.
6. En el panel Servidores virtuales de equilibrio de carga, abra los servidores virtuales que ha creado y compruebe la configuración.

Caso de uso 12: Configurar XenDesktop para el equilibrio de carga

August 20, 2021

Para mejorar el rendimiento en la entrega de aplicaciones de escritorio virtual, puede integrar el dispositivo Citrix ADC con Citrix XenDesktop y utilizar la función de equilibrio de carga de Citrix ADC para distribuir la carga entre los servidores de Interfaz Web y los servidores de Desktop Delivery Controller (DDC).

Por lo general, se utiliza XenDesktop en situaciones en las que las aplicaciones no son compatibles con la ejecución en un servidor Terminal Server o XenApp, o si cada escritorio virtual tiene requisitos únicos. En tales casos, necesita un host de escritorio para cada usuario que se conecte. Sin embargo, los hosts se pueden agrupar para que solo necesite un host por cada usuario conectado actualmente.

El servicio principal de aplicaciones implementado para XenDesktop es Desktop Delivery Controller (DDC). El DDC está instalado en un servidor y su función principal es registrar hosts de escritorio y conexiones de cliente de broker a ellos.

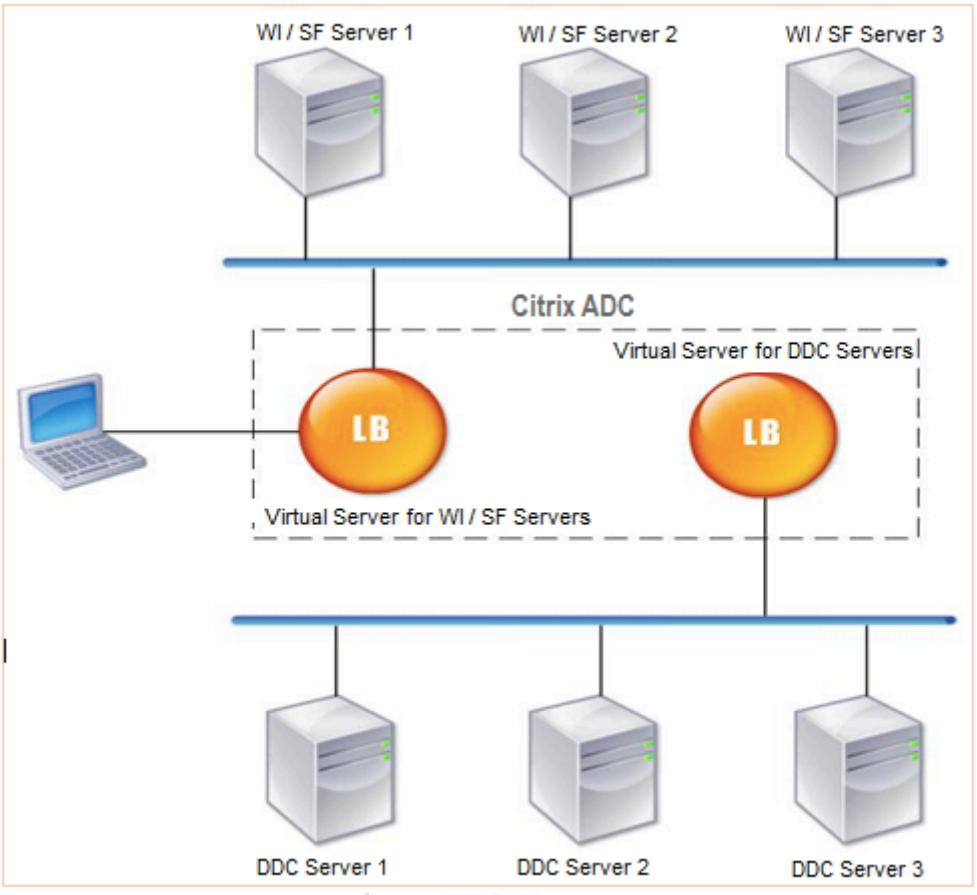
El DDC también autentica a los usuarios y administra el ensamblado de los entornos de escritorio virtual de los usuarios controlando el estado de los escritorios e iniciando y deteniendo los escritorios.

Por lo general, se instalan varios DDC para mejorar la disponibilidad.

Los servidores de Interfaz Web proporcionan acceso seguro a escritorios virtuales. La Interfaz Web es el portal de conexión inicial al Desktop Delivery Controller (DDC). El explorador web del dispositivo del usuario envía información al servidor web, que se comunica con el conjunto de servidores para proporcionar al usuario acceso al escritorio virtual.

En la siguiente ilustración se muestra la topología de un dispositivo Citrix ADC que trabaja con XenDesktop.

Ilustración 1. Equilibrio de carga de XenDesktop



Nota

Aunque puede utilizar el protocolo HTTP, Citrix recomienda utilizar SSL para la comunicación entre el cliente y el dispositivo Citrix ADC. Puede utilizar el protocolo HTTP para la comunicación entre Citrix ADC y los servidores DDC aunque utilice el protocolo SSL para la comunicación con el cliente.

Para configurar el equilibrio de carga para XenDesktop mediante la interfaz gráfica de usuario

1. Crear un servicio.
   a) Vaya a **Configuración** > **Administración del tráfico** > **Equilibrio de carga** > **Servicios** y haga clic en **Agregar**.
   b) Cree un servicio especificando un nombre, una dirección IP, un puerto y un tipo de protocolo y, a continuación, haga clic en **Aceptar**.
2. Cree un servidor virtual de equilibrio de carga.
   a) Vaya a **Configuración** > **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales** y haga clic en **Agregar**.
   b) Cree un servidor virtual especificando un nombre, una dirección IP, un puerto y un tipo de protocolo y, a continuación, haga clic en **Aceptar**.
3. Enlazar el servicio al servidor virtual de equilibrio de carga.
4. Vaya a **Configuración** > **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales** y seleccione un servidor.
   a) Haga clic en **Modificar**.
   b) En **Servicios y grupos de servicios**, haga clic en **>** y haga clic en **Agregar enlace**.
   c) Seleccione el servicio que quiere enlazar e introduzca el valor de peso.
   d) Haga clic en **Vincular**.

Para configurar el equilibrio de carga para XenDesktop mediante la interfaz de línea de comandos

- Para crear un servicio, en el símbolo del sistema, escriba:

```
add service <name> <serverName> <serviceType> <port>
<!--NeedCopy-->
```

Ejemplo:

```
add service Service-HTTP-1 192.0.2.5 HTTP 80
<!--NeedCopy-->
```

- Para crear un servidor virtual, en el símbolo del sistema, escriba:

```
add lb vserver <name> <serviceType> <ip> <port>
<!--NeedCopy-->
```


Ejemplo:

add lb vserver vserver-lb-1 HTTP 10.102.29.60 80

- Para enlazar un servicio a un servidor virtual de equilibrio de carga, en el símbolo del sistema, escriba:

```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Ejemplo:

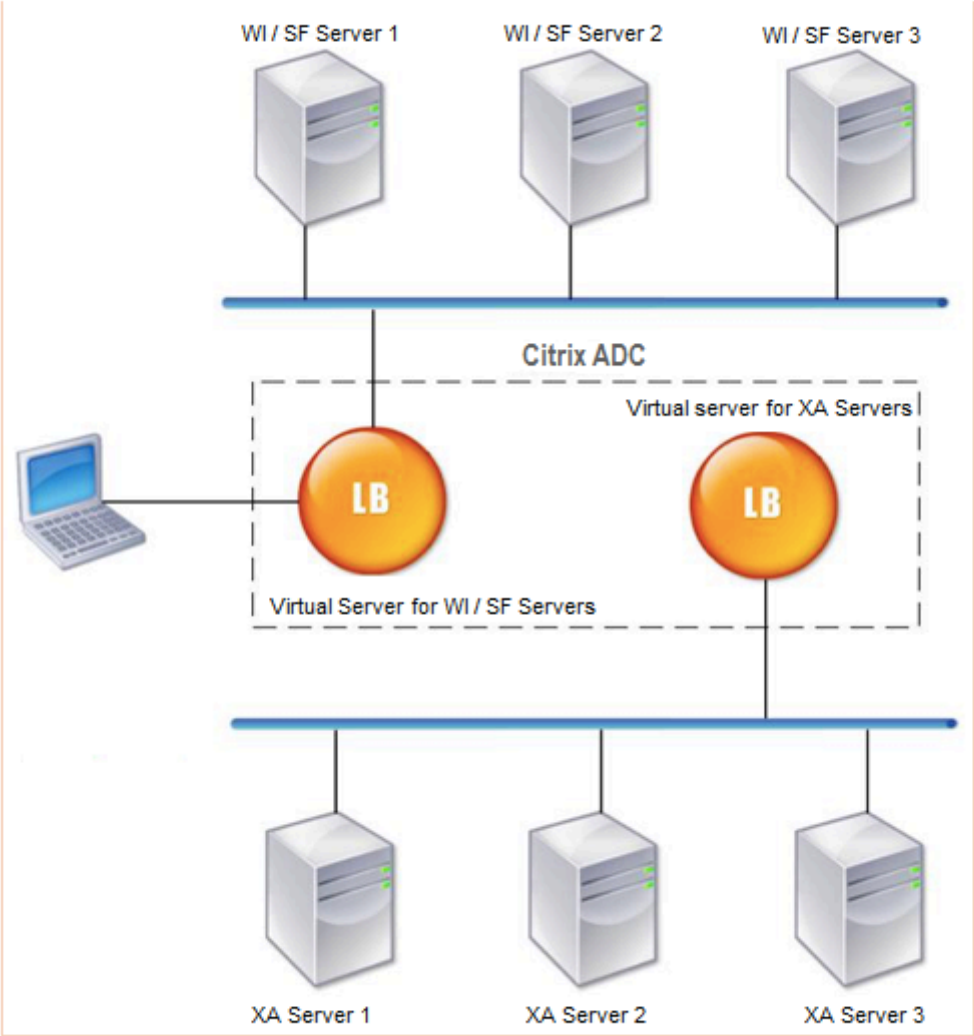
```
bind lb vserver Vserver-LB-1 Service-HTTP-1
<!--NeedCopy-->
```

Caso de uso 13: Configurar XenApp para el equilibrio de carga

August 20, 2021

Para una entrega eficiente de aplicaciones, puede integrar el dispositivo Citrix ADC con Citrix XenApp y utilizar la función de equilibrio de carga de Citrix ADC para distribuir la carga entre las comunidades de servidores XenApp. La siguiente ilustración es un diagrama de topología de dicha configuración.

Ilustración 1. Equilibrio de carga de XenApp



Los servidores de la Interfaz Web proporcionan acceso seguro a los recursos de las aplicaciones XenApp a través del explorador web del usuario. El cliente de Interfaz Web presenta a los usuarios todos los recursos, como aplicaciones, contenido y escritorios que están disponibles en las comunidades de servidores XenApp. Los usuarios pueden acceder a los recursos publicados a través de un explorador web estándar o a través del complemento en línea de Citrix.

El explorador web del dispositivo del usuario envía información al servidor web, que se comunica con los servidores de la comunidad de servidores para proporcionar al usuario acceso a los recursos.

La Interfaz Web y XML Broker son servicios complementarios. La Interfaz Web proporciona a los usuarios acceso a las aplicaciones y XML Broker evalúa los permisos del usuario para determinar qué aplicaciones aparecen en la Interfaz Web.

El servicio XML se instala en todos los servidores de la comunidad de servidores. El servicio XML especi-

ficado en la Interfaz Web funciona como agente XML. Según las credenciales de usuario transferidas por el servidor de interfaz web, el servidor XML Broker envía una lista de aplicaciones accesibles para el usuario.

En grandes empresas donde se implementan varios servidores de Interfaz Web y servidores XML Broker, Citrix recomienda equilibrar la carga de estos servidores mediante el dispositivo Citrix ADC. Configure un servidor virtual para equilibrar la carga de los servidores de interfaz web y otro para los servidores XML Broker. El método de equilibrio de carga y otras funciones se pueden configurar en el servidor virtual según sea necesario.

> **Nota**
>
> Aunque puede utilizar el protocolo HTTP, Citrix recomienda utilizar SSL para la comunicación entre el cliente y el Citrix ADC. Puede utilizar el protocolo HTTP para la comunicación entre Citrix ADC y los servidores WI aunque utilice el protocolo SSL para la comunicación con el cliente.

Para configurar el equilibrio de carga para XenApp mediante la interfaz gráfica de usuario

1. Crear un servicio.
   a) Vaya a **Configuración** > **Administración del tráfico** > **Equilibrio de carga** > **Servicios** y haga clic en **Agregar**.
   b) Cree un servicio especificando un nombre, una dirección IP, un puerto y un tipo de protocolo y, a continuación, haga clic en **Aceptar**.
2. Cree un servidor virtual de equilibrio de carga.
   a) Vaya a **Configuración** > **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales** y haga clic en **Agregar**.
   b) Cree un servidor virtual especificando un nombre, una dirección IP, un puerto y un tipo de protocolo y, a continuación, haga clic en **Aceptar**.
3. Enlazar el servicio al servidor virtual de equilibrio de carga.
4. Vaya a **Configuración** > **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales** y seleccione un servidor.
   a) Haga clic en **Modificar**.
   b) En **Servicios y grupos de servicios**, haga clic en **>** y haga clic en **Agregar enlace**.
   c) Seleccione el servicio que quiere enlazar e introduzca el valor de peso.
   d) Haga clic en **Vincular**.

Para configurar el equilibrio de carga para XenApp mediante la interfaz de línea de comandos

- Para crear un servicio, en el símbolo del sistema, escriba:


```
add service <name> <serverName> <serviceType> <port>
<!--NeedCopy-->
```

Ejemplo:

```
add service Service-HTTP-1 192.0.2.5 HTTP 80
<!--NeedCopy-->
```

- Para crear un servidor virtual, en el símbolo del sistema, escriba:

```
add lb vserver <name> <serviceType> <ip> <port>
<!--NeedCopy-->
```

Ejemplo:

```
add lb vserver Vserver-LB-1 HTTP 10.102.29.60 80
<!--NeedCopy-->
```

- Para enlazar un servicio a un servidor virtual de equilibrio de carga, en el símbolo del sistema, escriba:

```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Ejemplo:

```
bind lb vserver Vserver-LB-1 Service-HTTP-1
<!--NeedCopy-->
```

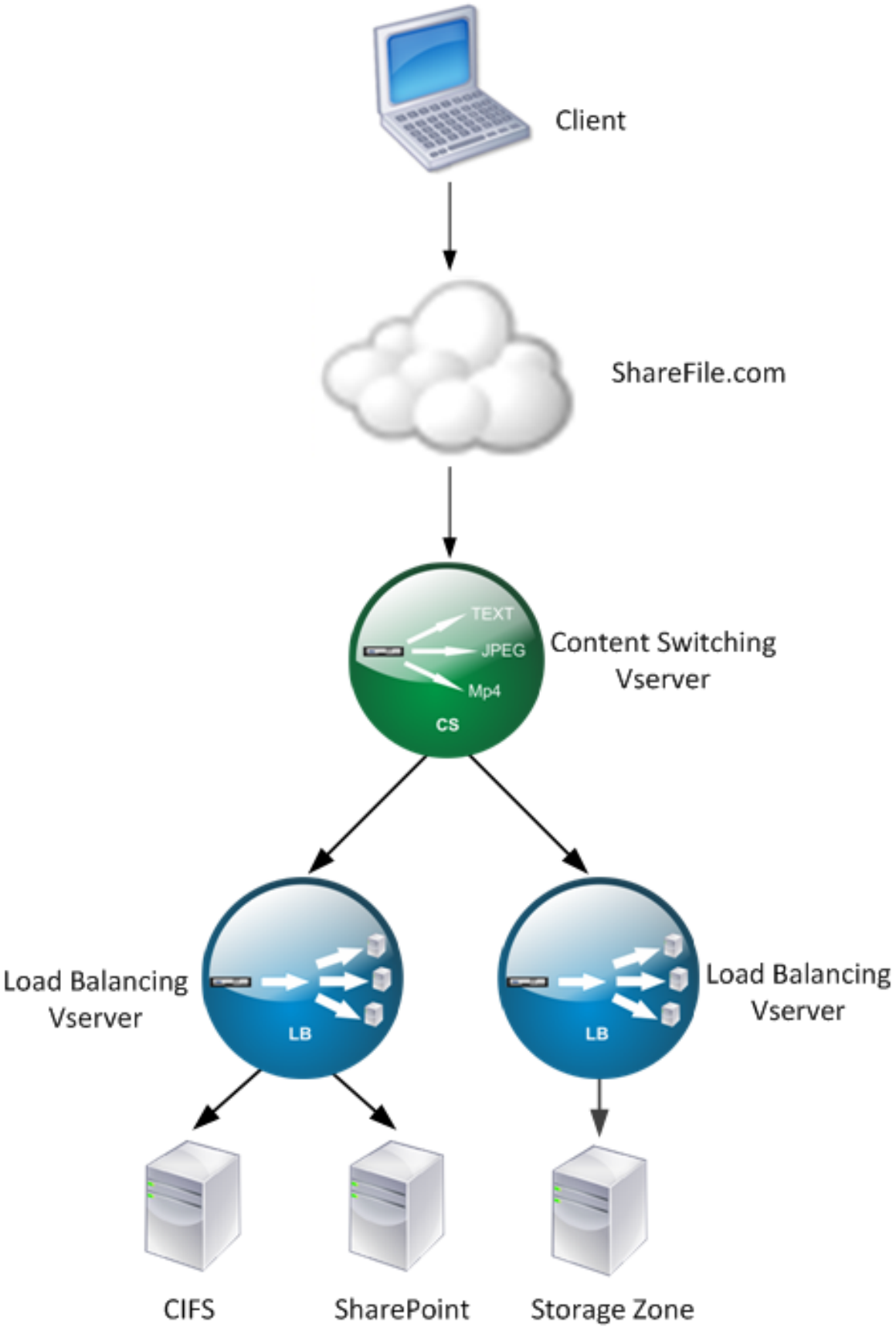
Caso de uso 14: Asistente para ShareFile para equilibrio de carga Citrix ShareFile

August 20, 2021

Puede configurar el equilibrio de carga para Citrix ShareFile mediante el asistente. El asistente de Citrix ShareFile ayuda a configurar la configuración de equilibrio de carga para el sitio de ShareFile en función del tipo de contenido solicitado. El servidor de conmutación de contenido dirige la solicitud en función de si se trata de una solicitud StorageZone, CIFS o SharePoint. El cambio de contenido se basa en directivas. El asistente genera automáticamente las directivas para identificar si la solicitud es para StorageZone, CIFS o SharePoint. El servidor virtual de conmutación de contenido utiliza estas directivas para dirigir la solicitud al servidor de equilibrio de carga correcto.

Un flujo de datos típico se puede representar como se muestra en el siguiente diagrama.

Ilustración 1. Equilibrio de carga de datos de ShareFile

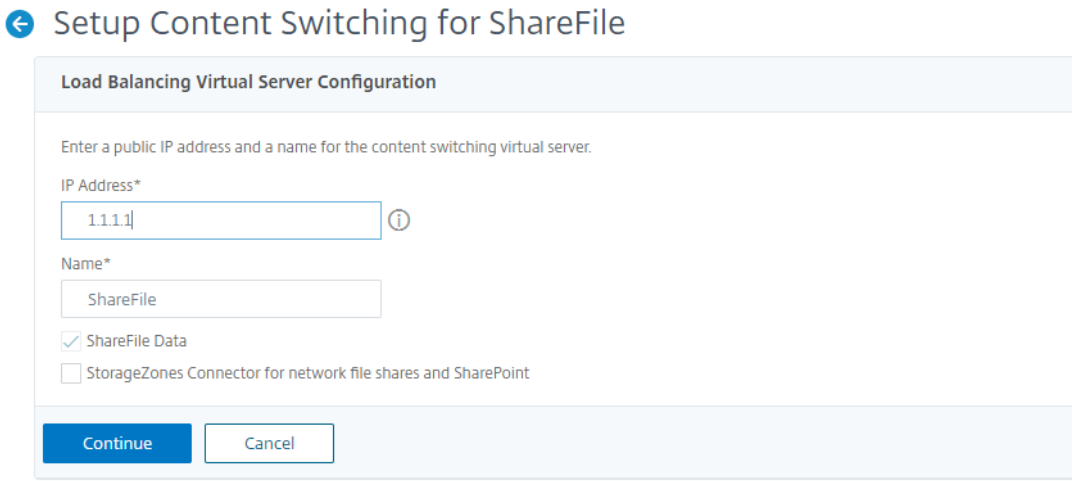


Puede ver los servidores virtuales de equilibrio de carga que crea el asistente para ShareFile navegando a **Administración del tráfico > Servidores y servicios virtuales> Servidores virtuales**. No puede quitar manualmente los servidores virtuales creados con el Asistente para ShareFile. Utilice el asistente para quitar los servidores virtuales.

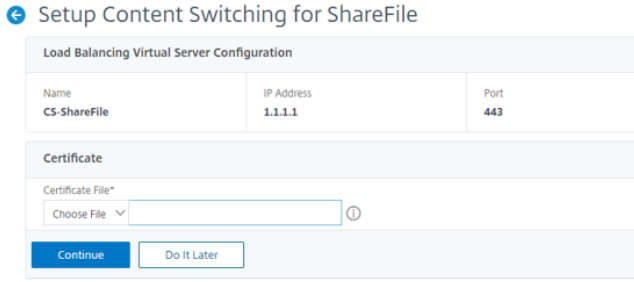
Citrix ADC utiliza la autenticación LDAP para la solicitud de SharePoint o CIFS. La autenticación hash se utiliza para autenticar solicitudes para StorageZones.

Para configurar un dispositivo Citrix ADC para equilibrar la carga Citrix ShareFile

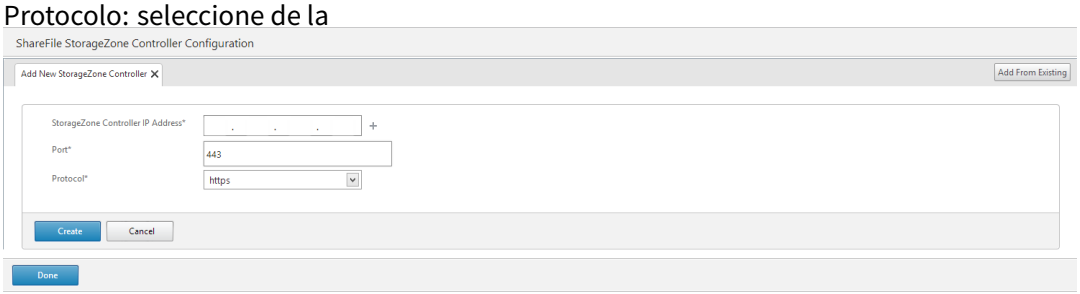
1. En el panel de navegación, haga clic en **Administración del tráfico**.
2. En la sección **Citrix ShareFile**, haga clic en **Configurar Citrix ADC para ShareFile**.
3. En la página **Configurar Cambio de contenido para ShareFile**, proporcione la siguiente información:
   - Dirección IP: Dirección IP del servidor virtual de conmutación de contenido.
   - Nombre: Nombre del servidor virtual de conmutación de contenido.
   - Si quiere configurar el equilibrio de carga para CIFS o SharePoint, haga clic en la casilla de verificación **Conector StorageZone para recursos compartidos de archivos de red/SharePoint** y, a continuación, haga clic en **Continuar**. De forma predeterminada, está activada la casilla **Datos de ShareFile** .



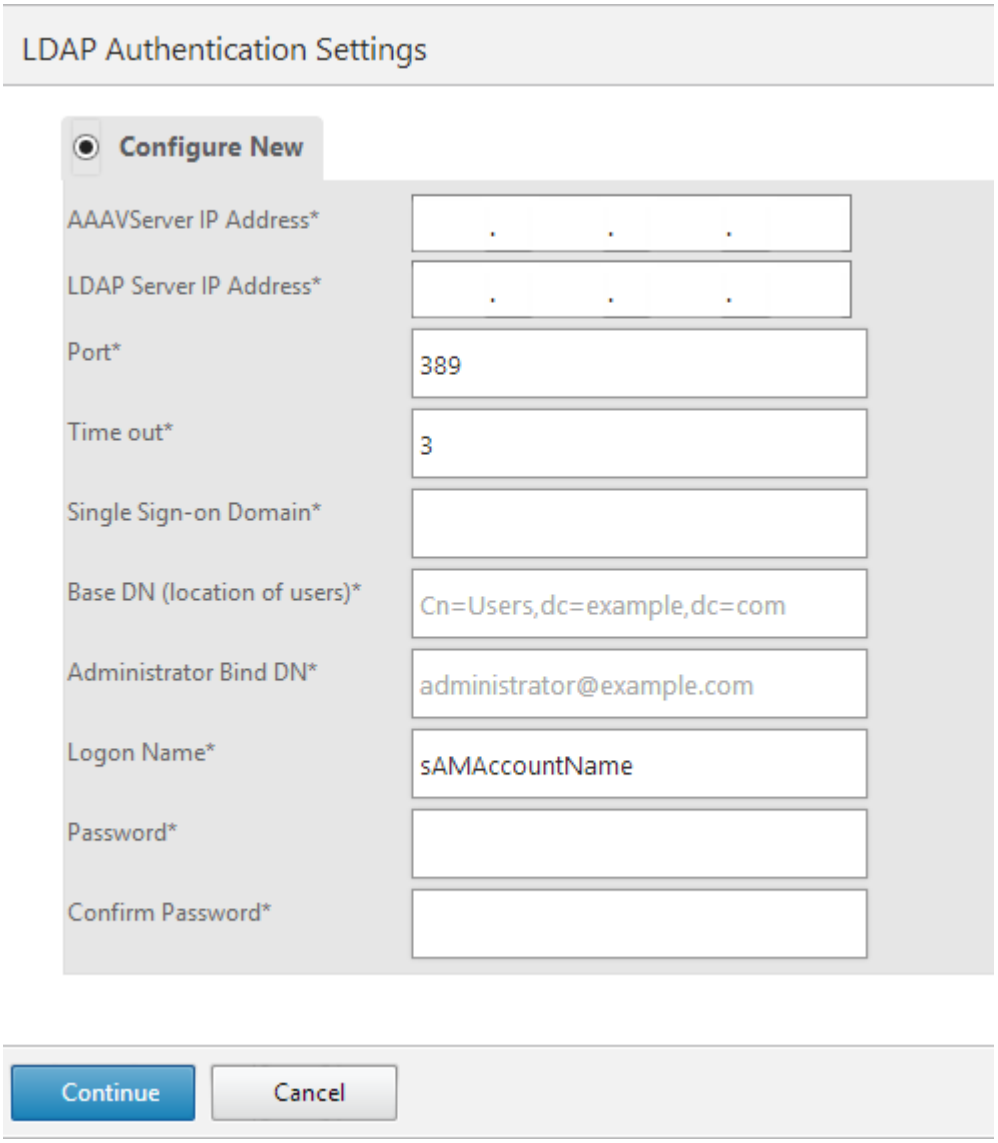
4. Proporcione un certificado válido. Si tiene un certificado, haga clic en **Elegir certificado** y, en la lista desplegable, seleccione el certificado. Si tiene que instalar un certificado, haga clic en **Instalar certificado** y proporcione el par Certificate-Key.



5. Haga clic en **Continuar**.
6. En el cuadro de diálogo **Agregar nuevo controlador StorageZone**, especifique los valores de los siguientes parámetros:
   - Dirección IP del controlador StorageZone: Dirección IP
   - Número de puerto. El valor predeterminado es 443.
   - Protocolo: seleccione de la



7. Haga clic en **Create** y, luego, en **Done**. El asistente crea automáticamente un servicio y genera automáticamente el nombre del servicio.
8. Si eligió el equilibrio de carga para CIFS o SharePoint en el paso 4.c, especifique los valores para Configuración de autenticación LDAP:
   - Dirección IP del servidor virtual Citrix ADC AAA: dirección IP del servidor virtual Citrix ADC AAA
   - Dirección IP del servidor LDAP: Dirección IP del servidor LDAP
   - Número de puerto. El valor predeterminado es 389
   - Tiempo de espera: el valor de tiempo de espera en minutos
   - Dominio de inicio de sesión único: Nombre de dominio de inicio de sesión único
   - DN base: Nombre de dominio base
   - Administrator Bind DN: Nombre de cuenta LDAP con el nombre de dominio, por ejemplo, adminstrator@domainname.com
   - Nombre de inicio de sesión: El nombre de inicio de sesión es samAccountName
   - Contraseña y confirmación de contraseña: introduzca la contraseña y confirme la contraseña



9. Haga clic en **Continuar** y luego haga clic en **Listo**

Para eliminar la configuración de equilibrio de carga para ShareFile

1. En el panel de navegación, haga clic en **Administración del tráfico**.
2. En la sección **Citrix ShareFile**, haga clic en **Quitar configuración de ShareFile**.

Caso práctico 15: Configurar el equilibrio de carga de capa 4 en el dispositivo Citrix ADC

October 5, 2021

El equilibrador de carga de capa 4 (puertos TCP y UDP) utiliza la información proporcionada en la capa de transporte de red para redirigir las solicitudes de los clientes a través de los grupos de servidores.

Cuando se establece una conexión de capa 4 entre un cliente y un servidor, tiene una vista de paquetes del tráfico intercambiado entre ellos. El equilibrador de carga de capa 4 toma sus decisiones de redirección en función de la información de dirección extraída de los primeros paquetes de la transmisión TCP y no inspecciona el contenido del paquete. Por lo tanto, el equilibrio de carga de capa 4 también se denomina equilibrio de cargas basado en conexión.

El equilibrador de carga de capa 4 supervisa el estado de un servidor. El tráfico no se redirige al servidor si está INACTIVO.

El equilibrio de cargas de capa 4 es útil para varias aplicaciones que utilizan cargas útiles TCP o UDP. Dichos protocolos intercambian datos como carga útil TCP y no tienen una estructura específica que seguir.

Para configurar el equilibrio de carga de capa 4 mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

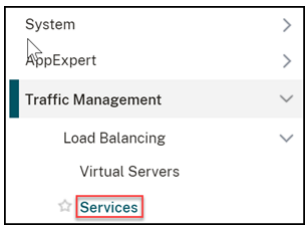
```
add service <name> <serverName> <serviceType> <port>
add lb vserver <name> <serviceType> <ip> <port>
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Ejemplo:

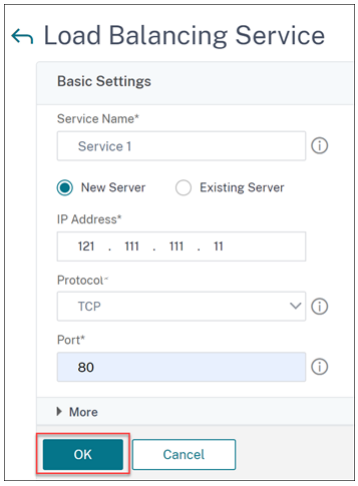
```
add service TCPservice 192.0.2.3 TCP 1
add lb vserver TCPserver TCP 192.0.2.4 1
bind lb vserver TCPserver TCPservice
<!--NeedCopy-->
```

Para configurar el equilibrio de carga de capa 4 mediante la interfaz gráfica de usuario

1. Vaya a **Traffic Management -> Load Balancing -> Services**.



2. Haga clic en **Agregar** para crear un servicio.
3. Especifique los detalles necesarios en **Nombre del servicio** y **dirección IP**.
4. Seleccione **TCP** o **UDP** en **Protocolo**.
5. Haga clic en **OK**.



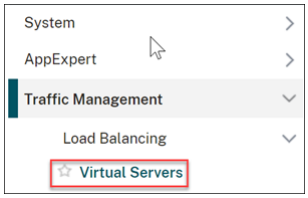
6. Haga clic en **Done**.

   Se crea un servicio.

   Cuando crea un servicio con UDP como protocolo de capa de transporte, un monitor de ping (monitor integrado) se enlza automáticamente al servicio. Al crear un servicio con TCP como protocolo de capa de transporte, un monitor **tcp_default** se enlza automáticamente al servicio.

   Para la configuración del equilibrio de carga, puede vincular su servicio a un tipo diferente de monitor o a varios monitores. Para los requisitos de supervisión anticipada, puede utilizar el monitor **tcp-ecv** y configurar los mensajes de solicitud y respuesta.

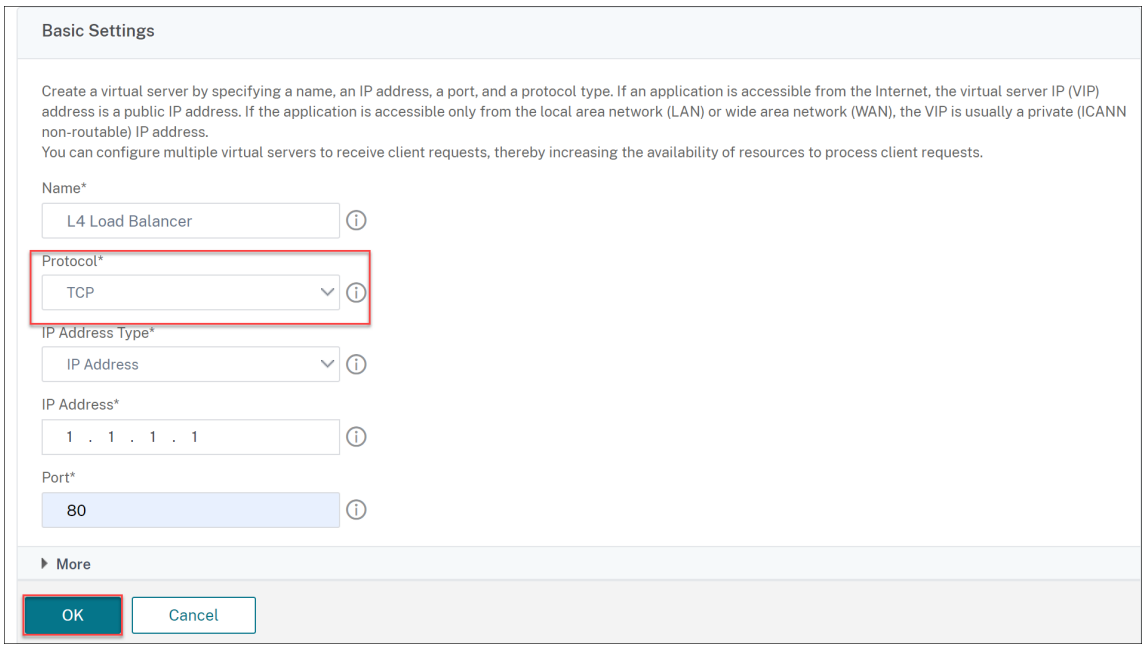
7. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.



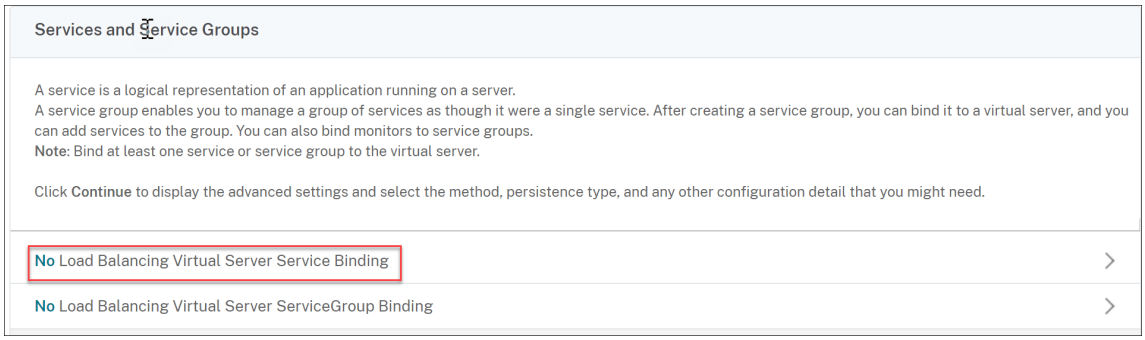
8. Haga clic en **Agregar** para crear un nuevo servidor virtual.

Cuando se configura el equilibrio de carga, puede conectarse al sitio web, aplicación o servidor con equilibrio de carga a través de la dirección IP o el FQDN del servidor virtual.

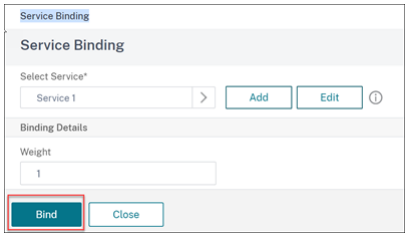
9. Especifique los detalles necesarios en **Nombre**, **Tipo de dirección IP**y **Dirección IP**.
10. Seleccione **TCP** o **UDP** en **Protocolo**.
11. Escriba un número de puerto (0—1023 según el tipo de servicio) en **Puerto**.
12. Haga clic en **OK**.



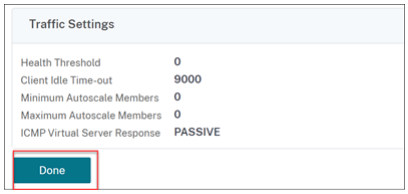
13. Haga clic en **Enlace de servicio de servidor virtual sin equilibrio de carga** en **Servicios y grupos de servicios**.



14. En la página **Enlace de servicio**, seleccione **Haga clic para seleccionar** en **Seleccionar servicio**.
15. Seleccione el servicio que se va a enlazar y haga clic en **Seleccionar**.
16. Haga clic en **Vincular** para enlazar el servicio al servidor virtual.



17. Haga clic en **Continue**.
18. Haga clic en **Done**.



Se ha completado la configuración del servidor virtual de equilibrio de carga de capa 4.

Solucionar problemas

August 20, 2021

Si el equilibrio de carga no funciona como se esperaba después de configurarlo, puede utilizar algunas herramientas comunes para acceder a los recursos de Citrix ADC y diagnosticar el problema.

Recursos para solucionar problemas de equilibrio de carga

Para obtener los mejores resultados, utilice los siguientes recursos para solucionar un problema de cambio de contenido en un dispositivo Citrix ADC:

- Último archivo ns.conf
- `newnslog` Archivos relevantes
- Traces etéreos de paquetes registrados en el dispositivo y en el cliente pertinente, si es posible
- El archivo ns.log

Además de los recursos anteriores, las siguientes herramientas aceleran la solución de problemas:

- Una herramienta de complemento del explorador que puede mostrar encabezados HTTP. Esto se puede utilizar para solucionar problemas relacionados con la persistencia.
- La aplicación Wireshark personalizada para los archivos de seguimiento Citrix ADC.

Solución de problemas de equilibrio de carga

- **Problema**

El uso de la CPU alcanza el 100% cuando un monitor de usuario está vinculado a un servicio vinculado a un servidor virtual en el que está habilitada la opción -m MAC.

- **Solución:**

Enlazar un monitor que no sea usuario al servicio.

- **Problema**

  Creé un script de usuario para supervisar, pero no está funcionando.

  Solución:

  Compruebe el número de argumentos en el script. El límite es 512. Es posible que un script con más de 512 argumentos no funcione correctamente. Utilice el script nsumon-debug.pl de la CLI para depurar el script.

- **Problema**

  Veo muchos sondeos de monitor, y parecen estar aumentando el tráfico de red innecesariamente. ¿Hay alguna forma de apagar las sondas del monitor?

  Solución:

  Puede configurar las conexiones de sonda de monitor inhabilitando el monitor o estableciendo el valor del parámetro HealthMonitor en el comando set service en NO. Con la opción NO, el dispositivo muestra el servicio como UP en todo momento.

- **Problema**

  He configurado monitores para servicios, pero las conexiones siguen dirigidas a servidores que están DOWN.

  Solución:

  Probablemente necesite reducir los intervalos de sondas del monitor. El dispositivo Citrix ADC no detecta el estado DOWN hasta que el monitor envía un sondeo.

- **Problema**

  Una métrica enlazada al monitor está presente en las tablas de métricas locales y personalizadas.

  Solución:

  Agregue el prefijo local al nombre de la métrica si la métrica se elige en la tabla de métricas local. Sin embargo, si la métrica se elige de la tabla personalizada, no es necesario agregar ningún prefijo.

- **Problema**

  Los sondeos del monitor a un servicio no están llegando al servicio.

Solución:

Compruebe si ha establecido un límite en el número de conexiones para un servicio. En caso afirmativo, exime de este límite las conexiones del monitor a la sonda estableciendo el parámetro MonitorSkipMaxClient en ENABLED.

- **Problema**

  Puedo hacer ping a los servidores, pero el estado de los servicios siempre se muestra como DOWN.

  Solución:

  Compruebe el tipo de monitores configurados. Por ejemplo, si un servidor no está configurado para SSL y utiliza un monitor HTTPS, el estado del servicio se marca como DOWN. En este caso, el uso de un monitor TCP debe cambiar el estado del servicio a UP.

- **Problema**

  Establecer un peso para monitores de carga no ayuda a decidir el estado del servicio.

  Solución:

  Los monitores de carga no pueden decidir el estado del servicio. Por lo tanto, establecer un peso en los monitores de carga no es apropiado.

- **Problema**

  Un servicio no es estable.

  Solución:

  Considere la solución de problemas de los siguientes componentes:

  - Compruebe que un servidor correcto está enlazado al servicio.
  - Compruebe el tipo de monitor enlazado al servicio.
  - Verifique los motivos de los errores del monitor. Puede abrir un servicio desde la página Servicios y verificar los detalles del número de sondeos, errores y estado de última respuesta del monitor en la ficha Monitores del cuadro de diálogo Configurar servicio. Para mostrar los detalles, haga clic en el monitor configurado.
  - Si se trata de un monitor personalizado, vincule un monitor TCP o ping al servicio y verifique el estado del monitor. Si esto resuelve el problema, hay algún problema con el monitor personalizado y el monitor requiere más investigación.
  - Puede registrar rastros de paquetes en el dispositivo Citrix ADC y verificar los sondeos del monitor y la respuesta del servidor para una investigación más detallada.

- **Problema**

  La dirección IP virtual (VIP) no es estable o su estado se muestra como DOWN.

  Solución:

Considere la solución de problemas de los siguientes componentes:

- Compruebe que la función de equilibrio de carga tenga licencia.
- Compruebe que la función está habilitada.
- Compruebe que un servicio adecuado está enlazado al servidor virtual.
- Si el estado de la dirección VIP se muestra como DOWN, compruebe que un administrador ha habilitado el servicio. Si no lo es, el estado del servicio debe ser Fuera de servicio. En tal caso, debe habilitar el servicio y verificar si se ha resuelto el problema.
- Verifique los servicios enlazados al servidor virtual y complete los pasos de solución de problemas mencionados para el problema de servicio no estable.
- Si la dirección VIP no es estable, todos los servicios vinculados al servidor virtual deben fallar. Por lo tanto, verifique si todos los servicios están fallando al mismo tiempo. Si es así, hay un problema de red entre el dispositivo Citrix ADC y los servidores.

- **Problema**

  El sitio está experimentando un equilibrio de carga desigual.

  Solución:

  Considere la solución de problemas de los siguientes componentes:

  - Compruebe el método de equilibrio de carga configurado en el dispositivo.
  - Verifique que los pesos asociados con los servicios sean los esperados.
  - Si el método de equilibrio de carga es distinto del round robin, compruebe el número de conexiones al servidor que ha iniciado sesión en el `newnslog` archivo. Puede ejecutar el siguiente comando para verificar el número del `newnslog` archivo:

    ```
    ## nsconmsg -K <newnslog_file> -s ConLb=2 -d oldconmsg
    ```

    Verifique los servicios del servidor virtual específico y compruebe el tiempo de respuesta, las conexiones abiertas establecidas (OE), el número de solicitudes, las solicitudes persistentes y la tasa persistente (P) para solucionar el problema más a fondo.
  - Si el método de equilibrio de carga es round robin, compruebe las solicitudes persistentes como se mencionó en el paso anterior. Además, verifique si el servicio no es estable. Si no es así, complete los pasos de solución de problemas mencionados para el problema de servicio no estable
  - Compruebe si la persistencia está configurada en el dispositivo.
  - Verifique si algún servicio no es estable. En caso afirmativo, complete los pasos de solución de problemas mencionados para el problema de servicio no estable.

- **Problema**

  El estado del servicio se muestra como DOWN.

Solución:

Considere la solución de problemas de los siguientes componentes:

- Compruebe si una dirección de recorte está configurada.
- Compruebe que los monitores adecuados están enlazados al servicio.
- Si los monitores personalizados están enlazados al servicio, vincule un monitor TCP o ping al servicio y verifique el estado del monitor. Si esto resuelve el problema, hay algún problema con el monitor personalizado y el monitor requiere más investigación.
- Compruebe si el estado del servicio se muestra como DOWN para el servidor que se encuentra en otra subred. En caso afirmativo, compruebe si Usar IP de subred (USNIP) resuelve el problema porque puede deberse a que la dirección MIP no puede comunicarse con el servidor.

- **Problema**

  Hay un problema con el tiempo de respuesta.

  Solución:

  Considere la solución de problemas de los siguientes componentes:

  - Compruebe el tiempo de respuesta del servidor desde las estadísticas de servicio ejecutando el siguiente comando:

    ```
    ## nsconmsg -K <newnslog_file> -s ConLb=2 -d oldconmsg
    ```

  - Compruebe si el servicio no es estable y el estado del servicio se muestra como problemas de DOWN.

- **Problema**

  Uno de los servidores sirve más solicitudes que los otros servidores con equilibrio de carga.

  Solución:

  Considere la solución de problemas de los siguientes componentes:

  - Verifique el método de equilibrio de carga. Utilice el método round robin para distribuir la solicitud del cliente por igual independientemente de la carga en los servidores.
  - Determine si la persistencia está habilitada para la configuración de equilibrio de carga. Si la persistencia está habilitada, un servidor determinado podría llevar una carga más pesada para mantener su sesión, especialmente si las sesiones de persistencia son largas.
  - Compruebe si los pesos están asignados a cada servicio. Asignar pesos adecuados ayuda a distribuir la carga correctamente.

- **Problema**

  Las conexiones a un servidor equilibrado de carga específico están estancadas. Por ejemplo, todas las conexiones a un servidor de Outlook pueden estar estancadas.

Solución:

Considere la solución de problemas de los siguientes componentes:

- Verifique el método de equilibrio de carga. Si es round robin, considere cambiar el método a menos conexiones.
- Considere reducir el período de tiempo de espera del monitor. Un período de tiempo de espera más corto ayuda a marcar antes un servicio como APAGADO, lo que ayudaría a dirigir el tráfico hacia el servidor que funciona.
- Si las conexiones están estancadas durante un período prolongado, se podría generar una cola de sobretensiones. Considere vaciar la cola de sobretensiones para evitar un aumento repentino de la carga en el servidor.
- Si los servidores están trabajando en su nivel máximo, considere agregar un nuevo servidor para un mejor rendimiento.

- **Problema**

  La mayoría de las conexiones se dirigen a un servidor determinado, incluso cuando se configura el método de menor conexión para el equilibrio de carga.

  Solución:

  Determine si la persistencia está configurada y es de tipo IP de origen. Si la persistencia de IP de origen se configura incluso con el método de menos conexiones, las solicitudes van a un servidor específico. La dirección IP del servidor es necesaria para mantener la información de la sesión. Considere el uso de cookies HTTP basadas en persistencia.

- **Sugerencias de solución**
  de problemas Para otros problemas, tenga en cuenta los siguientes consejos para solucionar un problema no mencionado anteriormente:

  - Si hay varios monitores de carga enlazados a un servicio, la carga en el servicio es la suma de todos los valores de los monitores de carga enlazados a él. Para que el equilibrio de carga funcione correctamente, debe vincular el mismo conjunto de monitores a todos los servicios.
  - Si inhabilita un monitor de carga vinculado al servicio y el servicio está vinculado a un servidor virtual, el servidor virtual utiliza el método round robin para el equilibrio de carga.
  - Cuando vincula un servicio a un servidor virtual donde el método de equilibrio de carga es CUSTOMLOAD y el estado del servicio es UP, el servidor virtual utiliza el método inicial de round robin para el equilibrio de carga. Sigue estando en fase redonda si el servicio no tiene monitores de carga personalizados o si el estado de al menos uno de los monitores de carga personalizados no está en UP.
  - Todos los servicios que están enlazados a un servidor virtual donde el método de equilibrio de carga es CUSTOMLOAD, los servicios deben tener monitores de carga enlazados a ellos.

- El método de equilibrio de carga CUSTOMLOAD también sigue el round robin de inicio.
- Si inhabilita un enlace basado en métricas y esta es la última métrica activa, el servidor virtual específico utiliza el método round robin para el equilibrio de carga. Una métrica se inhabilita estableciendo el umbral de métrica en cero.
- Cuando una métrica enlazada a un monitor cruza el valor de umbral, ese servicio concreto no se considera para el equilibrio de carga. Si todos los servicios han alcanzado el umbral, el servidor virtual utiliza el método round robin para el equilibrio de carga y aparece un mensaje de error "5xx: Server busy error".
- Se pueden enlazar al monitor un máximo de 10 métricas de una tabla personalizada.
- Los OID deben ser variables escalares.
- Para equilibrar la carga correctamente, el intervalo debe ser lo más bajo posible. Si el intervalo es alto, aumenta el período de tiempo para recuperar el valor de carga. Como resultado, el equilibrio de carga se lleva a cabo mediante valores incorrectos.
- Un usuario no puede modificar la tabla local.

Preguntas frecuentes sobre el equilibrio de carga

August 20, 2021

¿Cuáles son las diversas directivas de equilibrio de carga que puedo crear en el dispositivo Citrix ADC

Puede crear los siguientes tipos de directivas de equilibrio de carga en el dispositivo Citrix ADC:

- Menos conexiones
- Round Robin
- Tiempo de respuesta mínimo
- Ancho de banda mínimo
- Menos paquetes
- hash de URL
- Hash de nombres de dominio
- Hashing de direcciones IP de origen
- Hashing de direcciones IP de destino
- IP de origen: Hash IP de destino
- Token
- LRTM

¿Puedo lograr la seguridad de la comunidad de servidores web implementando el equilibrio de carga con el dispositivo Citrix ADC?

Sí. Puede lograr la seguridad de la comunidad de servidores web implementando el equilibrio de carga mediante el dispositivo Citrix ADC. El dispositivo Citrix ADC permite implementar las siguientes opciones de la función de equilibrio de carga:

- Ocultación de direcciones IP: Permite instalar los servidores reales para estar en el espacio de direcciones IP privado por razones de seguridad y para la conservación de direcciones IP. Este proceso es transparente para el usuario final porque el dispositivo Citrix ADC acepta solicitudes en nombre del servidor. Mientras se encuentra en el modo de ocultación de direcciones, el dispositivo aísla completamente las dos redes. Por lo tanto, un cliente puede acceder a un servicio que se ejecuta en la subred privada, como FTP o un servidor Telnet, a través de un VIP diferente en el dispositivo para ese servicio.
- Asignación de puertos: Permite que los servicios TCP reales se hospeden en puertos no estándar por razones de seguridad. Este proceso es transparente para el usuario final, ya que el dispositivo Citrix ADC acepta solicitudes en nombre del servidor en la dirección IP anunciada estándar y el número de puerto.

¿Cuáles son los distintos dispositivos que puedo utilizar para equilibrar la carga con un dispositivo Citrix ADC?

Puede equilibrar la carga de los siguientes dispositivos con un dispositivo Citrix ADC:

- Comunidades de servidores
- Cachés o proxy inverso
- Dispositivos Firewall
- Sistemas de detección de intrusiones
- Dispositivos de descarga SSL
- Dispositivos de compresión
- Servidores de inspección de contenido

¿Por qué implemento la función de equilibrio de carga para el sitio web?

Puede implementar la función de equilibrio de carga para que el sitio web tenga las siguientes ventajas:

- Reducir el tiempo de respuesta: Cuando implementa la función de equilibrio de carga para el sitio web, uno de los principales beneficios es el impulso que puede esperar en el tiempo de carga. Con dos o más servidores que comparten la carga del tráfico web, cada uno de los servidores ejecuta menos carga de tráfico que un solo servidor. Esto significa que hay más recursos

disponibles para satisfacer las solicitudes del cliente. Esto da como resultado un sitio web más rápido.
- Redundancia: La implementación de la función de equilibrio de carga introduce un poco de redundancia. Por ejemplo, si el sitio web está equilibrado en tres servidores y uno de ellos no responde en absoluto, los otros dos pueden seguir funcionando y los visitantes del sitio web ni siquiera notan ningún tiempo de inactividad. Cualquier solución de equilibrio de carga deja de enviar inmediatamente tráfico al servidor back-end que no está disponible.

¿Por qué necesito desactivar la opción de reenvío basado en Mac (MBF) para el equilibrio de carga de enlace (LLB)?

- Si habilita la opción MBF, el dispositivo Citrix ADC considera que el tráfico entrante del cliente y el tráfico saliente al mismo cliente fluyen a través del mismo enrutador ascendente. Sin embargo, la función LLB requiere que se elija la mejor ruta para el tráfico de retorno.
- Habilitar la opción MBF rompe este diseño de topología al enviar el tráfico saliente a través del enrutador que reenvió el tráfico de cliente entrante.

Redes

August 20, 2021

En los temas siguientes se proporciona una referencia conceptual e instrucciones para configurar los distintos componentes de red en el dispositivo Citrix ADC.

Dirección IP	Conozca los distintos tipos de direcciones IP propiedad de Citrix ADC y cómo crearlas, personalizarlas y quitarlas.
Interfaces	Configure algunas de las configuraciones de red básicas que se deben realizar para comenzar.
Listas de control de acceso (ACL)	Configure los diferentes tipos de listas de control de acceso y cómo crearlas, personalizarlas y quitarlas.
Redirección de IP	Aprenda y configure la funcionalidad de redirección del dispositivo Citrix ADC, tanto estático como dinámico.

Protocolo de Internet versión 6 (IPv6)	Descubra cómo el dispositivo Citrix ADC admite IPv6.
Dominios de tráfico	Aprenda y configure dominios de tráfico para segmentar el tráfico de red para diferentes aplicaciones.
VXLAN	Aprenda y configure las VXLAN para satisfacer las necesidades de escalabilidad de su centro de datos.

Dirección IP

January 12, 2021

Antes de configurar el dispositivo Citrix ADC, debe asignar la dirección NSIP, también conocida como dirección IP de administración. También puede crear otras direcciones IP propiedad de Citrix ADC para abstraer servidores y establecer conexiones con los servidores. En este tipo de configuración, el dispositivo sirve como proxy para los servidores abstractos. También puede proxy conexiones mediante traducciones de direcciones de red (INAT y RNAT). Al realizar conexiones proxy, el dispositivo puede comportarse como un dispositivo de conexión en puente (capa 2) o como un dispositivo de reenvío de paquetes (capa 3). Para que el reenvío de paquetes sea más eficiente, puede configurar entradas ARP estáticas. Para IPv6, puede configurar la detección de vecinos (ND).

Configuración de direcciones IP propiedad de Citrix ADC

January 12, 2021

Las direcciones IP propiedad de Citrix ADC (dirección NSIP, direcciones IP virtuales (VIP), direcciones IP de subred (SNIP) y direcciones IP de sitios de equilibrio de carga global del servidor (GSLBIP) solo existen en el dispositivo Citrix ADC. El NSIP identifica de forma exclusiva el Citrix ADC en la red y proporciona acceso al dispositivo. Un VIP es una dirección IP pública a la que un cliente envía solicitudes. Citrix ADC termina la conexión del cliente en el VIP e inicia una conexión con un servidor. Esta nueva conexión utiliza un SNIP o un MIP como dirección IP de origen para los paquetes reenviados al servidor. Si tiene varios centros de datos distribuidos geográficamente, cada centro de datos se puede identificar mediante un GSLBIP único. Puede configurar algunas direcciones IP propiedad de Citrix ADC para proporcionar acceso a las aplicaciones de administración.

Configuración de la dirección NSIP

August 20, 2021

La dirección NSIP es la dirección IP en la que se accede al dispositivo Citrix ADC con fines de administración. El dispositivo solo puede tener un NSIP, que también se denomina dirección IP de administración. Debe agregar esta dirección IP cuando configure Citrix ADC por primera vez. No se puede quitar una dirección NSIP. Por razones de seguridad, el NSIP debe ser una dirección IP no enrutable en la LAN de su organización.

Si modifica esta dirección, debe reiniciar el dispositivo Citrix ADC. Si la dirección de subred de la nueva dirección NSIP es diferente de la anterior, debe agregar una ruta predeterminada para esta subred para que la nueva dirección NSIP sea accesible desde otras redes de la LAN.

> **Importante**
>
> La configuración de la dirección NSIP es obligatoria.

Cambiar la dirección NSIP de un dispositivo Citrix ADC consta de las siguientes tareas:

- Cambie la dirección NSIP.
- Agregue una ruta predeterminada para la dirección de subred de la dirección NSIP, si no hay una.
- Guarde la configuración.
- Reinicie el dispositivo.

Procedimientos de línea de comandos

Para cambiar la dirección NSIP mediante la CLI:

En el símbolo del sistema, escriba:

- **set ns config -IPAddress** <ip_addr> **-netmask** <netmask>
- **mostrar configuración ns**

Para agregar una ruta predeterminada mediante la CLI:

En el símbolo del sistema, escriba:

- **add route 0 0** <gateway IP address>
- **show route**

Para guardar la configuración mediante la CLI:

En el símbolo del sistema, escriba:

- **save config**

Para reiniciar el dispositivo Citrix ADC mediante la CLI:

En el símbolo del sistema, escriba:

- **reboot**

Procedimientos de GUI

Para configurar la dirección NSIP mediante la GUI:

1. Haga clic en el icono de engranaje situado en la esquina superior derecha de la página **Configuración**.
2. Haga clic en el panel de **direcciones NSIP**.
3. En la página de **dirección NSIP**, establezca los parámetros siguientes y, a continuación, haga clic en **Listo** :
    - Dirección NSIP
    - Máscara de red

Para agregar una ruta predeterminada mediante la GUI:

Vaya a **Sistema** > **Red** > **Rutas** y, en la ficha **Básico**, agregue una ruta predeterminada con los parámetros siguientes y, a continuación, haga clic en **Crear**.

- Red (establecida en cero)
- Máscara de red (establecida en cero)
- Puerta de enlace (dirección IP de la Gateway)

Para reiniciar Citrix ADC mediante la GUI:

1. En la página de la ficha **Información del sistema** del nodo **Sistema**, haga clic en **Reiniciar**.
2. Cuando se le solicite reiniciar, seleccione **Guardar configuración** para asegurarse de que no pierde ninguna configuración.

Configuración de ejemplo

En el ejemplo siguiente, la dirección NSIP de un dispositivo Citrix ADC se cambia a 192.0.2.90, que tiene una dirección de subred diferente (192.0.2.0/24) que la dirección NSIP anterior. Por lo tanto, se agrega una ruta predeterminada para esta subred, de modo que la nueva dirección NSIP sea accesible desde otras redes.

```
1 > set nsconfig -ipAddress 192.0.2.90 -netmask 255.255.255.0
2
3  Warning: The configuration must be saved and the system rebooted for
      these settings to take effect
```



```
> add route 0 0 192.0.2.1

 Warning: The configuration must be saved and the system rebooted for
    these settings to take effect
> save config

 Done
> reboot
```

Configuración y administración de direcciones IP virtuales (VIP)

August 20, 2021

La configuración de una dirección IP (VIP) del servidor virtual no es obligatoria durante la configuración inicial del Citrix ADC. Cuando configura el equilibrio de carga, asigna direcciones VIP a servidores virtuales.

Para obtener más información sobre cómo configurar una configuración de equilibrio de carga, consulte Equilibrio de carga.

En algunas situaciones, debe personalizar atributos VIP o habilitar o inhabilitar una dirección VIP. Por lo general, una dirección VIP se asocia con un servidor virtual y algunos de los atributos VIP se personalizan para cumplir con los requisitos del servidor virtual. Puede alojar el mismo servidor virtual en varios dispositivos Citrix ADC que residen en el mismo dominio de difusión mediante los atributos ARP e ICMP. Después de agregar un VIP (o cualquier dirección IP), el dispositivo envía solicitudes ARP y, a continuación, responde a ellas. Los VIP son las únicas direcciones IP propiedad de Citrix ADC que se pueden inhabilitar. Cuando se inhabilita una dirección VIP, el servidor virtual que la utiliza se apaga y no responde a las solicitudes de servicio ARP, ICMP o L4. Como alternativa a la creación de direcciones VIP de una en una, puede especificar un rango consecutivo de direcciones VIP.

Para crear una dirección VIP mediante la CLI:

En el símbolo del sistema, escriba:

- add ns ip <IPAddress> <netmask> -type <type>
- show ns ip <IPAddress>

Ejemplo:

```
> add ns ip 10.102.29.59 255.255.255.0 -type VIP
 Done
<!--NeedCopy-->
```


Para crear un rango de direcciones VIP mediante la CLI:

En el símbolo del sistema, escriba:

- add ns ip <IPAddress> <netmask> -type <type>
- show ns ip <IPAddress>

Ejemplo:

```
> add ns ip 10.102.29.[60-64] 255.255.255.0 -type VIP
ip ”10.102.29.60” added
ip ”10.102.29.61” added
ip ”10.102.29.62” added
ip ”10.102.29.63” added
ip ”10.102.29.64” added
 Done
<!--NeedCopy-->
```

Para habilitar o inhabilitar una dirección VIP IPv4 mediante la CLI:

En el símbolo del sistema, escriba uno de los siguientes conjuntos de comandos para habilitar o inhabilitar un VIP y verificar la configuración:

- <IPAddress>habilitar ns ip
- show ns ip <IPAddress>
- <IPAddress>desactivar ns ip
- show ns ip <IPAddress>

Ejemplo:

```
> enable ns ip 10.102.29.79
 Done
> show ns ip 10.102.29.79

        IP: 10.102.29.79
        Netmask: 255.255.255.255
        Type: VIP
        state: Enabled
        arp: Enabled
        icmp: Enabled
        vserver: Enabled
        management access: Disabled
          telnet: Disabled
          ftp: Disabled
```



```
15            ssh: Disabled
16            gui: Disabled
17            snmp: Disabled
18          Restrict access: Disabled
19          dynamic routing: Disabled
20          hostroute: Disabled
21  Done
22 > disable ns ip 10.102.29.79
23  Done
24 > show ns ip 10.102.29.79
25
26          IP: 10.102.29.79
27          Netmask: 255.255.255.255
28          Type: VIP
29          state: Disabled
30          arp: Enabled
31          icmp: Enabled
32          vserver: Enabled
33          management access: Disabled
34            telnet: Disabled
35            ftp: Disabled
36            ssh: Disabled
37            gui: Disabled
38            snmp: Disabled
39          Restrict access: Disabled
40          dynamic routing: Disabled
41          hostroute: Disabled
42
43  Done
44 <!--NeedCopy-->
```

Para configurar una dirección VIP mediante la GUI:

Vaya a **Sistema** > **Red** > **Direcciones IP** > **Direcciones IPv4** y agregue una nueva dirección IP o modifique una dirección existente.

Para crear un rango de direcciones VIP mediante la GUI:

1. Vaya a **Sistema** > **Red** > **Direcciones IP** > **Direcciones IPv4**.
2. En la lista **Acción**, seleccione **Agregar rango**.

Para habilitar o inhabilitar una dirección VIP mediante la GUI:

1. Vaya a **Sistema** > **Red** > **Direcciones IP** > **Direcciones IPv4**.
2. Lleve a cabo una de las siguientes acciones:
   - Seleccione una dirección VIP.

- Mantenga **pulsada la tecla Ctrl** y seleccione varias entradas de dirección del servidor.
- Mantenga pulsada la **tecla Mayús** y seleccione un rango de entradas de direcciones del servidor.
- Seleccione todas las direcciones seleccionando la casilla de verificación situada en el lado izquierdo de la fila de encabezado.

3. En la lista **Acción**, seleccione **Inhabilitar** o **Habilitar**.

Detección de un dispositivo Citrix ADC en una configuración de equilibrio de carga UDP mediante actualizaciones TTL

En la siguiente tabla se muestra cómo un dispositivo Citrix ADC maneja el valor TTL de los paquetes recibidos en diferentes funcionalidades.

Funcionalidad	Valor TTL
Servidor virtual	TTL se establece en 255 al reenviar la solicitud a los servidores back-end. TTL se reduce en 1 al reenviar la respuesta al cliente.
Modo L2	TTL no se cambia.
Modo L3	TTL se establece en 255.
INAT	TTL se establece en 255 al reenviar la solicitud al servidor back-end. TTL se reduce en 1 al reenviar la respuesta al cliente.

Algunas empresas/casos que ejecutan una aplicación de supervisión requieren que el dispositivo Citrix ADC de una configuración de equilibrio de carga se detecte como uno de los saltos en un traceroute. Un dispositivo Citrix ADC de una configuración de equilibrio de carga no se detecta en un traceroute porque, de forma predeterminada, el dispositivo establece el valor TTL en 255 en lugar de reducirlo al reenviar la solicitud a un servidor back-end.

Para cumplir con este requisito, se puede utilizar el parámetro **Decrement TTL** de una dirección VIP. Este parámetro se aplica a todos los servidores virtuales UDP que utilizan este VIP.

Cuando habilita el parámetro **Decrement TTL** de un VIP, el dispositivo Citrix ADC disminuye el valor TTL en 1 en lugar de establecerlo en 255 al reenviar solicitudes, que se reciben en los servidores virtuales UDP que utilizan este VIP.

La supervisión de aplicaciones que utilizan datos de traceroute ahora puede detectar la presencia de un dispositivo Citrix ADC de una configuración de equilibrio de carga UDP.

Antes de comenzar

Antes de comenzar a configurar un dispositivo Citrix ADC para que se detecte en un traceroute de una configuración de equilibrio de carga, tenga en cuenta los siguientes puntos:

- El parámetro TTL de decremento solo se admite para servidores virtuales de equilibrio de carga UDP.
- Se admite el parámetro TTL de decremento para direcciones VIP IPv4 y VIP IPv6 (VIP6).
- El parámetro Decrement TTL es compatible con dispositivos Citrix ADC independientes, así como con configuraciones de clúster y alta disponibilidad (HA).

Pasos de configuración

La configuración de un dispositivo Citrix ADC para que se detecte en un traceroute de una configuración de equilibrio de carga UDP consiste en las siguientes tareas:

- Crear una configuración de equilibrio de carga UDP
- Habilitar el parámetro Decrement TTL para la dirección VIP

Procedimientos CLI

Para habilitar la opción de decremento TTL para una dirección VIP mediante la CLI:

- Para habilitar la opción de decremento TTL para una dirección VIP mientras agrega la dirección VIP, en el símbolo del sistema, escriba:
  - **add ns ip** <ip> <mask> -**tipo VIP** -**DecrementTTL ENABLED**
  - **show ns ip** <VIP address>
- Para habilitar la opción de decremento TTL para una dirección VIP existente, en el símbolo del sistema, escriba:
  - **set ns ip** <ip> <mask> -**decrementTTL ENABLED**
  - **show ns ip** <VIP address>

Para habilitar la opción de decremento TTL para una dirección VIP6 mediante la CLI:

- Para habilitar la opción TTL decrement para una dirección VIP6 al agregar la dirección VIP6, en el símbolo del sistema, escriba:
  - **add ns ip6** <IP6/prefix> <mask> -**type VIP** -**decrementTTL ENABLED**
  - **show ns ip6** <VIP6/prefix>
- Para habilitar la opción de decremento TTL para una dirección VIP6 existente, en el símbolo del sistema, escriba:
  - **set ns ip6** <ip6/prefix> <mask> -**DecrementTTL ENABLED**
  - **show ns ip6** <VIP6 address>


```
    > add ns ip 203.0.113.30 -type VIP -decrementTTL ENABLED
     Done

    > add ns ip6  2001:DB8:5001::30 -type VIP -decrementTTL ENABLED
     Done
<!--NeedCopy-->
```

Procedimientos de GUI

Para habilitar la opción de decremento TTL para una dirección VIP mediante la GUI:

Vaya a **Sistema** > **Red** > **Direcciones IP** > **Direcciones IPv4** y habilite el parámetro **Decrement TTL** mientras agrega una nueva dirección VIP o modifica una dirección existente.

Para habilitar la opción TTL decrement para una dirección VIP6 mediante la GUI:

Vaya a **Sistema** > **Red** > **Direcciones IP** > **IPv6s** y habilite el parámetro **Decrement TTL** mientras agrega una nueva dirección VIP6 o modifica una dirección existente.

Configuración de la supresión de respuesta ARP para direcciones IP virtuales (VIP)

August 20, 2021

Puede configurar el dispositivo Citrix ADC para que responda o no responda a las solicitudes ARP de una dirección IP virtual (VIP) en función del estado de los servidores virtuales asociados a ese VIP.

Por ejemplo, si los servidores virtuales V1, de tipo HTTP, y V2, de tipo HTTPs, comparten la dirección VIP 10.102.29.45 en un dispositivo Citrix ADC, puede configurar el dispositivo para que no responda a ninguna solicitud ARP para VIP 10.102.29.45 si V1 y V2 están en estado DOWN.

Las tres opciones siguientes están disponibles para configurar la supresión de respuesta ARP para una dirección IP virtual.

- **NINGUNO**. El dispositivo Citrix ADC responde a cualquier solicitud ARP para la dirección VIP, independientemente del estado de los servidores virtuales asociados a la dirección.
- **UN SERVIDOR VV**. El dispositivo Citrix ADC responde a cualquier solicitud ARP para la dirección VIP si al menos uno de los servidores virtuales asociados está en estado ACTIVO.
- **TODOS LOS SERVIDORES VIRTUALES**. El dispositivo Citrix ADC responde a cualquier solicitud ARP para la dirección VIP si todos los servidores virtuales asociados están en estado ACTIVO.

La siguiente tabla muestra el comportamiento de ejemplo del dispositivo Citrix ADC para un VIP configurado con dos servidores virtuales:

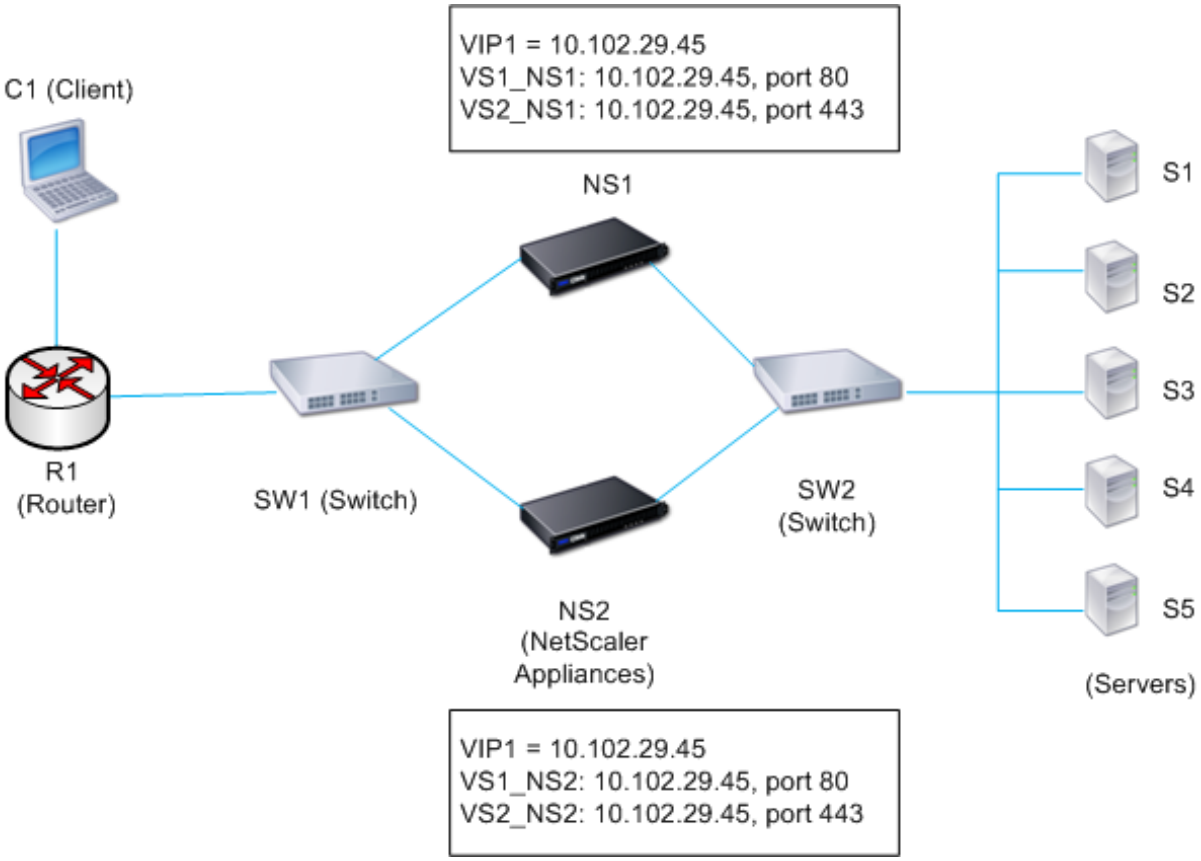
Servidores virtuales asociados para un VIP	ESTADO 1	ESTADO 2	ESTADO 3	ESTADO 4
NONE				
V1	ACTIVO	ACTIVO	INACTIVO	INACTIVO
V2	ACTIVO	INACTIVO	ACTIVO	INACTIVO
¿Responder a una solicitud ARP para este VIP?	Sí	Sí	Sí	Sí
UN VSERVER				
V1	ACTIVO	ACTIVO	INACTIVO	INACTIVO
V2	ACTIVO	INACTIVO	ACTIVO	INACTIVO
¿Responder a una solicitud ARP para este VIP?	Sí	Sí	Sí	No
TODOS LOS SERVIDORES VIRTUALES				
V1	ACTIVO	ACTIVO	INACTIVO	INACTIVO
V2	ACTIVO	INACTIVO	ACTIVO	INACTIVO
¿Responder a una solicitud ARP para este VIP?	Sí	No	No	No

Considere un ejemplo en el que quiere probar el rendimiento de dos servidores virtuales, V1 y V2, que tienen la misma dirección VIP pero son de diferentes tipos y están configurados cada uno en los dispositivos Citrix ADC NS1 y NS2. Llamemos a la dirección VIP compartida *VIP1*.

V1 equilibra la carga de los servidores S1, S2 y S3. V2 equilibra la carga de los servidores S4 y S5.

En NS1 y NS2, para VIP1, el parámetro de supresión ARP se establece en ALL_VSERVER. Si quiere probar el rendimiento de V1 y V2 en NS1, debe inhabilitar manualmente V1 y V2 en NS2, de modo que NS2 no responda a ninguna solicitud ARP para VIP1.

Ilustración 1.



El flujo de ejecución es el siguiente:

1. El cliente C1 envía una solicitud a V1. La solicitud llega a R1.
2. R1 no tiene una entrada APR para la dirección IP (VIP1) de V1, por lo que R1 transmite una solicitud ARP para VIP1.
3. NS1 responde con la dirección MAC de origen MAC1 y la dirección IP de origen VIP1. NS2 no responde a la solicitud ARP.
4. SW1 aprende el puerto para VIP1 a partir de la respuesta ARP y actualiza su tabla de puente, y R1 actualiza la entrada ARP con MAC1 y VIP1.
5. R1 reenvía el paquete a la dirección VIP1 en NS1.
6. El algoritmo de equilibrio de carga de NS1 selecciona el servidor S2 y NS1 abre una conexión entre una de sus direcciones SNIP y S2. Cuando S2 envía una respuesta al cliente, la respuesta devuelve por la misma ruta.
7. Ahora quiere probar el rendimiento de V1 y V2 en NS2, de modo que habilite V1 y V2 en NS2 y los inhabilite en NS1. NS2 ahora transmite un mensaje ARP para VIP1. En el mensaje, MAC2 es la dirección MAC de origen y VIP1 es la dirección IP de origen.
8. SW1 aprende el número de puerto para llegar a MAC2 desde la difusión ARP y actualiza su tabla de puente para enviar solicitudes de cliente posteriores para VIP1 a NS2. R1 actualiza su tabla ARP.

9. Ahora supongamos que la entrada ARP para VIP1 se agita en la tabla ARP de R1, y el cliente C1 envía una solicitud para V1. Como R1 no tiene una entrada APR para VIP1, emite una solicitud ARP para VIP1.
10. NS2 responde con una dirección MAC de origen y VIP1 como dirección IP de origen. NS1 no responde a la solicitud ARP.

Para configurar la supresión de respuesta ARP mediante la CLI:

En el símbolo del sistema, escriba:

- **set ns ip** -**ArpResponse** <arpResponse>]
- **sh ns ip** <IPAddress>

Ejemplo:

```
1 > set ns ip 10.102.29.96 -arpResponse ALL_VSERVERS
2  Done
3 <!--NeedCopy-->
```

Para configurar la supresión de respuesta ARP mediante la GUI:

1. Vaya a **Sistema** > **Red** > **Direcciones IP** > **Direcciones IPv4**.
2. Abra una entrada de dirección IP y seleccione el tipo de respuesta ARP.

Configuración de Direcciones IP de Subred (SNIP)

August 20, 2021

Una dirección IP de subred (SNIP) es una dirección IP propiedad de Citrix ADC que utiliza Citrix ADC para comunicarse con los servidores.

El Citrix ADC utiliza la dirección IP de la subred como dirección IP de origen para proxy las conexiones de cliente a los servidores. También utiliza la dirección IP de subred cuando genera sus propios paquetes, como paquetes relacionados con protocolos de redirección dinámica, o para enviar sondeos de monitor para comprobar el estado de los servidores. Dependiendo de la topología de red, es posible que tenga que configurar uno o más SNIP para diferentes casos.

Para configurar una dirección SNIP en un dispositivo Citrix ADC, agregue la dirección SNIP y, a continuación, habilite el modo global Usar IP de subred (USNIP). Como alternativa a la creación de SNIP de uno en uno, puede especificar un rango consecutivo de SNIP.

Para configurar una dirección SNIP mediante la CLI:

En el símbolo del sistema, escriba:

- add ns ip <IPAddress> <netmask> -type SNIP
- show ns ip <IPAddress>

Ejemplo:

```
> add ns ip 10.102.29.203 255.255.255.0 -type SNIP
 Done
<!--NeedCopy-->
```

Para crear un rango de direcciones SNIP mediante la CLI:

En el símbolo del sistema, escriba:

- add ns ip <IPAddress> <netmask> -type SNIP
- show ns ip <IPAddress>

Ejemplo:

```
> add ns ip 10.102.29.[205-209] 255.255.255.0 -type SNIP
ip "10.102.29.205" added
ip "10.102.29.206" added
ip "10.102.29.207" added
ip "10.102.29.208" added
ip "10.102.29.209" added
 Done
<!--NeedCopy-->
```

Para habilitar o inhabilitar el modo USNIP mediante la CLI:

En el símbolo del sistema, escriba uno de los siguientes comandos:

- enable ns modeUSNIP
- disable ns modeUSNIP

Para configurar una dirección SNIP mediante la GUI:

Desplácese hasta Sistema > Red > Direcciones IP > Direcciones IPv4 y agregue una nueva dirección SNIP o modifique una dirección existente.

Para crear un rango de direcciones SNIP mediante la GUI:

1. Vaya a Sistema > Red > Direcciones IP > Direcciones IPv4.
2. En la lista Acción, seleccione Agregar rango.

Para habilitar o inhabilitar el modo USNIP mediante la CLI:

En el símbolo del sistema, escriba uno de los siguientes comandos:

- enable ns mode USNIP
- disable ns mode USNIP

Para habilitar o inhabilitar el modo USNIP mediante la GUI:

1. Desplácese hasta Sistema > Configuración, en el grupo Modos y funciones, haga clic en Cambiar modos.
2. Seleccione o desactive la opción Usar IP de subred.

Uso de SNIP para una subred de servidor conectada directamente

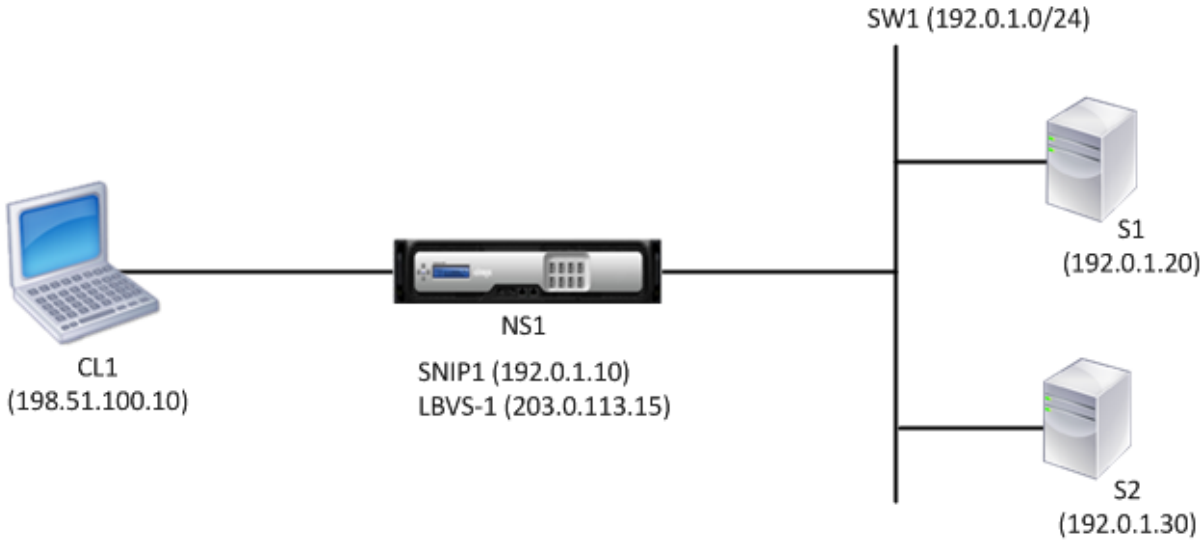
Para habilitar la comunicación entre el Citrix ADC y un servidor que esté conectado directamente al Citrix ADC o conectado solo a través de un conmutador L2, debe configurar una dirección IP de subred que pertenezca a la subred del servidor. Debe configurar al menos una dirección IP de subred para cada subred conectada directamente, excepto para la subred de administración conectada directamente que está conectada a través de NSIP.

Considere un ejemplo de configuración de equilibrio de carga en la que el servidor virtual de equilibrio de carga LBVS1 en Citrix ADC NS1 se utiliza para equilibrar la carga servidores S1 y S2, que están conectados a NS1 a través del conmutador L2 SW1. S1 y S2 pertenecen a la misma subred.

La dirección SNIP SNIP1, que pertenece a la misma subred que S1 y S2, se configura en NS1. Tan pronto como SNIP1 está configurado, NS1 transmite paquetes ARP para SNIP1.

Los servicios SVC-S1 y SVC-S2 en NS1 representan S1 y S2. Tan pronto como se configuran estos servicios, NS1 transmite solicitudes ARP para S1 y S2 para resolver la asignación de IP a Mac. Después de responder S1 y S2, NS1 les envía sondas de supervisión a intervalos regulares, desde la dirección SNIP1, para comprobar su estado.

Para obtener más información sobre cómo configurar el equilibrio de carga en un Citrix ADC, consulte Equilibrio de carga.



A continuación se presenta el flujo de tráfico en este ejemplo:

1. El cliente C1 envía un paquete de solicitud a LBVS-1. El paquete de solicitud tiene:
   - IP de origen = dirección IP del cliente (198.51.100.10)
   - IP de destino = dirección IP de LBVS-1 (203.0.113.15)
2. LBVS1 de NS1 recibe el paquete de solicitud.
3. El algoritmo de equilibrio de carga de LBVS1 selecciona el servidor S2.
4. Dado que S2 está conectado directamente a NS1 y SNIP1 (192.0.1.10) es la única dirección IP en NS1 que pertenece a la misma subred que S2, NS1 abre una conexión entre SNIP1 y S2.
5. NS1 envía el paquete de solicitud a S2 desde SNIP1. El paquete de solicitud tiene:
   - IP de origen = SNIP1 (192.0.1.10)
   - IP de destino = dirección IP de S2 (192.0.1.30)
6. La respuesta de S2 regresa por la misma ruta.

Uso de SNIP para subredes de servidor conectadas a través de un router

Para habilitar la comunicación entre Citrix ADC y los servidores en subredes conectadas a través de un enrutador, debe configurar al menos una dirección IP de subred que pertenezca a la subred de la interfaz conectada directamente al enrutador. El ADC utiliza esta dirección IP de subred para comunicarse con servidores en subredes a las que se puede acceder a través del enrutador.

Considere un ejemplo de una configuración de equilibrio de carga en la que el servidor virtual de equilibrio de carga LBVS1 en Citrix ADC NS1 se utiliza para equilibrar la carga servidores S1, S2, S3 y S4, que están conectados a NS1 a través del enrutador R1.

S1 y S2 pertenecen a la misma subred, 192.0.2.0/24, y están conectados a R1 a través del conmutador L2 SW1. S3 y S4 pertenecen a una subred diferente, 192.0.3.0/24, y están conectados a R1 a través del conmutador L2 SW2.

Citrix ADC NS1 está conectado al router R1 a través de la subred 192.0.1.0/24. La dirección SNIP SNIP1, que pertenece a la misma subred que la interfaz conectada directamente al router (192.0.1.0/24), está configurada en NS1. NS1 utiliza esta dirección para comunicarse con los servidores S1 y S2, y con los servidores S3 y S4.

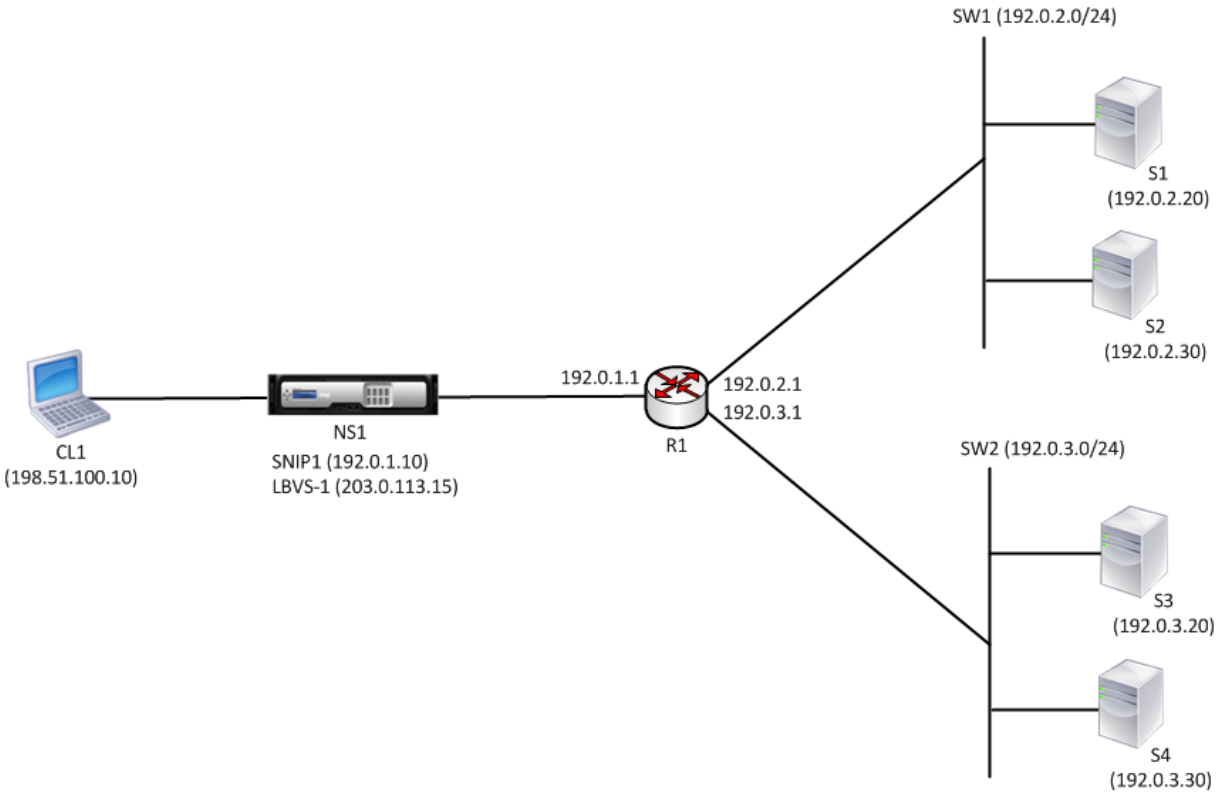
Para obtener más información sobre cómo configurar el equilibrio de carga en un Citrix ADC, consulte Equilibrio de carga.

Tan pronto como se configura la dirección SNIP1, NS1 transmite paquetes de anuncio ARP para SNIP1.

La tabla de redirección de NS1 consiste en entradas de ruta para S1, S2, S3 y S4 a R1. Estas entradas de ruta son entradas de ruta estáticas o anunciadas por R1 a NS1, mediante protocolos de redirección dinámica.

Los servicios SVC-S1, SVC-S2, SVC-S3 y SVC-S4 en NS1 representan los servidores S1, S2, S3 y S4. NS1 encuentra, en sus tablas de redirección, que estos servidores son accesibles a través de R1. NS1 les envía sondeos de supervisión a intervalos regulares, desde la dirección SNIP1, para comprobar su estado.

Para obtener más información sobre la redirección IP en un Citrix ADC, consulte Redirección de IP.



A continuación se presenta el flujo de tráfico en este ejemplo:

1. El cliente C1 envía un paquete de solicitud a LBVS-1. El paquete de solicitud tiene:
   - IP de origen = dirección IP del cliente (198.51.100.10)

    - IP de destino = dirección IP de LBVS-1 (203.0.113.15)
2. LBVS1 de NS1 recibe el paquete de solicitud.
3. El algoritmo de equilibrio de carga de LBVS1 selecciona el servidor S3.
4. NS1 comprueba su tabla de redirección y descubre que S3 es accesible a través de R1. SNIP1 (192.0.1.10) es la única dirección IP en NS1 que pertenece a la misma subred que el router R1, NS1 abre una conexión entre SNIP1 y S3 a R1.
5. NS1 envía el paquete de solicitud a R1 desde SNIP1. El paquete de solicitud tiene:
    - Dirección IP de origen = SNIP1 (192.0.1.10)
    - Dirección IP de destino = dirección IP de S3 (192.0.3.20)
6. La solicitud llega a R1, que comprueba su tabla de redirección y reenvía el paquete de solicitud a S3.
7. La respuesta de S3 devuelve por la misma ruta.

Uso de SNIP para varias subredes de servidor (VLAN) en un conmutador L2

Cuando tiene varias subredes de servidor (VLAN) en un conmutador L2 conectado a un dispositivo Citrix ADC, debe configurar al menos una dirección SNIP para cada una de las subredes de servidor, de modo que Citrix ADC pueda comunicarse con estas subredes de servidor.

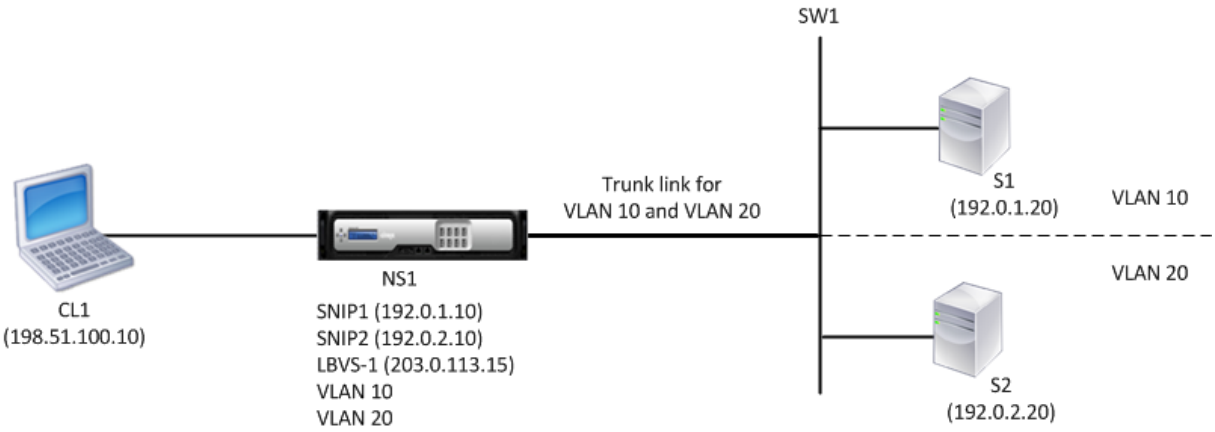
Considere un ejemplo de configuración de equilibrio de carga en la que el servidor virtual de equilibrio de carga LBVS1 en Citrix ADC NS1 se utiliza para equilibrar la carga servidores S1 y S2, que están conectados a NS1 a través del conmutador L2 SW1. S1 y S2 pertenecen a diferentes subredes y forman parte de VLAN 10 y VLAN20, respectivamente. El vínculo entre NS1 y SW1 es un enlace troncal y lo comparten VLAN10 y VLAN20.

Para obtener más información sobre cómo configurar el equilibrio de carga en un Citrix ADC, consulte Equilibrio de carga.

Las direcciones IP de subred SNIP1 (solo para fines de referencia) y SNIP2 (solo para fines de referencia) se configuran en NS1. NS1 utiliza SNIP1 (en VLAN 10) para comunicarse con el servidor S1, y SNIP2 (en VLAN 20) para comunicarse con S2. Tan pronto como SNIP1 y SNIP2 se configuran, NS1 transmite paquetes de anuncio ARP para SNIP1 y SNIP2.

Para obtener más información sobre la configuración de VLAN en un Citrix ADC, consulte Configuración de una VLAN.

Los servicios SVC-S1 y SVC-S2 en NS1 representan los servidores S1 y S2. Tan pronto como se configuran estos servicios, NS1 transmite solicitudes ARP para ellos. Después de responder S1 y S2, NS1 les envía sondas de supervisión a intervalos regulares para comprobar su estado. NS1 envía sondeos de supervisión a S1 desde la dirección SNIP1 y a S2 desde la dirección SNIP2.



A continuación se presenta el flujo de tráfico en este ejemplo:

1. El cliente C1 envía un paquete de solicitud a LBVS-1. El paquete de solicitud tiene:
   - IP de origen = dirección IP del cliente (198.51.100.10)
   - IP de destino = dirección IP de LBVS-1 (203.0.113.15)
2. LBVS1 de NS1 recibe el paquete de solicitud.
3. El algoritmo de equilibrio de carga de LBVS1 selecciona el servidor S2.
4. Dado que S2 está conectado directamente a NS1 y SNIP2 (192.0.2.10) es la única dirección IP en NS1 que pertenece a la misma subred que S2, NS1 abre una conexión entre SNIP2 y S2.
   Nota: Si se selecciona S1, NS1 abre una conexión entre SNIP1 y S1.
5. NS1 envía el paquete de solicitud a S2 desde SNIP2. El paquete de solicitud tiene:
   - IP de origen = SNIP1 (192.0.2.10)
   - IP de destino = dirección IP de S2 (192.0.2.20)
6. La respuesta de S2 regresa por la misma ruta.

Configuración de direcciones IP del sitio GSLB (GSLBIP)

August 20, 2021

Una dirección IP de sitio GSLB (GSLBIP) es una dirección IP asociada a un sitio GSLB. No es obligatorio especificar una dirección GSLBIP al configurar inicialmente el dispositivo Citrix ADC. Una dirección GSLBIP solo se utiliza cuando se crea un sitio GSLB.

Para obtener más información sobre cómo crear una dirección IP de sitio GSLB, consulte Equilibrio de carga global del servidor.

Eliminación de una dirección IP propiedad de Citrix ADC

January 19, 2021

Puede eliminar cualquier dirección IP excepto el NSIP. La tabla siguiente proporciona información acerca de los procesos que debe seguir para eliminar los distintos tipos de direcciones IP. Antes de eliminar un VIP, quite el servidor virtual asociado.

Tipo de dirección IP	Implicaciones
Dirección IP de subred (SNIP)	Si la dirección IP que se quita es la última dirección IP de la subred, la ruta asociada se elimina de la tabla de rutas. Si la dirección IP que se quita es la Gateway de la entrada de ruta correspondiente, la Gateway de esa ruta de subred se cambia a otra dirección IP propiedad de Citrix ADC.
Dirección IP del servidor virtual (VIP)	Antes de eliminar un VIP, primero debe quitar el servidor virtual asociado a él. Para obtener información sobre cómo quitar el servidor virtual, consulte Equilibrio de carga.
Dirección IP del sitio-GSLB	Antes de eliminar una dirección IP del sitio GSLB, debe quitar el sitio asociado a él. Para obtener información sobre cómo quitar el sitio, consulte Equilibrio de carga global del servidor.

Para eliminar una dirección IP mediante la CLI:

En el símbolo del sistema, escriba:

<IPaddress>rm ns ip

Ejemplo:

```
1 > rm ns ip 10.102.29.54
2 Done
3 <!--NeedCopy-->
```

Para eliminar una dirección IP mediante la GUI:

Vaya a **Sistema** > **Red** > **Direcciones IP** > **Direcciones IPv4**, elimine la dirección IP.

Configuración de controles de acceso a aplicaciones

August 20, 2021

Los controles de acceso a aplicaciones, también conocidos como controles de acceso de administración, forman un mecanismo unificado para administrar la autenticación de usuarios y la implementación de reglas que determinan el acceso de los usuarios a las aplicaciones y los datos. Puede configurar SNIP para proporcionar acceso a las aplicaciones de administración. El acceso de administración para el NSIP está habilitado de forma predeterminada y no se puede inhabilitar. Sin embargo, puede controlarlo mediante ACL.

Para obtener información sobre el uso de ACL, consulte Listas de control de acceso (ACL).

El dispositivo Citrix ADC no admite el acceso de administración a los VIP.

La siguiente tabla proporciona un resumen de la interacción entre el acceso de administración y la configuración de servicio específica para Telnet.

Acceso a la administración	Telnet (estado configurado en Citrix ADC)	Telnet (Estado efectivo a nivel de IP)
Enable	Enable	Enable
Enable	Disable	Disable
Disable	Enable	Disable
Disable	Disable	Disable

En la tabla siguiente se proporciona una descripción general de las direcciones IP utilizadas como direcciones IP de origen en el tráfico saliente.

Aplicación/IP	NSIP	SNIP	VIP
ARP	Sí	Sí	No
Tráfico del lado del servidor	No	Sí	No
RNAT	No	Sí	Sí
PING DE ICMP	Sí	Sí	No
Redirección dinámica	Sí	Sí	Sí

La tabla siguiente proporciona una descripción general de las aplicaciones disponibles en estas direcciones IP.

Aplicación/IP	NSIP	SNIP	VIP
SNMP	Sí	Sí	Sí
Acceso al sistema	Sí	Sí	No

Puede acceder a Citrix ADC y administrarlo mediante aplicaciones como Telnet, SSH, GUI y FTP.

Nota: Telnet y FTP están inhabilitados en Citrix ADC por razones de seguridad. Para habilitarlos, póngase en contacto con el servicio de atención al cliente. Una vez habilitadas las aplicaciones, puede aplicar los controles en el nivel IP.

Para configurar Citrix ADC para que responda a estas aplicaciones, debe habilitar las aplicaciones de administración específicas. Si inhabilita el acceso de administración para una dirección IP, las conexiones existentes que utilizan la dirección IP no se terminan, pero no se pueden iniciar nuevas conexiones.

Además, las aplicaciones que no son de administración que se ejecutan en el sistema operativo FreeBSD subyacente están abiertas a ataques de protocolo, y estas aplicaciones no aprovechan las capacidades de prevención de ataques del dispositivo Citrix ADC.

Puede bloquear el acceso a estas aplicaciones que no son de administración en un SNIP o NSIP. Cuando se bloquea el acceso, un usuario que se conecta a un dispositivo Citrix ADC mediante el SNIP o NSIP no puede acceder a las aplicaciones que no son de administración que se ejecutan en el sistema operativo subyacente.

Para configurar el acceso de administración para una dirección IP mediante la CLI:

En el símbolo del sistema, escriba:

set ns ip <IPAddress> -mgmtAccess <value> -**telnet** <value> -**ftp** <value> -**gui** <value> -**ssh** <value> -**snmp** <value> -**restrictAccess** (**ENABLED** | **DISABLED**)

Ejemplo:

```
1  > set ns ip 10.102.29.54 -mgmtAccess enabled -restrictAccess ENABLED
2   Done
3 <!--NeedCopy-->
```

Para habilitar el acceso de administración para una dirección IP mediante la GUI:

1. Vaya a **Sistema** > **Red** > **Direcciones IP** > **Direcciones IPv4**.

2. Abra una entrada de dirección IP y seleccione la opción **Habilitar el control de acceso de administración** para admitir las aplicaciones enumeradas.

Habilitar el acceso seguro a la GUI de Citrix ADC mediante una dirección IP de subred (SNIP)

El acceso seguro a la GUI de Citrix ADC está habilitado de forma predeterminada para la IP de Citrix ADC (NSIP). También puede habilitar el acceso seguro al dispositivo Citrix ADC mediante una dirección IP de subred del dispositivo.

Después de configurar una dirección SNIP para obtener acceso seguro a un par de alta disponibilidad, el acceso seguro está disponible para el dispositivo principal, si accede a la dirección SNIP.

Procedimiento CLI de Citrix ADC

Para habilitar el acceso seguro a la GUI de Citrix ADC mediante una dirección IP de subred (SNIP) mediante la CLI:

En el símbolo del sistema, escriba:

set ns ip <SNIP_Address>**-type SNIP -gui SECUREONLY -MGMTAccess HABILITADO**

Ejemplo:

```
1  > set ns ip 203.0.113.99 -mgmtAccess enabled -restrictAccess ENABLED
2
3   Done
4 <!--NeedCopy-->
```

Cómo se conectan los proxies Citrix ADC

August 20, 2021

Cuando un cliente inicia una conexión, el dispositivo Citrix ADC termina la conexión del cliente, inicia una conexión con un servidor apropiado y envía el paquete al servidor. El dispositivo no realiza esta acción para el tipo de servicio UDP o CUALQUIERA.

Para obtener más información sobre los tipos de servicio, consulte Equilibrio de carga.

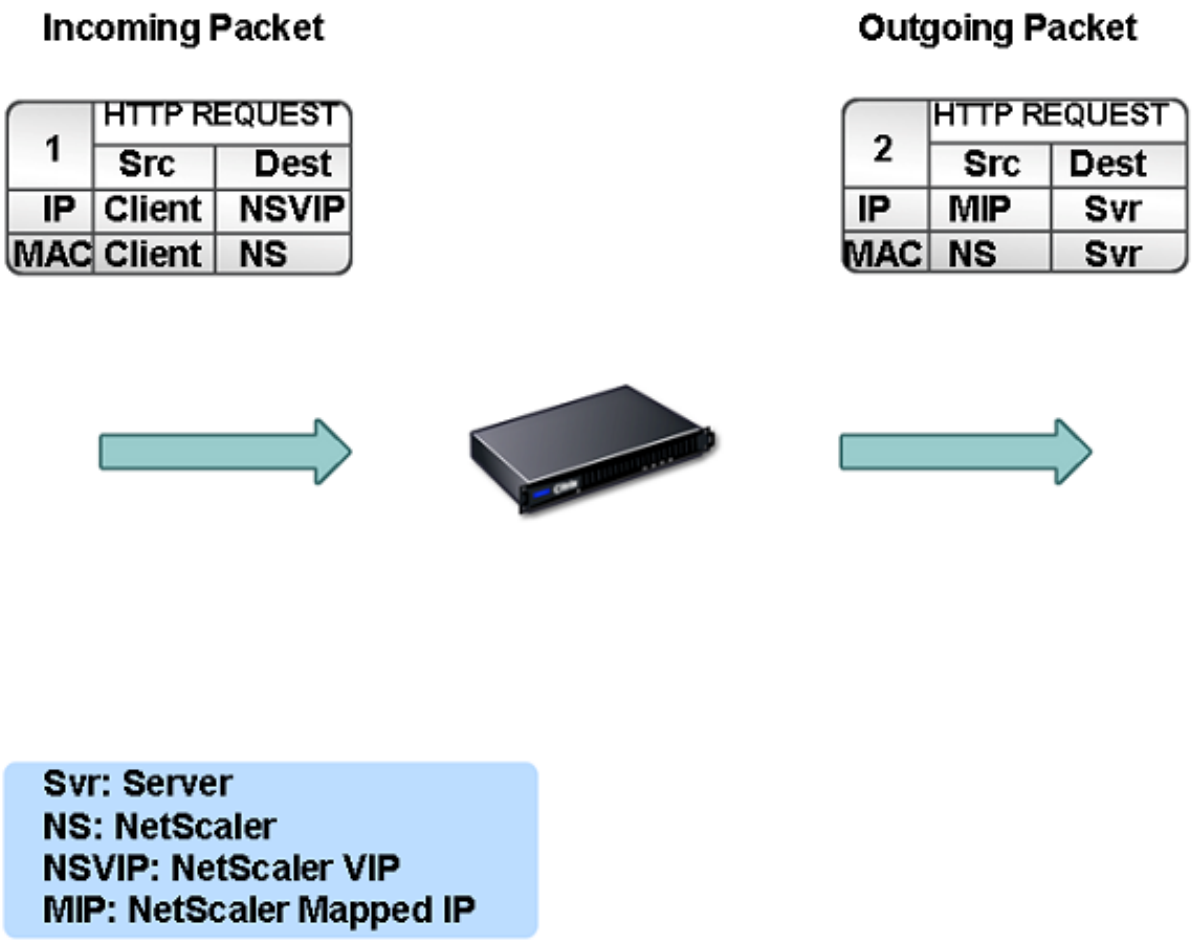
Puede configurar Citrix ADC para que procese el paquete antes de iniciar la conexión con un servidor. El comportamiento predeterminado es cambiar las direcciones IP de origen y destino de un paquete

antes de enviar el paquete al servidor. Puede configurar Citrix ADC para conservar la dirección IP de origen de los paquetes habilitando el modo Usar IP de origen.

Cómo se selecciona la dirección IP de destino

El tráfico enviado al dispositivo Citrix ADC se puede enviar a un servidor virtual o a un servicio. El dispositivo administra el tráfico a servidores y servicios virtuales de manera diferente. Citrix ADC termina el tráfico recibido en una dirección IP (VIP) del servidor virtual y cambia la dirección IP de destino a la dirección IP del servidor antes de reenviar el tráfico al servidor, como se muestra en el siguiente diagrama.

Ilustración 1. Proxying de conexiones a VIPs



Los paquetes destinados a un servicio se envían directamente al servidor apropiado y Citrix ADC no modifica las direcciones IP de destino. En este caso, Citrix ADC funciona como proxy.

Cómo se selecciona la dirección IP de origen

Cuando el dispositivo Citrix ADC se comunica con los servidores físicos o dispositivos del mismo nivel, de forma predeterminada, no utiliza la dirección IP del cliente. Citrix ADC mantiene un grupo de direcciones IP de subred (SNIP) y selecciona una dirección IP de este grupo para utilizarla como dirección IP de origen de una conexión con el servidor físico. Dependiendo de la subred en la que se coloque el servidor físico, Citrix ADC selecciona una dirección SNIP específica.

Nota: Si está activada la opción Usar IP de origen (USIP), el dispositivo utiliza la dirección IP del cliente.

Habilitar el modo IP de uso de origen

August 20, 2021

Cuando el dispositivo Citrix ADC se comunica con los servidores físicos o dispositivos del mismo nivel, de forma predeterminada, utiliza una de sus propias direcciones IP como IP de origen. El dispositivo mantiene un grupo de direcciones IP de subred (SNIP) y selecciona una dirección IP de este grupo para utilizarla como dirección IP de origen para una conexión con el servidor físico. La decisión de seleccionar una dirección SNIP depende de la subred en la que reside el servidor físico.

Si es necesario, puede configurar el dispositivo Citrix ADC para que utilice la dirección IP del cliente como IP de origen. Algunas aplicaciones necesitan la dirección IP real del cliente. Los siguientes casos de uso son algunos ejemplos:

- La dirección IP del cliente en el registro de acceso web se utiliza para fines de facturación o análisis de uso.
- La dirección IP del cliente se utiliza para determinar el país de origen del cliente o el ISP de origen del cliente. Por ejemplo, muchos motores de búsqueda como Google proporcionan contenido relevante para la ubicación a la que pertenece el usuario.
- La aplicación debe conocer la dirección IP del cliente para verificar que la solicitud proviene de una fuente confiable.
- A veces, aunque un servidor de aplicaciones no necesite la dirección IP del cliente, un firewall situado entre el servidor de aplicaciones y el Citrix ADC puede necesitar la dirección IP del cliente para filtrar el tráfico.

Habilite el modo Usar modo IP de origen (USIP) si quiere que Citrix ADC utilice la dirección IP del cliente para comunicarse con los servidores.

En la siguiente ilustración se muestra cómo el dispositivo utiliza las direcciones IP en modo USIP.

Antes de comenzar

Antes de habilitar el modo USIP, tenga en cuenta los siguientes puntos:

- Habilite USIP en las siguientes situaciones:
  - Equilibrio de carga de servidores del sistema de detección de intrusiones (IDS)
  - Equilibrio de carga SMTP
  - Failover de conexión sin estado
  - Equilibrio de carga sin sesión
  - Si utiliza el modo de devolución directa del servidor (DSR)
- La configuración global de USIP se aplica solo a los servicios que se crean después de realizar la configuración global de USIP. En otras palabras, la configuración global de USIP no se aplica a los servicios existentes cuando se realiza la configuración global de USIP. Por ejemplo, Inhabilitar USIP globalmente no inhabilita USIP en los servicios existentes. Pero impide que los servicios creados posteriormente tengan USIP habilitado automáticamente.

  Para habilitar o inhabilitar USIP en un conjunto de servicios existentes, debe habilitar o inhabilitar USIP en cada uno de estos servicios.
- Cuando USIP está habilitado, debe establecer la Gateway del servidor en una de las direcciones IP propiedad de Citrix ADC (de tipo IP de subred (SNIP) para que la respuesta del servidor siempre pase por el dispositivo Citrix ADC.
- Si habilita USIP, establezca el tiempo de espera inactivo para las conexiones del servidor en un valor inferior al valor predeterminado, de modo que las conexiones inactivas se borren rápidamente en el lado del servidor.
- Para la redirección de caché transparente, si habilita USIP, habilite también L2CONN.
- Debido a que las conexiones HTTP no se reutilizan cuando USIP está habilitado, puede acumularse un gran número de conexiones del lado del servidor. Las conexiones de servidor inactivas

pueden bloquear las conexiones de otros clientes. Por lo tanto, establezca límites en el número máximo de conexiones a un servicio. Citrix también recomienda establecer el valor de tiempo de espera del servidor HTTP, para un servicio en el que USIP está habilitado, en un valor inferior al predeterminado, de modo que las conexiones inactivas se borren rápidamente en el servidor.

- Como alternativa al modo USIP, tiene la opción de insertar la dirección IP del cliente (CIP) en el encabezado de solicitud de la conexión del lado del servidor para un servidor de aplicaciones que necesite la dirección IP del cliente.
- En versiones anteriores de Citrix ADC, el modo USIP tenía las siguientes opciones de puerto de origen para las conexiones del lado del servidor:
  - **Use el puerto del cliente**. Con esta opción, las conexiones no se pueden reutilizar. Para cada solicitud del cliente, se realiza una nueva conexión con el servidor físico.
  - **Utilice el puerto proxy**. Con esta opción, la reutilización de la conexión es posible para todas las solicitudes del mismo cliente.

  En las versiones posteriores de Citrix ADC, si USIP está habilitado, el valor predeterminado es utilizar un puerto proxy para las conexiones del lado del servidor y no reutilizar las conexiones. La no reutilización de conexiones puede no afectar a la velocidad de establecimiento de conexiones.

  De forma predeterminada, la opción Usar puerto proxy está habilitada si el modo USIP está habilitado.

  Nota: Si habilita el modo USIP, se recomienda activar la opción Usar puerto proxy.

  Para obtener más información sobre la opción Usar puerto proxy, consulte Configurar el puerto de origen para las conexiones del lado del servidor.

Pasos de configuración

Habilite el modo Usar modo IP de origen (USIP) si quiere que Citrix ADC utilice la dirección IP del cliente para comunicarse con los servidores. De forma predeterminada, el modo USIP está inhabilitado. El modo USIP se puede habilitar globalmente en Citrix ADC o en un servicio específico. Si lo habilita globalmente, USIP está habilitado de forma predeterminada para todos los servicios creados posteriormente. Si habilita USIP para un servicio específico, la dirección IP del cliente se utiliza únicamente para el tráfico dirigido a ese servicio.

Procedimientos CLI

Para habilitar o inhabilitar globalmente el modo USIP mediante la CLI:

En el símbolo del sistema, escriba uno de los siguientes comandos:

- **enable ns mode USIP**

- **disable ns mode USIP**

Para habilitar el modo USIP para un servicio mediante la CLI:

En el símbolo del sistema, escriba:

set service <name>@ -**usip** (**YES** | **NO**)

Ejemplo:

```
1 > set service Service-HTTP-1 -usip YES
2 Done
3 <!--NeedCopy-->
```

Procedimientos de GUI

Para habilitar o inhabilitar globalmente el modo USIP mediante la GUI:

1. Desplácese hasta **Sistema** > **Configuración**, en el grupo **Modos y funciones**, haga clic en **Cambiar modos**.
2. Seleccione o desactive la opción **Usar IP de origen**.

Para habilitar el modo USIP para un servicio mediante la GUI:

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servicios** y modifique un servicio.
2. En **Configuración avanzada**, seleccione **Configuración de servicio** y seleccione **Usar dirección IP de origen**.

Configuración de la traducción de direcciones de red

January 12, 2021

La traducción de direcciones de red (NAT) implica la modificación de las direcciones IP de origen y/o destino y/o de los números de puerto TCP/UDP de los paquetes IP que pasan a través del dispositivo Citrix ADC. Habilitar NAT en el dispositivo mejora la seguridad de la red privada y la protege de una red pública como Internet, modificando las direcciones IP de origen de las redes cuando los datos pasan a través del Citrix ADC. Además, con la ayuda de entradas NAT, toda su red privada puede ser representada por algunas direcciones IP públicas compartidas. Citrix ADC admite los siguientes tipos de traducción de direcciones de red:

- **NAT (INAT) entrante.** Citrix ADC reemplaza la dirección IP de destino en los paquetes generados por el cliente con la dirección IP privada del servidor.

- **NAT inversa (RNAT).** Citrix ADC reemplaza la dirección IP de origen en los paquetes generados por los servidores con las direcciones IP NAT públicas.

Traducción de direcciones de red entrantes

August 20, 2021

Cuando un cliente envía un paquete a un dispositivo Citrix ADC configurado para la traducción de direcciones de red entrante (INAT), el dispositivo traduce la dirección IP de destino pública del paquete a una dirección IP de destino privada y reenvía el paquete al servidor en esa dirección.

Se admiten las siguientes configuraciones:

- **Asignación IPv4-IPv4**: Una dirección IPv4 pública en el dispositivo Citrix ADC escucha las solicitudes de conexión en nombre de un servidor IPv4 privado. El dispositivo Citrix ADC traduce la dirección IP de destino público del paquete a la dirección IP de destino del servidor. A continuación, el dispositivo reenvía el paquete al servidor en esa dirección.
- **Asignación IPv4-IPv6**: Una dirección IPv4 pública en el dispositivo Citrix ADC escucha las solicitudes de conexión en nombre de un servidor IPv6 privado. El dispositivo Citrix ADC crea un paquete de solicitud IPv6 con la dirección IP del servidor IPv6 como dirección IP de destino.
- **Asignación IPv6-IPv4**: Una dirección IPv6 pública en el dispositivo Citrix ADC escucha las solicitudes de conexión en nombre de un servidor IPv4 privado. El dispositivo Citrix ADC crea un paquete de solicitud IPv4 con la dirección IP del servidor IPv4 como dirección IP de destino.
- **Asignación IPv6-IPv6**: Una dirección IPv6 pública del dispositivo Citrix ADC escucha las solicitudes de conexión en nombre de un servidor IPv6 privado. El dispositivo Citrix ADC traduce la dirección IP de destino público del paquete a la dirección IP de destino del servidor. A continuación, el dispositivo reenvía el paquete al servidor en esa dirección.

Cuando el dispositivo reenvía un paquete a un servidor, la dirección IP de origen asignada al paquete se determina de la siguiente manera:

- Si se habilita el modo IP de subred (USNIP) y se inhabilita el modo IP de origen (USIP), el dispositivo utiliza una dirección IP de subred (SNIP) como dirección IP de origen.
- Si el modo USIP está habilitado y el modo USNIP está inhabilitado, el dispositivo utiliza la dirección IP del cliente (CIP) como dirección IP de origen.
- Si ambos modos USIP y USNIP están habilitados, el modo USIP tiene prioridad.
- También puede configurar Citrix ADC para que utilice una dirección IP única como dirección IP de origen, estableciendo el parámetro ProxyIP.
- Si ninguno de los modos anteriores está habilitado y no se ha especificado una dirección IP única, Citrix ADC intenta utilizar un MIP como dirección IP de origen.

- Si ambos modos USIP y USNIP están habilitados y se ha especificado una dirección IP única, el orden de prioridad es el siguiente: USIP-Unique IP-USNIP-MIP-Error.

Para proteger Citrix ADC de ataques DoS, puede habilitar el proxy TCP. Sin embargo, si se utilizan otros mecanismos de protección en la red, puede inhabilitarlos.

Configurar reglas INAT

Puede crear, modificar o eliminar una entrada INAT.

Procedimientos CLI

Para crear una entrada INAT mediante la CLI:

En el símbolo del sistema, escriba los siguientes comandos para crear una entrada INAT y verificar su configuración:

- **add inat** <name><publicIP><privateIP>[-**tcpproxy** (**HABILITADO** | **DESHABILITADO**)] [-**ftp** (**HABILITADO** | **DESHABILITADO**)] [-**usip** (****ACTIVADO** | DESACTIVADO**)] [-**usnip** (****ACTIVADO** | DESACTIVADO**)] [-**ProxyIP** ** \ < ip_addr **ipv6_addr>**]
- **mostrar inat** []<name>

Ejemplo:

```
> add inat ip4-ip4 172.16.1.2 192.168.1.1 -proxyip 10.102.29.171
 Done
<!--NeedCopy-->
```

Para modificar una entrada INAT mediante la CLI:

Para modificar una entrada INAT, escriba el `set inat` comando, el nombre de la entrada y los parámetros que se van a cambiar, con sus nuevos valores.

Para eliminar una configuración de INAT mediante la CLI:

En el símbolo del sistema, escriba:

- **rm inat** <name>

Ejemplo:

```
> rm inat ip4-ip4
 Done
<!--NeedCopy-->
```


Procedimientos de GUI

Para configurar una entrada INAT mediante la GUI:

Vaya a **Sistema** > **Red** > **Rutas** > **INAT** y agregue una entrada INAT o modifique una entrada INAT existente.

Para eliminar una configuración INAT mediante la GUI:

Vaya a **Sistema** > **Red** > **Rutas** > **INAT**, elimine la configuración INAT.

Conmutación por error de conexión para reglas INAT

La conmutación por error de conexión o el reflejo de conexiones permite al nodo principal duplicar la información de conexión y persistencia en el nodo secundario en una alta disponibilidad. La información de estado de la conexión se comparte con el nodo secundario regularmente cuando se habilita la creación de reflejo de conexión.

Habilitar la conmutación por error de conexión proporciona más fiabilidad, pero se produce a costa de un tiempo del sistema que se utiliza para compartir la información de estado. Los datos de conexión se sincronizan con la unidad en espera con cada actualización de estado de flujo o paquete. Por lo tanto, debe usarse solo en lugares donde la fiabilidad del nivel de conexión es de suma importancia.

Las configuraciones de alta disponibilidad del dispositivo Citrix ADC admiten la conmutación por error de conexión para conexiones INAT. El nodo principal envía asignaciones INAT y otra información de conexión relacionada con INAT al nodo secundario a intervalos regulares. El dispositivo secundario utiliza la información de asignación y conexión solo en caso de conmutación por error.

Cuando se produce una conmutación por error, el nuevo nodo principal tiene información sobre las conexiones INAT establecidas antes de la conmutación por error. Por lo tanto, continúa sirviendo esas conexiones incluso después de la conmutación por error.

Desde la perspectiva del cliente, la conmutación por error es transparente. Durante el período de transición, el cliente y el servidor pueden experimentar una breve interrupción y retransmisiones. La conmutación por error de conexión se puede habilitar por regla INAT.

Para habilitar la conmutación por error de conexión en una regla INAT, habilite el `connFailover` parámetro de esa regla RNAT específica mediante CLI.

Procedimiento de CLI

Para habilitar la conmutación por error de conexión para una regla INAT mediante la CLI:

Para habilitar la conmutación por error de conexión al agregar una regla INAT, escriba en el símbolo del sistema:

- **add inat** <name><publicIP><privateIP>[-**tcpproxy** (**HABILITADO** | **DESHABILITADO**)] [-**ftp** (**HABILITADO** | **DESHABILITADO**)] [-**usip** (****ACTIVADO** | DESACTIVADO**)] [-**usnip** (****ACTIVADO** | DESACTIVADO**)] [-**ProxyIP** \ <ip_addr|ipv6_addr] -**connfailover** (**HABILITADO** | **DISCAPACITADO**)
- **mostrar inat** <name>

Para habilitar la conmutación por error de conexión al modificar una regla INAT existente, escriba en el símbolo del sistema:

- **set inat -connfailover** (**ENABLED** | **DISABLED**)
- **mostrar inat** <name>

Convivencia de INAT y Servidores Virtuales

January 12, 2021

Si se configuran tanto INAT como RNAT, la regla INAT tiene prioridad sobre la regla RNAT. Si RNAT está configurado con una dirección IP de traducción de direcciones de red (NAT IP), la dirección IP de NAT se selecciona como dirección IP de origen para ese cliente RNAT.

La IP de destino público predeterminada en una configuración INAT es la dirección IP virtual (VIP) del dispositivo Citrix ADC. Los servidores virtuales también usan VIP. Cuando INAT y un servidor virtual utilizan la misma dirección IP, la configuración del servidor virtual anula la configuración del INAT.

A continuación se presentan algunos ejemplos de casos de configuración de configuración y sus efectos.

Caso	Resultado
Ha configurado un servidor virtual y un servicio para enviar directamente al servidor todos los paquetes de datos recibidos en un puerto Citrix ADC específico. También ha configurado INAT y habilitado TCP. La configuración de INAT de esta manera envía todos los paquetes de datos recibidos a través de un motor TCP antes de enviarlos al servidor.	Todos los paquetes recibidos en Citrix ADC, excepto los recibidos en el puerto especificado, pasan a través del motor TCP.

Caso	Resultado
Ha configurado un servidor virtual y un servicio para enviar todos los paquetes de datos del tipo de servicio TCP, que se reciben en un puerto específico del Citrix ADC, al servidor después de pasar por el motor TCP. También ha configurado INAT e inhabilitado TCP. La configuración de INAT de esta manera envía los paquetes de datos recibidos directamente al servidor.	Solo los paquetes recibidos en el puerto especificado pasan a través del motor TCP.
Ha configurado un servidor virtual y un servicio para enviar todos los paquetes de datos recibidos a cualquiera de los dos servidores. Está intentando configurar INAT para enviar todos los paquetes de datos recibidos a un servidor diferente.	La configuración INAT no está permitida.
Ha configurado INAT para enviar todos los paquetes de datos recibidos directamente a un servidor. Está intentando configurar un servidor virtual y un servicio para enviar todos los paquetes de datos recibidos a dos servidores diferentes.	La configuración del servidor virtual no está permitida.

NAT46 sin estado

August 20, 2021

La función NAT46 sin estado permite la comunicación entre redes IPv4 e IPv6 a través de la traducción de paquetes IPv4 a IPv6, y viceversa, sin mantener ninguna información de sesión en el dispositivo Citrix ADC.

Para una configuración NAT46 sin estado, el dispositivo traduce un paquete IPv4 a IPv6 o un paquete IPv6 a IPv4, tal como se define en RFC 6145 y 2765.

Una configuración NAT46 sin estado en el dispositivo Citrix ADC tiene los siguientes componentes:

- **Entrada INAT IPv4-IPv6.** Entrada INAT que define una relación 1:1 entre una dirección IPv4 y una dirección IPv6. En otras palabras, una dirección IPv4 del dispositivo escucha las solicitudes

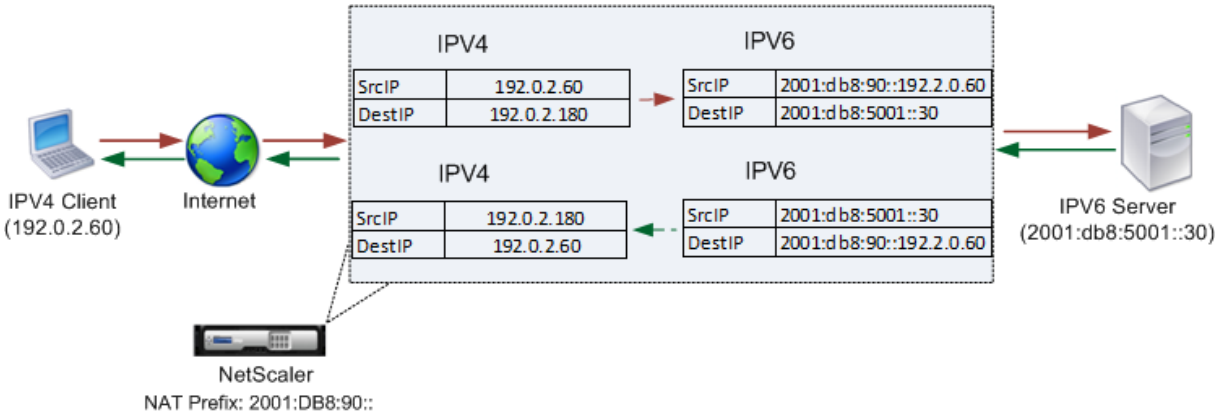
de conexión en nombre de un servidor IPv6. Un paquete de solicitud IPv4 para esta dirección IPv4 se traduce en un paquete IPv6 y, a continuación, el paquete IPv6 se envía al servidor IPv6.

El dispositivo traduce un paquete de respuesta IPv6 en un paquete de respuesta IPv4 con su campo de dirección IP de origen establecido como la dirección IPv4 especificada en la entrada INAT. El paquete traducido se envía al cliente.

- **Prefijo IPv6 NAT46.** Prefijo IPv6 global de 96 bits de longitud (128-32=96) configurado en el dispositivo. Durante la traducción de paquetes IPv4 a paquetes IPv6, el dispositivo establece la dirección IP de origen del paquete IPv6 traducido en una concatenación del prefijo IPv6 NAT46 de [96 bits] y la dirección de origen IPv4 de [32 bits] recibida en el paquete de solicitud.

  Durante la traducción de paquetes IPv6 a paquetes IPv4, el dispositivo establece la dirección IP de destino del paquete IPv4 traducido en los últimos 32 bits de la dirección IP de destino del paquete IPv6.

Considere un ejemplo en el que una empresa aloja el sitio www.example.com en el servidor S1, que tiene una dirección IPv6. Para habilitar la comunicación entre los clientes IPv4 y el servidor IPv6 S1, el dispositivo Citrix ADC NS1 se implementa con una configuración NAT46 sin estado que incluye una entrada INAT IPv4-IPv6 para el servidor S1 y un prefijo NAT46. La entrada INAT incluye una dirección IPv4 en la que el dispositivo escucha las solicitudes de conexión de los clientes IPv4 en nombre del servidor IPv6 S1.



En la tabla siguiente se enumeran los parámetros utilizados en este ejemplo:

Entidades	Nombre	Valor
Dirección IP del cliente	Client_IPv4 (solo para fines de referencia)	192.0.2.60
Dirección IPv6 del servidor	SEVR_IPv6 (solo para fines de referencia)	2001:DB8:5001::30

Entidades	Nombre	Valor
Dirección IPv4 definida en la entrada INAT para el servidor IPv6 S1	Map-Sevr-IPv4 (solo para fines de referencia)	192.0.2.180
Prefijo IPv6 para traducción NAT 46	NAT46_Prefijo (solo para fines de referencia)	2001:DB8:90::

A continuación se presenta el flujo de tráfico en este ejemplo:

1. El cliente IPv4 CL1 envía un paquete de solicitud a la dirección Map-Sevr-IPv4 (192.0.2.180) en el dispositivo Citrix ADC.
2. El dispositivo recibe el paquete de solicitud y busca en las entradas INAT NAT46 la dirección IPv6 asignada a la dirección Map-Sevr-IPv4 (192.0.2.180). Encuentre la dirección SEVR-IPv6 (2001:DB 8:5001: :30).
3. El dispositivo crea un paquete de solicitud IPv6 traducido con:
   - Campo de dirección IP de destino = SEVR-IPv6 = 2001:DB 8:5001: :30
   - Campo de dirección IP de origen = Concatenación de prefijo NAT (primeros 96 bits) y client_IPv4 (últimos 32 bits) = 2001:DB 8:90: :192.0.2.60
4. El dispositivo envía la solicitud IPv6 traducida a SEVR-IPv6.
5. El servidor IPv6 S1 responde enviando un paquete IPv6 al dispositivo Citrix ADC con:
   - Campo de dirección IP de destino = Concatenación de prefijo NAT (primeros 96 bits) y client_IPv4 (últimos 32 bits) = 2001:DB 8:90: :192.0.2.60
   - Campo de dirección IP de origen = SEVR-IPv6 = 2001:DB 8:5001: :30
6. El dispositivo recibe el paquete de respuesta IPv6 y comprueba que su dirección IP de destino coincide con el prefijo NAT46 configurado en el dispositivo. Dado que la dirección de destino coincide con el prefijo NAT46, el dispositivo busca en las entradas INAT NAT46 la dirección IPv4 asociada a la dirección SEVR-IPv6 (2001:DB 8:5001: :30). Busca la dirección Map-Sevr-IPv4 (192.0.2.180).
7. El dispositivo crea un paquete de respuesta IPv4 con:
   - Campo de dirección IP de destino = El prefijo NAT46 eliminado de la dirección de destino de la respuesta IPv6 = Client_IPv4 (192.0.2.60)
   - Campo de dirección IP de origen = Dirección Map-Sevr-IPv4 (192.0.2.180)
8. El dispositivo envía la respuesta IPv4 traducida al cliente CL1.

Limitaciones de los apátridas NAT46

Las siguientes limitaciones se aplican a NAT46 apátridas:

- No se admite la traducción de opciones IPv4.

- No se admite la traducción de encabezados de redirección IPv6.
- No se admite la traducción de encabezados de extensión de salto por salto de paquetes IPv6.
- No se admite la traducción de encabezados ESP y EH de paquetes IPv4.
- No se admite la traducción de paquetes de multidifusión.
- No se admite la traducción de encabezados de opciones de destino y encabezados de redirección de origen.
- No se admite la traducción de paquetes UDP IPv4 fragmentados que no contienen suma de comprobación UDP.

Configurar NAT46 sin estado

La creación de las entidades necesarias para la configuración NAT46 sin estado en el dispositivo Citrix ADC implica los siguientes procedimientos:

1. Cree una entrada INAT de asignación IPv4-IPv6 con el modo sin estado habilitado.
2. Cree un prefijo IPv6 NAT46.

Procedimientos CLI

Para configurar una entrada de asignación INAT mediante la CLI:

En el símbolo del sistema, escriba:

- add inat <name> <publicIPv4> <privateIPv6> -mode STATELESS
- mostrar inat <name>

Para crear un prefijo NAT46 mediante la CLI:

En el símbolo del sistema, escriba:

- set inatparam -NAT46v6prefix <ipv6_addr|*>
- show inatparam

Ejemplo:

```
 > add inat exmpl-com-stls-nat46 192.0.2.180
2001:DB8:5001::30 -mode stateless
Done

> set inatparam -nat46v6Prefix 2001:DB8:90::/96
Done
<!--NeedCopy-->
```


Procedimientos de GUI

Para crear una entrada de asignación INAT mediante la GUI:

1. Vaya a Sistema > Red > Rutas > INAT.
2. Agregue una nueva entrada INAT o modifique una entrada INAT existente.
3. Defina los siguientes parámetros:
   - Nombre*
   - Dirección IP pública*
   - Dirección IP privada* (Active la casilla de verificación IPv6 e introduzca la dirección en formato IPv6).
   - Modo (seleccione Sin estado en la lista desplegable).

   *Un parámetro requerido

Para crear un prefijo NAT46 mediante la GUI:

Vaya a **Sistema** > **Red**, en el grupo **Configuración**, haga clic en **Configurar parámetros INAT**y defina el parámetro **Prefijo**.

Configuración de parámetros globales para NAT46 sin estado

El dispositivo proporciona algunos parámetros globales opcionales para configuraciones NAT46 sin estado.

Para establecer parámetros globales para NAT46 sin estado mediante la CLI:

En el símbolo del sistema, escriba:

set inatparam [-**NAT46IGNORETOS** (**SÍ**	**NO**)] [-**NAT46ZeroChecksum** (**HABILITADO**	**DESHABILITADO**)] [-**NAT46V6MTU**] \ <positive_integer>[-**NAT46FragHeader** (**HABILITADO**	**DESHABILITADO**)]

-
- **show inatparam**

Ejemplo:

```
1 > set inatparam -nat46IgnoreTOS YES -nat46ZeroCheckSum DISABLED -
     nat46v6Mtu 1400 -nat46FragHeader DISABLED
```



```
2   Done
3 <!--NeedCopy-->
```

Para establecer parámetros globales para NAT46 sin estado mediante la GUI:

Vaya a **Sistema** > **Red**, en el grupo **Configuración**, haga clic en **Configurar parámetros INAT**.

DNS64

August 20, 2021

La función Citrix ADC DNS64 responde con un registro AAAA DNS sintetizado a un cliente IPv6 que envía una solicitud AAAA para un dominio solo IPv4. La función DNS64 se utiliza con la función NAT64 para permitir una comunicación perfecta entre los clientes solo IPv6 y los servidores solo IPv4. DNS64 permite la detección del dominio IPv4por parte de los clientes solo IPv6, y NAT64 permite la comunicación entre los clientes y los servidores.

Para sintetizar un registro AAAA, el dispositivo Citrix ADC obtiene un registro DNS A de un servidor DNS. El prefijo DNS64 es un prefijo IPv6 de 96 bits configurado en el dispositivo Citrix ADC. El dispositivo Citrix ADC sintetiza el registro AAAA mediante la concatenación del prefijo DNS64 (96 bits) y la dirección IPv4 (32 bits).

Para habilitar la comunicación entre clientes IPv6 y servidores IPv4, un dispositivo Citrix ADC con configuración DNS64 y NAT64 se puede implementar en el lado del cliente IPv6 o en el lado del servidor IPv4. En ambos casos, la configuración DNS64 del dispositivo Citrix ADC es similar e incluye un servidor virtual de equilibrio de carga que actúa como servidor proxy para servidores DNS. Si el dispositivo Citrix ADC se implementa en el lado del cliente, el servidor virtual de equilibrio de carga debe especificarse, en el cliente IPv6, como servidor de nombres de un dominio.

Considere un ejemplo en el que un dispositivo Citrix ADC con configuración DNS64 y NAT64 está configurado en el lado IPv4. En este ejemplo, una empresa aloja el sitio www.example.com en el servidor S1, que tiene una dirección IPv4. Para habilitar la comunicación entre los clientes IPv6 y el servidor IPv4 S1, el dispositivo Citrix ADC NS1 se implementa con una configuración DNS64 y NAT64 con estado.

La configuración DNS64 incluye el servidor virtual de equilibrio de carga DNS LBVS-DNS64-1, en el que está habilitada la opción DNS64. Una directiva DNS64 denominada DNS64-Policy-1 y una acción DNS64 asociada denominada DNS64-Acción1, también se configuran en NS1, y DNS64-Policy-1 está enlazada a LBVS-DNS64-1. LBVS-DNS64-1 actúa como servidor proxy DNS para los servidores DNS DNS-1 y DNS-2.

Cuando el tráfico que llega a LBVS-DNS64-1 coincide con las condiciones especificadas en DNS64-Policy1, el tráfico se procesa de acuerdo con la configuración de DNS64-Acción1. DNS64-acción1 es-

pecifica el prefijo DNS64 utilizado, con el registro A recibido de un servidor DNS, para sintetizar un registro AAAA.

El parámetro DNS global cacherecords está habilitado en el dispositivo Citrix ADC, por lo que el dispositivo almacena en caché los registros DNS. Esta configuración es necesaria para que el DNS64 funcione correctamente.

En la tabla siguiente se enumeran los ajustes utilizados en el ejemplo anterior: configuración de ejemplo de DNS64.

A continuación se presenta el flujo de tráfico en este ejemplo:

1. El cliente IPv6 CL1 envía una solicitud AAAA DNS para la dirección IPv6 del sitio www.example.com.
2. La solicitud la recibe el servidor virtual de equilibrio de carga DNS LBVS-DNS64-1 en el dispositivo Citrix ADC NS1.
3. NS1 comprueba sus registros de caché DNS para el registro AAAA solicitado y encuentra que el registro AAAA para el sitio www.example.com no existe en la caché DNS.
4. El algoritmo de equilibrio de carga de LBVS-DNS64-1 selecciona el servidor DNS DNS-1 y reenvía la solicitud AAAA a él.
5. Dado que el sitio www.example.com está alojado en un servidor IPv4, el servidor DNS DNS-1 no tiene ningún registro AAAA para el sitio www.example.com.
6. DNS-1 envía una respuesta DNS AAAA vacía o un mensaje de error a LBVS-DNS64-1.
7. Dado que la opción DNS64 está habilitada en LBVS-DNS64-1 y la solicitud AAAA de CL1 coincide con la condición especificada en DNS64-policy-1, NS1 envía una solicitud DNS A a DNS-1 para la dirección IPv4 de www.example.com.
8. DNS-1 responde enviando el registro DNS A de www.example.com a LBVS-DNS64-1. El registro A incluye la dirección IPv4 de www.example.com.
9. NS1 sintetiza un registro AAAA para el sitio www.example.com con:
    - Dirección IPv6 para el sitio www.example.com = Concatenación del prefijo DNS64 (96 bits) especificado en la acción DNS64asociada y dirección IPv4 del registro DNS A (32 bits) = 2001:DB 8:300: :192.0.2.60
10. NS1 envía el registro AAAA sintetizado al cliente IPv6 CL1. NS1 también almacena en caché el registro A en su memoria. NS1 utiliza el registro A almacenado en caché para sintetizar registros AAAA para solicitudes AAAA posteriores.

Puntos a considerar para una configuración DNS64

Antes de configurar DNS64 en un dispositivo Citrix ADC, tenga en cuenta los siguientes puntos:

- La función DNS64 del dispositivo Citrix ADC es compatible con RFC 6174.
- La función DNS64 del dispositivo Citrix ADC no admite DNSSEC. El dispositivo Citrix ADC no sintetiza un registro AAAA a partir de una respuesta DNSSEC recibida de un servidor DNS. Una respuesta se clasifica como una respuesta DNSSEC, solo si contiene registros RRSIG.

- El dispositivo Citrix ADC admite el prefijo DNS64 de longitud de solo 96 bits.
- Aunque la función DNS64 se utiliza con la función NAT64, las configuraciones DNS64 y NAT64 son independientes en el dispositivo Citrix ADC. Para un flujo determinado, debe especificar el mismo valor de prefijo IPv6 para el prefijo DNS64 y los parámetros de prefijo NAT64, de modo que las direcciones IPv6 sintetizadas recibidas por el cliente se enrutan a la configuración NAT64 concreta. Para obtener más información sobre la configuración de NAT64 en un dispositivo Citrix ADC, consulte NAT64 con estado.
- A continuación se presentan los diferentes casos de procesamiento de DN64 por parte del dispositivo Citrix ADC:
  - Si la respuesta AAAA del servidor DNS incluye registros AAAA, cada registro de la respuesta se comprueba para el conjunto de reglas de exclusión configurado en el dispositivo Citrix ADC para la configuración concreta de DNS64. Citrix ADC quita de la respuesta las direcciones IPv6, cuyo prefijo coincide con la regla de exclusión. Si la respuesta resultante incluye al menos un registro IPv6, el dispositivo Citrix ADC reenvía esta respuesta al cliente; de lo contrario, el dispositivo sintetiza una respuesta AAAA del registro A del dominio y la envía al cliente IPv6.
  - Si la respuesta AAAA del servidor DNS es una respuesta vacía, el dispositivo solicita registros de recursos A con el mismo nombre de dominio o busca en sus propios registros si el dispositivo es un servidor de nombres de dominio auténtico para el dominio. Si la solicitud da como resultado una respuesta vacía o un error, el mismo se reenvía al cliente.
  - Si la respuesta del servidor DNS incluye RCODE=1 (error de formato), el dispositivo Citrix ADC reenvía el mismo al cliente. Si no hay respuesta antes del tiempo de espera, el dispositivo Citrix ADC envía una respuesta con RCODE=2 (error del servidor) al cliente.
  - Si la respuesta del servidor DNS incluye un CNAME, se sigue la cadena hasta que se alcanza el registro A o AAAA de terminación. Si CNAME no tiene ningún registro de recursos AAAA, el dispositivo Citrix ADC obtiene el registro DNS A que se utilizará para sintetizar el registro AAAA. La cadena CNAME se agrega a la sección de respuesta junto con el registro AAAA sintetizado y luego se envía al cliente.
- La función DNS64 del dispositivo Citrix ADC también admite responder a solicitudes PTR. Cuando se recibe una solicitud PTR para un dominio de una dirección IPv6 en el dispositivo y la dirección IPv6 coincide con cualquiera de los prefijos DNS64 configurados, el dispositivo crea un registro CNAME que asigna el dominio IP6-ARPA en el IN-ADDR correspondiente. El dominio ARPA y el nuevo dominio IN-ADDR.ARPA se utilizan para la resolución. El dispositivo busca en los registros PTR locales y, si los registros no están presentes, el dispositivo envía una solicitud PTR para el dominio IN-ADDR.ARPA al servidor DNS. El dispositivo Citrix ADC utiliza la respuesta del servidor DNS para sintetizar la respuesta de la solicitud PTR inicial.

Pasos de configuración

La creación de las entidades necesarias para la configuración NAT64 con estado en el dispositivo Citrix ADC implica los siguientes procedimientos:

- **Agregar servicios DNS.** Los servicios DNS son una representación lógica de los servidores DNS para los que el dispositivo Citrix ADC actúa como servidor proxy DNS. Para obtener más información sobre la configuración de parámetros opcionales de un servicio, consulte Equilibrio de carga.
- **Agregue la acción DNS64 y la directiva DNS64 y, a continuación, vincule la acción DNS64 a la directiva DNS64.** Una directiva DNS64 especifica las condiciones que deben coincidir con el tráfico para el procesamiento DNS64 de acuerdo con la configuración de la acción DNS64 asociada. La acción DNS64 especifica el prefijo DNS64 obligatorio y la configuración opcional de regla de exclusión y regla asignada.
- **Cree un servidor virtual de equilibrio de carga DNS y vincule los servicios DNS y la directiva DNS64 a él.** El servidor virtual de equilibrio de carga DNS actúa como un servidor proxy DNS para los servidores DNS representados por los servicios DNS enlazados. El tráfico que llega al servidor virtual coincide con la directiva DNS64 vinculada para el procesamiento DNS64. Para obtener más información sobre la configuración de parámetros opcionales de un servidor virtual de equilibrio de carga, consulte Equilibrio de carga.

  Nota: La CLI tiene comandos separados para estas dos tareas, pero la GUI los combina en un solo cuadro de diálogo.

  Habilitar el almacenamiento en caché de registros DNS. Habilite el parámetro global para el dispositivo Citrix ADC para almacenar en caché los registros DNS, que se obtienen mediante operaciones de proxy DNS. Para obtener más información sobre cómo habilitar el almacenamiento en caché de registros DNS, consulte Sistema de nombres de dominio.

Procedimientos CLI

Para crear un servicio de tipo DNS mediante la CLI:

En el símbolo del sistema, escriba:

- add service <name> <IP> <serviceType> <port> …

Para crear una acción DNS64 mediante la CLI:

En el símbolo del sistema, escriba:

- add dns action64 <actionName>-Prefijo <ipv6_addr|*> [-MappeDrule] <expression>[-ExcluderUle]<expression>

Para crear una directiva DNS64 mediante la CLI:

En el símbolo del sistema, escriba:

- add dns policy64 <name> -rule <expression> -action <string>

Para crear un servidor virtual de equilibrio de carga DNS mediante la CLI:

En el símbolo del sistema, escriba:

- add lb vserver <name>DNS <IPAddress><port>-dns64 (HABILITADO | DESHABILITADO) [-BypassaAAA (SÍ | NO)]…

Para enlazar los servicios DNS y la directiva DNS64 al servidor virtual de equilibrio de carga DNS mediante la CLI:

En el símbolo del sistema, escriba:

- bind lb vserver <name> <serviceName> …
- bind lb vserver <name> -policyName <string> -priority <positive_integer> …

Procedimientos de GUI

Para crear un servicio de tipo DNS mediante la GUI:

1. Vaya a Administración del tráfico > Equilibrio de carga > Servicios y agregue un nuevo servicio.
2. Defina los siguientes parámetros:
    - Nombre del servicio*
    - Servidor*
    - Protocolo* (Seleccione DNS en la lista desplegable).
    - Puerto*

Para crear una acción DNS64 mediante la GUI:

Vaya a Administración del tráfico > DNS > Acciones, en la ficha Acciones DNS 64, agregue una nueva acción DNS64.

Para crear una directiva DNS64 mediante la interfaz gráfica de usuario:

Vaya a Administración del tráfico > DNS > Directivas, en la ficha Directivas DNS64, agregue una nueva directiva DNS64.

Para crear un servidor virtual de equilibrio de carga DNS y enlazar los servicios DNS y la directiva DNS64 con él mediante la GUI:

1. Vaya a Administración del tráfico > Equilibrio de carga > Servidores virtuales y agregue un nuevo servidor virtual.
2. Defina los siguientes parámetros:
    - Nombre*
    - Dirección IP*
    - Protocolo* (Seleccione DNS en la lista desplegable).

- Puerto*

3. Seleccione la opción Habilitar DNS64.
4. En el panel Servicios, vincule el servicio al servidor virtual.
5. En el panel Directivas, vincule la directiva al servidor virtual.

Configuración de ejemplo

```
 > add service SVC-DNS-1 203.0.113.50 DNS 53
 Done

> add service SVC-DNS-2 203.0.113.60 DNS 53
 Done

> add dns Action64 DNS64-Action-1 -Prefix 2001:DB8:300::/96
 Done

> add dns Policy64 DNS64-Policy-1 -rule ”CLIENT.IPv6.SRC.IN_SUBNET
   (2001:DB8:5001::/64)”
-action DNS64-Action-1
 Done

> add lb vserver LBVS-DNS64-1 DNS 2001:DB8:9999::99 53 -dns64 ENABLED
 Done

> bind lb vserver LBVS-DNS64-1 SVC-DNS-1
 Done

> bind lb vserver LBVS-DNS64-1 SVC-DNS-2
 Done

> bind lb vserver LBVS-DNS64-1 -policyname DNS64-Policy-1 -priority 2
 Done

<!--NeedCopy-->
```

Traducción con estado NAT64

August 20, 2021

La función NAT64 con estado permite la comunicación entre clientes IPv6 y servidores IPv4 a través de la traducción de paquetes IPv6 a IPv4, y viceversa, mientras mantiene la información de sesión en

el dispositivo Citrix ADC.

Una configuración NAT64 con estado en el dispositivo Citrix ADC tiene los siguientes componentes:

- **Regla NAT64**: Entrada que consiste en una regla ACL6 y un perfil de red, que consiste en un grupo de direcciones SNIP propiedad de Citrix ADC.
- **Prefijo IPv6 NAT64**: Prefijo IPv6 global de 96 bits de longitud (128-32=96) configurado en el dispositivo.
  Nota: Actualmente, el dispositivo Citrix ADC admite solo un prefijo que se utilizará normalmente con todas las reglas NAT 64.

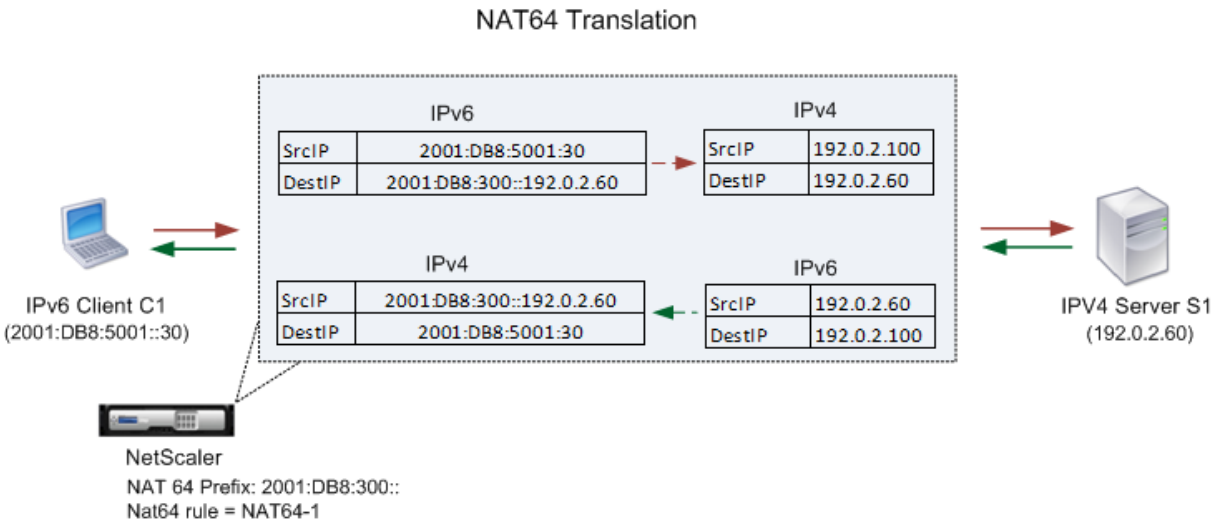
El dispositivo Citrix ADC considera un paquete IPv6 entrante para la traducción NAT64 cuando se cumplen todas las condiciones siguientes:

- El paquete IPv6 entrante coincide con la regla ACL6 vinculada a una regla NAT64.
- La dirección IP de destino del paquete IPv6 coincide con el prefijo IPv6 NAT64.

Cuando un paquete de solicitud IPv6 recibido por el dispositivo Citrix ADC coincide con un ACL6 definido en una regla NAT64 y la dirección IP de destino del paquete coincide con el prefijo IPv6 NAT64, el dispositivo Citrix ADC considera el paquete IPv6 para su traducción.

El dispositivo traduce este paquete IPv6 en un paquete IPv4 con una dirección IP de origen que coincide con una de las direcciones IP vinculadas al perfil de red definido en la regla NAT64 y una dirección IP de destino que consta de los últimos 32 bits de la dirección IPv6 de destino del paquete de solicitud IPv6. El dispositivo Citrix ADC crea una sesión NAT64 para este flujo concreto y reenvía el paquete al servidor IPv4. Las respuestas posteriores del servidor IPv4 y las solicitudes del cliente IPv6 son traducidas en consecuencia por el dispositivo, sobre la base de la información de la sesión NAT64 en particular.

Considere un ejemplo en el que una empresa aloja el sitio www.example.com en el servidor S1, que tiene una dirección IPv4. Para habilitar la comunicación entre los clientes IPv6 y el servidor IPv4 S1, el dispositivo Citrix ADC NS1 se implementa con una configuración NAT64 con estado que incluye una regla NAT64 y un prefijo NAT64. Una dirección IPv6 asignada del servidor S1 se forma concatenando el prefijo IPv6 NAT64 de [96 bits] y la dirección de origen IPv4 de [32 bits]. Esta dirección IPv6 asignada se configura manualmente en los servidores DNS. Los clientes IPv6 obtienen la dirección IPv6 asignada de los servidores DNS para comunicarse con el servidor IPv4 S1.



En la tabla siguiente se enumeran los ajustes utilizados en este ejemplo: Configuración de ejemplo de traducción NAT64 con estado.

A continuación se presenta el flujo de tráfico en este ejemplo:

1. El cliente IPv6 CL1 envía un paquete de solicitud a la dirección Map-Sevr-IPv6 (2001:DB 8:300: :192.0.2.60).
2. El dispositivo Citrix ADC recibe el paquete de solicitud. Si el paquete de solicitud coincide con el ACL6 definido en la regla NAT64 y la dirección IP de destino del paquete coincide con el prefijo IPv6 NAT64, el Citrix ADC considera el paquete IPv6 para la traducción.
3. El dispositivo crea un paquete de solicitud IPv4 traducido con:
   - Campo de dirección IP de destino que contiene el prefijo NAT64 eliminado de la dirección de destino de la solicitud IPv6 (sevr_IPv4 = 192.0.2.60)
   - Campo de dirección IP de origen que contiene una de las direcciones IPv4 enlazada a Netprofile-1 (en este caso, 192.0.2.100)
4. El dispositivo Citrix ADC crea una sesión NAT64 para este flujo y envía la solicitud IPv4 traducida al servidor S1.
5. El servidor IPv64 S1 responde enviando un paquete IPv4 al dispositivo Citrix ADC con:
   - Campo de dirección IP de destino que contiene 192.0.2.100
   - Campo de dirección IP de origen que contiene la dirección deSevr_IPv4 (192.0.2.60)
6. El dispositivo recibe el paquete de respuesta IPv4, busca todas las entradas de sesión y encuentra que el paquete de respuesta IPv6 coincide con la entrada de sesión NAT64 creada en el paso 4. El dispositivo considera el paquete IPv4 para la traducción.
7. El dispositivo crea un paquete de respuesta IPv6 traducido con:
   - Campo de dirección IP de destino=client_ipv6=2001:db 8:5001: :30

- Campo de dirección IP de origen = Concatenación del prefijo NAT64 (primeros 96 bits) y SEVR_IPv4 (últimos 32 bits) =2001:DB 8:300: :192.0.2.60

8. El dispositivo envía la respuesta IPv6 traducida al cliente CL1.

Limitaciones de Statful NAT64

Las siguientes limitaciones se aplican a NAT64 con estado:

- No se admite la traducción de opciones IPv4.
- No se admite la traducción de encabezados de redirección IPv6.
- No se admite la traducción de encabezados de extensión de salto por salto de paquetes IPv6.
- No se admite la traducción de encabezados ESP y EH de paquetes IPv6.
- No se admite la traducción de paquetes de multidifusión.
- Los paquetes de Protocolo de transmisión de control de flujo (SCTP), Protocolo de control de congestión de datagramas (DCCP) e IPSec no se traducen.

Configuración de NAT64 con estado

La creación de las entidades necesarias para la configuración NAT64 con estado en el dispositivo Citrix ADC implica los siguientes procedimientos:

1. Agregue una regla ACL6 con la acción ALLOJY.
2. Agregue un ipset, que enlaza varias direcciones IP.
3. Agregue un perfil de red y vincule el ipset a él. Si quiere vincular solo una dirección IP, no necesita crear una entidad ipset. En ese caso, vincule la dirección IP directamente al perfil de red.
4. Agregue una regla NAT64, que incluye vincular la regla ACL6 y el perfil de red a la regla NAT 64.
5. Agregue un prefijo IPv6 NAT64.

Procedimientos CLI

Para agregar una regla ACL6 mediante la CLI:

En el símbolo del sistema, escriba:

- agregar ns acl6 <acl6name> <acl6action>…

Para agregar un IPSet y enlazar varias IP mediante la CLI:

En el símbolo del sistema, escriba:

- add ipset <name>
- <name> enlazar ipset

Para agregar un perfil de red mediante la CLI:

En el símbolo del sistema, escriba:

- add netprofile <name> -srcIP <IPaddress or IPset>

Para agregar una regla NAT64 mediante la CLI:

En el símbolo del sistema, escriba:

- <string>add nat64 <name> <acl6name> -NetProfile

Para agregar un prefijo NAT64 mediante la CLI:

En el símbolo del sistema, escriba:

- establecer ipv6 -natprefix <ipv6_addr|*>

Ejemplo:

```
 > add acl6 ACL6-1 ALLOW -srcIPv6 2001:DB8:5001::30
 Done

> apply acls6
 Done

> add ip 192.0.2.100 255.255.255.0  - type SNIP
 Done

> add ip 192.0.2.102 255.255.255.0   - type SNIP
 Done

> add ipset IPset-1
 Done

> bind ipset IPset-1 192.0.2.100 192.0.2.102
IPAddress ”192.0.2.100” bound
IPAddress ”192.0.2.102” bound
 Done

> add netprofile Netprofile-1 -srcIP IPset-1
 Done

> add nat64 NAT64-1 ACL6-1 -netprofile Netprofile-1
 Done

> set ipv6 -natprefix 2001:DB8:300::/96
 Done
<!--NeedCopy-->
```


Procedimientos de GUI

Para agregar una regla NAT64 mediante la GUI:

Desplácese hasta Sistema > Red > Rutas > NAT64 y una nueva regla NAT64, o modifique una regla existente.

Para agregar un prefijo NAT64 mediante la GUI:

Vaya a Sistema > Red, en el grupo Configuración, haga clic en Configurar parámetros INATy defina el parámetro Prefijo.

RNAT

August 20, 2021

En Traducción inversa de direcciones de red (RNAT), el dispositivo Citrix ADC reemplaza las direcciones IP de origen de los paquetes generados por los servidores con direcciones IP NAT públicas. De forma predeterminada, el dispositivo utiliza una dirección SNIP como dirección IP NAT. También puede configurar el dispositivo para que utilice una dirección IP NAT única para cada subred. También puede configurar RNAT mediante Listas de control de acceso (ACL). Los modos Usar IP de origen (USIP), Usar IP de subred (USNIP) y Equilibrio de carga de enlace (LLB) afectan al funcionamiento de RNAT. Puede mostrar estadísticas para supervisar RNAT.

Nota: El intervalo de puertos efímeros para RNAT en el dispositivo Citrix ADC es 1024-65535.

Puede utilizar una dirección de red o una ACL extendida como condición para una entrada RNAT:

- **Uso de una dirección de red.** Cuando se utiliza una dirección de red, el procesamiento RNAT se realiza en todos los paquetes procedentes de la red especificada.
- **Uso de ACL extendidas.** Cuando utiliza ACL, el procesamiento RNAT se realiza en todos los paquetes que coinciden con las ACL. Para configurar el dispositivo Citrix ADC para que utilice una dirección IP única para el tráfico que coincida con una ACL, debe realizar las tres tareas siguientes:

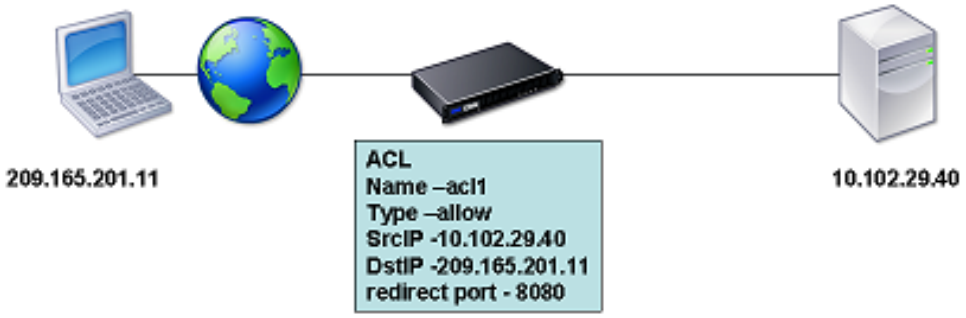
  1. Configure la ACL.
  2. Configure RNAT para cambiar la dirección IP de origen y el puerto de destino.
  3. Aplique la ACL.

  El siguiente diagrama ilustra RNAT configurado con una ACL.

  Ilustración 1. RNAT con una ACL

Source IP Address	Destination IP Address	Destination Port
209.165.202.129	209.165.201.11	8080

Source IP Address	Destination IP Address
10.102.29.40	209.165.201.11

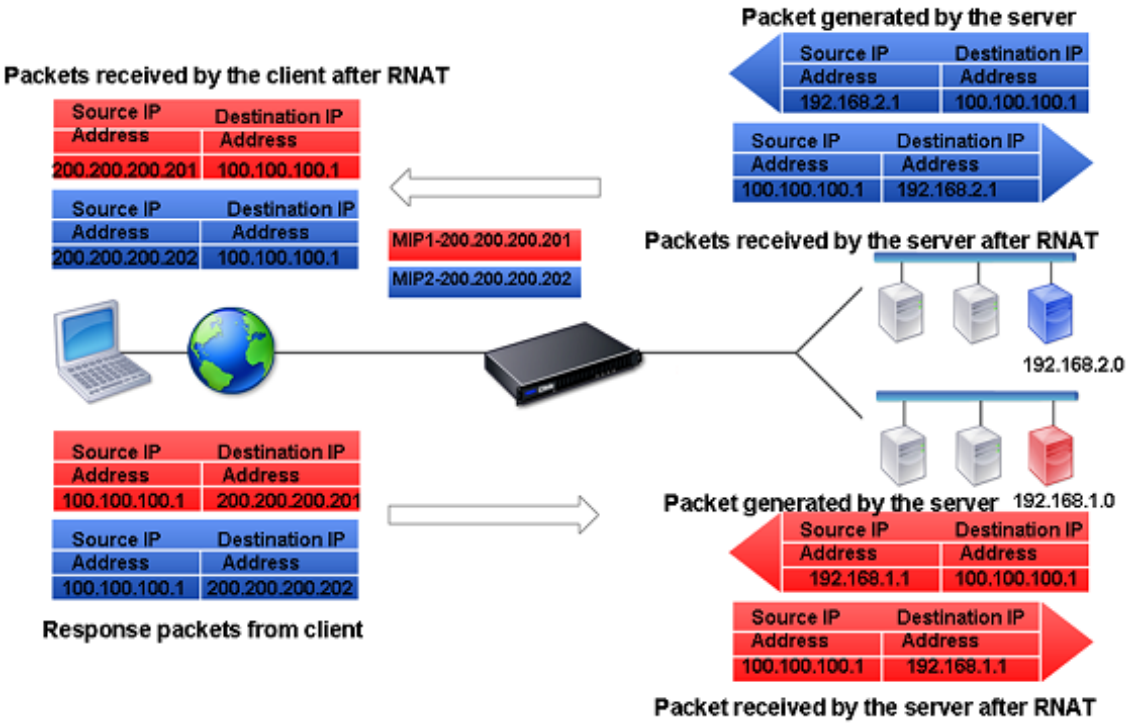


Tiene las siguientes opciones básicas para el tipo de dirección IP NAT:

- **Uso de un SNIP como dirección IP NAT.** Cuando se utiliza un SNIP como dirección IP NAT, el dispositivo Citrix ADC reemplaza las direcciones IP de origen de los paquetes generados por el servidor por un SNIP. Por lo tanto, la dirección SNIP debe ser una dirección IP pública. Si el modo Usar IP de subred (USNIP) está habilitado, el Citrix ADC puede usar una dirección IP de subred (SNIP) como dirección IP de NAT.
- **Usar una dirección IP única como dirección IP NAT.** Cuando se utiliza una dirección IP única como dirección IP NAT, el dispositivo Citrix ADC reemplaza las direcciones IP de origen de los paquetes generados por el servidor por la dirección IP única especificada. La dirección IP única debe ser una dirección IP pública propiedad de Citrix ADC. Si se configuran varias direcciones IP NAT para una subred, la selección de IP NAT utiliza el algoritmo round robin.

  Esta configuración se ilustra en el siguiente diagrama.

  Ilustración 2. Uso de una dirección IP única como dirección IP NAT



Antes de comenzar

Antes de configurar una regla RNAT, tenga en cuenta los siguientes puntos:

- Cuando RNAT y Usar IP de origen (USIP) están configurados en el dispositivo Citrix ADC, RNAT tiene prioridad. En otras palabras, la dirección IP de origen de los paquetes, que coincide con una regla RNAT, se reemplaza de acuerdo con la configuración de la regla RNAT.
- En una topología en la que el dispositivo Citrix ADC realiza Equilibrio de carga de enlace (LLB) y RNAT para el tráfico procedente del servidor, el dispositivo selecciona la dirección IP de origen según el enrutador. La configuración LLB determina la selección del router. Para obtener más información sobre LLB, consulte Equilibrio de carga de vínculos.

Configurar RNAT

Las siguientes instrucciones proporcionan procedimientos de línea de comandos independientes para crear entradas RNAT que utilizan condiciones diferentes y diferentes tipos de direcciones IP NAT. En la GUI, todas las variaciones se pueden configurar en el mismo cuadro de diálogo, por lo que solo hay un procedimiento para los usuarios de GUI.

Procedimientos CLI

Para crear una regla RNAT mediante la CLI:

En el símbolo del sistema, para crear la regla y verificar la configuración, escriba:

- `add rnat <name> (<network> | (<aclname> [-redirectPort <port>]))`
- `bind rnat <name> <natIP>@ …`
- `show rnat`

Para modificar o quitar una regla RNAT mediante la CLI:

- Para modificar una regla RNAT:

  `set rnat <name> (<aclname> [-redirectPort <port>])`

- Para quitar una regla RNAT, escriba el comando.

  `rm rnat <name>`

Utilice el siguiente comando para verificar la configuración:

- `show rnat`

Ejemplos:

```
A network address as the condition and a SNIP address as the NAT IP
    address:

> add rnat RNAT-1 192.168.1.0 255.255.255.0
Done

A network address as the condition and a unique IP address as the NAT
    IP address:

> add rnat RNAT-2 192.168.1.0 255.255.255.0
Done

> bind rnat RNAT-2 -natip 10.102.29.50
Done

If instead of a single NAT IP address you specify a range, RNAT entries
     are created with all the Citrix ADC-owned IP addresses, except the
    NSIP, that fall within the range specified:

> add rnat RNAT-3 192.168.1.0 255.255.255.0
Done

> bind rnat RNAT-3 -natip 10.102.29.[50-110]
Done


```



```
An ACL as the condition and a SNIP address as the NAT IP address:

> add rnat RNAT-4 acl1
Done

An ACL as a condition and a unique IP address as the NAT IP address:

> add rnat RNAT-4 acl1
Done

> bind rnat RNAT-4 -natip 10.102.29.50
Done

If instead of a single NAT IP address you specify a range, RNAT entries
     are created with all the Citrix ADC-owned IP addresses, except the
    NSIP, that fall within the range specified:

> add rnat RNAT-5 acl1
Done

> bind rnat RNAT-5 -natip 10.102.29.[50-70]
Done

<!--NeedCopy-->
```

Procedimientos de GUI

Para crear una entrada RNAT mediante la GUI:

Vaya a **Sistema** > **Red** > **NAT**, haga clic en la ficha **RNAT** y agregue una nueva regla RNAT, o modifique una regla existente.

Monitorizar RNAT

Puede mostrar estadísticas de RNAT para solucionar problemas relacionados con la traducción de direcciones IP.

En la siguiente tabla se describen las estadísticas asociadas con RNAT y RNAT IP.

Estadística	Descripción
Bytes recibidos	Bytes recibidos durante las sesiones RNAT
Bytes enviados	Bytes enviados durante las sesiones RNAT

Estadística	Descripción
Paquetes recibidos	Paquetes recibidos durante las sesiones RNAT
Paquetes enviados	Paquetes enviados durante sesiones RNAT
Syn enviado	Solicitudes de conexiones enviadas durante las sesiones RNAT
Períodos de sesiones en curso	Sesiones RNAT activas actualmente

Para ver las estadísticas de RNAT mediante la CLI:

En el símbolo del sistema, escriba:

- **stat rnat**

Ejemplo:

```
> stat rnat

RNAT summary
                                Rate (/s)            Total
Bytes Received                    0                    0
Bytes Sent                        0                    0
Packets Received                  0                    0
Packets Sent                      0                    0
Syn Sent                          0                    0
Current RNAT sessions            --                    0
 Done
>
<!--NeedCopy-->
```

Para supervisar RNAT mediante la GUI:

Vaya a **Sistema** > **Red** > **NAT**, haga clic en la ficha **RNAT** y, a continuación, haga clic en **Estadísticas**.

Configurar RNAT6

Las reglas de traducción inversa de direcciones de red (RNAT) para paquetes IPv6 se denominan RNAT6s. Cuando un paquete IPv6 generado por un servidor coincide con las condiciones especificadas en la regla RNAT6, el dispositivo reemplaza la dirección IPv6 de origen del paquete IPv6 por una dirección IPv6 NAT configurada antes de reenviarla al destino. La dirección NAT IPv6 es una de las direcciones SNIP6 o VIP6 propiedad de Citrix ADC.

Al configurar una regla RNAT6, puede especificar un prefijo IPv6 o un ACL6 como condición:

- **Utilizar una dirección de red IPv6**. Cuando se utiliza un prefijo IPv6, el dispositivo realiza el procesamiento RNAT en los paquetes IPv6 cuya dirección IPv6 coincide con el prefijo.
- **Mediante ACL6s**. Cuando se utiliza un ACL6, el dispositivo realiza el procesamiento RNAT en los paquetes IPv6 que coinciden con las condiciones especificadas en el ACL6.

Tiene una de las siguientes opciones para establecer la dirección IP NAT:

- Especifique un conjunto de direcciones SNIP6 y VIP6 propiedad de Citrix ADC para una regla RNAT6. El dispositivo Citrix ADC utiliza cualquiera de las direcciones IPv6 de este conjunto como dirección IP NAT para cada sesión. La selección se basa en el algoritmo round robin y se realiza para cada sesión.
- No especifique ninguna dirección SNIP6 o VIP6 propiedad de Citrix ADC para una regla RNAT6. El dispositivo Citrix ADC utiliza cualquiera de las direcciones SNIP6 o VIP6 propiedad de Citrix ADC como dirección IP NAT. La selección se basa en la red de salto siguiente a la que está destinado un paquete IPv6 que coincide con la regla RNAT.

Procedimientos CLI

Para crear una regla RNAT6 mediante la CLI:

En el símbolo del sistema, para crear la regla y verificar la configuración, escriba:

- **add rnat6** <name>(<network>| (<acl6name>[-**RedirectPort**]<port>))
- **bind rnat6** <name> <natIP6>@ …
- **show rnat6**

Para modificar o quitar una regla RNAT6 mediante la CLI:

- Para modificar una regla RNAT6 cuya condición es ACL6, escriba el <name> comando **set rnat6**, seguido de un nuevo valor para el parámetro **RedirectPort**.
- Para quitar una regla RNAT6, escriba el <name> comando **clear rnat6**.

Procedimientos de GUI

Para configurar una regla RNAT6 mediante la GUI:

Vaya a **Sistema** > **Red** > **NAT**, haga clic en la ficha **RNAT6** y agregue una nueva regla RNAT6, o modifique una regla existente.

Monitor RNAT6

Puede mostrar estadísticas relacionadas con la función RNAT6 para supervisar el rendimiento o para solucionar problemas relacionados con la función RNAT6. Puede mostrar un resumen de las estadísti-

cas de las reglas RNAT6 o de una regla RNAT6 concreta. Los contadores estadísticos reflejan los eventos desde que se reinició por última vez el dispositivo Citrix ADC. Todos estos contadores se restablecen a 0 cuando se reinicia el dispositivo Citrix ADC.

A continuación se enumeran algunos de los contadores de estadísticas asociados con la función RNAT6:

- **Bytes recibidos**: Bytes totales recibidos durante las sesiones RNAT6.
- **Bytes enviados**: Número total de bytes enviados durante las sesiones RNAT6.
- **Paquetes recibidos**: Número total de paquetes recibidos durante las sesiones RNAT6.
- **Paquetes enviados**: Número total de paquetes enviados durante las sesiones RNAT6.
- **Syn enviado**: Número total de solicitudes de conexiones enviadas durante las sesiones RNAT6
- **Sesiones actuales: Sesiones** RNAT6 actualmente activas

Para mostrar una estadística resumida de todas las reglas de RNAT6 mediante la CLI:

En el símbolo del sistema, escriba:

- **inicio rnat6**

Para mostrar estadísticas de una regla RNAT6 especificada mediante la CLI:

En el símbolo del sistema, escriba:

- **inicio rnat6** []<rnat6 rule name>

Para mostrar las estadísticas de RNAT6 mediante la GUI:

Vaya a **Sistema** > **Red** > **NAT**, haga clic en la ficha **RNAT6** y, a continuación, haga clic en **Estadísticas**.

```
> stat rnat6

RNAT6 summary

                          Rate (/s)               Total

Bytes Received             178                20644

Bytes Sent                 178                20644

Packets Received            5                  401

Packets Sent                5                  401

Syn Sent                    0                    2

Current RNAT6 sessions      --                   1
```



```
18
19 Done
20
21 <!--NeedCopy-->
```

Hora de inicio de registro y razones de cierre de conexión en entradas de registro de RNAT

Para diagnosticar o solucionar problemas relacionados con RNAT, el dispositivo Citrix ADC registra las sesiones de RNAT cada vez que se cierran.

Un mensaje de registro para una sesión RNAT consta de la siguiente información:

- Dirección IP propiedad de Citrix ADC (dirección NSIP o dirección SNIP) desde la que se origina el mensaje de registro
- Marca de tiempo de creación de registros
- Protocolo de la sesión RNAT
- Dirección IP de origen
- Dirección IP RNAT
- Dirección IP de destino
- Hora de inicio de la sesión RNAT
- Hora de cierre de la sesión RNAT
- Total de bytes enviados por el dispositivo Citrix ADC para esta sesión de RNAT
- Total de bytes recibidos por el dispositivo Citrix ADC para esta sesión de RNAT
- Motivo del cierre de la sesión RNAT. El dispositivo Citrix ADC registra el motivo de cierre de las sesiones TCP RNAT que no utilizan el proxy TCP (proxy TCP inhabilitado) del dispositivo. Los siguientes son el tipo de motivos de cierre que se registran para las sesiones TCP RNAT:
  - **TCP FIN**. La sesión RNAT se cerró debido a un TCP FIN enviado por el dispositivo de origen o de destino.
  - **TCP RST**. La sesión de RNAT se cerró debido a un restablecimiento de TCP enviado por el dispositivo de origen o de destino.
  - **Tiempo de espera**. Se agotó el tiempo de espera de la sesión RNAT.

En la siguiente tabla se muestran algunas entradas de registro de ejemplo para sesiones RNAT.

Tipo de entrada	Entrada de registro de ejemplo
Entrada de registro de ejemplo para sesión de RNAT UDP	Dec 1 15:28:12 10.102.53.114 12/01/2015:15:28:12 GMT 0-PPE-0: Default UDP NAT_OTHERCONN_DELINK 154 0: Source 1.2.2.5:23431: Destination 192.168.123.122:22: NatIP 192.168.123.1:4045: Destination 192.168.123.122:22: Start Time 12/01/2015:15:26:58 GMT: Delink Time 12/01/2015:15:28:12 GMT: Total_bytes_send 2511: Total_bytes_recv 3725
Entrada de registro de muestra para sesión TCP RNAT. La entrada de registro muestra que la sesión se cerró debido a TCP Restablecer	Dec 1 15:29:59 10.102.53.114 12/01/2015:15:27:59 GMT 0-PPE-0: Default TCP NAT_OTHERCONN_DELINK 152 0: Source 1.2.2.5:33826: Destination 192.168.123.122:22: NatIP 192.168.123.1:2384: Destination 192.168.123.122:22: Start Time 12/01/2015:15:27:40 GMT: Delink Time 12/01/2015:15:27:59 GMT: Total_bytes_send 2147: Total_bytes_recv 3257: Closure Reason TCP RST
Entrada de registro de muestra para sesión TCP RNAT. La entrada de registro muestra que se agotó el tiempo de espera de la sesión	Dec 1 15:30:12 10.102.53.114 12/01/2015:15:30:12 GMT 0-PPE-0: Default TCP NAT_OTHERCONN_DELINK 155 0: Source 1.2.2.5:64976: Destination 192.168.123.115:22: NatIP 192.168.123.1:19636: Destination 192.168.123.115:22: Start Time 12/01/2015:15:27:25 GMT: Delink Time 12/01/2015:15:30:12 GMT: Total_bytes_send 0: Total_bytes_recv 0: Closure Reason TIMEOUT

Failover de conexión con estado para RNAT

La conmutación por error de conexión ayuda a evitar la interrupción del acceso a las aplicaciones implementadas en un entorno distribuido. El dispositivo Citrix ADC ahora admite la conmutación por error de conexión con estado para conexiones relacionadas con reglas RNAT en una configuración de alta disponibilidad (HA) de Citrix ADC. En una configuración de alta disponibilidad, la conmutación por error de conexión (o reflejo de conexión) hace referencia al proceso de mantener activa una conexión TCP o UDP establecida cuando se produce una conmutación por error.

El dispositivo principal envía mensajes al dispositivo secundario para sincronizar la información actual sobre las conexiones RNAT. El dispositivo secundario utiliza esta información de conexión solo en caso de que se produzca una conmutación por error. Cuando se produce una conmutación por error, el nuevo dispositivo Citrix ADC principal tiene información sobre las conexiones establecidas antes de la conmutación por error y, por lo tanto, continúa sirviendo esas conexiones incluso después de la conmutación por error. Desde la perspectiva del cliente, esta conmutación por error es transparente. Durante el período de transición, el cliente y el servidor pueden experimentar una breve interrupción y retransmisiones.

La conmutación por error de conexión se puede habilitar por regla de RNAT. Para habilitar la conmutación por error de conexión en una regla RNAT, habilite el parámetro ConnFailover (conmutación por error de conexión) de esa regla RNAT específica mediante CLI o GUI.

Para habilitar la conmutación por error de conexión para una regla RNAT mediante la CLI:

En el símbolo del sistema, escriba:

- `set rnat <name> -connfailover (ENABLED | DISABLED)`
- `show rnat`

Para habilitar la conmutación por error de conexión para una regla RNAT mediante la GUI:

1. Vaya a **Sistema** > **Red** > **NATs**y, a continuación, haga clic en la ficha **RNAT**.
2. Seleccione **Failover de conexión** mientras agrega una nueva regla RNAT o mientras modifica una regla existente.

Reserva del puerto de origen para conexiones RNAT a servidores

Para una solicitud que llega a una configuración de RNAT que tiene una o más direcciones IP RNAT y el parámetro Usar puerto proxy inhabilitado, el dispositivo Citrix ADC utiliza una de las direcciones IP RNAT y el puerto de origen de la solicitud RNAT para conectarse a los servidores. Antes de la compilación 13.0 47.x, la conexión RNAT (mediante el puerto de origen del cliente RNAT) al servidor falla si el mismo puerto de origen ya se ha utilizado en otras conexiones.

- **Puerto de origen inferior a 1024**. De forma predeterminada, el dispositivo Citrix ADC reserva los primeros 1024 puertos de cualquier dirección IP propiedad de Citrix ADC (incluidas las direcciones IP RNAT). Antes de la compilación 13.0 47.x, la conexión RNAT (mediante el puerto de origen del cliente RNAT) al servidor falla si el puerto de origen de la solicitud RNAT es inferior o igual a 1024. Con la compilación 13.0 47.x, la conexión RNAT (mediante el puerto de origen del cliente RNAT) al servidor se realiza correctamente incluso si el puerto de origen de la solicitud RNAT es inferior o igual a 1024.
- **Puerto de origen superior a 1024**. Antes de la compilación 13.0 47.x, la conexión RNAT (mediante el puerto de origen del cliente RNAT) al servidor falla si el mismo puerto de origen ya se ha utilizado en otras conexiones. Con la compilación 13.0 47.x, puede especificar un rango de

puertos de origen cliente RNAT en el parámetro `Retain Source Port range` (`retainsourceportrange`) como parte de una configuración de RNAT. El dispositivo Citrix ADC reserva estos puertos de origen de cliente RNAT en la dirección IP RNAT para que se utilicen únicamente para la conexión RNAT a los servidores.

Eliminación de sesiones de RNAT

Puede eliminar todas las sesiones RNAT no deseadas o ineficientes del dispositivo Citrix ADC. El dispositivo libera inmediatamente los recursos (como el puerto de la dirección IP de NAT y la memoria) asignados para estas sesiones, lo que hace que los recursos estén disponibles para las sesiones nuevas. El dispositivo también elimina todos los paquetes posteriores relacionados con estas sesiones eliminadas. Puede quitar todas las sesiones de RNAT o seleccionadas del dispositivo Citrix ADC.

Para borrar todas las sesiones de RNAT mediante la CLI:

En el símbolo del sistema, escriba:

- **flush rnatsession**

Para borrar sesiones RNAT selectivas mediante la CLI:

En el símbolo del sistema, escriba:

- **flush rnatsession** ((-**network** <ip_addr> -**netmask** <netmask>) | -**natIP** <ip_addr> | -**aclname** <string>)

Para borrar todas o selectivas sesiones RNAT mediante la GUI:

1. Vaya a **Sistema** > **Red** > **NAT y,**a continuación, haga clic en la ficha **RNAT** .
2. En el menú **Acciones**, haga clic en **Vacar sesiones RNAT** para quitar todas las sesiones RNAT selectivas o todas (por ejemplo, quitar sesiones RNAT con una IP RNAT específica o pertenecer a una regla RNAT basada en red o ACL específica).

Configuraciones de ejemplo:

```
1     Clear all RNAT sessions existing on a Citrix ADC appliance
2
3     > flush rnatsession
4
5     Done
6
7     Clear all RNAT sessions belonging to network based RNAT rules that
         has 203.0.113.0/24 network as the matching condition.
8
9     > flush rnatsession -network 203.0.113.0 -netmask 255.255.255.0
10
```



```
11      Done
12
13      Clear all RNAT sessions with RNAT IP 192.0.2.90.
14
15      > flush rnatsession -natIP 192.0.2.90
16
17      Done
18
19      Clear all RNAT sessions belonging to ACL based RNAT rules that has
           ACL-RNAT-1 as the matching condition.
20
21      > flush rnatsession -aclname ACL-RNAT-1
22
23      Done
24  <!--NeedCopy-->
```

Configuración de la traducción IPv6-IPv4 basada en prefijos

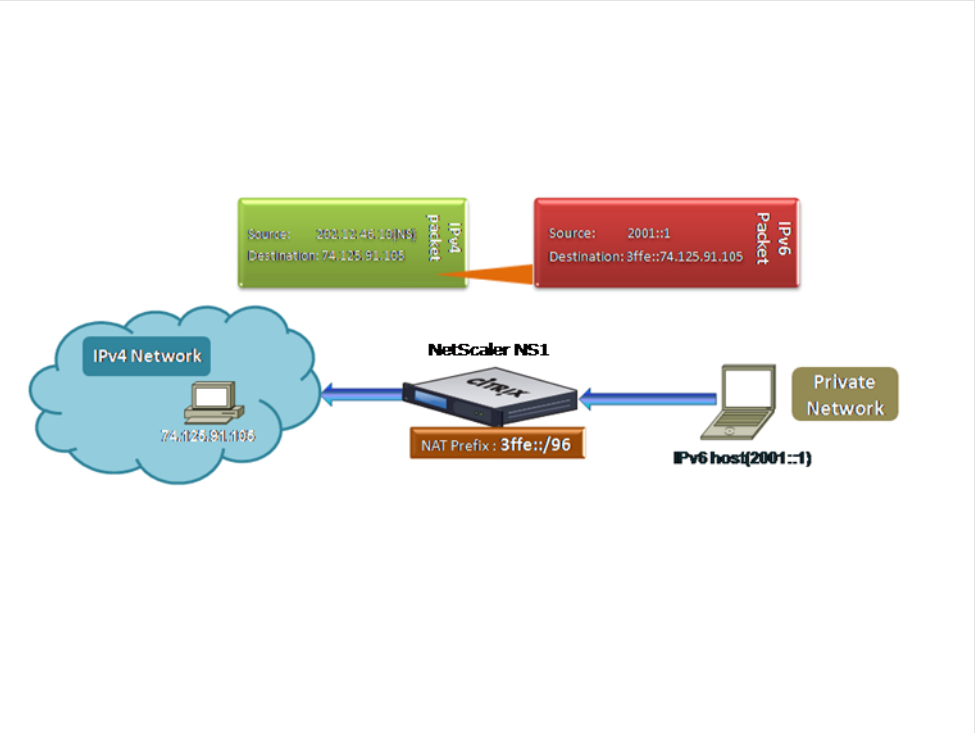
August 20, 2021

La traducción basada en prefijos es un proceso de conversión de paquetes enviados desde servidores IPv6 privados a paquetes IPv4, mediante un prefijo IPv6 configurado en el dispositivo Citrix ADC. Este prefijo tiene una longitud de 96 bits (128-32=96). Los servidores IPv6 incrustan la dirección IP de destino de los servidores o hosts IPv4 en los últimos 32 bits del campo de dirección IP de destino de los paquetes IPv6. Los primeros 96 bits del campo de dirección IP de destino se establecen como el prefijo NAT IPv6.

El dispositivo Citrix ADC compara los primeros 96 bits de la dirección IP de destino de todos los paquetes IPv6 entrantes con el prefijo configurado. Si hay una coincidencia, el dispositivo Citrix ADC genera un paquete IPv4 y establece la dirección IP de destino como los últimos 32 bits de la dirección IP de destino del paquete IPv6 coincidente. Los paquetes IPv6 dirigidos a este prefijo deben enrutarse al Citrix ADC para que el Citrix ADC realice la traducción IPv6-IPv4.

En el diagrama siguiente, 3ffe: :/96 se configura como el prefijo NAT IPv6 en Citrix ADC NS1. El host IPv6 envía un paquete IPv6 con la dirección IP de destino 3ffe: :74.125.91.105. NS1 compara los primeros 96 bits de la dirección IP de destino de todos los paquetes IPv6 entrantes con el prefijo configurado y coinciden. NS1 genera un paquete IPv4 y establece la dirección IP de destino como 74.125.91.105.

Ilustración 1. Traducción basada en prefijos IPv6-IPv4



Para configurar la traducción IPv6-IPv4 basada en prefijos mediante la CLI:

En el símbolo del sistema, escriba:

```
set ipv6 [-natprefijo\ <ipv6_addr                    \ *]
```

-
- show ipv6

Ejemplo:

```
1 > set ipv6 -natprefix 3ffe::/96
2  Done
3 <!--NeedCopy-->
```

Para configurar la traducción IPv6-IPv4 basada en prefijos mediante la GUI:

Vaya a Sistema > Red, en el grupo Configuración, haga clic en Configurar parámetros INATy defina el parámetro Prefijo.

Prefijo IP NAT

January 12, 2021

El dispositivo Citrix ADC admite la traducción de una parte de la dirección IP de origen en lugar de la dirección completa de los paquetes recibidos en el dispositivo. El prefijo IP NAT incluye cambiar uno o más octetos o bits de la dirección IP de origen.

El dispositivo Citrix ADC admite NAT de prefijo IP para configuraciones de equilibrio de carga de los siguientes tipos: ANY, UDP, DNS, TCP y HTTP.

Caso de uso: Zonificación de clientes para una implementación de un dispositivo Citrix ADC y un dispositivo de optimización

El prefijo IP NAT es muy útil en una implementación que incluye un dispositivo Citrix ADC y un dispositivo de optimización (por ejemplo, Citrix ByteMobile). Este tipo de implementación tiene diferentes redes de cliente ubicadas geográficamente, que comparten la misma dirección de red. El dispositivo Citrix ADC debe enviar el tráfico recibido de cada una de las redes cliente al dispositivo de optimización antes de reenviarlo al destino.

El dispositivo devuelve el tráfico optimizado al dispositivo Citrix ADC. Dado que el requisito de optimización es diferente para el tráfico de cada red cliente, el dispositivo de optimización debe reconocer la red cliente de cada paquete que recibe. La solución consiste en separar el tráfico de cada red cliente en una zona diferente mediante VLAN. Prefijo IP NAT con una configuración diferente se configura para cada zona. El dispositivo Citrix ADC traduce el último octeto de la dirección IP de origen de cada paquete y el valor del octeto traducido es diferente para cada zona.

Considere un ejemplo de dos zonas, Z1 y Z2, que comparten la dirección de red 192.0.2.0/24. En el dispositivo Citrix ADC, las entidades NAT de prefijo IP denominadas natrule-1 y natrule-2 se configuran para estas dos zonas. Antes de que el dispositivo reenvíe un paquete desde Z1, natrule-1 traduce el último octeto de la dirección IP de origen del paquete a 100. Del mismo modo, para los paquetes de Z2, natrule-2 traduce el último octeto de la dirección IP de origen a 200. Para dos clientes, CL1-Z1 en la zona Z1 y CL1-Z2 en la zona Z2, cada uno con dirección IP 192.0.2.30, el dispositivo Citrix ADC traduce la dirección IP de origen de los paquetes de CL1-Z1 a 100.0.2.30 y de los paquetes de CL1-Z2 a 200.0.2.30. El dispositivo de optimización al que el dispositivo Citrix ADC envía los paquetes traducidos está configurado para utilizar la dirección IP de origen de un paquete para reconocer la zona, por lo que aplica la optimización adecuada configurada para la zona desde la que se originó el paquete.

Pasos de configuración

La configuración de NAT del prefijo IP consta de los siguientes pasos:

- **Cree un perfil de red y establezca el parámetro Regla NAT de un perfil de red**. Una regla NAT especifica dos direcciones IP y una máscara de red. La primera dirección IP (especificada por el parámetro Dirección IP) es la dirección IP de origen que se va a traducir con la segunda (especificada por el parámetro Rewrite IP). La máscara de red especifica la parte de la dirección IP de origen que se va a traducir con la misma parte de la segunda dirección IP.
- **Enlace el perfil de red a servidores o servicios virtuales de equilibrio de carga**. Un perfil de red con configuración de regla NAT se puede enlazar a un servidor virtual o servicio de tipo CUY, UDP, DNS, TCP y HTTP. Después de vincular un perfil de red a un servidor virtual o servicio, el dispositivo Citrix ADC coincide con la dirección IP de origen de los paquetes entrantes relacionados con el servidor virtual o servicio con la configuración de la regla NAT. A continuación, Citrix ADC realiza NAT de prefijo IP para paquetes que coinciden con la regla NAT.

Para configurar la traducción NAT del prefijo IP mediante la línea de comandos:

En el símbolo del sistema, escriba:

- **bind netProfile** <name> (-**natRule** <ip_addr> <netmask> <rewriteIp>)
- **show netprofile** <name>

Para configurar el prefijo IP NAT mediante la GUI:

1. Vaya a **Sistema** > **Red** > **Perfiles de red**.
2. Defina los siguientes parámetros en Reglas de NAT al agregar o modificar NetProfiles.
    - Dirección IP
    - Máscara de red
    - Volver a escribir IP

Configuración de ejemplo

En la siguiente configuración de ejemplo, el perfil de red PARTIAL-NAT-1 tiene la configuración de NAT de prefijo IP y está enlazado al servidor virtual de equilibrio de carga LBVS-1, que es de tipo ANY. Para los paquetes recibidos en LBVS-1 desde 192.0.0.0/8, el dispositivo Citrix ADC traduce el último octeto de la dirección IP de origen del paquete a 100. Por ejemplo, un paquete con dirección IP de origen 192.0.2.30 recibido en LBVS-1, el dispositivo Citrix ADC traduce la dirección IP de origen a 100.0.2.30 antes de enviarla uno de los servidores enlazados.

```
1 > add netprofile PARTIAL-NAT-1
2 Done
3
4 > bind netprofile PARTIAL-NAT-1  - natrule 192.0.0.0 255.0.0.0 100.0.0.0
5 Done
6
```



```
> add lb vserver LBVS-1 ANY 203.0.113. 61 * -netprofile PARTIAL-NAT-1
Done
<!--NeedCopy-->
```

ARP estático

August 20, 2021

Puede agregar entradas ARP estáticas a y eliminar entradas ARP estáticas de la tabla ARP. Después de agregar una entrada, debe verificar la configuración. Si la dirección IP, el puerto o la dirección MAC cambian después de crear una entrada ARP estática, debe quitar o ajustar manualmente la entrada estática. Por lo tanto, no se recomienda crear entradas ARP estáticas a menos que sea necesario.

Para agregar una entrada ARP estática mediante la CLI:

En el símbolo del sistema, escriba:

- **add arp -dirección IP** <ip_addr> -**mac**<mac_addr> -**ifnum** <interface_name>
- **show arp** <IPAddress>

Ejemplo:

```
> add arp -ip 10.102.29.6 -mac 00:24:e8:73:ca:ec -ifnum 1/1
 Done
<!--NeedCopy-->
```

Para eliminar una entrada ARP estática mediante la CLI:

En el símbolo del sistema, escriba el comando **rm arp** y la dirección IP.

Para agregar una entrada ARP estática mediante la GUI:

Vaya a **Sistema** > **Red** > **Tabla ARP** y agregue una entrada ARP estática.

Especificar una VLAN en una entrada ARP estática

En una entrada ARP estática, puede especificar la VLAN a través de la cual se puede acceder al dispositivo de destino. Esta función es útil cuando la interfaz especificada en la entrada ARP estática forma parte de varias VLAN etiquetadas y el destino es accesible a través de una de las VLAN. El dispositivo Citrix ADC incluye el ID de VLAN especificado en los paquetes salientes que coinciden con la entrada ARP estática. Si no especifica un ID de VLAN en una entrada ARP y la interfaz especificada forma parte de varias VLAN etiquetadas, el dispositivo asigna la VLAN nativa de la interfaz a la entrada ARP.

Por ejemplo, supongamos que la interfaz 1/2 de Citrix ADC forma parte de la VLAN 2 nativa y de las VLAN etiquetadas 3 y 4, y agrega una entrada ARP estática para el dispositivo de red A, que forma parte de la VLAN 3 y es accesible a través de la interfaz 1/2. Debe especificar VLAN 3 en la entrada ARP para el dispositivo de red A. El dispositivo Citrix ADC incluye la VLAN 3 etiquetada en todos los paquetes destinados al dispositivo de red A y los envía desde la interfaz 1/2.

Si no especifica un ID de VLAN, el dispositivo Citrix ADC asigna VLAN 2 nativa a la entrada ARP. Los paquetes destinados al dispositivo A se eliminan en la ruta de red, porque no especifican la VLAN 3 etiquetada, que es la VLAN para el dispositivo A.

Para especificar una VLAN en una entrada ARP estática mediante la CLI:

En el símbolo del sistema, escriba:

- **add arp -IP Address** <ip_addr>**-mac**<mac_addr>**-ifnum** <interface_name>[-**vlan**]<positive_integer>
- **show arp** <IPAddress>

Ejemplo:

```
1 > add arp -ip 198.51.100.91 -mac 36:db:4b:f6:12:15 -ifnum 1/2 -vlan 3
2 Done
3 <!--NeedCopy-->
```

Establecer el tiempo de espera para entradas ARP dinámicas

January 12, 2021

Puede establecer globalmente un tiempo de caducidad (valor de tiempo de espera) para las entradas ARP aprendidas dinámicamente. El nuevo valor se aplica solo a las entradas ARP que se aprenden dinámicamente después de establecer el nuevo valor. Las entradas de ARP existentes anteriormente caducan después del tiempo de caducidad configurado previamente. Puede especificar un valor de tiempo de espera ARP de 1 a 1200 segundos.

Para establecer el tiempo de espera para las entradas ARP dinámicas mediante la CLI:

En el símbolo del sistema, escriba:

- **set arpparam** -**tiempo de espera** <positive_integer>]
- **show arpparam**

Ejemplo:


```
> set arpparam -timeout 500
 Done
<!--NeedCopy-->
```

Para establecer el tiempo de espera para las entradas ARP dinámicas en su valor predeterminado mediante la CLI:

En el símbolo del sistema, escriba:

- **unset arpparam**
- **show arpparam**

Ejemplo:

```
> unset arpparam
 Done
<!--NeedCopy-->
```

Para establecer el tiempo de espera para las entradas ARP dinámicas mediante la GUI:

Desplácese hasta **Sistema** > **Red**, en el grupo **Configuración**, haga clic en **Configurar parámetros globales de ARP** y establezca el parámetro **Tiempo de espera de entrada de tabla ARP**.

Descubrimiento de vecinos

August 20, 2021

Neighbor Discovery (ND) es uno de los protocolos más importantes de IPv6. Es un protocolo basado en mensajes que combina la funcionalidad del Protocolo de resolución de direcciones (ARP), Protocolo de mensajes de control de Internet (ICMP) y detección de enrutadores. ND permite a los nodos anunciar sus direcciones de capa de enlace y obtener las direcciones MAC o las direcciones de capa de enlace de los nodos vecinos. Este proceso lo realiza el protocolo Neighbor Discovery (ND6).

El descubrimiento de vecinos puede realizar las siguientes funciones:

- **Detección de enrutadores**: Permite que un host descubra los enrutadores locales en un enlace conectado y configure automáticamente un enrutador predeterminado.
- **Detección de prefijos**: Permite que el host detecte los prefijos de red para destinos locales.

  Nota: El dispositivo Citrix ADC no admite la detección de prefijos.
- **Detección de parámetros**: Permite a un host detectar parámetros operativos adicionales, como MTU y el límite de saltos predeterminado para el tráfico saliente.

- **Configuración automática de direcciones**: Permite a los hosts configurar automáticamente direcciones IP para interfaces con y sin servicios de configuración de direcciones con estado, como DHCPv6. Citrix ADC no admite la configuración automática de direcciones para direcciones IPv6 globales.
- **Resolución de direcciones**: Equivalente a ARP en IPv4, permite que un nodo resuelva la dirección IPv6 de un nodo vecino a su dirección de capa de vínculos.
- **Detección de inalcanzabilidad de vecino**: Habilita un nodo para determinar el estado de accesibilidad de un vecino.
- **Detección de direcciones duplicadas**: Habilita un nodo para determinar si una dirección NSIP ya está en uso por un nodo vecino.
- **Redireccionamiento**: Equivalente al mensaje IPv4 ICMP Redirect, permite que un router redirija el host a una mejor dirección IPv6 de primer salto para llegar a un destino.

Nota: El dispositivo Citrix ADC no admite IPv6 Redirect.

Pasos de configuración

La configuración de la detección de vecinos consiste en las siguientes tareas:

- Agregar vecinos IPv6
- (Opcional) Eliminación de vecinos IPv6

Procedimientos CLI

Para agregar un vecino IPv6 mediante la CLI:

En el símbolo del sistema, escriba:

- **add nd6** <neighbor><mac><ifnum>[-**vlan**]<integer>
- **sh nd6**

Ejemplo:

```
1 > add nd6 2001::1 00:04:23:be:3c:06 1/1  - vlan 1
2  Done
3
4 > show nd6
5    Neighbor                MAC-Address(Vlan, Interface)       State
                TIME
6    --------                ----------------------------       -----
             --------
```



```
1) ::1                      00:d0:68:0b:58:da(   1,  LO/1)   REACHABLE
        PERMANENT
2) fe80::2d0:68ff:fe0b:58da 00:d0:68:0b:58:da(   1,  LO/1)   REACHABLE
        PERMANENT
3) 2001::1                  00:04:23:be:3c:06(   1,   1/1)   REACHABLE
          STATIC
 Done
<!--NeedCopy-->
```

Para quitar una entrada de detección de vecinos mediante la CLI:

En el símbolo del sistema, escriba:

- **rm nd6** <VLANID> <Neighbor> -**vlan**

Ejemplo:

```
 rm nd6 3ffe:100:100::1 -vlan 1
<!--NeedCopy-->
```

Para eliminar todas las entradas de detección de vecinos mediante la CLI:

En el símbolo del sistema, escriba:

- **borrar nd6**

Procedimientos de GUI

Para agregar un vecino IPv6 mediante la GUI:

Vaya a **Sistema** > **Red** > **Vecinos IPv6** y agregue un nuevo vecino IPv6.

Para quitar una entrada de detección de vecinos mediante la GUI:

Vaya a **Sistema** > **Red** > **Vecinos IPv6**, elimine el vecino IPv6.

Para eliminar todas las entradas de detección de vecinos mediante la GUI:

Vaya a **Sistema** > **Red** > **Vecinos IPv6** y haga clic en **Borrar**.

Túneles IP

August 20, 2021

Un túnel IP es un canal de comunicación, que se puede crear mediante tecnologías de encapsulación, entre dos redes que no tienen una ruta de redirección. Cada paquete IP compartido entre las dos redes se encapsula dentro de otro paquete y luego se envía a través del túnel.

El dispositivo Citrix ADC implementa el túnel IP de las siguientes maneras:

- **Citrix ADC como encapsulador (Load Balancing with DSR Mode)**: Considere una organización que tenga varios centros de datos en diferentes países, donde el Citrix ADC tal vez esté en una ubicación y los servidores back-end se encuentren en un país diferente. En esencia, el Citrix ADC y los servidores back-end se encuentran en diferentes redes y están conectados a través de un enrutador.

  Al configurar la devolución directa del servidor (DSR) en este Citrix ADC, el Citrix ADC encapsula el paquete enviado desde la subred de origen y se envía a través de un enrutador y un túnel al servidor back-end apropiado. El servidor back-end descapsulará el paquete y responde directamente al cliente, sin permitir que el paquete pase a través del Citrix ADC.

- **Citrix ADC como Deccapsulator:** considere una organización que tenga varios centros de datos cada uno con ADC Citrix y servidores back-end. Cuando se envía un paquete desde el centro de datos A al centro de datos B, generalmente se envía a través de un intermediario, por ejemplo, un enrutador u otro Citrix ADC. Citrix ADC procesa el paquete y, a continuación, lo reenvía al servidor back-end. Sin embargo, si se envía un paquete encapsulado, Citrix ADC debe poder descapsular el paquete antes de enviarlo a los servidores back-end. Para permitir que Citrix ADC funcione como un decapsulador, se agrega un túnel entre el router y el Citrix ADC. Cuando el paquete encapsulado, con información adicional de encabezado, llega al Citrix ADC, el paquete de datos se descapsulará, es decir, se elimina la información adicional del encabezado y el paquete se reenvía a los servidores back-end apropiados.

  El Citrix ADC también se puede utilizar como un decapsulador para la función de equilibrio de carga, específicamente en casos en los que el número de conexiones en un servidor vserver supera un valor de umbral y todas las conexiones nuevas se desvían a un servidor vserver de copia de seguridad.

Configurar túneles IP

La configuración de túneles IP en un dispositivo Citrix ADC consiste en crear entidades de túnel IP. Una entidad de túnel IP especifica las direcciones IP de punto final del túnel local y remoto y el protocolo que se utilizará para el túnel IP.

Nota: Al configurar un túnel IP en una configuración de clúster, la dirección IP local debe ser una dirección SNIP seccionada.

Procedimientos CLI

Para crear un túnel IP mediante la CLI:

En el símbolo del sistema, escriba:

- **add iptunnel** <name> <remote> <remoteSubnetMask> <local> -**type** -**protocol** (**ipoverip** | **GRE**)
- **show iptunnel**

Para eliminar un túnel IP mediante la CLI:

Para eliminar un túnel IP, escriba el comando **rm iptunnel** y el nombre del túnel.

Para crear un túnel IPv6 mediante la CLI:

En el símbolo del sistema, escriba:

- **add ip6tunnel** <name> <remoteIp> <local>
- **show ip6tunnel**

Para eliminar un túnel IPv6 mediante la CLI:

Para quitar un túnel IPv6, escriba el comando **rm ip6tunnel** y el nombre del túnel.

Procedimientos de GUI

Para crear un túnel IP mediante la GUI:

Vaya a **Sistema** > **Red** > **Túneles IP**, agregue un nuevo túnel IP.

Para crear un túnel IPv6 mediante la GUI:

Vaya a **Sistema** > **Red** > **Túneles IP** > **Túneles IPv6** y agregue un nuevo túnel IPv6.

Personalización de túneles IP globalmente

Al especificar globalmente la dirección IP de origen, puede asignar una dirección IP de origen común en todos los túneles. Además, dado que la fragmentación requiere mucha CPU, puede especificar globalmente que el dispositivo Citrix ADC descarte cualquier paquete que requiera fragmentación. Alternativamente, si quiere fragmentar todos los paquetes siempre que no se alcance un valor de umbral de CPU, puede especificar globalmente el valor de umbral de CPU.

Procedimientos CLI

Para personalizar globalmente los túneles IP mediante la CLI:

En el símbolo del sistema, escriba:

- **configurar IPTunnelParam** -**srcIP** <sourceIPAddress>-**SRCIProUndRobin** (**SÍ** | **NO**) -**DropFrag** [**SÍ** | **NO**] -**DropFragcpuThreshold** <Positive integer>
- **show ipTunnelParam**

Ejemplo:

```
> set iptunnelparam  - srcIP 12.12.12.22 -dropFrag Yes  -
   dropFragCpuThreshold 50
 Done

> set iptunnelparam -srcIPRoundRobin YES -dropFrag Yes  -
   dropFragCpuThreshold 50
 Done
<!--NeedCopy-->
```

Para personalizar globalmente los túneles IPv6 mediante la CLI:

En el símbolo del sistema, escriba:

- **set ip6tunnelparam** -**srcIP** <IPv6Address> -**srcIPRoundRobin** (**YES** | NO)-**dropFrag** [**SÍ** | **NO**] -**dropFragCpuThreshold** <Positive integer>
- **show ip6tunnelparam**

Procedimientos de GUI

Para personalizar globalmente los túneles IP mediante la GUI:

Desplácese hasta **Sistema** > **Red**, en el grupo Configuración, haga clic en **Configuración global del túnel IPv4**.

1. Vaya a **Sistema** > **Red**, en el grupo **Configuración**, haga clic en **Configuración global del túnel IPv6**.
2. En el cuadro de diálogo **Configurar parámetros globales de túnel IP**, defina los parámetros.

Para personalizar globalmente los túneles IPv6 mediante la interfaz gráfica de usuario:

1. Vaya a **Sistema** > **Red**, en el grupo **Configuración**, haga clic en **Configuración global del túnel IPv6**.
2. En el cuadro de diálogo **Configurar parámetros globales de túnel IP**, defina los parámetros.

Opciones de carga GRE en un túnel IP GRE

Para un túnel IP GRE configurado, el dispositivo Citrix ADC encapsula todo el paquete de capa 2, incluidos el encabezado Ethernet y el encabezado VLAN (etiqueta VLAN dot1q). Es posible que los túneles

IP GRE entre dispositivos Citrix ADC y algunos dispositivos de terceros no sean estables, ya que estos dispositivos de terceros no están programados para procesar algunos o los encabezados de paquetes de capa 2. Para configurar un túnel GRE IP estable entre un dispositivo Citrix ADC y un dispositivo de terceros, puede utilizar el parámetro GRE payload del conjunto de comandos GRE IP tunnel. La configuración de carga GRE también se puede aplicar a un GRE con túnel IPSec.

Puede establecer el parámetro de carga útil GRE para realizar una de las siguientes acciones antes de que el paquete se envíe a través del túnel GRE:

- **Ethernet con DOT1Q**. Lleve el encabezado Ethernet así como el encabezado VLAN. Esta es la opción predeterminada. Para un túnel enlazado a una netbridge, el encabezado Ethernet interno y el encabezado VLAN contienen información de la tabla ARP y puente del dispositivo Citrix ADC. Para un túnel establecido como siguiente salto a una regla PBR, la dirección MAC de destino de Ethernet interna se establece en cero y el encabezado de VLAN especifica la VLAN predeterminada. El paquete encapsulado (GRE) enviado desde el punto final del túnel Citrix ADC tiene el siguiente formato:

Outer Ethernet Header	Outer IP Header	GRE Header	Inner Ethernet	Inner VLAN header	Inner IP/IPv6/ARP header	Inner TCP/UDP Header	Payload

- **Ethernet**. Lleve el encabezado Ethernet pero suelte el encabezado VLAN. Dado que los paquetes no contienen información de VLAN en el túnel, para un túnel con esta configuración y enlazado a un netbridge, debe enlazar una VLAN adecuada a la netbridge para que, al recibir cualquier paquete en el túnel, el Citrix ADC pueda reenviar estos paquetes a la VLAN especificada. Si el túnel se establece como siguiente salto en una regla PBR, Citrix ADC enruta los paquetes que se reciben en el túnel. El paquete encapsulado (GRE) enviado desde el punto final del túnel Citrix ADC tiene el siguiente formato:

Outer Ethernet header	Outer IP header	GRE Header	Inner Ethernet header	Inner IP/IPv6/ARP header	Inner TCP/UDP header	Payload

- **IP**. Suelte el encabezado Ethernet, así como el encabezado VLAN. Dado que los túneles con esta configuración no llevan encabezados de capa 2, estos túneles no se pueden enlazar a un netbridge, sino que se pueden establecer como un salto siguiente en una regla PBR. El dispositivo de extremo del túnel del mismo nivel al recibir el paquete lo consume o lo enruta. El paquete encapsulado (GRE) enviado desde el punto final del túnel Citrix ADC tiene el siguiente formato:

Outer Ethernet header	Outer IP header	GRE header	Inner IP/IPv6 header	Inner TCP/UDP header	Payload

Para eliminar encabezados de capa 2 de paquetes en un túnel IP GRE mediante la CLI:

- **add IPtunnel** <name><remote><remoteSubnetMask><local>[-**protocolo** \ [-**vlan**]<GRE><positive_integer>] [-**grepayload**] [-**ipsecProfileName**]\ <string>
- **show iptunnel** <tunnelname>

Ejemplo:

```
> add iptunnel IPTUNNEL-1 203.0.113.133 255.255.255.0 198.51.100.15 -
    protocol GRE - grepayload Ethernet -ipsecProfileName IPTUNNEL-IPSEC
    -1
Done
<!--NeedCopy-->
```

Tráfico IPv6 a través de túneles GRE IPv4

El dispositivo Citrix ADC admite la transferencia de tráfico IPv6 a través de un túnel GRE IPv4. Esta función se puede utilizar para habilitar la comunicación entre redes IPv6 aisladas sin actualizar la infraestructura IPv4 entre ellas.

Para configurar esta función, asocia una regla PBR6 con el túnel GRE IPv4 configurado a través del cual quiere que Citrix ADC envíe y reciba tráfico IPv6. Los parámetros de dirección IPv6 de origen y dirección IPv6 de destino de la regla PBR6 especifican las redes IPv6 cuyo tráfico va a atravesar el túnel GRE IPv4.

Nota: El protocolo IPSec no es compatible con los túneles GRE IPv4 configurados para transferir paquetes IPv6.

Para crear un túnel IPv4 GRE mediante la CLI:

En el símbolo del sistema, escriba:

- **add ipTunnel** <name> <remote> <remoteSubnetMask> <local> -**protocol GRE**
- **show ipTunnel** <name>

Para asociar una regla PBR6 a un túnel IPv4 GRE mediante la CLI:

- **add ns pbr6** <tunnelName> <pbrName> **ALOJAR** -**SRCIPv6** <network-range> -**DSIPv6** <network-range> -**IPTunnel**
- **show pbr**

Configuración de ejemplo

En la siguiente configuración de ejemplo, se crea el túnel IP GRE Tunnel-v6onv4 con la dirección IP del extremo del túnel remoto 10.10.6.30 y la dirección IP del extremo del túnel local 10.10.5.30. El túnel se une entonces a pbr6 pbr6-v6onv4. El SRCIPv6 especifica la red IPv6 conectada al extremo local

y DestIPv6 especifica la red IPv6 conectada al extremo remoto. El tráfico de estas redes IPv6 puede atravesar el túnel IPv4 GRE.

```
1 > add ipTunnel TUNNEL-V6onV4 10.10.6.30 255.255.255.255 10.10.5.30 -
     protocol GRE
2 -ipsecProfileName None
3 Done
4 > add ns pbr6 PBR6-V6onV4 ALLOW -srcIPv6 = 2001:0db8:1::1-2001:0db8
     :1::255 -destIPv6 =
5 1-2001:0db8:4::255 -ipTunnel TUNNEL-V6onV4
6 <!--NeedCopy-->
```

Enviar tráfico de respuesta a través de un túnel IP-IP

Puede configurar un dispositivo Citrix ADC para que envíe tráfico de respuesta a través de un túnel IP-IP en lugar de enrutarlo de nuevo al origen. De forma predeterminada, cuando el dispositivo recibe una solicitud de otro Citrix ADC o de un dispositivo de terceros a través de un túnel IP-IP, enruta el tráfico de respuesta en lugar de enviarlo a través del túnel. Puede utilizar rutas basadas en directivas (PBRs) o habilitar el reenvío basado en MAC (MBF) para enviar la respuesta a través del túnel.

En una regla PBR, especifique las subredes en ambos puntos finales cuyo tráfico va a atravesar el túnel. También establezca el siguiente salto como nombre del túnel. Cuando el tráfico de respuesta coincide con la regla PBR, el dispositivo Citrix ADC envía el tráfico a través del túnel.

Como alternativa, puede habilitar MBF para cumplir este requisito, pero la funcionalidad se limita al tráfico para el que el dispositivo Citrix ADC almacena información de sesión (por ejemplo, tráfico relacionado con el equilibrio de carga o configuraciones RNAT). El dispositivo utiliza la información de sesión para enviar el tráfico de respuesta a través del túnel.

Procedimientos CLI

Para crear una regla PBR y asociar el túnel IP-IP mediante la CLI:

En el símbolo del sistema, escriba:

- **add ns pbr** <pbr_name> **ALLOW** -**srcIP** = <local_subnet_range> -**destIP** = <remote_subnet_range> -**ipTunnel** <tunnel_name>
- **apply ns pbrs**
- **show ns pbr** <pbr_name>

Para habilitar el reenvío basado en Mac mediante la CLI:

En el símbolo del sistema, escriba:

- **enable ns mode MBF**
- **show ns mode**

Procedimientos de GUI

Para crear una regla PBR y asociar el túnel IP-IP mediante la GUI:

1. Vaya a **Sistema** > **Red** > **PBRs**. En la ficha **PBRs**, cree una regla **PBR**.
2. Al crear el PBR, establezca el **Tipo de salto siguiente** en **túnel IP** y Nombre de **túnel IP en el nombre** de túnel IP-IP configurado.

Para habilitar el reenvío basado en Mac mediante la GUI:

1. Vaya a **Sistema** > **Configuración**, en **Modos y funciones**, haga clic en **Configurar modos**.
2. En la página **Configurar modos**, seleccione **Reenvío basado en Mac**.

Configuración de ejemplo

Considere un ejemplo de un túnel IPIP, NS1-NS2-IPIP, que se configura entre dos dispositivos Citrix ADC NS1 y NS2.

De forma predeterminada, para cualquier solicitud que NS2 reciba a través del túnel, su ruta el tráfico de respuesta al origen en lugar de enviarlo (a NS1) a través del túnel.

Puede configurar rutas basadas en directivas (PBRs) o habilitar el reenvío basado en MAC (MBF) en NS2 para habilitarlo para enviar la respuesta a través del túnel.

En la siguiente configuración de ejemplo en NS2, NS1-NS2-IPIP es un túnel IPIP y NS1-NS2-IPIP-PBR es una regla PBR. Para las solicitudes (con dirección IP de origen interno en el rango 10.102.147.0-10.102.147.255 y dirección IP de destino interno en el rango 10.102.147.0-10.102.147.255) recibidas por NS2 a través del túnel, NS2 envía la respuesta correspondiente a través del túnel (a NS1) en lugar de enrutarlo al origen. La funcionalidad está limitada al tráfico que coincide con la regla PBR.

```
1 > add iptunnel NS1-NS2-IPIP 192.0.2.99 255.255.255.255 203.0.113.99 -
     protocol IPIP
2
3 Done
4 > add pbr NS1-NS2-IPIP-PBR -srcIP 10.102.147.0-10.102.147.255  - destIP
     10.20.1.0-10.20.1.255  - ipTunnel NS1-NS2-IPIP
5
6 Done
7 > apply pbrs
8
9 Done
```


Alternativamente, MBF se puede habilitar en NS2. La funcionalidad se limita al tráfico para el que NS2 almacena información de sesión (por ejemplo, tráfico relacionado con el equilibrio de carga o configuraciones RNAT).

```
1 > enable ns mode MBF
2
3 Done
```

Paquetes IPv4 de clase E

January 12, 2021

De forma predeterminada, el dispositivo Citrix ADC elimina cualquier paquete si contiene cualquier dirección IPv4 de clase E en los campos IP de origen o IP de destino. Si la configuración utiliza direcciones IPv4 de clase E, puede configurar el dispositivo Citrix ADC para que procese paquetes IPv4 de clase E.

Antes de comenzar

Antes de comenzar a configurar un dispositivo Citrix ADC para procesar paquetes IPv4 de clase E, tenga en cuenta los siguientes puntos:

- Los dispositivos Citrix ADC no admiten la configuración de ninguna dirección IPv4 propiedad de Citrix ADC (por ejemplo, SNIP y VIP) en el rango de clase E. Los dispositivos Citrix ADC solo admiten el procesamiento de paquetes IPv4 de clase E.
- Un dispositivo Citrix ADC utiliza internamente direcciones IPv4 de clase E para la función IPv6. El dispositivo Citrix ADC no admite ambas funciones (procesamiento de paquetes IPv4 de clase E y compatibilidad con IPv6) que funcionen al mismo tiempo. El dispositivo Citrix ADC impone una restricción para no habilitar la función IPv6 cuando se habilita el procesamiento de paquetes IPv4 de clase E, y viceversa.

Pasos de configuración

La configuración de un dispositivo Citrix ADC para procesar paquetes IPv4 de clase E consiste en habilitar el parámetro de nivel 3 de **clientes de direcciones IPv4 Clase E** (**AllowClasseIPv4**).

Procedimientos CLI

Para configurar el dispositivo Citrix ADC para que procese paquetes IPv4 de clase E mediante la CLI:

En el símbolo del sistema, escriba:

- **set l3param** -**allowClassEIPv4** (**ENABLED**|**DISABLED**)
- **show l3param**

Configuración de ejemplo:

```
> set l3param -allowClassEIPv4 ENABLED

Done

> sh l3param

    Network L3 related Configuration Parameters

    icmpgen_rate_threshold      : 100

    srcnat                      : ENABLED

    override_rnat               : DISABLED

    drop_df_flag                : DISABLED

    .

    .

    .

    IPv6DynamicRouting          : DISABLED

    allowClassEIPv4             : ENABLED

Done
<!--NeedCopy-->
```

Procedimientos de GUI

Para configurar el dispositivo Citrix ADC para que procese paquetes IPv4 de clase E mediante la GUI:

1. Vaya a **Sistema** > **Red** y, a continuación, en la sección **Configuración**, haga clic en **Configurar parámetros de capa 3**.
2. Seleccione **Clientes de direcciones IPv4 Clase E** y haga clic en **Aceptar**.

Supervisar los puertos libres disponibles en un dispositivo Citrix ADC para una nueva conexión back-end

March 9, 2022

Para la comunicación con los servidores físicos u otros dispositivos del mismo nivel, el dispositivo Citrix ADC utiliza una dirección IP propiedad de Citrix como dirección IP de origen. El dispositivo Citrix ADC mantiene un conjunto de sus direcciones IP y selecciona dinámicamente una dirección IP mientras se conecta con un servidor. En función de la subred en la que se coloque el servidor físico, el dispositivo decide qué dirección IP se va a utilizar. Este grupo de direcciones se utiliza para enviar sondeos de tráfico y monitorizar.

Puede mostrar el número total de puertos libres disponibles en las direcciones IP propiedad de Citrix ADC para una nueva conexión back-end. Esta información lo ayuda a decidir la necesidad de más direcciones IP propiedad de Citrix si los puertos gratuitos disponibles están a punto de agotarse.

Puede proporcionar la siguiente información para que el dispositivo Citrix ADC calcule la cantidad total de puertos libres disponibles para una nueva conexión back-end:

- Dirección IP propiedad de Citrix (opcional)
- Dirección IP de destino
- Puerto de destino
- Protocolo TCP o no TCP

Cuando especifica toda la información, excepto especificar una dirección IP propiedad de Citrix:

- El dispositivo Citrix ADC realiza una búsqueda de ruta para encontrar todas las direcciones IP propiedad de Citrix que se pueden conectar a la dirección IP de destino. A continuación, el dispositivo busca y muestra el número total de puertos libres disponibles en estas direcciones IP propiedad de Citrix para la nueva conexión back-end especificada.

  > **Nota:**
  >
  > El dispositivo Citrix ADC no realiza una búsqueda ECMP, la ruta de búsqueda LLB o la ruta de búsqueda PBR para encontrar las direcciones IP propiedad de Citrix que se pueden conectar a la dirección IP de destino.

Cuando especifica toda la información, incluida la especificación de una dirección IP propiedad de Citrix:

- El dispositivo Citrix ADC muestra la cantidad de puertos libres disponibles en la dirección IP especificada para la nueva conexión back-end especificada.

Antes de comenzar

Antes de mostrar el número total de puertos libres disponibles para una nueva conexión de back-end, tenga en cuenta los siguientes puntos:

- El dispositivo Citrix ADC no realiza una búsqueda ECMP, la ruta de búsqueda LLB o la ruta de búsqueda PBR para encontrar las direcciones IP propiedad de Citrix que se pueden conectar a la dirección IP de destino.
- El dispositivo Citrix ADC no admite la visualización de puertos libres disponibles en una dirección IP local de enlace.

Pasos para mostrar la cantidad de puertos libres disponibles en un dispositivo Citrix ADC para una nueva conexión back-end

Para mostrar el número total de puertos libres disponibles en un dispositivo Citrix ADC para una nueva conexión back-end:

En el símbolo del sistema, escriba:

- **show portallocation** [-**srCip** \ <ip_addr|ipv6_addr>] -**DESTiP** <ip_addr|ipv6_addr> -**destPort** <port>-**protocolo** <1 for TCP, 0 for non-TCP protocol>

Ejemplo: número total de puertos libres disponibles en un dispositivo Citrix ADC independiente:

```
> show portallocation -destip 198.51.100.30 -destport 80 -protocol 1

        Freeports available : 64505
 Done


> show portallocation -srcip 192.0.2.30 -destip 198.51.100.30 -destport
    80 -protocol 1

        Freeports available for IPAddress 192.0.2.30 : 20505
 Done
<!--NeedCopy-->
```

Ejemplo: número total de puertos libres disponibles en una configuración de clúster:

El siguiente resultado de ejemplo muestra el número total de puertos libres disponibles en cada nodo de una configuración de clúster de dos nodos.


```
> show portallocation -destip 198.51.100.30 -destport 80 -protocol 1

    Node Id: 1
    Freeports available : 32321

    Node Id: 0
    Freeports available : 32184

Done
<!--NeedCopy-->
```

Supervisar el uso de puertos en un dispositivo Citrix ADC para conexiones back-end mediante SNMP

Puede usar la alarma SNMP `PORT-ALLOC-EXCEED` para supervisar el uso de puertos en un dispositivo Citrix ADC para conexiones back-end.

La alarma SNMP `PORT-ALLOC-EXCEED` incluye los parámetros `high-threshold` y `normal-threshold`, que especifican el total de puertos asignados de las direcciones IP propiedad de Citrix como porcentajes. Por ejemplo, si el parámetro `high-threshold` se establece en 90, el dispositivo Citrix ADC genera y envía mensajes de captura cuando ocurre el siguiente evento:

- cuando el porcentaje de asignación de puertos supera el 90 por ciento en cualquiera de las direcciones IP propiedad de Citrix ADC para las conexiones back-end

Las alertas SNMP lo ayudan a decidir la necesidad de más direcciones IP propiedad de Citrix si los puertos libres disponibles están a punto de agotarse.

Para supervisar el uso de puertos en un dispositivo Citrix ADC para conexiones back-end mediante SNMP

En el símbolo del sistema, escriba:

- **set snmp alarm PORT-ALLOC-EXCEED** -**logging** (ENABLED | DISABLED) -**severity** <severity> -**state** (ENABLED | DISABLED) -**thresholdValue** <positive_integer> [-**normalValue** \<positive_integer>] -**time** <secs>
- **sh snmp alarma PORT-ALLOC-EXCEED**

Ejemplo:

```
> set snmp alarm PORT-ALLOC-EXCEED -logging ENABLED  -severity Major -
    state ENABLED -thresholdValue 90 -time 1200
Done
```



```
3
4  > sh snmp alarm port-alloc-EXCEED
5
6  Alarm                   Alarm Threshold     Normal Threshold    Time
       State       Severity        Logging
7  -----                   ---------------     ----------------    ----
       --------    -------------   --------
8  1) PORT-ALLOC-EXCEED    80                  80                  7200
       ENABLED     Major           ENABLED
9  Done
10
11 <!--NeedCopy-->
```

Para obtener más información sobre la configuración de alarmas SNMP y detectores de capturas SNMP, consulte Configuración de Citrix ADC para generar capturas SNMP.

Interfaces

January 12, 2021

Antes de comenzar a configurar interfaces, decida si la configuración puede utilizar el modo de reenvío basado en Mac y habilite o inhabilite esta configuración del sistema en consecuencia. El número de interfaces de la configuración es diferente para los diferentes modelos del dispositivo Citrix ADC. Además de configurar interfaces individuales, puede agrupar lógicamente interfaces, mediante VLAN para restringir el flujo de datos dentro de un conjunto de interfaces, y puede agregar enlaces en canales. En una configuración de alta disponibilidad, puede configurar una dirección MAC virtual si es necesario. Si utiliza el modo L2, es posible que quiera modificar el envejecimiento de la tabla de puente.

Cuando finalice la configuración, decida si debe habilitar la configuración del sistema para la detección de MTU de paths. Los dispositivos Citrix ADC se pueden implementar en modo activo-activo mediante VRRP. Una implementación activa-activa, además de evitar el tiempo de inactividad, hace un uso eficiente de todos los dispositivos Citrix ADC en la implementación. Puede utilizar la herramienta Visualizador de red para ver la configuración de red de una implementación de Citrix ADC y configurar interfaces, canales, VLAN y grupos de puentes.

Configuración del reenvío basado en Mac

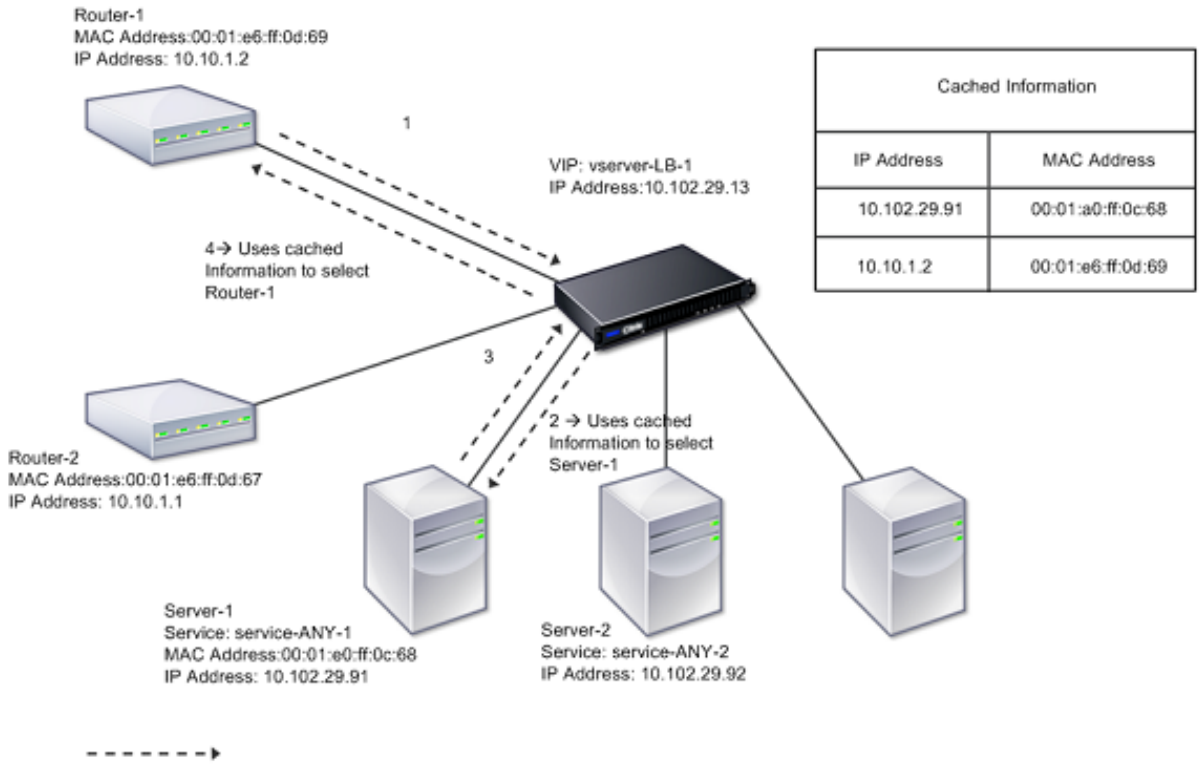
August 20, 2021

Con el reenvío basado en Mac (MBF) habilitado, cuando una solicitud llega al dispositivo Citrix ADC, el dispositivo recuerda la dirección MAC de origen de la trama y la utiliza como dirección MAC de destino para las respuestas resultantes. El reenvío basado en Mac se puede utilizar para evitar búsquedas de varias ruteas/ARP y para evitar flujos de paquetes asimétricos. El reenvío basado en Mac puede ser necesario cuando Citrix ADC está conectado a varios dispositivos con estado, como VPN o firewalls, porque garantiza que el tráfico de retorno se envíe al mismo dispositivo del que proviene el tráfico inicial.

El reenvío basado en Mac es útil cuando se utilizan dispositivos VPN, ya que garantiza que todo el tráfico que fluye a través de una VPN pasa a través del mismo dispositivo VPN.

El siguiente diagrama de topología ilustra el proceso de reenvío basado en Mac.

Ilustración 1. Modo de reenvío basado en Mac



Cuando el reenvío basado en Mac (MBF) está habilitado, Citrix ADC almacena en caché la dirección MAC de:

- El origen (un dispositivo de transmisión como un enrutador, un firewall o un dispositivo VPN) de la conexión entrante.
- El servidor que responde a las solicitudes.

Cuando un servidor responde a través del dispositivo Citrix ADC, el dispositivo establece la dirección MAC de destino del paquete de respuesta en la dirección almacenada en caché, asegurando que el tráfico fluya de manera simétrica y, a continuación, reenvía la respuesta al cliente. El proceso omite

la búsqueda de la tabla de ruta y las funciones de búsqueda ARP. Sin embargo, cuando Citrix ADC inicia una conexión, utiliza las tablas de ruta y ARP para la función de búsqueda. En una configuración de devolución directa del servidor, debe habilitar el reenvío basado en Mac.

Para obtener más información sobre las configuraciones de Direct Server Return, consulte Equilibrio de carga.

Algunas topologías de implementación pueden requerir que las rutas entrantes y salientes fluyan a través de diferentes enrutadores. El reenvío basado en Mac rompería este diseño de topología.

MBF debe inhabilitarse en las siguientes situaciones:

- **Cuando un servidor utiliza la creación de equipos de tarjetas de interfaz de red (NIC) sin utilizar LACP (802.1ad Link Aggregation).** Para habilitar el reenvío basado en Mac en esta situación, debe utilizar un dispositivo de capa 3 entre Citrix ADC y el servidor.
  Nota: MBF se puede habilitar cuando el servidor utiliza equipos NIC con LACP, ya que la interfaz virtual utiliza una dirección MAC.
- **Cuando se utiliza el clúster de firewall**. La agrupación en clústeres de firewall supone que ARP se utiliza para resolver la dirección MAC del tráfico entrante. A veces, la dirección MAC entrante puede ser una dirección MAC no agrupada y no debe utilizarse para el procesamiento de paquetes entrantes.

Cuando MBF está inhabilitado, el dispositivo utiliza conectividad L2 o L3 para reenviar las respuestas de los servidores a los clientes. Dependiendo de la tabla de rutas, los enrutadores utilizados para la conexión saliente y la conexión entrante pueden ser diferentes. En el caso de tráfico inverso (respuesta del servidor):

- Si el origen y el destino se encuentran en diferentes subredes IP, el dispositivo utiliza la búsqueda de ruta para localizar el destino.
- Si el origen se encuentra en la misma subred que el destino, Citrix ADC busca la tabla ARP para localizar la interfaz de red y reenvía el tráfico a ella. Si la tabla ARP no existe, Citrix ADC solicita las entradas ARP.

Para habilitar o inhabilitar el reenvío basado en Mac mediante la CLI:

En el símbolo del sistema, escriba:

- **enable ns mode MBF**
- **desactivar MBF modo ns**

Para habilitar o inhabilitar el reenvío basado en Mac mediante la GUI:

1. Vaya a **Sistema** > **Configuración**, en el grupo **Modos y funciones**, haga clic en **Configurar modos**.
2. Seleccione o desactive la opción de **reenvío basado en Mac**.

Reenvío basado en MAC para una configuración de equilibrio de carga

Algunas configuraciones de equilibrio de carga requieren que el dispositivo Citrix ADC omita el MBF global (si está habilitado) para estas configuraciones y, en su lugar, utilice las búsquedas de ruta/ARP para enviar paquetes al destino.

El parámetro MBF de un perfil de red se utiliza para habilitar o inhabilitar MBF para una configuración de equilibrio de carga específica. MBF se puede establecer para el lado del cliente, así como para el lado del servidor de una configuración de equilibrio de carga vinculando perfiles de red (MBF habilitado o inhabilitado) al servidor virtual y los servicios.

Por ejemplo, si un perfil de red con MBF inhabilitado está enlazado al servidor virtual de una configuración de equilibrio de carga, el dispositivo Citrix ADC omite el MBF global (si está habilitado) y, en su lugar, utiliza las búsquedas de ruta/ARP para enviar paquetes de respuesta a los clientes.

Antes de comenzar

Antes de comenzar a configurar MBF para una configuración de equilibrio de carga, tenga en cuenta los siguientes puntos:

- En una configuración de equilibrio de carga, el lado del cliente (servidor virtual) y el lado del servidor (grupos de servicio/servicio) pueden tener diferentes configuraciones de MBF.
- Una configuración de equilibrio de carga hereda la configuración global de MBF si MBF no se establece explícitamente en los perfiles de red enlazados al servidor virtual y a los servicios.
- En una configuración de equilibrio de carga, el lado del servidor (servicio) hereda la configuración de MBF del lado del cliente del perfil de red vinculado al servidor virtual si ningún perfil de red está vinculado al servicio.
- En una configuración de equilibrio de carga con modo de retorno directo del servidor, el lado del cliente hereda la configuración MBF en el perfil de red vinculado al servicio.
- En una configuración de conmutación de contenido, el lado del cliente toma la configuración MBF en el perfil de red vinculado al servidor virtual de conmutación de contenido en lugar de desde el servidor virtual de equilibrio de carga de destino.

Limitaciones

Antes de comenzar a configurar MBF para una configuración de equilibrio de carga, tenga en cuenta las siguientes limitaciones:

- La configuración de MBF para configuraciones de equilibrio de carga no se admite en una configuración de clúster.
- Para un servidor virtual de equilibrio de carga con configuración de modo MAC o L2Conn, MBF está habilitado independientemente de la configuración de MBF en el perfil de red enlazado al servidor virtual.

- El dispositivo Citrix ADC no admite la configuración de MBF para monitores de equilibrio de carga que utilicen el perfil de red. En otras palabras, la configuración MBF de un perfil de red no se aplica a los monitores a los que está vinculado el perfil de red. La configuración global de MBF se aplica a los monitores independientemente de la configuración de MBF del perfil de red enlazada.

Configurar MBF para la configuración de equilibrio de carga

La configuración de MBF para una configuración de equilibrio de carga consta de las siguientes tareas:

- Habilite el parámetro MBF en un perfil de red.
- Enlace el perfil de red a un servidor virtual de equilibrio de carga o servicios.

Para habilitar MBF en un perfil de red mediante la CLI:

- Para habilitar MBF al agregar un perfil de red, en el símbolo del sistema, escriba:
  - **add netProfile** <name> -**MBF** (**ENABLED** | **DISABLED**)
  - **show netprofile** <name>
- Para habilitar MBF en un perfil de red existente, en el símbolo del sistema, escriba:
  - **set netProfile** <name> -**MBF** (**ENABLED** | **DISABLED**)
  - **show netprofile** <name>

Para habilitar MBF en un perfil de red mediante GUI**

1. Vaya a **Sistema** > **Red** > **Perfiles de red**.
2. Habilite el parámetro **MBF** mientras agrega o modifica un perfil de red.

En la siguiente configuración de ejemplo, el perfil de red NETPROFILE-MBF-LBVS tiene MBF habilitado y está enlazado al servidor virtual de equilibrio de carga LBVS-1. Además, el perfil de red NETPROFILE-MBF-SVC tiene MBF habilitado y está vinculado a un servicio de equilibrio de carga SVC-1.

```
> add netprofile NETPROFILE-MBF-LBVS -MBF ENABLED

Done

> add netprofile NETPROFILE-MBF-SVC -MBF ENABLED

Done

> set lb vserver LBVS-1 -netprofile NETPROFILE-MBF-LBVS

Done

> set service SVC-1 -netprofile NETPROFILE-MBF-SVC
```



```
14
15 Done
16
17 <!--NeedCopy-->
```

Configurar interfaces de red

August 20, 2021

Las interfaces de red del dispositivo Citrix ADC están numeradas en notación <slot><port>. Después de configurar las interfaces, visualice las interfaces y sus parámetros para verificar la configuración. También puede mostrar esta información para solucionar un problema en la configuración.

Para administrar las interfaces de red, puede hacer lo siguiente:

- Habilite algunas interfaces e inhabilite otras.
- Restablecer una interfaz para renegociar su configuración.
- Borre las estadísticas acumuladas para una interfaz.

Para verificar la configuración, puede mostrar la configuración de la interfaz. Puede mostrar las estadísticas de una interfaz para evaluar su estado.

Establecer los parámetros de la interfaz de red

La configuración de la interfaz de red no está sincronizada ni propagada. Para un par HA, debe realizar la configuración en cada unidad de forma independiente.

Para establecer los parámetros de la interfaz de red mediante la CLI:

En el símbolo del sistema, escriba:

```
1 - set interface <id> [-speed <speed>] [-duplex <duplex>] [-flowControl
     <flowControl>] [-autoneg ( DISABLED | ENABLED )] [-haMonitor ( ON |
     OFF )] [ ( ON | OFF )] [-tagall ( ON | OFF )] [-lacpMode <lacpMode
    >] [-lacpKey<positive_integer>] [-lacpPriority <positive_integer>]
    [-lacpTimeout (LONG | SHORT )] [-ifAlias <string>] [-throughput <
    positive_integer>][-bandwidthHigh <positive_integer> [-
    bandwidthNormal <positive_integer>]]
2 - show interface [<id>]
3 <!--NeedCopy-->
```

Ejemplo:


```
> set interface 1/8 -duplex full
 Done
<!--NeedCopy-->
```

Para establecer los parámetros de la interfaz de red mediante la GUI:

Vaya a **Sistema > Red > Interfaces**, seleccione la interfaz de red que quiere modificar (por ejemplo, 1/8), haga clic en **Modificar** y, a continuación, establezca los parámetros.

Configuración del tamaño del anillo de recepción y el tipo de anillo para una interfaz

Puede aumentar el tamaño y el tipo de anillo de recepción para interfaces IX, F1X, F2X o F4X en plataformas Citrix ADC MPX y SDX.

Un mayor tamaño del anillo proporciona más amortiguación para manejar el tráfico de ráfagas, pero puede afectar el rendimiento. Se admite un tamaño de anillo de hasta 8192 para interfaces IX. Se admite un tamaño de anillo de hasta 4096 para interfaces F1X, F2X y F4X. El tamaño del anillo predeterminado sigue siendo 2048.

Los tipos de anillo de interfaz son elásticos de forma predeterminada. Aumentan o disminuyen de tamaño en función de la tasa de llegada del paquete. Puede configurar el tipo de anillo como “fijo”, en cuyo caso el tamaño del anillo no cambia según la tasa de tráfico.

Nota: Esta función es compatible con la versión 13.0 build 41.x, y es compatible con plataformas que tienen interfaces IX, F1X, F2X o F4X.

Utilice el comando `show hardware` para identificar si el dispositivo tiene interfaces IX, F1X, F2X o F4X.

Ejemplos:

El siguiente modelo tiene 16 interfaces F1X (10G) y 4 interfaces F4X (40G).

```
> sh hardware
        Platform: NSMPX-25000-40G 20\*CPU+16\*F1X+4\*F4X+2\*E1K+2*CVM
           N3 250040
        Manufactured on: 12/16/2016
        CPU: 2800MHZ
        Host Id: 234913926
        Serial no: N43RJCRV3X
        Encoded serial no: N43RJCRV3X
        Netscaler UUID: 336a32d6-2cfa-11e8-bf01-00e0ed5dd23c
        BMC Revision: 4.08
 Done
```



```
<!--NeedCopy-->
```

El siguiente modelo tiene 2 interfaces 1X (10G).

```
> sh hardware
        Platform: NSMPX-10500 8\*CPU+2\*E1K+8\*E1K+2\*IX+8*CVM 1620
           760100
        Manufactured on: 12/27/2010
        CPU: 2832MHZ
        Host Id: 1707114630
        Serial no: 7VZZV1ZXJ4
        Encoded serial no: 7VZZV1ZXJ4
        Netscaler UUID: eb1bfd72-5176-11e7-ba18-00e0ed1b0d12
 Done
<!--NeedCopy-->
```

Para configurar el tamaño y el tipo de anillo mediante la CLI
En la línea de comandos, escriba:

```
set interface <id> -ringsize <positive_integer> -ringtype ( Elastic |
   Fixed )
<!--NeedCopy-->
```

Parámetros:

`ringsize`:

El tamaño del anillo de recepción de la interfaz. Un número mayor proporciona más búferes para manejar el tráfico entrante.

Valor predeterminado: 2048 Valor
mínimo: 512 Valor
máximo: 16384

`ringtype`:

Tipo de anillo de recepción de la interfaz. Un tipo de anillo fijo preasigna el número configurado de búferes independientemente de la velocidad de tráfico. Por el contrario, un anillo elástico, se expande y se encoge en función de la tasa de tráfico entrante.

Valores posibles: Elástico, Fijo

Valor predeterminado: Elastic

Ejemplo:


```
> set interface 40/2 -ringsize 4096 -ringtype Fixed
 Done
> show interface 40/2

1)      Interface 40/2 (40G Ethernet, CR4, 40 Gbit) #21  flags=0xc020 <
    ENABLED, UP, UP, autoneg, HAMON, HEARTBEAT, 802.1q> MTU=1500, native
     vlan=10, MAC=00:e0:ed:75:14:2a, uptime 119h26m32s
        Requested: media AUTO, speed AUTO, duplex AUTO, fctl OFF,
           throughput 0
        Actual: media UTP, speed 40000, duplex FULL, fctl OFF,
           throughput 40000
        LLDP Mode: NONE, LR Priority: 1024
        RX: Pkts(1443972660032) Bytes(1457207315336105) Errs(0) Drops
           (53319) Stalls(0)
        TX: Pkts(1452311431262) Bytes(1458534011197761) Errs(0) Drops
           (788) Stalls(0)
        NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)
        Bandwidth thresholds are not set.
        Rx Ring: Configured size=4096, Actual size=4096, Type: Fixed
 Done
<!--NeedCopy-->
```

La última línea muestra el tamaño del anillo configurado y real, y el tipo de anillo.

Para configurar el tamaño y el tipo de anillo mediante la interfaz gráfica de usuario:

1. Vaya a **Sistema > Red > Interfaces**.
2. Seleccione su interfaz y haga clic en **Modificar**.
3. En **Tamaño de anillo**, especifique una de las siguientes opciones:
   - **IX interfaces:** 512, 1024, 2048, 4096 u 8192.
   - **Interfaces F1X, F2X o F4X:** 512, 1024, 2048 o 4096.
4. En **Tipo de anillo**, seleccione Elástico o Fijo.
5. Haga clic en **Aceptar**.

Habilitar e inhabilitar interfaces de red

De forma predeterminada, las interfaces de red están habilitadas. Inhabilite cualquier interfaz de red que no esté conectada a la red para que no pueda enviar ni recibir paquetes. Inhabilitar una interfaz de red conectada a la red en una configuración de alta disponibilidad puede provocar una conmutación por error.

Para obtener más información sobre la alta disponibilidad, consulte Alta disponibilidad.

Para habilitar o inhabilitar una interfaz de red mediante la CLI:

En el símbolo del sistema, escriba:

```
- enable interface <interface_num>
- show interface <interface_num>
- disable interface <interface_num>
- show interface <interface_num>
<!--NeedCopy-->
```

Ejemplo:

```
> enable interface 1/8
 Done
> show interface 1/8
        Interface 1/8 (Gig Ethernet 10/100/1000 MBits) #2
        flags=0x4004000 <ENABLED, DOWN, BOUND to LA/1, down, autoneg,
           802.1q>
        MTU=1514, MAC=00:d0:68:15:fd:3d, downtime 906h58m40s
        Requested: media UTP, speed AUTO, duplex FULL, fctl OFF,
           throughput 0
        RX: Pkts(0) Bytes(0) Errs(0) Drops(0) Stalls(0)
        TX: Pkts(0) Bytes(0) Errs(0) Drops(0) Stalls(0)
        NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)
        Bandwidth thresholds are not set.
Done
<!--NeedCopy-->
```

Para habilitar o inhabilitar una interfaz de red mediante la GUI:

1. Vaya a **Sistema > Red > Interfaces**.
2. Seleccione la interfaz de red y, en la lista **Acción**, seleccione Activar o Desactivar.

Restablecer interfaces de red

La configuración de la interfaz de red controla propiedades como dúplex y velocidad. Para renegociar la configuración de una interfaz de red, debe restablecerla.

Para restablecer una interfaz de red mediante la CLI:

En el símbolo del sistema, escriba:


```
-  reset interface <interface_num>
-  show interface <interface_num>
<!--NeedCopy-->
```

Ejemplo:

```
> reset interface 1/8
 Done
<!--NeedCopy-->
```

Para restablecer una interfaz de red mediante la GUI:

1. Vaya a **Sistema > Red > Interfaces**.
2. Seleccione la interfaz de red y, en la lista **Acción**, seleccione **Restablecer interfaz**.

Supervisar una interfaz de red

Puede mostrar estadísticas de interfaz de red para supervisar los parámetros y utilizar la información para comprobar el estado de la interfaz de red. Puede supervisar parámetros, como paquetes enviados y recibidos, rendimiento, unidades de datos del Protocolo de control agregado de enlace (LACP) y errores. Puede borrar las estadísticas de una interfaz de red para supervisar sus estadísticas desde el momento en que se borran las estadísticas.

Para mostrar las estadísticas de las interfaces de red mediante la CLI:

En el símbolo del sistema, escriba:

```
-  stat interface <interface_num>
<!--NeedCopy-->
```

Ejemplo:

```
> stat interface 1/8
 Done
<!--NeedCopy-->
```

Para borrar las estadísticas de una interfaz de red mediante la CLI:

En el símbolo del sistema, escriba:


```
-  clear interface <interface_num>
<!--NeedCopy-->
```

Ejemplo:

```
> clear interface 1/8
 Done
<!--NeedCopy-->
```

Para mostrar las estadísticas de una Interfaz mediante la GUI:

Vaya a **Sistema > Red > Interfaces**, seleccione la interfaz de red y haga clic en **Estadísticas de interfaz**.

Para borrar las estadísticas de una interfaz de red mediante la GUI:

1. Vaya a **Sistema > Red > Interfaces**.
2. Seleccione la interfaz de red y, en la lista **Acción**, seleccione **Borrar estadísticas**.

Configuración de reglas de sesión de reenvío

August 20, 2021

De forma predeterminada, el dispositivo Citrix ADC no crea entradas de sesión para el tráfico que solo reenvía (modo L3). En un caso en el que una solicitud de cliente que el dispositivo reenvíe a un servidor da como resultado una respuesta que tiene que devolver por la misma ruta de acceso, puede crear una regla de reenvío de sesión. Una regla de sesión de reenvío crea entradas de sesión de reenvío para el tráfico que se origina o está destinado a una red determinada y que el Citrix ADC reenvía. Puede crear reglas de sesión de reenvío para el tráfico IPv4, así como para el tráfico IPv6.

Al configurar una regla de sesión de reenvío IPv4, puede especificar una dirección de red IPv4 o una ACL extendida como condición para identificar el tráfico IPv4 para el que crear una entrada de sesión de reenvío:

- **Dirección de red**. Cuando especifica una dirección de red IPv4, el dispositivo crea sesiones de reenvío para el tráfico IPv4 cuyo origen o destino coincide con la dirección de red.
- **Regla ACL extendida**. Cuando especifica una regla de ACL extendida, el dispositivo crea sesiones de reenvío para el tráfico IPv4 que coincide con las condiciones especificadas en la regla de ACL extendida.

Al configurar una regla de reenvío de sesión IPv6, puede especificar un prefijo IPv6 o un ACL6 como condición para identificar el tráfico IPv6 para el que crear una entrada de sesión de reenvío:

- **Prefijo IPv6**. Cuando se especifica un prefijo IPv6, el dispositivo crea sesiones de reenvío para el tráfico IPv6 cuyo origen o destino coincide con el prefijo IPv6.
- **Regla ACL6**. Cuando se especifica una regla ACL6, el dispositivo crea sesiones de reenvío para el tráfico IPv6 que coincide con las condiciones especificadas en la regla ACL6.

Para crear una regla de sesión de reenvío IPv4 mediante la CLI:

En el símbolo del sistema, escriba los comandos siguientes para crear una regla de reenvío de sesión y compruebe la configuración:

- add forwardingSession <name>[\ ] <network><netmask>| [-aclname] <string>-connfailover (HABILITADO | DESHABILITADO)
- show forwardingSession

Ejemplo:

```
A network address as the condition:

> add forwardingSession fs-nw-1 10.102.105.51 255.255.255.255
 Done

An ACL as the condition:

> add forwardingSession fs-acl-1 acl1
 Done
<!--NeedCopy-->
```

Para configurar una regla de sesión de reenvío IPv4 mediante la GUI:

Vaya a Sistema > Red > Reenvío de sesiones, agregue una nueva sesión de reenvío IPv4 o modifique una sesión de reenvío existente.

Para crear una regla de sesión de reenvío IPv6 mediante la CLI:

- En el símbolo del sistema, escriba los comandos siguientes para crear una regla de reenvío de sesión y compruebe la configuración:
  - add ForwardingSession <name>[] <IPv6 prefix>| [-acl6name]<string>
  - show forwardingSession

  Ejemplo:

```
    An IPv6 prefix as the condition:

    > add forwardingSession fsv6-pfx-1 3ffe::/64
```



```
4       Done
5
6      An ACL6 rule as the condition:
7
8      > add forwardingSession fsv6-acl6-1  -acl6name ACL6-FS
9       Done
10 <!--NeedCopy-->
```

Para configurar una regla de sesión de reenvío IPv6 mediante la GUI:

Vaya a Sistema > Red > Reenvío de sesiones, agregue una nueva sesión de reenvío IPv6 o modifique una sesión de reenvío existente.

Asignación de una regla de ACL a una regla de sesión de reenvío existente

Puede asignar una regla de ACL a una regla de sesión de reenvío basada en dirección/prefijo IPV6, en cuyo caso se convierte en una regla de sesión de reenvío basada en ACL. También puede cambiar una regla de ACL existente a otra regla de ACL en una regla de sesión de reenvío basada en ACL. Una vez agotadas las entradas de sesión de reenvío relacionadas existentes (si las hay), las reglas comienzan a utilizar la ACL recién asignada para identificar el tráfico IPv4/IPv6 para el que se va a crear una entrada de sesión de reenvío.

Para asignar una regla de ACL extendida a una regla de sesión de reenvío IPv4 existente mediante la CLI:

En el símbolo del sistema, escriba:

- `set forwardingSession <name> [-aclname <string>]`
- `show forwardingSession <name>`

Para asignar una regla ACL6 a una regla de sesión de reenvío IPv6 existente mediante la CLI:

En el símbolo del sistema, escriba:

- `set forwardingSession <name> [-acl6name <string>]`
- `show forwardingSession <name>`

Ejemplo:

```
1 > add forwardingSession FS-1 -aclname ACL-9
2 Done
3
4 > add forwardingSession FS6-1  -acl6name ACL6-9
5 Done
```


Desactivación de la dirección para reenvío de sesiones en una configuración de clúster

El comportamiento predeterminado de un clúster de Citrix ADC es que el nodo que recibe tráfico (receptor de flujo) dirija el tráfico a otro nodo (procesador de flujo), que procesa el tráfico. Dirigir el tráfico desde el receptor de flujo al procesador de flujo se produce sobre el backplane del clúster y se denomina dirección.

La dirección puede ser una sobrecarga para el procesamiento en tiempo real o cuando la configuración incluye enlaces de alta latencia.

La dirección para las sesiones de reenvío ahora se puede desactivar para que el procesamiento se convierta en local para el receptor de flujo. Es decir, el receptor de flujo se convierte en el procesador de flujo.

Antes de comenzar

Tenga en cuenta los siguientes puntos antes de configurar reglas de sesión de reenvío en una configuración de clúster:

- Debe configurar los conjuntos de vínculos para que se utilicen para reenviar sesiones.
- Debe habilitar el reenvío basado en MAC (MBF) en la configuración del clúster.

Configuración de reglas de sesión de reenvío en una configuración de clúster

La desactivación de la dirección para reenviar reglas de sesión en una configuración de clúster se puede realizar en los dos niveles siguientes:

- **Nivel de regla de sesión de reenvío específico**. Habilite el parámetro Process Local mientras agrega una nueva regla de sesión de reenvío o modifica una regla de sesión de reenvío existente.
- A**nivel mundial**. Habilite el parámetro Process Local mientras agrega una nueva instancia de clúster o modifica una instancia de clúster existente. La configuración global tiene prioridad sobre la configuración de regla de sesión de reenvío.

Procedimientos CLI

Para inhabilitar la dirección de una regla de sesión de reenvío en una configuración de clúster mediante la CLI:

En el símbolo del sistema, escriba uno de los siguientes conjuntos de comandos:

- Si agrega una nueva regla de sesión de reenvío:
  - **add forwardingSession** <name>((<network []<netmask>) | -**acl6name** <string>| -**aclname** <string>) -**ProcessLocal ENABLED**
  - **show forwardingSession** <name>

- Si reconfigura una regla de sesión de reenvío existente:
  - **set ForwardingSession** <name> -**ProcessLocal ENABLED**
  - **show forwardingSession** <name>

Para inhabilitar la dirección para todas las reglas de sesión de reenvío (nivel global) en una configuración de clúster mediante la CLI:

En el símbolo del sistema, escriba uno de los siguientes conjuntos de comandos:

- Si agrega una nueva instancia de clúster:
  - **add cluster instance** <clid> -**processLocal Enabled**
  - **mostrar instancia de clúster** <clid>
- Si reconfigura una instancia de clúster existente:
  - **set cluster instance** <clid> -**ProcessLocal Enabled**
  - **mostrar instancia de clúster** <clid>

Configuración de ejemplo:

A continuación se presentan dos ejemplos de desactivación de la dirección en el nivel de regla de sesión de reenvío, y un ejemplo de desactivación de la dirección a nivel global.

```
An IPv4 forwarding session rule:

> add forwardingSession FWD-SESSN-PROCSS-LOCL-IPV4-1 10.102.105.51
    255.255.255.255 -processLocal Enabled
Done

An IPv6 forwarding session rule:

> add forwardingSession FWD-SESSN-PROCSS-LOCL-IPV6-1  - acl6name ACL6-
    FWD-SESSN-1 -processLocal Enabled
Done

A cluster setup, with an instance ID 10, has steering disabled at
    global level:

> set cluster instance 10 -processLocal Enabled
Done
<!--NeedCopy-->
```

Procedimientos de GUI

Para inhabilitar la dirección de una regla de sesión de reenvío en una configuración de clúster mediante la GUI:

Vaya a **Sistema** > **Red** > **Reenvío de sesiones**, seleccione **Procesar local** mientras agrega una nueva regla de sesión de reenvío o modifica una regla de sesión de reenvío existente.

Para inhabilitar la dirección para todas las reglas de sesión de reenvío (nivel global) en una configuración de clúster mediante la interfaz gráfica de usuario:

Desplácese hasta **Sistema** > **Clúster** y seleccione **Procesar local** mientras agrega una configuración de clúster o modifica una configuración de clúster existente.

Descripción de las VLAN

January 12, 2021

Un dispositivo Citrix ADC admite el puerto de Capa 2 y las VLAN etiquetadas IEEE 802.1q. Las configuraciones de VLAN son útiles cuando se necesita restringir el tráfico a determinados grupos de estaciones. Puede configurar una interfaz de red como parte de varias VLAN mediante el etiquetado IEEE 802.1q.

Puede configurar VLAN y vincularlas a subredes IP. A continuación, Citrix ADC realiza el reenvío de IP entre estas VLAN (si está configurado como el enrutador predeterminado para los hosts de estas subredes).

Citrix ADC admite los siguientes tipos de VLAN:

- **VLAN basadas en puertos.** La pertenencia a una VLAN basada en puerto se define mediante un conjunto de interfaces de red que comparten un dominio de difusión exclusivo y común de Capa 2. Puede configurar varias VLAN basadas en puertos. De forma predeterminada, todas las interfaces de red del Citrix ADC son miembros de la VLAN 1.

  Si aplica el etiquetado 802.1q al puerto, la interfaz de red pertenece a una VLAN basada en puerto. El tráfico de capa 2 se puentina dentro de una VLAN basada en puerto y las difusiones de capa 2 se envían a todos los miembros de la VLAN si el modo de capa 2 está habilitado. Cuando agrega una interfaz de red sin etiqueta como miembro de una VLAN nueva, se elimina de su VLAN actual.

- **VLAN predeterminada.** De forma predeterminada, las interfaces de red del Citrix ADC se incluyen en una única VLAN basada en puertos como interfaces de red sin etiquetas. Esta VLAN es la VLAN predeterminada. Tiene un ID de VLAN (VID) de 1. Esta VLAN existe permanentemente. No se puede eliminar y su VID no se puede cambiar.

  Cuando agrega una interfaz de red a una VLAN diferente como miembro sin etiqueta, la interfaz de red se elimina automáticamente de la VLAN predeterminada. Si desvincula una interfaz de red de su VLAN basada en puerto actual, se agrega de nuevo a la VLAN predeterminada.

- **VLAN etiquetadas.** El etiquetado 802.1q (definido en el estándar IEEE 802.1q) permite que un dispositivo de red (como Citrix ADC) agregue información a una trama en la capa 2 para identificar la pertenencia a VLAN del marco. El etiquetado permite que los entornos de red tengan VLAN que abarcan varios dispositivos. Un dispositivo que recibe el paquete lee la etiqueta y reconoce la VLAN a la que pertenece la trama. Algunos dispositivos de red no admiten recibir paquetes etiquetados y no etiquetados en la misma interfaz de red, en particular, conmutadores Force10. En tales casos, debe ponerse en contacto con el servicio de atención al cliente para obtener ayuda.

  La interfaz de red puede ser un miembro etiquetado o no etiquetado de una VLAN. Cada interfaz de red es un miembro sin etiqueta de una VLAN solamente (su VLAN nativa). Esta interfaz de red transmite las tramas de la VLAN nativa como tramas sin etiquetas. Una interfaz de red puede formar parte de más de una VLAN si las otras VLAN están etiquetadas.

  Cuando configure el etiquetado, asegúrese de que coincida con la configuración de la VLAN en ambos extremos del vínculo. El puerto al que se conecta Citrix ADC debe estar en la misma VLAN que la interfaz de red Citrix ADC.

  Nota: Esta configuración de VLAN no está sincronizada ni propagada, por lo que debe realizar la configuración en cada unidad en un par de HA de forma independiente.

Aplicación de reglas para clasificar marcos

Las VLAN tienen dos tipos de reglas para clasificar tramas:

- **Reglas de introducción.** Las reglas de introducción clasifican cada trama como perteneciente solo a una VLAN única. Cuando se recibe un marco en una interfaz de red, se aplican las siguientes reglas para clasificar el marco:
  - Si el marco no está etiquetado o tiene un valor de etiqueta igual a 0, el VID del marco se establece en el puerto VID (PVID) de la interfaz de recepción, que se clasifica como perteneciente a la VLAN nativa. (Los PVID se definen en el estándar IEEE 802.1q.)
  - Si el marco tiene un valor de etiqueta igual a FFF, el marco se elimina.
  - Si el VID de la trama especifica una VLAN de la que la interfaz de red receptora no es miembro, se elimina la trama. Por ejemplo, si un paquete se envía desde una subred asociada con el ID de VLAN 12 a una subred asociada con el ID de VLAN 10, se elimina el paquete. Si un paquete sin etiquetas con VID 9 se envía desde la subred asociada con VLAN ID 10 a una interfaz de red PVID 9, el paquete se elimina.
- **Reglas de salida.** Se aplican las siguientes reglas de salida:
  - Si el VID de la trama especifica una VLAN de la que la interfaz de red de transmisión no es miembro, se descarta la trama.

- Durante el proceso de aprendizaje (definido por el estándar IEEE 802.1q), SRC MAC y VID se utilizan para actualizar la tabla de búsqueda de bridge del Citrix ADC.
- Una trama se descarta si su VID especifica una VLAN que no tiene ningún miembro. (Los miembros se definen vinculando interfaces de red a una VLAN.)

VLAN y reenvío de paquetes en Citrix ADC

El proceso de reenvío en el dispositivo Citrix ADC es similar al de cualquier conmutador estándar. Sin embargo, Citrix ADC realiza el reenvío solo cuando el modo Capa 2 está activado. Las funciones clave del proceso de reenvío son:

- Se aplican restricciones de topología. La aplicación implica seleccionar cada interfaz de red en la VLAN como puerto de transmisión (dependiendo del estado de la interfaz de red), restricciones de conexión en puente (no reenviar en la interfaz de red receptora) y restricciones de MTU.
- Las tramas se filtran sobre la base de la información de la búsqueda de tabla de puente en la tabla de base de datos de reenvío (FDB) del Citrix ADC. La búsqueda de la tabla de puente se basa en el MAC de destino y el VID. Los paquetes dirigidos a la dirección MAC del Citrix ADC se procesan en las capas superiores.
- Todas las tramas de difusión y multidifusión se reenvían a cada interfaz de red que es miembro de la VLAN, pero el reenvío solo se produce si el modo L2 está habilitado. Si el modo L2 está inhabilitado, se descartan los paquetes de difusión y multidifusión. Esto también es cierto para las direcciones MAC que no están actualmente en la tabla de puente.
- Una entrada de VLAN tiene una lista de interfaces de red miembro que forman parte de su conjunto de miembros sin etiqueta. Al reenviar tramas a estas interfaces de red, no se inserta una etiqueta en el marco.
- Si la interfaz de red es un miembro etiquetado de esta VLAN, la etiqueta se inserta en el marco cuando se reenvía el marco.

Cuando un usuario envía paquetes de difusión o multidifusión sin identificar la VLAN, es decir, durante la detección de direcciones duplicadas (DAD) para NSIP o ND6 para el siguiente salto de la ruta, el paquete se envía en todas las interfaces de red, con el etiquetado adecuado basado en las reglas de entrada y salida. ND6 normalmente identifica una VLAN y solo se envía un paquete de datos en esta VLAN. Las VLAN basadas en puertos son comunes a IPv4 e IPv6. Para IPv6, Citrix ADC admite VLAN basadas en prefijos.

Configuración de una VLAN

August 20, 2021

Puede implementar VLAN en los siguientes entornos:

- Subred única
- Varias subredes
- LAN única
- VLAN (sin etiquetado)
- VLAN (etiquetado 802.1q)

Si configura VLAN que solo tienen interfaces de red sin etiquetar como miembros, el número total de VLAN posibles se limita al número de interfaces de red disponibles en Citrix ADC. Si se requieren más subredes IP con una configuración de VLAN, se debe utilizar el etiquetado 802.1q.

Cuando vincula una interfaz de red a una VLAN, la interfaz de red se elimina de la VLAN predeterminada. Si las interfaces de red necesitan formar parte de más de una VLAN, puede enlazar las interfaces de red a las VLAN como miembros etiquetados.

Puede configurar Citrix ADC para que reenvíe tráfico entre VLAN en la capa 3. En este caso, una VLAN está asociada a una única subred IP. Los hosts de una VLAN que pertenecen a una única subred utilizan la misma máscara de subred y una o más puertas de enlace predeterminadas conectadas a esa subred. La configuración de la capa 3 para una VLAN es opcional. La capa 3 se utiliza para el reenvío de IP (redirección entre VLAN). Cada VLAN tiene una dirección IP y una máscara de subred únicas que definen una subred IP para la VLAN. En una configuración de alta disponibilidad, esta dirección IP se comparte con los demás dispositivos Citrix ADC. Citrix ADC reenvía paquetes entre subredes IP configuradas (VLAN).

Al configurar Citrix ADC, no debe crear subredes IP superpuestas. Al hacerlo, se impide la funcionalidad de la capa 3.

Cada VLAN es un dominio de difusión único de capa 2. Dos VLAN, cada una enlazada a subredes IP separadas, no se pueden combinar en un solo dominio de difusión. El reenvío de tráfico entre dos VLAN requiere un dispositivo de reenvío (redirección) de capa 3, como el dispositivo Citrix ADC.

Configuración de VLAN en una instalación de HA

La configuración de VLAN para una configuración de alta disponibilidad requiere que los dispositivos Citrix ADC tengan la misma configuración de hardware, y las VLAN configuradas en ellos deben ser imágenes espejadas.

La configuración correcta de VLAN se implementa automáticamente cuando la configuración se sincroniza entre los dispositivos Citrix ADC. El resultado son acciones idénticas en todos los dispositivos. Por ejemplo, al agregar la interfaz de red 0/1 a VLAN2 se agrega esta interfaz de red a VLAN 2 en todos los dispositivos que participan en la configuración de alta disponibilidad.

Nota: Si utiliza comandos específicos de la interfaz de red en una configuración de alta disponibilidad, las configuraciones que cree no se propagarán al otro dispositivo Citrix ADC. Debe ejecutar estos co-

mandos en cada dispositivo de un par de alta disponibilidad para asegurarse de que la configuración de los dos dispositivos del par de alta disponibilidad permanece sincronizada.

Creación o modificación de una VLAN

Para configurar una VLAN, debe crear una entidad VLAN y, a continuación, enlazar las interfaces de red y las direcciones IP a la VLAN. Si quita una VLAN, sus interfaces miembro se agregan a la VLAN predeterminada.

Procedimientos CLI

Para crear una VLAN mediante la CLI:

En el símbolo del sistema, escriba:

- `add vlan <id> [-aliasName <string>] [-ipv6DynamicRouting (ENABLED|DISABLED)]`
- `sh vlan <id>`

Ejemplo:

```
1   > add vlan 2  - aliasName ”Network A”   Done
2 <!--NeedCopy-->
```

Para enlazar una interfaz a una VLAN mediante la CLI:

En el símbolo del sistema, escriba:

- `bind vlan <id> -ifnum <slot/port>`
- `sh vlan <id>`

Ejemplo:

```
1   > bind vlan 2 -ifnum 1/8   Done
2 <!--NeedCopy-->
```

Para enlazar una dirección IP a una VLAN mediante la CLI:

En el símbolo del sistema, escriba:

- `bind vlan <id> -IPAddress <IPAddress> <netMask>`
- `sh vlan <id>`

Ejemplo:

```
  > bind vlan 2 -IPAddress 10.102.29.54 255.255.255.0   Done
<!--NeedCopy-->
```

Para eliminar una VLAN mediante la CLI:

En el símbolo del sistema, escriba:

- `rm vlan <id>`

Procedimientos de GUI

Para configurar una VLAN mediante la GUI:

1. Vaya a Sistema > Red > VLAN, agregue una VLAN nueva o modifique una VLAN existente.
2. Para enlazar una dirección IP a una VLAN, en Enlaces IP, seleccione la opción Activo correspondiente a la dirección IP que quiere enlazar a la VLAN (por ejemplo, 10.102.29.54). La columna Tipo muestra el tipo de dirección IP (como IP asignada, IP virtual o IP de subred) para cada dirección IP de la columna Dirección IP.
3. Para enlazar una interfaz de red a una VLAN, en Vinculaciones de interfaz, seleccione la opción Activo correspondiente a la interfaz que quiere enlazar a la VLAN.

Supervisión de VLAN

Puede mostrar estadísticas de VLAN como paquetes recibidos, bytes recibidos, paquetes enviados y bytes enviados, y utilizar la información para identificar anomalías o depurar una VLAN.

Para ver las estadísticas de una VLAN mediante la CLI:

En el símbolo del sistema, escriba:

- `stat vlan <vlanID>`

Ejemplo:

```
  stat vlan 2
<!--NeedCopy-->
```

Para ver las estadísticas de una VLAN mediante la GUI:

1. Vaya a Sistema > Red > VLAN.
2. Seleccione la VLAN y haga clic en Estadísticas.

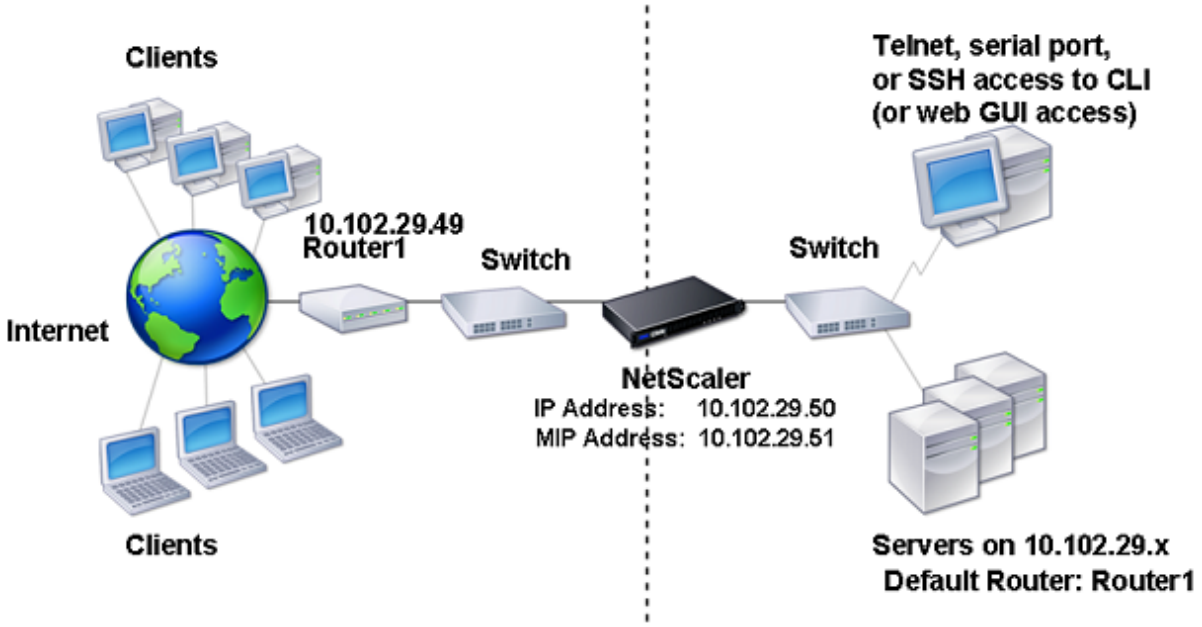
Configuración de VLAN en una única subred

August 20, 2021

Antes de configurar una VLAN en una sola subred, asegúrese de que el Modo Capa 2 está habilitado.

La siguiente ilustración muestra un entorno de subred único

Ilustración 1. VLAN en una única subred



En la ilustración anterior:

1. El enrutador predeterminado para Citrix ADC y los servidores es el enrutador 1.
2. El modo de capa 2 debe estar habilitado en Citrix ADC para que Citrix ADC tenga acceso directo a los servidores.
3. Para esta subred, se puede configurar un servidor virtual para equilibrar la carga en el dispositivo Citrix ADC.

Para configurar una VLAN en una única subred, siga los procedimientos descritos en Configuración de una VLAN.

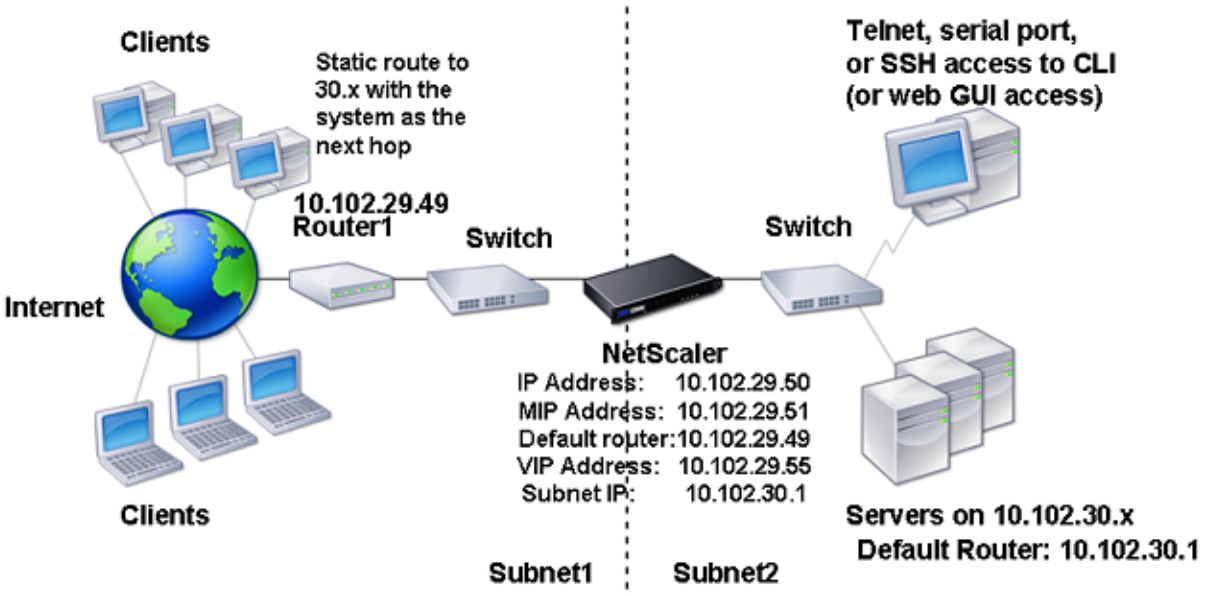
Configuración de VLAN en varias subredes

August 20, 2021

Para configurar una VLAN única en varias subredes, debe agregar un VIP para la VLAN y configurar la redirección correctamente. La siguiente ilustración muestra una única VLAN configurada en varias

subredes.

Ilustración 1. Varias subredes en una única VLAN



Para configurar una VLAN única en varias subredes, realice las siguientes tareas:

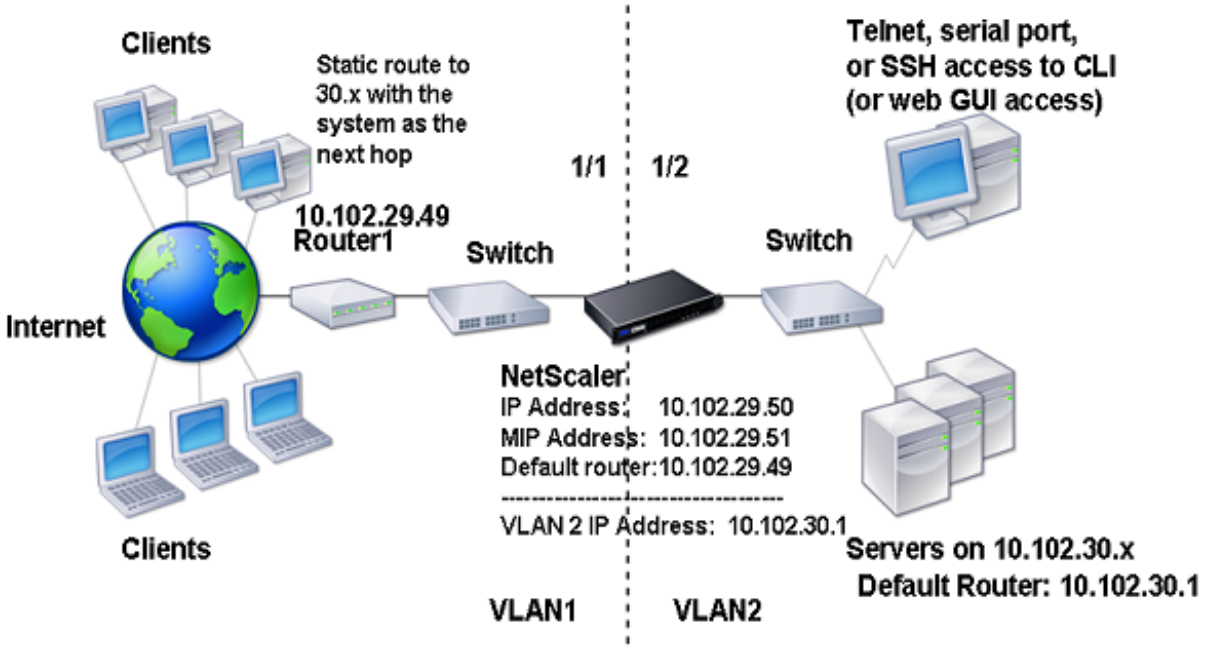
1. Inhabilite el modo Capa 2. Para obtener información sobre el procedimiento para inhabilitar el modo de capa 2, consulte Modos de reenvío de paquetes.
2. Agregar una dirección VIP. Para ver el procedimiento para agregar una dirección VIP, consulte Configuración y administración de direcciones IP virtuales (VIP).
3. Configure la regla RNAT. Para obtener información sobre el procedimiento para configurar el ID de RNAT, consulte Configuración de RNAT.

Configuración de varias VLAN sin etiquetar en varias subredes

August 20, 2021

En entornos con varias VLAN sin etiquetar en varias subredes, se configura una VLAN para cada subred IP. Una interfaz de red solo está enlazada a una VLAN. La siguiente ilustración muestra esta configuración.

Ilustración 1. Múltiples subredes con VLAN: Sin etiquetado



Para implementar la configuración mostrada en la ilustración anterior, realice las siguientes tareas:

1. Agregue VLAN 2.
2. Enlazar la interfaz de red 1/2 del Citrix ADC a la VLAN 2 como una interfaz de red sin etiquetas.
3. Enlazar la dirección IP y la máscara de subred a la VLAN 2.

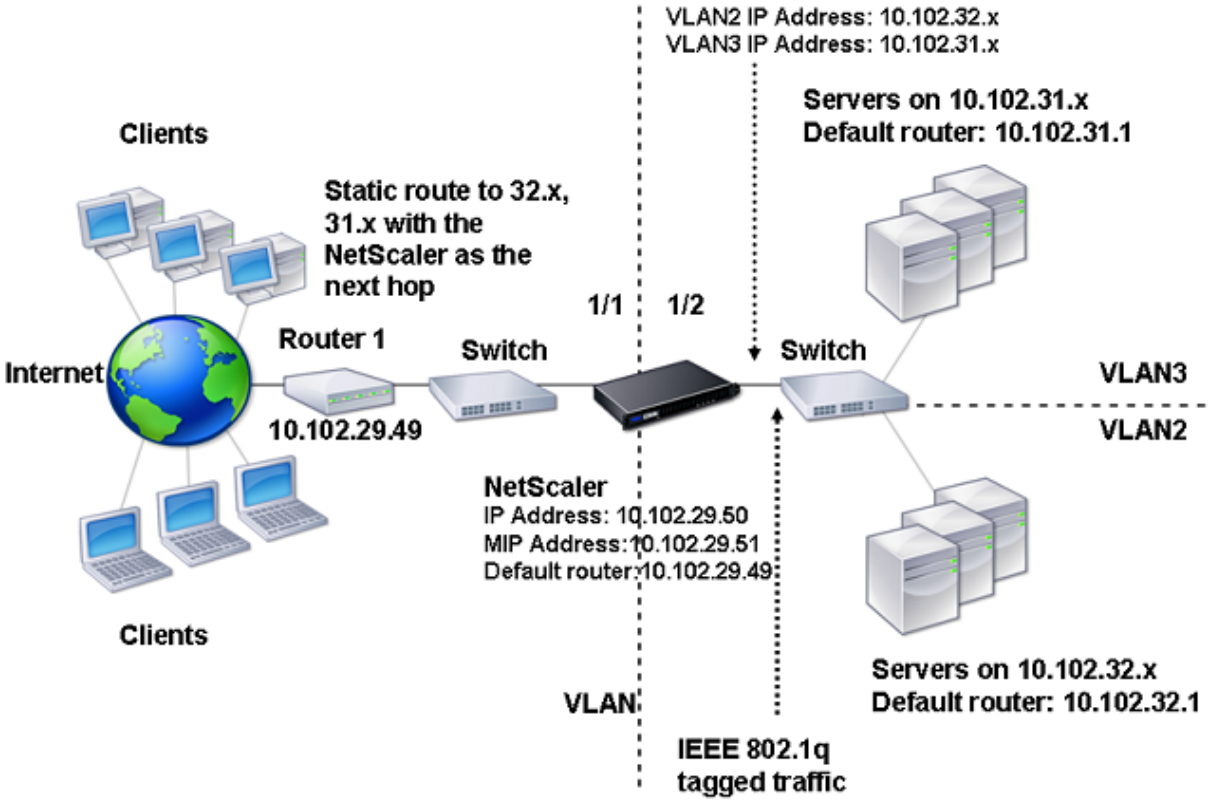
Para obtener información sobre los procedimientos sobre estas tareas, consulte Configuración de una VLAN.

Configuración de varias VLAN con etiquetado 802.1q

August 20, 2021

Para varias VLAN con etiquetado 802.1q, cada VLAN se configura con una subred IP diferente. Cada interfaz de red está en una VLAN. Una de las VLAN está configurada como etiquetada. La siguiente ilustración muestra esta configuración.

Ilustración 1. Varias VLAN con etiquetado IEEE 802.1q



Para implementar la configuración mostrada en la ilustración anterior, realice las siguientes tareas:

1. Agregue VLAN 2.
2. Enlazar la interfaz de red 1/2 del Citrix ADC a la VLAN 2 como una interfaz de red sin etiquetas.
3. Enlazar la dirección IP y la máscara de red a VLAN 2.
4. Agregue VLAN 3.
5. Enlazar la interfaz de red 1/2 del Citrix ADC a la VLAN 3 como una interfaz de red etiquetada.
6. Enlazar la dirección IP y la máscara de red a VLAN 3.

Para obtener información sobre los procedimientos sobre estas tareas, consulte Configuración de una VLAN.

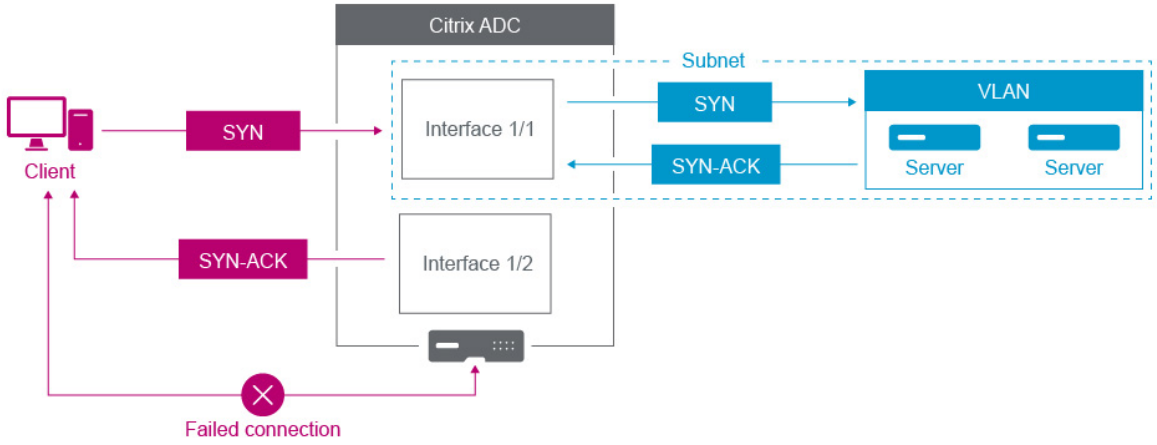
Asociar una subred IP a una interfaz Citrix ADC mediante VLAN

August 20, 2021

Por defecto, un dispositivo Citrix ADC no proporciona ninguna diferenciación entre interfaces de red. El dispositivo funciona más como un concentrador de red que como un conmutador. Esto puede conducir a bucles de red de Capa 3 donde el tráfico duplicado se transmite en varias interfaces.

En tales casos, dependiendo del diseño de la red, es posible que una solicitud se transmita en una

interfaz y que la respuesta correspondiente se reciba en una interfaz diferente.



Por ejemplo, un paquete SYN enviado en una interfaz y la respuesta SYN-ACK recibida en una interfaz diferente pueden dar lugar a un error en la conexión, ya que el dispositivo espera recibir el SYN-ACK en la misma interfaz que envió el paquete SYN original.

Para resolver estos problemas, el dispositivo puede utilizar VLAN internas o externas para asociar subredes específicas con interfaces.

Antes de comenzar

Antes de comenzar a asociar una subred IP con una interfaz Citrix ADC mediante VLAN, tenga en cuenta los siguientes puntos:

- La conectividad de red podría perderse accidentalmente al asociar una VLAN a la subred o interfaz que se está usando actualmente para acceder a la interfaz de línea de comandos o a la interfaz de línea de comandos de Citrix ADC. Por lo tanto, en tales situaciones, se recomienda encarecidamente que el cambio se realice accediendo a la interfaz de línea de comandos a través de la consola serie de un dispositivo Citrix ADC físico o a través de la consola serie virtual de un dispositivo Citrix ADC VPX.
- Las interfaces de administración de Citrix ADC carecen de ciertas funciones de optimización de hardware, lo que las hace menos deseables para su uso con tráfico de datos de producción. Por lo tanto, se recomienda configurar Citrix ADC para que solo utilice las interfaces de administración para el tráfico de administración (NSIP). En la configuración predeterminada, no hay diferenciación lógica entre las interfaces de administración y las interfaces de datos en un NetScaler de hardware. Para lograr este objetivo, se recomienda que el NSIP esté en una VLAN separada del tráfico de datos, lo que permite que el tráfico de administración esté en una interfaz separada.

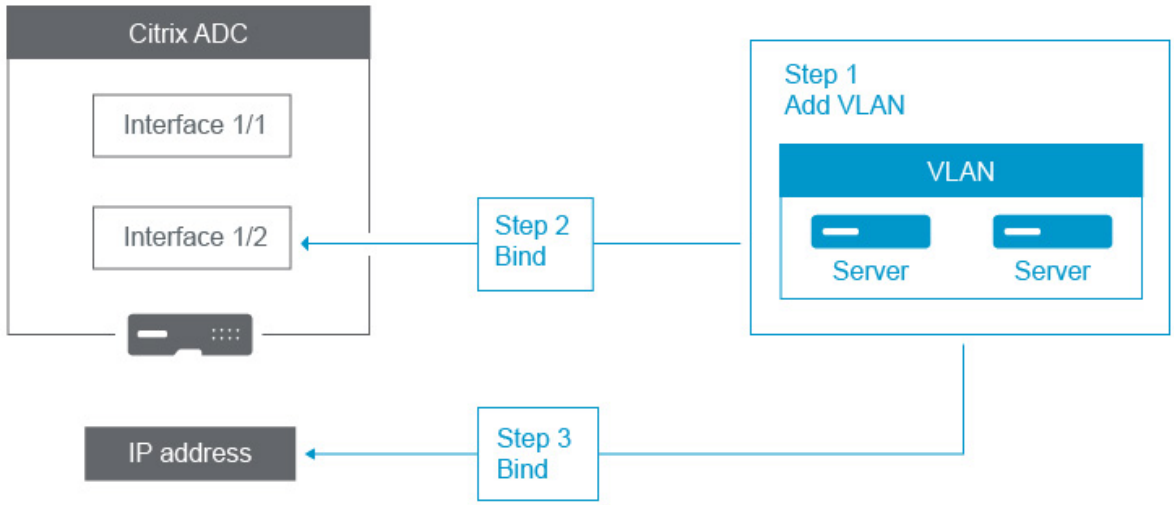
  Aunque el concepto es el mismo, para cambiar las asociaciones VLAN de la subred que contiene la dirección NSIP, debe configurar NSVLAN en lugar de las instrucciones siguientes. Dichos cam-

bios también requerirán un reinicio del Citrix ADC para que surtan efecto. Para obtener más información, consulte Configuración de NSVLAN.

- En Citrix ADC SDX, se recomienda encarecidamente que el NSIP de cada instancia esté en la misma subred y VLAN que el SVM (Management Service GUI) y XenServer de SDX. El SVM se comunica con instancias a través de la red. Si el SVM, XenServer y las instancias no se encuentran en la misma VLAN y subred, el tráfico de administración debe fluir fuera del SDX. En esta situación, los problemas de red pueden hacer que el estado de la instancia aparezca como amarillo o rojo y pueden impedir los cambios de administración y configuración de las instancias de Citrix ADC.

Pasos de configuración

Asociar una subred IP a una interfaz Citrix ADC consta de las siguientes tareas:



Agregue una VLAN. Al agregar una VLAN, si está etiquetando la VLAN, debe seleccionar un número de VLAN definido en el conmutador de red para el puerto del conmutador asociado. Si la VLAN no está etiquetada y es interna en el dispositivo, se recomienda seleccionar el número de VLAN disponible en la configuración del conmutador para facilitar la consulta.

Enlazar una interfaz a la VLAN. Durante el enlace, si utiliza Agregación de enlaces, asocie la VLAN con el canal LA (por ejemplo, LA/1) en lugar de la interfaz física. La VLAN debe estar asociada a una sola interfaz de red.

Si quiere etiquetar el tráfico en la interfaz, utilice la opción etiquetada (Etiqueta). De lo contrario, el tráfico deja el dispositivo sin etiquetar y se asocia con la VLAN nativa del puerto del conmutador.

Enlazar una dirección IP a la VLAN. Al enlazar, si vincula más de una dirección IP de la misma subred, se produce un error. Cuando una dirección IP está asociada a una VLAN, todas las direcciones IP de esa subred se asocian automáticamente a la VLAN.

> **Nota:**
>
> En una configuración de alta disponibilidad (HA), estas configuraciones de VLAN se agregan automáticamente desde el nodo principal al nodo secundario durante la sincronización de alta disponibilidad. Para obtener más información sobre las configuraciones de alta disponibilidad, consulte Alta disponibilidad.

Procedimientos CLI

Para agregar una VLAN mediante la CLI:

En el símbolo del sistema, escriba:

- **add vlan** <id>
- **sh vlan** <id>

Para enlazar una interfaz a una VLAN mediante la CLI:

En el símbolo del sistema, escriba:

- **bind vlan** <slot/port> <id> -**ifnum**
- **sh vlan** <id>

Para enlazar una dirección IP a una VLAN mediante la CLI:

En el símbolo del sistema, escriba:

- **bind vlan** <IPAddress> <netMask> <id> -**Dirección IP**
- **sh vlan** <id>

Ejemplo:

```
> add vlan 100

> bind vlan 100 -ifnum 1/1

> bind vlan 100 -ipAddress 10.0.1.0 255.255.255.0
<!--NeedCopy-->
```

Procedimientos de GUI

Para configurar una VLAN mediante la GUI:

1. Vaya a **Sistema** > **Red** > **VLAN**, agregue una VLAN nueva.
2. Para enlazar una interfaz de red a una VLAN, en **Enlaces de interfaz**, seleccione la opción **Activa** correspondiente a la interfaz que desea enlazar a la VLAN.

3. Para vincular una dirección IP a una VLAN, en **Enlaces IP**, seleccione la opción **Activo** correspondiente a la dirección IP que desea enlazar a la VLAN (por ejemplo, 10.102.29.54). La columna **Tipo** muestra el tipo de dirección IP para cada dirección IP en la columna **Dirección IP**.

Prácticas recomendadas para redes de dispositivos Citrix ADC y VLAN

August 20, 2021

Un dispositivo Citrix ADC utiliza VLAN para determinar qué interfaz se debe utilizar para qué tráfico. Además, el dispositivo Citrix ADC no participa en el árbol de expansión. Sin la configuración adecuada de VLAN, el dispositivo Citrix ADC no puede determinar qué interfaz usar y puede funcionar más como un HUB que un conmutador o un enrutador. En otras palabras, el dispositivo Citrix ADC puede utilizar todas las interfaces para cada conversación.

Síntomas de una configuración incorrecta de VLAN

El problema de configuración incorrecta de VLAN puede manifestarse de muchas formas, incluidos problemas de rendimiento, incapacidad para establecer conexiones, sesiones desconectadas aleatoriamente y, en situaciones graves, interrupciones de red aparentemente no relacionadas con el propio dispositivo Citrix ADC. El dispositivo Citrix ADC también puede informar sobre movimientos de MAC, interfaces silenciadas y/o transferencia o recepción de desbordamientos de búfer de interfaz de administración, dependiendo de la naturaleza exacta de la interacción con la red.

Mover MAC (contador nic_tot_bdg_mac_move): Este problema indica que el dispositivo Citrix ADC está usando más de una interfaz para comunicarse con el mismo dispositivo (dirección MAC), ya que no pudo determinar correctamente qué interfaz usar.

Interfaces silenciadas (contador nic_err_bdg_muted): este problema indica que el dispositivo Citrix ADC ha detectado que está creando un bucle de redirección debido a problemas de configuración de VLAN y, como tal, ha apagado una o varias de las interfaces ofensivas para evitar una red corte de suministro.

Desbordos de búfer de interfaz, que normalmente se refieren a interfaces de administración (contador nic_err_tx_overflow):Esteproblema puede ser causado si se transmite demasiado tráfico a través de una interfaz de administración. Las interfaces de administración del dispositivo Citrix ADC no están diseñadas para gestionar grandes volúmenes de tráfico, lo que puede deberse a configuraciones incorrectas de red y VLAN que activen el dispositivo Citrix ADC para utilizar una interfaz de administración para el tráfico de datos de producción. Esto ocurre a menudo porque el dispositivo Citrix ADC no tiene forma de diferenciar el tráfico en la VLAN/subred del NSIP (NSVLAN) del tráfico de producción normal. Se recomienda encarecidamente que el NSIP esté en una VLAN y una subred independientes de cualquier dispositivo de producción, como estaciones de trabajo y servidores.

ACK huérfanos (counter tcp_err_orphan_ack): Este problema indica que el dispositivo Citrix ADC recibió un paquete ACK que no esperaba, normalmente en una interfaz diferente a la del tráfico ACK'd originado. Esta situación puede deberse a configuraciones incorrectas de VLAN en las que el dispositivo Citrix ADC transmite en una interfaz diferente a la que el dispositivo de destino utiliza normalmente para comunicarse con el dispositivo Citrix ADC (que suele verse junto con movimientos MAC)

Altas tasas de retransmisiones o renuncias de retransmisión (contadores: Tcp_err_retransmit_giveups, tcp_err_7th_retransmit, varios otros contadores de retransmisión): El dispositivo Citrix ADC intenta retransmitir un paquete TCP un total de 7 veces antes de que abandone y termine la conexión. Aunque esta situación puede deberse a condiciones de red, a menudo ocurre como resultado de una mala configuración de la VLAN y de la interfaz.

Cerebro dividido de alta disponibilidad: Cerebro dividido es una condición en la que ambos nodos de alta disponibilidad creen que son primarios, lo que da lugar a duplicaciones de direcciones IP y a la pérdida de funcionalidad del dispositivo Citrix ADC. Esto se debe a que los dos nodos de alta disponibilidad no pueden comunicarse entre sí mediante Heartbeats de alta disponibilidad en el puerto UDP 3003 mediante el NSIP, a través de cualquier interfaz. Esto suele deberse a configuraciones incorrectas de VLAN en las que la VLAN nativa de las interfaces del dispositivo Citrix ADC no tiene conectividad entre dispositivos Citrix ADC.

Prácticas recomendadas para configuraciones de red y VLAN

1. Cada subred debe estar asociada a una VLAN.
2. Se puede asociar más de una subred a la misma VLAN (dependiendo del diseño de la red).
3. Cada VLAN debe estar asociada a una sola interfaz (para fines de esta discusión, un canal LA cuenta como una única interfaz).
4. Si necesita que se asocie más de una subred a una interfaz, las subredes deben etiquetarse.
5. Contrariamente a la creencia popular, la función de reenvío basado en Mac (MBF) del dispositivo Citrix ADC no está diseñada para mitigar este tipo de problema. MBF está diseñado principalmente para el modo DSR (retorno directo del servidor) del dispositivo Citrix ADC, que rara vez se utiliza en la mayoría de los entornos (está diseñado para permitir que el tráfico omita deliberadamente el dispositivo Citrix ADC en la ruta de retorno desde los servidores back-end). MBF puede ocultar problemas de VLAN en algunas instancias, pero no debe ser utilizado para resolver este tipo de problema.
6. Cada interfaz del dispositivo Citrix ADC requiere una VLAN nativa (a diferencia de Cisco, donde las VLAN nativas son opcionales), aunque la configuración TagAll de una interfaz se puede utilizar para que ningún tráfico sin etiquetar salga de la interfaz en cuestión.
7. La VLAN nativa se puede etiquetar si es necesario para el diseño de su red (esta es la opción TagAll para la interfaz).

8. La VLAN de la subred del NSIP del dispositivo Citrix ADC es un caso especial. Esto se llama NSVLAN. Los conceptos son los mismos, pero los comandos para configurarlo son diferentes y los cambios en NSVLAN requieren un reinicio del dispositivo Citrix ADC para surtir efecto. Si intenta vincular una VLAN a un SNIP que comparte la misma subred que el NSIP, obtendrá "Operación no permitida". Esto se debe a que debe usar los comandos NSVLAN en su lugar. Además, en algunas versiones de firmware, no se puede establecer un NSVLAN si ese número de VLAN existe mediante el comando `add VLAN`. Simplemente elimine la VLAN y vuelva a establecer la NSVLAN.

9. Los latidos de alta disponibilidad siempre usan la VLAN nativa de la interfaz respectiva (etiquetada opcionalmente si la opción TagAll está configurada en la interfaz).

10. Debe haber comunicación entre al menos un conjunto de VLAN nativas en los dos nodos de un par de alta disponibilidad (esto puede ser directo o a través de un router). Las VLAN nativas se utilizan para los latidos de alta disponibilidad. Si los dispositivos Citrix ADC no pueden comunicarse entre VLAN nativas en ninguna interfaz, esto dará lugar a fallas de alta disponibilidad y posiblemente a una situación de cerebro dividido en la que ambos dispositivos Citrix ADC creen que son primarios (dando lugar a direcciones IP duplicadas, entre otras cosas).

11. El dispositivo Citrix ADC no participa en el árbol de expansión. Por lo tanto, no es posible utilizar el árbol de expansión para proporcionar redundancia de interfaz cuando se utiliza un dispositivo Citrix ADC. En su lugar, utilice un formulario de agregación de enlaces (LACP o LAG manual) para este fin.

    Nota: Si quiere tener agregación de enlaces entre varios conmutadores físicos, debe tener los conmutadores configurados como un conmutador virtual, mediante una función como la pila de conmutadores de Cisco.

12. La sincronización de alta disponibilidad y el comando Propagación, de forma predeterminada, utilizan NSIP/NSVLAN. Para separarlos en una VLAN diferente, puede utilizar la opción SyncVLAN del comando `set HA node`.

13. No hay nada integrado en la configuración predeterminada del dispositivo Citrix ADC que denote que una interfaz de administración (0/1 ó 0/2) está restringida únicamente al tráfico de administración. Esta restricción debe ser impuesta por el usuario final a través de la configuración de VLAN. Las interfaces de administración no están diseñadas para manejar el tráfico de datos, por lo que el diseño de la red debe tener en cuenta este punto. Las interfaces de administración, contenidas en la placa base del dispositivo Citrix ADC, carecen de varias funciones de descarga, como descarga de CRC, búferes de paquetes más grandes y otras optimizaciones, lo que las hace mucho menos eficientes en el manejo de grandes cantidades de tráfico. Para separar los datos de producción y el tráfico de administración, el NSIP no debe estar en la misma subnet/VLAN que el tráfico de datos.

14. Si se quiere utilizar una interfaz de administración para transportar tráfico de administración,

es recomendable que la ruta predeterminada esté en una subred que no sea la subred del NSIP (NSVLAN).

En muchas configuraciones, se utiliza la ruta predeterminada para la comunicación de estaciones de trabajo (en un caso de Internet). Si la ruta predeterminada está en la misma subred que el NSIP, el dispositivo ADC puede utilizar la interfaz de administración para enviar y recibir tráfico de datos. Este uso del tráfico de datos puede sobrecargar la interfaz de administración.

15. Además, un SDX: SVM, XenServer y todos los NSIP de instancias de Citrix ADC deben estar en la misma VLAN y subred. No hay ningún **backplane** en el dispositivo SDX que permita la comunicación entre SVM/Xen/instancias. Si no están en la misma VLAN/subnet/interfaz, el tráfico entre ellos debe salir del hardware físico, ser enrutado en la red y regresar.

    Esta configuración puede provocar problemas obvios de conectividad entre las instancias y SVM y, como tal, no se recomienda. Un síntoma común de esto es un indicador de estado de instancia amarilla en el SVM para la instancia VPX en cuestión y la imposibilidad de utilizar el SVM para reconfigurar una instancia VPX.

16. Si algunas VLAN están enlazadas a subredes y otras no, durante una conmutación por error de alta disponibilidad, los paquetes GARP no se envían para ninguna dirección IP en ninguna de las subredes que no están enlazadas a una VLAN. Esta configuración puede causar problemas de conectividad y conexiones descartadas durante los failovers de alta disponibilidad. Este problema se debe a que el dispositivo Citrix ADC no puede notificar el cambio de direcciones IP de propiedad MAC de red en dispositivos Citrix ADC no configurados con VMAC.

    Los síntomas de esto son que durante o después de una conmutación por error de alta disponibilidad, el contador ip_tot_floating_ip_err se incrementa en el anterior dispositivo Citrix ADC principal durante más de unos segundos, lo que indica que la red no recibió ni procesó paquetes GARP y que la red continúa transmitiendo datos al nuevo dispositivo Citrix ADC secundario.

Configuración de NSVLAN

August 20, 2021

NSVLAN es una VLAN a la que está enlazada la subred de la dirección IP de administración de Citrix ADC (NSIP). La subred NSIP solo está disponible en interfaces asociadas con NSVLAN. De forma predeterminada, NSVLAN es VLAN 1, pero puede designar una VLAN diferente como NSVLAN. Si lo hace, debe reiniciar el dispositivo Citrix ADC para que el cambio surta efecto. Después del reinicio, el tráfico de subred NSIP se restringe al nuevo NSVLAN.

El tráfico de la subred IP de Citrix ADC se puede etiquetar (802.1q) con el ID de VLAN especificado para NSVLAN. Debe configurar la interfaz del conmutador conectada para etiquetar y permitir este mismo

ID de VLAN en la interfaz conectada. Si quita la configuración de NSVLAN, la subred NSIP se enlazará automáticamente a la VLAN 1, restaurando la NSVLAN predeterminada.

Para configurar NSVLAN mediante la CLI:

En el símbolo del sistema, escriba:

- set ns config -nsvlan <positive_integer>-ifnum<interface_name>… [-tagged (SÍ | NO)]
- mostrar configuración ns

  Nota: La configuración surtirá efecto después de reiniciar el dispositivo Citrix ADC.

Ejemplo:

```
> set ns config -nsvlan 300 -ifnum 1/1 1/2 1/3 -tagged NO
 Done

> save config
 Done
<!--NeedCopy-->
```

Para restaurar la configuración predeterminada de NSVLAN mediante la CLI:

En el símbolo del sistema, escriba:

- unset ns config -nsvlan
- mostrar configuración ns

Ejemplo:

```
> unset ns config -nsvlan
 Done
<!--NeedCopy-->
```

Para configurar NSVLAN mediante la GUI:

Vaya a Sistema > Configuración, en el grupo Configuración, haga clic en Cambiar configuración de NSVLAN.

Configuración de la MTU en la NSVLAN

De forma predeterminada, la MTU de la NSVLAN se establece en 1500 bytes. Puede modificar esta configuración para optimizar el rendimiento de la red y de la red. Por ejemplo, puede configurar NSVLAN para procesar tramas jumbo.

Para establecer la MTU de la NSVLAN mediante la CLI:

En el símbolo del sistema, escriba:

- **set vlan** <positive_integer> <id> **-mtu**
- **mostrar vlan** <id>

Para establecer la MTU de la NSVLAN mediante la GUI:

Vaya a **Sistema** > **Red** > **VLAN**, abra NSVLAN y establezca el parámetro **Unidad de transmisión máxima**.

Configuración de ejemplo:

En la siguiente configuración de ejemplo, VLAN 100 es NSVLAN.

```
> set ns config -nsvlan 100 -ifnum 1/1 -tagged no

  Warning: The configuration must be saved and the system rebooted for
      these settings to take effect

> set vlan 100 -mtu 1600

  Done

> sh vlan

  1)  VLAN ID: 1

      Link-local IPv6 addr:
    fe80::947b:52ff:fead:12d5/64

      Interfaces : 1/2 LO/1

  2)  VLAN ID: 100    VLAN Alias Name:

      MTU: 1600

      Interfaces : 1/1

      IPs :

          10.102.53.114     Mask: 255.255.255.0

  Done

```



```
30 > save config
31
32   Done
33 <!--NeedCopy-->
```

Configuración de la Lista de VLAN Permitida

August 20, 2021

Citrix ADC acepta y envía paquetes etiquetados de una VLAN en una interfaz si la VLAN está configurada explícitamente en el dispositivo Citrix ADC y la interfaz está enlazada a la VLAN. Algunas implementaciones (por ejemplo, Bump in the wire) requieren que el dispositivo Citrix ADC funcione como un dispositivo transparente para aceptar y reenviar paquetes etiquetados relacionados con un gran número de VLAN. Para este requisito, configurar y administrar un gran número de VLAN no es una solución viable.

La lista de VLAN permitidas en una interfaz especifica una lista de VLAN. La interfaz acepta y envía de forma transparente paquetes etiquetados relacionados con las VLAN especificadas sin necesidad de configurar explícitamente estas VLAN en el dispositivo.

Puntos a tener en cuenta antes de configurar la lista de VLAN permitida

Tenga en cuenta los siguientes puntos antes de configurar la lista de VLAN permitida

- En una configuración de alta disponibilidad, la lista de VLAN permitida no se propaga ni sincroniza. Por lo tanto, debe configurar la lista de VLAN permitida en ambos nodos.
- El tráfico de una VLAN nativa puede filtrarse a las interfaces que no son miembros que especifican la VLAN nativa en su lista de VLAN permitida.
- Se puede especificar un máximo de 60 rangos de VLAN como parte de la lista de VLAN permitida para una interfaz.
- El dispositivo Citrix ADC no admite la lista de VLAN permitida en interfaces que forman parte de canales de agregación de enlaces o conjuntos de interfaces redundantes. Para obtener más información sobre el conjunto de interfaces redundantes, consulte Conjunto de interfaces redundantes.
- La lista de VLAN permitida no se admite en una configuración de clúster de Citrix ADC.
- El dispositivo Citrix ADC no admite la lista de VLAN permitida para grupos Bridge.
- El dispositivo Citrix ADC no admite la lista de VLAN permitida para VXLAN.

Configuración de la Lista de VLAN Permitida

Para configurar la lista de VLAN permitida mediante la CLI:

En el símbolo del sistema, escriba:

- **set interface** <id **-trunkmode** (ON|OFF) **-TrunkAllowedVLAN** <int XMLMASKPLACEHOLDER6 - int XMLMASKPLACEHOLDER2 >…[]
- **show interface** <id>

Para configurar la lista de VLAN permitida mediante la GUI:

Vaya a **Sistema** > **Red** > **Interfaces**, seleccione una interfaz de red, haga clic en **Modificar** y, a continuación, establezca los siguientes parámetros:

- Modo troncal
- VLAN troncal permitida

Configuración de ejemplo:

En la siguiente configuración de ejemplo, las VLAN en los rangos 100-120, 190-200 y 300-330 se especifican como parte de la lista de VLAN permitida para la interfaz 1/2.

```
> set int 1/2 -trunkmode on -trunkallowedVlan 100-120 190-200 300-330

Done

> sh int 1/2

1)      Interface 1/2 (Gig Ethernet 10/100/1000 MBits) #6
        flags=0xc020

        <ENABLED, UP, UP, AUTONEG OFF, HEARTBEAT, 802.1q, trunkmode>

        Trunk Allowed Vlans:  100-120 190-200 300-330

Done

<!--NeedCopy-->
```

Configuración de grupos de puentes

August 20, 2021

Normalmente, cuando quiere combinar dos o más VLAN en un solo dominio, cambia la configuración de VLAN en todos los dispositivos de los dominios separados. Esto puede ser una tarea tediosa. Para combinar más fácilmente varias VLAN en un único dominio de difusión, puede utilizar grupos de puente.

La función de grupos de puentes funciona de la misma manera que una VLAN. Se pueden enlazar varias VLAN a un único grupo de puentes y todas las VLAN vinculadas al mismo grupo de puentes forman un único dominio de difusión. Solo puede enlazar VLAN de capa 2 a un grupo de puentes. Para la funcionalidad de Capa 3, debe asignar una dirección IP a un grupo de puentes.

En el modo de capa 2, un paquete de difusión recibido en una interfaz que pertenece a una VLAN determinada se conecta en puente a otras VLAN que pertenecen al mismo grupo de puentes. En el caso de un paquete de unidifusión, el dispositivo Citrix ADC busca en su tabla de puente las direcciones MAC aprendidas de todas las VLAN pertenecientes al mismo grupo de puentes.

En el modo de reenvío de capa 3, una subred IP está enlazada a un grupo de puentes. Citrix ADC acepta paquetes entrantes que pertenecen a la subred enlazada y reenvía los paquetes solo en las VLAN enlazadas al grupo de puentes.

La redirección IPv6 se puede habilitar en un grupo de puentes configurado.

> **Nota**
>
> La función Bridge Group y el modo Bridge BPDU no pueden funcionar juntos.

Pasos de configuración

Realice los siguientes pasos para configurar un grupo de puentes:

- Activar modo Capa 2
- Agregar un grupo de puentes y enlazar VLAN al grupo de puentes

Procedimientos CLI

Para habilitar el modo Capa 2 mediante la CLI:
En el símbolo del sistema, escriba:

- **habilitar el modo ns l2**
- **show ns mode**

Para agregar un grupo de puentes y enlazar VLAN mediante la CLI:

En el símbolo del sistema, escriba:

- **add bridgegroup** <id>[-**Redirección dinámica** IPv6(**HABILITADO** | **DESHABILITADO**)]
- **enlazar grupo de puentes** <positive_integer> <id> -**vlan**
- **show bridgegroup** <id>

Ejemplo:

```
> add bridgegroup 12
 Done
<!--NeedCopy-->
```

Para eliminar un grupo de puentes mediante la CLI:

En el símbolo del sistema, escriba:

- **rm bridgggroup** <id>

Ejemplo:

```
 rm bridgegroup 12
<!--NeedCopy-->
```

Procedimientos de GUI

Para configurar un grupo de puentes mediante la GUI:

Vaya a **Sistema** > **Red** > **Grupos de puentes**, agregue un nuevo grupo de puentes y vincule las VLAN al grupo de puentes, o modifique un grupo de puentes existente.

Configuración de MAC virtuales

August 20, 2021

Los nodos primario y secundario en una configuración de alta disponibilidad (HA) comparten la entidad flotante de dirección MAC virtual. El nodo principal posee las direcciones IP flotantes (como MIP, SNIP y VIP) y responde a las solicitudes ARP para estas direcciones IP con su propia dirección MAC. Por lo tanto, la tabla ARP de un dispositivo externo, como un enrutador ascendente, se actualiza con la dirección IP flotante y la dirección MAC del nodo principal.

Cuando se produce una conmutación por error, el nodo secundario se hace cargo como el nuevo nodo principal. El nodo secundario anterior utiliza ARP Gratuitous (GARP) para anunciar las direcciones IP flotantes que había aprendido del nodo principal antiguo. La dirección MAC que anuncia el nuevo nodo principal es la dirección MAC de su propia interfaz de red. Algunos dispositivos (algunos routers) no aceptan estos mensajes GARP. Por lo tanto, estos dispositivos externos conservan la asignación de

direcciones IP a MAC que el nodo principal anterior había anunciado. Esto puede provocar que un sitio GSLB se vaya abajo.

Por lo tanto, debe configurar un MAC virtual en ambos nodos de un par HA. Esto significa que ambos nodos tienen direcciones MAC idénticas. Cuando se produce una conmutación por error, la dirección MAC del nodo secundario permanece sin cambios y no es necesario actualizar las tablas ARP de los dispositivos externos.

Para obtener información sobre los procedimientos para configurar un MAC virtual, consulte Configuración de direcciones MAC virtuales.

Configuración de la agregación de vínculos

August 20, 2021

La agregación de enlaces combina datos procedentes de varios puertos en un único enlace de alta velocidad. La configuración de la agregación de vínculos aumenta la capacidad y la disponibilidad del canal de comunicación entre el dispositivo Citrix ADC y otros dispositivos conectados. Un enlace agregado también se conoce como un "canal". Puede configurar los canales manualmente o puede usar el Protocolo de control de agregación de vínculos (LACP). No se puede aplicar LACP a un canal configurado manualmente, ni tampoco se puede configurar manualmente un canal creado por LACP.

Cuando una interfaz de red está enlazada a un canal, los parámetros del canal tienen prioridad sobre los parámetros de la interfaz de red (es decir, los parámetros de la interfaz de red se ignoran). Una interfaz de red solo puede enlazarse a un canal.

Cuando una interfaz de red está enlazada a un canal, descarta su configuración de VLAN. Cuando las interfaces de red están enlazadas a un canal, ya sea manualmente o mediante LACP, se eliminan de las VLAN a las que pertenecían originalmente y se agregan a la VLAN predeterminada. Sin embargo, puede enlazar el canal a la VLAN antigua o a una nueva. Por ejemplo, si vincula las interfaces de red 1/2 y 1/3 a una VLAN con ID 2 y, a continuación, las vincula a un canal LA/1, las interfaces de red se mueven a la VLAN predeterminada, pero puede volver a vincularlas a VLAN 2.

Configuración Manual de Agregación de Enlaces

Cuando se crea un canal de agregación de vínculos, su estado es DOWN hasta que se une una interfaz activa a él. Puede modificar un canal en cualquier momento. Puede eliminar canales, o puede activar/desactivarlos.

Procedimientos CLI

Para crear un canal de agregación de enlaces mediante la CLI:

En el símbolo del sistema, escriba:

- agregar canal <id>[-ifnum<interfaceName>…] [-state (HABILITADO | DESHABILITADO)] [-speed] <speed>[-FlowControl] [-Hamonitor (ACTIVADO | DESACTIVADO)][-tagall (ON | OFF)] [-ifAlias] <string>[-throughput] <positive_integer>[-bandwidthHigh <positive_integer>[- Ancho de banda Normal]<positive_integer>]
- show channel

Ejemplo:

```
> add channel LA/1 -ifnum 1/8
Done
<!--NeedCopy-->
```

Para enlazar una interfaz o desvincular una interfaz de un canal de agregación de vínculos existente mediante la CLI:

En el símbolo del sistema, escriba uno de los siguientes comandos:

- bind channel <id> <interfaceName>
- unbind channel <id> <interfaceName>

Ejemplo:

```
bind channel LA/1 1/8
<!--NeedCopy-->
```

Para modificar un canal de agregación de enlaces mediante la CLI:

En el símbolo del sistema, escriba el comando
set channel, el ID del canal y los parámetros que se van a cambiar, con sus nuevos valores.

Para eliminar un canal de agregación de enlaces mediante la CLI:

Importante: Cuando se elimina un canal, las interfaces de red enlazadas a él inducen bucles de red que disminuyen el rendimiento de la red. Debe inhabilitar las interfaces de red antes de quitar el canal.

En el símbolo del sistema, escriba:

- <id>canal rm

Ejemplo:


```
> rm channel LA/1
 Done
<!--NeedCopy-->
```

Procedimientos de GUI

Para configurar un canal de agregación de enlaces mediante la GUI:

Vaya a Sistema > Red > Canales, agregue un canal nuevo o modifique un canal existente.

Para eliminar un canal de agregación de enlaces mediante la GUI:

> **Importante:**
>
> Cuando se elimina un canal, las interfaces de red enlazadas a él inducen bucles de red que disminuyen el rendimiento de la red. Debe inhabilitar las interfaces de red antes de quitar el canal.

Vaya a Sistema > Red > Canales, seleccione el canal que quiere eliminar y haga clic en Eliminar.

Configuración de la Agregación de Enlaces mediante el Protocolo de Control de Agregación de Enlaces

El Protocolo de control de agregación de enlaces (LACP) permite a los dispositivos de red intercambiar información de agregación de enlaces mediante el intercambio de unidades de datos LACP (LACPDU). Por lo tanto, no puede habilitar LACP en interfaces de red que son miembros de un canal creado manualmente.

Cuando se utiliza LACP para configurar la agregación de vínculos, se utilizan distintos comandos y parámetros para modificar los canales de agregación de vínculos que para crear canales de agregación de vínculos. Para eliminar un canal, debe inhabilitar LACP en todas las interfaces que forman parte del canal.

Nota: En una configuración de alta disponibilidad, las configuraciones LACP no se propagan ni sincronizan.

Configuración de la prioridad del sistema LACP

La prioridad del sistema LACP determina qué dispositivo del mismo nivel de un canal LA LACP puede tener control sobre el canal LA. Este número se aplica globalmente a todos los canales LACP del dispositivo. Cuanto menor sea el valor, mayor será la prioridad.

Para configurar la prioridad del sistema LACP mediante la CLI:

En el símbolo del sistema, escriba los comandos siguientes para establecer la prioridad de un dispositivo independiente y comprobar la configuración:

- <positive_integer>set lacp -Syspriority
- show lacp

Ejemplo:

```
set lacp -sysPriority 50
<!--NeedCopy-->
```

Para establecer la prioridad de un nodo de clúster específico, inicie sesión en la dirección IP del clúster y, en el símbolo del sistema, escriba los comandos siguientes:

- <positive_integer>set lacp -syspriority <positive_integer> -ownerNode
- show lacp

Ejemplo:

```
set lacp -sysPriority 50 -ownerNode 2
<!--NeedCopy-->
```

Para configurar la prioridad del sistema LACP mediante la GUI:

1. Vaya a Sistema > Red > Interfaces y, en la lista Acción, seleccione Establecer LACP.
2. Especifique la prioridad del sistema y el nodo propietario (aplicable solo para una configuración de clúster).

Creación de canales de agregación de vínculos

Para crear un canal de agregación de enlaces mediante LACP, debe habilitar LACP y especificar la misma clave LACP en cada interfaz que quiera formar parte del canal. Por ejemplo, si habilita LACP y establece la clave LACP en 3 en las interfaces 1/1 y 1/2, se crea un canal de agregación de enlaces LA/3 y las interfaces 1/1 y 1/2 se vinculan automáticamente a él.

Nota:

- Al habilitar LACP en una interfaz de red, debe especificar la clave LACP.
- De forma predeterminada, LACP está inhabilitado en todas las interfaces de red.

Para crear un canal LACP mediante la CLI:

En el símbolo del sistema, escriba:

- set interface <id>[-LACPMode] <lacpMode>[-LACPKey] <positive_integer>[-LACPPriority] <positive_integer>[-LACPTimeout (LARGO | CORTO)]
- mostrar interfaz []<id>

Para crear un canal LACP mediante la GUI:

Vaya a Sistema > Red > Interfaces, abra la interfaz de red y defina los parámetros.

Modificación de canales de agregación de vínculos

Después de crear un canal LACP especificando interfaces, puede modificar las propiedades del canal.

Para modificar un canal LACP mediante la CLI:

En el símbolo del sistema, escriba:

- set channel <id>[-ifnum<interfaceName>…] [-state (HABILITADO | DESHABILITADO)] [-speed] [-FlowControl] [-hamonitor (ACTIVADO | DESACTIVADO)] [-ifAlias] [-throughput] [-tagall (ACTIVADO | DESACTIVADO)] [-bandwidthHigh <positive_integer>[- Ancho de banda Normal]]
- show channel

Ejemplo:

```
> set channel LA/3 -state ENABLED -speed 10000
 Done
<!--NeedCopy-->
```

Para modificar un canal LACP mediante la GUI:

Vaya a Sistema > Red > Canales y modifique un canal LACP existente.

Eliminación de un canal de agregación de enlaces

Para eliminar un canal de agregación de enlaces que se creó mediante LACP, debe inhabilitar LACP en todas las interfaces que forman parte del canal.

Para eliminar un canal LACP mediante la CLI:

En el símbolo del sistema, escriba:

- set interface <id> -lacpMode Disable
- mostrar interfaz []

Para eliminar un canal LACP mediante la GUI:

Vaya a Sistema > Red > Interfaces, abra la interfaz de red y desactive la opción Habilitar LACP.

Redundancia de enlaces mediante canales LACP

La redundancia de vínculos mediante canales LACP permite al Citrix ADC dividir un canal LACP en subcanales lógicos, con un subcanal activo y los demás en modo de espera. Si el subcanal activo no alcanza un umbral mínimo de rendimiento, uno de los subcanales en espera se activa y se hace cargo.

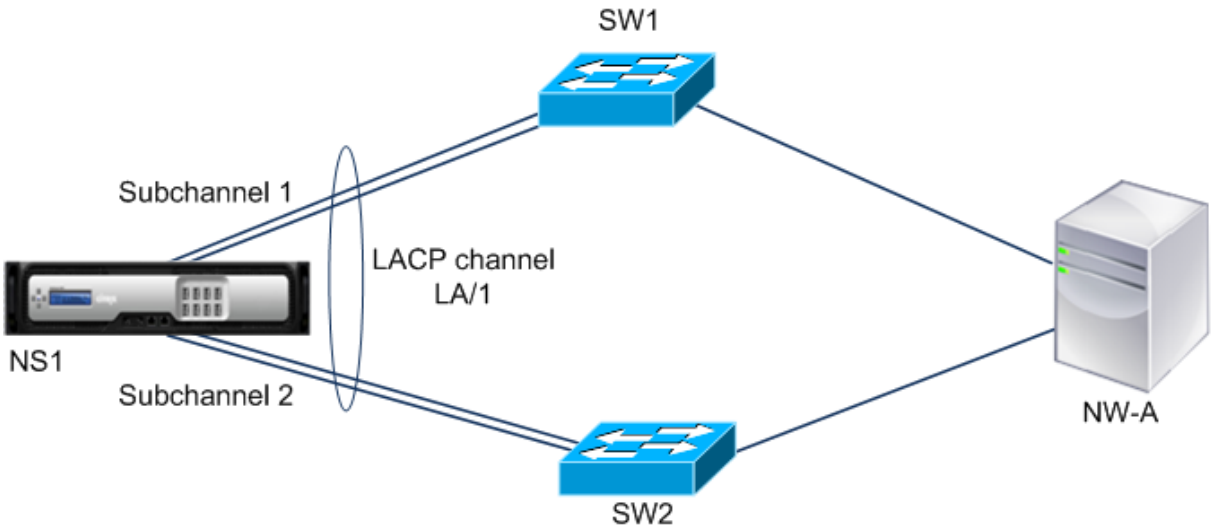
Un subcanal se crea a partir de vínculos que forman parte del canal LACP y están conectados a un dispositivo determinado. Por ejemplo, para un canal LACP con cuatro interfaces en un dispositivo Citrix ADC, con dos de las interfaces conectadas al dispositivo A y las otras dos conectadas al dispositivo B, el ADC crea dos subcanales lógicos, un subcanal con dos vínculos al dispositivo A y otro subcanal con dos vínculos al dispositivo B.

Para configurar la redundancia de enlace para un canal LACP, establezca el parámetro LRminThroughput, que especifica el umbral de rendimiento mínimo (en Mbps) que debe cumplir el subcanal activo. Al establecer este parámetro, se crean automáticamente los subcanales. Cuando el rendimiento máximo admitido del canal activo cae por debajo del valor LRminThroughput, se produce la conmutación por error de enlace y se activa un subcanal en espera.

Si desestablece el parámetro LRminThroughput de un canal LACP, o establece el valor en cero, la redundancia de vínculo para ese canal está inhabilitada, que es la configuración predeterminada.

Ejemplo

Considere un ejemplo de redundancia de vínculos configurada entre Citrix ADC NS1 y los conmutadores SW1 y SW2.



NS1 está conectado al dispositivo de red NW-A a través de SW1 y SW2.
En NS1, el canal LACP LA/1 se crea a partir de interfaces 1/1, 1/2, 1/3 y 1/4. Las interfaces 1/1 y 1/2 de NS1 están conectadas a SW1, y las interfaces 1/3 y 1/4 están conectadas a SW2. Cada uno de los cuatro enlaces admite un rendimiento máximo de 1000 Mbps.

Cuando el parámetro LRminThroughput se establece en algún valor (digamos 2000), NS1 crea dos subcanales lógicos a partir de LA/1, un subcanal (digamos subcanal 1) mediante interfaces 1/1 y 1/2 (conectado a SW1), y el otro subcanal (subcanal 2) mediante interfaces 1/3 y 1/4 (conectado a SW2).

NS1 aplica un algoritmo para activar un subcanal (por ejemplo, el subcanal 1) y poner el otro en espera. NS1 y el dispositivo de red NW-A son accesibles entre sí a través del subcanal activo.

Digamos que el subcanal 1 está activo y su rendimiento máximo admitido cae por debajo del valor LRminThroughput (por ejemplo, uno de sus enlaces falla y el rendimiento máximo admitido cae a 1000 Mbps). El subcanal 2 se activa y se hace cargo.

Redundancia de enlaces mediante canales LACP en una configuración de alta disponibilidad

En una configuración de alta disponibilidad (HA), si quiere configurar la conmutación por error de alta disponibilidad basada en rendimiento (parámetro de rendimiento) y la redundancia de enlace (parámetro LRminThroughput) en un canal LACP, debe establecer el parámetro de rendimiento en un valor menor o igual que el del parámetro LRminThroughput.

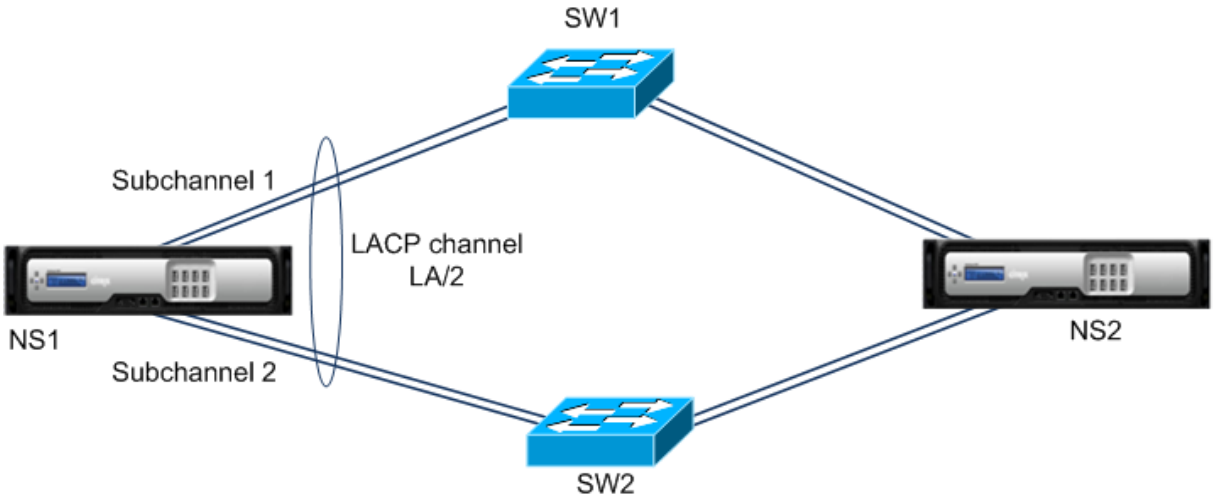
El rendimiento máximo admitido de un canal LACP se calcula como el rendimiento máximo admitido del subcanal activo.

Si el valor del parámetro de rendimiento es igual o menor que el valor del parámetro lrminthroughput, la conmutación por error de alta disponibilidad se produce cuando las dos condiciones siguientes existen al mismo tiempo:

- Ninguno de los rendimientos máximos admitidos de los subcanales cumple el valor del parámetro LRminThroughput.
- El rendimiento máximo soportado del canal LACP no cumple con el valor del parámetro de rendimiento

Considere un ejemplo de configuración de alta disponibilidad que tiene Citrix ADC NS1 y NS2, con conmutadores SW1 y SW2. NS1 está conectado a NS2 a través de SW1 y SW2.

En NS1, el canal LACP LA/1 se crea a partir de interfaces 1/1, 1/2, 1/3 y 1/4. Las interfaces 1/1 y 1/2 de NS1 están conectadas a SW1, y las interfaces 1/3 y 1/4 están conectadas a SW2. Cada uno de los cuatro enlaces admite un rendimiento máximo de 1000 Mbps.



A continuación se presentan los parámetros de LACP en este ejemplo:

Parámetro	Valor
Rendimiento	2000
Rendimiento mínimo	2000

NS1 forma dos subcanales de LA/1, un subcanal (por ejemplo, subcanal 1) mediante interfaces 1/1 y 1/2 (conectado a SW1), y el otro subcanal (subcanal 2) mediante interfaces 1/3 y 1/4 (conectado a SW2). Cada uno de los dos subcanales admite un rendimiento máximo de 2000 Mbps. Al aplicar un algoritmo, NS1 activa un subcanal (por ejemplo, el subcanal 1) y el otro en espera.

Digamos que el subcanal 1 está activo y su rendimiento máximo admitido cae por debajo del valor LRminThroughput (por ejemplo, uno de sus enlaces falla y el rendimiento máximo admitido cae a 1000 Mbps). El subcanal 2 se activa y se hace cargo. La conmutación por error de HA no se produce, porque el rendimiento máximo soportado del canal LACP no es inferior al valor del parámetro de rendimiento:

Rendimiento máximo admitido del canal LACP = Rendimiento máximo admitido del canal activo = Rendimiento máximo admitido del subcanal 2 = 2000 Mbps

Si el rendimiento máximo soportado del subcanal 2 también cae por debajo del valor lrminthroughput (por ejemplo, uno de sus enlaces falla y el rendimiento máximo soportado cae a 1000 Mbps), se produce una conmutación por error de HA, porque el rendimiento máximo soportado del canal LACP es entonces menor que el parámetro de rendimiento valor:

Configurar redundancia de vínculos mediante canales LACP

Para configurar la redundancia de vínculos para un canal LACP mediante la CLI:

En el símbolo del sistema, escriba los siguientes comandos para configurar el canal y verificar la configuración:

- **establecer canal** <positive_integer> <id> -lrminRendimiento
- **show channel**

Ejemplo:

```
> set channel la/1 -lrMinThroughput 2000
Done
> set channel la/2 -throughput 2000 -lrMinThroughput 2000
Done
<!--NeedCopy-->
```

Para configurar la redundancia de vínculos para un canal LACP mediante GUI

1. Vaya a Sistema > Red > Canales.
2. En el panel de detalles, seleccione un canal LACP para el que quiere configurar la redundancia de vínculos y, a continuación, haga clic en Modificar.
3. En el cuadro de diálogo Configurar canal LACP, defina el parámetro LRminThroughput.
4. Haga clic en Cerrar.

Conjunto de interfaces redundantes

January 12, 2021

Un conjunto de interfaces redundantes es un conjunto de interfaces donde una de las interfaces está activa y las restantes están en espera. Si la interfaz activa falla, una de las interfaces en espera se hace cargo y se activa.

Los siguientes son los principales beneficios del uso de conjuntos de interfaces redundantes:

- Un conjunto de interfaces redundantes garantiza la fiabilidad de la conexión entre el dispositivo Citrix ADC y un dispositivo del mismo nivel al proporcionar vínculos de copia de seguridad entre ellos.
- A diferencia de la redundancia de enlaces que utiliza LACP, no se requiere configuración en el dispositivo del mismo nivel para un conjunto de interfaces redundantes. Para el dispositivo del mismo nivel, el conjunto de interfaces redundantes aparece como interfaces individuales y no como un conjunto o colección.
- En una configuración de alta disponibilidad (HA), los conjuntos de interfaces redundantes pueden minimizar el número de conmutaciones de HA.

> **Nota**
>
> El conjunto de interfaces redundantes se conocía anteriormente como ‘paquete NIC ‘cuando se introdujo por primera vez en la versión 10.5.

Cómo funciona el conjunto de interfaces redundantes

Para un conjunto de interfaces redundantes, el dispositivo Citrix ADC deriva una dirección MAC sobre la base de un algoritmo interno y la asigna al conjunto de interfaces redundantes. Esta dirección MAC es compartida por todas las interfaces miembros y solo la utiliza la interfaz activa a la vez. La interfaz activa transmite mensajes GARP, que contiene la dirección MAC asignada al conjunto de interfaces redundantes y no la dirección MAC física propia de la interfaz. Cuando la interfaz activa actual falla y es tomada por otra interfaz, la nueva interfaz activa envía mensajes GARP. El dispositivo del mismo nivel actualiza su tabla de reenvío con la nueva información de la interfaz activa. Las interfaces en espera no envían ningún mensaje GARP. Las interfaces en espera no envían ningún paquete y descartan los paquetes que reciben.

En un conjunto de interfaces redundantes, la selección de la interfaz miembro como activa se basa en cualquiera de los siguientes factores:

- **Prioridad de interfaz redundante**. Este es un parámetro de una interfaz y define la prioridad de la interfaz en un conjunto de interfaces redundantes para la selección de miembros activos. Este parámetro especifica un entero positivo. Bajar el valor por encima de la prioridad de la selección de miembros activos. La interfaz miembro con la prioridad más alta (valor más bajo) se selecciona como interfaz activa del conjunto de interfaces redundantes.
- **Orden de enlace de las interfaces de miembro**. Si todas las interfaces miembro tienen la misma prioridad de interfaz redundante, la interfaz miembro enlazada primero al conjunto de interfaces redundantes se selecciona como interfaz activa del conjunto de interfaces redundantes.

En un conjunto de interfaces redundantes, la selección de interfaz activa se activa en uno de los siguientes eventos:

- Cuando se produce un error en la interfaz activa actual o se inhabilita.
- Cuando se establece la prioridad de una interfaz en espera en un valor inferior al de la interfaz activa actual. La interfaz en espera toma el control como interfaz activa.
- Cuando se vincula una interfaz cuya prioridad es menor que la de la interfaz activa actual. La interfaz recién enlazada toma el relevo como interfaz activa.

Puntos a tener en cuenta para configurar conjuntos de interfaces redundantes

Tenga en cuenta los siguientes puntos antes de configurar un conjunto de interfaces redundantes:

- En un dispositivo independiente o en un dispositivo con una configuración de alta disponibilidad, se especifica un conjunto redundante de vínculo en notación LR/X, donde X puede variar de 1 a 4. Por ejemplo, LR/1.
- En una configuración de alta disponibilidad, las configuraciones de conjuntos de interfaces redundantes no se propagan ni sincronizan con el nodo secundario.
- Puede configurar un máximo de cuatro conjuntos de interfaces redundantes en un dispositivo Citrix ADC.
- Puede enlazar un máximo de 16 interfaces a un conjunto de interfaces redundantes.
- Las interfaces miembros de un conjunto de interfaces redundantes no se pueden enlazar a otro conjunto de interfaces redundantes.
- Las interfaces miembro de un conjunto de interfaces redundantes no se pueden enlazar a un canal agregado de enlaces (LA).
- Los canales LA no se pueden enlazar a un conjunto de interfaces redundantes.
- Los conjuntos de interfaces redundantes no se pueden enlazar a un canal LA.
- En una configuración de clúster:
  - Los conjuntos de interfaces redundantes no se pueden enlazar a una agregación de vínculos de clúster.
  - Un conjunto redundante de enlace se especifica en la notación N/LR/X (por ejemplo, 1/LR/3). Donde:
    N es el ID del nodo del clúster en el que se va a crear el conjunto de interfaces redundantes.
    X es un identificador de conjunto redundante de vínculo en un nodo de clúster. X puede variar de 1 a 4.
  - Una agregación de vínculos de clúster no se puede enlazar a un conjunto de interfaces redundantes.
  - Un conjunto de interfaces redundantes solo puede incluir las interfaces del nodo al que pertenece el conjunto de interfaces redundantes.
  - Una configuración de conjunto de redundancia elink existente en un dispositivo independiente cambia automáticamente a la notación de clúster (N/LR/X) después de agregar el dispositivo a una configuración de clúster.

Pasos de configuración

La configuración del conjunto de interfaces redundantes en un dispositivo Citrix ADC consta de las siguientes tareas:

- **Cree un conjunto de interfaces redundantes**. Utilice la operación de comando channel para crear un conjunto de interfaces redundantes.

  En un dispositivo independiente o en un dispositivo con una configuración de alta disponibilidad, se especifica un conjunto redundante de vínculo en notación LR/X, donde X puede variar de 1 a 4. Por ejemplo, LR/1.

En una configuración de clúster, se especifica un conjunto redundante de vínculo en N/LR/X (por ejemplo, 1/LR/3), donde: N es el ID del nodo de clúster en el que se va a crear el conjunto de interfaces redundantes, X es el identificador de conjunto redundante de vínculo en un nodo de clúster. X puede variar de 1 a 4.

- **Enlazar interfaces al conjunto de interfaces redundantes**. Asocie las interfaces deseadas con el conjunto de interfaces redundantes. Una interfaz no puede formar parte de varios conjuntos de interfaces redundantes.
- **(Opcional) Establezca una prioridad de interfaz redundante en la interfaz miembro**. Utilice la operación de comando interface para establecer la prioridad de interfaz redundante en una interfaz miembro deseada de un conjunto de interfaces redundantes.

Para crear un conjunto de interfaces redundantes mediante la CLI:

En el símbolo del sistema:

- add channel <ID>
- show channel <ID>

Para enlazar interfaces a una interfaz redundante establecida mediante la CLI:

En el símbolo del sistema:

- <ID> <ifnum>canal de enlace
- show channel <ID>

Para establecer una prioridad de interfaz redundante de una interfaz mediante la CLI:

En el símbolo del sistema:

- <positive_integer>establecer interfaz <ID> -lrsetpriority
- show interface <ID>

Ejemplo de configuración 1:

En el ejemplo siguiente, se crea el conjunto de interfaces redundantes LR/1 y las interfaces 1/1, 1/2, 1/3 y 1/4 están enlazadas a LR/1. La prioridad de interfaz redundante se establece en un valor predeterminado de 1024 para todas estas interfaces miembro. La salida del comando show channel muestra que la interfaz 1/1 es la interfaz activa actual para la interfaz redundante set lr/1.

```
1 > add channel lr/1
2  Done
3 > bind channel lr/1 1/1 1/2 1/3 1/4
4  Done
5 > show channel
6 1)    Interface LR/1 (Link Redundant) #23
7         flags=0x100c020 <ENABLED, UP, LINKREDUNDANT, UP, HAMON, 802.1q>
```



```
        MTU=1500, native vlan=1, MAC=36:97:a2:b7:6b:a9, uptime 0h00m00s
        Requested: media NONE, speed AUTO, duplex NONE, fctl OFF,
                 throughput 0
        Actual: throughput 1000
        LLDP Mode: NONE,
        RX: Pkts(1) Bytes(52) Errs(0) Drops(1) Stalls(0)
        TX: Pkts(2) Bytes(84) Errs(0) Drops(4) Stalls(0)
        NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)
        Bandwidth thresholds are not set.
                1/1: UTP-1000-FULL-OFF          UP  0h14m06s    LR
                   Active Member
                1/2: UTP-1000-FULL-OFF          UP  0h14m06s    LR
                   Inactive Member
                1/3: UTP-1000-FULL-OFF          UP  0h14m06s    LR
                   Inactive Member
                1/4: UTP-1000-FULL-OFF          UP  0h14m06s    LR
                   Inactive Member
Done
<!--NeedCopy-->
```

Ejemplo de configuración 2:

En el ejemplo siguiente, la prioridad de interfaz redundante de la interfaz miembro 1/4 se establece en 100, que es menor que la prioridad de interfaz redundante establecida de todas las demás interfaces miembro de LR/1.

La salida del comando show channel muestra que la interfaz 1/4 es la interfaz activa actual para el conjunto de interfaces redundantes LR/1.

```
> set interface 1/4 -lrsetPriority 100
Done
> show channel
1)      Interface LR/1 (Link Redundant) #23
        flags=0x100c020 <ENABLED, UP, LINKREDUNDANT, UP, HAMON, 802.1q>
        MTU=1500, native vlan=1, MAC=36:97:a2:b7:6b:a9, uptime 0h00m00s
        Requested: media NONE, speed AUTO, duplex NONE, fctl OFF,
                 throughput 0
        Actual: throughput 1000
        LLDP Mode: NONE,
        RX: Pkts(1) Bytes(52) Errs(0) Drops(1) Stalls(0)
        TX: Pkts(2) Bytes(84) Errs(0) Drops(4) Stalls(0)
        NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)
        Bandwidth thresholds are not set.
                1/1: UTP-1000-FULL-OFF          UP  0h14m06s    LR
```



```
                    Inactive Member
16                  1/2: UTP-1000-FULL-OFF          UP  0h14m06s    LR
                    Inactive Member
17                  1/3: UTP-1000-FULL-OFF          UP  0h14m06s    LR
                    Inactive Member
18                  1/4: UTP-1000-FULL-OFF          UP  0h14m06s    LR
                    Active Member
19 Done
20 <!--NeedCopy-->
```

Ejemplo de configuración 3:

Considere una configuración de clúster de cuatro nodos N1, N2, N3 y N4. En este ejemplo, el conjunto de interfaces redundantes 1/LR/3 se crea en el nodo N1 y las interfaces 1/1/1, 1/1/2 y 1/1/3 están enlazadas a él. La prioridad de interfaz redundante se establece en un valor predeterminado de 1024 para todas estas interfaces miembro. La salida del comando show channel indica que la interfaz 1/1/1 es la interfaz activa actual para el conjunto de interfaces redundantes 1/LR/3.

```
1     > add channel 1/LR/3
2
3     Done
4     > bind channel 1/LR/3 1/1/1 1/1/2 1/1/3
5
6     Done
7     > show channel
8     1)    Interface 1/LR/3 (Link Redundant) #14
9             flags=0x100c020 <ENABLED, UP, LINKREDUNDANT, UP, HAMON,
                 802.1q>
10            MTU=1500, native vlan=1, MAC=36:97:a2:b7:6b:a9, uptime 0
                 h00m00s
11            Requested: media NONE, speed AUTO, duplex NONE, fctl OFF,
12            throughput 0
13            Actual: throughput 1000
14            LLDP Mode: NONE,
15            RX: Pkts(66) Bytes(4406) Errs(0) Drops(82) Stalls(0)
16            TX: Pkts(55) Bytes(2626) Errs(0) Drops(145) Stalls(0)
17            NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted
                 (0)
18            Bandwidth thresholds are not set.
19
20            1/1/1: UTP-1000-FULL-OFF UP  0h14m06s LR Active Member
21            1/1/2: UTP-1000-FULL-OFF UP  0h14m06s LR Inactive Member
22            1/1/3: UTP-1000-FULL-OFF UP  0h14m06s LR Inactive Member
```



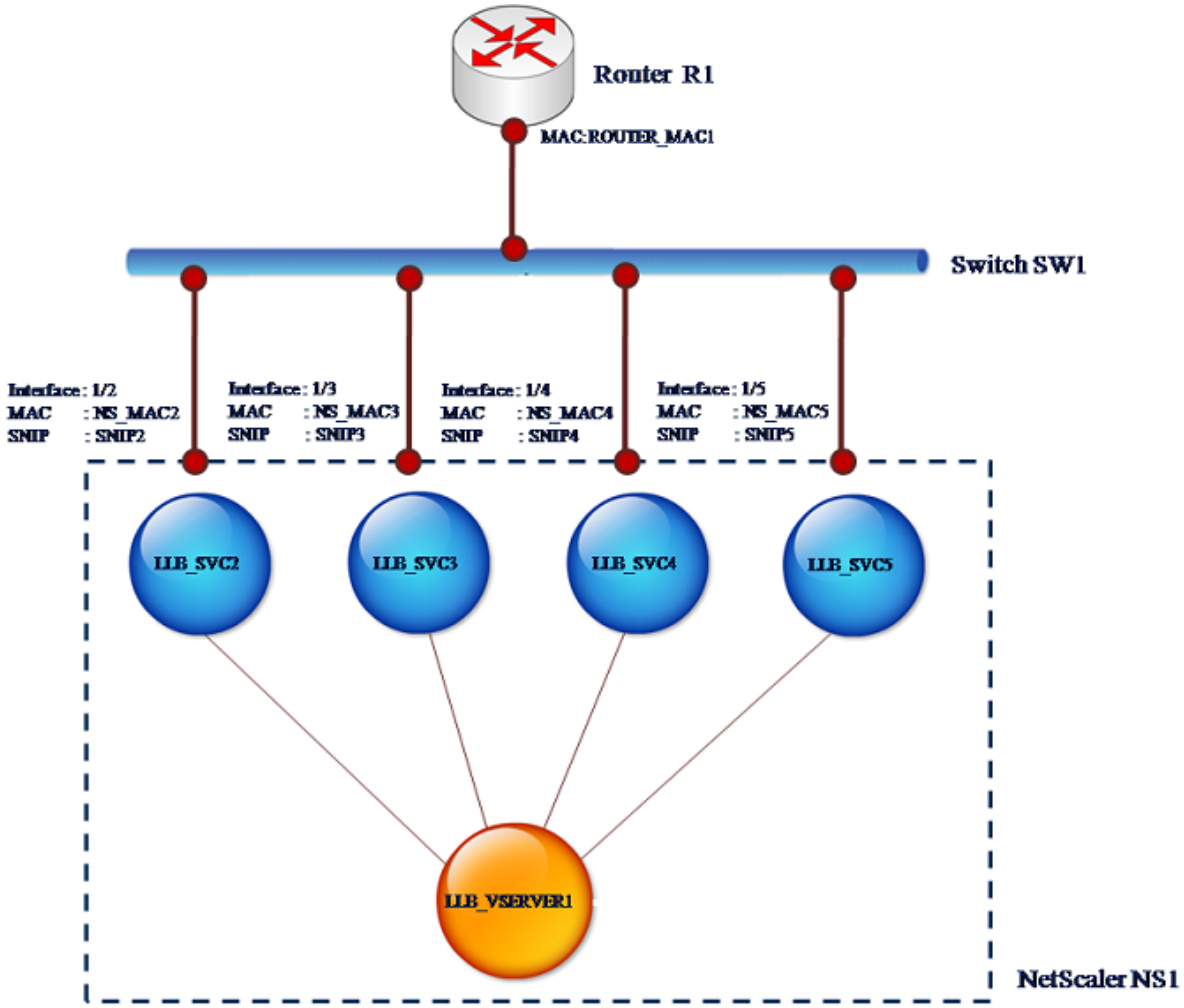
```
23
24      Done
25 <!--NeedCopy-->
```

Enlace de una dirección SNIP a una interfaz

August 20, 2021

Ahora puede enlazar una dirección SNIP propiedad de Citrix ADC a una interfaz sin utilizar VLAN de capa 3. Cualquier paquete relacionado con la dirección SNIP pasará solo a través de la interfaz enlazada.

Esta función puede ser útil en un caso en el que el conmutador ascendente no admite canales de agregación de vínculos y quiere que el dispositivo Citrix ADC equilibre la carga del tráfico, originado en un servidor, en los cuatro vínculos al conmutador ascendente, como se muestra en la siguiente ilustración.



Las tablas siguientes describen la configuración de ejemplo para el caso:

Entidad	Nombre	Valor
Direcciones SNIP en NS1	SNIP2 (solo para fines de referencia)	10.10.10.2
	SNIP3 (solo para fines de referencia)	10.10.10.3
	SNIP4 (solo para fines de referencia)	10.10.10.4
	SNIP5 (solo para fines de referencia)	10.10.10.5
Servidor virtual LLB en NS1	LLB_VSERVER1	-
Monitor transparente en NS1	TRANS_MON	-

Entidad	Nombre	Valor
Servicios LLB en NS1	LLB_SVC2	10.10.10.240
	LLB_SVC3	10.10.10.120
	LLB_SVC4	10.10.10.60
	LLB_SVC5	10.10.10.30
Dirección MAC de la interfaz 1/2 en NS1	NS_MAC_2 (solo para fines de referencia)	00:e0:ed:0f:bc:e0
Dirección MAC de la interfaz 1/3 en NS1	NS_MAC_3 (solo para fines de referencia)	00:e0:ed:0f:bc:df
Dirección MAC de la interfaz 1/4 en NS1	NS_MAC_4 (solo para fines de referencia)	00:e0:ed:0f:bc:de
Dirección MAC de la interfaz 1/5 en NS1	NS_MAC_5 (solo para fines de referencia)	00:e0:ed:1c:89:53
Dirección IP del router R1	IP Router_IP (solo para fines de referencia)	10.10.10.1
Dirección MAC de la interfaz de R1	ROUTER_MAC1 (solo para fines de referencia)	00:21:a1:2d:db:cc

Para configurar las opciones de ejemplo:

1. Agregue cuatro SNIP diferentes en diferentes rangos de subred. Esto es para que ARP se resuelva en cuatro enlaces diferentes. Para obtener más información sobre la creación de una dirección SNIP, consulte Configuración de direcciones IP de subred (SNIP).

   Ejemplo CLI:

```
> add ns ip 10.10.10.2 255.255.255.0 -type SNIP
 Done
> add ns ip 10.10.10.3 255.255.255.128 - type SNIP
Done
> add ns ip 10.10.10.4 255.255.255.192 - type SNIP
Done
> add ns ip 10.10.10.5 255.255.255.224 - type SNIP
Done
<!--NeedCopy-->
```

2. Agregue cuatro servicios ficticios diferentes en las subredes SNIP agregadas. Esto es para garan-

tizar que el tráfico se envía con IP de origen como uno de los cuatro SNIP configurados. Para obtener más información sobre la creación de un servicio, consulte Configuración del equilibrio de carga básico.

Ejemplo CLI:

```
> add service LLB_SVC2 10.10.10.240 any *
 Done
> add service LLB_SVC3 10.10.10.120 any *
 Done
> add service LLB_SVC4 10.10.10.60 any *
 Done
> add service LLB_SVC5 10.10.10.30 any *
 Done
<!--NeedCopy-->
```

3. Agregue un monitor de ping transparente para supervisar la Gateway. Enlazar el monitor a cada uno de los servicios ficticios configurados. Esto es para hacer que el estado de los servicios como UP. Para obtener más información sobre la creación de un monitor transparente, consulte Configurar monitores en una configuración de equilibrio de carga.

   Ejemplo CLI:

```
> add monitor TRANS_MON ping -destIP 10.10.10.1 -transparent YES
 Done
> bind monitor TRANS_MON LLB_SVC2
 Done
> bind monitor TRANS_MON LLB_SVC3
 Done
> bind monitor TRANS_MON LLB_SVC4
 Done
> bind monitor TRANS_MON LLB_SVC5
 Done
<!--NeedCopy-->
```

4. Agregue un servidor virtual de equilibrio de carga de vínculos (LLB) y vincule los servicios ficticios a él. Para obtener más información sobre la creación de un servidor virtual LLB, consulte Configuración de una configuración básica de LLB.

   Ejemplo CLI:


```
> add lb vserver LLB_VSERVER1 any
 Done
> set lb vserver LLB_VSERVER1 -lbmethod ROUNDROBIN
 Done
> bind lb vserver LLB_VSERVER1 LLB_SVC2
 Done
> bind lb vserver LLB_VSERVER1 LLB_SVC2
 Done
> bind lb vserver LLB_VSERVER1 LLB_SVC2
 Done
> bind lb vserver LLB_VSERVER1 LLB_SVC2
 Done
<!--NeedCopy-->
```

5. Agregue el servidor virtual LLB como ruta LLB predeterminada. Para obtener más información sobre la creación de una ruta LLB, consulte Configuración de una configuración básica de LLB.

   Ejemplo CLI:

```
> add lb route 0.0.0.0 0.0.0.0  LLB_VSERVER1
 Done
<!--NeedCopy-->
```

6. Agregue una entrada ARP para cada uno de los servicios ficticios con la dirección MAC de la Gateway. De esta manera, la Gateway es accesible a través de estos servicios ficticios. Para obtener más información sobre cómo agregar una entrada ARP, consulte Configuración de ARP estático.

   Ejemplo CLI:

```
> add arp -ipaddress 10.10.10.240 -mac 00:21:a1:2d:db:cc -ifnum
   1/2
 Done
> add arp -ipaddress 10.10.10.120 -mac 00:21:a1:2d:db:cc -ifnum
   1/3
 Done
> add arp -ipaddress 10.10.10.60 -mac 00:21:a1:2d:db:cc -ifnum 1/4
 Done
> add arp -ipaddress 10.10.10.30 -mac 00:21:a1:2d:db:cc -ifnum 1/5
 Done
<!--NeedCopy-->
```


7. Enlazar una interfaz específica a un SNIP agregando una entrada ARP para cada uno de estos SNIP. Esto es para garantizar que el tráfico de respuesta llegue a la misma interfaz a través de la cual se salió la solicitud. Para obtener más información sobre cómo agregar una entrada ARP, consulte Configuración de ARP estático.

   Ejemplo CLI:

```
> add arp -ipAddress 10.10.10.2 -mac 00:e0:ed:0f:bc:e0 -ifnum 1/2
 Done
> add arp -ipAddress 10.10.10.3 -mac 00:e0:ed:0f:bc:df -ifnum 1/3
 Done
> add arp -ipAddress 10.10.10.4 -mac 00:e0:ed:0f:bc:de -ifnum 1/4
 Done
> add arp -ipAddress 10.10.10.5 -mac 00:e0:ed:1c:89:53 -ifnum 1/5
 Done
<!--NeedCopy-->
```

Supervisar la tabla Bridge y cambiar el tiempo de antigüedad

January 12, 2021

El dispositivo Citrix ADC conecta tramas en función de la búsqueda de la tabla de puente de la dirección MAC de destino y el ID de VLAN. Sin embargo, el dispositivo solo realiza el reenvío cuando el modo Capa 2 está habilitado.

La tabla de puente se genera dinámicamente, pero puede mostrarla, modificar el tiempo de antigüedad de la tabla de puente y ver estadísticas de puente. Todas las entradas MAC de la tabla de puente se actualizan con el tiempo de caducidad.

Para establecer el tiempo de caducidad de las entradas de la tabla de puente mediante la CLI:

En el símbolo del sistema, escriba:

- **set l2param** <positive_integer> -**bridgeagetimeout**
- **show l2param**

Ejemplo:

```
> set l2param -bridgeagetimeout 90
 Done
<!--NeedCopy-->
```


Para ver las estadísticas de una tabla de puente mediante la CLI:

En el símbolo del sistema, escriba:

- **puente stat**

Para establecer el tiempo de caducidad de las entradas de la tabla de puente mediante la interfaz gráfica de usuario:

Vaya a **Sistema** > **Red**. En la página **Red**, en la sección **Configuración**, haga clic en **Configurar parámetros de capa2** y establezca el parámetro **Valor de tiempo de espera para las entradas de tabla de puente (segundos)**.

Para ver las estadísticas de una tabla de puente mediante la GUI:

Vaya a **Sistema** > **Red** > **Bridge Table**, seleccione la dirección MAC y haga clic en **Estadísticas**.

Dispositivos Citrix ADC en modo activo-activo mediante VRRP

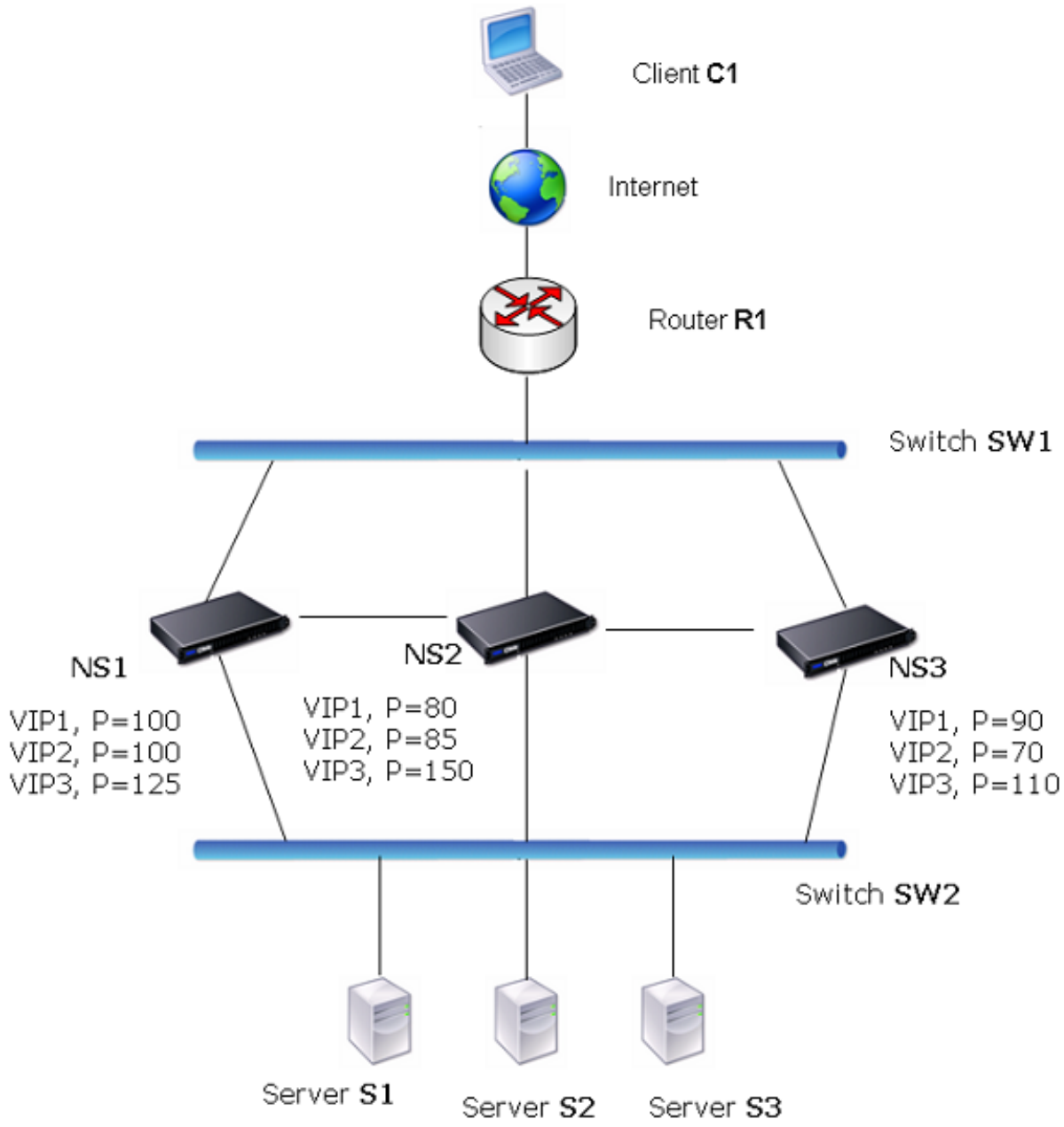
August 20, 2021

Una implementación activa-activa, además de evitar el tiempo de inactividad, hace un uso eficiente de todos los dispositivos Citrix ADC en la implementación. En el modo de implementación activo-activo, los mismos VIP se configuran en todos los dispositivos Citrix ADC de la configuración, pero con prioridades diferentes, de modo que un VIP determinado solo puede estar activo en un dispositivo cada vez.

El VIP activo se denomina VIP principal y los VIP correspondientes de los demás dispositivos Citrix ADC se denominan VIP de copia de seguridad. Si un VIP maestro falla, el VIP de copia de seguridad con la prioridad más alta toma el control y se convierte en el VIP maestro. Todos los dispositivos Citrix ADC en una implementación activa-activa utilizan el protocolo Virtual Router Redundancy Protocol (VRRP) para anunciar sus VIP y las prioridades correspondientes a intervalos regulares.

Los dispositivos Citrix ADC en modo activo-activo se pueden configurar para que ningún Citrix ADC esté inactivo. En esta configuración, hay diferentes conjuntos de VIP activos en cada Citrix ADC. Por ejemplo, en el diagrama siguiente, VIP1, VIP2, VIP3 y VIP4 se configuran en los dispositivos NS1, NS2 y NS3. Debido a sus prioridades, VIP1 y VIP 2 están activos en NS1, VIP3 está activo en NS2 y VIP 4 está activo en NS3. Si, por ejemplo, NS1 falla, VIP1 en NS3 y VIP2 en NS2 se activan.

Ilustración 1. Una configuración activo-activa



Los dispositivos Citrix ADC del diagrama anterior procesan el tráfico de la siguiente manera:

1. El cliente C1 envía una solicitud a VIP1. La solicitud llega a R1.
2. R1 no tiene una entrada ARP para VIP1, por lo que emite una solicitud ARP para VIP1.
3. VIP1 está activo en NS1, por lo que NS1 responde con una dirección MAC de origen como MAC virtual (por ejemplo, MAC1 virtual) asociado con VIP1, y VIP1 como dirección IP de origen.
4. SW1 aprende el puerto para VIP1 a partir de la respuesta ARP y actualiza su tabla de puente.
5. R1 actualiza la entrada ARP con MAC1 virtual y VIP1.

6. R1 reenvía el paquete al VIP1 en NS1.
7. El algoritmo de equilibrio de carga de NS1 selecciona el servidor S2 y NS1 abre una conexión entre una de sus direcciones SNIP y S2.
8. S2 responde al SNIP en Citrix ADC.
9. NS1 envía la respuesta de S2 al cliente. En la respuesta, NS1 inserta la dirección MAC de la interfaz física como dirección MAC de origen y VIP1 como dirección IP de origen.
10. Si NS1 falla, los dispositivos Citrix ADC utilizan el protocolo VRRP para seleccionar el VIP1 con la prioridad más alta. En este caso, VIP1 en NS3 se activa y los dos pasos siguientes actualizan la configuración activo-activa.
11. NS3 transmite un mensaje GARP para VIP1. En el mensaje, virtual MAC1 es la dirección MAC de origen y VIP1 es la dirección IP de origen.
12. SW1 aprende el nuevo puerto para el MAC1 virtual a partir de la difusión GARP y actualiza su tabla de puente para enviar solicitudes de clientes posteriores para VIP1 a NS3. R1 actualiza su tabla ARP.

La prioridad de un VIP se puede modificar mediante el seguimiento del estado. Si habilita el seguimiento de estado, debe asegurarse de que la preferencia también esté habilitada, de modo que un VIP cuya prioridad se reduzca pueda ser precedido por otro VIP.

En algunas situaciones, el tráfico puede llegar a un VIP de respaldo. Para evitar la eliminación de dicho tráfico, puede habilitar el uso compartido, por nodo, a medida que crea una configuración activo-activa. O bien, puede habilitar la opción global enviar al maestro. En un nodo en el que está habilitado el uso compartido, tiene prioridad sobre enviar al maestro.

Seguimiento del estado

La prioridad base (rango BP 1-255) determina normalmente qué VIP es el VIP principal, pero la prioridad efectiva (EP) también puede afectar a la determinación.

Por ejemplo, si un VIP en NS1 tiene una prioridad de 101 y el mismo VIP en NS2 tiene una prioridad de 99, el VIP en NS1 está activo. Sin embargo, si dos servidores virtuales están usando el VIP en NS1 y uno de ellos baja, el seguimiento del estado puede reducir el EP de VIP en NS1. VRRP hace que el VIP en NS2 sea el VIP activo.

Las siguientes son las opciones de seguimiento de estado para modificar EP:

- **NINGUNO.** No hay seguimiento. EP = PB
- **ALL**. Si todos los servidores virtuales están UP, entonces EP = BP. De lo contrario, EP = 0.
- **ONE.** Si al menos un servidor virtual está UP, entonces EP = BP. De lo contrario, EP = 0.
- **PROGRESSIVE.** Si TODOS los servidores virtuales están UP, entonces EP = BP. Si TODOS los servidores virtuales están DOWN, EP = 0. De lo contrario EP = BP (1: K/N), donde N es el número total de servidores virtuales asociados con el VIP y k es el número de servidores virtuales que están inactivos.

Nota: Si especifica un valor distinto de NONE, se debe activar la preferencia, de modo que el VIP de copia de seguridad con la prioridad más alta se active si la prioridad del VIP principal se rebaja.

Preferencia

La preferencia de un VIP activo por otro VIP que obtenga una prioridad más alta está habilitada de forma predeterminada, y normalmente debería habilitarse. En algunos casos, sin embargo, es posible que quiera inhabilitarlo. Preemption es una configuración por nodo para cada VIP.

La preferencia puede ocurrir en las siguientes situaciones:

- Un VIP activo baja y un VIP con una prioridad menor toma su lugar. Si el VIP con la prioridad más alta vuelve en línea, se anteponen al VIP activo actualmente.
- El seguimiento del estado hace que la prioridad de un VIP de copia de seguridad sea superior a la del VIP activo. A continuación, el VIP de copia de seguridad prejuzga al VIP activo.

Uso compartido

En el caso de que el tráfico llegue a un VIP de copia de seguridad, el tráfico se elimina a menos que la opción de compartir esté habilitada en el VIP de copia de seguridad. Este comportamiento es una configuración por nodo para cada VIP y está inhabilitado de forma predeterminada.

En la ilustración **Una configuración activa-activa** VIP1 en NS1 está activa y VIP1 VIP en NS2 y NS3 son copias de seguridad. En determinadas circunstancias, el tráfico puede llegar a VIP1 en NS2. Si el uso compartido está habilitado en NS2, este tráfico se procesa en lugar de descartado.

Configuración del modo activo-activo

August 20, 2021

En cada dispositivo Citrix ADC que quiera implementar en modo activo-activo, debe agregar un MAC virtual y enlazar el MAC virtual a un VIP. El MAC virtual de un VIP determinado debe ser el mismo en cada dispositivo. Por ejemplo, si se crea VIP 10.102.29.5 en los dispositivos, se debe crear un ID de enrutador virtual (VRID) en cada Citrix ADC y enlazarlo a VIP 10.102.29.5 en cada Citrix ADC. Cuando vincula un MAC virtual a un VIP, el dispositivo envía anuncios VRRP a cada VLAN enlazada a ese VIP. El MAC virtual puede ser compartido por diferentes VIP configurados en el mismo Citrix ADC.

Configuración del modo activo-activo IPv4

Realice las siguientes tareas en cada uno de los dispositivos Citrix ADC que se incluirán en la configuración activo-activa:

- **Agregue una dirección MAC virtual**. Agregue una dirección MAC virtual agregando un VRID. También puede especificar una prioridad y habilitar o inhabilitar la preferencia y el uso compartido en esta dirección VRID.
- **Agregue una dirección VIP y asocie el VRID del MAC virtual**. Agregue una dirección VIP y establezca el parámetro VRID en el VRID recién creado. Los atributos del VRID (por ejemplo, prioridad y preferencia) están vinculados a esta dirección VIP.
  Nota: Se debe agregar la misma dirección VIP a todos los demás dispositivos Citrix ADC.

Para agregar una dirección MAC virtual mediante la CLI

En el símbolo del sistema, escriba:

- **add vRID** <id>[-**prioridad**] <positive_integer>[-**preferencia** (**HABILITADO**|**DESHABILITADO**)][-**sharing** (**ENABLED**|**DISABLED**)] [-**seguimiento**]<tracking>
- **show vrid**

Para agregar una dirección VIP mediante la CLI:

En el símbolo del sistema, escriba:

- **add ns ip** <value> <IPv4Address> -type VIP -vrid
- **mostrar ns ip**

Para configurar un MAC virtual mediante la GUI:

1. Vaya a **Sistema** > **Red** > **VMAC**, en la ficha **VMAC**, agregue un nuevo MAC virtual o modifique un MAC virtual existente.
2. Defina los siguientes parámetros:
   - Id. de enrutador virtual
   - Prioridad
   - Rastreando
   - Preferencia
   - Uso compartido

Para configurar una dirección VIP y asociar el VRID a ella mediante la GUI:

1. Vaya a **Sistema** > **Red** > **Direcciones IP**, en la ficha **Direcciones IPv4**, agregue una dirección IP de tipo VIP.
2. Al agregar la dirección IP, seleccione el ID del enrutador **virtual en el cuadro desplegable ID del enrutador virtual**.

Configuración de ejemplo:

El siguiente ejemplo de configuración es para implementar dispositivos Citrix ADC NS1 y NS2 en modo activo-activo IPv4. La dirección VIP 203.0.113.10 está configurada en NS1 y NS2, con un valor de prioridad diferente en cada dispositivo. En cada dispositivo, esta dirección VIP está enlazada a una dirección MAC virtual. 203.0.113.10 es maestra en NS2, porque su prioridad (200) en NS2 es mayor que en NS1 (100).


```
    Settings on NS1

    > add vrid 10 -Priority 100 -Preemption Enabled -sharing Enabled

    Done

    > add ns ip 203.0.113.10 -type VIP -vrid 10

    Done

    Settings on NS2

    > add vrid 10 -Priority 200 -Preemption Enabled -sharing Enabled

    Done

    > add ns ip 203.0.113.10 -type VIP -vrid 10

    Done
<!--NeedCopy-->
```

Configuración del modo activo-activo IPv6

Realice las siguientes tareas en cada uno de los dispositivos Citrix ADC que se incluirán en la configuración activo-activa:

- **Agregue una dirección MAC6 virtual**. Agregue una dirección MAC6 virtual agregando un VRID6. También puede especificar una prioridad y habilitar o inhabilitar la preferencia y el uso compartido en esta dirección VRID6.
- **Agregue una dirección VIP6**. Agregue una dirección VIP6. Establezca el parámetro VRID6 en el VRID6 de la macvirtual recién creada 6.Los atributos del MAC6 virtual (por ejemplo, prioridad y preferencia) están enlazados a esta dirección VIP6.
  Nota: Se debe agregar la misma dirección VIP6 a todos los demás dispositivos Citrix ADC.

Para agregar una dirección MAC6 virtual mediante la CLI:

En el símbolo del sistema, escriba:

- **add vRId6** <id>[-**prioridad**] [-**preferencia** (**HABILITADO** | **DESHABILITADO**)] [-**uso compartido** (**HABILITADO** | **DESHABILITADO**)]
- **show vrID6**

Para agregar una dirección VIP6 mediante la CLI:

En el símbolo del sistema, escriba:

- **add ns ip6** <value> <IPv6Address> -**tipo** VIP -**vrid**
- **show ns ip6**

Para configurar un MAC6 virtual mediante la GUI:

1. Vaya a **Sistema** > **Red** > **VMAC**, en la ficha **VMAC6**, agregue un nuevo MAC6 virtual o modifique un **VMAC6** existente.
2. Defina los siguientes parámetros:
   - Id. de enrutador virtual
   - Prioridad
   - Preferencia
   - Uso compartido

Para configurar una dirección VIP6 y asociar el VRID a ella mediante la GUI:

1. Vaya a **Sistema** > **Red** > **IPs**, en la ficha **IPv6s**, agregue una dirección IPv6 de tipo VIP.
2. Mientras agrega la dirección VIP6, seleccione VRID6 en el cuadro desplegable **Virtual Router ID**.

Configuración de ejemplo:

El siguiente ejemplo de configuración es para implementar dispositivos Citrix ADC NS1 y NS2 en el modo activo-activo IPv6. La dirección VIP6 2001:db8: :5001 está configurada en NS1 y NS2, con un valor de prioridad diferente en cada dispositivo. En cada dispositivo, esta dirección VIP6 está enlazada a una dirección MAC6 virtual. 2001:db8: :5001 es maestra en NS2, porque su prioridad (200) en NS2 es mayor que en NS1 (100).

```
1     Settings on NS1
2     > add vrid6 10 -Priority 100 -Preemption Enable -sharing Enable
3
4     Done
5     > add ns ip6 2001:db8::5001 -type VIP -vrid6 10
6
7     Done
8     Settings on NS2
9     > add vrid6 10 -Priority 200 -Preemption Enable -sharing Enable
10
11    Done
12    > add ns ip6 2001:db8::5001 -type VIP -vrid6 10
13
14    Done
15 <!--NeedCopy-->
```

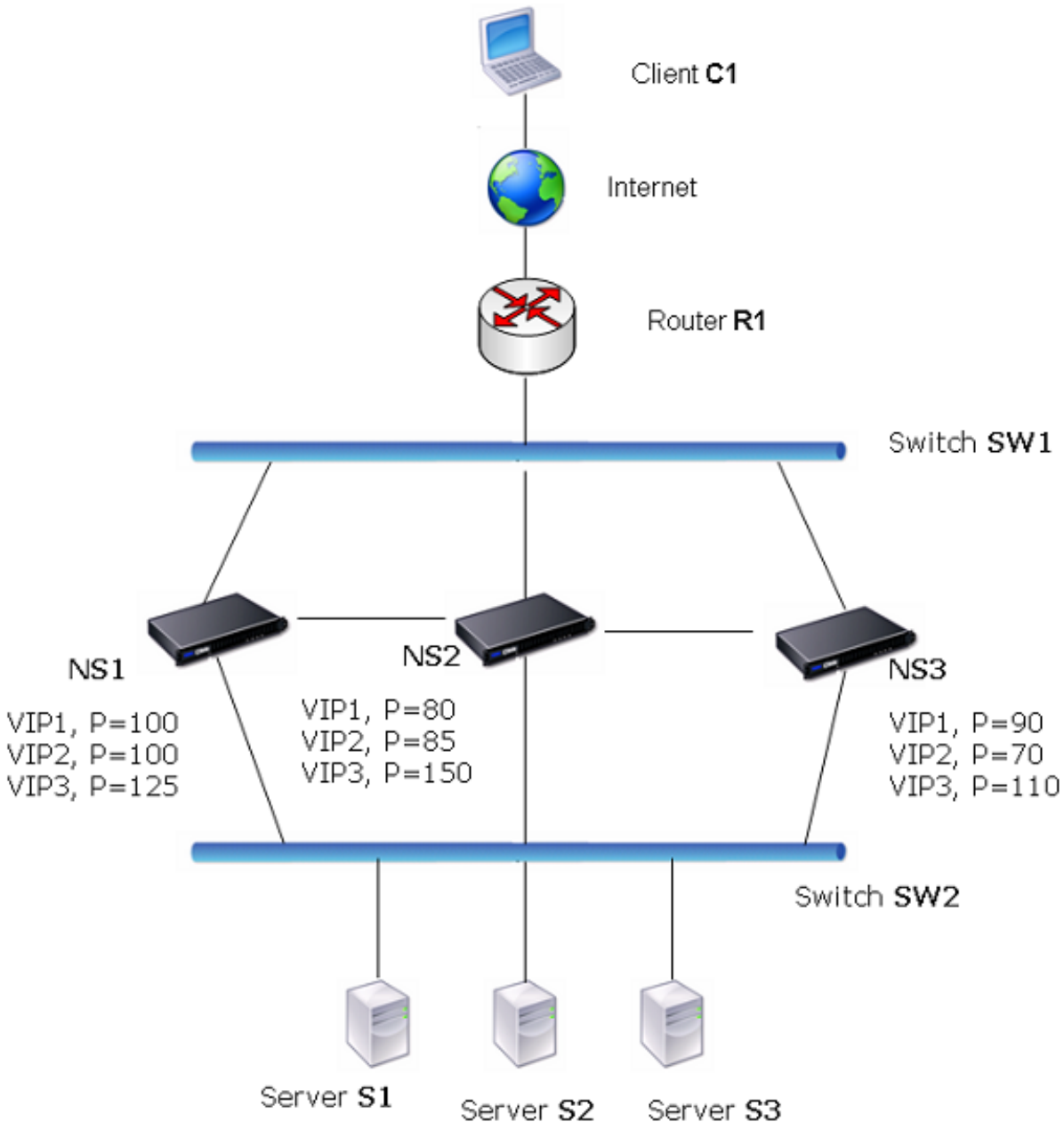

Configuración de Enviar al Maestro

January 12, 2021

Normalmente, el tráfico destinado a un VIP llega al dispositivo Citrix ADC en el que está activo el VIP, ya que una solicitud ARP con el VIP y un MAC virtual en ese dispositivo ha llegado al router ascendente. Sin embargo, en algunos casos, como las rutas estáticas configuradas en el enrutador ascendente para la subred VIP o una topología que bloquea esta ruta, el tráfico puede llegar a un dispositivo Citrix ADC en el que el VIP está en estado de copia de seguridad. Si quiere que este dispositivo reenvíe los paquetes de datos al dispositivo en el que está activo el VIP, debe habilitar la opción Enviar al maestro. Este comportamiento es una configuración por nodo y está inhabilitado de forma predeterminada.

Por ejemplo, en el diagrama siguiente, VIP1 está configurado en NS1, NS2 y NS3 y está activo en NS1. En determinadas circunstancias, el tráfico de VIP1 (activo en NS1) puede llegar a VIP1 en NS3. Cuando la opción Enviar a maestro está habilitada en NS3, NS3 reenvía el tráfico a NS1 a NS2 mediante entradas de ruta para NS1.

Ilustración 1. Una configuración activa-activa con la opción Enviar a maestro habilitada



Para habilitar el envío al maestro mediante la CLI:

En el símbolo del sistema, escriba:

```
set vrIDParam -sendToMaster (ENABLED          DISABLED)
```

Ejemplo:


```
> set vrIDParam -sendToMaster ENABLED
 Done
<!--NeedCopy-->
```

Para habilitar el envío al maestro mediante la GUI:

1. Vaya a **Sistema** > **Red**, en el grupo **Configuración**, haga clic en **Parámetros del enrutador virtual**.
2. Seleccione la opción **Enviar al maestro**.

Configuración de Intervalos de Comunicación VRRP

August 20, 2021

En una implementación activa-activa, todos los nodos Citrix ADC utilizan el Protocolo de redundancia de enrutador virtual (VRRP) para anunciar sus direcciones VIP maestras y las prioridades correspondientes en paquetes de anuncios VRRP (mensajes de saludo) a intervalos regulares.

VRRP utiliza los siguientes intervalos de comunicación:

- **Hello Interval**. Intervalo entre los mensajes de saludo VRRP que envía un nodo de una dirección VIP maestra a sus nodos del mismo nivel.
- **Dead Interval**. Tiempo después del cual un nodo de una dirección VIP de copia de seguridad considera el estado de la dirección VIP maestra como DOWN si los mensajes de saludo VRRP no se reciben desde el nodo de la dirección VIP maestra. Después del intervalo muerto, la dirección VIP de copia de seguridad se hace cargo y se convierte en la dirección VIP principal.

Puede cambiar estos intervalos a un valor deseado. Ambos intervalos de comunicación se configuran por nodo para todas las direcciones VIP de ese nodo.

Para configurar los intervalos de comunicación VRRP mediante la CLI:

En el símbolo del sistema, escriba:

- **set vridParam** [-**hola Intervalo**] <msecs>[-**Intervalo muerto**]<secs>
- **sh vrIDParam**

Ejemplo:

```
> set vrIDParam -helloInterval 500 -deadInterval 2
 Done
<!--NeedCopy-->
```


Para configurar los intervalos de comunicación VRRP mediante la GUI:

1. Vaya a **Sistema** > **Red**, en el grupo **Configuración**, haga clic en **Parámetros del enrutador virtual**.
2. En **Configure Virtual Router Parameter**, establezca los parámetros **Hello Interval** y **Dead Interval**.
3. Haga clic en **Aceptar**.

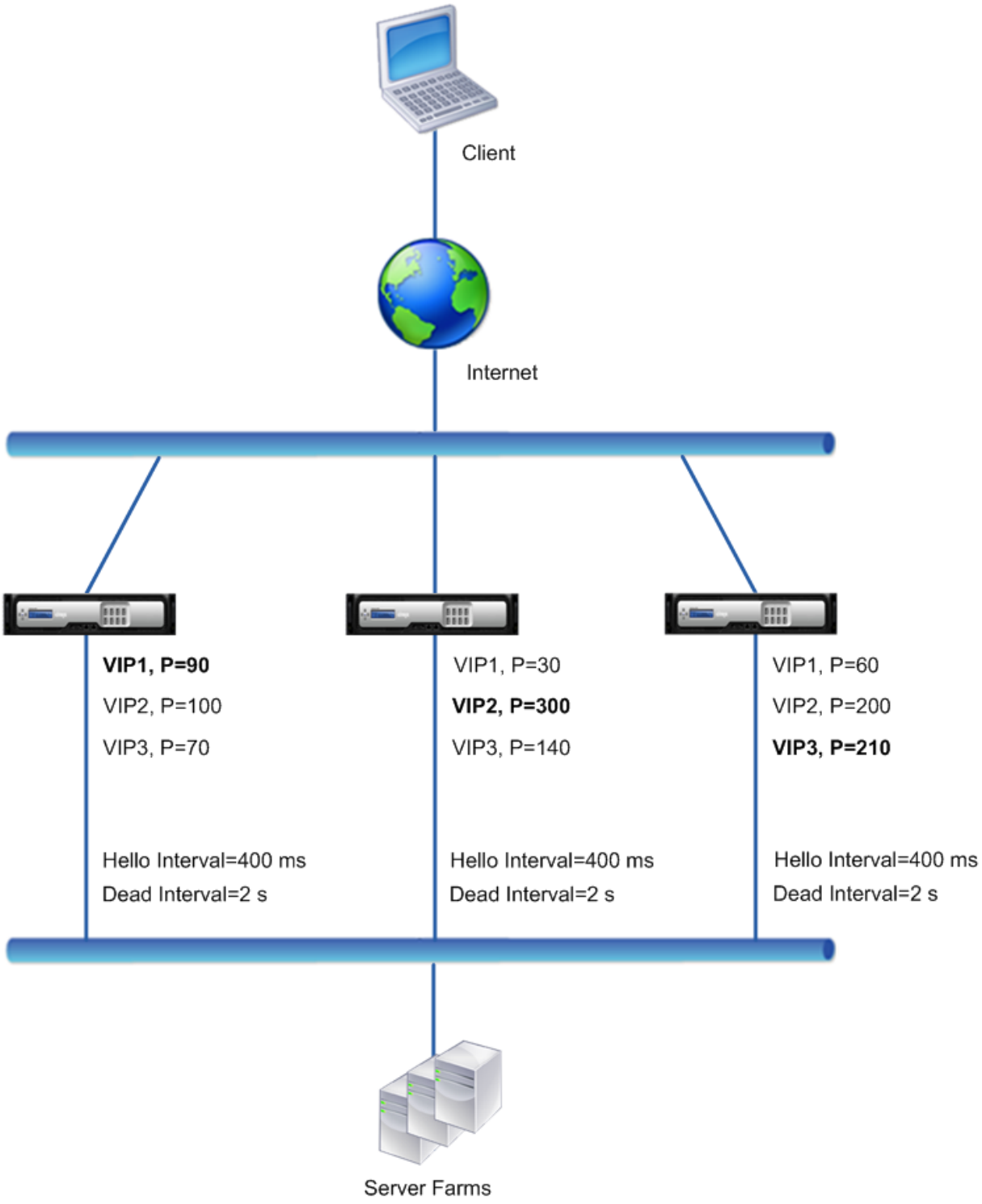
Ejemplo 1: Nodos con los mismos intervalos muertos VRRP

Considere una implementación activa-activa compuesta por Citrix ADC NS1, NS2 y NS3. Las direcciones IP virtuales VIP1, VIP2, VIP3 se configuran en cada uno de estos ADC. Debido a sus prioridades, VIP1 está activo en NS1, VIP2 está activo en NS2 y VIP3 está activo en NS3.

Como se muestra en la tabla siguiente, el intervalo muerto se establece en el mismo valor (2 segundos) en los tres nodos. Los intervalos de comunicación VRRP (intervalo de saludo e intervalo muerto) de un nodo se aplican a todos los VRID configurados en el nodo y, a su vez, se aplican a todas las direcciones VIP asociadas con los VRID del nodo.

En cada nodo, las direcciones VIP que están activas (master) en ese nodo utilizan el intervalo de saludo, y el intervalo muerto lo utilizan las direcciones VIP que están inactivas (copia de seguridad) en ese nodo. La preferencia está inhabilitada para las direcciones VIP en los tres nodos.

En la tabla siguiente se enumeran los valores utilizados en este ejemplo: configuración del ejemplo 1 del intervalo VRRP.



El flujo de ejecución es el siguiente:

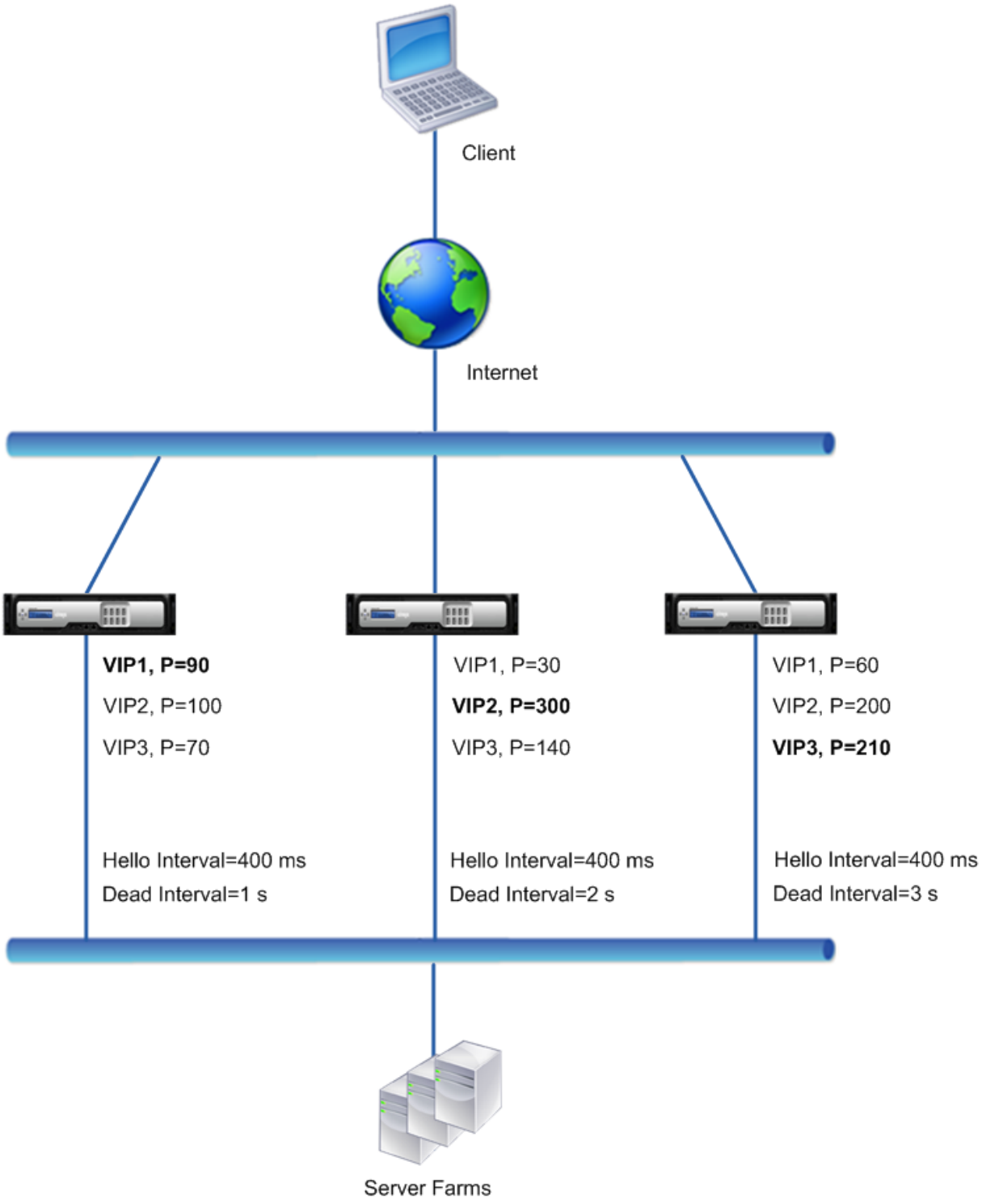
1. NS1 envía mensajes de saludo en un intervalo de saludo establecido de 400 ms a NS2 y NS3 para la dirección VIP1, porque VIP1 está activo (el maestro) en NS1. Del mismo modo, NS2 envía mensajes de saludo para VIP2 y NS3 envía mensajes de saludo para VIP3.

2. En NS1, el intervalo muerto establecido se aplica a VIP2 y VIP3, porque están inactivos (backups) en NS1. Del mismo modo, en NS2, el intervalo muerto establecido se aplica a VIP1 y VIP3, y en NS3, el intervalo muerto establecido se aplica a VIP1 y VIP2.
3. Si NS1 baja, NS2 y NS3 consideran que NS1 está indefinido si no reciben mensajes de saludo de NS1 durante 2 segundos (el intervalo muerto). VIP1 en NS3 se hace cargo y se activa (master) porque su prioridad VRID (60) es mayor que la de VIP1 de NS2 (30).

Ejemplo 2: Nodos con diferentes intervalos muertos VRRP

Considere una implementación VRRP similar a la descrita en Example1 pero con un intervalo muerto diferente en cada nodo (NS1, NS2 y NS3). La preferencia está inhabilitada para las direcciones VIP en los tres nodos.

En la tabla siguiente se enumeran los valores utilizados en este ejemplo: configuración del ejemplo 2 del intervalo VRRP.



El flujo de ejecución es el siguiente cuando NS1 baja:

1. NS2 considera que NS1 está indefinido después de no recibir ningún mensaje de saludo de NS1 durante 2 segundos (intervalo muerto de NS2).
2. VIP1 en NS2 toma el control y se activa (master). NS2 ahora comienza a enviar mensajes de

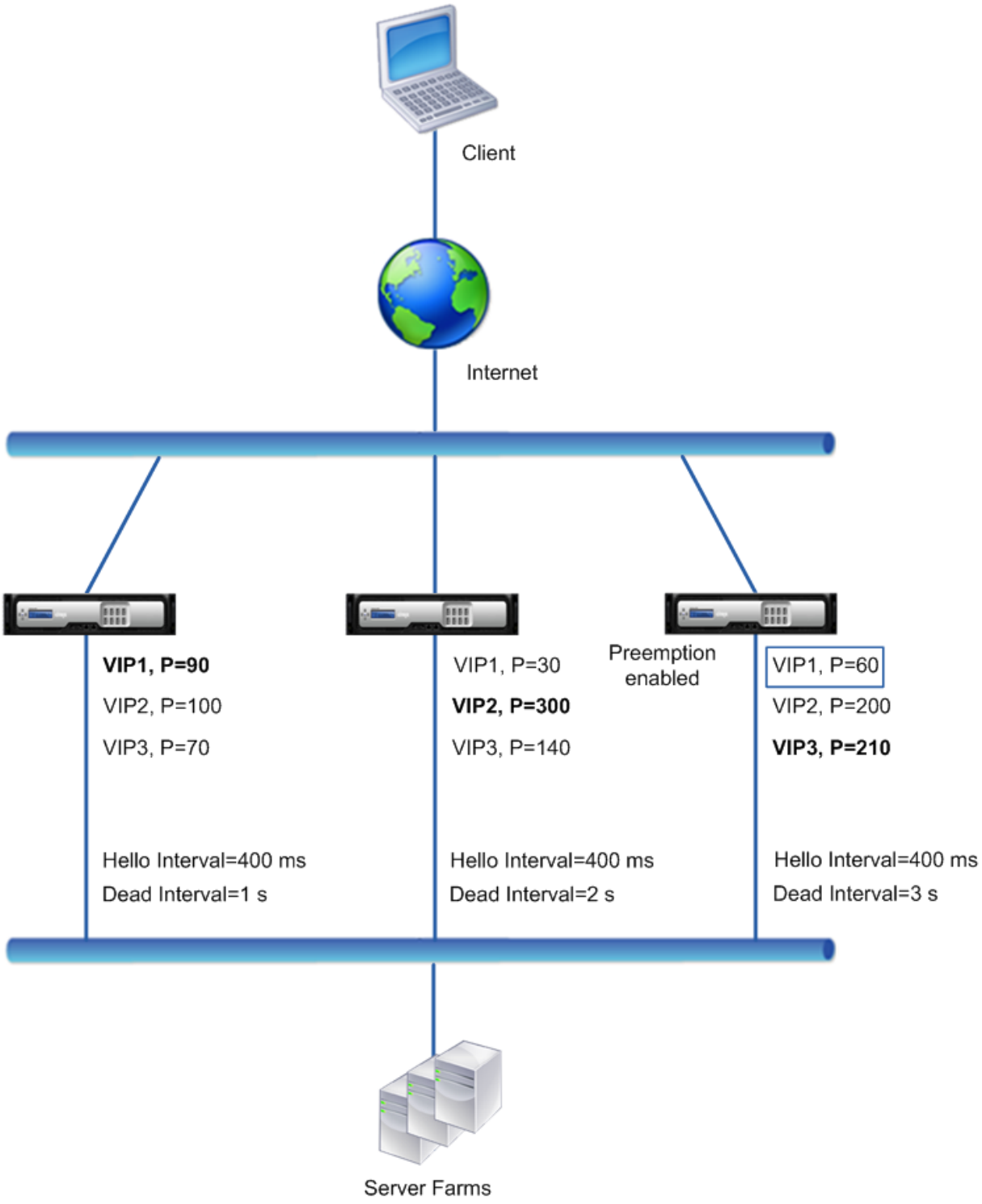
saludo para VIP1.

Aunque VIP1 en NS3 tiene una prioridad VRIP más alta (60) que VIP1 en NS2 (30), el intervalo muerto más grande de NS3 (3 segundos frente a 2 segundos para NS2) evita que VIP1 en NS3 se haga cargo antes de que VIP 1 en NS2 ya lo haya hecho.

Ejemplo 3: Nodos con diferentes intervalos muertos y preferencia activada

Considere una implementación VRRP similar a la descrita en Example1 pero con diferentes intervalos muertos en los tres nodos, NS1, NS2 y NS3, y con preferencia habilitada para la dirección VIP1 en NS3.

En la tabla siguiente se enumeran los valores utilizados en este ejemplo: configuración del ejemplo 3 del intervalo VRRP.



El flujo de ejecución es el siguiente cuando NS1 baja:

1. NS2 considera que NS1 está indefinido después de no recibir ningún mensaje de saludo de NS1 durante 2 segundos (intervalo indefinido establecido de NS2). En este momento, NS3, con un intervalo muerto de 3 segundos, no considera que NS1 esté indefinido.

2. VIP1 en NS2 toma el control y se activa (master). NS2 ahora comienza a enviar mensajes de saludo para VIP1.
3. Al recibir mensajes de saludo de NS2 para VIP1, NS3 prevalecen NS2 para VIP1 porque la preferencia está habilitada para VIP1 de NS3 y la prioridad VRID (60) de VIP1 de NS3 es mayor que la (30) de VIP1 de NS2.
4. VIP1 en NS3 toma el control y se activa (master). NS3 ahora comienza a enviar mensajes de saludo para VIP1.

Configuración del seguimiento de estado basado en el estado de la interfaz

August 20, 2021

Para asegurarse de que una dirección VIP de copia de seguridad toma el control como VIP principal antes de que el nodo de la dirección VIP principal actual se desconecte por completo, puede configurar un nodo para cambiar la prioridad de una dirección VIP cuando cambie el estado de una interfaz en el nodo. Por ejemplo, el nodo reduce la prioridad de una dirección VIP cuando el estado de una interfaz cambia a DOWN y aumenta la prioridad cuando el estado de la interfaz cambia a UP. Esta función es una configuración por nodo para cada dirección VIP.

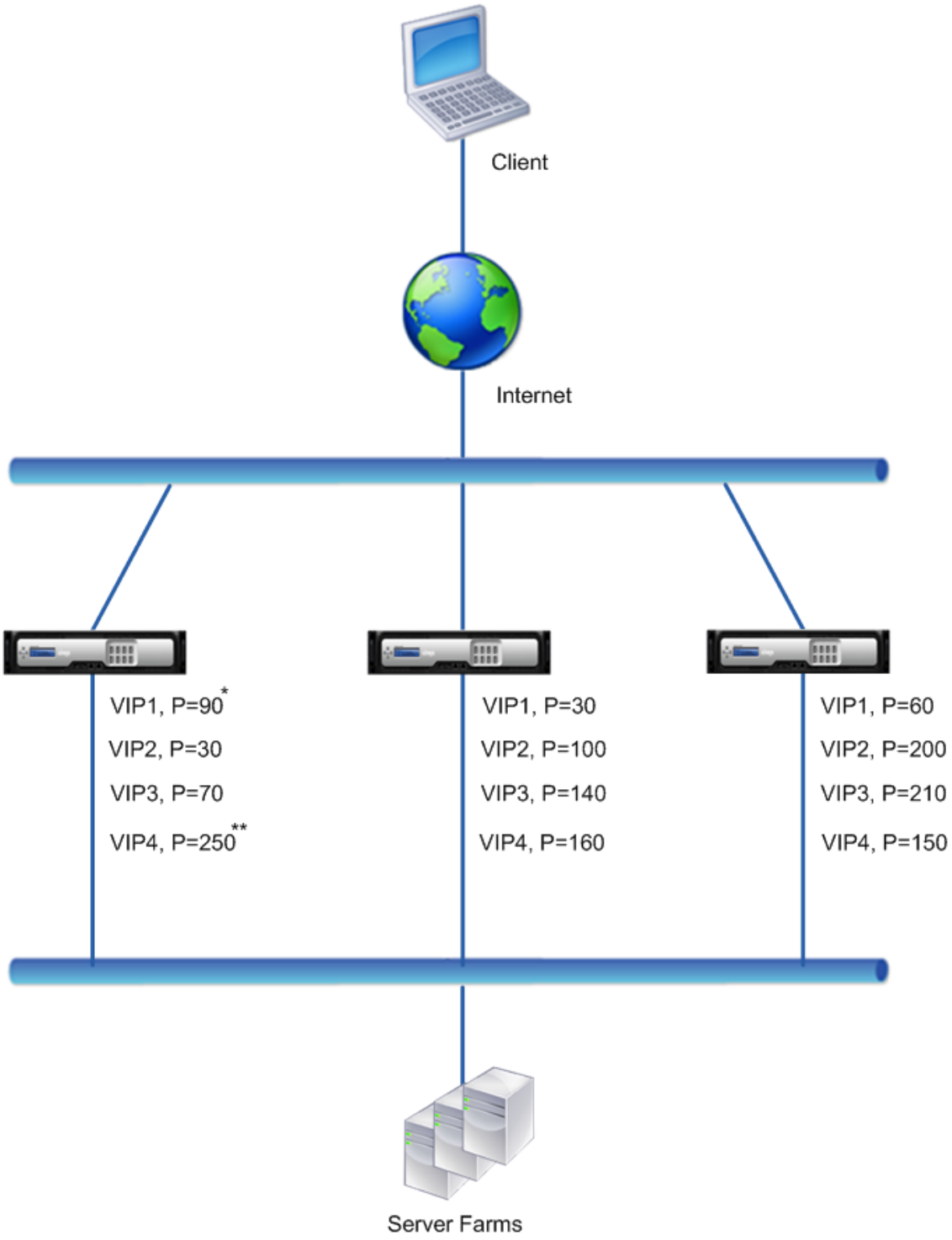
Ejemplo

Considere una implementación activa-activa compuesta por Citrix ADC NS1, NS2 y NS3. Las direcciones IP virtuales VIP1, VIP2, VIP3 y VIP4 se configuran en cada uno de estos ADC. Debido a sus prioridades, VIP1 y VIP4 están activos en NS1, VIP2 está activo en NS2 y VIP3 está activo en NS3.

Para garantizar que las direcciones VIP activas en NS1 sean asumidas por NS2 o NS3 antes de que NS1 se desactive por completo, se configura el seguimiento de estado basado en interfaz para las direcciones VIP1 y VIP4 en NS1. La configuración del seguimiento de estado basado en interfaz para una dirección VIP incluye asociar las interfaces deseadas y establecer el parámetro de prioridad reducida (TrackIfNumPriority) para el VRID asociado de la dirección VIP. Por ejemplo, en NS1, las interfaces 1/2, 1/3 y 1/5 están asociadas al VRID de VIP1, y la prioridad reducida se establece en 20.

La preferencia está habilitada para estas direcciones VIP en los tres nodos.

En la tabla siguiente se enumeran los ajustes utilizados en este ejemplo: Configuración de ejemplo de seguimiento de estado.



* Packet Interfaces = 1/2, 1/3, 1/5
Reduced Priority = 20

** Packet Interfaces = 1/5, 1/7
Reduced Priority = 55

El flujo de ejecución es el siguiente en NS1 cuando la interfaz múltiple en NS1 baja:

1. Si la interfaz 1/3 baja, la prioridad de la dirección VIP1 se reduce en 20 (valor de prioridad reducido de VIP1), ya que la interfaz 1/3 está asociada con VIP1:
   - Prioridad efectiva del VIP1 = (Prioridad actual: Prioridad reducida) = (90-20) = 70
2. Del mismo modo, si la interfaz 1/5 baja, la prioridad de la dirección VIP1 se reduce aún más:
   - Prioridad efectiva del VIP1 = (Prioridad actual: Prioridad reducida) = (70-20) = 50
3. En este punto, la prioridad efectiva de VIP1 en NS1 es menor que la prioridad de VIP1 en NS3. NS3 precede a NS1 para VIP1. VIP1 en NS3 toma el control y se activa (master).
4. Además, debido a que la interfaz 1/5 también está asociada con VIP4, la prioridad de VIP4 se reduce por el valor de prioridad reducido del VIP4 (55).
   - Prioridad efectiva del VIP4 = (250: 55) = 195
5. Si la interfaz 1/7 baja, la prioridad de VIP4 se reduce aún más:
   - Prioridad efectiva del VIP4 = (Prioridad actual: Prioridad reducida) = (195-55) = 145
6. En este punto, la prioridad efectiva de VIP4 en NS1 es menor que la prioridad de VIP4 en NS2. NS2 precede NS1 para VIP4. VIP4 en NS3 toma el control y se activa (master). Esta configuración garantiza que ninguna de las cuatro direcciones VIP esté activa en NS1 antes de que se desactive completamente.

Pasos de configuración para el modo activo-activo IPv4

Para configurar esta función en un nodo para una dirección VIP, establezca el parámetro Prioridad reducida (TrackIfNumPriority) y, a continuación, asocie las interfaces cuyo estado debe seguirse para cambiar la prioridad de la dirección VIP. Cuando cualquiera de los estados de la interfaz asociada cambia a DOWN o UP, el nodo reduce o aumenta la prioridad de la dirección VIP mediante el valor de Prioridad reducida (TrackIfNumPriority) configurado.

Para establecer una prioridad reducida y enlazar interfaces al ID del enrutador virtual mediante la CLI:

En el símbolo del sistema, escriba:

- **set vRiD** <id>[-**TrackIfNumPriority**]<positive_integer>
- **bind vrID** <id> -**trackifNum** <interface_name>
- **show vrID** <id>

Ejemplo:

```
1     > set vrID 125 -trackifNumPriority 10
2     Done
3
4     > bind vrID 125 -trackifNum 1/4 1/5
5     Done
6 <!--NeedCopy-->
```


Para establecer una prioridad reducida y enlazar interfaces con el ID del router virtual mediante la GUI:

1. Vaya a **Sistema** > **Red** > **VMAC.**
2. En la ficha **VMACS**, seleccione un ID de enrutador virtual y haga clic en **Modificar**.
3. En **Configurar MAC virtual**, establezca el parámetro **Prioridad reducida**.
4. Seleccione **Interfaces rastreadas para la opción VRID** y, en **Interfaces asociadas**, agregue interfaces al ID del enrutador virtual.

Pasos de configuración para el modo activo-activo IPv6

Para configurar esta función en un nodo para una dirección VIP6, establezca el parámetro Prioridad reducida (TrackIfNumPriority) y, a continuación, asocie las interfaces cuyo estado debe seguirse para cambiar la prioridad de la dirección VIP6. Cuando cualquiera de los estados de la interfaz asociada cambia a DOWN o UP, el nodo reduce o aumenta la prioridad de la dirección VIP6 mediante el valor configurado de Prioridad reducida (TrackIfNumPriority).

Para cambiar automáticamente la prioridad de una dirección VIP mediante la CLI:

En el símbolo del sistema, escriba uno de los siguientes conjuntos de comandos.

- Si agrega un nuevo MAC6 virtual:
  - **añadir vRId6** <id> [-**TrackIfNumPriority**]
  - **bind vrID6** <id> -**trackifNum** <interface_name>
  - **show vrID6** <id>
- Si se está reconfigurando un MAC6 virtual existente:
  - **establecer vRID6** <id> [-**TrackIfNumPriority**]
  - **bind vrID6** <id> -**trackifNum** <interface_name>
  - **show vrID6** <id>

Ejemplo:

```
    > set vrID6 130 -trackifNumPriority 10
    Done

    > bind vrID6 130 -trackifNum 1/4 1/5
    Done
<!--NeedCopy-->
```


Retrasar preferencia

August 20, 2021

De forma predeterminada, una dirección VIP de copia de seguridad precede a la dirección VIP principal inmediatamente después de que su prioridad sea mayor que la del VIP principal. Al configurar una dirección VIP de copia de seguridad, puede especificar una cantidad de tiempo para retrasar la preferencia. El tiempo de demora de preferencia es una configuración por nodo para cada dirección VIP de copia de seguridad.

La configuración de demora de preferencia para un VIP de copia de seguridad no se aplica en las siguientes condiciones:

- El nodo del VIP maestro baja. En este caso, el VIP de copia de seguridad toma el control como VIP principal después del intervalo muerto establecido en el nodo del VIP de copia de seguridad.
- La prioridad del VIP maestro se establece en cero. El VIP de copia de seguridad toma el control como VIP maestro después del intervalo muerto establecido en el nodo del VIP de copia de seguridad.

Ejemplo: Retrasar preferencia

Considere una implementación activa-activa compuesta por dispositivos Citrix ADC NS1 y NS2. La dirección IP virtual VIP1 se configura en cada uno de estos dispositivos. Debido a sus prioridades, VIP1 es maestro en NS2. La preferencia está habilitada y el tiempo de demora de preferencia se establece para VIP1 en estos dos nodos.

En la tabla siguiente se enumeran los parámetros utilizados en este ejemplo.

Entidad y parámetros	Configuración en NS1	Configuración en NS2
VIP1 (solo para fines de referencia)	**Dirección IP:** 192.0.1.10, **VRID:** 10, **Prioridad:** 100, **Prioridad:** Activada, **Tiempo de demora de preferencia:** 1000 segundos	**Dirección IP:** 192.0.1.10, **VRID:** **10**, **Prioridad:** 200, **Preferencia:** Activado, **Tiempo de demora de preferencia:** 2000 segundos
Intervalo muerto	1 segundos	2 segundos

A continuación se presentan algunos ejemplos del posible comportamiento de preferencia en esta configuración:

- Si la prioridad de VIP1 en NS1 se establece en un valor (por ejemplo, 210) mayor que el de VIP1 en NS2, VIP1 en NS1 se hace cargo como maestro después de su tiempo de demora de preferencia

establecido (1000 segundos).

- Si se agrega un tercer nodo NS3 con la siguiente configuración VRRP a esta implementación, VIP1 en NS3 se convierte en maestro después de su tiempo de demora establecido de preferencia (3000 segundos).
  - VIP1
    - VRID: 30
    - Dirección IP:
    - Prioridad = 300
    - Tiempo de demora de preferencia = 3000 segundos
- Si NS2 falla, VIP1 en NS1 toma el control como maestro después de 1 segundo (establece el intervalo muerto en NS1). El tiempo de demora de preferencia para VIP1 en NS1 no se aplica en este caso.
- Si NS2 baja y NS1 se reinicia, VIP1 en NS1 se convierte en maestro 1 segundo (intervalo muerto establecido en NS1) después de que aparezca NS1. El tiempo de demora de preferencia para VIP1 en NS1 no se aplica en este caso.
- Si la prioridad de VIP1 en NS2 está establecida en cero, VIP1 pasa al modo de espera. VIP1 en NS1 toma el control como maestro después de 1 segundo (establece el intervalo muerto en NS1). El tiempo de demora de preferencia para VIP1 en NS1 no se aplica en este caso.

Configuración de la preferencia de demora para el modo activo-activo IPv4

Para configurar el tiempo de demora de preferencia para una dirección VIP, establezca el parámetro del temporizador de demora de preferencia de la dirección MAC virtual asociada. Puede establecer este parámetro cuando agregue la dirección, o puede modificar una dirección MAC virtual existente.

Para configurar el tiempo de demora de preferencia mediante la CLI:

- Para establecer el tiempo de demora de preferencia al agregar un MAC virtual, en el símbolo del sistema, escriba:
  - **add vRid** <secs> <id> -**preemptiondelaytimer**
  - **show vrID**
- Para establecer el tiempo de demora de preferencia al modificar un MAC virtual, en el símbolo del sistema, escriba:
  - **set vRid** <secs> <id> -**preemptiondelaytimer**
  - **show vrID**

Para configurar el tiempo de demora de preferencia mediante la interfaz gráfica de usuario:

1. Vaya a **Sistema** > **Red** > **VMAC**.
2. En la ficha **VMAC**. Mientras agrega un nuevo MAC virtual o modifica un MAC virtual existente, establezca el parámetro **Temporizador de demora de preferencia**.

Configuración de ejemplo:

La siguiente configuración utiliza los valores enumerados en la tabla de la sección Ejemplo: Retrasar preferencia.

```
    Settings on NS1

    > set vrid param  -deadInterval 1

    Done

    > add ns ip 192.0.1.10 255.255.255.255  -type VIP

    Done

    > add vrid 10  -Priority 100  -Preemption Enable  -
       preemptiondelaytimer 1000

    Done

    > bind ns ip 192.0.1.10 255.255.255.255  -vrid 10

    Done

    Settings on NS2

    > set vrid param  -deadInterval 2

    Done

    > add ns ip 192.0.1.10 255.255.255.255  -type VIP

    Done

    > add vrid 20  -Priority 200  -Preemption Enable  -
       preemptiondelaytimer 2000

    Done

    > set ns ip 192.0.1.10 255.255.255.255  -vrid 10

    Done
<!--NeedCopy-->
```


Configuración de la preferencia de demora para el modo activo-activo IPv6

Para configurar el tiempo de demora de preferencia para una dirección VIP6, establezca el parámetro del temporizador de demora de preferencia de la dirección MAC6 virtual asociada. Puede establecer este parámetro al agregar la dirección MAC6 virtual o modificar una dirección MAC6 virtual existente.

Para configurar el tiempo de demora de preferencia mediante la CLI:

- Para establecer el tiempo de demora de preferencia al agregar un MAC6 virtual, en el símbolo del sistema, escriba:
  - **add vRID6** <id> -**preemptiondelaytimer** <secs>
  - **show vrID6**
- Para establecer el tiempo de demora de preferencia al modificar un MAC6 virtual, en el símbolo del sistema, escriba:
  - **set vRID6** <secs> <id> -**preemptiondelaytimer**
  - **show vrID6**

Para configurar el tiempo de demora de preferencia mediante la interfaz gráfica de usuario:

1. Vaya a **Sistema** > **Red** > **VMAC**.
2. En la ficha **VMAC6**. Al agregar una dirección MAC6 virtual o modificar una dirección MAC6 virtual existente, establezca el parámetro **Preemption Delay Timer**.

Mantener una dirección VIP en estado de copia de seguridad

January 12, 2021

Puede forzar una dirección VIP a permanecer siempre en estado de copia de seguridad. Esta operación es útil para el mantenimiento o la prueba de una implementación VRRP.

Cuando una dirección VIP se ve obligada a permanecer en estado de copia de seguridad, no participa en transiciones de estado VRRP. Además, no puede convertirse en maestro incluso si todos los demás nodos bajan.

Para forzar que una dirección VIP permanezca en estado de copia de seguridad, establezca la prioridad de la dirección MAC virtual asociada en cero. Para asegurarse de que ninguna de las direcciones VIP de un nodo controla el tráfico durante un proceso de mantenimiento en el nodo, establezca todas las prioridades en cero.

Puede establecer la prioridad de una dirección MAC virtual mientras agrega o modifica la dirección.

Para forzar que una dirección VIP permanezca en el estado de copia de seguridad mediante la CLI:

- Para establecer la prioridad al agregar un MAC virtual, en el símbolo del sistema, escriba:

- **add vrID** <id> -**priority** 0
- **show vrID**

- Para establecer la prioridad al modificar un MAC virtual, en el símbolo del sistema, escriba:
  - **establecer vRid** <id> -**prioridad** 0
  - **show vrID**

Para forzar que una dirección VIP permanezca en estado de copia de seguridad mediante la interfaz gráfica de usuario:

1. Vaya a **Sistema** > **Red** > **VMAC**.
2. En la ficha **VMAC**, mientras agrega un nuevo MAC virtual o modifica un MAC virtual existente, establezca el parámetro **Priority** en cero.

Visualizador de red

January 12, 2021

El visualizador de red muestra una vista gráfica de todas las interfaces, canales, VLAN, direcciones IP y enlaces a VLAN en un dispositivo Citrix ADC. Una interfaz o canal habilitado tiene una etiqueta negra. Una interfaz o canal inhabilitados tiene una etiqueta roja.

Esta imagen completa de las conexiones de red del dispositivo puede ser útil para detectar defectos en el diseño de la red y para optimizar la red. También puede ayudar a un nuevo administrador a comprender fácilmente la configuración de red del dispositivo.

Para abrir el visualizador de red:

Vaya a **Sistema** > **Red**. En **Conexiones de monitor**, haga clic en **Visualizador de red**.

Configuración del Protocolo de Detección de Capa de Enlace

August 20, 2021

Citrix ADC es compatible con el protocolo de detección de capa de enlace (LLDP) estándar de la industria (IEEE 802.1AB). LLDP es un protocolo de capa 2 que permite al Citrix ADC anunciar su identidad y capacidades a los dispositivos conectados directamente, así como conocer la identidad y las capacidades de estos dispositivos vecinos.

> **Nota: El**
> Protocolo de detección de capas de enlace (LLDP) solo se admite en las plataformas Citrix ADC MPX.

Mediante LLDP, Citrix ADC transmite y recibe información en forma de mensajes LLDP conocidos como unidades de datos de paquetes LLDP (LLDPU). Un LLDPU es una secuencia de elementos de información de tipo, longitud, valor (TLV). Cada TLV contiene un tipo específico de información sobre el dispositivo que transmite el LLDPDU. Citrix ADC envía los siguientes TLV en cada LLDPU:

- ID del chasis
- ID de puerto
- Valor del tiempo de vida
- Nombre del sistema
- Descripción del sistema
- Descripción del puerto
- Capacidades del sistema
- Dirección de gestión
- ID de VLAN de puerto
- Agregación de enlaces

Nota: No puede especificar los TLV que se van a enviar en los mensajes LLDP.

Las interfaces Citrix ADC admiten los siguientes modos LLDP:

- **NINGUNO**. La interfaz no recibe ni transmite mensajes LLDP al dispositivo conectado directamente.
- **Transmisor**. La interfaz transmite mensajes LLDP al dispositivo conectado directamente, pero no recibe mensajes LLDP del dispositivo conectado directamente.
- **RECEPTOR**. La interfaz recibe mensajes LLDP desde el dispositivo conectado directamente, pero no transmite mensajes LLDP al dispositivo conectado directamente.
- **Transceptor**. La interfaz transmite mensajes LLDP y recibe mensajes LLDP desde el dispositivo conectado directamente.

El modo LLDP de una interfaz depende del modo LLDP configurado en los niveles global y de la interfaz. En la tabla siguiente se muestran los modos resultantes de las combinaciones disponibles de configuraciones a nivel global e interfaz: modos LLDP de interfaz y nivel global.

Tenga en cuenta los siguientes puntos relacionados con los mensajes LLDP transmitidos o recibidos por Citrix ADC:

- **Transmisión de mensajes LLDP.** Citrix ADC transmite LLDPU desde interfaces que funcionan en modo TRANSMISTER o TRANSPECTER LLDP.

  A continuación se presentan los parámetros globales de transmisión LLDP en Citrix ADC:

  - **Temporizador**. Intervalo, en segundos, entre LLDPU que el Citrix ADC envía a un dispositivo conectado directamente.
  - **Multiplicador de tiempo de retención**. Multiplicador para calcular la duración durante la cual el dispositivo receptor almacena la información LLDP en su base de datos antes de

descartarla o eliminarla. La duración se calcula como el valor del parámetro **Multiplicador de tiempo de retención** multiplicado por el valor del parámetro Timer.

- **Recepción de mensajes LLDP.** El Citrix ADC almacena la información de LLDPDU en su base de información de administración (MIB). La información LLDP almacenada se clasifica o agrupa bajo el ID de la interfaz que recibió el LLDPDU. El Citrix ADC conserva esta información LLDP durante la duración especificada en la LLDPU recibida.

  Si el ADC recibe otro LLDPDU en una interfaz antes de descartar la información LLDP almacenada para esa interfaz, el ADC reemplaza la información LLDP almacenada para esa interfaz por información en el nuevo LLDPDU.

Pasos de configuración

La configuración de LLDP en un dispositivo Citrix ADC consta de las siguientes tareas:

1. **Establecer parámetros LLDP de nivel global.** En esta tarea, establece los parámetros globales LLDP, como el temporizador LLDP, el multiplicador de tiempo de espera y el modo LLDP.
2. **Defina los parámetros LLDP del nivel de interfaz.** En esta tarea, se establece el modo LLDP para una interfaz.
3. **(Opcional) Muestra la información del dispositivo vecino.** Puede mostrar la información LLDP del dispositivo vecino recopilada en todas las interfaces de Citrix ADC, o simplemente la información LLDP recopilada en interfaces especificadas. Si no especifica una interfaz, la información se muestra para todas las interfaces.

Los siguientes son los requisitos previos para configurar LLDP en un dispositivo Citrix ADC:

1. Asegúrese de que comprende el protocolo LLDP estándar (IEEE 802.1AB).
2. Compruebe que ha configurado LLDP en los dispositivos conectados directamente deseados.

Procedimientos CLI

Para establecer parámetros LLDP de nivel global mediante la CLI:

En el símbolo del sistema, escriba:

- set lldp param [- [-holdTimeTXmult][-timer <positive_integer>] <positive_integer>[-Mode]<Mode>
- show lldp param

Para configurar una interfaz para LLDP mediante la CLI:

En el símbolo del sistema, escriba:

- set interface <id> -lldpmode <lldpmode>
- mostrar interfaz <id>

Para mostrar la información del dispositivo vecino mediante la CLI:

En el símbolo del sistema, escriba uno de los siguientes comandos:

- show lldp neighbors
- show lldp neighbors <ifnum>

Procedimientos de GUI

Para establecer los parámetros LLDP de nivel global mediante la GUI:

1. Vaya a Sistema > Red y haga clic en Configurar parámetros LLDP.
2. Defina los siguientes parámetros:
    - Multiplicador de temporizador de retención
    - Temporizador
    - Modo

Para configurar una interfaz para LLDP mediante la GUI:

Vaya a Sistema > Red > Interfaces, abra la interfaz y defina el parámetro de modo LLDP.

Para mostrar la información del dispositivo vecino mediante la GUI:

Vaya a Sistema > Red > Interfaces y, en la lista Acción, seleccione Ver vecinos LLDP.

Compatibilidad con LLDP en una configuración de clúster

En una configuración de clúster, la GUI y la CLI muestran la configuración de vecinos LLDP de todos o nodos de clúster específicos cuando se accede a la GUI o CLI a través de la dirección IP del clúster (CLIP). Cualquier cambio realizado en el modo LLDP de nivel global se aplica al modo LLDP de nivel global en cada uno de los nodos del clúster.

Considere un ejemplo de configuración de clúster de tres nodos, NS1, NS2 y NS3. Cada uno de estos nodos está conectado a ambos routers Router-1 y Router-2. El siguiente resultado se muestra cuando se realiza la operación **show lldp neighbor -summary** en la CLI del clúster a la que se accede a través de la dirección IP del clúster (CLIP) de la configuración del clúster. La salida muestra la información de vecino LLDP de todos estos nodos.

```
1 > show lldp neighbor -summary
2
3 Node Id: 1
4 ------------------------------------------------------------
5     Interface    ChassisId           PortId     System name
6 ------------------------------------------------------------
```



```
1     1/1/1      fe:c7:3b:13:bd:11    1/1          Router-1

2     1/1/2      12:68:7b:9e:4c:11    1/1          Router-2

Node Id: 2
-------------------------------------------------------------
    Interface    ChassisId           PortId     System name
-------------------------------------------------------------
1     2/1/1      fe:c7:3b:13:bd:12    1/2         Router-1

2     2/1/2      12:68:7b:9e:4c:12    1/2         Router-2

Node Id: 3
-------------------------------------------------------------
    Interface    ChassisId           PortId     System name
-------------------------------------------------------------

1     3/1/1       fe:c7:3b:13:bd:13    1/3         Router-1

2     3/1/2       12:68:7b:9e:4c:13    1/3         Router-2

Done
<!--NeedCopy-->
```

Marcos Jumbo

January 12, 2021

Los dispositivos Citrix ADC admiten la recepción y transmisión de tramas jumbo que contienen hasta 9216 bytes de datos IP. Las tramas gigantes pueden transferir archivos grandes de forma más eficiente de lo que es posible con el tamaño MTU IP estándar de 1500 bytes.

Un dispositivo Citrix ADC puede utilizar tramas jumbo en los siguientes casos de implementación:

- Jumbo a Jumbo. El dispositivo recibe datos como tramas jumbo y los envía como tramas jumbo.
- No Jumbo a Jumbo. El dispositivo recibe datos como tramas normales y los envía como tramas jumbo.
- Jumbo a No Jumbo. El dispositivo recibe datos como tramas gigantes y los envía como tramas normales.

El dispositivo Citrix ADC admite tramas jumbo en una configuración de equilibrio de carga para los siguientes protocolos:

- TCP
- Cualquier protocolo sobre TCP (por ejemplo, HTTP)
- SIP
- RADIUS

Configuración de compatibilidad con tramas gigantes en un dispositivo Citrix ADC

August 20, 2021

Para permitir que el dispositivo Citrix ADC admita tramas jumbo, configure la MTU en más de 1500 en interfaces o canales LA y en VLAN en las que quiere que el dispositivo Citrix ADC admita tramas jumbo.

Puntos a tener en cuenta antes de configurar la MTU de interfaces, canales LA o VLAN en un dispositivo Citrix ADC

1. Al crear un canal LA, el canal toma la MTU de la primera interfaz enlazada si no se especifica MTU para el canal.
2. La MTU de un canal se propaga a todas las interfaces enlazadas.
3. Cuando una interfaz está enlazada al canal cuya MTU es diferente de la MTU de la interfaz, la interfaz pasa a la lista inactiva.
4. Cuando se cambia la MTU de una interfaz miembro, la interfaz pasa a la lista inactiva.
5. Cuando una interfaz está independiente del canal, la interfaz conserva el valor de MTU del canal.
6. Puede establecer la MTU para una interfaz, canal o VLAN en un valor del rango de 1500-9216.
7. No se puede establecer la MTU en la VLAN predeterminada. El dispositivo Citrix ADC utiliza la MTU de la interfaz a través de la cual recibe o envía datos desde o hacia la VLAN predeterminada.
8. Para el tráfico basado en TCP en una configuración de equilibrio de carga en un dispositivo Citrix ADC, los MSS se establecen en consecuencia en cada punto final para admitir tramas jumbo:
    - Para una conexión entre un cliente y un servidor virtual de equilibrio de carga en el dispositivo Citrix ADC, el MSS del dispositivo Citrix ADC se establece en un perfil TCP, que luego se enlaza al servidor virtual de equilibrio de carga.
    - Para una conexión entre el dispositivo Citrix ADC y un servidor, el MSS en NS1 se establece en un perfil TCP, que luego se vincula al servicio que representa el servidor en el dispositivo Citrix ADC.
    - De forma predeterminada, un perfil TCP nstcp_default_profile está enlazado a todos los servidores y servicios de equilibrio de carga basados en TCP del dispositivo Citrix ADC.

- Para admitir tramas jumbo, puede cambiar el valor MSS del perfil TCP nstcp_default_profile o crear un perfil TCP personalizado y establecer su MSS en consecuencia y, a continuación, enlazar el perfil TCP personalizado a los servidores y servicios virtuales de equilibrio de carga deseados.
- El valor MSS predeterminado de cualquier perfil TCP es 1460.

Procedimientos CLI

Para establecer la MTU de una interfaz mediante la CLI:

En el símbolo del sistema, escriba:

- <positive_integer>set interface <id> -mtu
- mostrar interfaz <id>

Ejemplo:

```
1 > set interface 10/1  - mtu 9000
2 Done
3 <!--NeedCopy-->
```

Para establecer la MTU de un canal mediante la CLI:

En el símbolo del sistema, escriba:

- <positive_integer>set channel <id> -mtu
- show channel <id>

Ejemplo:

```
1 > set channel LA/1  - mtu 9000
2 Done
3 <!--NeedCopy-->
```

Para establecer la MTU de una VLAN mediante la CLI:

En el símbolo del sistema, escriba:

- <positive_integer>add vlan <id> -mtu
- mostrar vlan <id>

Ejemplo:


```
> set vlan 20  - mtu 9000
Done
<!--NeedCopy-->
```

Procedimientos de GUI

Para establecer la MTU de una interfaz mediante la GUI:

Vaya a Sistema > Red > Interfaces, abra la interfaz y defina el parámetro Unidad máxima de transmisión.

Para establecer la MTU de un canal mediante la GUI:

Vaya a Sistema > Red > Canales, abra el canal y defina el parámetro Unidad de transmisión máxima.

Para establecer la MTU de una VLAN mediante la GUI:

Vaya a Sistema > Red > VLAN, abra la VLAN y establezca el parámetro Unidad de transmisión máxima.

Caso de uso 1: Configuración de Jumbo a Jumbo

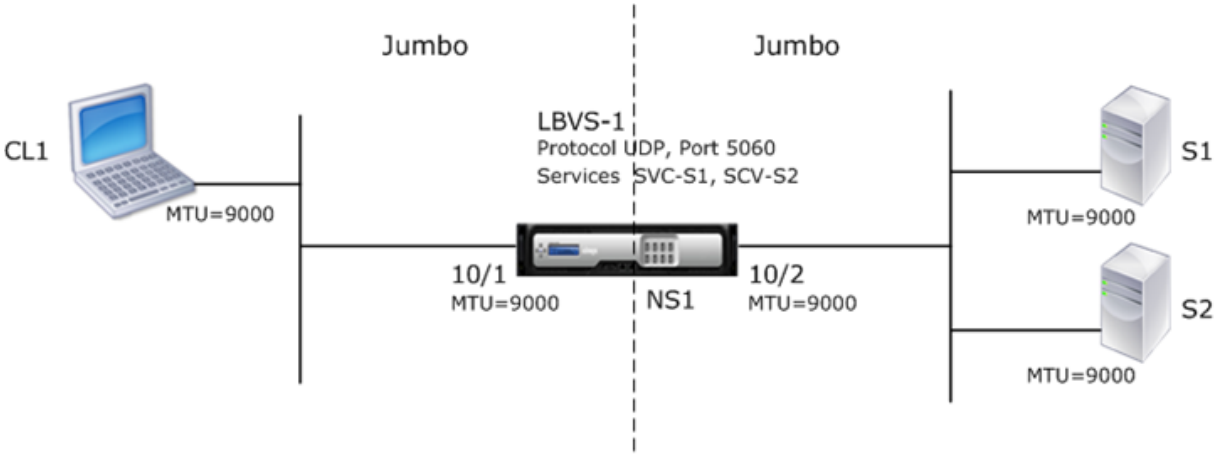
August 20, 2021

Considere un ejemplo de una configuración jumbo a jumbo en la que el servidor virtual de equilibrio de carga SIP LBVS-1, configurado en el dispositivo Citrix ADC NS1, se utiliza para equilibrar la carga del tráfico SIP en los servidores S1 y S2. La conexión entre el cliente CL1 y NS1 y la conexión entre NS1 y los servidores admiten tramas gigantes.

La interfaz 10/1 de NS1 recibe o envía tráfico desde o hacia el cliente CL1. La interfaz 10/2 de NS1 recibe o envía tráfico desde o hacia el servidor S1 o S2. Las interfaces 10/1 y 10/2 de NS1 forman parte de VLAN 10 y VLAN 20, respectivamente.

Para admitir tramas jumbo, la MTU se establece en 9216, en NS1, para las interfaces 10/1, 10/2 y VLAN VLAN 10, VLAN 20.

Todos los demás dispositivos de red, incluidos CL1, S1, S2, en este ejemplo de configuración también están configurados para admitir tramas gigantes.



En la tabla siguiente se enumeran los parámetros utilizados en el ejemplo.

Entidad	Nombre	Detalles
Dirección IP del cliente CL1	-	192.0.2.10
Dirección IP de los servidores	S1	198.51.100.19
	S2	198.51.100.20
Dirección SNIP en NS1		198.51.100.18
MTU especificada para interfaces y VLAN en NS1	10/1	9000
	10/2	9000
	VLAN 10	9000
	VLAN 20	9000
Servicios en NS1 que representan servidores	SVC-S1	**Dirección IP:** 198.51.100.19, **Protocolo:** SIP, **Puerto:** 5060
	SVC-S2	**Dirección IP:** 198.51.100.20, **Protocolo:** SIP, **Puerto:** 5060
Servidor virtual de equilibrio de carga en VLAN 10	LBVS-1	**Dirección IP:** 203.0.113.15, **Protocolo:** SIP, **Puerto:** 5060, **Servicios enlazados:** SVC-S1, SVC-S2

A continuación se presenta el flujo de tráfico de la solicitud de CL1 a NS1:

1. CL1 crea una solicitud SIP de 20000 bytes para enviarla a LBVS-1 de NS1.
2. CL1 envía los datos de solicitud en fragmentos IP a LBVS-1. El tamaño de cada fragmento IP es

igual o menor que la MTU (9000) establecida en la interfaz desde la que CL1 envía estos fragmentos a NS1.

- Tamaño del primer fragmento [IP = encabezado IP+encabezado UDP +segmento de datos SIP] = [20 + 8 + 8972] = 9000
- Tamaño del segundo fragmento IP = [encabezado IP + segmento de datos SIP] = [20 + 8980] = 9000
- Tamaño del último fragmento de IP[encabezado IP + segmento de datos SIP] = [20 + 2048] = 2068

3. NS1 recibe los fragmentos IP de solicitud en la interfaz 10/1. NS1 acepta estos fragmentos, porque el tamaño de cada uno de estos fragmentos es igual o menor que la MTU (9000) de la interfaz 10/1.
4. NS1 vuelve a ensamblar estos fragmentos IP para formar la solicitud SIP de 20000 bytes. NS1 procesa esta solicitud.
5. El algoritmo de equilibrio de carga de LBVS-1 selecciona el servidor S1.
6. NS1 envía los datos de solicitud en fragmentos IP a S1. El tamaño de cada fragmento IP es igual o menor que la MTU (9000) de la interfaz 10/2, desde la cual NS1 envía estos fragmentos a S1. Los paquetes IP se originan con una dirección SNIP de NS1.

   - Tamaño del primer fragmento IP = [IP = encabezado IP+encabezado UDP +segmento de datos SIP] = [20 + 8 + 8972] = 9000
   - Tamaño del segundo fragmento IP = [encabezado IP + segmento de datos SIP] = [20 + 8980] = 9000
   - Tamaño del último fragmento de IP = [encabezado IP + segmento de datos SIP] = [20 + 2048] = 2068

A continuación se presenta el flujo de tráfico de la respuesta de S1 a CL1 en este ejemplo:

1. El servidor S1 crea una respuesta SIP de 30000 bytes para enviarla a la dirección SNIP de NS1.
2. S1 envía los datos de respuesta en fragmentos IP a la dirección SNIP de NS1. El tamaño de cada fragmento IP es igual o menor que la MTU (9000) establecida en la interfaz desde la que S1 envía estos fragmentos a NS1.

   - Tamaño del primer fragmento IP = [IP = encabezado IP+encabezado UDP +segmento de datos SIP] = [20 + 8 + 8972] = 9000
   - Tamaño del segundo y tercer fragmento IP = [encabezado IP + segmento de datos SIP] = [20 + 8980] = 9000
   - Tamaño del último fragmento de IP[encabezado IP + segmento de datos SIP] = [20 + 3068] = 3088

3. NS1 recibe los fragmentos IP de respuesta en la interfaz 10/2. NS1 acepta estos fragmentos, porque el tamaño de cada fragmento es igual o menor que la MTU (9000) de la interfaz 10/2.

4. NS1 vuelve a ensamblar estos fragmentos IP para formar la respuesta SIP de 30000 bytes. NS1 procesa esta respuesta.
5. NS1 envía los datos de respuesta en fragmentos IP a CL1. El tamaño de cada fragmento IP es igual o menor que la MTU (9000) de la interfaz 10/1, desde la cual NS1 envía estos fragmentos a CL1. Los fragmentos IP se originan con la dirección IP de LBVS-1.
    - Tamaño del primer fragmento IP = [IP = encabezado IP+encabezado UDP +segmento de datos SIP] = [20 + 8 + 8972] = 9000
    - Tamaño del segundo y tercer fragmento IP = [encabezado IP + segmento de datos SIP] = [20 + 8980] = 9000
    - Tamaño del último fragmento de IP = [encabezado IP + segmento de datos SIP] = [20 + 3068] = 3088

Tareas de configuración

En la tabla siguiente se enumeran las tareas, los comandos de Citrix ADC y los ejemplos para crear la configuración necesaria en el dispositivo Citrix ADC.

Tarea	Sintaxis de comandos de Citrix ADC	Ejemplo
Establecer la MTU de las interfaces deseadas para admitir tramas jumbo	set interface <id> -mtu <positive_integer>, show interface <id>	set int 10/1 -mtu 9000 set int 10/2 -mtu 9000
Cree VLAN y configure la MTU de las VLAN deseadas para admitir tramas jumbo	add vlan <id> -mtu <positive_integer>, show vlan <id>	add vlan 10 -mtu 9000 add vlan 20 -mtu 9000
Vincular interfaces a VLAN	bind vlan <id> -ifnum <interface_name>, show vlan <id>	bind vlan 10 -ifnum 10/1 bind vlan 20 -ifnum 10/2
Agregar una dirección SNIP	add ns ip <IPAddress> <netmask> -type SNIP, show ns ip	add ns ip 198.51.100.18 255.255.255.0 -type SNIP
Crear servicios que representen servidores SIP	add service <serviceName> <ip> SIP_UDP <port>, show service <name>	add service SVC-S1 198.51.100.19 SIP_UDP 5060 add service SVC-S2 198.51.100.20 SIP_UDP 5060

Tarea	Sintaxis de comandos de Citrix ADC	Ejemplo
Cree servidores virtuales de equilibrio de carga SIP y enlace los servicios con él.	<name>add lb vserver <name> SIP_UDP <ip> <port> bind lb vserver <vserverName> <serviceName>, show lb vserver	add lb vserver LBVS-1 SIP_UDP 203.0.113.15 5060 enlace lb vserver LBVS-1 SVC-S1 enlace lb vserver LBVS-1 SVC-S2
Guardar la configuración	save ns config, show ns config	

Caso de uso 2: Configuración de no Jumbo a Jumbo

August 20, 2021

Considere un ejemplo de una configuración normal a jumbo en la que el servidor virtual de equilibrio de carga LBVS-1, configurado en un dispositivo Citrix ADC NS1, se utiliza para equilibrar la carga entre los servidores S1 y S2. La conexión entre el cliente CL1 y NS1 admite tramas normales, y la conexión entre NS1 y los servidores admite tramas jumbo.

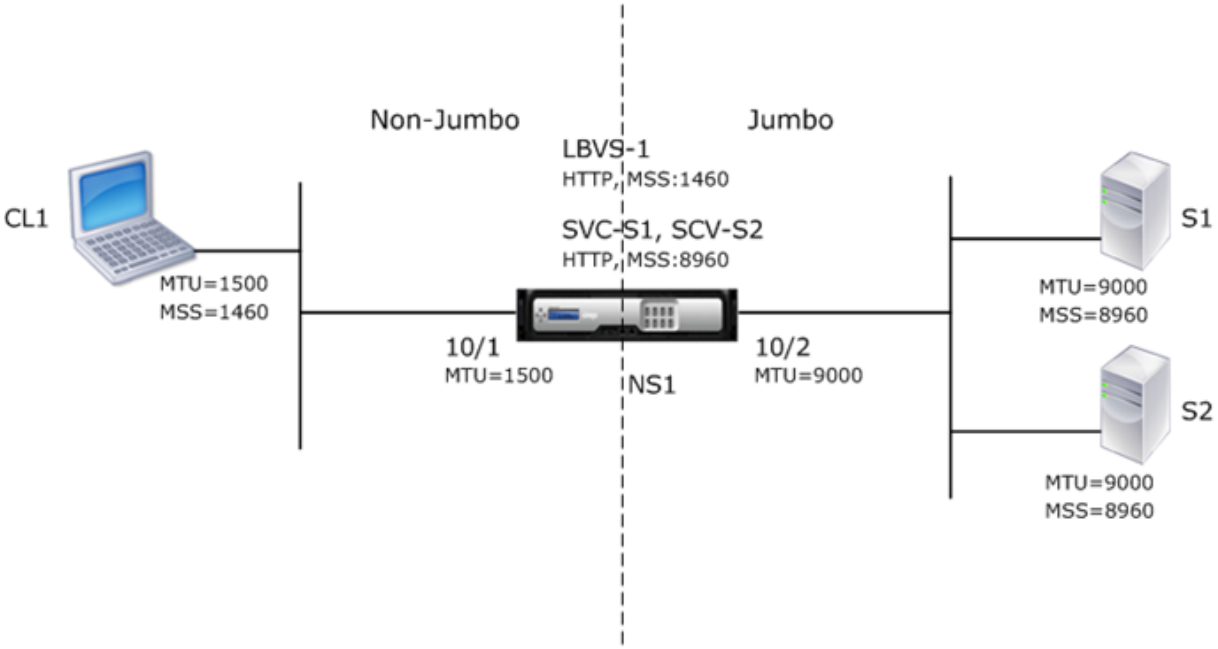
La interfaz 10/1 de NS1 recibe o envía tráfico desde o hacia el cliente CL1. La interfaz 10/2 de NS1 recibe o envía tráfico desde o hacia el servidor S1 o S2.

Las interfaces 10/1 y 10/2 de NS1 forman parte de VLAN 10 y VLAN 20, respectivamente. Para admitir solo tramas regulares entre CL1 y NS1, la MTU se establece en el valor predeterminado de 1500 tanto para la interfaz 10/1 como para la VLAN 10

Para admitir tramas gigantes entre NS1 y los servidores, la MTU se establece en 9000 para la interfaz 10/2 y VLAN 20. Los servidores y todos los demás dispositivos de red entre NS1 y los servidores también están configurados para admitir tramas gigantes.

Dado que el tráfico HTTP se basa en TCP, MSS se establecen en consecuencia en cada punto final para admitir tramas gigantes.

- Para admitir tramas jumbo para la conexión entre una dirección SNIP de NS1 y S1 o S2, el MSS en NS1 se establece en consecuencia en un perfil TCP personalizado, que está vinculado a los servicios (SVC-S1 y SVC-S1) que representan S1 y S2 en NS1.
- Para admitir solo tramas normales para la conexión entre CL1 y el servidor virtual LBVS-1 de NS1, se utiliza el perfil TCP predeterminado nstcp_default_profile que está enlazado de forma predeterminada a LBVS-1 y tiene el MSS establecido en el valor predeterminado de 1460.



En la tabla siguiente se enumeran los parámetros utilizados en este ejemplo.

Entidad	Nombre	Detalles
Dirección IP del cliente CL1		192.0.2.10
Dirección IP de los servidores	S1	198.51.100.19
	S2	198.51.100.20
Dirección SNIP en NS1		198.51.100.18
MTU especificada para interfaces y VLAN en NS1	10/1	1500
	10/2	9000
	VLAN 10	1500
	VLAN 20	9000
Perfil TCP predeterminado	nstcp_default_profile	MSS:1460
Perfil TCP personalizado	NS1-SERVERS-JUMBO	MSS: 8960
Servicios en NS1 que representan servidores	SVC-S1	Dirección IP: 198.51.100.19, Protocolo: HTTP, Puerto: 80, Perfil TCP: NS1-SERVERS-JUMBO (MSS: 8960)

Entidad	Nombre	Detalles
	SVC-S2	Dirección IP: 198.51.100.20, Protocolo: HTTP, Puerto: 80, Perfil TCP: NS1-SERVERS-JUMBO (MSS: 8960)
Servidor virtual de equilibrio de carga en VLAN 10	LBVS-1	Dirección IP = 203.0.113.15, Protocolo: HTTP, Puerto: 80, Servicios enlazados: SVC-S1, SVC-S2, Perfil TCP: Nstcp_default_profile (MSS:1460)

A continuación se presenta el flujo de tráfico de la solicitud de CL1 a S1 en este ejemplo:

1. El cliente CL1 crea una solicitud HTTP de 200 bytes para enviarla al servidor virtual LBVS-1 de NS1.
2. CL1 abre una conexión a LBVS-1 de NS1. CL1 y NS1 intercambian sus respectivos valores TCP MSS al establecer la conexión.
3. Dado que el MSS de NS1 es mayor que la solicitud HTTP, CL1 envía los datos de solicitud en un único paquete IP a NS1.

   Tamaño del paquete de solicitud = [Encabezado IP+Encabezado TCP + Solicitud TCP] = [20 + 20 + 200] = 240
4. NS1 recibe el paquete de solicitud en la interfaz 10/1 y, a continuación, procesa los datos de solicitud HTTP en el paquete.
5. El algoritmo de equilibrio de carga de LBVS-1 selecciona el servidor S1 y NS1 abre una conexión entre una de sus direcciones SNIP y S1. NS1 y CL1 intercambian sus respectivos valores TCP MSS al establecer la conexión.
6. Dado que el MSS de S1 es mayor que la solicitud HTTP, NS1 envía los datos de solicitud en un único paquete IP a S1.

   Tamaño del paquete de solicitud = [Encabezado IP+Encabezado TCP + [Solicitud TCP][20 + 20 + 200] = 240

A continuación se presenta el flujo de tráfico de la respuesta de S1 a CL1 en este ejemplo:

1. El servidor S1 crea una respuesta HTTP de 18000 bytes para enviarla a la dirección SNIP de NS1.

2. S1 segmenta los datos de respuesta en múltiplos del MSS de NS1 y envía estos segmentos en paquetes IP a NS1. Estos paquetes IP provienen de la dirección IP de S1 y están destinados a la dirección SNIP de NS1.
    - Tamaño de los dos primeros paquetes = [encabezado IP+encabezado TCP + (segmento TCP = tamaño MSS de NS1)] = [20 + 20 + 8960] = 9000
    - Tamaño del último paquete = [Encabezado IP + Encabezado TCP + (segmento TCP restante)] = [20 + 20 + 2080] = 2120
3. NS1 recibe los paquetes de respuesta en la interfaz 10/2.
4. A partir de estos paquetes IP, NS1 ensambla todos los segmentos TCP para formar los datos de respuesta HTTP de 18000 bytes. NS1 procesa esta respuesta.
5. NS1 segmenta los datos de respuesta en múltiplos del MSS de CL1 y envía estos segmentos en paquetes IP, desde la interfaz 10/1 hasta CL1. Estos paquetes IP provienen de la dirección IP de LBVS-1 y están destinados a la dirección IP de CL1.
    - Tamaño de todos los paquetes excepto el último = [encabezado IP+encabezado TCP + (carga útil TCP = tamaño MSS de CL1)] = [20 + 20 + 1460] = 1500
    - Tamaño del último paquete = [Encabezado IP + Encabezado TCP + (segmento TCP restante)] = [20 + 20 + 480] = 520

Tareas de configuración

En la tabla siguiente se enumeran las tareas, los comandos de Citrix ADC y los ejemplos para crear la configuración necesaria en el dispositivo Citrix ADC.

Tareas	Sintaxis CLI	Ejemplos
Establecer la MTU de las interfaces deseadas para admitir tramas jumbo	set interface <id> -mtu <positive_integer>, show interface <id>	set int 10/1 -mtu 1500 set int 10/2 -mtu 9000
Cree VLAN y configure la MTU de las VLAN deseadas para admitir tramas jumbo	add vlan <id> -mtu <positive_integer>, show vlan <id>	add vlan 10 -mtu 1500 add vlan 20 -mtu 9000
Vincular interfaces a VLAN	bind vlan <id> -ifnum <interface_name>, show vlan <id>	bind vlan 10 -ifnum 10/1 bind vlan 20 -ifnum 10/2
Agregar una dirección SNIP	add ns ip <IPAddress> <netmask> -type SNIP, show ns ip	add ns ip 198.51.100.18 255.255.255.0 -type SNIP

Tareas	Sintaxis CLI	Ejemplos
Cree servicios que representan servidores HTTP.	add service <serviceName> <ip> HTTP <port>, show service <name>	add service SVC-S1 198.51.100.19 http 80, add service SVC-S2 198.51.100.20 http 80
Cree servidores virtuales de equilibrio de carga HTTP y enlace los servicios con él.	<name>add lb vserver <name> HTTP <ip> <port>, bind lb vserver <vserverName> <serviceName>, show lb vserver	add lb vserver LBVS-1 http 203.0.113.15 80, enlazar lb vserver LBVS-1 SVC-S1, enlazar lb vserver LBVS-1 SVC-S2
Crear un perfil TCP personalizado y establecer su MSS para admitir tramas jumbo	<name>add tcpProfile <name> -mss <positive_integer>, show tcpProfile	agregar tcpprofile NS1-SERVERS-JUMBO -mss 8960
Enlazar el perfil TCP personalizado a los servicios deseados	<name>set service <Name> -tcpProfileName <string>, show service	establecer servicio SVC-S1 -TCPProfileName NS1-SERVERS-JUMBO, establecer servicio SVC-S2 -TCPProfileName NS1-SERVERS-JUMBO
Guardar la configuración	save ns config, show ns config	

Caso de uso 3: Coexistencia de flujos Jumbo y no Jumbo en el mismo conjunto de interfaces

August 20, 2021

Considere un ejemplo en el que los servidores virtuales de equilibrio de carga LBVS-1 y LBVS-2 están configurados en el dispositivo Citrix ADC NS1. LBVS-1 se utiliza para equilibrar la carga del tráfico HTTP entre los servidores S1 y S2, y LBVS-2 se utiliza para equilibrar la carga del tráfico entre los servidores S3 y S4.

CL1 está en VLAN 10, S1 y S2 en VLAN20, CL2 en VLAN 30 y S3 y S4 en VLAN 40. VLAN 10 y VLAN 20 admiten tramas gigantes, y VLAN 30 y VLAN 40 solo admiten tramas normales.

En otras palabras, la conexión entre CL1 y NS1 y la conexión entre NS1 y el servidor S1 o S2 admiten tra-

mas gigantes. La conexión entre CL2 y NS1, y la conexión entre NS1 y el servidor S3 o S4 solo admiten tramas normales.

La interfaz 10/1 de NS1 recibe o envía tráfico desde o hacia clientes. La interfaz 10/2 de NS1 recibe o envía tráfico desde o hacia los servidores.

La interfaz 10/1 está enlazada tanto a la VLAN 10 como a la VLAN 30 como una interfaz etiquetada, y la interfaz 10/2 está enlazada tanto a la VLAN 20 como a la VLAN 40 como una interfaz etiquetada.

Para admitir tramas gigantes, la MTU se establece en 9216 para las interfaces 10/1 y 10/2.

En NS1, la MTU se establece en 9000 para VLAN 10 y VLAN 20 para admitir tramas jumbo, y la MTU se establece en el valor predeterminado de 1500 para VLAN 30 y VLAN 40 para admitir solo tramas normales.

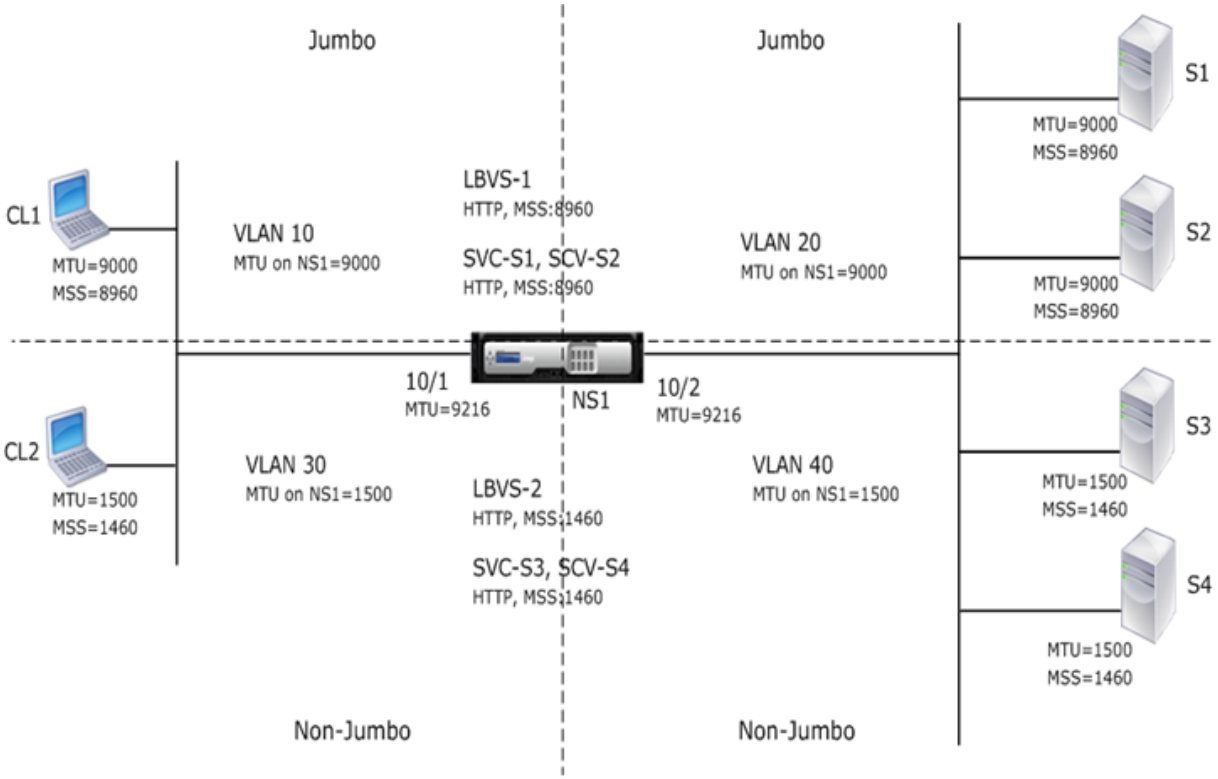
La MTU efectiva en una interfaz Citrix ADC para paquetes etiquetados de VLAN es de la MTU de la interfaz o de la MTU de la VLAN, lo que sea inferior. Por ejemplo:

- La MTU de la interfaz 10/1 es 9216. La MTU de la VLAN 10 es 9000. En la interfaz 10/1, la MTU de los paquetes etiquetados de VLAN 10 es 9000.
- La MTU de la interfaz 10/2 es 9216. La MTU de la VLAN 20 es 9000. En la interfaz 10/2, la MTU de los paquetes etiquetados de VLAN 20 es 9000.
- La MTU de la interfaz 10/1 es 9216. La MTU de la VLAN 30 es 1500. En la interfaz 10/1, la MTU de los paquetes etiquetados de VLAN 30 es 1500.
- La MTU de la interfaz 10/2 es 9216. La MTU de la VLAN 40 es 1500. En la interfaz 10/2, la MTU de los paquetes etiquetados de VLAN 40 es 9000.

CL1, S1, S2 y todos los dispositivos de red entre CL1 y S1 o S2 están configurados para tramas gigantes.

Dado que el tráfico HTTP se basa en TCP, MSS se establecen en consecuencia en cada punto final para admitir tramas gigantes.

- Para la conexión entre CL1 y el servidor virtual LBVS-1 de NS1, el MSS en NS1 se establece en un perfil TCP, que luego está enlazado a LBVS-1.
- Para la conexión entre una dirección SNIP de NS1 y S1, el MSS en NS1 se establece en un perfil TCP, que luego se vincula al servicio (SVC-S1) que representa a S1 en NS1.



En la tabla siguiente se enumeran los ajustes utilizados en este ejemplo: configuración de ejemplo de caso de uso 3 de marcos gigantes.

A continuación se presenta el flujo de tráfico de la solicitud de CL1 a S1:

1. Cliente CL1 crea una solicitud HTTP de 20000 bytes para enviar al servidor virtual LBVS-1 de NS1.
2. CL1 abre una conexión a LBVS-1 de NS1. CL1 y NS1 intercambian sus valores TCP MSS mientras establecen la conexión.
3. Dado que el valor MSS de NS1 es menor que la solicitud HTTP, CL1 segmenta los datos de solicitud en múltiplos de MSS de NS1 y envía estos segmentos en paquetes IP etiquetados como VLAN 10 a NS1.
    - Tamaño de los dos primeros paquetes = [Encabezado IP + Encabezado TCP + (Segmento TCP = NS1 MSS)] = [20 + 20 + 8960] = 9000
    - Tamaño del último paquete = [Encabezado IP + Encabezado TCP + (segmento TCP restante)] = [20 + 20 + 2080] = 2120
4. NS1 recibe estos paquetes en la interfaz 10/1. NS1 acepta estos paquetes porque el tamaño de estos paquetes es igual o menor que la MTU efectiva (9000) de la interfaz 10/1 para los paquetes etiquetados de VLAN 10.
5. Desde los paquetes IP, NS1 ensambla todos los segmentos TCP para formar la solicitud HTTP de 20000 bytes. NS1 procesa esta solicitud.
6. El algoritmo de equilibrio de carga de LBVS-1 selecciona el servidor S1 y NS1 abre una conexión entre una de sus direcciones SNIP y S1. NS1 y CL1 intercambian sus respectivos valores TCP MSS

al establecer la conexión.

7. NS1 segmenta los datos de solicitud en múltiplos del MSS de S1 y envía estos segmentos en paquetes IP etiquetados como VLAN 20 a S1.
    - Tamaño de los dos primeros paquetes = [Encabezado IP + Encabezado TCP + (Carga útil TCP = S1 MSS)] = [20 + 20 + 8960] = 9000
    - Tamaño del último paquete = [Encabezado IP + Encabezado TCP + (segmento TCP restante)] = [20 + 20 + 2080] = 2120

A continuación se presenta el flujo de tráfico de la respuesta de S1 a CL1:

1. El servidor S1 crea una respuesta HTTP de 30000 bytes para enviarla a la dirección SNIP de NS1.
2. S1 segmenta los datos de respuesta en múltiplos del MSS de NS1 y envía estos segmentos en paquetes IP etiquetados como VLAN 20 a NS1. Estos paquetes IP provienen de la dirección IP de S1 y están destinados a la dirección SNIP de NS1.
    - Tamaño de los tres primeros paquetes = [Encabezado IP+Encabezado TCP + (Segmento TCP = tamaño MSS de NS1)][20 + 20 + 8960] = 9000
    - Tamaño del último paquete = [Encabezado IP + Encabezado TCP + (segmento TCP restante)] = [20 + 20 + 3120] = 3160
3. NS1 recibe los paquetes de respuesta en la interfaz 10/2. NS1 acepta estos paquetes, porque su tamaño es igual o inferior al valor de MTU efectivo (9000) de la interfaz 10/2 para paquetes etiquetados de VLAN 20.
4. A partir de estos paquetes IP, NS1 ensambla todos los segmentos TCP para formar la respuesta HTTP de 30000 bytes. NS1 procesa esta respuesta.
5. NS1 segmenta los datos de respuesta en múltiplos del MSS de CL1 y envía estos segmentos en paquetes IP etiquetados como VLAN 10, desde la interfaz 10/1 hasta CL1. Estos paquetes IP provienen de la dirección IP de LBVS y están destinados a la dirección IP de CL1.
    - Tamaño de los tres primeros paquetes = [Encabezado IP + Encabezado TCP + [(Carga útil TCP = tamaño MSS de CL1)][20 + 20 + 8960] = 9000
    - Tamaño del último paquete = [Encabezado IP + Encabezado TCP + (segmento TCP restante)] = [20 + 20 + 3120] = 3160

Tareas de configuración

En la tabla siguiente se enumeran las tareas, los comandos y los ejemplos para crear la configuración necesaria en el dispositivo Citrix ADC: tareas de configuración del caso de uso 3 de tramas gigantes.

Compatibilidad con Citrix ADC para la implementación de Microsoft Direct Access

August 20, 2021

Microsoft Direct Access es una tecnología que permite a los usuarios remotos conectarse sin problemas y de forma segura a las redes internas de la empresa, sin necesidad de establecer una conexión VPN independiente. A diferencia de las conexiones VPN, que requieren la intervención del usuario para abrir y cerrar conexiones, un cliente habilitado para acceso directo se conecta automáticamente a las redes internas de la empresa cada vez que el cliente se conecta a Internet.

Administración de salida es una función de Microsoft Direct Access que permite a los administradores de la red empresarial conectarse a clientes de Direct Access fuera de la red y administrarlos (por ejemplo, realizar tareas de administración, como programar actualizaciones de servicios y proporcionar soporte remoto.

En una implementación de Direct Access, los dispositivos Citrix ADC proporcionan alta disponibilidad, escalabilidad, alto rendimiento y seguridad. La funcionalidad de equilibrio de carga de Citrix ADC envía tráfico de cliente a través del servidor más adecuado. Los dispositivos también pueden reenviar el tráfico de administración de salida a través de la ruta correcta para llegar al cliente.

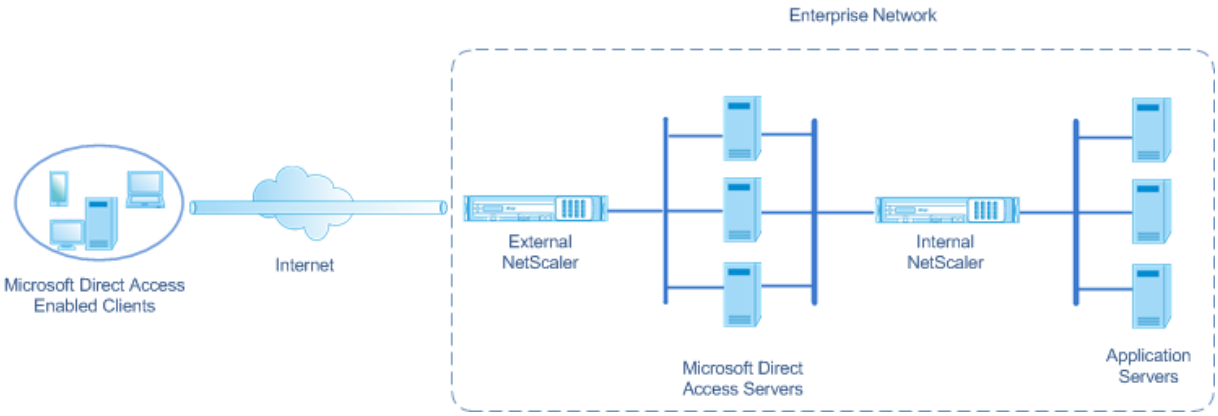
Arquitectura

La arquitectura de una implementación de Microsoft Direct Access consta de clientes habilitados para Direct Access, servidores de Direct Access, servidores de aplicaciones y dispositivos Citrix ADC internos y externos. Los clientes se conectan a un servidor de aplicaciones a través de un servidor de acceso directo. Un dispositivo Citrix ADC externo equilibra el tráfico del cliente a un servidor de Direct Access y un dispositivo interno Citrix ADC reenvía el tráfico del cliente desde el servidor de Direct Access al servidor de aplicaciones de destino. El acceso directo se utiliza para tunelizar el tráfico IPv6 del cliente a través de la red IPv4. Un servidor virtual de equilibrio de carga IPv4 en el dispositivo Citrix ADC externo equilibra el tráfico tunelizado del cliente con uno de los servidores de Direct Access. El servidor de acceso directo extrae los paquetes IPv6 de los paquetes IPv4 del cliente recibido y los envía al servidor de aplicaciones de destino a través del dispositivo Citrix ADC interno. El dispositivo interno Citrix ADC tiene reglas de sesión de reenvío con la opción de caché de ruta de origen habilitada para almacenar información de conexión de capa 2 y capa 3 sobre el tráfico del cliente desde el servidor de acceso directo. El dispositivo Citrix ADC almacena la siguiente información de capa 2 y capa 3 en una tabla denominada tabla de caché de ruta de origen:

- Dirección IP de origen del paquete recibido
- Dirección MAC del servidor de acceso directo que envió el paquete
- ID de VLAN del dispositivo Citrix ADC que recibió el paquete

- Id. de interfaz del dispositivo Citrix ADC que recibió el paquete

El dispositivo Citrix ADC utiliza la información de la tabla de caché de ruta de origen para reenviar una respuesta al mismo servidor de Direct Access porque tiene la información de túnel para llegar al cliente. Además, el dispositivo interno utiliza la tabla de caché de ruta de origen para reenviar el tráfico de administración de salida del servidor de aplicaciones al servidor de acceso directo adecuado para llegar a un cliente concreto.



Configuración de Citrix ADC Appliance interno en una implementación de Microsoft Direct Access

Para configurar el dispositivo interno de Citrix ADC para reenviar la respuesta de un servidor de aplicaciones y el tráfico de administración de salida a la puerta de enlace de acceso directo correspondiente, configure las reglas de sesión de reenvío. En cada regla, establezca el parámetro sourceroutecache en ENABLED.

Para crear una regla de sesión de reenvío mediante la CLI:

En el símbolo del sistema, escriba:

- **add forwardingSession** <name>((<network>[]<netmask>) | **-acl6name** <string>| **-aclname** <string>) **-sourceroutecache** (**HABILITADO** |DESHABILITADO**]
- **show forwardingsession** <name>

Configuración de ejemplo:

En el ejemplo siguiente, se crea la regla de reenvío de sesión MS-DA-FW-1 en el dispositivo interno de Citrix ADC. La sesión de reenvío almacena información de capa 2 y capa 3 para cualquier paquete IPv6 entrante de un servidor de acceso directo que coincida con el prefijo IPv6 de origen 2001:DB8: :/96.

```
1 > add forwardingSession MS-DA-FW-1 2001:DB8::/96 -sourceroutecache -
    ENABLED
2  Done
```


Visualización de la tabla Caché de Ruta de Origen

Puede mostrar la tabla de caché de ruta de origen para supervisar o detectar conexiones no deseadas entre servidores de acceso directo y servidores de aplicaciones.

Para mostrar la tabla de caché de ruta de origen mediante la CLI:

En el símbolo del sistema, escriba:

- **show sourceroutecachetable**

Ejemplo:

```
> show sourceroutecachetable
SOURCEIP            MAC                 VLAN    INTERFACE
2001:DB8:5001:10    56:53:24:3d:02:eb    30        1/2
2001:DB8:5003:30    60:54:35:3e:04:bd    60        1/3
Done
```

Borrado de la tabla de caché de ruta de origen

Puede borrar todas las entradas de la tabla de caché de ruta de origen en un dispositivo Citrix ADC.

Para borrar la tabla de caché de ruta de origen mediante la CLI:

En el símbolo del sistema, escriba:

- **flush ns sourceroutecachetable**

Listas de control de acceso

August 20, 2021

Las listas de control de acceso (ACL) filtran el tráfico IP y protegen su red del acceso no autorizado. Una ACL es un conjunto de condiciones que el Citrix ADC evalúa para determinar si se permite el acceso. Por ejemplo, el departamento de Finanzas probablemente no quiera permitir que otros departamentos tengan acceso a sus recursos, como recursos humanos y documentación, y esos departamentos desean restringir el acceso a sus datos.

Cuando Citrix ADC recibe un paquete de datos, compara la información del paquete de datos con las condiciones especificadas en la ACL y permite o deniega el acceso. El administrador de la organización puede configurar las ACL para que funcionen en los siguientes modos de procesamiento:

- Permitir: Procesa el paquete.

- Puente: Puente del paquete al destino sin procesarlo. El paquete es enviado directamente por el reenvío de Capa 2 y Capa 3.
- Deny: Suelta el paquete.

Las reglas de ACL son el primer nivel de defensa en Citrix ADC.

Citrix ADC admite los siguientes tipos de ACL:

- **Las ACL simples** filtran los paquetes según su dirección IP de origen y, opcionalmente, su protocolo, puerto de destino o dominio de tráfico. Se elimina cualquier paquete que tenga las funciones especificadas en la ACL.
- **Las ACL ampliadas** filtran los paquetes de datos en función de varios parámetros, como la dirección IP de origen, el puerto de origen, la acción y el protocolo. Una ACL extendida define las condiciones que un paquete debe cumplir para que el Citrix ADC procese el paquete, realice un puente sobre el paquete o deje caer el paquete.

Nomenclatura

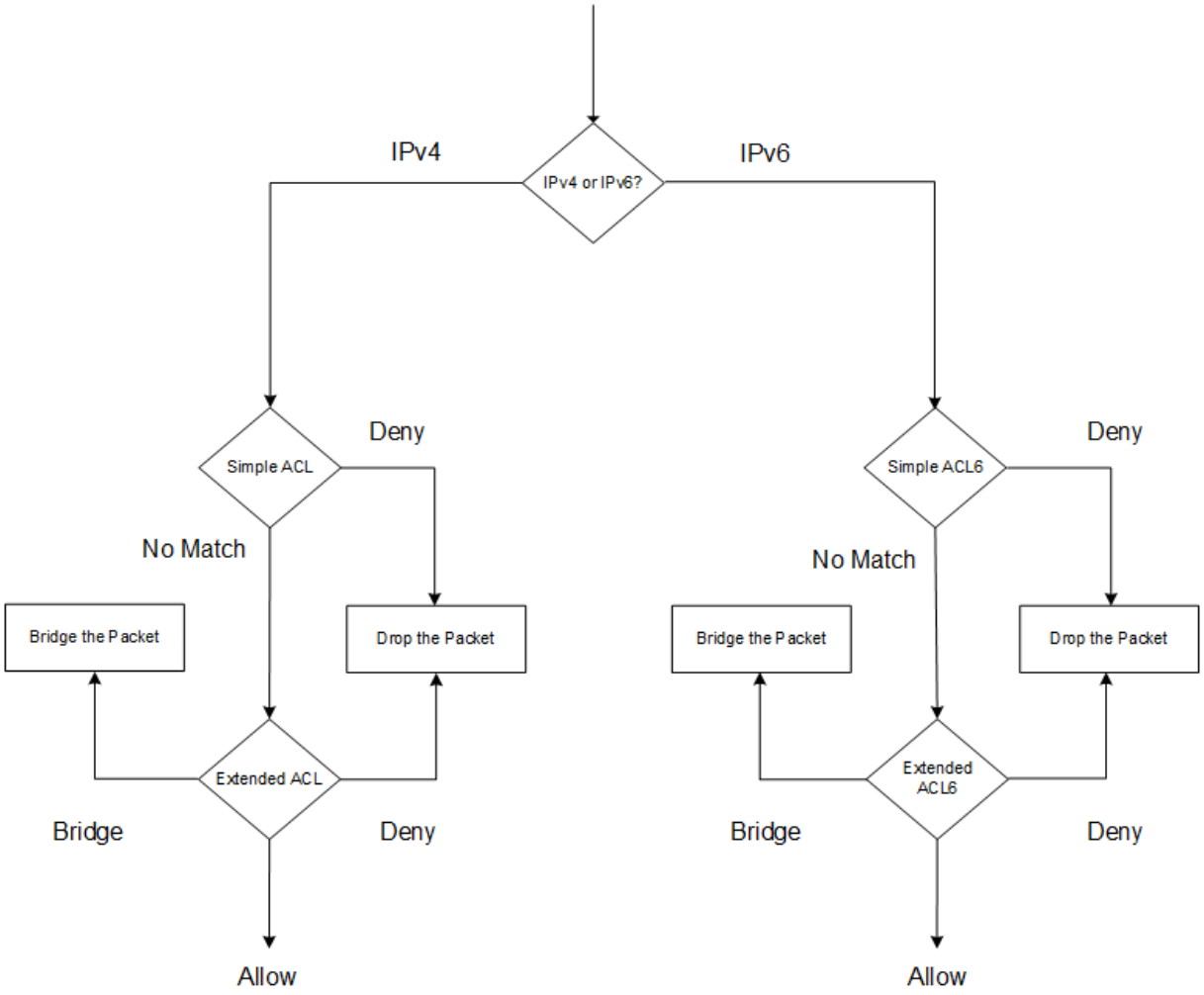
En las interfaces de usuario de Citrix ADC, los términos ACL simple y ACL extendida hacen referencia a ACL que procesan paquetes IPv4. Una ACL que procesa paquetes IPv6 se denomina ACL6 simple o ACL6 extendida. Al hablar de ambos tipos, esta documentación a veces se refiere a ambos como ACL simples o ACL extendidas.

Precedencia de ACL

Si se configuran las ACL simples y extendidas, los paquetes entrantes se comparan primero con las ACL simples.

El Citrix ADC determina primero si el paquete entrante es un paquete IPv4 o IPv6 y, a continuación, compara las funciones del paquete con ACL simples o ACL6s simples. Si se encuentra una coincidencia, se elimina el paquete. Si no se encuentra ninguna coincidencia, el paquete se compara con ACL extendidas o ACL6S extendidas. Si esa comparación da como resultado una coincidencia, el paquete se maneja como se especifica en la ACL. El paquete puede ser puenteado, descartado o permitido. Si no se encuentra ninguna coincidencia, se permite el paquete.

Ilustración 1. Secuencia de flujo de ACL simple y extendida



ACL simples y ACL6s simples

August 20, 2021

Una ACL simple o ACL6 simple utiliza pocos parámetros y solo se puede configurar para eliminar paquetes IP. Los paquetes se pueden eliminar en función de su dirección IP de origen y, opcionalmente, de su protocolo, puerto de destino o dominio de tráfico.

Al crear una ACL simple o ACL6 simple, puede especificar un tiempo de vida (TTL), en segundos, después del cual caduca la ACL. Las ACL con TTL no se guardan al guardar la configuración. Puede mostrar ACL simples y ACL6s simples para verificar su configuración, y puede mostrar sus estadísticas.

Configuración de ACL simples y ACL6s simples

La configuración de una ACL simple o ACL6 simple en un dispositivo Citrix ADC puede incluir las siguientes tareas.

- **Crear ACL simples o ACL6s**simples. Creación de ACL simples o ACL6 simples para eliminar (denegar) paquetes en función de su dirección IP de origen y, opcionalmente, en su protocolo, puerto de destino o dominio de tráfico.
- **Eliminar ACL simples o ACL6s**simples. Estas ACL no se pueden modificar una vez creadas. Si debe modificar una ACL simple o ACL6 simple, debe eliminarla y crear una.

Procedimientos CLI

Para crear una ACL simple mediante la CLI:

En el símbolo del sistema, escriba:

```
1 -  ns simpleacl <aclname> DENY -srcIP <ip_addr> [-destPort <port> -
     protocol ( TCP | UDP )] [-TTL <positive_integer>]
2 -  show ns simpleacl [<aclname>]
3 <!--NeedCopy-->
```

Ejemplo:

```
1 > add simpleacl rule1 DENY -srcIP 10.102.29.5 -TTL 600
2 Done
3 <!--NeedCopy-->
```

Para crear un ACL6 simple mediante la CLI:

En el símbolo del sistema, escriba:

```
1 -  add ns simpleacl6 <aclname> DENY - srcIPv6 <ipv6_addr|null> [-
     destPort <port> -protocol ( TCP | UDP )] [-TTL <positive_integer>]
2 -  show ns simpleacl6 [<aclname>]
3 <!--NeedCopy-->
```

Ejemplo:


```
1 >  add ns simpleacl6 rule1 DENY  -srcIPv6 3ffe:192:168:215::82 -
     destPort 80 -Protocol TCP -TTL 9000
2  Done
3 <!--NeedCopy-->
```

Para eliminar una ACL simple mediante la CLI:

En el símbolo del sistema, escriba:

- **rm ns simpleacl** <aclname>
- **show ns simpleacl**

Para eliminar un solo ACL6 simple mediante la CLI:

En el símbolo del sistema, escriba:

- **rm ns simpleacl6**<aclname>
- **show ns simpleacl6**

Para eliminar todas las ACL simples mediante la CLI:

En el símbolo del sistema, escriba:

- **claro ns simpleacl**
- **show ns simpleacl**

Para eliminar todos los ACL6s simples mediante la CLI:

En el símbolo del sistema, escriba:

- **claro ns simpleacl6**
- **show ns simpleacl6**

Procedimientos de GUI

Para crear una ACL simple mediante la GUI:

Vaya a **Sistema > Red > ACL** y, en la ficha **ACL simples**, agregue una nueva ACL simple.

Para crear un ACL6 simple mediante la GUI:

Vaya a **Sistema > Red > ACL** y, en la ficha **ACL6s simples**, agregue un nuevo ACL6 simple.

Para eliminar una ACL simple mediante la GUI:

Vaya a **Sistema > Red > ACL** y, en la ficha **ACL simples**, elimine la ACL simple.

Para eliminar un solo ACL6 simple mediante la GUI:

Vaya a **Sistema > Red > ACL** y, en la ficha **ACL6s simples**, elimine la ACL6 simple.

Para eliminar todas las ACL simples mediante la GUI:

1. Vaya a **Sistema > Red > ACL**.
2. En la ficha **ACL simples**, en la lista **Acción**, haga clic en **Borrar**.

Para eliminar todos los ACL6s simples mediante la GUI:

1. Vaya a **Sistema > Red > ACL**.
2. En la ficha **ACL6s simple**, en la lista **Acción**, haga clic en **Borrar**.

Visualización de estadísticas de ACL simples y ACL6 simples

Puede mostrar las estadísticas simples de ACL (o ACL6 simple), que incluyen el número de coincidencias, el número de errores y el número de ACL simples configuradas.

En la tabla siguiente se describen las estadísticas que se pueden mostrar para ACL simples y ACL6 simples.

Estadísticas	Indica
Coincidencia ACL	Paquetes que coinciden con una ACL
ACL falla	Paquetes que no coinciden con ninguna ACL
Recuento ACL	Número de ACL configuradas

Procedimientos CLI

Para mostrar estadísticas ACL simples mediante la CLI:

En el símbolo del sistema, escriba:

- **stat ns simpleacl**

Ejemplo:

```
1 > stat ns simpleacl
2
3 SimpleACL Statistics
4
5                                          Rate (/s)
                                              Total
6 SimpleACL hits                                   0
                        0
7 SimpleACL misses                                 0
      51872
```



```
8  SimpleACLs count                                    --
                          2
9  Done
10 <!--NeedCopy-->
```

Para mostrar estadísticas ACL6 simples mediante la CLI:

En el símbolo del sistema, escriba:

- **stat ns simpleacl6**

Procedimientos de GUI

Para mostrar estadísticas ACL simples mediante la GUI:

Vaya a **Sistema** > **Red** > **ACL** y, en la ficha **ACL simples**, seleccione la ACL y haga clic en **Estadísticas**.

Para mostrar estadísticas ACL6 simples mediante la GUI:

Vaya a **Sistema > Red > ACL** y, en la ficha **ACL6s simples**, seleccione la ACL6 simple y haga clic en **Estadísticas**.

Terminar conexiones establecidas

Para una ACL simple o ACL6 simple, Citrix ADC bloquea cualquier conexión nueva que coincida con las condiciones especificadas en la ACL. Los paquetes relacionados con conexiones existentes que se establecieron antes de crear la ACL no se bloquean. Para terminar las conexiones establecidas previamente que coincidan con una ACL existente, puede ejecutar una operación de vaciado desde la CLI o la GUI.

Flush puede ser útil en los siguientes casos:

- Recibirá una lista de direcciones IP en la lista de prohibidos y quiere bloquear completamente el acceso a Citrix ADC. En este caso, creará ACL simples o ACL6S simples para bloquear cualquier conexión nueva de estas direcciones IP y, a continuación, vaciará las conexiones existentes asociadas con esas direcciones.
- Desea finalizar muchas conexiones de una red en particular sin tomarse el tiempo de terminarlas una por una.

Antes de comenzar

- Cuando ejecuta flush, Citrix ADC busca en todas sus conexiones establecidas y finaliza las conexiones que cumplen las condiciones especificadas en cualquiera de las ACL simples configuradas en el ADC.

- Si planea crear más de una ACL simple y vaciar las conexiones existentes que coincidan con cualquiera de ellas, puede minimizar el efecto en el rendimiento creando primero todas las ACL simples y luego ejecutándolas solo una vez.

Procedimientos CLI

Para terminar todas las conexiones IPv4 establecidas que coincidan con cualquiera de las ACL simples configuradas mediante la CLI:

En el símbolo del sistema, escriba:

- **flush simpleacl -estSessions**

Para terminar todas las conexiones IPv6 establecidas que coincidan con cualquiera de sus ACL6s simples configurados mediante la CLI:

En el símbolo del sistema, escriba:

- **flush simpleacl6 -EstSessions**

Procedimientos de GUI

Para terminar todas las conexiones IPv4 establecidas que coincidan con cualquiera de las ACL simples configuradas mediante la GUI:

1. Vaya a **Sistema > Red > ACL**.
2. En la ficha **ACL simples**, en la lista **Acción**, haga clic en **Desactivar**.

Para terminar todas las conexiones IPv6 establecidas que coincidan con cualquiera de sus ACL6s simples configurados mediante la GUI:

1. Vaya a **Sistema > Red > ACL**.
2. En la ficha **ACL6s simple**, en la lista **Acción**, haga clic en **Desactivar**.

ACL ampliadas y ACL6 ampliadas

April 21, 2022

Las ACL extendidas y las ACL6S extendidas proporcionan parámetros y acciones que no están disponibles con ACL simples. Puede filtrar datos en función de parámetros tales como la dirección IP de origen, el puerto de origen, la acción y el protocolo. Puede especificar tareas para permitir un paquete, denegar un paquete o conectar un paquete.

Las ACL y ACL6 extendidas se pueden modificar una vez creadas y se pueden volver a numerar sus prioridades para especificar el orden en que se evalúan.

Nota: Si configura tanto las ACL simples como las extendidas, las ACL simples tienen prioridad sobre las ACL extendidas.

Se pueden realizar las siguientes acciones en ACL y ACL6 extendidas: Modificar, Aplicar, Inhabilitar, Activar, Quitar y Renumerar (la prioridad). Puede mostrar las ACL y ACL6 extendidas para verificar su configuración y mostrar sus estadísticas.

Puede configurar Citrix ADC para que registre los detalles de los paquetes que coinciden con una ACL extendida.

Aplicación de ACL extendidas y ACL6S extendidas: A diferencia de ACL simples y ACL6S, las ACL ampliadas y ACL6S creadas en Citrix ADC no funcionan hasta que se aplican. Además, si realiza cambios en una ACL extendida o ACL6, como inhabilitar las ACL, cambiar una prioridad o eliminar las ACL, debe volver a aplicar las ACL extendidas o ACL6. Debe volver a aplicarlos después de habilitar el registro. El procedimiento para aplicar ACL ampliadas o ACL6s vuelve a aplicarlas todas. Por ejemplo, si ha aplicado las reglas de ACL extendidas 1 a 10 y, a continuación, crea y aplica la regla 11, las primeras 10 reglas se aplican de nuevo.

Si una sesión tiene una ACL DENY relacionada, esa sesión finaliza cuando aplica las ACL.

Las ACL extendidas y ACL6 están habilitadas de forma predeterminada. Cuando se aplican, Citrix ADC comienza a comparar los paquetes entrantes con ellos. Sin embargo, si las inhabilitas, no se usarán hasta que las vuelvas a habilitar, aunque se vuelvan a aplicar.

Cambio de**numeración de las prioridades de las ACL extendidas y las ACL6 ampliadas:** los números de prioridad determinan el orden en que las ACL o ACL6 extendidas se comparan con un paquete. Una ACL con un número de prioridad inferior tiene una prioridad más alta. Se evalúa antes que las ACL con números de prioridad más altos (prioridades más bajas) y la primera ACL que coincida con el paquete determina la acción aplicada al paquete.

Al crear una ACL o ACL6 extendida, Citrix ADC le asigna automáticamente un número de prioridad múltiplo de 10, a menos que especifique lo contrario. Por ejemplo, si dos ACL extendidas tienen prioridades de 20 y 30, respectivamente, y quiere que una tercera ACL tenga un valor entre esos números, podría asignarle un valor de 25. Si más adelante quiere mantener el orden en que se evalúan las ACL pero restaura su numeración a múltiplos de 10, puede utilizar el procedimiento de renumeración.

Configuración de ACL extendidas y ACL6 ampliadas

La configuración de una ACL extendida o ACL6 en un Citrix ADC consiste en las siguientes tareas.

- **Cree una ACL o ACL6 extendida.** Cree una ACL o ACL6 extendida para permitir, denegar o conectar un paquete. Puede especificar una dirección IP o un intervalo de direcciones IP para que coincidan con las direcciones IP de origen o destino de los paquetes. Puede especificar un protocolo para que coincida con el protocolo de los paquetes entrantes.

- (Opcional) **Modifique una ACL o ACL6 extendida**. Puede modificar las ACL extendidas o ACL6 que creó anteriormente. O bien, si quiere dejar de usarlo temporalmente, puede desactivarlo y volver a activarlo más tarde.
- **Aplique ACL o ACL6 extendidas**. Después de crear, modificar, inhabilitar o volver a habilitar, o eliminar una ACL o ACL6 ampliadas, debe aplicar las ACL o ACL6 ampliadas para activarlas.
- (Opcional) **Cambie la numeración de las prioridades de las ACL o ACL6 ampliadas**. Si ha configurado ACL con prioridades que no son múltiplos de 10 y quiere restaurar la numeración a múltiplos de 10, utilice el procedimiento de renumeración.

Procedimientos CLI

Para crear una ACL extendida mediante la CLI:

En el símbolo del sistema, escriba:

- **add ns acl** <aclname> <aclaction> [-**srcIP** [\<operator>] <srcIPVal>] [-**srcPort** [\<operator>] <srcPortVal>] [-**destIP** [\<operator>] <destIPVal>] [-**destPort** [\<operator>] <destPortVal>] [-**TTL** \<positive_integer>] [-**srcMac** \<mac_addr>] [(-**protocol** \<protocol> [-established]) | -**protocolNumber** <positive_integer>] [-**vlan** \<positive_integer>] [-**interface** \<interface_name>] [-**icmpType** \<positive_integer> [-**icmpCode** \<positive_integer>]] [-**priority** \<positive_integer>] [-**state** (ENABLED | DISABLED)] [-**logstate** (ENABLED | DISABLED) [-**ratelimit** \<positive_integer>]]
- **show ns acl** [\<aclName>]

Para crear una ACL6 extendida mediante la CLI:

En el símbolo del sistema, escriba:

- **add ns acl6** <acl6name> <acl6action> [-**srcIPv6** [\<operator>] <srcIPv6Val>] [-**srcPort** [\<operator>] <srcPortVal>] [-**destIPv6** [\<operator>] <destIPv6Val>] [-**destPort** [\<operator>] <destPortVal>] [-**TTL** \<positive_integer>] [-**srcMac** \<mac_addr>] [(-**protocol** \<protocol> [-established]) | -**protocolNumber** <positive_integer>] [-**vlan** \<positive_integer>] [-**interface** \<interface_name>] [-**icmpType** \<positive_integer> [-**icmpCode** \<positive_integer>]] [-**priority** \<positive_integer>] [-**state** (ENABLED | DISABLED)]
- **show ns acl6** [\<aclName>]

Para modificar una ACL extendida mediante la CLI:

Para modificar una ACL extendida, escriba el comando **set ns acl**, el nombre de la ACL extendida y los parámetros que se van a cambiar, con sus nuevos valores.

Para modificar una ACL6 extendida mediante la CLI:

Para modificar una ACL6 extendida, escriba el comando **set ns acl6**, el nombre de la ACL6 extendida y los parámetros que se van a cambiar, con sus nuevos valores.

Para inhabilitar o habilitar una ACL extendida mediante la CLI:

En el símbolo del sistema, escriba uno de los siguientes comandos:

- **disable ns acl** <aclname>
- **enable ns acl** <aclname>

Para inhabilitar o habilitar una ACL6 extendida mediante la CLI:

En el símbolo del sistema, escriba uno de los siguientes comandos:

- **disable ns acl6** <aclname>
- **enable ns acl6** <aclname>

Para aplicar ACL extendidas mediante la CLI:

En el símbolo del sistema, escriba:

- **apply ns acls**

Para aplicar ACL6 extendidos mediante la CLI:

En el símbolo del sistema, escriba:

- **apply ns acls6**

Para renumerar las prioridades de las ACL extendidas mediante la CLI:

En el símbolo del sistema, escriba:

- **renumber ns acls**

Para renumerar las prioridades de los ACL6 extendidos mediante la CLI:

En el símbolo del sistema, escriba:

- **renumber ns acls6**

Procedimientos de GUI

Para configurar una ACL extendida mediante la GUI:

- Vaya a **Sistema** > **Red** > **ACL** y, en la ficha **ACL extendidas**, agregue una nueva ACL ampliada o modifique una ACL extendida existente. Para habilitar o inhabilitar una ACL extendida existente, selecciónela y, a continuación, seleccione **Habilitar** o **Inhabilitar** en la lista **Acción**.

Para configurar un ACL6 ampliado mediante la GUI:

- Vaya a **Sistema** > **Red** > **ACL** y, en la ficha **ACL6 extendidas**, agregue una nueva ACL6 ampliada o modifique una ACL6 extendida existente. Para habilitar o inhabilitar una ACL6 extendida existente, selecciónela y, a continuación, seleccione **Habilitar** o **Inhabilitar** en la lista **Acción**.

Para aplicar ACL extendidas mediante la GUI:

- Vaya a **Sistema** > **Red** > **ACL** y, en la ficha **ACL extendidas**, en la lista **Acción**, haga clic en **Aplicar**.

Para aplicar ACL6 ampliados mediante la GUI:

- Vaya a **Sistema** > **Red** > **ACL** y, en la ficha **ACL6 ampliadas**, en la lista **Acción**, haga clic en **Aplicar**.

Para volver a numerar las prioridades de las ACL extendidas mediante la GUI:

- Vaya a **Sistema** > **Red** > **ACL** y, en la ficha **ACL extendidas**, en la lista **Acción**, haga clic en **Renumerar prioridades**.

Para volver a numerar las prioridades de los ACL6 ampliados mediante la GUI:

- Vaya a **Sistema** > **Red** > **ACL** y, en la ficha **ACL6 ampliadas**, en la lista **Acción**, haga clic en **Renumerar prioridades**.

Configuraciones de ejemplo

En la tabla siguiente se muestran ejemplos de configuración de reglas ACL ampliadas a través de la interfaz de línea de comandos: configuraciones de ejemplo de ACL.

Registro de ACL extendidas

Puede configurar Citrix ADC para que registre los detalles de los paquetes que coinciden con las ACL extendidas.

Además del nombre de ACL, los detalles registrados incluyen información específica del paquete, como las direcciones IP de origen y destino. La información se almacena en el archivo syslog o en el archivo `nslog`, según el tipo de registro global (`syslog or nslog`) habilitado.

El registro debe estar habilitado tanto en el nivel global como en el nivel ACL. La configuración global tiene prioridad.

Para optimizar el registro, cuando varios paquetes del mismo flujo coinciden con una ACL, solo se registran los detalles del primer paquete y el contador se incrementa para cada paquete que pertenece al mismo flujo. Un flujo se define como un conjunto de paquetes que tienen los mismos valores para la dirección IP de origen, la dirección IP de destino, el puerto de origen, el puerto de destino y los parámetros del protocolo. Para evitar la inundación de mensajes de registro, Citrix ADC realiza una limitación de velocidad interna para que los paquetes pertenecientes al mismo flujo no se registren repetidamente. El número total de flujos diferentes que se pueden registrar en un momento dado está limitado a 10.000.

Nota: Debe aplicar las ACL después de habilitar el registro.

Procedimientos CLI

Para configurar el registro de ACL extendido mediante la CLI:

En el símbolo del sistema, escriba los siguientes comandos para configurar el registro y verificar la configuración:

- **set ns acl** <aclName>[-**logState** (HABILITADO | DESHABILITADO)] [-**RateLimit** \<positive_integer>]
- **apply acls**
- **mostrar ns acl** [\<aclName>]

Procedimientos de GUI

Para configurar el registro de ACL extendido mediante la interfaz gráfica de usuario:

1. Vaya a **Sistema > Red > ACL** y, en la ficha **ACL ampliadas**, abra la ACL extendida.
2. Defina los siguientes parámetros:
   - **Estado del registro**: Habilite o inhabilite el registro de eventos relacionados con la regla de ACL extendida. Los mensajes de registro se almacenan en el servidor `syslog or auditlog` configurado.
   - **Límite de velocidad de registro**: Número máximo de mensajes de registro que se generarán por segundo. Si establece este parámetro, debe habilitar el parámetro Estado de registro.

Configuración de ejemplo

```
1 > set ns acl restrict -logstate ENABLED -ratelimit 120
2 Warning: ACL modified, apply ACLs to activate change
3
4 > apply ns acls
5 Done
6 <!--NeedCopy-->
```

Registro de ACL6s extendidos

Puede configurar el dispositivo Citrix ADC para que registre los detalles de los paquetes que coinciden con una regla ACL6 ampliada. Además del nombre ACL6, los detalles registrados incluyen información específica del paquete, como las direcciones IP de origen y destino. La información se almacena en un syslog o en un archivo `nslog`, según el tipo de registros (`syslog or nslog`) que haya configurado en el dispositivo Citrix ADC.

Para optimizar el registro, cuando varios paquetes del mismo flujo coinciden con una ACL6, solo se registran los detalles del primer paquete. El contador se incrementa para todos los demás paquetes que pertenecen al mismo flujo. Un flujo se define como un conjunto de paquetes que tienen los mismos valores para los siguientes parámetros:

- IP de origen
- IP de destino
- Puerto de origen
- Puerto de destino
- Protocolo (TCP o UDP)

Si un paquete entrante no procede del mismo flujo, se crea un nuevo flujo. El número total de flujos diferentes que se pueden registrar en un momento dado está limitado a 10.000.

Procedimientos CLI

Para configurar el registro de una regla ACL6 ampliada mediante la CLI:

- Para configurar el registro mientras agrega la regla ACL6 extendida, en el símbolo del sistema, escriba:
  - **add acl6** <acl6Name><acl6action>[-**logState** (HABILITADO | DESHABILITADO)] [-**RateLimit** \<positive_integer>]
  - **apply acls6**
  - **mostrar acl6** [\<acl6Name>]
- Para configurar el registro de una regla ACL6 extendida existente, escriba en el símbolo del sistema:
  - **set acl6** <acl6Name>[-**logState** (HABILITADO | DESHABILITADO)] [-**RateLimit** \<positive_integer>]
  - **mostrar acl6** [\<acl6Name>]
  - **apply acls6**

Procedimientos de GUI

Para configurar el registro ACL6 extendido mediante la interfaz gráfica de usuario:

1. Vaya a **Sistema** > **Red** > **ACL** y, a continuación, haga clic en la ficha **ACL6s ampliados**.
2. Defina los siguientes parámetros al agregar o modificar una regla ACL6 extendida existente.
   - **Estado de registro**: Habilita o inhabilita el registro de eventos relacionados con la regla ACL6s ampliada. Los mensajes de registro se almacenan en el syslog o el servidor `auditlog` configurados.

- **Límite de velocidad de registro**: Número máximo de mensajes de registro que se generarán por segundo. Si establece este parámetro, debe habilitar el parámetro **Estado de registro**.

Configuración de ejemplo

```
> set acl6 ACL6-1 -logstate ENABLED -ratelimit 120
Done

> apply acls6
Done
<!--NeedCopy-->
```

Visualización de ACL extendidas y estadísticas ACL6 extendidas

Puede mostrar estadísticas de ACL ampliadas y ACL6.

En la tabla siguiente se enumeran las estadísticas asociadas a las ACL y ACL6 ampliadas y sus descripciones.

Estadística	Especifica
Permitir coincidencias de ACL	Paquetes que coinciden con ACL con el modo de procesamiento establecido en ALLOW. Citrix ADC procesa estos paquetes.
Partidos de NAT ACL	Paquetes que coinciden con una ACL NAT, lo que da como resultado una sesión NAT.
Partidos de Deny ACL	Paquetes eliminados porque coinciden con ACL con el modo de procesamiento establecido en DENY.
Partidos de Bridge ACL	Paquetes que coinciden con una ACL de puente, que en modo transparente omite el procesamiento del servicio.
Partidos ACL	Paquetes que coinciden con una ACL.
ACL falla	Paquetes que no coinciden con ninguna ACL.
Recuento ACL	Número total de reglas de ACL configuradas por los usuarios.

Estadística	Especifica
Recuento efectivo de ACL	Número total de ACL efectivas configuradas internamente. Para una ACL ampliada con un rango de direcciones IP, el dispositivo Citrix ADC crea internamente una ACL extendida para cada dirección IP. Por ejemplo, para una ACL ampliada con 1000 direcciones IPv4 (rango o conjunto de datos), Citrix ADC crea internamente 1000 ACL extendidas.

Procedimientos CLI

Para mostrar las estadísticas de todas las ACL extendidas mediante la CLI:

En el símbolo del sistema, escriba:

- **stat ns acl**

Para mostrar las estadísticas de todos los ACL6 ampliados mediante la CLI:

En el símbolo del sistema, escriba:

- **stat ns acl6**

Procedimientos de GUI

Para mostrar las estadísticas de una ACL extendida mediante la GUI:

- Vaya a **Sistema > Red > ACL**, en la ficha **ACL extendida**, seleccione la ACL extendida y haga clic en **Estadísticas**.

Para mostrar las estadísticas de una ACL6 ampliada mediante la interfaz gráfica de usuario:

- Vaya a **Sistema > Red > ACL**, en la ficha **ACL6 extendida**, seleccione la ACL extendida y haga clic en **Estadísticas**.

ACL con estado

Una regla de ACL con estado crea una sesión cuando una solicitud coincide con la regla y permite las respuestas resultantes incluso si estas respuestas coinciden con una regla de ACL de denegación del dispositivo Citrix ADC. Una ACL con estado descarga el trabajo de crear más reglas de ACL/reglas de sesión de reenvío para permitir estas respuestas específicas.

Las ACL con estado se pueden utilizar mejor en una implementación de firewall perimetral de un dispositivo Citrix ADC con los siguientes requisitos:

- El dispositivo Citrix ADC debe permitir las solicitudes iniciadas desde clientes internos y las respuestas relacionadas de Internet.
- El dispositivo debe descartar los paquetes de Internet que no están relacionados con ninguna conexión de cliente.

Antes de comenzar

Antes de configurar reglas de ACL con estado, tenga en cuenta los siguientes puntos:

- El dispositivo Citrix ADC admite reglas de ACL con estado y reglas ACL6 con estado.
- En una configuración de alta disponibilidad, las sesiones de una regla de ACL con estado no se sincronizan con el nodo secundario.
- No se puede configurar una regla de ACL como con estado si la regla está vinculada a cualquier configuración NAT de Citrix ADC. Algunos ejemplos de configuraciones NAT de Citrix ADC son:
  - RNAT
  - NAT a gran escala (NAT44 a gran escala, DS-Lite, NAT64 a gran escala)
  - NAT64
  - Sesión de reenvío
- No puede configurar una regla de ACL como con estado si se establecen los parámetros TTL y Establecida para esta regla de ACL.
- Las sesiones creadas para una regla de ACL con estado continúan existiendo hasta que se agote el tiempo de espera, independientemente de las siguientes operaciones de ACL:
  - Quitar ACL
  - Inhabilitar ACL
  - Borrar ACL
- Las ACL con estado no son compatibles con los siguientes protocolos:
  - FTP activo
  - TFTP

Configurar reglas ACL IPv4 con estado

La configuración de una regla de ACL con estado consiste en habilitar el parámetro con estado de una regla de ACL.

Para habilitar el parámetro con estado de una regla de ACL mediante la CLI:

- Para habilitar el parámetro con estado al agregar una regla de ACL, escriba en el símbolo del sistema:
  - **add acl** <lname> ALLOW -**stateful** (ENABLED | DISABLED)
  - **apply acls**
  - **show acl** <name>

- Para habilitar el parámetro con estado de una regla de ACL existente, en el símbolo del sistema, escriba:
  - **set acl** <name> -**stateful** (ENABLED | DISABLED)
  - **apply acls**
  - **show acl** <name>

Para habilitar el parámetro con estado de una regla de ACL mediante la GUI:

1. Vaya a **Sistema** > **Red** > **ACL** y, en la ficha **ACL extendidas**.
2. Habilite el parámetro **Stateful** al agregar o modificar una regla de ACL existente.

Configuración de ejemplo

```
> add acl ACL-1 allow -srciP 1.1.1.1 -stateful Yes

Done

> apply acls

Done

> show acl

1)         Name: ACL-1

    Action: ALLOW                          Hits: 0

    srcIP = 1.1.1.1

    destIP

    srcMac:

    Protocol:

    Vlan:                                 Interface:

    Active Status: ENABLED                 Applied Status: NOTAPPLIED

    Priority: 10                           NAT: NO

    TTL:

```



```
    Log Status: DISABLED

    Forward Session: NO

    Stateful: YES
<!--NeedCopy-->
```

Configurar reglas ACL6 con estado

La configuración de una regla ACL6 con estado consiste en habilitar el parámetro con estado de una regla ACL6.

Para habilitar el parámetro con estado de una regla ACL6 mediante la CLI:

- Para habilitar el parámetro con estado al agregar una regla ACL6, en el símbolo del sistema, escriba:
  - **add acl6** <name> ALLOW -stateful (ENABLED | DISABLD)
  - **apply acls6**
  - **show acl6** <name>
- Para habilitar el parámetro con estado de una regla ACL6 existente, en el símbolo del sistema, escriba:
  - **set acl6** <name> -**stateful** (ENABLED | DISABLED)
  - **apply acls6**
  - **show acl6** <name>

Para habilitar el parámetro con estado de una regla ACL6 mediante la GUI:

1. Vaya a **Sistema** > **Red** > **ACL** y, en la ficha **ACL6s extendidas**.
2. Habilite el parámetro **Stateful** al agregar o modificar una regla ACL6 existente.

Configuración de ejemplo

```
>  add acl6 ACL6-1 allow -srcipv6 1000::1  - stateful Yes

Done

>  apply acls6

Done

> show acl6

```



```
1)    Name: ACL6-1

    Action: ALLOW                          Hits: 0

    srcIPv6 = 1000::1

    destIPv6

    srcMac:

    Protocol:

    Vlan:                                 Interface:

    Active Status: ENABLED                 Applied Status: NOTAPPLIED

    Priority: 10                           NAT: NO

    TTL:

    Forward Session: NO

    Stateful: YES
<!--NeedCopy-->
```

ACL extendidas basadas en conjunto de datos

Se requieren muchas ACL en una empresa. Configurar y administrar muchas ACL es difícil y engorroso cuando requieren cambios frecuentes.

Un dispositivo Citrix ADC admite conjuntos de datos en ACL extendidas. El conjunto de datos es una función existente de un dispositivo Citrix ADC. Un conjunto de datos es una matriz de tipos de patrones indexados: número (entero), dirección IPv4 o dirección IPv6.

La compatibilidad con conjuntos de datos en las ACL ampliadas resulta útil para crear varias reglas de ACL, que requieren parámetros de ACL comunes.

Al crear una regla de ACL, en lugar de especificar los parámetros comunes, puede especificar un conjunto de datos, que incluye estos parámetros comunes.

Cualquier cambio realizado en el conjunto de datos se refleja automáticamente en las reglas de ACL que utilizan este conjunto de datos. Las ACL con conjuntos de datos son más fáciles de configurar y administrar. También son más pequeños y fáciles de leer que los ACL convencionales.

En la actualidad, el dispositivo Citrix ADC solo admite los siguientes tipos de conjuntos de datos para las ACL extendidas:

- Dirección IPv4 (para especificar la dirección IP de origen o la dirección IP de destino o ambas para una regla ACL)
- número (para especificar el puerto de origen o el puerto de destino o ambos para una regla de ACL)

Antes de comenzar

Antes de configurar reglas de ACL extendidas basadas en conjuntos de datos, tenga en cuenta los siguientes puntos:

- Asegúrese de estar familiarizado con la función de conjunto de datos de un dispositivo Citrix ADC. Para obtener más información sobre los conjuntos de datos, consulte Conjuntos de patrones y conjuntos de datos.
- El dispositivo Citrix ADC admite conjuntos de datos solo para ACL extendidas IPv4.
- El dispositivo Citrix ADC solo admite los siguientes tipos de conjuntos de datos para las ACL ampliadas:
  - Dirección IPv4
  - número
- El dispositivo Citrix ADC admite ACL extendidas basadas en conjuntos de datos para todas las configuraciones de Citrix ADC: autónomas, de alta disponibilidad y de clústeres.
- Para una ACL ampliada con conjuntos de datos que contienen rangos, el dispositivo Citrix ADC crea internamente una ACL ampliada para cada combinación de los valores del conjunto de datos.
  - **Ejemplo 1**: Para una ACL extendida basada en dataset IPv4 con 1000 direcciones IPv4 enlazadas al conjunto de datos y el conjunto de datos se establece en el parámetro IP de origen, el dispositivo Citrix ADC crea internamente 1000 ACL extendidas.
  - **Ejemplo 2**: ACL extendida basada en un conjunto de datos con los siguientes parámetros establecidos:
    - La IP de origen se establece en un conjunto de datos que contiene 5 direcciones IP.
    - La IP de destino se establece en un conjunto de datos que contiene 5 direcciones IP.
    - El puerto de origen se establece en un conjunto de datos que contiene 5 puertos.
    - El puerto de destino se establece en un conjunto de datos que contiene 5 puertos.

    El dispositivo Citrix ADC crea internamente 625 ACL extendidas. Cada una de estas ACL internas contiene una combinación única de los cuatro valores de parámetros mencionados anteriormente.

  - El dispositivo Citrix ADC admite un máximo de 10.000 ACL extendidas. Para una ACL extendida basada en datasets IPv4 con un rango de direcciones IP enlazadas al conjunto de datos, el dispositivo Citrix ADC deja de crear ACL internas una vez que el número total de ACL extendidas alcanza el límite máximo.
  - Los siguientes contadores están presentes como parte de las estadísticas de ACL ampliadas:
    * **Recuento de LCA**. Número total de reglas de ACL configuradas por los usuarios.
    * **Recuento efectivo del LCA**. Número total de reglas de ACL efectivas que el dispositivo Citrix ADC configura internamente.

    Para obtener más información, consulte Visualización de estadísticas ACL extendidas y ACL6 ampliadas.

- El dispositivo Citrix ADC no admite `set` ni realiza operaciones `unset` para asociar/disociar conjuntos de datos a los parámetros de una ACL extendida. Puede establecer los parámetros de ACL en un conjunto de datos solo durante la operación `add`.

Configurar ACL extendidas basadas en conjuntos de datos

La configuración de una regla de ACL ampliada basada en conjuntos de datos consta de las siguientes tareas:

- **Agrega un conjunto de datos**. Un conjunto de datos es una matriz de tipos de patrones indexados: número (entero), dirección IPv4 o dirección IPv6. En esta tarea, crea un tipo de conjunto de datos, por ejemplo, un conjunto de datos de tipo IPv4.
- **Enlazar valores al conjunto de datos**. Especifique un valor o un rango de valores en el conjunto de datos. Los valores especificados deben ser del mismo tipo que el tipo de conjunto de datos. Por ejemplo, puede especificar una dirección IPv4, un rango de direcciones IPv4 o un rango de direcciones IPv4 en notación CIDR para un conjunto de datos IPv4.
- **Agregue una ACL extendida y establezca los parámetros de ACL al conjunto de datos**. Agregue una ACL ampliada y defina los parámetros de ACL necesarios en el conjunto de datos. Esta configuración da como resultado que los parámetros se establezcan en los valores especificados en el conjunto de datos.
- **Aplicar ACL extendidas**. Aplique las ACL para activar cualquier ACL ampliada nueva o modificada.

Para agregar un conjunto de datos de directivas mediante la CLI:

En el símbolo del sistema, escriba:

- **add policy dataset** <name> <type>
- **show policy dataset**

Para enlazar un patrón al conjunto de datos mediante la CLI:

En el símbolo del sistema, escriba:

- **bind policy dataset** <name> <value> [-endRange \<string>]
- **show policy dataset**

Para agregar una ACL extendida y establecer los parámetros de ACL en el conjunto de datos mediante la CLI:

En el símbolo del sistema, escriba:

- **add ns acl** <aclname> <aclaction> [-**srcIP** [\<operator>] <srcIPVal>] [-**srcPort** [\<operator>] <srcPortVal>] [-**destIP** [\<operator>] <destIPVal>] [-**destPort** [\<operator>] <destPortVal>] …
- **show acls**

Para aplicar ACL extendidas mediante la CLI:

En el símbolo del sistema, escriba:

- **apply acls**

Configuración de ejemplo

En la siguiente configuración de ejemplo de una ACL extendida basada en conjuntos de datos, se crean dos conjuntos de datos IPv4 `DATASET_IP_ACL_1` y `DATASET_IP_ACL_2`. Se crean dos conjuntos de datos de puertos `DATASET_PORT_ACL_1` y `DATASET_PORT_ACL_1`.

Dos direcciones IPv4: 192.0.2.30 y 192.0.2.60 están vinculadas `DATASET_IP_ACL_1`. Dos intervalos de direcciones IPv4: (198.51.100.15 - 45) y (203.0.113.60-90) están vinculados a `DATASET_IP_ACL_2`. `DATASET_IP_ACL_1` se especifica en el parámetro `srcIP`, y `DATASET_IP_ACL_1` en el parámetro `destIP` de la ACL extendida `ACL-1`.

Dos números de puerto: 2001 y 2004, están vinculados `DATASET_PORT_ACL_1`. Dos intervalos de puertos: (5001 - 5040) y (8001 - 8040) están vinculados `DATASET-PORT-ACL-2`. `DATASET_IP_ACL_1` se especifica en el parámetro `srcIP`, y `DATASET_IP_ACL_1` en el parámetro `destIP` de la ACL extendida `ACL-1`.

```
add policy dataset DATASET_IP_ACL_1 IPV4
add policy dataset DATASET_IP_ACL_2 IPV4

add policy dataset DATASET_PORT_ACL_1 NUM
add policy dataset DATASET_PORT_ACL_2 NUM

bind dataset DATASET_IP_ACL_1 192.0.2.30
```



```
bind dataset DATASET_IP_ACL_1 192.0.2.60
bind dataset DATASET_IP_ACL_2 198.51.100.15 -endrange 198.51.100.45
bind dataset DATASET_IP_ACL_2 203.0.113.1/24

bind dataset DATASET_PORT_ACL_1 2001
bind dataset DATASET_PORT_ACL_1 2004
bind dataset DATASET_PORT_ACL_2 5001 -endrange 5040
bind dataset DATASET_PORT_ACL_2 8001 -endrange 8040

add ns acl ACL-1 ALLOW -srcIP DATASET_IP_ACL_1 -destIP DATASET_IP_ACL_2
-srcPort DATASET_PORT_ACL_1 -destPort DATASET_PORT_ACL_2  - protocol TCP
<!--NeedCopy-->
```

Máscara de comodín de dirección MAC para ACL

August 20, 2021

Se ha introducido un parámetro de máscara comodín para ACL y ACL6s extendidos y se utiliza con el parámetro de dirección MAC de origen para definir un rango de direcciones MAC que deben coincidir con la dirección MAC de origen de los paquetes entrantes.

Las máscaras comodín especifican qué dígitos hexadecimales de la dirección MAC se utilizan y qué dígitos hexadecimales se ignoran. El parámetro máscara comodín especifica una serie de unos y ceros y tiene una longitud de 12 dígitos. Cada dígito es una máscara para el dígito hexadecimal correspondiente de la dirección MAC. Un dígito cero en la máscara comodín indica que se debe considerar el dígito hexadecimal correspondiente de la dirección MAC y un dígito indica que el dígito hexadecimal correspondiente a ser ignorado.

La máscara comodín debe cumplir las siguientes condiciones:

- Tiene solo una serie de ceros
- Tiene solo una serie de unos
- Comience con una serie de ceros

Los siguientes son algunos de los ejemplos de máscaras comodín válidas:

- 000000111111
- 000000011111
- 000011111111

Los siguientes son algunos de los ejemplos de máscaras comodín no válidas:

- 000000111100
- 111110000000

- 010101010101

Para una ACL, una máscara comodín de 000000111111 para la dirección MAC 96:fa:95:1d:67:4a a define el rango de direcciones 96:FA:95:00:00:00 - 96:FA:95:FF:FF:FF. Este intervalo de direcciones MAC coincide con la dirección MAC de origen de los paquetes entrantes.

Para especificar un rango de direcciones MAC de origen en una regla ACL mediante la CLI:

En el símbolo del sistema, escriba:

```
1 -  add ns acl <name> <action> -srcMac <mac_addr> -srcMacMask <string>
2 -  show ns acl <aclname>
3 <!--NeedCopy-->
```

Ejemplo:

```
1 add ns acl ACL-1 ALLOW  - protocol TCP  - srcport 2000-3000 -srcMac 96:fa
     :95:1d:67:4a
2   - srcMacMask 000000111111
3 Done
4 <!--NeedCopy-->
```

Para especificar un rango de direcciones MAC de origen en una regla ACL6 mediante la CLI:

En el símbolo del sistema, escriba:

```
1 -  add ns acl6 <name> <action> -srcMac <mac_addr> -srcMacMask <string>
2 -  show ns acl6 <acl6name>
3 <!--NeedCopy-->
```

Ejemplo:

```
1 > add ns acl6 ACL6-1 ALLOW -destIPv6 2001::45 -srcMac 96:fa:90:1d:67:4a
2  - srcMacMask 000000001111
3 Done
4 <!--NeedCopy-->
```


Bloqueo del tráfico en puertos internos

August 20, 2021

De forma predeterminada, un dispositivo Citrix ADC no bloquea algún tipo de tráfico interno incluso mediante reglas de ACL.

En la tabla siguiente se enumeran los tipos de tráfico interno que un dispositivo Citrix ADC no bloquea incluso mediante reglas de ACL:

Configuración de Citrix ADC	Protocolo	Puerto de destino	Dirección IP de destino
Todas	TCP	3008–3011	NSIP o SNIP
Todas	TCP	179	NSIP o SNIP
Todas	UDP	520	NSIP o SNIP
Alta disponibilidad	UDP	3003	NSIP
Alta disponibilidad	TCP	4001	NSIP
Alta disponibilidad	TCP	22	NSIP
Clúster	UDP	7000	NSIP

Esta función de no bloquear los tipos de tráfico mencionados anteriormente se especifica mediante la configuración predeterminada del parámetro Layer-3 `Implicit ACL Allow` (`implicitACLAllow`) global.

Puede inhabilitar este parámetro si desea bloquear los tipos de tráfico mencionados anteriormente mediante las reglas de ACL. Un dispositivo en una configuración de alta disponibilidad realiza una excepción para su nodo asociado (principal o secundario). No bloquea el tráfico de ese nodo.

Para inhabilitar o habilitar este parámetro mediante la CLI:

En el símbolo del sistema, escriba:

set l3param -IMPLÍCITA CLPERMIT [HABILITADO	DESHABILITADO]

-
- **sh l3param**

Nota: El parámetro ImplicitAclAllow está habilitado de forma predeterminada.

Ejemplo:

```
> set l3param -implicitACLAllow DISABLED
Done
<!--NeedCopy-->
```

Redirección de IP

August 20, 2021

Los dispositivos Citrix ADC admiten redirección dinámica y estático. Dado que la redirección simple no es la función principal de un dispositivo Citrix ADC, el objetivo principal de ejecutar protocolos de redirección dinámica es habilitar la inyección de mantenimiento de rutas (RHI), de modo que un enrutador ascendente pueda elegir la mejor entre varias rutas a un servidor virtual distribuido topográficamente.

La mayoría de las implementaciones de Citrix ADC utilizan algunas rutas estáticas para reducir la sobrecarga de redirección. Puede crear rutas estáticas de copia de seguridad y supervisar rutas para habilitar la conmutación automática en caso de que una ruta estática se desactive. También puede asignar pesos para facilitar el equilibrio de carga entre rutas estáticas, crear rutas nulas para evitar bucles de redirección y configurar rutas estáticas IPv6. Puede configurar rutas basadas en directivas (PBRs), para las que las decisiones de redirección se basan en criterios que especifique.

Configuración de Rutas Dinámicas

August 20, 2021

Cuando se habilita un protocolo de redirección dinámica, el proceso de redirección correspondiente supervisa las actualizaciones de ruta y anuncia las rutas. Los protocolos de redirección permiten a un router ascendente utilizar la técnica de multirruta de igual coste (ECMP) para equilibrar la carga del tráfico a servidores virtuales idénticos alojados en dos dispositivos Citrix ADC independientes. El redirección dinámica en un dispositivo Citrix ADC utiliza tres tablas de redirección. En una configuración de alta disponibilidad, las tablas de redirección del dispositivo secundario reflejan las tablas del primario.

Para obtener guías de referencia de comandos y comandos no compatibles en el protocolo de redirección dinámica, consulte Guías de referencia de comandos del protocolo de redirección dinámica y comandos no compatibles.

Citrix ADC admite los siguientes protocolos:

- Protocolo de información de redirección (RIP) versión 2
- Abrir la ruta más corta primero (OSPF) versión 2
- Protocolo de puerta de enlace de frontera (BGP)
- Protocolo de información de redirección de próxima generación (RIPng) para IPv6
- Abrir la ruta más corta primero (OSPF) versión 3 para IPv6
- Protocolo ISIS

Puede habilitar más de un protocolo simultáneamente.

Tablas de redirección en Citrix ADC

En un dispositivo Citrix ADC, la tabla de redirección del kernel Citrix ADC, la tabla de redirección del kernel FreeBSD y la tabla de redirección de NSM FIB tienen un conjunto diferente de rutas y tienen un propósito diferente. Se comunican entre sí mediante el uso de sockets de redirección UNIX. Las actualizaciones de ruta no se propagan automáticamente de una tabla de redirección a otra. Debe configurar la propagación de actualizaciones de ruta para cada tabla de redirección.

Tabla de redirección del núcleo NS

La tabla de redirección del núcleo NS contiene rutas de subred correspondientes al NSIP y a cada SNIP y MIP. Por lo general, no hay rutas correspondientes a VIP en la tabla de redirección del núcleo NS. La excepción es un VIP agregado mediante el comando add ns ip y configurado con una máscara de subred que no sea 255.255.255.255. Si hay varias direcciones IP pertenecientes a la misma subred, se abstrae como una única ruta de subred. Además, esta tabla contiene una ruta a la red de loopback (127.0.0.0) y cualquier ruta estática agregada a través de la CLI (CLI). Citrix ADC utiliza las entradas de esta tabla en el reenvío de paquetes. Desde la CLI, se pueden inspeccionar con el comando show route.

Tabla de redirección de FreeBSD

El único propósito de la tabla de ruteo de FreeBSD es facilitar la iniciación y terminación del tráfico de gestión (telnet, ssh, etc.). En un dispositivo Citrix ADC, estas aplicaciones están estrechamente acopladas a FreeBSD, y es imperativo que FreeBSD disponga de la información necesaria para manejar el tráfico hacia y desde estas aplicaciones. Esta tabla de redirección contiene una ruta a la subred NSIP y una ruta predeterminada. Además, FreeBSD agrega rutas de tipo WasCloned (W) cuando Citrix ADC establece conexiones a hosts en redes locales. Debido a la utilidad altamente especializada de las entradas en esta tabla de ruteo, todas las demás actualizaciones de rutas desde el kernel de NS y las tablas de ruteo de NSM FIB pasan por alto la tabla de ruteo de FreeBSD. No lo modifique con el

comando route. La tabla de ruteo de FreeBSD puede ser inspeccionada mediante el comando netstat desde cualquier shell de UNIX.

Módulo de servicios de red (NSM) FIB

La tabla de redirección FIB de NSM contiene las rutas anunciables distribuidas por los protocolos de redirección dinámica a sus pares en la red. Puede contener:

- **Rutas conectadas**. Subredes IP a las que se puede acceder directamente desde Citrix ADC. Normalmente, las rutas correspondientes a la subred NSIP y las subredes sobre las que se habilitan los protocolos de redirección están presentes en NSM FIB como rutas conectadas.
- **Rutas del núcleo**. Todas las direcciones VIP en las que está habilitada la opción -HostRoute están presentes en NSM FIB como rutas del kernel si satisfacen los niveles RHI requeridos. Además, NSM FIB contiene cualquier ruta estática configurada en la CLI que tenga habilitada la opción: Advertise. Como alternativa, si el Citrix ADC funciona en modo de anuncio de ruta estática (SRADV), todas las rutas estáticas configuradas en la CLI están presentes en NSM FIB. Estas rutas estáticas se marcan como rutas del núcleo en NSM FIB, porque realmente pertenecen a la tabla de redirección del núcleo NS.
- **Rutas estáticas**. Normalmente, cualquier ruta estática configurada en VTYSH está presente en NSM FIB. Si se modifican las distancias administrativas de los protocolos, puede que no siempre sea el caso. Un punto importante a tener en cuenta es que estas rutas nunca pueden entrar en la tabla de redirección del núcleo NS.
- **Rutas aprendidas**. Si Citrix ADC está configurado para aprender rutas dinámicamente, NSM FIB contiene rutas aprendidas por los diversos protocolos de redirección dinámica. Sin embargo, las rutas aprendidas por OSPF necesitan un procesamiento especial. Se descargan en FIB solo si la opción fib-install está habilitada para el proceso OSPF. Esto se puede hacer desde la vista router-config en VTYSH.

Redirección dinámica en una configuración de alta disponibilidad

En una configuración de alta disponibilidad, el nodo principal ejecuta el proceso de redirección y propaga las actualizaciones de la tabla de redirección al nodo secundario. La tabla de redirección del nodo secundario refleja la tabla de redirección en el nodo principal.

Reenvío sin parar

Después de la conmutación por error, el nodo secundario tarda algún tiempo en iniciar el protocolo, aprender las rutas y actualizar su tabla de redirección. Pero esto no afecta a la redirección, ya que la tabla de redirección del nodo secundario es idéntica a la tabla de redirección del nodo principal. Este modo de operación se conoce como reenvío sin parar.

Mecanismo de evitación de agujeros negros

Después de la conmutación por error, el nuevo nodo principal inyecta todas sus rutas VIP en el router ascendente. Sin embargo, ese router conserva las rutas del nodo principal antiguo durante 180 segundos. Dado que el enrutador no conoce la conmutación por error, intenta equilibrar la carga del tráfico entre los dos nodos. Durante los 180 segundos anteriores a la expiración de las rutas antiguas, el router envía la mitad del tráfico al nodo primario antiguo e inactivo, que es, en efecto, un agujero negro.

Para evitar esto, el nuevo nodo principal, al inyectar una ruta, le asigna una métrica ligeramente inferior a la especificada por el nodo principal antiguo.

Interfaces para configurar el redirección dinámica

Para configurar el redirección dinámica, puede utilizar la GUI o una interfaz de línea de comandos. Citrix ADC admite dos interfaces de línea de comandos independientes: La CLI y el Shell de teletipo virtual (VTYSH). La CLI es el shell nativo del dispositivo. VTYSH es expuesto por ZebOS. El conjunto de redirección Citrix ADC se basa en ZebOS, la versión comercial de GNU Zebra.

> **Nota:**
>
> Citrix recomienda utilizar VTYSH para todos los comandos excepto aquellos que solo se pueden configurar en la CLI. El uso de la CLI debe limitarse generalmente a comandos para habilitar los protocolos de redirección, configurar el anuncio de ruta de host y agregar rutas estáticas para el reenvío de paquetes.

Guías de referencia de comandos de Dynamic Routing Protocol y comandos no admitidos

En la tabla siguiente se enumeran los enlaces de la guía de referencia de comandos, para varios protocolos de redirección dinámica y comandos no compatibles en el dispositivo Citrix ADC: guías de referencia del protocolo de redirección dinámica y comandos no compatibles.

Configuración de RIP

August 20, 2021

Protocolo de información de redirección (RIP) es un protocolo de vector de distancia. Citrix ADC admite RIP tal como se define en RFC 1058 y RFC 2453. RIP puede ejecutarse en cualquier subred.

Después de habilitar RIP, debe configurar el anuncio de rutas RIP. Para solucionar problemas, puede limitar la propagación RIP. Puede mostrar la configuración de RIP para verificar la configuración.

Activación y desactivación de RIP

Utilice cualquiera de los procedimientos siguientes para habilitar o inhabilitar RIP. Después de habilitar RIP, el dispositivo Citrix ADC inicia el proceso RIP. Después de inhabilitar RIP, el dispositivo detiene el proceso RIP.

Para habilitar o inhabilitar la redirección RIP mediante la CLI:

En el símbolo del sistema, escriba uno de los siguientes comandos para habilitar o inhabilitar RIP:

- **habilitar RIP de la función ns**
- **inhabilitar la función ns RIP**

Para habilitar o inhabilitar la redirección RIP mediante la GUI:

1. Desplácese hasta **Sistema** > **Configuración**, en el grupo **Modos y funciones**, haga clic en **Cambiar funciones avanzadas**.
2. Seleccione o desactive la opción **RIP Routing**.

Rutas publicitarias

RIP permite a un router ascendente equilibrar la carga del tráfico entre dos servidores virtuales idénticos alojados en dos dispositivos Citrix ADC independientes. El anuncio de ruta permite que un enrutador ascendente realice un seguimiento de las entidades de red ubicadas detrás del Citrix ADC.

Para configurar RIP para anunciar rutas mediante la línea de comandos VTYSH:

En el símbolo del sistema, escriba los siguientes comandos, en el orden que se muestra:

Comando	Especifica
VTYSH	Muestra el símbolo del sistema VTYSH.
configure terminal	Acceda al modo de configuración global.
router rip	Inicie el proceso de redirección RIP y entre en el modo de configuración para el proceso de redirección.
redistribute static	Redistribuir rutas estáticas.
redistribute kernel	Redistribuir las rutas del núcleo.

Ejemplo:

```
>VTYSH
NS# configure terminal
```



```
NS(config)# router rip
NS(config-router)# redistribute static
NS(config-router)# redistribute kernel
<!--NeedCopy-->
```

Limitación de las propagaciones RIP

Si necesita solucionar los problemas de su configuración, puede configurar el modo de solo escucha en cualquier interfaz dada.

Para limitar la propagación RIP mediante la línea de comandos VTYSH:

En el símbolo del sistema, escriba los siguientes comandos, en el orden que se muestra:

Comando	Especifica
VTYSH	Muestra el símbolo del sistema VTYSH.
configure terminal	Acceda al modo de configuración global.
router rip	Inicie el proceso de redirección RIP y entre en el modo de configuración para el proceso de redirección.
passive-interface < vlan_name>	Suprimir las actualizaciones de redirección en las interfaces enlazadas a la VLAN especificada.

Ejemplo:

```
>VTYSH
NS# configure terminal
NS(config)# router rip
NS(config-router)# passive-interface VLAN0
<!--NeedCopy-->
```

Verificación de la configuración RIP

Puede mostrar la tabla de redirección y otros parámetros de RIP.

Para ver la configuración de RIP mediante la línea de comandos VTYSH:

En el símbolo del sistema, escriba los comandos siguientes en el orden siguiente:

Comando	Especifica
VTYSH	Muestra el símbolo del sistema VTYSH.
sh rasgar	Muestra la tabla de redirección RIP actualizada.
<vlan_name>interfaz sh rip	Muestra información de RIP para la VLAN especificada.

Ejemplo:

```
NS# VTYSH
NS# sh rip
NS# sh rip interface VLAN0
<!--NeedCopy-->
```

Configuración de OSPF

December 2, 2021

Citrix ADC admite Open Shortest Path First (OSPF) versión 2 (RFC 2328). Las funciones de OSPF en Citrix ADC son:

- Si un vserver está activo, las rutas de host al vserver se pueden inyectar en los protocolos de redirección.
- El OSPF se puede ejecutar en cualquier subred.
- El aprendizaje de rutas anunciado por los enrutadores OSPF vecinos se puede inhabilitar en Citrix ADC.
- El Citrix ADC puede anunciar métricas externas de tipo 1 o tipo 2 para todas las rutas.
- El Citrix ADC puede anunciar la configuración de métricas especificada por el usuario para las rutas VIP. Por ejemplo, puede configurar una métrica por VIP sin mapas de ruta especiales.
- Puede especificar el ID de área OSPF para Citrix ADC.
- El Citrix ADC admite áreas no tan obstinadas (NSA). Una NSSA es similar a un área de código auxiliar de OSPF, pero permite la inyección de rutas externas de manera limitada en el área de código auxiliar. Para admitir los NSSA, se han definido un nuevo bit de opción (el bit N) y un nuevo tipo (Tipo 7) de área Link State Advertisement (LSA). Los LSA de tipo 7 admiten información de rutas externas dentro de una NSSA. Un enrutador de borde de área (ABR) de NSSA convierte un LSA de tipo 7 en un LSA de tipo 5 que se propaga al dominio OSPF. La especificación OSPF define solo las siguientes clases generales de configuración de área:

- LSA tipo 5: originado por los enrutadores internos del área se inundan en el dominio mediante enrutadores de borde AS (ASBR).
- Stub: Permite que no se propague LSA de tipo 5 ina/en toda la zona y, en su lugar, depende de la redirección predeterminado a destinos externos.

Después de habilitar OSPF, debe configurar la publicidad de las rutas OSPF. Para solucionar problemas, puede limitar la propagación de OSPF. Puede mostrar la configuración de OSPF para verificar la configuración.

Habilitación y desactivación de OSPF

Para habilitar o inhabilitar OSPF, debe usar la CLI o la GUI. Cuando OSPF está habilitado, Citrix ADC inicia el proceso OSPF. Cuando OSPF está inhabilitado, Citrix ADC detiene el proceso de redirección OSPF.

Para habilitar o inhabilitar la redirección OSPF mediante la CLI:

En el símbolo del sistema, escriba uno de los siguientes comandos:

1. **enable ns feature OSPF**
2. **disable ns feature OSPF**

Para habilitar o inhabilitar la redirección OSPF mediante la GUI:

1. Vaya a **Sistema** > **Configuración**, en el grupo **Modos y funciones**, haga clic en **Cambiar funciones avanzadas**.
2. Seleccione o desactive la opción de redirección**OSPF**.

Publicidad de rutas OSPF

OSPF permite que un enrutador ascendente equilibre la carga del tráfico entre dos servidores virtuales idénticos alojados en dos dispositivos Citrix ADC independientes. La publicidad de rutas permite que un enrutador ascendente realice un seguimiento de las entidades de red ubicadas detrás de Citrix ADC.

Para configurar OSPF para que anuncie rutas mediante la línea de comandos VTYSH:

En el símbolo del sistema, escriba los siguientes comandos, en el orden que se muestra:

Comando	Especifica
VTYSH	Muestra el símbolo del sistema VTYSH.
configure terminal	Entra en el modo de configuración global.

Comando	Especifica
router OSPF	Inicie el proceso de redirección OSPF e introduzca el modo de configuración para el proceso de redirección.
network A.B.C.D/M area <0-4294967295>	Habilitar la redirección en una red IP.
redistribute static	Redistribuya las rutas estáticas.
redistribute kernel	Redistribuya las rutas del núcleo.

Ejemplo:

```
>VTYSH
NS# configure terminal
NS(config)# router OSPF
NS(config-router)# network 10.102.29.0/24 area 0
NS(config-router)# redistribute static
NS(config-router)# redistribute kernel
<!--NeedCopy-->
```

Limitación de las propagaciones de OSPF

Si necesita solucionar problemas de configuración, puede configurar el modo de solo escucha en cualquier VLAN determinada.

Para limitar la propagación de OSPF mediante la línea de comandos VTYSH:

En el símbolo del sistema, escriba los siguientes comandos, en el orden que se muestra:

Comando	Especifica
VTYSH	Muestra el símbolo del sistema VTYSH.
configure terminal	Acceda al modo de configuración global.
router OSPF	Inicie el proceso de redirección OSPF y entre en el modo de configuración para el proceso de redirección.
passive-interface < vlan_name>	Suprimir las actualizaciones de redirección en las interfaces enlazadas a la VLAN especificada.

Ejemplo:

```
>VTYSH
NS# configure terminal
NS(config)# router OSPF
NS(config-router)# passive-interface VLAN0
<!--NeedCopy-->
```

Verificación de la configuración de OSPF

Puede mostrar los vecinos OSPF actuales y las rutas OSPF.

Para ver la configuración de OSPF mediante la línea de comandos VTYSH:

En el símbolo del sistema, escriba los siguientes comandos, en el orden que se muestra:

Comando	Especifica
VTYSH	Muestra el símbolo del sistema VTYSH.
sh OSPF neighbor	Muestra los vecinos actuales.
sh OSPF route	Muestra las rutas OSPF.

Ejemplo:

```
>VTYSH
NS# sh ip OSPF neighbor
NS# sh ip OSPF route
<!--NeedCopy-->
```

Configuración de reinicio estable para OSPF

En una configuración de alta disponibilidad (HA) no INC en la que se configura un protocolo de redirección, después de una conmutación por error, los protocolos de redirección se convergen y se aprenden las rutas entre el nuevo nodo principal y los enrutadores vecinos adyacentes. El aprendizaje en ruta tarda algún tiempo en completarse. Durante este tiempo, el reenvío de paquetes se retrasa, el rendimiento de la red puede verse afectado y los paquetes pueden caerse.

El reinicio estable permite que una configuración de alta disponibilidad durante una conmutación por error dirija a sus enrutadores adyacentes para que no eliminen las rutas aprendidas del nodo princi-

pal antiguo de sus bases de datos de redirección. Mediante la información de redirección del nodo principal antiguo, el nuevo nodo primario y los enrutadores adyacentes comienzan inmediatamente a reenviar paquetes, sin interrumpir el rendimiento de la red.

> **Nota:**
>
> El reinicio estable no es compatible con las configuraciones de alta disponibilidad en modo INC.

Para configurar el reinicio ordenado para OSPF mediante la línea de comandos VTYSH, en el símbolo del sistema, escriba los siguientes comandos, en el orden que se muestra:

Comando	Ejemplo	Descripción del comando
VTYSH	VTYSH	Entra en el símbolo del sistema VTYSH.
configure terminal	NS# configure terminal	Entra en el modo de configuración global.
router-id <id>	NS(config)# router-id 1.1.1.1	Establece un identificador de enrutador para el dispositivo Citrix ADC. Este identificador se establece para todos los protocolos de redirección dinámica. El mismo ID debe especificarse en el otro nodo en una configuración de alta disponibilidad para que el reinicio correcto funcione correctamente en la configuración de alta disponibilidad.
ospf restart grace-period <1-1800>	NS(config)# ospf restart grace-period 170	Especifica el período de gracia, en segundos, para el que se conservarán las rutas en los dispositivos auxiliares. Valor por defecto: 120 segundos.

Comando	Ejemplo	Descripción del comando
ospf restart helper max-grace-period <1-1800>	NS(config)# ospf restart helper max-grace-period 180	Este es un comando opcional para limitar el período de gracia máximo durante el cual el dispositivo Citrix ADC estará en modo auxiliar. Si el dispositivo Citrix ADC recibe un LSA opaco con un período de gracia mayor que el período máximo de gracia establecido, el LSA se descarta y el Citrix ADC no se coloca en modo auxiliar.
router ospf	NS(config)# router ospf	Inicia el proceso de redirección OSPF y entrará en el modo de configuración para el proceso de redirección.
network A.B.C.D/M area <0-4294967295>	NS(config-router)# network 192.0.2.0/24 area 0	Habilita la redirección en una red IP.
capability restart graceful	NS(config-router)# capability restart graceful	Habilita el reinicio estable en el proceso de redirección OSPF.
redistribute kernel	NS(config-router)# redistribute kernel	Redistribuye las rutas del núcleo.

Configuración de BGP

December 2, 2021

El dispositivo Citrix ADC admite BGP (RFC 4271). Las funciones de BGP en Citrix ADC son:

- El Citrix ADC anuncia rutas a pares BGP.
- Citrix ADC inyecta rutas de host a direcciones IP virtuales (VIP), según lo determinado por el estado de los servidores virtuales subyacentes.
- Citrix ADC genera archivos de configuración para ejecutar BGP en el nodo secundario después de la conmutación por error en una configuración de alta disponibilidad.

- Este protocolo admite intercambios de rutas IPv6.
- As-Override en el protocolo de puerta de enlace

Después de habilitar BGP, debe configurar el anuncio de las rutas BGP. Para solucionar problemas, puede limitar la propagación de BGP. Puede mostrar la configuración de BGP para verificar la configuración.

Requisitos previos para BGP IPv6

Antes de empezar a configurar BGP de IPv6, haga lo siguiente:

- Asegúrese de entender el protocolo BGP IPv6.
- Habilite la función IPv6.

Habilitación y desactivación de BGP

Para habilitar o inhabilitar BGP, debe usar la CLI o la GUI. Cuando BGP está habilitado, el dispositivo Citrix ADC inicia el proceso BGP. Cuando BGP está inhabilitado, el dispositivo detiene el proceso BGP.

Para habilitar o inhabilitar la redirección BGP mediante la CLI:

En el símbolo del sistema, escriba uno de los siguientes comandos:

- enable ns feature BGP
- disable ns feature BGP

Para habilitar o inhabilitar la redirección BGP mediante la GUI:

1. Vaya a Sistema > Configuración, en el grupo Modos y funciones, haga clic en Cambiar funciones avanzadas.
2. Seleccione o desactive la opción Redirección BGP.

Publicidad de rutas IPv4

Puede configurar el dispositivo Citrix ADC para anunciar rutas de host a VIP y para anunciar rutas a redes descendentes.

Para configurar BGP para que anuncie rutas IPv4 mediante la línea de comandos VTYSH:

En el símbolo del sistema, escriba los siguientes comandos, en el orden que se muestra:

Comando	Especifica
VTYSH	Muestra el símbolo del sistema VTYSH.
configure terminal	Acceda al modo de configuración global.

Comando	Especifica
router BGP < ASnumber>	Sistema autónomo BGP. < ASnumber> es un parámetro obligatorio. Valores posibles: De 1 a 4.294.967.295.
Neighbor < IPv4 address> remote-as < as-number>	Actualice la tabla de vecinos BGP de IPv4 con la dirección IPv4 local de enlace del vecino en el sistema autónomo especificado.
Address-family ipv4	Entre en el modo de configuración de la familia de direcciones.
Neighbor < IPv4 address> activate	Intercambie prefijos para la familia de enrutadores IPv4 entre el par y el nodo local mediante la dirección local del enlace.
redistribute kernel	Redistribuya las rutas del núcleo.
redistribute static	Redistribuya las rutas estáticas.

Ejemplo:

```
>VTYSH
NS# configure terminal
NS(config)# router BGP 5
NS(config-router)# Neighbor 10.102.29.170 remote-as 100
NS(config-router)# Address-family ipv4
NS(config-router-af)# Neighbor 10.102.29.170 activate
NS(config-router)# redistribute kernel
NS(config-router)# redistribute static
<!--NeedCopy-->
```

Requisitos previos para BGP IPv6

Antes de empezar a configurar BGP de IPv6, haga lo siguiente:

- Asegúrese de entender el protocolo BGP IPv6.
- Habilite la función IPv6.

Publicidad de rutas BGP IPv6

Border Gateway Protocol (BGP) permite que un enrutador ascendente equilibre la carga del tráfico entre dos servidores virtuales idénticos alojados en dos dispositivos Citrix ADC independientes. La publicidad de rutas permite que un enrutador ascendente realice un seguimiento de las entidades de red ubicadas detrás de Citrix ADC.

Para configurar BGP para que anuncie rutas IPv6 mediante la línea de comandos VTYSH:

En el símbolo del sistema, escriba los siguientes comandos, en el orden que se muestra:

Comando	Especifica
VTYSH	Muestra el símbolo del sistema VTYSH.
configure terminal	Acceda al modo de configuración global.
router BGP < ASnumber>	Sistema autónomo BGP. < ASnumber> es un parámetro obligatorio. Valores posibles: De 1 a 4.294.967.295.
Neighbor < IPv6 address> remote-as < as-number>	Actualice la tabla de vecinos BGP de IPv6 con la dirección IPv6 local de enlace del vecino en el sistema autónomo especificado.
Address-family ipv6	Entre en el modo de configuración de la familia de direcciones.
Neighbor < IPv6 address> activate	Intercambie prefijos para la familia de enrutadores IPv6 entre el par y el nodo local mediante la dirección local del enlace.
redistribute kernel	Redistribuya las rutas del núcleo.
redistribute static	Redistribuya las rutas estáticas.

Ejemplo:

```
>VTYSH
NS# configure terminal
NS(config)# router BGP 5
NS(config-router)# Neighbor a1bc::102 remote-as 100
NS(config-router)# Address-family ipv6
NS(config-router-af)# Neighbor a1bc::102 activate
NS(config-router)# redistribute kernel
NS(config-router)# redistribute static
```



```
<!--NeedCopy-->
```

Verificación de la configuración de BGP

Puede utilizar VTYSH para mostrar la configuración de BGP.

Para ver la configuración de BGP mediante la línea de comandos VTYSH

En el símbolo del sistema, escriba:

```
VTYSH
You are now in the VTYSH command prompt. An output similar to the
   following appears:
NS170#
At the VTYSH command prompt, type:
NS170# sh ip BGP
NS170# sh BGP
NS170# sh ip BGP neighbors
NS170# sh ip BGP summary
NS170# sh ip BGP route-map <map-tag>
<!--NeedCopy-->
```

As-Override en el protocolo de puerta de enlace

Como parte de la funcionalidad de prevención de bucles BGP, si un router recibe un paquete BGP que contiene el número de sistema autónomo (ASN) del router en la ruta de sistemas autónomos (AS), el router descarta el paquete. Se supone que el paquete se originó en el enrutador y ha llegado al lugar desde donde se originó.

Si una empresa tiene varios sitios con un mismo ASN, la prevención de bucles BGP hace que los sitios con un ASN idéntico no se vinculen con otro ASN. Las actualizaciones de redirección (paquetes BGP) se eliminan cuando otro sitio las recibe.

Para resolver este problema, se ha agregado la funcionalidad de BGP AS-Override al módulo de redirección ZebOS BGP del Citrix ADC.

Con AS-override habilitado para un dispositivo par, cuando el dispositivo Citrix ADC recibe un paquete BGP para reenviarlo al par y el ASN del paquete coincide con el del mismo, el dispositivo reemplaza el ASN del paquete BGP con su propio número ASN antes de reenviar el paquete.

Puede habilitar AS-Override para un vecino específico o un grupo de vecinos (grupo de pares) mediante la línea de comandos VTYSH.

Para configurar BGP AS-Override para un vecino IPv4 mediante la línea de comandos VTYSH:

Comando	Especifica
configure terminal	Acceda al modo de configuración global.
router BGP < ASnumber>	Sistema autónomo BGP. < ASnumber> es un parámetro obligatorio.
Neighbor < IPv4 address> remote-as < as-number>	Actualice la tabla de vecinos BGP de IPv4 con la dirección IPv4 del vecino en el sistema autónomo especificado.
Neighbor <IPv4 address> as-override	Habilite BGP como anulación para el vecino especificado.

```
1      > VTYSH NS# configure terminal
2      NS(config)# router BGP 200
3      NS(config-router)# Neighbor 192.0.2.100 remote-as 100
4      NS(config-router)# Neighbor 10.102.29.100 as-override
5  <!--NeedCopy-->
```

Para configurar BGP AS-Override para un grupo de pares BGP IPv4 mediante la línea de comandos VTYSH:

Comando	Especifica
configure terminal	Acceda al modo de configuración global.
router BGP < ASnumber>	Sistema autónomo BGP. < ASnumber> es un parámetro obligatorio.
Neighbor <peer group name> **peer-group**	Cree un grupo de pares BGP.
Neighbot <IPv4 address> **peer-group** <peer group name>	Asocia vecinos al grupo de pares especificado.
Neighbor <peer group name> remote-as < as-number>	Actualice la tabla de vecinos BGP de IPv4 con la dirección IPv4 del vecino en el sistema autónomo especificado.
Neighbor <peer group name> as-override	Habilite BGP como anulación para todos los vecinos que están asociados con el grupo de pares especificado.


```
1      > VTYSH NS# configure terminal
2      NS(config)# router BGP 200
3      NS(config-router)# neighbor external-peers-1 peer-group
4      NS(config-router)# neighbor 192.0.2.101 peer-group external-peers-1
5      NS(config-router)# neighbor 192.0.2.102 peer-group external-peers-1
6      NS(config-router)# neighbor 192.0.2.103 peer-group external-peers-1
7      NS(config-router)# Neighbor external-peers-1 remote-as 100
8      NS(config-router)# Neighbor external-peers-1 as-override
9  <!--NeedCopy-->
```

Para configurar BGP AS-Override para un vecino IPv6 mediante la línea de comandos VTYSH:

Comando	Especifica
configure terminal	Acceda al modo de configuración global.
router BGP < ASnumber>	Sistema autónomo BGP. < ASnumber> es un parámetro obligatorio.
Neighbor < IPv6 address> remote-as < as-number>	Actualice la tabla de vecinos BGP de IPv4 con la dirección IPv4 del vecino en el sistema autónomo especificado.
Neighbor <IPv6 address> as-override	Habilite BGP como anulación para el vecino especificado.
Address-family ipv6	Entre en el modo de configuración de la familia de direcciones.
Neighbor < IPv6 address> activate	Intercambie prefijos para la familia de enrutadores IPv6 entre el vecino especificado y el Citrix ADC mediante la dirección local del enlace.
Neighbor <IPv6 address> as-override	Habilite BGP como anulación para el vecino especificado.

```
1      > VTYSH NS# configure terminal
2      NS(config)# router BGP 200
3      NS(config-router)# Neighbor a1bc::102 remote-as 100
4      NS(config-router)# Neighbor a1bc::102 as-override
5      NS(config-router)# Address-family ipv6
6      NS(config-router-af)# Neighbor a1bc::102 activate
7      NS(config-router)# Neighbor a1bc::102 as-override
```



```
<!--NeedCopy-->
```

Para configurar BGP AS-Override para el grupo de pares IPv6 mediante la línea de comandos VTYSH:

Comando	Especifica
configure terminal	Acceda al modo de configuración global.
router BGP < ASnumber>	Sistema autónomo BGP. < ASnumber> es un parámetro obligatorio.
Neighbor <peer group name> **peer-group**	Cree un grupo de pares BGP.
Neighbor <IPv6 address> **peer-group** <peer group name>	Asocia un vecino al grupo de pares especificado.
Neighbor <peer group name> remote-as < as-number>	Actualice la tabla de vecinos BGP de IPv4 con la dirección IPv4 del vecino en el sistema autónomo especificado.
Neighbor <peer group name> as-override	Habilite BGP como anulación para todos los vecinos que están asociados con el grupo de pares especificado.
Address-family ipv6	Entre en el modo de configuración de la familia de direcciones.
Neighbor <peer group name> activate	Intercambie prefijos para la familia de enrutadores IPv6 entre los vecinos del grupo de pares especificado y el Citrix ADC mediante la dirección local del enlace.
Neighbor <peer group name> as-override	Habilite BGP como anulación para todos los vecinos que están asociados con el grupo de pares especificado.

```
> VTYSH NS# configure terminal
NS(config)# router BGP 200
NS(config-router)# neighbor external-peers-2 peer-group
NS(config-router)# neighbor 2001::1 peer-group external-peers-2
NS(config-router)# neighbor 2001::2 peer-group external-peers-2
NS(config-router)# Neighbor external-peers-2 remote-as 100
NS(config-router)# Neighbor external-peers-2 as-override
NS(config-router)# Address-family ipv6
NS(config-router-af)# Neighbor external-peers-2 activate
```



```
10      NS(config-router)# Neighbor external-peers-2 as-override
11  <!--NeedCopy-->
```

Reinicio estable

En una configuración de alta disponibilidad (HA) no INC en la que se configura un protocolo de redirección, después de una conmutación por error, los protocolos de redirección se convergen y se aprenden las rutas entre el nuevo nodo principal y los enrutadores vecinos adyacentes. El aprendizaje en ruta tarda algún tiempo en completarse. Durante este tiempo, el reenvío de paquetes se retrasa, el rendimiento de la red puede verse afectado y los paquetes pueden caerse.

El reinicio estable permite que una configuración de alta disponibilidad durante una conmutación por error dirija a sus enrutadores adyacentes para que no eliminen las rutas aprendidas del nodo principal antiguo de sus bases de datos de redirección. Mediante la información de redirección del nodo principal antiguo, el nuevo nodo primario y los enrutadores adyacentes comienzan inmediatamente a reenviar paquetes, sin interrumpir el rendimiento de la red.

> **Nota:**
>
> El reinicio estable no es compatible con las configuraciones de alta disponibilidad en modo INC.

Configuración de reinicio estable para BGP

Para configurar el reinicio estable para BGP mediante la línea de comandos VTYSH, en el símbolo del sistema, escriba los siguientes comandos, en el orden que se muestra:

Comando	Ejemplo	Descripción del comando
VTYSH	VTYSH	Entra en el símbolo del sistema VTYSH.
configure terminal	NS# configure terminal	Entra en el modo de configuración global.

Comando	Ejemplo	Descripción del comando
router-id <ID>	NS(config)# router-id 1.1.1.1	Un identificador de enrutador para el dispositivo Citrix ADC. Este identificador se establece para todos los protocolos de redirección dinámica. El mismo identificador debe especificarse en el otro nodo en una configuración de alta disponibilidad para que el reinicio correcto funcione correctamente.
router bgp <AS-number>	NS(config)# router bgp 5	Entra en el modo de configuración BGP.
bgp graceful-restart	NS(config)# bgp graceful-restart	Habilita el reinicio estable en el proceso de redirección BGP.
bgp graceful-restart restart-time <1-1800>	NS(config-router)# bgp graceful-restart restart-time 170	Especifica el período de gracia, en segundos, en el que los enrutadores auxiliares esperan una conexión TCP desde el nuevo nodo principal después de una conmutación por error. Durante esta cantidad de tiempo, los enrutadores auxiliares conservan las rutas.
bgp graceful-restart stalepath-time <1-1800>	NS(config-router)# bgp graceful-restart stalepath-time 180	Especifica el tiempo, en segundos, que el dispositivo Citrix ADC en modo auxiliar conserva las rutas obsoletas para reiniciar los enrutadores vecinos. El valor predeterminado es 360 segundos.

Comando	Ejemplo	Descripción del comando
neighbor <IPv4 address of the peer router> remote-as <AS-number>	NS(config-router)# neighbor 192.0.2.30 remote-as 2	Establece el interconexión BGP con el dispositivo de enrutador vecino especificado.
neighbor <IPv4 address of the peer router> capability graceful-restart	NS(config-router)# neighbor 192.0.2.30 capability graceful-restart	Permite un reinicio estable con el vecino especificado.
redistribute kernel	NS(config-router)# redistribute kernel	Redistribuye las rutas del núcleo.

Configuración de reinicio estable para IPv6 BGP

Para configurar el reinicio estable para BGP de IPv6 mediante la línea de comandos VTYSH, en el símbolo del sistema, escriba los siguientes comandos, en el orden que se muestra:

Comando	Ejemplo	Descripción del comando
VTYSH	VTYSH	Entra en el símbolo del sistema VTYSH.
configure terminal	NS# configure terminal	Entra en el modo de configuración global.
router-id <id>	NS(config)# router-id 1.1.1.1	Establece un identificador de enrutador para el dispositivo Citrix ADC. Este identificador se establece para todos los protocolos de redirección dinámica. El mismo identificador debe especificarse en el otro nodo en una configuración de alta disponibilidad para que el reinicio correcto funcione correctamente.
router bgp <AS-number>	NS(config)# router bgp 5	Entra en el modo de configuración del protocolo BGP.

Comando	Ejemplo	Descripción del comando
bgp graceful-restart	NS(config)# bgp graceful-restart	Habilita el reinicio estable en el proceso de redirección BGP.
bgp graceful-restart restart-time <1-1800>	NS(config-router)# bgp graceful-restart restart-time 170	Especifica el período de gracia, en segundos, en el que los enrutadores auxiliares esperan una conexión TCP desde el nuevo nodo principal después de una conmutación por error. Durante esta cantidad de tiempo, los enrutadores auxiliares conservan las rutas. El valor predeterminado es 360 segundos.
bgp graceful-restart stalepath-time <1-1800>	NS(config-router)# bgp graceful-restart stalepath-time 180	Especifica el tiempo, en segundos, que el dispositivo Citrix ADC en modo auxiliar conserva las rutas obsoletas para reiniciar los enrutadores vecinos. El valor predeterminado es 360 segundos.
neighbor <IPv6 address> remote-as <AS-number>	NS(config-router)# neighbor 2001:db8::10 remote-as 2	Establece el interconexión BGP con el dispositivo de enrutador vecino especificado.
address-family ipv6	NS(config-router)#address-family ipv6	Accede al modo de configuración de la familia de direcciones.
neighbor <IPv6 address of the neighbor> activate	NS(config-router-af)#neighbor 2001:db8::10 activate	Permite el intercambio de rutas de familias de direcciones con el dispositivo de enrutador vecino especificado.

Comando	Ejemplo	Descripción del comando
neighbor <IPv6 address of the neighbor> capability graceful-restart	NS(config-router-af)#neighbor 2001:db8::10 capability graceful-restart	Permite el reinicio estable con el dispositivo de enrutador vecino especificado.
redistribute kernel	NS(config-router-af)#redistribute kernel	Redistribuye las rutas del núcleo.
exit-address-family	NS(config-router-af)#exit-address-family	Sale del modo de configuración de la familia de direcciones.

Configuración de la autenticación MD5 para BGP de IPv4

El dispositivo Citrix ADC admite la autenticación MD5 para el protocolo Border Gateway (BGP). Cuando la autenticación está habilitada, cualquier segmento TCP perteneciente a BGP intercambiado entre el dispositivo Citrix ADC y su dispositivo del mismo nivel se verifica y acepta solo si la autenticación se realiza correctamente. Para que la autenticación sea correcta, ambos pares deben configurarse con la misma contraseña MD5. Si la autenticación falla, no se establece la relación de vecinos de BGP. La compatibilidad con la autenticación MD5 para BGP en el dispositivo Citrix ADC cumple con RFC 2385.

Antes de comenzar

Antes de empezar a configurar la autenticación BGP MD5, tenga en cuenta los siguientes puntos:

- Asegúrese de que comprende los diferentes componentes de la autenticación BGP MD5, descritos en RFC 2385.
- La autenticación BGP MD5 no se admite en las particiones de administración de Citrix ADC.
- La autenticación BGP MD5 no se admite para las configuraciones de BGP IPv6.
- La autenticación BGP MD5 es compatible con las configuraciones de clústeres de Citrix ADC, así como para las configuraciones de alta disponibilidad.
- Debido al siguiente problema en FreeBSD, Citrix recomienda establecer valores bajos de mantenimiento y tiempo de espera (por ejemplo, 5 y 15) y configurar el reinicio sin problemas para una sesión BGP en una configuración de alta disponibilidad de Capa 2. De lo contrario, con la autenticación MD5 habilitada, BGP podría tardar más en restablecer una conexión con el vecino después de una conmutación por error.
  - El último ACK de FreeBSD no contiene el resumen md5:
    * https://forums.freebsd.org/threads/11170/

* http://support.pfsense.narkive.com/povrH5HI/bgp-md5-weird-behavior-when-connection-closes

Configuración de la autenticación MD5 para BGP de IPv4

Para configurar la autenticación MD5 para BGP de IPv4 mediante la línea de comandos VTYSH, en el símbolo del sistema, escriba los siguientes comandos, en el orden que se muestra:

Comando	Especifica
vtysh	Muestra el símbolo del sistema VTYSH.
configure terminal	Entra en el modo de configuración global.
router bgp <AS-number>	Entra en el modo de configuración del protocolo BGP. <AS-number>es un número de sistema autónomo BGP y es un parámetro obligatorio.
neighbor <neighbour IPv4 address> remote-as < AS-number >	Actualiza la tabla BGP de IPv4 con la dirección IPv4 del vecino en el sistema autónomo especificado.
neighbor < neighbour IPv4 address > password < password in double quotes>	Configura la autenticación MD5 para el vecino especificado con la contraseña MD5 especificada. Para que la autenticación MD5 se realice correctamente, debe configurar la misma contraseña MD5 en el dispositivo Citrix ADC y en el dispositivo vecino.

```
> vtysh

ns# configure terminal

ns(config)#router bgp 5

ns(config-router)#neighbor 20.20.20.138 remote-as 1

ns(config-router)#neighbor 20.20.20.138 password  “secret”

ns(config-router)#redistribute kernel

```



```
ns(config-router)#exit

<!--NeedCopy-->
```

Configuración de IPv6 RIP

August 20, 2021

IPv6 Routing Information Protocol (RIP) o RipNG es un protocolo de vectores de distancia. Este protocolo es una extensión de RIP para admitir IPv6. Después de habilitar IPv6 RIP, debe configurar el anuncio de rutas RIP IPv6. Para solucionar problemas, puede limitar la propagación IPv6 RIP. Puede mostrar la configuración RIP de IPv6 para verificar la configuración.

Requisitos previos para IPv6 RIP

Antes de comenzar a configurar IPv6 RIP, haga lo siguiente:

- Asegúrese de comprender el protocolo RIP IPv6.
- Instale la licencia IPv6pt en el dispositivo Citrix ADC.
- Habilite la función IPv6.

Publicidad IPv6 RIP Rutas

IPv6 RIP permite a un router ascendente equilibrar la carga del tráfico entre dos servidores virtuales idénticos alojados en dos dispositivos Citrix ADC independientes. El anuncio de ruta permite que un enrutador ascendente realice un seguimiento de las entidades de red ubicadas detrás del Citrix ADC.

Para configurar IPv6 RIP para anunciar rutas IPv6 mediante la línea de comandos VTYSH:

En el símbolo del sistema, escriba los siguientes comandos, en el orden que se muestra:

Comando	Especifica
VTYSH	Muestra el símbolo del sistema VTYSH.
configure terminal	Acceda al modo de configuración global.
router ipv6 rip	Inicie el proceso de redirección RIP IPv6 e introduzca el modo de configuración para el proceso de redirección.
redistribute static	Redistribuir rutas estáticas.
redistribute kernel	Redistribuir las rutas del núcleo.

Ejemplo:

```
>VTYSH
NS# configure terminal
NS(config)# router ipv6 rip
NS(config-router)# redistribute static
NS(config-router)# redistribute kernel
<!--NeedCopy-->
```

Limitación de Propagaciones RIP IPv6

Si necesita solucionar los problemas de su configuración, puede configurar el modo de solo escucha en cualquier interfaz dada.

Para limitar la propagación RIP IPv6 mediante la línea de comandos VTYSH:

En el símbolo del sistema, escriba los siguientes comandos, en el orden que se muestra:

Comando	Especifica
VTYSH	Muestra el símbolo del sistema VTYSH.
configure terminal	Acceda al modo de configuración global.
router ipv6 rip	Inicie el proceso de redirección RIP IPv6 e introduzca el modo de configuración para el proceso de redirección.
passive-interface < vlan_name>	Suprimir las actualizaciones de redirección en las interfaces enlazadas a la VLAN especificada.

Ejemplo:

```
>VTYSH
NS# configure terminal
NS(config)# router ipv6 rip
NS(config-router)# passive-interface VLAN0
<!--NeedCopy-->
```


Verificación de la configuración RIP de IPv6

Puede utilizar VTYSH para mostrar la tabla de redirección IPv6 RIP e información RIP IPv6 para una VLAN especificada.

Para ver la configuración RIP de IPv6 mediante la línea de comandos VTYSH:

En el símbolo del sistema, escriba los siguientes comandos, en el orden que se muestra:

Comandos	Especifica
VTYSH	Muestra el símbolo del sistema VTYSH.
sh ipv6 rip	Muestra la tabla de redirección IPv6 RIP actualizada.
interfaz de rip sh ipv6 <vlan_name>	Muestra la información RIP de IPv6 para la VLAN especificada.

Ejemplo:

```
NS# VTYSH
NS# sh ipv6 rip
NS# sh ipv6 rip interface VLAN0
<!--NeedCopy-->
```

Configuración de OSPF IPv6

December 2, 2021

IPv6 OSPF u OSPF versión 3 (OSPF v3) es un protocolo de estado de enlace que se utiliza para intercambiar información de redirección IPv6. Después de habilitar OSPF IPv6, debe configurar el anuncio de las rutas OSPF IPv6. Para solucionar problemas, puede limitar la propagación de OSPF IPv6. Puede mostrar la configuración OSPF de IPv6 para verificar la configuración.

Requisitos previos para OSPF IPv6

Antes de comenzar a configurar OSPF de IPv6, haga lo siguiente:

- Asegúrese de entender el protocolo OSPF IPv6.
- Instale la licencia IPv6pt en el dispositivo Citrix ADC.
- Habilite la función IPv6.

Publicidad de rutas IPv6

IPv6 OSPF permite que un enrutador ascendente equilibre la carga del tráfico entre dos servidores virtuales idénticos alojados en dos dispositivos Citrix ADC independientes. La publicidad de rutas permite que un enrutador ascendente realice un seguimiento de las entidades de red ubicadas detrás de Citrix ADC.

Para configurar OSPF IPv6 para anunciar rutas IPv6 mediante la línea de comandos VTYSH:

En el símbolo del sistema, escriba los siguientes comandos, en el orden que se muestra:

Comandos	Especifica
VTYSH	Muestra el símbolo del sistema VTYSH.
configure terminal	Acceda al modo de configuración global.
router ipv6 OSPF	Inicie el proceso de redirección OSPF IPv6 e introduzca el modo de configuración para el proceso de redirección.
redistribute static	Redistribuya las rutas estáticas.
redistribute kernel	Redistribuya las rutas del núcleo.

Ejemplo:

```
>VTYSH
NS# configure terminal
NS(config)# router ipv6 OSPF
NS(config-router)# redistribute static
NS(config-router)# redistribute kernel
<!--NeedCopy-->
```

Limitación de las propagaciones OSPF IPv6

Si necesita solucionar problemas de configuración, utilice VTYSH para configurar el modo de solo escucha en cualquier VLAN determinada.

Para limitar la propagación de OSPF IPv6 mediante la línea de comandos VTYSH:

En el símbolo del sistema, escriba los siguientes comandos, en el orden que se muestra:

Comandos	Especifica
VTYSH	Muestra el símbolo del sistema VTYSH.
configure terminal	Acceda al modo de configuración global.
router ipv6 OSPF	Inicie el proceso de redirección OSPF IPv6 e introduzca el modo de configuración para el proceso de redirección.
passive-interface < vlan_name >	Suprimir las actualizaciones de redirección en las interfaces enlazadas a la VLAN especificada.

Ejemplo:

```
>VTYSH
NS# configure terminal
NS(config)# router ipv6 OSPF
NS(config-router)# passive-interface VLAN0
<!--NeedCopy-->
```

Verificación de la configuración de OSPF de IPv6

Utilice VTYSH para mostrar los vecinos actuales OSPF IPv6 y las rutas OSPF IPv6.

Para ver la configuración de OSPF de IPv6 mediante la línea de comandos VTYSH:

En el símbolo del sistema, escriba los siguientes comandos, en el orden que se muestra:

Comando	Especifica
VTYSH	Muestra el símbolo del sistema VTYSH.
sh ipv6 OSPF neighbor	Muestra los vecinos actuales.
sh ipv6 OSPF route	Muestra rutas OSPF IPv6.

Ejemplo:

```
>VTYSH
NS# sh ipv6 OSPF neighbor
NS# sh ipv6 OSPF route
```



```
<!--NeedCopy-->
```

Autenticación OSPFv3

Para garantizar la integridad, la autenticación del origen de los datos y la confidencialidad de los datos de los paquetes OSPFv3, la autenticación OSPFv3 debe configurarse en pares OSPFv3.

El dispositivo Citrix ADC admite la autenticación OSPFv3 y cumple parcialmente con RFC 4552. La autenticación OSPFv3 se basa en los dos protocolos IPSec: Encabezado de autenticación (AH) y Carga útil de seguridad de encapsulación (ESP). El dispositivo Citrix ADC solo admite el protocolo AH para la autenticación OSPFv3.

La autenticación OSPFv3 utiliza asociaciones de seguridad (SA) IPSec definidas manualmente entre los pares OSPFv3 y no se basa en el protocolo IKE para formar SA dinámicas. Las SA manuales definen los valores, los algoritmos y las claves del índice de seguridad (SPI) que se utilizarán entre los pares. Las SA manuales no requieren negociación entre los pares; por lo tanto, la misma SA debe definirse en ambos pares.

Puede configurar la autenticación OSPFv3 en una VLAN o para un área OSPFv3. Cuando se configura para una VLAN, los ajustes se aplican a todas las interfaces que son miembros de la VLAN. Al configurar la autenticación OSPFv3 para un área OSPF, la configuración se aplica a todas las VLAN de esa área. La configuración se aplica a su vez a todas las interfaces que son miembros de estas VLAN. Esta configuración no se aplica a las VLAN miembros en las que ha configurado la autenticación OSPFv3 directamente.

Tenga en cuenta los siguientes puntos y limitaciones antes de configurar la autenticación OSPFv3 en un dispositivo Citrix ADC:

- Asegúrese de que comprende los diferentes componentes de la autenticación OSPFv3, descritos en RFC 4552.
- Solo se admite el protocolo de encabezado de autenticación para la autenticación OSPFv3. No se admite la carga útil de seguridad encapsulante (ESP).
- Debe definir una SA con la misma configuración en la interfaz del mismo nivel.
- No se admite la reclave de las teclas manuales.

Para configurar la autenticación OSPFv3 en una VLAN mediante la línea de comandos VTYSH:

En el símbolo del sistema, escriba los siguientes comandos, en el orden mostrado: comandos de VLAN de autenticación OSPFv3.

Ejemplo:

```
> VTYSH NS# configure terminal
```



```
NS(config)# interface vlan2
NS(config-if)# ipv6 ospf authentication ipsec spi 256 md5 123456789
    ABCDEF0123456789ABCDEF0
<!--NeedCopy-->
```

Para configurar la autenticación OSPFv3 en un área OSPF mediante la línea de comandos VTYSH:

En el símbolo del sistema, escriba los siguientes comandos, en el orden indicado: autenticación OSPFv3 comandos de área OSPF.

Ejemplo:

```
> VTYSH NS# configure terminal
ns(config)#router ipv6 ospf 30
ns(config-router)# area 1 authentication ipsec spi 256
    md5123456789ABCDEF0123456789ABCDEF0
<!--NeedCopy-->
```

Configuración de reinicio estable para OSPF IPv6

En una configuración de alta disponibilidad (HA) no INC en la que se configura un protocolo de redirección, después de una conmutación por error, los protocolos de redirección se convergen y se aprenden las rutas entre el nuevo nodo principal y los enrutadores vecinos adyacentes. El aprendizaje en ruta tarda algún tiempo en completarse. Durante este tiempo, el reenvío de paquetes se retrasa, el rendimiento de la red puede verse afectado y los paquetes pueden caerse.

El reinicio estable permite que una configuración de alta disponibilidad durante una conmutación por error dirija a sus enrutadores adyacentes para que no eliminen las rutas aprendidas del nodo principal antiguo de sus bases de datos de redirección. Mediante la información de redirección del nodo principal antiguo, el nuevo nodo primario y los enrutadores adyacentes comienzan inmediatamente a reenviar paquetes, sin interrumpir el rendimiento de la red.

> **Nota:**
>
> El reinicio estable no es compatible con las configuraciones de alta disponibilidad en modo INC.

Para configurar el reinicio ordenado para OSPF IPv6 mediante la línea de comandos VTYSH, en el símbolo del sistema, escriba los siguientes comandos, en el orden que se muestra:

Comando	Ejemplo	Descripción del comando
VTYSH	> VTYSH	Entra en el símbolo del sistema VTYSH.

Comando	Ejemplo	Descripción del comando
configure terminal	NS# configure terminal	Entra en el modo de configuración global.
router-id id>	NS(config)#router-id 1.1.1.1	Establece un identificador de enrutador para el dispositivo Citrix ADC. Este identificador se establece para todos los protocolos de redirección dinámica. El mismo ID debe especificarse en el otro nodo en una configuración de alta disponibilidad para que el reinicio correcto funcione correctamente en la configuración de alta disponibilidad.
IPv6ospf restart grace-period <1-1800>	NS(config)# IPv6ospf restart grace-period 170	Especifica el período de gracia, en segundos, para el que se conservarán las rutas en los dispositivos auxiliares. Valor por defecto: 120 segundos.
IPv6 ospf restart helper max-grace-period <1-1800>	NS(config)# IPv6 ospf restart helper max-grace-period 180	Este es un comando opcional para limitar el período de gracia máximo durante el cual el dispositivo Citrix ADC estará en modo auxiliar. Si el dispositivo Citrix ADC recibe un LSA opaco con un período de gracia mayor que el período máximo de gracia establecido, el LSA se descarta y el Citrix ADC no se coloca en modo auxiliar.
interfaz <VLANID>	NS(config)#interface vlan3	Entra en el modo de configuración de VLAN.

Comando	Ejemplo	Descripción del comando
ipv6 router ospf area <area_id> tag <tag_id>	NS(config-if)#ipv6 router ospf area 0 tag 1	Inicia el proceso de redirección IPv6 OSPF en una VLAN.
exit	NS(config-if)#exit	Sale del modo de configuración de VLAN.
router ipv6 ospf	NS(config)# router ipv6 ospf 1	Inicia el proceso de redirección OSPF IPv6 y entrará en el modo de configuración para el proceso de redirección.
capability restart graceful	NS(config-router)#capability restart graceful	Habilita el reinicio estable en el proceso de redirección IPv6 OSPF.
redistribute kernel	NS(config-router)# redistribute kernel	Redistribuye las rutas del núcleo.

Configuración de ISIS

August 20, 2021

El dispositivo Citrix ADC admite el protocolo de redirección dinámica de sistema intermedio a sistema intermedio (IS-IS o ISIS). Este protocolo admite intercambios de rutas IPv4 así como IPv6. IS□IS es un protocolo de estado de enlace y, por lo tanto, es menos propenso a bucles de redirección. Con las ventajas de una convergencia más rápida y la capacidad de soportar redes más grandes, ISIS puede ser muy útil en redes de proveedores de servicios de Internet (ISP).

Requisitos previos para configurar ISIS

Antes de comenzar a configurar ISIS, haga lo siguiente:

- Asegúrese de entender el protocolo ISIS.
- Para rutas IPV6, habilite:
  - Función de traducción del protocolo IPv6.
  - Opción de redirección dinámica IPv6 en las VLAN en las que quiere ejecutar el protocolo ISIS.

Habilitación de ISIS

Utilice cualquiera de los procedimientos siguientes para habilitar la función de redirección de ISIS en el dispositivo Citrix ADC.

Para habilitar la redirección ISIS mediante la CLI:

En el símbolo del sistema, escriba:

habilitar el ISIS de función ns

Para habilitar la redirección de ISIS mediante la GUI:

1. Desplácese hasta Sistema > Configuración, en el grupo Modos y funciones, haga clic en Cambiar funciones avanzadas.
2. Seleccione o desactive la opción Redirección ISIS.

Creación de un proceso de redirección ISIS e iniciarlo en una VLAN

Para crear un proceso de redirección ISIS, debe utilizar la línea de comandos VTYSH.

En el símbolo del sistema, escriba los siguientes comandos, en el orden que se muestra:

Comando	Descripción
VTYSH	Muestra el símbolo del sistema VTYSH.
configure terminal	Accede al modo de configuración global.
[etiqueta]ISIS router	Crea un proceso de redirección ISIS y un modo de configuración para el proceso de redirección.
neto XX… XXXX.AAAAAA	Especifica un valor NET para el proceso de redirección, donde: · **XX… .XXXX** es la dirección de área (puede ser de 1 a 13 bytes), · **AAAAA** es el Id. del sistema (6 bytes), · **00** es el selector N (1 byte).
is-type (nivel-1|nivel-1-2|solo nivel 2)	Establece el proceso de redirección ISIS en el nivel especificado de redirección. Valor predeterminado: Nivel 1-2.
ns IPv6-routing	Inicia el daemon de redirección dinámica IPv6.
interfaz <vlan_name>	Entra en el modo de configuración de VLAN.
ip router ISIS	Habilita el proceso de redirección ISIS en la VLAN para intercambios de rutas IPv4.

Comando	Descripción
ISIS del enrutador ipv6	Habilita el proceso de redirección ISIS en la VLAN para intercambios de rutas IPv6.

Ejemplo:

```
> VTYSH
NS# configure terminal
NS(config)# router isis 11
NS(config-router)# net 15.aabb.ccdd.0097.00
NS(config-router)# is-type level-1
NS(config-router)# exit
NS(config)# ns IPv6-routing
NS(config)# interface vlan0
NS(config-if)#  ip router isis 11
NS(config-if)# ipv6 router isis 11
<!--NeedCopy-->
```

Rutas publicitarias

El anuncio de ruta permite a un enrutador ascendente realizar un seguimiento de las entidades de red ubicadas detrás del dispositivo Citrix ADC.

Para configurar ISIS para anunciar rutas mediante la línea de comandos VTYSH:

En el símbolo del sistema, escriba los siguientes comandos, en el orden que se muestra:

Comando	Descripción
VTYSH	Muestra el símbolo del sistema VTYSH.
configure terminal	Accede al modo de configuración global.
enrutador ISIS [etiqueta]	Inicia la instancia de redirección ISIS e introducirá al modo de configuración para el proceso de redirección.
redistribuir conectado (nivel 1 o nivel-1-2 o nivel 2)	Redistribuye rutas conectadas, donde: **nivel 1**: Redistribuye rutas conectadas en nivel 1, **nivel 1-2**: Redistribuye rutas conectadas en nivel 1 y nivel 2, **nivel 2**: Redistribuye rutas conectadas en nivel 2.

Comando	Descripción
redistribuir kernel (nivel-1 o nivel-1-2 o nivel 2)	Redistribuye las rutas del kernel, donde: **nivel-1**: Redistribuir las rutas del kernel en el nivel 1, **nivel-1-2**: Redistribuir las rutas del kernel en el nivel 1 y el nivel 2, **nivel 2**: redistribuir las rutas del kernel en el nivel 2.

Ejemplo:

```
>VTYSH
NS# configure terminal
NS(config)# router isis 11
NS(config-router)# redistribute connected level-1
NS(config-router)# redistribute kernel level-1
<!--NeedCopy-->
```

Limitación de Propagaciones de ISIS

Si necesita solucionar problemas de configuración, puede configurar el modo de solo escucha en cualquier VLAN determinada.

Para limitar la propagación de ISIS mediante la línea de comandos VTYSH:

En el símbolo del sistema, escriba los siguientes comandos, en el orden que se muestra:

Comando	Descripción
VTYSH	Muestra el símbolo del sistema VTYSH.
configure terminal	Accede al modo de configuración global.
router isis [etiqueta]	Accede al modo de configuración para el proceso de redirección.
interfaz pasiva <vlan_name>	Suprime las actualizaciones de redirección en interfaces enlazadas a la VLAN especificada.

Ejemplo:


```
>VTYSH
NS# configure terminal
NS(config)# router isis 11
NS(config-router)# passive-interface VLAN0
<!--NeedCopy-->
```

Verificación de la configuración ISIS

Puede utilizar VTYSH para mostrar la tabla de redirección de ISIS y la información de ISIS para una VLAN especificada.

Para ver la configuración de ISIS mediante la línea de comandos VTYSH:

En el símbolo del sistema, escriba los siguientes comandos, en el orden que se muestra:

Comandos	Descripción
VTYSH	Muestra el símbolo del sistema VTYSH.
show ip isis route	Muestra la tabla de redirección ISIS IPv4 actualizada.
show ipv6 isis route	Muestra la tabla de redirección ISIS IPv6 actualizada.
interfaz sh isis <vlan_name>	Muestra información de ISIS IPv6 para la VLAN especificada.

Ejemplo:

```
NS# VTYSH
NS#  show ip isis route
NS#  show ipv6 isis route
NS# sh isis interface VLAN0
<!--NeedCopy-->
```

Instalar rutas en la tabla de redirección Citrix ADC

August 20, 2021

El dispositivo Citrix ADC puede utilizar rutas aprendidas por varios protocolos de redirección después de instalar las rutas en la tabla de redirección del dispositivo.

Para instalar varias rutas en la tabla de redirección interno mediante la línea de comandos VTYSH:

En la CLI, escriba los siguientes comandos según corresponda para las rutas que quiera instalar:

Comandos	Especifica
VTYSH	Muestra el símbolo del sistema VTYSH.
configure terminal	Acceda al modo de configuración global.
ns route-install Predeterminado	Instale las rutas predeterminadas IPv4 en la tabla de redirección interno.
RIP de instalación de redirección ns	Instale rutas específicas RIP IPv4 en la tabla de redirección interno.
ns instalación de rute-install BGP	Instale rutas específicas de IPv4 BGP en la tabla de redirección interno.
ns rute-install OSPF	Instale rutas específicas de IPv4 OSPF en la tabla de redirección interno.
ns route-install IPv6 Predeterminado	Instale las rutas predeterminadas de IPv6 en la tabla de redirección interno.
RIP IPv6 de instalación de redirección ns	Instale las rutas específicas de RIP IPv6 en la tabla de redirección interno.
ns instalación de redirección IPv6 BGP	Instale las rutas específicas de IPv6 BGP en la tabla de redirección interno.
ns route-install IPv6 OSPF	Instale las rutas específicas de IPv6 OSPF en la tabla de redirección interno.

Ejemplo:

```
>VTYSH
NS# configure terminal
NS# ns route-install Default
NS(config)# ns route-install RIP
NS(config)# ns route-install BGP
NS(config)# ns route-install OSPF
NS# ns route-install IPv6 Default
NS(config)# ns route-install IPv6 RIP
NS(config)# ns route-install IPv6 BGP
```



```
NS(config)# ns route-install IPv6 OSPF
<!--NeedCopy-->
```

Anuncio de rutas SNIP y VIP a áreas selectivas

January 12, 2021

Para anunciar algunas direcciones SNIP en áreas selectivas, no se puede utilizar habilitar el modo DRADV o redistribuir las operaciones ZebOS de conexión. Esto se debe a que estas operaciones envían todas las rutas conectadas a ZebOS. Además, agregar rutas estáticas ficticias en ZebOS para las subredes necesarias, o agregar ACL en ZebOS para filtrar rutas conectadas no deseadas, es una tarea engorrosa y tediosa.

Las opciones Ruta de red y Etiqueta solucionan este problema. Puede habilitar la opción Ruta de red solo para una dirección SNIP por subred. La ruta conectada para esa dirección SNIP se envía como una ruta del núcleo a ZebOS.

Para las direcciones VIP y SNIP, Tag, se puede asignar un entero del 1 al 4294967295. Este parámetro solo se puede establecer cuando Ruta de host o Ruta de red están habilitados para direcciones VIP o SNIP. El valor de etiqueta asociado con las direcciones VIP y SNIP también se envía junto con sus rutas a ZebOS. Se pueden establecer etiquetas con diferentes valores para las rutas VIP y SNIP. Estos valores de etiqueta se pueden comparar en mapas de rutas en ZebOS y anunciarse en áreas selectivas.

Anunciar rutas SNIP a áreas selectivas

Para configurar la ruta de red y los parámetros de etiqueta de una dirección SNIP mediante la CLI:

En el símbolo del sistema, escriba:

- Si agrega una nueva dirección SNIP:
  - **add ns ip** <IPAddress>@ <netmask> -**type SNIP** -**networkroute** (**ENABLED** | **DISABLED**) -**tag** <positive_integer>
  - **show ns ip** <IPAddress>
- Si reconfigura una dirección SNIP existente:
  - **set ns ip** <IPAddress>@ <netmask> -**type SNIP**: **networkroute** (**ENABLED** | **DISABLED**) -**tag** <positive_integer>
  - **show ns ip** <IPAddress>

Para configurar la ruta de red y los parámetros de etiqueta de una dirección SNIP mediante GUI:

1. Vaya a **Sistema**> **Red** > **Direcciones IP** > **Direcciones IPv4**.

2. Establezca los parámetros **Ruta de red** y **Etiqueta** mientras agrega una dirección IP de subred (SNIP) o modifica una dirección IP de subred existente.

Anunciar rutas VIP a áreas selectivas

Para configurar los parámetros de ruta y etiqueta del host de una dirección VIP mediante la CLI:

En el símbolo del sistema, escriba uno de los siguientes conjuntos de comandos.

- Si agrega una nueva dirección VIP:
  - **add ns ip** <IPAddress>@ <netmask> -**type VIP** -**hostRoute** (**ENABLED** | **DISABLED**) -**tag** <positive_integer>
  - **show ns ip** <IPAddress>
- Si reconfigura una dirección VIP existente:
  - **set ns ip** <IPAddress>@ <netmask> -**type VIP** -**hostRoute** (**ENABLED** | **DISABLED**) -**tag** <positive_integer>
  - **show ns ip** <IPAddress>

Para configurar la ruta de red y los parámetros de etiqueta de una dirección VIP mediante la GUI:

1. Vaya a **Sistema** > **Red** > **Direcciones IP** > **Direcciones IPv4**.
2. Establezca los parámetros **Ruta del host** y **Etiqueta** mientras agrega una dirección VIP o modifica una dirección VIP existente.

Configuración de la detección de reenvío bidireccional

August 20, 2021

El protocolo de detección de reenvío bidireccional (BFD) es un mecanismo para la detección rápida de fallas de rutas de reenvío. BFD detecta errores de ruta en el orden de milisegundos. BFD se utiliza con protocolos de redirección dinámica.

En la operación BFD, los pares de redirección intercambian paquetes BFD en un intervalo negociado. Si no se recibe un paquete de un par dentro del intervalo negociado más el intervalo de gracia, se considera que el par está muerto y se enviará una notificación al conjunto de protocolos de redirección registrados. A su vez, los protocolos de redirección vuelven a calcular la mejor ruta y reprograman la tabla de redirección. BFD admite intervalos de tiempo más pequeños, en comparación con los temporizadores proporcionados por los protocolos de redirección, lo que resulta en una detección más rápida de fallas.

El dispositivo Citrix ADC admite BFD para los siguientes protocolos de redirección: BGP (IPv4 e IPv6), OSPFv2 (IPv4) y OSPFv3 (IPv6). La compatibilidad con BFD en el dispositivo Citrix ADC es compatible con RFC 5880, 5881 y 5883.

Puntos a considerar para configurar la detección de reenvío bidireccional

Antes de comenzar a configurar BFD, tenga en cuenta los siguientes puntos:

- Asegúrese de que comprende los diferentes componentes de BFD, descritos en RFC 5880, 5881 y 5883.
- BFD en un dispositivo Citrix ADC es compatible con los siguientes protocolos de redirección:
  - BGP (IPv4 e IPv6)
  - OSPFv2 (IPv4)
  - OSPFv3 (IPv6)
- BFD en un dispositivo Citrix ADC no es compatible con los siguientes protocolos de redirección:
  - ISIS
  - RIP (IPv4)
  - RipNG (IPv6)
- Las siguientes funciones de BFD no son compatibles con un dispositivo Citrix ADC:
  - Modo de eco BFD
  - Autenticación BFD
  - Modo asíncrono de demanda BFD
- Los valores mínimos para los temporizadores de intervalo BFD y BFD Rx son 100 milisegundos.
- Cuando BFD se utiliza en una topología con direcciones IP compartidas (por ejemplo, configuración de alta disponibilidad de capa 2 con direcciones SNIP o una configuración de clúster con direcciones IP seccionadas), BFD reduce las sesiones activas durante una conmutación por error porque el tiempo de detección de errores de BFD (orden de milisegundos) es menor que el HA intervalo de detección de conmutación por error (3 a 4 segundos). Por lo tanto, Citrix recomienda el uso de Graceful restart en topologías de alta disponibilidad de capa 2, ya que las rutas se conservan durante el proceso de conmutación por error.

Pasos de configuración

La configuración de BFD en un dispositivo Citrix ADC consta de las siguientes tareas:

- Configurar parámetros de BFD
- Configurar compatibilidad con BFD para protocolos de redirección dinámica

Configurar parámetros de BFD

El dispositivo Citrix ADC proporciona parámetros de sesión BFD independientes para sesiones de salto único, sesiones de salto múltiple IPv4 e sesiones de salto múltiple IPv6. Si no configura parámetros BFD para un tipo de sesión, se aplicarán los valores predeterminados para esa sesión.

El valor predeterminado de cada parámetro BFD es el mismo para sesiones de salto único, sesiones de salto múltiple IPv4 y sesiones de salto múltiple IPv6. En la siguiente tabla se muestra el valor predeterminado de cada parámetro BFD.

Nombre del parámetro BFD	Valor predeterminado
Intervalo	750 milésimas de segundo
Rx mínimo	500 milésimas de segundo
Multiplicador	3

> **IMPORTANTE:**
>
> Las NIC de Mellanox en un dispositivo Citrix tardan alrededor de 1500 ms en inicializarse. Debe establecer los temporizadores BFD en más de 1500 ms para un dispositivo Citrix ADC con NIC Mellanox. Citrix recomienda configurar los temporizadores BFD en 3000 ms:
>
> - Intervalo Tx = 600 ms
> - Rx mínimo = 600 ms
> - Multipler = 5

Configuración de parámetros BFD para una sesión de salto único

Para configurar los parámetros BFD para una sesión de salto único mediante la línea de VTYSH comandos, en el símbolo del sistema, escriba los siguientes comandos, en el orden mostrado:

Comando	Especifica
`vtysh`	Muestra el símbolo del sistema VTYSH.
`configure terminal`	Acceda al modo de configuración global.
`interface` `vlan ID>`	Entre en el modo de configuración de la interfaz.
`bfd singlehop-peer interval <num> minrx <num> multiplier <num>`	Configure los parámetros BFD en la interfaz especificada.

Configuración de ejemplo:

```
> vtysh

ns# configure terminal

ns(config)# interface vlan3

ns(config-if)# bfd singlehop-peer interval 200 minrx 200 multiplier 5

ns(config-if)# exit
<!--NeedCopy-->
```

Configuración de Parámetros BFD para Sesiones de Saltos Múltiples IPv4

Para configurar parámetros BFD para sesiones de saltos múltiples IPv4 mediante la línea de VTYSH comandos, en el símbolo del sistema, escriba los siguientes comandos, en el orden mostrado:

Comando	Especifica
`vtysh`	Muestra el símbolo del sistema VTYSH.
`configure terminal`	Acceda al modo de configuración global.
`bfd multihop-peer <ipv4addr> interval <num> minrx <num> multiplier <num>`	Configure los parámetros BFD para varias sesiones de saltos IPv4.

Configuración de ejemplo:

```
    > vtysh

    ns# configure terminal

    ns(config)# bfd multihop-peer 20.20.20.138 interval 300 minrx 300
       multiplier 5

    ns(config)# exit
<!--NeedCopy-->
```


Configuración de Parámetros de BFD para Sesiones de Saltos Múltiples IPv6

Para configurar los parámetros BFD para las sesiones de saltos múltiples IPv6 mediante la línea de VTYSH comandos, en el símbolo del sistema, escriba los siguientes comandos, en el orden mostrado:

Comando	Especifica
`vtysh`	Muestra el símbolo del sistema VTYSH.
`configure terminal`	Acceda al modo de configuración global.
`bfd multihop-peer ipv6 <ipv6addr> interval <num> minrx <num> multiplier <num>`	Configure los parámetros BFD para IPv6 múltiples sesiones de saltos.

Configuración de ejemplo:

```
1     > vtysh
2
3     ns(config)# bfd multihop-peer ipv6 20fe:125::138 interval 500 minrx
          500 multiplier 5
4
5     ns(config)# exit
6 <!--NeedCopy-->
```

Configurar compatibilidad con BFD para protocolos de redirección dinámica

Puede habilitar BFD para un protocolo de redirección dinámica para un tipo de sesión con un par de pares. Por ejemplo, salto único y saltos múltiples. El dispositivo Citrix ADC aplica la configuración de parámetros BFD relevantes a la sesión.

Configuración de BFD para una sesión de salto único BGP IPv4

Para configurar BFD para una sesión de salto único BGP IPv4 mediante la línea de VTYSH comandos, en el símbolo del sistema, escriba los siguientes comandos, en el orden mostrado:

Comando	Especifica
`vtysh`	Muestra el símbolo del sistema VTYSH.
`configure terminal`	Acceda al modo de configuración global.

Comando	Especifica
`router bgp <asnumber>`	Sistema autónomo BGP. `asnumber` es un parámetro obligatorio.
`neighbor <ipv4addr> remote-as <num>`	Actualice la tabla IPv4 BGP con la dirección IPv4 del vecino en el sistema autónomo especificado.
`neighbor <ipv4addr> fall-over bfd`	Habilite BFD para el vecino especificado.

Configuración de ejemplo:

```
    > vtysh

    ns# configure terminal

    ns(config)#router bgp 1

    ns(config-router)#neighbor 20.20.20.138 remote-as 1

    ns(config-router)#neighbor 20.20.20.138 fall-over bfd

    ns(config-router)#redistribute kernel

    ns(config-router)#exit
<!--NeedCopy-->
```

Configuración de BFD para una sesión de salto múltiple BGP IPv4

Para configurar BFD para una sesión de salto múltiple BGP IPv4 mediante la línea de `VTYSH` comandos, escriba los siguientes comandos en el símbolo del sistema, en el orden mostrado:

Comando	Especifica
`vtysh`	Muestra el símbolo del sistema `VTYSH`.
`configure terminal`	Acceda al modo de configuración global.
`router bgp <asnumber>`	Sistema autónomo BGP. `asnumber` es un parámetro obligatorio.

Comando	Especifica
`neighbor <ipv4addr> remote-as <num>`	Actualice la tabla IPv4 BGP con la dirección IPv4 del vecino en el sistema autónomo especificado.
`neighbor <ipv4addr> fall-over bfd multihop`	Habilite BFD para el vecino especificado.

Configuración de ejemplo:

```
    > vtysh

    ns# configure terminal

    ns(config)#router bgp 1

    ns(config-router)#neighbor 20.20.20.138 remote-as 1

    ns(config-router)#neighbor 20.20.20.138 fall-over bfd multihop

    ns(config-router)#redistribute kernel

    ns(config-router)#exit
<!--NeedCopy-->
```

Configuración de BFD para una sesión de salto único BGP IPv6

Para configurar BFD para una sesión de salto único BGP IPv6 mediante la línea de `VTYSH` comandos, escriba los comandos siguientes en el orden mostrado en el símbolo del sistema:

Comando	Especifica
`vtysh`	Muestra el símbolo del sistema `VTYSH`.
`configure terminal`	Acceda al modo de configuración global.
`router bgp <asnumber>`	Sistema autónomo BGP. `asnumber` es un parámetro obligatorio.
`neighbor <ipv6addr> remote-as <num>`	Actualice la tabla IPv6 BGP con la dirección IPv6 local del vínculo del vecino en el sistema autónomo especificado.

Comando	Especifica
`neighbor <ipv6addr> fall-over bfd`	Habilite BFD para el vecino especificado.
`address-family ipv6`	Introduzca el modo de configuración de familia de direcciones.
`neighbor <ipv6addr> activate`	Exchange prefijos para la familia de enrutadores IPv6 entre el par y el nodo local mediante la dirección local del vínculo.

Configuración de ejemplo:

```
> vtysh

ns# configure terminal ns(config)#router bgp 1

ns(config-router)#neighbor 30fe:123::124 remote-as 1

ns(config-router)#neighbor 30fe:123::124 fall-over bfd

ns(config-router)#address-family ipv6

ns(config-router-af)#neighbor 30fe:123::124 activate

ns(config-router-af)#redistribute kernel

ns(config-router-af)#exit

<!--NeedCopy-->
```

Configuración de BFD para una sesión de saltos múltiples BGP IPv6

Para configurar BFD para una sesión de salto múltiple BGP IPv6 mediante la línea de `VTYSH` comandos, escriba los siguientes comandos en el símbolo del sistema, en el orden mostrado:

Comando	Especifica
`vtysh`	Muestra el símbolo del sistema `VTYSH`.
`configure terminal`	Acceda al modo de configuración global.

Comando	Especifica
`router bgp <asnumber>`	Sistema autónomo BGP. `asnumber` es un parámetro obligatorio.
`neighbor <ipv6addr> remote-as <num>`	Actualice la tabla IPv6 BGP con la dirección IPv6 local del vínculo del vecino en el sistema autónomo especificado.
`neighbor <ipv6addr> fall-over bfd multihop`	Habilite BFD para el vecino especificado.
`address-family ipv6`	Introduzca el modo de configuración de familia de direcciones.
`neighbor <ipv6addr> activate`	Exchange prefijos para la familia de enrutadores IPv6 entre el par y el nodo local mediante la dirección local del vínculo.

Configuración de ejemplo:

```
> vtysh

ns# configure terminal

ns(config)# bfd multihop-peer ipv6 20fe:125::138 interval 500 minrx 500
     multiplier 5

ns(config)#router bgp 1

ns(config-router)#neighbor 20fe:125::138 remote-as 1

ns(config-router)#neighbor 20fe:125::138 fall-over bfd multihop

ns(config-router)#address-family ipv6

ns(config-router-af)#neighbor 20fe:125::138 activate

ns(config-router-af)#redistribute kernel

ns(config-router-af)#end

<!--NeedCopy-->
```


Configuración de BFD para OSPFv2 (IPv4) en interfaces

Puede habilitar BFD en todas o en una interfaz específica que utilice el protocolo OSPFv2.

Para configurar BFD para OSPFv2 en todas las interfaces mediante la línea de VTYSH comandos:

En el símbolo del sistema, escriba los siguientes comandos, en el orden que se muestra:

Comando	Especifica
`vtysh`	Muestra el símbolo del sistema VTYSH.
`configure terminal`	Acceda al modo de configuración global.
`router ospf <process tag>`	Introduzca el modo de configuración OSPFv2.
`bfd all-interfaces`	Habilite BFD en todas las interfaces que usan OSPFv2.

Configuración de ejemplo:

```
1      > vtysh
2
3      ns# configure terminal
4
5      ns(config)#router ospf 1
6
7      ns(config-router)#bfd all-interfaces
8
9      ns(config-router)#redistribute kernel
10
11     ns(config-router)#exit
12 <!--NeedCopy-->
```

Para configurar BFD para OSPFv2 en una interfaz específica mediante la línea de VTYSH comandos:

En el símbolo del sistema, escriba los siguientes comandos, en el orden que se muestra:

Comando	Especifica
`vtysh`	Muestra el símbolo del sistema VTYSH.
`configure terminal`	Acceda al modo de configuración global.
`interface` `<vlan ID>`	Entre en el modo de configuración de la interfaz.

Comando	Especifica
`ip ospf bfd`	Habilite BFD en la interfaz especificada que utiliza OSPFv2.

Configuración de ejemplo:

```
    > vtysh

    ns# configure terminal

    ns(config)# interface vlan5

    ns(config-if)# ip ospf bfd

    ns(config-if)# exit
<!--NeedCopy-->
```

Configuración de BFD para OSPFv3 (IPv6) en interfaces

Puede habilitar BFD en todas o en una interfaz específica que utilice el protocolo OSPFv3.

Para configurar BFD para OSPFv3 en todas las interfaces mediante la línea de `VTYSH` comandos:

En el símbolo del sistema, escriba los siguientes comandos, en el orden que se muestra:

Comando	Especifica
`vtysh`	Muestra el símbolo del sistema `VTYSH`.
`configure terminal`	Acceda al modo de configuración global.
`router ipv6 ospf <process tag>`	Introduzca el modo de configuración OSPFv3.
`bfd all-interfaces`	Habilite BFD en todas las interfaces que usan OSPFv3.

Configuración de ejemplo:

```
    > vtysh

```



```
3     ns# configure terminal
4
5     ns(config)#router ipv6 ospf 10
6
7     ns(config-router)#bfd all-interfaces
8
9     ns(config-router)#redistribute kernel
10
11    ns(config-router)#exit
12 <!--NeedCopy-->
```

Para configurar BFD para OSPFv3 en una interfaz específica mediante la línea de VTYSH comandos:

En el símbolo del sistema, escriba los siguientes comandos, en el orden que se muestra:

Comando	Especifica
`vtysh`	Muestra el símbolo del sistema VTYSH.
`configure terminal`	Acceda al modo de configuración global.
`interface` <vlan ID>	Entre en el modo de configuración de la interfaz.
`ipv6 ospf bfd`	Habilite BFD en la interfaz especificada que utiliza OSPFv3.

Configuración de ejemplo:

```
1     > vtysh
2
3     ns# configure terminal
4
5     ns(config)# interface vlan15
6
7     ns(config-if)# ipv6 ospf bfd
8
9     ns(config-if)# exit
10 <!--NeedCopy-->
```


Configuración de Rutas Estáticas

August 20, 2021

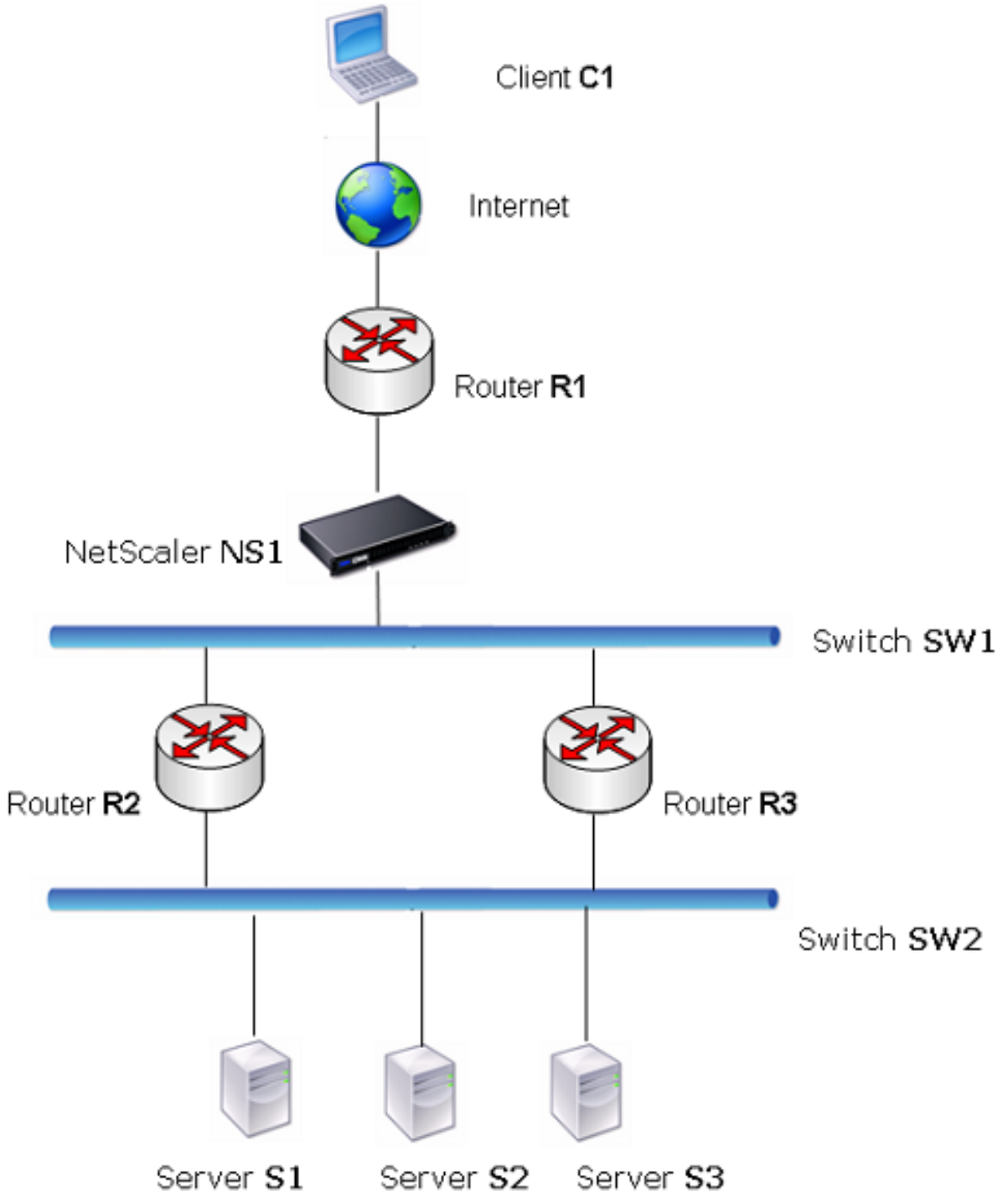
Las rutas estáticas se crean manualmente para mejorar el rendimiento de la red. Puede supervisar rutas estáticas para evitar interrupciones en el servicio. Además, puede asignar pesos a rutas ECMP y crear rutas nulas para evitar bucles de redirección.

Rutas estáticas supervisadas. Si una ruta creada manualmente (estática) cae, una ruta de copia de seguridad no se activa automáticamente. Debe eliminar manualmente la ruta estática primaria inactiva. Sin embargo, si configura la ruta estática como una ruta supervisada, el dispositivo Citrix ADC puede activar automáticamente una ruta de copia de seguridad.

La supervisión de rutas estáticas también puede basarse en la accesibilidad de la subred. Por lo general, una subred está conectada a una única interfaz, pero se puede acceder lógicamente a través de otras interfaces. Solo se puede acceder a las subredes enlazadas a una VLAN si la VLAN está abierta. Las VLAN son interfaces lógicas a través de las cuales el Citrix ADC transmite y recibe paquetes. Una ruta estática se marca como DOWN si el salto siguiente reside en una subred que es inalcanzable.

Nota: En una configuración de alta disponibilidad (HA), el valor predeterminado para las rutas de estado supervisadas (MSR) en el nodo secundario es UP. El valor se establece para evitar una brecha de transición de estado tras la conmutación por error, lo que podría provocar la caída de paquetes en esas rutas.

Considere la siguiente topología simple, en la que un dispositivo Citrix ADC está equilibrando la carga del tráfico hacia un sitio en varios servidores.



El router R1 mueve el tráfico entre el cliente y el dispositivo Citrix ADC. El dispositivo puede llegar a los servidores S1 y S2 a través de enrutadores R2 o R3. Tiene dos rutas estáticas a través de las cuales

llegar a la subred de los servidores, una con R2 como Gateway y otra con R3 como Gateway. Ambas rutas tienen activada la monitorización. La distancia administrativa de la ruta estática con la Gateway R2 es menor que la de la ruta estática con la Gateway R3. Por lo tanto, R2 es preferible a R3 para reenviar tráfico a los servidores. Además, la ruta predeterminada en Citrix ADC apunta a R1 para que todo el tráfico de Internet salga correctamente.

Si R2 falla mientras la supervisión está habilitada en la ruta estática, que usa R2 como Gateway, Citrix ADC lo marca como DOWN. El Citrix ADC ahora utiliza la ruta estática con R3 como Gateway y reenvía el tráfico a los servidores a través de R3.

Citrix ADC admite la supervisión de rutas estáticas IPv4 e IPv6. Puede configurar Citrix ADC para supervisar una ruta estática IPv4 creando un nuevo monitor ARP o PING o mediante monitores ARP o PING existentes. Puede configurar Citrix ADC para supervisar una ruta estática IPv6 creando un nuevo monitor de detección de vecinos para IPv6 (ND6) o PING o mediante los monitores ND6 o PING existentes.

Rutas estáticas ponderadas. Cuando el dispositivo Citrix ADC toma decisiones de redirección que implican rutas con la misma distancia y coste, es decir, rutas de ruta multirruta de igual coste (ECMP), equilibra la carga entre ellas mediante un mecanismo de hash basado en las direcciones IP de origen y destino. Sin embargo, para una ruta ECMP, puede configurar un valor de peso. A continuación, el Citrix ADC utiliza tanto el peso como el valor hash para equilibrar la carga.

Rutas nulas. Si la ruta elegida en una decisión de redirección está inactiva, el dispositivo Citrix ADC elige una ruta de copia de seguridad. Si no se puede acceder a todas las rutas de copia de seguridad, es posible que el dispositivo vuelva a enrutar el paquete al remitente, lo que podría dar lugar a un bucle de redirección que provoque congestión de la red. Para evitar esta situación, puede crear una ruta nula, que agrega una interfaz nula como Gateway. La ruta nula nunca es la ruta preferida, ya que tiene una distancia administrativa más alta que las otras rutas estáticas. Pero se selecciona si las otras rutas estáticas se vuelven inaccesibles. En ese caso, el dispositivo deja caer el paquete e impide que se produzca un bucle de redirección.

Configuración de Rutas Estáticas IPv4

Puede agregar una ruta estática simple o una ruta nula estableciendo algunos parámetros, o bien puede establecer parámetros adicionales para configurar una ruta estática supervisada o supervisada y ponderada. Puede cambiar los parámetros de una ruta estática. Por ejemplo, es posible que quiera asignar un peso a una ruta no ponderada o que quiera inhabilitar la supervisión en una ruta supervisada.

Procedimientos CLI

Para crear una ruta estática mediante la CLI:

En el símbolo del sistema, escriba:

- add route <network><netmask><gateway[-cost] <positive_integer>[-advertise (DESHABILITADO | HABILITADO)]
- mostrar ruta [\ []<network><netmask>] [] <routeType>[-detalle]

Ejemplo:

```
1 > add route 10.102.29.0 255.255.255.0 10.102.29.2 -cost 2 -advertise
     ENABLED
2  Done
3 <!--NeedCopy-->
```

Para crear una ruta estática supervisada mediante la CLI:

En el símbolo del sistema, escriba los siguientes comandos para crear una ruta estática supervisada y verificar la configuración:

- add route <network><netmask>[-distance] <positive_integer>[-weight][-msr (ENABLED | DISABLED) [-monitor <string>]<positive_integer>]
- show route [\ []] [] [-detalle]

Ejemplo:

```
1 > add route 10.102.29.0 255.255.255.0 10.102.29.3 -distance 5 -weight 6
       -msr ENBLED -monitor PING
2  Done
3 <!--NeedCopy-->
```

Para crear una ruta nula mediante la CLI:

En el símbolo del sistema, escriba:

- add route <network> <netmask> null
- show route <network> <netmask>

Ejemplo:

```
1 > add route 10.102.29.0 255.255.255.0 null
2  Done
3 <!--NeedCopy-->
```

Para eliminar una ruta estática mediante la CLI:

En el símbolo del sistema, escriba:

rm route <network> <netmask> <gateway>

Ejemplo:

```
> rm route 10.102.29.0 255.255.255.0 10.102.29.3
 Done
<!--NeedCopy-->
```

Procedimientos de GUI

Para configurar una ruta estática mediante la GUI:

Vaya a Sistema > Red > Rutas y, en la ficha Básico, agregue una nueva ruta estática o modifique una ruta estática existente.

Para eliminar una ruta mediante la interfaz gráfica de usuario:

Vaya a Sistema > Red > Rutas y, en la ficha Básico, elimine la ruta estática.

Configuración de Rutas Estáticas IPv6

Puede configurar un máximo de seis rutas estáticas IPv6 predeterminadas. Las rutas IPv6 se seleccionan sobre la base de si la dirección MAC del dispositivo de destino es accesible. Esto se puede determinar mediante la función IPv6 Neighbor Discovery. Las rutas están equilibradas de carga y solo se utilizan mecanismos hash basados en origen/destino. Por lo tanto, no se admiten mecanismos de selección de rutas como el round robin. La dirección de salto siguiente en la ruta predeterminada no necesita pertenecer a la subred NSIP.

Procedimientos CLI

Para crear una ruta IPv6 mediante la CLI:

En el símbolo del sistema, escriba los siguientes comandos para crear una ruta IPv6 y compruebe la configuración:

- agregar ruta6 <network>[-vlan]<positive_integer>
- mostrar ruta6 [\ []<network>

Ejemplo:


```
1 > add route6 ::/0 FE80::67 -vlan 5
2  Done
3 <!--NeedCopy-->
```

Para crear una ruta estática IPv6 supervisada mediante la CLI:

En el símbolo del sistema, escriba los siguientes comandos para crear una ruta estática IPv6 supervisada y compruebe la configuración:

- add route6 <network>[-msr (HABILITADO | DESHABILITADO) [-monitor]<string>
- mostrar ruta6 [\ []

Ejemplo:

```
1 > add route6 ::/0 2004::1 -msr ENABLED -monitor PING
2  Done
3 <!--NeedCopy-->
```

Para eliminar una ruta IPv6 mediante la CLI:

En el símbolo del sistema, escriba:

rm route6 <network> <gateway>

Ejemplo:

```
1 > rm route6 ::/0 FE80::67
2  Done
3 <!--NeedCopy-->
```

Procedimientos de GUI

Para configurar una ruta IPv6 mediante la GUI:

Vaya a Sistema > Red > Rutas y, en la ficha IPV6, agregue una nueva ruta IPv6 o modifique una ruta IPv6 existente.

Para eliminar una ruta IPv6 mediante la GUI:

Vaya a Sistema > Red > Rutas y, en la ficha IPV6, elimine la ruta IPv6.

Inyección de mantenimiento de ruta basada en la configuración del servidor virtual

August 20, 2021

La siguiente opción y parámetro se introducen para controlar la funcionalidad de inyección de mantenimiento de ruta (RHI) del dispositivo Citrix ADC para anunciar la ruta de una dirección VIP.

- **VSVR_CNTRLD**. Es una opción para el parámetro (Vserver RHI Level) de una dirección VIP. Cuando esta opción se establece en el parámetro Vserver RHI Level, el comportamiento RHI para la publicidad de la ruta de la dirección VIP depende de la configuración del parámetro RHI STATE en todos los servidores virtuales asociados de la dirección VIP junto con sus estados.
- **Estado RHI**. Es un parámetro de servidor virtual. Puede establecer el parámetro RHI STATE en PASSIVE o ACTIVE. De forma predeterminada, el parámetro RHI STATE se establece en PASIVO.

Para una dirección VIP, cuando el parámetro RHI (Vserver RHI Level) se establece en VSVR_CNTRLD, los siguientes son comportamientos RHI diferentes para la dirección VIP sobre la base de la configuración RHI STATE en los servidores virtuales asociados a la dirección VIP:

- Si establece RHI STATE como PASIVO en todos los servidores virtuales, Citrix ADC siempre anuncia la ruta de la dirección VIP.
- Si establece RHI STATE como ACTIVE en todos los servidores virtuales, Citrix ADC anuncia la ruta de la dirección VIP si al menos uno de los servidores virtuales asociados está en estado ACTIVO.
- Si establece RHI STATE en ACTIVE en algunos y PASIVO en otros, Citrix ADC anuncia la ruta de la dirección VIP si al menos uno de los servidores virtuales asociados, cuyo RHI STATE establecido en ACTIVE, está en estado ACTIVO.

La siguiente tabla muestra el comportamiento RHI de muestra para una dirección VIP sobre la base de la configuración RHI STATE en los servidores virtuales asociados a la dirección VIP. El dispositivo Citrix ADC tiene dos servidores virtuales V1 y V2 asociados a la dirección VIP:

Servidores virtuales asociados para un VIP	Estado 1	Estado 2	Estado 3	Estado 4
Estado RHI establecido en PASIVO en todos los servidores virtuales				

Servidores virtuales asociados para un VIP	Estado 1	Estado 2	Estado 3	Estado 4
V1	ACTIVO	ACTIVO	INACTIVO	INACTIVO
V2	ACTIVO	INACTIVO	ACTIVO	INACTIVO
¿Anunciar la ruta para esta dirección VIP?	Sí	Sí	Sí	Sí
Estado RHI establecido en ACTIVE en todos los servidores virtuales				
V1	ACTIVO	ACTIVO	INACTIVO	INACTIVO
V2	ACTIVO	INACTIVO	ACTIVO	INACTIVO
¿Anunciar la ruta para esta dirección VIP?	Sí	Sí	Sí	No
Estado RHI establecido en ACTIVE en un servidor virtual y PASIVO en el otro				
V1 (Estado RHI = ACTIVO)	ACTIVO	ACTIVO	INACTIVO	INACTIVO
V2 (Estado RHI = PASIVO)	ACTIVO	INACTIVO	ACTIVO	INACTIVO
¿Anunciar la ruta para esta dirección VIP?	Sí	Sí	No	No

Para configurar RHI para una dirección VIP, que se basará en la configuración del parámetro RHI (Estado RHI) de los servidores virtuales asociados, lleve a cabo los siguientes pasos:

- Establezca el parámetro RHI (Vserver RHI Level) en VSVR_CNTRLD para la dirección VIP.

- Establezca el parámetro Estado RHI para cada servidor virtual asociado a la dirección VIP.

Para establecer el nivel RHI de vServer para una dirección VIP mediante la CLI:

En el símbolo del sistema, escriba:

- **set ns ip** <IPAddress>[-**vServerRhiLevel**]<vserverRHILevel>

Para establecer el parámetro RHI State de un servidor virtual mediante la CLI:

En el símbolo del sistema, escriba:

- **set lb vserver** <name>[-**RHISTate** (**PASIVO** | **ACTIVO**)]

Para establecer el nivel RHI de vServer para una dirección VIP mediante GUI

1. Vaya a **Sistema** > **Red** > **IP**.
2. Seleccione una dirección VIP y, a continuación, haga clic en **Modificar**.
3. Establezca el parámetro **Vserver RHI Level** en **VSVR_CNTRLD** y, a continuación, haga clic en **Aceptar**.

Para establecer el parámetro RHI State de un servidor virtual mediante GUI

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**.
2. Seleccione un servidor virtual de equilibrio de carga y, a continuación, haga clic en **Modificar**.
3. Establezca el parámetro **Estado RHI** y, a continuación, haga clic en **Aceptar**.

Configuración de Rutas Basadas en Directivas

August 20, 2021

La redirección basada en directivas basa las decisiones de redirección en los criterios que especifique. Una ruta basada en directivas (PBR) especifica criterios para seleccionar paquetes y, normalmente, un salto siguiente al que enviar los paquetes seleccionados. Por ejemplo, puede configurar el dispositivo Citrix ADC para que enrute los paquetes salientes desde una dirección IP o rango específicos a un enrutador de salto siguiente determinado. Cada paquete se compara con cada PBR configurado, en el orden determinado por las prioridades especificadas, hasta que se encuentra una coincidencia. Si no se encuentra ninguna coincidencia, o si el PBR coincidente especifica una acción DENY, Citrix ADC aplica la tabla de redirección para la redirección basada en destino normal.

Un PBR basa las decisiones de redirección para los paquetes de datos en parámetros como la dirección IP de origen, el puerto de origen, la dirección IP de destino, el puerto de destino, el protocolo y la dirección MAC de origen. Un PBR define las condiciones que debe cumplir un paquete para que Citrix ADC enrute el paquete. Estas acciones se conocen como “modos de procesamiento.” Los modos de procesamiento son:

- **ALLOW.** El dispositivo envía el paquete al enrutador de siguiente salto designado.

- **DENY.** El Citrix ADC aplica la tabla de redirección para la redirección basada en destino normal.

Puede crear PBRs para el tráfico IPv4 e IPv6 saliente.

Muchos usuarios comienzan por crear PBRs y luego modificarlos. Para activar un nuevo PBR, debe aplicarlo. Para desactivar un PBR, puede eliminarlo o inhabilitarlo. Puede cambiar el número de prioridad de un PBR para darle una prioridad mayor o menor.

Rutas basadas en directivas (PBR) para tráfico IPv4

August 20, 2021

La configuración de PBRs implica las siguientes tareas:

- Cree un PBR.
- Aplicar PBRs.
- (Opcional) Inhabilite o habilite un PBR.
- (Opcional) Renumérese la prioridad del PBR.

Creación o Modificación de un PBR

No se pueden crear dos PBRs con los mismos parámetros. Si intenta crear un duplicado, aparecerá un mensaje de error.

Puede configurar la prioridad de un PBR. La prioridad (un valor entero) define el orden en que el dispositivo Citrix ADC evalúa los PBRs. Cuando crea un PBR sin especificar una prioridad, Citrix ADC asigna automáticamente una prioridad que es un múltiplo de 10.

Si un paquete coincide con la condición definida por el PBR, Citrix ADC realiza una acción. Si el paquete no coincide con la condición definida por el PBR, Citrix ADC compara el paquete con el PBR con la siguiente prioridad más alta.

En lugar de enviar los paquetes seleccionados a un enrutador de salto siguiente, puede configurar PBR para enviarlos a un servidor virtual de equilibrio de carga de enlace al que haya enlazado varios saltos siguientes. Esta configuración puede proporcionar una copia de seguridad si falla un vínculo de salto siguiente.

Considere el siguiente ejemplo. Dos PBRs, p1 y p2, se configuran en el Citrix ADC y se asignan automáticamente las prioridades 20 y 30. Debe agregar un tercer PBR, p3, para ser evaluado inmediatamente después del primer PBR, p1. El nuevo PBR, p3, debe tener una prioridad entre 20 y 30. En este caso, puede especificar la prioridad como 25.

Procedimientos CLI

Para crear un PBR mediante la CLI:

En el símbolo del sistema, escriba:

- add ns pbr <name><action>[-SrCip [] <operator><srcIPVal>] [-SrcPort [] <operator><srcPortVal>] [-Destip [] <operator><destIPVal>] [-DestPort [] <operator><destPortVal>] [-NextHop] <nextHopVal>[- srcMac] <mac_addr>[-protocol\ |-ProtocolNumber] <protocol><positive_integer>[-vlan] <positive_integer>[-interface] <interface_name>[-priority] <positive_integer>[-msr (HABILITADO | DESHABILITADO) [-monitor]<string>] [-state (HABILITADO | DESHABILITADO)]
- mostrar ns pbr

Ejemplo:

```
1 > add ns pbr pbr1  allow -srcip 10.102.37.252 -destip 10.10.10.2 -
     nexthop 10.102.29.77
2  Done
3 <!--NeedCopy-->
```

Para modificar la prioridad de un PBR mediante la CLI:

En el símbolo del sistema, escriba los siguientes comandos para modificar la prioridad y verificar la configuración:

- set ns pbr <name>[-action (PERMITIR | DENEGAR)] [-SrCip [] <srcIPVal>] [-SrcPort [] <srcPortVal>] [-Destip [] <destIPVal>[-DestPort [] <destPortVal>] [-NextHop] [- srcMac] [-protocol\ | -ProtocolNumber] [-vlan] [-interface] [-priority] [-msr (HABILITADO | DESHABILITADO) [-monitor]<protocol><positive_integer>] [-state (HABILITADO | DESHABILITADO)]
- mostrar ns pbr []<name>

Ejemplo:

```
1 > set ns pbr pbr1 -priority 23
2  Done
3 <!--NeedCopy-->
```

Para eliminar uno o todos los PBRs mediante la CLI:

En el símbolo del sistema, escriba uno de los siguientes comandos:

- rm ns pbr <name>
- borrar ns pbrs

Ejemplo:

```
> rm ns pbr pbr1
 Done

> clear ns PBRs
 Done
<!--NeedCopy-->
```

Procedimientos de GUI

Para crear un PBR mediante la GUI:

Vaya a Sistema > Red > PBRs, en la ficha PBRs, agregue un nuevo PBR o modifique un PBR existente.

Para eliminar uno o todos los PBRs mediante la GUI:

Vaya a Sistema > Red > PBRs, en la ficha PBRs, elimine el PBR.

Aplicación de un PBR

Debe aplicar un PBR para activarlo. El siguiente procedimiento vuelve a aplicar todos los PBRs que no haya inhabilitado. Los PBRs constituyen un árbol de memoria (tabla de búsqueda). Por ejemplo, si crea 10 PBRs (p1: P10) y, a continuación, crea otro PBR (p11) y lo aplica, todos los PBRs (p1: P11) se aplican de nuevo y se crea una nueva tabla de búsqueda. Si una sesión tiene una PBR DENY relacionada con ella, la sesión se destruye.

Debe aplicar este procedimiento después de cada modificación que realice a cualquier PBR. Por ejemplo, debe seguir este procedimiento después de inhabilitar un PBR.

Nota: Los PBRs creados en el dispositivo Citrix ADC no funcionan hasta que se aplican.

Para aplicar un PBR mediante la CLI:

En el símbolo del sistema, escriba:

aplicar ns PBRs

Para aplicar un PBR mediante la GUI:

1. Vaya a Sistema > Red > PBRs.
2. En la ficha PBRs, seleccione el PBR, en la lista Acción, seleccione Aplicar.

Activación o desactivación de PBRs

De forma predeterminada, los PBRs están habilitados. Esto significa que cuando se aplican los PBRs, el dispositivo Citrix ADC compara automáticamente los paquetes entrantes con los PBRs configurados. Si no se requiere un PBR en la tabla de búsqueda, pero debe conservarse en la configuración, debe inhabilitarse antes de aplicar los PBRs. Después de aplicar los PBRs, Citrix ADC no compara los paquetes entrantes con los PBRs inhabilitados.

Para habilitar o inhabilitar un PBR mediante la CLI:

En el símbolo del sistema, escriba uno de los siguientes comandos:

- habilitar ns pbr <name>
- disable ns pbr <name>

Ejemplo:

```
> enable ns PBR pbr1
 Done
> show ns PBR pbr1
1)      Name: pbr1
        Action: ALLOW                           Hits: 0
        srcIP = 10.102.37.252
        destIP = 10.10.10.2
        srcMac:                                 Protocol:
        Vlan:                                   Interface:
        Active Status: ENABLED                  Applied Status: APPLIED
        Priority: 10
        NextHop: 10.102.29.77

 Done

> disable ns PBR pbr1
Warning: PBR modified, use 'apply pbrs' to commit this operation

> apply pbrs
 Done

> show ns PBR pbr1
1)      Name: pbr1
        Action: ALLOW                           Hits: 0
        srcIP = 10.102.37.252
        destIP = 10.10.10.2
        srcMac:                                 Protocol:
        Vlan:                                   Interface:
```



```
29          Active Status: DISABLED                Applied Status:
               NOTAPPLIED
30          Priority: 10
31          NextHop: 10.102.29.77
32  Done
33  <!--NeedCopy-->
```

Para habilitar o inhabilitar un PBR mediante la GUI:

1. Vaya a Sistema > Red > PBRs.
2. En la ficha PBRs, seleccione el PBR, en la lista Acción, seleccione Habilitar o Inhabilitar.

Renumeración de los PBRs

Puede volver a numerar automáticamente los PBRs para establecer sus prioridades en múltiplos de 10.

Para volver a numerar los PBRs mediante la CLI:

En el símbolo del sistema, escriba:

- renumerar ns pbrs

Para volver a numerar los PBRs mediante la GUI:

Vaya a Sistema > Red > PBRs, en la ficha PBRs, en la lista Acción, seleccione Renumerar Prioridad (s).

Caso de uso: PBR con múltiples saltos

Considere un caso en el que dos PBRs, PBR1 y PBR2, estén configurados en Citrix ADC Appliance NS1. PBR1 enruta todos los paquetes salientes, con la dirección IP de origen como 10.102.29.30, al router R1 de salto siguiente. PBR2 enruta todos los paquetes salientes, con la dirección IP de origen como 10.102.29.90, al enrutador de salto siguiente R2. R3 es otro router de salto siguiente conectado a NS1.

Si el router R1 falla, se descartan todos los paquetes salientes que coinciden con PBR1. Para evitar esta situación, puede especificar un servidor virtual de equilibrio de carga de vínculos (LLB) en el campo de salto siguiente mientras crea o modifica un PBR. Varios saltos siguientes están enlazados al servidor virtual LLB como servicios (por ejemplo, R1, R2 y R3). Ahora, si R1 falla, todos los paquetes que coinciden con PBR1 se enrutan a R2 o R3 según lo determinado por el método LB configurado en el servidor virtual LLB.

El dispositivo Citrix ADC genera un error si intenta crear un PBR con un servidor virtual LLB como salto siguiente en los siguientes casos:

- Agregar otro PBR con el mismo servidor virtual LLB.
- Especificar un servidor virtual LLB inexistente.

- Especificar un servidor virtual LLB para el que los servicios enlazados no son saltos siguientes.
- Especificar un servidor virtual LLB para el que el método LB no está establecido en uno de los siguientes:
  - ROUNDROBIN
  - DESTINATIONIFASH
  - SOURCEIPHASH
  - SRCIPDESTIPHASH
  - LEASTPACKETS
  - LEASTBANDWIDTH
  - LTRM
  - CALIDHASH
  - CUSTOM LOAD
- Especificar un servidor virtual LLB para el que el tipo de persistencia LB no está establecido en uno de los siguientes:
  - DESTIP
  - SOURCEIP
  - SRCDSTIP

En la siguiente tabla se enumeran los nombres y valores de las entidades configuradas en el dispositivo Citrix ADC:

Tipo de entidad	Nombre	Dirección IP
Servidor virtual de equilibrio de carga de enlace	LLB1	NA
Servicios (próximos saltos)	Router1	1.1.1.254
	Router2	2.2.2.254
	Router3	3.3.3.254
PBRs	PBR1	NA
	PBR2	NA

Cuadro 1 Valores de ejemplo para crear entidades

Para implementar la configuración descrita anteriormente, debe:

1. Cree servicios Router1, Router2 y Router3 que representen los routers de salto siguiente R1, R2 y R3.
2. Cree el servidor virtual LLB1 de equilibrio de carga de enlace y vincule los servicios Router1, Router2 y Router3 a él.
3. Cree PBRs PBR1 y PBR2, con campos de salto siguiente establecidos como LLB1 y 2.2.2.254 (di-

rección IP del enrutador R2), respectivamente.

Para crear un servicio mediante la CLI:

En el símbolo del sistema, escriba:

- add service <name> <IP> <serviceType> <port>
- show service <name>

Ejemplo:

```
> add service Router1 1.1.1.254 ANY *
 Done
> add service Router2 2.2.2.254 ANY *
 Done
> add service Router3 3.3.3.254 ANY *
 Done
<!--NeedCopy-->
```

Para crear un servicio mediante la GUI:

Vaya a Administración del tráfico > Equilibrio de carga > Serviciosy cree un servicio.

Para crear un servidor virtual de equilibrio de carga de vínculos y enlazar un servicio mediante la CLI:

En el símbolo del sistema, escriba:

- add lb vserver <name> <serviceType>
- bind lb vserver < name> <serviceName>
- show lb vserver <name>

Ejemplo:

```
> add lb vserver LLB1 ANY
 Done
> bind lb vserver LLB1 Router1 Router2 Router3
 Done
<!--NeedCopy-->
```

Para crear un servidor virtual de equilibrio de carga de vínculos y enlazar un servicio mediante la GUI:

1. Vaya a Administración del tráfico > Equilibrio de carga > Servidores virtuales y cree un servidor virtual para el equilibrio de carga de vínculos. Especifique **CUALQUIERA** en el campo **Protocolo**. Nota: Asegúrese de que
   Directamente Directamente Directamente Directamente está desactivada.

2. En la ficha **Servicios**, en la columna **Activo**, active la casilla de verificación del servicio que quiere enlazar al servidor virtual.

Para crear un PBR mediante la CLI:

En el símbolo del sistema, escriba:

- add ns pbr <name> <action> [-SrCip [] <srcIPVal>] [-NextHop]
- mostrar ns pbr

Ejemplo:

```
> add pbr PBR1 ALLOW -srcIP 10.102.29.30 -nextHop LLB1
 Done
> add pbr PBR2 ALLOW -srcIP 10.102.29.90 -nextHop 2.2.2.254
 Done
<!--NeedCopy-->
```

Para crear un PBR mediante la GUI:

Vaya a Sistema > Red > PBRs, en la ficha PBRs, agregue un nuevo PBR.

Rutas basadas en directivas (PBR6) para tráfico IPv6

August 20, 2021

La configuración de PBR6s implica las siguientes tareas:

- Cree un PBR6.
- Aplicar PBR6s.
- (Opcional) Inhabilite o habilite un PBR6.
- (Opcional) Renumérese la prioridad del PBR6.

Creación o modificación de un PBR6

No se pueden crear dos PBR6s con los mismos parámetros. Si intenta crear un duplicado, aparecerá un mensaje de error.

Puede configurar la prioridad de un PBR6. La prioridad (un valor entero) define el orden en que el dispositivo Citrix ADC evalúa los PBR6s. Cuando crea un PBR6 sin especificar una prioridad, Citrix ADC asigna automáticamente una prioridad que es un múltiplo de 10.

Si un paquete coincide con la condición definida por el PBR6, Citrix ADC realiza una acción. Si el paquete no coincide con la condición definida por el PBR6, Citrix ADC compara el paquete con el PBR6 con la siguiente prioridad más alta.

Procedimientos CLI

Para crear un PBR6 mediante la CLI:

En el símbolo del sistema, escriba:

- **add ns pbr6** <name><action>[-srcIPv6 [] <operator><srcIPv6Val>] [-SrcPort [] <operator><srcPortVal>] [-destipV6 [] <operator><destIPv6Val>] [-DestPort [] <operator><destPortVal>] [-SRCMac <mac_addr>] [-protocol\|-ProtocolNumber] <protocol><positive_integer>[-vlan] <positive_integer>[-interface\ -priority] <interface_name>[-state] <positive_integer>[(HABILITADO | DESHABILITADO)] [-msr (HABILITADO | DESHABILITADO) [- monitor]<string>] [-NextHop] <nextHopVal>[-NextHopvlan]<positive_integer>
- mostrar ns pbr

Para modificar o quitar un PBR6 mediante la CLI:

Para modificar un PBR6, escriba el <name> comando **set pbr6** y los parámetros que se van a cambiar, con sus nuevos valores.

Para eliminar uno o todos los PBR6s mediante la CLI:

En el símbolo del sistema, escriba uno de los siguientes comandos:

- **rm ns pbr6** <name>
- **clear ns pbr6**

Procedimientos de GUI

Para crear o modificar un PBR6 mediante la GUI:

Vaya a Sistema > Red > PBRs y, en la ficha PBR6s, agregue un PBR6 nuevo o modifique un PBR6 existente.

Para eliminar uno o todos los PBR6s mediante la GUI:

Vaya a Sistema > Red > PBRs y, en la ficha PBR6s, elimine el PBR6.

Aplicando PBR6s

Debe aplicar un PBR6 para activarlo. El siguiente procedimiento vuelve a aplicar todos los PBR6s que no haya inhabilitado. Los PBR6s constituyen un árbol de memoria (tabla de búsqueda). Por ejemplo, si crea 10 PBR6s (p6_1: P6_10) y, a continuación, crea otro PBR6 (p6_11) y lo aplica, todos los PBR6s

(p6_1: P6_11) se aplican de nuevo y se crea una nueva tabla de búsqueda. Si una sesión tiene un DENY PBR6 relacionado con ella, la sesión se destruye.

Debe aplicar este procedimiento después de cada modificación que realice en cualquier PBR6. Por ejemplo, debe seguir este procedimiento después de inhabilitar un PBR6.

Nota: Los PBR6s creados en el dispositivo Citrix ADC no funcionan hasta que se aplican.

Para aplicar PBR6s mediante la CLI:

En el símbolo del sistema, escriba:

- **apply ns PBR6**

Para aplicar PBR6s mediante la GUI:

1. Vaya a Sistema > Red > PBRs.
2. En la ficha PBR6s, seleccione el PBR6, en la lista Acción, seleccione Aplicar.

Activación o desactivación de un PBR6

De forma predeterminada, los PBR6s están habilitados. Esto significa que cuando se aplica PBR6s, el dispositivo Citrix ADC compara automáticamente los paquetes IPv6 salientes con los PBR6s configurados. Si no se requiere un PBR6 en la tabla de búsqueda, pero debe conservarse en la configuración, debe inhabilitarse antes de aplicar los PBR6s. Después de aplicar los PBR6s, Citrix ADC no compara los paquetes entrantes con los PBR6s inhabilitados.

Para habilitar o inhabilitar un PBR6 mediante la CLI:

En el símbolo del sistema, escriba uno de los siguientes comandos:

- **habilitar ns pbr** <name>
- **disable ns pbr** <name>

Para habilitar o inhabilitar un PBR6 mediante la GUI:

1. Vaya a Sistema > Red > PBRs.
2. En la ficha PBR6s, seleccione el PBR6, en la lista Acción, seleccione Habilitar o Inhabilitar.

Cambio de numeración de PBR6s

Puede volver a numerar automáticamente los PBR6s para establecer sus prioridades en múltiplos de 10.

Para volver a numerar PBR6s mediante la CLI:

En el símbolo del sistema, escriba:

- **renumerar ns pbr6**

Para volver a numerar PBR6s mediante la GUI:

Vaya a Sistema > Red > PBRs, en la ficha PBR6s, en la lista Acción, seleccione Renumerar Prioridad (s).

Máscara de comodín de dirección MAC para PBRs

August 20, 2021

Se ha introducido un parámetro de máscara comodín para los PBRs y PBR6s extendidos y se utiliza con el parámetro de dirección MAC de origen para definir un rango de direcciones MAC que deben coincidir con la dirección MAC de origen de los paquetes salientes.

Las máscaras comodín especifican qué dígitos hexadecimales de la dirección MAC se utilizan y qué dígitos hexadecimales se ignoran. El parámetro máscara comodín especifica una serie de unos y ceros y tiene una longitud de 12 dígitos. Cada dígito es una máscara para el dígito hexadecimal correspondiente de la dirección MAC. Un dígito cero en la máscara comodín indica que se debe considerar el dígito hexadecimal correspondiente de la dirección MAC y un dígito indica que el dígito hexadecimal correspondiente a ser ignorado.

La máscara comodín debe cumplir las siguientes condiciones:

- Tiene solo una serie de ceros
- Tiene solo una serie de unos
- Comience con una serie de ceros

Los siguientes son algunos de los ejemplos de máscaras comodín válidas:

- 000000111111
- 000000011111
- 000011111111

Los siguientes son algunos de los ejemplos de máscaras comodín no válidas:

- 000000111100
- 111110000000
- 010101010101

Para una regla PBR, una máscara comodín de 000000111111 para la dirección MAC 96:fa: 95:1 d: 67:4 a define el rango de direcciones MAC 96:FA: 95:00:00:00: 96:FA:95:FF:FF. Este intervalo de direcciones MAC coincide con la dirección MAC de origen de los paquetes salientes.

Para especificar un rango de direcciones MAC de origen en una regla PBR mediante la CLI:

En el símbolo del sistema, escriba:

- **add ns pbr** <name> <action> -**srcMac** <mac_addr> -**srcMacMask** <string>

- **show ns pbr** <pbrname>

Ejemplo:

```
> add ns pbr PBR-1 ALLOW -srcip 192.0.2.34 -srcMac 96:fa:95:1d:67:4a
   - srcMacMask 000000111111 -nexthop 198.51.100.1

 Done
```

Para especificar un rango de direcciones MAC de origen en una regla PBR6 mediante la CLI:

En el símbolo del sistema, escriba:

- **add ns pbr6** <name> <action> -**srcMac** <mac_addr> -**srcMacMask** <string>
- **show pbr6** <pbr6name>

Ejemplo:

```
> add ns pbr6 PBR6-1 ALLOW  - srcipv6 2001:db8:0::7 -srcMac 96:fa:95:1d
   :67:4a   - srcMacMask 000000001111 -nexthop 2001:db8:0::1
 Done
```

Uso de rutas basadas en directivas NULL para eliminar paquetes salientes

August 20, 2021

Algunas situaciones pueden exigir que el dispositivo Citrix ADC descarta paquetes salientes específicos en lugar de enrutarlos, por ejemplo, en casos de prueba y durante la migración de la implementación.

Las rutas basadas en directivas NULL se pueden utilizar para eliminar paquetes salientes específicos. Un PBR NULL es un tipo de PBR que tiene el parámetro nexthop establecido en NULL. El dispositivo Citrix ADC elimina los paquetes salientes que coinciden con un PBR NULL.

Configuración de PBRs NULL para paquetes IPv4

Para crear un PBR NULL mediante la CLI:

En el símbolo del sistema, escriba:

- **add ns pbr** <name>ALLOW [**-td**] <positive_integer>[-**srcIP** [] <operator><srcIPVal>] [-**srcPort** [] <operator><srcPortVal>] [-**DesTip** [<operator>] <destIPVal>] [-**DestPort** [] <operator><destPortVal>] (-**NextHop NULL**) [**srcMac** \ [-**srcMacMask**]<mac_addr><string>] [-**protocolo** <protocol>| -**ProtocolNumber**] <positive_integer>[-**vlan** \ | -**vxlan**] <positive_integer><positive_i **interfaz**] <interface_name>[-**prioridad**] \ <positive_integer>[-**msr** (**HABILITADO** | **DESHABILITADO**) [-**monitor**]<string>] [-**estado** (**HABILITADO** | **DISCAPACITADO**) [-**Grupo Propietario**]<string>
- **apply ns pbrs**
- **show ns pbr**<id>

Para configurar un PBR NULL mediante la GUI:

Desplácese hasta **Sistema** > **Red** > **PBRs**, en la ficha **PBRs**, agregue un **nuevo PBR NULL** o modifique un PBR NULL existente.

Configuración de ejemplo

En la siguiente configuración de ejemplo, NULL PBR6 PBR6-NULL-EJEMPLO-1 está configurado para eliminar cualquier paquete IPv6 saliente de la interfaz 1/5.

```
> add ns pbr PBR6-NULL-EXAMPLE-1 ALLOW  - nextHop NULL -interface 1/5
 Done

> apply ns pbr6
 Done
```

Distribución del tráfico en varias rutas basadas en información de cinco tuplas

January 12, 2021

En una configuración de equilibrio de carga, un dispositivo Citrix ADC puede tener varias rutas para enviar un paquete a su destino. Por ejemplo: a un servidor y a un cliente.

Un dispositivo Citrix ADC utiliza un algoritmo de hash para seleccionar una ruta para enviar el paquete a su destino.

El algoritmo hash utiliza las dos tuplas siguientes de un paquete para calcular un hash, en función del cual el dispositivo Citrix ADC selecciona una ruta para el paquete.

- Dirección IP de origen
- Dirección IP de destino

La selección de rutas basada en información de dos tuplas puede causar una distribución desigual del tráfico en las rutas disponibles. Esta distribución desigual del tráfico conduce a la sobrecarga del tráfico en algunas rutas.

Para resolver este problema, desde la compilación 13.0 71.x, el dispositivo Citrix ADC utiliza la siguiente información de cinco tuplas de un paquete en el algoritmo hash para seleccionar una ruta para el paquete:

- Dirección IP de origen (IP del cliente)
- Puerto de origen (puerto cliente)
- Dirección IP de destino (IP de servicio)
- Puerto de destino (puerto de servicio)
- Número de protocolo

La selección de rutas basada en información de cinco tuplas garantiza una distribución uniforme del tráfico en las rutas disponibles. Esta distribución uniforme del tráfico evita la sobrecarga del tráfico en una ruta.

Considere un ejemplo de configuración de equilibrio de carga donde un cliente envía una solicitud a la dirección VIP. El dispositivo Citrix ADC utiliza la siguiente información de cinco tuplas para seleccionar una ruta para enviar el paquete de solicitud al servidor con equilibrio de carga:

- Dirección IP de origen (Dirección IP del cliente)
- Puerto de origen (puerto cliente)
- Dirección IP de destino (dirección IP del servicio)
- Puerto de destino (número de puerto de servicio)
- Número de protocolo

Prioridad con respecto a otras funciones de Citrix ADC basadas en la selección de rutas

En esta sección se habla de la prioridad de la selección de ruta basada en la función de cinco tuplas y otras funciones relacionadas con la selección de rutas en un dispositivo Citrix ADC.

- **Rutas basadas en directivas (PBR)**. Las reglas PBR siempre tienen prioridad sobre la selección de ruta basada en cinco tuplas.
- **Reenvío basado en Mac (MBF)**. En una configuración de equilibrio de carga, la selección de MBF o ruta basada en cinco tuplas tiene prioridad en los siguientes casos:
  - Para un tráfico iniciado por el cliente a la dirección VIP de la configuración de equilibrio de carga en el dispositivo Citrix ADC:
    * Solicitar tráfico destinado a un servidor con equilibrio de carga. La selección de ruta basada en cinco tuplas tiene preferencia sobre MBF.

        * Tráfico de respuesta destinado al cliente. MBF tiene preferencia sobre la selección de ruta basada en cinco tuplas.
    - Para un tráfico iniciado por el servidor a la dirección de SNIP en el dispositivo Citrix ADC:
        * Tráfico de respuesta destinado al cliente. La selección de ruta basada en cinco tuplas tiene preferencia sobre MBF.
        * Solicitar tráfico destinado a un servidor con equilibrio de carga. MBF tiene preferencia sobre la selección de ruta basada en cinco tuplas.

Solución de problemas de redirección

August 20, 2021

Para que su proceso de solución de problemas sea lo más eficiente posible, comience recopilando información sobre su red. Debe obtener la siguiente información sobre el dispositivo Citrix ADC y otros sistemas de la red:

- Diagrama completo de topología, incluida la conectividad de la interfaz y los detalles del conmutador intermedio.
- Ejecución de Configuración. Puede utilizar el comando show running para obtener la configuración en ejecución para ns.conf y ZebOS.conf.
- Salida del comando History, para determinar si se realizaron cambios en la configuración cuando se produjo el problema.
- Salida de los comandos Top y ps -ax, para determinar si algún demonio de redirección está usando la CPU o se está comportando mal.
- Cualquier archivo principal relacionado con la redirección en /var/core: Nsm, bgpd, ospfd o ripd. Compruebe la marca de tiempo para ver si son relevantes.
- dr_error.log and dr_info.log files from /var/log.
- Salida del comando date y los detalles de hora para todos los sistemas relevantes. Imprima fechas en todos los dispositivos una tras otra, de modo que las horas de los mensajes de registro se puedan correlacionar con varios eventos.
- Archivos ns.log relevantes, newnslog.
- Archivos de configuración, archivos de registro y detalles del historial de comandos de los routers ascendentes y descendentes.

Preguntas frecuentes sobre la redirección genérico

August 20, 2021

Los usuarios suelen tener las siguientes preguntas acerca de cómo solucionar problemas de redirección genérica:

- ¿Cómo guardo los archivos de configuración?

  El comando write de VTYSH guarda solo ZebOS.conf. Ejecute el comando save ns config desde CLI para guardar los archivos ns.conf y ZebOS.conf.

- Si he configurado una ruta predeterminada estática y una ruta predeterminada aprendida dinámicamente, ¿cuál es la ruta predeterminada preferida?

  La ruta aprendida dinámicamente es la ruta predeterminada preferida. Este comportamiento es exclusivo de las rutas predeterminadas. Sin embargo, en el caso del módulo de servicios de red (NSM), a menos que se modifiquen las distancias administrativas, se prefiere una ruta configurada estáticamente en el RIB sobre una ruta dinámica. La ruta que se descarga en NSM FIB es la ruta estática.

- ¿Cómo bloqueo el anuncio de rutas predeterminadas?

  La ruta predeterminada no se inyecta en ZebOS.

- ¿Cómo veo la salida de depuración de los demonios de red?

  Puede escribir la salida de depuración de los demonios de red en un archivo introduciendo el siguiente comando de archivo de registro desde la vista de configuración global en VTYSH:

  ```
  ns(config)# log file /var/ZebOS.log
  <!--NeedCopy-->
  ```

  Puede dirigir la salida de depuración a la consola introduciendo el comando del monitor de terminal desde la vista de usuario de VTYSH:

  ```
  ns# terminal monitor
  <!--NeedCopy-->
  ```

- ¿Cómo recojo núcleos de demonios en ejecución?

  Puede usar la utilidad gcore para recopilar núcleos de daemons en ejecución para procesarlos por gdb. Esto podría ser útil para depurar demonios que se comportan mal sin que se detenga toda la operación de redirección.

  ```
  gcore [-s] [-c core] [executable] pid
  <!--NeedCopy-->
  ```


La opción -s detiene temporalmente el demonio mientras recopila la imagen principal. Esta es una opción recomendada, ya que garantiza que la imagen resultante muestra el núcleo en un estado consistente.

```
root@ns#gcore -s -c nsm.core /netscaler/nsm 342
<!--NeedCopy-->
```

- ¿Cómo ejecuto un lote de comandos de ZebOS?

  Puede ejecutar un lote de comandos ZebOS desde un archivo introduciendo el <gile-name> comando VTYSH -f. Esto no reemplaza la configuración en ejecución, sino que se anexa a ella. Sin embargo, al incluir comandos para eliminar la configuración existente en el archivo por lotes y luego agregarlos para la nueva configuración deseada, puede utilizar este mecanismo para reemplazar una configuración específica:

```
!
router bgp 234
network 1.1.1.1 255.255.255.0
!
route-map bgp-out2 permit 10
 set metric 9900
 set community 8602:300
!
<!--NeedCopy-->
```

Solución de problemas específicos de OSPF

January 12, 2021

Antes de comenzar a depurar cualquier problema específico de OSPF, debe recopilar información del dispositivo Citrix ADC y de todos los sistemas de la LAN afectada, incluidos los enrutadores ascendentes y descendentes. Para comenzar, introduzca los siguientes comandos:

1. show interface from both nscli and VTYSH
2. interfaz show ip ospf
3. show ip ospf neighbor detail
4. show ip route

5. show ip ospf route
6. resumen de la base de datos show ip ospf
    - Si solo hay pocos LSA en la base de datos, introduzca show ip ospf database router, show ip ospf database A. network, show ip ospf database external y otros comandos para obtener los detalles completos de LSA.
    - Si hay un gran número de LSA en la base de datos, introduzca el comando show ip ospf database self-originado.
7. show ip ospf
8. show ns ip. Esto garantiza que se incluyan los detalles de todos los VIP de interés.
9. Obtenga los registros de dispositivos de peering y ejecute el siguiente comando:

```
gcore -s -c xyz.core /netscaler/ospfd <pid>
```

Nota: El comando gcore no es disruptivo.

Recopile información adicional del Citrix ADC de la siguiente manera:

1. Habilite el registro de mensajes de error introduciendo el siguiente comando desde la vista de configuración global en VTYSH:

```
ns(config)# log file /var/ospf.log
<!--NeedCopy-->
```

2. Habilite la depuración de eventos ospf y regístrelos mediante el siguiente comando:

```
ns(config) #log file /var/ospf.log
<!--NeedCopy-->
```

Habilite debug ospf lsa packet solo si el número de LSA en la base de datos es relativamente pequeño (< 500).

Protocolo de Internet versión 6 (IPv6)

August 20, 2021

Un dispositivo Citrix ADC admite IPv6 del lado del servidor y del lado del cliente y, por lo tanto, puede funcionar como un nodo IPv6. Puede aceptar conexiones de nodos IPv6 (tanto hosts como enrutadores) y de nodos IPv4, y puede realizar la traducción de protocolos (RFC 2765) antes de enviar tráfico a los servicios.

En la tabla siguiente se enumeran algunas de las funciones IPv6 que admite el dispositivo Citrix ADC.

Cuadro 1 Algunas funciones IPv6 admitidas

Funciones IPv6
Direcciones IPv6 para SNIP (NSIP6, VIP6 y SNIP6)
Detección de vecinos (resolución de direcciones, detección de direcciones duplicadas, detección de inaccesibilidad de vecinos, detección de enrutadores)
Aplicaciones de administración (ping6, telnet6, ssh6)
Redirección estática y redirección dinámica (OSPF, BGP, RIPng e ISIS)
VLAN basadas en puertos
Listas de control de acceso para direcciones IPv6 (ACL6)
Protocolos IPv6 (TCP6, UDP6, ICMP6)
Soporte del lado del servidor (direcciones IPv6 para servidores virtuales, servicios)
USIP (Usar IP de origen) y DSR (retorno directo del servidor) para IPv6
SNMP y CVPN para IPv6
HA con dirección de nodo IPv6 nativa
Direcciones IPv6 para MIP
Detección de rutas de MTU para IPv6

Implementación de la compatibilidad con IPv6

Debe habilitar la función IPv6 en un dispositivo Citrix ADC antes de poder usarla o configurarla. Si IPv6 está inhabilitado, Citrix ADC no procesa paquetes IPv6. Muestra la siguiente advertencia cuando ejecuta un comando no compatible:

```
1 ”Warning: Feature(s) not enabled [IPv6PT]”
2 <!--NeedCopy-->
```

Utilice cualquiera de los procedimientos siguientes para habilitar o inhabilitar IPv6.

Procedimientos CLI

Para habilitar o inhabilitar IPv6 mediante la CLI:

En el símbolo del sistema, escriba uno de los siguientes comandos:

- habilitar la función ns ipv6pt
- inhabilitar la función ns ipv6pt

Procedimientos de GUI

Para habilitar o inhabilitar IPv6 mediante la GUI:

1. Vaya a **Sistema** > **Configuración**, en el grupo **Modos y funciones**, haga clic en **Configurar funciones avanzadas**.
2. Seleccione o desactive la opción **Traducción de protocolos IPv6**.

Compatibilidad con VLAN

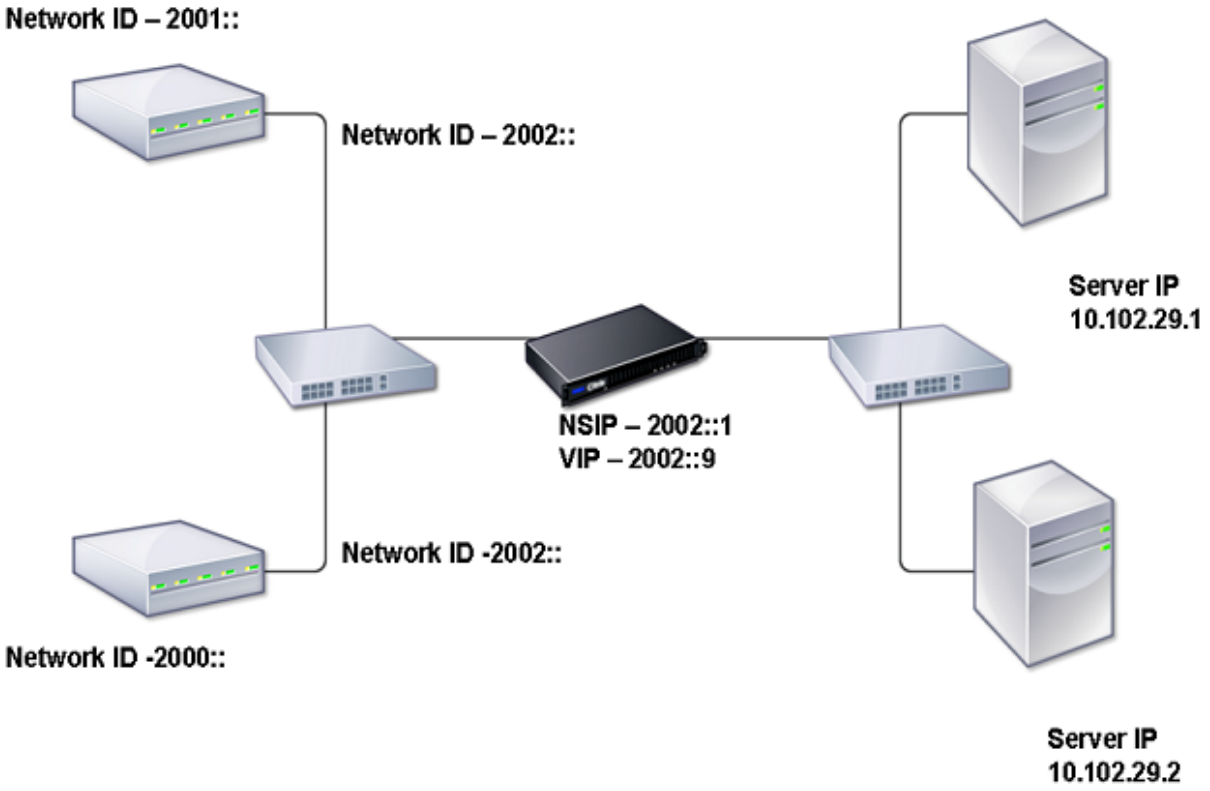
Si necesita enviar paquetes de difusión o multidifusión sin identificar la VLAN (por ejemplo, durante DAD para NSIP o ND6 para el siguiente salto de la ruta), puede configurar el dispositivo Citrix ADC para que envíe el paquete en todas las interfaces con el etiquetado adecuado. La VLAN se identifica mediante ND6 y solo se envía un paquete de datos en la VLAN. Para obtener más información sobre ND6 y las VLAN, consulte Configuración de la detección de vecinos.

Las VLAN basadas en puertos son comunes para IPv4 e IPv6. Las VLAN basadas en prefijos son compatibles con IPv6.

Caso de implementación simple

A continuación se muestra un ejemplo de una configuración de equilibrio de carga simple que consiste en un vserver IPv6 e IPv4 servicios, como se ilustra en el siguiente diagrama de topología.

Ilustración 1. Topología de ejemplo de IPv6



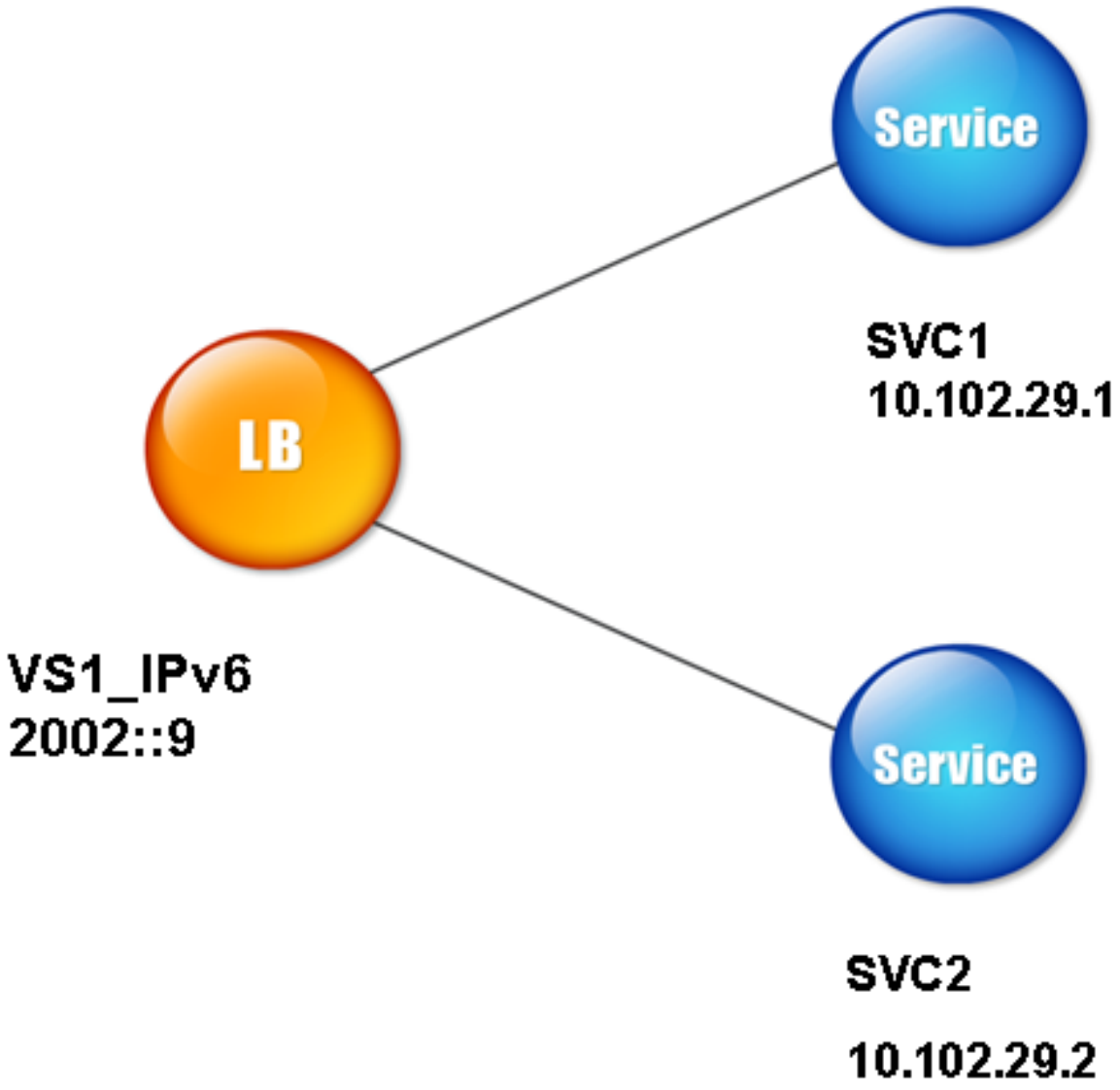
En la siguiente tabla se resumen los nombres y valores de las entidades que se deben configurar en Citrix ADC.

Tabla 2. Valores de ejemplo para crear entidades

Tipo de entidad	Nombre	Valor
Servidor LB	VS1_IPv6	2002::9
Servicios	SVC1	10.102.29.1
	SVC2	10.102.29.2

En la siguiente ilustración se muestran las entidades y los valores de los parámetros que se configurarán en Citrix ADC.

Ilustración 2. Diagrama de entidad IPv6



Para configurar este caso de implementación, debe hacer lo siguiente:

1. Cree un servicio IPv6.
2. Cree un vserver LB IPv6.
3. Enlazar los servicios al servidor vserver.

Procedimientos CLI

Para crear servicios IPv4 mediante la CLI:

En el símbolo del sistema, escriba:

- **add service** <Name> <IPAddress> <Protocol> <Port>
- **servicio sh** <Name>

Ejemplo:

```
> add service SVC1 10.102.29.1 HTTP 80
Done

>add service SVC2 10.102.29.2 HTTP 80
Done
<!--NeedCopy-->
```

Para crear vserver IPv6 mediante la CLI:

En el símbolo del sistema, escriba:

- **add lb vserver** <Name> <IPAddress> <Protocol> <Port>
- **sh lb vserver** <Name>

Ejemplo:

```
> add lb vserver VS1_IPv6 2002::9 HTTP 80
Done
<!--NeedCopy-->
```

Para enlazar un servicio a un servidor LB mediante la CLI:

En el símbolo del sistema, escriba:

- **enlazar lb vserver** <name> <service>
- **sh lb vserver** <name>

Ejemplo:

```
> bind lb vserver VS1_IPv6 SVC1
Done
<!--NeedCopy-->
```

Procedimientos de GUI

Para crear servicios IPv4 mediante la GUI:

Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servicios**, haga clic en **Agregar** y, a continuación, establezca los parámetros siguientes:

- Nombre del servicio
- Dirección IP
- Protocolo
- Port

Para crear vserver IPv6 mediante la GUI:

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**, haga clic en **Agregar** y active la casilla de verificación **IPv6**.
2. Defina los siguientes parámetros:
    - Nombre
    - Protocolo
    - Tipo de dirección IP
    - Dirección IP
    - Port

Para enlazar un servicio a un servidor LB mediante la GUI:

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**.
2. En la página **Servidores virtuales de equilibrio de carga**, seleccione el servidor virtual para el que quiere enlazar el servicio (por ejemplo, VS1_IPv6).
3. Haga clic en **Abrir**.
4. En el cuadro de diálogo **Configurar servidor virtual (equilibrio de carga)**, en la ficha **Servicios**, active la casilla de verificación **Activo** correspondiente al servicio que quiere enlazar al servidor vserver (por ejemplo, SVC1).
5. Haga clic en **Aceptar**.
6. Repita los pasos 1-4 para enlazar el servicio (por ejemplo, SVC2 al servidor vserver).

Modificación de encabezado de host

Cuando una solicitud HTTP tiene una dirección IPv6 en el encabezado del host y el servidor no entiende la dirección IPv6, debe asignar la dirección IPv6 a una dirección IPv4. A continuación, se utiliza la dirección IPv4 en el encabezado del host de la solicitud HTTP enviada al servidor vserver.

Procedimientos CLI

Para cambiar la dirección IPv6 en el encabezado del host a una dirección IPv4 mediante la CLI:

En el símbolo del sistema, escriba:

- **set ns ip6** <IPv6Address> -**map** <IPAddress>
- **sh ns ip6** <IPv6Address>

Ejemplo:


```
> set ns ip6 2002::9 -map 200.200.200.200
Done
<!--NeedCopy-->
```

Procedimientos de GUI

Para cambiar la dirección IPv6 en el encabezado del host a una dirección IPv4 mediante la GUI:

1. Vaya a **Sistema** > **Red** > **IPs** y, en la ficha **IPv6s**, seleccione la dirección IP para la que quiere configurar una dirección IP asignada, por ejemplo, 2002:0:0:0:0:0:0:9 y haga clic en Modificar.
2. En el cuadro de texto **IP asignada**, escriba la dirección IP asignada que quiere configurar, por ejemplo, 200.200.200.200.

Inserción VIP

Si se envía una dirección IPv6 a un servidor basado en IPv4, es posible que el servidor no comprenda la dirección IP en el encabezado HTTP y que genere un error. Para evitar esto, puede asignar una dirección IPv4 al IPv6 VIP. A continuación, puede habilitar la inserción VIP para habilitar la inserción de la dirección VIP IPv4 y el número de puerto en las solicitudes HTTP enviadas a los servidores.

Procedimientos CLI

Para configurar una dirección IPv6 de mapa mediante la CLI:

En el símbolo del sistema, escriba:

set ns ip6 <IPv6Address> -**map** <IPAddress>

Ejemplo:

```
> set ns ip6 2002::9 -map 200.200.200.200
 Done
<!--NeedCopy-->
```

Para habilitar la inserción VIP mediante la CLI:

En el símbolo del sistema, escriba:

- **set lb vserver** <Value> <name> -**InsertVServeripPort**
- **sh lb vserver** <name>

Ejemplo:

```
> set lb vserver VS1_IPv6 -insertVserverIPPort ON
 Done

<!--NeedCopy-->
```

Procedimientos de GUI

Para configurar una dirección IPv6 de mapa mediante la GUI:

1. Vaya a **Sistema** > **Red** > **IPs**, en la ficha **IPv6s**, seleccione la dirección IP para la que quiere configurar una dirección IP de mapa, por ejemplo, 2002:0:0:0:0:0:0:9 y haga clic en **Modificar**.
2. En el cuadro de texto **IP asignada**, escriba la dirección IP de mapa que quiere configurar, por ejemplo, 200.200.200.200.

Para habilitar la inserción VIP mediante la GUI:

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**, seleccione el servidor virtual que quiere habilitar la inserción del puerto y haga clic en **Modificar**.
2. En la ficha **Avanzadas**, en **Configuración del tráfico**, en el cuadro de lista desplegable **Inserción del puerto IP de Vserver**, seleccione **VIPADDR**.
3. En el cuadro de texto **Inserción del puerto IP del servidor virtual**, escriba el encabezado vip.

Dominios de tráfico

October 5, 2021

> **Advertencia**
>
> Citrix recomienda utilizar Particiones de administración en lugar de utilizar Dominios de tráfico. Para obtener más información, consulte la página Partición de administrador .

Los dominios de tráfico son una forma de segmentar el tráfico de red para diferentes aplicaciones. Puede utilizar dominios de tráfico para crear varios entornos aislados en un dispositivo Citrix ADC. Una aplicación que pertenece a un dominio de tráfico específico se comunica con entidades y procesa el tráfico dentro de ese dominio. El tráfico que pertenece a un dominio de tráfico no puede cruzar el límite de otro dominio de tráfico.

Beneficios del uso de dominios de tráfico

Las principales ventajas de utilizar dominios de tráfico en un dispositivo Citrix ADC son las siguientes:

- **Uso de direcciones IP duplicadas en una red**. Los dominios de tráfico permiten utilizar direcciones IP duplicadas en la red. Puede asignar la misma dirección IP o dirección de red a varios dispositivos de una red o a varias entidades de un dispositivo Citrix ADC, siempre y cuando cada una de las direcciones duplicadas pertenezca a un dominio de tráfico diferente.
- **Uso de entidades duplicadas en el dispositivo Citrix ADC**. Los dominios de tráfico también permiten utilizar entidades de funciones Citrix ADC duplicadas en el dispositivo. Puede crear entidades con la misma configuración siempre que cada entidad esté asignada a un dominio de tráfico independiente.
  Nota: No se admiten entidades duplicadas con el mismo nombre.
- **Multiarrendamiento**. Con los dominios de tráfico, puede proporcionar servicios de alojamiento a varios clientes aislando el tipo de tráfico de aplicaciones de cada cliente dentro de un espacio de direcciones definido en la red.

Un dominio de tráfico se identifica de forma exclusiva mediante un identificador, que es un valor entero. Cada dominio de tráfico necesita una VLAN o un conjunto de VLAN. La funcionalidad de aislamiento del dominio de tráfico depende de las VLAN enlazadas al dominio de tráfico. Se puede enlazar más de una VLAN a un dominio de tráfico, pero la misma VLAN no puede formar parte de varios dominios de tráfico. Por lo tanto, el número máximo de dominios de tráfico que se pueden crear depende del número de VLAN configuradas en el dispositivo.

Dominio de tráfico predeterminado

Un dispositivo Citrix ADC tiene un dominio de tráfico preconfigurado, denominado *dominio de tráfico predeterminado*, que tiene un ID de 0. Todos los ajustes y configuraciones de fábrica forman parte del dominio de tráfico predeterminado. Puede crear otros dominios de tráfico y, a continuación, segmentar el tráfico entre el dominio de tráfico predeterminado y cada uno de los demás dominios de tráfico. No se puede quitar el dominio de tráfico predeterminado del dispositivo Citrix ADC. Cualquier entidad de entidad que cree sin establecer el ID de dominio de tráfico se asocia automáticamente al dominio de tráfico predeterminado.

Nota: Algunas funciones y configuraciones solo se admiten en el dominio de tráfico predeterminado. No funcionan en dominios de tráfico no predeterminados. Para obtener una lista de las funciones admitidas en todos los dominios de tráfico, consulte Funciones de Citrix ADC compatibles en dominios de tráfico.

Cómo funcionan los dominios de tráfico

Como ilustración de los dominios de tráfico, considere un ejemplo en el que dos dominios de tráfico, con los ID 1 y 2, están configurados en el dispositivo Citrix ADC NS1.

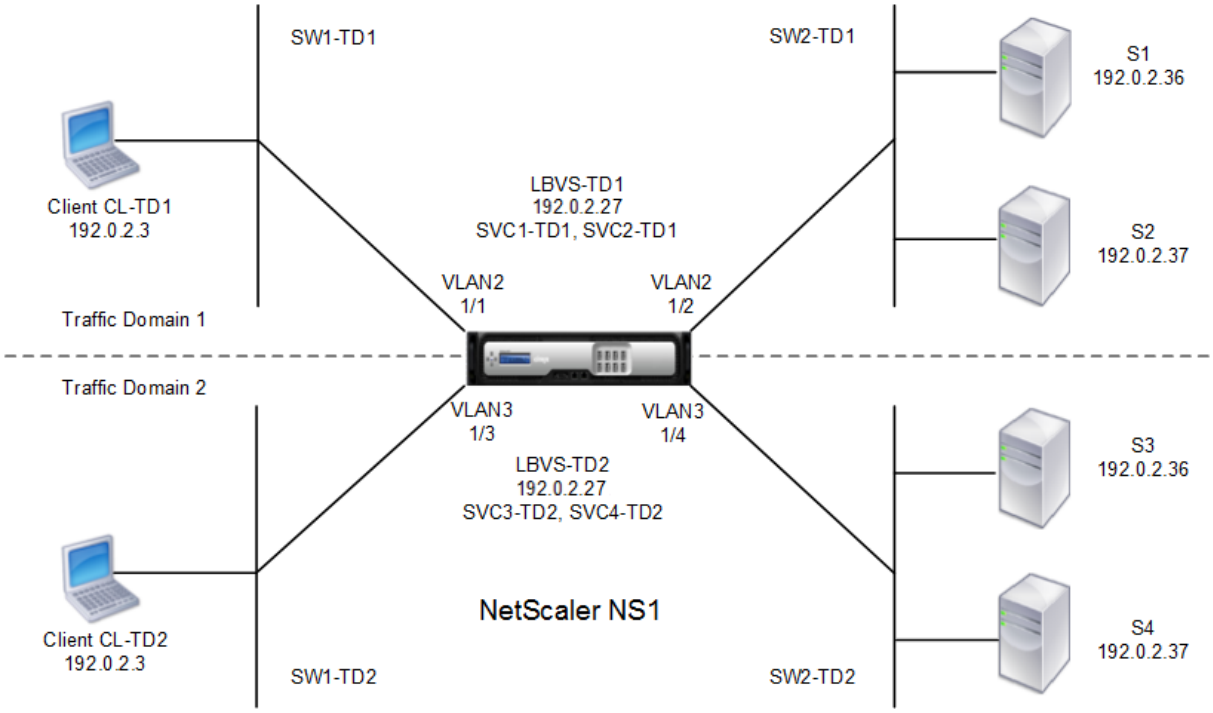
En el dominio de tráfico 1, el servidor virtual de equilibrio de carga LBVS-TD1 está configurado para equilibrar la carga del tráfico entre los servidores S1 y S2. En el dispositivo Citrix ADC, los servidores S1 y S2 están representados por los servicios SVC1-TD1 y SVC2-TD1, respectivamente. Los servidores S1 y S2 están conectados a NS1 a través del conmutador L2 SW2-TD1. El cliente CL-TD1 se encuentra en una red privada conectada a NS1 a través del conmutador L2 SW1-TD1. SW1-TD1 y SW2-TD1 están conectados a la VLAN 2 de NS1. La VLAN 2 está vinculada al dominio de tráfico 1, lo que significa que el cliente CL-TD1 y los servidores S1 y S2 forman parte del dominio de tráfico 1.

Del mismo modo, en el dominio de tráfico 2, el servidor virtual de equilibrio de carga LBVS-TD2 está configurado para equilibrar la carga del tráfico en S3 y S4. En el dispositivo Citrix ADC, los servidores S3 y S4 están representados por los servicios SVC3-TD2 y SVC4-TD2, respectivamente. Los servidores S3 y S4 están conectados a NS1 a través del conmutador L2 SW2-TD2. El cliente CL-TD2 se encuentra en una red privada conectada a NS1 a través del conmutador L2 SW1-TD2. SW1-TD2 y SW2-TD2 están conectados a la VLAN 3 de NS1. La VLAN 3 está vinculada al dominio de tráfico 2, lo que significa que el cliente CL-TD2 y los servidores S3 y S4 forman parte del dominio de tráfico 2.

En el dispositivo Citrix ADC, las entidades LBVS-TD1 y LBVS-TD2 comparten la misma configuración, incluida la dirección IP. Lo mismo ocurre con SVC1-TD1 y SVC3-TD2, y para SVC2-TD1 y SVC4-TD2. Esto es posible porque estas entidades se encuentran en dominios de tráfico diferentes.

Del mismo modo, los servidores S1 y S3, S2 y S4 comparten la misma dirección IP y los clientes CL-TD1 y CL-TD2 tienen la misma dirección IP.

Ilustración 1. Cómo funcionan los dominios de tráfico



En la tabla siguiente se enumeran los parámetros utilizados en el ejemplo.

Entidad	Nombre	Detalles
Configuración en el dominio de tráfico 1		
VLAN enlazadas al dominio de tráfico 1	VLAN 2	ID de VLAN: 2 interfaces enlazadas: 1/1, 1/2
Cliente conectado a TD1	CL-TD1 (solo para fines de referencia)	Dirección IP: 192.0.2.3
Servidor virtual de equilibrio de carga en TD1	LBVS-TD1	Dirección IP: 192.0.2.27
Servicio vinculado al servidor virtual LBVS-TD1	SVC1-TD1	Dirección IP: 192.0.2.36
Servicio vinculado al servidor virtual LBVS-TD1	SVC2-TD1	Dirección IP: 192.0.2.37
RECORTAR	SNIP-TD1 (solo para fines de referencia)	Dirección IP: 192.0.2.27
Configuración del dominio de tráfico 2		

Entidad	Nombre	Detalles
VLAN enlazada al dominio de tráfico 2	VLAN 3	ID de VLAN: 3 interfaces enlazadas: 1/3, 1/4
Cliente conectado a TD2	CL-TD2 (solo para fines de referencia)	Dirección IP: 192.0.2.3
Servidor virtual de equilibrio de carga en TD2	LBVS-TD2	Dirección IP: 192.0.2.27
Servicio vinculado al servidor virtual LBVS-TD2	SVC3-TD2	Dirección IP: 192.0.2.36
Servicio vinculado al servidor virtual LBVS-TD2	SVC4-TD2	Dirección IP: 192.0.2.37
SNIP en TD2	SNIP-TD2 (solo como referencia)	Dirección IP: 192.0.2.29

A continuación se presenta el flujo de tráfico en el dominio de tráfico 1:

1. El cliente CL-TD1 transmite una solicitud ARP para la dirección IP de 192.0.2.27 a través del conmutador L2 SW1-TD1.
2. La solicitud ARP llega a NS1 en la interfaz 1/1, que está vinculada a la VLAN 2. Debido a que la VLAN 2 está vinculada al dominio de tráfico 1, NS1 actualiza la tabla ARP del dominio de tráfico 1 para la dirección IP del cliente CL-TD1.
3. Dado que la solicitud ARP se recibe en el dominio de tráfico 1, NS1 busca una entidad configurada en el dominio de tráfico 1 que tenga una dirección IP de 192.0.2.27. NS1 descubre que un servidor virtual de equilibrio de carga LBVS-TD1 está configurado en el dominio de tráfico 1 y tiene la dirección IP 192.0.2.27.
4. NS1 envía una respuesta ARP con la dirección MAC de la interfaz 1/1.
5. La respuesta ARP llega a CL-TD1. CL-TD1 actualiza su tabla ARP para la dirección IP de LBVS-TD1 con la dirección MAC de la interfaz 1/1 de NS1.
6. El cliente CL-TD1 envía una solicitud a 192.0.2.27. LBVS-TD1 recibe la solicitud en el puerto 1/1 de NS1.
7. El algoritmo de equilibrio de carga del LBVS-TD1 selecciona el servidor S2 y NS1 abre una conexión entre un SNIP del dominio de tráfico 1 (192.0.2.27) y S2.
8. S2 responde al SNIP 192.0.2.27 en NS1.
9. NS1 envía la respuesta de S2 al cliente CL-TD1.

A continuación se presenta el flujo de tráfico en el dominio de tráfico 2:

1. El cliente CL-TD2 transmite una solicitud ARP para la dirección IP de 192.0.2.27 a través del conmutador L2 SW1-TD2.

2. La solicitud ARP llega a NS1 en la interfaz 1/3, que está vinculada a la VLAN 3. Debido a que la VLAN 3 está vinculada al dominio de tráfico 2, NS1 actualiza la entrada de tabla ARP del dominio de tráfico 2 para la dirección IP del cliente CL-TD2, aunque ya haya una entrada ARP para la misma dirección IP (CL-TD1) en la tabla ARP del dominio de tráfico 1.
3. Dado que la solicitud ARP se recibe en el dominio de tráfico 2, NS1 busca en el dominio de tráfico 2 una entidad que tiene una dirección IP 192.0.2.27. NS1 descubre que el servidor virtual de equilibrio de carga LBVS-TD2 está configurado en el dominio de tráfico 2 y tiene la dirección IP 192.0.2.27. NS1 ignora LBVS-TD1 en el dominio de tráfico 1, aunque tenga la misma dirección IP que LBVS-TD2.
4. NS1 envía una respuesta ARP con la dirección MAC de la interfaz 1/3.
5. La respuesta ARP llega a CL-TD2. CL-TD2 actualiza su entrada de tabla ARP para la dirección IP de LBVS-TD2 con la dirección MAC de la interfaz 1/3 de NS1.
6. El cliente CL-TD2 envía una solicitud a 192.0.2.27. LBVS-TD2 recibe la solicitud en la interfaz 1/3 de NS1.
7. El algoritmo de equilibrio de carga de LBVS-TD2 selecciona el servidor S3 y NS1 abre una conexión entre un SNIP del dominio de tráfico 2 (192.0.2.29) y S3.
8. S2 responde al SNIP 192.0.2.29 en NS1.
9. NS1 envía la respuesta de S2 al cliente CL-TD2.

Funciones de Citrix ADC compatibles en dominios de tráfico

Las funciones de Citrix ADC de la lista siguiente son compatibles con todos los dominios de tráfico.

> **Importante**
>
> Cualquier función de Citrix ADC que no se menciona a continuación solo se admite en el dominio de tráfico predeterminado.

- Mesa ARP
- Tabla de ND6
- Mesa puente
- Todos los tipos de direcciones IPv4 e IPv6
- Rutas IPv4 e IPv6
- ACL y ACL6
- PBR y PBR6
- INAT
- RNAT
- RNAT6
- MSR
- MSR6
- Perfiles de red

- MIB SNMP
- Fragmentación
- Monitores (no se admiten monitores con guiones)
- Conmutación de contenido
- Redirección de caché
- Persistencia (no se admiten grupos de persistencia)
- Servicio (los servicios basados en dominio no son compatibles)
- Grupo de servicios (no se admiten grupos de servicios basados en dominios)
- Directivas (*)
- PING
- TRACEROUTE
- PMTU
- Alta disponibilidad (no se admite la duplicación de conexiones)
- Clúster (compatible con clústeres L2. No se admite en clústeres L3)
- Persistencia de cookies
- MSS
- Registro (Syslog no es compatible)
- Protección contra picos de tensión
- Equilibrio de carga (no se admiten los siguientes tipos:)
  - TFTP
  - RTSP
  - Diameter
  - SIP
  - SMPP
- NAT46
- NAT64
- DNS64
- Reglas de sesión de reenvío
- SNMP

Nota

- * Las directivas no tienen puntos de enlace globales para los dominios de tráfico. Sin embargo, las directivas se pueden enlazar a un servidor virtual de equilibrio de carga específico de un dominio de tráfico.
- Las funciones Global Server Loading Balancing (GSLB) y ADNS de Citrix ADC no conocen los dominios de tráfico. Si es necesario compartir la configuración de GSLB entre todos los dominios de tráfico, los métodos GSLB Proximidad estática y Tiempo de ida y vuelta (RTT) no funcionan. Como solución alternativa en este caso, puede utilizar métodos GSLB distintos de RTT y Proximidad estática. Para obtener más información, consulte http://support.

> citrix.com/article/CTX202277.

Configuración de dominios de tráfico

La configuración de un dominio de tráfico en el dispositivo Citrix ADC consta de las siguientes tareas:

- **Agregue VLAN.** Cree VLAN y vincule las interfaces especificadas a ellas.
- **Cree una entidad de dominio de tráfico y vincule las VLAN a ella.** Esto implica las dos tareas siguientes:
  - Cree una entidad de dominio de tráfico identificada de forma exclusiva mediante un ID, que es un valor entero.
  - Enlazar las VLAN especificadas a la entidad de dominio de tráfico. Todas las interfaces enlazadas a las VLAN especificadas están asociadas al dominio de tráfico. Se puede enlazar más de una VLAN a un dominio de tráfico, pero una VLAN no puede formar parte de varios dominios de tráfico.
- **Cree entidades de entidad en el dominio del tráfico**. Cree las entidades de entidad necesarias en el dominio del tráfico. Los comandos de CLI y los cuadros de diálogo de configuración de todas las funciones admitidas en un dominio de tráfico no predeterminado incluyen un parámetro denominado *identificador de dominio de tráfico* (td). Al configurar una entidad de entidad, si quiere que la entidad se asocie a un dominio de tráfico concreto, debe especificar la td. Cualquier entidad de entidad que cree sin establecer el td se asocia automáticamente con el dominio de tráfico predeterminado.

Para darle una idea de cómo se asocian las entidades de entidades a un dominio de tráfico, en este tema se describen los procedimientos para configurar todas las entidades mencionadas en la ilustración titulada Cómo funcionan los dominios de tráfico.

La CLI tiene dos comandos para estas dos tareas, pero la GUI los combina en un solo cuadro de diálogo.

Procedimientos CLI

Para crear una VLAN y enlazar interfaces a ella mediante la CLI:

En el símbolo del sistema, escriba:

- **agregar vlan** <id>
- **bind vlan** <id- **info** <slot/port>
- **show vlan** <id>

Para crear una entidad de dominio de tráfico y enlazar VLAN a ella mediante la CLI:

En el símbolo del sistema, escriba:

- **add ns trafficdomain** <td>
- **bind ns trafficdomain** <td> -**vlan** <id>

- **show ns trafficdomain** <td>

Para crear un servicio mediante la CLI:

En el símbolo del sistema, escriba:

- **agregar servicio** <name><IP><serviceType><port>-**td** <id>
- **servicio de espectáculos** <name>

Para crear un servidor virtual de equilibrio de carga y enlazar servicios a él mediante la CLI:

En el símbolo del sistema, escriba:

- **agregar lb vserver** <name><serviceType><IPAddress><port>-**td** <id>
- **vincular lb vserver** <name><serviceName>
- **mostrar servidor lb** <name>

Procedimientos de GUI

Para crear una VLAN mediante la GUI:

Vaya a **Sistema** > **Red** > **VLAN**, haga clic en **Agregar**y defina los parámetros.

Para crear una entidad de dominio de tráfico mediante la interfaz gráfica de usuario:

Vaya a **Sistema** > **Red** > **Dominios de tráfico**, haga clic en **Agregar**y, en el cuadro de diálogo **Crear dominio de tráfico**, defina los parámetros.

Para crear un servicio mediante la interfaz gráfica de usuario:

Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servicios**, haga clic en **Agregar**y defina los parámetros.

Para crear un servidor virtual de equilibrio de carga mediante la interfaz gráfica de usuario:

Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**, haga clic en **Agregar**y defina los parámetros.

Vinculaciones de entidades de dominio entre tráfico

January 12, 2021

Puede enlazar servicios de un dominio de tráfico a un servidor virtual de otro dominio de tráfico. Todos los servicios que se vincularán a un servidor virtual en un dominio de tráfico diferente deben residir en el mismo dominio de tráfico.

Para configurar este soporte, utilice el comando bind lb vserver existente o el procedimiento GUI relacionado.

Esta capacidad puede facilitar la interacción entre diferentes dominios de tráfico. En una empresa, los servidores se pueden agrupar en diferentes dominios de tráfico. Los servidores virtuales se crean en un dominio de tráfico que enfrenta a Internet. Un servidor virtual de este dominio de tráfico se puede configurar para que los servidores de equilibrio de carga de otro dominio de tráfico. Este servidor virtual recibe solicitudes de conexión de Internet para ser reenviadas a los servidores enlazados.

Cuando se utiliza un dispositivo Citrix ADC en una infraestructura de nube, se puede asignar a cada arrendatario un dominio de tráfico independiente y todos los recursos (incluidos los servidores) de un arrendatario se pueden agrupar en el dominio de tráfico del arrendatario. Para cada arrendatario, se crea un servidor virtual para los servidores de equilibrio de carga en su dominio de tráfico. Todos estos servidores virtuales se agrupan en un único dominio de tráfico que enfrenta a Internet.

Considere un ejemplo de en qué proveedor de servicios en la nube Example-Cloud-A tiene tres dominios de tráfico, con identificadores 10, 20 y 30, configurados en el dispositivo Citrix ADC NS1.

Example-Org-A y Example-Org-B son arrendatarios de Example-Cloud-A. Al arrendatario A se le asigna el dominio de tráfico 20 y al arrendatario B se le asigna el dominio 30. Los servidores S1 y S2 residen en el dominio de tráfico 20 y los servidores S3 y S4 residen en el dominio de tráfico 30.

El dominio de tráfico 10 se enfrenta a Internet. Los servidores virtuales LBVS-1 y LBVS-2 se crean en el dominio de tráfico 10. LBVS-1, en el dominio de tráfico 10, está configurado para equilibrar la carga de los servidores S1 y S2, que están en el dominio de tráfico 20. LBVS-2, en el dominio de tráfico 10, está configurado para equilibrar la carga de los servidores S3 y S4, que están en el dominio de tráfico 30.

Por lo tanto, estos servidores virtuales aceptan solicitudes de conexión a Internet para servidores que se encuentran en un dominio de tráfico diferente al de los servidores virtuales.

Dominios de tráfico basados en MAC virtuales

August 20, 2021

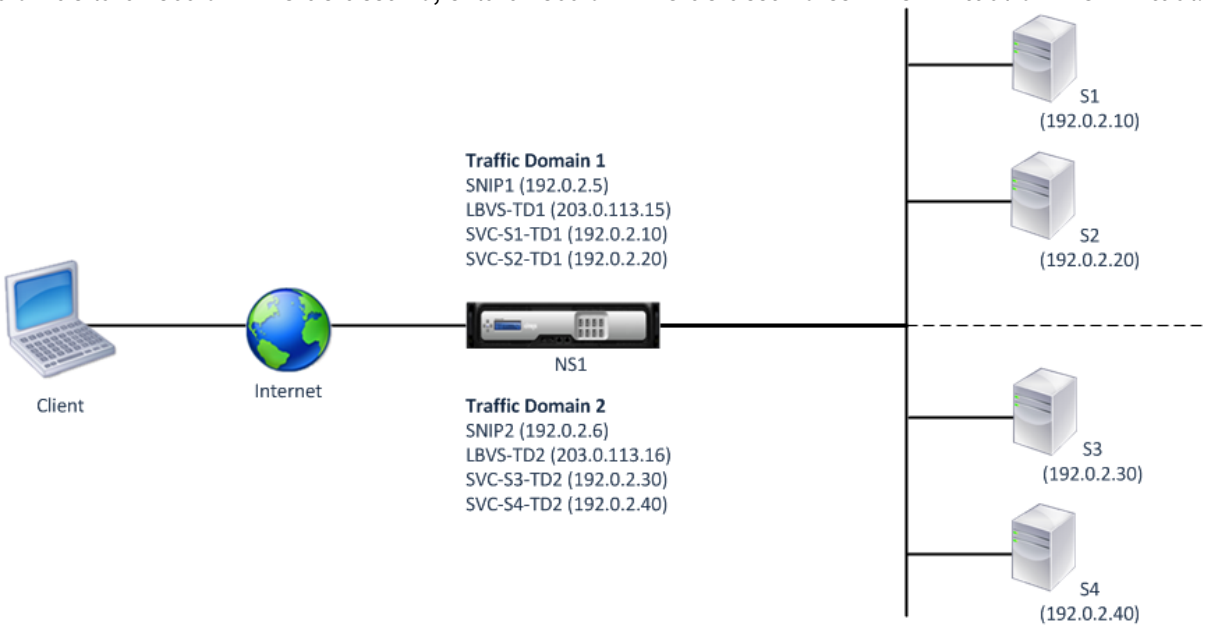
Puede asociar un dominio de tráfico con una dirección MAC virtual en lugar de con VLAN. A continuación, Citrix ADC envía la dirección MAC virtual del dominio de tráfico en todas las respuestas a las consultas ARP para entidades de red en ese dominio. Como resultado, el ADC puede segregar el tráfico entrante posterior para diferentes dominios de tráfico sobre la base de la dirección MAC de destino, ya que la dirección MAC de destino es la dirección MAC virtual de un dominio de tráfico. Después de crear entidades en un dominio de tráfico, puede administrarlas y supervisarlas fácilmente realizando operaciones a nivel de dominio de tráfico.

Considere un ejemplo en el que dos dominios de tráfico, con identificadores 1 y 2, están configurados en Citrix ADC Appliance NS1. Citrix ADC crea una dirección MAC virtual MAC1 virtual y la asocia con el dominio de tráfico 1. Del mismo modo, Citrix ADC creó otra dirección MAC virtual MAC2 y se asocia con el dominio de tráfico 2.

En el dominio de tráfico 1, el servidor virtual de equilibrio de carga LBVS-TD1 está configurado para equilibrar la carga del tráfico entre los servidores S1 y S2. En el dispositivo Citrix ADC, los servidores S1 y S2 están representados por los servicios SVC1-TD1 y SVC2-TD1, respectivamente. Se configura una dirección IP de subred (SNIP) SNIP1 para permitir que Citrix ADC se comunique con S1 y S2. Dado que el MAC1 virtual está asociado con el dominio de tráfico 1, el dispositivo envía el MAC1 virtual como dirección MAC en todos los anuncios ARP y las respuestas ARP para LBVS-TD1 y SNIP1.

Del mismo modo, en el dominio de tráfico 2, el servidor virtual de equilibrio de carga LBVS-TD2 está configurado para equilibrar la carga del tráfico en S3 y S4. En el dispositivo Citrix ADC, los servidores S3 y S4 están representados por los servicios SVC3-TD2 y SVC4-TD2, respectivamente. Se configura una dirección SNIP SNIP2 para permitir que Citrix ADC se comunique con S3 y S4. Dado que el MAC2 virtual está asociado con el dominio de tráfico 2, el dispositivo envía el MAC2 virtual como dirección MAC en todos los anuncios ARP y las respuestas ARP para LBVS-TD2 y SNIP2.

Citrix ADC segrega el tráfico entrante subsiguiente para los dominios de tráfico 1 o 2 en función de la dirección MAC de destino, si la dirección MAC de destino es MAC1 virtual o MAC2 virtual.



En la tabla siguiente se enumeran los ajustes utilizados en el ejemplo: Configuración de ejemplo de dominio de tráfico basada en MAC virtual.

Antes de comenzar

Los siguientes son puntos a tener en cuenta antes de configurar el dominio de tráfico basado en MAC virtual:

1. Los dominios de tráfico basados en MAC virtuales son la forma más fácil de lograr la segregación del tráfico de red.

2. Dado que los dominios de tráfico basados en MAC virtuales segregan el tráfico de red basado en direcciones MAC virtuales y no en VLAN, no puede crear direcciones IP duplicadas en dominios de tráfico basados en MAC virtuales diferentes en un dispositivo Citrix ADC.
3. Los dominios de tráfico basados en MAC virtual no funcionan cuando Citrix ADC se implementa solo en modo L2.
4. Los dominios de tráfico basados en VLAN y MAC virtual pueden coexistir en un dispositivo Citrix ADC. Los dominios de tráfico basados en MAC virtual se ejecutan en todas las VLAN que no están enlazadas a ningún dominio de tráfico basado en VLAN.

Pasos de configuración

La configuración de un dominio de tráfico basado en MAC virtual en un dispositivo Citrix ADC consta de las siguientes tareas:

- Cree una entidad de dominio de tráfico y habilite la opción MAC virtual. Cree una entidad de dominio de tráfico identificada de forma única por un ID, que es un valor entero y, a continuación, habilite la opción MAC virtual. Después de crear la entidad de dominio de tráfico, Citrix ADC crea una dirección MAC virtual y, a continuación, la asocia a la entidad de dominio de tráfico.
- Cree entidades de entidad en el dominio de tráfico. Cree las entidades de entidad necesarias en el dominio de tráfico especificando el identificador de dominio de tráfico (td) al configurar estas entidades de entidad. Las entidades de red propiedad de Citrix ADC creadas en un dominio de tráfico basado en MAC virtual están asociadas a la dirección MAC virtual, que está asociada al dominio de tráfico. A continuación, Citrix ADC envía la dirección MAC virtual del dominio de tráfico en anuncios ARP y respuestas ARP para estas entidades de red.

Procedimientos CLI

Para crear un dominio de tráfico basado en MAC virtual mediante la CLI:

En el símbolo del sistema, escriba:

```
agregar ns TrafficDomain <td> [-vmac (                DISABLED )]
ENABLED
```

-
- mostrar ns trafficdomain <td>

Para configurar una dirección SNIP mediante la CLI:

En el símbolo del sistema, escriba:

- add ns ip <IPAddress> <netmask> -type SNIP –td <id>

- show ns ip <IPAddress> -td <id>

Para crear un servicio mediante la CLI:

En el símbolo del sistema, escriba:

- add service <name> <IP> <serviceType> <port> -td <id>
- show service <name> -td <id>

Para crear un servidor virtual de equilibrio de carga y enlazar servicios con él mediante la CLI:

En el símbolo del sistema, escriba:

- add lb vserver <id> <name> <serviceType> <IPAddress> <port> -td
- enlazar lb vserver <name> <serviceName>
- show lb vserver <name> -td <id>

Ejemplo:

```
> add ns trafficDomain 1 -vmac ENABLED
 Done
> add ns trafficDomain 2 -vmac ENABLED
 Done

> add ns ip 192.0.2.5 255.255.255.0 -type -SNIP -td 1
 Done
> add service  SVC-S1-TD1  192.0.2.10 HTTP 80 -td 1
 Done
> add service  SVC-S2-TD1  192.0.2.20 HTTP 80 -td 1
 Done
> add lb vserver  LBVS-TD1 HTTP   203.0.113.15 80 -td 1
 Done
> bind lb vserver  LBVS-TD1 SVC-S1-TD1
 Done
> bind lb vserver  LBVS-TD1 SVC-S2-TD1
 Done

> add ns ip 192.0.2.6 255.255.255.0 -type -SNIP -td 2
 Done
> add service  SVC-S3-TD2  192.0.2.30 HTTP 80 -td 2
 Done
> add service  SVC-S4-TD2  192.0.2.40 HTTP 80 -td 2
 Done
> add lb vserver  LBVS-TD1 HTTP   203.0.113.16 80 -td 1
 Done
> bind lb vserver  LBVS-TD2 SVC-S3-TD2
```



```
 Done
> bind lb vserver  LBVS-TD2 SVC-S3-TD2
 Done
<!--NeedCopy-->
```

Procedimientos de GUI

Para crear un dominio de tráfico basado en MAC virtual mediante la GUI:

1. Vaya a Sistema > Red > Interfaces.
2. En el panel de detalles, haga clic en Agregar.
3. En la página Crear dominio de tráfico, establezca los siguientes parámetros:
   - ID de dominio de tráfico*
   - Habilitar Mac
4. Haga clic en Crear.

Para configurar una dirección SNIP mediante la GUI:

1. Vaya a Sistema > Red > IPs > IPv4
2. Navegue a Red > IPs > IPv4
3. En el panel de detalles, haga clic en Agregar
4. En la página Crear IP, establezca los siguientes parámetros. Para obtener una descripción de un parámetro, coloque el cursor del cursor sobre el campo correspondiente.
   - Dirección IP
   - Máscara de red
   - Tipo de IP
   - Id. de dominio de tráfico
5. Haga clic en Crear.

Para crear un servicio mediante la GUI:

1. Vaya a Administración de Tráfico > Equilibrio de carga > Servicios.
2. En el panel de detalles, haga clic en Agregar.
3. En la página Configuración básica, establezca los siguientes parámetros. Para obtener una descripción de un parámetro, coloque el cursor del cursor sobre el campo correspondiente.
   - Nombre del servicio
   - Servidor
   - Protocolo
   - Port
   - Id. de dominio de tráfico
4. Haga clic en Continuar y haga clic en Listo.
5. Repita los pasos 2-4 para crear otro servicio.
6. Haga clic en Cerrar.

Para crear un servidor virtual de equilibrio de carga y enlazar servicios con él mediante la GUI:

1. Vaya a Administración del tráfico > Equilibrio de carga > Servidores virtuales.
2. En el panel Servidores virtuales de equilibrio de carga, haga clic en Agregar.
3. En el cuadro de diálogo Crear servidores virtuales (equilibrio de carga), defina los siguientes parámetros. Para obtener una descripción de un parámetro, coloque el cursor del cursor sobre el campo correspondiente.
    - Nombre
    - Dirección IP
    - Protocolo
    - Port
    - Id. de dominio de tráfico
4. Haga clic en Continuar, en el Panel de servicios, haga clic en >.
5. En la página Servicio, haga clic en Insertar y, a continuación, active la casilla de verificación de los servicios que quiere vincular al servidor virtual.
6. Haga clic en Continuar y haga clic en Listo.
7. Repita los pasos 2-5 para crear otro servidor virtual

VXLAN

August 20, 2021

Los dispositivos Citrix ADC admiten redes de área local virtual extensible (VXLAN). Una VXLAN superpone redes de capa 2 en una infraestructura de capa 3 encapsulando tramas de capa 2 en paquetes UDP. Cada red de superposición se conoce como segmento VXLAN y se identifica mediante un identificador único de 24 bits denominado VXLAN Network Identifier (VNI). Solo los dispositivos de red dentro de la misma VXLAN pueden comunicarse entre sí.

Las VXLAN proporcionan los mismos servicios de red Ethernet de Capa 2 que las VLAN, pero con mayor extensibilidad y flexibilidad. Las dos ventajas principales del uso de VXLAN son las siguientes:

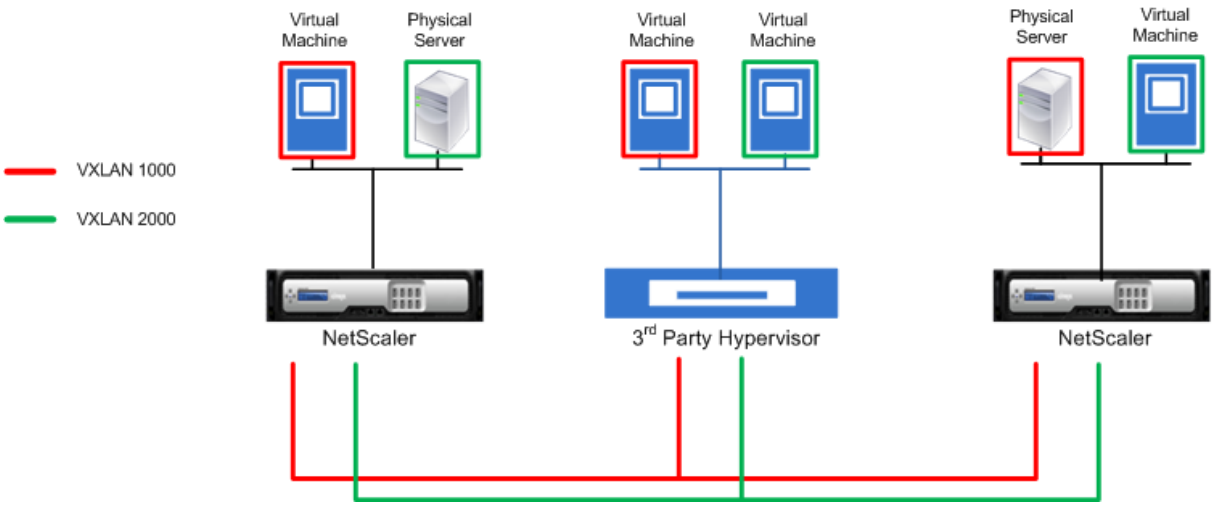
- **Mayor escalabilidad.** La virtualización de servidores y las arquitecturas de cloud computing han aumentado considerablemente la demanda de redes aisladas de capa 2 en un centro de datos. La especificación de VLAN utiliza un ID de VLAN de 12 bits para identificar una red de capa 2, de modo que no puede escalar más allá de 4094 VLAN. Ese número puede ser inadecuado cuando el requisito es para miles de redes aisladas de Capa 2. El VNI de 24 bits aloja hasta 16 millones de segmentos VXLAN en el mismo dominio administrativo.
- **Mayor flexibilidad.** Debido a que VXLAN lleva tramas de datos de Capa 2 a través de paquetes de Capa 3, las VXLAN extienden las redes L2 a través de diferentes partes de un centro de datos y a través de centros de datos separados geográficamente. Las aplicaciones que están alojadas

en diferentes partes de un centro de datos y en diferentes centros de datos pero que forman parte de la misma VXLAN aparecen como una red contigua.

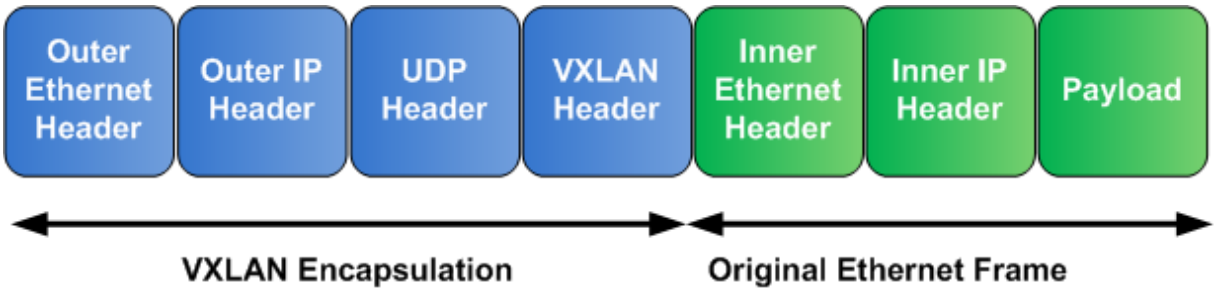
Cómo funcionan las VXLAN

Los segmentos VXLAN se crean entre los puntos finales del túnel VXLAN (VTEP). Los VTEP admiten el protocolo VXLAN y realizan encapsulación y descapsulación VXLAN. Puede pensar en un segmento VXLAN como un túnel entre dos VTEP, donde un VTEP encapsula una trama Layer2 con un encabezado UDP y un encabezado IP y lo envía a través del túnel. El otro VTEP recibe y descapsulará el paquete para obtener el marco de Capa 2. Un Citrix ADC es un ejemplo de VTEP. Otros ejemplos son hipervisores de terceros, máquinas virtuales compatibles con VXLAN y conmutadores compatibles con VXLAN.

La siguiente ilustración muestra máquinas virtuales y servidores físicos conectados a través de túneles VXLAN.



En la siguiente ilustración se muestra el formato de un paquete VXLAN.



Las VXLAN en un dispositivo Citrix ADC utilizan un mecanismo de capa 2 para enviar tramas de difusión, multidifusión y unidifusión desconocidas. Una VXLAN admite los siguientes modos para enviar estas tramas L2.

- **Modo de unidifusión**: En este modo, se especifican las direcciones IP de los VTEP mientras

se configura una VXLAN en un dispositivo Citrix ADC. El Citrix ADC envía tramas de difusión, multidifusión y unidifusión desconocidas a través de la capa 3 a todos los VTEP de esta VXLAN.

- **Modo de multidifusión**: En este modo, se especifica una dirección IP de grupo de multidifusión mientras se configura una VXLAN en un dispositivo Citrix ADC. Los ADC de Citrix no admiten el protocolo de protocolo de administración de grupos de Internet (IGMP). Los ADC de Citrix dependen del enrutador ascendente para unirse a un grupo de multidifusión, que comparte una dirección IP común de grupo de multidifusión. El Citrix ADC envía tramas de difusión, multidifusión y unidifusión desconocidas a través de la capa 3 a la dirección IP del grupo de multidifusión de esta VXLAN.

Al igual que una tabla de puente de capa 2, los ADC de Citrix mantienen tablas de asignación de VXLAN basadas en el encabezado interno y externo de los paquetes VXLAN recibidos. Esta tabla asigna direcciones MAC de host remoto a direcciones IP VTEP para una VXLAN determinada. El Citrix ADC utiliza la tabla de asignación de VXLAN para buscar la dirección MAC de destino de una trama de capa 2. Si hay una entrada para esta dirección MAC en la tabla VXLAN, Citrix ADC envía la trama de Capa 2 sobre Capa 3, mediante el protocolo VXLAN, a la dirección IP VTEP asignada especificada en la entrada de asignación para una VXLAN.

Dado que las VXLAN funcionan de manera similar a las VLAN, la mayoría de las funciones de Citrix ADC que admiten VLAN como parámetro de clasificación admiten VXLAN. Estas funciones incluyen un parámetro VXLAN opcional, que especifica el VNI VXLAN.

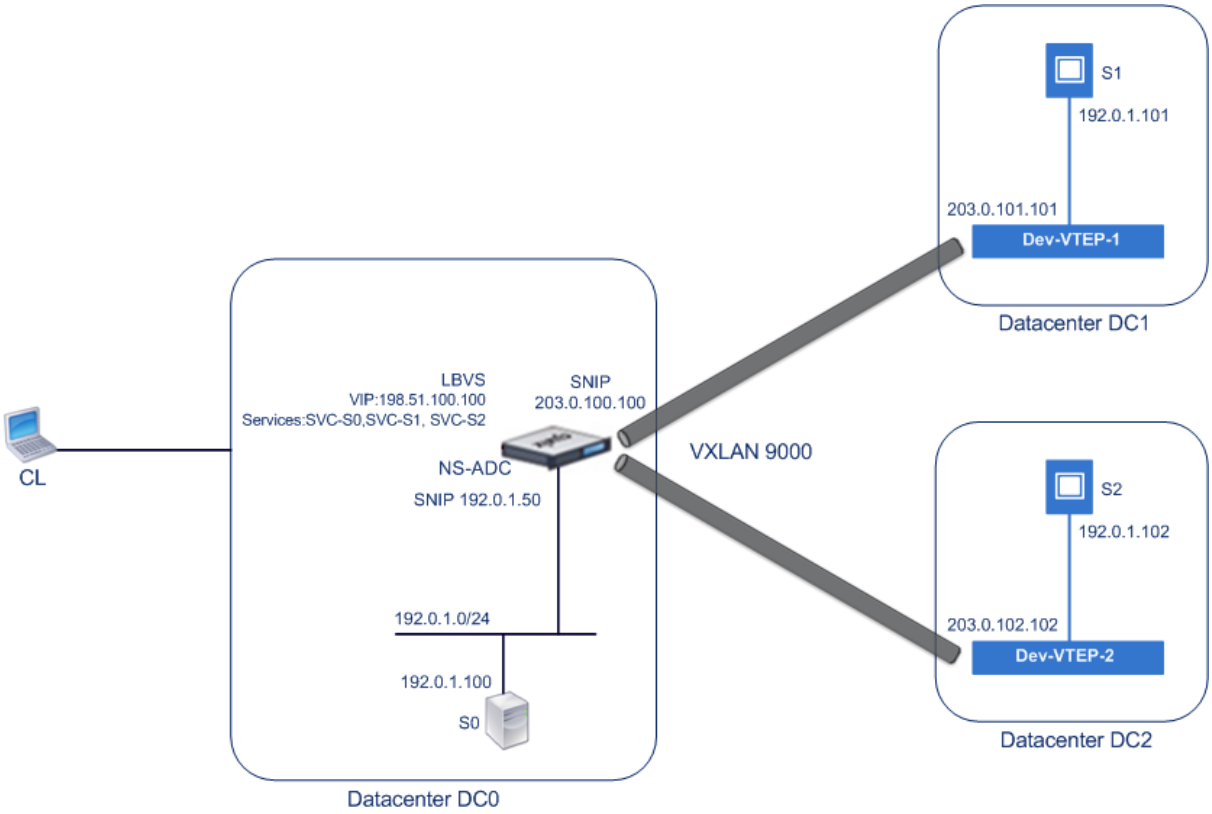
En una configuración de alta disponibilidad (HA), la configuración de VXLAN se propaga o sincroniza con el nodo secundario.

Caso de uso de VXLAN: Equilibrio de carga entre centros de datos

Para comprender la funcionalidad VXLAN de un dispositivo Citrix ADC, considere un ejemplo en el que Example Corp aloja un sitio en www.example.com. Para garantizar la disponibilidad de las aplicaciones, el sitio está alojado en tres servidores, S0, S1 y S2. Para equilibrar estos servidores se utiliza un servidor virtual de equilibrio de carga, LBVS, en Citrix ADC NS-ADC. S0, S1 y S2 residen en centros de datos DC0, DC1 y DC2, respectivamente. En DC0, el servidor S0 está conectado a NS-ADC.

S0 es un servidor físico, y S1 y S2 son máquinas virtuales (VM). S1 se ejecuta en el dispositivo host de virtualización Dev-VTEP-1 en el centro de datos DC1, y S2 se ejecuta en el dispositivo host Dev-VTEP-2 en DC2. NS-ADC, Dev-VTEP-1 y Dev-VTEP-2 admiten el protocolo VXLAN.

S0, S1 y S2 forman parte de la misma subred privada, 192.0.1.0/24. S0, S1 y S2 forman parte de un dominio de difusión común, VXLAN 9000 está configurado en NS-ADC, Dev-VTEP-1 y Dev-VTEP-2. Los servidores S1 y S2 forman parte de VXLAN9000 en Dev-VTEP-1 y Dev-VTEP-2, respectivamente.



En la tabla siguiente se enumeran los ajustes utilizados en este ejemplo:
configuración de VXLAN.

Los servicios SVC-S0, SVC-S1 y SVC-S2 en NS-ADC representan S0, S1 y S2. Tan pronto como se configuran estos servicios, NS-ADC emite solicitudes ARP para S0, S1 y S2 para resolver la asignación de IP a Mac. Estas solicitudes ARP también se envían a través de VXLAN 9000 a Dev-VTEP-1 y Dev-VTEP-2.

A continuación se presenta el flujo de tráfico para resolver la solicitud ARP para S2:

1. NS-ADC transmite una solicitud ARP para S2 para resolver la asignación de IP a Mac. Este paquete tiene:
   - Dirección IP de origen = Dirección IP de subred SNIP para servidores (192.0.1.50)
   - Dirección MAC de origen = dirección MAC de la interfaz del NS-ADC desde la que se envía el paquete = NS-MAC-1
2. NS-ADC prepara el paquete ARP para ser enviado a través de la VXLAN 9000 encapsulando el paquete con los siguientes encabezados:
   - Encabezado VXLAN con un ID (VNI) de 9000
   - Encabezado UDP estándar, suma de comprobación UDP establecida en 0×0000 y puerto de destino establecido en 4789.
3. NS-ADC envía el paquete encapsulado resultante a Dev-VTEP-1 y Dev-VTEP-2 en VXLAN-9000. El paquete encapsulado tiene:
   - Dirección IP de origen = SNIP-VTEP-0 (203.0.100.100).

4. Dev-VTEP-2 recibe el paquete UDP y descapsulará el encabezado UDP, desde el que Dev-VTEP-2 aprende que el paquete es un paquete relacionado con VXLAN. A continuación, dev-VTEP-2 descapsulará el encabezado VXLAN y aprenderá el ID de VXLAN del paquete. El paquete resultante es el paquete de solicitud ARP para S2, que es el mismo que en el paso 1.
5. Desde el encabezado interno y externo del paquete VXLAN, Dev-VTEP-2 realiza una entrada en su tabla de asignación VXLAN que muestra la asignación de direcciones MAC (NS-MAC-1) y SNIP-VTEP-0 (203.0.100.100) para VXLAN9000.
6. Dev-VTEP-2 envía el paquete ARP a S2. El paquete de respuesta de S2 alcanza Dev-VTEP-2. Dev-VTEP-2 realiza una búsqueda en su tabla de asignación VXLAN y obtiene una coincidencia para la dirección MAC de destino NS-MAC-1. El Dev-VTEP-2 ahora sabe que NS-MAC-1 es accesible a través de SNIP-VTEP-0 (203.0.100.100) a través de VXLAN 9000.
7. S2 responde con su dirección MAC (MAC-S2). El paquete de respuesta ARP tiene:
   - Dirección IP de destino = Dirección IP de subred SNIP para servidores (192.0.1.50)
   - Dirección MAC de destino = NS-MAC-1
8. El paquete de respuesta de S2 alcanza Dev-VTEP-2. Dev-VTEP-2 realiza una búsqueda en su tabla de asignación VXLAN y obtiene una coincidencia para la dirección MAC de destino NS-MAC-1. El Dev-VTEP-2 ahora sabe que NS-MAC-1 es accesible a través de SNIP-VTEP-0 (203.0.100.100) a través de VXLAN 9000. Dev-VTEP-2 encapsula la respuesta ARP con encabezados VXLAN y UDP, y envía el paquete resultante a SNIP-VTEP-0 (203.0.100.100) de NS-ADC.
9. NS-ADC al recibir el paquete, descapsulará el paquete mediante la eliminación de los encabezados VXLAN y UDP. El paquete resultante es la respuesta ARP de S2. NS-ADC actualiza la tabla de asignación VXLAN para la dirección MAC de S2 (MAC-S2) con la dirección IP de Dev-VTEP-2 (203.0.102.102) para VXLAN 9000. NS-ADC también actualiza la tabla ARP para la dirección IP de S2 (192.0.1.102) con la dirección MAC de S2 (MAC-S2).

A continuación se presenta el flujo de tráfico para el equilibrio de carga del servidor virtual LBVS en este ejemplo:

1. Cliente CL envía un paquete de solicitud a LBVS de NS-ADC. El paquete de solicitud tiene:
   - Dirección IP de origen = dirección IP del cliente CL (198.51.100.90)
   - Dirección IP de destino = dirección IP (VIP) de LBVS = 198.51.110.100
2. LBVS de NS-ADC recibe el paquete de solicitud y su algoritmo de equilibrio de carga selecciona el servidor S2 del centro de datos DC2.
3. NS-ADC procesa el paquete de solicitud, cambiando su dirección IP de destino a la dirección IP de S2 y su dirección IP de origen a una de las direcciones IP de subred (SNIP) configuradas en NS-ADC. El paquete de solicitud tiene:
   - Dirección IP de origen = Dirección IP de subred en NS-ADC= SNIP para servidores (192.0.1.50)
   - Dirección IP de destino = dirección IP de S2 (192.0.1.102)
4. NS-ADC encuentra una entrada de asignación VXLAN para S2 en su tabla de puente. Esta entrada indica que S2 es accesible a través de Dev-VTEP-2 a través de VXLAN 9000.

5. NS-ADC prepara el paquete para ser enviado a través de la VXLAN 9000 encapsulando el paquete con los siguientes encabezados:
    - Encabezado VXLAN con un ID (VNI) de 9000
    - Encabezado UDP estándar, suma de comprobación UDP establecida en 0×0000 y puerto de destino establecido en 4789.
6. NS-ADC envía el paquete encapsulado resultante a Dev-VTEP-2. El paquete de solicitud tiene:
    - Dirección IP de origen = dirección SNIP = SNIP-VTEP-0 (203.0.100.100)
    - Dirección IP de destino = dirección IP de Dev-VTEP-2 (203.0.102.102)
7. Dev-VTEP-2 recibe el paquete UDP y descapsulará el encabezado UDP, desde el que Dev-VTEP-2 aprende que el paquete es un paquete relacionado con VXLAN. A continuación, dev-VTEP-2 descapsulará el encabezado VXLAN y aprenderá el ID de VXLAN del paquete. El paquete resultante es el mismo paquete que en el paso 3.
8. Dev-VTEP-2 reenvía el paquete a S2.
9. S2 procesa el paquete de solicitud y envía la respuesta a la dirección SNIP de NS-ADC. El paquete de respuesta tiene:
    - Dirección IP de origen = dirección IP de S2 (192.0.1.102)
    - Dirección IP de destino = Dirección IP de subred en NS-ADC= SNIP para servidores (192.0.1.50)
10. Dev-VTEP-2 encapsula el paquete de respuesta de la misma manera que NS-ADC encapsuló el paquete de solicitud en los pasos 4 y 5. Dev-VTEP-2 envía el paquete UDP encapsulado a la dirección SNIP SNIP para servidores (192.0.1.50) de NS-ADC.
11. NS-ADC, al recibir el paquete UDP encapsulado, descapsulará el paquete quitando los encabezados UDP y VXLAN de la misma manera que Dev-VTEP-2 decapsuló el paquete en el paso 7. El paquete resultante es el mismo paquete de respuesta que en el paso 9.
12. A continuación, NS-ADC utiliza la tabla de sesión para el equilibrio de carga del servidor virtual LBVS y reenvía el paquete de respuesta al cliente CL. El paquete de respuesta tiene:
    - Dirección IP de origen = dirección IP del cliente CL (198.51.100.90)
    - Dirección IP de destino = dirección IP (VIP) de LBVS (198.51.110.100)

Puntos a considerar para configurar las VXLAN

Tenga en cuenta los siguientes puntos antes de configurar VXLAN en un dispositivo Citrix ADC:

- Se puede configurar un máximo de 2048 VXLAN en un dispositivo Citrix ADC.
- Las VXLAN no son compatibles con un clúster.
- Las direcciones IPv6 locales de vínculo no se pueden configurar para cada VXLAN.
- Los ADC de Citrix no admiten el protocolo de protocolo de administración de grupos de Internet (IGMP) para formar un grupo de multidifusión. Los ADC de Citrix confían en el protocolo IGMP de su router ascendente para unirse a un grupo de multidifusión, que comparten una dirección IP

común de grupo de multidifusión. Puede especificar una dirección IP de grupo de multidifusión al crear entradas de tabla de puente VXLAN, pero el grupo de multidifusión debe configurarse en el enrutador ascendente. El Citrix ADC envía tramas de difusión, multidifusión y unidifusión desconocidas a través de la capa 3 a la dirección IP del grupo de multidifusión de esta VXLAN. A continuación, el router ascendente reenvía el paquete a todos los VTEP que forman parte del grupo de multidifusión.

- La encapsulación VXLAN agrega una sobrecarga de 50 bytes a cada paquete:

  Encabezado Ethernet externo (14) + encabezado UDP (8) + encabezado IP (20) + encabezado VXLAN (8) = 50 bytes

  Para evitar la fragmentación y la degradación del rendimiento, debe ajustar la configuración de MTU de todos los dispositivos de red en una ruta VXLAN, incluidos los dispositivos VTEP de VXLAN, para controlar los 50 bytes de sobrecarga en los paquetes VXLAN.

  Importante: Las tramas gigantes no son compatibles con los dispositivos virtuales Citrix ADC VPX, los dispositivos Citrix ADC SDX y los dispositivos Citrix ADC MPX 15000/17000. Estos dispositivos admiten un tamaño de MTU de solo 1500 bytes y no se pueden ajustar para controlar la sobrecarga de 50 bytes de los paquetes VXLAN. El tráfico VXLAN puede estar fragmentado o sufrir una degradación del rendimiento, si uno de estos dispositivos se encuentra en la ruta VXLAN o actúa como un dispositivo VXLAN VTEP.
- En dispositivos Citrix ADC SDX, el filtrado de VLAN no funciona para paquetes VXLAN.
- No se puede establecer un valor de MTU en una VXLAN.
- No se pueden enlazar interfaces a una VXLAN.

Pasos de configuración

La configuración de una VXLAN en un dispositivo Citrix ADC consta de las siguientes tareas.

- **Agregue una entidad VXLAN**. Cree una entidad VXLAN identificada de forma única por un entero positivo, que también se denomina identificador de red VXLAN (VNI). En este paso, también puede especificar el puerto UDP de destino del VTEP remoto en el que se está ejecutando el protocolo VXLAN. De forma predeterminada, el parámetro de puerto UDP de destino se establece en 4789 para la entidad VXLAN. Esta configuración del puerto UDP debe coincidir con la configuración de todos los VTEP remotos para esta VXLAN. También puede enlazar VLAN a esta VXLAN. El tráfico (que incluye difusiones, multidifusión, unicast desconocidos) de todas las VLAN enlazadas se permite a través de esta VXLAN. Si no hay VLAN enlazadas a la VXLAN, Citrix ADC permite el tráfico de todas las VLAN, en esta VXLAN, que no formen parte de ninguna otra VXLAN.
- **Enlace la dirección IP VTEP local y a la entidad VXLAN**. Enlazar una de las direcciones SNIP configuradas a la VXLAN para enviar paquetes VXLAN salientes.

- **Agregue una entrada Bridgetable**. Agregue una entrada bridgetable que especifique el ID de VXLAN y la dirección IP de VTEP remota para la VXLAN que se va a crear.
- **(Opcional) Enlazar diferentes entidades de entidad a la VXLAN configurada**. Las VXLAN funcionan de manera similar a las VLAN, la mayoría de las funciones Citrix ADC que admiten VLAN como parámetro de clasificación también admiten VXLAN. Estas funciones incluyen un parámetro VXLAN opcional, que especifica el VNI VXLAN.
- **(Opcional) Muestra la tabla de asignación de VXLAN**. Muestra la tabla de asignación de VXLAN, que incluye entradas de asignación para la dirección MAC del host remoto a la dirección IP de VTEP para una VXLAN determinada. En otras palabras, una asignación de VXLAN indica que un host es accesible a través del VTEP en una VXLAN determinada. El Citrix ADC aprende las asignaciones VXLAN y actualiza su tabla de asignaciones desde los paquetes VXLAN que recibe. El Citrix ADC utiliza la tabla de asignación de VXLAN para buscar la dirección MAC de destino de un marco de capa 2. Si hay una entrada para esta dirección MAC en la tabla VXLAN, Citrix ADC envía la trama de Capa 2 sobre Capa 3, mediante el protocolo VXLAN, a la dirección IP VTEP asignada especificada en la entrada de asignación para una VXLAN.

Procedimientos CLI

Para agregar una entidad VXLAN mediante CLI:

En el símbolo del sistema, escriba:

- **add vxlan** <id>
- **show vxlan**<id>

Para enlazar la dirección IP de VTEP local a la VXLAN mediante CLI:

En el símbolo del sistema, escriba:

- **bind vxlan** <id> -**srCIP** <IPaddress>
- **show vxlan** <id>

Para agregar un puente mediante CLI:

En el símbolo del sistema, escriba:

- **add bridgetable** -**mac** <macaddress> -**vxlan** <ID> -**vtep** <IPaddress>
- **show bridgetable**

Para mostrar la tabla de reenvío de VXLAN mediante la línea de comandos:

En el símbolo del sistema, escriba:

- **show bridgetable**

Procedimientos de GUI

Para agregar una entidad VXLAN y enlazar una dirección IP VTEP local mediante la GUI:

Vaya a **Sistema** > **Red** > **VXLAN** y agregue una nueva entidad VXLAN o modifique una entidad VXLAN existente.

Para agregar un bridgetable mediante la GUI:

Vaya a **Sistema** > **Red** > **Tabla de puente**, defina los siguientes parámetros al agregar o modificar una entrada de tabla de puente VXLAN:

- MAC
- VTEP
- ID DE VXLAN

Para mostrar la tabla de reenvío de VXLAN mediante la GUI:

Vaya a **Sistema** > **Red** > **Tabla de puente**.

```
Example
> add vxlan 9000
Done
> bind vxlan 9000 -srcIP 203.0.100.100

Done
> add bridgetable -mac 00:00:00:00:00:00 -vxlan 9000 -vtep
   203.0.101.101

Done
> add bridgetable -mac 00:00:00:00:00:00 -vxlan 9000 -vtep
   203.0.102.102

Done
```

Compatibilidad con protocolos de redirección dinámica IPv6 en VXLAN

El dispositivo Citrix ADC admite protocolos de redirección dinámica IPv6 para VXLAN. Puede configurar varios protocolos de redirección dinámica IPv6 (por ejemplo, OSPFv3, RIPng, BGP) en VXLAN desde la línea de comandos VTYSH. Se ha agregado una opción Protocolo de redirección dinámica IPv6 al conjunto de comandos de VXLAN para habilitar o inhabilitar protocolos de redirección dinámica IPv6 en una VXLAN. Después de habilitar los protocolos de redirección dinámica IPv6 en una VXLAN, es necesario que los procesos relacionados con los protocolos de redirección dinámica IPv6 se inicien en la VXLAN mediante la línea de comandos VTYSH.

Para habilitar los protocolos de redirección dinámica IPv6 en una VXLAN mediante la CLI:

- **add vxlan** <ID>[-**Redirección dinámica** IPv6(**HABILITADO** | **DESHABILITADO**)]
- **show vxlan**

```
In the following sample configuration, VXLAN-9000 is created and has
    IPv6 dynamic routing protocols enabled on it. Then, using the VTYSH
    command line, process for the IPv6 OSPF protocol is started on the
    VXLAN.

> add vxlan 9000 -ipv6DynamicRouting ENABLED

Done
> bind vxlan 9000 -srcIP 203.0.100.100

Done
> add bridgetable -mac 00:00:00:00:00:00 -vxlan 9000 -vtep
    203.0.101.101

Done
> VTYSH
NS# configure terminal
NS(config)# ns IPv6-routing
NS(config)# interface VXLAN-9000
NS(config-if)# ipv6 router OSPF area 3
```

Ampliación de VLAN desde varias empresas a una nube mediante Mapas VXLAN-VLAN

Los túneles de CloudBridge Connector se utilizan para extender la VLAN de una empresa a una nube. Las VLAN ampliadas desde varias empresas pueden tener identificadores de VLAN superpuestos. Puede aislar las VLAN de cada empresa, asignándolas a una VXLAN única en la nube. En un dispositivo Citrix ADC, que es el punto final del conector CloudBridge en la nube, puede configurar un mapa VXLAN-VLAN que vincule las VLAN de una empresa a una VXLAN única en la nube. Las VXLAN admiten el etiquetado VLAN para extender varias VLAN de una empresa desde CloudBridge Connector a la misma VXLAN.

Realice las siguientes tareas para extender las VLAN de varias empresas a una nube:

1. Cree un mapa VXLAN-VLAN.
2. Enlazar el mapa VXLAN-VLAN a una configuración de túnel de CloudBridge Connector basada en puentes de red o PBR en el dispositivo Citrix ADC en la nube.
3. (Opcional) Habilite el etiquetado de VLAN en una configuración de VXLAN.

Procedimientos CLI

Para agregar un mapa VXLAN-VLAN mediante la CLI:

- **add vxlanVlanMap** <name>
- **show vxlanVlanMap** <name>

Para enlazar una VXLAN y VLAN a un mapa VXLAN-VLAN mediante la CLI:

- **bind vxlanVlanMap** <name>[-**vxlan** \ -**vlan** <int [-int]<positive_integer»…]
- **show vxlanVlanMap** <name>

Para enlazar un mapa VXLAN-VLAN a un túnel de CloudBridge Connector basado en un puente de red mediante la CLI:

En el símbolo del sistema, escriba uno de los siguientes conjuntos de comandos.

si se agrega un nuevo puente de red:

- **add netbridge** <name [-**vxlanVLANMap**]<string>
- **show netbridge** <name>

si se reconfigura un puente de red existente:

- **set netbridge** <name> [-**vxlanVLANMap**]
- **show netbridge** <name>

Para enlazar un mapa VXLAN-VLAN a un túnel de CloudBridge Connector basado en PBR mediante la CLI:

En el símbolo del sistema, escriba uno de los siguientes conjuntos de comandos.

si se agrega un nuevo PBR:

- **add pbr** <name>**ALLOW** (-**IPtunnel** <ipTunnelName>[-**vxlanVLANMap**]<name>)
- **show pbr** <name>

si se reconfigura un PBR existente:

- **set pbr** <name> **ALLOW** (-**ipTunnel** <ipTunnelName> [-**vxlanVLANMap**])
- **show pbr** <name>

Para incluir etiquetas VLAN en paquetes relacionados con una VXLAN mediante la CLI:

En el símbolo del sistema, escriba uno de los siguientes conjuntos de comandos.

si agrega una nueva VXLAN:

- **add vxlan** <vnid> -**vlanTag** (**ENABLED** | **DISABLED**)
- **show vxlan** <vnid>

si se reconfigura una VXLAN existente:

- **set vxlan** <vnid> -**vlanTag** (**ENABLED** | **DISABLED**)

- **show vxlan** <vnid>

Procedimientos de GUI

Para agregar un mapa VXLAN-VLAN mediante la GUI:

Vaya a **Sistema** > **Red** > Mapa de **VLAN de VXLAN, agregue un mapa** de VXLAN VLAN.

Para enlazar un mapa VXLAN-VLAN a un túnel de CloudBridge Connector basado en netbridge mediante la interfaz gráfica de usuario:

Vaya a **System** > **CloudBridge Connector** > **Network Bridge**, seleccione un mapa VXLAN-VLAN de la lista desplegable **VXLAN VLAN** mientras agrega un nuevo puente de red o reconfigura un puente de red existente.

Para enlazar un mapa VXLAN-VLAN a un túnel de CloudBridge Connector basado en PBR mediante la interfaz gráfica de usuario:

Vaya a **Sistema** > **Red** > **PBRs**, en la ficha Redirección basada en directivas (PBRs), seleccione un mapa **VXLAN-VLANde la lista desplegable VXLAN VLAN** mientras agrega un nuevo PBR o reconfigura un PBR existente.

Para incluir etiquetas VLAN en paquetes relacionados con una VXLAN mediante la GUI:

Vaya a **Sistema** > **Red** > **VXLAN**, habilite el **etiquetado de VLAN interna** mientras agrega una VXLAN nueva o reconfigure una VXLAN existente.

```
> add vxlanVlanMap VXLANVLAN-DC1

Done

> bind vxlanvlanmap VXLANVLAN-DC1 -vxlan 3000 -vlan 3

Done

> bind vxlanvlanmap VXLANVLAN-DC1 -vxlan 3500 -vlan 4

Done

>add vxlanVlanMap VXLANVLAN-DC2

Done

> bind vxlanvlanmap VXLANVLAN-DC1 -vxlan 8000 -vlan 3 4

```



```
19 Done
20
21 > set pbr PBR-CBC-DC-1-CLOUD ALLOW  -ipTunnel  CBC-DC-1-CLOUD -
      vxlanVlanMap VXLANVLAN-DC1
22
23 Done
24
25 > set pbr PBR-CBC-DC-2-CLOUD ALLOW  -ipTunnel  CBC-DC-2-CLOUD -
      vxlanVlanMap VXLANVLAN-DC2
26
27 Done
```

Túneles de GENEVE

July 27, 2022

Un dispositivo Citrix ADC admite el protocolo Generic Network Virtualization Encapsulation (GENEVE) como se define en RFC 8926.
La virtualización de servidores y la arquitectura de computación en la nube han aumentado la demanda de redes de capa 2 aisladas en un centro de datos.

El límite de VLAN de 4094 ha demostrado ser inadecuado y se introdujeron protocolos de encapsulación como VXLAN y NVGRE para superar esta limitación. Estos protocolos difieren principalmente en la implementación del plano de control. El protocolo GENEVE no define las especificaciones para el plano de control. El protocolo deja que la implementación defina las especificaciones del plano de control.

El protocolo GENEVE es una tecnología de encapsulación que tiene como objetivo crear redes superpuestas de capa 2 sobre la infraestructura de capa 3 encapsulando tramas de capa 2 en paquetes UDP.

Un identificador único de 24 bits denominado VNID identifica cada VLAN. Solo dentro del mismo ID de segmento (VNID) pueden comunicarse entre sí. Un dispositivo Citrix ADC admite la encapsulación Geneve en el puerto UDP 6081.

Hay dos tipos de túneles de GENEVE que se pueden crear:

- Los túneles pueden extender una VLAN existente en modo L2 o L3. En el modo L2, la conexión en puente se produce entre la VLAN y el túnel y las entradas se actualizan en la tabla de puentes.

  En el modo L3, el ARP proxy entra en vigor para aprender la dirección MAC y la información del túnel de la dirección cliente/servidor. La tabla ARP incluye la información de túnel y MAC correspondiente.

- El túnel de GENEVE puede funcionar con diferentes VLAN en modo L3 mediante el uso de rutas basadas en directivas (PBR).
  Cuando se debe enviar un paquete a un host al que se puede acceder en un segmento de túnel de GENEVE, el dispositivo Citrix ADC encapsula el paquete en un encabezado de túnel de GENEVE y lo envía al extremo del túnel.

Citrix ADC también puede actuar como un dispositivo de punto final de túnel. Un punto final de túnel origina y termina los túneles de GENEVE. Cuando el modo de capa 2 está ACTIVADO, el dispositivo Citrix ADC actúa como un extremo de túnel y conecta paquetes entre las VLAN y los túneles de GENEVE. El Citrix ADC aprende el VNID y el extremo del túnel en el que se puede acceder a una dirección MAC. A continuación, almacena esta información en la tabla de conexión en puente.

El túnel de GENEVE es compatible con las particiones de administración de Citrix ADC, las configuraciones de alta disponibilidad de Citrix ADC y las configuraciones de clúster de Citrix ADC.

En una configuración de alta disponibilidad, una configuración de túnel de GENEVE se propaga o sincroniza con el nodo secundario. En una configuración de clúster, la configuración del túnel de GENEVE (en bandas) es idéntica y está presente en todos los nodos del clúster.

Configuración de túneles de GENEVE

La configuración de un túnel de GENEVE en un dispositivo Citrix ADC consta de las siguientes tareas:

- Agregar un túnel IP con protocolo
- Agregar un puente de red
- vincular el túnel de GENEVE al puente de la red

Para agregar un túnel IP con el protocolo GENEVE mediante la CLI:

En el símbolo del sistema, escriba:

- **add iptunnel** <name> <remote> <remoteSubnetMask> <local> -**protocol** <Geneve> -**destPort** <port> -**tosInherit** (**ENABLED** | **DISABLED**) -**vlanTagging** (**ENABLED** | **DISABLED**) -**vnid**
- **show iptunnel**

Para agregar un puente de red mediante la CLI:

En el símbolo del sistema, escriba:

- **add netbridge** <nombre>
- **show netbridge**

Para vincular el túnel de GENEVE al puente de la red mediante la CLI:

En el símbolo del sistema, escriba:

- **bind netbridge** <name> -**vlan** <Vlan ID> -**tunnel** <tunnel name>
- **show netbridge**

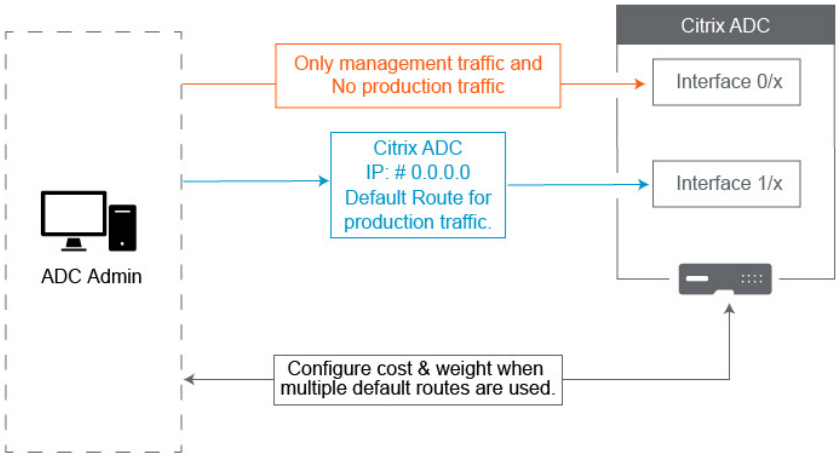
Prácticas recomendadas para configuraciones de red

August 20, 2021

En las siguientes secciones se describen algunas prácticas recomendadas para configurar funciones de red en un dispositivo Citrix ADC.

Redirección y rutas predeterminadas

Las siguientes son algunas de las prácticas recomendadas para configurar las funciones de la capa 3 en un dispositivo Citrix ADC.



- **La interfaz `0/x` en un dispositivo Citrix ADC o Citrix SDX no debe utilizarse para el tráfico de producción**. En un MPX o SDX, las interfaces llamadas `0/x` se refieren a las interfaces de administración. Esto no significa que deba usar estas interfaces para Administración. Lo que significa es que estas interfaces NO están diseñadas para el tráfico de producción. No tienen los búferes de hardware y la optimización necesarios para lograr un rendimiento sostenido de 1 Gbps. Por lo tanto, si su ruta predeterminada está en la misma subred que su NSIP, debe cambiar la ruta predeterminada o utilizar una interfaz `1/x` para su red de administración, ya que las interfaces `1/x` están totalmente optimizadas para un tráfico de producción de 1 Gbps.

  > **Nota**:
  >
  > Esto no se aplica a un dispositivo Citrix ADC VPX.

  - **Opción 1**. No conectar a interfaces `0/x`: Desconecte el cable de la interfaz `0/1`. NetScaler escucha el NSIP en las otras interfaces. (NOTA: Esta no es una opción para SDX, ya que SVM y XenServer solo pueden hablar con interfaces `0/x`)

  - **Opción 2**. Cambie la ruta predeterminada a una interfaz diferente como se detalla en la siguiente sección.

- **La puerta de enlace predeterminada (ruta 0.0.0.0) debe estar en una red de producción y no en ninguna interfaz `0/x`**. Al configurar por primera vez un NetScaler, le pide la dirección NSIP, la máscara de subred y la puerta de enlace. El problema que esto crea para los administradores es que acaban de configurar su ruta predeterminada para estar en su red de administración mediante la interfaz 0/1.

  - Para comprobar cuáles son sus rutas, ejecute en CLI `show route` y su puerta de enlace predeterminada es la IP en la línea donde la red y la máscara de red son 0.0.0.0. Aquí hay un ejemplo donde la puerta de enlace está en la línea 1:

```
1  > sh route
2          Network          Netmask          Gateway/OwnedIP
               State   Traffic Domain  Type
3          -------          -------          ---------------
               -----   --------------  ----
4  1)      0.0.0.0          0.0.0.0          10.25.213.65     UP
            0               STATIC
5  2)      127.0.0.0        255.0.0.0        127.0.0.1        UP
            0               PERMANENT
6  3)      10.25.213.64     255.255.255.192  10.25.213.68     UP
            0               DIRECT
7  4)      172.16.0.0       255.255.255.0    172.16.0.1       UP
            0               DIRECT
8
9  <!--NeedCopy-->
```

  - Para comprobar la interfaz y la VLAN utilizadas para la puerta de enlace predeterminada, compruebe la tabla ARP mediante `sh arp` en CLI. También puede buscar la IP específica mediante `show arp | grep 10.25.213.65`. A continuación se muestra un ejemplo en el que la puerta de enlace 10.25.213.65 utiliza la interfaz 1/1 y VLAN 1:

```
1  > sh arp
2          IP               MAC                Iface VLAN
               Origin     TTL     Traffic Domain
3          --               ---                ----- ----
               ------     ---     --------------
4  1)      127.0.0.1        02:00:18:a4:00:1e  LO/1  1
      PERMANENT  N/A    0
```



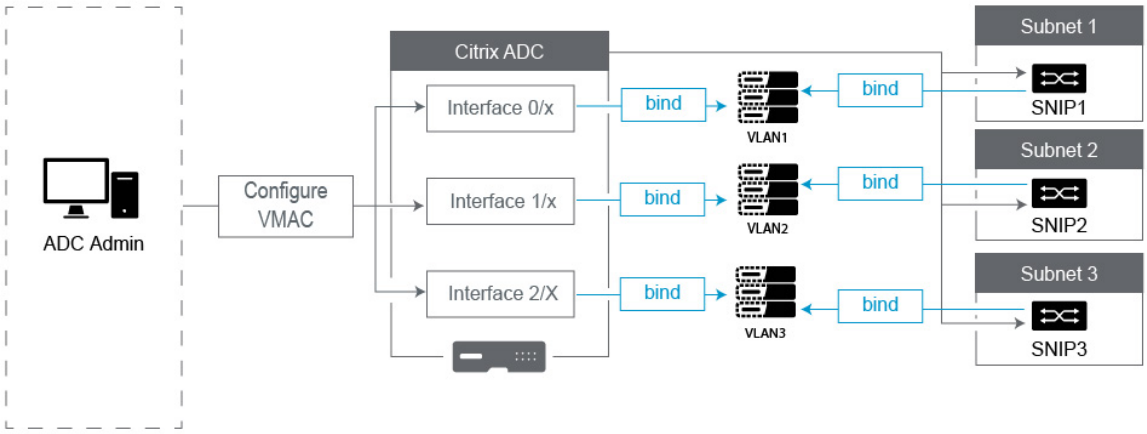
```
2)      10.25.213.70     02:00:0f:46:00:28  1/1   1
    DYNAMIC    967    0
3)      10.25.213.68     02:00:18:a4:00:1e  LO/1  1
    PERMANENT  N/A    0
4)      10.25.213.67     02:00:0f:46:00:28  1/1   1
    DYNAMIC    641    0
5)      10.25.213.65     00:08:e3:ff:fd:90  1/1   1
    DYNAMIC    483    0
<!--NeedCopy-->
```

- Cambie la ruta predeterminada para utilizar una puerta de enlace en la subred de producción y la interfaz. Supongamos que la red de administración es 10.0.0.0/24 con Gateway 10.0.0.1 y la red de producción es 10.1.1.0/24 con Gateway 10.1.1.1. Configure su configuración de esta manera:
  - SNIP: (Acceso de administración inhabilitado) 10.1.1.2
  - NSIP: (Acceso de administración habilitado) 10.0.0.2
  - Ruta predeterminada: 0.0.0.0 0.0.0.0 10.1.1.1 (Sistema > Red > Rutas). Esto utiliza un enrutador en la red SNIP en lugar de la red NSIP.

    > **Nota**:
    >
    > Cambiar la Gateway predeterminada podría interrumpir el tráfico de administración a menos que configure rutas estáticas, una ruta basada en directivas o habilite el reenvío basado en MAC.

Interfaces, canales y VLAN

Las siguientes son algunas de las prácticas recomendadas para configurar las funciones de la capa 2 en un dispositivo Citrix ADC.



- **No conecte múltiples interfaz/canales a la misma VLAN, incluida la VLAN 1**:
  - Si no configura correctamente las VLAN, puede provocar una redirección de paquetes inesperado en la red y un bucle de capa 2 en cualquier momento en que haya más de una interfaz activa con la misma VLAN (nativa o etiquetada).
  - De forma predeterminada, todas las interfaces y canales están en VLAN 1 nativa. Esto crea dos posibles problemas:
    * NetScaler cree que todo el tráfico recibido está en la misma red, por lo que utiliza cualquier interfaz para enviar el tráfico hacia fuera. Si tiene una VLAN nativa diferente en la interfaz en la que envió los datos, entonces el tráfico no se enrutará como esperaba.
    * Si NetScaler recibe paquetes de difusión en un puerto, puede retransmitir en otro puerto. Si ambos puertos de conmutación están en la misma VLAN, acaba de crear un bucle de capa 2.
  - Para eliminar una interfaz/canal de la VLAN 1:
    * Si no está usando VLAN nativas en el canal de puerto o interfaz del switch. Cambie la VLAN nativa en NetScaler Interface/Channel a un número de VLAN no utilizado, como 999. No debe usar el mismo número de VLAN no utilizado para varios canales o interfaces, ya que crea un bucle de capa 2.
    * Si está usando VLAN nativas en su canal de interface/puerto del switch. Cambie la VLAN nativa en NetScaler Interface/Channel para que coincida. Sin embargo, tenga cuidado de no tener múltiples interfaces o canales activos en la misma VLAN, ya que al hacerlo crea bucles de Capa 2.
    * No se puede quitar la VLAN nativa. En su lugar, puede cambiarlo o establecer TagAll para la interfaz o el canal. Si el puerto del switch no está configurado con una VLAN

nativa sin etiquetar, habilite el tagall en la interfaz para que se etiqueten los paquetes de latido de alta disponibilidad.

  - Para ver la VLAN nativa en una interfaz, ejecute `sh interface` en CLI. Esto también le informará si la interfaz está usando la opción TAGALL.

- **Enlazar una interfaz a su VLAN**: NetScaler, de forma predeterminada, no conecta una nueva VLAN a una interfaz. Esto significa que la VLAN no se utilizará hasta que la vincule a una interfaz. Cuando la nueva VLAN no está enlazada a una interfaz y esa VLAN está etiquetada, NetScaler elimina todo el tráfico entrante de esa VLAN. Además, no vincule la misma VLAN a más de una interfaz.

  - Enlazar subredes a las VLAN. NetScaler no funciona como un router típico. La mayoría de los enrutadores conectan IP a las interfaces. En un NetScaler, las IPs flotan en cualquier interfaz a menos que se configure lo contrario. Por lo tanto, cualquier subred que quiera asegurarse de que NetScaler envía a través de una VLAN específica, especialmente cuando NetScaler está iniciando ese tráfico, debe enlazar un SNIP dentro de esa subred a la VLAN.

  - Un argumento común que escuchamos en contra de esto es que solía funcionar bien y ahora no lo hace sin vincular la Subred a la VLAN. Esto ocurre a menudo porque NetScaler aprende qué VLAN enviar tráfico, pero esto puede llevar tiempo a medida que crea sus tablas ARP. Después de reiniciar o actualizar el firmware, a medida que comienza a crear las tablas ARP de nuevo, es posible que inicialmente aprenda y, por lo tanto, esté mediante una ruta diferente de la que quiera, como la ruta predeterminada. Lo mejor es indicarle qué ruta tomar vinculando el SNIP a la VLAN. Una vez que un SNIP está enlazado a una VLAN, toda la subred del SNIP se enlazará a la VLAN.

  - Asegúrese de que cada SNIP está enlazado a una VLAN (excepto en los casos en que tenga más de un SNIP en una subred, entonces solo debe enlazar uno) y que la VLAN, a su vez, esté enlazada a una sola interfaz o canal. A menudo también es mejor tener un SNIP en cada subred, pero eso no es necesario ya que la ruta más específica se utilizará para cualquier subred de destino que no tenga un SNIP.

- Para identificar la VLAN y la interfaz utilizadas por una subred:

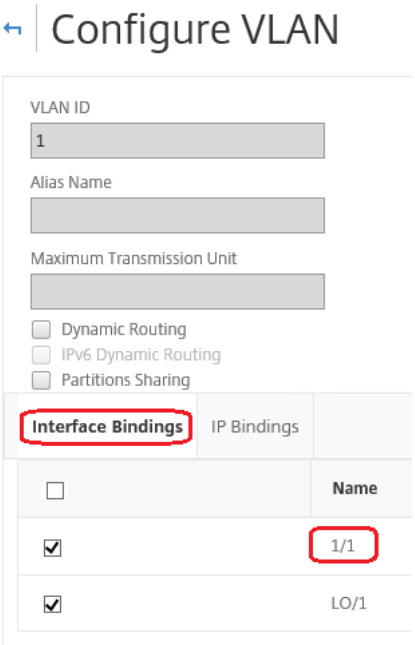
  1. Vaya a **Sistema>Red > VLAN**.
  2. Modifique cada VLAN configurada, a su vez, hasta que encuentre la dirección IP correcta como se explica en el siguiente paso.
  3. Haga clic en la ficha Enlaces IP para ver qué IP y, por lo tanto, qué subred está enlazada y, por lo tanto, está usando esta VLAN.
  4. Una vez que identifique la VLAN que tiene una IP enlazada a ella, donde esa IP se encuentra dentro de la subred de la ruta predeterminada, haga clic en los enlaces de interfaz. Se utilizará cada interfaz o canal vinculado a esta VLAN.

Ejemplo

Supongamos que la ruta predeterminada es `0.0.0.0 0.0.0.0 10.1.1.1`.

Supongamos que tiene dos SNIP de 10.0.0.5 y 10.1.1.69. Puesto que 10.1.1.69 está en la subred de la ruta predeterminada, esa es la que quiere buscar. En las siguientes capturas de pantalla, estamos revisando la VLAN 1 y vemos que la IP 10.1.1.69 está vinculada a esta VLAN, por lo que sabemos que estamos buscando la VLAN correcta.

Ahora haga clic en Enlaces de interfaz. En los enlaces de interfaz VLAN vemos que la interfaz `1/1` se utiliza para esta subred, y por lo tanto se utiliza para la ruta predeterminada.



> **NOTA**:
>
> Si no tiene ninguna IP enlazada a sus VLAN, entonces de forma predeterminada se enviará VLAN 1, por lo que en ese caso, mire qué interfaces están enlazadas a VLAN 1. Esto también significa que NetScaler no utilizará las VLAN configuradas para el tráfico que inicia a menos que vincule una IP a la nueva VLAN.

ARP gratuito

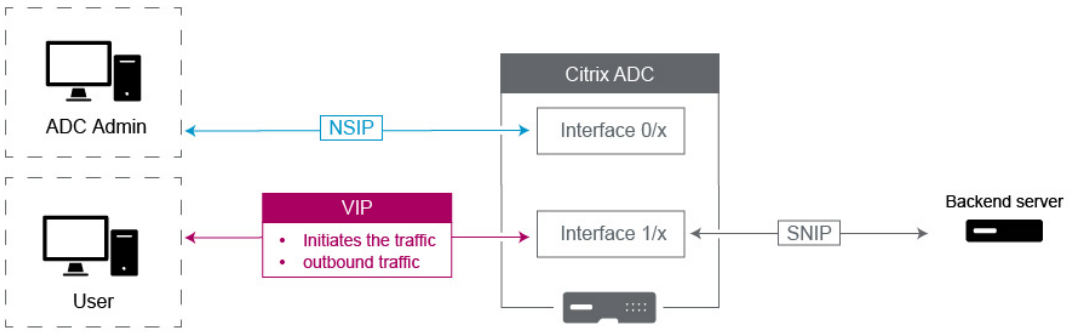
Si GARP no funciona, use VMAC: De forma predeterminada, NetScaler utiliza GARP para anunciar sus enlaces de direcciones IP a MAC a otros dispositivos de red. Normalmente, esto funciona sin problemas; sin embargo, a medida que crea más servicios en NetScaler, puede comenzar a experimentar problemas al realizar una conmutación por error en un par de HA. El problema más común es que los servicios permanecen inservidos en NetScaler en el que ha fallado debido a que algunos dispositivos de red no han actualizado sus tablas ARP con la nueva dirección MAC. Puede verificarlo fácilmente comprobando sus tablas ARP para ver si las direcciones MAC coinciden con las del NetScaler

Now-Primary. Cuando esto ocurre, es muy probable que algunos de sus dispositivos de red estén limitando el número de anuncios GARP que honran. En este caso es necesario configurar VMAC en todas sus interfaces y/o canales activos. Si espera tener una configuración grande en su NetScaler, puede ser mejor configurar VMAC para todas las interfaces y canales durante la implementación inicial.

> **NOTA**: No
>
> olvide configurar VMAC para la interfaz o el canal utilizado por su ruta predeterminada.

Direcciones IP propiedad de Citrix ADC

En esta sección se describen las prácticas recomendadas para configurar direcciones IP propiedad de Citrix ADC:



- **Citrix ADC IP (NSIP)**: Generalmente esta IP se utiliza para Administración porque es la única IP exclusiva de un NetScaler individual en un entorno de alta disponibilidad o clúster. También es importante tener en cuenta que LDAP, RADIUS y el tráfico de Monitor con scripts de usuario (como el monitor LDAP y el monitor StoreFront) se originará desde el NSIP y, por lo tanto, se enrutará a través de la VLAN y la interfaz a la que está enlazado NSIP (VLAN nativa predeterminada 1). Si necesita que el tráfico LDAP y RADIUS se genere desde el SNIP, cree un servidor virtual LB para los servidores back-end.
- **IP de subred (SNIP)**: Esta dirección IP se utiliza para iniciar la comunicación con los servidores back-end y siempre va a iniciar el tráfico. Dicho esto, puede ser el destino del tráfico en estos casos:
  - Se puede usar como dirección Gateway en otros dispositivos cuando se realiza la redirección de Capa 3 en NetScaler.
  - Cuando está habilitado, puede aceptar servicios de administración, como el acceso a la GUI, SSH y SNMP.

- **IP virtual (VIP)**: El VIP es único en el sentido de que nunca se usará para iniciar el tráfico saliente. Está destinado a recibir tráfico solamente. Una vez que recibe tráfico, responde y envía el tráfico saliente al cliente. En otras palabras, la dirección VIP no inicia el tráfico saliente.

Tenga en cuenta que esto también significa que no se utiliza como fuente para comunicarse con servidores back-end utilizados, por ejemplo, en un servidor virtual LB.

Configurar para obtener el origen del tráfico de datos de Citrix ADC FreeBSD desde una dirección de SNIP

August 20, 2021

Algunas funciones de datos de Citrix ADC se ejecutan en el sistema operativo FreeBSD subyacente en lugar de en el SO Citrix ADC. Por esta razón, estas funciones envían tráfico proveniente de la dirección IP (NSIP) de Citrix ADC en lugar de procederse de una dirección SNIP. No es deseable abastecer el tráfico de datos desde la dirección NSIP si la configuración tiene configuraciones para separar todo el tráfico de datos y administración.

Las siguientes funciones de datos de Citrix ADC se ejecutan en el sistema operativo FreeBSD subyacente y envían el tráfico procedente de la dirección IP (NSIP) de Citrix ADC:

- Monitores de scripts de equilibrio de carga
- Sincronización automática GSLB

Para resolver este problema, puede utilizar el parámetro global Layer-2: `useNetprofileBSDtraffic`. Cuando habilita este parámetro, las funciones de Citrix ADC envían tráfico procedente de una de las direcciones SNIP de un perfil de red asociado a la entidad.

Antes de comenzar

Antes de configurar el dispositivo Citrix ADC para que origen el tráfico relacionado con las funciones de Citrix ADC desde una dirección de SNIP, tenga en cuenta los siguientes puntos:

- Actualmente, el parámetro global de capa 2 solo `useNetprofileBSDtraffic` se admite para monitores de scripts de equilibrio de carga.

  Para configurar el dispositivo Citrix ADC para que origen el tráfico de sincronización automática GSLB desde una dirección SNIP, puede utilizar reglas de ACL extendidas y reglas RNAT como solución alternativa.

- La `useNetprofileBSDtraffic` compatibilidad con monitores de scripts de equilibrio de carga solo se aplica a los perfiles de red vinculados a los servicios relacionados. El

`useNetprofileBSDtraffic` soporte no es aplicable a los perfiles de red enlazados a los grupos de servicios relacionados.

En otras palabras, el dispositivo Citrix ADC no utiliza ninguna dirección de SNIP de los perfiles de red enlazados a los grupos de servicios para el abastecimiento de scripts de equilibrio de carga supervisa el tráfico.

- El `useNetprofileBSDtraffic` soporte no se aplica a los servicios SSL.

  En otras palabras, el dispositivo Citrix ADC no utiliza ninguna dirección SNIP de los perfiles de red vinculados a los servicios SSL para abastecimiento de equilibrio de carga, monitorea el tráfico.

Configurar el dispositivo Citrix ADC para que el script de origen supervise el tráfico desde una dirección de SNIP

La configuración del dispositivo Citrix ADC para que se ejecute scripts de origen supervisa el tráfico desde una dirección de SNIP consiste en las siguientes tareas:

- Habilite el parámetro global de capa 2 `useNetprofileBSDtraffic`.
- Cree un perfil de red y vincule al menos una dirección de SNIP.
- Enlazar el perfil de red a los servicios de equilibrio de carga que utilizan monitores con scripts.

Para habilitar el parámetro Layer-2 UseNetProfileBSDTraffic mediante la CLI:

En el símbolo del sistema, escriba:

- **set l2param** -**UseNetProfileBSDTraffic** (**HABILITADO**/DESHABILITADO**)
- **show l2param**

Para crear un perfil de red y enlazar direcciones SNIP a él mediante la CLI:

En el símbolo del sistema, escriba:

- **agregar NetProfile** <name> -**SRCIP** <string>
- **mostrar perfil de red**

Para enlazar un perfil de red a un servicio de equilibrio de carga mediante la CLI:

En el símbolo del sistema, escriba:

- **set service** <name> -**NetProfile** <string>
- **show service** <name>

Configuración de ejemplo

La siguiente configuración de ejemplo permite a un dispositivo Citrix ADC obtener scripts de origen supervisa el tráfico desde una dirección de SNIP. Un perfil de red NETPROFILE-1 está configurado con la

dirección SNIP 198.51.100.20 enlazada a él. Se crea un monitor de usuario/scripts USER-MONITOR-1 y está vinculado a un servicio de equilibrio de carga SERVICE-1. NETPROFILE-1 está vinculado a SERVICE-1. El dispositivo Citrix ADC obtiene todas los scripts supervisa los paquetes de USER-MONITOR-1 desde la dirección SNIP 198.51.100.20.

```
set l2param -useNetprofileBSDtraffic ENABLED

set netprofile NETPROFILE-1 -srcip 198.51.100.20

add lb monitor USER-MONITOR-1 USER -scriptName nsftp.pl -scriptArgs ”
    file=Index.png;user=nsroot;password=nsroot” -dispatcherIP 127.0.0.1
    -dispatcherPort 3013 -destIP 203.0.113.90 -destPort 21

bind service SERVICE-1 -monitorName USER-MONITOR-1

set service SERVICE-1 -netProfile NETPROFILE-1

<!--NeedCopy-->
```

Configurar el dispositivo Citrix ADC para obtener el tráfico de sincronización automática GSLB desde una dirección de SNIP

La configuración del dispositivo Citrix ADC para que origen el tráfico de sincronización automática de GSLB desde una dirección de SNIP consiste en las siguientes tareas de solución:

- **Cree una regla de ACL extendida**. Una regla de ACL extendida identifica los paquetes de sincronización automática de GSLB. Esta identificación se basa en la IP de origen y las direcciones IP de destino.
- **Aplique ACL**. La aplicación de ACL activa la regla ACL recién creada.
- **Cree una regla RNAT basada en ACL**. Una regla RNAT cambia la dirección IP de origen de estos paquetes de la dirección NSIP a una dirección SNIP.

> **Nota:**
>
> En una configuración de clúster o de alta disponibilidad, debe agregar reglas ACL y RNAT para todas las direcciones NSIP de la instalación.

Para crear una ACL extendida mediante la CLI:

En el símbolo del sistema, escriba:

- **add acl** <aclname> **ALLOW** -**srcIP** = <NSIP address> -**destIP** = <destination IP address of the packets>
- **show acl** <aclName>

Para aplicar ACL extendidas mediante la CLI:

En el símbolo del sistema, escriba:

- **apply acls**

Para crear una regla RNAT basada en ACL mediante la CLI:

En el símbolo del sistema, escriba:

- **add rnat** <name> <aclname>
- **bind rnat** <name> -**NATip** <SNIP address: Source IP address for the packets>
- **show rnat** <name>

Configuración de ejemplo

La siguiente configuración de ejemplo permite a un dispositivo Citrix ADC generar tráfico de sincronización automática GSLB desde una dirección de SNIP. ACL-2 identifica los paquetes de sincronización automática GSLB, que provienen de la dirección NSIP 192.0.1.20 y destinados a la dirección IP del sitio GSLB 203.0.113.20. RNAT-2 cambia la dirección IP de origen a la dirección SNIP 198.51.100.20 para estos paquetes identificados.

```
add acl ACL-2 ALLOW -srcIP = 192.0.1.20  -destIP = 203.0.113.20

apply acls

add rnat RNAT-2 ACL-2

bind rnat RNAT-2 -natIP 198.51.100.20
<!--NeedCopy-->
```

Equilibrio de carga prioritario

February 16, 2021

La función de equilibrio de carga de prioridad permite asignar un número de prioridad para cada uno de los servicios o grupos de servicios vinculados a un servidor virtual de equilibrio de carga de prioridad. Un servicio o un grupo de servicios con el número más bajo tiene la prioridad más alta. El tráfico de aplicaciones se distribuye solo a este servicio o a un grupo de servicios siempre y cuando este servicio o el grupo de servicios estén UP. El servicio o el grupo de servicios al que se asigna el siguiente número de prioridad se pone en funcionamiento solo cuando todos los servicios o miembros

del grupo de servicios con la prioridad más alta están DOWN. Sin embargo, cuando cualquiera de los servicios o un miembro del grupo de servicios con la prioridad más alta vuelve a estar disponible, el tráfico se redirige a ese servicio o al grupo de servicios.

Por ejemplo, considere los grupos de servicios SVG1, SVG2 y SVG3 que están enlazados a un servidor virtual de equilibrio de carga de prioridad. El número máximo de grupos prioritarios se establece en tres. Asigne la prioridad a cada grupo de la siguiente manera:

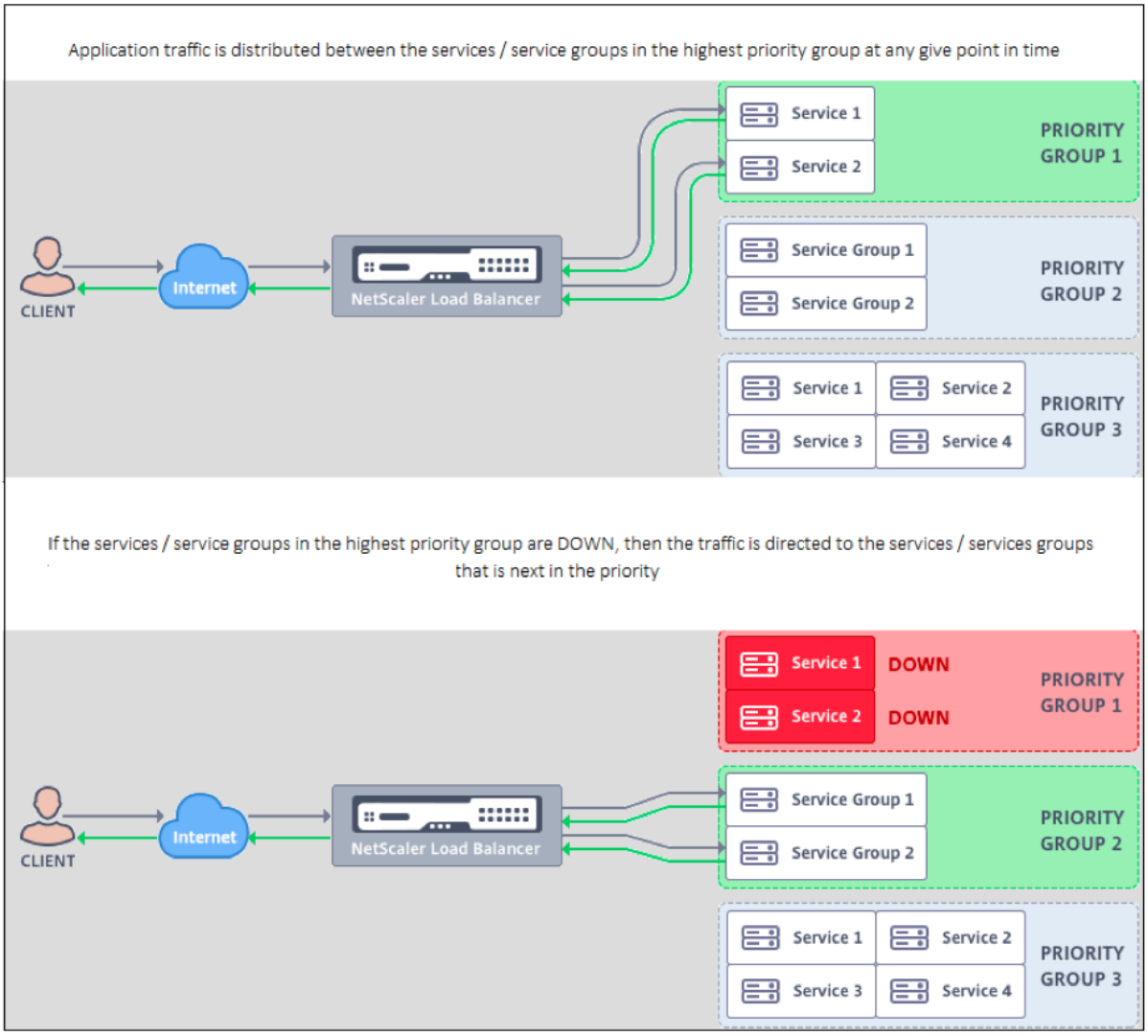
- SVG1: Prioridad 1
- SVG2: Prioridad 2
- SVG3: Prioridad 3

En este caso, el tráfico de la aplicación se dirige al grupo de servicios SVG1 porque a este grupo se le asigna el número de prioridad más bajo. Si todos los miembros de SVG1 están DOWN, el tráfico se distribuye al grupo de servicios SVG2 ya que a este grupo se le asigna el siguiente número de prioridad inferior. Si todos los miembros de SVG2 también están DOWN, el tráfico se distribuye a SVG3. Sin embargo, cuando cualquiera de los miembros de SVG1 es UP, el tráfico se redirige a SVG1 porque SVG1 tiene asignado el número más bajo y tiene la prioridad más alta.

Puede asignar una prioridad a un servicio o grupo de servicios para actualizar el servicio o grupo de servicios específico que tenga la prioridad más alta, siempre que sea necesario con un impacto mínimo o nulo en el tráfico de producción.

Además, si la actualización no se realiza correctamente, puede cambiar de forma segura al servicio o al grupo de servicios que es el siguiente en la prioridad, con un impacto mínimo o nulo en el tráfico de producción.

La siguiente ilustración ilustra la función de equilibrio de carga de prioridad.



Configurar el equilibrio de carga de prioridad

> **Nota**
>
> La configuración de equilibrio de carga de prioridad Citrix ADC solo se admite a través de la GUI. No puede configurar el equilibrio de carga de prioridad mediante la CLI.

1. Vaya a **Administración del tráfico** > **Equilibrio de carga de prioridad**> **Virtual*Servers** y especifique el protocolo para el servidor virtual, la dirección IP y el número de puerto del servidor virtual.
2. En el cuadro **Grupos de prioridad máxima**, escriba el número de servicios de prioridad o los grupos de servicios que se pueden enlazar a este servidor virtual. El valor predeterminado es 2 y la prioridad máxima que se puede establecer es 10. Este parámetro no se puede modificar después de configurarlo.

Nota:

Después de especificar el número máximo de grupos de prioridad y hacer clic en **Aceptar**, se crean un servidor virtual de cambio de contenido y un número “n” de servidores virtuales de equilibrio de carga de copia de seguridad. El alfabeto “n” representa el número máximo de grupos prioritarios.

Por ejemplo, si ha introducido el nombre del servidor virtual como vs1 y ha establecido el grupo de prioridad máxima como 5, se creará un servidor virtual de cambio de contenido con el nombre `_Pri.LB##vs1##MaxPri=5` y los siguientes 5 servidores virtuales de equilibrio de carga.

- `_Pri.LB##vs1##MaxPri=5_LB1`
- `_Pri.LB##vs1##MaxPri=5_LB2`
- `_Pri.LB##vs1##MaxPri=5_LB3`
- `_Pri.LB##vs1##MaxPri=5_LB4`
- `_Pri.LB##vs1##MaxPri=5_LB5`

3. Después de especificar el número máximo de grupos de prioridad y hacer clic en **Aceptar**, se le pedirá que elija los servicios o grupos de servicios que deben vincularse a este servidor virtual de cambio de contenido.

   - Para enlazar servicios al servidor virtual, haga clic en **Insertar** en la sección Servicios. A continuación, seleccione un servicio existente o cree un servicio y establezca la prioridad para este servicio. Además, establezca el número de prioridad al que debe enlazado este servicio.
   - Para enlazar grupos de servicios al servidor virtual, haga clic en **Insertar** en la sección Grupos de servicios. A continuación, seleccione un grupo de servicios existente o cree un grupo de servicios y establezca la prioridad para este grupo de servicios. Además, establezca el número de prioridad al que debe enlazado este grupo de servicios.

   Repita el paso 3, dependiendo del número máximo de grupos de prioridad que haya introducido.

   Nota:

   - El servicio o el grupo de servicios con la prioridad más alta está enlazado al servidor virtual de equilibrio de carga que representa la prioridad más alta.

   Por ejemplo, si ha asignado las prioridades 1 y 2 a los grupos de servicio `SG_App1 and SG_App2` respectivamente, entonces `SG_App1` está enlazado a `virtual server _Pri.LB##vs1##MaxPri=5_LB1 and SG_App2` está vinculado a `virtual server _Pri.LB##vs1##MaxPri=5_LB2` creado en el paso 2.

   - Para cambiar la prioridad del grupo de servicios o servicio, haga clic en el icono de edición de la página Servidor virtual de equilibrio de carga de prioridad y cambie la prioridad según sea necesario.

- No puede establecer explícitamente los métodos de equilibrio de carga y la persistencia para cada servidor virtual, ya que la configuración de todos los servidores virtuales de equilibrio de carga es idéntica.

4. En las secciones Configuración avanzada, complete la otra configuración que cumpla con sus requisitos.

> **Importante:**
>
> Las entidades creadas durante la configuración de equilibrio de carga de prioridad no deben modificarse desde otras fichas de la GUI y también desde la CLI. Se recomienda modificar las entidades de equilibrio de carga de prioridad solo desde la ficha Equilibrio de carga de prioridad.

Extensiones de Citrix ADC

January 19, 2021

Las extensiones Citrix ADC se pueden utilizar para personalizar un dispositivo Citrix ADC escribiendo código de extensión. Actualmente, se admiten extensiones de directivas y extensiones de protocolo. Las extensiones de directiva se pueden usar para extender el lenguaje de directivas. Las extensiones de protocolo se pueden usar para agregar compatibilidad con protocolos personalizados en un dispositivo Citrix ADC.

Las extensiones Citrix ADC también son compatibles con Citrix ADC CPX.

Este documento incluye la siguiente información:

- Extensiones de Citrix ADC: Descripción general del idioma
- Citrix ADC Extensions: Referencia de la biblioteca
- Referencia de la API de extensiones de Citrix ADC
- Extensiones de protocolo
- Extensiones de directivas

Extensiones de Citrix ADC: Descripción general del lenguaje

January 12, 2021

El lenguaje de extensión se basa en el lenguaje de programación Lua 5.2. Lua proporciona un motor de ejecución compacto con buen rendimiento que está diseñado para incrustar en programas C, como el software Citrix ADC.

El lenguaje de extensión se escribe dinámicamente, lo que significa que cada objeto lleva su propia información de tipo. Cualquier variable puede contener cualquier tipo en cualquier momento durante la ejecución, por lo que los tipos de variables no se declaran.

El lenguaje también es de forma libre, donde se ignora el espacio en blanco entre tokens. Las declaraciones pueden estar separadas por punto y coma, pero eso no es necesario y generalmente no se hace. Los bloques de sentencias suelen terminar al final. No hay corchetes alrededor de bloques como {y} en C o Java.

Los identificadores son secuencias de letras (de la a a la z y de la A a la Z), dígitos (de 0 a 9) y guiones bajos (_), que no comienzan en un dígito. Los identificadores distinguen entre mayúsculas y minúsculas, por lo que var, VAR y Var son identificadores diferentes.

Los comentarios se inician por —. Todo después de: Se ignora hasta el final de la línea. Ejemplo:

```
-- This is a comment.
```

Tipos simples

August 20, 2021

El lenguaje permite valores de los siguientes tipos simples:

- Números
- Cuerdas
- Booleano
- Cero
- Otros tipos

Números

Todos los números (enteros pares) están representados por valores de coma flotante IEEE 754. Los enteros de hasta 2 ^ 54 tienen representaciones exactas. Los valores numéricos se pueden representar mediante:

- Números enteros decimales con signo y sin signo (ejemplos: 10, -5)
- Números reales con puntos decimales (10,5, 3,14159)
- Números reales con exponentes (1.0e+10)
- Hexadecimales (0xff0000)

Las expresiones de directiva Citrix ADC tienen tres tipos numéricos:

- enteros de 32 bits (núm_at)
- enteros de 64 bits (unsigned_long_at)

- coma flotante de 64 bits (double_at)

Todos estos se convierten en el tipo de número cuando se pasan a una función de extensión, y los números se convierten al tipo numérico de directiva esperado cuando se devuelven.

Cuerdas

Las cadenas son secuencias de bytes de cualquier longitud. Se corresponden con el tipo **text_at** de directiva. Las cadenas pueden contener bytes nulos (0x00). Los datos binarios arbitrarios se pueden mantener en cadenas, incluida cualquier representación de código de caracteres (por ejemplo, UTF-8 y Unicode completo). Sin embargo, las funciones de cadena que **le gusta.upper ()** asumen ASCII de 8 bits.

Las cadenas se asignan automáticamente cuando se usan. No hay necesidad (o incluso forma) de asignar explícitamente búferes para cadenas. Las cadenas también se desasignan automáticamente por la recolección de elementos no utilizados cuando ya no están en uso. No hay necesidad (o incluso forma) de liberar cadenas explícitamente. Esta asignación automática y desasignación evita algunos problemas comunes en lenguajes como C, como pérdidas de memoria y punteros colgantes.

Los literales de cadena son cadenas de caracteres entre comillas dobles o simples. No hay diferencia entre los dos tipos de comillas: “un literal de cadena” es lo mismo que ‘un literal de cadena’. El escape de barra invertida habitual está disponible: \s (campana), \b (retroceso), \f (feed de formulario), \n (línea nueva/feed de línea), \t (tabulador horizontal), \\ (barra invertida), “(comillas dobles) y ‘(comillas simples). Los valores de bytes decimales se pueden introducir mediante una barra invertida y de uno a tres dígitos (\d, \dd, \ddd). Los valores de bytes hexadecimales se pueden introducir mediante una barra invertida, una x y dos dígitos hexadecimales (\xhh)

Una llamada de sintaxis especial la notación de corchetes largos se puede utilizar para literales de cadena de varias líneas largas. Esta notación encierra la cadena entre corchetes dobles con cero o más signos iguales entre los corchetes; la idea es crear una combinación de corchetes e iguales que no esté en la cadena. No se respetan secuencias de escape en la cadena. Algunos ejemplos:

[[Esta es una cadena de varias líneas que utiliza la notación de corchetes largos.]]

[= [Esta es una cadena multilínea que utiliza una notación larga con [[and]] y sin escapar.] =]

La notación de corchetes largos se puede utilizar para hacer un comentario de varias líneas. Ejemplo:

—[[
Este es un comentario de varias líneas.
–]]

Booleano

Se proporcionan los valores booleanos true y false habituales. Tenga en cuenta que los valores booleanos son diferentes a los valores numéricos, en contraste con C donde se supone que cero es falso y cualquier valor distinto de cero es verdadero.

Cero

nil es un valor especial que significa "sin valor". Es su propio tipo y no es equivalente a ningún otro valor, en contraste con C donde NULL se define como cero.

Otros tipos

Hay otros dos tipos, datos de usuario y subprocesos. Estos son temas avanzados y no se tratan aquí.

Variables

January 12, 2021

Las variables contienen valores que pueden cambiar durante la ejecución de la extensión. Debido a la tipificación dinámica, cualquier variable puede contener valores de cualquier tipo. No hay declaraciones de tipo para las variables. En su lugar, el tipo de una variable se determina en tiempo de ejecución. De hecho, el tipo de valor de una variable puede cambiar durante la ejecución, aunque esta no es una práctica recomendada. Una variable inicialmente tiene el valor nil.

Los nombres de variables son identificadores, al igual que las cadenas de letras, dígitos y guiones bajos que no comienzan en un dígito. Ejemplos: Encabezados, combined_headers.

Variables globales

En Lua, las variables que no se declaran de otro modo son globales dentro del programa. Sin embargo, las variables globales no están permitidas en las funciones de extensión de directivas, porque hay varios motores de paquetes en los que se puede ejecutar una función, y cada motor de paquetes tiene su propia memoria.

Si usa una variable global en su extensión, obtendrá un error de tiempo de ejecución: Intente actualizar o crear un global reportado en **/var/log/ns.log**.

Los errores tipográficos en nombres de variables son un problema potencial, porque la variable con el error tipográfico se interpretará como otra variable global, y no causará un error de sintaxis como en lenguaje como C o Java. Como se señaló anteriormente, obtendrá un error de tiempo de ejecución en su lugar.

Variables locales

Una variable puede declararse como local a un bloque de sentencias, como una función. Esto se hace por nombre variable local. La variable se aplicará al bloque, es decir, solo existirá dentro del bloque. La declaración local puede asignar opcionalmente un valor a la variable.

Ejemplos:

local headers = {}
local combined_headers = {}

Expresiones

August 20, 2021

Las expresiones calculan valores a partir de valores variables y literales.

- Operaciones aritméticas
- Operaciones Relacionales
- Operaciones Lógicas
- Concatenación
- Duración
- Precedencia

Operaciones aritméticas

Las operaciones aritméticas se realizan en valores numéricos. Si se utiliza un valor de cadena en una operación aritmética, se convierte en un número; si esto falla, se devuelve un error.

a + b	agregar a y b
a: B	restar b de a
a * b	multiplicar a y b
a/b	dividir a por b
% b	modulo = a: Math.floor (a/b) *b
a ^ b	elevar a la potencia b; b puede ser cualquier número
-a	negar a

Operaciones relacionales

Las operaciones relacionales comparan dos valores y devuelven verdadero si la relación está satisfecha y falso si no lo es. Las operaciones relacionales se pueden realizar entre valores de cualquier tipo. Si los valores no son del mismo tipo, se devuelve false. Los números se comparan de la manera habitual. Las cadenas se comparan mediante la secuencia de intercalación para la configuración regional actual.

a == b	a es igual a b
a ~= b	a no es igual a b
a < b	a es menor que b
a > b	a es mayor que b
a <= b	a es menor o igual que b
a >= b	a es mayor o igual que b

Operaciones lógicas

Las operaciones lógicas se realizan tradicionalmente en valores booleanos, pero en este lenguaje se pueden realizar en dos valores cualesquiera. nil y false se consideran false y cualquier otro valor se considera true. Las operaciones lógicas utilizan la evaluación de atajo, donde si el primer valor determina el resultado de la operación, el segundo valor no se evalúa.

a y b	si a es falso o nulo, devuelve un otro retorno b
a o b	si a no es falso y no nulo, devuelve un retorno b
no es un	si a no es falso o nulo devuelve falso else devuelve verdadero

Las operaciones e y o se pueden utilizar para la evaluación condicional dentro de una expresión:

a o b	se puede usar para proporcionar un valor predeterminado b si a no se inicializa (nil). Esto es útil para los parámetros opcionales en las funciones.
a y b o c	se puede usar para elegir no nil b o c en función de la condición a. Si a es verdadero, entonces a y b devuelve b, y b o c devuelve b. Si a es falso, entonces a y b devuelve false y false o c devuelve c. Esto es equivalente a un ? b: C en el lenguaje de programación C.

Concatenación

La concatenación de cadenas es s1.. s2. Esto crea una nueva cadena lo suficientemente grande como para contener el contenido de s1 y s2 y copia el contenido en la nueva cadena. Se produce un error si s1 o s2 no son cadenas. Tenga en cuenta que la concatenación repetida puede tener una sobrecarga de copia considerable. Si construye una cadena de n bytes concatenando un byte a la vez, esto copiará n* (n+1) /2 bytes. Para un mejor rendimiento, puede poner piezas de una cadena para concatenar en una tabla (discutido más adelante) y luego usar la función table.concat (). Un ejemplo de esto se muestra en el ejemplo COMBINE_HEADERS ().

Duración

La longitud de una cadena s es devuelta por #s. El operador # también se utiliza con tablas de matriz, como se discute más adelante.

Precedencia

La precedencia del operador determina el orden en el que se realizan las operaciones en una expresión, con operaciones de mayor precedencia realizadas antes que aquellas con menor precedencia. El orden de precedencia puede, como de costumbre, ser anulado por paréntesis. Por ejemplo, en `a + b \* c`, * tiene mayor prioridad que +, por lo que la expresión se evalúa como `a + (b \* c)`.

más alto	^
-	no #: (unario)

-	* / %
-	..
-	= ~= < > <= >=
-	y
más bajo	O bien:

Las operaciones con la misma precedencia se realizan de izquierda a derecha (asociativo de izquierda), excepto ^ y.. que se realizan de derecha a izquierda (asociativo de derecha). Entonces a^b^c se evalúa como a^ (b^c).

Asignación

January 12, 2021

La instrucción assignment evalúa una expresión y asigna el valor resultante a una variable.

```
variable = expression
```

Como se señaló anteriormente, los valores de cualquier tipo se pueden asignar a cualquier variable, por lo que se permite lo siguiente:

```
local v1 = ”a string literal”
v1 = 10
```

Una instrucción de asignación en realidad puede establecer múltiples variables, mediante el formulario

variable1, variable2, … = expression1, expression2, …

Si hay más variables que expresiones, a las variables adicionales se les asigna nil. Si hay más expresiones que variables, se descartan los valores de expresión adicionales. Las expresiones se evalúan antes de las asignaciones, por lo que se puede utilizar para intercambiar sucintamente los valores de dos variables:

v1, v2 = v2, v1

es equivalente a

tmp = v1
v2 = v1
v1 = tmp

Tablas

August 20, 2021

Las tablas son colecciones de entradas con claves y valores. Son la única estructura de datos agregada proporcionada. Todas las demás estructuras de datos (matrices, listas, conjuntos, etc.) se construyen a partir de tablas. Las claves y los valores de tabla pueden ser de cualquier tipo, incluidas otras tablas. Las claves y los valores de la misma tabla pueden mezclar tipos.

- Constructores de tablas
- Uso de tablas
- Tablas como matrices
- Tablas como registros

Constructores de tablas

Los constructores de tablas permiten especificar una tabla con claves y valores asociados. La sintaxis es:

{[key1] = value1, [key2] = value2, …}

donde las claves y valores son expresiones. Si las claves son cadenas que no son palabras reservadas, se pueden omitir los corchetes y comillas alrededor de las claves. Ejemplo:

{key1 = “value1”, key2 = “value2”, key3 = “value3”}

Una tabla vacía se especifica simplemente por {}.

Un constructor de tabla se puede utilizar en una asignación para establecer una variable para hacer referencia a una tabla. Ejemplos:

local t1 = {}: Establecer t1 en una tabla vacía
local t2 = {key1 = “value1”, key2 = “value2”, key3 = “value3”}

Tenga en cuenta que las tablas son anónimas. Más de una variable puede referirse a la misma tabla. Continuando con el ejemplo anterior:

local t3 = t2: Tanto t2 como t3 se refieren a la misma tabla

Uso de la tabla

Como era de esperar, puede usar claves para buscar valores en una tabla. La sintaxis es[clave]de tabla, donde tabla es una referencia de tabla (normalmente una variable asignada a una tabla) y clave es una expresión que proporciona la clave. Si se utiliza en una expresión y la clave existe en la tabla, devuelve el valor asociado a la clave. Si la clave no está en la tabla, esto devuelve nil. Si se utiliza como variable

en una asignación y la clave no existe en la tabla, se crea una nueva entrada para la clave y el valor. Si la clave ya existe en la tabla, reemplaza el valor de la clave por el nuevo valor. Ejemplos:

local t = {} — establece t en una tabla vacía
t[“k1”] = “v1” — crea una entrada para la clave “k1” y el valor “v1”
v1 = t[“k1”] — establece v1 en el valor de la clave “k1” = “v1”
t[“k1”] = “new_v1” — establece el valor de la clave “k1” en “new_v1”

Tabla como matrices

La matriz tradicional se puede implementar mediante una tabla con claves enteras como índices. Una matriz puede tener cualquier índice, incluidos los negativos, pero la convención es iniciar matrices en el índice 1 (no 0 como es el caso con lenguajes como C y Java). Hay un constructor de tabla de propósito especial para tales matrices:

{value1, value2, value3, … }

A continuación, las referencias de matriz son[índice]de matriz.

El operador de longitud # devuelve el número de elementos en una matriz con índices consecutivos comenzando en 1. Ejemplo:

local a = {“value1”, “value2”, “value3”} longitud
local = #a: Establece la longitud a la longitud de la matriz a = 3

Las matrices pueden ser dispersas, donde solo se asignan los elementos definidos. Pero # no se puede usar en una matriz dispersa con índices no consecutivos. Ejemplo:

local sparse_array = {} – Configurar una matriz vacía
sparse_array[1] = “value1” – Agregar un elemento en el índice 1
sparse_array[99] = “value99” – Agregar un elemento en el índice 99

Las matrices multidimensionales se pueden configurar como tablas de tablas. Por ejemplo, una matriz 3x3 podría configurarse mediante:

local m = {{1, 2, 3}, {4, 5, 6}, {7, 8, 9}
local v22 = m[2][2] — establece v22 en 5

Tablas como registros

Los registros con campos se pueden implementar como tablas con claves de nombre de campo. La tabla.field del formulario de referencia se puede utilizar para la tabla [“campo”]. Ejemplos:

local person = {name = “John Smith”, phone = “777-777-7777”}
local name = person.name – Establece el nombre en “John Smith”

Se puede utilizar una matriz de tablas para una secuencia de registros. Ejemplo:

local people = {
{name = “John Smith”, phone = “777-777-7777”},
{name = “Jane Doe”, phone = “888-888-8888”}
…
}

name = people[2].name – Establece el nombre en “Jane Doe”

Estructuras de control

January 12, 2021

El lenguaje de la función de extensión proporciona las instrucciones habituales para controlar la ejecución del programa.

- If Then Else
- While Do and Repeat Until
- Numeric For
- Pausa/Inter
- GoTo

If Then Else

Si las sentencias seleccionan bloques de sentencias para ejecutar en función de una o más condiciones. Hay tres formas:

If then Form

```
if expression then
     statements to execute if expression is not false or nil
end
<!--NeedCopy-->
```

If then else Form

```
if expression then
     statements to execute if expression is not false or nil
else
     statements to execute if expression is false or nil
```



```
end
<!--NeedCopy-->
```

If then elseif else Form

```
if expression1 then
     statements to execute if expression1 is not false or nil
     elseif expression2 then
          statements to execute if expression2 is not false or nil
. . .
else
     statements to execute if all expressions are false or nil
end
<!--NeedCopy-->
```

Ejemplo:

```
if headers[name] then

     local next_value_index = #(headers[name]) + 1
     headers[name][next_value_index] = value

else

     headers[name] = {
 name .. ":" .. value }


end
<!--NeedCopy-->
```

Nota:

- La expresión no está entre paréntesis como es el caso en C y Java.
- No hay equivalente a la instrucción C/Java switch. Tiene que usar una serie de sentencias if elseif para hacer el equivalente.

While Do and Repeat Until

Las sentencias **while** y **repeat** proporcionan bucles controlados por una expresión.


```
while expression do
     statements to execute while expression is not false or nil
end

repeat

     statements to execute until expression is not false or nil

until expression
<!--NeedCopy-->
```

Ejemplo de while:

```
local a = {
 1, 2, 3, 4 }

local sum, i = 0, 1 -- multiple assignment initializing sum and i
while i <= #a do -- check if at the end of the array
     sum = sum + a[i] -- add array element with index i to sum
     i = i + 1 -- move to the next element
end
<!--NeedCopy-->
```

Ejemplo de repeat:

```
sum, i = 0, 1 -- multiple assignment initializing sum and i
repeat
     sum = sum + a[i] -- add array element with index i to sum
     i = i + 1 -- move to the next element
until i > #a -- check if past the end of the array
<!--NeedCopy-->
```

Por supuesto, es posible escribir un bucle que no termine, por ejemplo, si omite la instrucción i = i + 1 en cualquiera de estos ejemplos. Cuando se ejecuta una función de este tipo, Citrix ADC detectará que la función no se completó en un tiempo razonable y la matará con un error de tiempo de ejecución:

`Cpu limit reached. Terminating extension execution in [[string "function extension function..."]]: line line-number.`

se informará en /var/log/ns.log.

Numeric For

Hay dos tipos de bucles for. El primero es el numérico para, que es similar al uso habitual de la declaración for en C y Java. La instrucción for numérica inicializa una variable, comprueba si la variable ha pasado un valor final y, si no, ejecuta un bloque de sentencias, incrementa la variable y se repite. La sintaxis para el bucle numérico for es:

```
for variable = initial, final, increment do

     statements in the loop body

end
<!--NeedCopy-->
```

donde inicial, final e incremento son todas las expresiones que producen (o se pueden convertir a) números. variable se considera que es local para el bloque de sentencia de bucle for; no se puede utilizar fuera del bucle. incremento se puede omitir; el valor predeterminado es 1. Las expresiones se evalúan una vez al principio del bucle. La condición de terminación es variable > final si el incremento es positivo y variable < final si el incremento es negativo. El bucle termina inmediatamente si el incremento es 0.

Ejemplo (equivalente a los bucles while y repeat en la sección anterior):

```
sum = 0
for i = 1, #a do -- increment defaults to 1
     sum = sum + a[i]
end
<!--NeedCopy-->
```

El segundo tipo de bucle for es el genérico para, que se puede utilizar para tipos de bucles más flexibles. Implica el uso de funciones, por lo que se discutirá más adelante después de que se hayan introducido las funciones.

Pausa/Inter

La sentencia break se utiliza dentro de un bucle while, repeat o for. Terminará el bucle y reanudará la ejecución en la primera declaración después del bucle. Ejemplo (también equivalente al anterior while, repeat y for loops):


```
sum, i = 0, 1
while true do
     if i > #a then
          break
     end
     sum = sum + a[i]
     i = i + 1
end
<!--NeedCopy-->
```

GoTo

La instrucción goto se puede utilizar para saltar hacia adelante o hacia atrás a una etiqueta. La etiqueta es un identificador y su sintaxis es:: Label:. La instrucción goto es goto label. Ejemplo (una vez más equivalente a los bucles anteriores):

```
sum, i = 0, 1
::start_loop::
     if i > #a then
          goto end_loop -- forward jump
     end
     sum = sum + a[i]
     i = i + 1
     goto start_loop -- backwards jump
::end_loop::
. . .
<!--NeedCopy-->
```

Ha habido una larga controversia sobre el uso de gotos en la programación. En general, debe intentar usar las otras estructuras de control para que sus funciones sean más legibles y confiables. Pero el uso juicioso ocasional de gotos puede conducir a mejores programas. En particular, los gotos pueden ser útiles en el manejo de errores.

Funciones

December 2, 2021

Las funciones son un componente básico de la programación: son una forma práctica y eficaz de agrupar sentencias que realizan una tarea. Son la interfaz entre el dispositivo Citrix ADC y el código

de extensión. Para las directivas, se definen funciones de extensión de directivas. En el caso de los protocolos, se implementan funciones de devolución de llamada para los comportamientos del protocolo. Las funciones consisten en definiciones de función que especifican qué valores se pasan a la función y qué instrucciones se ejecutan para la función, así como llamadas a funciones, que ejecutan funciones con datos de entrada específicos y obtienen resultados de la función.

Funciones de devolución de llamada de comportamiento de protocolo

El comportamiento del cliente TCP consiste en una función de devolución de llamada (on_data) que procesa los eventos del flujo de datos del cliente TCP. Para implementar el equilibrio de carga basado en mensajes (MBLB) para un protocolo basado en TCP, puede agregar código para esta función de devolución de llamada para procesar el flujo de datos TCP del cliente y analizar el flujo de bytes en mensajes de protocolo.

Las funciones de devolución de llamada de un comportamiento se llaman con un contexto, que es el estado del módulo de procesamiento. El contexto es la instancia del módulo de procesamiento. Por ejemplo, las devoluciones de llamada de comportamiento del cliente TCP se llaman con contextos diferentes para distintas conexiones TCP del cliente.

Además del contexto, las devoluciones de llamada de comportamiento pueden tener otros argumentos. Por lo general, el resto de los argumentos se pasan como carga útil, que es la colección de todos los argumentos. Por lo tanto, las instancias del módulo de procesamiento programable se pueden ver como una combinación de estado de instancia más funciones de devolución de llamada de evento, es decir, el contexto más el comportamiento. Y el tráfico fluye a través del proceso como carga útil de eventos.

Prototipo de función de devolución de llamada del cliente TCP:

```
1
2                 Function                client on_data (ctxt, payload)
3
4                                                 //.code
5
6                 end
7
8
9 <!--NeedCopy-->
```

Donde:

- ctxt - Contexto de procesamiento de cliente TCP
- payload — carga útil de eventos
  - payload.data - Datos TCP recibidos, disponibles como flujo de bytes

Funciones de extensión de directivas

Dado que se escribe el lenguaje de expresión de directivas de NetScaler, la definición de una función de extensión debe especificar los tipos de sus entradas y su valor devuelto. La definición de **función Lua** se ha ampliado para incluir los siguientes tipos:

```
function self-type: function-name(parameter1: parameter1-type, and so
   on): return-type
     statements
end

<!--NeedCopy-->
```

Donde:

Los tipos son NSTEXT, NSNUM, NSBOOL o NSDOUBLE.

El autotipo es el tipo de autoparámetro implícito que se pasa a la función. Cuando se utiliza la función de extensión en una expresión de directiva de Citrix ADC, este es el valor generado por la expresión situada a la izquierda de la función. Otra forma de verlo es que la función amplía ese tipo en el lenguaje de directivas de Citrix ADC.

Los tipos de parámetros son los tipos de cada parámetro especificado en la llamada a la función de extensión en la expresión de directiva. Una función de extensión puede tener cero o más parámetros.

Return-type es el tipo de valor devuelto por la llamada a la función de extensión. Es la entrada de la parte de la expresión de directiva, si la hay, a la derecha de la función, o bien es el valor del resultado de la expresión.

Ejemplo:

```
function NSTEXT:COMBINE_HEADERS(): NSTEXT
```

Uso de la función de extensión en una expresión de directiva:

```
HTTP.REQ.FULL_HEADER.AFTER_STR("HTTP/1.1\r\n").COMBINE_HEADERS()
```

Aquí el autoparámetro es el resultado de `HTTP.REQ.FULL_HEADER.AFTER_STR("HTTP/1.1\r\n")`, que es un valor de texto. El resultado de la llamada COMBINE_HEADERS() es texto y, como no hay nada a la derecha de esta llamada, el resultado de toda la expresión es texto.

Definición de función local

Además de las funciones de extensión, no se pueden definir funciones globales en un archivo de extensión. Pero las funciones locales se pueden definir dentro de las funciones de extensión utilizando la instrucción de función Lua normal. Esto declara el nombre de la función y los nombres de sus

parámetros (también conocidos como argumentos) y, como todas las declaraciones de Lua, no especifica ningún tipo. La sintaxis para esto es:

```
local function function-name(parameter1-name, parameter2-name, and so
   on)
     statements
end

<!--NeedCopy-->
```

Los nombres de las funciones y los parámetros son identificadores. (El nombre de la función es en realidad una variable y la instrucción de función es la abreviatura de nombre de función local = función (parameter1, etc.), pero no es necesario entender esta sutileza para usar funciones.)

Tenga en cuenta que aquí se utiliza y así sucesivamente para continuar el patrón de nombres de parámetros en lugar de lo habitual… Esto se debe a que… en sí mismo significa una lista de parámetros variables, que no se discutirán aquí.

Cuerpo de función y retorno

El bloque de sentencias entre la función y las sentencias end es el cuerpo de la función. En el cuerpo de la función, los parámetros de la función actúan como variables locales, con valores proporcionados por las llamadas a funciones, como se ha descrito anteriormente.

La instrucción return proporciona valores que se devolverán al autor de la llamada de la función. Debe aparecer al final de un bloque (en una función, si es entonces, bucle for, etc. Puede estar en su propio bloque, devolver… final). En él se especifican ninguno, uno o más de un valor devuelto:

```
return -- returns nil
return expression -- one return value
return expression1, expression2, ... -- multiple return values

<!--NeedCopy-->
```

Ejemplos:

```
local function fsum(a)
     local sum = 0
     for i = 1, #a do
          sum = sum + a[i]
```



```
5       end
6       return sum
7   end
8
9   Local function fsum_and_average(a)
10      local sum = 0
11      for i = 1, #a do
12          sum = sum + a[i]
13      end
14      return sum, sum/#a
15  end
16
17  <!--NeedCopy-->
```

Llamadas a funciones

Una llamada de función ejecuta el cuerpo de una función, suministra valores para sus parámetros y recibe resultados. La sintaxis de una llamada a función es nombre-función (expression1, expression2, etc.), donde los parámetros de función se establecen en las expresiones correspondientes. El número de expresiones y parámetros no tiene por qué ser el mismo. Si hay menos expresiones que parámetros, el resto de los parámetros se establece en cero. Por lo tanto, puede hacer que uno o más parámetros al final de la llamada sean opcionales, y su función puede comprobar si están especificados comprobando si no son nulo. Una forma común de hacerlo es con la operación OR:

```
1   function f(p1, p2) -- p2 is optional
2       p2 = p2 or 0 -- if p2 is nil, set to a default of 0
3       . . .
4   end
5
6   <!--NeedCopy-->
```

Si hay más expresiones que parámetros, se omiten los valores de expresión restantes.

Como se ha señalado anteriormente, las funciones pueden devolver varios valores. Estas devoluciones se pueden utilizar en una sentencia de asignación múltiple. Ejemplo:

```
1   local my_array = {
2    1, 2, 3, 4 }
3
4   local my_sum, my_ave = sum_and_average(my_array)
5
```



```
<!--NeedCopy-->
```

Funciones iterador y bucles for genéricos

Ahora que hemos introducido funciones, podemos hablar de bucles for genéricos. La sintaxis del bucle for genérico (con una variable) es:

```
for variable in iterator(parameter1, parameter2, and so on) do
     statements in the for loop body
end

<!--NeedCopy-->
```

Donde iterator () es una función con cero o más parámetros que proporcionan un valor para una variable en cada iteración del cuerpo del bucle. La función iterator realiza un seguimiento de dónde se encuentra en la iteración utilizando una técnica llamada cierre, de la que no tienes que preocuparte aquí. Señala el final de la iteración devolviendo nulo. Las funciones iteradoras pueden devolver más de un valor, para su uso en una asignación múltiple.

Escribir una función iteradora está fuera del alcance de este artículo, pero hay pocos iteradores integrados útiles que ilustren el concepto. Uno es el iterador pairs(), que recorre las entradas de una tabla y devuelve dos valores, la clave y el valor de la siguiente entrada.

Ejemplo:

```
local t = {
 k1 = ”v1”, k2 = ”v2”, k3 = ”v3” }

local a = {
  }
  -- array to accumulate key-value pairs
local n = 0 -- number of key-value pairs
for key, value in pairs(t) do
     n = n + 1
     a[n] = key.. ” = ”.. Value -- add key-value pair to the array
end
local s = table.concat(a, ”;”) -- concatenate all key-value pairs into
   one string

<!--NeedCopy-->
```


Otro iterador útil es la función `string.gmatch()`, que se usa en este ejemplo de `COMBINE_HEADERS()`.

Extensiones de Citrix ADC: Referencia de bibliotecas

August 20, 2021

La lista de bibliotecas admitidas en las extensiones de directivas.

- Biblioteca básica
- Biblioteca de cadenas
- Patrones de expresión regular: Clases de caracteres
- Patrones de expresión regular: Elementos de patrón
- Biblioteca de tablas
- Biblioteca de matemáticas
- Biblioteca bit a bit
- Biblioteca de sistemas operativos
- Biblioteca Citrix ADC

Biblioteca básica

assert (v[, mensaje])	Emitir un error, con un mensaje opcional, cuando v es falso.
error(message)	Termina una función e informa del mensaje de error.
ipairs(a)	Iterador para una matriz a. Devuelve un índice y un valor para cada iteración.
pairs(t)	Iterador para una tabla t. Devuelve una clave y un valor para cada iteración.
número de tono (e[, base])	Convierte e en un número, con una base opcional.
tostring(v)	Convierte v en una cadena
type(v)	Devuelve el tipo de v: Número, cadena, booleano, tabla, etc.

getmetatabla (object)	Devuelve nil si el objeto no tiene una metatabla. De lo contrario, si la metatabla del objeto tiene un campo “__metatabla”, devuelve el valor asociado. De lo contrario, devuelve la metatabla del objeto dado.
setmetatabla (table, metatabla)	Establece la metatabla para la tabla dada. (No puede cambiar la metatabla de otros tipos de Lua, solo desde C.) Si metatabla es nulo, elimina la metatabla de la tabla dada. Si la metatabla original tiene un campo “__metatabla”, genera un error.
select (index, ···)	Devuelve todos los argumentos después del índice de número de argumento. Si el índice es la cadena “#”, entonces devuelve el número total de argumentos adicionales que recibió.
pcall (f [, arg1, ··])	Llama a la función f con los argumentos dados en modo protegido. Devuelve el código de estado como primer resultado que indica si la llamada tuvo éxito o no. Si la llamada tuvo éxito, entonces junto con el código de estado también devuelve todos los resultados de la llamada, de lo contrario devuelve un mensaje de error.
xpcall (f, msgh [, arg1, ··])	Esta función es similar a pcall, excepto que también toma un argumento para el manejo de errores.
_VERSION	Devuelve la versión actual del intérprete.

Biblioteca de cadenas

string.byte (s[, i [, j]])	Devuelve los valores de bytes de s[i] a s[j]. Predeterminado i = 1 y j = i
cadena.char (…)	Devuelve una cadena construida a partir de los parámetros enteros.

string.find (s, pattern[, init [, plain])	Busca la primera coincidencia de un patrón de expresión regular en s. Devuelve el primer y último índice de coincidencia o nil. init es índice para empezar, por defecto 1. plain = true significa patrón no es una expresión regular.
string.format(form,…)	Devuelve una versión formateada de los parámetros.
string.gmatch(s,pattern)	Iterador para buscar s con el patrón de expresiones regulares. Devuelve valores coincidentes.
string.gsub (s, pattern, repl[, n])	Devuelve una copia de s en la que todas (o n) ocurrencias del patrón han sido reemplazadas por repl.
string.len(s)	Devuelve la longitud de la cadena.
string.lower(s)	Devuelve una copia de la cadena convertida en minúsculas.
cadena.match (s, patrón[, init])	Busca la primera coincidencia del patrón de expresiones regulares en s y devuelve las capturas o el patrón completo. init es el índice a comenzar, predeterminado 1.
string.rep (s, n[, sep])	Devuelve una cadena que es n copias de s, con separador sep, por defecto sin separador
string.reverse(s)	Devuelve una cadena que se invierte.
string.sub (s, i[, j])	Devuelve la subcadena de s desde s[i] a s[j]; por defecto j es el final de la cadena.
string.upper(s)	Devuelve una copia de la cadena convertida en mayúsculas.
string.dump (function)	Devuelve una cadena que contiene una representación binaria de la función dada.

Patrones de expresión regular: Clases de caracteres

x	el personaje x, excepto los personajes mágicos ^$ ()%.[]*+-?)
.	cualquier carácter
%a	cualquier letra
%c	cualquier carácter de control
%d	cualquier dígito
%g	cualquier carácter imprimible excepto el espacio
%l	cualquier letra minúscula
%p	cualquier carácter de puntuación
%s	cualquier carácter de espacio en blanco
%u	cualquier letra mayúscula
%w	cualquier letra alfanumérica
%x	un carácter mágico escapado x (por ejemplo%%)
[set]	un conjunto de caracteres: Secuencia de caracteres individuales, rangos x-y, y% clases
[^set]	caracteres no incluidos en el conjunto.

Patrones de expresión regular: Elementos de patrón

X	una clase de carácter
X*	0 o más repeticiones más largas de caracteres en X
X+	1 o más repeticiones de caracteres en X
X-	0 o más repeticiones más cortas de caracteres en X
X?	0 o 1 carácter en X
%n	n=1 a 9; coincide con la enésima cadena capturada

%bxy	coincide con la subcadena entre dos caracteres balanceados x e y. El ejemplo%b () coincide con la subcadena entre dos paréntesis equilibrados.
%f[set]	coincide con una cadena vacía en cualquier posición de tal manera que el siguiente carácter pertenece al conjunto y el carácter anterior no pertenece al conjunto.

Un patrón es una secuencia de elementos de patrón. ^pattern coincide con el comienzo de una cadena y pattern$ coincide con el final de la cadena.

Las subcadenas coincidentes se pueden capturar mediante (patrón). Los paréntesis sin patrón () capturan la posición actual de la cadena (un número).

Biblioteca de tablas

table.concat (lista[, sep [, i [, j]]])	Devuelve una lista de cadenas[i].. sep.. list[i+1].. sep.. list[j]. Por defecto sep es la cadena vacía. El valor predeterminado i es 1, j es #list.
table.insert (lista,[pos,]valor)	Inserta el valor en la lista en pos del índice. El valor predeterminado para pos es #list (final de la lista).
tabla.pack (…)	Devuelve una matriz que contiene los parámetros que comienzan en el índice 1, y una clave n con el número total de parámetros.
table.remove (lista[, pos])	Elimina de la lista el elemento en posición pos, desplazando los elementos para llenar la posición. Devuelve el elemento eliminado. Predeterminado para posis #list (final de la lista).
table.sort (lista[, comp])	Ordenar los elementos de la lista en su lugar. comp es la función de comparación a usar. El valor predeterminado para la comp es <.

table.unpack(list[, i [, j]])	Devuelve list[i] a través de list[j]. El valor predeterminado para i es 1 y j es #list <c/ode>.

Biblioteca de matemáticas

Diversas funciones trigonométricas y logarítmicas no se muestran.

math.abs (x)	Devuelve el valor absoluto de x.
math.ceil (x)	Devuelve el entero más pequeño >= x.
math.floor (x)	Devuelve el entero más grande <= x.
math.fmod (x, y)	Devuelve el resto de x/y redondeando el cociente hacia cero.
math.huge	Un valor >= cualquier otro número.
math.max (x,…)	Devuelve el argumento maximum.
math.min (x,…)	Devuelve el argumento mínimo.
math.modf (x)	Devuelve las partes integrales y fraccionarias de x.
math.random ()	Devuelve un número pseudo-aleatorio entre 0 y 1.
math.random (m)	Devuelve un entero pseudo-aleatorio entre 1 y m.
math.random (m, n)	Devuelve un entero pseudo-aleatorio entre m y n.
math.aleatorseed (x)	Establece el generador de números pseudo-aleatorios establecido en x.
math.sqrt (x)	Devuelve la raíz cuadrada de x (x^0.5)
math.acos (x)	Devuelve el arco coseno de x (en radianes).
math.asin (x)	Devuelve el arco seno de x (en radianes).
math.atan (x)	Devuelve el arco tangente de x (en radianes).
math.atan2 (y, x)	Devuelve el arco tangente de y/x (en radianes).
math.cos (x)	Devuelve el coseno de x.

math.cosh (x)	Devuelve el coseno hiperbólico de x.
math.sin (x)	Devuelve el seno de x.
math.sinh (x)	Devuelve el seno hiperbólico de x.
math.tan (x)	Devuelve la tangente de x.
math.tanh (x)	Devuelve la tangente hiperbólica de x.
math.deg (x)	Devuelve el ángulo x (en radianes) en grados.
math.exp (x)	Devuelve el valor e^x.
math.frexp (x)	Devuelve m y e tal que x = m2e, e es un entero y el valor absoluto de m está en el rango [0.5, 1).
math.ldexp (m, e)	Devuelve m2e (e debe ser un entero).
math.log (x [, base])	Devuelve el logaritmo de x en la base dada. El valor predeterminado para base es e.
math.pow (x, y)	Devuelve x^y.
math.rad (x)	Devuelve el ángulo x (dado en grados) en radianes.
Math.pi	El valor de π.

Biblioteca bit a bit

A menos que se indique lo contrario:

- Todas las funciones aceptan argumentos numéricos en el rango (-2^51, +2^51).
- Cada argumento se normaliza al resto de su división en 2^32 y se trunca a un entero (de alguna manera no especificada), de modo que su valor final cae en el rango [0,2^32 - 1].
- Todos los resultados están en el intervalo [0,2^32 - 1].

bit32.arshift (x, disp)	Devuelve x bits disp movidos aritméticamente a la derecha (+disp) o a la izquierda (-disp).
bit32.band (…)	Devuelve el bit a bit y de los argumentos.
bit32.bnot (x)	Devuelve la negación bit a bit de x.
bit32.bor(…)	Devuelve el bit a bit o de los argumentos.

bit32.btest(…)	Devuelve verdadero si el bit a bit y de los argumentos no es cero.
bit32.bxor(…)	Devuelve la exclusiva bit a bit o de los argumentos.
bit32.extract(n,field[,width])	Devuelve los bits en n de campo a campo + ancho: 1 (número de bits del más al menos significativo). El valor predeterminado para el ancho es 1.
bit32.replace(n,v,field[,width])	Devuelve una copia de n con bits de campo a campo + ancho -1 reemplazado por v. Ancho predeterminado es 1.
bit32.lrotate (x, disp)	Devuelve x bits de disp girados a la izquierda (+disp) o a la derecha (-disp).
bit32.lshift (x, disp)	Devuelve x bits disp desplazados a la izquierda (+disp) o a la derecha (-disp).
bit32.rrotate (x, disp)	Devuelve x bits de disp girados a la derecha (+disp) o a la izquierda (-disp).
bit32.rshift (x, disp)	Devuelve x bits disp desplazados a la derecha (+disp) o a la izquierda (-disp).

Biblioteca del sistema operativo

o.clock ()	Devuelve una aproximación de la cantidad en segundos del tiempo de CPU.
os.date ([formato [, hora]])	Devuelve una cadena o una tabla que contiene fecha y hora, con formato de acuerdo con el formato de cadena dado.
os.time ([tabla])	Devuelve la hora actual cuando se llama sin argumentos, o una hora que representa la fecha y hora especificadas por la tabla dada.
os.difftime (t2, t1)	Devuelve el número de segundos desde el tiempo t1 hasta el tiempo t2.

Biblioteca Citrix ADC

ns.logger:level (mensaje)	Para registrar mensajes donde el nivel sea de emergencia, alerta, crítica, error, advertencia, aviso, información o depuración. Los parámetros son los mismos que la función C printf (): Una cadena de formato y un número variable de argumentos para proporcionar valores para los especificadores% en la cadena de formato.

Referencia de la API de extensiones de Citrix ADC

August 20, 2021

Los comportamientos son una formalización de patrones programables comunes que están disponibles en un dispositivo Citrix ADC. Por ejemplo, un servidor virtual TCP admite un comportamiento de cliente TCP y un comportamiento de servidor TCP. Un comportamiento es un conjunto predefinido de funciones de devolución de llamada. Puede implementar comportamientos proporcionando funciones de devolución de llamada. Por ejemplo, un comportamiento de cliente TCP puede consistir en la función on_data, que procesa el flujo de datos TCP.

Comportamiento del cliente TCP

on_data: Función de devolución de llamada para eventos de datos de cliente TCP. La devolución de llamada toma dos argumentos:

- **ctxt**: Contexto de procesamiento de cliente TCP
- **carga útil: Carga** útil de evento
  - **payload.data: Datos** TCP recibidos, disponibles como una secuencia de bytes

Comportamiento del servidor TCP

on_data: Función de devolución de llamada para eventos de datos del servidor TCP, la devolución de llamada toma dos argumentos:

- **ctxt**: Contexto de procesamiento del servidor TCP
- **carga útil: Carga** útil de evento
  - **payload.data**: Datos tcp recibidos, disponibles como una secuencia de bytes

Contexto de cliente TCP

El contexto que se pasa a las devoluciones de llamada de evento de cliente TCP:

- **ctxt.output**: El siguiente contexto de procesamiento en el proceso. Los controladores de devolución de llamada de extensión pueden enviar datos de tipo ns.tcp.stream a ctxt.output mediante los eventos DATA, que significa mensaje parcial o EOM que significa mensaje final del protocolo. El evento EOM puede o no tener datos TCP con él. Un evento EOM con datos TCP se puede enviar sin un evento DATA anterior para enviar un mensaje de protocolo completo y marcar el final del mensaje. La decisión de equilibrio de carga se toma, aguas abajo por el servidor virtual de equilibrio de carga, en los primeros datos recibidos. Una nueva decisión de equilibrio de carga se toma después de la recepción del mensaje EOM. Por lo tanto, para transmitir datos de mensajes de protocolo, envíe varios eventos DATA con el último evento como EOM. Todos los eventos DATA contiguos y los siguientes eventos EOM se envían a la misma conexión de servidor seleccionada por la decisión de equilibrio de carga en el primer evento DATA de la secuencia.
- **ctxt.input**: El contexto de procesamiento anterior en el proceso de donde provienen los datos de flujo TCP.
- **ctxt:hold(data)**: Función para almacenar los datos para su procesamiento futuro. Al llamar a la retención con datos, los datos se almacenan en el contexto. Más tarde, cuando se reciben más datos en el mismo contexto, los datos recién recibidos se anexan a los datos almacenados anteriormente y el flujo de datos combinado se pasa a la función de devolución de llamada on_data. Después de llamar a una retención, la referencia de datos ya no es utilizable y da error en cualquier uso.
- **ctxt.vserver**: El contexto del servidor virtual.
- **ctxt.client**: Contexto de procesamiento de conexión de cliente. Este contexto de procesamiento se puede utilizar para enviar datos al cliente, y para obtener alguna información relacionada con la conexión, como dirección IP, puertos de origen y destino.
- **ctxt:close ()**: Cierra la conexión del cliente enviando FIN al cliente. Después de llamar a esta API, el contexto de procesamiento del cliente ya no es utilizable y da error en cualquier uso.

Contexto del servidor TCP

El contexto que se pasa a las devoluciones de llamada de eventos del servidor TCP:

- **ctxt.output**: El siguiente contexto de procesamiento en el proceso. Los controladores de devolución de llamada de extensión pueden enviar datos de tipo ns.tcp.stream a ctxt.output mediante los eventos DATA, que significa mensaje parcial o EOM que significa mensaje final del protocolo.
- **ctxt.input**: El contexto de procesamiento anterior en el proceso de donde provienen los datos de flujo TCP.

- **ctxt:hold(data)**: Función para almacenar los datos para su procesamiento futuro. Al llamar a la retención con datos, los datos se almacenan en el contexto. Más tarde, cuando se reciben más datos en el mismo contexto, los datos recién recibidos se anexan a los datos almacenados anteriormente y el flujo de datos combinado se pasa a la función de devolución de llamada on_data. Después de llamar a una retención, la referencia de datos ya no es utilizable y da error en cualquier uso.
- **ctxt.vserver**: El contexto del servidor virtual.
- **ctxt.server**: Contexto de procesamiento de conexión de servidor. Este contexto de procesamiento se puede utilizar para enviar datos al servidor y para obtener información relacionada con la conexión, como dirección IP, puertos de origen y destino.
- **ctxt:reuse_server_connection ()** : Esta API se utiliza para permitir que la conexión del servidor se reutilice para otras conexiones de cliente solo en el contexto del servidor. Esta API solo se puede utilizar si se utiliza un evento EOM (en la API ns.send ()) para enviar los datos en el contexto del cliente. De lo contrario, el dispositivo ADC genera un error.

  Para permitir que otros clientes reutilicen una conexión de servidor, se debe llamar a esta API al final de cada mensaje de respuesta. Después de llamar a esta API, si se reciben más datos en esta conexión de servidor, se trata como un error y se cierra la conexión del servidor. Si no se utiliza esta API, la conexión del servidor solo se puede utilizar para el cliente para el que se abrió. Además, si se selecciona el mismo servidor para otra decisión de equilibrio de carga para ese cliente, se utiliza la misma conexión de servidor para enviar los datos del cliente. Después de utilizar esta API, la conexión del servidor deja de vincularse a la conexión del cliente para la que se abrió y se puede volver a utilizar para una nueva decisión de equilibrio de carga para cualquier otra conexión del cliente. Después de llamar a esta API, el contexto del servidor ya no es utilizable y arroja un error en cualquier uso.

  Nota: Esta API está disponible en Citrix ADC 12.1, compilación 49.xx y versiones posteriores.
- **ctxt:close ()**: Cierra la conexión del servidor enviando FIN al servidor. Después de llamar a esta API, el contexto de procesamiento del cliente ya no es utilizable y muestra un error en cualquier uso.

  Nota: Esta API está disponible en Citrix ADC 12.1, compilación 50.xx y versiones posteriores.

Contexto de servidor virtual

El contexto del servidor virtual de usuario disponible a través de los contextos pasados a devoluciones de llamada:

- **vserver:counter_increment (counter_name)**: Incrementa el valor de un contador de servidor virtual pasado como argumento. Actualmente se admiten los siguientes contadores integrados.
  - **- invalid_messages**: Número de solicitudes/respuestas no válidas en este servidor virtual.

  - **- invalid_messages_Dropped**: Número de solicitudes o respuestas no válidas descartadas por este servidor virtual.
- **vserver.params**: Los parámetros configurados para el servidor virtual del usuario. Los parámetros proporcionan la configurabilidad de las extensiones. El código de extensión puede acceder a los parámetros especificados en la CLI para agregar un servidor virtual de usuario.

Contexto de conexión de cliente

Contexto de procesamiento de conexión de cliente para obtener información relacionada con la conexión.

- **client.ssl**: Contexto SSL
- **client.tcp**: Contexto TCP
- **client.is_ssl**: True si la conexión del cliente está basada en SSL

Contexto de conexión de servidor

Contexto de procesamiento de conexión del servidor para obtener información relacionada con la conexión.

- **server.ssl**: Contexto SSL
- **server.tcp**: Contexto TCP
- **server.is_ssl**: True si la conexión del servidor está basada en SSL

Contexto TCP

El contexto TCP opera en el protocolo TCP.

- **tcp.srcport**: Puerto de origen como número
- **tcp.dstport: Puerto** de destino como un número

Contexto de IP

El contexto IP funciona con datos de protocolo IP o IPv6.

- **ip.src**: Contexto de dirección IP de origen.
- **ip.dst**: Contexto de dirección IP de destino.

Nota: Esta API está disponible en Citrix ADC 12.1, compilación 51.xx y versiones posteriores.

Contexto de dirección IP

El contexto de la dirección IP funciona con datos de direcciones IP o IPv6.

- **<address>.to_s**: La cadena de dirección en la notación ASCII apropiada.
- **<address>.to_n**: El valor numérico de la dirección como una cadena de bytes en orden de red (4 bytes para IPv4 y 16 bytes para IPv6).
- **<address>.version**: Devuelve 4 para IPv4 y 6 para IPv6.
- **<address>:subnet(<prefix value>)**: Devuelve la cadena de dirección de subred después de aplicar el número de prefijo.
  - Para la dirección IPv4, el valor debe estar entre 0 y 32
  - Para la dirección IPv6, el valor debe estar entre 0 y 128.
- **<address>:apply_mask(<mask string>)**: Devuelve la cadena de dirección después de aplicar la cadena de máscara. API valida la versión del argumento y realiza la comprobación de errores adecuada.
- **address>:eq(<address string>)**: Devuelve verdadero o falso basado en si el argumento es equivalente al objeto de dirección. API valida la versión de los argumentos.

Nota: Esta API está disponible en Citrix ADC 12.1, compilación 51.xx y versiones posteriores.

Contexto de SSL

El contexto SSL proporciona información relacionada con la conexión SSL frontend.

- **ssl.cert**: Contexto de certificado SSL. Para la conexión de cliente, proporciona contexto de certificado de cliente y para la conexión de servidor, proporciona contexto de certificado de servidor.
- **ssl.version**: Un número que representa la versión del protocolo SSL de la transacción actual, de la siguiente manera:
  - - 0: The transaction is not SSL-based
  - - 0x002: The transaction is SSLv2
  - - 0x300: The transaction is SSLv3
  - - 0x301: The transaction is TLSv1
  - - 0x302: The transaction is TLSv1.1
  - - 0x303: The transaction is TLSv1.2
- **ssl.cipher_name**: Nombre de cifrado SSL como cadena si se invoca desde una conexión SSL, de lo contrario da cadena NULL.
- **ssl.cipher_bits**: Número de bits en clave criptográfica.

Contexto de certificado SSL

- **cert.version**: Número de versión del certificado. Si la conexión no está basada en SSL, devuelve 0.
- **cert.valid_not_before**: Fecha en formato de cadena antes de la cual el certificado no es válido.

- **CERT.VALID_NOT_After**: Fecha en formato de cadena después de la cual el certificado ya no es válido.
- **Cert.days_to_Expirate**: Número de días antes de los cuales el certificado es válido. Devuelve -1 para el certificado caducado.
- **Cert.to_PEM**: Certificado en formato binario.
- **cert.issuer**: Nombre distinguido (DN) del emisor en el certificado como una lista nombre-valor. Un signo igual ("=") es el delimitador para el nombre y el valor, y la barra diagonal ("/") es el delimitador que separa los pares nombre-valor.

  A continuación se muestra un ejemplo del DN devuelto:
  /C =us/o=miempresa/ou=www.mycompany.com/cn=www.mycompany.com/emailAddress=myuserid@mycompany.com
- **cert.auth_keyid**: Extensión del identificador de clave de contexto de autoridad del certificado X.509 V3.
  - **auth_keyid.exists**: TRUE si el certificado contiene una extensión de identificador de clave de autoridad.
  - **auth_keyid.issuer_name**: Emisor Distinguido Nombre en el certificado como una lista nombre-valor.
    Un signo igual ("=") es el delimitador para el nombre y el valor, y la barra diagonal ("/") es el delimitador que separa los pares nombre-valor.

  He aquí un ejemplo:
  /C=US/O=myCompany/OU=www.mycompany.com/CN=www.mycompany.com/emailAddress=myuserid@n
  - **auth_keyid.keyid**: Campo KeyIdentifier del identificador de clave de autoridad como un blob
  - **auth_keyid.cert_serialnumber**: Campo SerialNumber del identificador de clave de autoridad como un blob.
- **cert.pk_algorithm**: Nombre del algoritmo de clave pública utilizado por el certificado.
- **cert.pk_size**: Tamaño de la clave pública utilizada en el certificado.
- **cert.serialnumber: Número** de serie del certificado de cliente. Si se trata de una transacción que no sea SSL o hay un error en el certificado, esto da una cadena vacía.
- **cert.signature_algorithm**: Nombre del algoritmo criptográfico utilizado por la CA para firmar este certificado.
- **cert.subject_keyid**: Sujeto KeyID del certificado de cliente. Si no hay Subject KeyID, esto da un objeto de texto de longitud cero.
- **cert.subject**: Nombre distinguido del sujeto como nombre-valor. Un signo igual ("=") separa nombres y valores y una barra diagonal ("/") delimita los pares nombre-valor.

He aquí un ejemplo:
/C=US/O=myCompany/OU=www.mycompany.com/CN=www.mycompany.com/emailAddress=myuserid@mycom

Bibliotecas de Citrix ADC

- **ns.tcp.stream**: Cadena como biblioteca para el manejo de datos TCP como una secuencia de bytes. El tamaño máximo de los datos de flujo TCP en los que pueden trabajar estas API es de 128 KB. Las funciones de biblioteca ns.tcp.stream también se pueden llamar en el estilo habitual de llamada orientado a objetos de extensión. Por ejemplo, data:len () es lo mismo que ns.tcp.stream.len (data)
  - **ns.tcp.stream.len (data)**: Devuelve la longitud de los datos en bytes, similar al string.len de Lua
  - **ns.tcp.stream.find (data, pattern [, init])**- Función similar a la cadena.find de Lua. Además, también hace una coincidencia parcial al final de los datos. Tras la coincidencia parcial, se devuelve el índice inicial y el índice final se convierte en nulo.
  - **ns.tcp.stream.split (data, length)**: Divide los datos en dos fragmentos, el primer fragmento es de la longitud especificada. Después de una división correcta, los datos originales ya no se pueden utilizar como una secuencia de datos TCP. Cualquier intento de usarlo de esa manera causa un error.
  - **ns.tcp.stream.byte (data[, i [, j]])**- Función similar al string.byte de Lua. Devuelve los códigos numéricos internos de los caracteres data[i], data[i+1],..., data[j].
  - n**s.tcp.stream.sub (data, i [, j])**- Función similar a string.sub de Lua. Devuelve la subcadena de s que comienza en i y continúa hasta j.
  - **ns.tcp.stream.match (data, pattern,[, init])**: Función similar a la cadena de Lua. Busca la primera *coincidencia* de patrón en la cadena s.
- **ns.send (processing_ctxt, event_name, event_data)**: Función genérica para enviar eventos a un contexto de procesamiento. Los datos de eventos son una tabla Lua que puede tener cualquier contenido. El contenido depende del evento. Después de llamar a la API ns.send (), la referencia de datos ya no es utilizable. Cualquier intento de usarlo provoca un error.
- **ns.pipe (src_ctxt, dest_ctxt)**: Mediante una llamada a la API pipe (), el código de extensión puede conectar el contexto de origen a un contexto de destino. Después de una llamada a proceso, todos los eventos que se envían desde el contexto de origen al siguiente módulo del proceso van directamente al contexto de destino. Esta API suele ser utilizada por el módulo que realiza la llamada pipe (), para eliminarse del proceso.
- **ns.inet**: Biblioteca para direcciones de Internet.
  - **ns.inet.apply_mask (address_str, mask_str)**: Devuelve la cadena de dirección después de aplicar la cadena de máscara.

- **ns.inet.aton (address_str)**: Devuelve el valor numérico de la dirección como una cadena de bytes en orden de red (4 bytes para IPv4 y 16 para IPv6).
- **ns.inet.ntoa (byte_str)**: Convierte el valor de byte numérico como una cadena de bytes a la cadena de dirección.
- **ns.inet.ntohs (number)**: Convertir el orden de bytes de red dado al orden de bytes del host. Si la entrada es mayor que 2^16: 1, entonces arroja un error.
- **ns.inet.htons (number)**: Convierte el orden de bytes del host dado al orden de bytes de red. Si la entrada es mayor que 2^16: 1, entonces arroja un error.
- **ns.inet.ntohl (number)**: Convierte el orden de bytes de red dado al orden de bytes del host. Si la entrada es mayor que 2^32: 1, entonces arroja un error.
- **ns.inet.htonl (number)**: Convierte el orden de bytes del host dado al orden de bytes de red. Si la entrada es mayor que 2^32: 1, entonces arroja un error.
- **ns.inet.subnet (address_str, subnet_value)**: Devuelve la cadena de dirección de subred después de aplicar una subred dada.

Extensiones de protocolo

August 20, 2021

Los dispositivos Citrix ADC tienen compatibilidad nativa con protocolos como HTTP. Además de esto, puede usar extensiones de protocolo para agregar compatibilidad con protocolos personalizados. Actualmente solo se admiten protocolos personalizados basados en TCP, por ejemplo, el protocolo Message Queue Server Telemetry Transport (MQTT). Para transacciones seguras, TCP sobre SSL también es compatible.

Las extensiones de protocolo del dispositivo Citrix ADC forman parte de la infraestructura de scripts de alto nivel disponible en el dispositivo Citrix ADC. El lenguaje de scripting se basa en el lenguaje de programación Lua 5.2. Para agregar un protocolo personalizado a un dispositivo Citrix ADC, el usuario debe escribir código de extensión para implementar los comportamientos aplicables. Por ejemplo, los comportamientos ns.tcp.client y ns.tcp.server son aplicables a los protocolos basados en TCP. Para implementar un comportamiento, implemente solo las devoluciones de llamada que quiere personalizar. Si no se implementa la devolución de llamada, su valor predeterminado tiene efecto. Para obtener más información sobre el lenguaje de scripts, consulte Extensiones de Citrix ADC: descripción general del idioma. Para obtener más información sobre los comportamientos, consulte Referencia de API de Citrix ADC Extensions.

Las extensiones de protocolo Citrix ADC se pueden utilizar para lo siguiente:

- Agregue compatibilidad con nuevos protocolos en el dispositivo Citrix ADC mediante programación, mediante extensiones.

- Analice el tráfico de protocolo y realice el equilibrio de carga basado en mensajes específicos (MBLB).
- Configure la persistencia de equilibrio de carga definida por el usuario.

Extensiones de protocolo: Arquitectura

August 20, 2021

Para lograr la extensibilidad a nivel de tráfico, el procesamiento del tráfico en un dispositivo Citrix ADC se expone como una procesión de módulos de procesamiento independientes. El tráfico fluye a través de ellos a medida que lo procesa desde la entrada hasta la salida. Estos módulos en el proceso siguen un modelo de nada compartido. El paso de mensajes se utiliza para enviar los datos de tráfico de un módulo en el proceso al siguiente módulo.

Algunos puntos del proceso de procesamiento de tráfico se hacen extensibles, de modo que puede agregar código para personalizar el comportamiento de Citrix ADC.

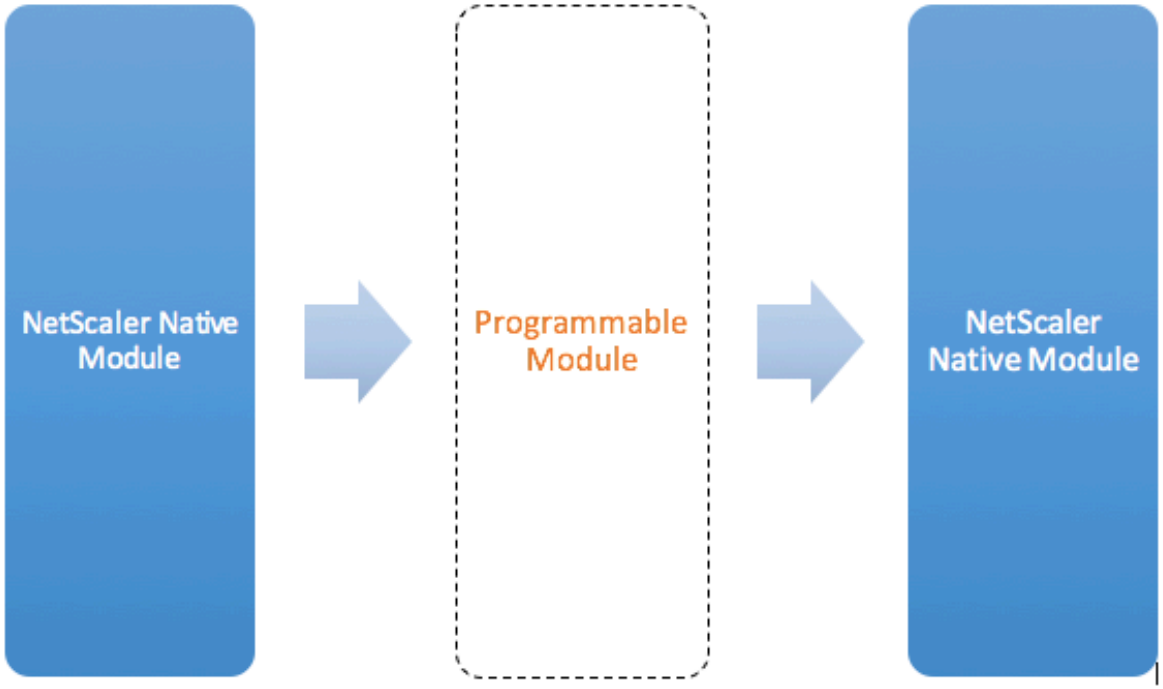


Figure: A Programmable Module In the Traffic Pipeline

De forma predeterminada, el tráfico omite un módulo programable al que no se agrega ningún código.

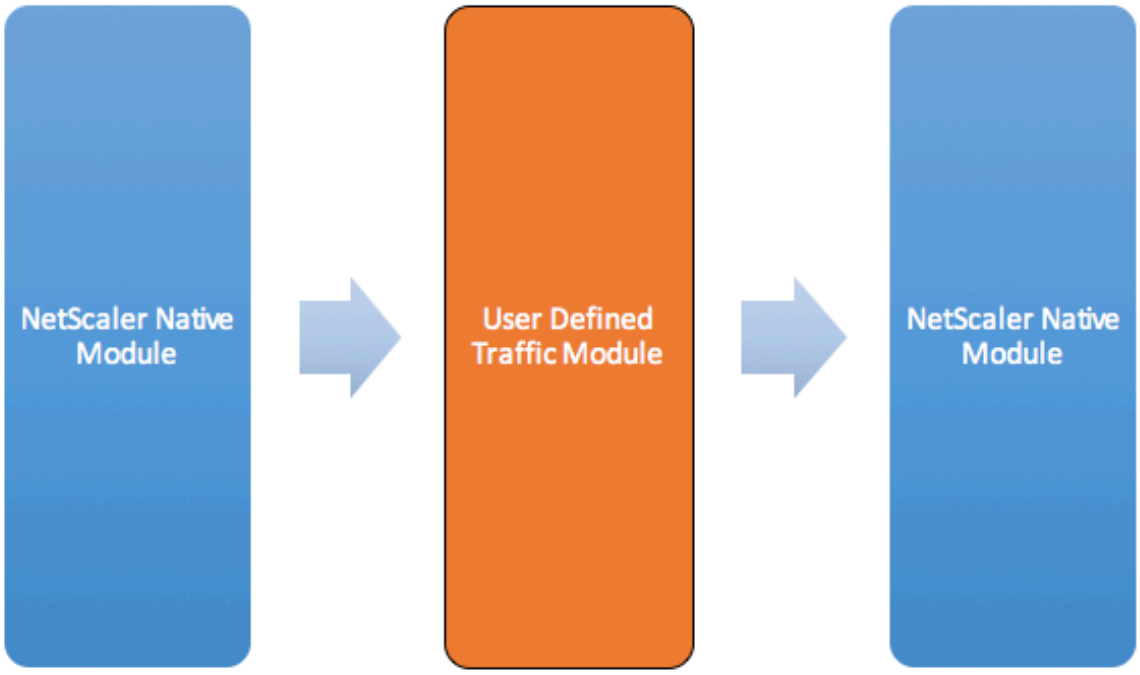


Figure: User Defined Traffic Module

Comportamientos

Las interfaces programables para personalizar el manejo del tráfico se denominan comportamientos. Los comportamientos son básicamente una formalización de patrones programables comunes que están disponibles en un dispositivo Citrix ADC. Los comportamientos consisten en un conjunto predefinido de funciones de devolución de llamada de eventos. Puede implementar un comportamiento proporcionando funciones de devolución de llamada que se ajusten al comportamiento.

Por ejemplo, el comportamiento del cliente TCP consiste en una función de devolución de llamada (on_data) que procesa eventos de flujo de datos del cliente TCP. Para implementar Equilibrio de carga basado en mensajes (MBLB) para un protocolo basado en TCP, puede agregar código para esta función de devolución de llamada para procesar la secuencia de datos TCP desde el cliente y analizar la secuencia de bytes en mensajes de protocolo.

Contexto:

Las funciones de devolución de llamada en un comportamiento se llaman con un contexto, que es el estado del módulo de procesamiento. El contexto es la instancia del módulo de procesamiento. Por ejemplo, las devoluciones de llamada del comportamiento del cliente TCP se llaman con contextos diferentes para diferentes conexiones TCP de cliente.

Carga útil:

Además del contexto, las devoluciones de llamada de comportamiento pueden tener otros argumentos. Por lo general, el resto de los argumentos se pasan como carga útil, que es la colección de todos los argumentos.

Por lo tanto, las instancias del módulo de procesamiento programable se pueden ver como una combinación de estado de instancia más funciones de devolución de llamada de evento, es decir, el contexto más comportamiento. Y el tráfico fluye a través del proceso como carga útil de eventos.

Para obtener información sobre las extensiones de API de Citrix ADC, consulte Referencia de la API de extensiones de Citrix ADC.

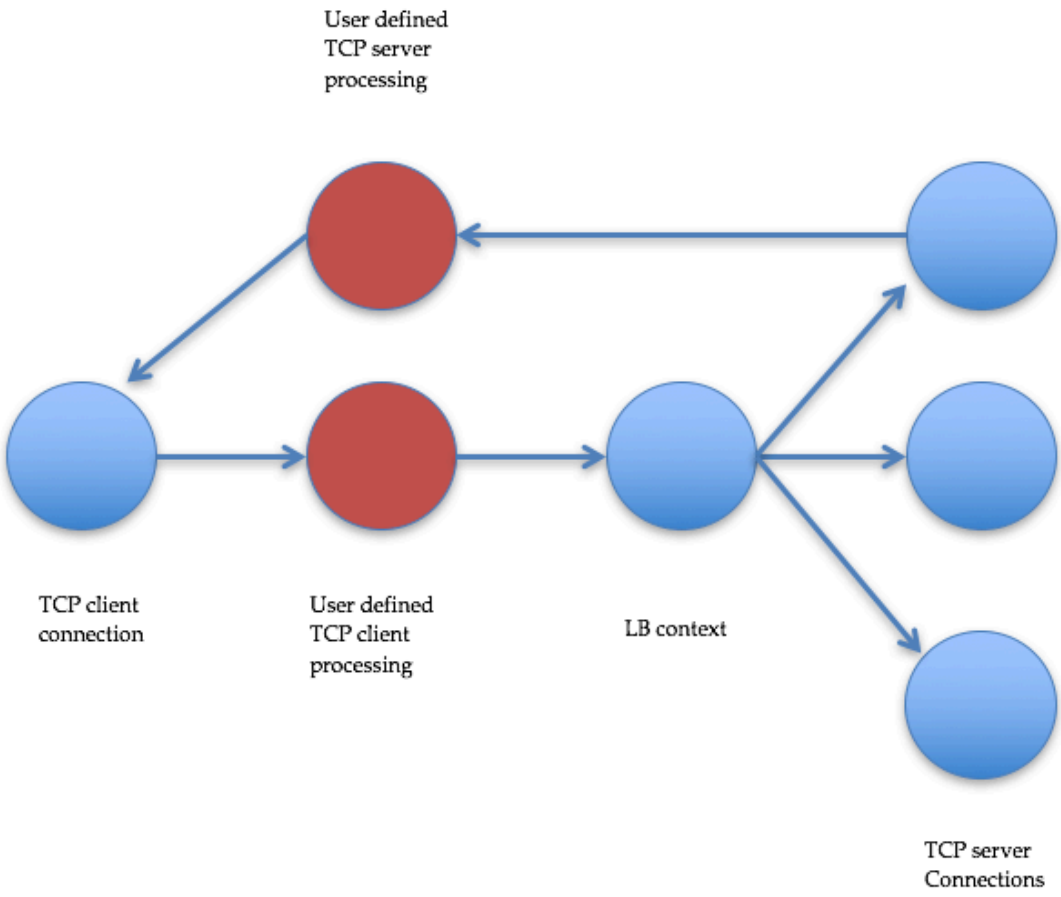
El siguiente fragmento de código muestra una función definida por el usuario para manejar eventos de flujo de datos de cliente TCP. El contexto y la carga útil se transfieren a la función mediante el código Citrix ADC. Este código simplemente reenvía los datos TCP recibidos en cada llamada al siguiente contexto del módulo de procesamiento en el proceso. En este caso, el siguiente módulo es el contexto de equilibrio de carga (LB), que es un módulo nativo de Citrix ADC.

```
function client.on_data(ctxt, payload)
    ns.send(ctxt.output, "DATA", {
 data = payload.data }
 )
end
<!--NeedCopy-->
```

Extensiones de protocolo: Proceso de tráfico para comportamientos de servidor y cliente TCP definidos por el usuario

August 20, 2021

La siguiente ilustración ilustra la extensión de protocolo de ejemplo: Proceso de tráfico para comportamientos de servidor y cliente TCP definidos por el usuario



Traffic Pipeline For User Defined TCP Client And Server Behaviors

Agregar un protocolo personalizado mediante extensiones de protocolo

Los comandos de interfaz de línea de comandos (CLI) para el protocolo personalizado utilizan la palabra clave “user” para indicar la naturaleza definida por el usuario de las entidades de configuración subyacentes. Con la ayuda del código de extensión, puede agregar un nuevo protocolo de usuario al sistema y agregar servidores virtuales de usuario para protocolos definidos por el usuario. Los servidores virtuales de usuario son a su vez configurables mediante la configuración de parámetros. Los valores configurados para los parámetros del servidor virtual están disponibles en el código de extensión.

El siguiente ejemplo ilustra el flujo de usuario para agregar compatibilidad con un nuevo protocolo. El ejemplo agrega compatibilidad con el protocolo MQTT al sistema. MQTT es un protocolo de conectividad “Internet de las cosas” de máquina a máquina. Es un transporte ligero de mensajería de publicación/suscripción. Este protocolo, útil para conexiones con ubicaciones remotas, utiliza herramientas de cliente y broker para publicar mensajes a los suscriptores.

1. Importe el archivo de implementación de la extensión del protocolo MQTT al sistema Citrix ADC. El listado de códigos para mqtt.lua se muestra a continuación. El siguiente ejemplo importa el archivo de extensión MQTT alojado en un servidor web.

   ```
   import extension http://10.217.24.48/extensions/mqtt.lua mqtt_code
   ```

2. Agregue un nuevo protocolo basado en TCP de usuario al sistema mediante la extensión.

   ```
   add user protocol MQTT -transport TCP -extension mqtt_code
   ```

3. Agregue un vserver de equilibrio de carga de usuario y enlace servicios de back-end a él.

   ```
   add service mqtt_svr1 10.217.24.48 USER_TCP 1501
   add service mqtt_svr2 10.217.24.48 USER_TCP 1502
   add lb vserver mqtt_lb USER_TCP  - lbmethod USER_TOKEN
   bind lb vserver mqtt_lb mqtt_svr1
   bind lb vserver mqtt_lb mqtt_svr2
   <!--NeedCopy-->
   ```

4. Agregue un vserver de usuario para el protocolo recién agregado. Establezca el valor defaultlb en el servidor LB configurado anteriormente.

   ```
   add user vserver mqtt_vs MQTT 10.217.24.28 8765 -defaultLb mqtt_lb
   ```

5. Opcionalmente, habilite la persistencia de sesión MQTT basada en ClientID, establezca el tipo de persistencia en USERSESSION.

   ```
   set lb vserver mqtt_lb -persistenceType USERSESSION
   ```

Extensiones de protocolo: Casos de uso

August 20, 2021

Las extensiones de protocolo se pueden usar para los siguientes casos de uso.

- Equilibrio de carga basado en mensajes (MBLB)
- Transmisión
- Equilibrio de carga basado en token
- Persistencia del equilibrio de carga
- Equilibrio de carga basado en conexión TCP
- Equilibrio de carga basado en contenido
- SSL
- Modificar tráfico
- Origen del tráfico en el cliente o servidor

- Procesar datos sobre el establecimiento de conexión

Equilibrio de carga basado en mensajes

Las extensiones de protocolo admiten Equilibrio de carga basado en mensajes (MBLB), que puede analizar cualquier protocolo en un dispositivo Citrix ADC y equilibrar la carga los mensajes de protocolo que llegan a una conexión de cliente, es decir, distribuir los mensajes a través de varias conexiones de servidor. MBLB se logra mediante el código de usuario que analiza la secuencia de datos TCP del cliente.

La secuencia de datos TCP se pasa a las devoluciones de llamada on_data para comportamientos de cliente y servidor. El flujo de datos TCP está disponible para las funciones de extensión a través de una cadena Lua como interfaz. Puede utilizar una API similar a la API de cadena de Lua para analizar la secuencia de datos TCP.

Las API útiles incluyen:

```
data:len()
```

```
data:find()
```

```
data:byte()
```

```
data:sub()
```

```
data:split()
```

Una vez que el flujo de datos TCP se ha analizado en un mensaje de protocolo, el código de usuario logra el equilibrio de carga simplemente enviando el mensaje de protocolo al siguiente contexto disponible desde el contexto pasado a la devolución de llamada on_data para el cliente.

La API ns.send () se utiliza para enviar mensajes a otros módulos de procesamiento. Además del contexto de destino, la API de envío toma el nombre del evento y la carga útil opcional como argumentos. Hay correspondencia uno a uno entre el nombre del evento y los nombres de las funciones de devolución de llamada para los comportamientos. Las devoluciones de llamada para eventos se llaman on_<event_name>. Los nombres de devolución de llamada utilizan solo minúsculas.

Por ejemplo, las devoluciones de llamada on_data del cliente TCP y del servidor son manejadores definidos por el usuario para eventos denominados “DATA”. Para enviar todo el mensaje de protocolo en una llamada de envío, se utiliza el evento EOM. EOM, que significa fin del mensaje, significa el final del mensaje de protocolo al flujo descendente del contexto LB, por lo que se toma una nueva decisión de equilibrio de carga para los datos que siguen a este mensaje.

Es posible que el código de extensión a veces no reciba todo el mensaje de protocolo en el evento on_data. En tal caso, los datos pueden conservarse mediante la API ctxt:hold (). La API de retención está disponible tanto para contextos TCP-cliente como de devolución de llamada de servidor. Cuando se llama a “retener con datos”, los datos se almacenan en el contexto. Cuando se reciben más datos

en el mismo contexto, los datos recién recibidos se anexan a los datos almacenados anteriormente y la función de devolución de llamada on_data se vuelve a llamar con los datos combinados.

Nota: El método de equilibrio de carga utilizado depende de la configuración del servidor virtual de equilibrio de carga correspondiente al contexto de equilibrio de carga.

El siguiente fragmento de código muestra el uso de la API de envío para enviar el mensaje de protocolo analizado.

Ejemplo:

```
    function client.on_data(ctxt, payload)
        --
        -- code to parse payload.data into protocol message comes here
        --
        -- sending the message to lb
        ns.send(ctxt.output, ”EOM”, {
data = message }
)
    end -- client.on_data

    function server.on_data(ctxt, payload)
        --
        -- code to parse payload.data into protocol message comes here
        --
        -- sending the message to client
        ns.send(ctxt.output, ”EOM”, {
data = message }
)

    end -- server.on_data
<!--NeedCopy-->
```

Transmisión

En algunos casos, es posible que no sea necesario mantener la secuencia de datos TCP hasta que se recopile todo el mensaje de protocolo. De hecho, no se aconseja a menos que sea necesario. Mantener los datos aumenta el uso de memoria en el dispositivo Citrix ADC y puede hacer que el dispositivo sea susceptible a ataques DDoS al agotar la memoria en el dispositivo Citrix ADC con mensajes de protocolo incompletos en muchas conexiones.

Los usuarios pueden lograr la transmisión de datos TCP en los controladores de devolución de llamada de extensión mediante la API de envío. En lugar de mantener los datos hasta que se recopile

todo el mensaje, los datos se pueden enviar en fragmentos. El envío de datos a ctxt.output mediante el evento DATA envía un mensaje de protocolo parcial. Puede ser seguido por más eventos DATA. Se debe enviar un evento EOM para marcar el final del mensaje de protocolo. El contexto de equilibrio de carga descendente toma la decisión de equilibrio de carga sobre los primeros datos recibidos. Una nueva decisión de equilibrio de carga se toma después de la recepción del mensaje EOM.

Para transmitir datos de mensajes de protocolo, envíe varios eventos DATA seguidos de un evento EOM. Los eventos DATA contiguos y el siguiente evento EOM se envían a la misma conexión de servidor seleccionada por decisión de equilibrio de carga para el primer evento DATA de la secuencia.

Para un contexto de envío al cliente, los eventos EOM y DATA son efectivamente los mismos, ya que no hay un manejo especial por parte del contexto cliente downstream para eventos EOM.

Equilibrio de carga basado en token

Para los protocolos compatibles de forma nativa, un dispositivo Citrix ADC admite un método de equilibrio de carga basado en token que utiliza expresiones PI para crear el token. Para las extensiones, el protocolo no se conoce de antemano, por lo que no se pueden usar expresiones PI. Para el equilibrio de carga basado en token, debe establecer el servidor virtual de equilibrio de carga predeterminado para utilizar el método de equilibrio de carga USER_TOKEN y proporcionar el valor del token desde el código de extensión llamando a la API de envío con un campo user_token. Si el valor del token se envía desde la API de envío y el método de equilibrio de carga USER_TOKEN se configura en el servidor virtual de equilibrio de carga predeterminado, la decisión de equilibrio de carga se toma calculando un hash basado en el valor del token. La longitud máxima del valor del token es de 64 bytes.

```
add lb vserver v\\_mqttlb USER\\_TCP -lbMethod USER\\_TOKEN
```

El fragmento de código del siguiente ejemplo utiliza una API de envío para enviar un valor de token LB.

Ejemplo:

```
1          -- send the message to lb
2
3
4
5
6          -- user_token is set to do LB based on clientID
7
8
9
10
11         ns.send(ctxt.output, ”EOM”, {
```



```
 data = message,

                                  user_token = token_info }
 )
<!--NeedCopy-->
```

Persistencia del equilibrio de carga

La persistencia del equilibrio de carga está estrechamente relacionada con el equilibrio de carga basado en token. Los usuarios deben poder calcular mediante programación el valor de la sesión de persistencia y usarlo para la persistencia de equilibrio de carga. La API de envío se utiliza para enviar parámetros de persistencia. Para utilizar la persistencia de equilibrio de carga, debe establecer el tipo de persistencia USERSESSION en el servidor virtual de equilibrio de carga predeterminado y proporcionar un parámetro de persistencia desde el código de extensión llamando a la API de envío con un campo user_session. La longitud máxima del valor del parámetro de persistencia es de 64 bytes.

Si necesita varios tipos de persistencia para un protocolo personalizado, debe definir tipos de persistencia de usuario y configurarlos. El implementador del protocolo decide los nombres de los parámetros utilizados para configurar los servidores virtuales. El valor configurado de un parámetro también está disponible para el código de extensión.

La siguiente CLI y fragmento de código muestra el uso de una API de envío para admitir la persistencia de equilibrio de carga. La lista de códigos de la sección Lista de códigos para mqtt.lua también ilustra el uso del campo user_session.

Para la persistencia, debe especificar el tipo de persistencia USERSESSION en el servidor virtual de equilibrio de carga y pasar el valor user_session desde la API ns.send.

```
add lb vserver v\\_mqttlb USER\\_TCP -persistencetype USERSESSION
```

Envíe el mensaje MQTT al equilibrador de carga, con el campo user_session establecido en ClientID en la carga útil.

Ejemplo:

```
-- send the data so far to lb

-- user_session is set to clientID as well (it will be used to persist
   session)

ns.send(ctxt.output,  “DATA” , {
 data = data, user_session = clientID }
```



```
 )
<!--NeedCopy-->
```

Equilibrio de carga basado en conexión TCP

Para algunos protocolos, MBLB podría no ser necesario. En su lugar, es posible que necesite equilibrio de carga basado en conexión TCP. Por ejemplo, el protocolo MQTT debe analizar la parte inicial de la secuencia TCP para determinar el token para el equilibrio de carga. Además, todos los mensajes MQTT en la misma conexión TCP deben enviarse a la misma conexión de servidor.

El equilibrio de carga basado en la conexión TCP se puede lograr mediante el uso de la API de envío con solo eventos DATA y no enviando ningún EOM. De esta forma, el contexto de equilibrio de carga descendente basa la decisión de equilibrio de carga en los datos recibidos primero y envía todos los datos posteriores a la misma conexión de servidor seleccionada por la decisión de equilibrio de carga.

Además, algunos casos de uso pueden requerir la capacidad de omitir el manejo de extensiones después de que se haya tomado la decisión de equilibrio de carga. Al omitir las llamadas de extensión se obtiene un mejor rendimiento, ya que el tráfico se procesa puramente mediante código nativo. Bypass se puede hacer mediante la API ns.pipe (). Una llamada al código de extensión API pipe () puede conectar el contexto de entrada a un contexto de salida. Después de la llamada a pipe (), todos los eventos provenientes del contexto de entrada van directamente al contexto de salida. Efectivamente, el módulo desde el que se realiza la llamada pipe () se elimina del proceso.

El siguiente fragmento de código muestra la transmisión y el uso de la API pipe () para omitir un módulo. La lista de códigos de la sección Lista de códigos para mqtt.lua también ilustra cómo hacer streaming y el uso de la API pipe () para omitir el módulo durante el resto del tráfico de la conexión.

Ejemplo:

```
        -- send the data so far to lb
        ns.send(ctxt.output, ”DATA”, {
 data = data,
                                        user_token = clientID }
 )
        -- pipe the subsequent traffic to the lb - to bypass the client
            on_data handler
        ns.pipe(ctxt.input, ctxt.output)
<!--NeedCopy-->
```


Equilibrio de carga basado en contenido

Para los protocolos nativos, se admite el cambio de contenido como función para las extensiones de protocolo. Con esta función, en lugar de enviar los datos al balance de carga predeterminado, puede enviar los datos al equilibrador de carga seleccionado.

La función de conmutación de contenido para las extensiones de protocolo se logra mediante el uso de la API ctxt:lb_connect (<lbname>). Esta API está disponible para el contexto del cliente TCP. Mediante esta API, el código de extensión puede obtener un contexto de equilibrio de carga correspondiente a un servidor virtual de equilibrio de carga ya configurado. A continuación, puede utilizar la API de envío con el contexto de equilibrio de carga así obtenido.

El contexto lb puede ser NULL a veces:

- El servidor virtual no existe
- El servidor virtual no es del tipo de protocolo de usuario
- El estado del servidor virtual no está UP
- El servidor virtual es un servidor virtual de usuario, no un servidor virtual de equilibrio de carga

Si quita el servidor virtual de equilibrio de carga de destino cuando esté en uso, se restablecerán todas las conexiones asociadas con ese servidor virtual de equilibrio de carga.

El siguiente fragmento de código muestra el uso de la API lb_connect (). El código asigna el ID del cliente a los nombres de servidor virtual de equilibrio de carga (lbname) mediante la tabla Lua lb_map y, a continuación, obtiene el contexto LB para lbname mediante lb_connect (). Y finalmente envía al contexto LB mediante la API de envío.

```
1     local lb_map = {
2
3        ["client1*"] = "lb_1",
4        ["client2*"] = "lb_2",
5        ["client3*"] = "lb_3",
6        ["client4*"] = "lb_4"
7      }
8
9
10    -- map the clientID to the corresponding LB vserver and connect to
         it
11    for client_pattern, lbname in pairs(lb_map) do
12       local match_idx = string.find(clientID, client_pattern)
13       if (match_idx == 1) then
14      lb_ctxt = ctxt:lb_connect(lbname)
15      if (lb_ctxt == nil) then
16         error("Failed to connect to LB vserver: " .. lbname)
17      end
```



```
18        break
19         end
20      end
21      if (lb_ctxt == nil) then
22      -- If lb context is NULL, the user can raise an error or send data
           to default LB
23         error("Failed to map LB vserver for client: " .. clientID)
24      end
25  -- send the data so far to lb
26  ns.send(lb_ctxt, "DATA", {
27   data = data }
28
29  <!--NeedCopy-->
```

SSL

SSL para protocolos que utilizan extensiones es compatible de formas similares a la compatibilidad con SSL para protocolos nativos. Mediante el mismo código de análisis para crear protocolos personalizados, puede crear una instancia de protocolo a través de TCP o SSL que luego se puede utilizar para configurar los servidores virtuales. Del mismo modo, puede agregar servicios de usuario a través de TCP o SSL.

Para obtener más información, consulte Configuración de la descarga SSL para MQTT y Configuración de la descarga SSL para MQTT con cifrado de extremo a extremo.

Multiplexación de conexión de servidor

A veces, el cliente envía una solicitud a la vez y envía la siguiente solicitud solo después de recibir la respuesta de la primera solicitud del servidor. En tal caso, la conexión del servidor se puede volver a utilizar para otras conexiones de cliente y para el siguiente mensaje en la misma conexión, después de que la respuesta se haya enviado al cliente. Para permitir la reutilización de la conexión del servidor por otras conexiones de cliente, debe utilizar la API ctxt: Reuse_server_connection () en el contexto del servidor.

Nota: Esta API está disponible en Citrix ADC 12.1, compilación 49.xx y versiones posteriores.

Modificar tráfico

Para modificar datos en la solicitud o respuesta, debe utilizar la función de reescritura nativa que utiliza una expresión de PI de directiva avanzada. Dado que no puede utilizar expresiones PI en extensiones, puede utilizar las siguientes API para modificar datos de una secuencia TCP.


```
data:replace(offset, length, new_string)
data:insert(offset, new_string)
data:delete(offset, length)
data:gsub(pattern, replace [,n]))
```

El siguiente fragmento de código muestra el uso de la API replace().

```
-- Get the offset of the pattern, we want to replace
   local old_pattern =  “pattern to repalace”
local old_pattern_length = old_pattern:len()
   local pat_off, pat_end = data:find(old_pattern)
   -- pattern is not present
if (not pat_off) then
    goto send_data
   end
  -- If the data we want to modify is not completely present, then
  -- wait for more data
  if (not pat_end) then
        ctxt:hold(data)
        data = nil
     goto done
  end
data:replace(pat_off, old_pattern_length,  “new pattern” )
::send_data::
ns.send(ctxt.output,  “EOM” , {
 data = data }
 )
::done::
```

El siguiente fragmento de código muestra el uso de la API de insert().

```
data:insert(5,  “pattern to insert” )
```

El siguiente fragmento de código muestra el uso de insert () API, cuando queremos insertar después o antes de algún patrón:

```
-- Get the offset of the pattern, after or before which we want to
    insert
   local pattern =  “pattern after/before which we need to insert”
local pattern_length = pattern:len()
```



```
    local pat_off, pat_end = data:find(pattern)
-- pattern is not present
    if (not pat_off) then
     goto send_data
    end
   -- If the pattern after which we want to insert is not
   -- completely present, then wait for more data
   if (not pat_end) then
         ctxt:hold(data)
         data = nil
      goto done
   end
-- Insert after the pattern
data:insert(pat_end + 1,  "pattern to insert" )
    -- Insert before the pattern
data:insert(pat_off,  "pattern to insert" )
::send_data::
     ns.send(ctxt.output,  "EOM" , {
 data = data }
 )
::done::
```

El siguiente fragmento de código muestra el uso de delete () API.

```
-- Get the offset of the pattern, we want to delete
    local delete_pattern =  "pattern to delete"
local delete_pattern_length = delete_pattern:len()
    local pat_off, pat_end = data:find(old_pattern)
    -- pattern is not present
if (not pat_off) then
          goto send_data
    end
   -- If the data we want to delete is not completely present,
   -- then wait for more data
   if (not pat_end) then
         ctxt:hold(data)
         data = nil
     goto done
   end
data:delete(pat_off, delete_pattern_length)
::send_data::
ns.send(ctxt.output,  "EOM" , {
 data = data }
```



```
20  )
21 ::done::
```

El siguiente fragmento de código muestra el uso de la API gsub ().

```
1     -- Replace all the instances of the pattern with the new string
2 data:gsub( “old pattern” , “new string” )
3 -- Replace only 2 instances of “old pattern”
4 data:gsub( “old pattern” , “new string” , 2)
5 -- Insert new_string before all instances of “http”
6 data:gsub( “input data” , “(http)” , “new_string%1” )
7 -- Insert new_string after all instances of “http”
8 data:gsub( “input data” , “(http)” , “%1new_string” )
9 -- Insert new_string before only 2 instances of “http”
10 data:gsub( “input data” , “(http)” , “new_string%1” , 2)
```

Nota: Esta API está disponible en Citrix ADC 12.1, compilación 50.xx y versiones posteriores.

Origen del tráfico en el cliente o servidor

Puede utilizar la API ns.send () para enviar datos que se originan desde el código de extensión a un cliente y un servidor back-end. Para enviar o recibir respuesta directamente con un cliente, desde el contexto del cliente, debe usar ctxt.client como destino. Para enviar o recibir respuesta directamente con un servidor back-end desde el contexto del servidor, debe usar ctxt.server como destino. Los datos en la carga útil pueden ser datos de flujo TCP o una cadena Lua.

Para detener el procesamiento del tráfico en una conexión, puede usar la API ctxt:close () desde el contexto del cliente o del servidor. Esta API cierra la conexión del lado del cliente o cualquier conexión del servidor vinculada a ella.

Cuando se llama a la API ctxt:close (), el código de extensión envía el paquete TCP FIN a las conexiones cliente y servidor y, si se reciben más datos del cliente o servidor en esta conexión, el dispositivo restablece la conexión.

El siguiente fragmento de código muestra el uso de las API ctxt.client y ctxt:close ().

```
1     -- If the input packet is not MQTT CONNECT type, then
2 -- send some error response to the client.
3 function client.on_data(ctxt, payload)
4     local data = payload.data
5     local offset = 1
6     local msg_type = 0
```



```
    local error_response =  “Missing MQTT Connect packet.”
    byte = data:byte(offset)
msg_type = bit32.rshift(byte, 4)
if (msg_type ~= 1) then
-- Send the error response
   ns.send(ctxt.client,  “DATA” , {
 data = error_response }
 )
-- Since error response has been sent, so now close the connection
    ctxt:close()
end
```

El siguiente fragmento de código muestra el ejemplo cuando el usuario puede inyectar los datos en el flujo de tráfico normal.

```
-- After sending request, send some log message to the server.
function client.on_data(ctxt, payload)
local data = payload.data
local log_message =  “client id :  “..data:sub(3, 7)..”  user name :  “
    data:sub(9, 15)
-- Send the request we get from the client to backend server
ns.send(ctxt.output,  “DATA” , {
 data = data }
 )
After sending the request, also send the log message
ns.send(ctxt.output,  “DATA” , {
 data = log_message”  }
 )
end
```

El siguiente fragmento de código muestra el uso de la API ctxt.to_server.

```
-- If the HTTP response status message is  “Not Found” ,
-- then send another request to the server.
function server.on_data(ctxt, payload)
    local data = payload.data
    local request  “GET /default.html HTTP/1.1\r\n\r\n” ss
    local start, end = data:find( “Not Found” )
    if (start) then
    -- Send the another request to server
        ns.send(ctxt.server,  “DATA” , {
 data = request }
```



```
 )
end
```

Nota: Esta API está disponible en Citrix ADC 12.1, compilación 50.xx y versiones posteriores.

Tratamiento de datos en el establecimiento de conexión

Puede haber un caso de uso en el que quiera enviar algunos datos al establecimiento de conexión (cuando se reciba el ACK final). Por ejemplo, en el protocolo proxy, es posible que quiera enviar direcciones IP y puertos de origen y destino del cliente al servidor back-end en el establecimiento de conexión. En este caso, puede utilizar el controlador de devolución de llamada client.init () para enviar los datos en el establecimiento de la conexión.

El siguiente fragmento de código muestra el uso de la devolución de llamada client.init ():

```
-- Send a request to the next processing context
-- on the connection establishment.
function client.init(ctxt)
   local request  "PROXY TCP4"  + ctxt.client.ip.src.to_s +  "  " +
      ctxt.client.ip.dst.to_s +  "  " + ctxt.client.tcp.srcport +  "  "
       +     ctxt.client.tcp.dstport
-- Send the another request to server
   ns.send(ctxt.output,  "DATA" , {
 data = request }
 )
  end
```

Nota: Esta API está disponible en Citrix ADC 13.0, compilación xx.xx y versiones posteriores.

Tutorial: Agregue el protocolo MQTT al dispositivo Citrix ADC mediante extensiones de protocolo

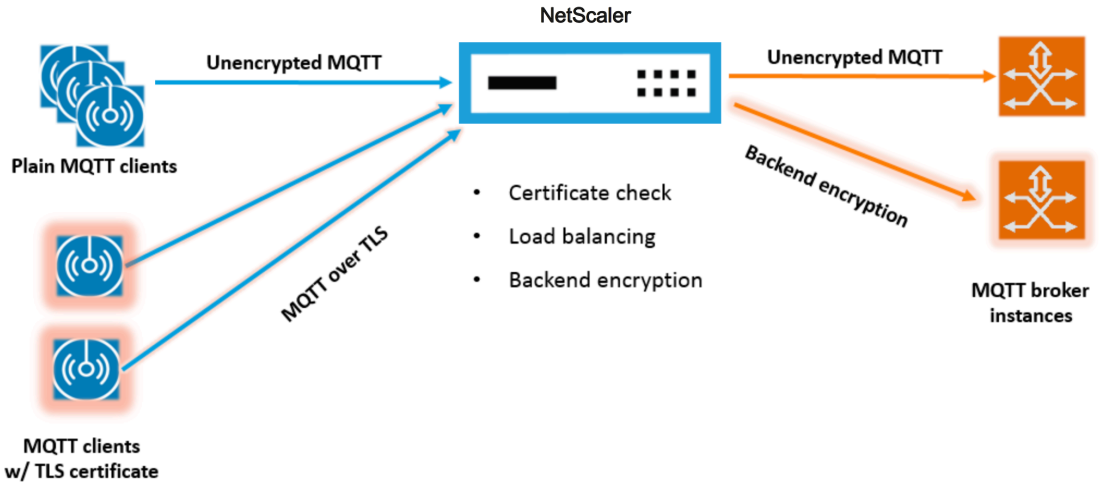
January 12, 2021

Los comandos de interfaz de línea de comandos (CLI) para el protocolo personalizado utilizan la palabra clave "user" para indicar la naturaleza definida por el usuario de las entidades de configuración subyacentes. Con la ayuda del código de extensión, puede agregar un nuevo protocolo de usuario al sistema y agregar servidores virtuales de usuario para protocolos definidos por el usuario. Los servidores virtuales de usuario son a su vez configurables mediante la configuración de parámetros. Los

valores configurados para los parámetros del servidor virtual están disponibles en el código de extensión.

El protocolo MQTT se utiliza con fines ilustrativos.

El siguiente diagrama ilustra un dispositivo Citrix ADC y las herramientas de agente y cliente MQTT.



Listado de códigos para mqtt.lua

January 12, 2021

La siguiente lista de códigos, mqtt.lua, proporciona el código para implementar el protocolo MQTT en Citrix ADC mediante extensiones de protocolo. El código solo tiene definida la función de devolución de llamada de datos del cliente TCP: Client.on_data (). Para los datos del servidor, no agrega una función de devolución de llamada y el servidor al cliente toma la ruta nativa rápida. Para los datos del cliente, el código analiza el mensaje del protocolo MQTT CONNECT y extrae el ID de cliente. A continuación, utiliza el ID de cliente para el valor user_token, que se utiliza para equilibrar la carga de todo el tráfico de cliente para la conexión basada en el ID de cliente estableciendo el método LB para el servidor de LB como USER_TOKEN. Utiliza el ID de cliente también para el valor user_session, que se puede utilizar para la persistencia de LB estableciendo el tipo de persistencia para el servidor de LB como USERSESSION. El código utiliza ns.send () para hacer LB y enviar los datos iniciales. Utiliza la API ns.pipe () para enviar el resto del tráfico del cliente directamente a la conexión del servidor, evitando las llamadas al controlador de devolución de llamada de extensión.

```
1 --[[
2
3   MQTT event handler for TCP client data
```



```
4
5       ctxt - TCP client side App processing context.
6
7       data - TCP Data stream received.
8
9       - parse the client ID from the connect message - the first message
            should be connect
10
11      - send the data to LB with ClientID as user token and session
12
13      - pipe the subsequent data to LB directly. This way the subsequent
            MQTT traffic will
14
15        bypass the tcp client on_data handler
16
17      - if a parse error is seen, throw an error so the connection is
            reset
18
19  --]]
20
21  function client.on_data(ctxt, payload)
22
23      local data = payload.data
24
25      local data_len = data:len()
26
27      local offset = 1
28
29      local byte = nil
30
31      local utf8_str_len = 0
32
33      local msg_type = 0
34
35      local multiplier = 1
36
37      local max_multiplier = 128 * 128 * 128
38
39      local rem_length = 0
40
41      local clientID = nil
42
43      -- check if MQTT fixed header is present (fixed header length is
            atleast 2 bytes)
44
```



```
45      if (data_len < 2) then
46
47          goto need_more_data
48
49      end
50
51      byte = data:byte(offset)
52
53      offset = offset + 1
54
55         -- check for connect packet - type value 1
56
57      msg_type = bit32.rshift(byte, 4)
58
59      if (msg_type ~= 1) then
60
61          error("Missing MQTT Connect packet.")
62
63      end
64
65      -- parse the remaining length
66
67      repeat
68
69          if (multiplier > max_multiplier) then
70
71             error("MQTT CONNECT packet parse error - invalid Remaining
                  Length.")
72
73         end
74
75         if (data_len < offset) then
76
77            goto need_more_data
78
79         end
80
81         byte = data:byte(offset)
82
83         offset = offset + 1
84
85         rem_length = rem_length + (bit32.band(byte, 0x7F) * multiplier)
86
87         multiplier = multiplier * 128
88
```



```
89      until (bit32.band(byte, 0x80) == 0)
90
91      -- protocol name
92
93      -- check if protocol name length is present
94
95      if (data_len < offset + 1) then
96
97         goto need_more_data
98
99      end
100
101     -- protocol name length MSB
102
103     byte = data:byte(offset)
104
105     offset = offset + 1
106
107     utf8_str_len = byte * 256
108
109     -- length LSB
110
111     byte = data:byte(offset)
112
113     offset = offset + 1
114
115     utf8_str_len = utf8_str_len + byte
116
117        -- skip the variable header for connect message
118
119     -- the four required fields (protocol name, protocol level, connect
            flags, keep alive)
120
121     offset = offset + utf8_str_len + 4
122
123     -- parse the client ID
124
125     --
126
127     -- check if client ID len is present
128
129     if (data_len < offset + 1) then
130
131        goto need_more_data
132
```



```
133     end
134
135        -- client ID length MSB
136
137     byte = data:byte(offset)
138
139     offset = offset + 1
140
141     utf8_str_len = byte * 256
142
143     -- length LSB
144
145     byte = data:byte(offset)
146
147     offset = offset + 1
148
149     utf8_str_len = utf8_str_len + byte
150
151     if (data_len < (offset + utf8_str_len - 1)) then
152
153         goto need_more_data
154
155     end
156
157     clientID = data:sub(offset, offset + utf8_str_len - 1)
158
159     -- send the data so far to lb, user_token is set to do LB based on
           clientID
160
161     -- user_session is set to clientID as well (it will be used to
           persist session)
162
163     ns.send(ctxt.output, "DATA", {
164  data = data,
165
166                                 user_token = clientID,
167
168                                 user_session = clientID }
169  )
170
171        -- pipe the subsequent traffic to the lb - to bypass the
              extension handler
172
173     ns.pipe(ctxt.input, ctxt.output)
174
```



```
175     goto parse_done
176
177     ::need_more_data::
178
179     ctxt:hold(data)
180
181     ::parse_done::
182
183     return
184
185 end
186 <!--NeedCopy-->
```

Configurar MQTT mediante extensiones de protocolo

August 20, 2021

Los pasos siguientes agregan un protocolo MQTT al dispositivo Citrix ADC.

Importe el archivo de extensión al dispositivo Citrix ADC, ya sea desde un servidor web (mediante HTTP) o desde su estación de trabajo local. Para obtener más información sobre cómo importar el archivo de extensión, consulte Importar extensiones.

```
import ns extension local:mqtt_generic_fs.lua mqtt_code
```

Agregue un nuevo protocolo basado en TCP de usuario al sistema mediante la extensión.

```
add user protocol MQTT -transport TCP -extension mqtt_code
```

Agregue un servicio de tipo USER_TCP para indicar que se trata de un protocolo definido por el usuario.

```
add service s1 10.102.90.112 USER_TCP 80
```

Agregue un vserver de equilibrio de carga de usuario y enlace servicios de back-end a él.

```
add lb vs mysv USER_TCP
```

```
bind lb vs mysv s1
```

Agregue un servidor virtual de usuario para el protocolo recién agregado y haga que el servidor virtual de equilibrio de carga configurado en el paso anterior sea el equilibrador de carga predeterminado.

```
add user vs v_mqtt MQTT 10.217.24.28 80 -defaultlb mysv
```

Opcionalmente, habilite la persistencia de sesión MQTT basada en ClientID, establezca el tipo de persistencia en USERSESSION.


```
set lb vserver mqtt_lb -persistenceType USERSESSION
```

Configuración de descarga SSL para MQTT

August 20, 2021

Puede implementar la descarga SSL para protocolos de usuario agregando una instancia SSL para el protocolo. El siguiente ejemplo muestra cómo hacer la descarga SSL para un protocolo de usuario. El tráfico a los servicios de back-end no está cifrado con esta configuración.

Nota: Este ejemplo no proporciona detalles relacionados con la adición o actualización de un par de claves de certificado y vincularlo a un servidor virtual. Para obtener más información, consulte Certificados SSL.

Los siguientes comandos agregan el protocolo MQTT_SSL incluyendo mqtt.lua con el valor de transporte “SSL”.

```
1 import extension http://10.217.24.48/extensions/mqtt.lua mqtt_code
2 add user protocol MQTT_SSL -transport SSL -extension mqtt_code
3 <!--NeedCopy-->
```

Los siguientes comandos agregan un servidor virtual de equilibrio de carga de usuario y vinculan servicios de back-end a él.

```
1 add service mqtt_svr1 10.217.24.48 USER_TCP 1501
2 add service mqtt_svr2 10.217.24.48 USER_TCP 1502
3 add lb vserver mqtt_lb USER_TCP  - lbMethod ROUNDROBIN
4 bind lb vserver mqtt_lb mqtt_svr1
5 bind lb vserver mqtt_lb mqtt_svr2
6 <!--NeedCopy-->
```

El siguiente comando agrega un servidor virtual de usuario para el protocolo MQTT_SSL recién agregado. El uso de MQTT_SSL significa que el dispositivo Citrix ADC realizará la descarga SSL, ya que MQTT_SSL se configuró con el transporte SSL. El comando también establece defaultlb en el servidor virtual de equilibrio de carga configurado en el paso anterior.

```
add user vserver mqtt_vs MQTT_SSL 10.217.24.28 8765 -defaultLb mqtt_lb
```

Para la descarga SSL, también debe habilitar la función SSL y vincular una clave de certificado al servidor virtual del usuario. Para obtener más información, consulte estos temas:

Agregar o actualizar un par de claves de certificado

Enlazar el par de claves de certificado al servidor virtual SSL

Ejemplo:

```
enable ns feature SSL

add SSL certKey mqtt_svr_cert_key -cert server1.cert -key server1.key

bind ssl vserver mqtt_vs  -certkeyName mqtt_svr_cert_key
<!--NeedCopy-->
```

Configuración de la descarga SSL con cifrado de extremo a extremo para MQTT

August 20, 2021

El siguiente ejemplo muestra cómo hacer la descarga SSL para MQTT con cifrado de extremo a extremo.

Nota: Este ejemplo no proporciona detalles relacionados con la adición o actualización de un par de claves de certificado y vincularlo a un servidor virtual. Para obtener más información, consulte Certificados SSL.

Los siguientes comandos importan el archivo de extensión y agregan el protocolo MQTT_SSL con el transporte SSL.

```
import extension http://10.217.24.48/extensions/mqtt.lua mqtt_code
add user protocol MQTT_SSL -transport SSL -extension mqtt_code
<!--NeedCopy-->
```

Los siguientes comandos agregan un servidor virtual de equilibrio de carga de usuario y vinculan servicios de back-end a él. Tanto el servidor virtual de equilibrio de carga como los servicios están configurados para el tipo de servicio USER_SSL_TCP.

```
add service mqtt_svr1 10.217.24.48 USER_SSL_TCP 1501
add service mqtt_svr2 10.217.24.48 USER_SSL_TCP 1502
add lb vserver mqtt_lb USER_SSL_TCP  - lbmethod RR
```



```
bind lb vserver mqtt_lb mqtt_svr1
bind lb vserver mqtt_lb mqtt_svr2
<!--NeedCopy-->
```

El siguiente comando agrega un servidor virtual de usuario para el protocolo MQTT_SSL recién agregado. El uso de MQTT_SSL significa que el dispositivo Citrix ADC realizará la descarga SSL, ya que MQTT_SSL se configuró con el transporte SSL. El comando también hace que el servidor virtual de equilibrio de carga, configurado en el paso anterior, sea el equilibrador de carga predeterminado.

```
add user vserver mqtt_vs MQTT_SSL 10.217.24.28 8765 -defaultLb mqtt_lb
```

Para el cifrado de extremo a extremo, también debe habilitar la función SSL y vincular una clave de certificado al usuario y a los servidores virtuales de equilibrio de carga predeterminados. Para obtener más información, consulte estos temas:

Agregar o actualizar un par de claves de certificado

Enlazar el par de claves de certificado al servidor virtual SSL

```
enable ns feature SSL

add SSL certKey mqtt_svr_cert_key -cert server1.cert -key server1.key

bind ssl vserver mqtt_lb  -certkeyName mqtt_svr_cert_key

bind ssl vserver mqtt_vs  -certkeyName mqtt_svr_cert_key
<!--NeedCopy-->
```

Tutorial: Equilibrio de carga de mensajes syslog mediante extensiones de protocolo

January 12, 2021

El protocolo Syslog disponible en el dispositivo Citrix ADC solo funciona para los mensajes generados en el dispositivo Citrix ADC. No equilibra la carga los mensajes procedentes de nodos externos. Para equilibrar la carga de dichos mensajes, debe utilizar la función de extensiones de protocolo y escribir la lógica de análisis de mensajes syslog mediante el lenguaje de programación Lua 5.2.

Código para analizar el mensaje syslog

El código solo tiene definida la función de devolución de llamada de datos del cliente TCP: Client.on_data (). Para los datos del servidor, no agrega una función de devolución de llamada y el servidor al cliente toma la ruta nativa rápida. El código identifica el límite del mensaje en función del carácter final. Si el paquete TCP contiene más de un mensaje syslog, entonces dividimos el paquete en función del carácter final y el equilibrio de carga de cada mensaje.

```
--[[

  Syslog event handler for TCP client data

    ctxt - TCP client side App processing context.

    data - TCP Data stream received.

--]]

function client.on_data(ctxt, payload)

                  local message = nil

                  local data_len

                  local data = payload.data

                  local trailing_character = "\n"

                  ::split_message::

                                    -- Get the offset of trailing
                                       character

                                    local new_line_character_offset =
                                       data:find(trailing_character)

                                    -- If trailing character is not
                                       found, then wait for more data.

                                    if (not new_line_character_offset)
                                       then

                                                        goto
```



```
                                                    need_more_data
32
33                                          end
34
35                                          -- Get the length of the current
                                               message
36
37                                          data_len = data:len()
38
39                                          -- Check whether we have more than
                                               one message
40
41                                          -- by comparing trailing character
                                               offset and
42
43                                          -- current data length
44
45                                          if (data_len >
                                               new_line_character_offset) then
46
47                                                      -- If we have
                                                           more than one
                                                           message, then
                                                           split
48
49                                                      -- the data into
                                                           two parts such
                                                            that first
                                                           part
50
51                                                      -- will contain
                                                           message upto
                                                           trailing
                                                           character
52
53                                                      -- offset and
                                                           second part
                                                           will contain
54
55                                                      -- remaining
                                                           message.
56
57                                                      message, data =
                                                           data:split(
                                                           new_line_character_offse
```



```
                                                                    )
58
59                                      else
60
61                                                          message = data
62
63                                                          data = nil
64
65                                      end
66
67  -- Send the data to the backend server.
68
69                                      ns.send(ctxt.output, ”EOM”, {
70   data = message }
71   )
72
73                                      goto done
74
75                                      ::need_more_data::
76
77                                                          -- Wait for more
                                                               data
78
79                                                          ctxt:hold(data)
80
81                                                          data = nil
82
83                                                          goto done
84
85                                      ::done::
86
87                                                          -- If we have
                                                               more data to
                                                               parse,
88
89                                                          -- then do
                                                               parsing again.
90
91                                                          if (data) then
92
93                                                                              goto
                                                                                  split_
94
```



```
95                                                                  end
96
97 end
98 <!--NeedCopy-->
```

Configurar el protocolo syslog mediante extensiones de protocolo

August 20, 2021

Los pasos siguientes agregan un protocolo SYSLOG de usuario al dispositivo Citrix ADC.

Importe el archivo de extensión al dispositivo Citrix ADC, ya sea desde un servidor web (mediante HTTP) o desde su estación de trabajo local. Para obtener más información sobre la importación del archivo de extensión, consulte Importación de extensiones.

```
import ns extension local:syslog_parser.lua syslog_parser_code
```

Agregue un nuevo protocolo basado en TCP de usuario al sistema mediante la extensión.

```
add user protocol USER_SYSLOG -transport TCP -extension syslog_parser_code
```

Agregue un servicio de tipo USER_TCP para indicar que se trata de un protocolo definido por el usuario.

```
add service s1 10.102.90.112 USER_TCP 80
```

Agregue un vserver de equilibrio de carga de usuario y enlace servicios de back-end a él.

```
1 add lb vs mysv USER_TCP
2
3 bind lb vs mysv s1
4 <!--NeedCopy-->
```

Agregue un servidor virtual de usuario para el protocolo recién agregado y haga que el servidor virtual de equilibrio de carga configurado en el paso anterior sea el equilibrador de carga predeterminado.

```
add user vs v_syslog USER_SYSLOG 10.217.24.28 80 -defaultlb mysv
```

Referencia de comandos de extensiones de protocolo

January 12, 2021

En la tabla siguiente se enumeran todos los nuevos comandos agregados para protocolos personalizados y los comandos existentes que se han modificado para protocolos personalizados.

`show lb persistentSessions [<vserv-name>]`

- **Comando CLI:**

  `add user protocol <name> -transport ( TCP | SSL )-extension <string> -comment <string>]>`

- **Descripción:**

  Agrega un nuevo protocolo de usuario al dispositivo Citrix ADC mediante extensiones. Actualmente solo se admiten protocolos de usuario con valor de transporte TCP o SSL.

  > **Ejemplo:**
  >
  > add user protocol MQTT -transport TCP -extension mqtt_code

- **Comando CLI:**

  `rm user protocol <name>`

- **Descripción:**

  Quita un protocolo de usuario agregado anteriormente al dispositivo Citrix ADC.

  > **Ejemplo:**
  >
  > rm user protocol mqtt

- **Comando CLI:**

  `set user protocol <name> -comment <string>`

- **Descripción:**

  Cambia la configuración de un protocolo de usuario agregado anteriormente al dispositivo Citrix ADC.

  > **Ejemplo:**
  >
  > establecer el protocolo de usuario mqtt -comment “implementación del protocolo MQTT”

- **Comando CLI:**

  `unset user protocol <name> -comment`

- **Descripción:**

  Elimina la configuración de un protocolo de usuario agregado anteriormente al dispositivo Citrix ADC.

> **Ejemplo:**
>
> unset user protocol mqtt -comment “MQTT protocol implementation”

- **Comando CLI:**

```
update ns extension <extension name>
```

- **Descripción:**

  Actualiza la implementación de un protocolo de usuario agregado anteriormente mediante extensiones.

  Puede actualizar la implementación del protocolo solo si el protocolo no está siendo utilizado por ningún servidor virtual de usuario.

> **Ejemplo:**
>
> update ns extension my-extension

- **Comando CLI:**

```
add lb vserver <name> [USER_TCP | USER_SSL_TCP] [-lbmethod USER_TOKEN]
[-persistencetype USERSESSION] [-timeout <value>]
```

- **Descripción:**

  Agrega un servidor virtual de equilibrio de carga al dispositivo Citrix ADC. Este es un comando CLI existente.

  Para servidores virtuales de usuario de equilibrio de carga, el tipo de servicio que se va a utilizar es USER_TCP o USER_SSL_TCP. La dirección IP y el puerto no están permitidos con los servidores virtuales de equilibrio de carga del usuario.

  Para los servidores virtuales de equilibrio de carga de usuario, solo se permite el método de equilibrio de carga ROUNDROBIN, y el valor del token lo proporciona el código de extensión. Del mismo modo, solo se permite la persistencia USERSESSION, y el valor de persistencia es proporcionado por el código de extensión.

> **Ejemplo:**
>
> add lb vserver mysv USER_TCP –lbmethod ROUNDROBIN

- **Comando CLI:**

```
add user vserver <name> <userProtocol> <IPAddress> <port> -defaultLB <
string> [-params <string>] [-comment <string>]
```

- **Descripción:**

  Agrega un servidor virtual para un protocolo de usuario mediante extensiones. El servidor virtual de equilibrio de carga de usuario predeterminado configurado está disponible para el con-

trolador de extensión de datos del cliente TCP como ctxt.output. Para un servidor virtual, los parámetros de extensión se pueden establecer mediante la opción -params con un nombre y un par de valores. El valor de parámetro correspondiente está disponible para los controladores de extensión como ctxt.vserver.params.<paramName>.

> **Ejemplo:**
>
> add user vs v_mqtt MQTT 10.217.24.28 80 -defaultlb mysv

- **Comando CLI:**

```
rm user vserver <name>
```

- **Descripción:**

Quita un servidor virtual de usuario agregado anteriormente al dispositivo Citrix ADC.

> **Ejemplo:**
>
> rm user vserver v_mqtt

- **Comando CLI:**

```
set user vserver <name> [-IPAddress <ip_addr|ipv6_addr|*>] [-defaultLB
<string>] [-params <string>] [-comment <string>]
```

- **Descripción:**

Cambia la configuración de un servidor virtual de usuario agregado anteriormente al dispositivo Citrix ADC. Cuando la opción -params asigna un nuevo valor a un parámetro de extensión, se sobrescribe el valor anterior.

> **Ejemplo:**
>
> set user vs v_mqtt MQTT 10.217.24.28 -defaultlb mysv -comment “MQTT protocol implementation”

- **Comando CLI:**

```
unset user vserver <name> [-params] [-comment]
```

- **Descripción:**

Elimina la configuración de un servidor virtual de usuario agregado anteriormente al dispositivo Citrix ADC. Si utiliza la opción —params para desactivar un parámetro de extensión, el valor de parámetro correspondiente disponible para los manejadores de extensiones se cambia a nil.

> **Ejemplo:**
>
> unset user vs v_mqtt MQTT 10.217.24.28 -defaultlb mysv -comment “MQTT protocol implementation”

- **Comando CLI:**

  ```
  show user protocol [<name>]
  ```

- **Descripción:**

  Muestra información sobre un protocolo de usuario, como la extensión y las devoluciones de llamada.

  > **Ejemplo:**
  >
  > show user protocol mqtt

- **Comando CLI:**

  ```
  show user vserver [<name>]
  ```

- **Descripción:**

  Muestra información sobre un servidor virtual de usuario.

  > **Ejemplo:**
  >
  > show user vserver vs_mqtt

- **Comando CLI:**

  ```
  stat user vserver [<name>]
  ```

- **Descripción:**

  Muestra estadísticas sobre un servidor virtual de usuario.

  > **Ejemplo:**
  >
  > stat user vserver vs_mqtt

- **Comando CLI:**

  ```
  show lb persistentSessions [<vserv-name>]
  ```

- **Descripción:**

  Muestra información sobre las sesiones persistentes. Esta es una CLI existente. Para los protocolos de usuario, el tipo de persistencia se muestra como USERSESSION.

- **Comando CLI:**

  ```
  rm lb vserver <name>
  ```

- **Descripción:**

  Quita un usuario LB vserver agregado anteriormente al dispositivo Citrix ADC.

> **Ejemplo:**
>
> rm lb vserver mysv

- **Comando CLI:**

```
add service <name> <IPAddr> (USER_TCP | USER_SSL_TCP)<Port>
```

- **Descripción:**

  Agrega un servicio back-end que se utilizará para un protocolo de usuario. Se trata de un comando CLI existente con nuevos tipos de servicio USER_TCP y USER_SSL_TCP.

> **Ejemplo:**
>
> add service mqtt_svr1 10.217.24.48 USER_TCP 1501
>
> **Nota**: Los comandos existentes "set service and unset service" se pueden utilizar para eliminar o cambiar la configuración de un servicio previamente agregado para un protocolo de usuario.

- **Comando CLI:**

```
bind lb vserver <name> <serviceName>
```

- **Descripción:**

  Enlaza un servicio a un servidor LB vserver de usuario. El tipo de servicio debe ser USER_TCP/USER_SSL_TCP para enlazar a un servidor LB con el tipo USER_TCP/USER_SSL_TCP.

> **Ejemplo:**
>
> bind lb vserver mysv mqtt_svr1

- **Comando CLI:**

```
unbind lb vserver <name> <serviceName>
```

- **Descripción:**

  Desvincula un servicio previamente enlazado a un servidor LB vserver de usuario.

> **Ejemplo:**
>
> unbind lb vserver mysv mqtt_svr1

- **Comando CLI:**

```
rm service <name>
```

- **Descripción:**

  Quita un servicio que se ha agregado anteriormente para un protocolo de usuario.

> **Ejemplo:**
>
> rm service mqtt_svr1

Solución de problemas de extensiones de protocolo

January 12, 2021

Si la función de extensión no se comporta como se esperaba, puede utilizar la funcionalidad de seguimiento de extensión para verificar el comportamiento de la función de extensión. También puede agregar el registro a la función de extensión mediante la funcionalidad de registro personalizado, donde puede definir el nivel de registro que se va a capturar en el dispositivo Citrix ADC.

Registro personalizado

También puede agregar su propio registro a su función de extensión. Para ello, utilice la función ns.logger:level () incorporada, donde level es emergencia, alerta, crítica, error, advertencia, aviso, información o depuración. Los parámetros son los mismos que la función C printf (): Una cadena de formato y un número variable de argumentos para proporcionar valores para el% especificado en la cadena de formato. Por ejemplo, puede agregar lo siguiente a la función COMBINE_HEADERS para registrar el resultado de una llamada:

```
local result_str = table.concat(combined_headers, "\r\n") .. "\r\n\r\n"

ns.logger:info("Result: %s", result_str)

return result_str
<!--NeedCopy-->
```

La función anterior registraría el siguiente mensaje a/var/log/ns.log para la entrada de ejemplo que se muestra en los ejemplos de mensajes de registro abreviados en la sección Seguimiento de extensión anterior.

```
... : default NSEXTENSION Message 143 0 : "Result: Host: 10.217.24.7:2000^M
 H1: abcd, 1234^M User-Agent: curl/7.24.0 (amd64-portbld-freebsd8.4)libcurl
/7.24.0 OpenSSL/0.9.8y zlib/1.2.3^M Accept: \*/\*^M H2: h2val1, h2val2,
h2val3^M ^M"
```


Extensiones de directivas

January 12, 2021

La función de extensión de directiva le permite escribir funciones de extensión para tipos de directiva integrados. Las extensiones se pueden utilizar en expresiones de directiva, al igual que las funciones integradas. Se ejecutan cuando se evalúan las expresiones de directiva correspondientes. Esta función es útil para:

- Adición de funciones personalizadas a directivas existentes.
- Implementación de construcciones lógicas para requerimientos complejos de clientes.

La función de extensión de directiva aborda estas limitaciones al permitir a los usuarios escribir funciones de extensión para los tipos de directiva integrados. Las extensiones se pueden utilizar en las expresiones de directiva, al igual que las funciones integradas. Se ejecutan cuando se evalúan las expresiones de directiva correspondientes.

En la tabla siguiente se enumeran los tipos de directivas que se pueden utilizar al escribir una extensión y sus asignaciones asociadas.

Tipo de directiva	Tipo de directiva asignado	Resultado
TEXTO_T	NSTEXT	Cadena
BOOL_AT	NSBOOL	Booleano
NÚMERO_AT	NSNUM	Número (punto flotante de doble precisión)
DOUBLE_AT	NSDOUBLE	Número (punto flotante de doble precisión)

Requisitos previos para el uso de extensiones de directiva

Las funciones importadas deben ajustarse a las normas de directiva existentes. Por lo tanto:

- El nombre de la función debe comenzar con una letra y puede contener números o guiones bajos.
- Las directivas Citrix ADC consideran que el nombre de la función no distingue entre mayúsculas y minúsculas.
- La función debe devolver un solo valor incluso si el lenguaje de extensión devuelve varios valores.
- Las funciones con un número variable de argumentos no son compatibles.

¿Cómo funcionan las extensiones de directivas?

Las directivas existentes en un dispositivo Citrix ADC utilizan un intérprete para evaluar las funciones, que se importan en un archivo de extensión de directiva. Cuando un usuario importa una nueva función en un archivo de extensión de directiva:

1. El archivo de extensión se valida para la sintaxis y otras condiciones.
2. Si la validación falla, el error se notifica al usuario.
3. Si la validación se realiza correctamente, el archivo de extensión se importa al dispositivo Citrix ADC y su contenido se puede utilizar en expresiones de directiva, al igual que cualquier función de directiva integrada
    a) Si la evaluación de la expresión de directiva devuelve un error durante el tiempo de ejecución, se informa como un evento undef y se incrementa el contador de errores asociado.
    Nota: Si se produce un evento undef de directiva y la regla de directiva contiene una o más funciones de extensión de directiva, el `show ns extension <name>` comando muestra los hits de undef cuando se aplican a esas extensiones de directiva. Si se anula la función de extensión, se incrementa el valor del contador de anulación.
    b) Si la evaluación de la expresión de directiva es correcta, la evaluación de la expresión se reanuda hasta que se evalúe toda la expresión o hasta que se aborte debido a un error.

Si la función de extensión tarda demasiado en ejecutarse, se anula y se incrementa el contador de errores correspondiente a esa función de extensión. La función de extensión está protegida, lo que impide:

- Uso excesivo de CPU en el dispositivo Citrix ADC.
- Uso excesivo de memoria en el dispositivo Citrix ADC.
- Uso de bibliotecas integradas perjudiciales o bibliotecas o binarios de terceros.
- Scripts de larga duración que podrían provocar el reinicio del dispositivo Citrix ADC.

Configuración de extensiones de directiva

August 20, 2021

Cuando el archivo de extensión de directiva esté listo, impórtelo al dispositivo Citrix ADC. El proceso de importación copia el archivo de extensión en un directorio del dispositivo Citrix ADC y comprueba si hay errores de sintaxis.

Después de la importación, debe hacer que el archivo de extensión esté disponible para su uso en las expresiones de directiva.

Nota: El comando de importación se utiliza para descargar el contenido del archivo de un origen externo \<src\>, o de un origen interno, en el sistema de archivos Citrix ADC. Para cargar el contenido

de este archivo en uno o varios motores de paquetes por primera vez, utilice el comando add. Si hay una actualización del contenido del archivo, el contenido actualizado se puede descargar en el sistema de archivos Citrix ADC ejecutando el comando import con el argumento de sobrescritura. El comando actualiza el contenido del sistema de archivos. Para cargar el contenido actualizado en uno o varios motores de paquetes, utilice el comando update.

Configurar extensiones de directiva mediante la CLI

1. Importe el archivo de extensión de directiva a Citrix ADC Appliance, ya sea desde un servidor web (mediante HTTP) o desde su estación de trabajo local.

   a) Importación HTTP

   Si tiene un servidor web disponible, puede almacenar el archivo de extensión en el directorio del servidor web e importarlo al dispositivo Citrix ADC.

```
import ns extension <src> <name> [-comment<string>] [-
   overwrite]
<!--NeedCopy-->
```

   Ejemplo:

```
import ns extension http://myhost/path/to/extension
   myextension -comment  “Custom crc calculation
<!--NeedCopy-->
```

   b) Importación local

   Puede utilizar el cliente SSH para copiar el archivo de extensión de la estación de trabajo al directorio /var/tmp del dispositivo Citrix ADC.

```
scp extension-file-name <ns-userid@ns-ip-addr>:/var/tmp
<!--NeedCopy-->
```

   donde:

   - `extension-file-name` es el nombre del archivo de extensión de su equipo cliente.
   - `ns-userid` es el usuario del dispositivo Citrix ADC con permiso para escribir en /var/tmp.
   - `ns-ip-addr` es la dirección IP de Citrix ADC.

Después de copiar el archivo en el dispositivo Citrix ADC, ejecute el comando de importación en el dispositivo Citrix ADC.

```
import ns extension local:<extension-file-name extension-name>
<!--NeedCopy-->
```

Nota: La CLI debe utilizarse para importar un archivo de extensión local ejecutando el comando
import .

2. Agregue la extensión de directiva al motor de paquetes para su evaluación.

```
add ns extension <name> [-comment <string>]
<!--NeedCopy-->
```

Ejemplo:

```
add ns extension myextension
<!--NeedCopy-->
```

Después de importar un archivo de extensión, puede actualizarlo, si ha incluido el parámetro -overwrite en el comando import, o quitarlo. También puede mostrar los detalles de un archivo de extensión importado.

Actualizar un archivo de extensión en el dispositivo Citrix ADC desde el origen

En el símbolo del sistema, escriba:

```
update ns extension <name>
<!--NeedCopy-->
```

Nota: Solo puede actualizar el archivo de extensión después de importar el archivo de extensión especificado al dispositivo Citrix ADC con el parámetro -overwrite.

Ejemplo:

```
update ns extension myextension
<!--NeedCopy-->
```


Quitar un archivo de extensión del dispositivo Citrix ADC

En el símbolo del sistema, escriba:

```
rm ns extension <name>
<!--NeedCopy-->
```

Ejemplo:

```
rm ns extension myextension
<!--NeedCopy-->
```

Mostrar los detalles de la función de extensión especificada en el dispositivo Citrix ADC

En el símbolo del sistema, escriba:

```
show ns extension <name>
<!--NeedCopy-->
```

Ejemplo:

```
show ns extension myextension
<!--NeedCopy-->
```

Configurar extensiones de directivas mediante la interfaz gráfica de usuario

1. Importe el archivo de extensión de directiva a Citrix ADC Appliance, ya sea desde un servidor web (mediante HTTP) o desde su estación de trabajo local.
   a) Vaya a **AppExpert** > **Extensiones** de **directiva, haga clic en Extensión** de directiva, en la lista desplegable **Importar desde**, seleccione la dirección URL de la ubicación del archivo de extensión que quiere importar.
   b) Vaya a **AppExpert** > **Extensiones**de **directivas, Extensión** de directiva e importe el archivo de extensión seleccionando Archivo en la lista desplegable **Importar** desde.
2. Agregue la extensión de directiva al motor de paquetes para su evaluación.

   Vaya a **AppExpert** > **Extensiones de directiva** y, en la ficha**Extensiones de directiva**, agregue el archivo de extensión.

Actualizar un archivo de extensión en el dispositivo Citrix ADC desde el origen

Vaya a **AppExpert** > **Extensiones de directiva** y, en la ficha **Extensiones de directiva**, actualice el archivo de extensión.

Quitar un archivo de extensión del dispositivo Citrix ADC

Vaya a **AppExpert** > **Extensiones de directivas** y, a la ficha **Extensiones de directiva**, elimine el archivo de extensión.

Mostrar los detalles de la función de extensión especificada en el dispositivo Citrix ADC

Vaya a **AppExpert** > **Extensiones de directiva** y, en la ficha **Funciones de extensiones de directiva**, haga clic en la flecha de la lista desplegable de clic de la función de extensión en la que desea ver los detalles.

Extensiones de directivas: Casos de uso

August 20, 2021

Algunas aplicaciones de cliente tienen requisitos que no se pueden abordar con directivas y expresiones existentes. La función de extensión de directivas permite a los clientes agregar funciones personalizadas a sus aplicaciones para satisfacer sus requisitos.

Los siguientes casos de uso ilustran la adición de nuevas funciones mediante la función de extensión de directivas en el dispositivo Citrix ADC.

- Caso 1: Hash personalizado
- Caso 2: Contraer barras diagonales dobles en las URL
- Caso 3: Combinar encabezados

Caso 1: Hash personalizado

La función CUSTOM_HASH proporciona un mecanismo para insertar cualquier tipo de valor hash en las respuestas enviadas al cliente. En este caso de uso, la función hash se utiliza para calcular el hash de la cadena de consulta para una solicitud HTTP de reescritura e insertar un encabezado HTTP llamado CUSTOM_HASH con el valor calculado. La función CUSTOM_HASH implementa el algoritmo hash DJB2.

Ejemplo de uso de CUSTOM_HASH:


```
> add rewrite action test_custom_hash insert_http_header "CUSTOM_HASH"
   "HTTP.REQ.URL.QUERY.CUSTOM_HASH"
<!--NeedCopy-->
```

Ejemplo de definición de CUSTOM_HASH ():

```
    -- Extension function to compute custom hash on the text

    -- Uses the djb2 string hash algorithm
    function NSTEXT:CUSTOM_HASH() : NSTEXT

        local hash = 5381

        local len = string.len(self)

        for i = 1, len do

            hash = bit32.bxor((hash * 33), string.byte(self, i))

        end

        return tostring(hash)

    end
<!--NeedCopy-->
```

Descripción línea por línea de la muestra anterior:

```
function NSTEXT:CUSTOM_HASH() : NSTEXT

Defines the CUSTOM_HASH() function, with text input and a text return
   value.

local hash = 5381
local len = string.len(self)

Declares two local variables:

 - hash. Accumulates the compute hash value and is seeded with the
    number 5381

```



```
 - len. Sets to the length of the self input text string, using the
    built-in string.len() function.

for i = 1, len do
     hash = bit32.bxor((hash * 33), string.byte(self, i))
end

Iterates through each byte of the input string and adds the byte to the
    hash. It uses the built-in string.byte() function to get the byte
   and the built-in bit32.bxor() function to compute the XOR of the
   existing hash value (multiplied by 33) and the byte.

return tostring(hash)

Calls the built-in tostring() function to convert the numeric hash
   value to a string and returns the string as the value of the
   function.
<!--NeedCopy-->
```

Caso 2: Contraer barras diagonales dobles en las URL

La contracción de barras dobles en las URL mejora el tiempo de representación del sitio web, ya que los exploradores analizan las URL de barra única de forma más eficiente. Las direcciones URL de barra única también para mantener la compatibilidad con aplicaciones que no aceptan barras dobles. La función de extensión de directivas permite a los clientes agregar una función que reemplaza las barras diagonales dobles por barras diagonales simples en las direcciones URL. El ejemplo siguiente ilustra la adición de una función de extensión de directiva que contrae barras dobles en las direcciones URL.

Ejemplo de definición de PULSE_DOUBLE_SLASES ():

```
    -- Collapse double slashes in URL to a single slash and return the
       result
    function NSTEXT:COLLAPSE_DOUBLE_SLASHES() : NSTEXT

        local result = string.gsub(self, "//", "/")

        return result

    end
<!--NeedCopy-->
```

Descripción línea por línea de la muestra anterior:


```
function NSTEXT:COLLAPSE_DOUBLE_SLASHES() : NSTEXT

Declares the COLLAPSE_DOUBLE_SLASHES() function with text input and
    return.

local result = string.gsub(self, "//", "/")

Declares a local variable named result and uses the built-in string.
    gsub() function to replace all double slashes with single slashes in
     the self input text.

The second parameter of string.gsub() is actually a regular expression
    pattern, although here a simple string is used for the pattern.

return result

Returns the resulting string.
<!--NeedCopy-->
```

Caso 3: Combinar encabezados

Ciertas aplicaciones de cliente no pueden manejar múltiples encabezados en una solicitud. Además, el análisis de encabezados duplicados con los mismos valores de encabezado, o múltiples encabezados con el mismo nombre pero valores diferentes en una solicitud, consume tiempo y recursos de red. La función de extensión de directiva permite a los clientes agregar una función para combinar estos encabezados en encabezados individuales con un valor que combina los valores originales. Por ejemplo, combinando los valores de los encabezados H1 y H2.

Solicitud original:

```
GET /combine_headers HTTP/1.1
User-Agent: amigo unit test
Host: myhost
H2: h2val1
H1: abcd
Accept: \*/\*
H2: h2val2
Content-Length: 0
H2: h2val3
H1: 1234
<!--NeedCopy-->
```


Solicitud modificada:

```
GET /combine_headers HTTP/1.1
User-Agent: amigo unit test
Host: myhost
H2: h2val1, h2val2, h2val3
H1: abcd, 1234
Accept: \*/\*
Content-Length: 0
<!--NeedCopy-->
```

En general, este tipo de modificación de solicitud se realiza mediante la función Rewrite, mediante expresiones de directiva para delinear la parte de la solicitud que se va a modificar (el destino) y la modificación que se va a realizar (la expresión del generador de cadenas). Sin embargo, las expresiones de directiva no tienen la capacidad de iterar sobre un número arbitrario de encabezados.

La solución a este problema requiere una extensión al servicio de directivas. Para ello, vamos a definir una función de extensión, llamada COMBINE_HEADERS. Con esta función, podemos configurar la siguiente acción de reescritura:

```
> add rewrite action combine_headers_act replace 'HTTP.REQ.FULL_HEADER
.AFTER_STR(”HTTP/1.1rn”)''HTTP.REQ.FULL_HEADER.AFTER_STR(”HTTP/1.1rn”).
COMBINE_HEADERS'
```

Aquí, el destino de reescritura es HTTP.REQ.FULL_HEADER.AFTER_STR (“HTTP/1.1RN”). El AFTER_STR (“HTTP/1.1RN”) es necesario porque FULL_HEADER incluye la primera línea de la solicitud HTTP (por ejemplo, GET /combine_headers HTTP/1.1).

La expresión del generador de cadenas es HTTP.REQ.FULL_HEADER.AFTER_STR (“HTTP/1.1RN”) .COMBINE_HEADERS, donde los encabezados (menos la primera línea) se introducen en la función de extensión COMBINE_HEADERS, que combina y devuelve los valores de los encabezados.

Ejemplo de definición de COMBINE_HEADERS ():

```
    -- Extension function to combine multiple headers of the same name
       into one header.


    function NSTEXT:COMBINE_HEADERS(): NSTEXT

```



```
7         local headers = {
8   }
9   -- headers
10
11        local combined_headers = {
12  }
13  -- headers with final combined values
14        -- Iterate over each header (format "name:valuer\r\n")
15
16        -- and build a list of values for each unique header name.
17
18        for name, value in string.gmatch(self, "([^:]+):([^\r\n]*)\r\n"
              ) do
19
20            if headers[name] then
21
22                local next_value_index = #(headers[name]) + 1
23
24                headers[name][next_value_index] = value
25
26            else
27
28                headers[name] = {
29  name .. ":" .. value }
30
31
32            end
33
34        end
35
36
37
38        -- iterate over the headers and concat the values with
              separator ","
39
40        for name, values in pairs(headers) do
41
42            local next_header_index = #combined_headers + 1
43
44            combined_headers[next_header_index] = table.concat(values,
                  ",")
45
46        end
47
48
```



```
49
50          -- Construct the result headers using table.concat()
51
52          local result_str = table.concat(combined_headers, "\r\n") .. "\
                r\n\r\n"
53
54          return result_str
55
56      end
57  <!--NeedCopy-->
```

Descripción línea por línea de la muestra anterior:

```
1   function NSTEXT:COMBINE_HEADERS(): NSTEXT
2
3   Defines the COMBINE_HEADERS extension function, with the text input
        into the function from the policy expression and a text return type
        to the policy expression.
4
5   local headers = {
6     }
7     -- headers
8   local combined_headers = {
9     }
10    -- headers with final combined values
11
12  Declares local variables headers and combined_headers and initialize
        these variables to empty tables. headers will be a table of arrays
        of strings, where each array holds one or more values for a header.
        combined_headers will be an array of strings, where each array
        element is a header with its combined values.
13
14  for name, value in string.gmatch(self, "([^:]+):([^\r\n]*)\r\n") do
15  . . .
16  end
17  <!--NeedCopy-->
```

Este genérico para bucle analiza cada encabezado en la entrada. El iterador es la función incorporada string.gmatch (). Esta función toma dos parámetros: Una cadena para buscar, y un patrón para usar para hacer coincidir las piezas de la cadena. La cadena a buscar es suministrada por el parámetro self implícito, que es el texto de los encabezados introducidos en la función.

El patrón se expresa mediante una expresión regular (expresión regular para abreviar). Esta expresión

regular coincide con el nombre de encabezado y el valor de cada encabezado, que el estándar HTTP define como *name*:*value*rn. Los paréntesis de la expresión regular especifican las partes coincidentes que se van a extraer, por lo que el esquema de expresiones regulares es (*nombre de coincidencia*): (*valor de coincidencia*) rn. El patrón de *nombre de coincidencia* debe coincidir con todos los caracteres excepto los dos puntos. Está escrito [^:]+ ([^:] es cualquier carácter excepto: y + es una o más repeticiones). Del mismo modo, el patrón de *valor* de coincidencia tiene que coincidir con cualquier carácter excepto el\ r\ n, por lo que está escrito [^\ r\ n]*([^\ r\ n] coincide con cualquier carácter excepto\ r y\ n y* es cero o más repeticiones). Esto hace que la expresión regular completa ([^:]+): ([^\ r\ n]*) \r\n.

La sentencia for utiliza una asignación múltiple para establecer el nombre y el valor de las dos coincidencias devueltas por el iterador string.gmatch (). Estas se declaran implícitamente como variables locales dentro del cuerpo del bucle for.

```
if headers[name] then
     local next_value_index = #(headers[name]) + 1
     headers[name][next_value_index] = value
else
     headers[name] = {
 name .. ":" .. value }

end
<!--NeedCopy-->
```

Estas instrucciones dentro del bucle for ponen los nombres y valores de encabezado en la tabla de encabezados. La primera vez que se analizada un nombre de encabezado (por ejemplo, H2: h2val1 en la entrada de ejemplo), no hay entrada de encabezado para el nombre y el[nombre] de los encabezados es nulo.

Dado que nil se trata como falso, se ejecuta la cláusula else. Esto establece la entrada de encabezados para el nombre en una matriz con un valor de cadena *name*:*value*.

Nota: El constructor de matriz en el bucle else equivale a {[1] = name.. ":".. value}, que establece el primer elemento de la matriz.) Para el primer encabezado H2, establece los encabezados["H2"] = {" H2:H2Val1"}.

En instancias posteriores de un encabezado, (por ejemplo, H2: H2val2 en la entrada de ejemplo). headers[nombre] no es nulo, por lo que se ejecuta la cláusula then. Esto determina el siguiente índice disponible en el valor de matriz para headers[nombre] y coloca el valor de encabezado en ese índice. Para el segundo encabezado H2, establece headers["H2"] = {"h2:h2val1", "h2val2"}.


```
for name, values in pairs(headers) do
    local next_header_index = #combined_headers + 1
    combined_headers[next_header_index] = table.concat(values, ",")
end
<!--NeedCopy-->
```

Después de analizar los encabezados originales y rellenar la tabla de encabezados, este bucle crea la matriz combined_headers. Utiliza la función pares () como iterador de bucle for.

Cada llamada a pares () devuelve el nombre y el valor de la siguiente entrada en la tabla de encabezados.

La siguiente línea determina el siguiente índice disponible en la matriz combined_headers, y la siguiente línea establece ese elemento de matriz en el encabezado combinado. Utiliza la función table.concat () incorporada, que toma como argumentos una matriz de cadenas y una cadena para usar como separador, y devuelve una cadena que es la concatenación de las cadenas de matriz, separadas por el separador.

Por ejemplo, para los valores = {"h2:h2val1", "h2val2"}, esto produce "h2:h2val1, h2val2"

```
local result_str = table.concat(combined_headers, "\r\n") .. "\r\n\r\n"
<!--NeedCopy-->
```

Después de construir la matriz combined_headers, concatena los elementos en una cadena, y agrega un rn doble que termina los encabezados HTTP.

```
return result_str
<!--NeedCopy-->
```

Devuelve una cadena como resultado de la función de extensión COMBINE_HEADERS.

Solución de problemas de extensiones de directivas

August 20, 2021

Si la función de extensión no se comporta como se esperaba, puede utilizar la funcionalidad de seguimiento de extensión para verificar el comportamiento de la función de extensión. También puede agregar el registro a la función de extensión mediante la funcionalidad de registro personalizado, donde puede definir el nivel de registro que se va a capturar en el dispositivo Citrix ADC.

En este tema se proporciona información sobre:

- Seguimiento de extensiones
- Registro personalizado

Seguimiento de extensiones

Para mostrar lo que está haciendo la función de extensión, la funcionalidad de seguimiento de extensiones registra la ejecución de la función en el registro del sistema Citrix ADC (/var/log/ns.log). El registro de seguimiento utiliza el nivel de registro DEBUG, que normalmente no está habilitado. Por lo tanto, debe habilitar TODOS los niveles de registro. A continuación, puede habilitar el rastreo estableciendo la opción -trace del comando set ns extension. Los ajustes disponibles son:

- desactivar la desactivación de rastreo (equivalente a la extensión ns no establecida -trace).
- llama a las llamadas de función de seguimiento con argumentos y devuelve la función con el primer valor de retorno.
- trazan los números de línea anteriores más para las líneas ejecutadas.
- todos rastrean lo anterior más las variables locales cambiadas por líneas ejecutadas.

Ejemplo:

```
set audit syslogParams -loglevel ALL

set ns extension combine_headers -trace all
<!--NeedCopy-->
```

Cada mensaje de seguimiento tiene el formato

```
log-header : default NSEXTENSION Message message-number 0 : "TRACE function
-name CALL call-number: event"
```

Donde:

- El encabezado de registro proporciona marcas de tiempo, la dirección IP de Citrix ADC y el ID del motor de paquetes.
- número de mensaje es un número secuencial que identifica el mensaje de registro.
- function-name es el nombre de la función de extensión.
- call-number es un número secuencial para cada llamada a la función de extensión. Se puede utilizar para agrupar todos los mensajes de seguimiento para una llamada a función de extensión.
- es uno de los siguientes:
  - CALLA function-name; parameter-values indica que se ha llamado a la función con los parámetros especificados.

- RETURN FDE function-name; return = value indica que una función ha devuelto el valor especificado (primero). (No se notifican valores de retorno adicionales).
- Línea número-línea; valores variables indica que se ha ejecutado una línea y enumera cualquier variable con valores modificados.

Donde:

- valor o valores es
  - un número, con o sin un punto decimal,
  - una cadena, entre comillas dobles y con caracteres escapados como se describió anteriormente,
  - un booleano verdadero o falso,
  - ninguna,
  - un constructor de tablas, del formato {[key1]=value1,[clave2]=valor2,…}.
- parámetro-valores es parámetro1 = valor1; parámetro2 = valor2,…
- variable-values es variable1 = valor1; variable2 = valor2,…

Un ejemplo de mensajes de registro abreviados:

```
>shell tail -f /var/log/ns.log | grep TRACE | more

... NSEXTENSION Message 3035 0 : ”TRACE combine_headers CALL 30 : CALL
   COMBINE_HEADERS; self = ”User-Agent: curl/7.24.0 (amd64-portbld-
   freebsd8.4) libcurl/7.24.0 OpenSSL/0.9.8y zlib/1.2.3\r\nHost:
   10.217.24.7\r\nAccept: \*/\*\r\nH2: h2val1\r\nH1: abcd\r\nH2: h2val2
   \r\nH2: h2val3\r\n\r\n””

... NSEXTENSION Message 3036 0 : ”TRACE combine_headers CALL 30 : LINE
   4; headers = {
  }
 ”

... NSEXTENSION Message 3037 0 : ”TRACE combine_headers CALL 30 : LINE
   5; combined_headers = {
  }
 ”

... NSEXTENSION Message 3038 0 : ”TRACE combine_headers CALL 30 : CALL
   gmatch”

... NSEXTENSION Message 3039 0 : ”TRACE combine_headers CALL 30 :
   RETURN FROM gmatch; return = function 0x2bee5a80”

```



```
... NSEXTENSION Message 3040 0 : "TRACE combine_headers CALL 30 : CALL for iterator"

... NSEXTENSION Message 3041 0 : "TRACE combine_headers CALL 30 : RETURN FROM for iterator; return = " curl/7.24.0 (amd64-portbld-freebsd8.4) libcurl/7.24.0 OpenSSL/0.9.8y zlib/1.2.3""

... NSEXTENSION Message 3042 0 : "TRACE combine_headers CALL 30 : LINE 9; name = "User-Agent"; value = " curl/7.24.0 (amd64-portbld-freebsd8.4) libcurl/7.24.0 OpenSSL/0.9.8y zlib/1.2.3""

... NSEXTENSION Message 3043 0 : "TRACE combine_headers CALL 30 : LINE 10"

... NSEXTENSION Message 3044 0 : "TRACE combine_headers CALL 30 : LINE 14; headers = {
 ["User-Agent"]={
 [1]="User-Agent: curl/7.24.0 (amd64-portbld-freebsd8.4) libcurl/7.24.0 OpenSSL/0.9.8y zlib/1.2.3" }
  }
 "


. . .

... NSEXTENSION Message 3117 0 : "TRACE combine_headers CALL 30 : CALL for iterator"

... NSEXTENSION Message 3118 0 : "TRACE combine_headers CALL 30 : RETURN FROM for iterator; return = nil"

... NSEXTENSION Message 3119 0 : "TRACE combine_headers CALL 30 : LINE 19"

... NSEXTENSION Message 3120 0 : "TRACE combine_headers CALL 30 : CALL concat"

... NSEXTENSION Message 3121 0 : "TRACE combine_headers CALL 30 : RETURN FROM concat; return = "User-Agent: curl/7.24.0 (amd64-portbld-freebsd8.4) libcurl/7.24.0 OpenSSL/0.9.8y zlib/1.2.3\r\nH1: abcd\r\nAccept: \*/\*\r\nHost: 10.217.24.7\r\nH2: h2val1, h2val2, h2val3""
... NSEXTENSION Message 3122 0 : "TRACE combine_headers CALL 30 : LINE 25; result_str = "User-Agent: curl/7.24.0 (amd64-portbld-freebsd8.4) libcurl/7.24.0 OpenSSL/0.9.8y zlib/1.2.3\r\nH1: abcd\r\nAccept: \*/\*\r\nHost: 10.217.24.7\r\nH2: h2val1, h2val2, h2val3\r\n\r\n""
```

```
42
43 ... NSEXTENSION Message 3123 0 : "TRACE combine_headers CALL 30 :
       RETURN FROM COMBINE_HEADERS; return = "User-Agent: curl/7.24.0 (
       amd64-portbld-freebsd8.4) libcurl/7.24.0 OpenSSL/0.9.8y zlib/1.2.3\r
       \nH1: abcd\r\nAccept: \*/\*\r\nHost: 10.217.24.7\r\nH2: h2val1,
       h2val2, h2val3\r\n\r\n""
44 <!--NeedCopy-->
```

Registro personalizado

También puede agregar su propio registro a su función de extensión. Para ello, utilice la función ns.logger:*level*() incorporada, donde el *nivel*es de emergencia, alerta, crítica, error, advertencia, aviso, información o depuración. Los parámetros son los mismos que la función C printf (): Una cadena de formato y un número variable de argumentos para proporcionar valores para el% especificado en la cadena de formato. Por ejemplo, puede agregar lo siguiente a la función COMBINE_HEADERS para registrar el resultado de una llamada:

```
1 local result_str = table.concat(combined_headers, "\r\n") .. "\r\n\r\n"
2
3 ns.logger:info("Result: %s", result_str)
4
5 return result_str
6 <!--NeedCopy-->
```

La función anterior registraría el siguiente mensaje a/var/log/ns.log para la entrada de ejemplo que se muestra en los ejemplos de mensajes de registro abreviados en la sección Seguimiento de extensión anterior.

```
... : default NSEXTENSION Message 143 0 : "Result: Host: 10.217.24.7:2000^M
 H1: abcd, 1234^M User-Agent: curl/7.24.0 (amd64-portbld-freebsd8.4)libcurl
/7.24.0 OpenSSL/0.9.8y zlib/1.2.3^M Accept: */*^M H2: h2val1, h2val2,
h2val3^M ^M"
```

Optimización

October 5, 2021

Las funciones de optimización de Citrix ADC reducen los tiempos de transacción entre los clientes y los servidores y reducen el consumo de ancho de banda. También mejoran el rendimiento del servidor al descargar algunas tareas y hacer que otras sean más eficientes.

Función	Descripción
Cliente Keep-Alive	Gestiona varias solicitudes en una única conexión de cliente. El cliente no tiene que negociar una nueva conexión para cada solicitud al servidor.
Compresión HTTP	Comprime las respuestas HTTP enviadas desde los servidores a los exploradores compatibles con la compresión. Las respuestas más pequeñas reducen el tiempo de descarga y ahorran ancho de banda.
Almacenamiento en caché integrado	Almacena respuestas a las solicitudes de los clientes. Las solicitudes posteriores del mismo contenido se entregan desde la memoria caché de Citrix ADC en lugar de reenviarse al servidor de origen.
Optimización de front-end	Reduce el tiempo de carga y renderizado de las páginas web simplificando y optimizando el contenido que se sirve en el explorador del cliente. **Nota**: Compatible con NetScaler 10.5 en adelante.
Acelerador de contenido	Almacena las respuestas del servidor en un dispositivo Citrix ByteMobile T2100. **Nota**: Compatible con NetScaler 10.1 en adelante.

Client keep-alive

August 20, 2021

La función de mantenimiento de cliente permite que se envíen varias solicitudes de clientes en una sola conexión. Esta función beneficia la gestión de transacciones. Cuando el modo Client Keep-Alive está habilitado en un dispositivo y la respuesta del servidor a la solicitud del cliente contiene la conexión: cierre el encabezado HTTP y realice las siguientes tareas:

- Cambia el nombre del encabezado de conexión existente mediante la mezcla de caracteres del nombre del encabezado.
- Añade un nuevo encabezado Connection: con Keep-Alive como valor del encabezado.

El modo Client Keep-Alive permite que el dispositivo Citrix ADC procese varias solicitudes y respuestas mediante la misma conexión de socket. La función mantiene abierta la conexión entre el cliente y el dispositivo (conexión del lado del cliente) incluso después de que el servidor cierra la conexión con el dispositivo. Esto permite múltiples solicitudes de clientes mediante una única conexión y guarda los viajes de ida y vuelta asociados al abrir y cerrar una conexión. El mantenimiento del cliente es más beneficioso en las sesiones SSL.

Client keepalive es útil para los siguientes casos:

- Si el servidor no es compatible con el cliente keep-alive.
- Si el servidor admite pero una aplicación en el servidor no es compatible con el cliente keep-alive.

> **Nota:**
> Keep-alive del cliente es aplicable para el tráfico HTTP y SSL. Client-Keep Alive se puede configurar globalmente para manejar todo el tráfico. Además, puede activarlo en servicios específicos.

En el entorno keep-alive del cliente, los servicios configurados interceptan el tráfico del cliente y la solicitud del cliente se dirige al servidor de origen. El servidor envía la respuesta y cierra la conexión entre el servidor y el dispositivo. Si hay un encabezado "Connection: Close" en la respuesta del servidor, el dispositivo corrompe este encabezado en la respuesta del cliente y la conexión del lado del cliente se mantiene abierta. Como resultado, el cliente no tiene que abrir una nueva conexión para la siguiente solicitud. En su lugar, se vuelve a abrir la conexión con el servidor.

> **Nota:**
> Si un servidor devuelve dos encabezados "Conexión: Cerrar", solo se modificará uno. Esto da lugar a retrasos significativos en la representación cliente del objeto porque un cliente no asume que el objeto se ha entregado completamente hasta que se cierra la conexión.

Configurar el mantenimiento del cliente

El mantenimiento del cliente, de forma predeterminada, está inhabilitado en Citrix ADC, tanto globalmente como a nivel de servicio. Por lo tanto, debe habilitar la función en el ámbito requerido.

> **Nota:**
> Si habilita el cliente keep-alive globalmente, se habilita para todos los servicios, independientemente de si lo habilita en el nivel de servicio. Además, debe configurar algunos parámetros HTTP para especificar lo siguiente:
>
> - el número máximo de conexiones HTTP retenidas en el grupo de reutilización de conexiones.
> - habilitar la multiplexación de conexiones y habilitar la persistencia `Etag`.
>
> **Nota:**

> Cuando Persistente ETag está habilitado, el ETag encabezado incluye información sobre el servidor que sirvió el contenido. Esto garantiza que las solicitudes condicionales de validación de caché o las solicitudes de explorador, para ese contenido, siempre lleguen al mismo servidor.

Configurar keep-alive de cliente mediante la interfaz de comandos de Citrix ADC

En el símbolo del sistema, haga lo siguiente:

1. Habilite el mantenimiento del cliente en Citrix ADC.
   - En el plano mundial- `enable ns mode cka`
   - A nivel de servicio- `set service <name> -CKA YES`

   > **Nota:**
   >
   > El mantenimiento del cliente solo se puede habilitar para los servicios HTTP y SSL.

2. Configure los parámetros HTTP en el perfil HTTP enlazado a uno o más servicios.

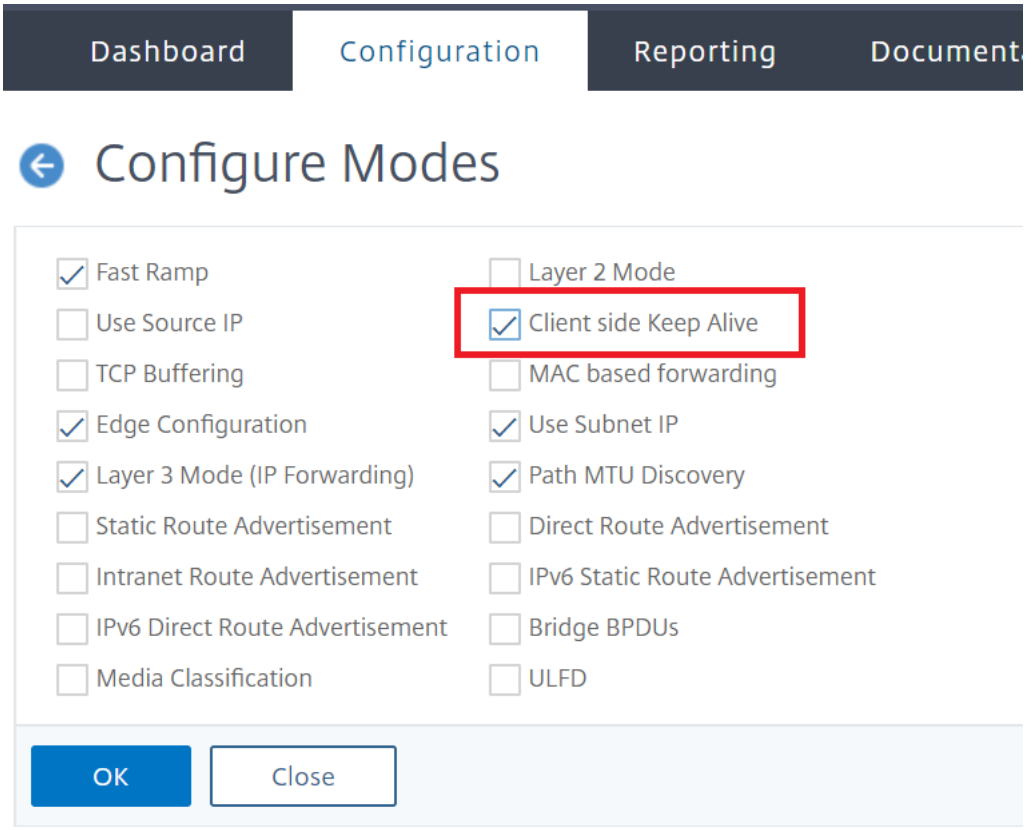
```
set ns httpProfile <name> -maxReusePool <value> -conMultiplex
    ENABLED -persistentETag ENABLED
<!--NeedCopy-->
```

> **Nota:**
>
> Configure estos parámetros en el perfil `nshttp_default _profile HTTP` para que estén disponibles globalmente.

Configurar mantenimiento de cliente mediante la GUI de Citrix ADC

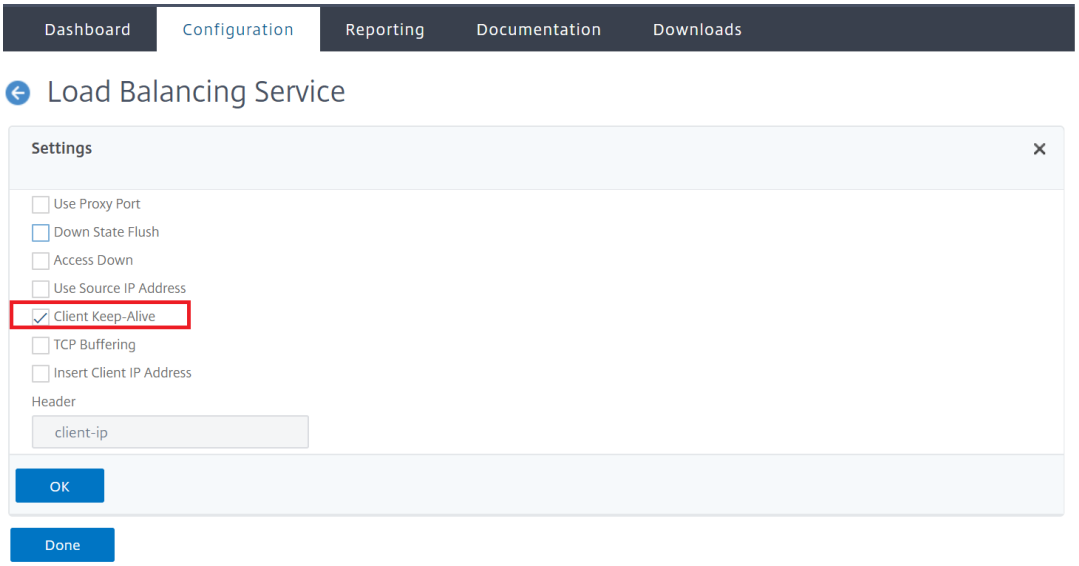
1. Habilite el mantenimiento del cliente en Citrix ADC.
   - A nivel mundial

     Vaya a **Sistema** > **Configuración**, haga clic en **Configurar modos** y seleccione **Mantener vivo en el lado del cliente**.



- A nivel de servicio

  Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servicios** y seleccione el servicio requerido. En la sección **Configuración**, active la casilla de verificación **Client Keep-Alive**.



2. Configure los parámetros HTTP requeridos en el perfil HTTP enlazado a uno o varios servicios.
3. Vaya a **Sistema** > **Perfiles** y, en la ficha **Perfiles HTTP**, seleccione el perfil requerido y actualice los parámetros HTTP requeridos.

Compresión HTTP

October 5, 2021

Para los sitios web con contenido comprimible, la función de compresión HTTP implementa compresión sin pérdidas para aliviar la latencia, los largos tiempos de descarga y otros problemas de rendimiento de la red mediante la compresión de las respuestas HTTP enviadas desde los servidores a exploradores compatibles con la compresión. Puede mejorar el rendimiento del servidor descargando la tarea de compresión con un uso intensivo de cómputo de los servidores al dispositivo Citrix ADC.

En la tabla siguiente se describen las capacidades de la función de compresión HTTP:

Funcionalidad	Descripción
Índice de compresión	La relación de compresión depende de los tipos de archivos de las respuestas, pero siempre es significativa, lo que reduce notablemente la cantidad de datos transmitidos a través de la red.
Conocimiento del explorador	Citrix ADC entrega datos comprimidos únicamente a exploradores que admiten compresión, lo que reduce el tiempo de transacción entre el cliente y el servidor. La mayoría de los exploradores web modernos admiten compresión HTTP.
Bloqueo de compresión	Puede definir filtros de contenido para bloquear selectivamente la compresión aplicando acciones integradas.
CachÉ de compresión	Con la función de almacenamiento en caché integrada habilitada, las solicitudes posteriores del mismo contenido se atienden desde la caché local, lo que reduce el número de viajes de ida y vuelta al servidor y mejora los tiempos de transacción.

Funcionalidad	Descripción
Soporte HTTPS	La compresión resulta útil en las conexiones SSL porque reduce la cantidad de contenido que debe cifrarse, ya sea en el servidor o en el dispositivo Citrix ADC, y que el cliente debe descifrar.
Filtrado inteligente de respuestas	El motor de compresión Citrix ADC filtra de forma inteligente las respuestas del servidor en función de los parámetros de compresión definidos. Por ejemplo, el motor de compresión detecta respuestas de longitud de contenido cero y respuestas comprimidas y no las comprime. La detección de respuestas comprimidas permite a los sitios de origen utilizar la compresión basada en servidor con la función de compresión de Citrix ADC.
Cambio de compresión	El dispositivo Citrix ADC dirige de forma transparente las solicitudes de los clientes sensibles a la compresión a servidores con capacidad de compresión, de modo que las respuestas a esos clientes se compriman y las respuestas a otros clientes no se retrasan debido al procesamiento de compresión.

Cómo funciona la compresión HTTP

Un Citrix ADC puede comprimir datos tanto estáticos como generados dinámicamente. Aplica el algoritmo de compresión GZIP o DEFLATE para eliminar información extraña y repetitiva de las respuestas del servidor y representar la información original en un formato más compacto y eficiente. Estos datos comprimidos se envían al explorador del cliente y se descomprimen según lo determine el algoritmo o algoritmos admitidos por el explorador (GZIP o DEFLATE).

La compresión de Citrix ADC trata el contenido estático y dinámico de forma diferente.

- Los archivos estáticos se comprimen una sola vez y una copia comprimida se almacena en la memoria local. Las solicitudes de los clientes posteriores de archivos almacenados en caché se atienden desde esa memoria.
- Las páginas dinámicas se crean dinámicamente cada vez que un cliente las solicita.

Cuando un cliente envía una solicitud al servidor:

1. La solicitud del cliente llega a Citrix ADC. El ADC examina los encabezados y almacena información sobre qué tipo de compresión, si la hay, admite el explorador.
2. El ADC reenvía la solicitud al servidor y recibe la respuesta.
3. El motor de compresión Citrix ADC examina la compresibilidad de la respuesta del servidor comparándola con las directivas.
4. Si la respuesta coincide con una directiva asociada a una acción de compresión y el explorador del cliente admite un algoritmo de compresión especificado por la acción, Citrix ADC aplica el algoritmo y envía la respuesta comprimida al explorador del cliente.
5. El cliente aplica el algoritmo de compresión compatible para descomprimir la respuesta.

Configurar compresión HTTP

De forma predeterminada, la compresión está inhabilitada en Citrix ADC. Debe habilitar la función antes de configurarla. Si la función está habilitada, el ADC comprime las solicitudes del servidor especificadas por las directivas de compresión.

Para habilitar la compresión HTTP mediante la CLI

La compresión solo se puede habilitar para los servicios HTTP y SSL. Puede habilitarla globalmente para que se aplique a todos los servicios HTTP y SSL, o puede habilitarla solo para servicios específicos.

En el símbolo del sistema, introduzca uno de los siguientes comandos para habilitar la compresión de forma global o para un servicio específico:

- `enable ns feature cmp`
  OR
- `set service \<name\> -CMP YES`

Para configurar la compresión mediante la interfaz gráfica de usuario

Lleve a cabo una de las siguientes acciones:

Para habilitar la compresión de forma global, vaya a Sistema > Configuración, haga clic en **Configurar funciones básicas**y seleccione Compresión HTTP.

Para habilitar la compresión de un servicio específico, vaya a **Administración del tráfico > Equilibrio de carga > Servicios**, seleccione el servicio y haga clic en Modificar. En el grupo Configuración, haga clic en el icono del lápiz y activa Compresión.

Configuración de una acción de compresión

Una acción de compresión especifica la acción que se debe llevar a cabo cuando una solicitud o respuesta coincide con la regla (expresión) de la directiva a la que está asociada la acción. Por ejemplo,

puede configurar una directiva de compresión que identifique las solicitudes que se enviarán a un servidor concreto y asociar la directiva a una acción que comprima la respuesta del servidor.

Hay cuatro acciones de compresión integradas:

- COMPRESS: Utiliza el algoritmo GZIP para comprimir datos de exploradores compatibles con GZIP o con GZIP y DEFLATE. Utiliza el algoritmo DEFLATE para comprimir datos de exploradores que solo admiten el algoritmo DEFLATE. Si el explorador no admite ninguno de los algoritmos, la respuesta del explorador no se comprime.
- NOCOMPRESS: No comprime datos.
- GZIP: utiliza el algoritmo GZIP para comprimir los datos de los exploradores compatibles con la compresión GZIP. Si el explorador no admite el algoritmo GZIP, la respuesta del explorador no se comprime.
- DEFLATE: Utiliza el algoritmo DEFLATE para comprimir datos de exploradores compatibles con el algoritmo DEFLATE. Si el explorador no admite el algoritmo DEFLATE, la respuesta del explorador no se comprime.Tras crear una acción, asociará la acción a una o varias directivas de compresión.

En el símbolo del sistema, escriba el siguiente comando para crear una acción de compresión:

```
add cmp action <name> <cmpType> [-addVaryHeader <addVaryHeader> -varyHeaderValue
<string>]
```

Para configurar una directiva de compresión mediante la CLI

Una directiva de compresión contiene una regla, que es una expresión lógica que permite al dispositivo Citrix ADC identificar el tráfico que se debe comprimir.

Cuando Citrix ADC recibe una respuesta HTTP de un servidor, evalúa las directivas de compresión integradas y las directivas de compresión personalizadas para determinar si se comprime la respuesta y, en caso afirmativo, el tipo de compresión que se va a aplicar. Las prioridades asignadas a las directivas determinan el orden en que se comparan las directivas con las solicitudes.

En el símbolo del sistema, introduzca el siguiente comando para crear una directiva de compresión:

```
add cmp policy <name> -rule <expression> -resAction <string>
```

Para crear una acción de compresión mediante la interfaz gráfica de usuario

Vaya a **Optimización** > **Compresión HTTP** > **Acciones**, haga clic en **Agregar** y cree una acción de compresión para especificar el tipo de compresión que se va a realizar en la respuesta HTTP.

Configuración de una directiva de compresión

Una directiva de compresión contiene una regla, que es una expresión lógica que permite al dispositivo Citrix ADC identificar el tráfico que se debe comprimir.

Cuando Citrix ADC recibe una respuesta HTTP de un servidor, evalúa las directivas de compresión integradas y las directivas de compresión personalizadas para determinar si se comprime la respuesta y, en caso afirmativo, el tipo de compresión que se va a aplicar. Las prioridades asignadas a las directivas determinan el orden en que se comparan las directivas con las solicitudes.

En la tabla siguiente se enumeran las directivas de compresión HTTP integradas. Estas directivas se activan globalmente al habilitar la compresión.

Directiva clásica o avanzada incorporada	Descripción
ns_nocmp_mozilla_47, ns_adv_nocmp_mozilla_	Impide la compresión de archivos CSS cuando se envía una solicitud desde un explorador Mozilla 4.7.
ns_cmp_mscss, ns_adv_cmp_mscss	Comprime los archivos CSS cuando la solicitud se envía desde un explorador Microsoft Internet Explorer.
ns_cmp_msapp, ns_adv_cmp_msapp	Comprime los archivos generados por las siguientes aplicaciones: Microsoft Office Word, Microsoft Office Excel, Microsoft Office PowerPoint.
ns_cmp_content_type, ns_adv_cmp_content_type	Comprime datos cuando la respuesta contiene encabezado Content-type y contiene texto.
ns_nocmp_xml_es, ns_adv_nocmp_xml_es	Impide la compresión cuando se envía una solicitud desde un explorador Microsoft Internet Explorer y la respuesta contiene un encabezado Content-Type y contiene texto o xml.

Vinculación de una directiva de compresión

Para aplicar una directiva de compresión, debe vincularla de forma global, de modo que se aplique a todo el tráfico que fluye a través de Citrix ADC o a un servidor virtual específico, de modo que la directiva se aplique únicamente a las solicitudes cuyo destino sea la dirección VIP de ese servidor virtual.

Cuando vincula una directiva, le asigna una prioridad. La prioridad determina el orden en que se evalúan las directivas que defina. Puede establecer la prioridad en cualquier número entero positivo.

Para enlazar una directiva de compresión mediante la CLI

En el símbolo del sistema, introduzca uno de los siguientes comandos para enlazar una directiva de

compresión de forma global o a un servidor virtual específico:

- `bind cmp global <policyName> [-priority <positive_integer>] [-state ( ENABLED|DISABLED)]...`
- `bind lb vserver <vserverName> -policyName <policyName> -priority < positive_integer>.`

Repita este comando para cada servidor virtual al que quiera enlazar la directiva de compresión.

Para enlazar una directiva de compresión mediante la interfaz gráfica de usuario

Lleve a cabo una de las siguientes acciones:

A nivel global, vaya a **Optimización** > **Compresión HTTP** > **Directivas**, haga clic en **Administrador** de directivas y vincule las directivas necesarias especificando el punto de enlace y el tipo de conexión (solicitud/respuesta) pertinentes.

A nivel de servidor virtual

Para el servidor virtual de equilibrio de carga, vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**, seleccione el servidor virtual necesario, haga clic en **Directivas**y vincule la directiva correspondiente.

Para el servidor virtual de conmutación de contenido, vaya a **Administración del tráfico > Conmutación de contenido > Servidores virtuales**, seleccione el servidor virtual necesario, haga clic en **Directivas**y vincule la directiva correspondiente.

Establezca los parámetros de compresión global para obtener un rendimiento óptimo

Muchos usuarios aceptan los valores predeterminados de los parámetros de compresión globales, pero es posible que pueda proporcionar una compresión más eficaz si personaliza esta configuración.

> **Nota**
> Después de configurar los parámetros de compresión globales, no es necesario reiniciar el dispositivo. Se aplican inmediatamente a los nuevos flujos.

En la tabla siguiente se describen los parámetros de compresión que se pueden establecer en Citrix ADC.

parámetros de compresión	Descripción
Tamaño cuántico	Tamaño, en KB, del búfer que se mantiene para acumular respuestas del servidor. Las respuestas se comprimen cuando el tamaño del búfer supera este valor. Por ejemplo, si establece el tamaño cuántico en 50 KB, Citrix ADC comprime el contenido del búfer cuando su tamaño supera los 50 KB. Valor mínimo: 1. Valor máximo: 63488. Valor predeterminado: 57344.
Nivel de compresión	Nivel de compresión que se aplicará a las respuestas del servidor. Valores posibles: Mejor velocidad, mejor compresión, óptima.
Tamaño mínimo de respuesta HTTP	Tamaño mínimo, en bytes, de una respuesta HTTP comprimida. Las respuestas inferiores al valor especificado por este parámetro se envían sin comprimirse.
Omitir la compresión en el uso de CPU	Uso de CPU de Citrix ADC, como porcentaje, igual o superior al que no se realiza ninguna compresión. Valor predeterminado: 100.
Tipo de directiva*	Tipo de directivas utilizadas para la compresión. Valores posibles: Directiva clásica, avanzada. Predeterminado: clásico.
Permitir compresión del lado del servidor	Permitir que los servidores envíen datos comprimidos a Citrix ADC.
Comprimir paquete push	Al recibir un paquete con un indicador TCP PUSH, comprima los paquetes acumulados inmediatamente, sin esperar a que se llene el búfer cuántico.
Caché externa	Emita una directiva de respuesta privada que indique que el mensaje de respuesta está destinado a un único usuario y que no debe almacenarse en caché mediante una caché compartida o proxy.

Para configurar la compresión HTTP mediante la interfaz gráfica de usuario

Lleve a cabo una de las siguientes acciones:

- Para habilitar la compresión de forma global, vaya a**Sistema**>**Configuración**, haga clic en**Configurar funciones básicas**y seleccione**Compresión HTTP**.
- Para habilitar la compresión de un servicio específico, vaya a**Administración del tráfico**>**Equilibrio de carga**>**Servicios**, seleccione el servicio y haga clic en**Modificar**.
- En el grupo**Configuración**, haga clic en el icono del lápiz y activa**Compresión**.

Para crear una acción de compresión mediante la interfaz gráfica de usuario

Vaya a**Optimización**>**Compresión HTTP**>**Acciones**, haga clic en**Agregar**y cree una acción de compresión para especificar el tipo de compresión que se va a realizar en la respuesta HTTP

Para crear una directiva de compresión mediante la interfaz gráfica de usuario

Vaya a**Optimización**>**Compresión HTTP**>**Directivas**, haga clic en**Agregar**y cree una directiva de compresión especificando la condición y la acción correspondiente que se va a ejecutar.

Evaluar la configuración de compresión

Puede ver las estadísticas de compresión en la utilidad de tablero o en un monitor SNMP. La utilidad de tablero muestra estadísticas resumidas y detalladas en formato tabular y gráfico.

De forma opcional, también puede ver las estadísticas de una directiva de compresión, incluido el número de solicitudes que el contador de directivas incrementa durante la compresión basada en directivas.

> **Nota**
>
> - Para obtener más información acerca de las estadísticas y los gráficos, consulte la ayuda del panel del dispositivo Citrix ADC.
> - Para obtener más información sobre SNMP, consulte el temaSNMP .

Para ver las estadísticas de compresión mediante la CLI

En el símbolo del sistema, introduzca los siguientes comandos para mostrar las estadísticas de compresión:

1. Para mostrar un resumen de las estadísticas de compresión.

```
stat cmp
```

> **Nota**
> El comando stat cmp policy muestra estadísticas únicamente para las directivas de compresión avanzada de directivas.

2. Para mostrar los detalles y los resultados de las directivas de compresión

```
show cmp policy \<name\>
```


3. Para mostrar estadísticas de compresión detalladas

```
stat cmp -detail
```

Para ver las estadísticas de compresión mediante el tablero de mandos:

En la utilidad Panel de control, puede mostrar los siguientes tipos de estadísticas de compresión:

- Seleccione Compresión para mostrar un resumen de las estadísticas de compresión.
- Para mostrar estadísticas de compresión detalladas por tipo de protocolo, haga clic en Detalles
- Para mostrar la tasa de solicitudes procesadas por la función de compresión, haga clic en la ficha Vista gráfica.

Para ver estadísticas de compresión mediante SNMP

Puede ver las siguientes estadísticas de compresión mediante la aplicación de administración de red SNMP.

- Número de solicitudes de compresión (OID: 1.3.6.1.4.1.5951.4.1.1.50.1)
- Número de bytes comprimidos transmitidos (OID: 1.3.6.1.4.1.5951.4.1.1.50.2)
- Número de bytes comprimibles recibidos (OID: 1.3.6.1.4.1.5951.4.1.1.50.3)
- Número de paquetes comprimibles transmitidos (OID: 1.3.6.1.4.1.5951.4.1.1.50.4)
- Número de paquetes comprimibles recibidos (OID: 1.3.6.1.4.1.5951.4.1.1.50.5)
- Relación de datos comprimibles recibidos y datos comprimidos transmitidos (OID: 1.3.6.1.4.1.5951.4.1.1.50.6)
- Relación entre el total de datos recibidos y el total de datos transmitidos (OID: 1.3.6.1.4.1.5951.4.1.1.50.7)

Para ver más estadísticas de compresión mediante la interfaz gráfica de usuario

1. Para mostrar estadísticas de compresión HTTP:

Vaya a **Optimización** >**Compresión HTTP**y haga clic en**Estadísticas**.

1. Para mostrar las estadísticas de una directiva de compresión.

Vaya a**Optimización** >**Compresión HTTP** >**Directivas** > seleccione la directiva y haga clic en **Estadísticas**.

1. Para mostrar las estadísticas de una etiqueta de directiva de compresión
2. Vaya a**Optimización** >**Compresión HTTP** >**Directivas** > seleccione una etiqueta de directiva y haga clic en **Estadísticas**.

Descarga de compresión HTTP

La compresión en un servidor puede afectar al rendimiento del servidor. Un Citrix ADC colocado frente a sus servidores web y configurado para compresión HTTP descarga la compresión del contenido estático y dinámico, lo que ahorra recursos y ciclos de CPU del servidor.

Puede descargar la compresión de los servidores web de dos maneras:

Inhabilite la compresión en los servidores web, habilite la función Citrix ADC Compression a nivel global y configure los servicios para la compresión.

Deje habilitada la función de compresión en los servidores web y configure el dispositivo Citrix ADC para quitar el encabezado "Aceptar codificación" de todas las solicitudes de cliente HTTP. A continuación, los servidores envían respuestas sin comprimir. Citrix ADC comprime las respuestas del servidor antes de enviarlas a los clientes.

> **Nota**
> La segunda opción no funciona si los servidores comprimen automáticamente todas las respuestas. Citrix ADC no intenta comprimir una respuesta que ya está comprimida.

El parámetro Servercmp permite al dispositivo Citrix ADC gestionar la compresión HTTP de descarga. De forma predeterminada, este parámetro está activado para que el servidor envíe datos comprimidos al dispositivo Citrix ADC. Para descargar la compresión HTTP, debe establecer el parámetro servercmp en OFF. En el símbolo del sistema, introduzca los siguientes comandos:

```
set service <service name> -CMP YES
```

Repita este comando para cada servicio para el que quiera habilitar la compresión.

```
show service <service name>
```

Repita este comando para cada servicio para comprobar que la compresión está habilitada.

```
Save config
```

```
set cmp parameter -serverCmp OFF
```

> **Nota:**
>
> Cuando el parámetro `Servercmp` está activado y el dispositivo recibe una respuesta comprimida del servidor, el dispositivo no comprime más los datos. En su lugar, reenvía la respuesta comprimida al cliente.

Almacenamiento en caché integrado

August 20, 2021

La caché integrada proporciona almacenamiento en memoria en el dispositivo Citrix ADC y ofrece contenido web a los usuarios sin necesidad de un viaje de ida y vuelta a un servidor de origen. Para el contenido estático, la caché integrada requiere poca configuración inicial. Después de habilitar la función de caché integrada y realizar la configuración básica (por ejemplo, determinar la cantidad de memoria del dispositivo Citrix ADC que puede utilizar la caché), la caché integrada utiliza directivas integradas para almacenar y servir tipos específicos de contenido estático, incluidas páginas web simples y archivos de imagen. También puede configurar la caché integrada para almacenar y servir

contenido dinámico marcado como no almacenable en caché por servidores web y de aplicaciones (por ejemplo, registros de bases de datos y cotizaciones de stock).

> **Nota:**
>
> El término Caché Integrado se puede utilizar indistintamente con AppCache; tenga en cuenta que desde el punto de vista de la funcionalidad, ambos términos significan lo mismo.

Cuando una solicitud o respuesta coincide con la regla (expresión lógica) especificada en una directiva integrada o en una directiva que haya creado. El dispositivo Citrix ADC realiza la acción asociada a la directiva. De forma predeterminada, todas las directivas almacenan objetos almacenados en caché y los recuperan del grupo de contenido predeterminado. Puede crear sus propios grupos de contenido para diferentes tipos de contenido.

Para permitir que el dispositivo busque objetos almacenados en caché en un grupo de contenido, puede configurar selectores. Los selectores hacen coincidir objetos almacenados en caché con expresiones, o bien puede especificar parámetros para buscar objetos en el grupo de contenido. Si utiliza selectores según lo recomendado por Citrix, configúrelos primero para que pueda especificar selectores al configurar grupos de contenido. A continuación, configure los grupos de contenido que quiera agregar para que estén disponibles al configurar las directivas. Para completar la configuración inicial, cree bancos de directivas vinculando cada directiva a un punto de enlace global o a un servidor virtual. O bien, puede vincular una etiqueta a la que se puede llamar desde otros bancos de directivas.

El almacenamiento en caché integrado se puede mejorar mediante el método de objetos almacenados en caché antes de que estén programados para caducar. Para administrar el manejo de datos almacenados en caché, puede configurar encabezados relacionados con la caché insertados en las respuestas. La caché integrada también puede actuar como proxy de reenvío para otros servidores de caché.

> **Nota:**
>
> El almacenamiento en caché integrado requiere cierta familiaridad con las solicitudes y respuestas HTTP.
> Para obtener información acerca de la estructura de los datos HTTP, consulte *Encabezados HTTP activos* en ”<http://livehttpheaders.mozdev.org/>.”

Cómo funciona la caché de integración

La caché integrada supervisa las solicitudes HTTP y SQL que fluyen a través del dispositivo Citrix ADC y compara las solicitudes con las directivas almacenadas. Dependiendo del resultado, la función de caché integrada busca la respuesta en la caché o reenvía la solicitud al servidor de origen. Para las solicitudes HTTP, el almacenamiento en caché integrado sirve como contenido parcial de la caché en respuesta a solicitudes de rango de bytes único y de rango de bytes de varias partes.

Los datos almacenados en caché se comprimen si el cliente acepta contenido comprimido. Puede configurar los tiempos de caducidad para un grupo de contenido y puede caducar selectivamente las entradas de un grupo de contenido.

Los datos que se sirven desde la caché integrada son una solicitud, y los datos servidos desde el origen son una falta de caché, como se describe en la tabla siguiente.

Tipo de transacción	Especificación
Golpe de caché	Respuestas que el dispositivo Citrix ADC sirve desde la caché, incluyendo: Objetos estáticos, por ejemplo, archivos de imagen y páginas web estáticas, 200 páginas OK, 203 páginas de respuesta no autoritativa, 300 páginas de opciones múltiples, 301 páginas movidas permanentemente, 302 páginas encontradas, 304 páginas no modificadas, Estas respuestas se conocen como respuestas positivas. El dispositivo Citrix ADC también almacena en caché las siguientes respuestas negativas: 307 páginas de redirección temporal, 403 páginas prohibidas, 404 páginas no encontradas, 410 páginas pasadas. Para mejorar aún más el rendimiento, puede configurar el dispositivo Citrix ADC para almacenar en caché más tipos de contenido.
Fallo de caché almacenable	Para una pérdida de memoria caché almacenable, el dispositivo Citrix ADC obtiene la respuesta del servidor de origen y almacena la respuesta en la caché antes de servirla al cliente.
Fallo de caché no almacenable	Una pérdida de caché no almacenable es inapropiada para el almacenamiento en caché. De forma predeterminada, cualquier respuesta que contenga los siguientes códigos de estado es una pérdida de caché no almacenable: 201, 202, 204, 205, 206 códigos de estado, Todos los códigos 4xx, excepto 403, 404 y 410, 5xx códigos de estado

> **Nota:**
> Para integrar el almacenamiento en caché dinámico con su infraestructura de aplicaciones, utilice la API NITRO para emitir comandos de caché de forma remota. Por ejemplo, puede configurar desencadenadores que caduquen las respuestas almacenadas en caché cuando se actualiza una tabla de base de datos.

Para garantizar la sincronización de las respuestas almacenadas en caché con los datos del servidor de origen, configure los métodos de caducidad. Cuando el dispositivo Citrix ADC recibe una solicitud que coincide con una respuesta caducada, actualiza la respuesta del servidor de origen.

> **Nota:**
> Citrix recomienda sincronizar las horas en el dispositivo Citrix ADC y uno o varios servidores backend.

Cómo funciona la caché dinámica

El almacenamiento en caché dinámico evalúa las solicitudes y respuestas HTTP en función de pares de parámetros, cadenas, patrones de cadenas u otros datos. Por ejemplo, supongamos que un usuario busca el error 31231 en una aplicación de informe de errores. El explorador envía la siguiente solicitud en nombre del usuario:

```
1     GET /mybugreportingsystem/mybugreport.dll?IssuePage&RecordId=31231&
          Template=view&TableId=1000
2
3     Host: mycompany.net
4
5     User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9)
          Gecko/2008052906 Firefox/3.0
6
7     Accept: text/html,application/xhtml+xml,application/xml;q
          =0.9,\*/\*;q=0.8
8
9     Accept-Language: en-us,en;q=0.5
10 <!--NeedCopy-->
```

En este ejemplo, las solicitudes GET para esta aplicación de informe de errores siempre contienen los siguientes parámetros:

- Página de emisión
- Grabado
- Plantilla
- Id. de tabla

Las solicitudes GET no actualizan ni alteran los datos, por lo que puede configurar estos parámetros en directivas y selectores de almacenamiento en caché, de la siguiente manera:

- Configurar una directiva de almacenamiento en caché que busca la cadena mybugreportingsystem y el método GET en las solicitudes HTTP. Esta directiva dirige las solicitudes coincidentes a un grupo de contenido para detectar errores.
- En el grupo de contenido para errores, configure un `hit` selector que coincida con varios pares de parámetros y valores, incluidos IssuePage, RecordID, etc.

> **Nota**
>
> Un explorador puede enviar varias solicitudes GET basadas en una acción de usuario. La siguiente es una serie de tres solicitudes GET separadas que un explorador emite cuando un usuario busca un error basado en un ID de error.

```
1     GET /mybugreportingsystem/mybugreport.dll?IssuePage&RecordId=31231&
         Template=view&TableId=1000
2
3     GET /mybugreportingsystem/mybugreport.dll?IssuePage&Template=
         viewbtns&RecordId=31231&TableId=1000
4
5     GET /mybugreportingsystem/mybugreport.dll?IssuePage&Template=
         viewbody&RecordId=31231&tableid=1000
6 <!--NeedCopy-->
```

Para cumplir con estas solicitudes, se envían varias respuestas al explorador del usuario, y la página web que el usuario ve es un conjunto de las respuestas.

Si un usuario actualiza un informe de error, las respuestas correspondientes en la caché deben actualizarse con datos del servidor de origen. La aplicación de informes de errores emite solicitudes HTTP POST cuando un usuario actualiza un informe de error. En este ejemplo, configure lo siguiente para asegurarse de que las solicitudes POST desencadenan la invalidación en la caché:

- Una directiva de invalidación de tiempo de solicitud que busca la cadena mybugreportingsystem y el método de solicitud HTTP POST, y dirige las solicitudes coincidentes al grupo de contenido para informes de errores.
- Un selector de invalidación para el grupo de contenido para los informes de errores que caducan el contenido almacenado en caché basado en el parámetro RecordID. Este parámetro aparece en todas las respuestas, por lo que el selector de invalidación puede caducar todos los elementos relevantes de la caché.

El siguiente extracto muestra una solicitud POST que actualiza el informe de error de ejemplo.


```
1     POST /mybugreportingsystem/mybugreport.dll?TransitionForm HTTP/1.1\
          r\n
2
3     User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
          Opera 7.23 [en]\r\n
4
5     Host: mybugreportingsystem\r\n
6
7     Cookie:ttSearch.134=%23options%3Afalse%23active%23owner%3Afalse%23
          unowned%3Afalse%23submitter%3Afalse%23incsub%3Atrue;
8
9     Cookie2: $Version=1\r\n
10
11    . . .
12
13    \r\n
14
15    ProjectId=2&RecordId=31231&TableId=1000&TransitionId=1&Action=
          Update&CopyProjectId=0&ReloadForm=0&State=&RecordLockId=49873+
          issues+in+HTTP&F43. . .
16 <!--NeedCopy-->
```

Cuando el dispositivo Citrix ADC recibe esta solicitud, realiza lo siguiente:

- Coincide la solicitud con una directiva de invalidación.
- Busca el grupo de contenido que se denomina en la directiva.
- Aplica el selector de invalidación para este grupo de contenido y caduca todas las respuestas que coincidan con RecordID=31231.

Cuando un usuario emite una nueva solicitud para este informe de error, el dispositivo Citrix ADC va al servidor de origen para obtener copias actualizadas de todas las respuestas asociadas a la instancia del informe. Almacena las respuestas en el grupo de contenido y las envía al explorador del usuario, que vuelve a ensamblar el informe y lo muestra.

Configurar caché integrada

Para utilizar la caché integrada, debe instalar la licencia y habilitar la función. Después de habilitar la caché integrada, el dispositivo Citrix ADC® almacena automáticamente en caché los objetos estáticos según lo especificado en las directivas integradas y genera estadísticas sobre el comportamiento de la caché. (Las directivas integradas tienen un guión bajo en la posición inicial del nombre de la directiva.)

Incluso si las directivas integradas son adecuadas para su situación, es posible que quiera modificar los atributos globales. Por ejemplo, es posible que quiera modificar la cantidad de memoria del dispositivo Citrix ADC asignada a la caché integrada.

Si desea observar el funcionamiento de la caché antes de cambiar la configuración, consulte "Visualización de objetos almacenados en caché y estadísticas de caché. "

> **Nota:**
>
> La caché de Citrix ADC es un almacén en memoria que se purga al reiniciar el dispositivo.

Para instalar la licencia de caché integrada

- Se requiere una licencia de caché integrada.
- Obtenga un código de licencia de Citrix, vaya a la interfaz de línea de comandos e inicie sesión.

En la interfaz de línea de comandos, copie el archivo de licencia en la `/nsconfig/license` carpeta.

- Reinicie el dispositivo Citrix ADC mediante el siguiente comando:

```
reboot
```

Para habilitar el almacenamiento en caché integrado:
cuando habilita el almacenamiento en caché integrado, el dispositivo Citrix ADC comienza a almacenar en caché las respuestas del servidor. Si no ha configurado ninguna directiva o grupo de contenido, las directivas integradas almacenan objetos almacenados en caché en el grupo de contenido predeterminado.

En el símbolo del sistema, escriba uno de los siguientes comandos para habilitar o inhabilitar el almacenamiento en caché integrado:

```
enable ns feature IC
```

Configurar atributos globales para el almacenamiento en caché

Los atributos globales se aplican a todos los datos almacenados en caché. Puede especificar la cantidad de memoria de Citrix ADC asignada a la caché integrada mediante la inserción de encabezado. Criterio para verificar que se debe servir un objeto almacenado en caché. La longitud máxima de un cuerpo POST permitido en la caché, si se debe omitir la evaluación de directivas para solicitudes HTTP GET y una acción que se debe realizar cuando una directiva no se puede evaluar.

La capacidad de memoria caché solo está limitada por la memoria del dispositivo de hardware. Además, cualquier motor de paquetes (concentrador de distribución central de todas las solicitudes TCP entrantes) del dispositivo NCore Citrix ADC conoce los objetos almacenados en caché por otros motores de paquetes en el dispositivo NCore Citrix ADC.

> **Nota:**
>
> Cuando el límite de memoria global predeterminado se establece como 0 y la función Almacenamiento en caché integrado (IC) está habilitada, el dispositivo no almacena en caché ningún objeto. Para el almacenamiento en caché, debe configurar explícitamente el límite de memoria

> global. Sin embargo, si habilita la opción “establecer autenticación, autorización y parámetro de auditoría EnableStaticPageCaching”, habrá cierta memoria predeterminada configurada en el dispositivo. Esta memoria no es suficiente para almacenar en caché objetos grandes, por lo que es necesario asignar un límite de memoria más alto para IC. Puede realizar esto configurando el comando “set cache parameter —memLimit”. La nueva configuración se aplica solo después de guardar la configuración y reiniciar el dispositivo.

Puede modificar el límite de memoria global configurado para almacenar en caché objetos. Sin embargo, cuando actualiza el límite de memoria global a un valor inferior al valor existente (por ejemplo, de 10 GB a 4 GB), el dispositivo continúa mediante el límite de memoria.

Esto significa que aunque el límite de almacenamiento en caché integrado está configurado con algún valor, el límite real utilizado puede ser mayor. Sin embargo, esta memoria excesiva se libera cuando los objetos se eliminan de la caché.

El resultado del comando show cache parameter indica el valor configurado (memory Usage limit) y el valor real que se está usando (memory use limit (memory use limit) (memory use limit (active value)).

En el símbolo del sistema, escriba:

```
1     set cache parameter [-memLimit <MBytes>] [-via <string>] [-
         verifyUsing <criterion>] [-maxPostLen <positiveInteger>] [-
         prefetchMaxPending <positiveInteger>] [-enableBypass(YES|NO)] [-
         undefAction (NOCACHE|RESET)]
2 <!--NeedCopy-->
```

Habilitar el almacenamiento en caché integrado mediante la GUI de Citrix ADC

Vaya a **Sistema** > **Configuración**, haga clic en **Configurar funciones básicas** y seleccione Almacenamiento en **caché integrado**.

Configurar la configuración global para el almacenamiento en caché mediante la GUI de Citrix ADC

Vaya a **Optimización** > Almacenamiento en **caché integrado**, haga clic en **Cambiar configuración de caché** y configure la configuración global para el almacenamiento en caché.

Configurar grupo de contenido integrado, conjunto de patrones y directivas para la caché integrada

El dispositivo Citrix ADC incluye una configuración integrada de almacenamiento en caché que puede utilizar para almacenar contenido en caché. La configuración consiste en un grupo de contenido de-

nominado ctx_cg_poc, un conjunto de patrones denominado ctx_file_extensions y un conjunto de directivas de caché integradas. En el grupo de contenido ctx_cg_poc, solo se almacenan en caché los objetos de 500 KB o menos. El contenido se almacena en caché durante 86000 segundos y el límite de memoria para el grupo de contenido es de 512 MB. El conjunto de patrones es una matriz indexada de extensiones comunes para la coincidencia de tipos de archivo.

En la siguiente tabla se enumeran las directivas integradas de almacenamiento en caché. De forma predeterminada, las directivas no están enlazadas a ningún punto de enlace. Debe enlazar las directivas a un punto de enlace si quiere que el dispositivo Citrix ADC evalúe el tráfico con las directivas. Las directivas almacenan en caché objetos del grupo de contenido ctx_cg_poc.

Nombre de directiva de almacenamiento en caché integrado	Regla de directiva
_cachevpnStaticObjects	HTTP.REQ.URL.SET_TEXT_MODE (IGNORECASE) .CONTAINS_INDEX (“ctx_file_extensions”) .BETNY (101,150)
_cachetCPvpnStaticObjects	HTTP.REQ.URL.ENDSWITH(“.css”)
_cacheocvpnStaticObjects	HTTP.REQ.URL.ENDSWITH(“.pdf”)
_cachewfstaticoObjects	HTTP.REQ.URL.ENDSWITH(“.js”)
- MaynoCacheReq	HTTP.RES.HEADER (“Content-Type”) .CONTIENE (“application/x-javascript”)
- Nochacherest	TRUE

Configuración de vaciado de caché

Puede vaciar un grupo de caché, grupos de caché o localizador de objetos de caché. Los siguientes son los comandos para vaciar objetos de caché.

En el símbolo del sistema, escriba:

```
flush cache contentgroup all
```

Ejemplo

```
1          0x00000089bae000000004 DEFAULT GET  //1.1.1.1:80/html/index.
               html?name=hello
2          0x00000089bae000000005 DEFAULT GET  //1.1.1.1:80/html/index.
               html?name=hi
3
4          Flush cache contentGroup all
```



```
5         done
6
7 `flush cache contentgroup <content group name>`
8 <!--NeedCopy-->
```

Ejemplo:

```
1         0x00000089bae000000004 DEFAULT GET  //1.1.1.1:80/html/index.
             html?name=hello
2         0x00000089bae000000005 DEFAULT GET  //1.1.1.1:80/html/index.
             html?name=hi
3
4         Flush cache ob -| 0x00000089bae000000004
5         done
6
7 `flush cache object (-locator <positive_integer> | (-url <URL> (-host <
     string> [-port <port>] [-groupName <string>] [-httpMethod ( GET |
     POST )])))`
8 <!--NeedCopy-->
```

Ejemplo:

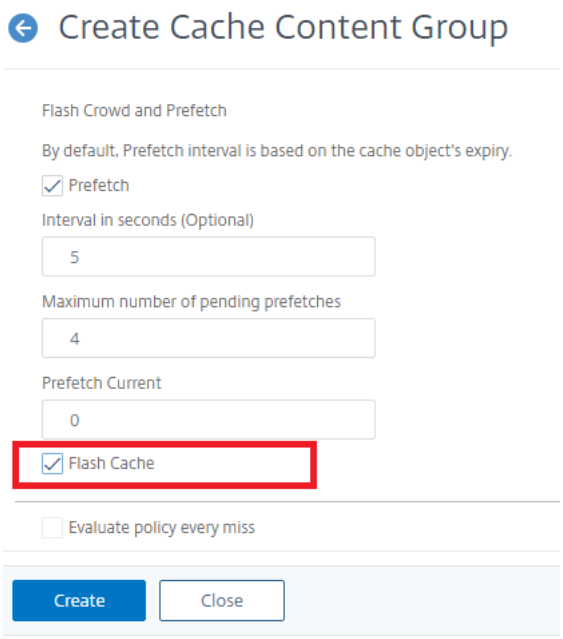
```
1         0x00000089bae000000006 DEFAULT GET //1.1.1.1:80/html/index.html
2
3         flush cache ob -URL /html/index.html -host 1.1.1.1 -groupName
             DEFAULT
4         done
5 <!--NeedCopy-->
```

Vaciar la configuración de caché mediante la GUI de Citrix ADC

Complete los pasos para configurar el vaciado de caché mediante la GUI de Citrix ADC

1. Vaya a **Optimización** > **Grupos de contenido**.
2. En el panel detallado **Grupos de contenido**, haga clic en **Agregar**.
3. En la página **Crear Grupos de Contenido de Caché**, defina el siguiente parámetro en la ficha **Otros** :
    a) Vaciar caché. Active la casilla de verificación para vaciar el objeto de caché.

4. Haga clic en **Crear** y **cerrar**.



Configurar el almacenamiento en caché integrado para varios casos

En la siguiente sección se describe la configuración del almacenamiento en caché integrado en el dispositivo NetScaler para varios casos.

A partir de la versión 9.2 de NetScaler, el almacenamiento en caché integrado tiene más memoria para el almacenamiento en caché. La memoria de almacenamiento en caché integrada solo está limitada por la memoria disponible en el dispositivo de hardware. Puede asignar hasta el 50 por ciento de la memoria disponible a la función de almacenamiento en caché integrado.

Para establecer la asignación de memoria para la caché mediante la CLI

En el símbolo del sistema, escriba:

```
set cache parameter -memlimit <value>
```

> **Nota:**
>
> El límite de memoria global predeterminado para el almacenamiento en caché integrado es cero. Por lo tanto, incluso si habilita la función de almacenamiento en caché integrado, el dispositivo NetScaler no almacena en caché ningún objeto hasta que se establezca explícitamente el límite de memoria global.

En la siguiente sección se indica que debe configurar el almacenamiento en caché integrado en diferentes casos.

> **Nota:**
>
> El límite de memoria del dispositivo NetScaler se identifica cuando se inicia el dispositivo. Por lo tanto, cualquier cambio en el límite de memoria requiere que reinicie el dispositivo para que los cambios sean aplicables a todos los motores de paquetes.

El almacenamiento en caché integrado está habilitado y el límite de memoria caché se establece en distinto de cero

Considere un caso en el que inicie el dispositivo, la función de almacenamiento en caché integrado está habilitada y el límite de memoria global se establece en un número positivo. La memoria que había configurado anteriormente se asigna a la función de almacenamiento en caché integrada durante el proceso de arranque. Es posible que quiera cambiar el límite de memoria a otro valor en función de la memoria disponible en el dispositivo.

Configuración mediante la CLI

1. Mostrar el parámetro de caché

```
1          > show cache parameter
2                  Integrated cache global configuration:
3                  Memory usage limit: 500 MBytes
4                  Memory usage limit (active value): 500 MBytes
5                  Maximum value for Memory usage limit: 843 MBytes
6                  Via header: NS-CACHE-9.3: 18
7                  Verify cached object using: HOSTNAME_AND_IP
8                  Max POST body size to accumulate: 0 bytes
9                  Current outstanding prefetches: 0
10                 Max outstanding prefetches: 4294967295
11                 Treat NOCACHE policies as BYPASS policies: YES
12                 Global Undef Action: NOCACHE
13 <!--NeedCopy-->
```

1. Establecer un límite de memoria distinto de cero

```
set cache parameter -memlimit 600
```

> **Nota:**
>
> El comando anterior muestra el siguiente mensaje de **advertencia: Advertencia: Para utilizar un nuevo límite de memoria caché integrada, guarde la configuración y reinicie el dispositivo NetScaler.**

1. Guardar la configuración

```
save config
```

1. Desde el símbolo del shell, ejecute el siguiente comando para verificar en el archivo de configuración.

```
root@ns## cat /nsconfig/ns.conf | grep memLimit
```

1. Cambiar el límite de memoria

```
set cache parameter -memLimit 600 -via NS-CACHE-9.3: 18 -verifyUsing
HOSTNAME_AND_IP -maxPostLen 0 -enableBypass YES -undefAction NOCACHE
```

1. Reiniciar el dispositivo

```
root@ns## reboot
```

1. Verifique el nuevo valor para el límite de memoria

```
1          > show cache parameter
2                  Integrated cache global configuration:
3                  Memory usage limit: 600 MBytes
4                  Memory usage limit (active value): 600 MBytes
5                  Maximum value for Memory usage limit: 843 MBytes
6                  Via header: NS-CACHE-9.3: 18
7                  Verify cached object using: HOSTNAME_AND_IP
8                  Max POST body size to accumulate: 0 bytes
9                  Current outstanding prefetches: 0
10                 Max outstanding prefetches: 4294967295
11                 Treat NOCACHE policies as BYPASS policies: YES
12                 Global Undef Action: NOCACHE
13 <!--NeedCopy-->
```

Después de que todos los motores de paquetes se inicien correctamente, la función de almacenamiento en caché integrado negocia la memoria que había configurado. Si el dispositivo no puede utilizar la memoria configurada, la memoria se asigna en consecuencia. Si la memoria disponible es inferior a la asignada, el dispositivo recomienda un número menor. La función de almacenamiento en caché integrada utiliza el mismo valor que el valor activo.

El almacenamiento en caché integrado está inhabilitado y el límite de memoria caché se establece en distinto de cero

En este caso, al iniciar el dispositivo, la función de almacenamiento en caché integrado se inhabilita y el límite de memoria global se establece en un número positivo. Por lo tanto, no se asigna memoria al almacenamiento en caché integrado durante el proceso de arranque.

Configuración mediante la CLI

1. Mostrar el parámetro de caché

```
        > show cache parameter
                Integrated cache global configuration:
                Memory usage limit: 600 MBytes
                Maximum value for Memory usage limit: 843 MBytes
                Via header: NS-CACHE-9.3: 18
                Verify cached object using: HOSTNAME_AND_IP
                Max POST body size to accumulate: 0 bytes
                Current outstanding prefetches: 0
                Max outstanding prefetches: 4294967295
                Treat NOCACHE policies as BYPASS policies: YES
                Global Undef Action: NOCACHE
<!--NeedCopy-->
```

1. Establecer un nuevo límite de memoria

```
set cache parameter -memlimit 500
```

> **Nota:**
>
> El comando anterior muestra el siguiente mensaje de advertencia: **Advertencia: Función no activada [IC]**.

1. Guardar la configuración

```
save config
```

1. Desde el símbolo del shell, ejecute el siguiente comando para verificar en el archivo de configuración

```
root@ns## cat /nsconfig/ns.conf | grep memLimit
```

1. Cambiar el límite de memoria

```
set cache parameter -memLimit 500 -via NS-CACHE-9.3: 18 -verifyUsing
HOSTNAME_AND_IP -maxPostLen 0 -enableBypass YES -undefAction NOCACHE
```

1. Verifique el nuevo valor para el límite de memoria

```
        > show cache parameter
                Integrated cache global configuration:
                Memory usage limit: 500 MBytes
                Maximum value for Memory usage limit: 843 MBytes
                Via header: NS-CACHE-9.3: 18
```



```
6                   Verify cached object using: HOSTNAME_AND_IP
7                   Max POST body size to accumulate: 0 bytes
8                   Current outstanding prefetches: 0
9                   Max outstanding prefetches: 4294967295
10                  Treat NOCACHE policies as BYPASS policies: YES
11                  Global Undef Action: NOCACHE
12  <!--NeedCopy-->
```

1. Habilitar la función de almacenamiento en caché integrado

```
enable ns feature IC
```

1. Verifique el nuevo valor para el límite de memoria

```
1           > show cache parameter
2                   Integrated cache global configuration:
3                   Memory usage limit: 500 Mbytes
4                   Memory usage limit (active value): 500 Mbytes
5                   Maximum value for Memory usage limit: 843 MBytes
6                   Via header: NS-CACHE-9.3: 18
7                   Verify cached object using: HOSTNAME_AND_IP
8                   Max POST body size to accumulate: 0 bytes
9                   Current outstanding prefetches: 0
10                  Max outstanding prefetches: 4294967295
11                  Treat NOCACHE policies as BYPASS policies: YES
12                  Global Undef Action: NOCACHE
13  <!--NeedCopy-->
```

> **Nota:**
>
> 500 MB de memoria se asignan a la función de almacenamiento en caché integrada.

1. Guarde la configuración para asegurarse de que la memoria se asigna automáticamente a la función cuando se reinicie el dispositivo.

El almacenamiento en caché integrado está habilitado y la memoria caché se establece en cero

En este caso, al iniciar el dispositivo, la función de almacenamiento en caché integrado está habilitada y el límite de memoria global se establece en cero. Por lo tanto, no se asigna memoria al almacenamiento en caché integrado durante el proceso de arranque.

Configuración mediante la CLI

1. Verifique los límites de memoria establecidos en el archivo ns.conf desde el símbolo del shell


```
root@ns## cat ns.conf | grep memLimit
```

1. Cambiar el límite de memoria

```
set cache parameter -memLimit 0 -via NS-CACHE-9.3: 18 -verifyUsing HOSTNAME_AND_IP
 -maxPostLen 4096 -enableBypass YES -undefAction NOCACHE
```

1. Verifique el valor del límite de memoria

```
1          > show cache parameter
2                  Integrated cache global configuration:
3                  Memory usage limit: 0 Mbytes
4                  Maximum value for Memory usage limit: 843 MBytes
5                  Via header: NS-CACHE-9.3: 18
6                  Verify cached object using: HOSTNAME_AND_IP
7                  Max POST body size to accumulate: 0 bytes
8                  Current outstanding prefetches: 0
9                  Max outstanding prefetches: 4294967295
10                 Treat NOCACHE policies as BYPASS policies: YES
11                 Global Undef Action: NOCACHE
12 <!--NeedCopy-->
```

> **Nota:**
>
> El límite de memoria se establece en 0 MB y no se asigna memoria a la función de almacenamiento en caché integrada.

1. Establezca los límites de memoria para garantizar que la función de almacenamiento en caché integrada almacena en caché objetos

```
set cache parameter -memLimit 600
```

Una vez ejecutado el comando anterior, el dispositivo negocia la memoria para la función de almacenamiento en caché integrada y la memoria disponible se asigna a la función. Esto da como resultado el almacenamiento en caché de objetos del dispositivo sin reiniciar el dispositivo.

1. Verifique el valor del límite de memoria

```
1          > show cache parameter
2                  Integrated cache global configuration:
3                  Memory usage limit: 600 Mbytes
4                  Memory usage limit (active value): 600 Mbytes
5                  Maximum value for Memory usage limit: 843 MBytes
6                  Via header: NS-CACHE-9.3:
7                  Verify cached object using: HOSTNAME_AND_IP
```



```
8                   Max POST body size to accumulate: 0 bytes
9                   Current outstanding prefetches: 0
10                  Max outstanding prefetches: 4294967295
11                  Treat NOCACHE policies as BYPASS policies: YES
12                  Global Undef Action: NOCACHE
13 <!--NeedCopy-->
```

> **Nota:**
>
> 600 MB de memoria se asignan a la función de almacenamiento en caché integrado.

1. Guarde la configuración. Asegúrese de que la memoria se asigna automáticamente a la función cuando se reinicie el dispositivo.
2. Verifique los límites de memoria establecidos en el archivo ns.conf desde el símbolo del shell

```
root@ns## cat /nsconfig/ns.conf | grep memLimit
```

1. Cambiar el límite de memoria

```
set cache parameter -memLimit 600 -via NS-CACHE-9.3: -verifyUsing HOSTNAME_AND_IP
 -maxPostLen 4096 -enableBypass YES -undefAction NOCACHE
```

El almacenamiento en caché integrado está inhabilitado y la memoria caché se establece en cero

En este caso, al iniciar el dispositivo, la función de almacenamiento en caché integrado se inhabilita y el límite de memoria global se establece en cero. Por lo tanto, no se asigna memoria al almacenamiento en caché integrado durante el proceso de arranque.

Configuración mediante la CLI

1. Verifique los límites de memoria establecidos en el archivo ns.conf desde el símbolo del shell

```
root@ns## cat /nsconfig/ns.conf | grep memLimit
```

1. Cambiar el límite de memoria

```
set cache parameter -memLimit 0 -via NS-CACHE-9.3: 18 -verifyUsing HOSTNAME_AND_IP
 -maxPostLen 4096 -enableBypass YES -undefAction NOCACHE
```

1. Verifique el valor del límite de memoria

```
1          > show cache parameter
2                  Integrated cache global configuration:
3                  Memory usage limit: 0 Mbytes
```



```
4                   Maximum value for Memory usage limit: 843 MBytes
5                   Via header: NS-CACHE-9.3: 18
6                   Verify cached object using: HOSTNAME_AND_IP
7                   Max POST body size to accumulate: 0 bytes
8                   Current outstanding prefetches: 0
9                   Max outstanding prefetches: 4294967295
10                  Treat NOCACHE policies as BYPASS policies: YES
11                  Global Undef Action: NOCACHE
12 <!--NeedCopy-->
```

> **Nota:**
>
> El límite de memoria se establece en 0 MB y no se asigna memoria a la función de almacenamiento en caché integrada. Además, al ejecutar cualquier comando de configuración de caché, se muestra el siguiente mensaje de advertencia: **Advertencia: Función no habilitada [IC]**.

1. Habilitar la función de almacenamiento en caché integrado

```
enable ns feature IC
```

> **Nota:**
>
> En esta etapa, cuando se habilita la función de almacenamiento en caché integrado, el dispositivo no asigna memoria a la función. Como resultado, no se almacena en caché ningún objeto en la memoria. Además, cuando ejecuta cualquier comando de configuración de caché, se muestra el siguiente mensaje de advertencia: **No hay memoria configurada para IC. Utilice el comando set cache parameter para establecer el límite de memoria.**

1. Establezca los límites de memoria para garantizar que la función de almacenamiento en caché integrada almacena en caché objetos

```
set cache parameter -memLimit 500
```

Una vez ejecutado el comando anterior, el dispositivo negocia la memoria para la función de almacenamiento en caché integrada y la memoria disponible se asigna a la función. El resultado es que el dispositivo almacenará en caché objetos sin reiniciar el dispositivo.

> **Nota:**
>
> El orden en el que habilita la función y establece los límites de memoria es importante. Si establece los límites de memoria antes de habilitar la función, aparecerá el siguiente mensaje de advertencia: **Advertencia: Función no habilitada [IC]**.

1. Verifique el valor del límite de memoria

```
1          > show cache parameter
```



```
                Integrated cache global configuration:
                Memory usage limit: 500 Mbytes
                Memory usage limit (active value): 500 Mbytes
                Maximum value for Memory usage limit: 843 MBytes
                Via header: NS-CACHE-9.3:
                Verify cached object using: HOSTNAME_AND_IP
                Max POST body size to accumulate: 0 bytes
                Current outstanding prefetches: 0
                Max outstanding prefetches: 4294967295
                Treat NOCACHE policies as BYPASS policies: YES
                Global Undef Action: NOCACHE
<!--NeedCopy-->
```

> **Nota:**
>
> 500 MB de memoria se asignan a la función de almacenamiento en caché integrada.

1. Guardar la configuración

```
save config
```

1. Verifique los límites de memoria establecidos en el archivo ns.conf desde el símbolo del shell

```
root@ns## cat /nsconfig/ns.conf | grep memLimit
```

1. Cambiar el límite de memoria

```
set cache parameter -memLimit 500 -via NS-CACHE-9.3: 18 -verifyUsing
HOSTNAME_AND_IP -maxPostLen 4096 -enableBypass YES -undefAction NOCACHE
```

Configurar selectores y grupos de contenido básico

August 20, 2021

Puede configurar selectores y aplicarlos a grupos de contenido. Cuando se agrega un selector a uno o varios grupos de contenido, se especifica si el selector se va a utilizar para identificar solicitudes de caché o identificar objetos almacenados en caché que se van a invalidar (caducado). Los selectores son opcionales. También puede configurar grupos de contenido para que utilicen `hit` parámetros y parámetros de invalidación. Sin embargo, Citrix recomienda configurar selectores.

Después de configurar selectores o de decidir utilizar parámetros en su lugar, está listo para configurar un grupo de contenido básico. Después de crear el grupo de contenido básico, debe decidir cómo deben caducar los objetos de la caché y configurar la caducidad de la caché. Puede modificar la caché como se describe en Mejora del rendimiento de la caché y Configuración de cookies, encabezados y sondeos, pero es posible que primero desee configurar las directivas de almacenamiento en caché.

> **Nota**
>
> Los parámetros y selectores de grupos de contenido se utilizan solo en el momento de la solicitud y, por lo general, los asocia con directivas que utilizan acciones MAY_CACHE o MAY_NOCACHE.

Ventajas de los selectores

Un selector es un filtro que localiza objetos concretos en un grupo de contenido. Si no configura un selector, el dispositivo Citrix® ADC busca una coincidencia exacta en el grupo de contenido. Esto puede dar lugar a que varias copias del mismo objeto residan en un grupo de contenido. Por ejemplo, un grupo de contenido que no tiene un selector puede necesitar almacenar direcciones URL para host1.domain.commypage.htm, host2.domain.commypage.htm y host3.domain.commypage.htm. Por el contrario, un selector puede coincidir solo con la URL (mypage.html, mediante la expresión http.req.url) y el dominio (.com, mediante la expresión http.req.hostname.domain), permitiendo que las solicitudes se satisfagan con la misma URL.

Las expresiones selectoras pueden realizar una coincidencia simple de parámetros (por ejemplo, para buscar objetos que coincidan con algunos parámetros de cadena de consulta y sus valores). Una expresión de selector puede utilizar lógica booleana, operaciones aritméticas y combinaciones de atributos para identificar objetos (por ejemplo, segmentos de un tallo de URL, una cadena de consulta, una cadena en un cuerpo de solicitud POST, una cadena en un encabezado HTTP, una cookie). Los selectores también pueden realizar funciones programáticas para analizar la información de una solicitud. Por ejemplo, un selector puede extraer texto en un cuerpo POST, convertir el texto en una lista y extraer un elemento específico de la lista.

Para obtener más información sobre las expresiones y lo que se puede especificar en una expresión, consulte Directivas y expresiones.

Usar parámetros en lugar de selectores

Aunque Citrix recomienda el uso de selectores con un grupo de contenido, puede configurar parámetros y `hit` parámetros de invalidación. Por ejemplo, supongamos que configura tres `hit` parámetros en un grupo de contenido para los informes de errores: BugID, Emiser y Asignnee. Si una solicitud contiene BugID=456, con Issuer=RohiTV y Assignee=Robert, el dispositivo Citrix ADC puede ofrecer respuestas que coincidan con estos pares de parámetros y valores.

Los parámetros de invalidación en un grupo de contenido caducan las entradas almacenadas en caché. Por ejemplo, supongamos que BugID es un parámetro de invalidación y un usuario emite una solicitud POST para actualizar un informe de error. Una directiva de invalidación dirige la solicitud a este grupo de contenido y el parámetro de invalidación del grupo de contenido caduca todas las respuestas almacenadas en caché que coincidan con el valor de BugID. (La próxima vez que un usuario envíe una solicitud GET para este informe, una directiva de almacenamiento en caché puede

permitir que el dispositivo Citrix ADC actualice la entrada almacenada en caché del informe desde el servidor de origen.)

Tenga en cuenta que el mismo parámetro se puede utilizar como `hit` parámetro o como parámetro de invalidación.

Los grupos de contenido extraen los parámetros de solicitud en el siguiente orden:

- Consulta de URL
- Cuerpo POST
- Encabezado de cookies

Después de la primera aparición de un parámetro, independientemente de dónde se produjo en la solicitud, todas sus ocurrencias posteriores se ignoran. Por ejemplo, si existe un parámetro tanto en la consulta URL como en el cuerpo POST, solo se considera el de la consulta URL.

Si decide utilizar parámetros de aciertos e invalidación para un grupo de contenido, configure los parámetros cuando configure el grupo de contenido.

Nota: Citrix recomienda utilizar selectores en lugar de grupos de contenido parametrizados, ya que los selectores son más flexibles y se pueden adaptar a más tipos de datos.

Configurar un selector

Un grupo de contenido puede utilizar un selector de visitas para recuperar aciertos de caché o utilizar un selector de invalidación para objetos caducados en caché y obtener otros nuevos desde el servidor de origen.

Un selector contiene un nombre y una expresión lógica, denominada *expresión avanzada*.

Para obtener más información sobre las expresiones avanzadas, consulte Directivas y expresiones.

Para configurar un selector, asigne un nombre e introduzca una o más expresiones. Como práctica recomendada, una expresión de selector debe incluir la dirección URL y el host, a menos que haya una razón fuerte para omitirlos.

Para configurar un selector mediante la CLI

En el símbolo del sistema, escriba:

```
add cache selector \<selectorName\> ( \<rule\> ... )
```

Para obtener información sobre la configuración de la expresión o expresiones, consulte Para configurar una expresión de selector mediante la interfaz de línea de comandos.

```
1 >add cache selector product_selector "http.req.url.query.value("
     ProductId")" "http.req.url.query.value("BatchNum")" "http.req.url.
     query.value("depotLocation")"
```



```
2
3 > add cache selector batch_selector "http.req.url.query.value("
    ProductId")" "http.req.url.query.value("BatchId")" "http.req.url.
    query.value("depotLocation")"
4
5 > add cache selector product_id_selector "http.req.url.query.value("
    ProductId")"
6
7 > add cache selector batchnum_selector "http.req.url.query.value("
    BatchNum")" "http.req.url.query.value("depotLocation")"
8
9 > add cache selector batchid_selector "http.req.url.query.value("
    depotLocation")" "http.req.url.query.value("BatchId")"
10
11 <!--NeedCopy-->
```

Para configurar un selector mediante la interfaz gráfica de usuario

Vaya a **Optimización > Almacenamiento en caché integrado > Selectores**de caché y agregue el selector de caché.

Grupos de contenido

Un grupo de contenido es un contenedor para objetos almacenados en caché que se pueden servir en una respuesta. Cuando habilita por primera vez la caché integrada, los objetos que se pueden almacenar en caché se almacenan en un grupo de contenido denominado Predeterminado. Puede crear grupos de contenido que tengan propiedades únicas. Por ejemplo, puede definir grupos de contenido separados para datos de imágenes, informes de errores y cotizaciones de valores, y puede configurar el grupo de contenido de cotización de valores para que se actualice con más frecuencia que los demás grupos.

Puede configurar la caducidad de un grupo de contenido completo o de las entradas seleccionadas de un grupo de contenido.

Los datos de un grupo de contenido pueden ser estáticos o dinámicos, como se indica a continuación:

- **Grupos de contenido estático**. Busca una coincidencia exacta entre el origen de URL y el nombre de host en la solicitud y el nombre de dirección URL y el nombre de host de la respuesta.
- **Grupos de contenido dinámicos**. Busca objetos que contengan pares de parámetros y valores concretos, cadenas arbitrarias o patrones de cadena. Los grupos de contenido dinámicos son útiles al almacenar en caché datos que se actualizan con frecuencia (por ejemplo, un informe de errores o una cotización de acciones).

Servir una solicitud de un grupo de contenido

1. Un usuario introduce criterios de búsqueda para un elemento, como un informe de error, y hace clic en el botón Buscar en un formulario HTML.
2. El explorador emite una o más solicitudes HTTP GET. Estas solicitudes contienen parámetros (por ejemplo, el propietario del error, ID del error, etc.).
3. Cuando el dispositivo Citrix ADC recibe las solicitudes, busca una directiva coincidente y, si encuentra una directiva de almacenamiento en caché que coincida con estas solicitudes, dirige las solicitudes a un grupo de contenido.
4. El grupo de contenido busca los objetos apropiados en el grupo de contenido, en función de los criterios que configure en un selector.

Por ejemplo, el grupo de contenido puede recuperar respuestas que coincidan `NameField=username and BugID=ID`.

1. Si encuentra objetos coincidentes, el dispositivo Citrix ADC puede servirlos al explorador del usuario, donde se ensamblan en una respuesta completa (por ejemplo, un informe de errores).

Invalidar un objeto en un grupo de contenido

1. Un usuario modifica los datos (por ejemplo, el usuario modifica el informe de errores y hace clic en el botón Enviar).
2. El explorador envía estos datos en forma de una o más solicitudes HTTP. Por ejemplo, puede enviar un informe de error en forma de varias solicitudes HTTP POST que contienen información sobre el propietario del error y el ID del error.
3. El dispositivo Citrix ADC hace coincidir las solicitudes con las directivas de invalidación. Normalmente, estas directivas se configuran para detectar el método HTTP POST.
4. Si la solicitud coincide con una directiva de invalidación, el dispositivo Citrix ADC busca el grupo de contenido asociado a esta directiva y caduca las respuestas que coinciden con los criterios de invalidación configurados.

Por ejemplo, un selector de invalidación puede encontrar respuestas que coincidan `NameField=username and BugID=ID`.

1. La próxima vez que el dispositivo Citrix ADC reciba una solicitud GET para estas respuestas, obtiene las versiones actualizadas del servidor de origen, almacena en caché las respuestas actualizadas y las envía al explorador del usuario, donde se ensamblan en un informe de errores completo.

Configurar un grupo de contenido básico

De forma predeterminada, todos los datos almacenados en caché se almacenan en el grupo de contenido predeterminado. Puede configurar más grupos de contenido y especificar estos grupos de contenido en una o varias directivas.

Puede configurar grupos de contenido para contenido estático y debe configurar grupos de contenido

para contenido dinámico. Puede modificar la configuración de cualquier grupo de contenido, incluido el grupo predeterminado.

Para configurar un grupo de contenido básico mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
add cache contentgroup <name> (-hitSelector <hitSelectorName> -invalSelector
 <invalidationSelectorName> | -hitParams <hitParamName> -invalParams<
invalidationParamName>)-type <type> [-relExpiry <sec> | -relExpiryMilliSec
<msec>] [-heurExpiryParam <positiveInteger>]
```

```
add cache contentgroup Products_Details -hitSelector product_selector -
invalSelector id_selector
```

```
add cache contentgroup bugrep -hitParams IssuePage RecordID Template
TableId -invalParams RecordID -relExpiry 864000
```

Para configurar un grupo de contenido básico mediante la interfaz gráfica de usuario

Vaya a **Optimización > Almacenamiento en caché integrado > Grupos de contenido** y cree el grupo de contenido.

Caducar o vaciar objetos almacenados en caché

Si una respuesta no tiene un encabezado Expira o un encabezado Cache-Control con un tiempo de caducidad (Max-Age o Smax-Age), debe caducar los objetos de un grupo de contenido mediante uno de los métodos siguientes:

- Configure la configuración de caducidad del grupo de contenido para determinar si quiere conservar el objeto y durante cuánto tiempo.
- Configure una directiva de invalidación y una acción para el grupo de contenido. Para obtener más información, consulte Configuración de directivas para almacenamiento en caché e invalidación.
- Expirar manualmente el grupo de contenido u objetos dentro de él.

Después de que caduque una respuesta almacenada en caché, el dispositivo Citrix ADC la actualizará la próxima vez que el cliente envíe una solicitud de respuesta. De forma predeterminada, cuando la caché está llena, el dispositivo Citrix ADC reemplaza primero la respuesta utilizada menos recientemente.

En la lista siguiente se describen los métodos para caducar las respuestas almacenadas en caché mediante la configuración de un grupo de contenido. Normalmente, estos métodos se especifican como porcentaje o en segundos:

- **Manual**. Invalide manualmente todas las respuestas de un grupo de contenido o todas las respuestas de la caché.

- **Basado en respuesta**. Intervalos de caducidad específicos para respuestas positivas y negativas. La caducidad basada en respuesta se considera solo si falta el encabezado Last-Modified en la respuesta.
- **Caducidad heurística**. Para las respuestas que tienen un encabezado Last-Modified, la caducidad heurística especifica el montaje del tiempo transcurrido desde el momento en que se modificó la respuesta (calculado como el tiempo actual menos el tiempo de última modificación, multiplicado por el valor de caducidad heurística). Por ejemplo, si un encabezado Last-Modified indica que una respuesta se actualizó hace 2 horas y la configuración de caducidad heurística es 10%, los objetos almacenados en caché caducan después de 0,2 horas. Este método supone que las respuestas actualizadas con frecuencia deben caducarse con más frecuencia.
- **Absoluto o relativo**. Especifique una hora exacta (absoluta) cuando la respuesta caduque todos los días, en formato HH:MM, hora local o GMT. La hora local puede no funcionar en todas las zonas horarias.

La caducidad relativa especifica algunos segundos o milisegundos desde el momento en que una falta de caché provoca un viaje al servidor de origen hasta la expiración de la respuesta. Si especifica la caducidad relativa en milisegundos, introduzca un múltiplo de 10. Esta forma de caducidad funciona para todas las respuestas positivas. Los encabezados Last-Modified, Expira y Cache-Control en la respuesta se ignoran.

La caducidad absoluta y relativa anula cualquier información de caducidad en la respuesta misma.

- **En descarga**. La opción Caducar después de completar la respuesta recibida caduca una respuesta cuando se descarga. Esto es útil para respuestas actualizadas con frecuencia, por ejemplo, cotizaciones de acciones. De forma predeterminada, esta opción está inhabilitada.

Habilitar Flash Cache y Expirar después de la respuesta completa recibida acelera el rendimiento de las aplicaciones dinámicas. Cuando habilita ambas opciones, el dispositivo Citrix ADC obtiene solo una respuesta para un bloque de solicitudes simultáneas.

- **Apuntado**. De forma predeterminada, cuando la caché está llena, el dispositivo Citrix ADC reemplaza primero la respuesta utilizada menos recientemente. El dispositivo Citrix ADC no aplica este comportamiento a grupos de contenido marcados como anclados.

Si no configura la configuración de caducidad para un grupo de contenido, las siguientes son más opciones para los objetos que caducan en el grupo:

- Configure una directiva con una acción INVAL que se aplique al grupo de contenido.
- Introduzca los nombres de los grupos de contenido al configurar una directiva que utilice una acción INVAL.

Cómo se aplican los métodos de caducidad

La caducidad funciona de manera diferente para las respuestas positivas y negativas. Las respuestas positivas y negativas se describen en el cuadro *Expiración de las respuestas positivas y negativas* que se mencionan a continuación.

Las siguientes son las reglas básicas para comprender el método de caducidad que se aplica a un grupo de contenido:

- Puede controlar si el dispositivo Citrix ADC evalúa los encabezados de respuesta al decidir si caduca un objeto.
- La caducidad absoluta y relativa hace que el dispositivo Citrix ADC ignore los encabezados de respuesta (anulan cualquier información de caducidad de la respuesta).
- La configuración de caducidad heurística y la caducidad "Positivo débil" y "Negativo débil" (etiquetados como valores **predeterminados** en la utilidad de configuración) hacen que el dispositivo Citrix ADC examine los encabezados de respuesta. Estas configuraciones funcionan juntas de la siguiente manera:
  - El valor de un encabezado Expira o Control de caché anula esta configuración de grupo de contenido.
  - Para respuestas positivas que carecen de un encabezado Expira o Cache-Control pero tienen un encabezado Last Modified, el dispositivo Citrix ADC compara la configuración de caducidad heurística con el valor del encabezado.
  - Para las respuestas positivas que carecen de un encabezado Expires, Cache-Control o Last-Modified, el dispositivo Citrix ADC utiliza el valor "positivo débil".
  - Para las respuestas negativas que carecen de un encabezado Expires o Cache-Control, el dispositivo Citrix ADC utiliza el valor "negativo débil".

En la tabla siguiente se describe cómo se aplican estos métodos.

Tipo de respuesta	Tipo de cabecera de	Configuración del grupo de contenido	Período en el que permanece el objeto en la caché
Positivo	Cualquier encabezado	Caducar contenido después (Relexpiry) sin ninguna otra configuración	Utilice el valor de la opción **Caducar contenido después**.
Positivo	Cualquier encabezado	Caducar contenido en (AbsExpiry) sin otra configuración	Reste la fecha actual del valor de la configuración **Caducar contenido en**.

Tipo de respuesta	Tipo de cabecera de	Configuración del grupo de contenido	Período en el que permanece el objeto en la caché
Positivo	Cualquier encabezado	Caducar contenido después de (RelexPry) y caducar contenido en (AbsExpiry)	Utilice el menor de los dos valores para la configuración del grupo de contenido. Vea las filas anteriores de esta tabla.
Positivo	Última modificación (con cualquier otro encabezado)	Heuristic (HeureXpiry Param) con cualquier otro ajuste	Resta la fecha de última modificación de la fecha actual, multiplique el resultado por el valor de la configuración de caducidad heurística y, a continuación, divida por 100.
Positivo	Última modificación (con cualquier otro encabezado)	Predeterminado (positivo) (WeakPorel Caducidad) y no hay otro ajuste	Utilice el valor de la configuración de caducidad predeterminada (positiva).
Positivo	Caduca o Cache-Control: El encabezado Max-Age está presente	El encabezado Última modificación está ausente, heurístico (HeureXpiry Param), Default (positivo) (Expiración WeakPorel), o ambos	Resta la fecha actual de la caducidad o la `Cache-Control: Max-Age` fecha.
Positivo	sin cabeceras de almacenamiento en caché	Predeterminado (positivo) (WeakPorel Caducidad) y cualquier otra configuración de caducidad	Utilice el valor de la configuración Predeterminado (positivo).

Tipo de respuesta	Tipo de cabecera de	Configuración del grupo de contenido	Período en el que permanece el objeto en la caché
Positivo	sin cabeceras de almacenamiento en caché	Heurístico (HeureXpiry Param) está presente, el ajuste Default (positivo) (Expiración WeakPorel) está ausente.	Si el encabezado Last-Modified está ausente, la respuesta no se almacena en caché o se almacena en caché con un estado Ya caducado. Si el encabezado Last-Modified está presente, utilice el valor de caducidad heurístico.
Negativo	Caduca o `Cache-Control:Max-Age`	Caducar contenido después de (Relexpiry), Caducar contenido en (AbsExpiry) o ambas opciones	Resta la fecha actual del valor de la cabecera Expira, o utilice el valor de la cabecera Cache-Control: Max-Age.
Negativo	Caduca o los encabezados Cache-Control están ausentes	Caducar contenido después de (Relexpiry), Caducar contenido en (AbsExpiry) o ambas opciones	La respuesta no se almacena en caché o se almacena en caché con un estado Ya caducado.
Negativo	Caduca o `Cache-Control:Max-Age`	Cualquier configuración	Resta la fecha actual de la fecha de caducidad o `Cache-Control:Max-Age` fecha.
Negativo	Expira y Cache-Control: Max-Age encabezados están ausentes	Predeterminado (negativo) (WeakNegrel Caducidad)	Utilice el valor de la configuración Predeterminado (negativo).

Tipo de respuesta	Tipo de cabecera de	Configuración del grupo de contenido	Período en el que permanece el objeto en la caché
Negativo	Expira y Cache-Control: Max-Age encabezados están ausentes	Cualquier configuración distinta de Predeterminado (negativo) (WeakNegrel Caducidad)	El objeto no se almacena en caché o se almacena en caché con un estado Ya caducado.

Caducar un grupo de contenido por método manual

Puede caducar manualmente todas las entradas de un grupo de contenido.

Para caducar manualmente todas las respuestas de un grupo de contenido mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
expire cache contentGroup <name>
```

Para caducar manualmente todas las respuestas de un grupo de contenido mediante la interfaz gráfica de usuario

Vaya a **Optimización > Almacenamiento en caché integrado > Grupos**de contenido, seleccione el grupo de contenido y haga clic en Invalidar para caducar todas las respuestas de un grupo de contenido.

Para caducar manualmente todas las respuestas en la caché mediante la interfaz gráfica de usuario

Vaya a **Optimización > Almacenamiento en caché integrado > Grupos de contenido** y haga clic en Invalidar todo para caducar todas las respuestas de la caché.

Configurar el vencimiento periódico de un grupo de contenido

Puede configurar un grupo de contenido para que realice la caducidad selectiva o completa de sus entradas. El intervalo de caducidad puede ser fijo o relativo.

Para configurar la expiración del grupo de contenido mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
set cache contentgroup \<name> (-relExpiry|-relExpiryMilliSec|-absExpiry
|-absExpiryGMT| -heurExpiryParam|-weakPosRelExpiry|-weakNegRelExpiry| -
expireAtLastBye)\<expirationValue>
```


Para configurar la expiración del grupo de contenido mediante la interfaz gráfica de usuario

Vaya a **Optimización** > Almacenamiento en **caché integrado** > **Grupos de contenido**, seleccione el grupo de contenido y especifique el método de caducidad.

Expirar respuestas individuales

La expiración de una respuesta obliga al dispositivo Citrix ADC a obtener una copia actualizada del servidor de origen. Las respuestas que no tienen validadores, por ejemplo, `ETag` o encabezados Last-Modified, no se pueden revalidar. Como resultado, el lavado de estas respuestas tiene el mismo efecto que expiarlas.

Para caducar una respuesta almacenada en caché en un grupo de contenido para datos estáticos, puede especificar una dirección URL que debe coincidir con la URL almacenada. Si la respuesta almacenada en caché forma parte de un grupo de contenido parametrizado, debe especificar el nombre del grupo y el tronco de URL exacto. El nombre de host y el número de puerto deben ser los mismos que en el encabezado de solicitud HTTP del host de la respuesta almacenada en caché. Si no se especifica el puerto, se asume el puerto 80.

Para caducar respuestas individuales en un grupo de contenido mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
expire cache object -url <URL> -host <hostName> [-port <port>] [-groupName<
contentGroupName>] [-httpMethod GET|POST]
```

Para caducar respuestas individuales en un grupo de contenido mediante la CLI

En el símbolo del sistema, escriba el siguiente comando:

```
expire cache object -locator <positiveInteger>
```

Para caducar una respuesta almacenada en caché mediante la interfaz gráfica de usuario

Vaya a **Optimización** > Almacenamiento en **caché integrado** > **Objetos almacenados en caché**, seleccione la respuesta almacenada en caché y caduque.

Para caducar una respuesta mediante la interfaz gráfica de usuario

Vaya a **Optimización** > Almacenamiento en **caché integrado** > **Objetos almacenados en caché**, haga clic en **Buscar** y defina los criterios de búsqueda para encontrar la respuesta requerida en caché y caducar.

Descarga de respuestas en un grupo de contenido

Puede quitar o vaciar todas las respuestas de un grupo de contenido, algunas respuestas de un grupo o todas las respuestas de la caché. El vaciado de una respuesta en caché libera memoria para nuevas

respuestas en caché.

> **Nota:**
>
> Para vaciar las respuestas de más de un objeto a la vez, utilice el método de utilidad de configuración. La interfaz de línea de comandos no ofrece esta opción.

Para vaciar respuestas de un grupo de contenido mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
flush cache contentGroup <name> [-query <queryString> | [-selectorValue <
selectorExpressionIDList> -host <hostName>]]
```

Para vaciar las respuestas de un grupo de contenido mediante la interfaz gráfica de usuario

1. Vaya a **Optimización** > Almacenamiento en **caché integrado** > **Grupos de contenido**.
2. En el panel de detalles, vacíe las respuestas de la siguiente manera:
   - Para vaciar todas las respuestas de todos los grupos de contenido, haga clic en Invalidar todo y vacíe todas las respuestas.
   - Para vaciar las respuestas de un grupo de contenido concreto, seleccione el grupo de contenido, haga clic en **Invalidar** y vacíe todas las respuestas.

> **Nota**:
> Si este grupo de contenido utiliza un selector, puede vaciar las respuestas de forma selectiva introduciendo una cadena en el cuadro de texto Valor del selector, introduciendo un nombre de host en el cuadro de texto Host. A continuación, haga clic en **Desactivar y Aceptar**. El valor Selector puede ser una cadena de consulta de hasta 2319 caracteres que se utiliza para la invalidación parametrizada.

Si el grupo de contenido utiliza un parámetro de invalidación, puede vaciar selectivamente las respuestas introduciendo una cadena en el campo **Consulta**.

Si el grupo de contenido utiliza un parámetro de invalidación y está configurado Invalidar objetos pertenecientes al host de destino, introduzca cadenas en los campos **Consulta y Host**.

Para vaciar una respuesta en caché mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
flush cache object -locator <positiveInteger> | -url <URL> -host <hostName>
 [-port <port>] [-groupName <contentGroupName>] [-httpMethod GET|POST]
```

Para vaciar una respuesta en caché mediante la interfaz gráfica de usuario

Vaya a **Optimización** > Almacenamiento en **caché integrado** > **Objetos almacenados en caché**, seleccione el objeto almacenado en caché y vaciado.

Eliminación de un grupo de contenido

Puede quitar un grupo de contenido si no lo usa ninguna directiva que almacene respuestas en la caché. Si el grupo de contenido está enlazado a una directiva, primero debe quitarla. Al quitar el grupo de contenido, se quitan todas las respuestas almacenadas en ese grupo.

No puede quitar el grupo Predeterminado, BASEFILE o Deltas. El grupo predeterminado almacena respuestas almacenadas en caché que no pertenecen a ningún otro grupo de contenido.

Para eliminar un grupo de contenido mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
rm cache contentgroup <name>
```

Para eliminar un grupo de contenido mediante la interfaz gráfica de usuario

Vaya a **Optimización** > Almacenamiento en **caché integrado** > **Grupos de contenido,** seleccione el grupo de contenido y suprima.

Configurar directivas para el almacenamiento en caché y la invalidación

August 20, 2021

Las directivas permiten que la caché integrada determine si se intenta ofrecer una respuesta desde la caché o desde el origen. El dispositivo NetScaler proporciona directivas integradas para el almacenamiento en caché integrado y puede configurar más directivas. Cuando configura una directiva, la asocia con una acción. Una acción almacena en caché los objetos a los que se aplica la directiva o invalida (caduca) los objetos. Normalmente, las directivas de almacenamiento en caché se basan en la información de las solicitudes GET y POST. Normalmente, las directivas de invalidación se basan en la presencia del método POST en las solicitudes, junto con otra información. Puede utilizar cualquier información en una solicitud GET o POST en un almacenamiento en caché o una directiva de invalidación.

Puede ver algunas de las directivas integradas en el nodo Directivas de la caché integrada en la utilidad de configuración. Los nombres de directiva integrados comienzan con un guión bajo (_).

Las acciones determinan lo que hace el dispositivo NetScaler cuando el tráfico coincide con una directiva. Las siguientes acciones están disponibles:

- **Acciones de almacenamiento en caché**. Las directivas que asocia con la acción CACHE almacenan las respuestas en la caché y las sirven desde la caché.
- **Acciones de invalidación**. Las directivas que asocia con la acción INVAL caducan inmediatamente las respuestas almacenadas en caché y las actualizan desde el servidor de origen. Para

las aplicaciones basadas en Web, las directivas de invalidación suelen evaluar las solicitudes POST.

- **Acciones "No almacenar en caché"**. Las directivas que asocia con una acción NOCACHE nunca almacenan objetos en la caché.
- **Acciones en caché provisionalmente**. Las directivas que asocia a una acción MAYCACHE o MAYNOCACHE dependen del resultado de más evaluaciones de directivas.

Aunque la caché integrada no almacena los objetos especificados por el método LOCK, puede invalidar los objetos almacenados en caché tras recibir una `LOCK` solicitud. Solo para las directivas de invalidación, puede especificarlo `LOCK` como método mediante la expresión `http.req.method.eq ( "lock" )`. A diferencia de las directivas `GET` y las `POST` solicitudes, debe incluir el método LOCK entre comillas porque el dispositivo NetScaler reconoce este nombre de método solo como cadena.

Después de crear una directiva, la vincula a un punto concreto del procesamiento general de solicitudes y respuestas. Aunque crea una directiva antes de vincularla, debe comprender cómo afectan los puntos de enlace al orden de procesamiento antes de crear las directivas.

Las directivas vinculadas a un punto de enlace determinado constituyen un banco de pólizas. Puede utilizar expresiones goto para modificar el orden de ejecución en un banco de directivas. También puede invocar directivas en otros bancos de directivas. Además, puede crear etiquetas y enlazar directivas a ellas. Dicha etiqueta no está asociada a un punto de procesamiento, pero las directivas vinculadas a ella pueden invocarse desde otros bancos de directivas.

Acciones para asociar con directivas de almacenamiento en caché integradas

En la siguiente tabla se describen las acciones de las directivas de almacenamiento en caché integradas.

Action	Especificación
CACHÉ	Sirve una respuesta de la caché si la respuesta no ha caducado. Si la respuesta se debe obtener desde el servidor de origen, el dispositivo NetScaler almacena en caché la respuesta antes de servirla. Incluso los datos que se actualizan y se accede con frecuencia se pueden almacenar en caché. Por ejemplo, las cotizaciones de acciones se actualizan con frecuencia, pero se pueden almacenar en caché para que se puedan servir rápidamente a varios usuarios. Si es necesario, los datos almacenados en caché se pueden actualizar inmediatamente después de descargarlos. Una acción CACHE puede ser anulada por directivas integradas.
NOCACHE	Siempre obtiene la respuesta del servidor de origen y marca la respuesta como no almacenable. Normalmente, se configuran las directivas NOCACHE para datos confidenciales o personalizados.

Action	Especificación
MAY_CACHE	Esta configuración, que se utiliza en una directiva de tiempo de solicitud, permite provisionalmente almacenar una respuesta en un grupo de contenido, a la espera de la evaluación de las directivas de tiempo de respuesta. Son posibles las siguientes: 1. Si una directiva de tiempo de respuesta coincidente tiene una acción CACHE pero no especifica un grupo de contenido, la respuesta se almacena en el grupo Predeterminado a menos que las directivas integradas reemplacen esta directiva. 2. Si una directiva de tiempo de respuesta coincidente tiene una acción CACHE y especifica el mismo grupo de contenido que el de la directiva de tiempo de solicitud, la respuesta se almacena en el grupo de contenido con nombre, a menos que las directivas integradas reemplacen esta directiva. 3. Si una directiva de tiempo de respuesta coincidente tiene una acción CACHE pero especifica un grupo de contenido diferente del de la directiva de tiempo de solicitud, se aplica una acción NOCACHE. 4. Si una directiva de tiempo de respuesta coincidente tiene una acción NOCACHE, realice una acción NOCACHE. 5. Si no hay ninguna directiva de tiempo de respuesta coincidente, se aplica una acción CACHE, a menos que una directiva integrada reemplice esta directiva.

Action	Especificación
MAY_NOCACHE	Para una directiva de tiempo de solicitud, esta configuración impide provisionalmente el almacenamiento en caché de la respuesta. En el momento de respuesta, se realiza una de las siguientes accione: Si ninguna directiva de tiempo de respuesta coincide con la solicitud, la acción final es NOCACHE. - Si una directiva de tiempo de respuesta coincidente contiene una acción CACHE, la acción final es CACHE, a menos que las directivas integradas anulen esta directiva. - Si una directiva de tiempo de respuesta coincidente contiene una acción NOCACHE, la acción final es NOCACHE. -Si una directiva de tiempo de respuesta coincidente tiene una acción CACHE pero no especifica un grupo de contenido, la acción final es CACHE la respuesta en el grupo de contenido predeterminado, a menos que las directivas integradas anulen esta directiva.
INVAL	Caduca las respuestas almacenadas en caché. Dependiendo de cómo se configuran la directiva y el grupo de contenido, todas las respuestas de uno o varios grupos de contenido caduquen o los objetos seleccionados en el grupo de contenido caduquen. Nota: Solo puede especificar acciones de INVAL en directivas de tiempo de solicitud.

Puntos de enlace para una directiva

Puede enlazar la directiva a uno de los siguientes puntos de enlace:

- **Un banco de directivas global**. Estos son los bancos de directivas de anulación de tiempo de solicitud, anulación de tiempo de solicitud, incumplimiento de tiempo de respuesta y anulación de tiempo de respuesta, como se describe en "Orden de evaluación de directivas. "
- **Un servidor virtual**. Las directivas que vincula a un servidor virtual se procesan después de

las directivas de anulación global y antes de las directivas predeterminadas globales, como se describe en "Orden de evaluación de directivas. " Al vincular una directiva a un servidor virtual, la vincula al procesamiento en tiempo de solicitud o en tiempo de respuesta.

- **Una etiqueta de directiva ad hoc**. Una etiqueta de directiva es un nombre asignado a un banco de directivas. Además de las etiquetas globales, la caché integrada tiene dos etiquetas de directiva personalizadas integradas:
  - _ReqBuiltInDefaults. Esta etiqueta de directiva, de forma predeterminada, se invoca desde el banco de directivas predeterminado de tiempo de solicitud.
  - _ResBuiltInDefaults. Esta etiqueta de directiva, de forma predeterminada, se invoca desde el banco de directivas predeterminado de tiempo de respuesta.

También puede definir nuevas etiquetas de directiva. Las directivas enlazadas a una etiqueta de directiva definida por el usuario deben invocarse desde un banco de directivas para uno de los puntos de enlace integrados.

> **Importante:**
> Debe vincular una directiva con una acción INVAL a una anulación en tiempo de solicitud o a un punto de enlace de anulación en tiempo de respuesta. Para eliminar una directiva, primero debe desvincularla.

Orden de evaluación de directivas

Para que una directiva avanzada surta efecto, debe asegurarse de que la directiva se invoca en algún momento durante el procesamiento del tráfico del dispositivo NetScaler. Para especificar el tiempo de invocación, asocie la directiva a un punto de enlace. Los siguientes son los puntos de enlace, enumerados en orden de evaluación:

- **Anulación de tiempo de solicitud**. Si una solicitud coincide con una directiva de anulación de tiempo de solicitud, de forma predeterminada finaliza la evaluación de la directiva de solicitud y tiempo y el dispositivo NetScaler almacena la acción asociada a la directiva de coincidencia.
- **Servidor virtual de equilibrio de carga en tiempo de solicitud**. Si la evaluación de directivas no se puede completar después de evaluar todas las directivas de reemplazo de tiempo de solicitud, el dispositivo NetScaler procesa las directivas de tiempo de solicitud enlazadas a servidores virtuales de equilibrio de carga. Si la solicitud coincide con una de estas directivas, la evaluación finaliza y el dispositivo NetScaler almacena la acción asociada a la directiva coincidente.
- **Servidor virtual de conmutación de contenido en tiempo de solicitud**. Las directivas que están enlazadas a este punto de enlace se evalúan después de las directivas de tiempo de solicitud que están enlazadas a servidores virtuales de equilibrio de carga.
- **Tiempo de solicitud predeterminado**. Si la evaluación de directivas no se puede completar después de todo el tiempo de solicitud, se evalúan las directivas específicas del servidor virtual,

el dispositivo NetScaler procesa las directivas predeterminadas de hora de solicitud. Si la solicitud coincide con una directiva predeterminada de petición-hora, de forma predeterminada finaliza la evaluación de la directiva de solicitud y tiempo y el dispositivo NetScaler almacena la acción asociada a la directiva coincidente.

- **Anulación en tiempo de respuesta**. Similar a la evaluación de directivas de anulación en el tiempo de solicitud.
- **Servidor virtual de equilibrio de carga en tiempo de respuesta**. Similar a la evaluación de directivas de servidor virtual en tiempo de solicitud.
- **Cambio de contenido en tiempo de respuesta al servidor virtual**. Similar a la evaluación de directivas de servidor virtual en tiempo de solicitud.
- **Tiempo de respuesta predeterminado**. Similar a la evaluación de directivas predeterminada en el tiempo de solicitud.

Puede asociar varias directivas a cada punto de enlace. Para controlar el orden de evaluación de las directivas asociadas con el punto de enlace, se configura un nivel de prioridad. En ausencia de cualquier otra información de control de flujo, las directivas se evalúan de acuerdo con el nivel de prioridad, comenzando con el valor de prioridad numérico más bajo.

> **Nota:**
> Las directivas de tiempo de solicitud para los datos POST o los encabezados de cookie deben invocarse durante la evaluación de anulación de tiempo de solicitud, ya que las directivas de tiempo de solicitud integradas en la caché integrada devuelven una `NOCACHE` acción para las solicitudes POST y una `MAY_NOCACHE` acción para las solicitudes con cookies. Asociaría `MAY_CACHE` o `MAY_NOCACHE` acciones a una directiva de tiempo de solicitud que apunte a un grupo de contenido parametrizado. La directiva de tiempo de respuesta determina si la transacción se almacena en la caché.

Configurar una directiva para el almacenamiento en caché integrado

Configurar nuevas directivas para controlar los datos que las directivas integradas no pueden procesar. Configurar directivas separadas para el almacenamiento en caché, evitar que se produzca el almacenamiento en caché y para invalidar los datos almacenados en caché. Los siguientes son los principales componentes de una directiva para el almacenamiento en caché integrado:

- Regla: Expresión lógica que evalúa una solicitud o respuesta HTTP.
- Acción: Asocia una directiva a una acción para determinar qué hacer con una solicitud o respuesta que coincida con la regla de directiva.

Grupos de contenido: Asocie la directiva a uno o varios grupos de contenido para identificar dónde se va a realizar la acción.

Para configurar una directiva para el almacenamiento en caché mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
add cache policy <policyName> -rule <expression> -actionCACHE|MAY_CACHE
|NOCACHE|MAY_NOCACHE [-storeInGroup <contentGroupName>] [-undefAction
NOCACHE|RESET]
> add cache policy image_cache -rule ”http.req.url.contains(\”jpg\”)|| http
.req.url.contains(\”jpeg\”)”-action CACHE -storeingroup myImages_group -
undefaction NOCACHE

> add cache policy bugReportPolicy -rule ”http.req.url.query.contains(\”
IssuePage\”)”-action CACHE -storeInGroup bugReportGroup

> add cache policy my_form_policy -rule ”http.req.header(\”Host\”)contains
(\”my.company.com\”)&& http.req.method.eq(\”GET\”)&& http.req.url.query.
contains(\”v=7\”)”-action CACHE -storeInGroup my_form_event

> add cache policy viewproducts_policy -rule ”http.req.url.contains(\”
viewproducts.aspx\”)”-action CACHE -storeInGroup Product_Details
```

Para configurar una directiva para la invalidación mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
add cache policy <policyName> -rule <expression> -action INVAL [-
    invalObjects ”<contentGroupName1>[,<selectorName1>”]. . .]] | [-
    invalGroup <contentGroupName1>[, <contentGroupName2>. . .]] [-
    undefAction NOCACHE|RESET]
<!--NeedCopy-->
```

```
> add cache policy invalidation_events_policy -rule ”http.req.header(”
    Host”)contains(”my.company.com”) && http.req.method.eq(”GET”) &&
    http.req.url.query.contains(”v=8”) -action INVAL -invalObjects
    my_form_event -undefaction NOCACHE
<!--NeedCopy-->
```

```
> add cache policy inval_all -rule ”http.req.method.eq(”POST”) && http.
    req.url.contains(”jpeg”)” -action INVAL -invalGroups myImages_group
    myApps_group PDF_group
<!--NeedCopy-->
```



```
1 > add cache policy bugReportInvalidationPolicy -rule "http.req.url.
    query.contains("TransitionForm")" -action INVAL -invalObjects
    bugReport`
2 `> add cache policy editproducts_policy  - rule "http.req.url.contains("
    editproducts.aspx")"  - action INVAL -invalObjects "Product_Details,
    batchnum_sel" "Products_In_Depots,batchid_sel"
3 <!--NeedCopy-->
```

Para configurar una directiva para el almacenamiento en caché o la invalidación mediante la interfaz gráfica de usuario

Vaya a **Optimización** > **Almacenamiento en caché integrado** > **Directivas** y cree la nueva directiva.

Enlazar globalmente una directiva de almacenamiento en caché integrada

Cuando vincula globalmente una directiva, está disponible para todos los servidores virtuales del dispositivo NetScaler.

Para vincular una directiva de almacenamiento en caché integrada de forma global mediante la interfaz de línea de comandos:

En el símbolo del sistema, escriba:

```
1 bind cache global <policy> -priority <positiveInteger> [-
    typeREQ_OVERRIDE|REQ_DEFAULT|RES_OVERRIDE|RES_DEFAULT] [-
    gotoPriorityExpression <expression>] [-invoke <labelType> <labelName
    >]
2 <!--NeedCopy-->
```

```
1 > bind cache global myCachePolicy -priority 100 -type req_default
2 <!--NeedCopy-->
```

> **Nota:**
>
> El argumento type es opcional para las directivas enlazadas globalmente, a fin de mantener la compatibilidad con las directivas definidas mediante versiones anteriores del dispositivo NetScaler. Si omite el tipo, la directiva está enlazada a REQ_DEFAULT o RES_DEFAULT, en función de si la regla de directiva es una expresión de tiempo de respuesta o de tiempo de solicitud. Si la regla contiene parámetros de tiempo de solicitud y tiempo de respuesta, está enlazada a RES_DEFAULT. Lo que sigue es un ejemplo de un enlace que omite el tipo

Lo que sigue es un ejemplo de un enlace que omite el tipo.

```
> bind cache global myCache Policy 200
```

Para enlazar globalmente una directiva de almacenamiento en caché integrada mediante la utilidad de configuración

Vaya a **Optimización** > Almacenamiento en **caché integrado**, haga clic en **Administrador de directivas de caché** y vincule las directivas especificando el punto de enlace y el tipo de conexión pertinentes (Solicitud/Respuesta).

Enlazar una directiva de almacenamiento en caché integrada a un servidor virtual

Cuando vincula una directiva a un servidor virtual, solo está disponible para las solicitudes y respuestas que coinciden con la directiva y que fluyen a través del servidor virtual pertinente.

Al utilizar la GUI, puede vincular la directiva mediante el cuadro de diálogo de configuración del servidor virtual. Esto le permite ver todas las directivas de todos los módulos Citrix ADC que están enlazados a este servidor virtual. También puede utilizar el cuadro de diálogo de **configuración de Policy Manager** para la caché integrada. Esto le permite ver solo las directivas de almacenamiento en caché integradas enlazadas al servidor virtual.

Para vincular una directiva de almacenamiento en caché integrada a un servidor virtual mediante la interfaz de línea de comandos:

En el símbolo del sistema, escriba:

```
1 bind lb vserver <name>@ -policyName <policyName> -priority <
     positiveInteger> -type(REQUEST|RESPONSE)
2 <!--NeedCopy-->
```

```
1 bind cs vserver <name>@ -policyName <policyName> -priority <
     positiveInteger> -type(REQUEST|RESPONSE)
2 <!--NeedCopy-->
```

Para enlazar una directiva de almacenamiento en caché integrada a un servidor virtual mediante la utilidad de configuración (método de servidor virtual)

- CS Virtual Server - Navegue **aAdministración de tráfico > Content Switching > Servidores virtuales**, seleccione el servidor virtual y vincule las directivas de caché relevantes.
- LB Virtual Server: vaya a **Administración de tráfico > Equilibrio de carga > Servidores virtuales**, seleccione el servidor virtual y vincule las directivas de caché pertinentes.

Para vincular una directiva de almacenamiento en caché integrada a un servidor virtual mediante la GUI (método Policy Manager).

Vaya a **Optimización** > Almacenamiento en **caché integrado**, haga clic en **Administrador de directivas de caché** y vincule las directivas de caché especificando el punto de enlace y el tipo de conexión pertinentes.

> **Nota:**
> Puede vincular directivas de caché tanto al servidor virtual de equilibrio de carga como al servidor virtual de conmutación de contenido seleccionando el punto de enlace adecuado.

Cómo almacenar en caché versiones comprimidas y descomprimidas de un archivo

De forma predeterminada, un cliente que puede gestionar la compresión puede recibir respuestas sin comprimir o respuestas comprimidas en formato gzip, deflate, compress y pack200-gzip. Si el cliente controla la compresión, se envía un encabezado de `Accept-Encoding:compression` formato en la solicitud. El tipo de compresión aceptado por el cliente debe coincidir con el tipo de compresión del objeto almacenado en caché. Por ejemplo, un `cached.gzip` archivo no se puede servir en respuesta a una solicitud con un `Accept-Encoding:deflate` encabezado.

Un cliente que no puede gestionar la compresión recibe un fallo de caché si la respuesta almacenada en caché está comprimida.

Para el almacenamiento en caché dinámico, debe configurar dos grupos de contenido, uno para datos comprimidos y otro para versiones sin comprimir de los mismos datos. A continuación se muestra un ejemplo de configuración de los selectores, grupos de contenido y directivas para servir archivos sin comprimir desde la caché a clientes que no pueden manejar la compresión y enviar versiones comprimidas de los mismos archivos al cliente que pueden manejar la compresión.

```
add cache selector uncompressed_response_selector http.req.url "http.req.
header(\"Host\")"

add cache contentGroup uncompressed_group -hitSelector uncompressed_responst_selector
 -invalSelector uncomp_resp_sel

add cache policy cache_uncompressed -rule "HTTP.REQ.URL.CONTAINS(\"xyz\")&&
 !HTTP.REQ.HEADER(\"Accept-Encoding\").EXISTS"-action CACHE -storeInGroup
uncompressed_group

bind cache global cache_uncompressed -priority 100 -gotoPriorityExpression
END -type REQ_OVERRIDE

add cache selector compressed_response_selector HTTP.REQ.URL "HTTP.REQ.
HEADER(\"Host\")""HTTP.REQ.HEADER(\"Accept-Encoding\")"
```



```
add cache contentGroup compressed_group -hitSelector compressed_response_selector


add cache policy cache_compressed -rule ”HTTP.REQ.URL.CONTAINS(\”xyz\”)&&
 HTTP.REQ.HEADER(\”Accept-Encoding\”).EXISTS”-action CACHE -storeInGroup
compressed_group

bind cache global cache_compressed -priority 200 -gotoPriorityExpression
END -type REQ_OVERRIDE
```

Configurar un banco de directivas para el almacenamiento en caché

Todas las directivas asociadas a un punto de enlace determinado se conocen colectivamente como banco de directivas. Además de configurar los niveles de prioridad para las directivas de un banco, puede modificar el orden de evaluación en un banco configurando las expresiones Goto. Puede modificar aún más el orden de evaluación invocando un banco de directivas externo desde el banco de directivas actual. También puede configurar bancos de directivas nuevos, a los que asigna sus propias etiquetas. Dado que estos bancos de pólizas no están vinculados a ningún punto del ciclo de procesamiento, solo pueden invocarse desde otros bancos de pólizas. Para mayor comodidad, los bancos de directivas cuyas etiquetas no corresponden a un punto de enlace integrado se denominan etiquetas de directiva.

Además de controlar el orden de evaluación de directivas vinculando la directiva y asignando un nivel de prioridad, como se describe en “Directivas vinculantes”, puede establecer el flujo dentro de un banco de directivas configurando una expresión Goto. Una expresión Goto anula el flujo determinado por los niveles de prioridad. También puede controlar el flujo de evaluación invocando un banco de directivas externo después de evaluar una entrada en el banco actual. La evaluación siempre regresa al banco actual una vez completada la evaluación.

En la siguiente tabla se resumen las entradas para controlar la evaluación en un banco de directivas.

Atributo	Especifica
Nombre	El nombre de una directiva o, para invocar a otro banco de directivas sin evaluar la directiva, la palabra clave NOPOTIVE. Puede especificar NOPOLICY más de una vez en un banco de directivas, pero solo puede especificar una directiva con nombre una vez.
Prioridad	Un número entero. Cuanto menor sea el número entero, mayor será la prioridad.

Atributo	Especifica
Expresión de GoTo	Determina la siguiente directiva o banco de directivas que se va a evaluar. Puede proporcionar uno de los siguientes valores: 1. SIGUIENTE: Vaya a la directiva con la siguiente prioridad más alta. 2. FIN: Detener la evaluación. 3. USE_INVLATION_RESULT: Aplicable si esta entrada invoca otro banco de directivas. Si el GoTo final en el banco invocado tiene un valor de END, la evaluación se detiene. Si el Goto final es algo distinto de END, el banco de pólizas actual realiza un NEXT. 4. Número positivo: Número de prioridad de la próxima directiva a evaluar. 5. Expresión numérica: Expresión que produce el número de prioridad de la siguiente directiva que se va a evaluar. El GoTo solo puede avanzar en un banco de directivas. Omitir la expresión Goto es lo mismo que especificar END.
Tipo de invocación	Designa un tipo de banco de directivas. El valor puede ser uno de los siguientes: 1. Solicitar servidor virtual: invoca directivas de tiempo de solicitud asociadas a un servidor virtual. 2. Servidor virtual de respuesta: Invoca directivas de tiempo de respuesta asociadas a un servidor virtual. 3. Etiqueta de directiva: Invoca a otro banco de directivas, identificado por la etiqueta de directiva del banco.
Nombre de invocación	Nombre de un servidor virtual o una etiqueta de directiva, según el valor especificado para el tipo de invocación.

La caché integrada tiene dos etiquetas de directiva integradas y puede configurar más etiquetas de directiva:

`_reqBuiltInDefaults`: Esta etiqueta de directiva se invoca desde el punto de enlace predeterminado de hora de solicitud.
`_resBuiltInDefaults`: Esta etiqueta de directiva se invoca desde el punto de enlace predetermi-

nado en tiempo de respuesta.

Para invocar una etiqueta de directiva en un banco de directivas de almacenamiento en caché mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
bind cache policylabel <labelName> -policname<policyName> -priority<
    priority> [-gotoPriorityExpression <gotoprioritыExpression>] [-
    invoke <labelType> <labelName>]
<!--NeedCopy-->
```

Para invocar una etiqueta de directiva en un banco de directivas de almacenamiento en caché mediante la GUI:

1. Vaya a **Optimización** > Almacenamiento en **caché integrado, haga clic en Administrador de directivas** de caché y especifique el punto de enlace pertinente (Anular Global o Global predeterminado) y el tipo de conexión para ver la lista de directivas enlazadas a este punto de enlace.
2. Si quiere invocar una etiqueta de directiva sin evaluar una directiva, haga clic en **NOPOLICY**.

> **Nota:**
>
> Para invocar un banco de directivas externo, haga clic en el campo de la columna Tipo de invocación y seleccione el tipo de banco de directivas que quiere invocar en este punto del banco de directivas. Esto puede ser una etiqueta global o un banco de servidores virtuales. En el campo Invocar nombre, escriba la etiqueta o el nombre del servidor virtual.

Para invocar una etiqueta de directiva de almacenamiento en caché en un banco de directivas de servidor virtual mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
bind lb vserver <name>@ -policyName <policyName>|<NOPOLICY-CACHE> -
    priority<positiveInteger> -gotoPriorityExpression <expression> -type
     REQUEST|RESPONSE -invoke<labelType> <labelName>
<!--NeedCopy-->
```

```
bind cs vserver <name> -policyName <policyName>|<NOPOLICY-CACHE> -
    priority<positiveInteger> -gotoPriorityExpression <expression> -type
     REQUEST|RESPONSE -invoke<labelType> <labelName>
<!--NeedCopy-->
```


Para invocar una etiqueta de directiva de almacenamiento en caché en un banco de directivas de servidor virtual mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico** > **Equilibrio de carga/Cambio de contenido** > **Servidores virtuales**, seleccione el servidor virtual y haga clic en **Directivas**.
2. Si está configurando una entrada existente en este banco, omita este paso. Si va a agregar una nueva directiva a este banco de directivas o quiere utilizar la entrada NOPOLICY "ficticia", haga clic en **Agregar** y realice una de las acciones siguientes:
   - Para configurar una nueva directiva, haga clic en Caché y configure la nueva directiva como se describe en Configuración de una directiva en la caché integrada.
   - Para invocar un banco de directivas sin procesar una directiva como regla, seleccione la `NOPOLICY-CACHE` opción.

> **Nota:**
>
> Para invocar un banco de directivas externo, haga clic en el campo de la columna Tipo de invocación y seleccione el tipo de banco de directivas que quiere invocar en este punto del banco de directivas. Esto puede ser una etiqueta global o un banco de servidores virtuales. En el campo Invocar nombre, escriba la etiqueta o el nombre del servidor virtual.

Configurar una etiqueta de directiva en una caché integrada

Además de configurar directivas en un banco de directivas para uno de los puntos de enlace integrados o un servidor virtual, puede crear etiquetas de directiva de almacenamiento en caché y configurar bancos de directivas para estas nuevas etiquetas.

Solo se puede invocar una etiqueta de directiva para la caché integrada desde uno de los puntos de enlace que puede ver en el Administrador de directivas en el panel de detalles **Almacenamiento en caché integrado** (anulación de solicitud, solicitud predeterminada, anulación de respuesta o respuesta predeterminada) o las etiquetas de directivas integradas `\\_reqBuiltinDefaults` y `\\_resBuiltinDefaults`. Puede invocar una etiqueta de directiva varias veces a diferencia de una directiva, que solo se puede invocar una vez.

La GUI de Citrix ADC proporciona una opción para cambiar el nombre de una etiqueta de directiva. Cambiar el nombre de una etiqueta de directiva no afecta al proceso de evaluación de las directivas enlazadas a la etiqueta.

> **Nota**:
>
> Puede utilizar la directiva `NOPOLICY` "ficticia" para invocar cualquier etiqueta de directiva de otro banco de directivas. La `NOPOLICY` entrada es un marcador de posición que no procesa ninguna regla.

Para configurar una etiqueta de directiva para el almacenamiento en caché mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba el siguiente comando para crear una etiqueta de directiva y verificar la configuración:

- `add cache policylabel <labelName> -evaluates (REQ|RES)`
- `show cache policylabel <labelName>`

Invocar esta etiqueta de directiva desde un banco de directivas.

Para configurar una etiqueta de directiva para el almacenamiento en caché mediante la GUI:

Vaya a **Optimización** > Almacenamiento en **caché integrado** > **Etiquetas de directiva**, agregue una etiqueta de directiva y vincule las directivas almacenadas en caché.

> **Nota:**
> Para asegurarse de que Citrix ADC procesa la etiqueta de directiva en el momento adecuado, configure una invocación de esta etiqueta en uno de los bancos de directivas asociados a los puntos de enlace integrados.

Para cambiar el nombre de una etiqueta de directiva mediante la GUI:

Vaya a **Optimización** > Almacenamiento en **caché integrado** > **Etiquetas de directiva**, seleccione la etiqueta de directiva y cambie el nombre.

Desenlazar y eliminar una directiva de almacenamiento en caché integrada y una etiqueta de directiva

Puede desvincular una directiva de un banco de directivas y eliminarla. Para eliminar la directiva, primero debe desvincularla. También puede quitar una invocación de etiqueta de directiva y eliminar una etiqueta de directiva. Para eliminar la etiqueta de directiva, primero debe quitar las invocaciones que haya configurado para la etiqueta.

No puede desenlazar ni eliminar las etiquetas de los puntos de enlace integrados (solicitud predeterminada, anulación de solicitud, respuesta predeterminada y anulación de respuesta).

Para desvincular una directiva de almacenamiento en caché global mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
unbind cache global <policy>
```

Para desvincular una directiva de almacenamiento en caché específica del servidor virtual mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
(unbind lb vserver|unbind cs vserver)<vserverName> -policyName <policyName>
 -type(REQUEST|RESPONSE)
```


Para eliminar una directiva de almacenamiento en caché mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
rm cache policy <policyName>
```

Para desvincular una directiva de almacenamiento en caché mediante la GUI:

Vaya a **Optimización** > Almacenamiento en **caché integrado**, haga clic en **Administrador de directivas de caché** y desvincule directivas especificando el punto de enlace y el tipo de conexión pertinentes (Solicitud/Respuesta).

Para eliminar una invocación de etiquetas de directiva mediante la GUI:

1. Vaya a **Optimización** > Almacenamiento en **caché integrado, haga clic en Administrador de directivas**de caché y especifique el punto de enlace correspondiente (servidor virtual de equilibrio de carga o servidor virtual de conmutación de contenido) y el tipo de conexión para ver la lista de directivas de caché vinculadas a este servidor virtual.
2. En la columna Invoke de directiva, desactive la entrada.

Compatibilidad con caché para protocolos de base de datos

August 20, 2021

La función de caché integrada supervisa y almacena en caché solicitud de base de datos según lo determinado por las directivas de caché. Los usuarios deben configurar las directivas de caché para los protocolos MYSQL y MSSQL, ya que el dispositivo Citrix ADC no proporciona directivas predeterminadas. Al configurar los protocolos predeterminados, recuerde que las directivas basadas en solicitudes solo admiten acciones CACHE e INVAL, mientras que las directivas basadas en respuesta solo admiten la acción “NOCACHE”. Después de configurar las directivas, debe enlazarlas a servidores virtuales. Las directivas MYSQL y MSSQL, tanto de solicitud como de respuesta, están vinculadas solo a servidores virtuales.

Antes de crear una directiva de caché, debe crear un grupo de contenido de caché de tipo MYSQL o MSSQL. Cuando cree un grupo de contenido de caché, asocie al menos un selector de selección con él. Consulte Configuración de un grupo de contenido básico para configurar un grupo de contenido de caché.

En el siguiente ejemplo se explica cómo configurar y verificar el soporte de caché para protocolos SQL.

```
1 > enable feature IC
2 > set cache parameter -memlimit 100
3 > add cache selector sel1 mssql.req.query.text
```



```
4
5  > add cache contentgroup cg1  -type ”MSSQL” -hitselector ”sel1” -
       invalselector ”inval_sel” -relExpiry ”500” -maxResSize
6   ”100”
7  > add cache policy cp1  -rule ”mssql.req.query.command.contains(”select
       ”)” -action ”CACHE” -storeInGroup ”cg1”
8  > add cache policy cp2  -invalObjects ”cg1” -rule ”mssql.req.query.text
       .contains(”insert”)” -action ”INVAL”
9  > add db user user1  -password ”Pass1”
10 > add service svc_sql_1 10.102.147.70 mssql 64834 -healthMonitor ”NO” -
       downstateflush ”ENABLED”
11 > add lb vserver lb_mssql1 mssql 10.102.147.77 1433  -lbmethod ”
       roundrobin”
12 > bind lb vserver lb_mssql1 svc_sql_1
13 > bind lb vserver lb_mssql1 -policyName cp1  -type ”REQUEST” -priority
       ”2”
14 > bind lb vserver lb_mssql1 -policyName cp2  -type ”REQUEST” -priority
       ”1”
15
16 > show cache selector sel1
17       Name:sel1
18                      Expressions:
19                      1)mssql.req.query.text
20 > show cache policy cp1
21                      Name:cp1
22       Rule:mssql.req.query.command.contains(”select”)
23                      CacheAction:CACHE
24                      Stored in group: cg1
25                      UndefAction:Use Global
26                  Hits:2
27                      Undef Hits:0
28                      Policy is bound to following entities
29                      1) Bound to:
30                                  REQ VSERVER lb_mssql1
31                                  Priority:2
32                                  GotoPriorityExpression: END
33 <!--NeedCopy-->
```

Nota:

Los métodos para reducir las multitudes de flash, como se explica en Reducción de multitudes flash, no son compatibles con los protocolos MYSQL y MSSQL.

Configurar expresiones para directivas y selectores de almacenamiento en caché

October 5, 2021

Una expresión de tiempo de solicitud examina los datos de la transacción de tiempo de solicitud y una expresión de tiempo de respuesta examina los datos de una transacción en tiempo de respuesta. En una directiva de almacenamiento en caché, si una expresión coincide con los datos de una solicitud o respuesta, el dispositivo Citrix ADC realiza la acción asociada a la directiva. En un selector, las expresiones de tiempo de solicitud se utilizan para buscar respuestas coincidentes almacenadas en un grupo de contenido.

Antes de configurar directivas y selectores para la caché integrada, debe conocer, como mínimo, los nombres de host, las rutas de acceso y las direcciones IP que aparecen en las URL de solicitud y respuesta HTTP. Y probablemente necesites conocer el formato de las solicitudes y respuestas HTTP completas. Programas como Live HTTP Headers `http://livehttpheaders.mozdev.org/)or HTTPFox https://addons.mozilla.org/en-US/firefox/addon/6647` pueden ayudarle a investigar la estructura de los datos HTTP con los que trabaja su organización.

A continuación se muestra un ejemplo de solicitud HTTP GET para un programa de cotización de acciones:

```
GET /quote.dll?page=dynamic&mode=data&mode=stock&symbol=CTXS&page=multi
    &selected=CTXS&random=0.00792039478975548 HTTP/1.1

Host: quotes.mystockquotes.com

User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9)
    Gecko/2008052906 Firefox/3.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q
    =0.8

Accept-Language: en-us,en;q=0.5

Accept-Encoding: gzip,deflate,compress,pack200-gzip

Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7

Keep-Alive: 300

Connection: keep-alive
```



```
18
19 Referer: http://quotes.mystockquotes.com/quote.dll?mode=stock&symbol=
      CTXS&page=multi&selected=CTXS
20
21 Cookie: __qca=1210021679-72161677-10297606
22 <!--NeedCopy-->
```

Al configurar una expresión, tenga en cuenta las siguientes limitaciones:

Tipo de expresión	Restricciones
Solicitar	No configure expresiones de tiempo de solicitud en una directiva con una acción CACHE o NOCACHE. Utilice MAY_CACHE o MAY_NOCACHE en su lugar.
Respuesta	Configure expresiones de tiempo de respuesta solo en las directivas de almacenamiento en caché. Los selectores solo pueden usar expresiones de tiempo de solicitud. No configurar expresiones de tiempo de respuesta en una directiva con una acción INVAL. Nota: No configure expresiones de tiempo de respuesta en una directiva con una acción CACHE y un grupo de contenido parametrizado. Utilice la acción MAY_CACHE.

> **Nota:**
> Para obtener un análisis exhaustivo de las expresiones avanzadas, consulte Directivas y expresiones.

Sintaxis de expresión

Los siguientes son los componentes básicos de la sintaxis:

- Separe las palabras clave con puntos (.), de la siguiente manera:

```
http.req.url
```

- Coloque los valores de cadena entre paréntesis y comillas, de la siguiente manera:

```
http.req.url.query.contains("this")
```


- Al configurar una expresión desde la línea de comandos, debe escapar las comillas internas (las comillas que delimitan los valores de la expresión, en lugar de las comillas que delimitan la expresión). Un método consiste en utilizar una barra diagonal, como se indica a continuación:

```
\”abc\”
```

Las expresiones de los selectores se evalúan por orden de apariencia y varias expresiones de una definición de selector se unen mediante un AND lógico. A diferencia de las expresiones de selección, puede especificar operadores booleanos y modificar la prioridad en una expresión avanzada de una regla de directiva.

Configurar una expresión en una directiva de almacenamiento en caché o en un selector

> **Nota:**
> La sintaxis de una expresión de directiva es distinta a la de una expresión selectora. Para obtener un análisis exhaustivo de las expresiones avanzadas, consulte “Directivas y expresiones. “

Para configurar una expresión de directiva mediante la interfaz de línea de comandos

1. Inicie la definición de la directiva tal y como se describe en “Vinculación global de una directiva de almacenamiento en caché integrada”.
2. Para configurar la regla de directivas, delimita toda la regla entre comillas y delimita los valores de cadena dentro de la regla entre comillas de escape.

A continuación, se muestra un ejemplo:

“http.req.url.contains(“jpg”)”

Para agregar valores booleanos, inserte &&,	o! operadores.

1.

Los siguientes son ejemplos:

```
”http.req.url.contains(\”jpg\”)|| http.req.url.contains(\”jpeg\”)”
```

```
”http.req.url.query.contains(\”IssuePage\”)”
```

```
”http.req.header(\”Host\”)contains(\”my.company.com\”)&& http.req.method.eq
(\”GET\”)&& http.req.url.query.contains(\”v=7\”)”
```

1. Para configurar un orden de evaluación para las partes constitutivas de un compuesto

```
”http.req.url.contains(\”jpg\”)|| (http.req.url.contains(\”jpeg\”)&& http.
req.method.eq(\”GET\”))”
```


Para configurar una expresión de selector mediante la interfaz de línea de comandos:

1. Inicie la definición del selector como se describe en “Acerca de los grupos de contenido.”
2. Para configurar la expresión selectora, delimita toda la regla entre comillas y delimita los valores de cadena dentro de la regla entre comillas de escape.

A continuación, se muestra un ejemplo:

```
”http.req.url.contains(\”jpg\”)”
```

No se pueden agregar valores booleanos, insertar &&,	ni! operadores. Introduzca cada elemento de expresión delimitado entre comillas. Las expresiones múltiples de la definición se tratan como una expresión compuesta unida por ANDs lógicos.

1.

Los siguientes son ejemplos:

```
1 ”http.req.url.query.value(”ProductId”)” ”http.req.url.query.value(”
     BatchNum”)” ”http.req.url.query.value(”depotLocation”)”
2 <!--NeedCopy-->
```

Para configurar una directiva o expresión de selector mediante la interfaz gráfica de usuario

1. Inicie la definición de directiva o selector como se describe en “Para configurar una directiva de almacenamiento en caché o invalidación mediante la utilidad de configuración” o “Para configurar un selector mediante la utilidad de configuración. “
2. En el campo **Expresión**, puede escribir manualmente la directiva Avanzada haciendo clic en Cambiar a sintaxis clásica o crear una nueva **expresión con el Editor**de expresiones.

Para insertar un operador entre dos partes de una expresión compuesta, haga clic en el botón Operadores y seleccione el tipo de operador. A continuación se muestra un ejemplo de una expresión configurada con OR booleana (señalada por barras verticales dobles,	):

3.

4. Haga clic en la lista desplegable **Expresiones usadas con** frecuencia para insertar las expresiones más utilizadas.

5. Para probar la expresión, haga clic en **Evaluar**. En el cuadro de diálogo **Evaluador de expresiones**, seleccione el tipo de flujo que coincida con la expresión. En el campo data, pegue la solicitud o respuesta HTTP que quiere analizar con la expresión y haga clic en **Evaluar**.

Mostrar objetos en caché y estadísticas de caché

Puede ver objetos almacenados en caché concretos y ver estadísticas resumidas sobre solicitudes de caché, errores y uso de memoria. Las estadísticas proporcionan información sobre la cantidad de datos que se suministran desde la caché, qué elementos son responsables del mayor beneficio de rendimiento y qué se puede ajustar para mejorar el rendimiento de la caché.

Esta sección incluye los siguientes detalles:

- Visualización de objetos en caché
- Búsqueda de respuestas determinadas en caché
- Visualización de estadísticas de caché

Ver objetos almacenados en caché

Después de habilitar el almacenamiento en caché, podrá ver los detalles de los objetos almacenados en caché. Por ejemplo, puede ver los siguientes elementos:

- Tamaños de respuesta y tamaños de encabezado
- Códigos de estado
- Grupos de contenido
- ETagencabezados, Última modificación y Cache-Control

- URL de solicitud
- Parámetros hit
- Direcciones IP de destino
- Tiempos de solicitud y respuesta

Para ver una lista de objetos almacenados en caché mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
show cache object
```

Propiedades	Descripción
Tamaño de respuesta (bytes)	Tamaño del encabezado y del cuerpo de la respuesta.
Tamaño del encabezado de respuesta (bytes)	Tamaño de la parte del encabezado de la respuesta.
Código de estado de respuesta	El código de estado enviado con la respuesta.
ETag	El encabezado ETag insertado en la respuesta. Normalmente, este encabezado indica si la respuesta ha cambiado recientemente.
Modificado por última vez	El encabezado Last-Modified insertado en la respuesta. Este encabezado indica la fecha en que se modificó por última vez la respuesta.
Control de caché	El encabezado Cache-Control insertado en la respuesta.
Fecha	El encabezado Fecha que indica cuándo se envió la respuesta.
Grupo de contenido	Grupo de contenido en el que se almacena la respuesta.
Partido complejo	Si este objeto se almacenó en caché en función de valores parametrizados, este valor de campo es SÍ.
Host	El host especificado en la URL que solicitó esta respuesta.
Puerto host	El puerto de escucha del host especificado en la URL que solicitó esta respuesta
URL	Dirección URL emitida para la respuesta almacenada.

Propiedades	Descripción
IP de destino	Dirección IP del servidor del que se ha obtenido esta respuesta.
Puerto de destino	Puerto de escucha del servidor de destino.
Parámetros de resultados	Si el grupo de contenido que almacena la respuesta utiliza parámetros de resultados, se muestran en este campo.
Selector de resultados	Si este grupo de contenido utiliza un selector de resultados, aparece en este campo.
Selector de invalidación	Si este grupo de contenido utiliza un selector de invalidación, aparece en este campo.
Expresiones selectoras	Si este grupo de contenido utiliza un selector, este campo muestra la expresión que define la regla de selección.
Tiempo de la solicitud	Tiempo en milisegundos desde que se emitió la solicitud.
Tiempo de respuesta	Tiempo en milisegundos desde que la caché empezó a recibir la respuesta.
Edad	Cantidad de tiempo que el objeto ha estado en la caché.
Caducidad	Tiempo transcurrido el cual el objeto se marca como caducado.
Vaciado	Indica si la respuesta se ha vaciado después del vencimiento.
Prerrecuperación	Si se ha configurado la prerrecuperación para este grupo de contenido, la cantidad de tiempo antes de que caduque el objeto se recupera del origen. La captura previa no se aplica a objetos negativos (por ejemplo, respuestas 404 de “objeto no encontrado”).

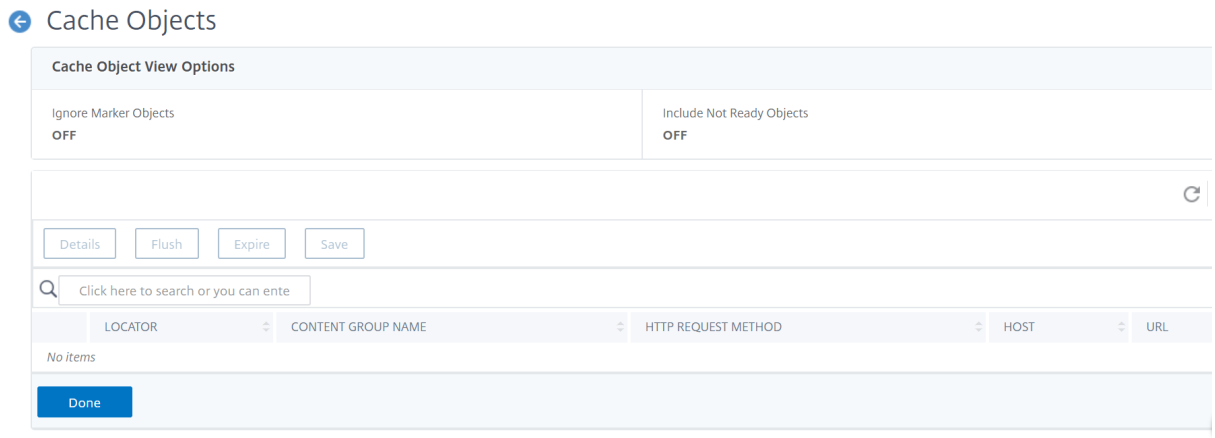
Propiedades	Descripción
Lectores actuales	Aproximadamente el número actual de solicitudes que se están atendiendo. Cuando se descarga una respuesta con un objeto de encabezado Content-Length, los valores actuales que faltan y los valores de los lectores actuales suelen ser 1. Cuando se descarga un objeto de respuesta en trozos, el valor actual de errores suele ser 1, pero el valor de los lectores actuales suele ser 0, porque la respuesta en trozos que se envía al cliente no proviene de los búferes de almacenamiento en caché integrados.
Pérdidas actuales	El número actual de solicitudes que han provocado la pérdida de caché y la obtención del servidor de origen. Este valor suele ser 0 o 1. Si la opción Encuesta cada vez está habilitada para un grupo de contenido, el recuento puede ser superior a 1.
Resultados	Número de resultados de caché de este objeto.
Pérdidas	El número de pérdidas de caché de este objeto.
Formato de compresión	Tipo de compresión aplicada a este objeto. Los formatos de compresión incluyen gzip, deflate, compress y pack200-gzip.
Versión HTTP en respuesta	Versión de HTTP que se utilizó para enviar la respuesta.
Etag débil presente en respuesta	Los encabezados etag fuertes cambian si cambian los bits de una entidad. Los encabezados fuertes se basan en los valores de octeto de un objeto. Los encabezados etag débiles cambian si cambia el significado de una entidad. Los valores etag débiles se basan en la identidad semántica. Los valores de etags débiles comienzan con una “W”.

Propiedades	Descripción
Celda marcadora negativa	Un objeto marcador se puede almacenar en caché, pero aún no cumple todos los criterios para ser almacenado en caché. Por ejemplo, el objeto puede superar el tamaño máximo de respuesta del grupo de contenido. Se crea una celda marcadora para objetos de este tipo. La próxima vez que un usuario envíe una solicitud para este objeto, se entregará un error de caché.
Marcador de motivo creado	El motivo por el que se creó una celda marcadora (por ejemplo, “Esperando minhit”, “Los datos de respuesta de longitud del contenido no están en el límite de tamaño del grupo”).
Encuesta automática cada vez	Si la caché integrada recibe una respuesta 200 OK ya caducada con los validadores (ya sea la cabecera de respuesta de última modificación o la ETag), almacena la respuesta y la marca como PET automático (sondeo automático cada vez).
Citrix ADC Etag insertado en respuesta	Variación del encabezado ETag generado por el dispositivo Citrix ADC. El valor SÍ aparece si Citrix ADC inserta una Etag en la respuesta.
Respuesta completa presente en caché	Indica si se trata de una respuesta completa.
IP de destino verificada por DNS	Indica si se ha realizado la resolución DNS al almacenar el objeto.
Objeto almacenado mediante un proxy de reenvío de caché	Indica si esta respuesta se ha almacenado debido a un proxy de reenvío configurado en la memoria caché integrada.
El objeto es un archivo base Delta	Respuesta comprimida por delta.
Esperando minhits	Indica si este grupo de contenido requiere un número mínimo de servidores de origen para almacenar en caché una respuesta.

Propiedades	Descripción
Recuento de minhit	Si este grupo de contenido requiere un número mínimo de solicitudes del servidor de origen antes de almacenar en caché un objeto, este campo muestra un recuento del número de solicitudes recibidas hasta el momento.
Método de solicitud HTTP	Método, GET o POST, utilizado en la solicitud que obtuvo este objeto.
Almacenado por directiva	Nombre de la directiva de almacenamiento en caché que ha provocado el almacenamiento de este objeto. El valor NO DISPONIBLE indica que la directiva se ha desactivado o eliminado. El valor NONE indica que el objeto no coincide con una directiva visible, sino que se ha almacenado según criterios internos de almacenamiento en caché.
Existen metadatos del firewall de aplicaciones	Este parámetro se utiliza cuando el firewall de aplicaciones y la caché integrada están habilitados. El firewall de aplicaciones analiza el contenido de una página de respuesta, almacena sus metadatos (por ejemplo, las URL y los formularios contenidos en la página) y exporta los metadatos con la respuesta a la caché. La caché almacena la página y los metadatos y, cuando la caché sirve la página, envía los metadatos a la sesión de la solicitud.
Objeto de llamada HTTP, nombre, tipo, respuesta	Estas celdas indican si estos datos se almacenaron como resultado de una expresión de llamada HTTP y proporcionan información sobre varios aspectos de la llamada y la respuesta correspondiente. Para obtener más información sobre las llamadas HTTP, consulte “Llamadas HTTP”.

Para ver objetos almacenados en caché mediante la interfaz gráfica de usuario

Vaya a **Optimización** > Almacenamiento en **caché integrado> Objetos**de caché Puede ver todos los objetos almacenados en caché y ordenarlos según sus necesidades.



Buscar respuestas específicas almacenadas en caché

Puede buscar elementos individuales en la caché según los criterios de búsqueda. Existen diferentes métodos para buscar elementos almacenados en caché, en función de si el grupo de contenido que contiene los datos utiliza selectores de aciertos e invalidación, como se indica a continuación:

- Si el grupo de contenido utiliza selectores, solo puede realizar la búsqueda con el ID de localizador del elemento almacenado en caché.
- Si el grupo de contenido no utiliza selectores, la búsqueda se realiza mediante criterios como URL, host o nombre del grupo de contenido.

Al buscar una respuesta almacenada en caché, puede localizar algunos elementos por URL y host. Si la respuesta se encuentra en un grupo de contenido que utiliza un selector, solo puede encontrarla mediante un número de localizador (por ejemplo, 0x00000000ad7af00000050). Para guardar un número de localizador para utilizarlo más adelante, haga clic con el botón derecho en la entrada y seleccione **Copiar**. Para obtener más información sobre los selectores, consulte "Configuración de selectores y grupos de contenido básico. "

Para mostrar respuestas almacenadas en caché en grupos de contenido que no tienen selector mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
show cache object [-locator <positiveInteger>] | [(-url <URL> (-host <
hostName> [-port <port>] [-groupName <contentGroupName>] [-httpMethod GET
 | POST ]))| [-httpStatus <positive integer>] | -group <contentGroupName> |
 -ignoreMarkerObjects (ON | OFF)| -includeNotReadyObjects (ON | OFF)]
```

Para mostrar respuestas almacenadas en caché en grupos de contenido que tienen un selector mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:


```
show cache object -locator <locatorString> MarkerObjects ( ON | OFF )| -
includeNotReadyObjects ( ON | OFF )| [-httpStatus<positive integer>]
```

Para mostrar respuestas almacenadas en caché en grupos de contenido que no tienen selector mediante la utilidad de configuración

Vaya a **Optimización > Almacenamiento en caché integrado > Objetos de caché**, haga clic en Buscar y establezca los criterios de búsqueda para ver la respuesta almacenada en caché requerida.

Si aún no ha configurado ningún grupo de contenido, todos los objetos se encuentran en el grupo Predeterminado.

Ver estadísticas de caché

En la tabla siguiente se resumen las estadísticas de caché detalladas que se pueden ver.

Contador	Descripción
Accesos	Respuestas que se encuentran y se sirven desde la memoria caché integrada. Incluye objetos estáticos como archivos de imagen, páginas con códigos de estado 200, 203, 300, 301, 302, 304, 307, 403, 404, 410 y respuestas que coinciden con una directiva definida por el usuario con una acción CACHE.
echa de menos	Solicitudes HTTP interceptadas en las que la respuesta se recuperó en última instancia del servidor de origen.
Solicitudes	Número total de solicitudes de caché más errores totales de caché.
No 304 hits	Si el usuario solicita un elemento más de una vez y el elemento de la caché no cambia desde la última vez que el dispositivo Citrix ADC lo sirvió, el dispositivo Citrix ADC ofrece una respuesta 304 en lugar del objeto almacenado en caché.
Esta estadística indica cuántos elementos ha servido el dispositivo Citrix ADC desde la memoria caché, con exclusión de 304 respuestas.	

Contador	Descripción
304 aciertos	Número de 304 respuestas (objeto no modificado) que el dispositivo Citrix ADC ha servido desde la memoria caché.
Proporción de aciertos 304 (%)	Porcentaje de 304 respuestas que ha servido el dispositivo Citrix ADC en relación con otras respuestas.
Proporción de aciertos (%)	Porcentaje de respuestas que el dispositivo Citrix ADC ha servido desde la memoria caché (solicitudes de caché) en relación con las respuestas que no se han podido entregar desde la caché.
Ancho de banda de origen ahorrado (%)	Estimación de la capacidad de procesamiento que el dispositivo Citrix ADC guardó en el servidor de origen debido a la entrega de respuestas de la caché.
Bytes servidos por Citrix ADC	Número total de bytes que el dispositivo Citrix ADC ha servido desde el servidor de origen y la caché.
Bytes servidos por la cache	Número total de bytes que el dispositivo Citrix ADC ha servido desde la caché.
Proporción de aciertos de bytes (%)	Porcentaje de datos que el dispositivo Citrix ADC proporcionó desde la caché, en relación con todos los datos de todas las respuestas servidas.
Bytes comprimidos de la cache	Cantidad de datos, en bytes, que el dispositivo Citrix ADC ha servido en forma comprimida.
Falla almacenable	Si el dispositivo Citrix ADC no encuentra un objeto solicitado en la caché, lo recupera del servidor de origen. Esto se conoce como un fallo de caché. Un error de caché almacenable se puede almacenar en la memoria caché.
Incisiones no almacenables	Un error de caché no almacenable no se puede almacenar en la caché.
Misses	Se pierde toda la caché.

Contador	Descripción
Revalidaciones	La configuración Max-Age de un encabezado de Cache-Control determina, en segundos, cuándo una caché intermedia debe revalidar el contenido con la caché integrada antes de servirlo al usuario.
Para obtener más información, consulta “Insertar un encabezado de control de caché. “	
Revalidaciones satisfactorias	Número de revalidaciones que se han realizado.
Para obtener más información, consulta “Insertar un encabezado de control de caché. “	
Conversiones a requerimiento condicional	Una solicitud de agente de usuario para un objeto PET almacenado en caché siempre se convierte en una solicitud condicional y se envía al servidor de origen.
Para obtener más información, consulta “Sondeo del servidor de origen cada vez que se recibe una solicitud. “	
Proporción de errores almacenables (%)	La caché almacenable falla como porcentaje de errores de caché no almacenables.
Ratio de revalidación satisfactoria (%)	Revalidaciones satisfactorias como porcentaje de todos los intentos de revalidación.
Para obtener más información, consulta “Insertar un encabezado de control de caché. “	
Caduca al último byte	Número de veces que la caché ha caducado el contenido inmediatamente después de recibir el último byte de cuerpo. Solo se aplica a las respuestas positivas, como se describe en la tabla “Resultados y pérdidas de caché”.
Para obtener más información, consulta “Ejemplo de optimización del rendimiento. “	

Contador	Descripción
Flashcache Misses	Si habilita Flash Cache, la caché solo permite que una solicitud llegue al servidor, eliminando las multitudes de flash. Esta estadística indica el número de solicitudes de Flash Cache que se han perdido en la memoria caché.
Para obtener más información, “Solicitudes de cola en la caché. “	
Visitas de Flashcache	Número de solicitudes de Flash Cache que fueron aciertos de caché.
Para obtener más información, consulta “Poner en cola las solicitudes en la caché”. “	
Solicitudes invales parametrizadas	Solicitudes que coinciden con una directiva con una acción de invalidación (INVAL) y un grupo de contenido que utiliza un selector de invalidación o parámetros para caducar selectivamente los objetos almacenados en caché del grupo.
Solicitudes invales completas	Solicitudes que coinciden con una directiva de invalidación en la que el parámetro InvalGroups está configurado y caduca uno o varios grupos de contenido.
Solicitudes inval	Solicitudes que coinciden con una directiva de invalidación y dan como resultado la caducidad de respuestas almacenadas en caché específicas o grupos de contenido completos.
Solicitudes parametrizadas	Número de solicitudes de caché procesadas mediante una directiva con un grupo de contenido parametrizado.
Hits no 304 parametrizados	Número de solicitudes de caché que se procesaron mediante una directiva con un grupo de contenido parametrizado, donde se encontró una respuesta almacenada en caché completa y la respuesta no fue una respuesta 304 (objeto no actualizado).

Contador	Descripción
304 visitas parametrizadas	Número de solicitudes de caché procesadas mediante una directiva con un grupo de contenido parametrizado, donde se encontró el objeto almacenado en caché y el objeto fue una respuesta 304 (objeto no actualizado).
Número total de visitas parametrizadas	Número de solicitudes de caché procesadas mediante una directiva con un grupo de contenido parametrizado, donde se encontró el objeto almacenado en caché.
Proporción de aciertos 304 parametrizada (%)	Porcentaje de 304 respuestas (objeto no actualizado) que se encontraron mediante una directiva parametrizada, en relación con todas las visitas de caché.
Encuesta cada vez que solicitudes	Si está habilitada la opción Poll Every Time, el dispositivo Citrix ADC siempre consulta el servidor de origen antes de servir un objeto almacenado.
Para obtener más información, consulta “Sondeo del servidor de origen cada vez que se recibe una solicitud. “	
Sondear con cada resultado	Número de veces que se ha encontrado una visita de caché mediante el método Poll Every Time.
Para obtener más información, consulta “Sondeo del servidor de origen cada vez que se recibe una solicitud. “	
Relación de cada visita de sondeo (%)	Porcentaje de aciertos de caché utilizando el método Poll Every Time, en relación con todas las búsquedas de objetos almacenados en caché mediante Poll Every Time. Para obtener más información, consulta “Sondeo del servidor de origen cada vez que se recibe una solicitud. “

Contador	Descripción
Memoria máxima (KB)	Cantidad máxima de memoria del dispositivo Citrix ADC asignada a la caché. Para obtener más información, consulta “Configuración de atributos globales para el almacenamiento en caché. “
Valor máximo de memoria activa (KB)	Cantidad máxima de memoria (valor activo) que se establecerá después de asignar la memoria a la caché. Para obtener más información, consulte “How to Configure the Integrated Caching Feature of a Citrix ADC Appliance for various Scenarios. “
Memoria utilizada (KB)	Cantidad de memoria que se está usando realmente.
Fallos de asignación de memoria	Número de intentos fallidos para utilizar la memoria con el propósito de almacenar una respuesta en la caché.
La respuesta más grande hasta el momento	La respuesta más grande en bytes se encuentra en el caché o en el servidor de origen y se envía al cliente.
Objetos almacenados en caches	Número de objetos en la caché, incluidas las respuestas que aún no se han descargado completamente y las respuestas que se han caducado pero aún no se han vaciado.
Objetos marcado	Los objetos marcadores se crean cuando una respuesta supera el tamaño máximo o mínimo de respuesta para el grupo de contenido, o aún no ha recibido el número mínimo de visitas para el grupo de contenido.
Hits que se están sirve	Número de hits que se han servido desde la caché.
Se pierde la gestión	Respuestas que se obtuvieron del servidor de origen, se almacenan en el caché y luego se sirven. Debe aproximarse al número de errores almacenables. No incluye errores no almacenables.

Para ver estadísticas de caché de resumen mediante la interfaz de línea de comandos:

En el símbolo del sistema, escriba:

```
stat cache
```

Para ver estadísticas de caché específicas mediante la interfaz de línea de comandos:

En el símbolo del sistema, escriba:

```
stat cache -detail
```

```
> stat cache -detail

Integrated Cache Statistics - Detail
Integrated Cache Statistics - Summary
                                                Rate (/s)
                                                   Total


Hits                                                  0
                        0

Misses                                                0
                        0

Requests                                              0
                        0

Hit ratio(%)                                         --
                        0

Origin bandwidth saved(%)                            --
                        0
Cached objects                                       --
                        0

Marker objects                                       --
                        0
                                                Rate (/s)
                                                   Total

Requests                                              0
                        0


```



```
Hit Statistics

                                                Rate (/s)
                                                   Total


Non-304 hits                                          0
                        0

304 hits                                              0
                        0


Sql hits                                              0
                        0


Hits                                                  0
                        0

304 hit ratio(%)                                     --
                        0

Hit ratio(%)                                         --
                        0

Origin bandwidth saved(%)                            --
                        0
Byte Statistics
                                                Rate (/s)
                                                   Total


Bytes served by Citrix ADC                          648
    55379204

Bytes served by cache                                 0
                        0
Byte hit ratio(%)                                    --
                        0
Compressed bytes from cache                           0
                        0

Miss Statistics

```



```
                                                Rate (/s)
                                                   Total

Storable misses                                        0
                        0

Non-storable misses                                    0
                        0

Misses                                                 0
                        0

Revalidations                                          0
                        0

Successful revalidations                               0
                        0

Conversions to conditional req                         0
                        0


Storable miss ratio(%)                                --
                        0
Successful reval ratio(%)                             --
                        0

Flashcache Statistics
                                                Rate (/s)
                                                   Total


Expire at last byte                                    0
                        0

Flashcache misses                                      0
                        0
Flashcache hits                                        0
                        0

Invalidation Statistics

                                                Rate (/s)
                                                   Total
```



```
88
89  Parameterized inval requests                          0
                          0
90
91
92  Full inval requests                                   0
                          0
93
94
95
96  Inval requests                                        0
                          0
97
98  Parameterized Caching Statistics
99
100                                                 Rate (/s)
                                                       Total
101
102
103 Parameterized requests                                0
                          0
104
105 Parameterized non-304 hits                            0
                          0
106
107 Parameterized 304 hits                                0
                          0
108
109
110 Total parameterized hits                              0
                          0
111
112 Parameterized 304 hit ratio(%)                       --
                          0
113
114 Poll Every Time (PET) Statistics
115
116                                                 Rate (/s)
                                                       Total
117
118
119 Poll every time requests                              0
                          0
120
121 Poll every time hits                                  0
```



```
                          0
122
123 Poll every time hit ratio(%)                        --
                          0
124
125 Memory Usage Statistics
126                                                  Total
127
128 Maximum memory(KB)                                  0
129
130 Maximum memory active value(KB)                     0
131
132 Utilized memory(KB)                                 0
133
134 Memory allocation failures                          0
135
136 Largest response so far(B)                          0
137
138 Cached objects                                      0
139
140 Marker objects                                      0
141
142 Hits being served                                   0
143 Misses being handled                                0
144  Done
145 <!--NeedCopy-->
```

Para ver estadísticas de caché de resumen mediante la interfaz gráfica de usuario

1. Haga clic en la ficha **Panel** de control en la parte superior de la página.
2. Desplácese hacia abajo hasta la sección **Almacenamiento en caché integrado** de la ventana.
3. Para ver estadísticas detalladas, haga clic en el enlace Más… en la parte inferior de la tabla.

Para ver estadísticas de caché específicas mediante la interfaz gráfica de usuario

1. Haga clic en la ficha **Informes** en la parte superior de la página.
2. En Informes integrados, expanda **Caché integrada**y, a continuación, haga clic en el informe con las estadísticas que quiere ver.
3. Para guardar el informe como plantilla, haga clic en **Guardar como y asigne** un nombre al informe. El informe guardado aparece en Informes **personalizados** .

Mostrar objetos almacenados en caché y estadísticas de caché

August 20, 2021

Puede ver determinados objetos almacenados en caché, y puede ver estadísticas de resumen sobre visitas de caché, errores y uso de memoria. Las estadísticas proporcionan información sobre la cantidad de datos que se están sirviendo desde la caché, qué elementos son responsables del mayor beneficio de rendimiento y qué puede ajustar para mejorar el rendimiento de la caché.

Esta sección incluye los siguientes detalles:

- Visualización de objetos almacenados en caché
- Búsqueda de respuestas específicas almacenadas en caché
- Visualización de Estadísticas de Caché

Ver objetos almacenados en caché

Después de habilitar el almacenamiento en caché, puede ver los detalles de los objetos almacenados en caché. Por ejemplo, puede ver los siguientes elementos:

- Tamaños de respuesta y tamaños de encabezado
- Códigos de estado
- Grupos de contenido
- `ETag`, Última modificación y encabezados Cache-Control
- Solicitar URL
- Parámetros de Hit
- Direcciones IP de destino
- Tiempos de solicitud y respuesta

Para ver una lista de objetos almacenados en caché mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
show cache object
```

Propiedades	Especificación
Tamaño de respuesta (bytes)	El tamaño del encabezado y el cuerpo de la respuesta.
Tamaño del encabezado de respuesta (bytes)	El tamaño de la parte de encabezado de la respuesta.
Código de estado de respuesta	El código de estado enviado con la respuesta.

Propiedades	Especificación
ETag	El ETag encabezado insertado en la respuesta. Normalmente, este encabezado indica si la respuesta ha cambiado recientemente.
Última modificación	El encabezado Last-Modified insertado en la respuesta. Este encabezado indica la fecha en que se cambió la respuesta por última vez.
Cache-Control	El encabezado Cache-Control insertado en la respuesta.
Fecha	El encabezado Date que indica cuándo se envió la respuesta.
Contentgroup	El grupo de contenido donde se almacena la respuesta.
Coincidencia compleja	Si este objeto se almacenó en caché basándose en valores parametrizados, este valor de campo es YES.
Host	El host especificado en la dirección URL que solicitó esta respuesta.
Puerto host	El puerto de escucha para el host especificado en la URL que solicitó esta respuesta
URL	La URL emitida para la respuesta almacenada.
IP de destino	La dirección IP del servidor desde el que se obtuvo esta respuesta.
Puerto de destino	El puerto de escucha del servidor de destino.
Parámetros de Hit	Si el grupo de contenido que almacena la respuesta utiliza parámetros de éxito, aparecen en este campo.
Selector de pulsación	Si este grupo de contenido utiliza un selector de aciertos, aparece en este campo.
Selector Inval	Si este grupo de contenido utiliza un selector de invalidación, aparece en este campo.
Expresiones del selector	Si este grupo de contenido utiliza un selector, este campo muestra la expresión que define la regla de selección.

Propiedades	Especificación
Request time (Tiempo de la solicitud)	Tiempo en milisegundos desde que se emitió la solicitud.
Tiempo de respuesta	Tiempo en milisegundos desde que la caché comenzó a recibir la respuesta.
Edad	Cantidad de tiempo que el objeto ha estado en la caché.
Caducidad	Cantidad de tiempo después del cual el objeto se marca como caducado.
Vaciado	Si la respuesta se ha vaciado después de la expiración.
Prebúsqueda	Si se ha configurado Prefetch para este grupo de contenido, la cantidad de tiempo antes de la expiración durante la cual el objeto se obtiene del origen. Prefetch no se aplica a objetos negativos (por ejemplo, 404 respuestas “objeto no encontrado”).
Lectores actuales	Aproximadamente el número actual de visitas que se están sirviendo. Cuando se descarga una respuesta con un objeto de encabezado Content-Length, los valores actuales fallan y los lectores actuales son normalmente 1. Cuando se descarga un objeto de respuesta fragmentada, el valor actual de errores suele ser 1, pero el valor de lectores actuales suele ser 0, porque la respuesta fragmentada que se sirve al cliente no proviene de los búferes de almacenamiento en caché integrados.
Fallos actuales	El número actual de solicitudes que resultaron en una pérdida de caché y en la obtención del servidor de origen. Este valor suele ser 0 o 1. Si la opción Sondear cada vez está habilitada para un grupo de contenido, el recuento puede ser mayor que 1.
Accesos	El número de aciertos de caché para este objeto.

Propiedades	Especificación
- Faldas	El número de errores de caché para este objeto.
Formato de compresión	Tipo de compresión aplicada a este objeto. Los formatos de compresión incluyen gzip, deflate, compress y pack200-gzip.
Versión HTTP en respuesta	Versión de HTTP que se utilizó para enviar la respuesta.
`etag` Presente débil en respuesta	`etag` Los encabezados fuertes cambian si cambian los bits de una entidad. Los encabezados fuertes se basan en los valores de octetos de un objeto. `etag` Los encabezados débiles cambian si cambia el significado de una entidad. `etag` Los valores débiles se basan en la identidad semántica. `etags` Los valores débiles comienzan con una “W”.
Célula de marcador negativo	Un objeto marcador se puede almacenar en caché, pero aún no cumple todos los criterios para almacenarse en caché. Por ejemplo, el objeto puede superar el tamaño máximo de respuesta para el grupo de contenido. Se crea una celda de marcador para objetos de este tipo. La próxima vez que un usuario envíe una solicitud para este objeto, se servirá una pérdida de caché.
Marcador de motivo creado	La razón por la que se creó una celda de marcador (por ejemplo, “Esperando minhit”, “Los datos de respuesta de longitud del contenido no están en el límite de tamaño del grupo”).
Sondeo automático cada vez	Si la caché integrada recibe una respuesta 200 OK ya caducada con validadores (ya sea los encabezados Last-Modified o los encabezados de `ETag` respuesta), almacena la respuesta y la marca como Autopet (sondear automáticamente cada vez).

Propiedades	Especificación
Citrix ADC Etag insertado en respuesta	Variación del `ETag` encabezado generado por el dispositivo Citrix ADC. Aparece un valor YES si Citrix ADC inserta un `Etag` en la respuesta.
Respuesta completa presente en la memoria caché	Indica si se trata de una respuesta completa.
IP de destino verificado por DNS	Indica si se realizó la resolución DNS al almacenar el objeto.
Objeto almacenado a través de un proxy de reenvío de caché	Indica si esta respuesta se almacenó debido a un proxy de reenvío configurado en la caché integrada.
El objeto es un archivo base Delta	Una respuesta que está comprimido por delta.
Esperando minhits	Indica si este grupo de contenido requiere un número mínimo de servidores de origen afectados antes de almacenar en caché una respuesta.
Recuento de minhit	Si este grupo de contenido requiere un número mínimo de servidores de origen golpeados antes de almacenar en caché un objeto, este campo muestra un recuento del número de visitas recibidas hasta el momento.
Método de solicitud HTTP	El método, GET o POST, utilizado en la solicitud que obtuvo este objeto.
Almacenado por directiva	El nombre de la directiva de almacenamiento en caché que causó el almacenamiento de este objeto. Un valor NO DISPONIBLE indica que la directiva se ha desactivado o eliminado. Un valor de NONE indica que el objeto no coincide con una directiva visible, pero se almacenó de acuerdo con criterios internos para el almacenamiento en caché.

Propiedades	Especificación
Existen metadatos de firewall de aplicaciones	Este parámetro se utiliza cuando el firewall de la aplicación y la caché integrada están activados. El firewall de la aplicación analiza el contenido de una página de respuesta, almacena sus metadatos (por ejemplo, direcciones URL y formularios contenidos en la página) y exporta los metadatos con la respuesta a la caché. La caché almacena la página y los metadatos, y cuando la caché sirve la página, envía los metadatos de vuelta a la sesión de la solicitud.
Objeto de llamada HTTP, nombre, tipo, respuesta	Estas celdas indican si estos datos se almacenaron como resultado de una expresión de llamada HTTP y proporcionan información sobre varios aspectos de la llamada y la respuesta correspondiente. Para obtener más información acerca de las llamadas HTTP, consulte “Llamadas HTTP”.

Buscar respuestas específicas almacenadas en caché

Puede encontrar elementos individuales en la caché según criterios de búsqueda. Existen diferentes métodos para buscar elementos almacenados en caché, dependiendo de si el grupo de contenido que contiene los datos utiliza selectores de aciertos e invalidación, como se indica a continuación:

Si el grupo de contenido utiliza selectores, solo puede realizar la búsqueda mediante el Id. de localizador para el elemento almacenado en caché.

Si el grupo de contenido no utiliza selectores, debe realizar la búsqueda mediante criterios como URL, host o nombre del grupo de contenido.

Al buscar una respuesta en caché, puede localizar algunos elementos por URL y host. Si la respuesta está en un grupo de contenido que utiliza un selector, solo puede encontrarla mediante un número de localizador (por ejemplo, 0x00000000ad7af00000050). Para guardar un número de localizador para utilizarlo posteriormente, haga clic con el botón derecho en la entrada y seleccione Copiar. Para obtener más información acerca de los selectores, consulte “Configuración de selectores y grupos de contenido básico.”

Para mostrar respuestas almacenadas en caché en grupos de contenido que no tienen un selector

mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
show cache object [-locator <positiveInteger>] | [(-url <URL> (-host <
hostName> [-port <port>] [-groupName <contentGroupName>] [-httpMethod GET
 | POST ]))| [-httpStatus<positive integer>] | -group <contentGroupName> |
-ignoreMarkerObjects (ON | OFF)| -includeNotReadyObjects (ON | OFF)]
```

Para mostrar respuestas almacenadas en caché en grupos de contenido que tienen un selector mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
show cache object -locator <locatorString> MarkerObjects ( ON | OFF )| -
includeNotReadyObjects ( ON | OFF )| [-httpStatus<positive integer>]
```

Para mostrar respuestas almacenadas en caché en grupos de contenido que no tienen un selector mediante la interfaz gráfica de usuario

Vaya a **Optimización** > Almacenamiento en **caché integrado> Objetos**en caché, haga clic en**Buscar**y defina los criterios de búsqueda para ver la respuesta almacenada en caché requerida.

Si aún no ha configurado ningún grupo de contenido, todos los objetos se encuentran en el grupo Predeterminado.

Para mostrar respuestas almacenadas en caché en grupos de contenido que tienen un selector mediante la interfaz gráfica de usuario

Vaya a **Optimización** > Almacenamiento en **caché integrado** > **Objetos en caché**, haga clic en **Buscar** y establezca los criterios de búsqueda del selector para ver la respuesta requerida en caché.

Ver estadísticas de caché

En la siguiente tabla se resumen las estadísticas de caché.

Contador

Especificación

Visualización de estadísticas de caché

Actualizado el: 28/10/2013

En la siguiente tabla se resumen las estadísticas detalladas de caché que puede ver.

Contador	Especifica
Accesos	Respuestas que se encuentran y se sirven desde la caché integrada. Incluye objetos estáticos como archivos de imagen, páginas con códigos de estado 200, 203, 300, 301, 302, 304, 307, 403, 404, 410 y respuestas que coinciden con una directiva definida por el usuario con una acción CACHE.
- Faldas	Solicitudes HTTP interceptadas donde finalmente se obtuvo la respuesta del servidor de origen.
Solicitudes	Total de aciertos de caché más errores totales de caché.
No 304 visitas	Si el usuario solicita un elemento más de una vez y el elemento de la caché no cambia desde la última vez que el dispositivo Citrix ADC lo sirvió, el dispositivo Citrix ADC ofrece una respuesta 304 en lugar del objeto almacenado en caché. Esta estadística indica cuántos elementos ha servido el dispositivo Citrix ADC desde la caché, excluyendo las respuestas 304.
304 visitas	Número de 304 respuestas (objeto no modificado) que el dispositivo Citrix ADC ha servido desde la caché.
304 aciertos (%)	Porcentaje de 304 respuestas que el dispositivo Citrix ADC sirvió, en relación con otras respuestas.
Relación de aciertos (%)	Porcentaje de respuestas que el dispositivo Citrix ADC sirvió desde la caché (visitas de caché) en relación con las respuestas que no se pudieron servir desde la caché.
Ancho de banda de origen guardado (%)	Estimación de la capacidad de procesamiento que el dispositivo Citrix ADC guardó en el servidor de origen debido a la publicación de respuestas desde la caché.

Contador	Especifica
Bytes servidos por Citrix ADC	Número total de bytes que el dispositivo Citrix ADC sirvió desde el servidor de origen y la caché.
Bytes servidos por caché	Número total de bytes que el dispositivo Citrix ADC sirvió desde la caché.
Relación de aciertos de bytes (%)	Porcentaje de datos que el dispositivo Citrix ADC ha servido desde la caché, en relación con todos los datos de todas las respuestas servidas.
Bytes comprimidos de caché	Cantidad de datos, en bytes, que el dispositivo Citrix ADC sirvió en formato comprimido.
Fallos almacenables	Si el dispositivo Citrix ADC no encuentra un objeto solicitado en la caché, lo recupera del servidor de origen. Esto se conoce como un fallo de caché. Una pérdida de caché almacenable se puede almacenar en la caché.
Fallos no almacenables	Una pérdida de caché no almacenable no se puede almacenar en la caché.
- Faldas	Todos los cachés fallan.
Revalidaciones	La configuración Max-Age en un encabezado Cache-Control determina, en número de segundos, cuándo una caché intermedia debe revalidar el contenido con la caché integrada antes de servirlo al usuario. Para obtener más información, consulte “Inserción de un encabezado de control de caché. “
Revalidaciones correctas	Número de revalidaciones que se han realizado. Para obtener más información, consulte “Inserción de un encabezado de control de caché. “

Contador	Especifica
Conversiones a condicional req	Una solicitud de agente de usuario para un objeto PET almacenado en caché siempre se convierte en una solicitud condicional y se envía al servidor de origen. Para obtener más información, consulte “Sondeo del servidor de origen cada vez que se recibe una solicitud. “
Relación de fallas almacenables (%)	La caché almacenable falla como porcentaje de errores de caché no almacenable.
Relación de reval correcta (%)	Revalidaciones correctas como porcentaje de todos los intentos de revalidación. Para obtener más información, consulte “Inserción de un encabezado de control de caché. “
Caducar en el último byte	Número de veces que el contenido de caché caducó inmediatamente después de recibir el último byte de cuerpo. Solo aplicable a las respuestas positivas, como se describe en la tabla “Cache Hits and Misses. “Para obtener más información, consulte “Ejemplo de Optimización del Rendimiento. “
Faltas de caché flash	Si habilita Flash Cache, la caché permite que solo una solicitud llegue al servidor, eliminando las multitudes flash. Esta estadística indica el número de solicitudes de caché de Flash que se han perdido en caché. Para obtener más información, “Poner en cola solicitudes a la caché. “
`Flashcache` éxitos	Número de solicitudes de caché de Flash que fueron aciertos de caché. Para obtener más información, consulte “Solicitudes de cola en la caché. “
Solicitudes de inval parametrizadas	Solicitudes que coinciden con una directiva con una acción de invalidación (INVAL) y un grupo de contenido que utiliza un selector de invalidación o parámetros para caducar selectivamente los objetos almacenados en caché del grupo.

Contador	Especifica
Solicitudes de inval completas	Solicitudes que coinciden con una directiva de invalidación en la que se configura el parámetro InvalGroups y caduca uno o varios grupos de contenido.
Solicitudes Inval	Solicitudes que coinciden con una directiva de invalidación y dan como resultado la expiración de respuestas específicas almacenadas en caché o grupos de contenido completos.
Solicitudes parametrizadas	Número de solicitudes de caché procesadas mediante una directiva con un grupo de contenido parametrizado.
aciertos parametrizados no 304	Número de solicitudes de caché procesadas mediante una directiva con un grupo de contenido parametrizado, donde se encontró una respuesta completa en caché y la respuesta no era una respuesta 304 (objeto no actualizado).
304 aciertos parametrizados	Número de solicitudes de caché procesadas mediante una directiva con un grupo de contenido parametrizado, donde se encontró el objeto almacenado en caché y el objeto fue una respuesta 304 (objeto no actualizado).
Total de aciertos parametrizados	Número de solicitudes de caché procesadas mediante una directiva con un grupo de contenido parametrizado, donde se encontró el objeto almacenado en caché.
Relación de aciertos 304 parametrizada (%)	Porcentaje de 304 respuestas (objeto no actualizado) que se encontraron mediante una directiva parametrizada, en relación con todos los aciertos de caché.

Contador	Especifica
Encuesta cada vez que se solicita	Si Poll Every Time está habilitado, el dispositivo Citrix ADC siempre consulta el servidor de origen antes de servir un objeto almacenado. Para obtener más información, consulte “Sondeo del servidor de origen cada vez que se recibe una solicitud. “
Encuesta cada vez que se golpea	Número de veces que se encontró una coincidencia de caché mediante el método Poll Every Time. Para obtener más información, consulte “Sondeo del servidor de origen cada vez que se recibe una solicitud. “
Encuesta cada vez que aciertos (%)	Porcentaje de aciertos de caché que utilizan el método Poll Every Time, en relación con todas las búsquedas de objetos almacenados en caché que utilizan Poll Every Time. Para obtener más información, consulte “Sondeo del servidor de origen cada vez que se recibe una solicitud. “
Memoria máxima (KB)	Cantidad máxima de memoria en el dispositivo Citrix ADC asignada a la caché. Para obtener más información, consulte “Configuración de atributos globales para almacenamiento en caché”.
Valor máximo de memoria activa (KB)	Cantidad máxima de memoria (valor activo) que se establecerá después de que la memoria se asigne realmente a la caché. Para obtener más información, consulte “How to Configure the Integrated Caching Feature of a Citrix ADC Appliance for various Scenarios. “
Memoria utilizada (KB)	Cantidad de memoria que se está usando realmente.
Errores de asignación de memoria	Número de intentos fallidos para utilizar la memoria con el propósito de almacenar una respuesta en la caché.

Contador	Especifica
La respuesta más grande hasta ahora	La respuesta más grande en bytes se encuentra en la caché o en el servidor de origen y se envía al cliente.
Objetos almacenados en caché	Número de objetos en la caché, incluidas las respuestas que aún no se han descargado completamente y las respuestas que se han caducado pero que aún no se han vaciado.
Objetos de marcador	Los objetos Marker se crean cuando una respuesta supera el tamaño máximo o mínimo de respuesta para el grupo de contenido o aún no ha recibido el número mínimo de visitas para el grupo de contenido.
Hits que se están sirviendo	Número de visitas que se han servido desde la caché.
Faltan las manejadas	Respuestas que se obtuvieron del servidor de origen, se almacenaron en la caché y luego se sirvieron. Debe aproximarse el número de errores almacenables. No incluye errores no almacenables.

Para ver estadísticas de caché de resumen mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
stat cache
```

Para ver estadísticas específicas de caché mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
1 stat cache -detail
2
3     > stat cache -detail
4     Integrated Cache Statistics - Detail
5     Integrated Cache Statistics - Summary
6                                                 Rate (/s)
                                                     Total
7     Hits                                              0
                            0
```



```
8      Misses                                                  0
                           0
9      Requests                                                0
                           0
10     Hit ratio(%)                                           --
                           0
11     Origin bandwidth saved(%)                              --
                           0
12     Cached objects                                         --
                           0
13     Marker objects                                         --
                           0
14                                                 Rate (/s)
                                                      Total
15     Requests                                                0
                           0
16     Hit Statistics
17                                                 Rate (/s)
                                                      Total
18     Non-304 hits                                            0
                           0
19     304 hits                                                0
                           0
20     Sql hits                                                0
                           0
21     Hits                                                    0
                           0
22     304 hit ratio(%)                                       --
                           0
23     Hit ratio(%)                                           --
                           0
24     Origin bandwidth saved(%)                              --
                           0
25
26     Byte Statistics
27                                                 Rate (/s)
                                                      Total
28     Bytes served by Citrix ADC                            648
          55379204
29     Bytes served by cache                                   0
                           0
30     Byte hit ratio(%)                                      --
                           0
31     Compressed bytes from cache                             0
                           0
```



```
32     Miss Statistics
33                                                  Rate (/s)
                                                       Total
34     Storable misses                                     0
                            0
35     Non-storable misses                                 0
                            0
36     Misses                                              0
                            0
37     Revalidations                                       0
                            0
38     Successful revalidations                            0
                            0
39     Conversions to conditional req                      0
                            0
40     Storable miss ratio(%)                             --
                            0
41     Successful reval ratio(%)                          --
                            0
42     Flashcache Statistics
43                                                  Rate (/s)
                                                       Total
44     Expire at last byte                                 0
                            0
45     Flashcache misses                                   0
                            0
46     Flashcache hits                                     0
                            0
47
48     Invalidation Statistics
49                                                  Rate (/s)
                                                       Total
50     Parameterized inval requests                        0
                            0
51     Full inval requests                                 0
                            0
52     Inval requests                                      0
                            0
53
54     Parameterized Caching Statistics
55                                                  Rate (/s)
                                                       Total
56     Parameterized requests                              0
                            0
57     Parameterized non-304 hits                          0
```



```
                              0
58      Parameterized 304 hits                                  0
                              0
59      Total parameterized hits                                0
                              0
60      Parameterized 304 hit ratio(%)                         --
                              0
61
62      Poll Every Time (PET) Statistics
63                                                  Rate (/s)
                                                       Total
64      Poll every time requests                             0
                              0
65      Poll every time hits                                 0
                              0
66      Poll every time hit ratio(%)                        --
                              0
67      Memory Usage Statistics
68                                                    Total
69      Maximum memory(KB)                                   0
70      Maximum memory active value(KB)                      0
71      Utilized memory(KB)                                  0
72      Memory allocation failures                           0
73      Largest response so far(B)                           0
74      Cached objects                                       0
75      Marker objects                                       0
76      Hits being served                                    0
77      Misses being handled                                 0
78       Done
79  <!--NeedCopy-->
```

Para ver las estadísticas de caché de resumen mediante la interfaz gráfica de usuario

1. Haga clic en la ficha **Panel** de control en la parte superior de la página.
2. Desplácese hacia abajo hasta la sección Almacenamiento en caché integrado de la ventana.
3. Para ver estadísticas detalladas, haga clic en el enlace Más… en la parte inferior de la tabla.

Para ver estadísticas específicas de caché mediante la interfaz gráfica de usuario

1. Haga clic en la ficha Informes en la parte superior de la página.
2. En Informes integrados, expanda Caché integrada y, a continuación, haga clic en el informe con las estadísticas que quiere ver.
3. Para guardar el informe como plantilla, haga clic en Guardar como y asigne un nombre al informe. El informe guardado aparece en Informes personalizados.

Mejorar el rendimiento de la caché

August 20, 2021

Puede mejorar el rendimiento de la caché integrada, incluido el manejo de solicitudes simultáneas para los mismos datos almacenados en caché, evitar retrasos asociados con la actualización de las respuestas almacenadas en caché del servidor de origen y garantizar que una respuesta se solicite con la suficiente frecuencia como para que valga la pena almacenar en caché.

Reducir las multitudes de flash

Las multitudes de flash ocurren cuando muchos usuarios solicitan simultáneamente los mismos datos. Las solicitudes en una multitud flash pueden convertirse en errores de caché si configuró la caché para que sirva visitas solo después de descargar todo el objeto.

Las siguientes técnicas pueden reducir o eliminar las multitudes de flash:

- **PREFETCH**: Actualiza una respuesta positiva antes de que caduque para asegurarse de que nunca se vuelve obsoleta o inactiva. Para obtener más información, consulte la sección "Actualización de una respuesta antes de la expiración".
- **Almacenamiento en búfer de caché**: comienza a servir una respuesta a varios clientes cuando recibe el encabezado de respuesta del servidor de origen, en lugar de esperar a que se descargue toda la respuesta. El único límite en el número de clientes que pueden descargar una respuesta simultáneamente son los recursos del sistema disponibles. El dispositivo Citrix ADC descarga y ofrece respuestas incluso si el cliente que inició la descarga se detiene antes de que se complete la descarga. Si la respuesta excede el tamaño de la caché o si la respuesta está cortada, la caché deja de almacenar la respuesta, pero el servicio a los clientes no se interrumpe.
- **Caché Flash:** Caché Flash pone en cola las solicitudes en la caché y permite que solo una solicitud llegue al servidor a la vez.

Para obtener más información, consulte la sección "Solicitudes de cola en la caché".

Actualizar una respuesta antes de la expiración

Para asegurarse de que una respuesta almacenada en caché esté fresca siempre que sea necesaria, la opción PREFETCH actualiza una respuesta antes de su tiempo de caducidad calculado. El intervalo de captura previa se calcula después de recibir la primera solicitud del cliente. A partir de ese momento, el dispositivo Citrix ADC actualiza la respuesta almacenada en caché en un intervalo de tiempo que se configura en el parámetro PREFETCH.

Esta configuración es útil para los datos que se actualizan con frecuencia entre las solicitudes. No se aplica a las respuestas negativas (por ejemplo, 404 mensajes).

Para configurar la captura previa de un grupo de contenido mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
set cache contentgroup <name> -prefetch YES [-prefetchPeriod <seconds> | -
prefetchPeriodMilliSec <milliseconds>] [-prefetchMaxPending <positiveInteger
>]
```

*Para configurar la captura previa de un grupo de contenido mediante la interfaz gráfica de usuario

Vaya a **Optimización** > Almacenamiento en **caché integrado** > **Grupos de contenido**y seleccione el **grupo de contenido**.

En la ficha **Otros**, en el grupo Multitud de Flash y Recuperación **previa, seleccione la opción Recuperación previa** y especifique los valores en los cuadros de texto Intervalo y Número máximo de recuperaciones previas pendientes.

Solicitudes de cola en la caché

La opción Caché Flash pone en cola las solicitudes que llegan simultáneamente (una multitud flash), recupera la respuesta y la distribuye a todos los clientes cuyas solicitudes están en la cola. Si, durante este proceso, la respuesta no se puede almacenar en caché, el dispositivo Citrix ADC deja de servir la respuesta desde la caché y, en su lugar, sirve la respuesta del servidor de origen a los clientes en cola. Si la respuesta no está disponible, los clientes recibirán un mensaje de error.

Flash Cache está inhabilitado de forma predeterminada. No puede habilitar la encuesta cada vez (PET) y la caché de Flash en el mismo grupo de contenido.

Una desventaja de Flash Cache es que si el servidor responde con un error (por ejemplo, un 404 que se soluciona rápidamente), el error se aviva a los clientes en espera.

> **Nota**:
> Si Flash Cache está habilitado, en algunas situaciones el dispositivo Citrix ADC no puede hacer coincidir correctamente el encabezado Accept-Encoding en la solicitud del cliente con el encabezado Content-Encoding en la respuesta. El dispositivo Citrix ADC puede suponer que estos encabezados coinciden y dan un resultado erróneo. Como solución alternativa, puede configurar las directivas de almacenamiento en caché integrado para que no permita el servicio de visitas a clientes que no tengan un encabezado Accept-Encoding apropiado.

Para habilitar Flash Cache mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
set cache contentgroup <contentGroupName> -flashcache yes
```

Para habilitar Flash Cache mediante la interfaz gráfica de usuario

Vaya a **Optimización** > Almacenamiento en **caché integrado** > **Grupos de contenido**y seleccione el grupo de contenido.

En la ficha **Otros**, en el grupo Flash Crowd y Prefetch, seleccione la opción **Prefetch**.

Caché una respuesta después de que un cliente detenga una descarga

Puede establecer el parámetro Abortar rápido para continuar almacenando en caché una respuesta, incluso si el cliente detiene una solicitud antes de que la respuesta esté en la caché.

Si el tamaño de respuesta descargado es menor o igual que el tamaño de Abortar rápido, el dispositivo Citrix ADC deja de descargar la respuesta. Si establece el parámetro Abortar rápido en 0, todas las descargas se detienen.

Para configurar el tamaño de anulación rápida mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
set cache contentgroup <name> -quickAbortSize <integerInKBytes>
```

Para configurar el tamaño de anulación rápida mediante la interfaz gráfica de usuario

1. Vaya a **Optimización** > Almacenamiento en **caché integrado** > **Grupos de contenido**y seleccione el grupo de contenido.
2. En la ficha **Memoria**, establezca el valor relevante en Abortar rápido: Continuar el almacenamiento en caché si hay más de cuadro de texto.

Requerir un número mínimo de visitas de servidor antes de almacenar en caché

Puede configurar el número mínimo de veces que se debe encontrar una respuesta en el servidor de origen antes de que se pueda almacenar en caché. Debe considerar aumentar los hits mínimos si la memoria caché se llena rápidamente y tiene una relación de aciertos inferior a la esperada.

El valor predeterminado para el número mínimo de visitas es 0. Este valor almacena en caché la respuesta después de la primera solicitud.

Para configurar el número mínimo de visitas que se requieren antes del almacenamiento en caché mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
set cache contentgroup <name> -minhits <positiveInteger>
```

Para configurar el número mínimo de visitas que se requieren antes del almacenamiento en caché mediante la interfaz gráfica de usuario

1. Vaya a **Optimización** > Almacenamiento en **caché integrado** > **Grupos de contenido**y seleccione el grupo de contenido.

2. En la ficha **Memoria**, establezca el valor relevante en No almacenar en caché, si las visitas son menores que el cuadro de texto.

Ejemplo de optimización del rendimiento

En este ejemplo, un cliente accede a una cotización de acciones. Las cotizaciones bursátiles son muy dinámicas. Configure la caché integrada para que sirva la misma cotización de stock a clientes simultáneos sin enviar varias solicitudes al servidor de origen. La cotización de acciones caduca después de que se descarga a los clientes, y la siguiente solicitud se obtiene del servidor de origen. Esto garantiza que la cotización esté siempre actualizada.

La siguiente descripción general de la tarea describe los pasos para configurar la caché para la aplicación de cotización de stock.

Configurar el almacenamiento en caché para una aplicación de cotización de acciones

Crear un grupo de contenido para cotizaciones de acciones

Para obtener más información, consulte “Acerca de los grupos de contenido.”

Configure lo siguiente para este grupo de contenido:

1. En la ficha **Método de caducidad**, active la casilla de verificación Expirar después de que se haya recibido la respuesta completa.
2. En la ficha **Otros**, active la casilla de verificación **Caché Flash** y haga clic en **Crear**.
3. Agregue una directiva de caché para almacenar en caché las cotizaciones de acciones.

Para obtener más información, consulte “Configuración de una directiva en la caché integrada.”

Configure lo siguiente para la directiva

1. En las listas **Acción y Almacenar en grupo**, seleccione **CACHE** y seleccione el grupo que definió en el paso anterior.
2. Haga clic en **Agregar** y, en el cuadro de diálogo **Agregar expresión**, configure una expresión que identifique las solicitudes de cotización de acciones, por ejemplo: Http.req.url.contains (“cgi-bin/stock-quote.pl”)
3. Active la directiva.

Para obtener más información, consulte “Vinculación global de una directiva de almacenamiento en caché integrada.” En este ejemplo, vincula esta directiva para el procesamiento de anulación de tiempo de solicitud y establece la prioridad en un valor bajo.

Configurar cookies, encabezados y sondeos

December 2, 2021

En este tema se explica cómo configurar la memoria caché para administrar las cookies, los encabezados HTTP y el sondeo del servidor de origen. Esto incluye modificar el comportamiento predeterminado que hace que la memoria caché difiera de los estándares documentados, anular los encabezados HTTP que podrían provocar que el contenido almacenable en caché no se almacene en la memoria caché y configurar la memoria caché para que siempre sondee el origen del contenido actualizado.

Divergencia del comportamiento de la memoria caché con respecto a los estándares

De forma predeterminada, la memoria caché integrada se adhiere a los siguientes estándares RFC:

- RFC 2616, “HTTP HTTP/1.1”
- Los comportamientos de almacenamiento en caché descritos en RFC 2617, “Autenticación HTTP: autenticación de acceso básica y implícita”
- El comportamiento de almacenamiento en caché descrito en RFC 2965, “Mecanismo de administración del estado HTTP”

Las directivas integradas y los atributos del grupo de contenido predeterminado garantizan el cumplimiento de la mayoría de estos estándares.

El comportamiento predeterminado de la memoria caché integrada difiere de la especificación de la siguiente manera:

- La funcionalidad es limitada para el encabezado Vary. De forma predeterminada, cualquier respuesta que contenga un encabezado Vary no se puede almacenar en caché a menos que se comprima. Una respuesta comprimida contiene codificación de contenido: gzip, codificación de contenido: desinflar o codificación de contenido: pack200-gzip y se puede almacenar en caché incluso si contiene el encabezado Vary: Accept-coding.
- La caché integrada ignora los valores del control de caché de encabezados: sin caché y control de caché: privado. Por ejemplo, una respuesta que contiene control de caché: no-cache=”Set-cookie” se trata como si la respuesta contenía Cache-Control: sin caché. De forma predeterminada, la respuesta no se almacena en caché.
- Una imagen (tipo de contenido = image/*) siempre se considera almacenable en caché, incluso si una respuesta de imagen contiene encabezados set-cookie o set-cookie2, o si una solicitud de imagen contiene un encabezado de cookie. La memoria caché integrada elimina los encabezados set-cookie y set-cookie2 de una respuesta antes de almacenarla en caché. Esto difiere del RFC 2965. Puede configurar el comportamiento compatible con RFC de la siguiente manera:

```
1 add cache policy rfc_compliant_images_policy -rule ”http.res.header.set
     -cookie2.exists || http.res.header.set-cookie.exists” -action
     NOCACHE
2
3
```



```
4 bind cache global rfc_compliant_images_policy -priority 100 -type
     REQ_OVERRIDE
5 <!--NeedCopy-->
```

- Los siguientes encabezados de control de caché en una solicitud obligan a una memoria caché compatible con RFC a recargar una respuesta almacenada en caché desde el servidor de origen:

```
Cache-control: max-age=0
```

```
Cache-control: no-cache
```

Para protegerse de los ataques de denegación de servicio, este comportamiento no es el predeterminado.

- Por defecto, el módulo de almacenamiento en caché considera que una respuesta se puede almacenar en caché a menos que una cabecera de respuesta indique lo contrario. Para que este comportamiento sea compatible con RFC 2616, establezca `-weakPosRelExpiry` y `-weakNegResExpiry` en 0 para todos los grupos de contenido.

Eliminar las cookies de una respuesta

Las cookies a menudo se personalizan para un usuario y, por lo general, no deben almacenarse en caché. El parámetro `Remove Response Cookies` elimina los encabezados `Set-Cookie and Set-Cookie2` antes de almacenar en caché una respuesta. De forma predeterminada, la opción `Remove Response Cookies` de un grupo de contenido evita el almacenamiento en caché de las respuestas con encabezados `Set-Cookie` o `Set-Cookie2`.

> **Nota:**
> Cuando las imágenes se almacenan en caché, el comportamiento integrado es eliminar `Set-Cookie2` los encabezados `Set-Cookie` y antes del almacenamiento en caché, sin importar cómo esté configurado el grupo de contenido.
>
> Citrix recomienda que acepte el valor predeterminado `Remove Response Cookies` para cada grupo de contenido que almacene respuestas incrustadas, por ejemplo, imágenes.

Para configurar `Remove Response Cookies` un grupo de contenido mediante la interfaz de línea de comandos:

En el símbolo del sistema, escriba:

```
set cache contentgroup <name> -removeCookies YES
```


Configurar Eliminar cookies de respuesta para un grupo de contenido mediante la GUI de Citrix ADC

1. Vaya a **Optimización** > Almacenamiento en **caché integrado** > **Grupos de contenido**y seleccione el grupo de contenido.
2. En la ficha **Otros**, en el grupo **Configuración**, seleccione la opción Eliminar cookies de respuesta.

Inserción de encabezados HTTP en tiempo de respuesta

La memoria caché integrada puede insertar encabezados HTTP en las respuestas que resultan de las solicitudes de caché. El dispositivo Citrix ADC no modifica los encabezados en las respuestas que resultan de errores de caché.

En la siguiente tabla se describen los encabezados que se pueden insertar en una respuesta.

Encabezado	Especificación
Edad	Proporciona la antigüedad de la respuesta en segundos, calculada a partir del momento en que se generó la respuesta en el servidor de origen. De forma predeterminada, la caché inserta un encabezado Age para cada respuesta que se sirve desde la caché.
vía	Enumera los protocolos y los destinatarios entre los puntos de inicio y finalización de una solicitud o una respuesta. El dispositivo Citrix ADC inserta un encabezado Via en cada respuesta que sirve desde la memoria caché. El valor predeterminado del encabezado insertado es `NS-CACHE-10.0`: último octeto de la dirección IP de Citrix ADC". Para obtener más información, consulte "Configuración de atributos globales para el almacenamiento en caché. "

Encabezado	Especificación
Tag	La memoria caché admite la validación de respuestas mediante Last-Modified y encabezados Tag para determinar si una respuesta está obsoleta. La memoria caché inserta una Tag en una respuesta solo si almacena en caché la respuesta y el servidor de origen no ha insertado su propia cabecera Tag. El valor Tag es un número único y arbitrario. El valor Tag de una respuesta cambia si se actualiza desde el servidor de origen, pero permanece igual si el servidor envía una respuesta 304 (objeto no actualizado). Los servidores de origen normalmente no generan validadores para el contenido dinámico porque el contenido dinámico se considera que no se puede almacenar en caché. Puede anular este comportamiento. Con la inserción de encabezados Tag, se permite que la memoria caché no sirva respuestas completas. En cambio, se requiere que el agente de usuario almacene en caché la respuesta dinámica enviada por la memoria caché integrada la primera vez. Para forzar a un agente de usuario a almacenar en caché una respuesta, configure la memoria caché integrada para insertar un encabezado Tag y reemplazar el encabezado Cache-Control proporcionado por el origen.

Encabezado	Especificación
Control de caché	El dispositivo Citrix ADC normalmente no modifica los encabezados de capacidad de caché en las respuestas que se sirven desde el servidor de origen. Si el servidor de origen envía una respuesta etiquetada como no almacenable en caché, el cliente trata la respuesta como no almacenable en caché, incluso si el dispositivo Citrix ADC almacena en caché la respuesta. Para almacenar en caché las respuestas dinámicas en un agente de usuario, puede reemplazar los encabezados de Cache-Control del servidor de origen. Esto se aplica solo a los agentes de usuario y a otras memorias caché intervinientes. No afectan a la memoria caché integrada.

Encabezado	Especificación
Edad	Proporciona la antigüedad de la respuesta en segundos, calculada a partir del momento en que se generó la respuesta en el servidor de origen. De forma predeterminada, la caché inserta un encabezado Age para cada respuesta que se sirve desde la caché.
vía	Enumera los protocolos y los destinatarios entre los puntos de inicio y finalización de una solicitud o una respuesta. El dispositivo Citrix ADC inserta un encabezado Via en cada respuesta que sirve desde la memoria caché. El valor predeterminado del encabezado insertado es “NS-CACHE-9.2: último octeto de la dirección IP de Citrix ADC”. Para obtener más información, consulte “Configuración de atributos globales para el almacenamiento en caché. “

Encabezado	Especificación
Tag	La memoria caché admite la validación de respuestas mediante las cabeceras Last-Modified y Tag para determinar si una respuesta está obsoleta. La memoria caché inserta una Tag en una respuesta solo si almacena en caché la respuesta y el servidor de origen no ha insertado su propia cabecera Tag. El valor Tag es un número único y arbitrario. El valor Tag de una respuesta cambia si se actualiza desde el servidor de origen, pero permanece igual si el servidor envía una respuesta 304 (objeto no actualizado). Los servidores de origen normalmente no generan validadores para el contenido dinámico porque el contenido dinámico se considera que no se puede almacenar en caché. Puede anular este comportamiento. Con la inserción de encabezados Tag, se permite que la memoria caché no sirva respuestas completas. En cambio, se requiere que el agente de usuario almacene en caché la respuesta dinámica enviada por la memoria caché integrada la primera vez. Para forzar a un agente de usuario a almacenar en caché una respuesta, configure la memoria caché integrada para insertar un encabezado Tag y reemplazar el encabezado Cache-Control proporcionado por el origen.

Encabezado	Especificación
Control de caché	El dispositivo Citrix ADC normalmente no modifica los encabezados de capacidad de caché en las respuestas que se sirven desde el servidor de origen. Si el servidor de origen envía una respuesta etiquetada como no almacenable en caché, el cliente trata la respuesta como no almacenable en caché, incluso si el dispositivo Citrix ADC almacena en caché la respuesta. Para almacenar en caché las respuestas dinámicas en un agente de usuario, puede reemplazar los encabezados de Cache-Control del servidor de origen. Esto se aplica solo a los agentes de usuario y a otras memorias caché intervinientes. No afectan a la memoria caché integrada.

Insertar un encabezado de edad, vía o etiqueta

Los siguientes procedimientos describen cómo insertar encabezados Age, Via y ETag.

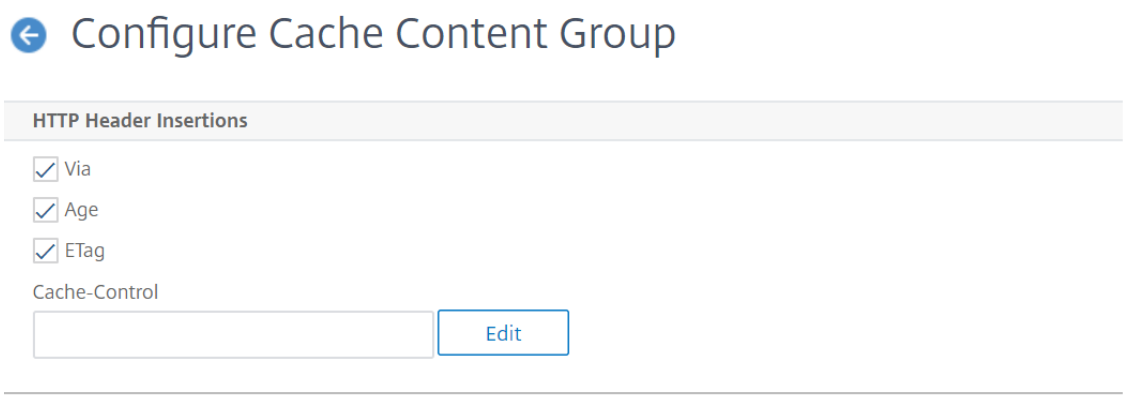
Inserte un encabezado Age, Via o Etag mediante la interfaz de comandos de Citrix ADC:

En el símbolo del sistema, escriba:

```
set cache contentgroup <name> -insertVia YES -insertAge YES -insertETag YES
```

Configure el encabezado Age, Via o Etag mediante la GUI de Citrix ADC

1. Vaya a **Optimización** > Almacenamiento en **caché integrado** > **Grupos de contenido** y seleccione el **grupo de contenido**.
2. En la ficha **Otros**, en el grupo Inserciones de encabezado HTTP, seleccione las opciones **Vía**, **Edad**o **ETag**, según corresponda.
3. Los valores de los demás tipos de encabezado se calculan automáticamente. Configure el valor Via en la configuración principal de la memoria caché.



Insertar un encabezado de control de caché

Cuando la memoria caché integrada reemplaza un encabezado de Cache-Control que el servidor de origen insertó, también reemplaza el encabezado Expires. El nuevo encabezado Expires contiene una fecha de caducidad en el pasado. Esto garantiza que los clientes y las memorias caché HTTP/1.0 (que no entienden el encabezado Cache-Control) no almacenan en caché el contenido.

Inserte un encabezado cache-control mediante la interfaz de comandos de Citrix ADC

En el símbolo del sistema, escriba:

```
set cache contentgroup <name> -cacheControl <value>
```

Inserte un encabezado de control de caché mediante la GUI de Citrix ADC

1. Vaya a **Optimización** > Almacenamiento en **caché integrado** > **Grupos de contenido**y
   a) Haga clic en la ficha **Método de caducidad**, borre la configuración de caducidad heurística y predeterminada y establezca el valor relevante en el cuadro de texto Caducar contenido después.
   b) Haga clic en la ficha **Otros** y escriba el encabezado que quiere insertar en el cuadro de texto Cache-Control. También puede hacer clic en Configurar para establecer las directivas de Cache-Control en las respuestas almacenadas en caché.

Ignorar los encabezados de control de caché y pragma en las solicitudes

De forma predeterminada, el módulo de almacenamiento en caché procesa los encabezados de Cache-Control y Pragma. Los siguientes tokens en las cabeceras Cache-Control se procesan como se describe en RFC 2616.

- edad máx
- max-rancio

- solo en caché
- sin caché

Un encabezado Pragma: sin caché en una solicitud se trata de la misma manera que un encabezado Cache-Control: sin caché.

Si configura el módulo de almacenamiento en caché para que ignore los encabezados Cache-Control y Pragma, una solicitud que contenga un encabezado Cache-Control: No-Cache hace que el dispositivo Citrix ADC recupere la respuesta del servidor de origen, pero la respuesta almacenada en caché no se actualiza. Si el módulo de almacenamiento en caché procesa los encabezados Cache-Control y Pragma, la respuesta almacenada en caché se actualiza.

En la siguiente tabla se resumen las implicaciones de varias configuraciones para estos encabezados y la configuración Ignorar solicitud de recarga del explorador.

Configuración para ignorar encabezados Cache-Control y Pragma	**Configuración para ignorar solicitud de recarga del explorador**	**Resultado**
Sí	Sí o no	Ignore los encabezados Cache-Control y Pragma del cliente, incluida la directiva Cache-Control: sin caché.
No	Sí	El encabezado Cache-Control: sin caché produce un error de caché, pero una respuesta que ya está en la memoria caché no se actualiza.
No	No	Una solicitud que contiene un encabezado Cache-Control: sin caché provoca una falta de caché y la respuesta almacenada se actualiza.

Para ignorar los encabezados Cache-Control y Pragma en una solicitud mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
set cache contentgroup <name> -ignoreReqCachingHdrs YES
```

Para ignorar las solicitudes de recarga del explorador mediante la interfaz de línea de comandos

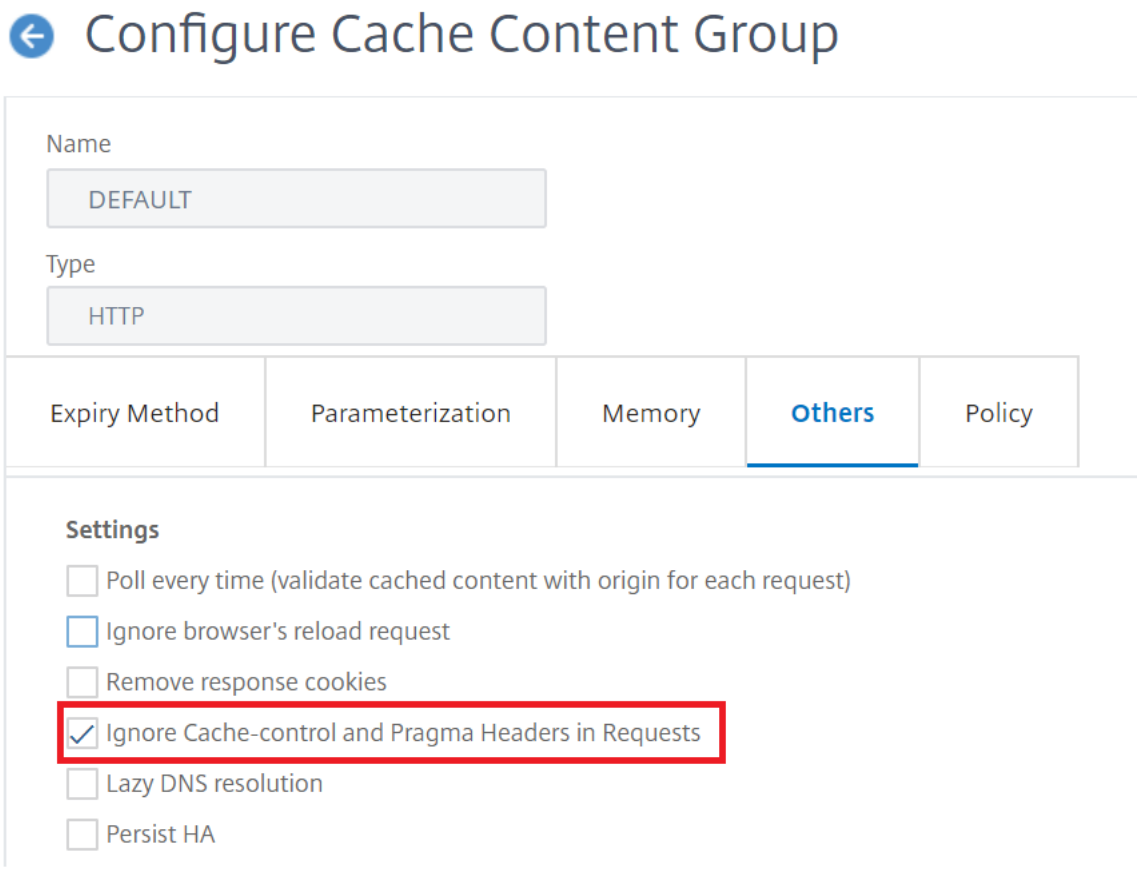
En el símbolo del sistema, escriba:


```
set cache contentgroup <name> -ignoreReloadReq NO
```

> **Nota:**
> De forma predeterminada, el parámetro -IgnoreReloadReq se establece en YES.

Ignorar los encabezados de Cache-Control y Pragma en una solicitud mediante la GUI

1. Vaya a **Optimización** > Almacenamiento en **caché integrado** > **Grupos de contenido**y seleccione el grupo de contenido.
2. En la ficha **Otros**, en el grupo **Configuración**, seleccione **Ignorar encabezados de control de caché y Pragma** en la opción **Solicitudes**.



Ejemplo de una directiva para ignorar los encabezados de Cache-Control:

En el siguiente ejemplo, configura una directiva de anulación de tiempo de solicitud para almacenar en caché las respuestas que contienen Content-type: image/* independientemente del encabezado Cache-Control en la respuesta.

Para configurar una directiva de anulación de tiempo de solicitud para almacenar en caché todas las respuestas con imagen/*

Vaciar la memoria caché con la opción Invalidar todo.

Configure una nueva directiva de caché y dirija la directiva a un grupo de contenido en particular. Para obtener más información, consulte “Configuración de una directiva en la memoria caché integrada. “

Asegúrese de que el grupo de contenido que utiliza la directiva esté configurado para ignorar los encabezados de Cache-Control, como se describe en “Ignorar encabezados de Cache-Control y Pragma en Solicitudes. “

Enlazar la directiva al banco de directivas de anulación de tiempo de solicitud.

Para obtener más información, consulte el tema Vinculación global de una directiva de almacenamiento en caché integrada.

Servidor de origen de sondeo cada vez que se recibe una solicitud

Puede configurar el dispositivo Citrix ADC para que consulte siempre el servidor de origen antes de ofrecer una respuesta almacenada. Esto se conoce como Encuesta Cada vez (PET). Cuando el dispositivo Citrix ADC consulta el servidor de origen y la respuesta PET no ha caducado, una respuesta completa del servidor de origen no sobrescribe el contenido en caché. Esta propiedad es útil cuando se publica contenido específico del cliente.

Cuando caduca una respuesta PET, el dispositivo Citrix ADC la actualiza cuando llega la primera respuesta completa del servidor de origen.

La función Poll Every Time (PET) funciona de la siguiente manera:

Para una respuesta en caché que tiene validadores en forma de etiqueta o encabezado de última modificación, si la respuesta caduca, se marca automáticamente como PET y se almacena en caché.

Puede configurar PET para un grupo de contenido.

Si configura un grupo de contenido como PET, todas las respuestas del grupo de contenido se marcan como PET. El grupo de contenido PET puede almacenar respuestas que no tienen validadores. Las respuestas que se marcan automáticamente como PET siempre caducan. Las respuestas que pertenecen a un grupo de contenido PET pueden caducar tras un retraso, en función de cómo configure el grupo de contenido.

Los sondeos afectan a dos tipos de solicitudes:

- Solicitudes condicionales: un cliente emite una solicitud condicional para garantizar que la respuesta que tiene es la copia más reciente. Una solicitud de agente de usuario para una respuesta PET almacenada en caché siempre se convierte en una solicitud condicional y se envía al servidor de origen. Una solicitud condicional tiene validadores en los encabezados `If-Modified-Since` o `If-None-Match`. El encabezado `If-Modified-Since` contiene el tiempo desde el encabezado `Last-Modified`. Un encabezado If-None-Match contiene el valor del encabezado Tag de la respuesta. Si la copia de la respuesta del cliente es nueva, el servidor de origen responde con 304 No modificado. Si la copia está obsoleta, una respuesta condicional genera 200 OK que contiene toda la respuesta.

- Solicitudes no condicionales: una solicitud no condicional solo puede generar 200 OK que contenga la respuesta completa.

Respuesta del servidor de origen	Acción
Envía la respuesta completa	El servidor de origen envía la respuesta tal cual al cliente. Si la respuesta en caché ha caducado, se actualiza.
304 no modificado	Los siguientes valores de encabezado en la respuesta 304 se fusionan con la respuesta almacenada en caché y la respuesta en caché se sirve al cliente: Tokens Date, Expires, Age, Cache-Control header Max-Age y S-Maxage
401 no autorizado; 400 solicitudes incorrectas; 405 método no permitido; 406 no aceptable; se requiere autenticación de proxy 407	La respuesta del origen se entrega tal cual al cliente. La respuesta almacenada en caché no cambia.
Cualquier otra respuesta de error, por ejemplo, 404 Not Found	La respuesta del origen se entrega tal cual al cliente. La respuesta almacenada en caché se elimina.

> **Nota:**
> El parámetro Poll Every Time trata las respuestas afectadas como no almacenables.

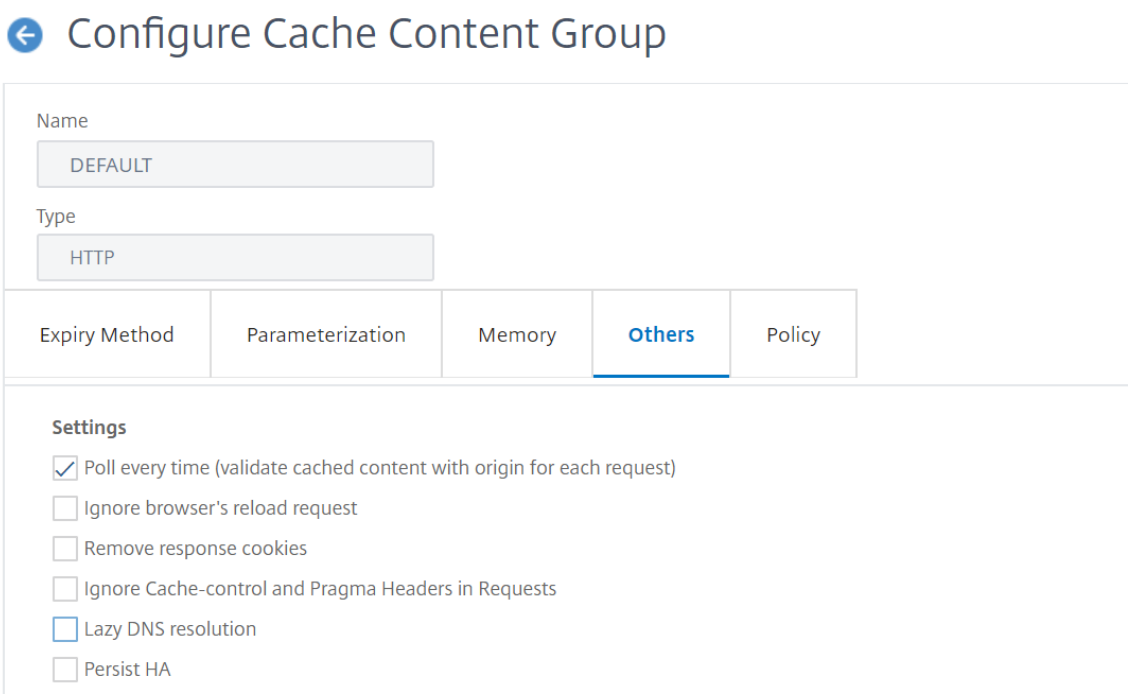
Para configurar el sondeo cada vez mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
add cache contentgroup <contentGroupName> -pollEveryTime YES
```

Encuesta mediante la interfaz gráfica de usuario

1. Vaya a **Optimización** > Almacenamiento en **caché integrado** > **Grupos de contenido**y seleccione el grupo de contenido.
2. En la ficha **Otros**, en el grupo Configuración, seleccione la opción Encuesta cada vez (validar el contenido en caché con origen para cada solicitud).



PET y contenido específico del cliente

La función PET puede garantizar que el contenido se personalice para un cliente. Por ejemplo, un sitio web que ofrece contenido en varios idiomas examina el encabezado de solicitud Accept-Language para seleccionar el idioma del contenido que publica. Para un sitio web multilingüe en el que el inglés es el idioma predominante, todo el contenido en inglés se puede almacenar en caché en un grupo de contenido PET. Esto garantiza que cada solicitud vaya al servidor de origen para determinar el idioma de la respuesta. Si la respuesta es en inglés y el contenido no ha cambiado, el servidor de origen puede entregar 304 No modificado a la memoria caché.

El siguiente ejemplo muestra comandos para almacenar en caché las respuestas en inglés en un grupo de contenido PET, configurar una expresión con nombre que identifique las respuestas en inglés en la memoria caché y configurar una directiva que utilice este grupo de contenido y la expresión con nombre. Bold se usa para enfatizar:

```
1 add cache contentgroup EnglishLanguageGroup -pollEveryTime YES
2 add expression containsENExpression  - rule ”http.res.header(\\”Content-
     Language\\”).contains(\\”en\\”)”
3 add cache policy englishPolicy -rule containsENExpression -action CACHE
      -storeInGroup englishLanguageGroup
4 bind cache policy englishPolicy -priority 100 -precedeDefRules NO
5 <!--NeedCopy-->
```


PET y autenticación, autorización y auditoría

Outlook Web Access (OWA) es un buen ejemplo de contenido generado dinámicamente que se beneficia del PET. Todas las respuestas de correo (objetos *.EML) tienen un validador `ETag` que permite que se almacenen como respuestas PET.

Cada solicitud de respuesta de correo se dirige al servidor de origen, incluso si la respuesta se almacena en caché. El servidor de origen determina si el solicitante está autenticado y autorizado. También verifica que la respuesta exista en el servidor de origen. Si todos los resultados son positivos, el servidor de origen envía una respuesta 304 No modificada.

Configurar la caché integrada como proxy de reenvío

January 12, 2021

La caché integrada puede funcionar como un dispositivo proxy de reenvío que transfiere solicitudes a otros dispositivos Citrix ADC o a otros tipos de servidores de caché. La caché integrada se configura como un proxy de reenvío identificando las direcciones IP del servidor o servidores de caché. Después de configurar el proxy de reenvío, el dispositivo Citrix ADC envía solicitudes que contienen la dirección IP configurada al servidor de caché en lugar de involucrar a la caché integrada.

Para configurar Citrix ADC como proxy de caché de reenvío mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
add cache forwardProxy <IPAddress> <port>
```

Para configurar Citrix ADC como proxy de caché de reenvío mediante la interfaz gráfica de usuario

1. Vaya a **Optimización** > Almacenamiento en **caché integrado** > **Proxy de reenvío** y agregue un proxy de reenvío especificando la dirección IP y el número de puerto.

Configuración predeterminada para la caché integrada

August 20, 2021

La función de caché integrada de Citrix ADC proporciona directivas integradas con la configuración predeterminada y la configuración inicial para el grupo de contenido predeterminado. La información de esta sección define los parámetros para las directivas integradas y el grupo de contenido predeterminado.

Directivas predeterminadas de almacenamiento en caché

La caché integrada tiene directivas integradas. El dispositivo Citrix ADC evalúa las directivas en un orden determinado, como se explica en las secciones siguientes.

Puede reemplazar estas directivas integradas con una directiva definida por el usuario vinculada a un banco de directivas de sustitución de tiempo de solicitud o sustitución de tiempo de respuesta.

> **Nota**
> Si configuró directivas antes de la versión 9.0 y especificó el parámetro -precedeDefRules al enlazar las directivas, se asignan automáticamente a los puntos de enlace de tiempo de anulación durante la migración.

Ver directivas predeterminadas

Los nombres de directiva integrados comienzan con un guión bajo (_). Puede ver las directivas integradas desde la línea de comandos y la consola administrativa mediante el comando show cache policy.

Directivas de solicitud predeterminadas

Puede reemplazar las siguientes directivas integradas de tiempo de solicitud configurando nuevas directivas y vinculándolas al punto de procesamiento de anulación de tiempo de solicitud. En las directivas siguientes, tenga en cuenta que la acción MAY_NOCACHE estipula que la transacción se almacena en caché solo cuando hay una directiva CACHE configurada por el usuario o integrada en el tiempo de respuesta.

Las siguientes directivas están enlazadas a la etiqueta de directiva _ReqBuiltInDefaults. Se enumeran en orden de prioridad.

No almacenar en caché una respuesta para una solicitud que utiliza cualquier método que no sea GET.

El nombre de la directiva es _NongeTreq. La siguiente es la regla de directiva:

```
!HTTP.REQ.METHOD.eq(GET)
```

Establezca una acción NOCACHE para una solicitud con valor de encabezado que contenga If-Match o If-Unmodified-Since.

El nombre de la directiva es _AdvancedConditionalReq. La siguiente es la regla de directiva:

```
HTTP.REQ.HEADER("If-Match").EXISTS || HTTP.REQ.HEADER("If-Unmodified-Since"
).EXISTS
```

Establezca una acción MAY_NOCACHE para una solicitud con los siguientes valores de encabezado: Cookie, Autorización, Proxy-Authorization o una solicitud que contenga el encabezado NTLM o Negotiate.

El nombre de la directiva es _PersonalizeReq. La siguiente es la regla de directiva:

```
HTTP.REQ.HEADER("Cookie").EXISTS || HTTP.REQ.HEADER("Authorization").EXISTS
 || HTTP.REQ.HEADER("Proxy-Authorization").EXISTS || HTTP.REQ.IS_NTLM_OR_NEGOTIATE
```

Directivas de respuesta predeterminadas

Puede reemplazar las siguientes directivas predeterminadas de tiempo de respuesta configurando nuevas directivas y vinculándolas al punto de procesamiento de anulación de tiempo de respuesta.

Las siguientes directivas están enlazadas a la etiqueta de directiva **_ResBuiltInDefaults** y se evalúan en el orden en que se enumeran:

1. No almacene en caché las respuestas HTTP a menos que sean de tipo 200, 304, 307, 203 o si los tipos están entre 400 y 499 o entre 300 y 302.

   El nombre de la directiva es **_UncacheableStatusRes**. La siguiente es la regla de directiva:

   ```
   !((HTTP.RES.STATUS.EQ(200))|| (HTTP.RES.STATUS.EQ(304))|| (HTTP.RES.
   STATUS.BETWEEN(400,499))|| (HTTP.RES.STATUS.BETWEEN(300, 302))|| (HTTP.
   RES.STATUS.EQ(307))|| (HTTP.RES.STATUS.EQ(203)))
   ```

2. No almacene en caché una respuesta HTTP si tiene un encabezado Vary con un valor distinto de Accept-Encoding.

   El módulo de compresión inserta el encabezado Vary: Accept_Encoding. El nombre de esta expresión es **_UncacheaLevaryRes**. La siguiente es la regla de directiva:

   ```
   ((HTTP.RES.HEADER("Vary").EXISTS)&& ((HTTP.RES.HEADER("Vary").INSTANCE
   (1).LENGTH > 0)|| (!HTTP.RES.HEADER("Vary").STRIP_END\\_WS.SET_TEXT_MODE
   (IGNORECASE).eq("Accept-Encoding"))))
   ```

3. No almacene en caché una respuesta si su valor de encabezado Cache-Control es No-Cache, No-Store o Private, o si el encabezado Cache-Control no es válido.

   El nombre de la directiva es **_UncacheableCacheControlres**. La siguiente es la regla de directiva:

   ```
   ((HTTP.RES.CACHE\\_CONTROL.IS\\_PRIVATE)|| (HTTP.RES.CACHE\\_CONTROL.IS
   \\_NO\\_CACHE)|| (HTTP.RES.CACHE\\_CONTROL.IS\\_NO\\_STORE)|| (HTTP.RES
   .CACHE\\_CONTROL.IS\\_INVALID))
   ```

4. Responde en caché si el encabezado Cache-Control tiene uno de los siguientes valores: Public, Debe-Revalidate, Proxy-Revalidate, MaxAge, S-Maxage.

   El nombre de la directiva es **_cacheableCacheControlres**. La siguiente es la regla de directiva:


```
((HTTP.RES.CACHE_CONTROL.IS_PUBLIC)|| (HTTP.RES.CACHE_CONTROL.IS_MAX_AGE
)|| (HTTP.RES.CACHE_CONTROL.IS_MUST_REVALIDATE)|| (HTTP.RES.CACHE_CONTROL
.IS_PROXY_REVALIDATE)|| (HTTP.RES.CACHE_CONTROL.IS_S_MAXAGE))
```

5. No almacenar en caché las respuestas que contengan un encabezado de Pragma.

   El nombre de la directiva es **_UncacheablePragmares**. La siguiente es la regla de directiva:

   ```
   HTTP.RES.HEADER("Pragma").EXISTS
   ```

6. Respuestas de caché que contienen un encabezado Expira.

   El nombre de la directiva es **_cacheableExpiryRes**. La siguiente es la regla de directiva:

   ```
   HTTP.RES.HEADER("Expires").EXISTS
   ```

7. Si la respuesta contiene un encabezado Content-Type con un valor de Image, elimine las cookies del encabezado y almacene en caché.

   El nombre de la directiva es **_Imageres**. La siguiente es la regla de directiva:

   ```
   HTTP.RES.HEADER("Content-Type").SET_TEXT_MODE(IGNORECASE).STARTSWITH("
   image/")
   ```

   Puede configurar el siguiente grupo de contenido para que funcione con esta directiva:

   ```
   add cache contentgroup nocookie -group -removeCookies YES
   ```

8. No almacene en caché una respuesta que contenga un encabezado Set-Cookie.

   El nombre de la directiva es **_ PersonalizeDRES**. La siguiente es la regla de directiva:

HTTP.RES.HEADER (“Set-Cookie”) .EXISTS	HTTP.RES.HEADER(“Set-Cookie2”).EXISTS

Restricciones a las directivas predeterminadas

No puede reemplazar las siguientes directivas integradas de tiempo de solicitud con directivas definidas por el usuario.

Estas directivas se enumeran en orden de prioridad.

1. No almacene en caché ninguna respuesta si la solicitud HTTP correspondiente carece de un método GET o POST.
2. No almacene en caché ninguna respuesta para una solicitud si la longitud de la URL de la solicitud HTTP más el nombre de host supera los 1744 bytes.
3. No almacenar en caché una respuesta para una solicitud que contiene un encabezado If-Match.
4. No almacene en caché una solicitud que contenga un encabezado If-Unmodified-Since.

> **Nota**
> Esto es diferente del encabezado If-Modified-Since.

1. No almacene en caché una respuesta si el servidor no establece un encabezado de caducidad.

No puede reemplazar las siguientes directivas integradas de tiempo de respuesta. Estas directivas se evalúan en el orden en que se enumeran:

1. No almacene en caché las respuestas que tengan un código de estado de respuesta HTTP 201, 202, 204, 205 o 206.
2. No almacene en caché las respuestas que tengan un código de estado de respuesta HTTP 4xx, con las excepciones de los códigos de estado 403, 404 y 410.
3. No almacene las respuestas si el tipo de respuesta es FIN terminado o la respuesta no tiene uno de los siguientes atributos: Content-Length o Transfer-Encoding: Chunked.
4. No almacene en caché la respuesta si el módulo de almacenamiento en caché no puede analizar su encabezado Cache-Control.

Configuración inicial del grupo de contenido predeterminado

Cuando habilita por primera vez el almacenamiento en caché integrado, el dispositivo Citrix ADC proporciona un grupo de contenido predefinido denominado grupo de contenido predeterminado. Para obtener información detallada, consulte Tabla Configuración de grupo de contenido predeterminada
.

Solucionar problemas

August 20, 2021

Si la función de caché integrada no funciona como se esperaba después de configurarla, puede utilizar algunas herramientas comunes para acceder a los recursos de Citrix ADC y diagnosticar el problema.

Recursos para solucionar problemas

Para obtener más información sobre los recursos disponibles para la solución de problemas y configuraciones de ejemplo, consulte Recurso para solucionar problemas del archivo PDF.

Optimización de front-end

August 20, 2021

> **Nota:** La optimización de front-end está disponible si tiene una licencia Advanced o Premium Citrix ADC y está ejecutando Citrix ADC versión 10.5 o posterior.

Los protocolos HTTP que subyacen a las aplicaciones web se desarrollaron originalmente para admitir la transmisión y representación de páginas web simples. Las nuevas tecnologías, como JavaScript y hojas de estilo en cascada (CSS), y los nuevos tipos de medios, como los vídeos Flash y las imágenes ricas en gráficos, imponen grandes exigencias al rendimiento front-end, es decir, al rendimiento a nivel del explorador.

La función de optimización de front-end (FEO) de Citrix ADC soluciona estos problemas y reduce el tiempo de carga y el tiempo de procesamiento de las páginas web al:

- Reducir el número de solicitudes.
- Necesario para representar cada página.
- Reducir el número de bytes en las respuestas de página.

Simplificar y optimizar el contenido servido al explorador del cliente.

Puede personalizar su configuración de FEO para proporcionar los mejores resultados a sus usuarios. Los ADC de Citrix admiten numerosas optimizaciones de contenido web para usuarios de escritorio y móviles. En las tablas siguientes se describen las optimizaciones front-end proporcionadas por la función FEO y las operaciones realizadas en diferentes tipos de archivos.

Optimización realizada por la función FEO

Optimización web	Problema	Qué hace la función Citrix ADC FEO	Ventajas
Inlineado	Los exploradores web cliente a menudo envían varias solicitudes a los servidores para cargar CSS externos, imágenes y JavaScript asociados con la página web.	CSS en línea, JavaScript en línea, CSS combine	Cargar el CSS externo, las imágenes y JavaScript en línea con los archivos HTML mejora el tiempo de representación de la página. Esta optimización es beneficiosa para el contenido que se visualiza una sola vez y para dispositivos móviles con tamaños de caché limitados.

Optimización web	Problema	Qué hace la función Citrix ADC FEO	Ventajas
Minificación	Los datos obtenidos de los servidores incluyen caracteres no esenciales como espacios en blanco, comentarios y caracteres de nueva línea. El tiempo que los exploradores dedican a procesar dichos datos crea latencia en el sitio web.	Minificación de CSS, minificación de JavaScript, eliminación de comentarios HTML	Los archivos minificados consumen menos ancho de banda y evitan la latencia causada por el procesamiento especial.
Optimización de imágenes	Los exploradores móviles a menudo tienen velocidades de conexión lentas y memoria caché limitada. La descarga de imágenes en clientes móviles consume más ancho de banda, tiempo de procesamiento y espacio en caché, lo que genera latencia del sitio web.	Optimización JPEG, inlineación de imágenes CSS, atributos de **reducción de imagen**, conversión de GIF a PNG, inlineación de imágenes HTML, conversión de imágenes WebP, JPEG, GIF, conversión de imágenes PNG a JPEG-XR	Reduce la imagen al tamaño indicado en la etiqueta de imagen por Citrix ADC, lo que permite a los exploradores web cliente cargar imágenes más rápido.

Optimización web	Problema	Qué hace la función Citrix ADC FEO	Ventajas
Reposicionar	El procesamiento ineficiente de CSS externo, imágenes y JavaScript aumenta el tiempo de carga de páginas.	Carga diferida de la imagen, CSS se mueve a Head, JavaScript se mueve a fin	Cambia la posición de los elementos HTML, para reducir el tiempo de representación de las páginas web y permitir que los exploradores web cliente carguen los objetos más rápidamente.
Administración de conexiones	Muchos exploradores establecen límites en el número de conexiones simultáneas que se pueden establecer a un solo dominio. Esto puede hacer que los exploradores descarguen recursos de páginas web de uno en uno, lo que da como resultado un mayor tiempo de navegación.	Fragmentos de dominio	Supera la limitación de conexión, lo que mejora el tiempo de representación de páginas al permitir que los exploradores cliente descarguen más recursos en paralelo.

Optimizaciones web en diferentes tipos de archivos:

Citrix ADC puede realizar optimizaciones web en CSS, imágenes, Javascript y HTML. Para obtener más información, consulte Optimizaciones web PDF.

> **Nota:**
> La función de optimización front-end solo admite caracteres ASCII. No es compatible con el juego de caracteres Unicode.

Cómo funciona la optimización de front-end

Después de que Citrix ADC reciba la respuesta del servidor:

1. Analiza el contenido de la página, crea una entrada en la caché (donde corresponda) y aplica la directiva FEO.

   Por ejemplo, un dispositivo Citrix ADC puede aplicar las siguientes reglas de optimización:

   - Eliminar espacios en blanco o comentarios presentes dentro de un CSS o JavaScript.
   - Combine uno o más archivos CSS en un archivo.
   - Convertir formato de imagen GIF a formato PNG.

2. Vuelve a escribir los objetos incrustados y guarda el contenido optimizado en la caché, con una firma diferente a la utilizada para la entrada de caché inicial.
3. Para solicitudes posteriores, recupera los objetos optimizados de la caché, no del servidor, y reenvía las respuestas al cliente.

**

Elimine información extraña, como espacios en blanco y comentarios.

Período durante el cual el explorador puede usar el recurso almacenado en caché sin comprobar si el contenido nuevo está disponible en el servidor.

Configurar la optimización de front-end

Opcionalmente, puede cambiar los valores de la configuración global de optimización de front-end. De lo contrario, comience creando acciones que especifiquen las reglas de optimización que se aplicarán a los objetos incrustados.

Después de configurar las acciones, cree directivas, cada una con una regla que especifique un tipo de solicitud para la que optimizar la respuesta y asocie las acciones con las directivas.

> **Nota:** Citrix ADC evalúa las directivas de optimización front-end solo en el momento de la solicitud, no en el momento de la respuesta.

Para poner en práctica las directivas, vincularlas a puntos de enlace. Puede enlazar una directiva globalmente, de modo que se aplique a todo el tráfico que fluye a través del Citrix ADC, o bien puede enlazar la directiva a un servidor virtual de equilibrio de carga o cambio de contenido de tipo HTTP o SSL. Cuando vincule una directiva, asígnele una prioridad. Un número de prioridad inferior indica un valor mayor. El Citrix ADC aplica las directivas en el orden de sus prioridades.

Requisitos previos

La optimización de front-end requiere que se habilite la función de almacenamiento en caché integrado de Citrix ADC. Además, debe realizar las siguientes configuraciones integradas de almacenamiento en caché:

- Asignar memoria caché.

- Establezca el tamaño máximo de respuesta y el límite de memoria para un grupo de contenido de caché predeterminado.

Para obtener más información sobre la configuración del almacenamiento en caché integrado, consulte Almacenamiento en caché integrado.

Nota: El término Caché Integrado se puede utilizar indistintamente con AppCache; tenga en cuenta que desde el punto de vista de la funcionalidad, ambos términos significan lo mismo.

Configurar la optimización de front-end mediante la interfaz de comandos de Citrix ADC

En el símbolo del sistema, haga lo siguiente:

1. Habilite la función de optimización de front-end.

```
enable ns feature FEO
```

1. Cree una o más acciones de optimización front-end.

```
add feo action <name> [-imgShrinkToAttrib] [-imgGifToPng] ...
```

Ejemplo: Para agregar una acción de optimización front-end para convertir imágenes en formato GIF a formato PNG y extender el período de caducidad de la caché:

```
add feo action allact -imgGifToPng -pageExtendCache
```

1. [Opcional] Especifique valores no predeterminados para la configuración global de optimización de front-end.

```
set feo parameter [-cacheMaxage <integer>] [-JpegQualityPercent <integer>]
[-cssInlineThresSize <integer>] [-inlineJsThresSize <integer> [-inlineImgThresSize
 <integer>]
```

Ejemplo: Para especificar el período máximo de caducidad de la caché:

```
set feo parameter -cacheMaxage 10
```

1. Cree una o varias directivas de optimización de front-end.

```
add feo policy <name> <rule> <action>
```

Ejemplo: Para agregar una directiva de optimización de front-end y asociarla con la acción allact especificada anteriormente:

```
1 >add feo policy pol1 TRUE all act
2 >add feo policy pol1 ”(HTTP.REQ.URL.CONTAINS(”testsite”))” allact1
3 <!--NeedCopy-->
```


1. Enlazar la directiva a un servidor virtual de equilibrio de carga o conmutación de contenido, o vincularla globalmente.

```
bind lb vserver <name> -policyName <string> -priority <num>

bind cs vserver <name> -policyName <string> -priority <num>

bind feo global <policyName> <priority> -type <type> <gotoPriorityExpression
>
```

Ejemplo: Para aplicar la directiva de optimización front-end a un servidor virtual denominado “abc”:

```
> bind lb vserver abc -policyName pol1 -priority 1 -type NONE
```

Ejemplo: Para aplicar la directiva de optimización de front-end para todo el tráfico que llega al ADC:

```
> bind feo global pol1 100 -type REQ_DEFAULT
```

1. Guarde la configuración. save ns config

Configure la optimización de front-end mediante la interfaz gráfica de usuario

1. Vaya a **Optimización** > **Optimización front-end** > **Acciones**y haga clic en **Agregar** y cree una acción de optimización front-end especificando los detalles relevantes.
2. [Opcional] Especifique la configuración global de optimización de front-end.
3. Vaya a **Optimización** > **Optimización de front-end** y, en el panel derecho, en Configuración, haga clic en **Cambiar configuración de optimización de front-end** y especifique la configuración global de optimización de front-end.
4. Cree una directiva de optimización front-end.
5. Vaya a **Optimización** > **Optimización de front-end** > **Directivas**, haga clic en **Agregar** y cree una directiva de optimización de front-end especificando los detalles pertinentes.
6. Enlazar la directiva a un servidor virtual de equilibrio de carga o cambio de contenido.
   a) Vaya a **Optimización** > **Optimización front-end** > **Directivas**.
   b) Seleccione una directiva de optimización front-end y haga clic en **Administrador de directivas**.
   c) En **Front End Optimization Policy Manager**, vincule la directiva de optimización front-end a un servidor virtual de equilibrio de carga o conmutación de contenido.

Verificar la configuración de optimización de front-end

La utilidad de panel muestra estadísticas detalladas y de resumen en formatos tabulares y gráficos. Puede ver las estadísticas de FEO para evaluar su configuración de FEO.

Si lo quiere, también puede mostrar estadísticas de una directiva de FEO, incluido el número de selección que el contador de directivas incrementa durante el FEO basado en directivas.

> **Nota:**
> Para obtener más información acerca de las estadísticas y los gráficos, consulte la ayuda del panel del dispositivo Citrix ADC.

Ver las estadísticas de FEO mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para mostrar un resumen de las estadísticas de FEO, selección y detalles de la directiva de FEO, y estadísticas detalladas de FEO, respectivamente:

- `stat feo` Nota: El comando stat feo policy muestra estadísticas solo para las directivas avanzadas de FEO.
- `show feo policy name`
- `stat feo -detail`

Ver las estadísticas de FEO en el panel de Citrix ADC

En la interfaz gráfica de usuario del panel, puede:

- Seleccione Optimización de Front End para mostrar un resumen de `FEO` las estadísticas.
- Haga clic en la ficha **Vista gráfica** para mostrar la tasa de solicitudes procesadas por la función FEO.

Optimización de ejemplo:

Consulte el PDF de ejemplo para obtener algunos ejemplos de acciones de optimización de contenido que se aplican al contenido HTML y a los objetos incrustados dentro del contenido HTML.

Acelerador de contenido

August 20, 2021

> **Importante:**
>
> La función Acelerador de contenido ya no es compatible con el dispositivo Citrix ADC.

El acelerador de contenido es una función de Citrix ADC que puede utilizar en una implementación de Citrix ByteMobile T1100 para almacenar datos en un dispositivo Citrix ByteMobile T2100.

El almacenamiento de datos en un dispositivo T2100 ahorra ancho de banda y proporciona tiempos de respuesta más rápidos, ya que Citrix ADC no tiene que conectarse al servidor para solicitudes repetidas de los mismos datos.

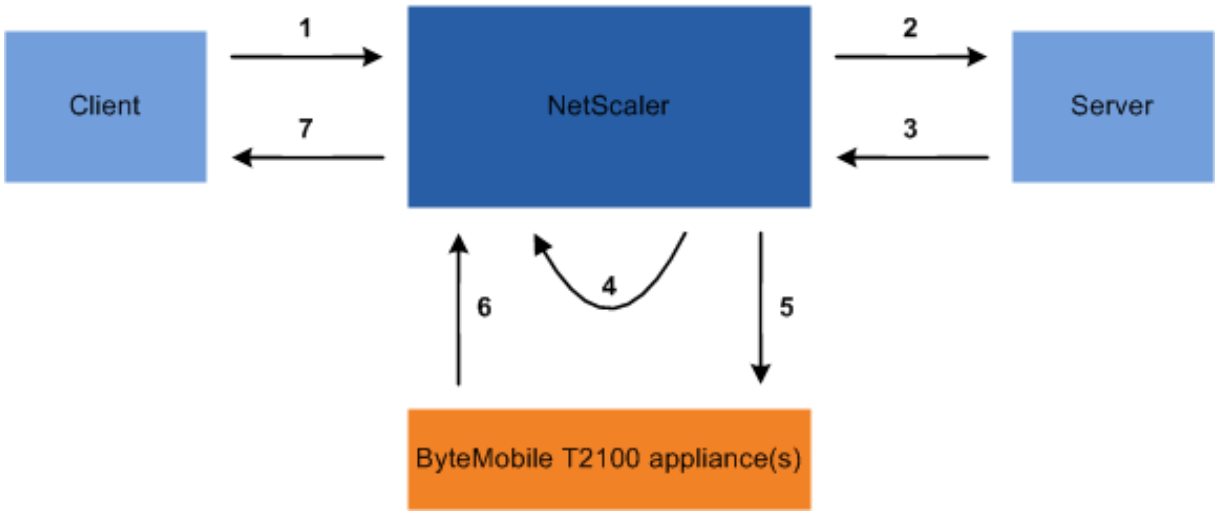
> **Nota:** El acelerador de contenido funciona con una licencia de Citrix ByteMobile Premium. Póngase en contacto con el servicio de atención al cliente para obtener más información y obtener la licencia.

Cómo funciona el acelerador de contenido

Cuando un servidor virtual de equilibrio de carga o cambio de contenido recibe una solicitud de cliente, el dispositivo Citrix ADC evalúa una directiva de acelerador de contenido enlazada al servidor virtual. La directiva filtra las solicitudes para identificar las a las que se va a aplicar la función Acelerador de contenido.

> **Nota:**
>
> Para las solicitudes HTTP, la función acelerador de contenido puede servir contenido parcial en respuesta a solicitudes de rango de byte único.

La siguiente ilustración ilustra las operaciones que realiza el dispositivo cuando una solicitud de cliente llega a un servidor virtual configurado para utilizar la función Acelerador de contenido:



El flujo del proceso es el siguiente:

1. El cliente envía la solicitud.
2. Citrix ADC reenvía la solicitud al servidor.
3. El servidor responde con el tamaño predefinido de la respuesta (especificado por el parámetro AccumResSize del comando add ca action).
4. Citrix ADC calcula un hash de la respuesta enviada por el servidor.
5. Citrix ADC busca el hash en el dispositivo T2100.
6. Una búsqueda correcta indica que los datos están disponibles y que el dispositivo T2100 los envía al Citrix ADC.

> **Nota:**
> Cuando la búsqueda de la base de datos no se realiza correctamente, el dispositivo obtiene los datos solicitados del servidor, envía los datos al cliente y actualiza los datos en el dispositivo T2100.
> El dispositivo T2100 se puede configurar para especificar el número de solicitudes para las que se van a almacenar en caché los datos.

7. Citrix ADC envía la respuesta al cliente.

Configurar acelerador de contenido

Antes de configurar la función del acelerador de contenido, debe habilitarla en el dispositivo Citrix ADC.

Debe configurar la función de acelerador de contenido para utilizar uno o varios dispositivos T2100. Debe agregar cada dispositivo T2100 como servicio y enlazar estos servicios a un servidor virtual de equilibrio de carga dedicado a distribuir la carga entre los dispositivos T2100 configurados.

Debe configurar una acción del acelerador de contenido para buscar los datos en el dispositivo T2100. La acción debe especificar el servidor virtual de equilibrio de carga T2100 y el tamaño de los datos (en KB) que se van a obtener del servidor para calcular el hash.

La acción debe estar enlazada a una directiva de aceleración de contenido que defina el tráfico en el que se va a realizar la aceleración de contenido. La directiva del acelerador de contenido debe estar enlazada a un servidor virtual de conmutación de contenido o equilibrio de carga que reciba tráfico de cliente. Alternativamente, puede enlazar la directiva globalmente a todos los servidores virtuales aplicables.

Para configurar el acelerador de contenido mediante la interfaz de línea de comandos

En el símbolo del sistema, haga lo siguiente:

1. Habilite la función Acelerador de contenido.

   ```
   enable ns feature ca
   ```

2. Identifique los dispositivos T2100 y agregue cada uno como un servicio en el dispositivo Citrix ADC.

   ```
   add service <name> <IPAddress> <serviceType> <port>
   ```

   Ejemplo:

```
1 > add service T2100-A 10.102.29.61 HTTP 30
2 > add service T2100-B 10.102.29.62 HTTP 40
3 > add service T2100-C 10.102.29.63 HTTP 50
```



```
4 <!--NeedCopy-->
```

> **Nota:**
> Los servicios deben ser de tipo HTTP solamente.

3. Cree un servidor virtual de equilibrio de carga para los dispositivos T2100. Especifique el método de equilibrio de carga del token y la regla que se muestra en la siguiente sintaxis.

```
1 add lb vserver <name> <serviceType> <IPAddress> <port> -lbMethod
     TOKEN -rule "http.req.url.after_str("/lookup/") alt http.req.
     url.path.SKIP(1).PREFIX(64)"
2 <!--NeedCopy-->
```

Ejemplo:

```
1 add lb vserver T2100-lbvserver HTTP 10.102.29.64 99 -lbMethod
     TOKEN -rule "http.req.url.after_str("/lookup/") alt http.req.
     url.path.SKIP(1).PREFIX(64)"
2 <!--NeedCopy-->
```

4. Enlazar los servicios T2100 al servidor virtual de equilibrio de carga que creó para ellos.

```
bind lb vserver <name> <serviceName>
```

Ejemplo:

```
1 > bind lb vserver T2100-lbvserver T2100-A
2 > bind lb vserver T2100-lbvserver T2100-B
3 > bind lb vserver T2100-lbvserver T2100-C
4 <!--NeedCopy-->
```

5. Defina una acción de aceleración de contenido.

```
add ca action <name> accumResSize <KBytes> -lbvserver <string> -type
lookup
```

Ejemplo:

```
> add ca action ca_action1 -type lookup -lbvserver T2100-lbvserver -
accumResSize 60
```

6. Defina una directiva de acelerador de contenido.


```
add ca policy <name> -rule <expression> -action <name>
```

Ejemplo:

Para crear una directiva de acelerador de contenido que almacena en caché todos los formatos de vídeo.

```
> add ca policy ca_mp4_pol -rule ns_video -action ca_action1
```

donde ns_vídeo es una expresión incorporada.

7. Enlazar la directiva del acelerador de contenido a un servidor virtual que recibe tráfico o globalmente al sistema Citrix ADC.

```
bind lb vserver <name> -policyName <string>
```

```
bind cs vserver <name> -policyName <string>
```

```
bind ca global -policyName <string> -priority <num> -type <type>
```

Ejemplo: Para aplicar la directiva del acelerador de contenido a un servidor virtual denominado "traf_rec"

```
bind lb vserver traf_rec -policyName ca_mp4_pol
```

Ejemplo: Para aplicar la directiva del acelerador de contenido a todo el tráfico que llega al Citrix ADC.

```
bind ca global -policyName ca_mp4_pol -priority 100 -type RES_DEFAULT
```

8. Guarde la configuración.

```
save ns config
```

Configuración del acelerador de contenido mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **Configuración** > **Configurar funciones avanzadas** y seleccione **Acelerador de contenido**.
2. Cree un servicio para cada uno de los dispositivos T2100.
   a) Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servicios**.
   b) Haga clic en **Agregar** y especifique los detalles pertinentes. En el campo **Servidor**, asegúrese de especificar la dirección IP del dispositivo T2100. En el campo **Protocolo**, seleccione HTTP.
3. Cree un servidor virtual y vincule los servicios T2100 a él.
   a) Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**.
   b) Haga clic en **Agregar** y especifique los detalles pertinentes.
   c) En la ficha **Método y persistencia**, especifique el método como **token**.
   d) En la ficha **Directivas**, especifique la regla como http.req.url.after_str ("/lookup/") alt http.req.url.path.skip (1) .PREFIX (64).
   e) En la ficha **Servicios**, seleccione los servicios T2100 que quiere vincular al servidor virtual.

4. Cree una acción de acelerador de contenido.
   a) Vaya a **Optimización** > **Acelerador de contenido** > **Acciones**.
   b) Especifique los detalles pertinentes.
5. Cree una directiva de acelerador de contenido.
   a) Vaya a **Optimización** > **Acelerador de contenido** > **Directivas**.
   b) Haga clic en **Agregar**, especifique la regla de directiva y asocie la acción del acelerador de contenido.
6. Enlazar la directiva del acelerador de contenido globalmente o a un servidor virtual.
   a) Vaya a **Optimización** > **Acelerador de contenido**.
   b) En las secciones de **Content Accelerator Policy Manager** [REQUEST] o Content Accelerator Policy Manager [RESPONSE], vincule la directiva del acelerador de contenido globalmente o a un servidor virtual.

Clasificación de medios

August 20, 2021

Comprender el tipo de tráfico en la red ayuda a los administradores de red a administrar el consumo de ancho de banda para un rendimiento óptimo de la red. El modo de clasificación de medios supervisa y muestra las estadísticas del tráfico de medios que pasa a través del dispositivo Citrix ADC.

Con este modo habilitado, un administrador de red puede recopilar estadísticas que muestren la cantidad de datos a los que se accede y los tipos de dispositivos desde los que se ha accedido a los archivos multimedia. El dispositivo Citrix ADC también admite solicitudes de intervalo de bytes en este modo.

Actualmente, el dispositivo Citrix ADC puede supervisar y mostrar estadísticas de los siguientes tipos de archivos multimedia:

Multimedia	Tipo de archivo
Transmisión fluida de Microsoft	Vídeo
Transmisión en vivo de Apple	Vídeo
Transmisión de transporte de datos de audio (ADTS)	Sonido
Codificación avanzada de audio (AAC)	Sonido
Vídeo Flash (FLV)	Audio y Vídeo
3GP	Audio y Vídeo

El dispositivo puede mostrar estadísticas para los siguientes dispositivos:

Plataforma del dispositivo	Tipo de dispositivo
iOS	iPad e iPod
Android	Móviles y tabletas
Equipo portátil o de escritorio	Equipos portátiles y de escritorio con Windows
Otros	Otros dispositivos móviles (móviles y tabletas)

Los administradores de red pueden comprobar los siguientes contadores de estadísticas para conocer la cantidad de datos a los que se accede a través del dispositivo Citrix ADC para varios tipos de tráfico de medios.

Nombre de archivo multimedia	Contador de estadísticas
Transmisión fluida de Microsoft	`mcmssmthstrmvid`: este contador registra el número total de vídeos de Microsoft Smooth Streaming servidos por el dispositivo Citrix ADC;`Mcmssmthstrvidpl`—Este contador registra el número total de listas de reproducción de vídeo de Microsoft Smooth Streaming servidas por el dispositivo Citrix ADC;`Mcmssmthstrmvidbytes`—Este contador registra el número total de bytes de datos servidos para el tráfico multimedia de Microsoft Smooth Streaming en el dispositivo Citrix ADC;`Mcmssmthstrmplvidbytespl`: este contador registra el número total de bytes de lista de reproducción de Microsoft Smooth Streaming servidos por el dispositivo Citrix ADC.

Nombre de archivo multimedia	Contador de estadísticas
Transmisión en vivo de Apple	mccaplelivestrmngvid: este contador registra el número total de vídeos de Apple Live Streaming que ofrece el dispositivo Citrix ADC.Mccapplelivestrmngvidpl—Este contador registra el número total de listas de reproducción de vídeo de Apple Live Streaming servidas por el dispositivo Citrix ADC.Mcapplelivestreamingvidbytes: este contador registra el número total de bytes de datos servidos para el tráfico multimedia de Apple Live Streaming en el dispositivo Citrix ADC.Mcapplelivestreamingplaylistvidbytespl: este contador registra el número total de bytes de lista de reproducción de Apple Live servidos por el dispositivo Citrix ADC.
Transmisión de transporte de datos de audio (ADTS)	mcadtsaudio: este contador registra el número total de clips de audio ADTS servidos por el dispositivo Citrix ADC.Mcadtsaudiobytes: este contador registra el número total de bytes de datos servidos para el tráfico multimedia ADTS en el dispositivo Citrix ADC.
Codificación avanzada de audio (AAC)	Mcaacaudio: este contador registra el número total de clips de audio AAC servidos por el dispositivo Citrix ADC.Mcaacaudiobytes: este contador registra el número total de bytes de datos servidos para el tráfico de medios AAC en el dispositivo Citrix ADC.
Vídeo Flash (FLV)	Mcflvvid: este contador registra el número total de vídeos flash que ofrece el dispositivo Citrix ADC.Mcflvvidbytes: este contador registra el número total de bytes de datos servidos para vídeos flash en el dispositivo Citrix ADC.

Nombre de archivo multimedia	Contador de estadísticas
3GP	`mc3gpvidbytes`: este contador registra el número total de bytes de datos servidos para el tráfico multimedia 3GP en el dispositivo Citrix ADC.

El dispositivo Citrix ADC detecta los tipos de archivos multimedia mediante sus firmas en los *bytes iniciales del cuerpo* de las respuestas. Por ejemplo, los bytes de cuerpo iniciales de un archivo mp4 tienen la siguiente firma en la respuesta:

```
**....ftypmp42** ....isommp42....moov...lmvhd.....c.\!.c.\!..
```

El dispositivo Citrix ADC detecta el tipo de dispositivo cliente mediante la *cadena de agente de usuario* que el dispositivo cliente incluye en la solicitud HTTP GET. Por ejemplo, un teléfono de ventana que utiliza un explorador de UC tiene la siguiente cadena de agente de usuario en la solicitud HTTP GET:

```
User-Agent: **UCWEB**/2.0 (**Windows**; U; wds 8.10; en-US; HTC; 8X by HTC)
U2/1.0.0
```

Habilitar clasificación de medios

De forma predeterminada, la clasificación de medios está inhabilitada en el dispositivo Citrix ADC. Debe habilitar el modo antes de usarlo.

Para habilitar la clasificación de medios mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
enable ns mode Mediaclassification
```

Para habilitar la clasificación de medios mediante la interfaz gráfica de usuario

Habilitar la clasificación de medios en el dispositivo Citrix ADC

Vaya a **Sistema** > **Configuración** > **Configurar modos** y seleccione **Clasificación de medios**.

Para ver las estadísticas de tráfico de medios en el dispositivo Citrix ADC

Vaya a **Optimización** y haga clic en **Clasificación de medios** para ver las estadísticas de tráfico de medios.

Verificar estadísticas de clasificación de medios

Puede ver las estadísticas de tráfico de medios en la utilidad del panel o mediante la interfaz de línea de comandos. La utilidad de panel muestra estadísticas detalladas y de resumen en formato tabular y gráfico.

> **Nota**
> Para obtener más información acerca de estadísticas y gráficos, consulte la ayuda del Panel de control de su dispositivo Citrix ADC.

Para ver estadísticas de clasificación de medios mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba uno de los siguientes comandos para mostrar un resumen de las estadísticas de clasificación de medios, mostrar estadísticas detalladas o borrar la visualización:

```
stat Mediaclassification

stat Mediaclassification -detail

stat Mediaclassification -clearstats
```

Para ver las estadísticas de clasificación de medios en el panel

En la utilidad **Panel**, puede mostrar los siguientes tipos de estadísticas de clasificación de medios:

1. Seleccione **Clasificación de medios** para mostrar un resumen de las estadísticas de tráfico de medios.
2. Para mostrar estadísticas detalladas de tráfico de medios, haga clic en **Detalles**.
3. Para borrar las estadísticas de tráfico de medios, haga clic en **Borrar**.

Reputación

January 19, 2021

Citrix ofrece seguridad basada en la reputación. Mediante la evaluación de la reputación para determinar el riesgo de procesar solicitudes, puede realizar acciones como bloquear o descartar determinadas solicitudes para mejorar el rendimiento de la aplicación.

La función de reputación IP de Citrix ADC utiliza comprobaciones de reputación IP para evitar ataques de día cero y proporcionar protección contra fuentes malintencionadas asociadas con ataques web, actividades de phishing o análisis web.

Para obtener más información, consulte Reputación IP.

Reputación de IP

December 2, 2021

La reputación IP es una herramienta que identifica las direcciones IP que envían solicitudes no deseadas. Mediante la lista de reputación de IP puede rechazar las solicitudes que provengan de una

dirección IP con mala reputación. Optimice el rendimiento de Web Application Firewall filtrando las solicitudes que no quiere procesar. Restablecer, eliminar una solicitud o incluso configurar una directiva de respuesta para realizar una acción de respuesta específica.

A continuación se presentan algunos ataques que puede evitar mediante la reputación de IP:

- **Equipos personales infectados por virus**. (PC domésticos) son la fuente más importante de spam en Internet. La reputación IP puede identificar la dirección IP que envía solicitudes no deseadas. La reputación de IP puede ser especialmente útil para bloquear ataques DDoS, DoS o inundaciones SYN anómalas a gran escala procedentes de fuentes infectadas conocidas.
- **Botnet automatizada y administrada de forma centralizada**. Los atacantes han ganado popularidad por robar contraseñas, porque no lleva mucho tiempo cuando cientos de equipos trabajan juntos para descifrar su contraseña. Es fácil lanzar ataques de botnet para descubrir contraseñas que utilizan palabras de diccionario de uso común.
- **Servidor web comprometido**. Los ataques no son tan comunes porque el conocimiento y la seguridad del servidor han aumentado, por lo que los hackers y los spammers buscan objetivos más fáciles. Todavía hay servidores web y formularios en línea que los hackers pueden comprometer y utilizar para enviar spam (como virus y pornografía). Esta actividad es más fácil de detectar y cerrar rápidamente, o bloquear con una lista de reputación como SpamRats.
- **Exploits de Windows**. (como IP activas que ofrecen o distribuyen malware, código shell, rootkits, gusanos o virus).
- **Spammers y hackers conocidos**.
- **Campañas de marketing masivo por correo electrónico**
- **Proxies de phishing** (direcciones IP que alojan sitios de phishing y otros fraudes, como fraude de clics en anuncios o fraude de juegos).
- **Proxies anónimos** (IP que proporcionan servicios de proxy y anonimización, incluido The Onion Router, también conocido como TOR).

Un dispositivo Citrix ADC utiliza **Webroot** como proveedor de servicios de una base de datos IP maliciosa generada dinámicamente y los metadatos de esas direcciones IP. Los metadatos pueden incluir detalles de geolocalización, categoría de amenazas, recuento de amenazas, etc. El motor Webroot Threat Intelligence recibe datos en tiempo real de millones de sensores. Captura, escanea, analiza y califica los datos de forma automática y continua mediante aprendizaje automático avanzado y análisis de comportamiento. La información sobre una amenaza se actualiza continuamente.

El dispositivo Citrix ADC valida una solicitud entrante por su mala reputación mediante la base de datos de reputación de IP de Webroot. La base de datos tiene una enorme colección de categorías de amenazas IP basadas en clasificadas de direcciones IP. A continuación se presentan las categorías de amenazas de IP y su descripción.

- Fuentes de spam. Las fuentes de spam incluyen tunelización de mensajes de spam a través de proxy, actividades SMTP anómalas, actividades de spam en el foro.
- Exploits de Windows. La categoría de vulnerabilidad de Windows incluye direcciones IP activas

que ofrecen o distribuyen malware, código de shell, rootkits, gusanos o virus

- Ataques web. La categoría de ataques web incluye scripts entre sitios, inyección de iFrame, inyección SQL, inyección entre dominios o ataques de fuerza bruta de contraseña de dominio
- Botnets. La categoría de botnet incluye canales de Botnet C&C y máquina zombie infectada controlada por Bot master
- Escáneres. La categoría de escáneres incluye todos los reconocimientos, como sondas, escaneo de host, escaneo de dominio y ataque de fuerza bruta de contraseña
- Denegación de servicio. La categoría de denegación de servicios incluye DOS, DDOS, inundación de sincronización anómala, detección de tráfico anómalo
- Reputación. Denegar el acceso desde direcciones IP actualmente conocidas por estar infectadas con malware. Esta categoría también incluye IP con una puntuación media baja del Índice de Reputación de Webroot. Habilitar esta categoría impedirá el acceso desde las fuentes identificadas a los puntos de distribución de malware de contacto
- Phishing. La categoría de phishing incluye direcciones IP, sitios de phishing, otros tipos de actividades fraudulentas, como el fraude de clics en anuncios o el fraude de juegos.
- Proxy. La categoría de proxy incluye direcciones IP que proporcionan servicios de proxy y def.
- Amenazas móviles. La categoría de amenazas móviles incluye direcciones IP de aplicaciones móviles maliciosas y no deseadas. Esta categoría aprovecha los datos del equipo de investigación de amenazas móviles de Webroot.
- Proxy Tor. La categoría de proxy Tor incluye direcciones IP que actúan como nodos de salida para la red Tor. Los nodos de salida son el último punto de la cadena proxy y establecen una conexión directa con el destino previsto del remitente.

Cuando se detecta una amenaza en cualquier parte de la red, la dirección IP se marca como maliciosa y todos los dispositivos conectados a la red quedan protegidos de inmediato. Los cambios dinámicos en las direcciones IP se procesan con alta velocidad y precisión mediante el aprendizaje automático avanzado.

Como se indica en la hoja de datos de Webroot, la red de sensores de Webroot identifica muchos tipos de amenazas IP clave, incluidas las fuentes de spam, las vulnerabilidades de Windows, las botnets, los escáneres y otros. (Consulte el diagrama de flujo en la hoja de datos).

El dispositivo Citrix ADC utiliza un proceso de cliente `iprep` para obtener la base de datos de Webroot. El cliente `iprep` utiliza el método HTTP GET para obtener la lista de IP absoluta de Webroot por primera vez. Más tarde, comprueba los cambios delta una vez cada 5 minutos.

> **Importante:**
>
> - Asegúrese de que el dispositivo Citrix ADC tenga acceso a Internet y que el DNS esté configurado antes de usar la función de reputación de IP.
> - Para acceder a la base de datos de Webroot, el dispositivo Citrix ADC debe poder conectarse a **api.bcti.brightcloud.com** en el **puerto 443**. Cada nodo de la implementación de alta

> disponibilidad o clúster obtiene la base de datos de Webroot y debe poder acceder a este nombre de dominio completo (FQDN).
>
> - Webroot aloja actualmente su base de datos de reputación en AWS. Por lo tanto, Citrix ADC debe poder resolver los dominios de AWS para descargar la base de datos de reputación. Además, el firewall debe estar abierto para dominios de AWS.
>
> **Nota:**
>
> Cada motor de paquetes requiere al menos 4 GB para funcionar correctamente cuando la función de reputación IP está habilitada.

Expresiones de directivas avanzadas. Configure la función Reputación de IP mediante expresiones de directivas avanzadas (expresiones de directivas avanzadas) en las directivas enlazadas a los módulos admitidos, como Web Application Firewall y Responder. A continuación se presentan dos ejemplos que muestran expresiones que se pueden utilizar para detectar si la dirección IP del cliente es maliciosa.

1. **CLIENT.IP.SRC.IPREP_IS_MALICIOUS**: Esta expresión se evalúa como TRUE si el cliente está incluido en la lista de direcciones IP malintencionadas.
2. **CLIENT.IP.SRC.IPREP_THREAT_CATEGORY (CATEGORY)**: Esta expresión se evalúa como TRUE si la IP del cliente es una IP maliciosa y se encuentra en la categoría de amenaza especificada.
3. **CLIENT.IPV6.SRC.IPREP_IS_MALICIOUS y CLIENT.IPV6.SRC.IPREP_THREAT_CATEGORY**: Esta expresión se evalúa como TRUE si la IP del cliente es de tipo IPv6 y es una dirección IP maliciosa en una categoría de amenaza especificada.

Los siguientes son los valores posibles para la categoría de amenaza:

SPAM_SOURCES, WINDOWS_EXPLOITS, WEB_ATTACKS, BOTNETS, ESCÁNERES, DOS, REPUTACIÓN, PHISHING, PROXY, RED, CLOUD_PROVIDERS, MOBILE_THREATS, TOR_PROXY.

> **Nota:**
>
> La función de reputación IP comprueba las direcciones IP de origen y de destino. Detecta IP maliciosas en el encabezado. Si la expresión PI de una directiva puede identificar la dirección IP, la comprobación de reputación IP determina si es malintencionada.

Mensaje de registro de iPrep. El archivo `/var/log/iprep.log` contiene mensajes útiles que capturan información sobre la comunicación con la base de datos de Webroot. La información puede ser sobre las credenciales utilizadas durante la comunicación de Webroot, la falta de conexión con Webroot o la información incluida en una actualización (como el número de direcciones IP de la base de datos).

Creación de una lista de bloqueo o de permitidos de IP mediante un conjunto de datos de directivas. Puede mantener una lista de permisos para permitir el acceso a direcciones IP específicas que están bloqueadas en la base de datos de Webroot. También puede crear una lista de direcciones IP

bloqueadas personalizada para complementar la comprobación de reputación de Webroot. Estas listas se pueden crear mediante un **conjunto de datos**de directivas. Un conjunto de datos es una forma especializada de conjunto de patrones que es ideal para la coincidencia de direcciones IPv4 o IPv6. Para utilizar conjuntos de datos, primero cree el conjunto de datos y vincule las direcciones IPv4 o IPv6 a él. Al configurar una directiva para comparar una cadena de un paquete, utilice un operador adecuado y pase el nombre del conjunto de patrones o conjunto de datos como argumento.

Para crear una lista de direcciones permitidas que se tratarán como excepciones durante la evaluación de reputación de IP:

- Configure la directiva para que la expresión PI se evalúe como False aunque Webroot (o cualquier proveedor de servicios) indique una dirección de la lista de permitidos como maliciosa.

Habilitar o inhabilitar la reputación de IP. La reputación de IP forma parte de la función de reputación general, que se basa en licencias. Al habilitar o inhabilitar la función de reputación, habilita o inhabilita la reputación de IP.

Procedimiento general. La implementación de la reputación de IP implica las siguientes tareas

- Compruebe que la licencia instalada en el dispositivo Citrix ADC admite reputación IP. Las licencias de firewall de aplicaciones premium e independientes admiten la función de reputación de IP.
- Habilite las funciones de reputación de IP y firewall de aplicaciones.
- Agregue un perfil de firewall de aplicaciones.
- Agregue una directiva de firewall de aplicaciones mediante las expresiones PI para identificar las direcciones IP maliciosas en la base de datos de reputación IP.
- Enlazar la directiva de firewall de aplicaciones a un punto de enlace adecuado.
- Compruebe que cualquier solicitud recibida de una dirección maliciosa se registra en el archivo `ns.log` para mostrar que la solicitud se procesó según lo especificado en el perfil.

Configurar la función de reputación IP mediante la CLI

En el símbolo del sistema, escriba:

- `enable feature reputation`
- `disable feature reputation`

En los ejemplos siguientes se muestra cómo agregar una directiva de firewall de aplicaciones mediante la expresión PI para identificar direcciones maliciosas. Puede utilizar los perfiles integrados, agregar un perfil o configurar un perfil existente para invocar la acción deseada cuando una solicitud coincida con una directiva.

Los ejemplos 3 y 4 muestran cómo crear un conjunto de datos de directivas para generar una lista de bloqueo o una lista de direcciones IP permitidas.

Ejemplo 1:

El siguiente comando crea una directiva que identifica las direcciones IP maliciosas y bloquea la solicitud si se activa una coincidencia:

```
add appfw policy pol1 CLIENT.IP.SRC.IPREP_IS_MALICIOUS APPFW_BLOCK
add appfw policy pol1 CLIENT.IPv6.SRC.IPREP_IS_MALICIOUS APPFW_BLOCK
add appfw policy pol1 ”HTTP.REQ.HEADER(\”X-Forwarded-For\”).TYPECAST_IPv6_ADDRESS_AT
.IPREP_IS_MALICIOUS”APPFW_RESET
```

Ejemplo 2:

El siguiente comando crea una directiva que utiliza el servicio de reputación para comprobar la dirección IP del cliente en el encabezado `X-Forwarded-For` y restablecer la conexión si se activa una coincidencia.

```
> add appfw policy pol1 ”HTTP.REQ.HEADER(\”X-Forwarded-For\”).TYPECAST_IP_ADDRESS_AT
.IPREP_IS_MALICIOUS”APPFW_RESET**
```

Ejemplo 3:

En el ejemplo siguiente se muestra cómo agregar una lista para agregar excepciones que permiten direcciones IP especificadas:

```
> add policy dataset Allow_list1 ipv4

> bind policy dataset Allow_list1 10.217.25.17 -index 1

> bind policy dataset Allow_list1 10.217.25.18 -index 2
```

El siguiente ejemplo muestra cómo agregar una lista para agregar excepciones que permitan direcciones IPv6 especificadas:

```
1 add policy dataset Allow_list_ipv6 ipv6
2 bind policy dataset Allow_list_ipv6 fe80::98c7:d8ff:fe3a:b562 -index 1
3 bind policy dataset Allow_list_ipv6 fe80::98c7:d8ff:fe3a:b563  -index 2
4
5 <!--NeedCopy-->
```

Ejemplo 4:

En el siguiente ejemplo se muestra cómo agregar la lista personalizada para marcar las direcciones IP especificadas como maliciosas:

```
> add policy dataset Block_list1 ipv4

> bind policy dataset Block_list1 10.217.31.48 -index 1

> bind policy dataset Block_list1 10.217.25.19 -index 2
```


El siguiente ejemplo muestra cómo agregar la lista personalizada para marcar las direcciones IPv6 especificadas como maliciosas.

```
add policy dataset Block_list_ipv6 ipv6
bind policy dataset Block_list_ipv6 fe80::98c7:d8ff:ff3b:b562 -index 1
bind policy dataset Block_list_ipv6 fe80::ffc7:d8ff:fe3a:b562 -index 2
<!--NeedCopy-->
```

Ejemplo 5:

En el siguiente ejemplo se muestra una expresión de directiva para bloquear la IP del cliente en las siguientes condiciones:

- Coincide con una dirección IP configurada en la lista Block_list1 personalizada (ejemplo 4)
- Coincide con una dirección IP incluida en la base de datos de Webroot a menos que se relaje mediante su inclusión en Allow_list1 (ejemplo 3).

```
> add appfw policy "Ip_Rep_Policy" "((CLIENT.IP.SRC.IPREP_IS_MALICIOUS
    || CLIENT.IP.SRC.TYPECAST_TEXT_T.CONTAINS_ANY("Block_list1")) && ! (
    CLIENT.IP.SRC.TYPECAST_TEXT_T.CONTAINS_ANY("Allow_list1")))"
    APPFW_BLOCK
<!--NeedCopy-->
```

El siguiente ejemplo muestra una expresión de directiva para bloquear el IPv6 del cliente en las siguientes condiciones:

1. Coincide con una dirección IPv6 configurada en el Block_list_IPv6 personalizado (ejemplo 4)
2. Coincide con una dirección IPv6 incluida en la base de datos de Webroot a menos que se relaje mediante su inclusión en allow_list_IPv6 (ejemplo 3).

```
add appfw policy "Ip_Rep_v6_Policy" "((CLIENT.IPV6.SRC.
    IPREP_IS_MALICIOUS || CLIENT.IPV6.SRC.TYPECAST_TEXT_T.CONTAINS_ANY("
    Block_list_ipv6")) && ! (CLIENT.IPV6.SRC.TYPECAST_TEXT_T.
    CONTAINS_ANY("Allow_list_ipv6")))" APPFW_BLOCK
<!--NeedCopy-->
```

Uso del servidor proxy:

Si el dispositivo Citrix ADC no tiene acceso directo a Internet y está conectado a un proxy, configure el cliente de reputación IP para que envíe solicitudes al proxy.

En el símbolo del sistema, escriba:


```
set reputation settings -proxyServer <proxy server ip> -proxyPort <proxy server port>
```

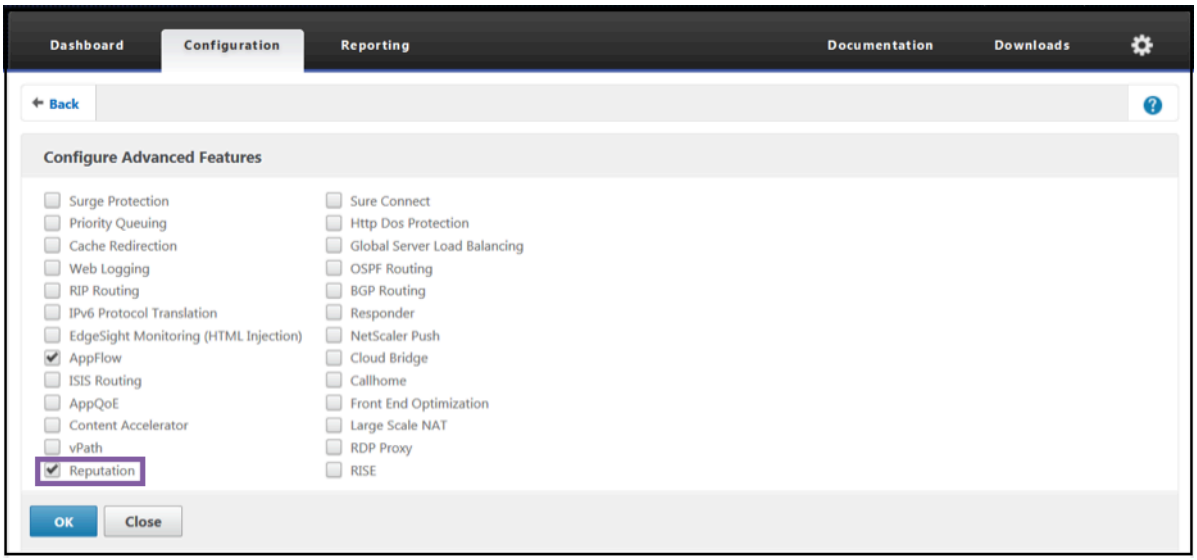
Ejemplo:

```
> set reputation settings proxyServer 10.102.30.112 proxyPort 3128
> set reputation settings -proxyServer testproxy.citrite.net -proxyPort 3128
> unset reputation settings -proxyserver -proxyport
> sh reputation settings
```

> **Nota:**
>
> La IP del servidor proxy puede ser una dirección IP o un nombre de dominio completo (FQDN).

Configurar la reputación de IP mediante la interfaz gráfica de usuario de Citrix ADC

1. Vaya a **Sistema > Configuración**. En la sección **Modos y funciones**, haga clic en el enlace para acceder al panel **Configurar funciones avanzadas** y active la casilla de verificación **Reputación**.
2. Haga clic en **Aceptar**.

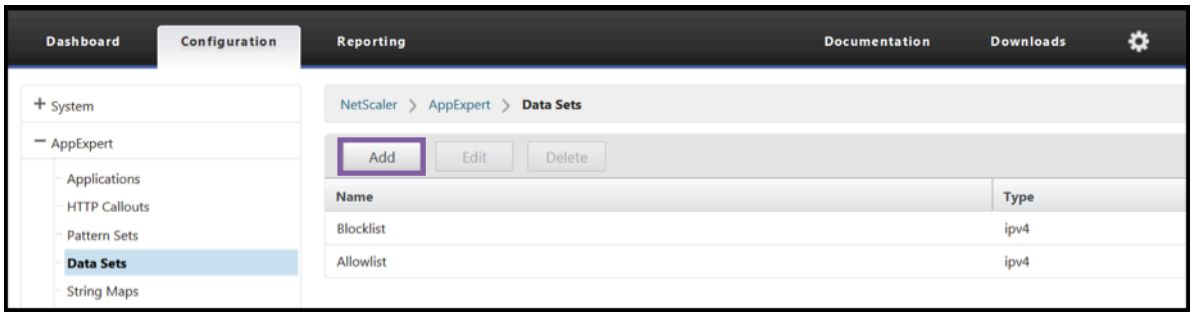


Para configurar un servidor proxy mediante la GUI de Citrix ADC

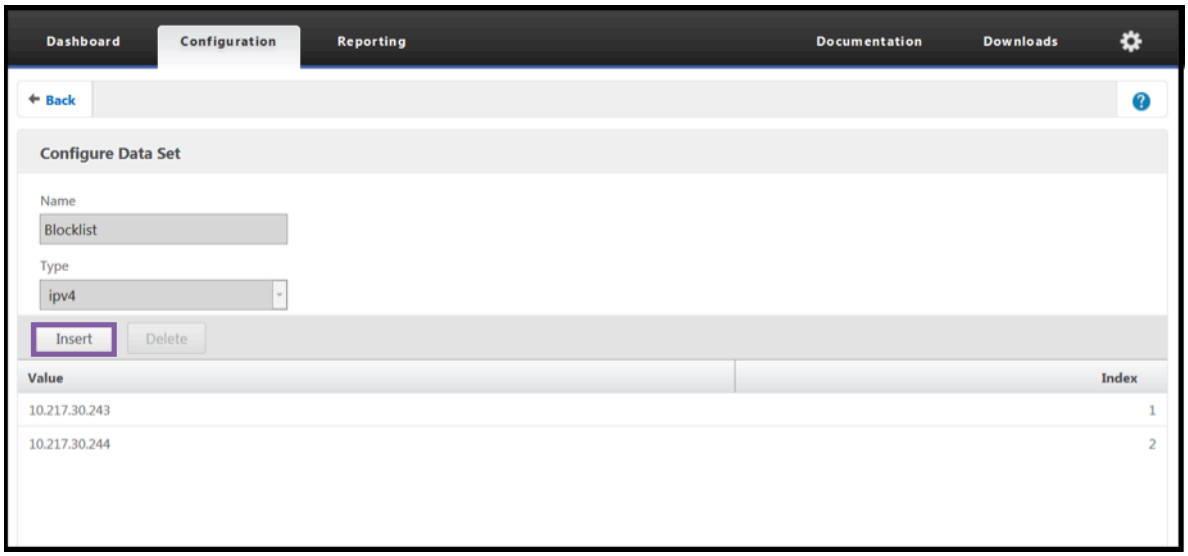
1. En la ficha de configuración, vaya a **Seguridad > Reputación**. En **Configuración**, haga clic en **Cambiar configuración de reputación** para configurar un servidor proxy. También puede activar o desactivar la función de reputación. El**servidor proxy** puede ser una dirección IP o un nombre de dominio completo (FQDN). **El puerto proxy** acepta valores comprendidos entre [1 y 65535].

Crear una lista de permitidos y una lista de bloqueo de direcciones IP de clientes mediante la interfaz gráfica de usuario

1. En la ficha **Configuración**, vaya a **AppExpert > Conjuntos de datos**.
2. Haga clic en **Agregar**.



- En el panel **Crear conjunto de datos** (o **Configurar conjunto de datos**), proporcione un nombre significativo para la lista de direcciones IP. El nombre debe reflejar el propósito de la lista.
- Seleccione **Tipo** como **IPv4** o **IPv6**.
- Haga clic en **Insertar** para agregar una entrada.



- En el panel de **enlace Configurar conjunto de datos de directivas**, agregue una dirección IP con formato IPv4 o IPv6 en el cuadro de entrada Valor.
- Proporciona un índice.
- Agrega un comentario que explique el propósito de la lista. Este paso es opcional, pero se recomienda porque un comentario descriptivo es útil para administrar la lista.

Del mismo modo, puede crear una lista de bloqueo y agregar las direcciones IP que se considerarán maliciosas.

Consulte también Conjuntos de patrones y conjuntos de datos para obtener más información sobre el uso de conjuntos de datos y la configuración de expresiones de directivas avanzadas.

Configurar una directiva de firewall de aplicaciones mediante la GUI de Citrix ADC

1. En la ficha **Configuración**, vaya a **Seguridad > Firewall de aplicaciones > Directivas > Firewall**. Haga clic en **Agregar** para agregar una directiva mediante las expresiones PI para utilizar la reputación de IP.

También puede utilizar el editor de expresiones para crear su propia expresión de directiva. En la lista se muestran las opciones preconfiguradas que resultan útiles para configurar una expresión mediante las categorías de amenazas.

Resumen

- Detenga de forma rápida y precisa el tráfico incorrecto en el borde de la red desde direcciones IP maliciosas conocidas que representan diferentes tipos de amenazas. Puede bloquear la solicitud sin analizar el cuerpo.
- Configure dinámicamente la funcionalidad de reputación de IP para varias aplicaciones.
- Proteja su red contra la filtración de datos sin que se produzca una penalización en el rendimiento y consolide las protecciones en un único tejido de servicios mediante implementaciones rápidas y sencillas.
- Puede realizar comprobaciones de reputación de IP en las IP de origen y destino.
- También puede inspeccionar los encabezados para detectar IP maliciosas.
- La comprobación de reputación de IP se admite tanto en las implementaciones de proxy directo como de proxy inverso.
- El proceso de reputación de IP se conecta con Webroot y actualiza la base de datos cada 5 minutos.
- Cada nodo de la implementación de alta disponibilidad (HA) o clúster obtiene la base de datos de Webroot.
- Los datos de reputación de IP se comparten en todas las particiones de las implementaciones de particiones de administración.
- Puede utilizar un conjunto de datos de AppExpert para crear listas de direcciones IP con el fin de agregar excepciones para las IP incluidas en la lista de bloqueo de la base de datos de Web-

root. También puede crear su propia lista de bloqueo personalizada para designar IP específicas como maliciosas.

- El archivo iprep.db se crea en la carpeta `/var/nslog/iprep`. Una vez creada, no se elimina incluso si la entidad está inhabilitada.
- Cuando la función de reputación está habilitada, se descarga la base de datos de Citrix ADC Webroot. Después de eso, se actualiza cada 5 minutos.
- La versión principal de la base de datos de Webroot es la versión: 1.
- La versión secundaria se actualiza todos los días. La versión de actualización se incrementa cada 5 minutos y se restablece a 1 cuando se incrementa la versión secundaria.
- Las expresiones PI permiten utilizar la reputación IP con otras funciones, como responder y reescribir.
- Las direcciones IP de la base de datos están en notación decimal.

Sugerencias de depuración

- Si no puede ver la función de reputación en la interfaz gráfica de usuario, compruebe que tiene la licencia correcta.
- Supervisar los mensajes en `var/log/iprep.log` para depurar errores.
- **Conectividad de Webroot**: Si vaya el mensaje `ns iprep: Not able to connect/ resolve WebRoot`, asegúrese de que el dispositivo tenga acceso a Internet y que DNS esté configurado.
- **Servidor proxy**: Si vaya el mensaje `ns iprep: iprep_curl_download: 88 curl_easy_perform failed. Error code: 5 Err msg:couldnt resolve proxy name`, asegúrese de que la configuración del servidor proxy sea correcta.
- La**función de reputación de IP no funciona**: el proceso de reputación de IP tarda unos cinco minutos en iniciarse después de habilitar la función de reputación. Es posible que la función de reputación de IP no funcione durante ese tiempo.
- **Descarga de la base**de datos: si la descarga de datos de la base de datos IP falla después de habilitar la función de reputación IP, se muestra el siguiente error en los registros.

```
iprep: iprep_curl_download:86 curl_easy_perform failed. Error code:7 Err
msg:Couldn't connect to server
```

Solución: Permita el tráfico de salida a las siguientes direcciones URL o configure un proxy para resolver el problema.

```
localdb-ip-daily.brightcloud.com:443
localdb-ip-rtu.brightcloud.com:443
api.bcti.brightcloud.com:443
<!--NeedCopy-->
```


Descarga y aceleración de SSL

January 12, 2021

Un dispositivo Citrix ADC configurado para la aceleración SSL acelera de manera transparente las transacciones SSL al descargar el procesamiento SSL del servidor. Para configurar la descarga SSL, configure un servidor virtual para interceptar y procesar transacciones SSL, y envíe el tráfico descifrado al servidor (a menos que configure el cifrado de extremo a extremo, en cuyo caso el tráfico se vuelve a cifrar). Al recibir la respuesta del servidor, el dispositivo completa la transacción segura con el cliente. Desde la perspectiva del cliente, la transacción parece estar directamente con el servidor. Un Citrix ADC configurado para la aceleración SSL también realiza otras funciones configuradas, como el equilibrio de carga.

La configuración de la descarga SSL requiere un certificado SSL y un par de claves, que debe obtener si aún no tiene un certificado SSL. Otras tareas relacionadas con SSL que podría necesitar realizar incluyen la administración de certificados, la administración de listas de revocación de certificados, la configuración de la autenticación de clientes y la administración de acciones y directivas SSL.

Un dispositivo Citrix ADC que no sea FIPS almacena la clave privada del servidor en el disco duro. En un dispositivo FIPS, la clave se almacena en un módulo criptográfico conocido como módulo de seguridad de hardware (HSM).

Todos los dispositivos Citrix ADC que no admiten una tarjeta FIPS (incluidos los dispositivos virtuales) admiten los HSM externos Thales nShield® Connect y SafeNet. (Los dispositivos MPX 9700/10500/12500/15500 no admiten un HSM externo).

Nota: Las opciones relacionadas con FIPS para algunos de los procedimientos de configuración SSL descritos en este documento son específicas de un dispositivo Citrix ADC habilitado para FIPS.

Configuración de descarga SSL

June 2, 2022

Para configurar la descarga SSL, debe habilitar el procesamiento SSL en el dispositivo Citrix ADC y configurar un servidor virtual basado en SSL. El servidor virtual interceptará el tráfico SSL, lo descifrará y lo reenviará a un servicio que esté enlazado al servidor virtual. Para proteger el tráfico urgente, como la transmisión de contenido multimedia, puede configurar un servidor virtual DTLS. Para habilitar la descarga SSL, debe importar un certificado y una clave válidos y vincular el par al servidor virtual.

> Nota
>
> A partir de la versión 13.1 compilación 17.x, los protocolos inferiores a TLSv1.2 están inhabilitados

en los servicios internos de SSL.

- Si el perfil predeterminado está habilitado, `ns_default_ssl_profile_internal_frontend_servic` está enlazado a los servicios internos SSL y los protocolos SSLv3, TLSv1.0 y TLSv1.1 están inhabilitados en este perfil.
- Si el perfil predeterminado no está habilitado, los protocolos SSLv3, TLSv1.0 y TLSv1.1 se inhabilitan en los parámetros de servicios internos de SSL.

Habilitar SSL

Para procesar el tráfico SSL, debe habilitar el procesamiento SSL. Puede configurar entidades basadas en SSL, como servidores y servicios virtuales, sin habilitar el procesamiento SSL. Sin embargo, no funcionan hasta que el procesamiento SSL esté habilitado.

Habilitar el procesamiento SSL mediante la CLI

En el símbolo del sistema, escriba:

```
enable ns feature ssl

show ns feature
<!--NeedCopy-->
```

Ejemplo:

```
enable ns feature SSL
 Done
show ns feature

        Feature                         Acronym             Status
        -------                         -------             ------
 1)     Web Logging                     WL                  OFF
 2)     Surge Protection                SP                  ON
 3)     Load Balancing                  LB                  ON
 .
 .
 .
 9)     SSL Offloading                  SSL                 ON
 .
 .
 .
```



```
 24)    NetScaler Push                  push                  OFF
 Done
<!--NeedCopy-->
```

Habilitar el procesamiento SSL mediante la interfaz gráfica de usuario

Vaya a **Sistema > Configuración** y, en el grupo **Modos y funciones**, haga clic en **Configurar funciones básicas** y, a continuación, en **Descarga SSL**.

Configurar servicios

En el dispositivo Citrix ADC, un servicio representa un servidor físico o una aplicación en un servidor físico. Una vez configurados, los servicios se encuentran en estado inhabilitado hasta que el dispositivo puede llegar al servidor físico de la red y supervisar su estado.

Agregar un servicio mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para agregar un servicio y verificar la configuración:

```
add service <name> (<IP> | <serverName>) <serviceType> <port>
show service <serviceName>
<!--NeedCopy-->
```

Ejemplo:

```
add service sslsvc 198.51.100.225 SSL 443

Done

sh ssl service sslsvc

            Advanced SSL configuration for Back-end SSL Service sslsvc:
            DH: DISABLED
            DH Private-Key Exponent Size Limit: DISABLED    Ephemeral
                RSA: DISABLED
            Session Reuse: ENABLED          Timeout: 300 seconds
            Cipher Redirect: DISABLED
            SSLv2 Redirect: DISABLED
            ClearText Port: 0
```



```
14              Server Auth: DISABLED
15              SSL Redirect: DISABLED
16              Non FIPS Ciphers: DISABLED
17              SNI: DISABLED
18              OCSP Stapling: DISABLED
19              SSLv2: DISABLED  SSLv3: ENABLED  TLSv1.0: ENABLED  TLSv1.1:
                    ENABLED  TLSv1.2: ENABLED  TLSv1.3: DISABLED
20              Send Close-Notify: YES
21              Strict Sig-Digest Check: DISABLED
22              Zero RTT Early Data: ???
23              DHE Key Exchange With PSK: ???
24              Tickets Per Authentication Context: ???
25
26              ECC Curve: P_256, P_384, P_224, P_521
27
28      1)      Cipher Name: DEFAULT_BACKEND
29              Description: Default cipher list for Backend SSL session
30       Done
31  <!--NeedCopy-->
```

Modificar o eliminar un servicio mediante la CLI

Para modificar un servicio, use el comando set service, que es igual que usar el comando add service, excepto que introduce el nombre de un servicio existente.

Para eliminar un servicio, use el comando rm service, que solo acepta el argumento <name>.

```
1  rm service <servicename>
2  <!--NeedCopy-->
```

Ejemplo:

```
1  rm service sslsvc
2  <!--NeedCopy-->
```

Para modificar un servicio, use el comando set service, seleccione cualquier parámetro y cambie su configuración.

```
1  set service <name> (<IP> | <serverName>) <serviceType> <port>
2  <!--NeedCopy-->
```


Ejemplo:

```
set service sslsvc 198.51.100.225 SSL 443
<!--NeedCopy-->
```

Configurar un servicio mediante la interfaz gráfica de usuario

Vaya a **Administración del tráfico > Equilibrio de carga > Servicios**, cree un servicio y especifique el protocolo como SSL.

Configuración del servidor virtual SSL

Las sesiones seguras requieren establecer una conexión entre el cliente y un servidor virtual basado en SSL en el dispositivo Citrix ADC. El servidor virtual SSL intercepta el tráfico SSL, lo descifra y lo procesa antes de enviarlo a los servicios que están enlazados al servidor virtual.

Nota: El servidor virtual SSL se marca como inactivo en el dispositivo Citrix ADC hasta que un par de certificado/clave válido y al menos un servicio estén vinculados a él. Un servidor virtual basado en SSL es un servidor virtual de equilibrio de carga de tipo de protocolo SSL o SSL_TCP. La función de equilibrio de carga debe estar habilitada en el dispositivo Citrix ADC.

Agregar un servidor virtual basado en SSL mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para crear un servidor virtual basado en SSL y compruebe la configuración:

```
add lb vserver <name> (serviceType) <IPAddress> <port>
show ssl vserver <name>
<!--NeedCopy-->
```

Ejemplo:

```
add lb vserver sslvs SSL 192.0.2.240 443
Done

sh ssl vserver sslvs

            Advanced SSL configuration for VServer sslvs:
```



```
7               DH: DISABLED
8               DH Private-Key Exponent Size Limit: DISABLED    Ephemeral
                    RSA: ENABLED          Refresh Count: 0
9               Session Reuse: ENABLED          Timeout: 120 seconds
10              Cipher Redirect: DISABLED
11              SSLv2 Redirect: DISABLED
12              ClearText Port: 0
13              Client Auth: DISABLED
14              SSL Redirect: DISABLED
15              Non FIPS Ciphers: DISABLED
16              SNI: DISABLED
17              OCSP Stapling: DISABLED
18              HSTS: DISABLED
19              HSTS IncludeSubDomains: NO
20              HSTS Max-Age: 0
21              SSLv2: DISABLED  SSLv3: ENABLED  TLSv1.0: ENABLED  TLSv1.1:
                     ENABLED  TLSv1.2: ENABLED  TLSv1.3: DISABLED
22              Push Encryption Trigger: Always
23              Send Close-Notify: YES
24              Strict Sig-Digest Check: DISABLED
25              Zero RTT Early Data: DISABLED
26              DHE Key Exchange With PSK: NO
27              Tickets Per Authentication Context: 1
28              ECC Curve: P_256, P_384, P_224, P_521
29
30      1)      Cipher Name: DEFAULT
31              Description: Default cipher list with encryption strength
                    >= 128bit
32       Done
33  <!--NeedCopy-->
```

Modificar o eliminar un servidor virtual basado en SSL mediante la CLI

Para modificar las propiedades de equilibrio de carga de un servidor virtual SSL, use el comando `set lb vserver`. El comando set es similar al comando `add lb vserver`, excepto que se introduce el nombre de un servidor virtual existente. Para modificar las propiedades **SSL** de un servidor virtual basado en SSL, use el comando `set ssl vserver`. Para obtener más información, consulte la sección “Parámetros del servidor virtual SSL” más adelante en esta página.

Para eliminar un servidor virtual SSL, use el comando `rm lb vserver`, que solo acepta el argumento `<name>`.

Configurar un servidor virtual basado en SSL mediante la interfaz gráfica de usuario

Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**, cree un servidor virtual y especifique el protocolo como SSL.

Enlazar servicios al servidor virtual SSL

El dispositivo ADC reenvía los datos SSL descifrados a los servidores de la red. Para reenviar datos, los servicios que representan a estos servidores físicos deben estar vinculados al servidor virtual que recibe los datos SSL.

Por lo general, el enlace entre el dispositivo ADC y el servidor físico es seguro. Por lo tanto, la transferencia de datos entre el dispositivo y el servidor físico no tiene que cifrarse. Sin embargo, puede proporcionar cifrado de extremo a extremo cifrando la transferencia de datos entre el dispositivo y el servidor. Para obtener más información, consulte Configurar la descarga de SSL con cifrado de extremo a extremo.

Nota: Habilite la función de equilibrio de carga en el dispositivo ADC antes de enlazar servicios al servidor virtual basado en SSL.

Enlazar un servicio a un servidor virtual mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para vincular el servicio al servidor virtual y verificar la configuración:

```
bind lb vserver <name> <serviceName>
show lb vserver <name>
<!--NeedCopy-->
```

Ejemplo:

```
bind lb vserver sslvs sslsvc
     Done

sh lb vserver sslvs

            sslvs (192.0.2.240:443) - SSL       Type: ADDRESS
            State: DOWN[Certkey not bound]
            Last state change was at Wed May  2 11:43:04 2018
            Time since last state change: 0 days, 00:13:21.150
            Effective State: DOWN
```



```
            Client Idle Timeout: 180 sec
            Down state flush: ENABLED
            Disable Primary Vserver On Down : DISABLED
            Appflow logging: ENABLED
            No. of Bound Services :  1 (Total)       0 (Active)
            Configured Method: LEASTCONNECTION      BackupMethod:
               ROUNDROBIN
            Mode: IP
            Persistence: NONE
            Vserver IP and Port insertion: OFF
            Push: DISABLED  Push VServer:
            Push Multi Clients: NO
            Push Label Rule: none
            L2Conn: OFF
            Skip Persistency: None
            Listen Policy: NONE
            IcmpResponse: PASSIVE
            RHIstate: PASSIVE
            New Service Startup Request Rate: 0 PER_SECOND, Increment
               Interval: 0
            Mac mode Retain Vlan: DISABLED
            DBS_LB: DISABLED
            Process Local: DISABLE
            Traffic Domain: 0
            TROFS Persistence honored: ENABLED
            Retain Connections on Cluster: NO
    1) sslsvc (198.51.100.225: 443) - SSL State: DOWN       Weight: 1
     Done
<!--NeedCopy-->
```

Desvincular un servicio de un servidor virtual mediante la CLI

En el símbolo del sistema, escriba el siguiente comando:

```
unbind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Ejemplo:

```
unbind lb vserver sslvs sslsvc
     Done
```



```
<!--NeedCopy-->
```

Enlazar un servicio a un servidor virtual mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. Abra un servidor virtual y haga clic en el mosaico **Enlaces de servicios de servidor virtual de equilibrio de carga** en la sección **Servicios y grupos de servicios**.
3. En la página **Enlace de servicio de servidor virtual de equilibrio de carga**, haga clic en la ficha **Agregar enlaces**, **haga clic en Haga clic para seleccionaren Seleccionar servicio**y seleccione la casilla de verificación junto al servicio que se va a vincular.
4. Haga clic en **Seleccionar** y en **Enlazar**

Configurar un servidor virtual de indicación de nombre de servidor (SNI) para el alojamiento seguro de varios sitios

Los servidores web utilizan el alojamiento virtual para alojar más de un nombre de dominio con la misma dirección IP. El dispositivo admite el alojamiento de varios dominios seguros mediante la descarga del procesamiento SSL de los servidores web mediante servicios SSL transparentes o la descarga SSL basada en servidor virtual. Sin embargo, cuando varios sitios web están alojados en el mismo servidor virtual, el protocolo de enlace SSL se completa antes de que se envíe el nombre de host esperado al servidor virtual. Como resultado, el dispositivo no puede determinar qué certificado debe presentar al cliente después de que se establezca una conexión. Este problema se resuelve habilitando el SNI en el servidor virtual. SNI es una extensión de seguridad de la capa de transporte (TLS) que utiliza el cliente para proporcionar el nombre de host durante el inicio del protocolo de enlace. El dispositivo ADC compara este nombre de host con el nombre común y, si no coincide, lo compara con el nombre alternativo del sujeto (SAN). Si el nombre coincide, el dispositivo presenta el certificado correspondiente al cliente.

Un certificado SSL comodín ayuda a habilitar el cifrado SSL en varios subdominios si la misma organización controla estos dominios y el nombre de dominio de segundo nivel es el mismo. Por ejemplo, un certificado comodín emitido para una red deportiva con el nombre común "*.sports.net" se puede usar para proteger dominios, como "login.sports.net" y "help.sports.net". No puede proteger el dominio "login.ftp.sports.net".

Nota:
En un dispositivo ADC, solo se comparan las entradas DNS de nombre de dominio, URL e ID de correo electrónico en el campo **SAN**.

Puede vincular varios certificados de servidor a un solo servidor virtual SSL o servicio transparente

mediante la opción -SNICert. El servidor o servicio virtual emite estos certificados si el SNI está habilitado en el servidor o servicio virtual. Puede habilitar el SNI en cualquier momento.

Enlazar varios certificados de servidor a un único servidor virtual SSL mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para configurar el SNI y verificar la configuración:

```
set ssl vserver <vServerName>@ [-SNIEnable ( ENABLED | DISABLED )]

bind ssl vserver <vServerName>@ -certkeyName <string> -SNICert

show ssl vserver <vServerName>
<!--NeedCopy-->
```

Para vincular varios certificados de servidor a un servicio transparente mediante la CLI, reemplace `vserver` por “service” y `vservername` por “service name” en los comandos anteriores.

Nota: Cree el servicio SSL con la opción `-clearTextPort 80`.

Enlazar varios certificados de servidor a un único servidor virtual SSL mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. Abra un servidor virtual SSL y, en **Certificados**, seleccione **Certificado de servidor**.
3. Agregue un certificado o seleccione uno de la lista y haga clic en **Certificado de servidor para SNI**.
4. En **Configuración avanzada**, seleccione **Parámetros SSL**.
5. Haga clic **en Habilitar SNI**.

Compatibilidad con SNI en el servicio back-end

> **Nota**: El SNI no se admite en un servicio back-end de DTLS.

El dispositivo Citrix ADC admite la indicación de nombre del servidor (SNI) en el back-end. Es decir, el nombre común se envía como el nombre del servidor en el cliente hola al servidor back-end para completar con éxito el apretón de manos. Esta compatibilidad ayuda a cumplir con los requisitos de seguridad del cliente de integradores de sistemas federales Además, el SNI ofrece la ventaja de usar solo un puerto en lugar de abrir cientos de direcciones IP y puertos diferentes en un firewall.

Los requisitos de seguridad del cliente para integradores de sistemas federales incluyen compatibilidad con Active Directory Federation Services (ADFS) 3.0 en 2012R2 y servidores WAP. Para cumplir con

este requisito, se requiere compatibilidad con SNI en el back-end en un dispositivo Citrix ADC.

> **Nota:**
>
> Para que SNI funcione, el nombre del servidor en el saludo del cliente debe coincidir con el nombre de host configurado en el servicio back-end que está enlazado a un servidor virtual SSL. Por ejemplo, si el nombre de host del servidor back-end es www.mail.example.com, el servicio back-end habilitado para SNI debe configurarse con el nombre del servidor como https://www.mail.example.com. Y este nombre de host debe coincidir con el nombre del servidor en el saludo del cliente.

Compatibilidad con SNI dinámico en el servicio back-end

El dispositivo Citrix ADC admite SNI dinámico en las conexiones TLS de back-end. Es decir, el dispositivo aprende el SNI en la conexión del cliente y lo usa en la conexión del lado del servidor. Ya no necesita especificar un nombre común en el servicio, el grupo de servicios o el perfil SSL. El nombre común recibido en la extensión SNI del mensaje Client Hello se reenvía a la conexión SSL de back-end.

Anteriormente, tenía que configurar el SNI estático en los servicios SSL, los grupos de servicios y los perfiles SSL. Como resultado, solo se envió al servidor la extensión SNI estática configurada. Si un cliente necesitaba acceder a varios dominios al mismo tiempo, el dispositivo ADC no podía enviar el SNI recibido del cliente al servicio back-end. En cambio, envió el nombre común estático que se configuró. Ahora, si el servidor back-end está configurado para varios dominios, el servidor puede responder con el certificado correcto en función del SNI recibido en el mensaje Client Hello del dispositivo.

Punto a tener en cuenta:

- El SNI debe estar habilitado en el front-end y el certificado SNI correcto debe estar vinculado al servidor virtual SSL. Si no habilita el SNI en el front-end, la información del SNI no se pasa al back-end.
- Cuando la autenticación de servidor está habilitada, el certificado de servidor se verifica mediante el certificado de CA y las entradas de nombre común/SAN en el certificado de servidor coinciden con el SNI. Por lo tanto, el certificado de CA debe estar vinculado al servicio.
- La reutilización de la conexión back-end y la sesión SSL se basa en el SNI cuando se habilita el SNI dinámico.

Los monitores SSL no envían SNI cuando el SNI dinámico está habilitado. Para el sondeo basado en SNI, adjunte un perfil back-end en el que esté configurado el SNI estático a los monitores SSL. El monitor debe configurarse con el mismo encabezado personalizado que el SNI.

Configurar el SNI en el servicio back-end mediante la CLI

En el símbolo del sistema, escriba:

```
add service <name>  <IP>  <serviceType>  <port>

add lb vserver <name>  <IPAddress> <serviceType>  <port>

bind lb vserver <name> <serviceName>

set ssl service <serviceName> -SNIEnable ENABLED -commonName <string>

set ssl profile <name> -SNIEnable ENABLED
<!--NeedCopy-->
```

Ejemplo:

```
    add service service_ssl 198.51.100.100 SSL 443

    add lb vserver ssl-vs 203.0.113.200 SSL 443

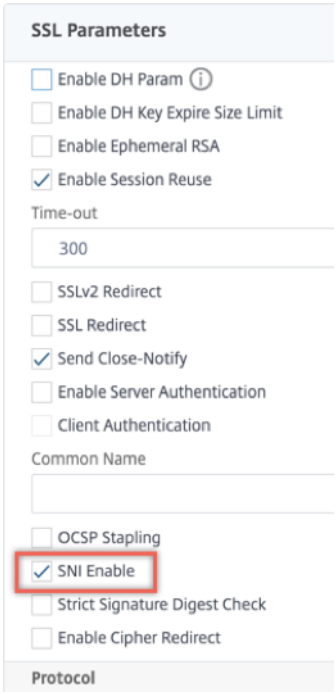
    bind lb vserver ssl-vs service_ssl

    set ssl service service_ssl -SNIEnable ENABLED  - commonName www.
       example.com

    set ssl profile sslprof -SNIEnable ENABLED
<!--NeedCopy-->
```

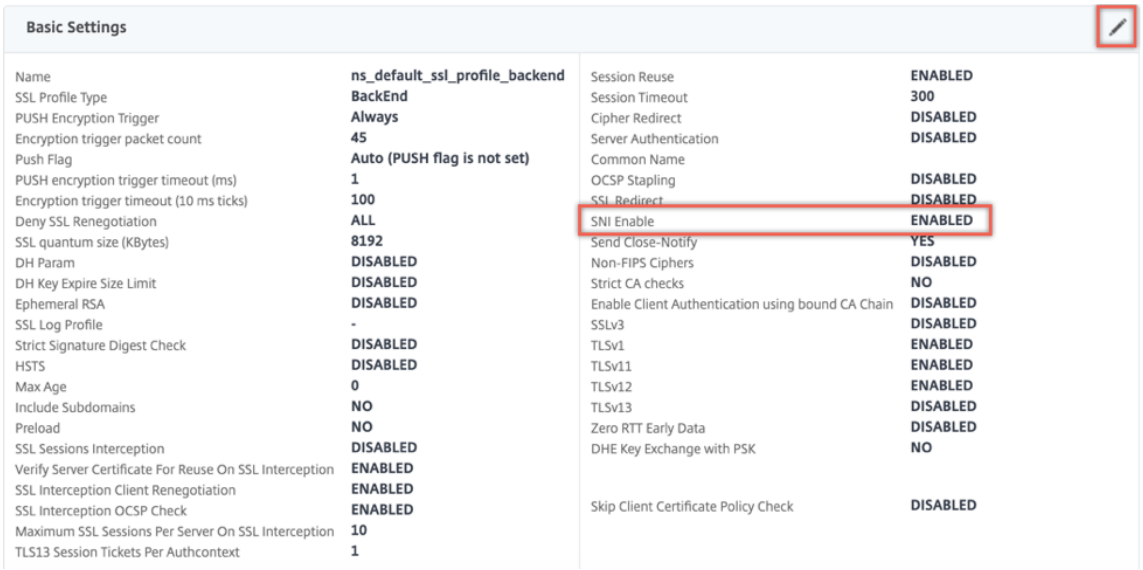
Configurar el SNI en el servicio back-end mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servicios**.
2. Seleccione un servicio SSL y, en **Configuración avanzada**, haga clic en **Parámetros SSL**.
3. Haga clic **en Habilitar SNI**.



Configurar el SNI en el perfil SSL mediante la interfaz gráfica de usuario

1. Vaya a **Sistema > Perfiles > Perfil SSL**.
2. Haga clic en **Agregar**.
3. En **Configuración básica**, seleccione **Habilitar SNI**.



4. Haga clic en **Aceptar**.

Enlazar un monitor seguro a un servicio back-end habilitado para SNI

Puede vincular monitores seguros de tipo HTTP, HTTP-ECV, TCP o TCP-ECV a los servicios de back-end y a los grupos de servicios que admiten SNI. Sin embargo, los sondeos de monitor no envían la extensión SNI si el SNI dinámico está habilitado. Para enviar sondeos de SNI, habilite el SNI estático en el perfil SSL de back-end y vincule el perfil al monitor. Establezca el encabezado personalizado en el monitor en el nombre del servidor que se envía como la extensión SNI en el saludo del cliente de la sonda del monitor.

Configurar y vincular un monitor seguro a un servicio de back-end habilitado para SNI mediante la CLI

En el símbolo del sistema, escriba:

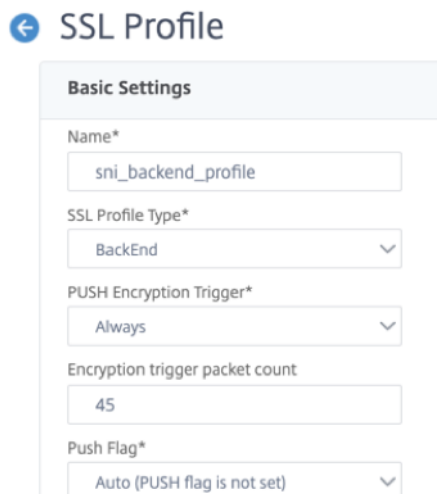
```
add lb monitor <monitorName> <type> -secure YES
add ssl profile <name> -sslProfileType BackEnd
set lb monitor <monitorName> <type> -customHeaders <string> -sslprofile
    <backend ssl profile>
set ssl profile <name> -sniEnable ENABLED -commonName <string>
bind service <name> -monitorName <string>
<!--NeedCopy-->
```

Ejemplo:

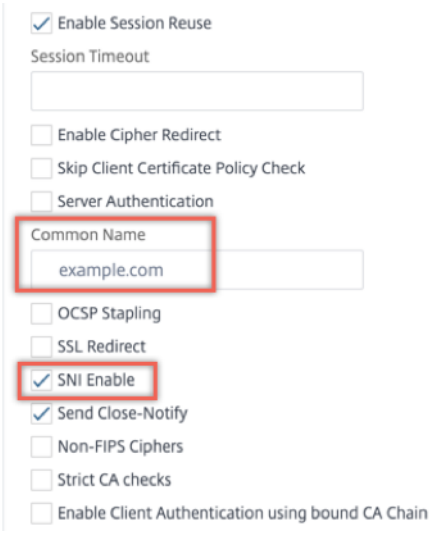
```
add ssl profile sni_backend_profile -sslProfileType BackEnd
set ssl profile sni_backend_profile -sniEnable ENABLED -commonName
   example.com
add lb monitor http-ecv-mon HTTP-ECV -secure YES
set monitor http-ecv-mon HTTP-ECV -customHeaders "Host: example.com\r\n
   " -sslprofile sni_backend_profile
bind service ssl_service  - monitorName http-ecv-mon
<!--NeedCopy-->
```

Configurar y vincular un monitor seguro a un servicio back-end habilitado para SNI mediante la interfaz gráfica de usuario

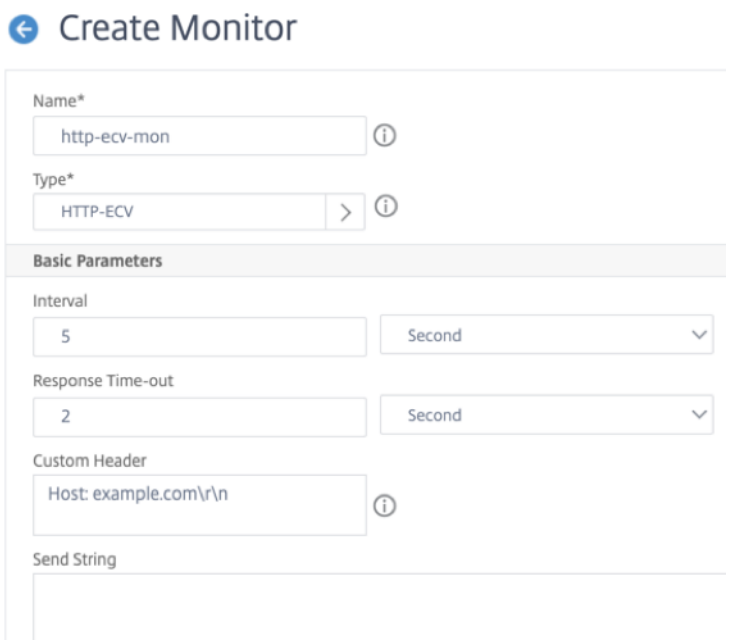
1. Vaya a **Sistema > Perfiles > Perfiles SSL**.
2. Haga clic en **Agregar**.
3. Especifique un nombre para el perfil y, en **Tipo de perfil SSL**, seleccione **Backend**.



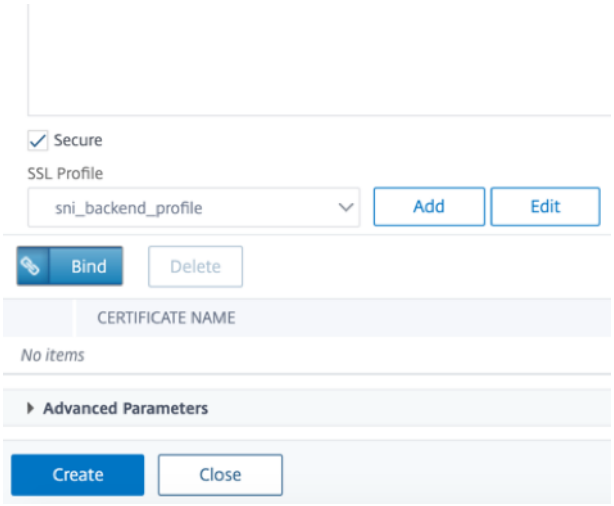
4. Especifique el nombre común (igual que el encabezado del host) y seleccione **Habilitar SNI**.



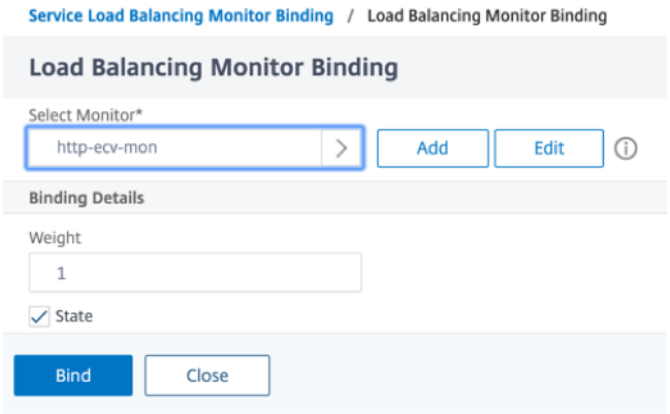
5. Haga clic en **Aceptar**.
6. Vaya a **Administración del tráfico > Equilibrio de carga > Supervisar**
7. Haga clic en **Agregar**.
8. Especifique un nombre para el monitor. En **Tipo**, seleccione HTTP, HTTP-ECV, TCP o TCP-ECV.
9. Especifique un **encabezado personalizado**.



10. Selecciona **Proteger**.
11. En **Perfil SSL**, seleccione el perfil SSL back-end creado en los pasos anteriores.
12. Haga clic en **Crear**.



13. Vaya a **Administración del tráfico > Equilibrio de carga > Servicios**.
14. Seleccione un servicio SSL y haga clic en **Modificar**.
15. En **Monitores**, haga clic en **Agregar enlace**, seleccione el monitor creado en los pasos anteriores y haga clic en **Enlazar**.



Configurar y vincular un monitor seguro a un servicio de back-end habilitado para SNI mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Supervisar**
2. Agregue un monitor de tipo **HTTP-ECV** o **TCP-ECV**y especifique un **encabezado personalizado**.
3. Seleccione **Crear**.
4. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servicios**.
5. Seleccione un servicio SSL y haga clic en **Modificar**.
6. En **Monitores**, haga clic en **Agregar enlace**, seleccione el monitor creado en el paso 3 y haga clic en **Enlazar**.

Agregar o actualizar un par de claves de certificado

> **Notas:**
>
> Si no tiene un certificado y una clave existentes, consulte Crear un certificado.
>
> Para crear un par de claves de certificado ECDSA, haga clic en Crear un par de claves de certificado ECDSA.
>
> Desde la compilación 41.x, se admiten nombres de certificado de hasta 63 caracteres.
>
> A partir de la versión 13.0 compilación 79.x, los pares de claves de certificado protegidos por contraseña siempre se agregan correctamente. Anteriormente, si se habilitaba una opción de contraseña segura en un dispositivo Citrix ADC, a veces no se agregaban los pares de claves de certificado protegidos con contraseña. Sin embargo, la configuración de la clave de certificado se pierde si se baja a una compilación anterior. Además, en la respuesta de la API de NITRO para pares de claves de certificado, la variable `passplain` se envía en lugar de la variable `passcrypt`.

Para cualquier transacción SSL, el servidor necesita un certificado válido y el par de claves privadas y públicas correspondientes. Los datos SSL se cifran con la clave pública del servidor, que está disponible a través del certificado del servidor. El descifrado requiere la clave privada correspondi-

ente. La contraseña de la clave privada utilizada al agregar un par de claves de certificado SSL se guarda con una clave de cifrado única para cada dispositivo Citrix ADC.

El dispositivo ADC descarga las transacciones SSL del servidor. Por lo tanto, el certificado y la clave privada del servidor deben estar presentes en el dispositivo y el certificado debe estar emparejado con su clave privada correspondiente. Este par de claves de certificado debe estar vinculado al servidor virtual que procesa las transacciones SSL.

Nota: El certificado predeterminado en un dispositivo Citrix ADC es de 2048 bits. En compilaciones anteriores, el certificado predeterminado era de 512 bits o 1024 bits. Después de actualizar a la versión 11.0, debe eliminar todos los pares de claves de certificado anteriores que comiencen por y "ns-", a continuación, reiniciar el dispositivo para generar automáticamente un certificado predeterminado de 2048 bits.

Tanto el certificado como la clave deben estar en el almacenamiento local en el dispositivo Citrix ADC antes de que se puedan agregar al dispositivo. Si el archivo de certificado o clave no está en el dispositivo, cárguelo en el dispositivo antes de crear el par.

Importante: Los certificados y las claves se almacenan en el directorio /nsconfig/ssl de forma predeterminada. Si sus certificados o claves se almacenan en cualquier otra ubicación, debe proporcionar la ruta absoluta a los archivos en el dispositivo Citrix ADC. Los dispositivos FIPS de Citrix ADC no admiten claves externas (claves que no sean FIPS). En un dispositivo FIPS, no puede cargar claves desde un dispositivo de almacenamiento local, como un disco duro o una memoria flash. Las claves FIPS deben estar presentes en el módulo de seguridad de hardware (HSM) del dispositivo.

Solo se admiten claves RSA en los dispositivos Citrix ADC.

Establezca el período de notificación y permita que el supervisor de caducidad emita un mensaje antes de que caduque el certificado.

El dispositivo Citrix ADC admite los siguientes formatos de entrada del certificado y los archivos de clave privada:

- PEM: correo con privacidad mejorada
- DER: regla de codificación distinguida
- PFX - Intercambio de información personal

El software detecta automáticamente el formato. Por lo tanto, ya no es necesario que especifique el formato en el parámetro inform. Si especifica el formato (correcto o incorrecto), el software lo ignora. El formato del certificado y el archivo de clave deben ser los mismos.

Nota: Un certificado debe firmarse con uno de los siguientes algoritmos hash:

- MD5
- SHA-1
- SHA-224
- SHA-256

- SHA-384
- SHA-512

Un dispositivo MPX admite certificados de 512 bits o más, hasta los siguientes tamaños:

- Certificado de servidor de 4096 bits en el servidor virtual
- Certificado de cliente de 4096 bits en el servicio
- Certificado de CA de 4096 bits (incluye certificados intermedios y raíz)
- Certificado de 4096 bits en el servidor back-end
- Certificado de cliente de 4096 bits (si la autenticación de cliente está habilitada en el servidor virtual)

Un dispositivo virtual VPX admite certificados de 512 bits o más, hasta los siguientes tamaños:

- Certificado de servidor de 4096 bits en el servidor virtual
- Certificado de cliente de 4096 bits en el servicio
- Certificado de CA de 4096 bits (incluye certificados intermedios y raíz)
- Certificado de 4096 bits en el servidor back-end
- Certificado de cliente de 4096 bits (si la autenticación de cliente está habilitada en el servidor virtual)

A partir de la versión 13.1 compilación 17.x, todas las plataformas Citrix ADC admiten certificados que se firman con los algoritmos RSASSA-PSS.
Estos algoritmos se admiten en la validación de rutas de certificados X.509.
En la siguiente tabla se muestran los conjuntos de parámetros RSASSA-PSS compatibles con el dispositivo Citrix ADC.

OID de clave pública	Función de generación de máscaras (MGF)	Función de resumen de MGF	Función Signature Digest	Longitud de sal
rsaEncryption	MGF1	SHA-256	SHA-256	32 bytes
rsaEncryption	MGF1	SHA-384	SHA-384	48 bytes
rsaEncryption	MGF1	SHA-512	SHA-512	64 bytes

> **Nota**
>
> Un dispositivo Citrix ADC SDX admite certificados de 512 bits o más. Cada instancia de Citrix ADC VPX alojada en el dispositivo admite los tamaños de certificado anteriores para un dispositivo virtual VPX. Sin embargo, si se asigna un chip SSL a una instancia, esa instancia admite los tamaños de certificado admitidos por un dispositivo MPX.

Agregar un par de claves de certificado mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para agregar un par de claves de certificado y verificar la configuración:

```
add ssl certKey <certkeyName> -cert <string>[(-key <string> [-password
    ]) | -fipsKey <string>] [-inform ( DER | PEM )] [<passplain>] [-
    expiryMonitor ( ENABLED | DISABLED ) [-notificationPeriod <
    positive_integer>]]

show ssl certKey [<certkeyName>]
<!--NeedCopy-->
```

Ejemplo:

```
add ssl certKey sslckey -cert server_cert.pem -key server_key.pem -
    password ssl -expiryMonitor ENABLED -notificationPeriod 30
 Done
Note: For FIPS appliances, replace -key with -fipskey

show ssl certKey sslckey
        Name: sslckey           Status: Valid,   Days to expiration
            :8418
        Version: 3
        Serial Number: 01
        Signature Algorithm: md5WithRSAEncryption
        Issuer:  C=US,ST=SJ,L=SJ,O=NS,OU=NSSSL,CN=www.root.com
        Validity
                Not Before: Jul 15 02:25:01 2005 GMT
                Not After : Nov 30 02:25:01 2032 GMT
        Subject:  C=US,ST=SJ,L=SJ,O=NS,OU=NSSSL,CN=www.server.com
        Public Key Algorithm: rsaEncryption
        Public Key size: 2048
 Done
<!--NeedCopy-->
```

Actualizar o eliminar un par de claves de certificado mediante la CLI

Para modificar el supervisor de caducidad o el período de notificación en un par de claves de certificado, utilice el comando `set ssl certkey`. Para reemplazar el certificado o la clave en un par de claves de certificado, use el comando `update ssl certkey`. El comando `update ssl certkey`

tiene un parámetro adicional para supeditar la comprobación de dominio. Para ambos comandos, introduzca el nombre de un par de claves de certificado existente. Para eliminar un par de claves de certificado SSL, use el comando `rm ssl certkey`, que solo acepta el argumento `<certkeyName>`.

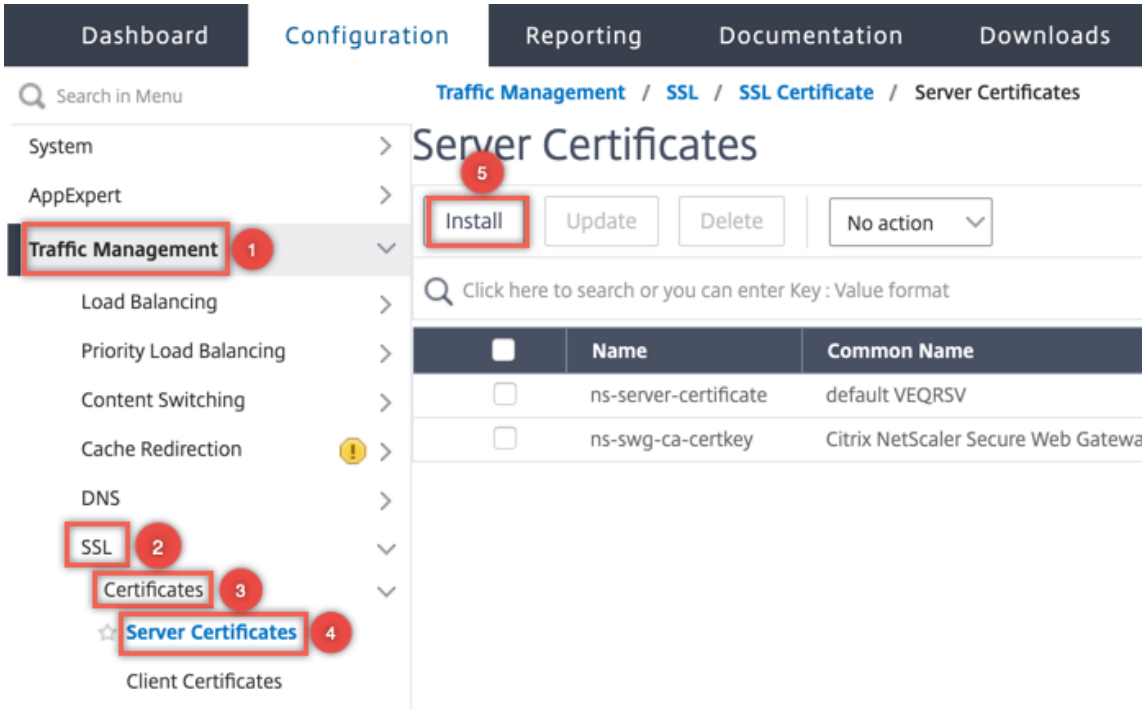
Ejemplo:

```
set ssl certKey <certkeyName> [-expiryMonitor ( ENABLED | DISABLED )
       [-notificationPeriod <positive_integer>]]

update ssl certKey <certkeyName> [-cert <string> [-password]] [-key
       <string> | -fipsKey <string>] [-inform <inform>] [-noDomainCheck
          ]
<!--NeedCopy-->
```

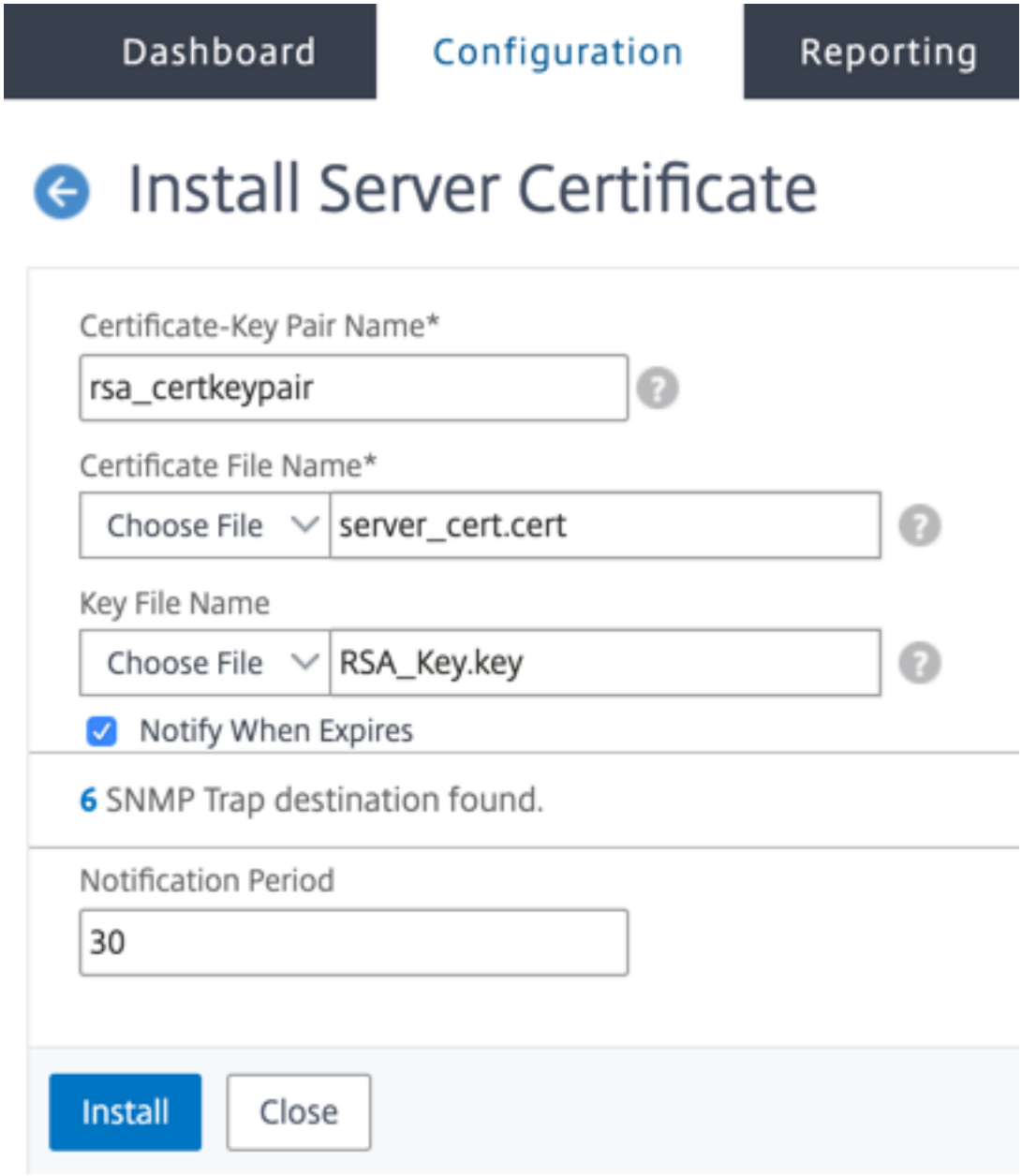
Agregar o actualizar un par de claves de certificado mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > SSL > Certificados > Servidor**.



2. Introduzca los valores de los siguientes parámetros y haga clic en **Instalar**.
   - Nombre del par de claves de certificado: nombre para el par de certificado y clave privada.
   - Nombre del archivo del certificado: certificado firmado recibido de la entidad de certificación.

- Nombre de archivo de clave: nombre y, opcionalmente, ruta de acceso al archivo de clave privada que se utiliza para formar el par de claves de certificado.



Enlazar el par de claves de certificado al servidor virtual SSL

Importante: Vincule los certificados intermedios a este certificado antes de vincularlo a un servidor virtual SSL. Para obtener información sobre la vinculación de certificados, consulte Creación de una cadena de certificados.

El certificado que se utiliza para procesar transacciones SSL debe estar enlazado al servidor virtual que recibe los datos SSL. Si tiene varios servidores virtuales que reciben datos SSL, debe vincularse

un par de claves de certificado válido a cada uno de ellos.

Use un certificado SSL válido y existente que haya cargado en el dispositivo Citrix ADC. Como alternativa para realizar pruebas, cree su propio certificado SSL en el dispositivo. Los certificados intermedios creados mediante una clave FIPS en el dispositivo no pueden enlazarse a un servidor virtual SSL.

Durante el enlace SSL, en el mensaje de solicitud de certificado durante la autenticación del cliente, el servidor enumera los nombres distintivos (DN) de todas las entidades de certificación (CA) enlazadas al servidor. El servidor acepta un certificado de cliente solo de esta lista. Si no quiere que el nombre de DN de un certificado de CA específico se envíe al cliente SSL, establezca la marca `skipCA`. Esta configuración indica que el nombre distintivo del certificado de CA concreto no debe enviarse al cliente SSL.

Para obtener más información sobre cómo crear su propio certificado, consulte Administración de certificados.

Nota: Citrix recomienda utilizar solo certificados SSL válidos emitidos por una entidad emisora de certificados de confianza.

Enlazar un par de claves de certificado SSL a un servidor virtual mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para vincular un par de claves de certificado SSL a un servidor virtual y verificar la configuración:

```
1 - bind ssl vserver <vServerName> -certkeyName <certificate-KeyPairName
    > -CA -skipCAName
2 - show ssl vserver <vServerName>
3 <!--NeedCopy-->
```

Ejemplo:

```
1 bind ssl vs vs1 -certkeyName cert2 -CA -skipCAName
2  Done
3 sh ssl vs vs1
4
5  Advanced SSL configuration for VServer vs1:
6
7  DH: DISABLED
8
9  Ephemeral RSA: ENABLED Refresh Count: 0
10
```



```
 Session Reuse: ENABLED Timeout: 120 seconds

 Cipher Redirect: DISABLED

 SSLv2 Redirect: DISABLED

 ClearText Port: 0

 Client Auth: DISABLED

 SSL Redirect: DISABLED

 Non FIPS Ciphers: DISABLED

 SNI: DISABLED

 OCSP Stapling: DISABLED

 HSTS: DISABLED

 IncludeSubDomains: NO

 HSTS Max-Age: 0

 SSLv2: DISABLED SSLv3: ENABLED  TLSv1.0: ENABLED  TLSv1.1: DISABLED
    TLSv1.2: DISABLED

 Push Encryption Trigger: Always

 Send Close-Notify: YES

 Strict Sig-Digest Check: DISABLED

ECC Curve: P_256, P_384, P_224, P_521

 1) CertKey Name: cert1 CA Certificate OCSPCheck: Optional CA_Name Sent
 2) CertKey Name: cert2 CA Certificate OCSPCheck: Optional CA_Name
    Skipped
 1) Cipher Name: DEFAULT

Description: Default cipher list with encryption strength >= 128bit
Done
<!--NeedCopy-->
```


Desvincular un par de claves de certificado SSL de un servidor virtual mediante la CLI

Si intenta desvincular un par de claves de certificado de un servidor virtual mediante el comando `unbind ssl certKey <certkeyName>`, aparece un mensaje de error. El error aparece porque la sintaxis del comando ha cambiado. En el símbolo del sistema, escriba el siguiente comando:

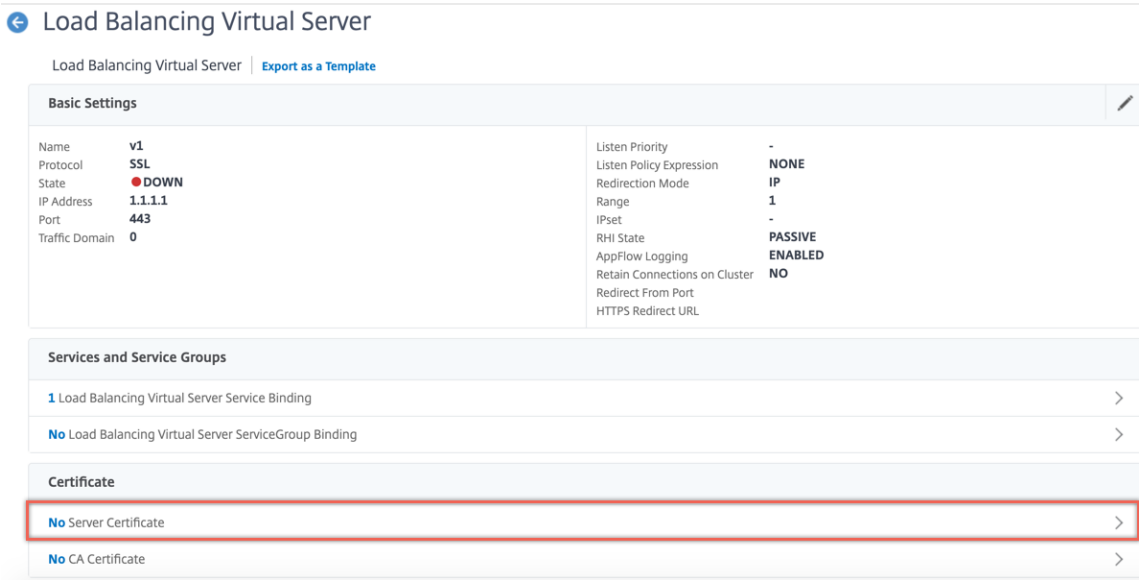
```
1 unbind ssl vserver <vServerName> -certkeyName <string>
2 <!--NeedCopy-->
```

Ejemplo:

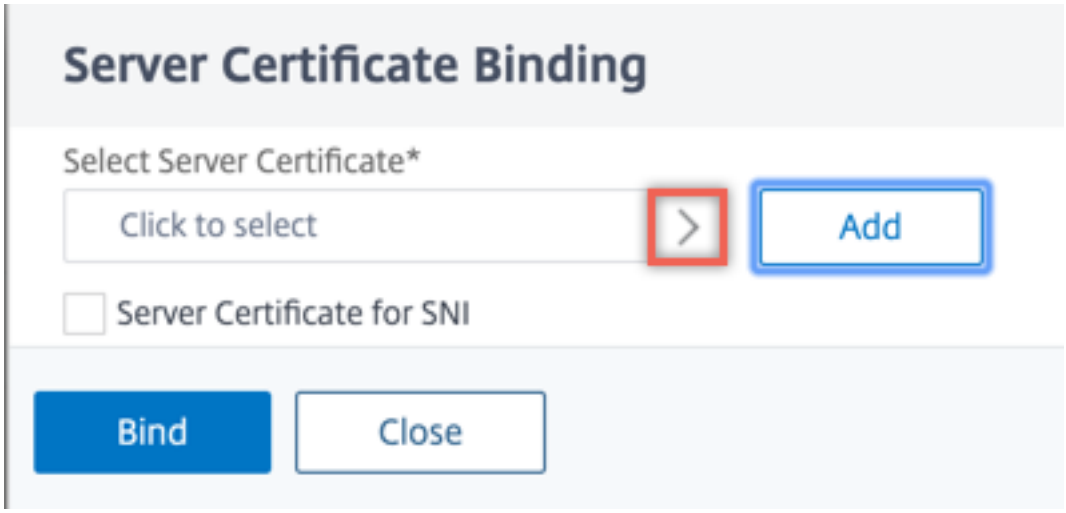
```
1 unbind ssl vserver vssl -certkeyName sslckey
2 <!--NeedCopy-->
```

Enlazar un par de claves de certificado SSL a un servidor virtual mediante la interfaz gráfica de usuario

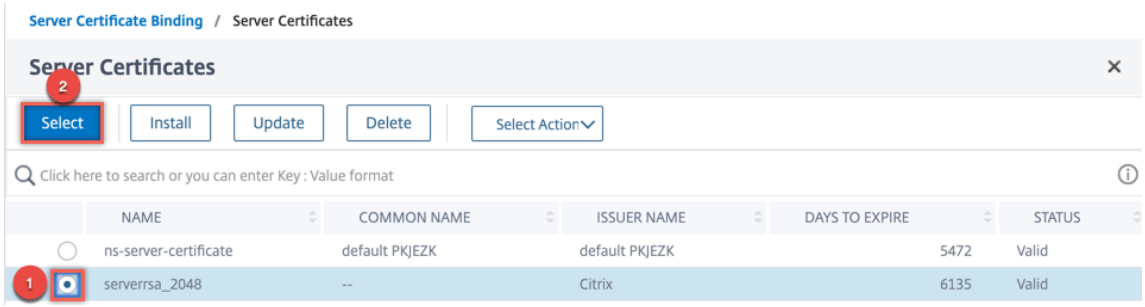
1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales** y abra un servidor virtual SSL. Haga clic en la sección **Certificado**.



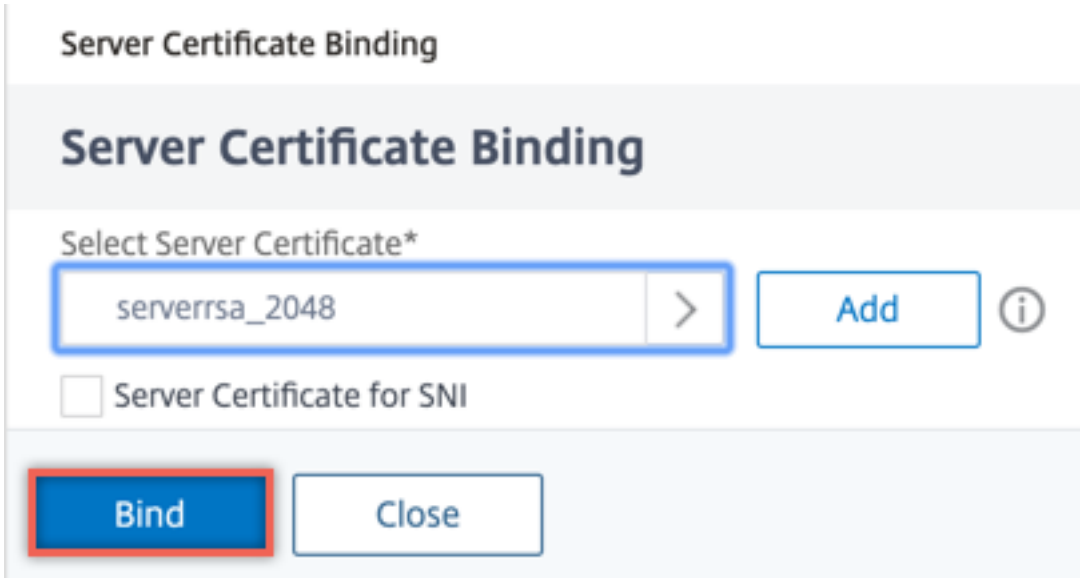
2. Haga clic en la flecha para seleccionar el par de claves de certificado.



3. Seleccione el par de claves de certificado de la lista.



4. Enlace el par de claves de certificado al servidor virtual. Para agregar un certificado de servidor como certificado SNI, seleccione **Certificado de servidor para SNI**.



Parámetros del servidor virtual SSL

Establezca la configuración SSL avanzada para un servidor virtual SSL. También puede establecer muchos de estos parámetros en un perfil SSL. Para obtener información sobre los parámetros que se pueden establecer en un perfil SSL, consulte Parámetros de perfil SSL.

Establecer los parámetros del servidor virtual SSL mediante la CLI

En el símbolo del sistema, escriba:

```
set ssl vserver <vServerName>@ [-clearTextPort <port>] [-dh ( ENABLED |
    DISABLED ) -dhFile <string>] [-dhCount <positive_integer>][-
    dhKeyExpSizeLimit ( ENABLED | DISABLED )] [-eRSA ( ENABLED |
    DISABLED) [-eRSACount <positive_integer>]] [-sessReuse ( ENABLED |
    DISABLED )[-sessTimeout <positive_integer>]] [-cipherRedirect (
    ENABLED | DISABLED ) [-cipherURL <URL>]] [-sslv2Redirect ( ENABLED |
     DISABLED )[-sslv2URL <URL>]] [-clientAuth ( ENABLED | DISABLED ) [-
    clientCert ( Mandatory | Optional )]] [-sslRedirect ( ENABLED |
    DISABLED )][-redirectPortRewrite ( ENABLED | DISABLED )] [-ssl2 (
    ENABLED | DISABLED )] [-ssl3 ( ENABLED | DISABLED )] [-tls1 (
    ENABLED | DISABLED )] [-tls11 ( ENABLED | DISABLED )] [-tls12 (
    ENABLED | DISABLED )][-tls13 ( ENABLED | DISABLED )] [-SNIEnable (
    ENABLED | DISABLED )][-ocspStapling ( ENABLED | DISABLED )] [-
    pushEncTrigger <pushEncTrigger>] [-sendCloseNotify ( YES | NO )] [-
    dtlsProfileName <string>] [-sslProfile <string>] [-HSTS ( ENABLED |
    DISABLED )][-maxage <positive_integer>] [-IncludeSubdomains ( YES |
    NO )][-strictSigDigestCheck ( ENABLED | DISABLED )] [-
    zeroRttEarlyData (ENABLED | DISABLED )] [-
    tls13SessionTicketsPerAuthContext <positive_integer>] [-
    dheKeyExchangeWithPsk ( YES | NO )]
<!--NeedCopy-->
```

Parámetros de Diffie-Hellman (DH)

Para utilizar cifrados en el dispositivo que requieren un intercambio de claves DH para configurar la transacción SSL, habilite el intercambio de claves DH en el dispositivo. Configure otros ajustes en función de su red.

Para enumerar los cifrados para los que se deben configurar los parámetros DH mediante la CLI, escriba: sh cipher DH.

Para enumerar los cifrados para los que se deben establecer parámetros DH mediante la utilidad de configuración, vaya a **Traffic Management > SSL > Cipher Groups** y haga doble clic en **DH**.

Para obtener más información sobre cómo habilitar el intercambio de claves DH, consulte Generar una clave Diffie-Hellman (DH).

Configure los parámetros DH mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para configurar los parámetros DH y verificar la configuración:

```
- `set ssl vserver <vserverName> -dh <Option> -dhCount <
   RefreshCountValue> -filepath <string>
- show ssl vserver <vServerName>`
<!--NeedCopy-->
```

Ejemplo:

```
set ssl vserver vs-server -dh ENABLED  -dhFile /nsconfig/ssl/ns-server.
   cert -dhCount 1000
Done

show ssl vserver vs-server

            Advanced SSL configuration for VServer vs-server:
            DH: ENABLED
            Ephemeral RSA: ENABLED          Refresh Count: 1000
            Session Reuse: ENABLED          Timeout: 120 seconds
            Cipher Redirect: DISABLED
            SSLv2 Redirect: DISABLED
            ClearText Port: 0
            Client Auth: DISABLED
            SSL Redirect: DISABLED
            Non FIPS Ciphers: DISABLED
            SNI: DISABLED
            OCSP Stapling: DISABLED
            HSTS: DISABLED
            HSTS IncludeSubDomains: NO
            HSTS Max-Age: 0
            SSLv2: DISABLED SSLv3: ENABLED  TLSv1.0: ENABLED TLSv1.2:
               ENABLED  TLSv1.2: ENABLED

     1)     Cipher Name: DEFAULT
            Description: Predefined Cipher Alias
Done
```



```
<!--NeedCopy-->
```

Configurar los parámetros DH mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**y abra un servidor virtual.
2. En la sección **Parámetros SSL**, seleccione **Habilitar parámetro DH** y especifique un recuento de actualizaciones y una ruta de archivo.

RSA efímero

El RSA efímero permite que los clientes de exportación se comuniquen con el servidor seguro incluso si el certificado del servidor no admite clientes de exportación (certificado de 1024 bits). Si quiere evitar que los clientes de exportación accedan al objeto o recurso web seguro, debe inhabilitar el intercambio efímero de claves RSA.

De forma predeterminada, esta función está habilitada en el dispositivo Citrix ADC, con el recuento de actualizaciones establecido en cero (uso infinito).

Nota:

La clave RSA efímera se genera automáticamente cuando vincula un cifrado de exportación a un servidor o servicio virtual SSL o SSL basado en TCP. Al eliminar el cifrado de exportación, la clave eRSA no se elimina. Se reutiliza más adelante cuando otro cifrado de exportación se vincula a un servidor o servicio virtual SSL o SSL basado en TCP. La clave eRSA se elimina cuando se reinicia el sistema.

Configurar RSA efímero mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para configurar RSA efímero y verificar la configuración:

```
set ssl vserver <vServerName> -eRSA (enabled | disabled) -eRSACount <
   positive_integer>
show ssl vserver <vServerName>
<!--NeedCopy-->
```

Ejemplo:

```
set ssl vserver vs-server -eRSA ENABLED -eRSACount 1000
 Done
```



```
3
4  show ssl vserver vs-server
5
6          Advanced SSL configuration for VServer vs-server:
7          DH: DISABLED
8          Ephemeral RSA: ENABLED          Refresh Count: 1000
9          Session Reuse: ENABLED          Timeout: 120 seconds
10         Cipher Redirect: DISABLED
11         SSLv2 Redirect: DISABLED
12         ClearText Port: 0
13         Client Auth: DISABLED
14         SSL Redirect: DISABLED
15         Non FIPS Ciphers: DISABLED
16         SNI: DISABLED
17         OCSP Stapling: DISABLED
18         HSTS: DISABLED
19         HSTS IncludeSubDomains: NO
20         HSTS Max-Age: 0
21         SSLv2: DISABLED SSLv3: ENABLED  TLSv1.0: ENABLED TLSv1.2:
               ENABLED  TLSv1.2: ENABLED
22
23 1)      Cipher Name: DEFAULT
24         Description: Predefined Cipher Alias
25  Done
26 <!--NeedCopy-->
```

Configurar RSA efímero mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**y abra un servidor virtual.
2. En la sección **Parámetros de SSL**, seleccione **Habilitar RSA efímero**y especifique un recuento de actualizaciones.

Reutilización de sesiones

Para las transacciones SSL, establecer el protocolo de enlace SSL inicial requiere operaciones de cifrado de clave pública que hacen un uso intensivo de la CPU. La mayoría de las operaciones de apretón de manos están asociadas con el intercambio de la clave de sesión SSL (mensaje de intercambio de claves de cliente). Cuando una sesión de cliente está inactiva durante algún tiempo y, a continuación, se reanuda, el protocolo de enlace SSL se lleva a cabo de nuevo. Con la reutilización de sesión habilitada, se evita el intercambio de claves de sesión para las solicitudes de reanudación de sesión recibidas del cliente.

La reutilización de sesiones está habilitada en el dispositivo Citrix ADC de forma predeterminada. Habilitar esta función reduce la carga del servidor, mejora el tiempo de respuesta y aumenta la cantidad de transacciones SSL por segundo (TPS) que el servidor puede admitir.

Configurar la reutilización de sesiones mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para configurar la reutilización de sesiones y verificar la configuración:

```
set ssl vserver <vServerName> -sessReuse ( ENABLED | DISABLED ) -
   sessTimeout <positive_integer>
show ssl vserver <vServerName>
<!--NeedCopy-->
```

Ejemplo:

```
set ssl vserver vs-ssl -sessreuse enabled -sesstimeout 600
 Done

show ssl vserver vs-ssl

        Advanced SSL configuration for VServer vs-ssl:
        DH: DISABLED
        Ephemeral RSA: ENABLED          Refresh Count: 1000
        Session Reuse: ENABLED          Timeout: 600 seconds
        Cipher Redirect: DISABLED
        SSLv2 Redirect: DISABLED
        ClearText Port: 0
        Client Auth: DISABLED
        SSL Redirect: DISABLED
        Non FIPS Ciphers: DISABLED
        SNI: DISABLED
        OCSP Stapling: DISABLED
        HSTS: DISABLED
        HSTS IncludeSubDomains: NO
        HSTS Max-Age: 0
        SSLv2: DISABLED SSLv3: ENABLED  TLSv1.0: ENABLED TLSv1.2:
           ENABLED  TLSv1.2: ENABLED

1)      CertKey Name: Auth-Cert-1       Server Certificate

1)      Cipher Name: DEFAULT
```



```
        Description: Predefined Cipher Alias
 Done
<!--NeedCopy-->
```

Configurar la reutilización de sesiones mediante la GUI

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**y abra un servidor virtual.
2. En la sección **Parámetros SSL**, seleccione **Habilitar la reutilización de la sesión**y especifique el tiempo durante el que quiere mantener la sesión activa.

Configuración del protocolo SSL

El dispositivo Citrix ADC admite los protocolos SSLv3, TLSv1, TLSv1.1 y TLSv1.2. Cada uno de estos protocolos se puede configurar en el dispositivo según lo requiera la implementación y el tipo de clientes que se conectan al dispositivo.

Las versiones 1.0, 1.1 y 1.2 del protocolo TLS son más seguras que las versiones anteriores del protocolo TLS/SSL. Sin embargo, para admitir sistemas heredados, muchas implementaciones de TLS mantienen la compatibilidad con versiones anteriores del protocolo SSLv3. En un protocolo de enlace SSL, se utiliza la versión de protocolo más alta común para el cliente y el servidor virtual SSL configurado en el dispositivo Citrix ADC.

En el primer intento de establecimiento de enlace, un cliente TLS ofrece la versión de protocolo más alta que admite. Si el apretón de manos falla, el cliente ofrece una versión de protocolo inferior. Por ejemplo, si un apretón de manos con la versión 1.1 de TLS no tiene éxito, el cliente intenta renegociar ofreciendo el protocolo TLSv1.0. Si el intento no es correcto, el cliente vuelve a intentar con el protocolo SSLv3. Un atacante “hombre en el medio” (MITM) puede romper el apretón de manos inicial y desencadenar la renegociación con el protocolo SSLv3, y luego explotar una vulnerabilidad en SSLv3. Para mitigar tales ataques, puede inhabilitar SSLv3 o no permitir la renegociación mediante un protocolo degradado. Sin embargo, este enfoque puede no resultar práctico si su implementación incluye sistemas heredados. Una alternativa es reconocer un valor de conjunto de cifrado de señalización (TLS_FALLBACK_SCSV) en la solicitud del cliente.

Un valor TLS_FALLBACK_SCSV en un mensaje de saludo del cliente indica al servidor virtual que el cliente ha intentado conectarse anteriormente con una versión de protocolo superior y que la solicitud actual es una alternativa. Si el servidor virtual detecta este valor y admite una versión superior a la indicada por el cliente, rechaza la conexión con una alerta grave. El apretón de manos se realiza correctamente si se cumple una de las siguientes condiciones:

- El valor TLS_FALLBACK_SCSV no se incluye en el mensaje de saludo del cliente.

- La versión del protocolo en el saludo del cliente es la versión de protocolo más alta admitida por el servidor virtual.

Configurar la compatibilidad con el protocolo SSL mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para configurar la compatibilidad con el protocolo SSL y verificar la configuración:

```
set ssl vserver <vServerName> -ssl2 ( ENABLED | DISABLED ) -ssl3 (
    ENABLED | DISABLED ) -tls1 ( ENABLED | DISABLED ) -tls11 ( ENABLED |
     DISABLED ) -tls12 ( ENABLED | DISABLED )

show ssl vserver <vServerName>
<!--NeedCopy-->
```

Ejemplo:

```
set ssl vserver vs-ssl -tls11 ENABLED -tls12 ENABLED
Done

sh ssl vs vs-ssl

        Advanced SSL configuration for VServer vs-ssl:
            DH: DISABLED
            Ephemeral RSA: ENABLED                              Refresh
               Count: 0
            Session Reuse: ENABLED                                Timeout
               : 120 seconds
            Cipher Redirect: DISABLED
            SSLv2 Redirect: DISABLED
            ClearText Port: 0
            Client Auth: DISABLED
            SSL Redirect: DISABLED
            Non FIPS Ciphers: DISABLED
            SNI: DISABLED
            SSLv2: DISABLED        SSLv3: ENABLED    TLSv1.0: ENABLED
               TLSv1.1: ENABLED  TLSv1.2: ENABLED
            Push Encryption Trigger: Always
            Send Close-Notify: YES
            1 bound certificate:

    1)      CertKey Name: mycert  Server Certificate
```



```
23              1 configured cipher:
24
25      1)      Cipher Name: DEFAULT
26              Description: Predefined Cipher Alias
27
28  Done
29  <!--NeedCopy-->
```

Configurar la compatibilidad con el protocolo SSL mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**y abra un servidor virtual.
2. En la sección **Parámetros SSL**, seleccione un protocolo para habilitarlo.

Cerrar notificar

Una notificación cercana es un mensaje seguro que indica el final de la transmisión de datos SSL. Se requiere una configuración de notificación cercana a nivel global. Esta configuración se aplica a todos los servidores, servicios y grupos de servicios virtuales. Para obtener información sobre la configuración global, consulte la sección “Parámetros SSL globales” más adelante en esta página.

Además de la configuración global, puede establecer el parámetro de notificación de cierre en el nivel de servidor virtual, servicio o grupo de servicios. Por lo tanto, tiene la flexibilidad de establecer el parámetro para una entidad y desconfigurarlo para otra entidad. Sin embargo, asegúrese de establecer este parámetro a nivel global. De lo contrario, la configuración a nivel de entidad no se aplica.

Configurar la notificación de cierre a nivel de entidad mediante la CLI

En el símbolo del sistema, escriba cualquiera de los siguientes comandos para configurar la función de notificación de cierre y verificar la configuración:

1. Para configurar en el nivel de servidor virtual, escriba:

```
1  set ssl vserver <vServerName> -sendCloseNotify ( YES | NO )
2  show ssl vserver <vServerName>
3  <!--NeedCopy-->
```

1. Para configurar en el nivel de servicio, escriba:


```
set ssl service <serviceName> -sendCloseNotify ( YES | NO )
show ssl service <serviceName>
<!--NeedCopy-->
```

1. Para configurar en el nivel de grupo de servicios, escriba:

```
set ssl serviceGroup <serviceGroupName> -sendCloseNotify ( YES | NO )
show ssl serviceGroup <serviceGroupName>
<!--NeedCopy-->
```

Ejemplo:

```
set ssl vserver sslvsvr -sendCloseNotify YES

Done
<!--NeedCopy-->
```

Configurar la función de notificación de cierre en el nivel de entidad mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**y abra un servidor virtual.
2. En la sección **Parámetros SSL**, seleccione **Enviar notificación cerrada**.

Parámetros SSL globales

La personalización avanzada de su configuración SSL aborda problemas específicos. Puede usar el comando `set ssl parameter` o la utilidad de configuración para especificar lo siguiente:

- Tamaño cuántico que se utilizará para las transacciones SSL.
- Tamaño de memoria CRL.
- Tamaño de caché de OCSP.
- Denegar la renegociación de SSL.
- Defina el indicador PUSH para los registros descifrados, cifrados o todos.
- Descarta las solicitudes si el cliente inicia el apretón de manos para un dominio y envía una solicitud HTTP para otro dominio.
- Defina el tiempo tras el que se activa el cifrado.
  Nota: El tiempo que especifique solo se aplica si utiliza el

`set ssl vserver` comando o la utilidad de configuración para establecer el cifrado basado en temporizador.

- Comprobación del certificado de conformidad de NDCPP: se aplica cuando el dispositivo actúa como cliente (conexión back-end). Durante la verificación del certificado, ignore el nombre común si la SAN está presente en el certificado SSL.
- Habilite un clúster heterogéneo de dispositivos basados en chips Cavium, como MPX 14000, y dispositivos basados en chips Intel Coleto, como dispositivos MPX 15000 con una cantidad diferente de motores de paquetes. (Compatibilidad agregada en la versión 13.0 compilación 47.x).
- Habilite la renegociación segura en el back-end (función agregada desde la versión 1.0, compilación 58.x).
- Control de tráfico SSL adaptable (compatibilidad agregada en la versión 13.0 compilación 58.x).

Configurar parámetros SSL globales mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para configurar los valores SSL avanzados y verificar la configuración:

```
set ssl parameter [-quantumSize <quantumSize>] [-crlMemorySizeMB <
    positive_integer>] [-strictCAChecks (YES | NO)] [-sslTriggerTimeout
    <positive_integer>] [-sendCloseNotify (YES | NO)] [-
    encryptTriggerPktCount <positive_integer>] [-denySSLReneg <
    denySSLReneg>] [-insertionEncoding (Unicode|UTF-8)] [-ocspCacheSize
    <positive_integer>][- pushFlag <positive_integer>] [-
    dropReqWithNoHostHeader (YES | NO)] [-pushEncTriggerTimeout <
    positive_integer>] [-ndcppComplianceCertCheck ( YES | NO)] [-
    heterogeneousSSLHW (ENABLED | DISABLED )]
show ssl parameter
<!--NeedCopy-->
```

Ejemplo:

```
set ssl parameter -quantumSize 8 -crlMemorySizeMB 256 -strictCAChecks
    no -ssltriggerTimeout 100 -sendClosenotify no -
    encryptTriggerPktCount 45 -denySSLReneg NONSECURE -insertionEncoding
     unicode -ocspCacheSize 10 -pushFlag 3 -dropReqWithNoHostHeader YES
     -pushEncTriggerTimeout 100 ms -ndcppComplianceCertCheck YES
Done

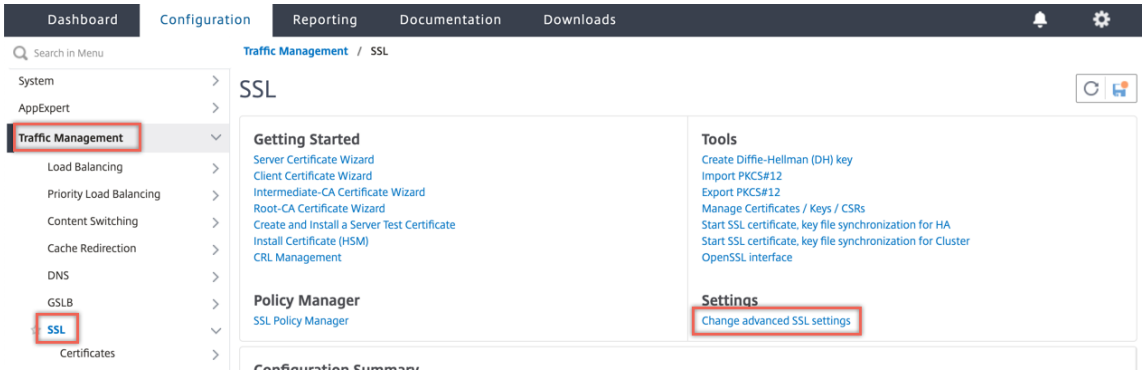
show ssl parameter
```



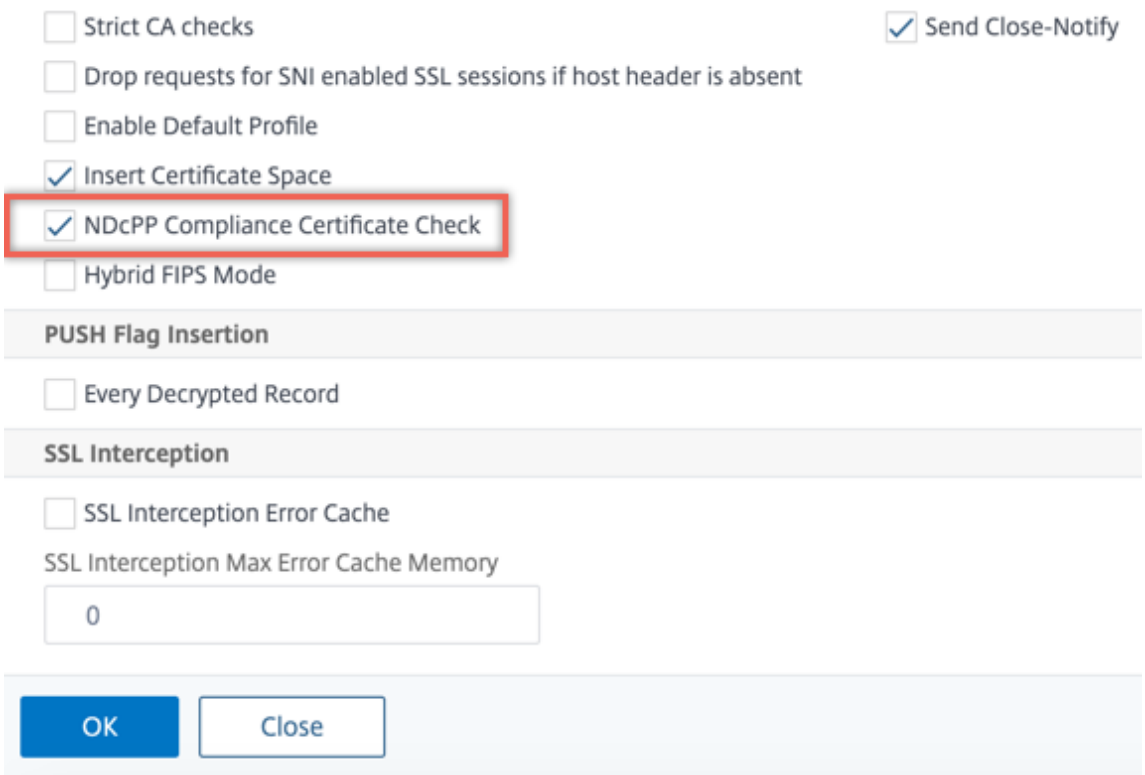
```
Advanced SSL Parameters
-----------------------
    SSL quantum size                                    : 8 KB
    Max CRL memory size                                 : 256 MB
    Strict CA checks                                    : NO
    Encryption trigger timeout                          : 100 ms
    Send Close-Notify                                   : NO
    Encryption trigger packet count                     : 45
    Deny SSL Renegotiation                              : NONSECURE
    Subject/Issuer Name Insertion Format                : Unicode
    OCSP cache size                                     : 10 MB
    Push flag                                           : 0x3 (On
       every decrypted and encrypted record)
    Strict Host Header check for SNI enabled SSL sessions : YES
    PUSH encryption trigger timeout                     : 100 ms
    Crypto Device Disable Limit                         : 0
    Global undef action for control policies            : CLIENTAUTH
    Global undef action for data policies               : NOOP
    Default profile                                     : DISABLED
    SSL Insert Space in Certificate Header              : YES
    Disable TLS 1.1/1.2 for SSL_BRIDGE secure monitors  : NO
    Disable TLS 1.1/1.2 for dynamic and VPN services    : NO
    Software Crypto acceleration CPU Threshold          : 0
    Hybrid FIPS Mode                                    : DISABLED
    Signature and Hash Algorithms supported by TLS1.2   : ALL
    SSL Interception Error Learning and Caching         : DISABLED
    SSL Interception Maximum Error Cache Memory         : 0 Bytes
    NDCPP Compliance Certificate Check                  : YES
    Heterogeneous SSL HW (Cavium and Intel Based)       : ENABLED
 Done
<!--NeedCopy-->
```

Configurar la comprobación de certificados de conformidad de NDcPP mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > SSL** y, en el grupo **Configuración**, seleccione **Cambiar la configuración SSL avanzada**.



2. Seleccione **Comprobación del certificado de conformidad del NDCPP**. Haga clic en **Aceptar**.



Compatibilidad con renegociación segura en el back-end de un dispositivo Citrix ADC

Nota: Esta función se admite en la versión 13.0 compilación 58.x y posteriores. En versiones y compilaciones anteriores, solo se admitía la renegociación no segura en el back-end.

La función se admite en las siguientes plataformas:

- VPX
- Plataformas MPX que contienen chips N2 o N3
- Plataformas basadas en chip Intel Coleto SSL

La función aún no se admite en la plataforma FIPS.

La renegociación segura se deniega de forma predeterminada en el back-end de un dispositivo ADC. Es decir, el parámetro denySSLReneg se establece en ALL (predeterminado).

Para permitir la renegociación segura en el back-end, seleccione una de las siguientes configuraciones para el parámetro denySSLReneg:

- NO
- FRONTEND_CLIENT
- FRONTEND_CLIENTSERVER
- NO SEGURO

Habilite la renegociación segura mediante la CLI

En el símbolo del sistema, escriba:

```
set ssl parameter -denySSLReneg <denySSLReneg>
```

Ejemplo:

```
set ssl parameter -denySSLReneg NONSECURE
 Done

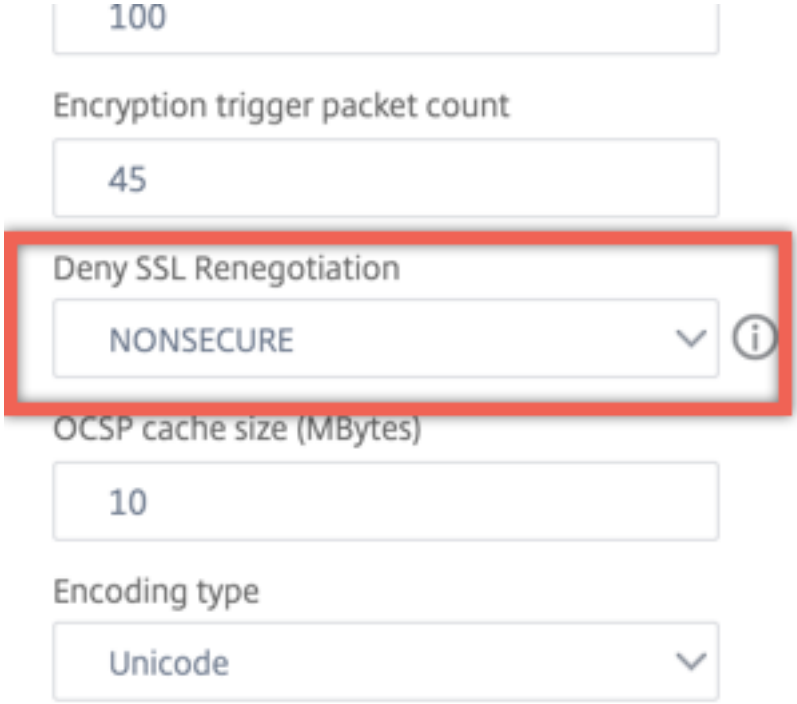
sh ssl parameter
Advanced SSL Parameters
-----------------------
    SSL quantum size                                    : 8 KB
    Max CRL memory size                                 : 256 MB
    Strict CA checks                                    : NO
    Encryption trigger timeout                          : 100 ms
    Send Close-Notify                                   : YES
    Encryption trigger packet count                     : 45
    Deny SSL Renegotiation                              : NONSECURE
    Subject/Issuer Name Insertion Format                : Unicode
    OCSP cache size                                     : 10 MB
    Push flag                                           : 0x0 (Auto)
    Strict Host Header check for SNI enabled SSL sessions : NO
    Match HTTP Host header with SNI                     : CERT
    PUSH encryption trigger timeout                     : 1 ms
    Crypto Device Disable Limit                         : 0
    Global undef action for control policies            : CLIENTAUTH
    Global undef action for data policies               : NOOP
    Default profile                                     : ENABLED
    SSL Insert Space in Certificate Header              : YES
    Disable TLS 1.1/1.2 for SSL_BRIDGE secure monitors  : NO
    Disable TLS 1.1/1.2 for dynamic and VPN services    : NO
```



```
    Software Crypto acceleration CPU Threshold              : 0
    Hybrid FIPS Mode                                        : DISABLED
    Signature and Hash Algorithms supported by TLS1.2       : ALL
    SSL Interception Error Learning and Caching             : DISABLED
    SSL Interception Maximum Error Cache Memory             : 0 Bytes
    NDCPP Compliance Certificate Check                      : NO
    Heterogeneous SSL HW (Cavium and Intel Based)           : DISABLED
    Crypto Operation Queue Limit                            : 150%
 Done
<!--NeedCopy-->
```

Habilite la renegociación segura mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > SSL > Cambiar la configuración avanzada de SSL**.
2. Establezca **Denegar renegociación SSL** en cualquier valor que no sea ALL.



Control de tráfico SSL adaptativo

Nota: Esta función se admite en la versión 13.0 compilación 58.x y posteriores.

Cuando se recibe mucho tráfico en el dispositivo y la capacidad de aceleración criptográfica está llena, el dispositivo comienza a poner en cola las conexiones para procesarlas más adelante. Actualmente, el tamaño de esta cola se fija en 64 K y el dispositivo comienza a interrumpir las conexiones si se supera este valor.

A partir de la versión 13.0 build 58.x, el usuario puede configurar un valor que sea un porcentaje de la capacidad real. Con esta mejora, el dispositivo pierde nuevas conexiones si el número de elementos en la cola es mayor que el límite que se calcula de forma adaptativa y dinámica. Este enfoque controla las conexiones SSL entrantes y evita el consumo excesivo de recursos y otros errores, como el error de supervisión del equilibrio de carga o la respuesta lenta a las aplicaciones seguras, en el dispositivo.

Si la cola está vacía, el dispositivo puede seguir aceptando conexiones. Si la cola no está vacía, el sistema de cifrado ha alcanzado su capacidad y el dispositivo comienza a poner en cola las conexiones.

El límite se calcula en función de:

- La capacidad real del dispositivo.
- Valor configurado por el usuario como porcentaje de la capacidad real. El valor predeterminado se establece en 150%.

Por ejemplo, si la capacidad real de un dispositivo es de 1000 operaciones/segundo en un momento dado y se configura el porcentaje predeterminado, el límite después del cual el dispositivo interrumpe las conexiones es de 1500 (150% de 1000).

Para configurar el límite de cola de operaciones mediante la CLI

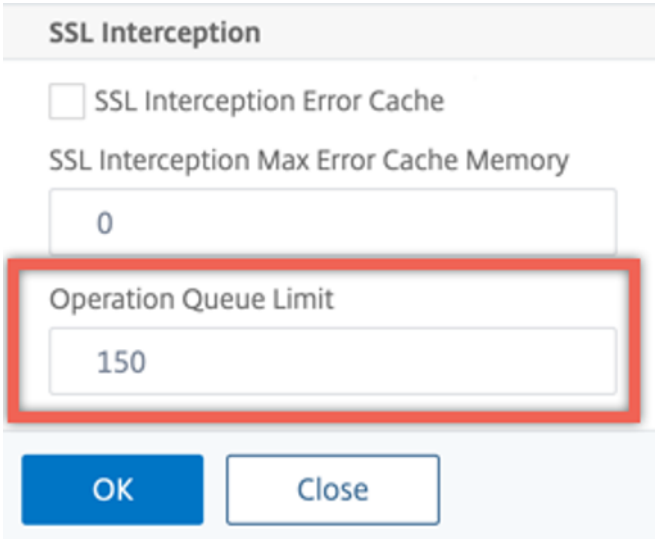
En el símbolo del sistema, escriba:

```
set ssl parameter -operationQueueLimit <positive_integer>
```

Límite de**cola de operaciones: límite** en porcentaje de la capacidad de la cola de operaciones criptográficas más allá del cual no se aceptan nuevas conexiones SSL hasta que se reduzca la cola. Valor por defecto: 150. Valor mínimo: 0. Valor máximo: 10000.

Para configurar el límite de cola de operaciones mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > SSL**.
2. En **Parámetros**, haga clic en **Cambiar parámetros SSL avanzados**.
3. Escriba un valor en **Límite de cola de operaciones**. El valor predeterminado es 150.
4. Haga clic en **Aceptar**.



Implementaciones de clústeres heterogéneos

A partir de la versión 13.0 compilación 47.x, puede formar una implementación heterogénea en clúster de dispositivos Citrix ADC MPX con un número diferente de motores de paquetes configurando el parámetro SSL “HW SSL heterogéneo” en HABILITADO. Por ejemplo, para formar un clúster de dispositivos basados en chips Cavium (MPX 14000 o similar) y dispositivos basados en chip Intel Coleto (MPX 15000 o similar), habilite el parámetro SSL “HW SSL heterogéneo”. Para formar un clúster de plataformas con el mismo chip, mantenga el valor predeterminado (DISABLED) para este parámetro.

> **Notas:**
>
> Las siguientes funciones no se admiten en un clúster heterogéneo:
>
> - Instancias VPX alojadas en dispositivos Citrix ADC SDX.
> - Protocolo SSLv3 en entidades SSL, como servidores virtuales, servicios, grupos de servicios y servicios internos.
> - Umbral de CPU de aceleración criptográfica de software (mediante hardware y software para mejorar el rendimiento del cifrado ECDSA y ECDHE).

Para obtener más información sobre las plataformas admitidas en un clúster heterogéneo, consulte https://docs.citrix.com/en-us/citrix-adc/current-release/clustering/support-for-heterogeneous-cluster.html.

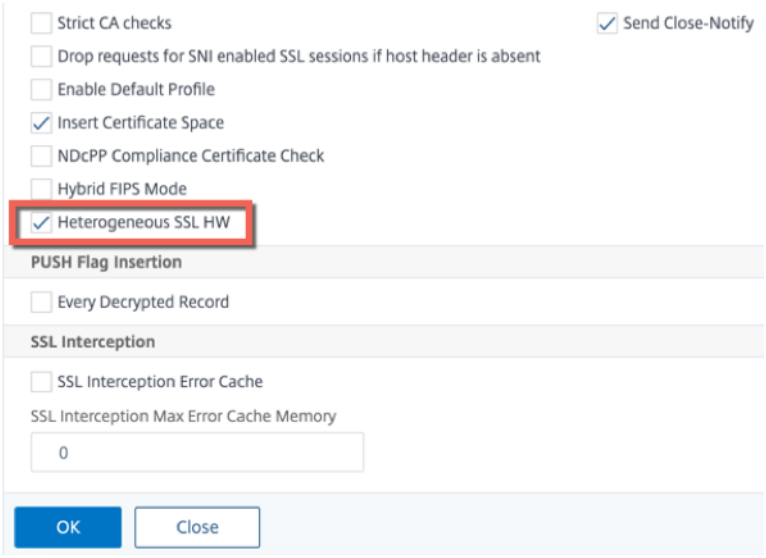
Habilitar un clúster heterogéneo mediante la CLI

En el símbolo del sistema, escriba:

```
set ssl parameter -heterogeneousSSLHW ENABLED
```


Habilitar un clúster heterogéneo mediante la GUI

1. Vaya a **Administración del tráfico > SSL** y, en el grupo **Configuración**, seleccione **Cambiar la configuración SSL avanzada**.
2. Seleccione **HW SSL heterogéneo**. Haga clic en **Aceptar**.



Mecanismo desencadenador de cifrado basado en indicadores PUSH

El mecanismo de activación de cifrado que se basa en el indicador TCP de PSH ahora le permite hacer lo siguiente:

- Combine paquetes consecutivos en los que el indicador PSH esté configurado en un único registro SSL, o ignore el indicador PSH.
- Realice un cifrado basado en temporizador, en el que el valor de tiempo de espera se establece globalmente mediante el comando `set ssl parameter -pushEncTriggerTimeout <positive_integer>`.

Configurar el cifrado basado en marcas PUSH mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para configurar el cifrado basado en marcas PUSH y verificar la configuración:

```
1 set ssl vserver <vServerName> [-pushEncTrigger <pushEncTrigger>]
2
3 show ssl vserver
4 <!--NeedCopy-->
```


Ejemplo:

```
set ssl vserver vserver1 -pushEncTrigger always

Done

sh ssl vserver vserver1

            Advanced SSL configuration for VServer vserver1:
            DH: DISABLED
            DH Private-Key Exponent Size Limit: DISABLED    Ephemeral
                RSA: ENABLED

                Refresh Count: 0
            Session Reuse: ENABLED          Timeout: 120 seconds
            Cipher Redirect: DISABLED
            SSLv2 Redirect: DISABLED
            ClearText Port: 0
            Client Auth: DISABLED
            SSL Redirect: DISABLED
            Non FIPS Ciphers: DISABLED
            SNI: DISABLED
            OCSP Stapling: DISABLED
            HSTS: DISABLED
            HSTS IncludeSubDomains: NO
            HSTS Max-Age: 0
            SSLv2: DISABLED  SSLv3: ENABLED  TLSv1.0: ENABLED  TLSv1.1:
                ENABLED  TLSv1.2: ENABLED  TLSv1.3: DISABLED
            Push Encryption Trigger: Always
            Send Close-Notify: YES
            Strict Sig-Digest Check: DISABLED
            Zero RTT Early Data: DISABLED
            DHE Key Exchange With PSK: NO
            Tickets Per Authentication Context: 1
            ECC Curve: P_256, P_384, P_224, P_521

    1)      Cipher Name: DEFAULT
            Description: Default cipher list with encryption strength
                >= 128bit
Done
<!--NeedCopy-->
```


Configurar el cifrado basado en indicadores PUSH mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales** y abra un servidor virtual SSL.
2. En la sección **Parámetros SSL**, en la lista **Desencadenador de cifrado PUSH**, seleccione un valor.

Compatibilidad con el algoritmo hash de firma TLS1.2

El dispositivo Citrix ADC cumple completamente con la extensión hash de firma TLS1.2.

En un protocolo de enlace SSL, un cliente envía una lista de algoritmos hash de firma admitidos. El cliente indica al servidor qué pares de algoritmos hash de firma se pueden usar en los mensajes de enlace SSL (SKE y CCV) mediante la extensión "signature_algorithms". El campo "extension_data" de esta extensión contiene un valor "supported_signature_algorithms" en el mensaje Client Hello. El protocolo de enlace SSL continúa si el servidor admite uno de estos algoritmos de hash de firma. Si el servidor no admite ninguno de estos algoritmos, se interrumpe la conexión.

Del mismo modo, si el servidor solicita un certificado de cliente para la autenticación de clientes, el mensaje de solicitud de certificado contiene un valor "supported_signature_algorithms". El certificado de cliente se selecciona en función de este algoritmo de hash de firma.

> **Nota:**
>
> El dispositivo Citrix ADC actúa como servidor para un cliente y como cliente para el servidor back-end.

El dispositivo solo admite RSA-SHA1 y RSA-SHA256 en el front-end, y RSA-MD5, RSA-SHA1 y RSA-SHA256 en el back-end.

El dispositivo MPX/SDX/VPX admite las siguientes combinaciones de hash de firma. En un dispositivo SDX, si se asigna un chip SSL a una instancia VPX, se aplica la compatibilidad de cifrado de un dispositivo MPX. De lo contrario, se aplica la función de cifrado normal de una instancia VPX.

- En una instancia VPX y en un dispositivo MPX/SDX sin chips N3:
  - RSA-MD5
  - RSA-SHA1
  - RSA-SHA224
  - RSA-SHA256
  - RSA-SHA384
  - RSA-SHA512
- En un dispositivo MPX/SDX con chips N3:
  - RSA-MD5
  - RSA-SHA1
  - RSA-SHA224

- RSA-SHA256
- RSA-SHA384
- RSA-SHA512
- ECDSA-SHA1
- ECDSA-SHA224
- ECDSA-SHA256
- ECDSA-SHA384
- ECDSA-SHA512

De forma predeterminada, todos los algoritmos de hash de firma están habilitados. Sin embargo, solo puede habilitar unos pocos algoritmos de hash de firma mediante el siguiente comando:

```
1  set ssl parameter -sigDigestType <sigDigestType>
2
3  Parameters
4
5  sigDigestType
6
7  Signature digest algorithms supported by the appliance. The platform
       determines the list of algorithms supported by default.
8
9                 On VPX: RSA-MD5 RSA-SHA1 RSA-SHA224 RSA-SHA256 RSA-SHA384
                      RSA-
10
11                SHA512
12
13                On MPX with N3 cards: RSA-MD5 RSA-SHA1 RSA-SHA224 RSA-
14
15                SHA256 RSA-SHA384 RSA-SHA512 ECDSA-SHA1 ECDSA-SHA224
                      ECDSA-
16
17                SHA256 ECDSA-SHA384 ECDSA-SHA512
18
19                Other MPX Platforms: RSA-MD5 RSA-SHA1 RSA-SHA224 RSA-
                      SHA256 RSA-SHA384 RSA-
20
21                SHA512.
22
23     set ssl parameter -sigDigestType RSA-SHA224 RSA-SHA256 RSA-SHA384
          RSA-SHA512
24 <!--NeedCopy-->
```


Validar el certificado de pares

Según RFC 5246, el certificado de pares debe firmarse con uno de los algoritmos hash de firma incluidos en la extensión Client Hello. Puede usar el parámetro `strictSigDigestCheck`. En función de la lista hash de firmas enviada por el cliente, si se habilita `strictSigDigestCheck`, el dispositivo devuelve un certificado firmado por uno de los algoritmos hash de firma mencionados en la extensión Client Hello. Si el par no tiene un certificado adecuado, se interrumpe la conexión. Si este parámetro está inhabilitado, el hash de firma no se comprueba en el certificado de pares.

Puede configurar una verificación de resumen de firmas estricta en un servidor y servicio virtual SSL. Si habilita este parámetro en un servidor virtual SSL, el certificado de servidor enviado por el servidor debe estar firmado por uno de los algoritmos hash de firma enumerados en la extensión Client Hello. Si la autenticación de clientes está habilitada, el certificado de cliente recibido por el servidor debe firmarse con uno de los algoritmos de hash de firma que se enumeran en la solicitud de certificado enviada por el servidor.

Si habilita este parámetro en un servicio SSL, el certificado de servidor recibido por el cliente debe estar firmado por uno de los algoritmos hash de firma enumerados en la extensión Client Hello. El certificado de cliente debe firmarse con uno de los algoritmos hash de firma que se enumeran en el mensaje de solicitud de certificado.

Si el perfil predeterminado está habilitado, puede usarlo para configurar una verificación de resumen de firma estricta en un servidor virtual SSL, un servicio SSL y un perfil SSL.

Configurar la verificación de resumen de firmas estricta en un servidor, servicio o perfil virtual SSL mediante la CLI

En el símbolo del sistema, escriba:

```
set ssl vserver <vServerName> -strictSigDigestCheck ( ENABLED |
   DISABLED )

set ssl service <serviceName> -strictSigDigestCheck ( ENABLED |
   DISABLED )

set ssl profile <name>-strictSigDigestCheck ( ENABLED | DISABLED )

Parameters

strictSigDigestCheck

             Check whether peer entity certificate is signed using one
                 of the signature-hash algorithms supported by the
```



```
                    Citrix ADC appliance.

                Possible values: ENABLED, DISABLED

                Default: DISABLED
<!--NeedCopy-->
```

Ejemplo:

```
set ssl vserver v1 -strictSigDigestCheck Enabled
set ssl service s1 -strictSigDigestCheck Enabled
set ssl profile p1 -strictSigDigestCheck Enabled
<!--NeedCopy-->
```

> **Importante:**
>
> Si los cifrados DH, ECDHE o ECDSA están configurados en el dispositivo, el mensaje SKE debe firmarse con uno de los hashes de firma comunes a la lista de clientes y la lista configurada en el dispositivo. Si no hay un hash de firma común, se elimina la conexión.

Configurar SSL para el acceso a la interfaz de usuario del administrador

Se requiere un par de claves de certificado para el acceso HTTPS a la utilidad de configuración y para las llamadas seguras a procedimientos remotos. En un dispositivo Citrix ADC MPX o un dispositivo virtual VPX, un par de claves de certificado se vincula automáticamente a los servicios internos. Sin embargo, es posible que los exploradores no confíen en este certificado. Debe cargar certificados de CA válidos en el explorador para completar la autenticación sin errores.

Configurar HTTPS seguro mediante la CLI

Para configurar HTTPS seguro mediante la CLI, siga estos pasos:

1. Agregue un par de claves de certificado.

```
add certkey server -cert servercert -key serverkey
<!--NeedCopy-->
```

2. Enlazar este par de claves de certificado a los siguientes servicios internos.


```
bind ssl service nshttps-127.0.0.1-443 -certkeyname server

bind ssl service nshttps-::11-443 -certkeyname server
<!--NeedCopy-->
```

Configurar HTTPS seguro mediante la GUI

Para configurar HTTPS seguro mediante la GUI, siga estos pasos:

1. Vaya a **Administración del tráfico > SSL > Certificados**.
2. En el panel de detalles, haga clic en **Instalar**.
3. En el cuadro de diálogo **Instalar certificado**, escriba los detalles del certificado.
4. Haga clic en **Instalar** y, después, en **Cerrar**.
5. Vaya a **Administración del tráfico > Equilibrio de carga > Servicios**.
6. En el panel de detalles, en la ficha **Acción**, haga clic en **Servicios internos**.
7. Seleccione `nshttps-127.0.0.1-443` de la lista y, a continuación, haga clic en **Abrir**.
8. En la ficha **Configuración de SSL**, en el panel **Disponible**, seleccione el certificado creado en el paso 4, haga clic en **Vincular** y, a continuación, haga clic en **Aceptar**.
9. Seleccione `nshttps-::11-443` de la lista y, a continuación, haga clic en **Abrir**.
10. En la ficha **Configuración de SSL**, en el panel **Disponible**, seleccione el certificado creado en el paso 4, haga clic en **Vincular** y, a continuación, haga clic en **Aceptar**.
11. Haga clic en **Aceptar**.

Compatibilidad con protocolos TLSv1.3 tal como se define en RFC 8446

July 27, 2022

Los dispositivos Citrix ADC VPX y Citrix ADC MPX ahora admiten el protocolo TLSv1.3, especificado en RFC 8446.

> **Notas:**
>
> - A partir de la versión 13.0 compilación 71.x y versiones posteriores, la aceleración de hardware TLS1.3 es compatible con las siguientes plataformas:
>   - MPX 5900
>   - MPX/SDX 8900
>   - MPX/SDX 9100
>   - MPX/SDX 15000
>   - MPX/SDX 15000-50G

  - MPX/SDX 26000
  - MPX/SDX 26000-50S
  - MPX/SDX 26000-100G

- La compatibilidad con solo software para el protocolo TLSV1.3 está disponible en todos los demás dispositivos Citrix ADC MPX y SDX, excepto los dispositivos Citrix ADC FIPS.

- TLSV1.3 solo es compatible con el perfil mejorado. Para habilitar el perfil mejorado, consulte Habilitar el perfil mejorado.
- Para utilizar TLS1.3, debe utilizar un cliente que cumpla con la especificación RFC 8446.

Funciones de Citrix ADC compatibles

Se admiten las siguientes funciones SSL:

1. Suites de cifrado TLSv1.3:
   - TLS1.3-AES256-GCM-SHA384 (0x1302)
   - TLS1.3_CHACHA20_POLY1305_SHA256 (0x1303)
   - TLS1.3-AES128_GCM-SHA256 (0x1301)
2. Curvas ECC para el intercambio efímero de claves Diffie-Hellman:
   - P_256
   - P_384
   - P_521
3. Contactos iniciales (handshakes) abreviados cuando la reanudación de sesión basada en tíquets está habilitada
4. Datos de aplicación temprana 0-RTT
5. Autenticación de cliente basada en certificados opcional u obligatoria, con la función de validación de OCSP y CRL de certificados de cliente
6. Extensión de nombre de servidor: selección de certificados de servidor mediante SNI
7. Negociación del protocolo de aplicación (ALPN) mediante la extensión application_level_protocol_negotiati
8. Grapado OCSP
9. Los mensajes de registro y los registros de AppFlow se generan para los apretones de manos TLSv1.3.
10. Registro opcional de secretos de tráfico TLS 1.3 mediante la utilidad `nstrace` de captura de paquetes.
11. Interoperabilidad con clientes TLS que implementan RFC 8446. Por ejemplo, Mozilla Firefox, Google Chrome y OpenSSL.

Exploradores web compatibles

Las siguientes versiones del explorador son compatibles y compatibles con la implementación de Citrix ADC del protocolo TLS 1.3:

- Google Chrome - Versión 72.0.3626.121 (compilación oficial) (64 bits)
- Mozilla Firefox - 65.0.2 (64 bits)
- Opera - Versión:58.0.3135.79

Configuración

TLSv1.3 está inhabilitado de forma predeterminada en un perfil SSL.

Agregar un perfil SSL mediante la CLI

En el símbolo del sistema, escriba:

```
add ssl profile <tls13-profile-name>
<!--NeedCopy-->
```

Ejemplo:

```
add ssl profile tls13profile

sh ssl profile tls13profile
1)  Name: tls13profile           (Front-End)
    SSLv3: DISABLED               TLSv1.0: ENABLED  TLSv1.1: ENABLED
       TLSv1.2: ENABLED  TLSv1.3: DISABLED
    Client Auth: DISABLED
    Use only bound CA certificates: DISABLED
    Strict CA checks:   NO
    Session Reuse: ENABLED                      Timeout: 120 seconds
    DH: DISABLED
    DH Private-Key Exponent Size Limit: DISABLED   Ephemeral RSA:
       ENABLED                             Refresh Count: 0
    Deny SSL Renegotiation                                ALL
    Non FIPS Ciphers: DISABLED
    Cipher Redirect: DISABLED
    SSL Redirect: DISABLED
    Send Close-Notify: YES
    Strict Sig-Digest Check: DISABLED
    Zero RTT Early Data: DISABLED
```



```
    DHE Key Exchange With PSK: NO
    Tickets Per Authentication Context: 1
    Push Encryption Trigger: Always
    PUSH encryption trigger timeout:             1 ms
    SNI: DISABLED
    OCSP Stapling: DISABLED
    Strict Host Header check for SNI enabled SSL sessions: NO
    Push flag:            0x0 (Auto)
    SSL quantum size:                            8 kB
    Encryption trigger timeout           100 mS
    Encryption trigger packet count:               45
    Subject/Issuer Name Insertion Format: Unicode

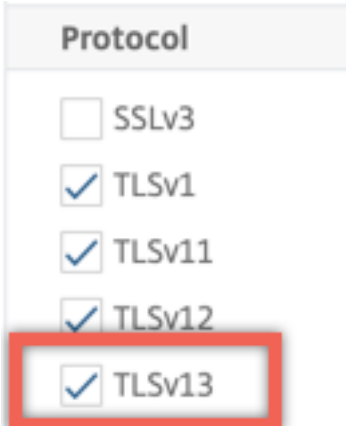
    SSL Interception: DISABLED
    SSL Interception OCSP Check: ENABLED
    SSL Interception End to End Renegotiation: ENABLED
    SSL Interception Maximum Reuse Sessions per Server:  10
    Session Ticket: DISABLED
    HSTS: DISABLED
    HSTS IncludeSubDomains: NO
    HSTS Max-Age: 0

    ECC Curve: P_256, P_384, P_224, P_521

1)  Cipher Name: DEFAULT Priority :1
    Description: Predefined Cipher Alias
Done
<!--NeedCopy-->
```

Agregar un perfil SSL mediante la interfaz gráfica de usuario

1. Vaya a **Sistema > Perfiles**. Seleccione **Perfiles SSL**.
2. Haga clic en **Agregar** y especifique un nombre para el perfil.
3. En **Protocolo**, seleccione **TLSv13**.



4. Haga clic en **Aceptar**.

Enlazar un perfil SSL a un servidor virtual SSL mediante la CLI

En el símbolo del sistema, escriba:

```
set ssl vserver <vServerName> -sslProfile <tls13-profile-name>
<!--NeedCopy-->
```

Ejemplo:

```
set ssl vserver ssl-vs -sslProfile tls13profile
```

Enlazar un perfil SSL a un servidor virtual SSL mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**y seleccione un servidor virtual SSL.
2. En **Configuración avanzada**, haga clic en **Perfil SSL**.
3. Seleccione el perfil TLSv1.3 creado anteriormente.
4. Haga clic en **Aceptar**.
5. Haga clic en **Listo**.

Parámetros de perfil SSL para el protocolo TLSv1.3

1. Habilite o inhabilite los parámetros TLS1.3 en un perfil SSL.

   tls13: Estado de la compatibilidad del protocolo TLSv1.3 para el perfil SSL.

   Valores posibles: ENABLED, DISABLED

   Valor por defecto: DISABLED


```
set ssl profile tls13profile -tls13 enable
<!--NeedCopy-->
```

```
set ssl profile tls13profile -tls13 disable
<!--NeedCopy-->
```

2. Establece el número de tickets de sesión emitidos.

   tls13SessionTicketsPerAuthContext: Número de tíquets que el servidor virtual SSL emite cuando TLS1.3 se negocia, se habilita la reanudación basada en tíquets y (1) se completa un protocolo de enlace o (2) se completa la autenticación del cliente después del protocolo de enlace.

   Este valor se puede aumentar para permitir que los clientes abran varias conexiones paralelas mediante un tíquet nuevo para cada conexión.

   No se envían tíquets si la reanudación está desactivada.

   Valor por defecto: 1

   Valor mínimo: 1

   Valor máximo: 10

```
set ssl profile tls13profile -tls13sessionTicketsPerAuthContext 1

set ssl profile tls13profile -tls13sessionTicketsPerAuthContext 10
<!--NeedCopy-->
```

3. Establecer intercambio de claves DH

   `dheKeyExchangeWithPsk`: Especifica si un servidor virtual SSL requiere que se produzca un intercambio de claves DHE cuando se acepta una clave previamente compartida durante un protocolo de enlace de reanudación de sesión de TLS 1.3. Un intercambio de claves de DHE garantiza el secreto directo, incluso si las claves de los tíquets se ven comprometidas, a expensas de los recursos adicionales requeridos para llevar a cabo el intercambio de claves de **DHE**.

   Los ajustes disponibles funcionan de la siguiente manera, si el tíquet de sesión está habilitado:

   SÍ: se requiere el intercambio de claves DHE cuando se acepta una clave previamente compartida, independientemente de si el cliente admite el intercambio de claves. El apretón de manos se anula con una alerta irrecuperable si el cliente no admite el intercambio de claves DHE cuando ofrece una clave previamente compartida.

NO: El intercambio de claves DHE se realiza cuando se acepta una clave previamente compartida, solo si el cliente lo solicita.

Valores posibles: SÍ, NO

Valor por defecto: NO

```
set ssl profile tls13profile dheKeyExchangeWithPsk yes

set ssl profile tls13profile dheKeyExchangeWithPsk no
<!--NeedCopy-->
```

4. Habilitar o inhabilitar la aceptación temprana de datos 0-RTT

   `zeroRttEarlyData`: Estado de los datos de aplicación temprana de TLS 1.3. Los ajustes aplicables funcionan de la siguiente manera:

   HABILITADO: Los datos de la aplicación temprana pueden procesarse antes de que se complete el apretón de manos
   INHABILITADO: se ignoran los datos de las aplicaciones

   Valores posibles: ENABLED, DISABLED

   Valor por defecto: DISABLED

```
set ssl profile tls13profile -zeroRttEarlyData ENABLED

set ssl profile tls13profile -zeroRttEarlyData DISABLED
<!--NeedCopy-->
```

Grupo de cifrado predeterminado

El grupo de cifrado predeterminado incluye cifrados TLS1.3.

```
sh cipher DEFAULT
1) Cipher Name: TLS1-AES-256-CBC-SHA    Priority : 1
    Description: SSLv3 Kx=RSA      Au=RSA  Enc=AES(256)  Mac=SHA1
       HexCode=0x0035

2)  Cipher Name: TLS1-AES-128-CBC-SHA    Priority : 2
    Description: SSLv3 Kx=RSA      Au=RSA  Enc=AES(128)  Mac=SHA1
       HexCode=0x002f
```



```
...
...
27) Cipher Name: TLS1.3-AES256-GCM-SHA384         Priority : 27
    Description: TLSv1.3 Kx=any      Au=any  Enc=AES-GCM(256) Mac=AEAD
         HexCode=0x1302

28) Cipher Name: TLS1.3_CHACHA20_POLY1305_SHA256     Priority : 28
    Description: TLSv1.3 Kx=any      Au=any  Enc=CHACHA20/POLY1305(256)
        Mac=AEAD   HexCode=0x1303

29) Cipher Name: TLS1.3-AES128_GCM-SHA256        Priority : 29
    Description: TLSv1.3 Kx=any      Au=any  Enc=AES-GCM(128) Mac=AEAD
         HexCode=0x1301
Done
<!--NeedCopy-->
```

Limitaciones

- TLSv1.3 no se admite en el back-end.
- TLSv1.3 no se admite en un dispositivo Citrix Secure Web Gateway ni en un dispositivo Citrix ADC FIPS.

Limitaciones de seguridad

Los operadores de servidores TLSv1.3 deben tener en cuenta las siguientes restricciones de seguridad para la compatibilidad con versiones anteriores descritas en RFC 8446. La configuración predeterminada de un dispositivo NetScaler cumple con estas restricciones. Sin embargo, un dispositivo NetScaler no exige que se cumplan estas reglas.

- La seguridad de los conjuntos de cifrado RC4 se considera insuficiente como se describe en RFC7465. Las implementaciones no deben ofrecer ni negociar conjuntos de cifrado RC4 para ninguna versión de TLS.
- Las versiones antiguas de TLS permitían el uso de cifrados de baja intensidad. Los cifrados con una intensidad inferior a 112 bits no deben ofrecerse ni negociarse para ninguna versión de TLS.
- La seguridad de SSL 3.0 [SSLv3] se considera insuficiente, como se describe en RFC7568, y no debe negociarse. Inhabilitar SSLv3 cuando TLSV1.3 está habilitado (SSLv3 está inhabilitado de forma predeterminada).
- La seguridad de SSL 2.0 [SSLv2] se considera insuficiente, como se describe en RFC6176, y no debe negociarse. Inhabilite SSLv2 cuando TLS 1.3 está habilitado (SSLv2 está inhabilitado de forma predeterminada).

> **Nota:**
>
> Para obtener información sobre los protocolos de solución de problemas que se ejecutan en TLS1.3, consulte Descifrar el tráfico TLS1.3 del seguimiento de paquetes.

Artículos de procedimientos

August 20, 2021

Los artículos de procedimientos son sencillos y fáciles de usar con pasos de configuración para implementaciones comunes. Haga clic en un vínculo para ver el artículo.

Crear una solicitud de firma de certificados y utilizar certificados SSL en un dispositivo Citrix ADC

Configurar la acción SSL para reenviar el tráfico del cliente

Configurar la acción SSL para reenviar tráfico de cliente si no se admite un cifrado en el ADC

Configurar autenticación por cliente de directorio

Configurar la compatibilidad con el acceso web de Outlook

Configurar inserción de encabezado basado en SSL

Configurar la descarga SSL con cifrado de extremo a extremo

Configurar aceleración SSL transparente

Configurar la aceleración SSL con HTTP en el front-end y SSL en el back-end

Configurar la descarga SSL con otros protocolos TCP

Configurar conexión en puente SSL

Configurar la supervisión SSL cuando la autenticación de cliente está habilitada en el servicio back-end

Configurar un servidor de cambio de contenido seguro

Configurar un servidor virtual HTTPS para aceptar tráfico HTTP

Configurar la limpieza correcta de las sesiones SSL

Configurar la compatibilidad con HTTP estricta seguridad de transporte (HSTS)

Configurar la redirección de SSLv2

Configurar la sincronización de archivos en una configuración de alta disponibilidad

Inhabilitar TLS 1.0 y TLS 1.1 en NSIP

Exportar certificados utilizados en el dispositivo Citrix ADC como archivo PFX

Certificados de SSL

October 5, 2021

Un certificado SSL, que forma parte de cualquier transacción SSL, es un formulario de datos digitales (X509) que identifica a una empresa (dominio) o a un individuo. El certificado tiene un componente de clave pública visible para cualquier cliente que quiera iniciar una transacción segura con el servidor. La clave privada correspondiente, que reside de forma segura en el dispositivo Citrix ADC, se utiliza para completar el cifrado y descifrado de clave asimétrica (o clave pública).

Puede obtener un certificado y una clave SSL de cualquiera de las siguientes maneras:

- De una entidad emisora de certificados (CA) autorizada, como Verisign
- Al generar un nuevo certificado SSL y una clave en el dispositivo Citrix ADC

También puede utilizar un certificado SSL existente en el dispositivo.

El dispositivo Citrix ADC clasifica los certificados en cuatro tipos:

- **Certificados de servidor:** un certificado de servidor autentica la identidad del servidor ante el cliente. En el front-end, el dispositivo ADC actúa como servidor. Enlaza un certificado de servidor y una clave privada a un servidor virtual SSL del dispositivo ADC.
- **Certificados de cliente:** un certificado de cliente autentica la identidad del cliente en el servidor. En el back-end, el dispositivo ADC actúa como cliente. Enlaza un certificado de cliente y una clave privada al servicio o grupo de servicios SSL del dispositivo ADC.
- **Certificados de CA:** los certificados de CA emiten los certificados de usuario final (certificados de cliente y servidor). Un certificado de CA puede ser una CA raíz de confianza (autofirmada por la entidad emisora de certificados) o una CA intermedia (firmada por una CA raíz de confianza). Normalmente, los certificados de CA no necesitan claves privadas.
- **Certificados desconocidos:** todos los demás certificados pertenecen a esta categoría.

Importante: Citrix recomienda utilizar certificados obtenidos de CA autorizadas, como Verisign, para todas sus transacciones SSL. Utilice los certificados generados en el dispositivo Citrix ADC únicamente con fines de prueba, no en ninguna implementación activa.

- Si al agregar un par de claves de certificado, agrega un archivo de certificado con el mismo nombre que un archivo de certificado existente, el archivo de certificado original se sobrescribe sin previo aviso. Esta acción puede causar problemas después de reiniciar el dispositivo porque el archivo de certificado original ya no está disponible en el directorio `/nsconfig/ssl`.
- La eliminación de cualquier certificado o archivo de clave en un entorno de clúster restringe la configuración adicional del dispositivo ADC. Vuelva a agregar los archivos en la misma ubicación para realizar cualquier cambio de configuración.

Nota: Puede utilizar el panel SSL de ADM para facilitar la administración de certificados SSL y estable-

cer notificaciones para certificados que no se utilicen o que caduquen pronto. Para obtener más información, consulte Administración de certificados SSL.

Crear un certificado

April 5, 2022

Una entidad de certificación (CA) es una entidad que emite certificados digitales para su uso en criptografía de clave pública. Aplicaciones, como exploradores web, que realizan transacciones SSL certificados de confianza emitidos o firmados por una entidad de certificación. Estas aplicaciones mantienen una lista de las CA en las que confían. Si alguna de las entidades emisoras de certificados de confianza firma el certificado que se está usando para la transacción segura, la aplicación procede con la transacción.

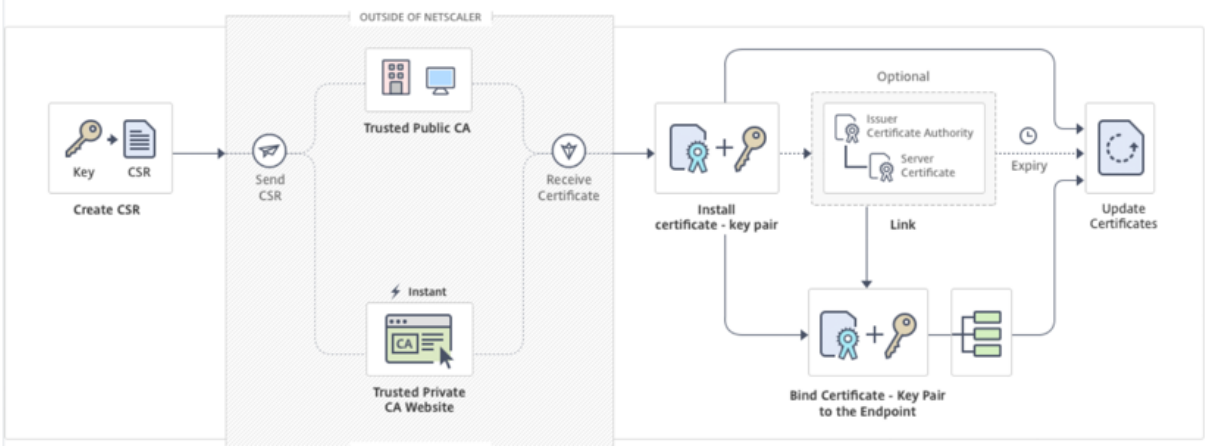
Precaución: Citrix recomienda utilizar certificados obtenidos de CA autorizadas, como Verisign, para todas las transacciones SSL. Utilice los certificados generados en el dispositivo Citrix ADC únicamente con fines de prueba, no en ninguna implementación activa.

Para importar un certificado y una clave existentes, consulte Importación de un certificado.

Realice los siguientes pasos para crear un certificado y vincularlo a un servidor virtual SSL. Los únicos caracteres especiales permitidos en los nombres de archivo son guiones bajos y puntos.

- Crea una clave privada.
- Cree una solicitud de firma de certificado (CSR).
- Envíe la CSR a una entidad de certificación.
- Cree un par de claves de certificado.
- Enlazar el par de claves de certificado a un servidor virtual SSL

El siguiente diagrama ilustra el flujo de trabajo.



Enlace de vídeo a Cómo creo e instalo un nuevo certificado.

Crear una clave privada

> **Notas:**
>
> - A partir de la versión 12.1 compilación 49.x, puede usar el algoritmo AES256 con formato de clave PEM para cifrar una clave privada en el dispositivo. El AES con clave de 256 bits es más eficiente y seguro matemáticamente en comparación con la clave de 56 bits del Estándar de cifrado de datos (DES).
> - A partir de la versión 12.1 compilación 50.x, puede crear una clave RSA en formato PKCS #8.

La clave privada es la parte más importante de un certificado digital. Por definición, esta clave no se debe compartir con nadie y debe mantenerse de forma segura en el dispositivo Citrix ADC. Todos los datos cifrados con la clave pública solo se pueden descifrar mediante el uso de la clave privada.

El certificado que recibe de la CA solo es válido con la clave privada que se usó para crear la CSR. La clave es necesaria para agregar el certificado al dispositivo Citrix ADC.

El dispositivo solo admite los algoritmos de cifrado RSA para crear claves privadas. Puede enviar cualquier tipo de clave privada a la entidad de certificación (CA). El certificado que recibe de la CA solo es válido con la clave privada que se usó para crear la CSR. La clave es necesaria para agregar el certificado al dispositivo Citrix ADC.

Importante:

> - Asegúrese de limitar el acceso a su clave privada. Cualquier persona que tenga acceso a su clave privada puede descifrar sus datos SSL.
> - La longitud del nombre de clave SSL permitida incluye la longitud del nombre de ruta absoluto si la ruta se incluye en el nombre de la clave.

Todos los certificados y claves SSL se almacenan en la carpeta `/nsconfig/ssl` del dispositivo. Para mayor seguridad, puede utilizar el algoritmo DES o triple DES (3DES) para cifrar la clave privada almacenada en el dispositivo.

Crear una clave privada RSA mediante la CLI

En el símbolo del sistema, escriba:

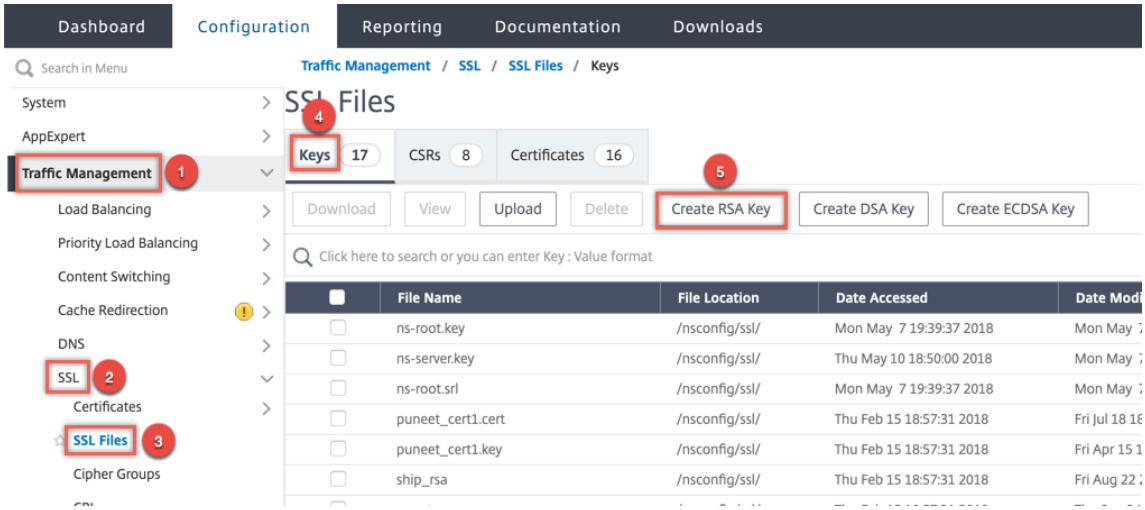
```
1 create ssl rsakey <keyFile> <bits> [-exponent ( 3 | F4 )] [-keyform (
     DER | PEM )] [-des | -des3 | -aes256] {
2  -password  }
3   [-pkcs8]
4 <!--NeedCopy-->
```

Ejemplo:

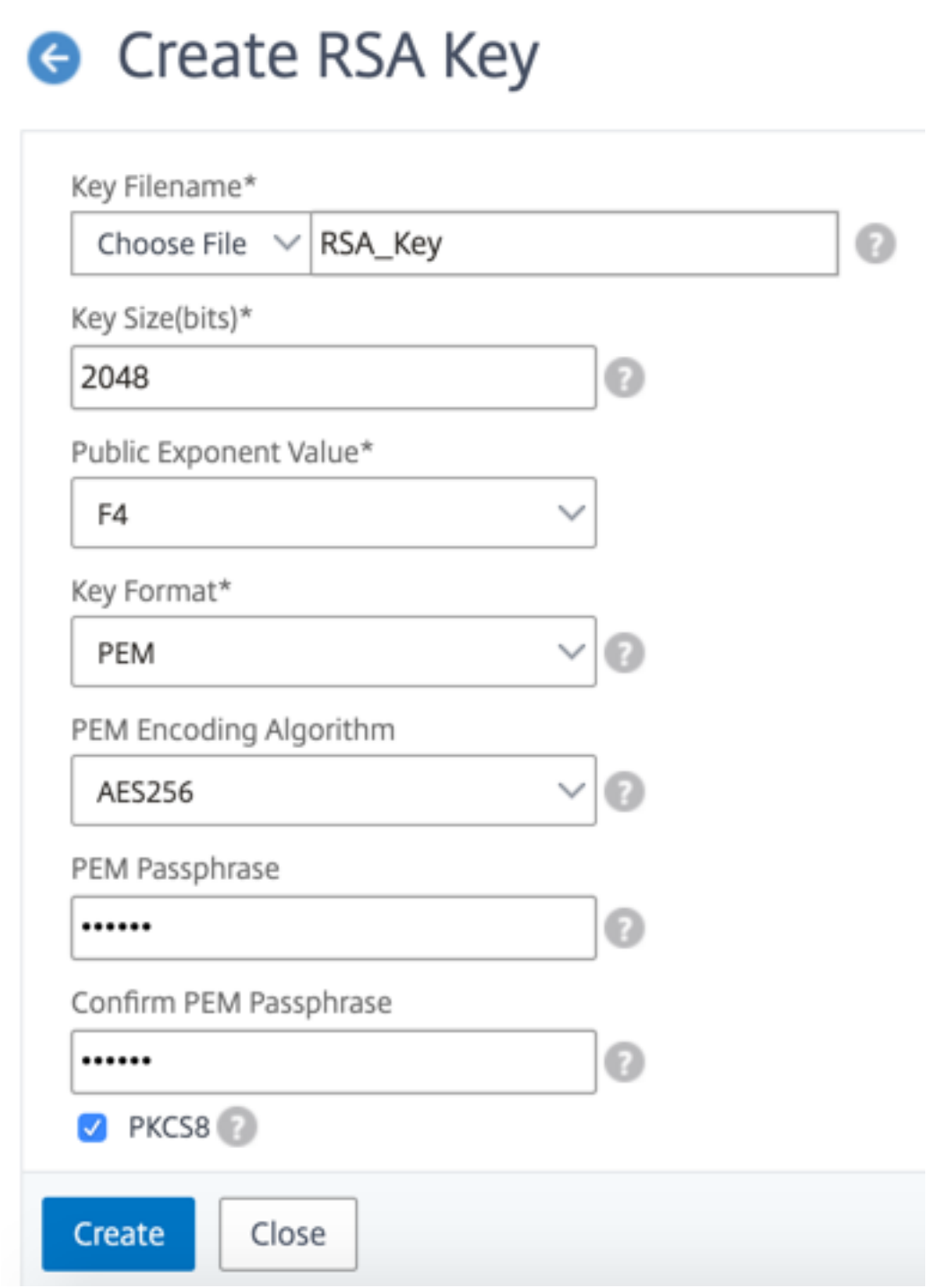

```
create rsakey testkey 2048 -aes256 -password 123456 -pkcs8
<!--NeedCopy-->
```

Crear una clave privada RSA mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > SSL > Archivos SSL**.
2. En la ficha **Claves**, selecciona **Crear clave RSA**.



3. Introduzca los valores de los siguientes parámetros y haga clic en **Crear**.
   - Nombre de**archivo clave: nombre** y, opcionalmente, ruta al archivo de clave RSA. /nsconfig/ssl/ es la ruta predeterminada.
   - **Tamaño de clave**: Tamaño, en bits, de la clave RSA. Puede variar de 512 bits a 4096 bits.
   - **Valor de exponente** público: exponente público para la clave RSA. El exponente forma parte del algoritmo de cifrado y es necesario para crear la clave RSA.
   - **Formato de clave**: Formato en el que se almacena el archivo de clave RSA en el dispositivo.
   - **Algoritmo de codificación PEM**: Encripte la clave RSA generada mediante el algoritmo AES 256, DES o Triple-DES (DES3). De forma predeterminada, las claves privadas no se cifran.
   - **Frase de contraseña PEM**: Si la clave privada está cifrada, introduzca una frase de contraseña para la clave.



Seleccione un algoritmo de codificación AES256 en una clave RSA mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > SSL > Archivos SSL > Crear clave RSA**.

2. En **Formato de clave**, seleccione **PEM**.
3. En **PEM Encoding Algorithm**, seleccione **AES256**.
4. Seleccione **PKCS8**.

Crear una solicitud de firma de certificado mediante la CLI

En el símbolo del sistema, escriba:

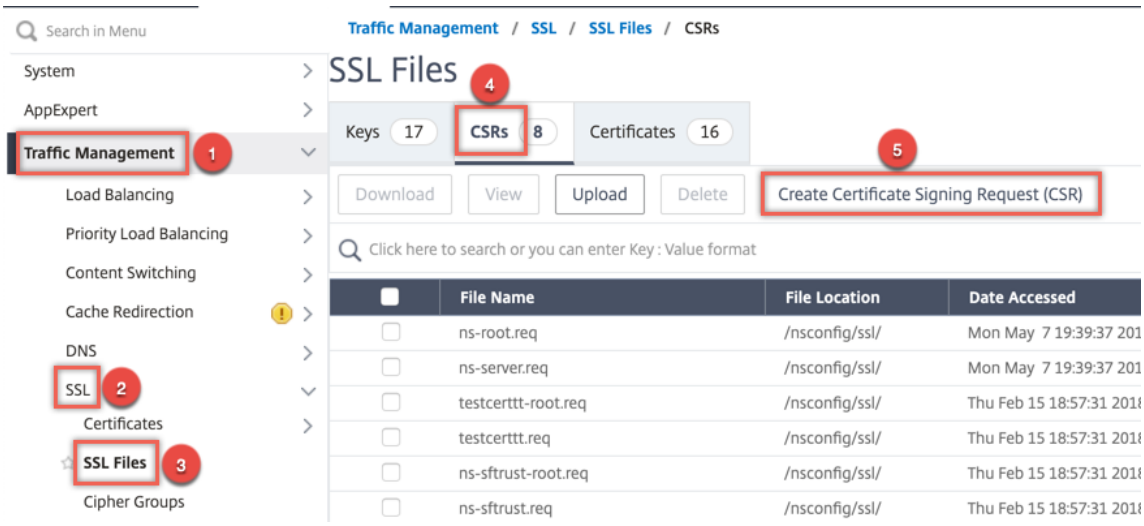
```
create ssl certreq <reqFile> -keyFile <input_filename> | -fipsKeyName <
   string>) [-keyForm (DER | PEM) {
 -PEMPassPhrase  }
 ] -countryName <string> -stateName <string> -organizationName <string>
     -organizationUnitName <string> -localityName <string> -commonName
    <string> -emailAddress <string> {
 -challengePassword  }
  -companyName <string> -digestMethod ( SHA1 | SHA256 )
<!--NeedCopy-->
```

Ejemplo:

```
create ssl certreq priv_csr_sha256 -keyfile priv_2048_2 -keyform PEM -
   countryName IN -stateName Karnataka -localityName Bangalore -
   organizationName Citrix -organizationUnitName NS -digestMethod
   SHA256
<!--NeedCopy-->
```

Crear una solicitud de firma de certificado mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > SSL**.
2. En Certificado **SSL**, haga clic en **Crear solicitud de firma de certificado (CSR)**.



3. En Método de **resumen**, seleccione **SHA256**.

Consulte Crear una CSR para obtener más información.

Compatibilidad con el nombre alternativo del sujeto en una solicitud de firma de certificado

El campo Nombre alternativo del sujeto (SAN) de un certificado le permite asociar varios valores, como nombres de dominio y direcciones IP, con un solo certificado. En otras palabras, puede proteger varios dominios, como www.example.com, www.example1.com, www.example2.com, con un solo certificado.

Algunos exploradores web, como Google Chrome, ya no admiten un nombre común en una solicitud de firma de certificado (CSR). Aplican el SAN en todos los certificados de confianza pública.

El dispositivo Citrix ADC admite agregar valores de SAN al crear una CSR. Puede enviar una CSR con una entrada de SAN a una entidad de certificación para obtener un certificado firmado con esa entrada de SAN. Cuando el dispositivo recibe una solicitud, comprueba si hay un nombre de dominio coincidente en las entradas de SAN del certificado del servidor. Si se encuentra una coincidencia, envía el certificado al cliente y completa el protocolo de enlace SSL. Puede usar la CLI o la GUI para crear una CSR con valores de SAN.

> **Nota:** El dispositivo Citrix ADC procesa solo valores de SAN basados en DNS.

Cree una CSR con el nombre alternativo del sujeto mediante la CLI

```
create ssl certReq <reqFile> (-keyFile <input_filename> | -fipsKeyName
    <string>) [-subjectAltName <string>] [-keyform ( DER | PEM )  {
 -PEMPassPhrase  }
```



```
3   ] -countryName <string> -stateName <string> -organizationName <string>
        [-organizationUnitName <string>] [-localityName <string>] [-
       commonName <string>] [-emailAddress <string>] {
4   -challengePassword  }
5    [-companyName <string>] [-digestMethod ( SHA1 | SHA256 )]
6   <!--NeedCopy-->
```

Parámetros:

subjectAltName: El nombre alternativo del sujeto (SAN) es una extensión de X.509 que permite asociar varios valores a un certificado de seguridad mediante un campo subjectAltName. Estos valores se denominan "Nombres alternativos del sujeto" (SAN). Los nombres incluyen:

1. Direcciones IP (prefijo con "IP:" Ejemplo: IP: 198.51.10.5 IP: 192.0.2.100)
2. Nombres DNS (prefijo con "DNS:" Ejemplo: DNS: www.example.com DNS: www.example.org DNS: www.example.net)

En la línea de comandos, introduzca los valores entre comillas. Separe dos valores con un espacio. No se requieren comillas en la interfaz gráfica de usuario.
Longitud máxima: 127

Ejemplo:

```
1   create certReq test1.csr -keyFile test1.ky -countryName IN -stateName
       Kar -organizationName citrix -commonName ctx.com -subjectAltName "
       DNS:*.example.com DNS:www.example.org DNS:www.example.net"
2   <!--NeedCopy-->
```

> **Nota:**
>
> En un dispositivo FIPS, debe reemplazar el nombre del archivo de clave por el nombre de clave FIPS si crea la clave FIPS directamente en el dispositivo.
>
> ```
> 1   create certReq <csrname> -fipsKeyName fipskey.ky -countryName IN -
>        stateName Kar -organizationName citrix -commonName ctx.com -
>        subjectAltName "DNS:www.example.com DNS:www.example.org DNS:www.
>        example.net"
> 2   <!--NeedCopy-->
> ```

Crear una CSR mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico** > **SSL** > **Archivos SSL**.

2. En la ficha **CSR**, haga clic en **Crear solicitud de firma de certificado (CSR)**.
3. Introduzca los valores y haga clic en **Crear**.

Limitaciones

Para usar SAN al crear un certificado SSL, debe especificar explícitamente los valores de SAN. Los valores no se leen automáticamente del archivo CSR.

Presentar la CSR a la entidad de certificación

La mayoría de las autoridades de certificación (CA) aceptan envíos de certificados por correo electrónico. La CA devuelve un certificado válido a la dirección de correo electrónico desde la que envía el CSR.

La CSR se almacena en la carpeta `/nsconfig/ssl`.

Generar un certificado de prueba

> **Nota:**
>
> Para generar un certificado de prueba de servidor, consulte Generación de un certificado de prueba de servidor.

El dispositivo Citrix ADC tiene un conjunto de herramientas de CA integrado que puede utilizar para crear certificados autofirmados con fines de prueba.

Precaución: Como el dispositivo Citrix ADC firma estos certificados, y no una CA real, no debe usarlos en un entorno de producción. Si intenta utilizar un certificado autofirmado en un entorno de producción, los usuarios reciben una advertencia de "certificado no válido" cada vez que se accede al servidor virtual.

El dispositivo admite la creación de los siguientes tipos de certificados:

- Certificados de CA raíz
- Certificados de CA intermedia
- Certificados de usuario final
  - certificados de servidor
  - certificados de cliente

Antes de generar un certificado, cree una clave privada y utilícela para crear una solicitud de firma de certificado (CSR) en el dispositivo. A continuación, en lugar de enviar la CSR a una CA, use Citrix ADC CA Tools para generar un certificado.

Crear un certificado mediante un asistente

1. Vaya a **Administración del tráfico > SSL**.
2. En el panel de detalles, en **Introducción**, seleccione el asistente para el tipo de certificado que desea crear.
3. Siga las instrucciones que aparecen en pantalla.

Crear un certificado de CA raíz mediante la CLI

En el símbolo del sistema, escriba el siguiente comando:

```
create ssl cert <certFile> <reqFile> <certType> [-keyFile <
    input_filename>] [-keyform ( DER | PEM )] [-days <positive_integer>]
<!--NeedCopy-->
```

En el siguiente ejemplo, csreq1 es la CSR y rsa1 es la clave privada que se creó anteriormente.

Ejemplo:

```
create ssl cert cert1 csreq1 ROOT_CERT -keyFile rsa1 -keyForm PEM -days
     365

  Done
<!--NeedCopy-->
```

Crear un certificado de CA intermedia mediante la CLI

```
create ssl cert <certFile> <reqFile> <certType> [-keyFile <
    input_filename>] [-keyform ( DER | PEM )] [-days <positive_integer>]
     [-certForm ( DER | PEM )] [-CAcert <input_filename>] [-CAcertForm (
     DER | PEM )] [-CAkey <input_filename>] [-CAkeyForm ( DER | PEM )]
    [-CAserial <output_filename>]
<!--NeedCopy-->
```

En el siguiente ejemplo, csr1 es la CSR creada anteriormente. Cert1 y rsakey1 son el certificado y la clave correspondiente del certificado autofirmado (CA raíz), y pvtkey1 es la clave privada del certificado de CA intermedia.

Ejemplo:


```
create ssl cert certsy csr1 INTM_CERT -CAcert cert1 -CAkey rsakey1 -
    CAserial 23
Done

create ssl rsakey pvtkey1 2048 -exponent F4 -keyform PEM
Done
<!--NeedCopy-->
```

Crear un certificado de CA raíz mediante la interfaz gráfica de usuario

Vaya a **Administración del tráfico > SSL** y, en el grupo Introducción, seleccione **Asistente para certificados de CA raíz**y configure un certificado de CA raíz.

Crear un certificado de CA intermedia mediante la interfaz gráfica de usuario

Vaya a **Administración del tráfico > SSL** y, en el grupo Introducción, seleccione **Asistente para certificados de CA intermedia**y configure un certificado de CA intermedio.

Crear un certificado de usuario final

Un certificado de usuario final puede ser un certificado de cliente o un certificado de servidor. Para crear un certificado de usuario final de prueba, especifique el certificado de CA intermedia o el certificado de CA raíz autofirmado.

> **Nota:** Para crear un certificado de usuario final para uso en producción, especifique un certificado de CA de confianza y envíe la CSR a una entidad de certificación (CA).

Crear un certificado de usuario final de prueba mediante la interfaz de línea de comandos

```
create ssl cert <certFile> <reqFile> <certType> [-keyFile <
    input_filename>] [-keyform ( DER | PEM )] [-days<positive_integer>]
    [-certForm ( DER | PEM )] [-CAcert <input_filename>] [-CAcertForm (
    DER | PEM )] [-CAkey<input_filename>] [-CAkeyForm ( DER | PEM )] [-
    CAserial <output_filename>]
<!--NeedCopy-->
```

Si no hay un certificado intermedio, utilice los valores de certificado (cert1) y de la clave privada (rsakey1) del certificado de CA raíz en `CAcert` y `CAkey`.

Ejemplo:


```
create ssl cert cert12 csr1 SRVR_CERT -CAcert cert1 -CAkey rsakey1 -
    CAserial 23

Done
<!--NeedCopy-->
```

Si hay un certificado intermedio, utilice los valores del certificado (`certsy`) y de la clave privada (pvtkey1) del certificado intermedio en `CAcert` y `CAkey`.

Ejemplo:

```
create ssl cert cert12 csr1 SRVR_CERT -CAcert certsy -CAkey pvtkey1 -
    CAserial 23

Done
<!--NeedCopy-->
```

Crear un certificado SAN autofirmado mediante OpenSSL

Para crear un certificado SAN autofirmado con varios nombres alternativos de sujeto, lleve a cabo los siguientes pasos:

1. Cree un archivo de configuración de OpenSSL en su equipo local modificando los campos relacionados según los requisitos de la empresa.

   Nota: En el ejemplo siguiente, el archivo de configuración es “req.conf”.

   ```
   [req]
   distinguished_name = req_distinguished_name
   x509_extensions = v3_req
   prompt = no
   [req_distinguished_name]
   C = US
   ST = VA
   L = SomeCity
   O = MyCompany
   OU = MyDivision
   CN = www.company.com
   [v3_req]
   keyUsage = keyEncipherment, dataEncipherment
   extendedKeyUsage = serverAuth
   ```



```
subjectAltName = @alt_names
[alt_names]
DNS.1 = www.company.net
DNS.2 = company.com
DNS.3 = company.net
<!--NeedCopy-->
```

2. Cargue el archivo en el directorio /nsconfig/ssl del dispositivo Citrix ADC
3. Inicie sesión en la CLI de Citrix ADC como usuario `nsroot` y cambie al símbolo del shell.
4. Ejecute el siguiente comando para crear el certificado:

```
cd /nsconfig/ssl
openssl req -x509 -nodes -days 730 -newkey rsa:2048 -keyout cert.
   pem -out cert.pem -config req.conf -extensions 'v3_req'
<!--NeedCopy-->
```

5. Ejecute el siguiente comando para verificar el certificado:

```
openssl x509 -in cert.pem -noout  - text
Certificate:
Data:
Version: 3 (0x2)
Serial Number:
ed:90:c5:f0:61:78:25:ab
Signature Algorithm: md5WithRSAEncryption
Issuer: C=US, ST=VA, L=SomeCity, O=MyCompany, OU=MyDivision, CN=
   www.company.com
Validity
Not Before: Nov 6 22:21:38 2012 GMT
Not After : Nov 6 22:21:38 2014 GMT
Subject: C=US, ST=VA, L=SomeCity, O=MyCompany, OU=MyDivision, CN=
   www.company.com
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (2048 bit)
Modulus (2048 bit):
…
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Key Usage:
Key Encipherment, Data Encipherment
```



```
X509v3 Extended Key Usage:
TLS Web Server Authentication
X509v3 Subject Alternative Name:
DNS:www.company.net, DNS:company.com, DNS:company.net
Signature Algorithm: md5WithRSAEncryption …
<!--NeedCopy-->
```

Instalar, vincular y actualizar certificados

April 5, 2022

Para instalar un certificado, consulte Agregar o actualizar un par de claves de certificado.

Vincular certificados

Muchos certificados de servidor están firmados por varias autoridades de certificación (CA) jerárquicas, lo que significa que los certificados forman una cadena como la siguiente:

```
Root CA
|
+------------ Intermediate CA
|
+------------------------ End-Entity (Server) Certificate
```

A veces, la CA intermedia se divide en un certificado de CA intermedio principal y secundario. Luego, los certificados forman una cadena como la siguiente:

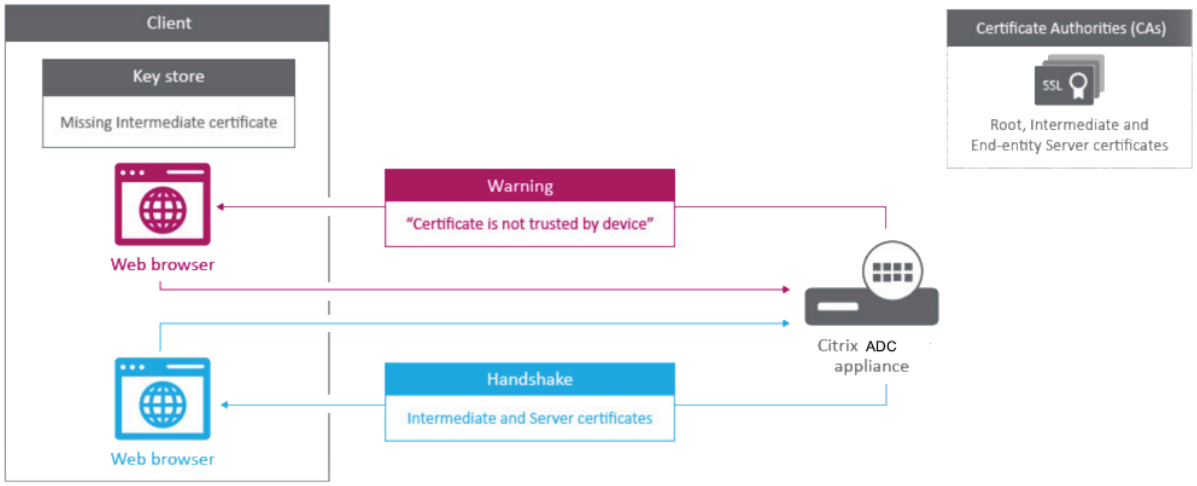
```
Root CA
|
+------- Primary Intermediate CA
|+--------------- Secondary Intermediate CA
|
+------------------------ End-Entity (Server) Certificate
```

Las máquinas cliente suelen contener el certificado de CA raíz en su almacén de certificados local, pero no uno o más certificados de CA intermedios. El dispositivo ADC debe enviar uno o más certificados de CA intermedios a los clientes.

Nota: El dispositivo no debe enviar el certificado de CA raíz al cliente. El modelo de relación de confianza de la infraestructura de clave pública (PKI) requiere que los certificados de CA raíz se instalen en los clientes mediante un método fuera de banda. Por ejemplo, los certificados se incluyen con el sistema operativo o el explorador web. El cliente ignora un certificado de CA raíz enviado por el dispositivo.

A veces, una CA intermedia que los exploradores web estándar no reconocen como CA de confianza, emite el certificado del servidor. En este caso, se deben enviar uno o más certificados de CA al cliente

con el certificado propio del servidor. De lo contrario, el explorador finaliza la sesión SSL porque no puede autenticar el certificado del servidor.



Enlace de vídeo a Cómo vinculo un certificado de autoridad intermedia.

Consulte las siguientes secciones para agregar el servidor y los certificados intermedios:

- Vinculación manual de certificados
- Vinculación automática de certificados
- Crea una cadena de certificados

Vinculación manual de certificados

Nota: Esta función no se admite en la plataforma FIPS de Citrix ADC ni en una configuración de clúster.

En lugar de agregar y vincular certificados individuales, ahora puede agrupar un certificado de servidor y hasta nueve certificados intermedios en un solo archivo. Puede especificar el nombre del archivo al agregar un par de claves de certificado. Antes de hacerlo, asegúrese de que se cumplen los siguientes requisitos previos.

- Los certificados del archivo están en el siguiente orden:
  - Certificado de servidor (debe ser el primer certificado del archivo)
  - Opcionalmente, una clave de servidor
  - Certificado intermedio 1 (ic1)
  - Certificado intermedio 2 (ic2)
  - Certificado intermedio 3 (ic3), etc.

    Nota: Los archivos de certificado intermedios se crean para cada certificado intermedio con el nombre "<certificatebundlename>.pem_ic<*n*>", donde n está entre 1 y 9. Por ejemplo, bundle.pem_ic1, donde **bundle** es el nombre del conjunto de certificados e ic1 es el primer certificado intermedio del conjunto.
- Se selecciona la opción de paquete.

- No hay más de nueve certificados intermedios en el archivo.

El archivo se analiza y se identifican el certificado del servidor, los certificados intermedios y la clave del servidor (si está presente). En primer lugar, se agregan el certificado y la clave del servidor. A continuación, se agregan los certificados intermedios, en el orden en que se agregaron al archivo, y se vinculan en consecuencia.

Se informa de un error si se da alguna de las siguientes condiciones:

- Existe un archivo de certificado para uno de los certificados intermedios en el dispositivo.
- La clave se coloca antes del certificado del servidor en el archivo.
- Se coloca un certificado intermedio antes del certificado del servidor.
- Los certificados intermedios no se colocan en el archivo en el mismo orden en que se crean.
- No hay certificados en el archivo.
- Un certificado no tiene el formato PEM correcto.
- El número de certificados intermedios en el archivo supera los nueve.

Agregar un conjunto de certificados mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para crear un conjunto de certificados y verificar la configuración:

```
1 add ssl certKey <certkeyName> -cert <string> -key <string> -bundle (YES
      | NO)
2
3 show ssl
4
5 show ssl certlink
6 <!--NeedCopy-->
```

En el siguiente ejemplo, el conjunto de certificados (bundle.pem) contiene los siguientes archivos:

Certificado de servidor (paquete) vinculado a bundle_ic1

Primer certificado intermedio (bundle_ic1) vinculado a bundle_ic2

Segundo certificado intermedio (bundle_ic2) vinculado a bundle_ic3

Tercer certificado intermedio (bundle_ic3)

```
1 add ssl certKey bundletest -cert bundle9.pem -key bundle9.pem -bundle
     yes
2
3 sh ssl certkey
```



```
1)      Name: ns-server-certificate
        Cert Path: ns-server.cert
        Key Path: ns-server.key
        Format: PEM
        Status: Valid,   Days to expiration:5733
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
        Certificate Type: Server Certificate
        Version: 3
        Serial Number: 01
        Signature Algorithm: sha256WithRSAEncryption
        Issuer:  C=US,ST=California,L=San Jose,O=Citrix ANG,OU=NS
           Internal,CN=default OULLFT
        Validity
                Not Before: Apr 21 15:56:16 2016 GMT
                Not After : Mar  3 06:30:56 2032 GMT
        Subject:  C=US,ST=California,L=San Jose,O=Citrix ANG,OU=NS
           Internal,CN=default OULLFT
        Public Key Algorithm: rsaEncryption
        Public Key size: 2048

2)      Name: servercert
        Cert Path: complete/server/server_rsa_1024.pem
        Key Path: complete/server/server_rsa_1024.ky
        Format: PEM
        Status: Valid,   Days to expiration:7150
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
        Certificate Type: Server Certificate
        Version: 3
        Serial Number: 1F
        Signature Algorithm: sha1WithRSAEncryption
        Issuer:  C=IN,ST=KAR,O=Citrix R&D Pvt Ltd,CN=Citrix
        Validity
                Not Before: Sep  2 09:54:07 2008 GMT
                Not After : Jan 19 09:54:07 2036 GMT
        Subject:  C=IN,ST=KAR,O=Citrix Pvt Ltd,CN=Citrix
        Public Key Algorithm: rsaEncryption
        Public Key size: 1024

3)      Name: bundletest
        Cert Path: bundle9.pem
        Key Path: bundle9.pem
        Format: PEM
```



```
        Status: Valid,   Days to expiration:3078
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
        Certificate Type: Server Certificate
        Version: 3
        Serial Number: 01
        Signature Algorithm: sha256WithRSAEncryption
        Issuer:  C=IN,ST=ka,O=sslteam,CN=ICA9
        Validity
                Not Before: Nov 28 06:43:11 2014 GMT
                Not After : Nov 25 06:43:11 2024 GMT
        Subject:  C=IN,ST=ka,O=sslteam,CN=Server9
        Public Key Algorithm: rsaEncryption
        Public Key size: 2048

4)      Name: bundletest_ic1
        Cert Path: bundle9.pem_ic1
        Format: PEM
        Status: Valid,   Days to expiration:3078
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
        Certificate Type: Intermediate CA
        Version: 3
        Serial Number: 01
        Signature Algorithm: sha256WithRSAEncryption
        Issuer:  C=IN,ST=ka,O=sslteam,CN=ICA8
        Validity
                Not Before: Nov 28 06:42:56 2014 GMT
                Not After : Nov 25 06:42:56 2024 GMT
        Subject:  C=IN,ST=ka,O=sslteam,CN=ICA9
        Public Key Algorithm: rsaEncryption
        Public Key size: 2048

5)      Name: bundletest_ic2
        Cert Path: bundle9.pem_ic2
        Format: PEM
        Status: Valid,   Days to expiration:3078
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
        Certificate Type: Intermediate CA
        Version: 3
        Serial Number: 01
        Signature Algorithm: sha256WithRSAEncryption
        Issuer:  C=IN,ST=ka,O=sslteam,CN=ICA7
        Validity
```



```
                Not Before: Nov 28 06:42:55 2014 GMT
                Not After : Nov 25 06:42:55 2024 GMT
        Subject:  C=IN,ST=ka,O=sslteam,CN=ICA8
        Public Key Algorithm: rsaEncryption
        Public Key size: 2048

6)      Name: bundletest_ic3
        Cert Path: bundle9.pem_ic3
        Format: PEM
        Status: Valid,   Days to expiration:3078
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
        Certificate Type: Intermediate CA
        Version: 3
        Serial Number: 01
        Signature Algorithm: sha256WithRSAEncryption
        Issuer:  C=IN,ST=ka,O=sslteam,CN=ICA6
        Validity
                Not Before: Nov 28 06:42:53 2014 GMT
                Not After : Nov 25 06:42:53 2024 GMT
        Subject:  C=IN,ST=ka,O=sslteam,CN=ICA7
        Public Key Algorithm: rsaEncryption
        Public Key size: 2048

7)      Name: bundletest_ic4
        Cert Path: bundle9.pem_ic4
        Format: PEM
        Status: Valid,   Days to expiration:3078
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
        Certificate Type: Intermediate CA
        Version: 3
        Serial Number: 01
        Signature Algorithm: sha256WithRSAEncryption
        Issuer:  C=IN,ST=ka,O=sslteam,CN=ICA5
        Validity
                Not Before: Nov 28 06:42:51 2014 GMT
                Not After : Nov 25 06:42:51 2024 GMT
        Subject:  C=IN,ST=ka,O=sslteam,CN=ICA6
        Public Key Algorithm: rsaEncryption
        Public Key size: 2048

8)      Name: bundletest_ic5
        Cert Path: bundle9.pem_ic5
        Format: PEM
```



```
        Status: Valid,   Days to expiration:3078
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
        Certificate Type: Intermediate CA
        Version: 3
        Serial Number: 01
        Signature Algorithm: sha256WithRSAEncryption
        Issuer:  C=IN,ST=ka,O=sslteam,CN=ICA4
        Validity
                Not Before: Nov 28 06:42:50 2014 GMT
                Not After : Nov 25 06:42:50 2024 GMT
        Subject:  C=IN,ST=ka,O=sslteam,CN=ICA5
        Public Key Algorithm: rsaEncryption
        Public Key size: 2048

9)      Name: bundletest_ic6
        Cert Path: bundle9.pem_ic6
        Format: PEM
        Status: Valid,   Days to expiration:3078
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
        Certificate Type: Intermediate CA
        Version: 3
        Serial Number: 01
        Signature Algorithm: sha256WithRSAEncryption
        Issuer:  C=IN,ST=ka,O=sslteam,CN=ICA3
        Validity
                Not Before: Nov 28 06:42:48 2014 GMT
                Not After : Nov 25 06:42:48 2024 GMT
        Subject:  C=IN,ST=ka,O=sslteam,CN=ICA4
        Public Key Algorithm: rsaEncryption
        Public Key size: 2048

10)     Name: bundletest_ic7
        Cert Path: bundle9.pem_ic7
        Format: PEM
        Status: Valid,   Days to expiration:3078
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
        Certificate Type: Intermediate CA
        Version: 3
        Serial Number: 01
        Signature Algorithm: sha256WithRSAEncryption
        Issuer:  C=IN,ST=ka,O=sslteam,CN=ICA2
        Validity
```



```
                Not Before: Nov 28 06:42:46 2014 GMT
                Not After : Nov 25 06:42:46 2024 GMT
        Subject:  C=IN,ST=ka,O=sslteam,CN=ICA3
        Public Key Algorithm: rsaEncryption
        Public Key size: 2048

11)     Name: bundletest_ic8
        Cert Path: bundle9.pem_ic8
        Format: PEM
        Status: Valid,   Days to expiration:3078
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
        Certificate Type: Intermediate CA
        Version: 3
        Serial Number: 01
        Signature Algorithm: sha256WithRSAEncryption
        Issuer:  C=IN,ST=ka,O=sslteam,CN=ICA1
        Validity
                Not Before: Nov 28 06:42:45 2014 GMT
                Not After : Nov 25 06:42:45 2024 GMT
        Subject:  C=IN,ST=ka,O=sslteam,CN=ICA2
        Public Key Algorithm: rsaEncryption
        Public Key size: 2048

12)     Name: bundletest_ic9
        Cert Path: bundle9.pem_ic9
        Format: PEM
        Status: Valid,   Days to expiration:3078
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
        Certificate Type: Intermediate CA
        Version: 3
        Serial Number: 01
        Signature Algorithm: sha256WithRSAEncryption
        Issuer:  C=IN,ST=ka,O=sslteam,CN=RootCA4096
        Validity
                Not Before: Nov 28 06:42:43 2014 GMT
                Not After : Nov 25 06:42:43 2024 GMT
        Subject:  C=IN,ST=ka,O=sslteam,CN=ICA1
        Public Key Algorithm: rsaEncryption
        Public Key size: 2048
Done

sh ssl certlink

```



```
1)      Cert Name: bundletest    CA Cert Name: bundletest_ic1
2)      Cert Name: bundletest_ic1        CA Cert Name: bundletest_ic2
3)      Cert Name: bundletest_ic2        CA Cert Name: bundletest_ic3
4)      Cert Name: bundletest_ic3        CA Cert Name: bundletest_ic4
5)      Cert Name: bundletest_ic4        CA Cert Name: bundletest_ic5
6)      Cert Name: bundletest_ic5        CA Cert Name: bundletest_ic6
7)      Cert Name: bundletest_ic6        CA Cert Name: bundletest_ic7
8)      Cert Name: bundletest_ic7        CA Cert Name: bundletest_ic8
9)      Cert Name: bundletest_ic8        CA Cert Name: bundletest_ic9
Done
<!--NeedCopy-->
```

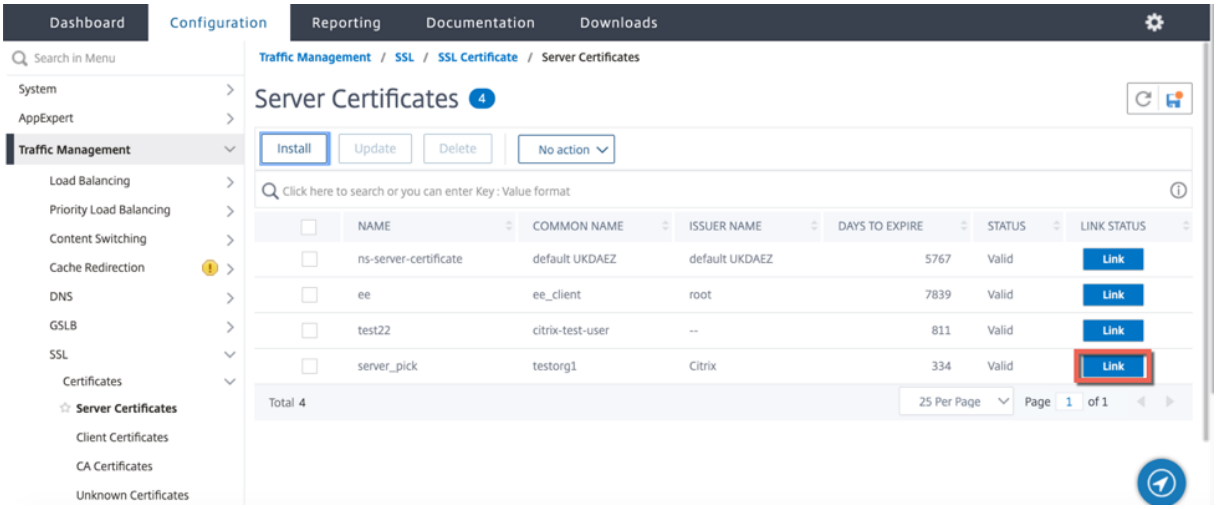
Agregar un conjunto de certificados mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico** > **SSL** > **Certificados > Certificadosde CA**.
2. En el panel de detalles, haga clic en **Instalar**.
3. En el cuadro de diálogo **Instalar certificado**, escriba los detalles, como el nombre del certificado y el archivo de clave, y, a continuación, seleccione **Paquete de certificados**.
4. Haga clic en **Instalar**y, después, en **Cerrar**.

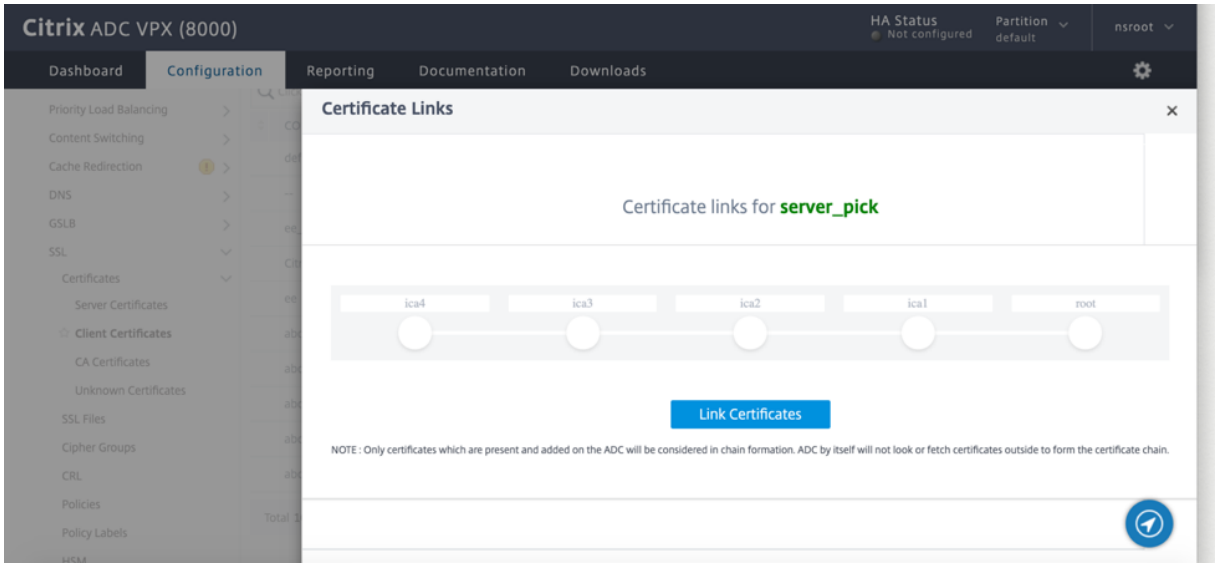
Vinculación automática de certificados

Nota: Esta función está disponible a partir de la versión 13.0 compilación 47.x.

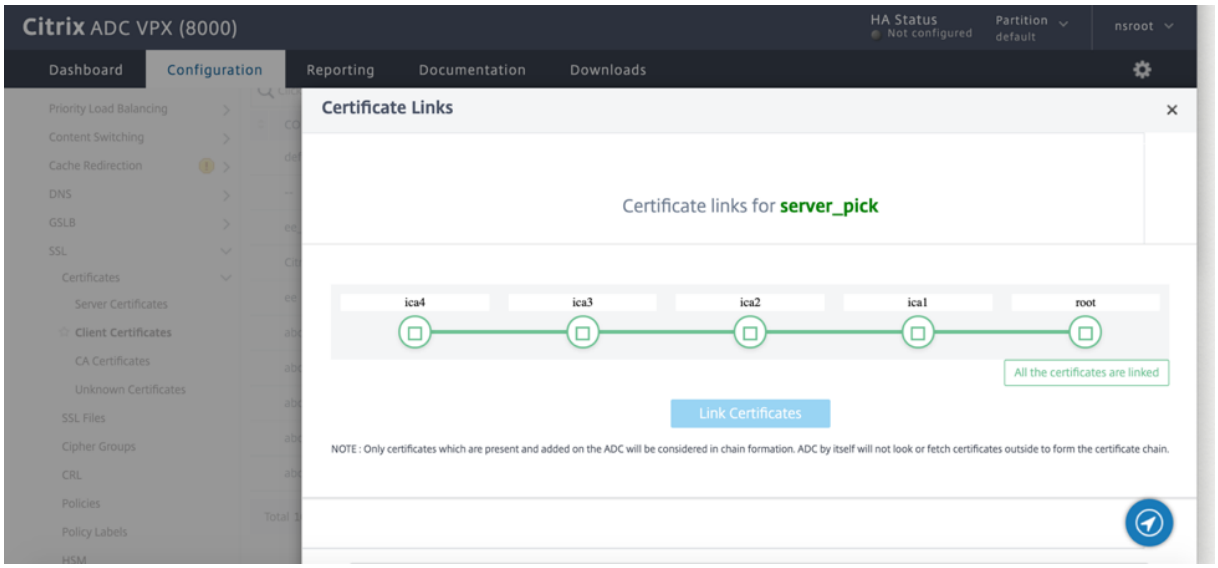
Ya no tiene que vincular manualmente un certificado a su emisor hasta el certificado raíz. Si los certificados de CA intermedios y el certificado raíz están presentes en el dispositivo, puede hacer clic en el botón **Vincular** en el certificado de usuario final.



Aparece la cadena de potencial.



Haga clic en **Vincular certificado** para vincular todos los certificados.



Crea una cadena de certificados

En lugar de utilizar un conjunto de certificados (un único archivo), puede crear una cadena de certificados. La cadena vincula el certificado del servidor a su emisor (la CA intermedia). Este enfoque requiere que el archivo de certificado de CA intermedio esté instalado en el dispositivo ADC y la aplicación cliente debe confiar en uno de los certificados de la cadena. Por ejemplo, vincule Cert-Intermediate-A con Cert-Intermediate-B, donde Cert-Intermediate-B está vinculado a Cert-Intermediate-C, que es un certificado en el que confía la aplicación cliente.

Nota: El dispositivo admite el envío de un máximo de 10 certificados en la cadena de certificados enviados al cliente (un certificado de servidor y nueve certificados de CA).

Crear una cadena de certificados mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para crear una cadena de certificados y verificar la configuración. (Repita el primer comando para cada eslabón nuevo de la cadena).

```
link ssl certkey <certKeyName> <linkCertKeyName>
show ssl certlink
<!--NeedCopy-->
```

Ejemplo:

```
link ssl certkey siteAcertkey CAcertkey
Done

show ssl certlink

linked certificate:
       1) Cert Name: siteAcertkey CA Cert Name: CAcertkey
Done
<!--NeedCopy-->
```

Crear una cadena de certificados mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico** > **SSL** > **Certificados**.
2. Seleccione un certificado de servidor y, en la lista **Acción**, seleccione **Vincular**y especifique un nombre de certificado de CA.

Compatibilidad con el paquete de certificados SSL

> **Nota:**
>
> Esta función está disponible a partir de la versión 13.1 compilación 12.x.

El diseño actual de un paquete de certificados presenta los siguientes inconvenientes:

- Al agregar un paquete de certificados, se agregan varios comandos en la configuración. Por lo tanto, no puede agregar otro paquete de certificados si los dos paquetes comparten un certificado intermedio común.
- La eliminación de un paquete de certificados es un proceso manual. Debe eliminar los archivos manualmente en un orden específico.
- No se admite la actualización de un paquete de certificados.

- No se admite el clúster.

El nuevo diseño de un paquete de certificados resuelve todos estos problemas. La nueva entidad funciona en un archivo de paquete de certificados. Por lo tanto, no es necesario crear archivos para cada certificado intermedio. La eliminación también es sencilla con esta nueva entidad.

Dos paquetes de certificados pueden compartir parte de la cadena de certificados intermedia. También puede agregar un par de claves de certificado con el mismo certificado y clave de servidor que también forma parte de un paquete de certificados.

En el siguiente ejemplo:

1. El paquete de certificados bundle1.pem contiene certificados de servidor (S1) e intermedios (IC1 e IC2).
2. El certificado del servidor es server_cert.pem (S1).
3. Los certificados intermedios son ic1.pem (IC1) e ic2.pem (IC2).

Puede agregar un paquete de certificados que contenga S1, IC1 e IC2.

```
add ssl certkeybundle b1 -bundlefile bundle1.pem
```

También puede agregar un par de claves de certificado mediante S1 e IC1.

```
add ssl certkey server-cert -cert server_cert.pem
```

```
add ssl certkey ic1 -cert ic1.pem
```

Importante.

- La creación del paquete falla si no se cumple el siguiente pedido:
  - El certificado de servidor (SC) debe colocarse en la parte superior del archivo del paquete.
  - `IC[1-9]` son certificados intermedios. `IC[i]` es emitido por `IC[i+1]`. Los certificados deben colocarse en una secuencia y todos los certificados intermedios deben estar presentes en el paquete.
- Los certificados deben tener formato PEM únicamente.
- La clave de certificado de servidor (SCK) se puede colocar en cualquier parte del paquete.
- Se admiten un máximo de 9 certificados intermedios.

Para agregar un paquete de certificados

En el símbolo del sistema, escriba:

```
add ssl certKeyBundle <bundle_name> -bundlefile <bundle_file_name> -passplain
 <>
```

Ejemplo:

```
add ssl certkeyBundle cert_bundle -bundlefile bundle_4096.pem
```


Para eliminar un paquete de certificados

En el símbolo del sistema, escriba:

```
rm ssl certKeyBundle <bundle_name>
```

Ejemplo:

```
rm ssl certkeybundle cert_bundle
```

Para vincular un paquete de certificados a un servidor virtual SSL

En el símbolo del sistema, escriba:

```
bind ssl vserver <vip-name> -certkeybundleName <certkeybundle_name> [ -SNICertkeybundle]
```

Ejemplo:

```
bind ssl vserver v_server -certkeyBundleName cert_bundle

show ssl certkeyBundle cert_bundle

1) Name: cert_bundle
        Bundle path: bundle_4096.pem
        Certificate:
                Status: Valid,   Days to expiration:278
                Serial Number: 83
                Subject:  C=IN,ST=KAR,O=CITRIX,CN=4096.com
                Issuer:  C=IN,ST=KAR,O=CITRIX,CN=ia24096.com
                Signature Algorithm: sha256WithRSAEncryption
                Validity
                        Not Before: Jul 13 10:17:57 2021 GMT
                        Not After : Jul 13 10:17:57 2022 GMT
                Public Key Algorithm: rsaEncryption
                Public Key size: 4096
                SAN ENTRIES: None


        CA Certificate:
                Status: Valid,   Days to expiration:278
                Serial Number: 82
                Subject:  C=IN,ST=KAR,O=CITRIX,CN=ia24096.com
                Issuer:  C=IN,ST=KAR,O=CITRIX,CN=ia14098.com
                Signature Algorithm: sha256WithRSAEncryption
                Validity
```



```
                        Not Before: Jul 13 10:15:37 2021 GMT
                        Not After : Jul 13 10:15:37 2022 GMT
                Public Key Algorithm: rsaEncryption
                Public Key size: 4096
                SAN ENTRIES: None

        CA Certificate:
                Status: Valid,   Days to expiration:278
                Serial Number: 81
                Subject:  C=IN,ST=KAR,O=CITRIX,CN=ia14098.com
                Issuer:  C=IN,ST=KAR,O=CITRIX,CN=root4098.com
                Signature Algorithm: sha256WithRSAEncryption
                Validity
                        Not Before: Jul 13 10:13:20 2021 GMT
                        Not After : Jul 13 10:13:20 2022 GMT
                Public Key Algorithm: rsaEncryption
                Public Key size: 4096
                SAN ENTRIES: None

        CA Certificate:
                Status: Valid,   Days to expiration:278
                Serial Number: 00
                Subject:  C=IN,ST=KAR,O=CITRIX,CN=root4098.com
                Issuer:  C=IN,ST=KAR,O=CITRIX,CN=root4098.com
                Signature Algorithm: sha256WithRSAEncryption
                Validity
                        Not Before: Jul 13 10:10:23 2021 GMT
                        Not After : Jul 13 10:10:23 2022 GMT
                Public Key Algorithm: rsaEncryption
                Public Key size: 2048
                SAN ENTRIES: None

1)      Vserver Name: v_server
<!--NeedCopy-->
```

Para vincular un paquete de certificados a un servidor virtual SSL como un paquete de certificados SNI

En el símbolo del sistema, escriba:

```
bind ssl vserver <vip-name> -certkeybundleName b2 -SNICertkeybundle
```

Ejemplo:


```
bind ssl vserver v_server -certkeyBundleName cert_bundle -
    sniCertkeybundle

sh ssl certkeybundle cert_bundle

1) Name: cert_bundle
        Bundle path: bundle_4096.pem
        Certificate:
                Status: Valid,   Days to expiration:278
                Serial Number: 83
                Subject:  C=IN,ST=KAR,O=CITRIX,CN=4096.com
                Issuer:  C=IN,ST=KAR,O=CITRIX,CN=ia24096.com
                Signature Algorithm: sha256WithRSAEncryption
                Validity
                        Not Before: Jul 13 10:17:57 2021 GMT
                        Not After : Jul 13 10:17:57 2022 GMT
                Public Key Algorithm: rsaEncryption
                Public Key size: 4096
                SAN ENTRIES: None


        CA Certificate:
                Status: Valid,   Days to expiration:278
                Serial Number: 82
                Subject:  C=IN,ST=KAR,O=CITRIX,CN=ia24096.com
                Issuer:  C=IN,ST=KAR,O=CITRIX,CN=ia14098.com
                Signature Algorithm: sha256WithRSAEncryption
                Validity
                        Not Before: Jul 13 10:15:37 2021 GMT
                        Not After : Jul 13 10:15:37 2022 GMT
                Public Key Algorithm: rsaEncryption
                Public Key size: 4096
                SAN ENTRIES: None

        CA Certificate:
                Status: Valid,   Days to expiration:278
                Serial Number: 81
                Subject:  C=IN,ST=KAR,O=CITRIX,CN=ia14098.com
                Issuer:  C=IN,ST=KAR,O=CITRIX,CN=root4098.com
                Signature Algorithm: sha256WithRSAEncryption
                Validity
                        Not Before: Jul 13 10:13:20 2021 GMT
                        Not After : Jul 13 10:13:20 2022 GMT
                Public Key Algorithm: rsaEncryption
```



```
44                 Public Key size: 4096
45                 SAN ENTRIES: None
46
47         CA Certificate:
48                 Status: Valid,   Days to expiration:278
49                 Serial Number: 00
50                 Subject:  C=IN,ST=KAR,O=CITRIX,CN=root4098.com
51                 Issuer:  C=IN,ST=KAR,O=CITRIX,CN=root4098.com
52                 Signature Algorithm: sha256WithRSAEncryption
53                 Validity
54                         Not Before: Jul 13 10:10:23 2021 GMT
55                         Not After : Jul 13 10:10:23 2022 GMT
56                 Public Key Algorithm: rsaEncryption
57                 Public Key size: 2048
58                 SAN ENTRIES: None
59
60 1)    Vserver Name: v_server
61 2)    Vserver Name: v_server
62 <!--NeedCopy-->
```

Para desvincular un paquete de certificados de un servidor virtual SSL

En el símbolo del sistema, escriba:

```
unbind ssl vserver <vip-name> -certkeybundleName <certkeybundle_name> [ -SNICertkeybundle]
```

Ejemplo:

```
unbind ssl vserver v_server -certkeybundleName cert_bundle
```

Casos de usuario para el enlace de paquetes

En los siguientes casos, se explica cómo el dispositivo ADC procesa una solicitud relacionada con los paquetes de certificados.

Caso 1: un par de claves de certificado y un paquete de certificados que contienen el mismo certificado de servidor están enlazados al mismo servidor virtual SSL

Al vincular un par de claves de certificado y un paquete de certificados que contiene el mismo certificado de servidor al mismo servidor virtual SSL, el orden de los comandos determina el enlace final.

Por ejemplo:

- El paquete de certificados bundle1.pem contiene el certificado de servidor S1 y los certificados intermedios IC1 e IC2.
- El archivo de certificado server_cert.pem contiene S1.

Tanto bundle1.pem como server_cert.pem tienen el mismo certificado de servidor S1.

Si los siguientes comandos se ejecutan en el orden especificado, el enlace del certificado del servidor al servidor virtual SSL reemplaza el enlace del paquete de certificados a ese servidor virtual.

1. `add ssl certkeybundle b1 -bundlefile bundle1.pem`
2. `add ssl certkey server_cert -cert server_cert.pem`
3. `bind ssl vserver v1 -certkeybundle b1`
4. `bind ssl vserver v1 -cert server_cert`

Caso 2: dos paquetes de certificados contienen la misma cadena de certificados intermedia

Puede agregar dos paquetes de certificados con la misma cadena de certificados intermedia. Los dos paquetes actúan como entidades independientes.

En el siguiente ejemplo, el paquete de certificados 1 contiene el certificado de servidor S1 y los certificados intermedios IC1 e IC2 en ese orden. El paquete de certificados 2 contiene el certificado de servidor S2 y los certificados intermedios IC1 e IC2 en ese orden.

- Paquete de certificados bundle1.pem (S1, IC1, IC2)
- Paquete de certificados bundle2.pem (S2, IC1, IC2)

Cuando se selecciona S1 en el paquete 1 en el proceso de establecimiento de enlace SSL, la cadena de certificados intermedia del paquete 1 se envía al cliente.

```
add ssl certkeybundle bundle-1 -bundlefile bundle1.pem
add ssl certkeybundle bundle-2 -bundlefile bundle2.pem
```

Caso 2: dos paquetes de certificados contienen algunos certificados intermedios comunes en la cadena

Puede agregar dos paquetes de certificados con algunos certificados intermedios comunes en la cadena.

En el siguiente ejemplo, el paquete 1 contiene el certificado de servidor S1 y los certificados intermedios IC1 e IC2. El paquete de certificados 2 contiene el certificado de servidor S2 y los certificados intermedios IC1, IC2 e IC3.

Paquete de certificados bundle1.pem (S1, IC1, IC2)
Paquete de certificados bundle2.pem (S2, IC1, IC2, IC3)

```
add ssl certkeybundle bundle-1 -bundlefile bundle1.pem
add ssl certkeybundle bundle-2 -bundlefile bundle2.pem
```


Cuando se selecciona S1 en el paquete 1 en el proceso de establecimiento de enlace SSL, la cadena de certificados intermedia del paquete 1 se envía al cliente. Es decir, (S1→IC1→IC2) se envía al cliente. No se agrega IC3.

Cuando se selecciona S2 en el paquete 2 en el proceso de enlace SSL, la cadena de certificados intermedia del paquete 2 solo se envía al cliente. Es decir, (S1→IC1→IC2→IC3) se envía al cliente.

Limitaciones del paquete de certificados

- No se admite la supervisión del estado de un certificado en el paquete de certificados.
- No se admite la actualización de un paquete de certificados.
- Los paquetes de certificados solo se pueden vincular a servidores virtuales SSL.
- No se admite el grapado OCSP.

Actualizar un certificado de servidor existente

Para cambiar un certificado de servidor existente manualmente, debe realizar los siguientes pasos:

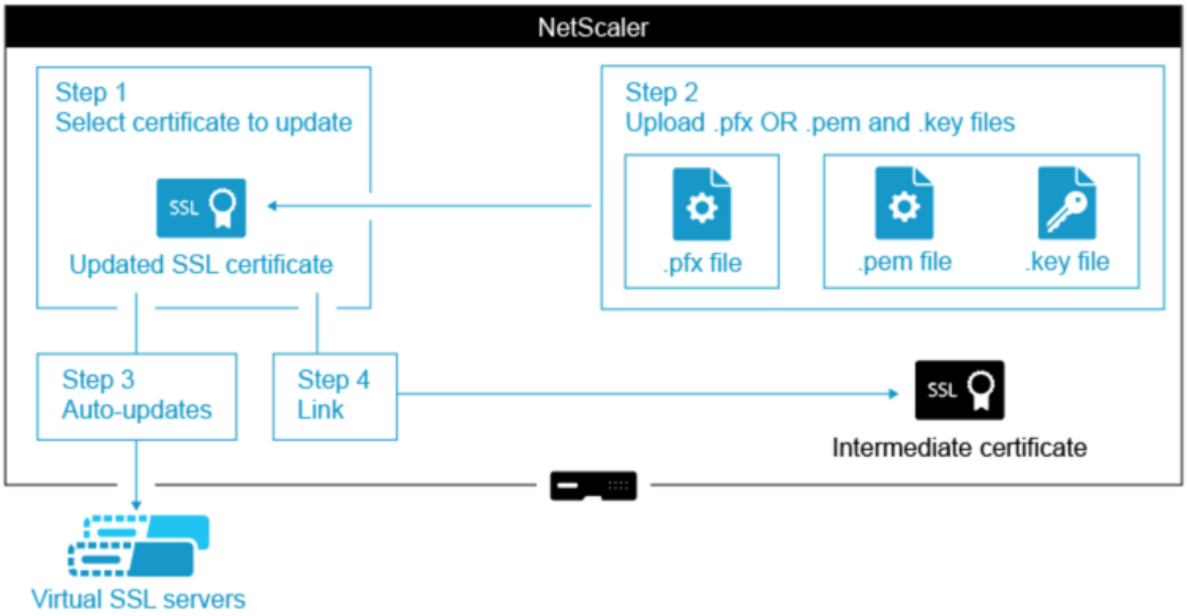
1. Desvincule el certificado antiguo del servidor virtual.
2. Retire el certificado del dispositivo.
3. Agregue el nuevo certificado al dispositivo.
4. Enlazar el nuevo certificado al servidor virtual.

Para reducir el tiempo de inactividad al reemplazar un par de claves de certificado, puede actualizar un certificado existente. Si quiere reemplazar un certificado por un certificado que se emitió para un dominio diferente, debe inhabilitar las comprobaciones de dominio antes de actualizar el certificado.

Para recibir notificaciones sobre certificados a punto de caducar, puede habilitar el control de caducidad.

Cuando quita o desvincula un certificado de un servidor o servicio virtual SSL configurado, el servidor o servicio virtual se vuelve inactivo. Se activan después de que se les vincule un nuevo certificado válido. Para reducir el tiempo de inactividad, puede usar la función de actualización para reemplazar un par de claves de certificado que esté vinculado a un servidor virtual SSL o a un servicio SSL.

Diagrama general de cómo actualizar un certificado SSL en el dispositivo Citrix ADC.



Enlace de vídeo a Cómo actualizo un certificado existente.

Actualizar un par de claves de certificado existente mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para actualizar un par de claves de certificado existente y verificar la configuración:

```
update ssl certkey <certkeyName> -cert <string> -key <string>

show ssl certKey <certkeyName>
<!--NeedCopy-->
```

Ejemplo:

```
update ssl certkey siteAcertkey -cert /nsconfig/ssl/cert.pem -key /
   nsconfig/ssl/pkey.pem

Done

show ssl certkey siteAcertkey

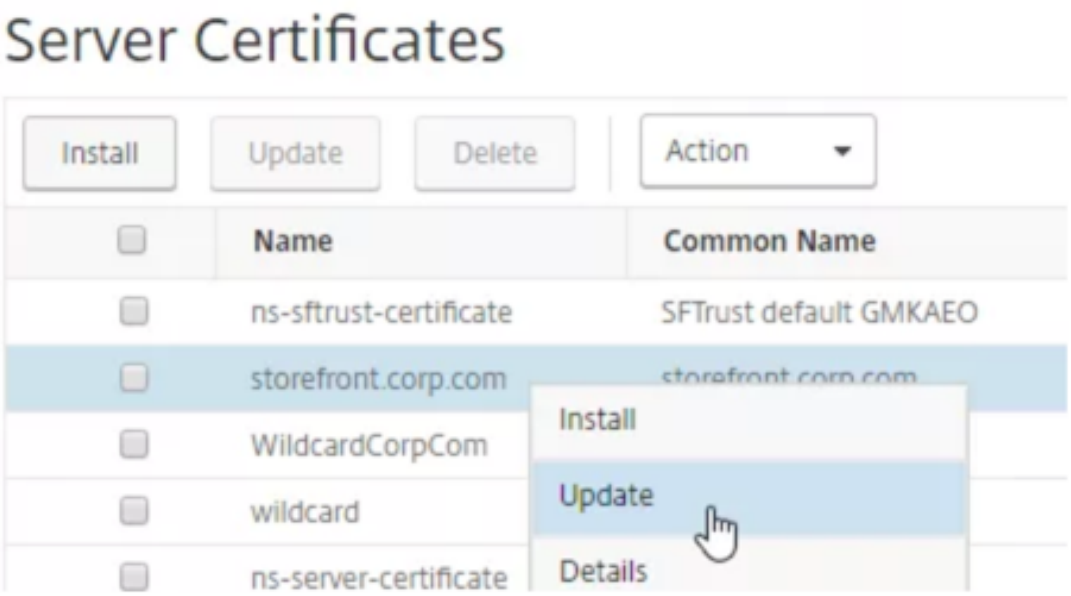
Name: siteAcertkey       Status: Valid
          Version: 3
          Serial Number: 02
          Signature Algorithm: md5WithRSAEncryption
```



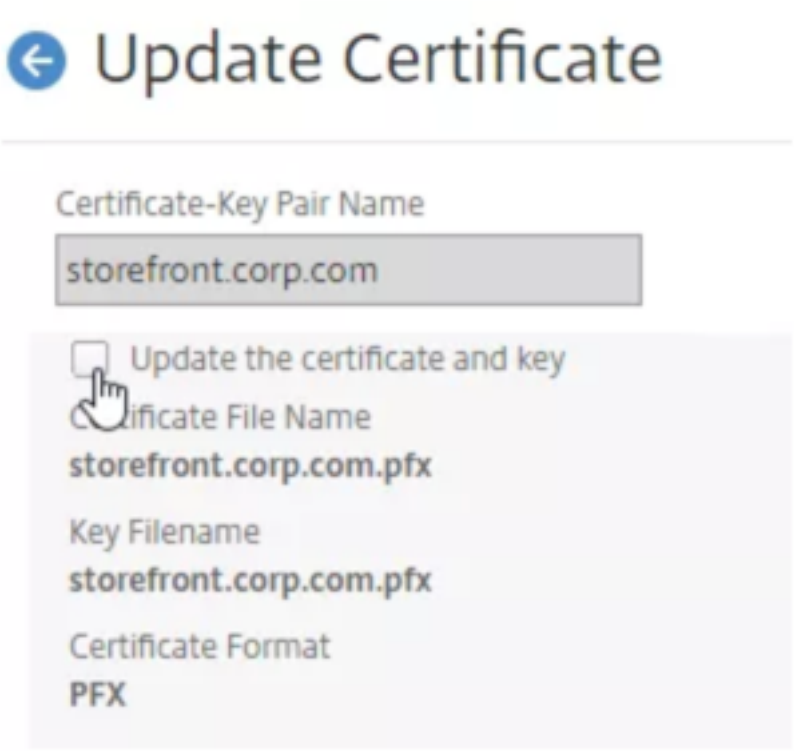
```
            Issuer: /C=US/ST=CA/L=Santa Clara/O=siteA/OU=Tech
            Validity
                 Not Before: Nov 11 14:58:18 2001 GMT
                 Not After: Aug 7 14:58:18 2004 GMT
            Subject: /C=US/ST-CA/L=San Jose/O=CA/OU=Security
            Public Key Algorithm: rsaEncryption
            Public Key size: 2048
Done
<!--NeedCopy-->
```

Actualizar un par de claves de certificado existente mediante la interfaz gráfica de usuario

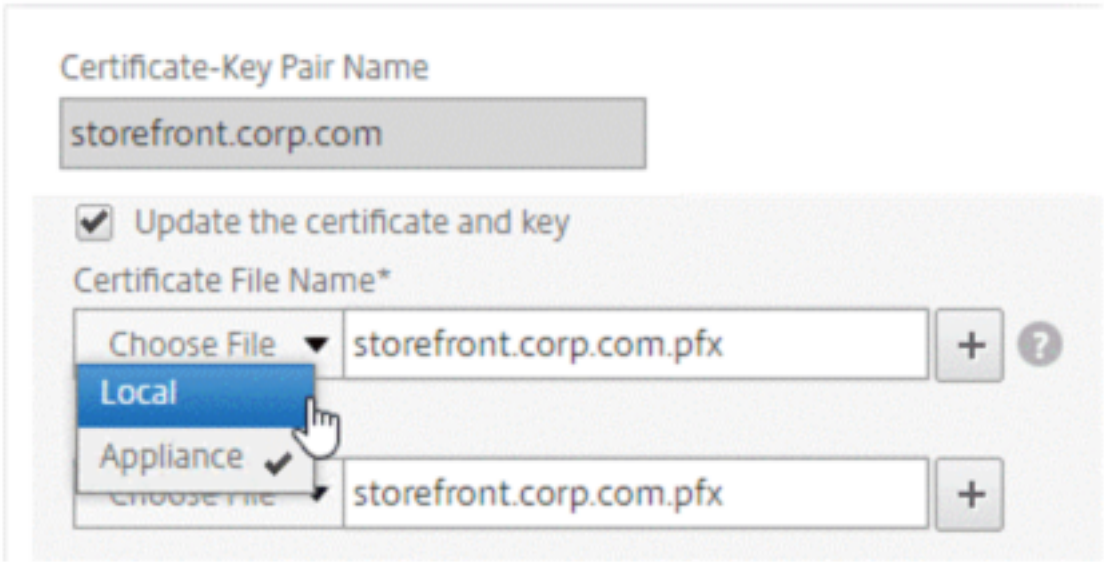
1. Vaya a **Administración del tráfico** > **SSL** > **Certificados** > **Certificados de servidor**.
2. Seleccione el certificado que quiere actualizar y haga clic en **Actualizar**.



3. Selecciona **Actualizar el certificado y la clave**.



4. En **Nombre de archivo de certificado**, haga clic en **Elegir archivo** > **Local** y busque el archivo .pfx o el archivo PEM de certificado actualizados.

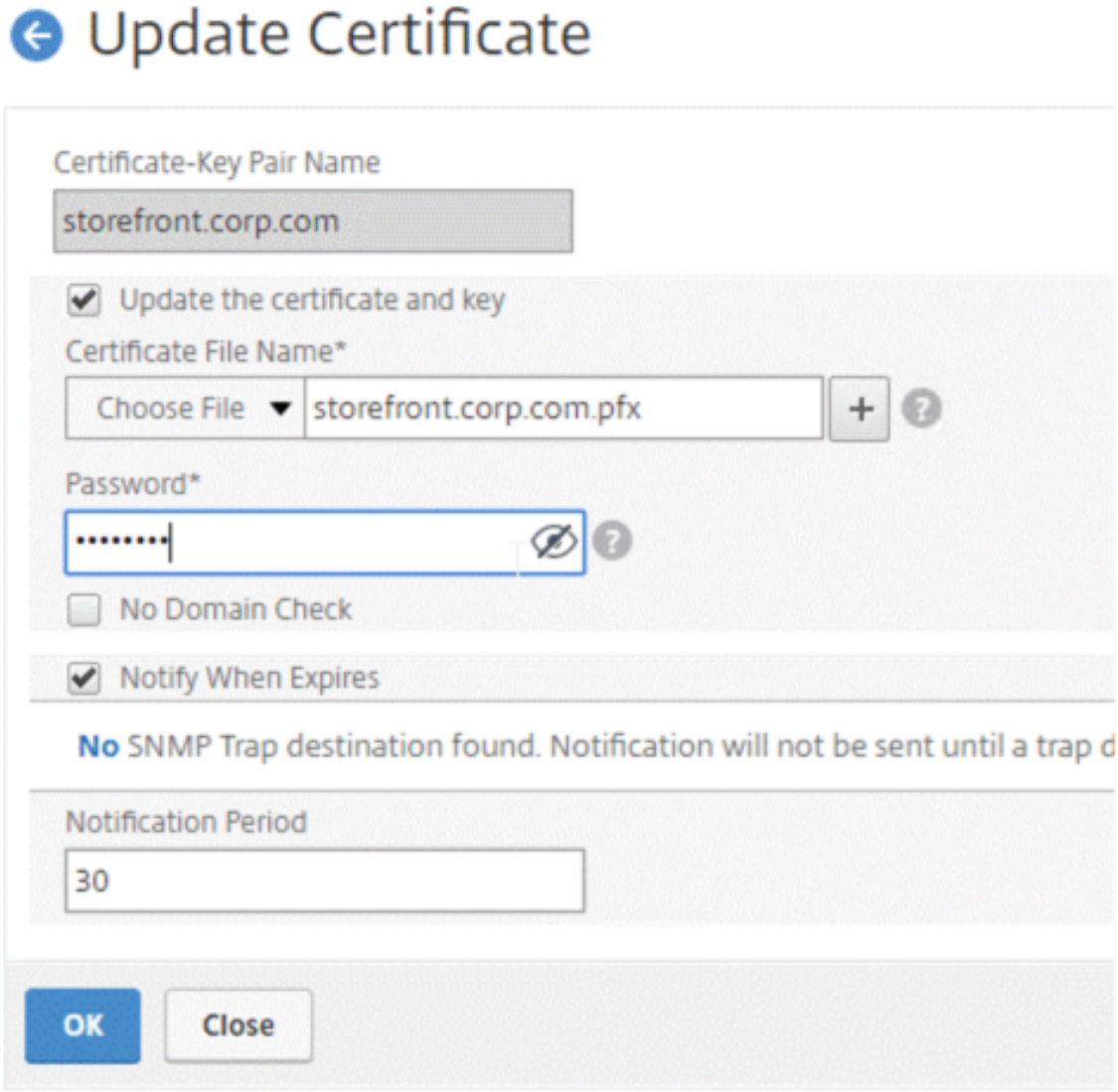


   - Si carga un archivo .pfx, se le pedirá que especifique la contraseña del archivo .pfx.
   - Si carga un archivo pem de certificado, también debe cargar un archivo de clave de certificado. Si la clave está cifrada, debe especificar la contraseña de cifrado.

5. Si el nombre común del nuevo certificado no coincide con el certificado anterior, seleccione **Sin**

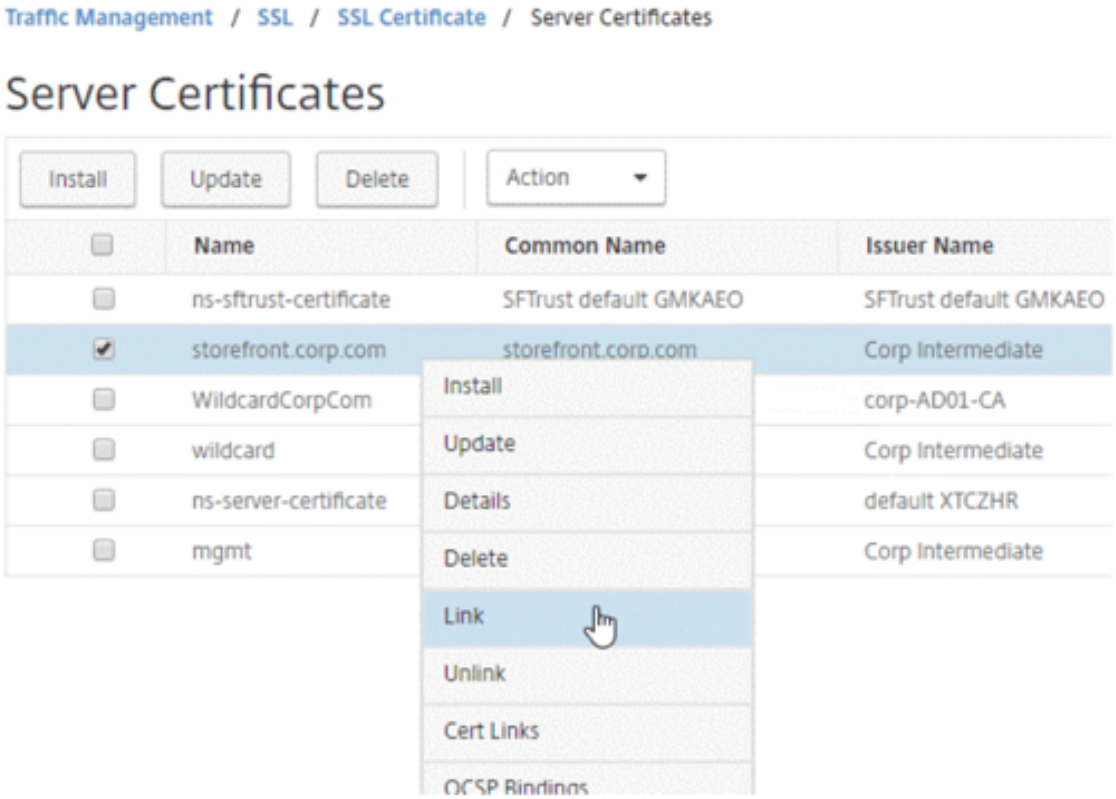
verificación de dominio.

6. Haga clic en **Aceptar**. Todos los servidores virtuales SSL a los que está vinculado este certificado se actualizan automáticamente.



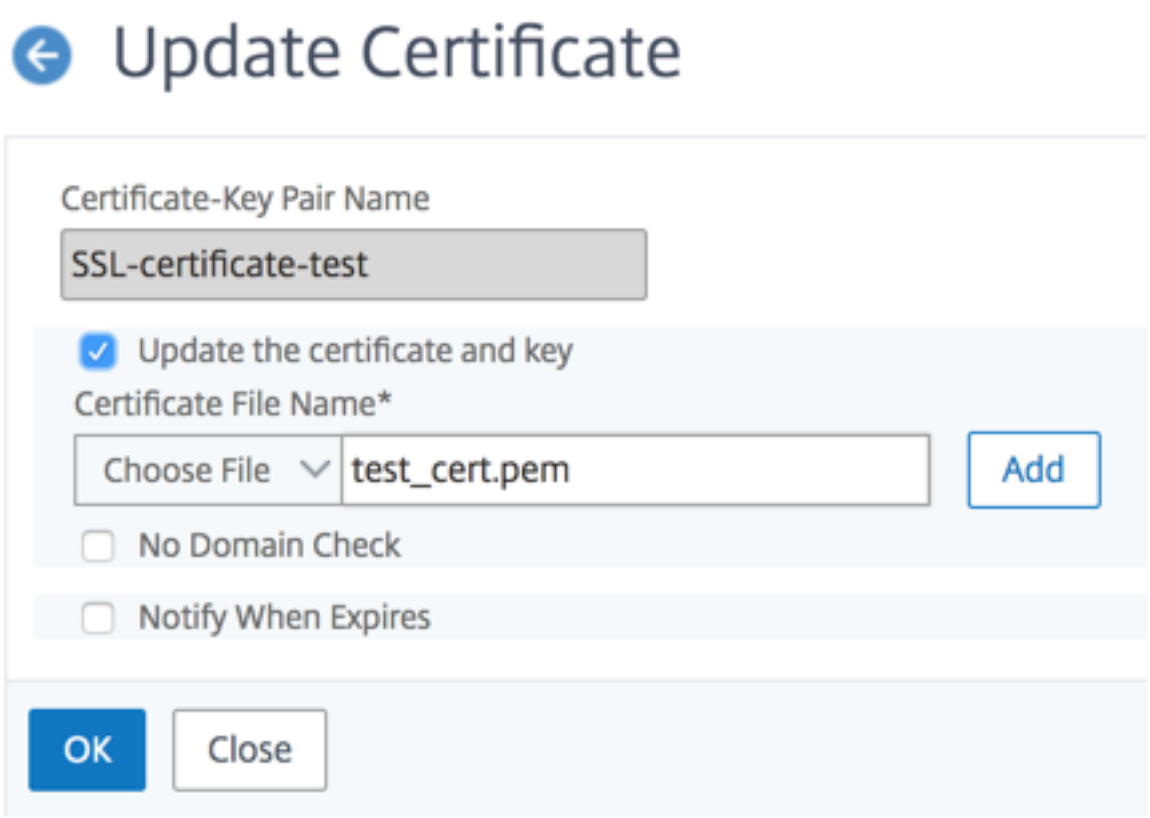
7. Después de reemplazar el certificado, es posible que tenga que actualizar el vínculo de certificado a un nuevo certificado intermedio. Para obtener más información sobre cómo actualizar un certificado intermedio sin romper los vínculos, consulte Actualizar un certificado intermedio sin romper los vínculos.
    - Haga clic con el botón secundario en el certificado actualizado y haga clic en **Vínculos**de certificado para ver si está vinculado a un certificado intermedio.
    - Si el certificado no está vinculado, haga clic con el botón secundario en el certificado actualizado y haga clic en Vincular para **vincularlo** a un certificado intermedio. Si no ve una opción para vincular, primero debe instalar un nuevo certificado intermedio en el dispos-

itivo en el nodo **Certificados de CA**.



Actualizar un certificado de CA existente

Los pasos para actualizar un certificado de CA existente son los mismos que para actualizar un certificado de servidor existente. La única diferencia es que no necesita una clave en el caso de los certificados de CA.



Inhabilitar las comprobaciones

Cuando se reemplaza un certificado SSL en el dispositivo, el nombre de dominio mencionado en el nuevo certificado debe coincidir con el nombre de dominio del certificado que se reemplaza. Por ejemplo, si tiene un certificado emitido para abc.com y lo actualiza con un certificado emitido para def.com, se producirá un error en la actualización del certificado.

Sin embargo, si quiere que el servidor que ha estado hospedando un dominio en particular aloje un dominio nuevo, inhabilite la comprobación de dominio antes de actualizar su certificado.

Inhabilitar la comprobación de dominio para un certificado mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para inhabilitar la verificación de dominio y verificar la configuración:

```
update ssl certKey <certkeyName> -noDomainCheck

show ssl certKey <certkeyName>
<!--NeedCopy-->
```


Ejemplo:

```
update ssl certKey sv -noDomainCheck

Done

show ssl certkey sv

Name: sv
Cert Path: /nsconfig/ssl/complete/server/server_rsa_512.pem
Key Path: /nsconfig/ssl/complete/server/server_rsa_512.ky
Format: PEM
Status: Valid,   Days to expiration:9349
Certificate Expiry Monitor: DISABLED
Done
<!--NeedCopy-->
```

Inhabilitar la comprobación de dominio para un certificado mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > SSL > Certificados**, seleccione un certificado y haga clic en **Actualizar**.
2. Seleccione **Sin verificación de dominio**.

Reemplazar el certificado predeterminado de un dispositivo ADC por un certificado de CA de confianza que coincida con el nombre de host del dispositivo

El siguiente procedimiento supone que el certificado predeterminado (`ns-server-certificate`) está vinculado a los servicios internos.

1. Vaya a **Administración del tráfico > SSL > Certificados SSL > Crear solicitud de certificado**.
2. En nombre común, escriba `test.citrixadc.com`.
3. Envíe la CSR a una entidad de certificación de confianza.
4. Después de recibir el certificado de la CA de confianza, copie el archivo `/nsconfig/ssl` en el directorio.
5. Vaya a **Administración del tráfico > SSL > Certificados > Certificados de servidor**.
6. Seleccione el certificado de servidor predeterminado (`ns-server-certificate`) y haga clic en **Actualizar**.
7. En el cuadro de diálogo **Actualizar certificado**, en **Nombre de archivo de certificado**, busque el certificado recibido de la CA después de firmar.

8. En el campo **Nombre de archivo de clave**, especifique el nombre de archivo de clave privada predeterminado (`ns-server.key`).
9. Seleccione **Sin verificación de dominio**.
10. Haga clic en **Aceptar**.

Habilitar el monitor de caducidad

Un certificado SSL es válido durante un período específico. Una implementación típica incluye varios servidores virtuales que procesan transacciones SSL y los certificados vinculados a ellos pueden caducar en momentos diferentes. Un monitor de caducidad configurado en el dispositivo crea entradas en los registros de auditoría syslog y ns del dispositivo cuando un certificado configurado caduca.

Si quiere crear alertas SNMP para la caducidad de certificados, debe configurarlas por separado.

Habilitar un monitor de caducidad para un certificado mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para habilitar un monitor de caducidad para un certificado y verificar la configuración:

```
set ssl certKey <certkeyName> [-expiryMonitor ( ENABLED | DISABLED ) [-
    notificationPeriod <positive_integer>]]

show ssl certKey <certkeyName>
<!--NeedCopy-->
```

Ejemplo:

```
set ssl certKey sv -expiryMonitor ENABLED  - notificationPeriod 60
Done
<!--NeedCopy-->
```

Habilitar un monitor de caducidad para un certificado mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > SSL > Certificados**, seleccione un certificado y haga clic en **Actualizar**.
2. Seleccione **Notificar cuando caduque**y, si lo quiere, especifique un período de notificación.

Actualizar un certificado intermedio sin romper los enlaces

Ahora puede actualizar un certificado intermedio sin romper ningún vínculo existente. La extensión "AuthorityKeyIdentifier", en el certificado vinculado emitido por el certificado que se va a reemplazar, no debe contener un campo de número de serie del certificado de autoridad ("authorityCertSerialNumber"). Si la extensión "AuthorityKeyIdentifier" contiene un campo de número de serie, los números de serie del certificado antiguo y el nuevo deben ser los mismos. Puede actualizar cualquier cantidad de certificados en el enlace, de uno en uno, si se cumple la condición anterior. Anteriormente, los enlaces se rompían si se actualizaba un certificado intermedio.

Por ejemplo, hay cuatro certificados: `CertA`, `CertB`, `CertC` y `CertD`. El certificado `CertA` es el emisor de `CertB`, `CertB` es el emisor de `CertC`, etc. Si quiere reemplazar un certificado intermedio `CertB` por `CertB_new`, sin romper el vínculo, se debe cumplir la siguiente condición:

El número de serie del certificado de `CertB` debe coincidir con el número de serie del certificado de `CertB_new` si se cumplen las dos condiciones siguientes:

- La extensión `AuthorityKeyIdentifier` está presente en `CertC`.
- Esta extensión contiene un campo de número de serie.

Si el nombre común en un certificado cambia, al actualizar el certificado, especifique `nodomaincheck` .

En el ejemplo anterior, para cambiar "www.ejemplo.com" por "*.ejemplo.com", seleccione el parámetro "Sin verificación de dominio". `CertD`

Actualizar el certificado mediante la CLI

En el símbolo del sistema, escriba:

```
update ssl certKey <certkeyName> -cert <string> [-password] -key <
    string>  [-noDomainCheck]
<!--NeedCopy-->
```

Ejemplo:

```
update ssl certkey siteAcertkey -cert /nsconfig/ssl/cert.pem -key /
    nsconfig/ssl/pkey.pem -noDomainCheck
<!--NeedCopy-->
```


Mostrar una cadena de certificados

Un certificado contiene el nombre de la autoridad emisora y el sujeto al que se emite el certificado. Para validar un certificado, debe mirar al emisor de ese certificado y confirmar si confía en él. Si no confía en el emisor, debe ver quién emitió el certificado de emisor. Suba en la cadena hasta llegar al certificado de CA raíz o a un emisor en el que confíe.

Como parte del protocolo de enlace SSL, cuando un cliente solicita un certificado, el dispositivo presenta un certificado y la cadena de certificados de emisor presentes en el dispositivo. Un administrador puede ver la cadena de certificados de los certificados presentes en el dispositivo e instalar los certificados que falten.

Ver la cadena de certificados de los certificados presentes en el dispositivo mediante la CLI

En el símbolo del sistema, escriba:

```
show ssl certchain <cert_name>
<!--NeedCopy-->
```

Ejemplos

Hay 3 certificados: c1, c2 y c3. El certificado c3 es el certificado de CA raíz y firma c2 y c2 firma c1. Los siguientes ejemplos ilustran la salida del
`show ssl certchain c1` comando en diferentes casos.

Caso 1:

El certificado c2 está vinculado a c1 y c3 está vinculado a c2.

El certificado c3 es un certificado de CA raíz.

Si ejecuta el siguiente comando, se muestran los vínculos del certificado hasta el certificado de CA raíz.

```
show ssl certchain c1

Certificate chain details of certificate name c1 are:
    1) Certificate name: c2              linked; not a root
       certificate
    2) Certificate name: c3              linked; root certificate
Done
<!--NeedCopy-->
```


Caso 2:

El certificado c2 está vinculado a c1.

El certificado c2 no es un certificado de CA raíz.

Si ejecuta el siguiente comando, se muestra la información de que el certificado c3 es un certificado de CA raíz pero no está vinculado a c2.

```
show ssl certchain c1

Certificate chain  details of certificate name c1 are:
    1) Certificate Name: c2              linked; not a root
       certificate
    2) Certificate Name: c3              not linked; root certificate
    Done
<!--NeedCopy-->
```

Caso 3:

Los certificados c1, c2 y c3 no están vinculados, sino que están presentes en el dispositivo.

Si ejecuta el siguiente comando, se muestra información sobre todos los certificados que comienzan por el emisor del certificado c1. También se especifica que los certificados no están vinculados.

```
show ssl certchain c1

Certificate chain details of certificate name c1 are:
    1) Certificate Name: c2              not linked; not a root
       certificate
    2) Certificate Name: c3              not linked; root certificate
    Done
<!--NeedCopy-->
```

Caso 4:

El certificado c2 está vinculado a c1.

El certificado c3 no está presente en el dispositivo.

Si ejecuta el siguiente comando, se muestra información sobre el certificado vinculado a c1. Se le solicitará que agregue un certificado con el nombre de sujeto especificado en c2. En este caso, se pide al usuario que agregue el certificado de CA raíz c3.


```
show ssl certchain c1

Certificate chain details of certificate name c1 are:
    1) Certificate Name: c2              linked; not a root
       certificate
    2) Certificate Name: /C=IN/ST=ka/O=netscaler/CN=test
       Action: Add a certificate with this subject name.
Done
<!--NeedCopy-->
```

Caso 5:

Un certificado no está vinculado al certificado c1 y el certificado del emisor de c1 no está presente en el dispositivo.

Si ejecuta el siguiente comando, se le pedirá que agregue un certificado con el nombre de sujeto en el certificado c1.

```
sh ssl certchain c1

Certificate chain details of certificate name c1 are:
    1) Certificate Name: /ST=KA/C=IN
       Action: Add a certificate with this subject name.
<!--NeedCopy-->
```

Generar un certificado de prueba de servidor

January 12, 2021

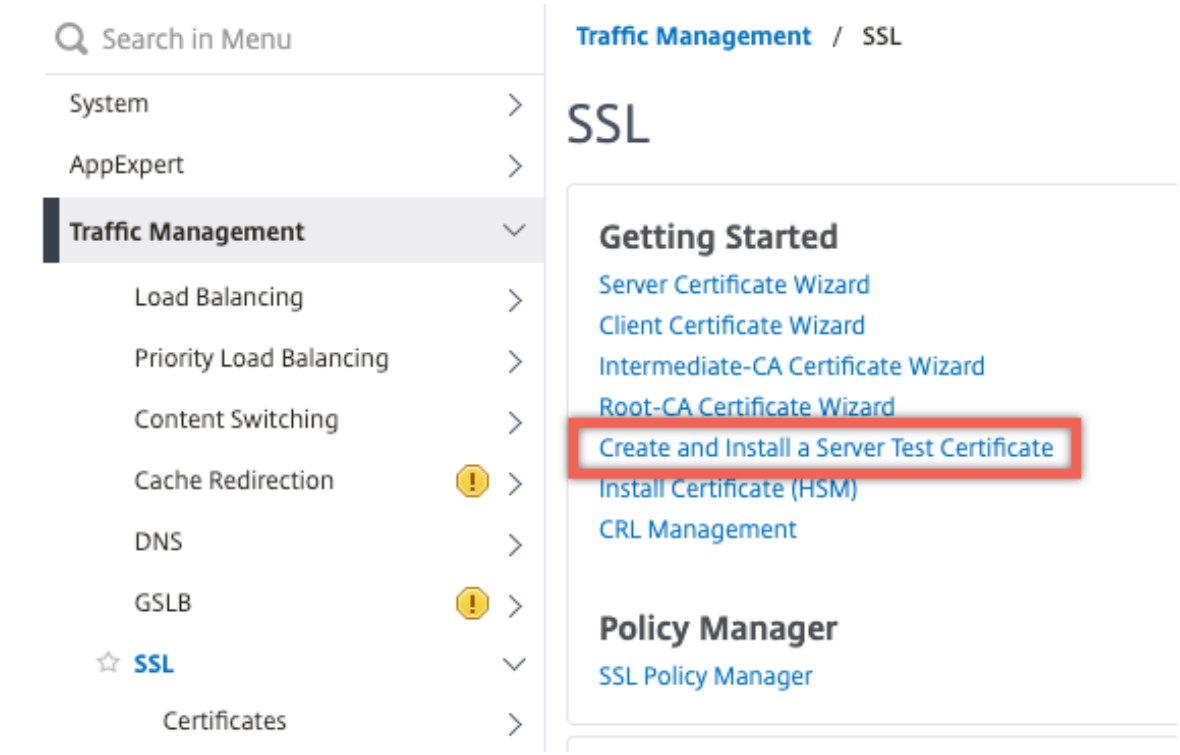
El dispositivo Citrix ADC permite crear un certificado de prueba para la autenticación del servidor mediante un asistente GUI en la utilidad de configuración. Un certificado de servidor se utiliza para autenticar e identificar un servidor en un protocolo de enlace SSL. Normalmente, una entidad emisora de certificados de confianza emite un certificado de servidor. El servidor envía el certificado a un cliente que lo utiliza para autenticar el servidor.

Para emitir un certificado de prueba de servidor, el dispositivo funciona como una entidad emisora de certificados. Este certificado se puede enlazar a un servidor virtual SSL para la autenticación en un protocolo de enlace SSL con un cliente. Este certificado es solo para fines de prueba. No utilizar en un entorno de producción.

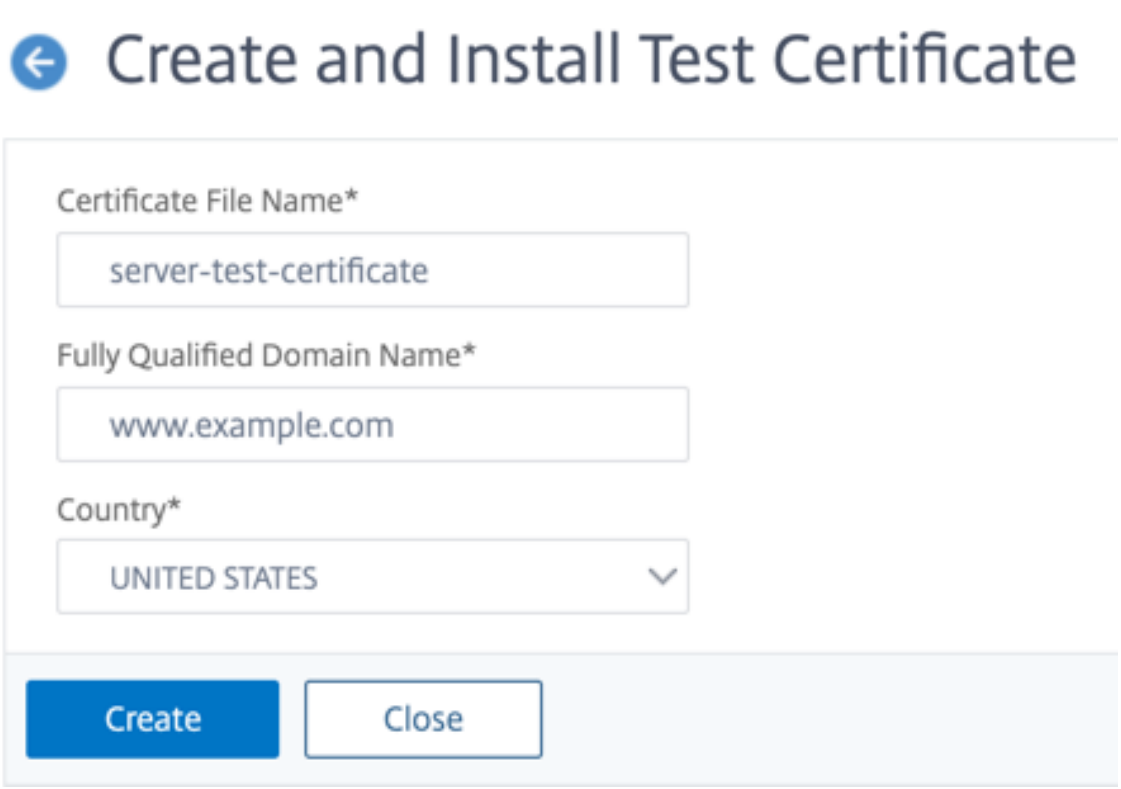
Puede instalar el certificado de prueba del servidor en cualquier servidor virtual que utilice el protocolo SSL o SSL_TCP.

Generar un certificado de prueba de servidor mediante la interfaz gráfica de usuario

1. Vaya a **Administración de tráfico > SSL** y, en el **grupo Certificados SSL**, seleccione **Crear e instalar un certificado de prueba de servidor**.



2. Introduzca los detalles de los parámetros y haga clic en **Crear**.



Importar y convertir archivos SSL

August 20, 2021

Ahora puede importar recursos SSL, como certificados, claves privadas, CRL y claves DH, desde hosts remotos incluso si el acceso FTP a estos hosts no está disponible. Esta función es especialmente útil en entornos donde el acceso de shell al host remoto está restringido. Las carpetas predeterminadas se crean en /nsconfig/ssl de la siguiente manera:

- Para archivos de certificado: /nsconfig/ssl/certfile
- Para claves privadas: El archivo /nsconfig/ssl/keyfile
- Para CRL: /var/netscaler/ssl/crlfile
- Para claves DH: /nsconfig/ssl/dhfile

Se admiten las importaciones de servidores HTTP y HTTPS. Sin embargo, la importación falla si el archivo está en un servidor HTTPS que requiere autenticación de certificado de cliente para el acceso.

> **Nota:**
>
> El comando import no se almacena en el archivo de configuración (ns.conf), ya que volver a im-

> portar el archivo después de reiniciar podría causar un error.

Importar un archivo de certificado

Puede utilizar la CLI y la GUI para importar un archivo (recurso) desde un host remoto.

Importar un archivo de certificado desde un host remoto mediante la CLI

En el símbolo del sistema, escriba:

```
import ssl certFile [<name>] [<src>]
<!--NeedCopy-->
```

Ejemplo:

```
import ssl certfile my-certfile http://www.example.com/file_1
<!--NeedCopy-->
```

```
show ssl certfile
     Name : my-certfile
     URL : http://www.example.com/file_1
<!--NeedCopy-->
```

Para quitar un archivo de certificado, utilice el `rm ssl certFile` comando, que solo acepta el argumento 'name'.

Importar un archivo de clave desde un host remoto mediante la CLI

En el símbolo del sistema, escriba:

```
import ssl keyFile [<name>] [<src>]
<!--NeedCopy-->
```

Ejemplo:


```
import ssl keyfile my-keyfile http://www.example.com/key_file
<!--NeedCopy-->
```

```
show ssl keyfile
     Name : my-keyfile
     URL : http://www.example.com/key_file
<!--NeedCopy-->
```

Para eliminar un archivo de claves, utilice el `rm ssl keyFile` comando, que solo acepta el argumento 'name'.

Importar un archivo CRL desde un host remoto mediante la CLI

En el símbolo del sistema, escriba:

```
import ssl crlFile [<name>] [<src>]
<!--NeedCopy-->
```

Para quitar un archivo CRL, utilice el `rm ssl crlFile` comando, que solo acepta el <name> argumento.

Ejemplo:

```
import ssl crlfile my-crlfile http://www.example.com/crl_file

show ssl crlfile

    Name : my-crlfile
    URL : http://www.example.com/crl_file
<!--NeedCopy-->
```

Importar un archivo DH desde un host remoto mediante la CLI

En el símbolo del sistema, escriba:

```
import ssl dhFile [<name>] [<src>]
<!--NeedCopy-->
```


Ejemplo:

```
import ssl dhfile my-dhfile http://www.example.com/dh_file
show ssl dhfile
     Name : my-dhfile
     URL : http://www.example.com/dh_file
<!--NeedCopy-->
```

Para quitar un archivo DH, utilice el `rm ssl dhFile` comando, que solo acepta el <name> argumento.

Importar un recurso SSL mediante la interfaz gráfica de usuario

Vaya a **Traffic Management > SSL > Imports** y, a continuación, seleccione la ficha correspondiente.

Importar certificados PKCS #8 y PKCS #12

Si quiere utilizar certificados y claves que ya tiene en otros servidores o aplicaciones seguros de la red, puede exportarlos e importarlos al dispositivo Citrix ADC. Es posible que tenga que convertir certificados y claves exportados antes de poder importarlos al dispositivo Citrix ADC.

Para obtener información detallada sobre cómo exportar certificados desde servidores seguros o aplicaciones de la red, consulte la documentación del servidor o aplicación desde la que quiere exportar.

> **Nota:**
>
> Para la instalación en el dispositivo Citrix ADC, los nombres de clave y certificados no pueden contener espacios ni caracteres especiales que no sean los que admite el sistema de archivos UNIX. Siga la convención de nomenclatura adecuada al guardar la clave y el certificado exportados.

Normalmente se envía un par de certificados y claves privadas en el formato PKCS #12. El dispositivo admite formatos PEM y DER para certificados y claves. Para convertir PKCS #12 a PEM o DER, o PEM o DER a PKCS #12, consulte la sección “Convertir certificados SSL para importar o exportar” más adelante en esta página.

El dispositivo Citrix ADC no admite claves PEM en formato PKCS #8. Sin embargo, puede convertir estas claves a un formato compatible mediante la interfaz OpenSSL, a la que puede acceder desde la CLI o la utilidad de configuración. Antes de convertir la clave, debe verificar que la clave privada esté en formato PKCS #8. Las claves en formato PKCS #8 suelen comenzar con el siguiente texto:

```
-----BEGIN ENCRYPTED PRIVATE KEY-----

```



```
3
4
5 leuSSZQZKgrgUQ==
6
7
8
9 -----END ENCRYPTED PRIVATE KEY-----
10 <!--NeedCopy-->
```

Abra la interfaz OpenSSL desde la CLI

1. Abra una conexión SSH al dispositivo mediante un cliente SSH, como PuTTY.
2. Inicie sesión en el dispositivo mediante las credenciales de administrador.
3. En el símbolo del sistema, escriba shell.
4. En el símbolo del shell, escriba `openssl`.

Abra la interfaz OpenSSL desde la GUI

Vaya a **Administración de tráfico > SSL** y, en el grupo Herramientas, seleccione **interfaz OpenSSL**.

Convertir un formato de clave PKCS #8 no compatible a un formato de clave compatible cifrado mediante la interfaz OpenSSL

En la solicitud de OpenSSL, escriba uno de los siguientes comandos, en función de si el formato de clave no admitido es de tipo RSA o ECDSA:

```
1 OpenSSL>rsa- in <PKCS#8 Key Filename> -des3 -out <encrypted Key
     Filename>
2
3 OpenSSL>ec -in <PKCS#8 Key Filename> -des3 -out <encrypted Key Filename
     >
4 <!--NeedCopy-->
```

Parámetros para convertir un formato de clave no admitido a un formato de clave admitido

- Nombre de**archivo de clave PKCS #8:** nombre de archivo de entrada de la clave privada PKCS #8 incompatible.
- nombre de**archivo de clave cifrada:** nombre de archivo de salida de la clave privada cifrada compatible en formato PEM.

- Nombre de**archivo de clave sin cifrar:** nombre de archivo de salida de la clave privada no cifrada compatible en formato PEM.

Convertir certificados SSL para importar o exportar

Un dispositivo Citrix ADC admite los formatos PEM y DER para certificados SSL. Otras aplicaciones, como los exploradores cliente y algunos servidores seguros externos, requieren varios formatos estándar de criptografía de clave pública (PKCS). El dispositivo puede convertir el formato PKCS #12 a formato PEM o DER para importar un certificado al dispositivo, y puede convertir PEM o DER a PKCS #12 para exportar un certificado. Para mayor seguridad, la conversión de un archivo para la importación puede incluir el cifrado de la clave privada con el algoritmo DES o DES3.

> **Nota:**
>
> Si utiliza la GUI para importar un certificado PKCS #12 y la contraseña contiene un signo de dólar ($), comillas (‘) o un carácter de escape (), la importación podría fallar. Si lo hace, aparecerá el mensaje ERROR: Contraseña no válida. Si debe usar un carácter especial en la contraseña, asegúrese de ponerle un prefijo con un carácter de escape () a menos que todas las importaciones se realicen mediante la CLI.

Convertir el formato de un certificado mediante la CLI

En el símbolo del sistema, escriba el siguiente comando:

```
convert ssl pkcs12 <outfile> [-import [-pkcs12File <inputFilename>] [-
    des | -des3] [-export [-certFile <inputFilename>] [-keyFile <
    inputFilename>]]
<!--NeedCopy-->
```

Durante la operación, se le pedirá que introduzca una contraseña de importación o una contraseña de exportación. Para un archivo cifrado, también se le pedirá que escriba una frase de contraseña.

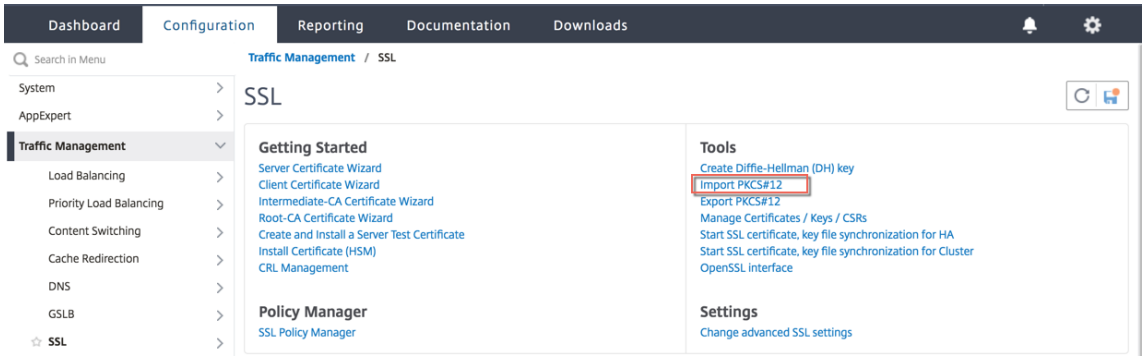
Ejemplo:

```
convert ssl pkcs12 Cert-Import-1.pem -import -pkcs12File Cert-Import-1.
    pfx -des

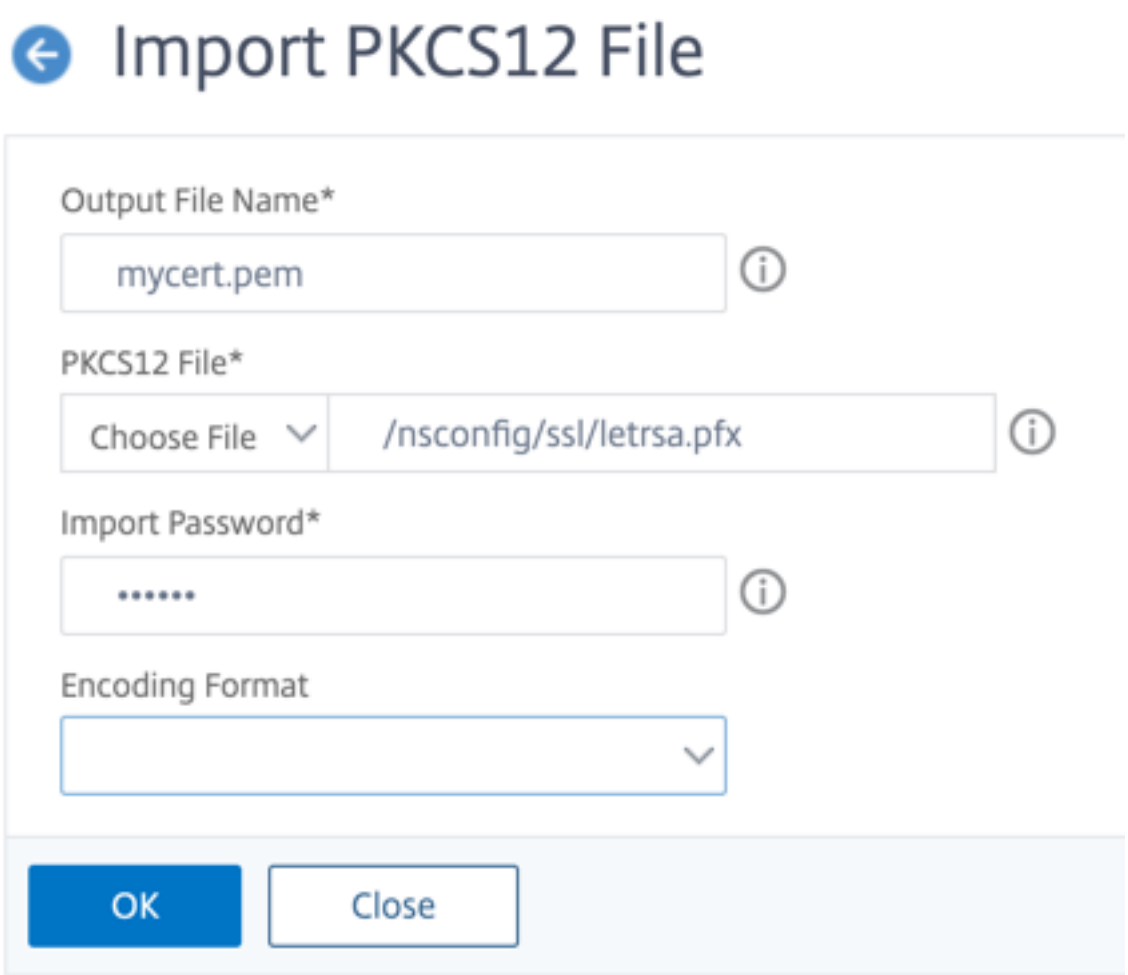
convert ssl pkcs12 Cert-Client-1.pfx -export -certFile Cert-Client-1 -
    keyFile Key-Client-1
<!--NeedCopy-->
```


Convertir el formato de un certificado mediante la interfaz gráfica de usuario

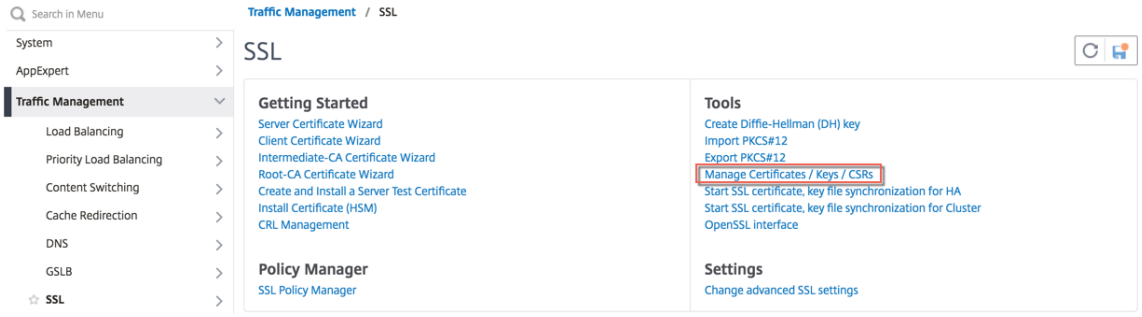
1. Vaya a **Administración de tráfico > SSL** y, en el grupo **Herramientas**, seleccione **Importar PKCS #12**.



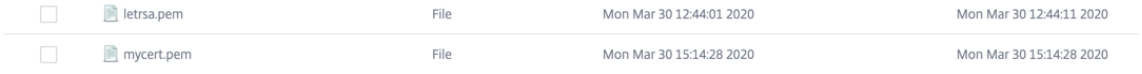
2. Especifique el nombre del certificado PEM en el campo **Nombre del archivo de salida**.
3. Busque la ubicación del certificado PFX en el equipo local o en el dispositivo.



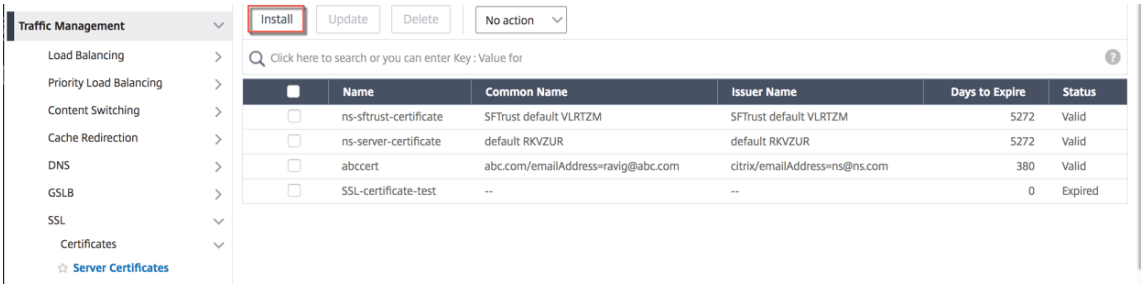
4. Haga clic en **Aceptar**.
5. Haga clic en **Administrar certificados, claves y CSR** para ver el archivo PEM convertido.



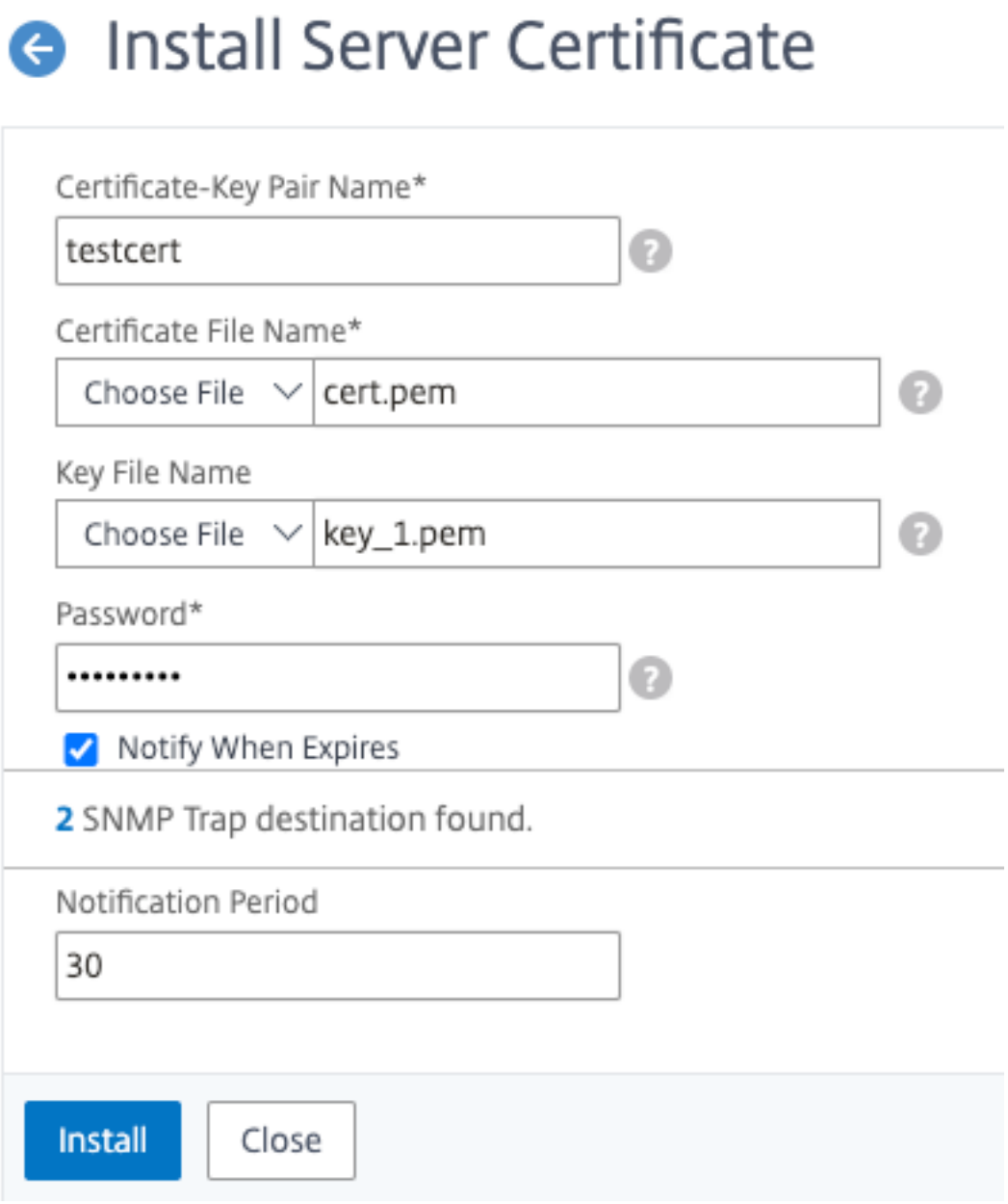
6. Puede ver el archivo PFX cargado y el archivo PEM convertido.



7. Vaya a **SSL** > **Certificados** > **Certificado sde servidor** y haga clic en **Instalar**.



8. Especifique un **nombre de par de claves de certificado**.
9. Vaya a la ubicación del archivo PEM.
10. Especifique la contraseña cuando se le solicite.
11. Haga clic en **Instalar**.



12. Enlazar el par de claves de certificado a un servidor virtual SSL.

Enlazar un certificado SSL a un servidor virtual del dispositivo Citrix ADC

October 5, 2021

Un certificado SSL es una parte esencial de los procesos de cifrado y descifrado SSL. El certificado se utiliza durante un enlace SSL para establecer la identidad del servidor SSL, que es el dispositivo Citrix ADC, ya que actúa como punto de terminación SSL para los clientes.

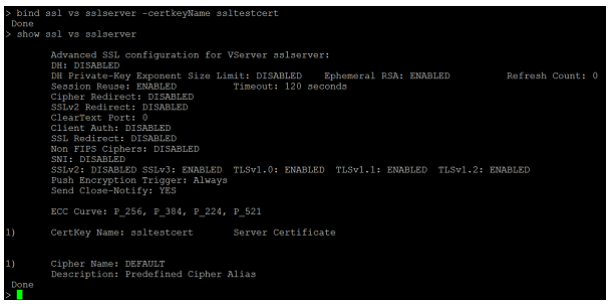
El certificado utilizado para procesar las transacciones SSL debe estar vinculado al servidor virtual (SSL) que recibe los datos SSL.

Para enlazar un certificado SSL a un servidor virtual SSL mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

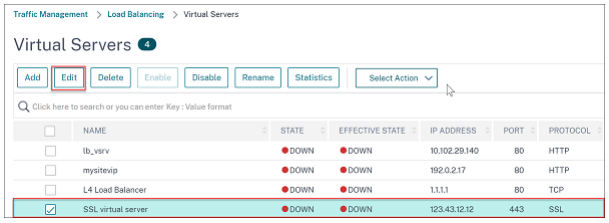
```
bind ssl vs <vServerName> -certkeyName <certificate-KeyPairName>
show ssl vs <vServerName>
<!--NeedCopy-->
```

Ejemplo:



Para enlazar un certificado SSL a un servidor virtual SSL mediante la interfaz gráfica de usuario

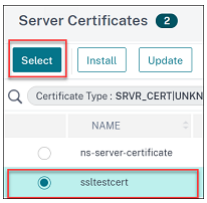
1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. Seleccione un servidor virtual de tipo SSL y haga clic en **Modificar**.



3. En la página **Servidor virtual de equilibrio de carga**, en la sección **Certificados**, haga clic en **Sin certificado de servidor**.

4. En la página **Vinculación de certificados de servidor**, haga clic **en Haga clic para seleccionar**.

5. Seleccione el certificado SSL y haga clic en **Seleccionar**.



6. Haga clic en **Vincular para enlazar** el certificado SSL al servidor virtual.
7. Haga clic en **Done**.

   Ha completado la vinculación del certificado SSL al servidor virtual.

Perfiles SSL

August 20, 2021

Un perfil SSL es una colección de configuraciones para entidades SSL. Ofrece facilidad de configuración y flexibilidad. En lugar de configurar los parámetros en cada entidad, puede configurarlos en un perfil y enlazar el perfil a todas las entidades a las que se aplica la configuración.

La infraestructura de perfil SSL se ha mejorado para utilizar los últimos cifrados y protocolos. Se resaltan las diferencias entre el perfil heredado (perfil antiguo) y el perfil SSL mejorado (perfil nuevo).

Diferencias entre la infraestructura de perfil SSL antigua y la nueva

Diferencias	Perfil antiguo	Nuevo perfil
Cifras y curvas ECC incluidas en el perfil	No	Sí
Insertar un cifrado o un grupo de cifrado en el medio de una lista existente	Desenlazar todos los cifrados y volver a enlazar en el orden de la prioridad requerida.	Agregue un cifrado y asígnele una prioridad. Si no se especifica una prioridad, se asigna al cifrado la prioridad más baja de la lista.

Diferencias	Perfil antiguo	Nuevo perfil
Desvincular todos los cifrados	`unbind ssl vserver \<name\> ciphername -ALL`	`unbind ssl profile -cipherName FlushAllCiphers` (La versión 11.0 compilación 64.x o posterior incluye el parámetro FlusHallCiphers para desvincular todos los cifrados o grupos de cifrado de un perfil, porque ALL se trata como un grupo de cifrado.)
Estado de SSLv3	n/d	Inhabilitado en el perfil front-end predeterminado (ns_default_ssl_profile_frontend). Nota: Antes de habilitar este perfil, SSLv3 está habilitado globalmente. Después de habilitar el perfil, SSLv3 se inhabilita en el perfil predeterminado de front-end.

SSL profile infrastructure

March 9, 2022

Las vulnerabilidades en la implementación de SSLv3 y RC4 han hecho hincapié en la necesidad de utilizar los cifrados y protocolos más recientes para negociar la configuración de seguridad de una conexión de red. La implementación de cualquier cambio en la configuración, como inhabilitar SSLv3 en miles de dispositivos de punto final SSL, es un proceso engorroso. Por lo tanto, los ajustes que formaban parte de la configuración de dispositivos de punto final SSL se han movido a los perfiles SSL, junto con los cifrados predeterminados. Para implementar cambios en la configuración, incluido el soporte de cifrado, solo necesita modificar el perfil que está enlazado a las entidades.

Los perfiles SSL front-end y back-end predeterminados contienen todos los cifrados y curvas ECC predeterminados, además de la configuración que formaba parte de los perfiles anteriores. En el apéndice se proporcionan resultados de muestra para los perfiles predeterminados. La operación Habilitar perfil predeterminado vincula automáticamente el perfil front-end predeterminado a todas

las entidades front-end y el perfil back-end predeterminado a todas las entidades back-end. Puede modificar un perfil predeterminado para adaptarlo a su implementación. También puede crear perfiles personalizados y vincularlos a entidades SSL.

El perfil front-end contiene parámetros aplicables a una entidad front-end. Es decir, se aplican a la entidad que recibe solicitudes de un cliente. Por lo general, esta entidad es un servidor virtual SSL o un servicio SSL transparente en el dispositivo Citrix ADC. El perfil back-end contiene parámetros aplicables a una entidad back-end. Es decir, se aplican a la entidad en el dispositivo ADC que envía solicitudes de clientes a un servidor back-end. Por lo general, esta entidad es un servicio SSL en el dispositivo Citrix ADC. Si intenta configurar un parámetro no compatible, aparece el error `ERROR: Specified parameters are not applicable for this type of SSL profile`.

> **Importante:**
>
> - Un perfil SSL tiene prioridad sobre los parámetros SSL. Es decir, si configura los parámetros SSL mediante el comando `set ssl parameter` y, posteriormente, vincula un perfil a una entidad SSL, la configuración del perfil tendrá prioridad.
> - Después de la actualización, si habilita los perfiles predeterminados, no podrá deshacer los cambios. Es decir, los perfiles no se pueden inhabilitar. Guarde la configuración y cree una copia del archivo de configuración (ns.conf) antes de habilitar los perfiles. Sin embargo, si no quiere utilizar las funciones del perfil predeterminado, puede seguir mediante los perfiles SSL antiguos. Para obtener más información sobre estos perfiles, consulte Perfil SSL heredado.
> - Desde la versión 11.1 51.x, en la GUI y la CLI, se agrega un mensaje de confirmación cuando habilita el perfil predeterminado para evitar que se habilite por error.

A partir de la versión 13.1 compilación 17.x, los protocolos inferiores a TLSv1.2 están inhabilitados en los servicios internos de SSL.

- Si el perfil predeterminado está habilitado, `ns_default_ssl_profile_internal_frontend_service` está enlazado a los servicios internos SSL y los protocolos SSLv3, TLSv1.0 y TLSv1.1 están inhabilitados en este perfil.
- Si el perfil predeterminado no está habilitado, los protocolos SSLv3, TLSv1.0 y TLSv1.1 se inhabilitan en los parámetros de servicios internos de SSL.

Comando:

```
set ssl parameter -defaultProfile ENABLED
    Save your configuration before enabling the Default profile. You
       cannot undo the changes. Are you sure you want to enable the
       Default profile? [Y/N]Y
Done
```



```
<!--NeedCopy-->
```

De forma predeterminada, algunos parámetros SSL, denominados *parámetros globales*, se aplican a todos los dispositivos de punto final SSL. Sin embargo, si un perfil está enlazado a un punto final SSL, los parámetros globales no se aplican. En su lugar, se aplica la configuración especificada en el perfil.

Puntos que tener en cuenta

1. Un perfil se puede vincular a varios servidores virtuales, pero un servidor virtual solo puede tener un perfil vinculado a él.
2. Para eliminar un perfil que está enlazado a un servidor virtual, primero desvincule el perfil.
3. Un grupo de cifrado o cifrado se puede vincular a varios perfiles con diferentes prioridades.
4. Un perfil puede tener varios cifrados y grupos de cifrado vinculados a diferentes prioridades.
5. Los cambios en un grupo de cifrado se reflejan inmediatamente en todos los perfiles y en todos los servidores virtuales a los que está vinculado uno de los perfiles.
6. Si un conjunto de cifrado forma parte de un grupo de cifrado, modifique el grupo de cifrado para eliminar ese conjunto de cifrado antes de eliminar el conjunto de cifrado del perfil.
7. Si no asigna una prioridad a un conjunto de cifrado o grupo de cifrado adjunto a un perfil, se le asigna la prioridad más baja dentro del perfil.
8. Puede crear un grupo de cifrado personalizado (también denominado grupo de cifrado definido por el usuario) a partir de grupos de cifrado y conjuntos de cifrado existentes. Si crea el grupo de cifrado A y le agrega los grupos de cifrado existentes X e Y, en ese orden, Y se asigna con una prioridad más baja que X. Es decir, el grupo que se agrega primero tiene una prioridad más alta.
9. Si un conjunto de cifrado forma parte de dos grupos de cifrado adjuntos al mismo perfil, el conjunto de cifrado no se agrega como parte del segundo grupo de cifrado. El conjunto de cifrado con la prioridad más alta está en vigor cuando se procesa el tráfico.
10. Los grupos de cifrado no se expanden en el perfil. Como resultado, el número de líneas en el archivo de configuración (ns.conf) se reduce considerablemente. Por ejemplo, si dos grupos de cifrado que contienen 15 cifrados cada uno están enlazados a mil servidores virtuales SSL, la expansión agrega 30*1000 entradas relacionadas con el cifrado en el archivo de configuración. Con el nuevo perfil, solo tendría dos entradas: una para cada grupo de cifrado vinculado a un perfil.
11. La creación de un grupo de cifrado definido por el usuario a partir de cifrados y grupos de cifrado existentes es una operación de copiar y pegar. Los cambios en el grupo original no se reflejan en el nuevo grupo.
12. Un grupo de cifrado definido por el usuario enumera todos los perfiles de los que forma parte.
13. Un perfil enumera todos los servidores virtuales SSL, los servicios y los grupos de servicios a los que está vinculado.
14. Si la función de perfil SSL predeterminada está habilitada, use el perfil para establecer o cambiar cualquiera de los atributos de una entidad SSL. Por ejemplo, un servidor virtual, un servicio, un

grupo de servicios o un servicio interno.

Guarde la configuración mediante la CLI

En el símbolo del sistema, escriba:

```
save config

shell

root@ns# cd /nsconfig

root@ns# cp ns.conf ns.conf.NS<currentreleasenumber><currentbuildnumber
   >
<!--NeedCopy-->
```

Ejemplo:

```
save config
shell
root@ns# cd /nsconfig
root@ns# cp ns.conf ns.conf.NS.11.0.jun.16
<!--NeedCopy-->
```

Habilitar el perfil predeterminado

> **Importante:**
>
> - Guarde la configuración antes de actualizar el software y habilite los perfiles predeterminados.
> - A partir de la versión 11.1 compilación 51.x, en la GUI y la CLI, aparece un mensaje de confirmación cuando habilita el perfil predeterminado para evitar habilitarlo por error.

Comando: El siguiente comando habilita el perfil predeterminado y lo vincula a las entidades SSL a las que ya está enlazado un perfil. Es decir, si un perfil (por ejemplo, P1) ya está enlazado a una entidad SSL, el perfil front-end predeterminado o el perfil back-end predeterminado reemplazan a P1. El perfil anterior (P1) no se elimina. Ahora es un perfil SSL mejorado y contiene la configuración anterior y los cifrados y las curvas ECC. Si no quiere el perfil predeterminado, puede vincular explícitamente P1 a la entidad SSL.


```
set ssl parameter -defaultProfile ENABLED
    Save your configuration before enabling the Default profile. You
       cannot undo the changes. Are you sure you want to enable the
       Default profile? [Y/N]Y
Done
<!--NeedCopy-->
```

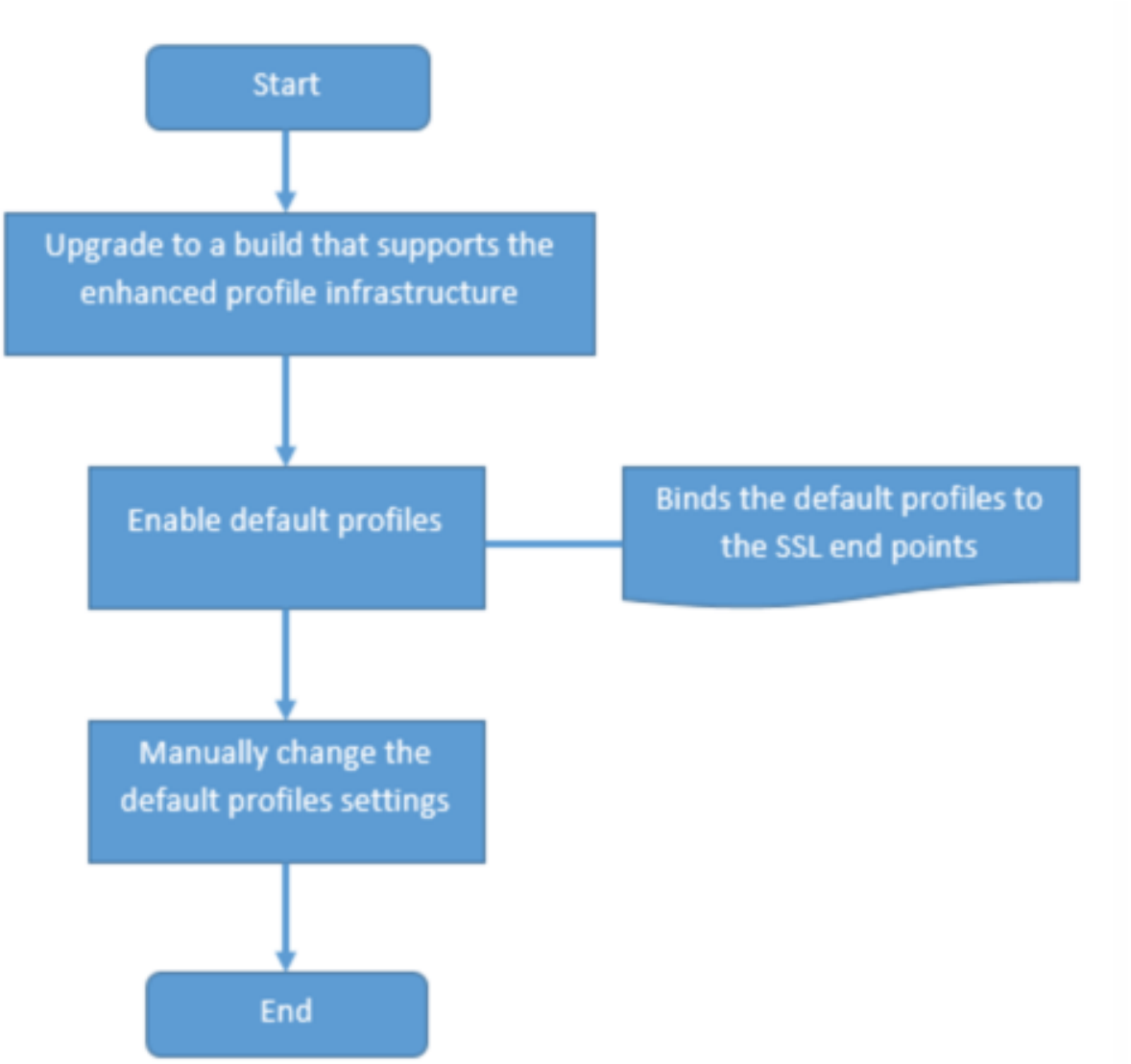
Actualice el software a una compilación que admita la infraestructura de perfiles mejorada y, a continuación, habilite los perfiles predeterminados.

> **Notas:**
>
> - Si un perfil heredado (P1) ya está enlazado a una entidad SSL y se habilita el perfil predeterminado, el perfil predeterminado anula el enlace anterior. Es decir, el perfil predeterminado está vinculado a las entidades SSL. Si no quiere que el perfil predeterminado esté enlazado, debe volver a vincular P1 a la entidad SSL.
> - Una sola operación (Habilitar perfil predeterminado o `set ssl parameter -defaultProfile ENABLED`) habilita (vincula) tanto el perfil front-end predeterminado como el perfil back-end predeterminado.

Caso de uso

Después de habilitar los perfiles predeterminados, se enlazan a todos los dispositivos de punto final SSL. Los perfiles predeterminados se pueden modificar. Si la implementación utiliza la mayoría de la configuración predeterminada y cambia solo unos pocos parámetros, puede modificar los perfiles predeterminados. Los cambios se reflejan inmediatamente en todos los dispositivos de punto final. También puede crear perfiles SSL personalizados con algunos parámetros personalizados y algunos predeterminados y vincularlos a las entidades SSL.

El siguiente diagrama de flujo explica los pasos que debe realizar:



1. Para obtener información sobre la actualización del software, consulte Actualización del software del sistema.
2. Habilite los perfiles predeterminados mediante la CLI o GUI.
   - En la línea de comandos, escriba: `set ssl parameter -defaultProfile ENABLED`
   - Si prefiere usar la GUI, vaya a **Administración del tráfico** > **SSL** > **Cambiar la configuración avanzada de SSL**, desplácese hacia abajo y seleccione **Habilitar perfil predeterminado**.

Si un perfil no estaba enlazado a un punto final antes de la actualización, un perfil predeterminado se enlazará al punto final SSL. Si un perfil estaba enlazado a un punto final antes de la actualización, el mismo perfil se enlaza después de la actualización y se agregan cifrados predeterminados al perfil.

1. (Opcional) Cambie manualmente cualquier configuración del perfil predeterminado.

- En la línea de comandos, escriba: `set ssl profile <name>` seguido de los parámetros que quiere modificar.
- Si prefiere usar la GUI, vaya a **Sistema** > **Perfiles**. En **Perfiles SSL**, seleccione un perfil y haga clic en **Modificar**.

Parámetros del perfil SSL

Puede establecer los siguientes parámetros SSL en un perfil SSL. Puede establecer algunos de estos parámetros en un servidor virtual SSL. Para obtener más información sobre los parámetros del servidor virtual SSL, consulte Parámetros de servidor virtual SSL.

Compatibilidad con renegociación segura en el back-end de un dispositivo Citrix ADC

Nota: Este parámetro se introdujo en la versión 13.0 compilación 58.x y posteriores. En versiones y compilaciones anteriores, solo se admitía la renegociación no segura en el back-end.

La función se admite en las siguientes plataformas:

- VPX
- Plataformas MPX que contienen chips N2 o N3
- Plataformas basadas en chips SSL Intel Coleto

La función aún no se admite en la plataforma FIPS.

La renegociación segura se deniega de forma predeterminada en el back-end de un dispositivo ADC. Es decir, el parámetro `denySSLReneg` se establece en ALL (predeterminado).

Para permitir la renegociación segura en el back-end, seleccione una de las siguientes configuraciones para el parámetro `denySSLReneg`:

- NO
- FRONTEND_CLIENT
- FRONTEND_CLIENTSERVER
- NO SEGURO

Habilite la renegociación segura mediante la CLI

En el símbolo del sistema, escriba:

```
set ssl profile <name> -denySSLReneg <denySSLReneg>
```

Ejemplo:


```
set ssl profile ns_default_ssl_profile_backend -denySSLReneg NONSECURE
 Done

sh ssl profile ns_default_ssl_profile_backend
1)  Name: ns_default_ssl_profile_backend    (Back-End)
    SSLv3: DISABLED TLSv1.0: ENABLED  TLSv1.1: ENABLED  TLSv1.2:
       ENABLED  TLSv1.3: DISABLED
    Server Auth: DISABLED
    Use only bound CA certificates: DISABLED
    Strict CA checks:       NO
    Session Reuse: ENABLED      Timeout: 300 seconds
    DH: DISABLED
    Ephemeral RSA: DISABLED
    Deny SSL Renegotiation      NONSECURE
    Non FIPS Ciphers: DISABLED
    Cipher Redirect: DISABLED
    SSL Redirect: DISABLED
    Send Close-Notify: YES
    Strict Sig-Digest Check: DISABLED
    Push Encryption Trigger: Always
    PUSH encryption trigger timeout:    1 ms
    SNI: DISABLED
    OCSP Stapling: DISABLED
    Strict Host Header check for SNI enabled SSL sessions:      NO
    Push flag:  0x0 (Auto)
    SSL quantum size:       8 kB
    Encryption trigger timeout  100 mS
    Encryption trigger packet count:    45

    ECC Curve: P_256, P_384, P_224, P_521

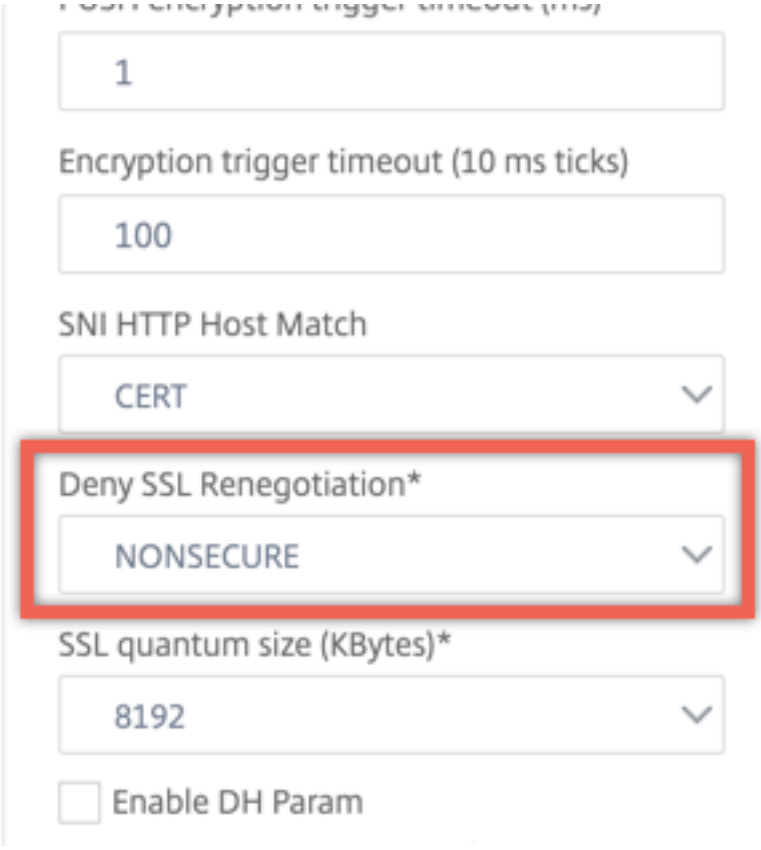
1)  Cipher Name: DEFAULT_BACKEND        Priority :2
    Description: Predefined Cipher Alias

1)  Service Name: s187
 Done
<!--NeedCopy-->
```

Habilite la renegociación segura mediante la interfaz gráfica de usuario

1. Vaya a **Sistema > Perfiles > Perfil SSL**.
2. Agregue o modifique un perfil.

3. Establezca **Denegar renegociación SSL** en cualquier valor que no sea ALL.



Validación de encabezados host

Nota: Este parámetro se introdujo en la versión 13.0 compilación 52.x.

Con HTTP/1.1, los clientes tenían que usar varias conexiones para procesar varias solicitudes. Con HTTP/2, los clientes pueden reutilizar las conexiones en los dominios que están cubiertos por el mismo certificado. Para una sesión habilitada para SNI, el dispositivo ADC debe poder controlar cómo se valida el encabezado de host HTTP para adaptarse a este cambio. En compilaciones anteriores, la solicitud se descartaba si el parámetro estaba habilitado (establecido en "Sí") y la solicitud no contenía el encabezado de host para una sesión habilitada para SNI. Si el parámetro estaba inhabilitado (establecido en "No"), el dispositivo no realizaba la validación. Se agrega un nuevo parámetro `SNIHTTPHostMatch` a un perfil SSL y a los parámetros globales SSL para tener un mejor control de esta validación. Este parámetro puede tomar tres valores: CERT, STRICT y NONE. Estos valores funcionan de la siguiente manera solo para las sesiones habilitadas para SNI. El SNI debe estar habilitado en el servidor virtual SSL o en el perfil enlazado al servidor virtual, y la solicitud HTTP debe contener el encabezado del host.

- CERT: la conexión se reenvía si el valor del encabezado del host en la solicitud está cubierto por el certificado utilizado para establecer esta sesión SSL.

- STRICT: la conexión se reenvía solo si el valor del encabezado del host en la solicitud coincide con el valor del nombre del servidor pasado en el mensaje Client Hello de la conexión SSL.
- NO: el valor del encabezado del host no se valida.

Valores posibles: NO, CERT, STRICT Valor
por defecto: CERT

Con la introducción del nuevo parámetro `SNIHTTPHostMatch`, se produce un cambio en el comportamiento del parámetro `dropReqWithNoHostHeader`. La configuración del parámetro `dropReqWithNoHostHeader` ya no afecta a la forma en que se valida el encabezado del host con respecto al certificado SNI.

Establecer los parámetros del perfil SSL mediante la CLI

En el símbolo del sistema, escriba:

```
set ssl profile <name> [-ssllogProfile <string>] [-dh ( ENABLED |
    DISABLED ) -dhFile <string>] [-dhCount <positive_integer>][-
    dhKeyExpSizeLimit ( ENABLED | DISABLED )] [-eRSA ( ENABLED |
    DISABLED) [-eRSACount <positive_integer>]] [-sessReuse ( ENABLED |
    DISABLED )
[-sessTimeout <positive_integer>]] [-cipherRedirect ( ENABLED |
    DISABLED ) [-cipherURL <URL>]] [-clientAuth ( ENABLED | DISABLED )[-
    clientCert ( Mandatory | Optional )]] [-sslRedirect ( ENABLED |
DISABLED )] [-redirectPortRewrite ( ENABLED | DISABLED )] [-ssl3 (
    ENABLED | DISABLED )] [-tls1 ( ENABLED | DISABLED )] [-tls11 (
    ENABLED| DISABLED )] [-tls12 ( ENABLED | DISABLED )] [-tls13 (
    ENABLED |DISABLED )] [-SNIEnable ( ENABLED | DISABLED )] [-
    ocspStapling (ENABLED | DISABLED )] [-serverAuth ( ENABLED |
    DISABLED )] [-commonName <string>] [-pushEncTrigger <pushEncTrigger
    >] [-sendCloseNotify ( YES |
NO )] [-clearTextPort <port|*>] [-insertionEncoding ( Unicode | UTF-8)]
     [-denySSLReneg <denySSLReneg>] [-quantumSize <quantumSize>]
[-strictCAChecks ( YES | NO )] [-encryptTriggerPktCount <
    positive_integer>] [-pushFlag <positive_integer>][-
    dropReqWithNoHostHeader ( YES | NO )] [-SNIHTTPHostMatch <
    SNIHTTPHostMatch>] [-pushEncTriggerTimeout <positive_integer>]
[-sslTriggerTimeout <positive_integer>] [-clientAuthUseBoundCAChain (
    ENABLED | DISABLED )] [-sslInterception ( ENABLED | DISABLED )][-
    ssliReneg ( ENABLED | DISABLED )] [-ssliOCSPCheck ( ENABLED |
    DISABLED )] [-ssliMaxSessPerServer <positive_integer>] [-HSTS (
    ENABLED| DISABLED )] [-maxage <positive_integer>] [-
    IncludeSubdomains ( YES | NO )] [-preload ( YES | NO )] [-
```

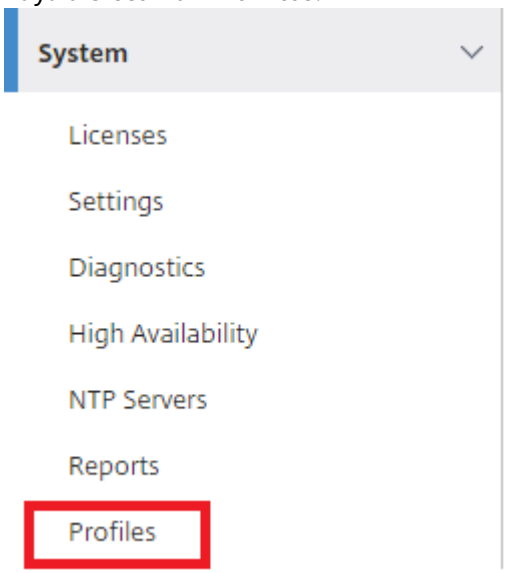


```
      sessionTicket ( ENABLED | DISABLED )][-sessionTicketLifeTime <
      positive_integer>] [-sessionTicketKeyRefresh (ENABLED | DISABLED )]
      {
 -sessionTicketKeyData  }
  [-sessionKeyLifeTime <positive_integer>] [-prevSessionKeyLifeTime <
     positive_integer>]
[-cipherName <string> -cipherPriority <positive_integer>][-
   strictSigDigestCheck ( ENABLED | DISABLED )]
[-skipClientCertPolicyCheck ( ENABLED | DISABLED )] [-zeroRttEarlyData
   ( ENABLED | DISABLED )] [-tls13SessionTicketsPerAuthContext
<positive_integer>] [-dheKeyExchangeWithPsk ( YES | NO )]
<!--NeedCopy-->
```

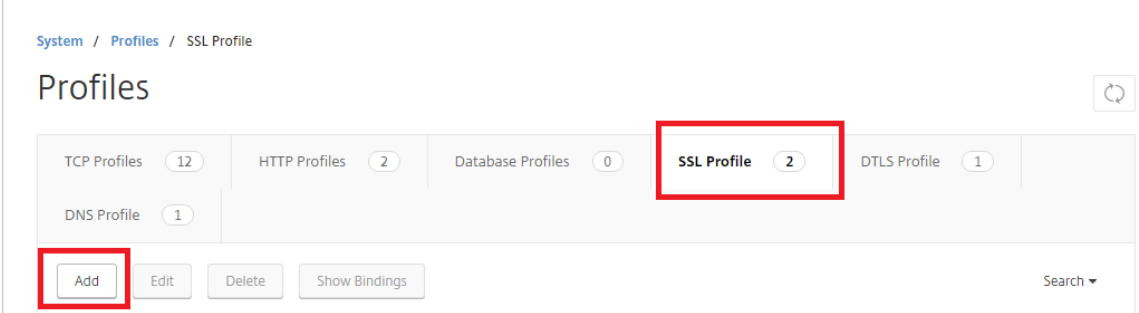
Establecer los parámetros del perfil SSL mediante la interfaz gráfica de usuario

Para agregar un perfil:

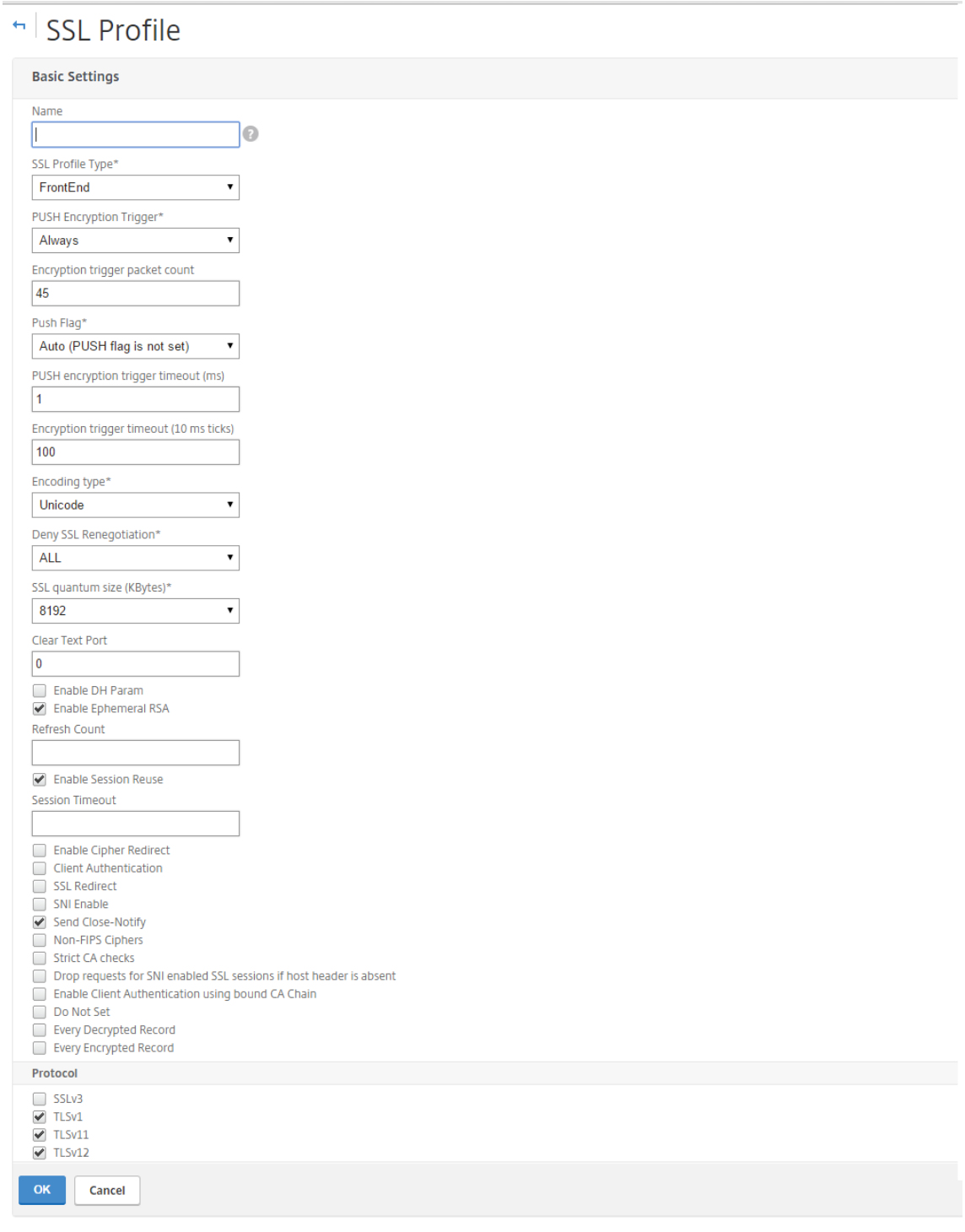
1. Vaya a **Sistema > Perfiles**.



2. Seleccione **Perfiles SSL**. Haga clic en **Agregar**.



3. Especifique los valores de los distintos parámetros.



4. Haga clic en **Aceptar**.
5. Haga clic en **Listo**.

Para reutilizar un perfil SSL existente:

1. Vaya a **Sistema > Perfiles**.

2. Seleccione un perfil existente y haga clic en **Agregar**.
3. Especifique un nombre diferente, cambie los parámetros y haga clic en **Aceptar**.
4. Haga clic en **Listo**.

Extensión de ticket de sesión de TLS

Un protocolo de enlace SSL es una operación que hace un uso intensivo de la CPU. Si la reutilización de sesiones está habilitada, la operación de intercambio de claves de servidor/cliente se omite para los clientes existentes. Se les permite reanudar sus sesiones. Esta acción mejora el tiempo de respuesta y aumenta la cantidad de transacciones SSL por segundo que puede admitir un servidor. Sin embargo, el servidor debe almacenar detalles de cada estado de sesión, lo que consume memoria y es difícil de compartir entre varios servidores si las solicitudes se equilibran en carga entre los servidores.

Los dispositivos Citrix ADC admiten la extensión sessionTicket TLS. El uso de esta extensión indica que los detalles de la sesión se almacenan en el cliente en lugar de en el servidor. El cliente debe indicar que admite este mecanismo mediante la inclusión de la extensión TLS del ticket de sesión en el mensaje Hello del cliente. Para los clientes nuevos, esta extensión está vacía. El servidor envía un nuevo tíquet de sesión en el mensaje de enlace NewsessionTicket. El vale de sesión se cifra mediante un par de claves que solo conoce el servidor. Si un servidor no puede emitir un nuevo ticket ahora, completa un apretón de manos normal.

Esta función solo está disponible en perfiles SSL front-end y solo en la parte frontal de la comunicación en la que el dispositivo actúa como servidor y genera tickets de sesión.

Limitaciones

- Esta función no se admite en una plataforma FIPS.
- Esta función solo se admite con las versiones 1.1 y 1.2 de TLS.
- La persistencia del identificador de sesión SSL no se admite con los tickets de sesión.

Habilitar la extensión de ticket de sesión TLS mediante la CLI

En el símbolo del sistema, escriba:

```
set ssl profile <name> -sessionTicket (ENABLED | DISABLED ) [-
    sessionTicketLifeTime <positive_integer>
<!--NeedCopy-->
```

Argumentos:

sessionTicket: Estado de extensión de tíquet de sesión TLS. El uso de esta extensión indica que los detalles de la sesión se almacenan en el cliente en lugar de en el servidor, como se define en RFC 5077.

Valores posibles: ENABLED, DISABLED

Valor por defecto: DISABLED

sessionTicketLifetime: Especifique una hora, en segundos, después de la cual caduca el tíquet de sesión y se debe iniciar un nuevo protocolo de enlace SSL.

Valor por defecto: 300

Valor mínimo: 0

Valor máximo: 172800

Ejemplo:

```
1 add ssl profile profile1 -sessionTicket ENABLED -sessionTicketlifeTime
     300
2 Done
3 <!--NeedCopy-->
```

Habilitar la extensión de ticket de sesión TLS mediante la GUI

1. Vaya a **Sistema** > **Perfiles**. Seleccione **Perfiles SSL**.
2. Haga clic en **Agregar** y especifique un nombre para el perfil.
3. Seleccione **Ticket de sesión**.
4. Si lo quiere, especifique **Duración del ticket de sesión (segundos)**.

Implementación segura de tickets de sesión

Mediante el uso de tickets de sesión TLS, los clientes pueden usar apretones de manos abreviados para una reconexión más rápida a los servidores. Sin embargo, si los tickets de sesión no se cifran o cambian durante largos períodos de tiempo, pueden suponer un riesgo para la seguridad. Puede proteger los tickets de sesión cifrándolos con una clave simétrica. Para lograr la confidencialidad directa, puede especificar un intervalo de tiempo en el que se actualiza la clave del ticket de sesión.

El dispositivo genera las claves de ticket de sesión de forma predeterminada. Sin embargo, si varios dispositivos de una implementación necesitan descifrar los tickets de sesión de los demás, todos deben usar la misma clave de ticket de sesión. Por lo tanto, debe establecer (agregar o cargar) los mismos datos de clave de ticket de sesión manualmente en todos los dispositivos. Los datos clave del ticket de sesión incluyen la siguiente información:

- Nombre del ticket de sesión.
- Clave AES de sesión utilizada para cifrar o descifrar el vale.
- Clave HMAC de sesión utilizada para calcular el resumen del ticket.

Ahora puede configurar datos de clave de ticket de sesión de 64 bytes de longitud para admitir claves HMAC de 256 bits, como se recomienda en RFC 5077. También se admiten longitudes de clave de 48 bytes para compatibilidad con versiones anteriores.

> **Nota:**
>
> Al escribir los datos clave del ticket de sesión manualmente, asegúrese de que la configuración en todos los dispositivos Citrix ADC en una configuración de alta disponibilidad o en una configuración de clúster sea la misma.

El parámetro `sessionTicketKeyLifeTime` especifica la frecuencia con la que se actualiza una clave de ticket de sesión. Puede configurar el parámetro `prevSessionTicketKeyLifeTime` para especificar cuánto tiempo se mantendrá la clave de ticket de sesión anterior para descifrar los tickets que usen esa clave, después de que se genere una nueva clave. El parámetro `prevSessionTicketKeyLifeTime` extiende el tiempo durante el cual un cliente puede usar un desafío mutuo abreviado para volver a conectarse. Por ejemplo, si `sessionTicketKeyLifeTime` se establece en 10 minutos y `prevSessionTicketKeyLifeTime` en 5 minutos, se genera una nueva clave después de 10 minutos y se usa para todas las sesiones nuevas. Sin embargo, los clientes conectados anteriormente tienen otros 5 minutos para los que se aceptan boletos emitidos anteriormente por un apretón de manos abreviado.

Configurar los datos del ticket de sesión SSL mediante la CLI

En el símbolo del sistema, escriba:

```
set ssl profile <name> -sessionTicket ENABLED -sessionTicketLifeTime <
    positive_integer> -sessionTicketKeyRefresh ( ENABLED | DISABLED )] -
    sessionTicketKeyLifeTime <positive_integer> [-
    prevSessionTicketKeyLifeTime <positive_integer>]
<!--NeedCopy-->
```

Argumentos:

sessionTicket: Utilice los tíquets de sesión como se describe en RFC 5077. Establecer el apretón de manos inicial requiere operaciones de cifrado de clave pública intensivas en la CPU. Con la configuración **ENABLED**, un servidor emite un vale de sesión a un cliente, que el cliente puede usar para realizar un apretón de manos abreviado.

Valores posibles: ENABLED, DISABLED. Predeterminado: INHABILITADO

sessionTicketLifetime: Vida útil, en segundos, del tíquet de sesión. Una vez transcurrido este tiempo, los clientes no pueden usar este ticket para reanudar sus sesiones.

Valor máximo: 172800. Valor mínimo: 0. Predeterminado: 300.

sessionTicketKeyRefresh: Cuando el tiempo especificado por el parámetro de duración de la clave de tíquet de sesión caduca, vuelva a generar la clave de tíquet de sesión utilizada para cifrar o descifrar los tíquets de sesión. Activado automáticamente si sessionTicket está habilitado. Se inhabilita si un administrador ingresa los datos del ticket de sesión.

Valores posibles: ENABLED, DISABLED. Predeterminado: HABILITADO

SessionKeyLifetime: Duración, en segundos, de una clave simétrica utilizada para cifrar los tickets de sesión emitidos por un dispositivo Citrix ADC.

Valor máximo: 86400. Valor mínimo: 600. Predeterminado: 3000

prevSessionKeyLifetime: El tiempo, en segundos, durante el cual la clave simétrica anterior utilizada para cifrar los tickets de sesión sigue siendo válida para los clientes existentes después de que caduque la vida útil de la clave de ticket de sesión. Dentro de este tiempo, los clientes existentes pueden reanudar sus sesiones utilizando la clave de ticket de sesión anterior. Los tickets de sesión para los nuevos clientes se cifran con la nueva clave.

Valor máximo: 172800. Valor mínimo: 0. Predeterminado: 0

Ejemplo:

```
set ssl profile ns_default_ssl_profile_frontend -sessionTicket ENABLED
   -sessionTicketlifeTime 120 -sessionTicketKeyRefresh ENABLED -
   sessionTicketKeyLifeTime 100 -prevSessionTicketKeyLifeTime 60

Done

show ssl profile ns_default_ssl_profile_frontend

    Session Ticket: ENABLED
    Session Ticket Lifetime: 120 (secs)
    Session Key Auto Refresh: ENABLED
    Session Key Lifetime: 100 (secs)
    Previous Session Key Lifetime: 60 (secs)
<!--NeedCopy-->
```

Configurar los datos del ticket de sesión SSL mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **Perfiles**y seleccione **Perfil SSL**.
2. Seleccione **ns_default_ssl_profile_frontend** y haga clic en **Modificar**.
3. En la sección **Parámetros básicos**, haga clic en el icono del lápiz y configure estos parámetros:
   - Boleto de sesión

- Duración del ticket de sesión (segundos)
- Actualización automática de clave de ticket de sesión
- Duración de la clave del ticket de sesión (segundos)
- Duración de la clave del ticket de sesión anterior (segundos)

4. Haga clic en **Aceptar**.

Escriba los datos del vale de sesión SSL manualmente mediante la CLI

En el símbolo del sistema, escriba:

```
set ssl profile <name> -sessionTicket ENABLED

set ssl profile <name> -sessionTicketKeyData

show ssl profile ns_default_ssl_profile_frontend
<!--NeedCopy-->
```

Argumentos:

sessionTicket: Uso de tíquets de sesión según lo descrito por RFC 5077. Establecer el apretón de manos inicial requiere operaciones de cifrado de clave pública intensivas en la CPU. Con la configuración **ENABLED**, un servidor emite un vale de sesión a un cliente, que el cliente puede usar para realizar un apretón de manos abreviado.

Valores posibles: ENABLED, DISABLED. Predeterminado: INHABILITADO

sessionTicketKeyData: Contains the session ticket name (0-15 bytes), the session AES key used to encrypt or decrypt the session ticket (16-31 bytes), and the session HMAC key used to compute the digest of the ticket (32-63 bytes). Externally generated by an administrator and added to a Citrix ADC appliance.

Longitud máxima: 64 bytes

Ejemplo:

```
set ssl profile ns_default_ssl_profile_frontend -sessionTicket ENABLED

Done

set ssl profile ns_default_ssl_profile_frontend -sessionTicketKeyData
    11111111111111111111111111111111111111111111111111
```



```
6
7  Done
8
9  show ssl profile ns_default_ssl_profile_frontend
10
11     1) Name: ns_default_ssl_profile_frontend (Front-End)
12     SSLv3: ENABLED TLSv1.0: ENABLED TLSv1.1: ENABLED TLSv1.2: ENABLED
13     Client Auth: DISABLED
14     Use only bound CA certificates: DISABLED
15     Strict CA checks: NO
16     Session Reuse: ENABLED Timeout: 120 seconds
17     DH: DISABLED
18     DH Private-Key Exponent Size Limit: DISABLED Ephemeral RSA: ENABLED
           Refresh Count: 0
19     Deny SSL Renegotiation ALL
20     Non FIPS Ciphers: DISABLED
21     Cipher Redirect: DISABLED
22     SSL Redirect: DISABLED
23     Send Close-Notify: YES
24     Push Encryption Trigger: Always
25     PUSH encryption trigger timeout: 1 ms
26     SNI: DISABLED
27     OCSP Stapling: DISABLED
28     Strict Host Header check for SNI enabled SSL sessions: NO
29     Push flag: 0x0 (Auto)
30     SSL quantum size: 8 kB
31     Encryption trigger timeout 100 mS
32     Encryption trigger packet count: 45
33     Subject/Issuer Name Insertion Format: Unicode
34     Session Ticket: ENABLED
35     Session Ticket Lifetime: 300 (secs)
36     Session Key Auto Refresh: DISABLED
37     Session Key Lifetime: 3000 (secs)
38     Previous Session Key Lifetime: 0 (secs)
39     Session Key Data: 84
          dad1afc6d56b0deeb0a7fd7f299a207e8d8c15cdd087a5684a11a329fd732e87a0535d9088
40     47
          e8c181ba266f5c8838ae472cb3ab9255b683bf922fad32cee816c329989ef7cdeb278e93ac
41
42     ECC Curve: P_256, P_384, P_224, P_521
43
44     1) Cipher Name: DEFAULT Priority :4
45     Description: Predefined Cipher Alias
```



```
46
47      1) Internal Service Name (Front-End): nsrnatsip-127.0.0.1-5061
48      2) Internal Service Name (Front-End): nskrpcs-127.0.0.1-3009
49      3) Internal Service Name (Front-End): nshttps-::1l-443
50      4) Internal Service Name (Front-End): nsrpcs-::1l-3008
51      5) Internal Service Name (Front-End): nshttps-127.0.0.1-443
52      6) Internal Service Name (Front-End): nsrpcs-127.0.0.1-3008
53      7) Vserver Name: v1
54
55  Done
56  <!--NeedCopy-->
```

Escriba los datos del vale de sesión SSL manualmente mediante la interfaz gráfica de usuario

1. Vaya a **Sistema > Perfiles**y seleccione **Perfil SSL**.
2. Seleccione **ns_default_ssl_profile_frontend** y haga clic en **Modificar**.
3. En la sección **Parámetros básicos**, haga clic en el icono del lápiz y configure estos parámetros:
   - Boleto de sesión
   - Datos clave del ticket de sesión
   - Confirmar datos clave del ticket de sesión
4. Haga clic en **Aceptar**.

Compatibilidad con Secreto maestro extendido en el protocolo de enlace SSL en plataformas Citrix ADC no FIPS

Nota: Este parámetro se introdujo en la versión 13.0 compilación 61.x.

Secreto maestro extendido (EMS) es una extensión opcional del protocolo de seguridad de la capa de transporte (TLS). Se agrega un nuevo parámetro que se aplica a los perfiles SSL front-end y back-end para admitir EMS en el dispositivo Citrix ADC. Si el parámetro está habilitado y el par admite EMS, el dispositivo ADC utiliza el cálculo de EMS. Si el par no admite EMS, el cálculo de EMS no se utiliza para la conexión aunque el parámetro esté habilitado en el dispositivo. Para obtener más información sobre EMS, consulte RFC 7627.

Nota: EMS solo se aplica a los apretones de manos que utilizan el protocolo TLS versión 1.0, 1.1 o 1.2.

Soporte de plataforma para EMS

- Plataformas MPX y SDX que contienen chips Cavium N3 o tarjetas criptográficas Intel Coleto Creek. Las siguientes plataformas se entregan con chips Intel Coleto:

- MPX 5900
- MPX/SDX 8900
- MPX/SDX 26000
- MPX/SDX 26000-50
- MPS/SDX 26000-100 G
- MPX/SDX 15000-50G

También puede utilizar el comando `show hardware` para identificar si su dispositivo tiene chips Coleto (COL) o N3.

- Plataformas MPX y SDX sin tarjetas criptográficas (solo software).
- Plataformas solo de software: VPX, CPX y BLX.

EMS no se puede habilitar en las siguientes plataformas:

- Plataformas FIPS MPX 9700 y FIPS MPX 14000.
- Plataformas MPX y SDX que contienen chips criptográficos Cavium N2.

Si el parámetro está habilitado, el dispositivo ADC intenta usar EMS en conexiones TLS 1.2, TLS 1.1 y TLS 1.0. La configuración no afecta a las conexiones TLS 1.3 o SSLv3.

Para permitir que EMS se negocie con el par, habilite la configuración en el perfil SSL vinculado al servidor virtual (front-end) o al servicio (back-end).

Habilitar EMS mediante la CLI

En el símbolo del sistema, escriba:

```
set ssl profile <profile name> [-allowExtendedMasterSecret (YES | NO)]
```

Ejemplos

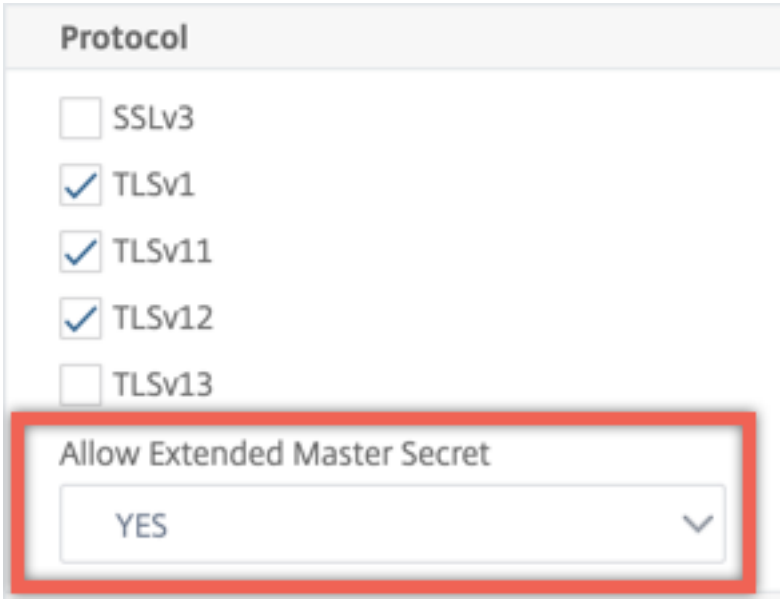
```
1 set ssl profile ns_default_ssl_profile_frontend  -
     allowExtendedMasterSecret YES
2
3 set ssl profile ns_default_ssl_profile_backend  -
     allowExtendedMasterSecret YES
4 <!--NeedCopy-->
```

En la siguiente tabla se muestra el valor predeterminado del parámetro `allowExtendedMasterSecret` en diferentes perfiles predeterminados y definidos por el usuario.

Perfil	Configuración predeterminada
Perfil front-end predeterminado	NO
Perfil seguro front-end predeterminado	SÍ
Perfil back-end predeterminado	NO
Perfil definido por el usuario	NO

Habilitar EMS mediante la GUI

1. Vaya a **Sistema > Perfiles > Perfil SSL**.
2. Agregue un perfil o modifique un perfil.
3. Establezca **Permitir secreto maestro extendido** en SÍ.



Soporte para el procesamiento de la extensión ALPN en el mensaje de saludo del cliente

Nota: Esta función se admite en la versión 13.0 compilación 61.x y posteriores.

Se agrega un parámetro `alpnProtocol` a los perfiles SSL front-end para negociar el protocolo de aplicación en la extensión ALPN para las conexiones gestionadas por el servidor virtual SSL_TCP. Solo se negocia el protocolo especificado en el perfil SSL, si se recibe el mismo protocolo en la extensión ALPN del mensaje de saludo del cliente.

Nota: El parámetro `alpnProtocol` solo se admite en perfiles SSL front-end y se aplica a las conexiones SSL administradas por servidores virtuales de tipo SSL_TCP.

Establecer el protocolo en el perfil SSL front-end mediante la CLI

En el símbolo del sistema, escriba:

```
set ssl profile ns_default_ssl_profile_frontend -alpnProtocol <protocol_name
>
```

El parámetro `alpnProtocol` puede tener tres valores. Longitud máxima: 4096 bytes.

- **NINGUNO:** La negociación del protocolo de aplicación no se lleva a cabo. Este es el valor predeterminado.
- **HTTP1:** HTTP1 se puede negociar como protocolo de aplicación.
- **HTTP2:** HTTP2 se puede negociar como protocolo de aplicación.

Ejemplo:

```
set ssl profile ns_default_ssl_profile_frontend -ALPNProtocol HTTP2
> sh ssl profile ns_default_ssl_profile_frontend
1)  Name: ns_default_ssl_profile_frontend   (Front-End)
    SSLv3: DISABLED TLSv1.0: ENABLED  TLSv1.1: ENABLED  TLSv1.2:
       ENABLED  TLSv1.3: DISABLED
    Client Auth: DISABLED
    Use only bound CA certificates: DISABLED
    Strict CA checks:   NO
    Session Reuse: ENABLED  Timeout: 120 seconds
    DH: DISABLED
    DH Private-Key Exponent Size Limit: DISABLED    Ephemeral RSA:
       ENABLED  Refresh Count: 0
    Deny SSL Renegotiation  ALL
    Non FIPS Ciphers: DISABLED
    Cipher Redirect: DISABLED
    SSL Redirect: DISABLED
    Send Close-Notify: YES
    Strict Sig-Digest Check: DISABLED
    Zero RTT Early Data: DISABLED
    DHE Key Exchange With PSK: NO
    Tickets Per Authentication Context: 1
    Push Encryption Trigger: Always
    PUSH encryption trigger timeout:    1 ms
    SNI: DISABLED
    OCSP Stapling: DISABLED
    Strict Host Header check for SNI enabled SSL sessions:  NO
    Match HTTP Host header with SNI:    CERT
    Push flag:  0x0 (Auto)
    SSL quantum size:   8 kB
```



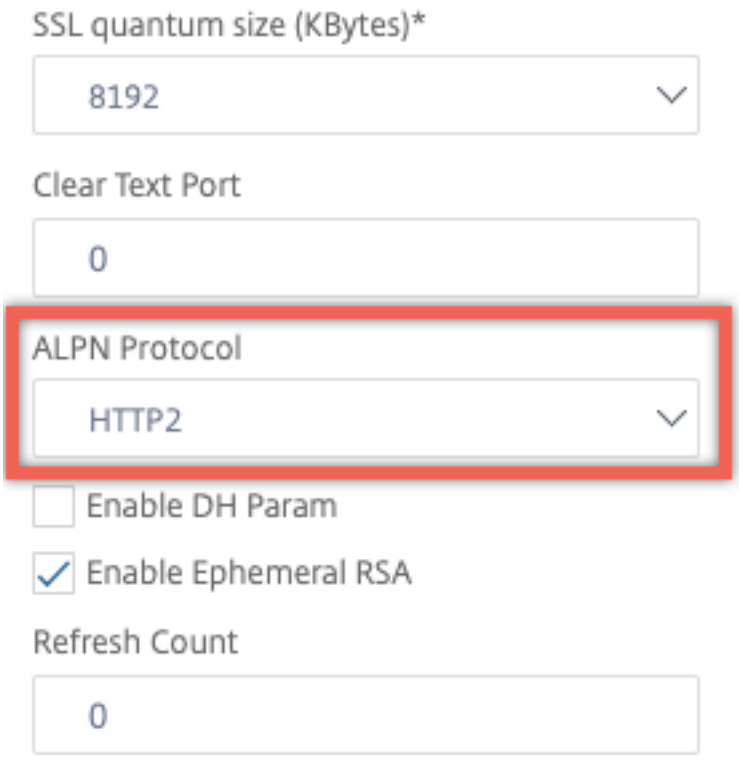
```
    Encryption trigger timeout  100 mS
    Encryption trigger packet count:    45
    Subject/Issuer Name Insertion Format:   Unicode

    SSL Interception: DISABLED
    SSL Interception OCSP Check: ENABLED
    SSL Interception End to End Renegotiation: ENABLED
    SSL Interception Maximum Reuse Sessions per Server: 10
    Session Ticket: DISABLED
    HSTS: DISABLED
    HSTS IncludeSubDomains: NO
    HSTS Max-Age: 0
    HSTS Preload: NO
    Allow Extended Master Secret: NO
    Send ALPN Protocol: HTTP2

 Done
 <!--NeedCopy-->
```

Establecer el protocolo en el perfil SSL front-end mediante la interfaz gráfica de usuario

1. Vaya a **Sistema > Perfiles**y seleccione **Perfil SSL**.
2. Seleccione **ns_default_ssl_profile_frontend** y haga clic en **Modificar**.
3. En la lista **Protocolo ALPN**, seleccione **HTTP2**.



Cargue una configuración antigua

La activación de los perfiles predeterminados no es reversible. Sin embargo, si decide que su implementación no requiere los perfiles predeterminados, puede cargar una configuración anterior que guardó antes de habilitar los perfiles predeterminados. Los cambios surtirán efecto después de reiniciar el dispositivo.

Cargar una configuración antigua mediante la CLI

En el símbolo del sistema, escriba:

```
shell

root@ns# clear config

root@ns# cd /nsconfig

root@ns# cp ns.conf.NS.11.0.jun.16 ns.conf

root@ns# reboot
<!--NeedCopy-->
```


Perfil de front-end seguro

February 16, 2021

Además de un perfil front-end predeterminado y un perfil back-end predeterminado, hay disponible un nuevo perfil front-end seguro predeterminado a partir de la versión 12.1. Los ajustes necesarios para una calificación A+ (a partir de mayo de 2018) de Qualys SSL Labs están precargados en este perfil. Anteriormente, tenía que establecer explícitamente cada uno de los parámetros necesarios para una calificación A+ en un perfil front-end SSL o en un servidor virtual SSL. Ahora puede enlazar el perfil ns_default_ssl_profile_secure_frontend a su servidor virtual SSL y los parámetros requeridos se establecen automáticamente en su servidor virtual SSL.

> **Nota:**
>
> El perfil front-end seguro no se puede modificar.

Cuando habilita el perfil predeterminado, el perfil front-end predeterminado se vincula automáticamente a todos los servidores virtuales SSL. Para obtener una calificación A+, debe vincular explícitamente el perfil ns_default_ssl_profile_secure_frontend y también vincular un certificado de servidor SHA2/SHA256 a su servidor virtual SSL.

Parámetros de perfil front-end seguros

Los parámetros con su configuración predeterminada se enumeran aquí:

```
SSLv3: DISABLED  TLSv1.0: DISABLED  TLSv1.1: DISABLED  TLSv1.2: ENABLED
     TLSv1.3: DISABLED

Deny SSL Renegotiation: NONSECURE

HSTS: ENABLED

HSTS IncludeSubDomains: YES

HSTS Max-Age: 15552000

Cipher Name: SECURE    Priority :1
<!--NeedCopy-->
```


Alias de cifrado seguro

Se agrega un nuevo alias de cifrado seguro que se vincula al perfil de front-end seguro. Para enumerar los cifrados que forman parte de este alias, escriba en el símbolo del sistema: Show cipher SECURE

```
show cipher SECURE

    1) Cipher Name: TLS1.2-ECDHE-RSA-AES256-GCM-SHA384 Priority : 1
           Description: TLSv1.2 Kx=ECC-DHE  Au=RSA  Enc=AES-GCM(256)
              Mac=AEAD   HexCode=0xc030
    2) Cipher Name: TLS1.2-ECDHE-RSA-AES128-GCM-SHA256 Priority : 2
           Description: TLSv1.2 Kx=ECC-DHE  Au=RSA  Enc=AES-GCM(128)
              Mac=AEAD   HexCode=0xc02f
    3) Cipher Name: TLS1.2-ECDHE-ECDSA-AES256-GCM-SHA384
       Priority : 3
           Description: TLSv1.2 Kx=ECC-DHE  Au=ECDSA Enc=AES-GCM(256)
              Mac=AEAD   HexCode=0xc02c
    4) Cipher Name: TLS1.2-ECDHE-ECDSA-AES128-GCM-SHA256
       Priority : 4
           Description: TLSv1.2 Kx=ECC-DHE  Au=ECDSA Enc=AES-GCM(128)
              Mac=AEAD   HexCode=0xc02b
Done
<!--NeedCopy-->
```

Configuración

Siga estos pasos:

1. Agregue un servidor virtual de equilibrio de carga de tipo SSL.
2. Enlazar un certificado SHA2/SHA256.
3. Habilite el perfil predeterminado.
4. Enlazar el perfil front-end seguro al servidor virtual SSL.

Obtenga una calificación A+ para un servidor virtual SSL mediante la CLI

En el símbolo del sistema, escriba:

```
add lb vserver <name> <serviceType> <IPAddress> <port>
bind ssl vserver <vServerName> -certkeyName <string>
set ssl parameter -defaultProfile ENABLED
```



```
set ssl vserver <vServerName> -sslProfile
   ns_default_ssl_profile_secure_frontend
show ssl vserver [<vServerName>]
<!--NeedCopy-->
```

Ejemplo:

```
add lb vserver ssl-vsvr SSL 192.0.2.240 443

bind ssl vserver ssl-vsvr -certkeyName letrsa

set ssl parameter -defaultProfile ENABLED

Save your configuration before enabling the Default profile. You cannot
    undo the changes. Are you sure you want to enable the Default
   profile? [Y/N]y

set ssl vserver ssl-vsvr -sslProfile
   ns_default_ssl_profile_secure_frontend
<!--NeedCopy-->
```

```
sh ssl vserver ssl-vsvr

    Advanced SSL configuration for VServer ssl-vsvr:
    Profile Name :ns_default_ssl_profile_secure_frontend
    1) CertKey Name: letrsa     Server Certificate
Done
<!--NeedCopy-->
```

```
sh ssl profile ns_default_ssl_profile_secure_frontend

    1) Name: ns_default_ssl_profile_secure_frontend (Front-End)
    SSLv3: DISABLED  TLSv1.0: DISABLED  TLSv1.1: DISABLED  TLSv1.2:
       ENABLED  TLSv1.3: DISABLED
    Client Auth: DISABLED
    Use only bound CA certificates: DISABLED
    Strict CA checks:                  NO
    Session Reuse: ENABLED   Timeout: 120 seconds
    DH: DISABLED
```



```
10      DH Private-Key Exponent Size Limit: DISABLED    Ephemeral RSA:
           ENABLED     Refresh Count: 0
11      Deny SSL Renegotiation                NONSECURE
12      Non FIPS Ciphers: DISABLED
13      Cipher Redirect: DISABLED
14      SSL Redirect: DISABLED
15      Send Close-Notify: YES
16      Strict Sig-Digest Check: DISABLED
17      Zero RTT Early Data: DISABLED
18      DHE Key Exchange With PSK: NO
19      Tickets Per Authentication Context: 1
20      Push Encryption Trigger: Always
21      PUSH encryption trigger timeout:  1 ms
22      SNI: DISABLED
23      OCSP Stapling: DISABLED
24      Strict Host Header check for SNI enabled SSL sessions:
                              NO
25      Push flag:             0x0 (Auto)
26      SSL quantum size:                8 kB
27      Encryption trigger timeout       100 mS
28      Encryption trigger packet count: 45
29      Subject/Issuer Name Insertion Format:  Unicode
30      SSL Interception: DISABLED
31      SSL Interception OCSP Check: ENABLED
32      SSL Interception End to End Renegotiation: ENABLED
33      SSL Interception Maximum Reuse Sessions per Server:   10
34      Session Ticket: DISABLED
35      HSTS: ENABLED
36      HSTS IncludeSubDomains: YES
37      HSTS Max-Age: 15552000
38      ECC Curve: P_256, P_384, P_224, P_521
39      1) Cipher Name: SECURE    Priority :1
40      Description: Predefined Cipher Alias
41      1) Vserver Name: v2
42  Done
43  <!--NeedCopy-->
```

Obtenga una calificación A+ para un servidor virtual SSL mediante la interfaz gráfica de usuario

1. Vaya a **Administración de tráfico > Equilibrio de carga > Servidores virtuales** y seleccione un servidor virtual SSL.
2. En Configuración avanzada, haga clic en Perfil SSL.
3. Seleccione ns_default_ssl_profile_secure_frontend.

4. Haga clic en Aceptar.
5. Haga clic en Done.

Apéndice A: Ejemplo de migración de la configuración SSL después de la actualización

January 12, 2021

Nota: Este contenido se ha eliminado porque el script de migración SSL para el nuevo perfil predeterminado ya no es compatible.

Apéndice B: Configuración predeterminada del perfil SSL de front-end y back-end

January 12, 2021

Un perfil de cliente predeterminado tiene la siguiente configuración:

```
sh ssl profile ns_default_ssl_profile_frontend

1)Name: ns_default_ssl_profile_frontend

      Configuration for Front-End SSL profile
      DH: DISABLED
      Ephemeral RSA: ENABLED          Refresh Count: 0
      Session Reuse: ENABLED          Timeout: 120 seconds
      Non FIPS Ciphers: DISABLED
      Cipher Redirect: ENABLED   Redirect URL: http://10.102.28.212/
         redirect.html
      Client Auth: DISABLED
      SSL Redirect: DISABLED
      SNI: DISABLED
      SSLv3: DISABLED TLSv1.0: ENABLED  TLSv1.1: ENABLED  TLSv1.2:
         ENABLED
      Push Encryption Trigger: Always
      PUSH encryption trigger timeout:     1 ms
      Send Close-Notify: YES
      Push flag: 0x0 (Auto)
      Deny SSL Renegotiation          NO
```



```
20       SSL quantum size:          8 kB
21       Strict CA checks:          NO
22       Encryption trigger timeout 100 mS
23       Encryption trigger packet count:     45
24       Use only bound CA certificates: DISABLED
25       Subject/Issuer Name Insertion Format: Unicode
26       Strict Host Header check for SNI enabled SSL sessions:          NO
27
28       ECC Curve: P_256, P_384, P_521
29
30  1)   Cipher Name: AES     Priority :2
31       Description: Predefined Cipher Alias
32
33  1)   Vserver Name: v1
34  2)   Vserver Name: nshttps-::1l-443
35  3)   Vserver Name: nsrpcs-::1l-3008
36  4)   Vserver Name: nskrpcs-127.0.0.1-3009
37  5)   Vserver Name: nshttps-127.0.0.1-443
38  6)   Vserver Name: nsrpcs-127.0.0.1-3008
39  Done
40  <!--NeedCopy-->
```

Un perfil de back-end predeterminado tiene la siguiente configuración:

```
1  sh ssl profile ns_default_ssl_profile_backend
2
3  1)Name: ns_default_ssl_profile_backend
4
5       Configuration for Back-End SSL profile
6       Session Reuse: ENABLED          Timeout: 300 seconds
7       Non FIPS Ciphers: DISABLED
8       Server Auth: DISABLED
9       SSLv3: DISABLED TLSv1.0: ENABLED  TLSv1.1: DISABLED  TLSv1.2:
           DISABLED
10      Push Encryption Trigger: Always
11      PUSH encryption trigger timeout:     1 ms
12      Send Close-Notify: YES
13      Push flag: 0x0 (Auto)
14      Deny SSL Renegotiation          ALL
15      SSL quantum size:          8 kB
16      Strict CA checks:          NO
17      Encryption trigger timeout 100 mS
18      Encryption trigger packet count:     45
```



```
      Use only bound CA certificates: DISABLED

      ECC Curve: P_256, P_224, P_521

1)    Cipher Name: AES      Priority :1
      Description: Predefined Cipher Alias

2)    Cipher Name: RC4      Priority :2
      Description: Predefined Cipher Alias

1)    Service Name: s2
2)    Service Name: s1
Done
<!--NeedCopy-->
```

Perfil SSL heredado

August 20, 2021

> **Nota:**
>
> Citrix recomienda utilizar los perfiles mejorados en lugar de los perfiles heredados. Para obtener información sobre la infraestructura de perfiles mejorada, consulte Infraestructura de perfiles SSL.

Importante:

> Enlazar un perfil SSL a un servidor virtual SSL. No enlazar un perfil DTLS a un servidor virtual SSL. Para obtener información sobre los perfiles DTLS, consulte Perfiles DTLS.

Puede utilizar un perfil SSL para especificar cómo un dispositivo Citrix ADC procesa el tráfico SSL. El perfil es una colección de parámetros SSL para entidades SSL, como servidores virtuales, servicios y grupos de servicios, y ofrece facilidad de configuración y flexibilidad. No se limita a configurar solo un conjunto de parámetros globales. Puede crear varios conjuntos (perfiles) de parámetros globales y asignar diferentes conjuntos a diferentes entidades SSL. Los perfiles SSL se clasifican en dos categorías:

- Perfiles front-end, que contienen parámetros aplicables a la entidad front-end. Es decir, se aplican a la entidad que recibe solicitudes de un cliente.
- Perfiles de back-end, que contienen parámetros aplicables a la entidad back-end. Es decir, se aplican a la entidad que envía solicitudes de cliente a un servidor.

A diferencia de un perfil TCP o HTTP, un perfil SSL es opcional. Por lo tanto, no hay ningún perfil SSL predeterminado. El mismo perfil se puede reutilizar en varias entidades. Si una entidad no tiene un

perfil asociado, se aplicarán los valores establecidos en el nivel global. Para los servicios aprendidos dinámicamente, se aplican los valores globales actuales.

En la tabla siguiente se enumeran los parámetros que forman parte de cada perfil.

Perfil de extremo delantero	Perfil de back-end
cipherRedirect, cipherURL	denySSLReneg
clearTextPort*	encryptTriggerPktCount
clientAuth, clientCert	nonFipsCiphers
denySSLReneg	pushEncTrigger
dh, dhFile, dhCount	pushEncTriggerTimeout
dropReqWithNoHostHeader	pushFlag
encryptTriggerPktCount	quantumSize
eRSA, eRSACount	serverAuth
insertionEncoding	commonName
nonFipsCiphers	sessReuse, sessTimeout
pushEncTrigger	`SNIEnable`
pushEncTriggerTimeout	ssl3
pushFlag	sslTriggerTimeout
quantumSize	strictCAChecks
redirectPortRewrite	tls1
sendCloseNotify	-
sessReuse, sessTimeout	-
`SNIEnable`	-
ssl3	-
sslRedirect	-
sslTriggerTimeout	-
strictCAChecks	-
tls1, tls11, tls12	-

* El parámetro ClearTextPort se aplica solo a un servidor virtual SSL.

Aparece un mensaje de error si intenta establecer un parámetro que no forma parte del perfil. Por

ejemplo, si intenta establecer el parámetro ClientAuth en un perfil de back-end.

Algunos parámetros SSL, como el tamaño de la memoria CRL, el tamaño de caché de OCSP, el control de undefaction y los datos de desdefacción, no forman parte de ninguno de los perfiles anteriores, ya que estos parámetros son independientes de las entidades.

Un perfil SSL admite las siguientes operaciones:

- Agregar: Crea un perfil SSL en Citrix ADC. Especifique si el perfil es front-end o back-end. El front-end es el valor predeterminado.
- Definir: Permite modificar la configuración de un perfil existente.
- Desestablecer: Establece los parámetros especificados en sus valores predeterminados. Si no especifica ningún parámetro, aparecerá un mensaje de error. Si desestablece un perfil en una entidad, el perfil está independiente de la entidad.
- Eliminar: Permite borrar un perfil. Un perfil que está siendo utilizado por ninguna entidad no se puede eliminar. Al borrar la configuración, se eliminan todas las entidades. Como resultado, los perfiles también se eliminan.
- Mostrar: Muestra todos los perfiles disponibles en Citrix ADC. Si se especifica un nombre de perfil, se muestran los detalles de ese perfil. Si se especifica una entidad, se muestran los perfiles asociados a esa entidad.

Crear un perfil SSL mediante la CLI

- Para agregar un perfil SSL, escriba:

```
add ssl profile <name> [-sslProfileType ( BackEnd | FrontEnd )]
<!--NeedCopy-->
```

- Para modificar un perfil existente, escriba:

```
set ssl profile <name>
<!--NeedCopy-->
```

- Para anular la configuración de un perfil existente, escriba:

```
unset ssl profile <name> [-dh] [-dhFile] [-dhCount] [-eRSA] ...
<!--NeedCopy-->
```

- Para anular la configuración de un perfil existente de una entidad, escriba:


```
unset ssl vserver <vServerName>  - sslProfile
<!--NeedCopy-->
```

- Para eliminar un perfil existente, escriba:

```
rm ssl profile <name>
<!--NeedCopy-->
```

- Para mostrar un perfil existente, escriba:

```
sh ssl profile <name>
<!--NeedCopy-->
```

Crear un perfil SSL mediante la interfaz gráfica de usuario

Vaya a **Sistema** > **Perfiles**, seleccione la ficha Perfiles SSL y cree un perfil SSL.

Habilitar un control más estricto en la validación de certificados de cliente

El dispositivo Citrix ADC acepta certificados de CA intermedia válidos si una sola CA raíz los ha emitido. Es decir, si solo el certificado de CA raíz está enlazado al servidor virtual y esa CA de raíz valida cualquiera de los certificados intermedios enviados con el certificado de cliente, el dispositivo confía en la cadena de certificados y el enlace se realiza correctamente.

Sin embargo, si un cliente envía una cadena de certificados en el protocolo de enlace, los certificados intermedios se pueden validar mediante un contestador CRL u OCSP solo si ese certificado está enlazado al servidor virtual SSL. Por lo tanto, incluso si se revoca uno de los certificados intermedios, el protocolo de enlace se realiza correctamente. Como parte del protocolo de enlace, el servidor virtual SSL envía la lista de certificados de CA que están enlazados a él. Para un control más estricto, puede configurar el servidor virtual SSL para que acepte solo un certificado que haya firmado uno de los certificados de CA enlazados a ese servidor virtual. Para ello, debe habilitar la `ClientAuthUseBoundCAChain` configuración en el perfil SSL enlazado al servidor virtual. El protocolo de enlace falla si uno de los certificados de CA enlazados al servidor virtual no ha firmado el certificado de cliente.

Por ejemplo, digamos que dos certificados de cliente, clientcert1 y clientcert2, están firmados por los certificados intermedios INT-CA-A e INT-CA-B, respectivamente. Los certificados intermedios están firmados por el certificado raíz Root-CA. Int-ca-A y Root-CA están enlazados al servidor virtual SSL.

En el caso predeterminado (ClientAuthUseBoundCachain inhabilitado), se aceptan tanto clientcert1 como clientcert2. Sin embargo, si ClientAuthUseBoundCachain está habilitado, el dispositivo Citrix ADC solo acepta clientcert1.

Habilitar un control más estricto en la validación de certificados de cliente mediante la CLI

En el símbolo del sistema, escriba: `set ssl profile <name> -ClientAuthUseBoundCAChain Enabled`

Habilitar un control más estricto en la validación de certificados de cliente mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **Perfiles**, seleccione la ficha **Perfiles SSL** y cree un perfil SSL o seleccione un perfil existente.
2. Seleccione **Habilitar autenticación de cliente mediante cadena de CA enlazada**.

Listas de revocación de certificados

August 20, 2021

Normalmente, un certificado emitido por una entidad emisora de certificados sigue siendo válido hasta su fecha de caducidad. Sin embargo, en algunas circunstancias, la entidad emisora de certificados podría revocar el certificado emitido antes de la fecha de caducidad. Por ejemplo, cuando la clave privada de un propietario se ve comprometida, el nombre de una empresa o individuo cambia, o cambia la asociación entre el sujeto y la entidad emisora de certificados.

Una lista de revocación de certificados (CRL) identifica los certificados no válidos por número de serie y emisor.

Las autoridades certificadoras emiten CRL regularmente. Puede configurar el dispositivo Citrix ADC para que utilice una CRL para bloquear las solicitudes de cliente que presenten certificados no válidos.

Si ya tiene un archivo CRL de una CA, agréguese al dispositivo Citrix ADC. Puede configurar las opciones de actualización. También puede configurar Citrix ADC para que sincronice el archivo CRL automáticamente en un intervalo especificado, ya sea desde una ubicación web o desde una ubicación LDAP. El dispositivo admite CRL en formato PEM o DER. Asegúrese de especificar el formato de archivo del archivo CRL que se va a agregar al dispositivo Citrix ADC.

Si ha utilizado el ADC como entidad emisora de certificados para crear certificados que se utilizan en implementaciones SSL, también puede crear una CRL para revocar un certificado determinado. Esta función se puede utilizar, por ejemplo, para asegurarse de que los certificados autofirmados que se

crean en Citrix ADC no se utilizan ni en un entorno de producción ni más allá de una fecha determinada.

Nota:

De forma predeterminada, las CRL se almacenan en el directorio /var/netscaler/ssl del dispositivo Citrix ADC.

Crear una CRL en el dispositivo ADC

Dado que puede utilizar el dispositivo ADC para actuar como entidad emisora de certificados y crear certificados autofirmados, también puede revocar los siguientes certificados:

- Certificados que ha creado.
- Certificados cuyo certificado de CA posee.

El dispositivo debe revocar certificados no válidos antes de crear una CRL para dichos certificados. El dispositivo almacena los números de serie de los certificados revocados en un archivo de índice y actualiza el archivo cada vez que revoca un certificado. El archivo de índice se crea automáticamente la primera vez que se revoca un certificado.

Revocar un certificado o crear una CRL mediante la CLI

En el símbolo del sistema, escriba el siguiente comando:

```
create ssl crl <CAcertFile> <CAkeyFile> <indexFile> (-revoke <
    input_filename> | -genCRL <output_filename>)
<!--NeedCopy-->
```

Ejemplo:

```
create ssl crl Cert-CA-1 Key-CA-1 File-Index-1 -revoke Invalid-1

create ssl crl Cert-CA-1 Key-CA-1 File-Index-1 -genCRL CRL-1
<!--NeedCopy-->
```

Revocar un certificado o crear una CRL mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > SSL** y, en el grupo Introducción, seleccione Administración de CRL.

2. Introduzca los detalles del certificado y, en la lista **Elegir operación**, seleccione **Revocar certificado**o **Generar CRL**.

Agregar una CRL existente al ADC

Antes de configurar la CRL en el dispositivo Citrix ADC, asegúrese de que el archivo CRL se almacena localmente en el dispositivo Citrix ADC. En una instalación de HA, el archivo CRL debe estar presente en ambos dispositivos ADC y la ruta del directorio al archivo debe ser la misma en ambos dispositivos.

Agregue una CRL en Citrix ADC mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para agregar una CRL en Citrix ADC y compruebe la configuración:

```
add ssl crl <crlName> <crlPath> [-inform (DER | PEM)]

show ssl crl [<crlName>]
<!--NeedCopy-->
```

Ejemplo:

```
> add ssl crl crl-one /var/netscaler/ssl/CRL-one -inform PEM

Done

> show ssl crl crl-one

            Name: crl-one   Status: Valid,  Days to expiration: 29
            CRL Path: /var/netscaler/ssl/CRL-one
            Format: PEM     CAcert: samplecertkey
            Refresh: DISABLED
            Version: 1
            Signature Algorithm: sha1WithRSAEncryption
            Issuer:  C=US,ST=California,L=Santa Clara,O=NetScaler Inc.,
               OU=SSL Acceleration,CN=www.ns.com/emailAddress=
               support@Citrix ADC appliance.com
            Last_update:Jun 15 10:53:53 2010 GMT
            Next_update:Jul 15 10:53:53 2010 GMT

    1)      Serial Number: 00
            Revocation Date:Jun 15 10:51:16 2010 GMT
```



```
19       Done
20 <!--NeedCopy-->
```

Agregue una CRL en Citrix ADC mediante la interfaz gráfica de usuario

Vaya a **Administración del tráfico** > **SSL** > **CRL** y agregue una CRL.

Configurar parámetros de actualización de CRL

Una entidad de certificación genera y publica una CRL periódicamente o, a veces, inmediatamente después de revocar un certificado determinado. Citrix recomienda actualizar las CRL en el dispositivo Citrix ADC con regularidad, para protegerse contra los clientes que intentan conectarse con certificados que no son válidos.

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

Nota: En la versión 10.0 y posteriores, el método para actualizar una CRL no se incluye de forma predeterminada. Especifique un método HTTP o LDAP. Si va a actualizar de una versión anterior a la versión 10.0 o posterior, debe agregar un método y ejecutar el comando de nuevo.

Configurar la actualización automática de CRL mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para configurar la actualización automática de CRL y comprobar la configuración:

```
1 set ssl crl <crlName> [-refresh ( ENABLED | DISABLED )] [-CAcert <
     string>] [-server <ip_addr|ipv6_addr|*> | -url <URL>] [-method (
     HTTP | LDAP )] [-port <port>] [-baseDN <string>] [-scope ( Base |
     One )] [-interval <interval>] [-day <positive_integer>] [-time <HH:
     MM>][-bindDN <string>] {
2  -password  }
3   [-binary ( YES | NO )]
4
5 show ssl crl [<crlName>]
6 <!--NeedCopy-->
```

Ejemplo:


```
1     set CRL crl1  -refresh enabled -method ldap -inform DER -CAcert ca1
          -server 10.102.192.192 -port 389 -scope base -baseDN "cn=
         clnt_rsa4_multicert_der,ou=eng,o=ns,c=in" -time 00:01
2
3     set ssl crl crl1 -refresh enabled -method http -cacert ca1 -port 80
          -time 00:10 -url http://10.102.192.192/crl/ca1.crl
4
5
6     > sh crl
7
8     1)          Name: crl1        Status: Valid,     Days to expiration:
          355
9                  CRL Path: /var/netscaler/ssl/crl1
10                 Format: PEM      CAcert: ca1
11                 Refresh: ENABLED          Method: HTTP
12                 URL: http://10.102.192.192/crl/ca1.crl
                      Port:80
13                 Refresh Time: 00:10
14                 Last Update: Successful, Date:Tue Jul  6 14:38:13 2010
15    Done
16 <!--NeedCopy-->
```

Configurar la actualización automática de CRL mediante LDAP o HTTP mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > SSL > CRL**.
2. Abra una CRL y seleccione **Activar actualización automática de CRL**.

> **Nota**
>
> Si la nueva CRL se ha actualizado en el repositorio externo antes de su hora de actualización real, tal como se especifica en el campo **Hora de última actualización** de la CRL, debe hacer lo siguiente: Actualice
>
> inmediatamente la CRL en el dispositivo Citrix ADC.

Para ver la última hora de actualización, seleccione la CRL y haga clic en **Detalles**.

Sincronizar CRL

El dispositivo Citrix ADC utiliza la CRL distribuida más recientemente para evitar que los clientes con certificados revocados accedan a recursos seguros.

Si las CRL se actualizan con frecuencia, el dispositivo Citrix ADC necesita un mecanismo automatizado para obtener las CRL más recientes del repositorio. Puede configurar el dispositivo para que actualice las CRL automáticamente en un intervalo de actualización especificado.

El dispositivo mantiene una lista interna de CRL que deben actualizarse a intervalos regulares. A estos intervalos especificados, el dispositivo analiza la lista en busca de CRL que deben actualizarse. A continuación, se conecta al servidor LDAP remoto o al servidor HTTP, recupera las CRL más recientes y, a continuación, actualiza la lista de CRL local con las nuevas CRL.

> **Nota:**
>
> Si la comprobación CRL se establece en obligatoria cuando el certificado de CA está enlazado al servidor virtual y falla la actualización inicial de CRL, se realiza la siguiente acción para las conexiones:
>
> Todas las conexiones de autenticación de cliente con el mismo emisor que la CRL se rechazan como REVOKED hasta que la CRL se actualiza correctamente.

Puede especificar el intervalo en el que se debe realizar la actualización de CRL. También puede especificar la hora exacta.

Sincronizar actualización automática de CRL mediante la CLI

En el símbolo del sistema, escriba el siguiente comando:

```
set ssl crl <crlName> [-interval <interval>] [-day <integer>] [-time <
    HH:MM>]
<!--NeedCopy-->
```

Ejemplo:

```
set ssl crl CRL-1 -refresh ENABLE -interval MONTHLY -days 10 -time
    12:00
<!--NeedCopy-->
```

Sincronizar actualización CRL mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > SSL > CRL**.
2. Abra una CRL, seleccione **Activar actualización automática de CRL** y especifique el intervalo.

Realizar la autenticación de cliente mediante una lista de revocación de certificados

Si hay una lista de revocación de certificados (CRL) en un dispositivo Citrix ADC, se realiza una comprobación de CRL independientemente de si la comprobación de CRL está establecida como obligatoria u opcional.

El éxito o fracaso de un apretón de manos depende de una combinación de los siguientes factores:

- Regla para comprobación CRL
- Regla para la comprobación de certificados de cliente
- Estado de la CRL configurada para el certificado de CA

En la siguiente tabla se enumeran los resultados de las posibles combinaciones de un protocolo de enlace que implica un certificado revocado.

Cuadro 1 Resultado de un apretón de manos con un cliente que utiliza un certificado revocado

Regla para comprobación CRL	Regla para comprobación de certificados de cliente	Estado de la CRL configurada para el certificado de CA	Resultado de un apretón de manos con un certificado revocado
Opcional	Opcional	Desaparecido	Operación correctamente realizada.
Opcional	Obligatorio	Desaparecido	Operación correctamente realizada.
Opcional	Obligatorio	Presente	Fallo
Obligatorio	Opcional	Desaparecido	Operación correctamente realizada.
Obligatorio	Obligatorio	Desaparecido	Fallo
Obligatorio	Opcional	Presente	Operación correctamente realizada.
Obligatorio	Obligatorio	Presente	Fallo
Opcional/Obligatorio	Opcional	Caducado	Operación correctamente realizada.
Opcional/Obligatorio	Obligatorio	Caducado	Fallo

Nota:

- La comprobación CRL es opcional de forma predeterminada. Para cambiar de opcional a obligatorio o a la inversa, primero debe desenlazar el certificado del servidor virtual SSL y, a continuación, enlazarlo de nuevo después de cambiar la opción.
- En la salida del comando `sh ssl vserver`, la comprobación OCSP: Opcional implica que una comprobación CRL también es opcional. La configuración de comprobación CRL se muestra en la salida del `sh ssl vserver` comando solo si la comprobación CRL está establecida en obligatoria. Si la comprobación de CRL se establece en opcional, los detalles de la comprobación CRL no aparecerán.

Para configurar la comprobación CRL mediante la CLI

En el símbolo del sistema, escriba el siguiente comando:

```
bind ssl vserver <vServerName> -certkeyName <string> [(-CA -crlCheck (
   Mandatory | Optional ))]
sh ssl vserver
<!--NeedCopy-->
```

Ejemplo:

```
bind ssl vs v1 -certkeyName ca -CA -crlCheck mandatory
> sh ssl vs v1

Advanced SSL configuration for VServer v1:

DH: DISABLED
DH Private-Key Exponent Size Limit: DISABLED
Ephemeral RSA: ENABLED Refresh Count: 0
Session Reuse: ENABLED Timeout: 120 seconds
Cipher Redirect: DISABLED
SSLv2 Redirect: DISABLED
ClearText Port: 0
Client Auth: ENABLED Client Cert Required: Mandatory
SSL Redirect: DISABLED
Non FIPS Ciphers: DISABLED
SNI: DISABLED
OCSP Stapling: DISABLED
HSTS: DISABLED
HSTS IncludeSubDomains: NO
```



```
20 HSTS Max-Age: 0
21 SSLv2: DISABLED SSLv3: ENABLED TLSv1.0: ENABLED TLSv1.1: ENABLED TLSv1
       .2: ENABLED
22 Push Encryption Trigger: Always
23 Send Close-Notify: YES
24
25 ECC Curve: P_256, P_384, P_224, P_521
26
27 1) CertKey Name: ca CA Certificate CRLCheck: Mandatory CA_Name Sent
28
29 1) Cipher Name: DEFAULT
30 Description: Predefined Cipher Alias
31 Done
32 <!--NeedCopy-->
```

Configurar la comprobación CRL mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**y abra un servidor virtual SSL.
2. Haga clic en la sección **Certificados**.
3. Seleccione un certificado y, en la lista **Comprobación de OCSP y CRL**, seleccione **Obligatorio de CRL**.

Resultado de un apretón de manos con un certificado revocado o válido

Regla para comprobación CRL	Regla para la comprobación de certificados de cliente	Estado de la CRL configurada para el certificado de CA	Resultado de un apretón de manos con un certificado revocado	Resultado de un apretón de manos con un certificado válido
Obligatorio	Obligatorio	Presente	Fallo	Operación correctamente realizada.
Obligatorio	Obligatorio	Caducado	Fallo	Fallo
Obligatorio	Obligatorio	Desaparecido	Fallo	Fallo
Obligatorio	Obligatorio	No definida	Fallo	Fallo
Opcional	Obligatorio	Presente	Fallo	Operación correctamente realizada.

Regla para comprobación CRL	Regla para la comprobación de certificados de cliente	Estado de la CRL configurada para el certificado de CA	Resultado de un apretón de manos con un certificado revocado	Resultado de un apretón de manos con un certificado válido
Opcional	Obligatorio	Caducado	Operación correctamente realizada.	Operación correctamente realizada.
Opcional	Obligatorio	Desaparecido	Operación correctamente realizada.	Operación correctamente realizada.
Opcional	Obligatorio	No definida	Operación correctamente realizada.	Operación correctamente realizada.
Obligatorio	Opcional	Presente	Operación correctamente realizada.	Operación correctamente realizada.
Obligatorio	Opcional	Caducado	Operación correctamente realizada.	Operación correctamente realizada.
Obligatorio	Opcional	Desaparecido	Operación correctamente realizada.	Operación correctamente realizada.
Obligatorio	Opcional	No definida	Operación correctamente realizada.	Operación correctamente realizada.
Opcional	Opcional	Presente	Operación correctamente realizada.	Operación correctamente realizada.
Opcional	Opcional	Caducado	Operación correctamente realizada.	Operación correctamente realizada.
Opcional	Opcional	Desaparecido	Operación correctamente realizada.	Operación correctamente realizada.

Regla para comprobación CRL	Regla para la comprobación de certificados de cliente	Estado de la CRL configurada para el certificado de CA	Resultado de un apretón de manos con un certificado revocado	Resultado de un apretón de manos con un certificado válido
Opcional	Opcional	No definida	Operación correctamente realizada.	Operación correctamente realizada.

Supervisar el estado del certificado con OCSP

February 16, 2021

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

Implementación de OCSP

La validación de OCSP en un dispositivo Citrix ADC comienza cuando el dispositivo recibe un certificado de cliente durante un protocolo de enlace SSL. Para validar el certificado, el dispositivo crea una solicitud OCSP y la reenvía al respondedor OCSP. Para ello, el dispositivo utiliza una dirección URL configurada localmente. La transacción se encuentra en un estado suspendido hasta que el dispositivo evalúa la respuesta del servidor y determina si quiere permitir la transacción o rechazarla. Si la respuesta del servidor se retrasa más allá del tiempo configurado y no hay otros respondedores configurados, el dispositivo permite la transacción o muestra un error, dependiendo de si la comprobación OCSP se ha establecido como opcional u obligatoria, respectivamente.

El dispositivo admite el procesamiento por lotes de solicitudes de OCSP y el almacenamiento en caché de las respuestas de OCSP para reducir la carga en el respondedor de OCSP y proporcionar respuestas más rápidas.

lotes de solicitudes OCSP

Cada vez que el dispositivo recibe un certificado de cliente, envía una solicitud al respondedor de OCSP. Para evitar sobrecargar el respondedor OCSP, el dispositivo puede consultar el estado de más de un certificado de cliente en la misma solicitud. Para que esta función funcione de manera eficiente, es necesario definir un tiempo de espera para que el procesamiento de un único certificado no se retrase excesivamente mientras se espera formar un lote.

Almacenamiento en caché de respuesta de OCSP

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

> **Nota**: A partir de la versión 12.1 compilación 49.x, el límite de tiempo de espera de caché ahora se incrementa a un máximo de 43200 minutos (30 días). Anteriormente, el límite era 1440 minutos (un día). El límite aumentado ayuda a reducir las búsquedas en el servidor OCSP y evitar cualquier error de conexión SSL/TLS en caso de que el servidor OCSP no sea accesible debido a problemas de red u otros.

Configuración del respondedor OCSP

La configuración de OCSP implica agregar un respondedor OCSP, enlazar el respondedor OCSP a un certificado de entidad emisora de certificados (CA) y enlazar el certificado a un servidor virtual SSL. Si necesita enlazar un certificado diferente a un respondedor OCSP que ya se ha configurado, primero debe desenlazar el respondedor y, a continuación, enlazar el respondedor a un certificado diferente.

Agregar un respondedor OCSP mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para configurar OCSP y verificar la configuración:


```
add ssl ocspResponder <name> -url <URL> [-cache ( ENABLED | DISABLED )
    [-cacheTimeout <positive_integer>]] [ -batchingDepth <
    positive_integer>][-batchingDelay <positive_integer>] [-resptimeout
    <positive_integer>] [-responderCert <string> | -trustResponder] [-
    producedAtTimeSkew <positive_integer>][-signingCert <string>][-
    useNonce ( YES | NO )][ -insertClientCert( YES | NO )]
<!--NeedCopy-->
```

```
bind ssl certKey [<certkeyName>] [-ocspResponder <string>] [-priority <
    positive_integer>]
<!--NeedCopy-->
```

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

```
show ssl ocspResponder [<name>]
<!--NeedCopy-->
```

Ejemplo:

```
add ssl ocspResponder ocsp_responder1 -url ”http:// www.myCA.org:80/
    ocsp/” -cache ENABLED -cacheTimeout 30 -batchingDepth 8 -
    batchingDelay 100 -resptimeout 100 -responderCert responder_cert -
    producedAtTimeSkew 300 -signingCert sign_cert  -insertClientCert YES
<!--NeedCopy-->
```

```
bind ssl certKey ca_cert -ocspResponder ocsp_responder1 -priority 1
<!--NeedCopy-->
```

```
bind ssl vserver vs1 -certkeyName ca_cert -CA -ocspCheck Mandatory
<!--NeedCopy-->
```



```
sh ocspResponder ocsp_responder1

    1)Name: ocsp_responder1
    URL: http://www.myCA.org:80/ocsp/, IP: 192.128.22.22
    Caching: Enabled        Timeout: 30 minutes
    Batching: 8 Timeout: 100 mS
    HTTP Request Timeout: 100mS
    Request Signing Certificate: sign_cert
    Response Verification: Full, Certificate: responder_cert
    ProducedAt Time Skew: 300 s
    Nonce Extension: Enabled
     Client Cert Insertion: Enabled
    Done
<!--NeedCopy-->
```

```
show certkey ca_cert

    Name: ca_cert     Status: Valid,   Days to expiration:8907
    Version: 3
    …

    1)  VServer name: vs1      CA Certificate
    1)  OCSP Responder name: ocsp_responder1     Priority: 1
Done
<!--NeedCopy-->
```

```
sh ssl vs vs1

    Advanced SSL configuration for VServer vs1:
    DH: DISABLED
    …

    1) CertKey Name: ca_cert CA Certificate OCSPCheck: Mandatory
    1) Cipher Name: DEFAULT
      Description: Predefined Cipher Alias
    Done
<!--NeedCopy-->
```


Modificar un respondedor OCSP mediante la CLI

No se puede modificar el nombre del respondedor. Todos los demás parámetros se pueden cambiar mediante el `set ssl ocspResponder` comando.

En el símbolo del sistema, escriba los siguientes comandos para establecer los parámetros y verificar la configuración:

```
set ssl ocspResponder <name> [-url <URL>] [-cache ( ENABLED | DISABLED)
    ] [-cacheTimeout <positive_integer>] [-batchingDepth <
    positive_integer>] [-batchingDelay <positive_integer>] [-resptimeout
     <positive_integer>] [ -responderCert <string> | -trustResponder][-
    producedAtTimeSkew <positive_integer>][-signingCert <string>] [-
    useNonce ( YES | NO )]

unbind ssl certKey [<certkeyName>] [-ocspResponder <string>]

bind ssl certKey [<certkeyName>] [-ocspResponder <string>] [-priority <
    positive_integer>]

show ssl ocspResponder [<name>]
<!--NeedCopy-->
```

Configurar un respondedor OCSP mediante la interfaz gráfica de usuario

1. Vaya a **Administración de tráfico** > **SSL** > **Respondedor de OCSP** y configure un respondedor de OCSP.
2. Vaya a **Administración del tráfico** > **SSL** > **Certificados**, seleccione un certificado y, en la lista **Acción**, seleccione **Enlaces de OCSP**. Enlazar un respondedor OCSP.
3. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**, abra un servidor virtual y haga clic en la sección Certificados para enlazar un certificado de CA.
4. Si lo quiere, **seleccione Obligatorio OCSP**.

Grapado OCSP

January 12, 2021

La implementación de Citrix ADC de CRL y OCSP informa únicamente del estado de revocación de certificados de cliente. Para comprobar el estado de revocación de un certificado de servidor recibido

durante un protocolo de enlace SSL, un cliente debe enviar una solicitud a una entidad emisora de certificados.

Para sitios web con mucho tráfico, muchos clientes reciben el mismo certificado de servidor. Si cada cliente envía una consulta para el estado de revocación del certificado del servidor, la entidad emisora de certificados se inundaría con solicitudes OCSP para comprobar la validez del certificado.

Solución de grapado OCSP

Para evitar la congestión innecesaria, el dispositivo Citrix ADC admite ahora el grapado OCSP. Es decir, el dispositivo ahora puede enviar el estado de revocación de un certificado de servidor a un cliente, en el momento de la conexión SSL, después de validar el estado del certificado desde un respondedor OCSP. El estado de revocación de un certificado de servidor está "grapado" a la respuesta que el dispositivo envía al cliente como parte del protocolo de enlace SSL. Para utilizar la función de grapado OCSP, debe habilitarla en un servidor virtual SSL y agregar un respondedor OCSP al dispositivo.

Nota:

- Los dispositivos Citrix ADC admiten el grapado OCSP tal como se define en RFC 6066.
- El grapado OCSP solo se admite en el front-end de los dispositivos Citrix ADC.

> **Importante:**
>
> La compatibilidad con Citrix ADC para el grapado OCSP se limita a los apretones de manos que utilizan el protocolo TLS versión 1.0 o superior.

Almacenamiento en caché de respuesta OCSP de certificados de servidor

Durante el protocolo de enlace SSL, cuando un cliente solicita el estado de revocación del certificado de servidor, el dispositivo comprueba en primer lugar la entrada de este certificado en su caché local. Si se encuentra una entrada válida, se evalúa y el certificado del servidor y su estado se presentan al cliente. Si no se encuentra una entrada de estado de revocación, el dispositivo envía una solicitud para el estado de revocación del certificado de servidor al respondedor de OCSP. Si recibe una respuesta, envía el certificado y el estado de revocación al cliente. Si el siguiente campo de actualización está presente en la respuesta de OCSP, la respuesta se almacena en caché durante el período de tiempo configurado (valor especificado en el campo de tiempo de espera).

> **Nota**: Desde la versión 12.1 compilación 49.x, puede borrar la respuesta almacenada en caché del certificado del servidor del respondedor OCSP incluso antes de que expire el tiempo de espera. Anteriormente, no era posible descartar el estado almacenado en caché en el par de claves certificadas hasta que finalice el tiempo de espera configurado.

Para borrar el estado almacenado en caché mediante la CLI, en el símbolo del sistema, escriba:


```
clear ssl certKey <certkey name> -ocspstaplingCache
<!--NeedCopy-->
```

Ejemplo:

```
clear ssl certKey s1 -ocspstaplingCache
<!--NeedCopy-->
```

Para borrar el estado almacenado en caché mediante la interfaz gráfica de usuario

1. En la GUI, vaya a **Administración de tráfico** > **SSL** > **Certificados > Certificadosde CA**.
2. En el panel de detalles, seleccione un certificado.
3. En la lista **Seleccionar acción**, seleccione **Borrar**. Cuando se le pida que confirme, haga clic en **Sí**.

Configuración de grapado OCSP

La configuración del grapado OCSP implica habilitar la función y configurar OCSP. Para configurar OCSP, debe agregar un respondedor OCSP, enlazar el respondedor OCSP a un certificado de CA y enlazar el certificado a un servidor virtual SSL.

> **Nota:**
>
> Se admiten respondedores OCSP con solo URL basada en HTTP.

Habilitar el grapado de OCSP mediante la CLI

En el símbolo del sistema, escriba:

```
set ssl vserver <name> -ocspstapling [ENABLED | DISABLED]
<!--NeedCopy-->
```

Ejemplo:

```
set ssl vserver vip1 -ocspStapling ENABLED
Done

sh ssl vserver vip1

```



```
6       Advanced SSL configuration for VServer vip1:
7       DH: DISABLED
8       DH Private-Key Exponent Size Limit: DISABLED Ephemeral RSA:
            ENABLED Refresh Count: 0
9       Session Reuse: ENABLED Timeout: 120 seconds
10      Cipher Redirect: DISABLED
11      SSLv2 Redirect: DISABLED
12      ClearText Port: 0
13      Client Auth: DISABLED
14      SSL Redirect: DISABLED
15      Non FIPS Ciphers: DISABLED
16      SNI: ENABLED
17      OCSP Stapling: ENABLED
18      SSLv2: DISABLED SSLv3: DISABLED TLSv1.0: ENABLED  TLSv1.1: ENABLED
             TLSv1.2: ENABLED
19      Push Encryption Trigger: Always
20      Send Close-Notify: YES
21
22      ECC Curve: P_256, P_384, P_224, P_521
23
24     1) CertKey Name: server_certificate1 Server Certificate
25
26     1) Cipher Name: DEFAULT
27      Description: Default cipher list with encryption strength >= 128
            bit
28  Done
29  <!--NeedCopy-->
```

Nota: Si el perfil predeterminado (mejorado) está habilitado, utilice el comando `set ssl profile <profile name> -ocspStapling [ENABLED | DISABLED]` para habilitar o inhabilitar OCSP.

Habilitar el grapado de OCSP mediante la interfaz gráfica de usuario

1. Vaya a **Administración de tráfico** > **SSL** > **Servidor virtual**.
2. Abra un servidor virtual y, en **Parámetros SSL**, seleccione **Grapado OCSP**.

Configuración OCSP

Se agrega un respondedor de OCSP de forma dinámica o manual para enviar solicitudes de grapado de OCSP. Un respondedor interno se agrega dinámicamente al agregar un certificado de servidor y su certificado de emisor basado en la dirección URL de OCSP en el certificado de servidor. Se agrega un respondedor OCSP manual desde la CLI o GUI. Para enviar una solicitud OCSP para un certificado de servidor, el dispositivo Citrix ADC selecciona un respondedor OCSP en función de la prioridad que se

le asigna al vincularlo a un certificado emisor. Si un respondedor no envía una solicitud de grapado OCSP, se selecciona el respondedor con la prioridad siguiente para enviar la solicitud. Por ejemplo, si solo se configura manualmente un respondedor y falla y existe un respondedor enlazado dinámicamente, se selecciona para enviar la solicitud OCSP.

Si la dirección URL de OCSP es distinta de HTTP, no se crea un respondedor OCSP interno.

> **Nota**
>
> Un respondedor OCSP agregado manualmente tiene prioridad sobre un respondedor agregado dinámicamente.

Diferencia entre un respondedor OCSP creado manualmente y un respondedor OCSP creado internamente

Respondedor OCSP creado manualmente	Respondedor OCSP creado internamente (dinámicamente)
Creado de forma manual y explícita enlazado al certificado emisor con prioridad.	Creado y enlazado de forma predeterminada, al tiempo que agrega un certificado de servidor y su certificado de emisor (certificado de CA). El nombre comienza con “ns_internal_”.
La prioridad entre 1 y 127 está reservada para un respondedor configurado.	La prioridad se asigna automáticamente a partir de 128.
URL y profundidad de lotes se pueden cambiar.	La URL y la profundidad de lotes no se pueden cambiar.
Eliminado directamente.	Se elimina solo cuando se elimina el certificado de servidor o el certificado de CA.
Puede vincularse a cualquier certificado de CA.	Encuadernado de forma predeterminada a un certificado de CA. No se puede vincular a ningún otro certificado de CA.
Guardado en la configuración (ns.conf).	Los comandos de adición no se guardan en la configuración. Solo se guardan los comandos de conjunto.

Si vincula tres respondedores de OCSP al mismo certificado de emisor con las prioridades 1, 2 y 3 respectivamente, y posteriormente desvincula la prioridad 2, las demás prioridades no se verán afectadas.	Tres respondedores de OCSP se vinculan automáticamente a un certificado de emisor con las prioridades 128, 129 y 130 respectivamente. Si quita el certificado de servidor que se utilizó para crear un respondedor vinculado con la prioridad 129, se elimina ese respondedor. Además, la prioridad del siguiente respondedor (prioridad 130) se cambia automáticamente a 129.

> **Ejemplo de manejo de solicitudes**:

1. Agregue un servidor virtual (VIP1).
2. Agregue el certificado emisor (CA1) y vincularlo a VIP1.
3. Agregue tres certificados S1, S2 y S3. Los respondedores internos resp1, resp2 y resp3 respectivamente se crean de forma predeterminada.
4. Enlazar S3 a VIP1.
5. Una solicitud llega a VIP1. Responder resp3 está seleccionado.

Para crear dinámicamente un respondedor OCSP interno, el dispositivo necesita lo siguiente:

- Certificado del emisor del certificado de servidor (normalmente el certificado de CA).
- Par de certificados y claves del certificado de servidor. Este certificado debe contener la dirección URL de OCSP proporcionada por la entidad emisora de certificados. La URL se utiliza como nombre del respondedor interno agregado dinámicamente.

Un respondedor OCSP interno tiene los mismos valores predeterminados que un respondedor configurado manualmente.

> **Nota:**
>
> El almacenamiento en caché está inhabilitado de forma predeterminada en un respondedor interno. Utilice el `set ssl ocspResponder` comando para habilitar el almacenamiento en caché.

Configurar OCSP mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para configurar OCSP y verificar la configuración:


```
add ssl certKey <certkeyName> (-cert <string> [-password]) [-key <
    string> | -fipsKey <string> | -hsmKey <string>] [-inform <inform>]
    [-expiryMonitor ( ENABLED | DISABLED ) [-notificationPeriod <
    positive_integer>]] [-bundle ( YES | NO )]

add ssl ocspResponder <name> -url <URL> [-cache ( ENABLED | DISABLED )
    [-cacheTimeout <positive_integer>]] [-resptimeout <positive_integer
    >] [-responderCert <string> | -trustResponder] [-producedAtTimeSkew
    <positive_integer>][-signingCert <string>][-useNonce ( YES | NO )][
    -insertClientCert ( YES | NO )]

bind ssl certKey [<certkeyName>] [-ocspResponder <string>] [-priority <
    positive_integer>]

show ssl ocspResponder [<name>]
<!--NeedCopy-->
```

Parámetros:

Método HttpTod:

Método HTTP utilizado para enviar solicitudes OCSP. Para las solicitudes de menos de 255 bytes de longitud, puede configurar el método HTTP GET para las consultas a un servidor OCSP. Si especifica el método GET pero la longitud es mayor que 255 bytes, el dispositivo utiliza el método predeterminado (POST).

Valores posibles: GET, POST

Valor predeterminado: POST

OCSpurlResolveTimeout:

Tiempo, en milisegundos, para esperar una resolución de URL OCSP. Una vez transcurrido este tiempo, se selecciona el respondedor con la siguiente prioridad más alta. Si todos los respondedores fallan, aparece un mensaje de error o se elimina la conexión, dependiendo de la configuración del servidor virtual.

Valor mínimo: 100

Valor máximo: 2000

Ejemplo:

```
add ssl certkey root_ca1 -cert root_cacert.pem
add ssl ocspResponder ocsp_responder1 -url "http:// www.myCA.org:80/
    ocsp/" -cache ENABLED -cacheTimeout 30  -resptimeout 100 -
```



```
    responderCert responder_cert -producedAtTimeSkew 300 -signingCert
    sign_cert  -insertClientCert YES
bind ssl certKey root_ca1 -ocspResponder ocsp_responder1 -priority 1
sh ocspResponder ocsp_responder1
    1)Name: ocsp_responder1
    URL: http://www.myCA.org:80/ocsp/, IP: 192.128.22.22
    Caching: Enabled        Timeout: 30 minutes
    Batching: 8 Timeout: 100 mS
    HTTP Request Timeout: 100mS
    Request Signing Certificate: sign_cert
    Response Verification: Full, Certificate: responder_cert
    ProducedAt Time Skew: 300 s
    Nonce Extension: Enabled
     Client Cert Insertion: Enabled
    Done

show certkey root_ca1
    Name: root_ca1     Status: Valid,   Days to expiration:8907
    Version: 3
    …
    1)  OCSP Responder name: ocsp_responder1     Priority: 1
    Done
<!--NeedCopy-->
```

Modificar OCSP mediante la CLI

No se puede modificar el nombre de un respondedor de OCSP, pero puede utilizar el `set ssl ocspResponder` comando para cambiar cualquiera de los demás parámetros.

En el símbolo del sistema, escriba los siguientes comandos para establecer los parámetros y verificar la configuración:

```
set ssl ocspResponder <name> [-url <URL>] [-cache ( ENABLED | DISABLED)
    ] [-cacheTimeout <positive_integer>]  [-resptimeout <
    positive_integer>] [ -responderCert <string> | -trustResponder][-
    producedAtTimeSkew <positive_integer>][-signingCert <string>] [-
    useNonce ( YES | NO )]

unbind ssl certKey [<certkeyName>] [-ocspResponder <string>]

bind ssl certKey [<certkeyName>] [-ocspResponder <string>] [-priority <
    positive_integer>]

```



```
show ssl ocspResponder [<name>]
<!--NeedCopy-->
```

Configurar OCSP mediante la interfaz gráfica de usuario

1. Vaya a **Administración de tráfico** > **SSL** > **Respondedor de OCSP** y configure un respondedor de OCSP.
2. Vaya a **Administración del tráfico** > **SSL** > **Certificados**, seleccione un certificado y, en la lista **Acción**, seleccione **Enlaces de OCSP**. **Enlazar un respondedor OCSP**.
3. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**, abra un servidor virtual y haga clic en la sección Certificados para enlazar un certificado de CA.
4. Si lo quiere, seleccione **Obligatorio OCSP**.

> **Nota:**
>
> El parámetro de certificado de cliente de insertar en `add ssl ocspResponder` y los `set ssl ocspResponder` comandos ya no es válido. Es decir, el parámetro se ignora durante la configuración.

Cifrados disponibles en los dispositivos Citrix ADC

June 22, 2022

El dispositivo Citrix ADC se entrega con un conjunto predefinido de grupos de cifrado. Para usar cifrados que no forman parte del grupo de cifrado DEFAULT, debe vincularlos explícitamente a un servidor virtual SSL. También puede crear un grupo de cifrado definido por el usuario para enlazar al servidor virtual SSL. Para obtener más información sobre la creación de un grupo de cifrado definido por el usuario, consulte Configurar grupos de cifrado definidos por el usuario en el dispositivo ADC.

> **Notas**
>
> El cifrado RC4 no se incluye en el grupo de cifrado predeterminado del dispositivo Citrix ADC. Sin embargo, es compatible con el software de los dispositivos basados en N3. El cifrado RC4, incluido el apretón de manos, se realiza en el software.
>
> Citrix recomienda no utilizar este cifrado porque RFC 7465 lo considera inseguro y está obsoleto.
>
> Utilice el comando “show hardware” para identificar si su dispositivo tiene chips N3.

```
sh hardware

```



```
Platform: NSMPX-22000 16\*CPU+24\*IX+12\*E1K+2\*E1K+4*CVM N3 2200100

Manufactured on: 8/19/2013

CPU: 2900MHZ

Host Id: 1006665862

Serial no: ENUK6298FT

Encoded serial no: ENUK6298FT
<!--NeedCopy-->
```

- Para mostrar información sobre los conjuntos de cifrado enlazados de forma predeterminada en el front-end (a un servidor virtual), escriba: `sh cipher DEFAULT`
- Para mostrar información sobre los conjuntos de cifrado enlazados de forma predeterminada en el back-end (a un servicio), escriba: `sh cipher DEFAULT_BACKEND`
- Para mostrar información sobre todos los grupos de cifrado (alias) definidos en el dispositivo, escriba: `sh cipher`
- Para mostrar información sobre todos los conjuntos de cifrado que forman parte de un grupo de cifrado específico, escriba: `sh cipher <alias name>`. Por ejemplo, el cifrado sh ECDHE.

En los siguientes vínculos se enumeran los conjuntos de cifrado admitidos en diferentes plataformas Citrix ADC y en módulos de seguridad de hardware (HSM) externos:

- Dispositivo**Citrix ADC MPX/SDX Intel Lewisburg: compatibilidad con cifrado en un dispositivo**basado en chip SSL Intel Lewisburg Citrix MPX/SDX
- Dispositivo**Citrix ADC MPX/SDX (N3): compatibilidad con cifrado en un dispositivo**Citrix ADC MPX/SDX (N3)
- Dispositivo**Citrix ADC MPX/SDX Intel Coleto: compatibilidad con cifrado en un dispositivo**basado en chip Citrix ADC MPX/SDX Intel Coleto SSL
- **Dispositivo Citrix ADC VPX**: compatibilidad con cifrado en un dispositivo Citrix ADC VPX
- Dispositivo**FIPS Citrix ADC MPX/SDX 14000: compatibilidad con cifrado en un dispositivo**FIPS Citrix ADC MPX/SDX 14000
- **HSM externo (Thales/Safenet)**: cifrado compatible con un HSM externo (Thales/Safenet)
- Dispositivo**Citrix ADC MPX/SDX (N2): compatibilidad con cifrado en un dispositivo**Citrix ADC MPX/SDX (N2)
- **Dispositivo FIPS Citrix ADC MPX 9700**: compatibilidad con cifrado en un Citrix ADC MPX 9700 FIPS con firmware 2.2
- Dispositivos**FIPS y MPX FIPS Citrix ADC VPX: compatibilidad con cifrado en dispositivos**certificados Citrix ADC VPX FIPS y MPX FIPS

> **Nota:**
>
> Para obtener compatibilidad con cifrado DTLS, consulte Compatibilidad con cifrado DTLS en dispositivos Citrix ADC VPX, MPX y SDX.

Tabla1: Soporte en servidor virtual/servicio frontend/servicio interno:

Protocolo/plataforma	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX 9700* FIPS con firmware 2.2	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
TLS 1.3	13.1 todas las compilaciones	13.1 todas las compilaciones	13.1 todas las compilaciones	No se admite	No se admite	13.1 todas las compilaciones
	13.0 todas las compilaciones	13.0 todas las compilaciones	13.0 todas las compilaciones	No se admite	No se admite	13.0 todas las compilaciones
	12.1-50.x	12.1-50.x	12.1-50.x	No se admite	No se admite	12.1-50.x
TLS 1.1/1.2	13.1 todas las compilaciones	13.1 todas las compilaciones	13.1 todas las compilaciones	13.1 todas las compilaciones	13.1 todas las compilaciones	13.1 todas las compilaciones
	13.0 todas las compilaciones	13.0 todas las compilaciones	13.0 todas las compilaciones	13.0 todas las compilaciones	13.0 todas las compilaciones	13.0 todas las compilaciones
	12.1 todas las compilaciones	12.1 todas las compilaciones	12.1 todas las compilaciones	12.1 todas las compilaciones	12.1 todas las compilaciones	12.1 todas las compilaciones para MPX 5900/8900, 12.1-50.x para MPX 15000-50G y MPX 26000-100G

Protocolo/plataforma	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX 9700* FIPS con firmware 2.2	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
	12.0 todas las compila-ciones	12.0 todas las compila-ciones	12.0 todas las compila-ciones	12.0 todas las compila-ciones	12.0 todas las compila-ciones	12.0 todas las compila-ciones para MPX 5900/8900, 12.0-57.x para MPX 15000-50G, 12.0-60.x para MPX 26000-100G
	11.1 todas las compila-ciones	11.1 todas las compila-ciones	11.1 todas las compila-ciones	11.1 todas las compila-ciones	11.1 todas las compila-ciones	11.1—56.x para MPX 5900/8900 y MPX 15000-50G, 11.1-60.x para MPX 26000-100G
	11.0 todas las compila-ciones	11.0 todas las compila-ciones	11.0 todas las compila-ciones	11.0 todas las compila-ciones	11.0 todas las compila-ciones	11.0—70.x (solo en MPX 5900/8900)
	10.5 todas las compila-ciones	10.5 todas las compila-ciones	10.5–57.x	10.5 58.1108.e	10,5—59,1359.e	10.5—67.x, 10.5-63.47 (solo en MPX 5900/8900)

Protocolo/plataforma	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX 9700* FIPS con firmware 2.2	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
ECDHE/DHE (ejemplo TLS1-ECDHE-RSA-AES128-SHA)	13.1 todas las compila-ciones	13.1 todas las compila-ciones	13.1 todas las compila-ciones	13.1 todas las compila-ciones	13.1 todas las compila-ciones	13.1 todas las compila-ciones
	13.0 todas las compila-ciones	13.0 todas las compila-ciones	13.0 todas las compila-ciones	13.0 todas las compila-ciones	13.0 todas las compila-ciones	13.0 todas las compila-ciones
	12.1 todas las compila-ciones	12.1 todas las compila-ciones	12.1 todas las compila-ciones	12.1 todas las compila-ciones	12.1 todas las compila-ciones	12.1 todas las compila-ciones para MPX 5900/8900, 12.1-50.x para MPX 15000-50G y MPX 26000-100G

Protocolo/plataforma	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX 9700* FIPS con firmware 2.2	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
	12.0 todas las compila-ciones	12.0 todas las compila-ciones	12.0 todas las compila-ciones	12.0 todas las compila-ciones	12.0 todas las compila-ciones	12.0 todas las compila-ciones para MPX 5900/8900, 12.0-57.x para MPX 15000-50G, 12.0-60.x para MPX 26000-100G
	11.1 todas las compila-ciones	11.1 todas las compila-ciones	11.1 todas las compila-ciones	11.1 todas las compila-ciones	11.1—51.x	11.1—56.x para MPX 5900/8900 y MPX 15000-50G, 11.1-60.x para MPX 26000-100G
	11.0 todas las compila-ciones	11.0 todas las compila-ciones	11.0 todas las compila-ciones			11.0—70.114 (solo en MPX 5900/8900)
	10,5—53,x	10,5—53,x	10.5 todas las compila-ciones	10,5—59,1306.e		10.5—67.x, 10.5-63.47 (solo en MPX 5900/8900)

Protocolo/plataforma	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX 9700* FIPS con firmware 2.2	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
AES-GCM (ejemplo TLS1.2-AES128-GCM-SHA256)	13.1 todas las compilaciones	13.1 todas las compilaciones	13.1 todas las compilaciones	13.1 todas las compilaciones	13.1 todas las compilaciones	13.1 todas las compilaciones
	13.0 todas las compilaciones	13.0 todas las compilaciones	13.0 todas las compilaciones	13.0 todas las compilaciones	13.0 todas las compilaciones	13.0 todas las compilaciones
	12.1 todas las compilaciones	12.1 todas las compilaciones	12.1 todas las compilaciones	12.1 todas las compilaciones	12.1 todas las compilaciones	12.1 todas las compilaciones para MPX 5900/8900, 12.1-50.x para MPX 15000-50G y MPX 26000-100G
	12.0 todas las compilaciones	12.0 todas las compilaciones	12.0 todas las compilaciones	12.0 todas las compilaciones	12.0 todas las compilaciones	12.0 todas las compilaciones para MPX 5900/8900, 12.0-57.x para MPX 15000-50G, 12.0-60.x para MPX 26000-100G

Protocolo/plataforma	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX 9700* FIPS con firmware 2.2	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
	11.1 todas las compila-ciones	11.1 todas las compila-ciones	11.1 todas las compila-ciones	11.1—51.x (ver nota)	11.1—51.x (ver nota)	11.1—56.x para MPX 5900/8900 y MPX 15000-50G, 11.1-60.x para MPX 26000-100G
	11.0 todas las compila-ciones	11.0 todas las compila-ciones	11.0—66.x			11.0—70.114 (solo en MPX 5900/8900)
	10,5—53,x	10,5—53,x				10.5—67.x, 10.5-63.47 (solo en MPX 5900/8900)
Cifrados SHA-2 (ejemplo TLS1.2-AES-128-SHA256)	13.1 todas las compila-ciones	13.1 todas las compila-ciones	13.1 todas las compila-ciones	13.1 todas las compila-ciones	13.1 todas las compila-ciones	13.1 todas las compila-ciones
	13.0 todas las compila-ciones	13.0 todas las compila-ciones	13.0 todas las compila-ciones	13.0 todas las compila-ciones	13.0 todas las compila-ciones	13.0 todas las compila-ciones

Protocolo/plataforma	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX 9700* FIPS con firmware 2.2	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
	12.1 todas las compilaciones	12.1 todas las compilaciones	12.1 todas las compilaciones	12.1 todas las compilaciones	12.1 todas las compilaciones	12.1 todas las compilaciones para MPX 5900/8900, 12.1-50.x para MPX 15000-50G y MPX 26000-100G
	12.0 todas las compilaciones	12.0 todas las compilaciones	12.0 todas las compilaciones	12.0 todas las compilaciones	12.0 todas las compilaciones	12.0 todas las compilaciones para MPX 5900/8900, 12.0-57.x para MPX 15000-50G, 12.0-60.x para MPX 26000-100G
	11.1 todas las compilaciones	11.1 todas las compilaciones	11.1 todas las compilaciones	11.1—52.x	11.1—52.x	11.1—56.x para MPX 5900/8900 y MPX 15000-50G, 11.1-60.x para MPX 26000-100G

Protocolo/plataforma	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX 9700* FIPS con firmware 2.2	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
	11.0 todas las compila-ciones	11.0 todas las compila-ciones	11.0—66.x			11.0—72.x, 11.0-70.114 (solo en MPX 5900/8900)
	10,5—53,x	10,5—53,x				10.5—67.x, 10.5-63.47 (solo en MPX 5900/8900)
ECDSA (ejemplo TLS1-ECDHE-ECDSA-AES256-SHA)	No se admite	13.1 todas las compila-ciones	13.1 todas las compila-ciones	13.1 todas las compila-ciones	13.1 todas las compila-ciones	13.1 todas las compila-ciones
	No se admite	13.0 todas las compila-ciones	13.0 todas las compila-ciones	13.0 todas las compila-ciones	13.0 todas las compila-ciones	13.0 todas las compila-ciones
	No se admite	12.1 todas las compila-ciones	12.1 todas las compila-ciones	12.1 todas las compila-ciones	12.1 todas las compila-ciones	12.1 todas las compila-ciones para MPX 5900/8900, 12.1-50.x para MPX 15000-50G y MPX 26000-100G

Protocolo/plataforma	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX 9700* FIPS con firmware 2.2	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
	No se admite	12.0 todas las compilaciones	12.0—57.x	No aplicable	No se admite	12.0 todas las compilaciones para MPX 5900/8900, 12.0-57.x para MPX 15000-50G, 12.0-60.x para MPX 26000-100G
		11.1 todas las compilaciones				11.1—56.x, 11.1-54.126 (solo se admiten las curvas ECC P_256 y P_384).
CHACHA20	No se admite	13.1 todas las compilaciones	13.1 todas las compilaciones	No se admite	No se admite	13.1 todas las compilaciones
	No se admite	13.0 todas las compilaciones	13.0 todas las compilaciones	No se admite	No se admite	13.0 todas las compilaciones
	No se admite	No se admite	12.1 todas las compilaciones	No se admite	No se admite	12.1-49.x (solo en MPX 5900/8900)
	No se admite	No se admite	12.0—56.x	No se admite	No se admite	No se admite

Tabla 2: Soporte en servicios de backend:

TLS 1.3 no se admite en el back-end.

Protocolo/plataforma	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX 9700* FIPS con firmware 2.2	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
TLS 1.1/1.2	13.1 todas las compilaciones	13.1 todas las compilaciones	13.1 todas las compilaciones	13.1 todas las compilaciones	13.1 todas las compilaciones	13.1 todas las compilaciones
	13.0 todas las compilaciones	13.0 todas las compilaciones	13.0 todas las compilaciones	13.0 todas las compilaciones	13.0 todas las compilaciones	13.0 todas las compilaciones
	12.1 todas las compilaciones	12.1 todas las compilaciones	12.1 todas las compilaciones	12.1 todas las compilaciones	12.1 todas las compilaciones	12.1 todas las compilaciones para MPX 5900/8900, 12.1-50.x para MPX 15000-50G y MPX 26000-100G
	12.0 todas las compilaciones	12.0 todas las compilaciones	12.0 todas las compilaciones	12.0 todas las compilaciones	12.0 todas las compilaciones	12.0 todas las compilaciones para MPX 5900/8900, 12.0-57.x para MPX 15000-50G, 12.0-60.x para MPX 26000-100G

Protocolo/plataforma	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX 9700* FIPS con firmware 2.2	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
	11.1 todas las compila-ciones	11.1 todas las compila-ciones	11.1 todas las compila-ciones	11.1 todas las compila-ciones	11.1 todas las compila-ciones	11.1—56.x para MPX 5900/8900 y MPX 15000-50G, 11.1-60.x para MPX 26000-100G
	11.0—50.x	11.0—50.x	11.0—66.x	11.0 todas las compila-ciones		11.0—70.119 (solo en MPX 5900/8900)
	10.5—59.x	10.5—59.x		10.5–58.1108.e	10,5—59,1359.e	10.5—67.x, 10.5-63.47 (solo en MPX 5900/8900)
ECDHE/DHE (ejemplo TLS1-ECDHE-RSA-AES128-SHA)	13.1 todas las compila-ciones	13.1 todas las compila-ciones	13.1 todas las compila-ciones	13.1 todas las compila-ciones	13.1 todas las compila-ciones	13.1 todas las compila-ciones
	13.0 todas las compila-ciones	13.0 todas las compila-ciones	13.0 todas las compila-ciones	13.0 todas las compila-ciones	13.0 todas las compila-ciones	13.0 todas las compila-ciones

Protocolo/plataforma	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX 9700* FIPS con firmware 2.2	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
	12.1 todas las compilaciones	12.1 todas las compilaciones	12.1 todas las compilaciones	12.1 todas las compilaciones	12.1 todas las compilaciones	12.1 todas las compilaciones para MPX 5900/8900, 12.1-50.x para MPX 15000-50G y MPX 26000-100G
	12.0 todas las compilaciones	12.0 todas las compilaciones	12.0—56.x	12.0 todas las compilaciones	12.0 todas las compilaciones	12.0 todas las compilaciones para MPX 5900/8900, 12.0-57.x para MPX 15000-50G, 12.0-60.x para MPX 26000-100G
	11.1 todas las compilaciones	11.1 todas las compilaciones		11.1 todas las compilaciones	11.1—51.x	11.1—56.x para MPX 5900/8900 y MPX 15000-50G, 11.1-60.x para MPX 26000-100G

Protocolo/plataforma	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX 9700* FIPS con firmware 2.2	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
	11.0—50.x	11.0—50.x				11.0—70.119 (solo en MPX 5900/8900)
	10.5—58.x	10.5—58.x		10,5—59,1306.e		10.5—67.x, 10.5-63.47 (solo en MPX 5900/8900)
AES-GCM (ejemplo TLS1.2-AES128-GCM-SHA256)	13.1 todas las compila-ciones	13.1 todas las compila-ciones	13.1 todas las compila-ciones	13.1 todas las compila-ciones	13.1 todas las compila-ciones	13.1 todas las compila-ciones
	13.0 todas las compila-ciones	13.0 todas las compila-ciones	13.0 todas las compila-ciones	13.0 todas las compila-ciones	13.0 todas las compila-ciones	13.0 todas las compila-ciones
	12.1 todas las compila-ciones	12.1 todas las compila-ciones	12.1 todas las compila-ciones	12.1 todas las compila-ciones	12.1 todas las compila-ciones	12.1 todas las compila-ciones para MPX 5900/8900, 12.1-50.x para MPX 15000-50G y MPX 26000-100G

Protocolo/plataforma	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX 9700* FIPS con firmware 2.2	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
	12.0 todas las compila-ciones	12.0 todas las compila-ciones	No se admite	12.0 todas las compila-ciones	12.0 todas las compila-ciones	12.0 todas las compila-ciones para MPX 5900/8900, 12.0-57.x para MPX 15000-50G, 12.0-60.x para MPX 26000-100G
	11.1 todas las compila-ciones	11.1 todas las compila-ciones		11.1—51.x	11.1—51.x	11.1—56.x para MPX 5900/8900 y MPX 15000-50G, 11.1-60.x para MPX 26000-100G
Cifrados SHA-2 (ejemplo TLS1.2-AES-128-SHA256)	13.1 todas las compila-ciones	13.1 todas las compila-ciones	13.1 todas las compila-ciones	13.1 todas las compila-ciones	13.1 todas las compila-ciones	13.1 todas las compila-ciones
	13.0 todas las compila-ciones	13.0 todas las compila-ciones	13.0 todas las compila-ciones	13.0 todas las compila-ciones	13.0 todas las compila-ciones	13.0 todas las compila-ciones

Protocolo/plataforma	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX 9700* FIPS con firmware 2.2	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
	12.1 todas las compilaciones	12.1 todas las compilaciones	12.1 todas las compilaciones	12.1 todas las compilaciones	12.1 todas las compilaciones	12.1 todas las compilaciones para MPX 5900/8900, 12.1-50.x para MPX 15000-50G y MPX 26000-100G
	12.0 todas las compilaciones	12.0 todas las compilaciones	No se admite	12.0 todas las compilaciones	12.0 todas las compilaciones	12.0 todas las compilaciones para MPX 5900/8900, 12.0-57.x para MPX 15000-50G, 12.0-60.x para MPX 26000-100G
	11.1 todas las compilaciones	11.1 todas las compilaciones		11.1—52.x	11.1—52.x	11.1—56.x para MPX 5900/8900 y MPX 15000-50G, 11.1-60.x para MPX 26000-100G

Protocolo/plataforma	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX 9700* FIPS con firmware 2.2	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
ECDSA (ejemplo TLS1-ECDHE-ECDSA-AES256-SHA)	No se admite	13.1 todas las compila-ciones	13.1 todas las compila-ciones	13.1 todas las compila-ciones	13.1 todas las compila-ciones	13.1 todas las compila-ciones
	No se admite	13.0 todas las compila-ciones	13.0 todas las compila-ciones	13.0 todas las compila-ciones	13.0 todas las compila-ciones	13.0 todas las compila-ciones
	No se admite	12.1 todas las compila-ciones	12.1 todas las compila-ciones	12.1 todas las compila-ciones	12.1 todas las compila-ciones	12.1 todas las compila-ciones para MPX 5900/8900, 12.1-50.x para MPX 15000-50G y MPX 26000-100G

Protocolo/plataforma	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX 9700* FIPS con firmware 2.2	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
	No se admite	12.0 todas las compilaciones	12.0–57.x	No aplicable	No se admite	12.0 todas las compilaciones para MPX 5900/8900, 12.0-57.x para MPX 15000-50G, 12.0-60.x para MPX 26000-100G
		11.1—51.x		No aplicable		11.1—56.x para MPX 5900/8900 y MPX 15000-50G, 11.1-60.x para MPX 26000-100G (solo se admiten las curvas ECC P_256 y P_384).
CHACHA20	No se admite	13.1 todas las compilaciones	13.1 todas las compilaciones	No se admite	No se admite	13.1 todas las compilaciones
	No se admite	13.0 todas las compilaciones	13.0 todas las compilaciones	No se admite	No se admite	13.0 todas las compilaciones

Protocolo/plataforma	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX 9700* FIPS con firmware 2.2	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
	No se admite	No se admite	12.1 todas las compila-ciones	No se admite	No se admite	12.1-49.x para MPX 5900/8900, 12.1-50.x para MPX 15000-50G y MPX 26000-100G
	No se admite	No se admite	12.0—56.x	No se admite	No se admite	No se admite

Para obtener la lista detallada de los cifrados ECDSA compatibles, consulte Compatibilidad con ECDSA Cipher Suites.

> Nota
>
> - El conjunto de cifrado TLS-Fallback_SCSV se admite en todos los dispositivos desde la versión 10.5 compilación 57.x
> - La compatibilidad con HTTP Strict Transport Security (HSTS) se basa en directivas.
> - Todos los certificados firmados SHA-2 (SHA256, SHA384, SHA512) se admiten en el front-end de todos los dispositivos. En la versión 11.1 compilación 54.x y posteriores, estos certificados también se admiten en el back-end de todos los dispositivos. En la versión 11.0 y anteriores, solo los certificados firmados SHA256 se admiten en el back-end de todos los dispositivos.
> - En la versión 11.1 compilación 52.x y versiones anteriores, los siguientes cifrados solo se admiten en el front-end de los dispositivos FIPS MPX 9700 y MPX/SDX 14000:
>   - TLS1.2-ECDHE-RSA-AES-256-SHA384
>   - TLS1.2-ECDHE-RSA-AES256-GCM-SHA384 From release 11.1 build 53.x, and in release 12.0, these ciphers are also supported on the back end.
> - Todos los cifrados ChaCha20-Poly1035 utilizan una función pseudo aleatoria TLS (PSF) con

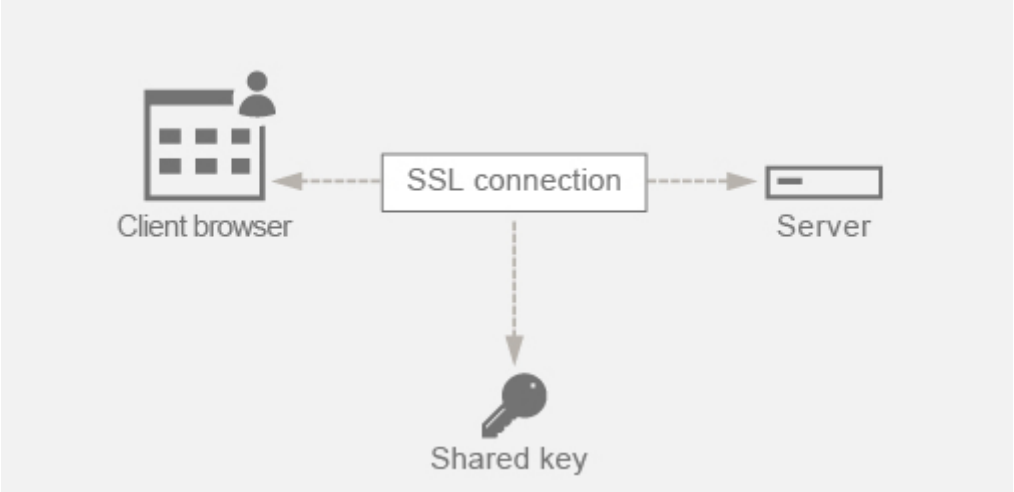
> la función hash SHA-256.

Secrecía de avance perfecto (PFS)

Perfect Forward Secrecy garantiza la protección de las comunicaciones SSL actuales incluso si la clave de sesión de un servidor web se ve comprometida en un momento posterior.

¿Por qué necesitas Perfect Forward Secrecy (PFS)?

Se utiliza una conexión SSL para proteger los datos que se transmiten entre un cliente y un servidor. Esta conexión comienza con el protocolo de enlace SSL que tiene lugar entre el explorador web de un cliente y el servidor web contactado. Durante este apretón de manos, el explorador y el servidor intercambian cierta información para llegar a una clave de sesión que sirve de medio para cifrar los datos durante el resto de la comunicación.

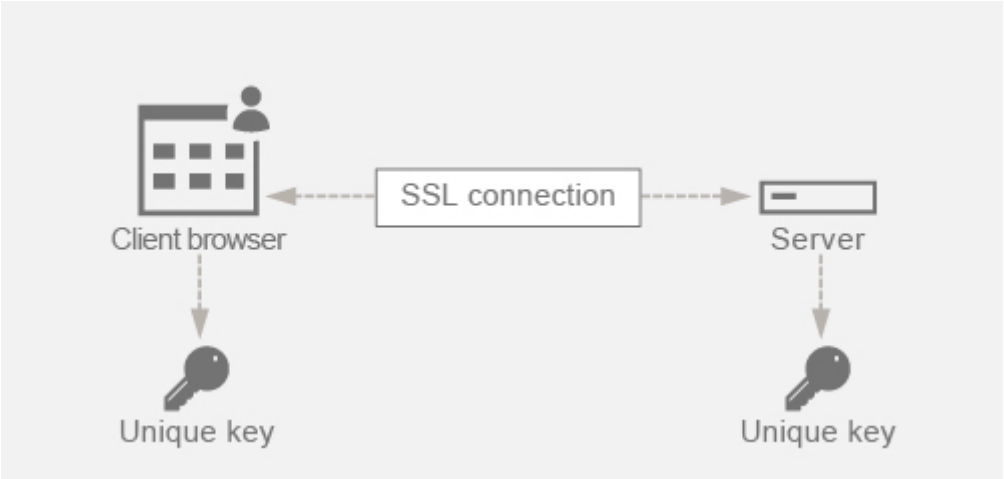


RSA es el algoritmo más utilizado para el intercambio de claves. El explorador web utiliza la clave pública del servidor para cifrar y enviar el secreto premaestro a un servidor. Este secreto previo al maestro se utiliza para llegar a la clave de sesión. El problema en el enfoque de intercambio de claves RSA es que si un atacante logra obtener la clave privada del servidor en cualquier momento en el futuro, el atacante obtiene el secreto premaestro con el que se puede obtener la clave de sesión. Ahora el atacante puede usar esta clave de sesión para descifrar todas las conversaciones SSL. Como resultado, su comunicación SSL histórica que antes era segura ya no es segura porque la clave privada robada del servidor se puede usar para llegar a la clave de sesión y, por lo tanto, descifrar cualquier conversación histórica guardada también.

La necesidad es poder proteger la comunicación SSL pasada incluso si la clave privada del servidor se ha visto comprometida. La configuración de Perfect Forward Secrecy (PFS) ayuda a solucionar este problema.

¿Cómo ayuda PFS?

PFS protege la comunicación SSL anterior haciendo que el cliente y el servidor acuerden una nueva clave para cada sesión y manteniendo en secreto el cálculo de esta clave de sesión. Funciona sobre la base de que el compromiso de una clave de servidor no debe dar lugar a comprometer la clave de sesión. La clave de sesión se deriva por separado en ambos extremos y nunca se transfiere a través del cable. Las claves de sesión también se destruyen una vez finalizada la comunicación. Estos hechos garantizan que, incluso si alguien obtiene acceso a la clave privada del servidor, no pueda llegar a la clave de sesión. Por lo tanto, no podrían descifrar los datos anteriores.



Explicación con ejemplo

Supongamos que estamos mediante DHE para obtener PFS. El algoritmo DH garantiza que, aunque un hacker obtenga la clave privada del servidor, el hacker no pueda llegar a la clave de sesión. La razón es que la clave de sesión y los números aleatorios (utilizados para llegar a la clave de sesión) se mantienen en secreto en ambos extremos y nunca se intercambian por cable.
El PFS se puede lograr mediante el intercambio de claves Ephemeral Diffie-Hellman, que crea nuevas claves temporales para cada sesión SSL.

La otra cara de crear una clave para cada sesión es que requiere un cálculo adicional. Sin embargo, este problema se puede superar mediante el uso de la curva elíptica, que tiene tamaños de clave más pequeños.

Configuración de PFS en el dispositivo Citrix ADC

PFS se puede configurar en un Citrix ADC configurando los cifrados DHE o ECDHE. Estos cifrados garantizan que la clave de sesión secreta creada no se comparta en el cable (algoritmo DH) y que la clave de sesión permanezca activa solo durante un breve período de tiempo (efímero). Ambas configuraciones se explican en las secciones siguientes.

Nota: El uso de cifrados ECDHE en lugar de DHE hace que la comunicación sea más segura con tamaños de clave más pequeños.

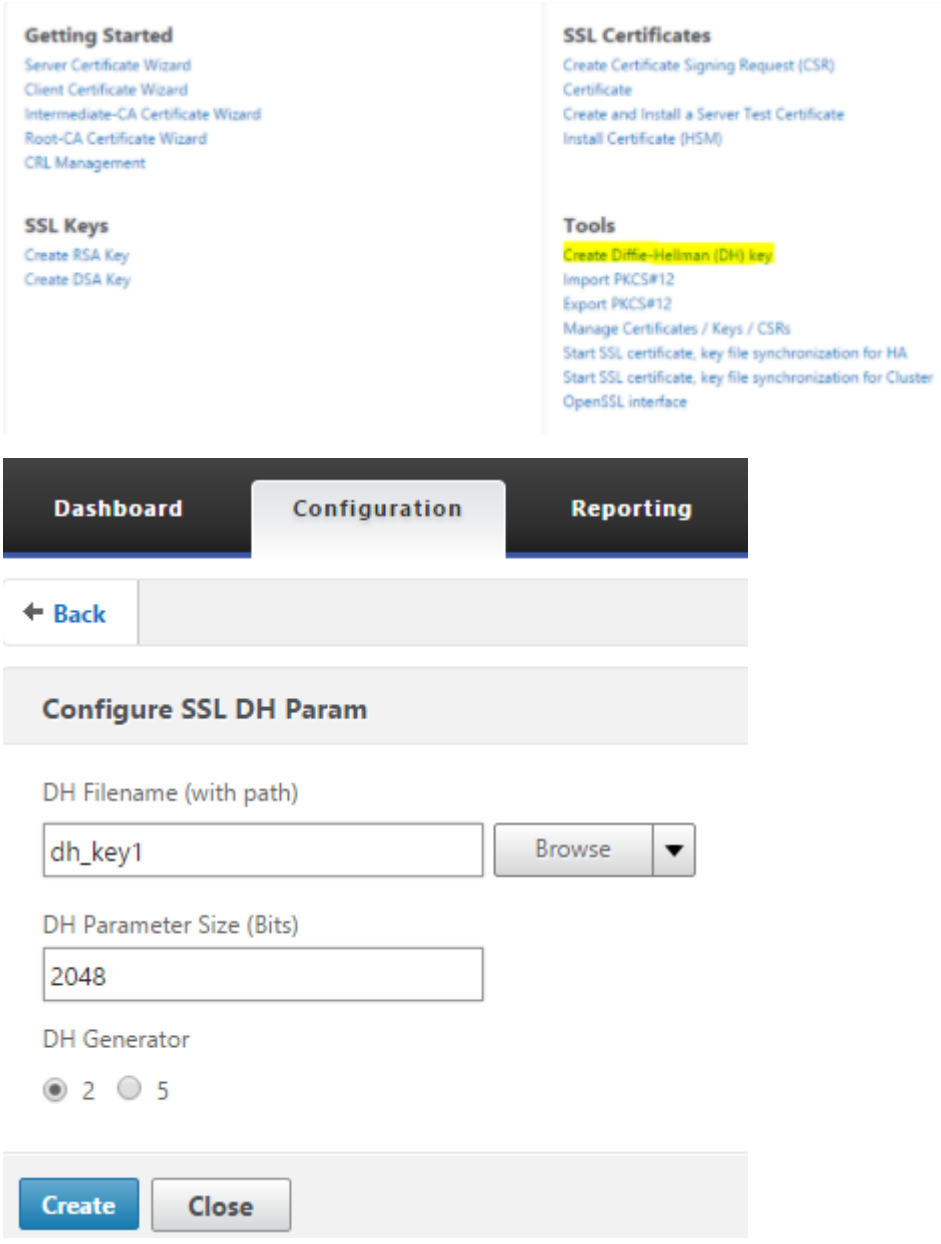
Configurar DHE mediante la GUI

1. Genere una clave DH.

   a. Vaya a **Administración del tráfico > SSL > Herramientas**.

   b. Haga clic en **Crear clave Helman Diffie (DH)**.

   Nota: La generación de una clave DH de 2048 bits puede tardar hasta 30 minutos.

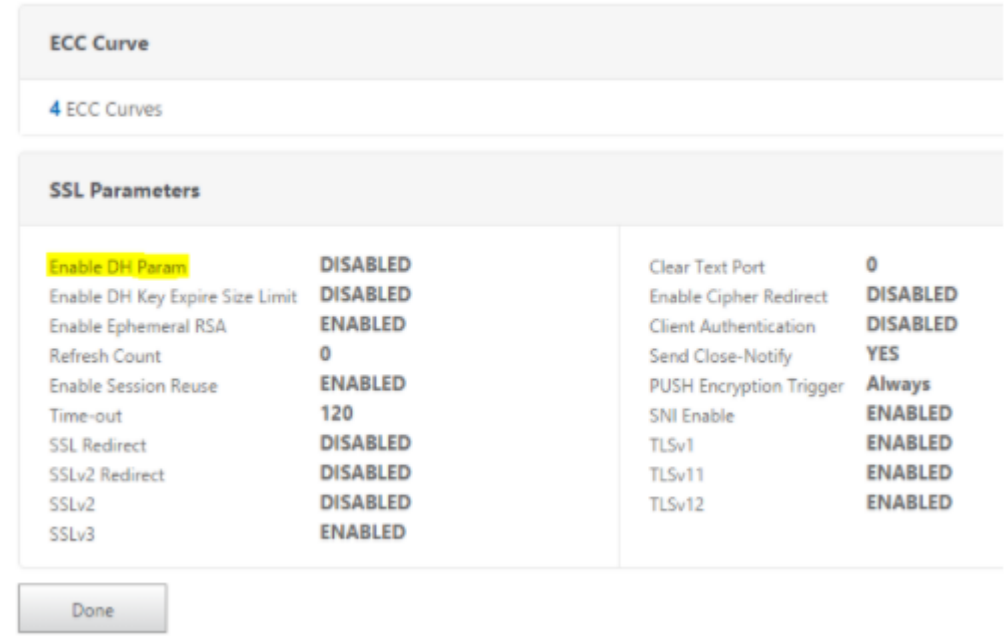


2. Habilite DH Param para el servidor virtual SSL y adjunte la clave DH al servidor virtual SSL.

   a. Vaya a **Configuración > Administración del tráfico > Servidores virtuales**.

   b. Seleccione el servidor virtual en el que quiere habilitar DH.

   c. Haga clic en **Modificar**, en **Parámetros SSL**y, a continuación, en **Habilitar parámetro DH**.



3. Enlazar los cifrados DHE al servidor virtual.

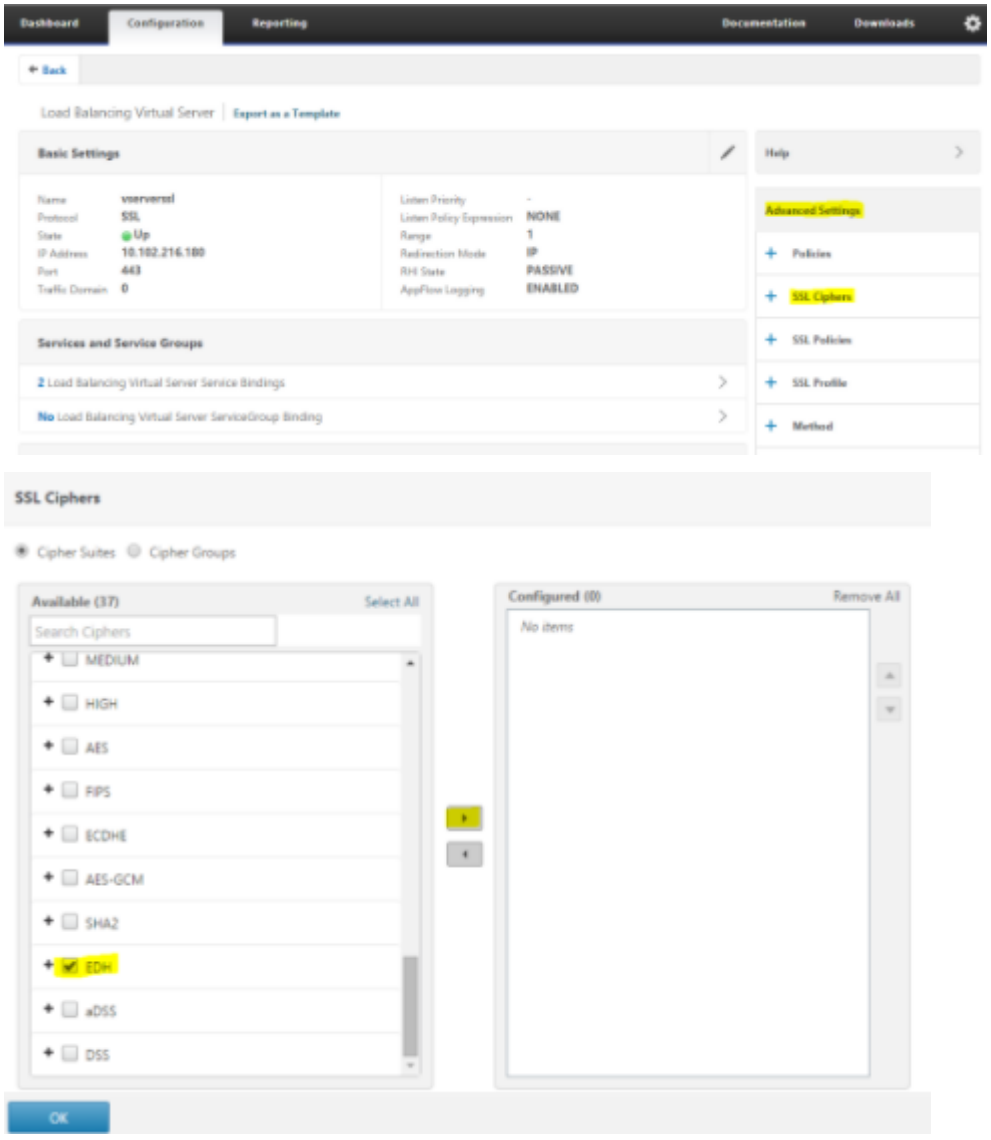
   a. Vaya a **Configuración > Administración del tráfico > Servidores virtuales**.

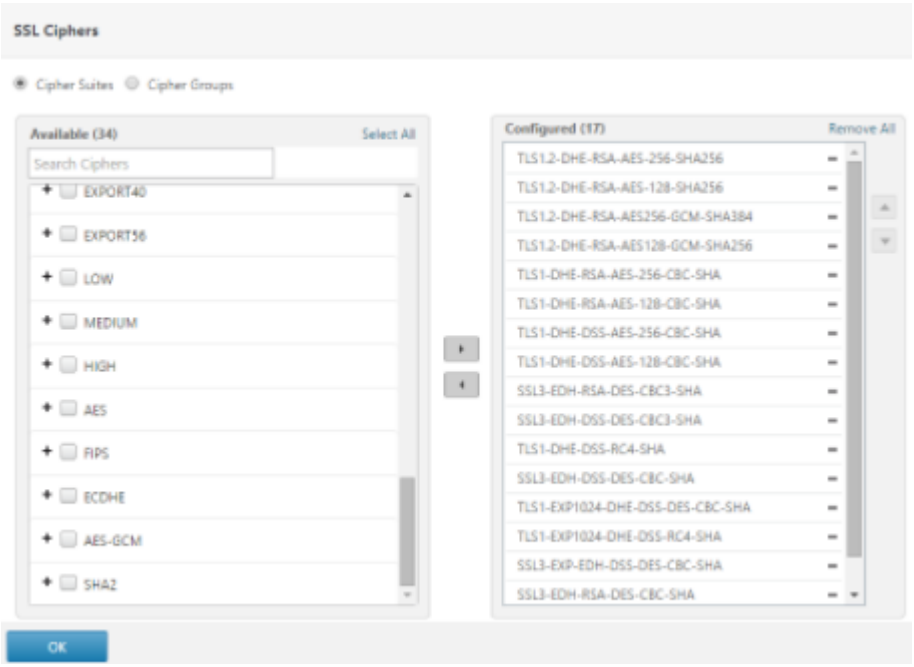
   b. Seleccione el servidor virtual en el que quiere habilitar DH y haga clic en el icono del lápiz

para modificarlo.

c. En **Configuración avanzada**, haga clic en el icono más junto a **Cifrados SSL** y seleccione los grupos de cifrado DHE y haga clic en **Aceptar** para vincular.

Nota: Asegúrese de que los cifrados DHE estén en la parte superior de la lista de cifrado enlazada al servidor virtual.





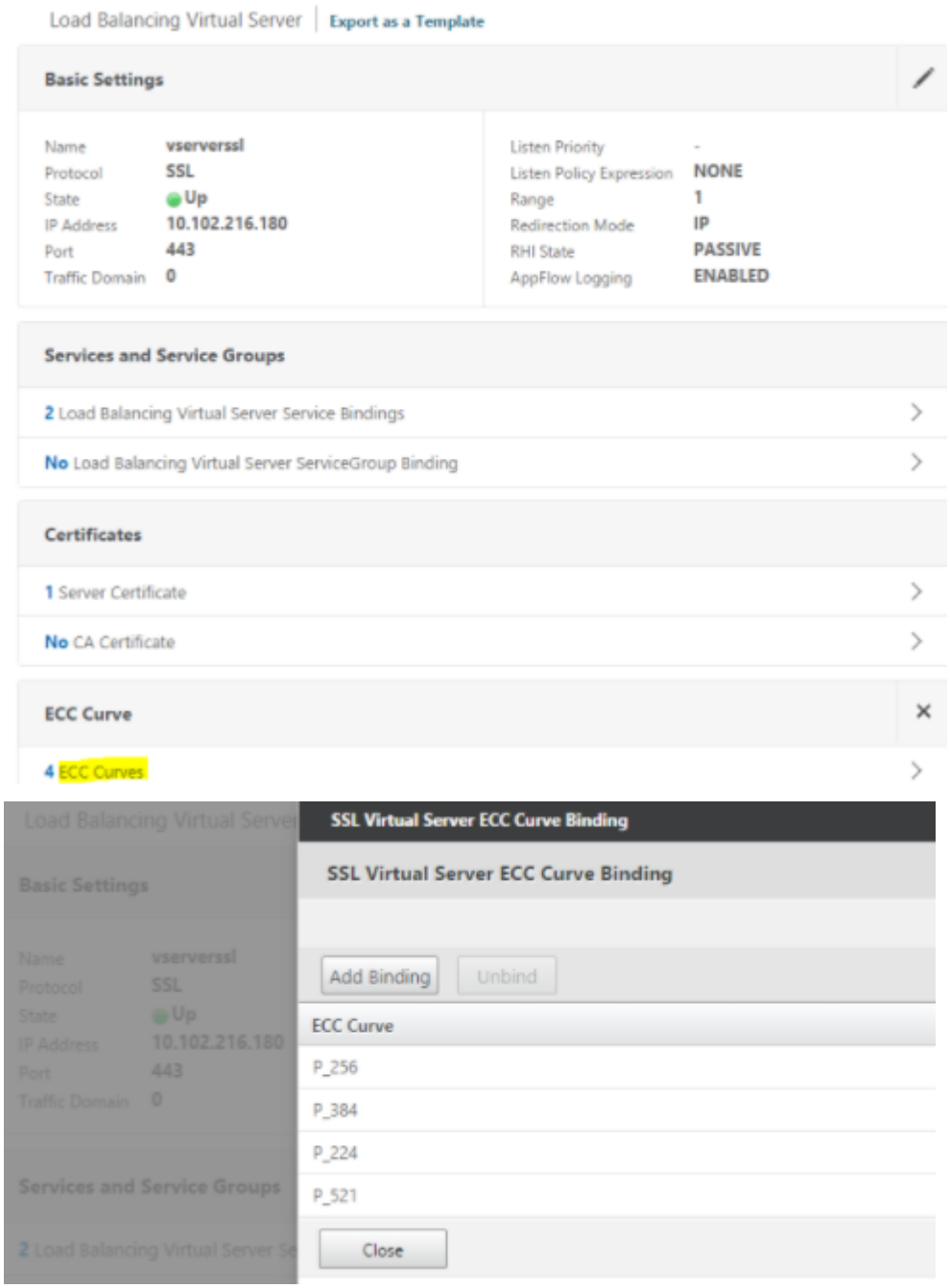
Configurar ECDHE mediante la GUI

1. Enlazar las curvas ECC al servidor virtual SSL.

   a. Vaya a **Configuración > Administración del tráfico > Equilibrio de carga > Servidores virtuales**.

   b. Seleccione el servidor virtual SSL que quiere modificar, haga clic en **Curva ECC** y, a continuación, en **Agregar enlace**.

   c. Enlazar la curva ECC requerida al servidor virtual.

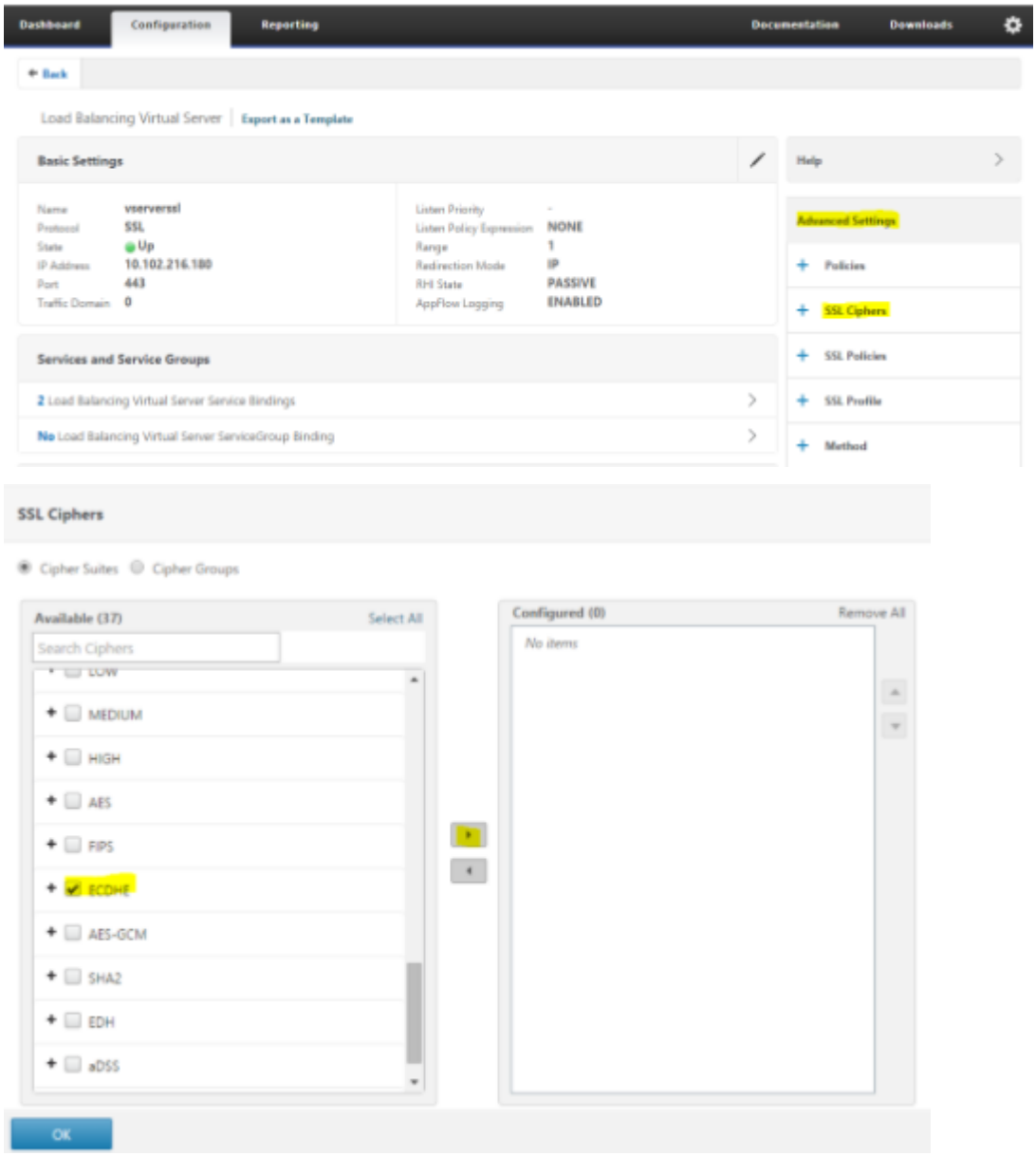


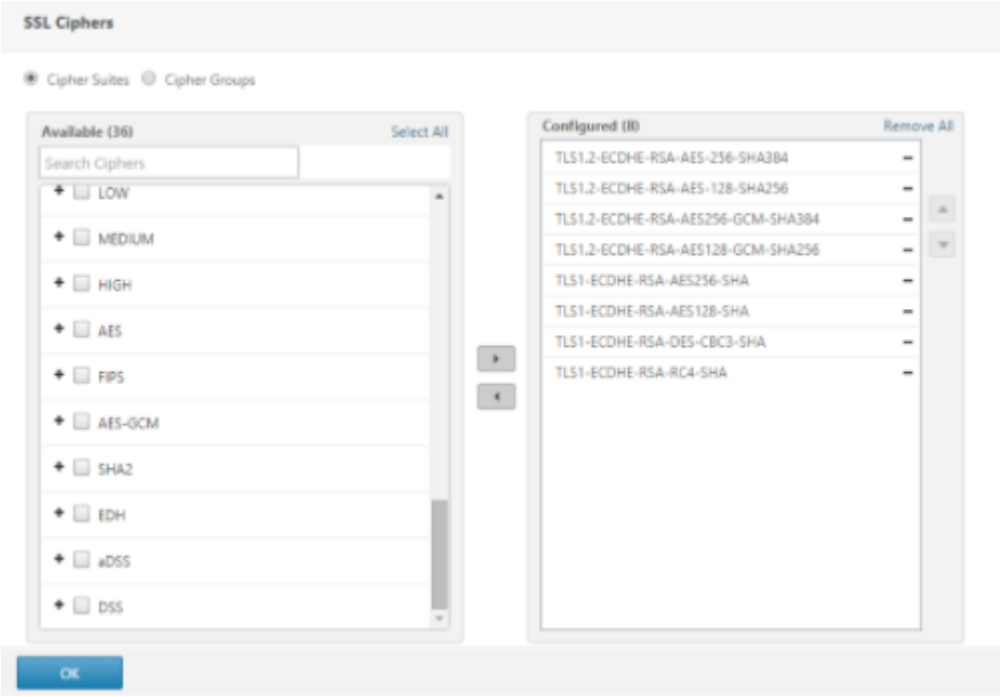
2. Enlazar los cifrados ECDHE al servidor virtual.

   a. Vaya a **Configuración > Administración del tráfico > Servidores virtuales** y seleccione el servidor virtual en el que quiere habilitar DH.

   b. Haga clic en **Modificar > Cifrados SSL**, seleccione los grupos de cifrado ECDHE y haga clic en **Enlazar**.

   Nota: Asegúrese de que los cifrados ECDHE estén en la parte superior de la lista de cifrados enlazados al servidor virtual.





Nota: Para cada caso, compruebe que el dispositivo Citrix ADC admite los cifrados que quiere utilizar para la comunicación.

Configurar PFS mediante un perfil SSL

Nota: La opción de configurar PFS (cifrado o ECC) mediante un perfil SSL se introduce a partir de la versión 11.0 64.x en adelante. Ignore la siguiente sección si se encuentra en versiones anteriores.

Para habilitar PFS mediante un perfil SSL, es necesario realizar una configuración similar (como se explica en secciones de configuración anteriores) pero en el perfil SSL en lugar de configurarla directamente en un servidor virtual.

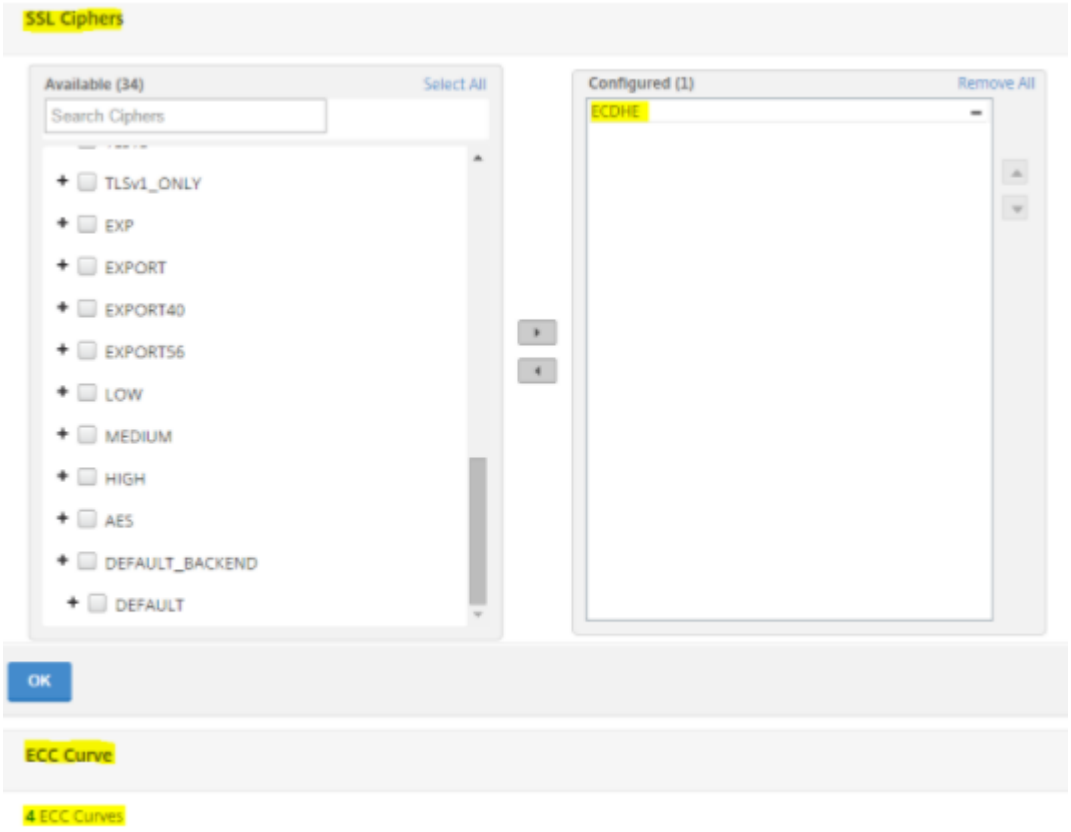
Configurar PFS mediante un perfil SSL mediante la GUI

1. Enlazar las curvas ECC y los cifrados ECDHE en el perfil SSL.

   Nota: Las curvas ECC ya están enlazadas de forma predeterminada a todos los perfiles SSL.

   a. Vaya a **Sistema > Perfiles > Perfiles SSL** y elija el perfil en el que quiere habilitar PFS.

   b. Enlazar los cifrados ECDHE.



2. Enlazar el perfil SSL al servidor virtual.

   a. Vaya a **Configuración > Administración del tráfico > Servidores virtuales** y seleccione el servidor virtual.

   b. Haga clic en el icono del lápiz para modificar el perfil SSL.

   c. Haga clic en **Aceptar** y en **Listo**.

Configurar PFS mediante SSL mediante la CLI

En el símbolo del sistema, escriba:

1. Enlazar curvas ECC al perfil SSL.


```
bind sslprofile <SSLProfileName> -eccCurveName <Name_of_curve>
<!--NeedCopy-->
```

2. Enlazar el grupo de cifrado ECDHE.

```
bind sslprofile <SSLProfileName> cipherName <ciphergroupName>
<!--NeedCopy-->
```

3. Establezca la prioridad del cifrado ECDHE como 1.

```
set sslprofile <SSLProfileName> cipherName <ciphergroupName>
   cipherPriority <positive_integer>
<!--NeedCopy-->
```

4. Enlazar el perfil SSL al servidor virtual.

```
set SSL vserver <vservername> sslProfile <SSLProfileName>
<!--NeedCopy-->
```

Cifras ECDHE

August 20, 2021

Todos los dispositivos Citrix ADC admiten el grupo de cifrado ECDHE en el front-end y el back-end. En un dispositivo SDX, si se asigna un chip SSL a una instancia VPX, se aplica la compatibilidad con cifrado de un dispositivo MPX. De lo contrario, se aplica el soporte de cifrado normal de una instancia VPX.

Para obtener más información sobre las compilaciones y plataformas que admiten estos cifrados, consulte Cifrados disponibles en los dispositivos Citrix ADC.

Los conjuntos de cifrado ECDHE utilizan criptografía de curva elíptica (ECC). Debido a su tamaño de clave más pequeño, ECC es especialmente útil en un entorno móvil (inalámbrico) o en un entorno interactivo de respuesta de voz, donde cada milisegundo es importante. Los tamaños de clave más pequeños ahorran energía, memoria, ancho de banda y costes computacionales.

Un dispositivo Citrix ADC admite las siguientes curvas ECC:

- P_256

- P_384
- P_224
- P_521

Nota: Si actualiza desde una compilación anterior a la versión 10.1, compilación 121.10, debe vincular explícitamente las curvas ECC a los servidores y servicios virtuales SSL existentes. Las curvas están enlazadas de forma predeterminada a todos los servidores y servicios virtuales que cree después de la actualización.

Puede enlazar una curva ECC a entidades frontales y back-end SSL. Por defecto, las cuatro curvas están enlazadas, en el orden siguiente: P_256, P_384, P_224, P_521. Para cambiar el orden, primero debe desenlazar todas las curvas y, a continuación, vincularlas en el orden deseado.

Vincular curvas ECC a un servidor virtual SSL mediante la CLI

En el símbolo del sistema, escriba:

```
bind ssl vserver <vServerName > -eccCurveName <eccCurveName >
```

Ejemplo:

```
bind ssl vserver  v1 -eccCurveName P_224

sh ssl vserver v1

Advanced SSL configuration for VServer v1:
DH: DISABLED
Ephemeral RSA: ENABLED Refresh Count: 0
Session Reuse: ENABLED Timeout: 120 seconds
Cipher Redirect: DISABLED
SSLv2 Redirect: DISABLED
ClearText Port: 0
Client Auth: DISABLED
SSL Redirect: DISABLED
Non FIPS Ciphers: DISABLED
SNI: DISABLED
SSLv2: DISABLED SSLv3: ENABLED TLSv1.0: ENABLED  TLSv1.1: DISABLED
   TLSv1.2: DISABLED
Push Encryption Trigger: Always
Send Close-Notify: YES
ECC Curve: P_224

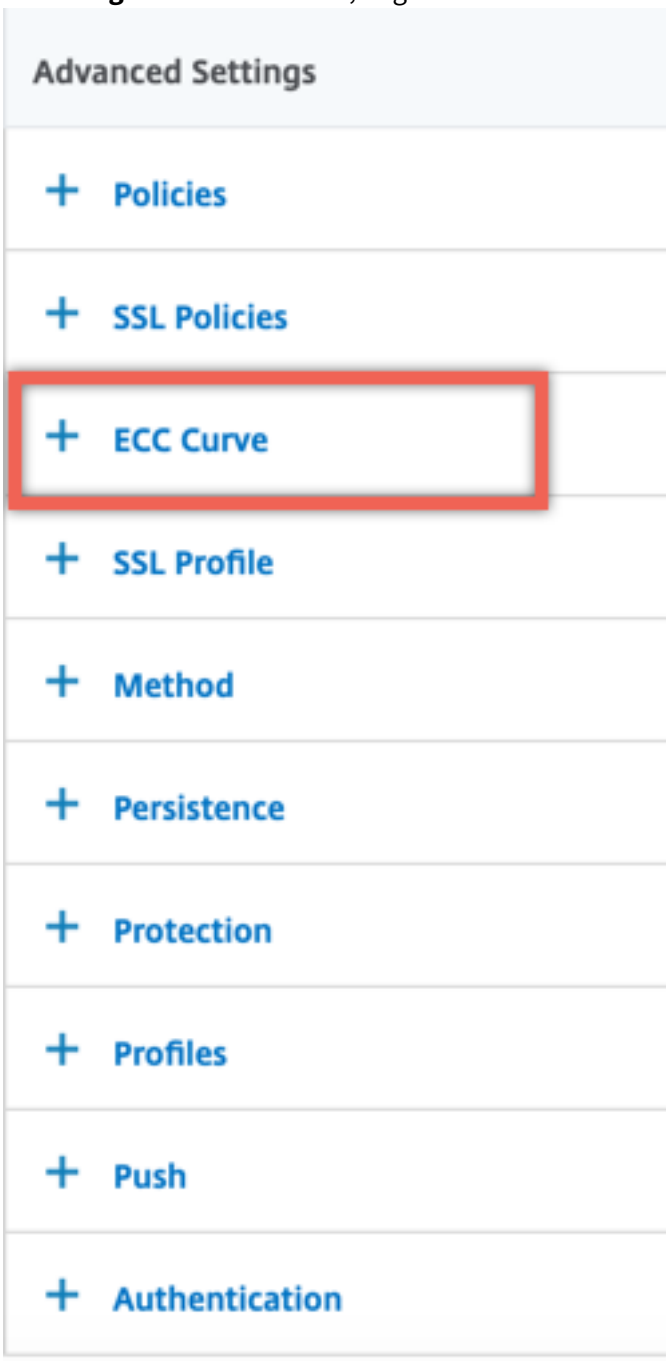
1) Cipher Name: DEFAULT
Description: Predefined Cipher Alias
```



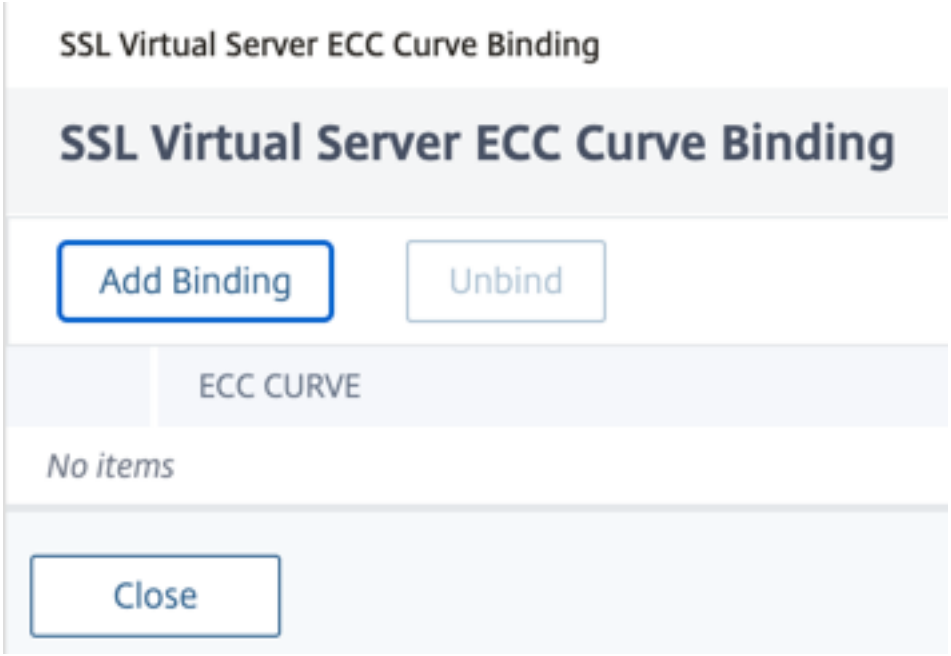
```
Done
<!--NeedCopy-->
```

Enlazar curvas ECC a un servidor virtual SSL mediante la GUI

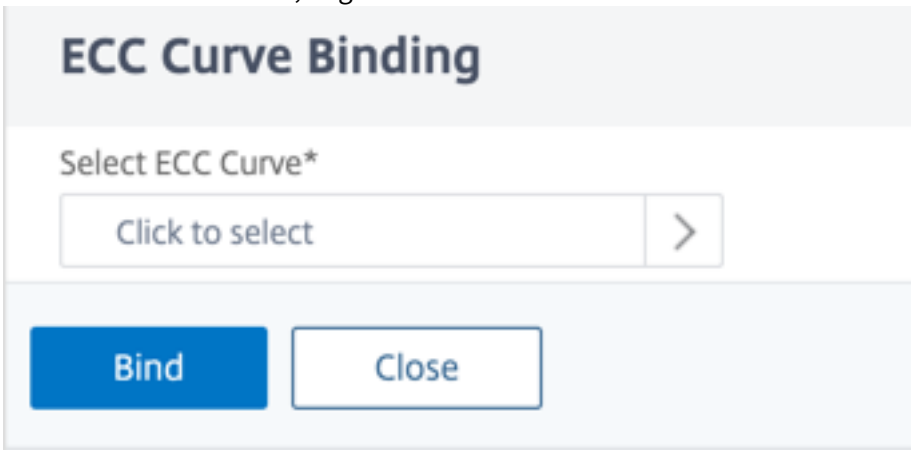
1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. Seleccione un servidor virtual SSL y haga clic en **Modificar**.
3. En **Configuración avanzada**, haga clic en **Curva ECC**.



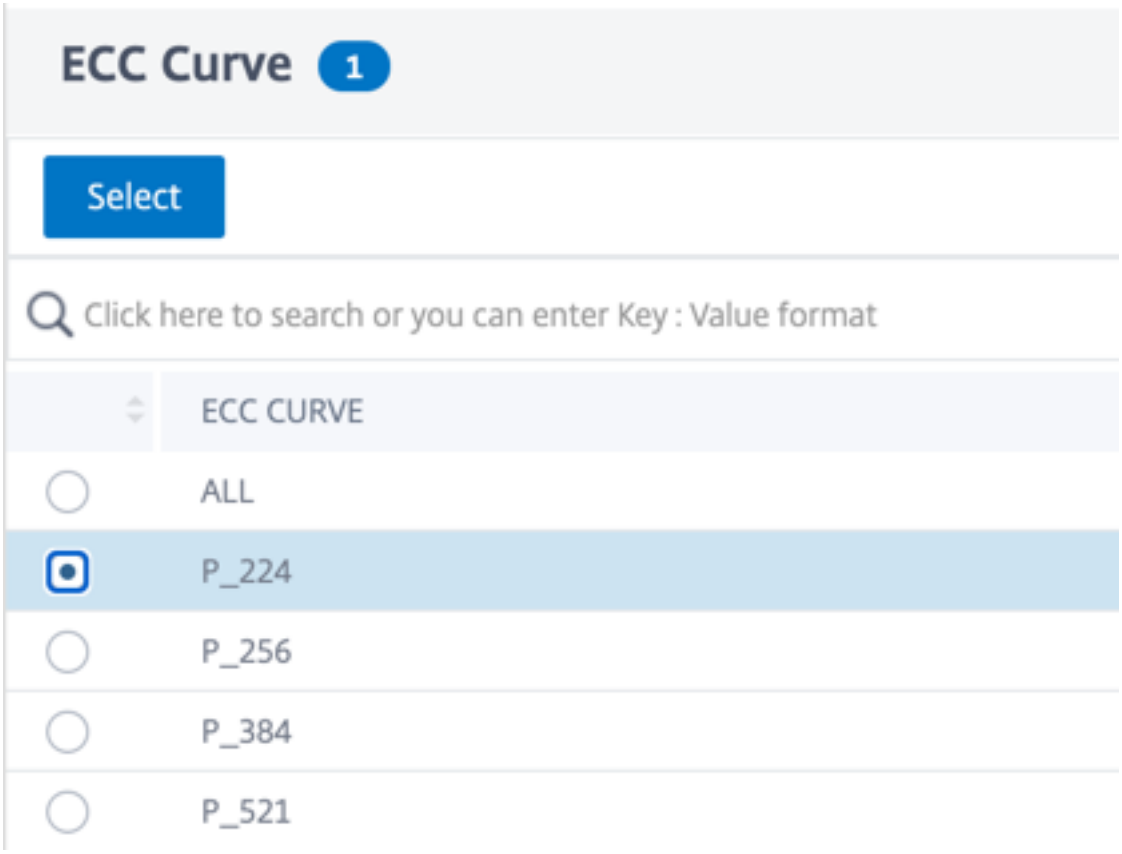
4. Haga clic dentro de la sección de curva ECC.
5. En la página **Enlace de Curvas ECC de Servidor Virtual SSL**, haga clic en **Agregar enlace**.



6. En **Enlace de curva ECC**, haga clic en **Seleccionar curva ECC**.



7. Seleccione un valor y, a continuación, haga clic en **Seleccionar**.



8. Haga clic en **Vincular**.
9. Haga clic en **Cerrar**.
10. Haga clic en **Done**.

Vincular curvas ECC a un servicio SSL mediante la CLI

En el símbolo del sistema, escriba:

```
bind ssl service <vServerName > -eccCurveName <eccCurveName >
```

Ejemplo:

```
> bind ssl service sslsvc -eccCurveName P_224
 Done
> sh ssl service sslsvc

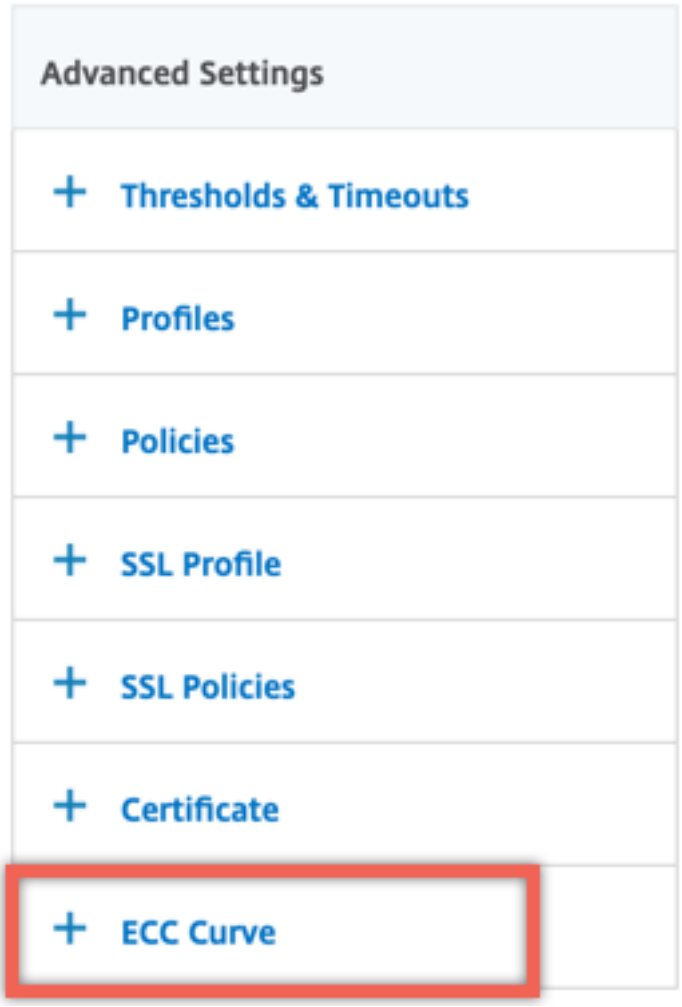
    Advanced SSL configuration for Back-end SSL Service sslsvc:
    DH: DISABLED
    DH Private-Key Exponent Size Limit: DISABLED    Ephemeral RSA:
       DISABLED
    Session Reuse: ENABLED      Timeout: 300 seconds
```



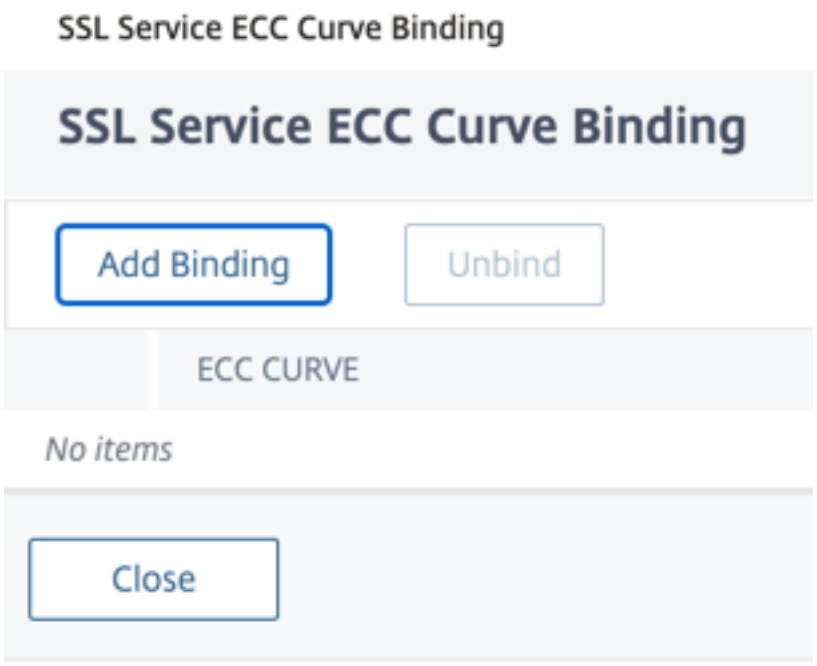
```
9       Cipher Redirect: DISABLED
10      ClearText Port: 0
11      Server Auth: DISABLED
12      SSL Redirect: DISABLED
13      Non FIPS Ciphers: DISABLED
14      SNI: DISABLED
15      OCSP Stapling: DISABLED
16      SSLv3: ENABLED  TLSv1.0: ENABLED  TLSv1.1: ENABLED  TLSv1.2:
            ENABLED  TLSv1.3: DISABLED
17      Send Close-Notify: YES
18      Strict Sig-Digest Check: DISABLED
19      Zero RTT Early Data: ???
20      DHE Key Exchange With PSK: ???
21      Tickets Per Authentication Context: ???
22
23      ECC Curve: P_224
24
25
26  1)  Cipher Name: DEFAULT_BACKEND
27      Description: Default cipher list for Backend SSL session
28   Done
29  <!--NeedCopy-->
```

Vincular curvas ECC a un servicio SSL mediante la GUI

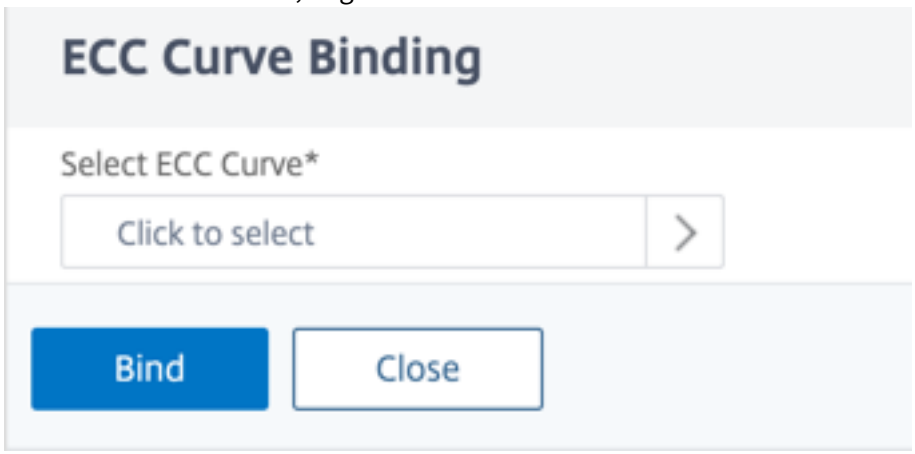
1. Vaya a **Administración de Tráfico > Equilibrio de carga > Servicios**.
2. Seleccione un servicio SSL y haga clic en **Modificar**.
3. En **Configuración avanzada**, haga clic en **Curva ECC**.



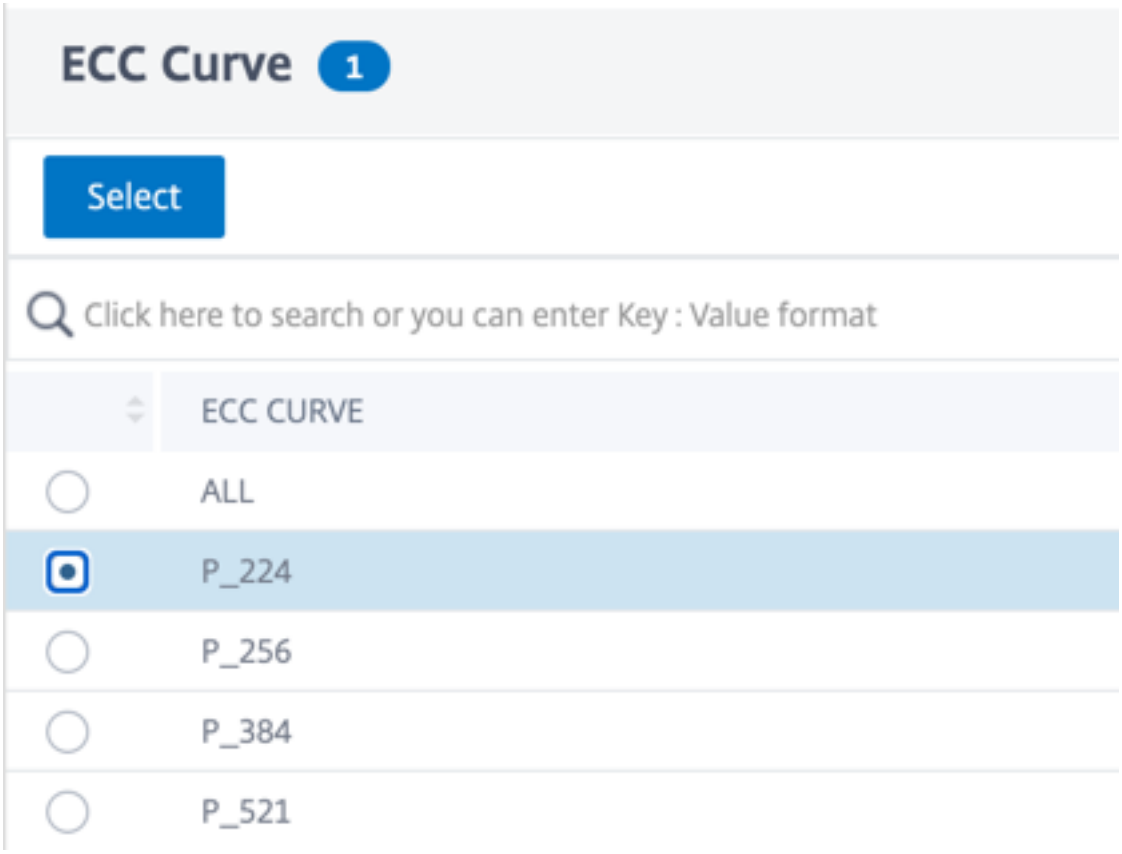
4. Haga clic dentro de la sección de curva ECC.
5. En la página **Enlace de Curvas ECC de Servicio SSL**, haga clic en **Agregar enlace**.



6. En **Enlace de curva ECC**, haga clic en **Seleccionar curva ECC**.



7. Seleccione un valor y, a continuación, haga clic en **Seleccionar**.



8. Haga clic en **Vincular**.
9. Haga clic en **Cerrar**.
10. Haga clic en **Done**.

Generación de parámetros Diffie-Hellman y consecución de PFS con DHE

August 20, 2021

El intercambio de claves Diffie-Hellman (DH) es una forma para que dos partes involucradas en una transacción SSL acuerden un secreto compartido sobre un canal inseguro. Estas partes no tienen conocimiento previo el uno del otro. Este secreto se puede convertir en material de claves criptográficas para algoritmos de cifrado de claves simétricas que requieren dicho intercambio de claves.

Esta función está inhabilitada de forma predeterminada. Se configuró la función para admitir cifrados que utilizan DH como algoritmo de intercambio de claves.

> **Nota**:
>
> La generación de parámetros DH de 2048 bits puede tardar mucho tiempo (hasta 30 minutos).

Generar parámetros DH mediante la CLI

En el símbolo del sistema, escriba el siguiente comando:

```
create ssl dhparam <dhFile> [<bits>] [-gen (2 | 5)]
<!--NeedCopy-->
```

Ejemplo:

```
create ssl dhparam Key-DH-1 512 -gen 2
<!--NeedCopy-->
```

Generar parámetros DH mediante la interfaz gráfica de usuario

Vaya a **Administración del tráfico** > **SSL** y, en el grupo **Herramientas**, seleccione **Crear clave Diffie-Hellman (DH)** y **Configurar SSL DH Param**.

> **Nota:**
>
> Para obtener información sobre los parámetros de DH, consulte Parámetros de Diffie-Hellman.

Consiga un secreto directo perfecto con DHE

La generación de parámetros DH es una operación intensiva de CPU. En versiones anteriores, la generación de parámetros, en un dispositivo VPX, tardó mucho tiempo porque se hacía en el software. La generación de parámetros se optimiza configurando el parámetro `dhKeyExpSizeLimit`. Puede establecer este parámetro para un servidor virtual SSL o un perfil SSL y, a continuación, enlazar el perfil a un servidor virtual.

Puede mantener el secreto de envío perfecto (PFS) en los dispositivos Citrix ADC MPX estableciendo el recuento DH igual a cero. Como resultado, se generan parámetros DH para cada transacción (el mínimo `DHcount` es 0) en dispositivos Citrix ADC MPX. Los parámetros se generan sin una caída significativa en el rendimiento, ya que la operación está optimizada. Anteriormente, el recuento mínimo de DH permitido era de 500. Es decir, no puede regenerar la clave para hasta 500 transacciones.

En un dispositivo Citrix ADC VPX, puede generar parámetros DH para cada 500 transacciones como mínimo (`DHcount` = 500). Si establece `DHcount` igual a 0, los parámetros DH no se regeneran.

> **Limitación:**
>
> No puede lograr PFS en VPX hoy con los cifrados DH.

Optimizar la generación de parámetros DH mediante la CLI

En el símbolo del sistema, escriba los comandos 1 y 2 o escriba el comando 3:

```
1. add ssl profile <name> [-sslProfileType ( BackEnd | FrontEnd )] [-
   dhCount <positive_integer>] [-dh ( ENABLED | DISABLED) -dhFile <
   string>] [-dhKeyExpSizeLimit ( ENABLED | DISABLED)]
2. set ssl vserver <vServerName> [-sslProfile <string>]
<!--NeedCopy-->
```

```
3. set ssl vserver <vServerName> [-dh ( ENABLED | DISABLED) -dhFile <
   string>] [-dhCount <positive_integer>] [-dhKeyExpSizeLimit ( ENABLED
    | DISABLED )]
<!--NeedCopy-->
```

Optimizar la generación de parámetros DH mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**y abra un servidor virtual.
2. En la sección **Parámetros SSL**, seleccione **Habilitar Límite de tamaño de caducidad de clave DH**.

Redirección de cifrado

August 20, 2021

Durante el protocolo de enlace SSL, el cliente SSL (generalmente un explorador web) anuncia el conjunto de cifrados que admite, en el orden configurado de preferencia de cifrado. A partir de esa lista, el servidor SSL selecciona un cifrado que coincida con su propia lista de cifrados configurados.

Si los cifrados anunciados por el cliente no coinciden con los cifrados configurados en el servidor SSL, se produce un error en el enlace SSL. El error se anuncia mediante un mensaje de error críptico que se muestra en el explorador. Estos mensajes rara vez mencionan la causa exacta del error.

Con la redirección de cifrado, puede configurar un servidor virtual SSL para que proporcione mensajes de error precisos y significativos cuando falla un protocolo de enlace SSL. Cuando falla un protocolo de enlace SSL, el dispositivo ADC redirige al usuario a una dirección URL previamente configurada o, si no hay ninguna URL configurada, muestra una página de error generada internamente.

Configurar la redirección de cifrado mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para configurar la redirección de cifrado y verificar la configuración:

```
- set ssl vserver <vServerName> -cipherRedirect < ENABLED | DISABLED>
   -cipherURL < URL>
- show ssl vserver <vServerName>
<!--NeedCopy-->
```

Ejemplo:

```
set ssl vserver vs-ssl -cipherRedirect ENABLED -cipherURL http://
   redirectURl

Done

show ssl vserver vs-ssl

Advanced SSL configuration for VServer vs-ssl:
DH: DISABLED
Ephemeral RSA: ENABLED          Refresh Count: 1000
Session Reuse: ENABLED          Timeout: 600 seconds
Cipher Redirect: ENABLED        Redirect URL: http://redirectURl
SSLv2 Redirect: DISABLED
ClearText Port: 0
Client Auth: DISABLED
SSL Redirect: DISABLED
Non FIPS Ciphers: DISABLED
SNI: DISABLED
OCSP Stapling: DISABLED
HSTS: DISABLED
HSTS IncludeSubDomains: NO
HSTS Max-Age: 0
SSLv2: DISABLED SSLv3: ENABLED  TLSv1.0: ENABLED TLSv1.2: ENABLED
   TLSv1.2: ENABLED
    1)      CertKey Name: Auth-Cert-1       Server Certificate
    1)      Cipher Name: DEFAULT
            Description: Predefined Cipher Alias
Done
<!--NeedCopy-->
```


Configure la redirección de cifrado mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**y abra un servidor virtual.
2. En la sección **Parámetros SSL**, seleccione **Enable Cipher Redirect** y especifique una dirección URL de redirección.

Utilice hardware y software para mejorar el rendimiento de cifrado ECDHE y ECDSA

February 16, 2021

> **Nota:**
>
> Esta mejora solo se aplica a las siguientes plataformas:
>
> - MPX/SDX 11000
> - MPX/SDX 14000
> - MPX 22000, MPX 24000 y MPX 25000
> - MPX/SDX 14000 FIPS

Anteriormente, el cálculo ECDHE y ECDSA en un dispositivo Citrix ADC se realizaba únicamente en el hardware (chips Cavium), lo que limitaba el número de sesiones SSL en un momento dado. Con esta mejora, algunas operaciones también se realizan en el software. Es decir, el procesamiento se realiza tanto en los chips Cavium como en los núcleos de CPU para mejorar el rendimiento de cifrado ECDHE y ECDSA.

El procesamiento se realiza primero en software, hasta el umbral de cifrado de software configurado. Una vez alcanzado este umbral, las operaciones se descartan en el hardware. Por lo tanto, este modelo híbrido utiliza hardware y software para mejorar el rendimiento SSL. Puede habilitar el modelo híbrido configurando el parámetro "SoftwareCryptoThreshold" para que se adapte a sus necesidades. Para inhabilitar el modelo híbrido, establezca este parámetro en 0.

Los beneficios son mayores si la utilización actual de la CPU no es demasiado alta, porque el umbral de la CPU no es exclusivo del cálculo ECDHE y ECDSA. Por ejemplo, si la carga de trabajo actual en el dispositivo consume el 50% de los ciclos de CPU y el umbral se establece en 80%, el cálculo ECDHE y ECDSA solo puede utilizar el 30%. Una vez alcanzado el umbral de cifrado de software configurado del 80%, se descargó el cálculo ECDHE y ECDSA al hardware. En ese caso, la utilización real de la CPU podría superar el 80%, ya que realizar cálculos ECDHE y ECDSA en hardware consume algunos ciclos de CPU.

Habilitar el modelo híbrido mediante la CLI

En el símbolo del sistema, escriba:

```
set ssl parameter -softwareCryptoThreshold <positive_integer>

Synopsis:

softwareCryptoThreshold:

Citrix ADC CPU utilization threshold (as a percentage) beyond which
   crypto operations are not done in software. A value of zero implies
   that CPU is not utilized for doing crypto in software.

Default = 0

Min = 0

Max = 100
<!--NeedCopy-->
```

Ejemplo:

```
set ssl parameter - softwareCryptoThreshold 80
Done

show ssl parameter
Advanced SSL Parameters

SSL quantum size                  : 8 KB
Max CRL memory size               : 256 MB
Strict CA checks                  : NO
Encryption trigger timeout        : 100 ms
Send Close-Notify                 : YES
Encryption trigger packet c       : 45
Deny SSL Renegotiation            : ALL
Subject/Issuer Name Insertion Format : Unicode
OCSP cache size                   : 10 MB
Push flag                         : 0x0 (Auto)
Strict Host Header check for SNI enabled SSL sessions : NO
PUSH encryption trigger timeout   : 1 ms
Crypto Device Disable Limit       : 0
Global undef action for control policies : CLIENTAUTH
```



```
Global undef action for data policies : NOOP
Default profile                   : DISABLED
Disable TLS 1.1/1.2 for SSL_BRIDGE secure monitors    : NO
Disable TLS 1.1/1.2 for dynamic and VPN services : NO
Software Crypto acceleration CPU Threshold : 80
Signature and Hash Algorithms supported by TLS1.2 : ALL
<!--NeedCopy-->
```

Habilite el modelo híbrido mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico** > **SSL** > **Cambiar la configuración avanzada de SSL**.
2. Introduzca un valor para **Umbral de cifrado de software (%)**.

Establecer una alarma SNMP para el tipo de cambio ECDHE

El intercambio de claves basado en ECDHE puede provocar la caída de las transacciones por segundo en el dispositivo. Desde la versión 13.0 compilación 52.x, puede configurar una alarma SNMP para transacciones basadas en ECDHE. En esta alarma, puede establecer el umbral y los límites normales para el tipo de cambio ECDHE. Se agregó un nuevo contador `nsssl_tot_sslInfo_ECDHE_Tx`. Este contador es la suma de todos los contadores de transacciones basados en ECDHE en el front-end y back-end del dispositivo. Cuando el intercambio de claves basado en ECDHÉ cruza los límites configurados, se envía una captura SNMP. Otra trampa se envía cuando el valor vuelve al valor normal configurado.

Establecer una alarma SNMP para el tipo de cambio ECDHE mediante la CLI

En el símbolo del sistema, escriba:

```
set snmp alarm ECDHE-EXCHANGE-RATE -logging ( ENABLED | DISABLED ) -
    severity <severity>
 -state ( ENABLED | DISABLED ) -thresholdValue <positive_integer>  [-
     normalValue <positive_integer>] -time <secs>
<!--NeedCopy-->
```

Ejemplo:

```
set snmp alarm ECDHE-EXCHANGE-RATE -logging eNABLED -severity critical
    -state eNABLED -thresholdValue 100 -normalValue 50
<!--NeedCopy-->
```


Compatibilidad con los conjuntos de cifrado ECDSA

August 20, 2021

Los conjuntos de cifrado ECDSA utilizan criptografía de curva elíptica (ECC). Debido a su tamaño más pequeño, resulta útil en entornos donde la potencia de procesamiento, el espacio de almacenamiento, el ancho de banda y el consumo de energía están limitados.

Cuando se utiliza el grupo de cifrado ECDHE_ECDSA, el certificado del servidor debe contener una clave pública compatible con ECDS.

En la siguiente tabla se enumeran los cifrados ECDSA admitidos en los dispositivos Citrix ADC MPX y SDX con chips N3, dispositivos Citrix ADC VPX, MPX 5900/26000 y MPX/SDX 8900/15000.

Nombre de cifrado	Prioridad	Descripción	Algoritmo de intercambio de claves	Algoritmo de autenticación	Algoritmo de cifrado (tamaño de clave)	Algoritmo de código de autenticación de mensajes (MAC)	Hexcode
TLS1-ECDHE-ECDSA-AES128-SHA	1	SSLv3	ECC-DHE	ECDSA	AES(128)	SHA1	0xc009
TLS1-ECDHE-ECDSA-AES256-SHA	2	SSLv3	ECC-DHE	ECDSA	AES(256)	SHA1	0xc00a
TLS1.2-ECDHE-ECDSA-AES128-SHA256	3	TLSv1.2	ECC-DHE	ECDSA	AES(128)	SHA-256	0xc023

Nombre de cifrado	Prioridad	Descripción	Algoritmo de intercambio de claves	Algoritmo de autenticación	Algoritmo de cifrado (tamaño de clave)	Algoritmo de código de autenticación de mensajes (MAC)	Hexcode
TLS1.2-ECDHE-ECDSA-AES256-SHA384	4	TLSv1.2	ECC-DHE	ECDSA	AES(256)	SHA-384	0xc024
TLS1.2-ECDHE-ECDSA-AES128-GCM-SHA256	5	TLSv1.2	ECC-DHE	ECDSA	AES-GCM(128)	SHA-256	0xc02b
TLS1.2-ECDHE-ECDSA-AES256-GCM-SHA384	6	TLSv1.2	ECC-DHE	ECDSA	AES-GCM(256)	SHA-384	0xc02c
TLS1-ECDHE-ECDSA-RC4-SHA	7	SSLv3	ECC-DHE	ECDSA	RC4 (128)	SHA1	0xc007
TLS1-ECDHE-ECDSA-DES-CBC3-SHA	8	SSLv3	ECC-DHE	ECDSA	3DES (168)	SHA1	0xc008

Nombre de cifrado	Prioridad	Descripción	Algoritmo de intercambio de claves	Algoritmo de autenticación	Algoritmo de cifrado (tamaño de clave)	Algoritmo de código de autenticación de mensajes (MAC)	Hexcode
TLS1.2-ECDHE-ECDSA-CHACHA20-POLY1305	9	TLSv1.2	ECC-DHE	ECDSA	CHACHA20/	AEAD	0xcca9

Selección de certificados y cifrado ECDSA/RSA

Puede enlazar certificados de servidor ECDSA y RSA al mismo tiempo a un servidor virtual SSL. Cuando los certificados ECDSA y RSA están enlazados al servidor virtual, selecciona automáticamente el certificado de servidor adecuado para presentarlo al cliente. Si la lista de cifrado del cliente incluye cifrados RSA, pero no incluye cifrados ECDSA, el servidor virtual presenta el certificado del servidor RSA. Si ambos cifrados están presentes en la lista del cliente, el certificado de servidor presentado depende de la prioridad de cifrado establecida en el servidor virtual. Es decir, si RSA tiene una prioridad más alta, se presenta el certificado RSA. Si ECDSA tiene una prioridad más alta, el certificado ECDSA se presenta al cliente.

Autenticación de cliente mediante un certificado ECDSA o RSA

Para la autenticación de cliente, el certificado de CA vinculado al servidor virtual puede estar firmado por ECDSA o RSA. El dispositivo admite una cadena de certificados mixta. Por ejemplo, se admite la siguiente cadena de certificados.

Certificado de cliente (ECDSA) <-> Certificado de CA (RSA) <-> Certificado intermedio (RSA) <-> Certificado raíz (RSA)

En la tabla siguiente se muestran las curvas elípticas admitidas en los distintos dispositivos Citrix ADC con grupos de cifrado ECDSA y certificados ECDSA:

Curvas elípticas	Plataformas admitidas
prime256v1	Todas las plataformas, incluido FIPS.
secp384r1	Todas las plataformas, incluido FIPS.

Curvas elípticas	Plataformas admitidas
secp521r1	MPX 5900, MPX/SDX 8900, MPX/SDX 15000, MPX/SDX 26000, VPX
secp224r1	MPX 5900, MPX/SDX 8900. MPX/SDX 15000, MPX/SDX 26000, VPX

Crear un par de certificados ECDSA

Puede crear un par de claves de certificado ECDSA directamente en un dispositivo Citrix ADC mediante la CLI o la GUI. Anteriormente, podía instalar y enlazar un par de claves de certificado ECC en el dispositivo, pero tenía que usar OpenSSL para crear un par de claves de certificado.

Solo se admiten curvas P_256 y P_384.

> **Nota**
>
> Este soporte está disponible en todas las plataformas excepto MPX 9700/1050/12500/15500.

Para crear un par de certificados ECDSA mediante la CLI:

En el símbolo del sistema, escriba:

```
create ssl ecdsaKey <keyFile> -curve ( P_256 | P_384 ) [-keyform ( DER | PEM )] [-des | -des3] {
 -password  }
  [-pkcs8]
<!--NeedCopy-->
```

Ejemplo:

```
create ecdsaKey ec_p256.ky -curve P_256 -pkcs8
Done
create ecdsaKey ec_p384.ky -curve P_384
Done
<!--NeedCopy-->
```

Para crear un par de certificados ECDSA mediante la interfaz gráfica de usuario:

1. Vaya a **Administración del tráfico > SSL > Archivos SSL > Claves** y haga clic en **Crear clave ECDSA**.
2. Para crear una clave en formato PKCS #8, seleccione **PKCS8**.

Configurar grupos de cifrado definidos por el usuario en el dispositivo ADC

August 20, 2021

Un grupo de cifrado es un conjunto de conjuntos de cifrado que se vincula a un servidor virtual SSL, servicio o grupo de servicios en el dispositivo Citrix ADC. Un conjunto de cifrado comprende un protocolo, un algoritmo de intercambio de claves (Kx), un algoritmo de autenticación (Au), un algoritmo de cifrado (Enc) y un código de autenticación de mensajes (Mac) algoritmo. El dispositivo se envía con un conjunto predefinido de grupos de cifrado. Cuando crea un servicio SSL o un grupo de servicios SSL, el grupo de cifrado ALL se vincula automáticamente a él. Sin embargo, al crear un servidor virtual SSL o un servicio SSL transparente, el grupo de cifrado DEFAULT se vincula automáticamente a él. Además, puede crear un grupo de cifrado definido por el usuario y vincularlo a un servidor virtual SSL, servicio o grupo de servicios.

Nota: Si su dispositivo MPX no tiene ninguna licencia, solo el cifrado EXPORT está enlazado al servidor virtual SSL, servicio o grupo de servicios.

Para crear un grupo de cifrado definido por el usuario, primero debe crear un grupo de cifrado y, a continuación, enlazar cifradores o grupos de cifrado a este grupo. Si especifica un alias de cifrado o un grupo de cifrado, todos los cifrados del alias o grupo de cifrado se agregan al grupo de cifrado definido por el usuario. También puede agregar cifrados individuales (conjuntos de cifrado) a un grupo definido por el usuario. Sin embargo, no se puede modificar un grupo de cifrado predefinido. Antes de quitar un grupo de cifrado, desvincule todos los conjuntos de cifrado del grupo.

Al enlazar un grupo de cifrado a un servidor virtual SSL, servicio o grupo de servicios, se anexan los cifrados a los cifrados existentes enlazados a la entidad. Para enlazar un grupo de cifrado específico a la entidad, primero debe desvincular los cifrados o el grupo de cifrados enlazados a la entidad. A continuación, vincule el grupo de cifrado específico a la entidad. Por ejemplo, para enlazar solo el grupo de cifrado AES a un servicio SSL, realice los siguientes pasos:

1. Desenlazar el grupo de cifrado predeterminado ALL que está enlazado de forma predeterminada al servicio cuando se crea el servicio.

```
unbind ssl service <service name> -cipherName ALL
<!--NeedCopy-->
```

2. Vincular el grupo de cifrado AES al servicio

```
bind ssl service <Service name> -cipherName AE
```



```
<!--NeedCopy-->
```

Si quiere enlazar el grupo de cifrado DES además de AES, en el símbolo del sistema, escriba:

```
bind ssl service <service name> -cipherName DES
<!--NeedCopy-->
```

Nota: El dispositivo virtual Citrix ADC gratuito solo admite el grupo de cifrado DH.

Configurar un grupo de cifrado definido por el usuario mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para agregar un grupo de cifrado o para agregar cifrados a un grupo creado anteriormente y compruebe la configuración:

```
add ssl cipher <cipherGroupName>
bind ssl cipher <cipherGroupName> -cipherName <cipherGroup/cipherName>
show ssl cipher <cipherGroupName>
<!--NeedCopy-->
```

Ejemplo:

```
add ssl cipher test

Done

bind ssl cipher test -cipherName ECDHE

Done

sh ssl cipher test

1)      Cipher Name: TLS1-ECDHE-RSA-AES256-SHA  Priority : 1
Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=AES(256)  Mac=SHA1   HexCode
   =0xc014
2)      Cipher Name: TLS1-ECDHE-RSA-AES128-SHA  Priority : 2
Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=AES(128)  Mac=SHA1   HexCode
   =0xc013
3)      Cipher Name: TLS1.2-ECDHE-RSA-AES-256-SHA384    Priority : 3
Description: TLSv1.2 Kx=ECC-DHE  Au=RSA  Enc=AES(256)  Mac=SHA-384
   HexCode=0xc028
```



```
4)      Cipher Name: TLS1.2-ECDHE-RSA-AES-128-SHA256    Priority : 4
Description: TLSv1.2 Kx=ECC-DHE  Au=RSA  Enc=AES(128)  Mac=SHA-256
   HexCode=0xc027
5)      Cipher Name: TLS1.2-ECDHE-RSA-AES256-GCM-SHA384 Priority : 5
Description: TLSv1.2 Kx=ECC-DHE  Au=RSA  Enc=AES-GCM(256) Mac=AEAD
   HexCode=0xc030
6)      Cipher Name: TLS1.2-ECDHE-RSA-AES128-GCM-SHA256 Priority : 6
Description: TLSv1.2 Kx=ECC-DHE  Au=RSA  Enc=AES-GCM(128) Mac=AEAD
   HexCode=0xc02f
7)      Cipher Name: TLS1-ECDHE-ECDSA-AES256-SHA        Priority : 7
Description: SSLv3 Kx=ECC-DHE  Au=ECDSA Enc=AES(256)  Mac=SHA1
   HexCode=0xc00a
8)      Cipher Name: TLS1-ECDHE-ECDSA-AES128-SHA        Priority : 8
Description: SSLv3 Kx=ECC-DHE  Au=ECDSA Enc=AES(128)  Mac=SHA1
   HexCode=0xc009
9)      Cipher Name: TLS1.2-ECDHE-ECDSA-AES256-SHA384   Priority : 9
Description: TLSv1.2 Kx=ECC-DHE  Au=ECDSA Enc=AES(256)  Mac=SHA-384
   HexCode=0xc024
10)     Cipher Name: TLS1.2-ECDHE-ECDSA-AES128-SHA256   Priority : 10
Description: TLSv1.2 Kx=ECC-DHE  Au=ECDSA Enc=AES(128)  Mac=SHA-256
   HexCode=0xc023
11)     Cipher Name: TLS1.2-ECDHE-ECDSA-AES256-GCM-SHA384
   Priority : 11
Description: TLSv1.2 Kx=ECC-DHE  Au=ECDSA Enc=AES-GCM(256) Mac=AEAD
   HexCode=0xc02c
12)     Cipher Name: TLS1.2-ECDHE-ECDSA-AES128-GCM-SHA256
   Priority : 12
Description: TLSv1.2 Kx=ECC-DHE  Au=ECDSA Enc=AES-GCM(128) Mac=AEAD
   HexCode=0xc02b
13)     Cipher Name: TLS1-ECDHE-RSA-DES-CBC3-SHA        Priority : 13
Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=3DES(168) Mac=SHA1   HexCode
   =0xc012
14)     Cipher Name: TLS1-ECDHE-ECDSA-DES-CBC3-SHA      Priority : 14
Description: SSLv3 Kx=ECC-DHE  Au=ECDSA Enc=3DES(168) Mac=SHA1
   HexCode=0xc008
15)     Cipher Name: TLS1-ECDHE-RSA-RC4-SHA     Priority : 15
Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=RC4(128)  Mac=SHA1   HexCode
   =0xc011
16)     Cipher Name: TLS1-ECDHE-ECDSA-RC4-SHA   Priority : 16
Description: SSLv3 Kx=ECC-DHE  Au=ECDSA Enc=RC4(128)  Mac=SHA1
   HexCode=0xc007
17)     Cipher Name: TLS1.2-ECDHE-RSA-CHACHA20-POLY1305 Priority : 17
Description: TLSv1.2 Kx=ECC-DHE  Au=RSA  Enc=CHACHA20/POLY1305(256) Mac
   =AEAD   HexCode=0xcca8
18)     Cipher Name: TLS1.2-ECDHE-ECDSA-CHACHA20-POLY1305
```



```
    Priority : 18
46 Description: TLSv1.2 Kx=ECC-DHE  Au=ECDSA Enc=CHACHA20/POLY1305(256)
    Mac=AEAD   HexCode=0xcca9
47 Done
48
49 bind ssl cipher test -cipherName TLS1-ECDHE-RSA-DES-CBC3-SHA
50 <!--NeedCopy-->
```

Desenlazar los cifrados de un grupo de cifrados mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para desvincular los cifrados de un grupo de cifrado definido por el usuario y compruebe la configuración:

```
1 show ssl cipher <cipherGroupName>
2
3 unbind ssl cipher <cipherGroupName> -cipherName <string>
4
5 show ssl cipher <cipherGroupName>
6 <!--NeedCopy-->
```

Quitar un grupo de cifrado mediante la CLI

Nota: No se puede quitar un grupo de cifrado integrado. Antes de quitar un grupo de cifrado definido por el usuario, asegúrese de que el grupo de cifrado está vacío.

En el símbolo del sistema, escriba los comandos siguientes para quitar un grupo de cifrado definido por el usuario y compruebe la configuración:

```
1 rm ssl cipher <userDefCipherGroupName> [<cipherName> ...]
2 show ssl cipher <cipherGroupName>
3
4 <!--NeedCopy-->
```

Ejemplo:

```
1 rm ssl cipher test Done
2
3 sh ssl cipher test ERROR: No such resource [cipherGroupName, test]
4 <!--NeedCopy-->
```


Configurar un grupo de cifrado definido por el usuario mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > SSL > Grupos de cifrado**.
2. Haga clic en **Agregar**.
3. Especifique un nombre para el grupo de cifrado.
4. Haga clic en **Agregar** para ver los cifrados y los grupos de cifrado disponibles.
5. Seleccione un grupo de cifrado o cifrado y haga clic en el botón de flecha para agregarlos.
6. Haga clic en **Crear**.
7. Haga clic en **Cerrar**.

Para enlazar un grupo de cifrado a un servidor virtual SSL, servicio o grupo de servicios mediante la CLI:

En el símbolo del sistema, escriba una de las siguientes opciones:

```
bind ssl vserver <vServerName> -cipherName <string>

bind ssl service <serviceName> -cipherName <string>

bind ssl serviceGroup <serviceGroupName> -cipherName <string>

<!--NeedCopy-->
```

Ejemplo:

```
bind ssl vserver ssl_vserver_test -cipherName test
Done

bind ssl service  nshttps -cipherName test
Done

bind ssl servicegroup  ssl_svc  -cipherName test
Done
<!--NeedCopy-->
```

Para enlazar un grupo de cifrado a un servidor virtual SSL, servicio o grupo de servicios mediante la GUI:

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.

   Para el servicio, reemplace los servidores virtuales por servicios. En el caso de los grupos de servicios, reemplace los servidores virtuales por grupos de servicios.

Abra el servidor virtual, el servicio o el grupo de servicios.

2. En **Configuración avanzada**, seleccione **Cifrados SSL**.
3. Enlazar un grupo de cifrado al servidor virtual, servicio o grupo de servicios.

Vinculación de cifrados individuales a un servidor virtual SSL o servicio

También puede enlazar cifrados individuales, en lugar de un grupo de cifrados, a un servidor o servicio virtual.

Para enlazar un cifrado mediante la CLI:
En el símbolo del sistema, escriba:

```
bind ssl vserver <vServerName> -cipherName <string>
bind ssl service <serviceName> -cipherName <string>
<!--NeedCopy-->
```

Ejemplo:

```
bind ssl vserver v1 -cipherName TLS1.2-ECDHE-RSA-AES256-GCM-SHA384
Done

bind ssl service sslsvc -cipherName TLS1.2-ECDHE-RSA-AES256-GCM-SHA384
Done
<!--NeedCopy-->
```

Para enlazar un cifrado a un servidor virtual SSL mediante la GUI:

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. Seleccione un servidor virtual SSL y haga clic en **Modificar**.
3. En **Configuración avanzada**, seleccione **Cifrados SSL**.
4. En **Cipher Suites**, seleccione **Agregar**.
5. Busque el cifrado en la lista disponible y haga clic en la flecha para agregarlo a la lista configurada.
6. Haga clic en **Aceptar**.
7. Haga clic en **Done**.

Para enlazar un cifrado a un servicio SSL, repita los pasos anteriores después de reemplazar el servidor virtual con servicio.

Matriz de compatibilidad de certificados de servidor en el dispositivo ADC

June 2, 2022

A partir de la versión 13.0 compilación 41.x, el dispositivo ADC admite mensajes de certificados de servidor que se fragmentan en más de un registro si el tamaño total es inferior a 32 KB. Anteriormente, el tamaño máximo admitido era de 16 KB y la fragmentación no era compatible.

El dispositivo Citrix ADC admite los siguientes certificados de servidor.

Tabla 1: Asistencia en el servicio front-end (FE) y back-end (BE)

Certificado/plataforma de servidor	MPX/SDX (CHIPS N2) FR	MPX/SDX (CHIPS N2) BE	MPX/SDX (CHIPS N3) FE	MPX/SDX (CHIPS N3) BE	VPX FE	VPX BE
MD5	S	S	S	S	S	S
SHA1	S	S	S	S	S	S
SHA224	S	S	S	S	S	S
SHA256	S	S	S	S	S	S
SHA384	S	S	S	S	S	S
SHA512	S	S	S	S	S	S
Clave RSA	1024, 2048, 3072 y 4096 bits	1024, 2048, 3072 y 4096 bits	1024, 2048, 3072 y 4096 bits	1024, 2048, 3072 y 4096 bits	1024, 2048, 3072 y 4096 bits	1024, 2048, 3072 y 4096 bits
Clave DH	1024 bits y 2048 bits	1024 bits y 2048 bits	1024 bits y 2048 bits	1024 bits y 2048 bits	1024, 2048, 3072 y 4096 bits	1024, 2048, 3072 y 4096 bits

Certificado/plataforma de servidor	MPX/SDX 14030/14060/14080 FIPS FE	MPX/SDX 14030/14060/14080 FIPS BE
MD5	S	S
SHA1	S	S
SHA224	S	S
SHA256	S	S
SHA384	S	S

Certificado/plataforma de servidor	MPX/SDX 14030/14060/14080 FIPS FE	MPX/SDX 14030/14060/14080 FIPS BE
SHA512	S	S
Clave RSA	2048 bits y 3072 bits	2048 bits y 3072 bits
Clave DH	N	N

Certificado/plataforma de servidor	MPX 5900, MPX/SDX 8900, MPX/SDX 9100, MPX/SDX 15000, MPX/SDX 15000-50G, MPX/SDX 26000, MPX/SDX 26000-50G, MPX/SDX 26000-100G (frontend)	MPX 5900, MPX/SDX 8900, MPX/SDX 9100 MPX/SDX 15000, MPX/SDX 15000-50G, MPX/SDX 26000, MPX/SDX 26000-50G, MPX/SDX 26000-100G (back end)
MD5	S	S
SHA1	S	S
SHA224	S	S
SHA256	S	S
SHA384	S	S
SHA512	S	S
Clave RSA	1024, 2048, 3072 y 4096 bits	1024, 2048, 3072 y 4096 bits
Clave DH	1024, 2048, 3072 y 4096 bits	1024, 2048, 3072 y 4096 bits

Notas

- Los certificados 4k requieren ciclos de CPU más altos y pueden afectar al rendimiento de los dispositivos de gama baja.
- En la versión 11.1 y anteriores, un dispositivo Citrix ADC admite las siguientes extensiones de “algoritmos de firma” en el mensaje de saludo del cliente de back-end: RSA-MD5, RSA-SHA1 y RSA-SHA256.
  El dispositivo Citrix ADC no admite las extensiones de algoritmos de firma SHA 384 y SHA 512. Por lo tanto, algunos servidores, como los servidores IIS de Windows, restablecen la conexión.
- A partir de la versión 12.0, un dispositivo Citrix ADC admite todas las extensiones signature_algorithms.

Autenticación de clientes o TLS mutuo (MTL)

March 9, 2022

En una transacción SSL típica, el cliente que se conecta a un servidor a través de una conexión segura verifica la validez del servidor. Para ello, comprueba el certificado del servidor antes de iniciar la transacción SSL. Sin embargo, en ocasiones, es posible que quiera configurar el servidor para autenticar al cliente que se conecta a él.

Nota: A partir de la versión 13.0 compilación 41.x, el dispositivo Citrix ADC admite mensajes de solicitud de certificados que se fragmentan en más de un registro si el tamaño total es inferior a 32 KB. Anteriormente, el tamaño máximo admitido era de 16 KB y la fragmentación no era compatible.

Con la autenticación de cliente habilitada en un servidor virtual SSL, el dispositivo Citrix ADC solicita el certificado de cliente durante el protocolo de enlace SSL. El dispositivo comprueba el certificado presentado por el cliente en busca de restricciones normales, como la firma del emisor y la fecha de caducidad.

> **Nota**
>
> Para que el dispositivo verifique las firmas del emisor, el certificado de la CA que emitió el certificado de cliente debe ser:
>
> - Se instala en el dispositivo.
> - Enlazado al servidor virtual con el que el cliente realiza transacciones.

Si el certificado es válido, el dispositivo permite que el cliente acceda a todos los recursos seguros. Sin embargo, si el certificado no es válido, el dispositivo descarta la solicitud del cliente durante el protocolo de enlace SSL.

El dispositivo verifica el certificado de cliente formando primero una cadena de certificados, que comienza con el certificado de cliente y termina con el certificado de CA raíz para el cliente (por ejemplo, Verisign). El certificado de CA raíz puede contener uno o más certificados de CA intermedios (si la CA raíz no emite directamente el certificado de cliente).

Antes de habilitar la autenticación de clientes en el dispositivo Citrix ADC, asegúrese de que haya un certificado de cliente válido instalado en el cliente. A continuación, habilite la autenticación de clientes para el servidor virtual que gestiona las transacciones. Por último, vincule el certificado de la CA que emitió el certificado de cliente al servidor virtual del dispositivo.

Nota: Un dispositivo Citrix ADC MPX admite un tamaño de par de claves de certificado de 512 bits a 4096 bits. El certificado debe firmarse mediante uno de los siguientes algoritmos hash:

- MD5
- SHA-1
- SHA-224

- SHA-256
- SHA-384
- SHA-512

En un dispositivo SDX, si se asigna un chip SSL a una instancia VPX, se aplica la compatibilidad de tamaño de par de claves de certificado de un dispositivo MPX. De lo contrario, se aplica la compatibilidad normal de tamaño de par de claves de certificado de una instancia VPX.

Un dispositivo virtual Citrix ADC (instancia VPX) admite certificados de al menos 512 bits, hasta los siguientes tamaños:

- Certificado de servidor de 4096 bits en el servidor virtual
- Certificado de cliente de 4096 bits en el servicio
- Certificado CA de 4096 bits
- Certificado de 4096 bits en el servidor físico

A partir de la versión 13.1 compilación 17.x, todas las plataformas Citrix ADC admiten certificados que se firman con los algoritmos RSASSA-PSS.
Estos algoritmos se admiten en la validación de rutas de certificados X.509.
En la siguiente tabla se muestran los conjuntos de parámetros RSASSA-PSS compatibles con el dispositivo Citrix ADC.

OID de clave pública	Función de generación de máscaras (MGF)	Función de resumen de MGF	Función Signature Digest	Longitud de sal
rsaEncryption	MGF1	SHA-256	SHA-256	32 bytes
rsaEncryption	MGF1	SHA-384	SHA-384	48 bytes
rsaEncryption	MGF1	SHA-512	SHA-512	64 bytes

Nota: A partir de la versión 13.0 compilación 79.x, se admite la autenticación de clientes con un certificado de cliente RSA de 4096 bits durante un protocolo de enlace SSL en la plataforma VPX.

Notas:

- Para conocer las limitaciones de MPX FIPS, consulte Limitaciones de MPX FIPS.
- Para conocer las limitaciones FIPS de SDX, consulte Limitaciones de SDX FIPS.

Proporcionar el certificado de cliente

Antes de configurar la autenticación de clientes, se debe instalar un certificado de cliente válido en el cliente. Un certificado de cliente incluye detalles sobre el sistema cliente específico que crea sesiones

seguras con el dispositivo Citrix ADC. Cada certificado de cliente es único y solo debe usarlo un sistema cliente.

Ya sea que obtenga el certificado de cliente de una CA, use un certificado de cliente existente o genere un certificado de cliente en el dispositivo Citrix ADC, debe convertir el certificado al formato correcto. En el dispositivo Citrix ADC, los certificados se almacenan en formato PEM o DER y deben convertirse al formato PKCS #12 antes de instalarse en el sistema cliente. Después de convertir el certificado y transferirlo al sistema cliente, asegúrese de que esté instalado en ese sistema y configurado para la aplicación cliente. La aplicación, como un explorador web, debe formar parte de las transacciones SSL.

Para obtener instrucciones sobre cómo convertir un certificado de formato PEM o DER al formato PKCS #12, consulte Importación y conversión de archivos SSL.

Para obtener instrucciones sobre cómo generar un certificado de cliente, consulte Crear un certificado.

Habilitar la autenticación basada en certificados de cliente

De forma predeterminada, la autenticación del cliente está inhabilitada en el dispositivo Citrix ADC y todas las transacciones SSL se realizan sin autenticar al cliente. Puede configurar la autenticación del cliente para que sea opcional u obligatoria como parte del protocolo de enlace SSL.

Si la autenticación del cliente es opcional, el dispositivo solicita el certificado del cliente, pero continúa con la transacción SSL incluso si el cliente presenta un certificado no válido. Si la autenticación del cliente es obligatoria, el dispositivo finaliza el protocolo de enlace SSL si el cliente SSL no proporciona un certificado válido.

Precaución: Citrix recomienda definir directivas de control de acceso adecuadas antes de cambiar la comprobación de autenticación basada en certificados de cliente a opcional.

Nota: La autenticación de clientes se configura para servidores virtuales SSL individuales, no de forma global.

Habilitar la autenticación basada en certificados de cliente mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para habilitar la autenticación basada en certificados de cliente y verificar la configuración:

```
set ssl vserver <vServerName> [-clientAuth (ENABLED | DISABLED)] [-
    clientCert (MANDATORY | OPTIONAL)]
show ssl vserver <vServerName>
<!--NeedCopy-->
```


Ejemplo:

```
set ssl vserver vssl -clientAuth ENABLED -clientCert Mandatory
Done
show ssl vserver vssl

Advanced SSL configuration for VServer vssl:
DH: DISABLED
Ephemeral RSA: ENABLED Refresh Count: 0
Session Reuse: ENABLED Timeout: 120 seconds
Cipher Redirect: DISABLED
SSLv2 Redirect: DISABLED
ClearText Port: 0
Client Auth: ENABLED Client Cert Required: Mandatory
SSL Redirect: DISABLED
Non FIPS Ciphers: DISABLED
        SNI: DISABLED
        OCSP Stapling: DISABLED
        HSTS: DISABLED
        HSTS IncludeSubDomains: NO
        HSTS Max-Age: 0
SSLv2: DISABLED SSLv3: ENABLED TLSv1.0: ENABLED TLSv1.2: ENABLED TLSv1
   .2: ENABLED

1) CertKey Name: sslckey Server Certificate

1) Policy Name: client_cert_policy Priority: 0

1) Cipher Name: DEFAULT
Description: Predefined Cipher Alias
Done
<!--NeedCopy-->
```

Habilitar la autenticación basada en certificados de cliente mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**y abra un servidor virtual.
2. En la sección Parámetros SSL, seleccione Autenticación de cliente y, en la lista Certificado de cliente, seleccione Obligatorio.

> **Nota:**
>
> Si la autenticación del cliente se establece en obligatoria y si el certificado del cliente contiene extensiones de directiva, la validación del certificado falla. A partir de la versión 12.0-56.x, puede establecer un parámetro en el perfil SSL front-end para omitir esta comprobación. El parámetro está inhabilitado de forma predeterminada. Es decir, la comprobación se realiza de forma predeterminada.

Omitir la comprobación de la extensión de directivas durante la autenticación del cliente mediante la CLI

En el símbolo del sistema, escriba:

```
set ssl profile ns_default_ssl_profile_frontend -clientauth ENABLED -
   skipClientCertPolicyCheck ENABLED

Parameter

skipClientCertPolicyCheck

              Control policy extension check, if present inside the
                 X509 certificate chain. Applicable only if client
                 authentication is enabled and client certificate is
                 set to mandatory. Possible values functions as follows
                 :

- ENABLED: Skip the policy check during client authentication.

- DISABLED: Perform policy check during client authentication.

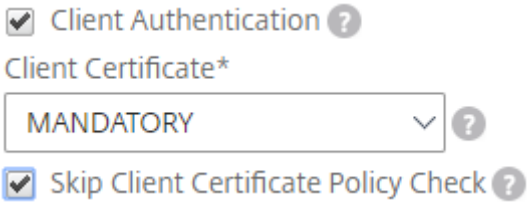
Possible values: ENABLED, DISABLED

Default: DISABLED
<!--NeedCopy-->
```

Omitir la comprobación de la extensión de directivas durante la autenticación del cliente mediante la GUI

1. Vaya a **Sistema** > **Perfiles** > **Perfiles SSL**.
2. Cree un nuevo perfil front-end o modifique un perfil front-end existente.

3. Compruebe que la autenticación del cliente esté habilitada y que el certificado del cliente esté configurado como obligatorio.
4. Seleccione **Omitir comprobación de directivas de certificados de cliente**.



Enlazar certificados de CA al servidor virtual

Una CA cuyo certificado esté presente en el dispositivo Citrix ADC debe emitir el certificado de cliente utilizado para la autenticación de clientes. Enlazar este certificado al servidor virtual Citrix ADC que lleva a cabo la autenticación del cliente.

Enlace el certificado de CA al servidor virtual SSL de tal manera que el dispositivo pueda formar una cadena de certificados completa cuando verifique el certificado de cliente. De lo contrario, la formación de la cadena de certificados falla y se deniega el acceso al cliente incluso si su certificado es válido.

Puede vincular certificados de CA al servidor virtual SSL en cualquier orden. El dispositivo forma el pedido correcto durante la verificación del certificado del cliente.

Por ejemplo, si el cliente presenta un certificado emitido por **CA_A**, donde **CA_A es una**CA intermedia cuyo certificado es emitido por **CA_B**, cuyo certificado es emitido a su vez por una CA raíz de confianza, **Root_CA**, una cadena de certificados que contienen estos tres certificados deben estar enlazados al servidor virtual del dispositivo Citrix ADC.

Para obtener instrucciones sobre cómo vincular uno o varios certificados al servidor virtual, consulte Vincular el par de claves de certificado al servidor virtual SSL.

Para obtener instrucciones sobre cómo crear una cadena de certificados, consulte Crear una cadena de certificados.

Control más estricto de la validación de certificados de cliente

El dispositivo Citrix ADC acepta certificados de CA intermedia válidos si los emite una sola CA raíz. Es decir, si solo el certificado de CA raíz está enlazado al servidor virtual y esa CA raíz valida cualquier certificado intermedio enviado con el certificado de cliente, el dispositivo confía en la cadena de certificados y el protocolo de enlace se realiza correctamente.

Sin embargo, si un cliente envía una cadena de certificados en el protocolo de enlace, ninguno de los certificados intermedios se puede validar mediante un respondedor CRL u OCSP, a menos que dicho

certificado esté enlazado al servidor virtual SSL. Por lo tanto, incluso si se revoca uno de los certificados intermedios, el apretón de manos tiene éxito. Como parte del apretón de manos, el servidor virtual SSL envía la lista de certificados de CA que están enlazados a él. Para un control más estricto, puede configurar el servidor virtual SSL para que acepte solo un certificado firmado por uno de los certificados de CA enlazados a ese servidor virtual. Para ello, debe habilitar la configuración **ClientAuthuseBoundCachain** en el perfil SSL enlazado al servidor virtual. El protocolo de enlace falla si uno de los certificados de CA enlazados al servidor virtual no ha firmado el certificado de cliente.

Por ejemplo, supongamos que dos certificados de cliente, clientcert1 y clientcert2, están firmados por los certificados intermedios Int-CA-A e Int-CA-B, respectivamente. Los certificados intermedios están firmados por el certificado raíz Root-CA. Int-CA-A y Root-CA están enlazados al servidor virtual SSL. En el caso predeterminado (ClientAuthUseBoundCAChain inhabilitado), se aceptan tanto clientcert1 como clientcert2. Sin embargo, si ClientAuthuseBoundCachain está habilitado, el dispositivo Citrix ADC solo acepta clientcert1.

Habilite un control más estricto en la validación de certificados de cliente mediante la CLI

En el símbolo del sistema, escriba:

```
set ssl profile <name> -ClientAuthUseBoundCAChain Enabled
<!--NeedCopy-->
```

Permitir un control más estricto de la validación de certificados de cliente mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **Perfiles**, seleccione la ficha **Perfiles SSL** y cree un perfil SSL o seleccione un perfil existente.
2. Seleccione **Habilitar autenticación de clientes mediante la cadena de CA enlazada**.

Autenticación del servidor

January 12, 2021

Dado que el dispositivo Citrix ADC realiza descarga y aceleración SSL en nombre de un servidor web, el dispositivo normalmente no autentica el certificado del servidor web. Sin embargo, puede autenticar el servidor en implementaciones que requieren cifrado SSL de extremo a extremo.

En tal situación, el dispositivo se convierte en cliente SSL y lleva a cabo una transacción segura con el servidor SSL. Comprueba que una entidad emisora de certificados cuyo certificado está enlazado al

servicio SSL ha firmado el certificado del servidor y comprueba la validez del certificado de servidor.

Para autenticar el servidor, habilite la autenticación del servidor y vincule el certificado de la CA que firmó el certificado del servidor al servicio SSL del dispositivo ADC. Al vincular el certificado, debe especificar el enlace como una opción de CA.

Habilitar (o inhabilitar) la autenticación de certificados de servidor

Puede utilizar la CLI y la GUI para habilitar e inhabilitar la autenticación de certificados del servidor.

Habilitar (o inhabilitar) la autenticación de certificados de servidor mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para habilitar la autenticación de certificados del servidor y verificar la configuración:

```
set ssl service <serviceName> -serverAuth ( ENABLED | DISABLED )
show ssl service <serviceName>
<!--NeedCopy-->
```

Ejemplo:

```
set ssl service ssl-service-1 -serverAuth ENABLED
<!--NeedCopy-->
```

```
show ssl service ssl-service-1

            Advanced SSL configuration for Back-end SSL Service ssl-
               service-1:`
            DH: DISABLED
            Ephemeral RSA: DISABLED
            Session Reuse: ENABLED          Timeout: 300 seconds
            Cipher Redirect: DISABLED
            SSLv2 Redirect: DISABLED
            Server Auth: ENABLED
            SSL Redirect: DISABLED
            Non FIPS Ciphers: DISABLED
            SSLv2: DISABLED SSLv3: ENABLED  TLSv1: ENABLED
    1)      Cipher Name: ALL
            Description: Predefined Cipher Alias
```



```
15 Done
16 <!--NeedCopy-->
```

Habilitar (o inhabilitar) la autenticación de certificados de servidor mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servicios**y abra un servicio SSL.
2. En la sección Parámetros SSL, seleccione Habilitar autenticación de servidor y especifique un nombre común.
3. En Configuración avanzada, seleccione Certificados y vincule un certificado de CA al servicio.

Vincular el certificado de CA al servicio mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para enlazar el certificado de CA al servicio y verificar la configuración:

```
1 bind ssl service <serviceName> -certkeyName <string> -CA
2
3 show ssl service <serviceName>
4 <!--NeedCopy-->
```

Ejemplo:

```
1 bind ssl service ssl-service-1 -certkeyName samplecertkey -CA
2 <!--NeedCopy-->
```

```
1 show ssl service ssl-service-1
2
3             Advanced SSL configuration for Back-end SSL Service ssl-
                 service-1:
4             DH: DISABLED
5             Ephemeral RSA: DISABLED
6             Session Reuse: ENABLED          Timeout: 300 seconds
7             Cipher Redirect: DISABLED
8             SSLv2 Redirect: DISABLED
9             Server Auth: ENABLED
10            SSL Redirect: DISABLED
11            Non FIPS Ciphers: DISABLED
```



```
12              SSLv2: DISABLED SSLv3: ENABLED  TLSv1: ENABLED
13      1)      CertKey Name: samplecertkey     CA Certificate
           CRLCheck: Optional
14      1)      Cipher Name: ALL
15              Description: Predefined Cipher Alias
16  Done
17  <!--NeedCopy-->
```

Configurar un nombre común para la autenticación de certificados de servidor

En el cifrado de extremo a extremo con autenticación de servidor habilitada, puede incluir un nombre común en la configuración de un servicio SSL o grupo de servicios. El nombre que especifique se compara con el nombre común en el certificado de servidor durante un protocolo de enlace SSL. Si los dos nombres coinciden, el apretón de manos se realiza correctamente.
Si los nombres comunes no coinciden, el nombre común especificado para el servicio o grupo de servicios se compara con los valores del campo Nombre alternativo del sujeto (SAN) del certificado. Si coincide con uno de esos valores, el apretón de manos se realiza correctamente. Esta configuración resulta especialmente útil si hay, por ejemplo, dos servidores detrás de un firewall y uno de los servidores suplantación de identidad del otro. Si el nombre común no está marcado, se acepta un certificado presentado por cualquiera de los servidores si la dirección IP coincide.

Nota: Solo se comparan las entradas DNS de nombre de dominio, URL e ID de correo electrónico en el campo SAN.

Configurar la verificación de nombres comunes para un servicio SSL o grupo de servicios mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para especificar la autenticación del servidor con verificación de nombre común y verificar la configuración:

1. Para configurar un nombre común en un servicio, escriba:

```
1  set ssl service <serviceName> -commonName <string> -serverAuth
       ENABLED
2  show ssl service <serviceName>
3  <!--NeedCopy-->
```

2. Para configurar un nombre común en un grupo de servicios, escriba:


```
set ssl serviceGroup <serviceGroupName> -commonName <string> -
    serverAuth ENABLED
show ssl serviceGroup <serviceGroupName>
<!--NeedCopy-->
```

Ejemplo:

```
> set ssl service svc1 -commonName xyz.com -serverAuth ENABLED
<!--NeedCopy-->
```

```
show ssl service svc

     Advanced SSL configuration for Back-end SSL Service svc1:
     DH: DISABLED
     Ephemeral RSA: DISABLED
     Session Reuse: ENABLED Timeout: 300 seconds
     Cipher Redirect: DISABLED
     SSLv2 Redirect: DISABLED
     Server Auth: ENABLED Common Name: www.xyz.com
     SSL Redirect: DISABLED
     Non FIPS Ciphers: DISABLED
     SNI: DISABLED
     SSLv2: DISABLED SSLv3: ENABLED TLSv1: ENABLED
    1) CertKey Name: cacert CA Certificate OCSPCheck: Optional
    1) Cipher Name: ALL
     Description: Predefined Cipher Alias
Done
<!--NeedCopy-->
```

Configurar la verificación de nombres comunes para un servicio SSL o grupo de servicios mediante la interfaz gráfica de usuario

1. Vaya a **Administración de Tráfico > Equilibrio de carga > Servicios** o Vaya a **Administración del Tráfico > Equilibrio de carga > Grupos**de servicios y abra un servicio o grupo de servicios.
2. En la sección Parámetros SSL, seleccione Habilitar autenticación de servidor y especifique un nombre común.

Acciones y directivas de SSL

October 5, 2021

Una directiva SSL evalúa el tráfico entrante y aplica una acción predefinida a las solicitudes que coinciden con una regla (expresión). Configure las acciones antes de crear las directivas, de modo que pueda especificar una acción al crear una directiva. Para poner en vigor una directiva, realice una de las siguientes acciones:

- Enlazar la directiva a un servidor virtual del dispositivo para que se aplique únicamente al tráfico que fluye a través de ese servidor virtual.
- Enlazar la directiva de forma global para que se aplique a todo el tráfico que fluye a través del dispositivo.

Las acciones SSL definen la configuración SSL que puede aplicar a las solicitudes seleccionadas. Se asocia una acción a una o varias directivas. Los datos de las solicitudes o respuestas de conexión del cliente se comparan con una regla especificada en la directiva y la acción se aplica a las conexiones que coinciden con la regla (expresión).

Puede configurar directivas clásicas con expresiones clásicas y directivas avanzadas con expresiones de directivas avanzadas para SSL.

Nota: Los usuarios que no tienen experiencia en la configuración de directivas en la CLI suelen encontrar que el uso de la utilidad de configuración resulta considerablemente más sencillo.

Puede asociar una acción definida por el usuario o una acción integrada a una directiva avanzada. Las directivas clásicas solo permiten acciones definidas por el usuario. En Directiva avanzada, también puede agrupar las directivas bajo un rótulo de directiva, en cuyo caso solo se aplican cuando se invocan desde otra directiva.

Los usos habituales de las acciones y directivas SSL incluyen la autenticación de cliente por directorio, la compatibilidad con Outlook web Access y las inserciones de encabezados basados en SSL. Las inserciones de encabezados basados en SSL contienen la configuración SSL necesaria para un servidor cuyo procesamiento SSL se ha descargado en el dispositivo Citrix ADC.

Directivas SSL

January 21, 2022

Las directivas del dispositivo Citrix ADC ayudan a identificar conexiones específicas que quiere procesar. El procesamiento se basa en las acciones configuradas para esa directiva concreta. Una vez creada la directiva y configurada una acción para ella, debe realizar una de las siguientes acciones:

- Enlazar la directiva a un servidor virtual del dispositivo para que se aplique únicamente al tráfico que fluye a través de ese servidor virtual.
- Enlazar la directiva de forma global para que se aplique a todo el tráfico que fluye a través de cualquier servidor virtual configurado en el dispositivo Citrix ADC.

La función SSL del dispositivo Citrix ADC admite directivas avanzadas (avanzadas). Para obtener una descripción completa de las expresiones de directivas avanzadas, cómo funcionan y cómo configurarlas manualmente, consulte Directivas y expresiones. Para obtener más información sobre las expresiones SSL, consulte Expresiones de directiva avanzadas: análisis de SSL.

> **Nota:**
>
> Los usuarios que no tienen experiencia en la configuración de directivas en la CLI suelen encontrar que utilizar la utilidad de configuración es mucho más fácil.

Las directivas SSL requieren que cree una acción antes de crear una directiva, de modo que pueda especificar las acciones al crear las directivas.
En las directivas SSL Advanced, también puede usar las acciones integradas. Para obtener más información sobre las acciones integradas, consulte Acciones integradas SSL y acciones definidas porel usuario.

Directivas SSL Advanced

Una directiva SSL Advanced, también conocida como directiva avanzada, define un control o una acción de datos que se debe realizar en las solicitudes. Por lo tanto, las directivas SSL se pueden clasificar como directivas de control y directivas de datos:

- **Directiva de control**. Una directiva de control utiliza una acción de control, como forzar la autenticación del cliente.
  Nota: En la versión 10.5 o posterior, denegar renegociación SSL (denySSLReneg) se establece, de forma predeterminada, en ALL. Sin embargo, las directivas de control, como CLIENTAUTH, desencadenan un apretón de manos de renegociación. Si utiliza dichas directivas, debe establecer DenysslReneg en NO.
- **Directiva de datos**. Una directiva de datos utiliza una acción de datos, como insertar algunos datos en la solicitud.

Los componentes esenciales de una directiva son una expresión y una acción. La expresión identifica las solicitudes en las que se va a realizar la acción.

Puede configurar una directiva avanzada con una acción integrada o una acción definida por el usuario. Puede configurar una directiva con una acción integrada sin crear una acción independiente. Sin embargo, para configurar una directiva con una acción definida por el usuario, primero configure la acción y, a continuación, configure la directiva.

Puede especificar una acción adicional, denominada acción UNDEF, que se realizará cuando la aplicación de la expresión a una solicitud tenga un resultado indefinido.

Configuración de directivas SSL

Puede configurar una directiva SSL Advanced mediante la CLI y la GUI.

Configurar una directiva SSL mediante la CLI

En el símbolo del sistema, escriba:

```
1 add ssl policy <name> -rule <expression> -Action <string> [-undefAction
      <string>] [-comment <string>]
2 <!--NeedCopy-->
```

Configurar una directiva SSL mediante la interfaz gráfica de usuario

Vaya a **Administración del tráfico > SSL > Directivas** y, en la ficha **Directivas**, haga clic en *Agregar*.

Compatibilidad con directivas SSL con protocolo TLS1.3

A partir de la versión 13.0 compilación 71.x y posteriores, se agrega compatibilidad con las directivas SSL con el protocolo TLS1.3. Cuando se negocia el protocolo TLSv1.3 para una conexión, las reglas de directiva que inspeccionan los datos TLS recibidos del cliente desencadenan ahora la acción configurada.

Por ejemplo, si la siguiente regla de directiva devuelve true, el tráfico se reenvía al servidor virtual definido en la acción.

```
1 add ssl action action1 -forward vserver2
2 add ssl policy pol1 -rule client.ssl.client_hello.sni.contains( “xyz” )
      -action action1
3 <!--NeedCopy-->
```

Limitaciones

- Las directivas de control no son compatibles.
- No se admiten las acciones siguientes:

- DOCLIENTAUTH
- NOCLIENTAUTH
- caCertGrpName
- clientCertVerification
- ssllogProfile

Acciones integradas SSL y acciones definidas por el usuario

August 20, 2021

A menos que solo necesite las acciones integradas en sus directivas, debe crear las acciones antes de crear las directivas. A continuación, puede especificar las acciones al crear las directivas. Las acciones integradas son de dos tipos, acciones de control y acciones de datos. Las acciones de control se utilizan en las directivas de control y las acciones de datos en las directivas de datos.

Las acciones de control integradas son:

- doClientAuth—Ejecute la autenticación de certificados de cliente. (No compatible con TLS1.3)
- NoClientAuth—No realice la autenticación de certificados de cliente. (No compatible con TLS1.3)

Las acciones de datos integradas son:

- Restablecer: cierre la conexión enviando un paquete RST al cliente.
- Descartar: Suelta todos los paquetes del cliente. La conexión permanece abierta hasta que el cliente la cierra.
- Noop: Reenvía el paquete sin realizar ninguna operación en él.

Nota: Las acciones dependientes de la autenticación del cliente, como ClientCertVerification y SSLLogProfile, no son compatibles con el protocolo TLS 1.3.

Puede crear acciones de datos definidas por el usuario. Si habilita la autenticación de cliente, puede crear una acción SSL para insertar datos de certificado de cliente en el encabezado de solicitud antes de reenviar la solicitud al servidor web.

Si una evaluación de directivas resulta en un estado indefinido, se realiza una acción del FNUD. Para una directiva de datos o una directiva de control, puede especificar RESET, DROP o NOOP como acción UNDEF. Para una directiva de control, también tiene la opción de especificar DOCENTEAUTH o NOCLIENTEAUTH.

Ejemplos de acciones integradas en una directiva

En el ejemplo siguiente, si el cliente envía un cifrado distinto de un cifrado de categoría EXPORT, el dispositivo Citrix ADC solicita la autenticación del cliente. El cliente tiene que proporcionar un certifi-

cado válido para una transacción correcta.

```
add ssl policy pol1 -rule CLIENT.SSL.CIPHER_EXPORTABLE.NOT -reqAction
   DOCLIENTAUTH
<!--NeedCopy-->
```

En los ejemplos siguientes se supone que la autenticación de cliente está habilitada.

Si la versión del certificado proporcionado por el usuario coincide con la versión de la directiva, no se realiza ninguna acción y se reenvía el paquete:

```
add ssl policy pol1 -rule CLIENT.SSL.CLIENT_CERT.VERSION.EQ(2) -
   reqAction NOOP
<!--NeedCopy-->
```

Si la versión del certificado proporcionado por el usuario coincide con la versión de la directiva, se elimina la conexión:

```
add ssl policy pol1 -rule CLIENT.SSL.CLIENT_CERT.VERSION.EQ(2) -
   reqAction DROP
<!--NeedCopy-->
```

Si la versión del certificado proporcionado por el usuario coincide con la versión de la directiva, se restablece la conexión:

```
add ssl policy pol1 -rule CLIENT.SSL.CLIENT_CERT.VERSION.EQ(2) -
   reqAction RESET
<!--NeedCopy-->
```

Verificación de certificados de cliente con autenticación de cliente basada en directivas

Puede establecer la verificación de certificados de cliente como obligatoria u opción cuando haya configurado la autenticación de cliente basada en directivas. El valor predeterminado es obligatorio.

Establezca la verificación de certificados de cliente como opcional mediante la CLI

En el símbolo del sistema, escriba:


```
add ssl action <name> ((-clientAuth ( DOCLIENTAUTH | NOCLIENTAUTH ) [-
    clientCertVerification ( Mandatory | Optional )]
<!--NeedCopy-->
```

Ejemplo:

```
add ssl action sslact -clientauth DOCLIENTAUTH -clientcertverification
    OPTIONAL
<!--NeedCopy-->
```

Establezca la verificación de certificados de cliente como opcional mediante la interfaz gráfica de usuario

1. Vaya a **Administración de Tráfico > SSL > Directivas**.
2. En la ficha **Acciones SSL**, haga clic en **Agregar**.
3. Especifique un nombre y, en la lista **Verificación de certificados de cliente**, seleccione **Opcional**.

Acciones SSL definidas por el usuario

Además de las acciones integradas, también puede configurar otras acciones SSL en función de su implementación. Estas acciones se denominan acciones definidas por el usuario.

Configurar una acción SSL definida por el usuario mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para configurar una acción y verificar la configuración:

```
add SSL action <name> -clientAuth(DOCLIENTAUTH | NOCLIENTAUTH) -
    clientCert (ENABLED | DISABLED) certHeader <string> -clientHeader <
    string> -clientCertSerialNumber (ENABLED | DISABLED) -
    certSerialHeader <string> -clientCertSubject (ENABLED | DISABLED) -
    certSubjectHeader <string> -clientCertHash (ENABLED | DISABLED) -
    certHashHeader <string> -clientCertIssuer (ENABLED | DISABLED) -
    certIssuerHeader <string> -sessionID (ENABLED | DISABLED) -
    sessionIDheader <string> -cipher (ENABLED | DISABLED) -cipherHeader
    <string> -clientCertNotBefore (ENABLED | DISABLED) -
    certNotBeforeHeader <string> -clientCertNotAfter (ENABLED | DISABLED
    ) -certNotAfterHeader <string> -OWASupport (ENABLED | DISABLED)
```



```
<!--NeedCopy-->
```

```
show ssl action [<name>]
<!--NeedCopy-->
```

Ejemplo:

```
add ssl action Action-SSL-ClientCert -clientCert ENABLED -certHeader "X
   -Client-Cert"
<!--NeedCopy-->
```

```
show ssl action Action-SSL-ClientCert

1)      Name: Action-SSL-ClientCert
        Data Insertion Action:
        Cert Header: ENABLED            Cert Tag: X-Client-Cert
Done
<!--NeedCopy-->
```

Configurar una acción SSL definida por el usuario mediante la interfaz gráfica de usuario

Vaya a **Administración del tráfico > SSL > Directivas** y, en la ficha **Acciones**, haga clic en **Agregar**.

Configurar una acción SSL para reenviar tráfico de cliente a otro servidor virtual

Los administradores pueden configurar una acción SSL para reenviar el tráfico de cliente recibido en un servidor virtual SSL a otro servidor virtual para evitar la descarga de SSL. O para finalizar la conexión en el dispositivo ADC. Este servidor virtual puede ser del tipo: SSL, TCP o SSL_BRIDGE. Por ejemplo, los administradores pueden optar por reenviar la solicitud a otro servidor virtual para que realice más acciones en lugar de terminar la conexión si alguno de los siguientes casos:

- El dispositivo no tiene un certificado.
- El dispositivo no admite un cifrado específico.

Para lograr lo anterior, se agrega un nuevo punto de enlace 'CLIENTHELLO_REQ' para evaluar el tráfico del cliente cuando se recibe un saludo de cliente. Si la directiva enlazada al servidor virtual que recibe tráfico de cliente se evalúa como true después de analizar el saludo del cliente, el tráfico se reenvía

a otro servidor virtual. Si este servidor virtual es de tipo SSL, realiza el protocolo de enlace. Si este servidor virtual es de tipo TCP o SSL_BRIDGE, el servidor back-end realiza el protocolo de enlace.

En la versión 12.1-49.x, solo se admiten las acciones de reenvío y restablecimiento para el punto de enlace CLIENTHELLO_REQ. Los prefijos de expresión siguientes están disponibles:

- CLIENT.SSL.CLIENT_HELLO.CIPHERS.HAS_HEXCODE
- CLIENT.SSL.CLIENT_HELLO.CLIENT_VERSION
- CLIENT.SSL.CLIENT_HELLO.IS_RENEGOTIATE
- CLIENT.SSL.CLIENT_HELLO.IS_REUSE
- CLIENT.SSL.CLIENT_HELLO.IS_SCSV
- CLIENT.SSL.CLIENT_HELLO.IS_SESSION_TICKET
- CLIENT.SSL.CLIENT_HELLO.LENGTH
- CLIENT.SSL.CLIENT_HELLO.SNI
- CLIENT.SSL.CLIENT_HELLO.ALPN.HAS_NEXTPROTOCOL (de la versión 13.0 compilación 61.x)

Para obtener una descripción de estos prefijos, consulte Expresiones de directivas avanzadas: análisis de SSL.

`forward` Se agrega un parámetro al `add SSL action` comando y `CLIENTHELLO_REQ` se agrega un nuevo punto de enlace al `bind ssl vserver` comando.

Configuración mediante la CLI

En el símbolo del sistema, escriba:

```
add ssl action <name> -forward <virtual server name>

add ssl policy <name> -rule <expression> -action <string>

bind ssl vserver <vServerName> -policyName <string> -priority <
   positive_integer> -type <type>
<!--NeedCopy-->
```

EJEMPLO:

```
add ssl action act1 -forward v2

add ssl policy pol1 -rule client.ssl.client_hello.ciphers.has_hexcode(0
   x002f) -action act1

bind ssl vserver v1 -policyName pol1 -priority 1 -type CLIENTHELLO_REQ
```



```
<!--NeedCopy-->
```

Configuración mediante la GUI

Vaya a **Administración de Tráfico > SSL > Directivas**.

Crear acción SSL:

1. En **Acciones SSL**, haga clic en **Agregar**.
2. En **Crear acción SSL**, especifique un nombre para la acción.
3. En el **Servidor virtual de acción directa**, seleccione un servidor virtual existente o agregue un nuevo servidor virtual al que reenviar el tráfico.
4. Opcionalmente, defina otros parámetros.
5. Haga clic en **Crear**.

Crear directiva SSL:

1. En **Directivas SSL**, haga clic en **Agregar**.
2. En **Crear directiva SSL**, especifique un nombre para la directiva.
3. En **Acción**, seleccione la acción que creó anteriormente.
4. En el **Editor de expresiones**, escriba la regla que quiere evaluar.
5. Haga clic en **Crear**.

Cree o agregue un servidor virtual y una directiva de enlace:

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**.
2. Agregue o seleccione un servidor virtual.
3. En **Configuración avanzada**, haga clic en **Directivas SSL**.
4. Haga clic en la sección Directiva SSL.
5. En **Seleccionar directiva**, seleccione la directiva que creó anteriormente.
6. En **Enlace de directivas**, especifique una prioridad para la directiva.
7. En **Tipo**, seleccione **CLIENTHELLO_REQ**.
8. Haga clic en **Vincular**.
9. Haga clic en **Done**.

Para obtener información sobre la configuración de extremo a extremo para los casos de uso más populares, consulte los siguientes temas:

- Configure la acción SSL para reenviar el tráfico de cliente si el dispositivo no tiene un certificado específico de dominio (SNI).
- Configure una acción SSL para reenviar el tráfico del cliente en función del protocolo de la extensión ALPN del mensaje de saludo del cliente.
- Configure la acción SSL para reenviar el tráfico de cliente si el ADC no admite un cifrado.

Acción SSL para seleccionar selectivamente CA basadas en SNI para la autenticación del cliente

Solo puede enviar la lista de CA basadas en SNI (dominio) en la solicitud de certificado de cliente en lugar de la lista de todas las CA enlazadas a un servidor virtual SSL. Por ejemplo, cuando se recibe un saludo de cliente, solo se envían los certificados de CA basados en la expresión de directiva SSL (por ejemplo, SNI). Para enviar un conjunto específico de certificados, debe crear un grupo de certificados de CA. A continuación, vincule este grupo a una acción SSL y vincule la acción a una directiva SSL. Si la directiva enlazada al servidor virtual que recibe tráfico de cliente se evalúa como true después de analizar el saludo del cliente, solo se envía un grupo de certificados de CA específico en el certificado de solicitud de cliente.

Anteriormente, tenía que enlazar certificados de CA a un servidor virtual SSL. Con esta mejora, puede simplemente agregar grupos de certificados de CA y asociarlos a una acción SSL.

Nota: Habilite la autenticación de cliente y SNI en el servidor virtual SSL. Enlazar los certificados SNI correctos al servidor virtual.

Siga estos pasos:

1. Agregue un grupo de certificados de CA.
2. Agregue pares de claves de certificado.
3. Enlazar los pares de clave de certificado a este grupo.
4. Agregue una acción SSL.
5. Agregue una directiva SSL. Especifique la acción en la directiva.
6. Enlazar la directiva a un servidor virtual SSL. Especifique el punto de enlace como CLIENTHELLO_REQ.

Configuración mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos en una secuencia:

```
1 add ssl caCertGroup <caCertGroupName>
2 add ssl certkey <certkey_name> -cert <cert> -key <key>
3 bind ssl caCertGroup <caCertGroupName> <certkey_name>
4 add ssl action <name> -caCertGrpName <string>
5 add ssl policy <name> -rule <expression> -action <string>
6 bind ssl vserver <vServerName> -policyName <string> -priority <
     positive_integer> -type CLIENTHELLO_REQ
7 <!--NeedCopy-->
```


Ejemplo:

```
add ssl cacertGroup ca_cert_group

add ssl certkey ca_certkey1 -cert cacert1 -key cakey1
add ssl certkey ca_certkey2 -cert cacert2 -key cakey2
add ssl certkey snicert -cert snicert -key snikey

bind ssl cacertGroup ca_cert_group ca_certkey1
bind ssl caCertGroup ca_cert_group ca_certkey2
<!--NeedCopy-->
```

```
sh ssl caCertGroup ca_cert_group

CA GROUP NAME:     ca_cert_group
ACTIONS REFERRING: 1

1) CertKey Name: ca_certkey1   CA Certificate   CRLCheck: Optional
   CA_Name Sent
2) CertKey Name: ca_certkey2   CA Certificate   CRLCheck: Optional
   CA_Name Sent
<!--NeedCopy-->
```

```
add ssl action pick_ca_group -cacertGrpName ca_cert_group
<!--NeedCopy-->
```

```
sh ssl action pick_ca_group
1) Name: pick_ca_group
   Type: Data Insertion
   PickCaCertGroup: ca_cert_group
   Hits: 0
   Undef Hits: 0
   Action Reference Count: 1
<!--NeedCopy-->
```



```
add ssl policy snipolicy -rule client.ssl.client_hello.sni.contains(”
    abc”) -action pick_ca_group
bind ssl vserver v_SSL -policyName snipolicy -type CLIENTHELLO_REQ -
    priority 10
<!--NeedCopy-->
```

```
sh ssl policy snipolicy
    Name: snipolicy
    Rule: client.ssl.client_hello.sni.contains(”abc”)
    Action: pick_ca_group
    UndefAction: Use Global
    Hits: 0
    Undef Hits: 0


    Policy is bound to following entities
1)  Bound to: CLIENTHELLO_REQ VSERVER v_SSL
    Priority: 10
<!--NeedCopy-->
```

```
set ssl vserver v_SSL -clientauth ENABLED -SNIEnable ENABLED
bind ssl vserver v_SSL -certkeyName snicert -sniCert
<!--NeedCopy-->
```

```
sh ssl vserver v_SSL

    Advanced SSL configuration for VServer v_SSL:
    DH: DISABLED
    DH Private-Key Exponent Size Limit: DISABLED   Ephemeral RSA:
       ENABLED   Refresh Count: 0
    Session Reuse: ENABLED   Timeout: 120 seconds
    Cipher Redirect: DISABLED
    SSLv2 Redirect: DISABLED
    ClearText Port: 0
    Client Auth: ENABLED   Client Cert Required: Mandatory
    SSL Redirect: DISABLED
    Non FIPS Ciphers: DISABLED
    SNI: ENABLED
    OCSP Stapling: DISABLED
```



```
15      HSTS: DISABLED
16      HSTS IncludeSubDomains: NO
17      HSTS Max-Age: 0
18      SSLv2: DISABLED  SSLv3: ENABLED  TLSv1.0: ENABLED  TLSv1.1: ENABLED
              TLSv1.2: ENABLED  TLSv1.3: DISABLED
19      Push Encryption Trigger: Always
20      Send Close-Notify: YES
21      Strict Sig-Digest Check: DISABLED
22      Zero RTT Early Data: DISABLED
23      DHE Key Exchange With PSK: NO
24      Tickets Per Authentication Context: 1
25
26      ECC Curve: P_256, P_384, P_224, P_521
27
28  1)  CertKey Name: snicert   Server Certificate for SNI
29
30
31      Data policy
32  1)  Policy Name: snipolicy  Priority: 10
33
34
35
36  1)  Cipher Name: DEFAULT
37      Description: Default cipher list with encryption strength >= 128bit
38  <!--NeedCopy-->
```

Configuración mediante la GUI

Cree un grupo de certificados de CA y vincule certificados al grupo:

1. Vaya a **Administración de tráfico > SSL > Grupo de certificados de CA**.
2. Haga clic en **Agregar** y especifique un nombre para el grupo.
3. Haga clic en **Crear**.
4. Seleccione el **grupo de certificados de CA** y, a continuación, haga clic en **Mostrar enlaces**.
5. Haga clic en **Vincular**.
6. En la página **Enlace de certificados de CA**, seleccione un certificado existente o haga clic en Agregar para agregar un certificado nuevo.
7. Haga clic en **Seleccionar** y, a continuación, haga clic en **Vincular**.
8. Para enlazar otro certificado, repita los pasos 5 a 7.
9. Haga clic en **Cerrar**.

Vaya a **Administración de Tráfico > SSL > Directivas**.

Crear acción SSL:

1. En **Acciones SSL**, haga clic en **Agregar**.
2. En **Crear acción SSL**, especifique un nombre para la acción.
3. En el **Servidor virtual de acción directa**, seleccione un servidor virtual existente o agregue un servidor virtual al que reenviar el tráfico.
4. Opcionalmente, defina otros parámetros.
5. Haga clic en **Crear**.

Crear directiva SSL:

1. En **Directivas SSL**, haga clic en **Agregar**.
2. En **Crear directiva SSL**, especifique un nombre para la directiva.
3. En **Acción**, seleccione la acción creada anteriormente.
4. En el **Editor de expresiones**, escriba la regla que quiere evaluar.
5. Haga clic en **Crear**.

Cree o agregue un servidor virtual y una directiva de enlace:

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**.
2. Agregue o seleccione un servidor virtual.
3. En **Configuración avanzada**, haga clic en **Directivas SSL**.
4. Haga clic en la sección Directiva SSL.
5. En **Seleccionar directiva**, seleccione la directiva que creó anteriormente.
6. En **Enlace de directivas**, especifique una prioridad para la directiva.
7. En **Tipo**, seleccione **CLIENTHELLO_REQ**.
8. Haga clic en **Vincular**.
9. Haga clic en **Done**.

Desenlazar un grupo de certificados de CA mediante la interfaz gráfica de usuario

1. Vaya a **Administración de tráfico > SSL > Grupo de certificados de CA**.
2. Seleccione un grupo de certificados y haga clic en **Mostrar enlaces**.
3. Seleccione el certificado que quiere quitar del grupo y haga clic en **Desenlazar**.
4. Si se le solicita confirmación, haga clic en **Sí••.
5. Haga clic en **Cerrar**.

Quitar un grupo de certificados de CA mediante la interfaz gráfica de usuario

1. Vaya a **Administración de tráfico > SSL > Grupo de certificados de CA**.
2. Seleccione un grupo de certificados y haga clic en **Eliminar**.
3. Si se le solicita confirmación, haga clic en **Sí**.

Enlace de directivas SSL

August 20, 2021

Puede enlazar directivas SSL globalmente o solo a un servidor virtual de tipo SSL. Las directivas enlazadas globalmente se evalúan después de evaluar todas las directivas vinculadas a servicios, servidores virtuales u otros puntos de enlace Citrix ADC. Si los datos entrantes coinciden con alguna de las reglas configuradas en la directiva SSL, se activa la directiva y se lleva a cabo la acción asociada.

Al vincular una directiva SSL a un servidor virtual, debe seleccionar uno de los siguientes puntos de enlace:

- REQUEST (Punto de enlace predeterminado. La evaluación de directivas se realiza en la capa HTTP después de completar el protocolo de enlace SSL.)
- INTERCEPT_REQ (Esta opción se aplica a una configuración de Citrix Secure Web Gateway. Para obtener más información, consulte Infraestructura de directivas SSL para la interceptaciónSSL).
- CLIENTHELLO_REQ

Del mismo modo, al desvincular una directiva de un servidor virtual, debe especificar el punto de enlace.

Si especifica CLIENTHELLO_REQ como punto de enlace, la directiva se evalúa cuando se recibe un mensaje de saludo del cliente. Las acciones permitidas son RESET, FORWARD y `caCertGrpName`. La acción de restablecimiento finaliza la conexión. La acción de reenvío reenvía la solicitud a un servidor virtual de equilibrio de carga para su procesamiento. La acción `caCertGrpName` elige de manera selectiva las CA basadas en SNI para la autenticación del cliente. Para obtener más información sobre las acciones SSL, consulte Acciones integradas de SSL y acciones definidas porel usuario.

Nota: La acción CacertGrpName no es compatible con el protocolo TLS 1.3.

Vincular una directiva SSL globalmente mediante la CLI

En el símbolo del sistema, escriba el siguiente comando para enlazar una directiva SSL global y verificar la configuración:

```
bind ssl global - policyName <string> [- priority <positive_integer>]
show ssl global
<!--NeedCopy-->
```

Ejemplo:


```
bind ssl global -policyName Policy-SSL-2 -priority 90
Done

sh ssl global

     1) Name: Policy-SSL-2 Priority: 90
     2) Name: Policy-SSL-1 Priority: 100
     Done
<!--NeedCopy-->
```

Enlazar una directiva SSL globalmente mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico** > **SSL** > **Directivas**.
2. En el panel de detalles, haga clic en **Vinculaciones globales**.
3. En el cuadro de diálogo **Vincular o desvincular directivas SSL a global**, haga clic en **Insertar directiva**.
4. En la lista **Nombre de directiva**, seleccione una directiva.
5. Si lo quiere, arrastre la entrada a una nueva posición en el banco de directivas para actualizar automáticamente el nivel de prioridad.
6. Haga clic en **Aceptar**. Aparece un mensaje en la barra de estado que indica que la directiva se ha enlazado correctamente.

Enlazar o desvincular una directiva SSL a un servidor virtual mediante la CLI

En el símbolo del sistema, escriba el siguiente comando para enlazar una directiva SSL a un servidor virtual y verificar la configuración:

```
bind ssl vserver <vServerName> -policyName <string> -priority <
   positive_integer> -type <type>

unbind ssl vserver <vServerName> -policyName <string> -priority <
   positive_integer> -type <type>

<!--NeedCopy-->
```

Ejemplo:

```
bind ssl vserver v1 -policyName pol1 -priority 1 -type CLIENTHELLO_REQ
<!--NeedCopy-->
```



```
unbind ssl vserver v1 -policyName pol1 -priority 1 -type
   CLIENTHELLO_REQ
<!--NeedCopy-->
```

```
show ssl vserver vs-server

Advanced SSL configuration for VServer vs-server:

DH: DISABLED

Ephemeral RSA: ENABLED          Refresh Count: 1000

Session Reuse: ENABLED          Timeout: 120 seconds

Cipher Redirect: DISABLED

SSLv2 Redirect: DISABLED

ClearText Port: 80

Client Auth: DISABLED

SSL Redirect: ENABLED

SSL-REDIRECT Port Rewrite: ENABLED

Non FIPS Ciphers: DISABLED

SSLv2: DISABLED SSLv3: ENABLED  TLSv1: ENABLED

1)      Policy Name: ssl-policy-1        Priority: 10

1)      Cipher Name: DEFAULT

            Description: Predefined Cipher Alias

Done
<!--NeedCopy-->
```


Enlazar una directiva SSL a un servidor virtual mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**y abra un servidor virtual SSL.
2. En **Configuración avanzada**, seleccione **Directiva SSL**. Haga clic en la sección **de directivas SSL** para enlazar una directiva al servidor virtual.
3. En la página **Enlace de directivas**, seleccione una directiva existente o agregue una nueva directiva.
4. Especifique la prioridad y el tipo (punto de enlace) para la directiva.
5. Seleccione **Vincular**.
6. Seleccione **Listo**.

Etiquetas de directiva SSL

January 12, 2021

Las etiquetas de directiva son titulares de las directivas. Una etiqueta de directiva ayuda a administrar un grupo de directivas, denominado banco de directivas, que se puede invocar desde otra directiva. Las etiquetas de directiva SSL pueden ser etiquetas de control o etiquetas de datos, según el tipo de directivas que se incluyen en la etiqueta de directiva. Solo puede agregar directivas de datos en una etiqueta de directiva de datos y solo directivas de control en una etiqueta de directiva de control. Para crear el banco de directivas, vincule las directivas a la etiqueta y especifique el orden de evaluación de cada directiva en relación con otras del banco de directivas para la etiqueta de directiva. En la CLI, introduzca dos comandos para crear una etiqueta de directiva y enlazar directivas a la etiqueta de directiva. En la utilidad de configuración, puede seleccionar opciones en un cuadro de diálogo.

Nota: Las etiquetas de directiva de control de tipo no son compatibles con el protocolo TLS 1.3.

Cree una etiqueta de directiva SSL y vincule directivas a la etiqueta mediante la CLI

En el símbolo del sistema, escriba:

```
add ssl policylabel <labelName> -type ( CONTROL | DATA )

bind ssl policylabel <labelName> <policyName> <priority> [<
   gotoPriorityExpression>] [-invoke (<labelType> <labelName>) ]
<!--NeedCopy-->
```

Ejemplo:


```
add ssl policylabel cpl1 -type CONTROL

add ssl policylabel dpl1 -type DATA

bind ssl policylabel cpl1 -policyName ctrlpol -priority 1

bind ssl policylabel dpl1 -policyName datapol -priority 1
<!--NeedCopy-->
```

Configure una etiqueta de directiva SSL y vincule directivas a la etiqueta mediante la interfaz gráfica de usuario

Vaya a **Administración del tráfico > SSL > Etiquetas de directiva**y configure una etiqueta de directiva SSL.

Registro SSL selectivo

April 5, 2022

En una implementación grande que comprende miles de servidores virtuales, se registra toda la información relacionada con SSL. Anteriormente, no era fácil filtrar los éxitos y fallos de autenticación del cliente y del apretón de manos SSL para algunos servidores virtuales críticos. Realizar un recorrido por todo el registro para obtener esta información era una tarea laboriosa y tediosa porque la infraestructura no ofrecía el control para filtrar los registros. Ahora, puede registrar información relacionada con SSL en `ns.log`, para un servidor virtual específico o para un grupo de servidores virtuales. Esta información es especialmente útil para depurar errores. Para registrar esta información, debe agregar un perfil de registro SSL.

Consulte la salida de ejemplo de ns.log para obtener una autenticación de cliente correcta al final de esta página.

> **Importante:**
>
> Establezca el nivel de registro de syslog en DEBUG. En el símbolo del sistema, escriba:
>
> `set audit syslogParams -logLevel DEBUG`
>
> Cuando se establece la depuración, se incluyen los registros SSL tanto para el front-end (servidores virtuales) como para el back end (servicios y grupos de servicios). Sin embargo, el registro SSL selectivo ofrece control solo sobre el front-end.

Perfil de registro SSL

Un perfil de registro SSL proporciona control sobre el registro de los siguientes eventos para un servidor virtual o un grupo de servidores virtuales:

- Éxitos y fallos de la autenticación del cliente, o solo fallos.
- Éxitos y fracasos del apretón de manos SSL, o solo fallos.

De forma predeterminada, todos los parámetros están inhabilitados.

Un perfil de registro SSL se puede establecer en un perfil SSL o en una acción SSL. Si se establece en un perfil SSL, puede registrar la información de éxito y error del protocolo de manos SSL tanto de la autenticación del cliente como del protocolo de manos SSL. Si se establece en una acción SSL, solo puede registrar la información de éxito y error de la autenticación del cliente porque el apretón de manos se ha completado antes de que se evalúe la directiva.

El éxito y los errores de la autenticación del cliente y del protocolo de manos SSL se registran incluso si no configura un perfil de registro SSL. Sin embargo, el registro selectivo solo es posible si se utiliza un perfil de registro SSL.

> **Nota:**
>
> El perfil de registro SSL se admite en configuraciones de clúster y alta disponibilidad.

Agregar un perfil de registro SSL mediante la CLI

En el símbolo del sistema, escriba:

```
add ssl logprofile <name> [-sslLogClAuth ( ENABLED | DISABLED )] [-
    ssllogClAuthFailures ( ENABLED | DISABLED )] [-sslLogHS ( ENABLED |
    DISABLED )] [-sslLogHSfailures ( ENABLED | DISABLED )]
<!--NeedCopy-->
```

Parámetros:

Name:

Nombre del perfil de registro SSL. Debe comenzar con un carácter alfanumérico o de subrayado (_) ASCII y debe contener solo caracteres alfanuméricos ASCII, guión bajo, hash (#), punto (.), espacio, dos puntos (:), en (@), igual (=) y guión (-). No se puede cambiar una vez creado el perfil.

El nombre es un argumento obligatorio. Longitud máxima: 127

`sslLogClAuth`:

Registra todos los eventos de autenticación de clientes. Incluye eventos de éxito y fracaso.

Valores posibles: ENABLED, DISABLED

Valor por defecto: DISABLED

sslogClAuthFailures:

Registra todos los eventos de error de autenticación del cliente.

Valores posibles: ENABLED, DISABLED

Valor por defecto: DISABLED

sslLogHS:

Registra todos los eventos relacionados con el apretón de manos SSL. Incluye eventos de éxito y fracaso.

Valores posibles: ENABLED, DISABLED

Valor por defecto: DISABLED

sslLogHSfailures:

Registra todos los eventos de error relacionados con el protocolo de manos SSL.

Valores posibles: ENABLED, DISABLED

Valor por defecto: DISABLED

Ejemplo:

```
> add ssl logprofile ssllog10 -sslLogClAuth ENABLED -sslLogHS ENABLED

 Done

sh ssllogprofile ssllog10

1)      Name: ssllog10

        SSL log ClientAuth [Success/Failures] : ENABLED

        SSL log ClientAuth [Failures] : DISABLED

        SSL log Handshake [Success/Failures] : ENABLED

        SSL log Handshake [Failures] : DISABLED

 Done
<!--NeedCopy-->
```


Agregar un perfil de registro SSL mediante la interfaz gráfica de usuario

Vaya a **Sistema > Perfiles > Perfil de registro SSL** y agregue un perfil.

Modificar un perfil de registro SSL mediante la CLI

En el símbolo del sistema, escriba:

```
set ssl logprofile <name> [-sslLogClAuth ( ENABLED | DISABLED )][-
    ssllogClAuthFailures ( ENABLED | DISABLED )] [-sslLogHS ( ENABLED |
    DISABLED )] [-sslLogHSfailures ( ENABLED | DISABLED )]
<!--NeedCopy-->
```

Ejemplo:

```
set ssllogprofile ssllog10 -ssllogClAuth en -ssllogClAuthFailures en -
    ssllogHS en -ssllogHSfailures en

Done

sh ssllogprofile ssllog10

    1)            Name: ssllog10

                    SSL log ClientAuth [Success/Failures] : ENABLED
                    SSL log ClientAuth [Failures] : ENABLED
                    SSL log Handshake [Success/Failures] : ENABLED
                    SSL log Handshake [Failures] : ENABLED
     Done
<!--NeedCopy-->
```

Modificar un perfil de registro SSL mediante la GUI

1. Vaya a **Sistema > Perfiles > Perfil de registro SSL**, seleccione un perfil y haga clic en **Modificar**.
2. Realice los cambios y haga clic en **Aceptar**.

Ver todos los perfiles de registro SSL mediante la CLI

En el símbolo del sistema, escriba:


```
sh ssl logprofile
<!--NeedCopy-->
```

Ejemplo:

```
sh ssl logprofile

    1)            Name: ssllogp1
                    SSL log ClientAuth [Success/Failures] : ENABLED
                    SSL log ClientAuth [Failures] : ENABLED
                    SSL log Handshake [Success/Failures] : DISABLED
                    SSL log Handshake [Failures] : ENABLED

    2)            Name: ssllogp2
                    SSL log ClientAuth [Success/Failures] : DISABLED
                    SSL log ClientAuth [Failures] : DISABLED
                    SSL log Handshake [Success/Failures] : DISABLED
                    SSL log Handshake [Failures] : DISABLED

    3)            Name: ssllogp3
                    SSL log ClientAuth [Success/Failures] : DISABLED
                    SSL log ClientAuth [Failures] : DISABLED
                    SSL log Handshake [Success/Failures] : DISABLED
                    SSL log Handshake [Failures] : DISABLED

    4)            Name: ssllog10
                    SSL log ClientAuth [Success/Failures] : ENABLED
                    SSL log ClientAuth [Failures] : ENABLED
                    SSL log Handshake [Success/Failures] : ENABLED
                    SSL log Handshake [Failures] : ENABLED
Done
<!--NeedCopy-->
```

Ver todos los perfiles de registro SSL mediante la interfaz gráfica de usuario

Vaya a **Sistema > Perfiles > Perfil de registro SSL**. Se enumeran todos los perfiles.

Adjuntar un perfil de registro SSL a un perfil SSL

Puede adjuntar (establecer) un perfil de registro SSL en un perfil SSL cuando cree un perfil SSL o, más adelante, al modificar el perfil SSL. Puede registrar los éxitos y fallos tanto de la autenticación del

cliente como del apretón de manos.

> **Importante:**
>
> El perfil SSL predeterminado debe estar habilitado para poder adjuntar un perfil de registro SSL. Para obtener más información sobre cómo habilitar el perfil SSL predeterminado, consulte Habilitar el perfil predeterminado.

Adjunte un perfil de registro SSL a un perfil SSL mediante la CLI

En el símbolo del sistema, escriba:

```
set ssl profile <name> [-ssllogProfile <string>]
<!--NeedCopy-->
```

Ejemplo:

```
set ssl profile fron_1 -ssllogProfile ssllog10
<!--NeedCopy-->
```

Adjunte un perfil de registro SSL a un perfil SSL mediante la GUI

1. Vaya a **Sistema > Perfiles > Perfil SSL**.
2. Haga clic en **Modificar** y, en **Perfil de registro SSL**, especifique un perfil.

Adjuntar un perfil de registro SSL a una acción SSL

Puede configurar un perfil de registro SSL solo al crear una acción SSL. No puede modificar una acción SSL para establecer el perfil de registro. Asocie la acción a una directiva. Solo puede registrar los éxitos y los errores de la autenticación del cliente.

Adjunte un perfil de registro SSL a una acción SSL mediante la CLI

En el símbolo del sistema, escriba:

```
add ssl action <name> -clientAuth ( DOCLIENTAUTH | NOCLIENTAUTH ) -
    ssllogProfile <string>
<!--NeedCopy-->
```


Ejemplo:

```
> add ssl action act1 -clientAuth DoCLIENTAUTH -ssllogProfile ssllog10

Done

> sh ssl action act1

    1)            Name: act1
                    Type: Client Authentication (DOCLIENTAUTH)
                    Hits: 0
                    Undef Hits: 0
                    Action Reference Count: 0
                    SSLlogProfile: ssllog10
Done
<!--NeedCopy-->
```

Adjuntar un perfil de registro SSL a una acción SSL mediante la GUI

1. Vaya a **Administración del tráfico > SSL > Directivas** y haga clic en **Acciones SSL**.
2. Haga clic en **Agregar**.
3. En Autenticación de clientes, seleccione **ACTIVADO**.
4. En Perfil de registro SSL, seleccione un perfil de la lista o haga clic en "+" para crear un perfil.
5. Haga clic en **Create**.

Salida de ejemplo del archivo de registro

A continuación se muestra un ejemplo de salida de registro de `ns.log` para una autenticación de cliente correcta.

```
Jan 24 16:24:25 <local0.debug> 10.102.57.80 01/24/2019:10:54:25 GMT  0-PPE-0 : default SSLLOG SSL_HANDSHAKE_SUCCESS 158 0 :  SPCBId 671 - ClientIP 10.102.1.98 - ClientPort 49451 - VserverServiceIP 10.102.57.82 - VserverServicePort 443 - ClientVersion TLSv1.2 - CipherSuite "AES-256-CBC-SHA TLSv1.2 Non-Export 256-bit" - Session New - CLIENT_AUTHENTICATED -SerialNumber "2A" - SignatureAlgorithm "sha1WithRSAEncryption" - ValidFrom "Sep 22 09:15:20 2008 GMT" - ValidTo "Feb  8 09:15:20 2036 GMT" - HandshakeTime 10 ms
Jan 24 16:24:25 <local0.debug> 10.102.57.80 01/24/2019:10:54:25 GMT  0-PPE-0 : default SSLLOG SSL_HANDSHAKE_ISSUERNAME 159 0 :  SPCBId 671
```



```
      - IssuerName " C=IN,ST=KAR,O=Citrix R&D Pvt Ltd,CN=Citrix"
3 Jan 24 16:24:25 <local0.debug> 10.102.57.80 01/24/2019:10:54:25 GMT  0-
    PPE-0 : default SSLLOG SSL_HANDSHAKE_SUBJECTNAME 160 0 :  SPCBId 671
     - SubjectName " C=IN,ST=KAR,O=Citrix Pvt Ltd,OU=A,CN=B"
4 Jan 24 16:24:25 <local0.debug> 10.102.57.80 01/24/2019:10:54:25 GMT  0-
    PPE-0 : default SSLLOG SSL_HANDSHAKE_SUCCESS 161 0 :  Backend SPCBId
     674 - ServerIP 10.102.57.85 - ServerPort 443 - ProtocolVersion
    TLSv1.2 - CipherSuite "AES-256-CBC-SHA TLSv1.2 Non-Export 256-bit" -
     Session Reuse - SERVER_AUTHENTICATED -SerialNumber "3E" -
    SignatureAlgorithm "sha1WithRSAEncryption" - ValidFrom "Sep 24
    06:40:37 2008 GMT" - ValidTo "Feb 10 06:40:37 2036 GMT" -
    HandshakeTime 1 ms
5 Jan 24 16:24:25 <local0.debug> 10.102.57.80 01/24/2019:10:54:25 GMT  0-
    PPE-0 : default SSLLOG SSL_HANDSHAKE_ISSUERNAME 162 0 :  SPCBId 674
    - IssuerName " C=IN,ST=KAR,O=Citrix Pvt Ltd"
6 Jan 24 16:24:25 <local0.debug> 10.102.57.80 01/24/2019:10:54:25 GMT  0-
    PPE-0 : default SSLLOG SSL_HANDSHAKE_SUBJECTNAME 163 0 :  SPCBId 674
     - SubjectName " C=IN,ST=P,L=Q,O=R"
7 <!--NeedCopy-->
```

Compatibilidad con el protocolo DTLS

April 21, 2022

> **Notas:**
>
> - El protocolo DTLSv1.0 es compatible con dispositivos FIPS Citrix ADC MPX/SDX (basados en N2 y N3), VPX y MPX 14000. No es compatible con los HSM externos.
> - El protocolo DTLS 1.0 se admite en dispositivos Citrix ADC que contienen chips SSL Intel Coleto.
> - El protocolo DTLSv1.2 se admite en el front-end de los dispositivos Citrix ADC VPX.
> - El protocolo DTLS 1.2 se admite en el front-end de los dispositivos Citrix ADC que contienen chips SSL Intel Coleto. Para obtener más información sobre las plataformas que contienen chips SSL Intel Coleto, consulte Compatibilidad con plataformas basadas en chips Intel Coleto SSL.
> - No se admiten grupos de servicio de tipo DTLS.
> - El protocolo DTLSv1.2 se admite en el front-end de los dispositivos Citrix ADC MPX (basados en N3).
> - Para obtener información sobre la función de Enlightened Data Transport (EDT) para Citrix Gateway, consulte Función de transporte de datos iluminado de HDX.

> • Para obtener información sobre las plataformas y compilaciones compatibles, consulte Matriz de compatibilidad de hardware y software de Citrix ADC MPX

Los protocolos SSL y TLS se han utilizado tradicionalmente para proteger el tráfico de streaming. Ambos protocolos se basan en TCP, que es lento. Además, TLS no puede gestionar paquetes perdidos o reordenados.

UDP es el protocolo preferido para aplicaciones de audio y vídeo, como Lync, Skype, iTunes, YouTube, vídeos de formación y flash. Sin embargo, UDP no es seguro ni fiable. El protocolo DTLS está diseñado para proteger los datos a través de UDP y se utiliza para aplicaciones como transmisión de medios, VOIP y juegos en línea para la comunicación. En DTLS, a cada mensaje de desafío mutuo se le asigna un número de secuencia específico dentro de ese desafío mutuo. Cuando un par recibe un mensaje de desafío mutuo, puede determinar rápidamente si ese mensaje es el siguiente esperado. Si es así, el par procesa el mensaje. De lo contrario, el mensaje se pone en cola para su administración después de haber recibido todos los mensajes anteriores.

Cree un servidor virtual DTLS y un servicio de tipo UDP. De forma predeterminada, un perfil DTLS (nsdtls_default_profile) está enlazado al servidor virtual. De forma opcional, puede crear y enlazar un perfil DTLS definido por el usuario al servidor virtual.

Nota: Los cifrados RC4 no son compatibles con un servidor virtual DTLS.

Configuración DTLS

Puede utilizar la línea de comandos (CLI) o la utilidad de configuración (GUI) para configurar DTLS en el dispositivo ADC.

Nota: El protocolo DTLS 1.2 se admite en la parte frontal de un dispositivo Citrix ADC VPX. Al configurar un servidor virtual DTLSv1.2, especifique DTLS12. El valor predeterminado es DTLS1.

En el símbolo del sistema, escriba:

```
set ssl vserver DTLS [-dtls1 ( ENABLED | DISABLED )] [-dtls12 ( ENABLED |
DISABLED )]
```

Crear una configuración DTLS mediante la CLI

En el símbolo del sistema, escriba:

```
1 add lb vserver <vserver_name> DTLS <IPAddress>  <port>
2 add service  <service_name>  <IPAddress> UDP 443
3 bind lb vserver  <vserver_name>  <udp_service_name>
4 <!--NeedCopy-->
```


Los pasos siguientes son opcionales:

```
add dtlsProfile dtls-profile -maxretryTime <positive_integer>
set ssl vserver <vserver_name> -dtlsProfileName <dtls_profile_name>
<!--NeedCopy-->
```

Crear una configuración DTLS mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. Cree un servidor virtual de tipo DTLS y vincule un servicio UDP al servidor virtual.
3. Un perfil DTLS predeterminado está enlazado al servidor virtual DTLS. Para enlazar un perfil diferente, en Parámetros SSL, seleccione un perfil DTLS diferente. Para crear un perfil, haga clic en el signo más (+) situado junto a Perfil DTLS.

Compatibilidad con SNI en un servidor virtual DTLS

Para obtener información sobre SNI, consulte Configurar un servidor virtual SNI para un alojamiento seguro de varios sitios.

Configurar SNI en un servidor virtual DTLS mediante la CLI

En el símbolo del sistema, escriba:

```
set ssl vserver <vServerName> -SNIEnable ENABLED
bind ssl vserver <vServerName> -certkeyName <string> -SNICert
show ssl vserver <vServerName>
<!--NeedCopy-->
```

Ejemplo:

```
set ssl vserver v1 -sniEnable ENABLED
bind ssl vserver  v1 -certkeyName san2 -sniCert
bind ssl vserver  v1 -certkeyName san13  - sniCert
bind ssl vserver  v1 -certkeyName san17  - sniCert
<!--NeedCopy-->
```



```
sh ssl vserver v1

Advanced SSL configuration for VServer v1:
DH: DISABLED
DH Private-Key Exponent Size Limit: DISABLED
Ephemeral RSA: ENABLED
Refresh Count: 0
Session Reuse: ENABLED
Timeout: 1800 seconds
Cipher Redirect: DISABLED

ClearText Port: 0
Client Auth: DISABLED
SSL Redirect: DISABLED
Non FIPS Ciphers: DISABLED
SNI: ENABLED
OCSP Stapling: DISABLED
HSTS: DISABLED
HSTS IncludeSubDomains: NO
HSTS Max-Age: 0
DTLSv1: ENABLED
Send Close-Notify: YES
Strict Sig-Digest Check: DISABLED
Zero RTT Early Data: DISABLED
DHE Key Exchange With PSK: NO
Tickets Per Authentication Context: 1

DTLS profile name: nsdtls_default_profile

ECC Curve: P_256, P_384, P_224, P_521

1) CertKey Name: ca
CA Certificate  OCSPCheck: OptionalCA_Name Sent
2) CertKey Name: san2 Server Certificate for SNI
3) CertKey Name: san17 Server Certificate for SNI
4) CertKey Name: san13 Server Certificate for SNI


1) Cipher Name: DEFAULT
Description: Default cipher list with encryption strength >= 128bit
Done
<!--NeedCopy-->
```


Configurar SNI en un servidor virtual DTLS mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. Abra un servidor virtual DTLS y, en Certificados, haga clic en **Certificado de servidor**.
3. Agregue un certificado o seleccione un certificado de la lista y seleccione **Certificado de servidor para SNI**.
4. En **Configuración avanzada**, haga clic en **Parámetros SSL**.
5. Seleccione **Habilitar SNI**.

Funciones no admitidas por un servidor virtual DTLS

Las siguientes opciones no se pueden habilitar en un servidor virtual DTLS:

- SSLv2
- SSLv3
- TLSv1
- TLSv1.1
- TLSv1.2
- Activador Push encrypt
- SSLv2Redirect
- SSLv2URL

Parámetros no utilizados por un servidor virtual DTLS

Un servidor virtual DTLS ignora los siguientes parámetros SSL, incluso si están configurados:

- Recuento de paquetes activadores de cifrado
- Tiempo de espera de activación de cifrado PUSH
- Tamaño cuántico SSL
- Tiempo de espera de activación de cifrado
- Formato de inserción de nombre de asunto/emisor

Configurar la renegociación en un servicio DTLS

La renegociación no segura es compatible con un servicio DTLS. Puede utilizar la CLI o la GUI para configurar este parámetro.

Configurar la renegociación en un servicio DTLS mediante la CLI

En el símbolo del sistema, escriba:


```
set ssl parameter -denysslreneg NONSECURE
<!--NeedCopy-->
```

Ejemplo:

```
set ssl parameter -denysslreneg NONSECURE


sh ssl parameter
Advanced SSL Parameters
-----------------------
SSL quantum size                                  : 8 KB
Max CRL memory size                               : 256 MB
Strict CA checks                                  : NO
Encryption trigger timeout                        : 100 ms
Send Close-Notify                                 : YES
Encryption trigger packet count                   : 45
Deny SSL Renegotiation                            : NONSECURE
Subject/Issuer Name Insertion Format              : Unicode
OCSP cache size                                   : 10 MB
Push flag                                         : 0x0 (Auto)
Strict Host Header check for SNI enabled SSL sessions : NO
PUSH encryption trigger timeout                   : 1 ms
Crypto Device Disable Limit                       : 0
Global undef action for control policies          : CLIENTAUTH
Global undef action for data policies             : NOOP
Default profile                                   : DISABLED
SSL Insert Space in Certificate Header            : YES
Disable TLS 1.1/1.2 for SSL_BRIDGE secure monitors    : NO
Disable TLS 1.1/1.2 for dynamic and VPN services      : NO
Software Crypto acceleration CPU Threshold        : 0
Hybrid FIPS Mode                                  : DISABLED
Signature and Hash Algorithms supported by TLS1.2     : ALL
SSL Interception Error Learning and Caching       : DISABLED
SSL Interception Maximum Error Cache Memory       : 0 Bytes
Done
<!--NeedCopy-->
```

Configurar la renegociación en un servicio DTLS mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servicios**.
2. Seleccione un servicio DTLS y haga clic en **Modificar**.

3. Vaya a **SSL** > **Configuración avanzada**.
4. Seleccione **Denegar renegociación de SSL**.

Funciones no admitidas por un servicio DTLS

Las siguientes opciones no se pueden habilitar en un servicio DTLS:

- SSLv2
- SSLv3
- TLSv1
- TLSv1.1
- TLSv1.2
- Activador Push encrypt
- SSLv2Redirect
- SSLv2URL
- SNI
- Renegociación segura

Parámetros no utilizados por un servicio DTLS

Un servicio DTLS ignora los siguientes parámetros SSL, aunque esté configurado:

- Recuento de paquetes activadores de cifrado
- Tiempo de espera de activación de cifrado PUSH
- Tamaño cuántico SSL
- Tiempo de espera de activación de cifrado
- Formato de inserción de nombre de asunto/emisor

> **Nota:**
>
> El protocolo de enlace de reutilización de sesiones SSL falla en un servicio DTLS porque actualmente los servicios DTLS no admiten la reutilización de sesiones.
>
> **Solución alternativa:** inhabilite manualmente la reutilización de sesiones en un servicio DTLS. En la CLI, escriba:
>
> ```
> set ssl service <dtls-service-name> -sessReuse DISABLED
> ```

Perfil DTLS

Un perfil DTLS con la configuración predeterminada se enlazará automáticamente a un servidor virtual DTLS. Sin embargo, puede crear un perfil DTLS con ajustes específicos que se adapten a sus necesidades.

Utilice un perfil DTLS con un servidor virtual DTLS o un servidor virtual DTLS VPN. No se puede utilizar un perfil SSL con un servidor virtual DTLS.

> **Nota:**
>
> Cambie la configuración del tamaño máximo de registro en el perfil DTLS en función de los cambios en la MTU y el tamaño del paquete. Por ejemplo, el tamaño máximo de registro predeterminado de 1459 bytes se calcula en función del tamaño del encabezado de una dirección IPv4. Con los registros IPv6, el tamaño del encabezado es mayor y, por lo tanto, el tamaño máximo de registro debe reducirse para cumplir los siguientes criterios.

```
max record size + UDP header(8bytes)+ IP header size < MTU
```

Ejemplo:

```
Default DTLS profile
    1) Name: nsdtls_default_profile
    PMTU Discovery: DISABLED
    Max Record Size: 1459 bytes
    Max Retry Time: 3 sec
    Hello Verify Request: ENABLED
    Terminate Session: DISABLED
    Max Packet Count: 120 bytes

Custom DTLS profile
    1) Name: ns_dtls_profile_ipv6_1
    PMTU Discovery: DISABLED
    Max Record Size: 1450 bytes
    Max Retry Time: 3 sec
    Hello Verify Request: ENABLED
    Terminate Session: DISABLED
    Max Packet Count: 120 bytes
<!--NeedCopy-->
```

Crear un perfil DTLS mediante la CLI

> **Notas:**
>
> - El parámetro `helloverifyrequest` está habilitado de forma predeterminada. Habilitar este parámetro ayuda a mitigar el riesgo de que un atacante o bots abruman el rendimiento de la red, lo que podría provocar un agotamiento del ancho de banda saliente. Es decir, ayuda a mitigar el ataque de amplificación DDoS DTLS.
> - Se agrega el parámetro `maxHoldQlen`. Este parámetro define el número de datagramas

> que se pueden poner en cola en la capa DTLS para su procesamiento. Un valor elevado del parámetro `maxHoldQlen` puede provocar la acumulación de memoria en la capa DTLS si la multiplexación UDP está transmitiendo un alto tráfico UDP. Por lo tanto, se recomienda configurar un valor inferior. El valor mínimo es 32, el valor máximo es 65535 y el valor predeterminado es 32.

Se introduce un nuevo parámetro `maxBadmacIgnorecount` en el perfil DTLS para ignorar los registros MAC incorrectos recibidos en una sesión DTLS. Con este parámetro, se ignoran los registros erróneos hasta el valor establecido en el parámetro. El dispositivo finaliza la sesión solo después de que se ha alcanzado el límite y envía una alerta.

Esta configuración de parámetros solo es efectiva cuando el parámetro `terminateSession` está habilitado.

```
ssl dtlsProfile <name> -maxRetryTime <positive_integer> -
    helloVerifyRequest ( ENABLED | DISABLED ) -terminateSession (ENABLED
     | DISABLED ) -maxHoldQLen <positive_integer> -maxBadmacIgnorecount
    <positive_integer>

helloVerifyRequest
               Send a Hello Verify request to validate the client.
               Possible values: ENABLED, DISABLED
               Default value: ENABLED

terminateSession
               Terminate the session if the message authentication code
                   (MAC)
               of the client and server do not match.
               Possible values: ENABLED, DISABLED
               Default value: DISABLED

maxHoldQLen
               Maximum number of datagrams that can be queued at DTLS
                   layer for
               processing
               Default value: 32
               Minimum value: 32
               Maximum value: 65535

maxBadmacIgnorecount
               Maximum number of bad MAC errors to ignore for a
                   connection prior disconnect. Disabling parameter
                   terminateSession
terminates session immediately when bad MAC is detected in the
```



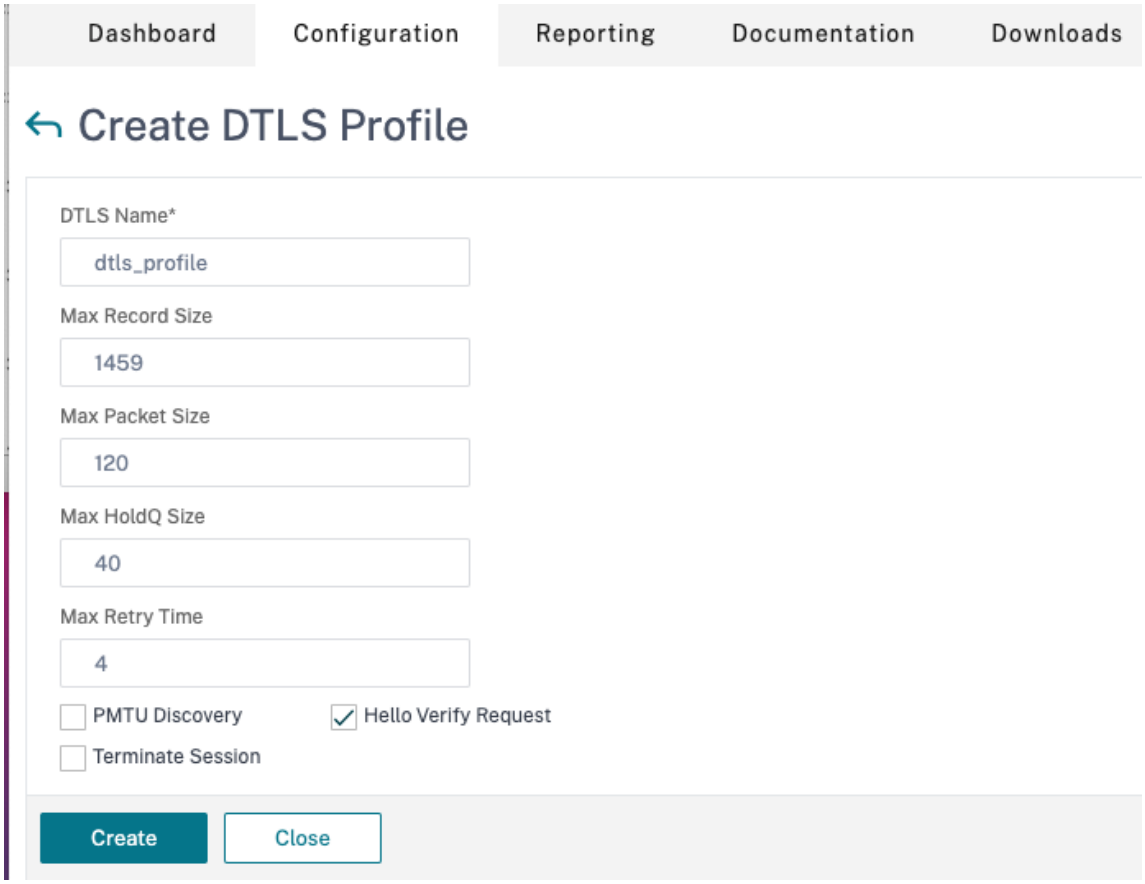
```
      connection.
24                Default value: 100
25                Minimum value: 1
26                Maximum value: 65535
27 <!--NeedCopy-->
```

Ejemplo:

```
1  > add ssl dtlsprofile dtls_profile -maxRetryTime 4 -helloVerifyRequest
      ENABLED -terminateSession ENABLED -maxHoldQLen 40 -
      maxBadmacIgnorecount 150
2   Done
3  > sh dtlsprofile dtls_profile
4  1)  Name: dtls_profile
5      PMTU Discovery: DISABLED
6      Max Record Size: 1459 bytes
7      Max Retry Time: 4 sec
8      Hello Verify Request: ENABLED
9      Terminate Session: ENABLED
10     Max Packet Count: 120 bytes
11     Max HoldQ Size: 40 datagrams
12     Max bad-MAC Ignore Count: 150
13
14  Done
15 <!--NeedCopy-->
```

Crear un perfil DTLS mediante la interfaz gráfica de usuario

1. Vaya a **Sistema > Perfiles > Perfiles DTLS** y haga clic en **Agregar**.
2. En la página **Crear perfil DTLS**, escriba valores para los distintos parámetros.



3. Haga clic en **Crear**.

Ejemplo para una configuración DTLS end-to-end

```
enable ns feature SSL LB

add server s1 198.51.100.2

en ns mode usnip

add service svc_dtls s1 DTLS 443

add lb vserver v1 DTLS 10.102.59.244 443

bind ssl vserver v1 -ciphername ALL

add ssl certkey servercert -cert servercert_aia_valid.pem -key
   serverkey_aia.pem

bind ssl vserver v1 -certkeyname servercert
```



```
16
17 bind lb vserver lb1 svc_dtls
18
19 sh lb vserver v1
20
21                     v1 (10.102.59.244:4433) - DTLS     Type: ADDRESS
22                     State: UP
23                     Last state change was at Fri Apr 27 07:00:27 2018
24                     Time since last state change: 0 days, 00:00:04.810
25                     Effective State: UP
26                     Client Idle Timeout: 120 sec
27                     Down state flush: ENABLED
28                     Disable Primary Vserver On Down : DISABLED
29                     Appflow logging: ENABLED
30                     No. of Bound Services :  1 (Total) 0 (Active)
31                     Configured Method: LEASTCONNECTION
32                     Current Method: Round Robin, Reason: A new service
                          is bound         BackupMethod: ROUNDROBIN
33                     Mode: IP
34                     Persistence: NONE
35                     L2Conn: OFF
36                     Skip Persistency: None
37                     Listen Policy: NONE
38                     IcmpResponse: PASSIVE
39                     RHIstate: PASSIVE
40                     New Service Startup Request Rate: 0 PER_SECOND,
                          Increment Interval: 0
41                     Mac mode Retain Vlan: DISABLED
42                     DBS_LB: DISABLED
43                     Process Local: DISABLED
44                     Traffic Domain: 0
45                     TROFS Persistence honored: ENABLED
46                     Retain Connections on Cluster: NO
47
48     1) svc_dtls (10.102.59.190: 4433) - DTLS State: UP  Weight: 1
49 Done
50
51
52 sh ssl vserver v1
53
54                     Advanced SSL configuration for VServer v1:
55                     DH: DISABLED
56                     DH Private-Key Exponent Size Limit: DISABLED
                                    Ephemeral RSA: ENABLED
                                                          Refresh Count: 0
```



```
                      Session Reuse: ENABLED                  Timeout:
                         1800 seconds
                      Cipher Redirect: DISABLED
                      ClearText Port: 0
                      Client Auth: DISABLED
                      SSL Redirect: DISABLED
                      Non FIPS Ciphers: DISABLED
                      SNI: DISABLED
                      OCSP Stapling: DISABLED
                      HSTS: DISABLED
                      HSTS IncludeSubDomains: NO
                      HSTS Max-Age: 0
                      DTLSv1: ENABLED
                      Send Close-Notify: YES
                      Strict Sig-Digest Check: DISABLED
                      Zero RTT Early Data: DISABLED
                      DHE Key Exchange With PSK: NO
                      Tickets Per Authentication Context: 1
                      DTLS profile name: nsdtls_default_profile

                      ECC Curve: P_256, P_384, P_224, P_521

    1)            CertKey Name: servercert               Server
       Certificate

    1)            Cipher Name: DEFAULT
                    Description: Default cipher list with encryption
                       strength >= 128bit

    2)            Cipher Name: ALL
                    Description: All ciphers supported by NetScaler,
                       excluding NULL ciphers
     Done

sh service svc_dtls

                      svc_dtls (10.102.59.190:4433) - DTLS
                      State: UP
                      Last state change was at Fri Apr 27 07:00:26 2018
                      Time since last state change: 0 days, 00:00:22.790
                      Server Name: s1
                      Server ID : None                  Monitor Threshold
                         : 0
                      Max Conn: 0        Max Req: 0           Max
                         Bandwidth: 0 kbits
```



```
                        Use Source IP: NO
                        Client Keepalive(CKA): NO
                        Access Down Service: NO
                        TCP Buffering(TCPB): NO
                        HTTP Compression(CMP): NO
                        Idle timeout: Client: 120 sec           Server: 120
                            sec
                        Client IP: DISABLED
                        Cacheable: NO
                        SC: OFF
                        SP: OFF
                        Down state flush: ENABLED
                        Monitor Connection Close : NONE
                        Appflow logging: ENABLED
                        Process Local: DISABLED
                        Traffic Domain: 0

     1)             Monitor Name: ping-default
                                      State: UP               Weight: 1
                                                          Passive: 0
                                    Probes: 5               Failed [Total
                                       : 0 Current: 0]
                                     Last response: Success - ICMP echo
                                        reply received.
                           Response Time: 2.77 millisec
      Done

sh ssl service svc_dtls

                        Advanced SSL configuration for Back-end SSL Service
                            svc_dtls:
                        DH: DISABLED
                        DH Private-Key Exponent Size Limit: DISABLED
                                  Ephemeral RSA: DISABLED
                        Session Reuse: ENABLED                  Timeout:
                           1800 seconds
                        Cipher Redirect: DISABLED
                        ClearText Port: 0
                        Server Auth: DISABLED
                        SSL Redirect: DISABLED
                        Non FIPS Ciphers: DISABLED
                        SNI: DISABLED
                        OCSP Stapling: DISABLED
                        DTLSv1: ENABLED
                        Send Close-Notify: YES
```



```
                      Strict Sig-Digest Check: DISABLED
                      Zero RTT Early Data: ???
                      DHE Key Exchange With PSK: ???
                      Tickets Per Authentication Context: ???
                      DTLS profile name: nsdtls_default_profile
                      ECC Curve: P_256, P_384, P_224, P_521
    1)            Cipher Name: DEFAULT_BACKEND
                      Description: Default cipher list for Backend SSL
                         session
     Done


> sh dtlsProfile nsdtls_default_profile
1)  Name: nsdtls_default_profile
    PMTU Discovery: DISABLED
    Max Record Size: 1459 bytes
    Max Retry Time: 3 sec
    Hello Verify Request: DISABLED
    Terminate Session: ENABLED
    Max Packet Count: 120 bytes
    Max HoldQ Size: 32 datagrams
    Max bad-MAC Ignore Count: 10

 Done
<!--NeedCopy-->
```

Compatibilidad con DTLS para direcciones IPv6

DTLS también es compatible con direcciones IPv6. Sin embargo, para utilizar DTLS con direcciones IPv6, el tamaño máximo de registro debe ajustarse en el perfil DTLS.

Si se utiliza el valor predeterminado para el tamaño máximo de registro, la conexión DTLS inicial podría fallar. Ajuste el tamaño máximo de registro mediante un perfil DTLS.

Compatibilidad con cifrado DTLS

De forma predeterminada, un grupo de cifrado DTLS está vinculado al crear un servidor o servicio virtual DTLS. DEFAULT_DTLS contiene los cifrados que admite una entidad DTLS front-end. Este grupo está enlazado de forma predeterminada al crear un servidor virtual DTLS. DEFAULT_DTLS_BACKEND contiene los cifrados compatibles con una entidad DTLS back-end. Este grupo está enlazado de forma predeterminada a un servicio back-end DTLS. DTLS_FIPS contiene los cifrados compatibles con la plataforma FIPS de Citrix ADC. Este grupo está enlazado de forma predeterminada a un servidor virtual DTLS o servicio creado en una plataforma FIPS.

Compatibilidad con cifrado DTLS en dispositivos Citrix ADC VPX, MPX/SDX (basados en N2 y N3)

Cómo leer las tablas:

A menos que se especifique un número de compilación, se admite un conjunto de cifrado para todas las compilaciones de una versión.

Ejemplo:

- **11.1, 12.1, 13.0, 13.1**: Todas las compilaciones de las versiones 11.1, 12.1, 13.0 y 13.1.
- **-NA-**: No aplicable.

Compatibilidad con cifrado DTLS en dispositivos Citrix ADC VPX, MPX/SDX (basados en N2, N3 y Coleto)

Nombre del conjunto de cifrado	Código hexadecimal	Nombre del conjunto de cifrado de Wireshark	Compilaciones compatibles (front-end)	Compilaciones compatibles (back-end)
TLS1-AES-256-CBC-SHA	0x0035	TLS_RSA_WITH_AI	11.1, 12.1, 13.0, 13.1	12.1, 13.0, 13.1
TLS1-AES-128-CBC-SHA	0x002f	TLS_RSA_WITH_AES_128_CBC_SHA	11.1, 12.1, 13.0, 13.1	12.1, 13.0, 13.1
SSL3-DES-CBC-SHA	0x0009	TLS_RSA_WITH_DI	11.1, 12.1, 13.0, 13.1	-N/A-
SSL3-DES-CBC3-SHA	0x000a	TLS_RSA_WITH_3DES_EDE_CBC_SHA	11.1, 12.1, 13.0, 13.1	12.1, 13.0, 13.1
SSL3-EDH-RSA-DES-CBC3-SHA	0x0016	TLS_DHE_RSA_WI	11.1, 12.1, 13.0, 13.1	-N/A-
SSL3-EDH-RSA-DES-CBC-SHA	0x0015	TLS_DHE_RSA_WITH_DES_CBC_SHA	11.1, 12.1, 13.0, 13.1	-N/A-
TLS1-ECDHE-RSA-AES256-SHA	0xc014	TLS_ECDHE_RSA_	12.1, 13.0, 13.1	12.1, 13.0, 13.1
TLS1-ECDHE-RSA-AES128-SHA	0xc013	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	12.1, 13.0, 13.1	12.1, 13.0, 13.1
TLS1-ECDHE-RSA-DES-CBC3-SHA	0xc012	TLS_ECDHE_RSA_	12.1, 13.0, 13.1	-N/A-

Nombre del conjunto de cifrado	Código hexadecimal	Nombre del conjunto de cifrado de Wireshark	Compilaciones compatibles (front-end)	Compilaciones compatibles (back-end)
TLS1-DHE-RSA-AES-128-CBC-SHA	0x0033	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	12.1, 13.0, 13.1	12.1, 13.0, 13.1
TLS1-DHE-RSA-AES-256-CBC-SHA	0x0039	TLS_DHE_RSA_WI	12.1, 13.0, 13.1	12.1, 13.0, 13.1

Para ver la lista de cifrados predeterminados admitidos en el front-end, en el símbolo del sistema, escriba:

```
show ssl cipher DEFAULT_DTLS
1)    Cipher Name: TLS1-AES-256-CBC-SHA    Priority : 1
    Description: SSLv3 Kx=RSA      Au=RSA  Enc=AES(256)  Mac=SHA1
       HexCode=0x0035
2)    Cipher Name: TLS1-AES-128-CBC-SHA    Priority : 2
    Description: SSLv3 Kx=RSA      Au=RSA  Enc=AES(128)  Mac=SHA1
       HexCode=0x002f
3)    Cipher Name: TLS1-ECDHE-RSA-AES256-SHA    Priority : 3
    Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=AES(256)  Mac=SHA1
       HexCode=0xc014
4)    Cipher Name: TLS1-ECDHE-RSA-AES128-SHA    Priority : 4
    Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=AES(128)  Mac=SHA1
       HexCode=0xc013
5)    Cipher Name: TLS1-DHE-RSA-AES-256-CBC-SHA    Priority : 5
    Description: SSLv3 Kx=DH       Au=RSA  Enc=AES(256)  Mac=SHA1
       HexCode=0x0039
6)    Cipher Name: TLS1-DHE-RSA-AES-128-CBC-SHA    Priority : 6
    Description: SSLv3 Kx=DH       Au=RSA  Enc=AES(128)  Mac=SHA1
       HexCode=0x0033
7)    Cipher Name: TLS1-ECDHE-RSA-DES-CBC3-SHA Priority : 7
    Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=3DES(168) Mac=SHA1
       HexCode=0xc012
8)    Cipher Name: SSL3-DES-CBC3-SHA    Priority : 8
    Description: SSLv3 Kx=RSA      Au=RSA  Enc=3DES(168) Mac=SHA1
       HexCode=0x000a
<!--NeedCopy-->
```


Para ver la lista de cifrados predeterminados admitidos en el back-end, en el símbolo del sistema, escriba:

```
show ssl cipher DEFAULT_DTLS_BACKEND
1)  Cipher Name: TLS1-AES-256-CBC-SHA    Priority : 1
    Description: SSLv3 Kx=RSA      Au=RSA  Enc=AES(256)  Mac=SHA1
       HexCode=0x0035
2)    Cipher Name: TLS1-AES-128-CBC-SHA    Priority : 2
    Description: SSLv3 Kx=RSA      Au=RSA  Enc=AES(128)  Mac=SHA1
       HexCode=0x002f
3)    Cipher Name: TLS1-ECDHE-RSA-AES256-SHA    Priority : 3
    Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=AES(256)  Mac=SHA1
       HexCode=0xc014
4)    Cipher Name: TLS1-ECDHE-RSA-AES128-SHA    Priority : 4
    Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=AES(128)  Mac=SHA1
       HexCode=0xc013
5)    Cipher Name: TLS1-DHE-RSA-AES-256-CBC-SHA    Priority : 5
    Description: SSLv3 Kx=DH       Au=RSA  Enc=AES(256)  Mac=SHA1
       HexCode=0x0039
6)    Cipher Name: TLS1-DHE-RSA-AES-128-CBC-SHA    Priority : 6
    Description: SSLv3 Kx=DH       Au=RSA  Enc=AES(128)  Mac=SHA1
       HexCode=0x0033
7)    Cipher Name: TLS1-ECDHE-RSA-DES-CBC3-SHA Priority : 7
    Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=3DES(168) Mac=SHA1
       HexCode=0xc012
8)    Cipher Name: SSL3-DES-CBC3-SHA    Priority : 8
    Description: SSLv3 Kx=RSA      Au=RSA  Enc=3DES(168) Mac=SHA1
       HexCode=0x000a
<!--NeedCopy-->
```

Compatibilidad con cifrado DTLS en la plataforma FIPS Citrix ADC MPX 14000

Nota: La plataforma FIPS permite Enlightened Data Support (EDT) si se cumplen las siguientes condiciones:

- El valor de UDT MSS establecido en StoreFront es 900.
- La versión del cliente Windows es 4.12 o posterior.
- La versión del VDA habilitada para DTLS es 7.17 o posterior.
- La versión de VDA que no es DTLS es 7.15 LTSR CU3 o posterior.

Cómo leer las tablas:

A menos que se especifique un número de compilación, se admite un conjunto de cifrado para todas

las compilaciones de una versión.

Ejemplo:

- **11.1, 12.1, 13.0, 13.1**: Todas las compilaciones de las versiones 11.1, 12.1, 13.0 y 13.1.
- **-NA-**: No aplicable.

Nombre del conjunto de cifrado	Código hexadecimal	Nombre de la suite Wireshark Cipher	Compilaciones compatibles (front-end)	Compilaciones compatibles (back-end)
TLS1-AES-256-CBC-SHA	0x0035	TLS_RSA_WITH_AI	11.1, 12.1-49.x, 13.0, 13.1	12.1-49.x, 13.0, 13.1
TLS1-AES-128-CBC-SHA	0x002f	TLS_RSA_WITH_AES_128_CBC_SHA	11.1, 12.1-49.x, 13.0, 13.1	12.1-49.x, 13.0, 13.1
SSL3-DES-CBC-SHA	0x0009	TLS_RSA_WITH_DI	11.1, 12.1-49.x, 13.0, 13.1	-N/A-
SSL3-DES-CBC3-SHA	0x000a	TLS_RSA_WITH_3DES_EDE_CBC_SHA	11.1, 12.1-49.x, 13.0, 13.1	12.1-49.x, 13.0, 13.1
SSL3-EDH-RSA-DES-CBC3-SHA	0x0016	TLS_DHE_RSA_WI	11.1, 12.1-49.x, 13.0, 13.1	-N/A-
SSL3-EDH-RSA-DES-CBC-SHA	0x0015	TLS_DHE_RSA_WITH_DES_CBC_SHA	11.1, 12.1-49.x, 13.0, 13.1	-N/A-
TLS1-ECDHE-RSA-AES256-SHA	0xc014	TLS_ECDHE_RSA_	12.1-49.x, 13.0, 13.1	12.1-49.x, 13.0, 13.1
TLS1-ECDHE-RSA-AES128-SHA	0xc013	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	12.1-49.x, 13.0, 13.1	12.1-49.x, 13.0, 13.1
TLS1-ECDHE-RSA-DES-CBC3-SHA	0xc012	TLS_ECDHE_RSA_	12.1-49.x, 13.0, 13.1	-N/A-
TLS1-DHE-RSA-AES-128-CBC-SHA	0x0033	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	12.1-49.x, 13.0, 13.1	12.1-49.x, 13.0, 13.1
TLS1-DHE-RSA-AES-256-CBC-SHA	0x0039	TLS_DHE_RSA_WI	12.1-49.x, 13.0, 13.1	12.1-49.x, 13.0, 13.1
TLS1-ECDHE-ECDSA-AES128-SHA	0xc009	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	12.1-49.x, 13.0, 13.1	12.1-49.x

Nombre del conjunto de cifrado	Código hexadecimal	Nombre de la suite Wireshark Cipher	Compilaciones compatibles (front-end)	Compilaciones compatibles (back-end)
TLS1-ECDHE-ECDSA-AES256-SHA	0xc00a	TLS_ECDHE_ECDS	13.1-21.x	13.1-21.x
TLS1-ECDHE-ECDSA-DES-CBC3-SHA	0xc008	TLS_ECDHE_ECDSA_WITH_3DES_CBC_SHA	13.1-21.x	13.1-21.x

Para ver la lista de cifrados predeterminados admitidos en un dispositivo Citrix ADC FIPS, en el símbolo del sistema, escriba:

```
show ssl cipher DTLS_FIPS
1)    Cipher Name: TLS1-AES-256-CBC-SHA    Priority : 1
    Description: SSLv3 Kx=RSA      Au=RSA  Enc=AES(256)  Mac=SHA1
       HexCode=0x0035
2)    Cipher Name: TLS1-AES-128-CBC-SHA    Priority : 2
    Description: SSLv3 Kx=RSA      Au=RSA  Enc=AES(128)  Mac=SHA1
       HexCode=0x002f
3)    Cipher Name: TLS1-ECDHE-RSA-AES256-SHA    Priority : 3
    Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=AES(256)  Mac=SHA1
       HexCode=0xc014
4)    Cipher Name: TLS1-ECDHE-RSA-AES128-SHA    Priority : 4
    Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=AES(128)  Mac=SHA1
       HexCode=0xc013
5)    Cipher Name: TLS1-ECDHE-RSA-DES-CBC3-SHA  Priority : 5
    Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=3DES(168) Mac=SHA1
       HexCode=0xc012
6)    Cipher Name: SSL3-DES-CBC3-SHA    Priority : 6
    Description: SSLv3 Kx=RSA      Au=RSA  Enc=3DES(168) Mac=SHA1
       HexCode=0x000a
<!--NeedCopy-->
```

Compatibilidad con cifrado DTLSv1.2 en los dispositivos VPX front-end, dispositivos MPX/SDX (basados en Coleto y N3)

En la tabla siguiente se enumeran los cifrados adicionales compatibles con el protocolo DTLSv1.2.

Nombre del conjunto de cifrado	Código hexadecimal	Nombre de la suite Wireshark Cipher	Compilaciones compatibles (front-end VPX)	Compilaciones compatibles (basadas en Coleto)	Compilaciones compatibles (basadas en N3)
—	—	—	—	—	—
TLS1.2-AES256-GCM-SHA384	0x009d	TLS_RSA_WITH_AES_256_GCM_SHA384	13.0–47.x, 13.1	13.0–52.x, 13.1	13.0–58.x, 13.1
TLS1.2-AES128-GCM-SHA256	0x009c	TLS_RSA_WITH_AES_128_GCM_SHA256	13.0—47.x, 13.1	13.0—52.x, 13.1	13.0—58.x, 13.1
TLS1.2-ECDHE-RSA-AES256-GCM-SHA384	0xc030	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	13.0—47.x, 13.1	13.0—52.x, 13.1	13.0—58.x, 13.1
TLS1.2-ECDHE-RSA-AES128-GCM-SHA256	0xc02f	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	13.0—47.x, 13.1	13.0—52.x, 13.1	13.0—58.x, 13.1
TLS1.2-DHE-RSA-AES256-GCM-SHA384	0x009f	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	13.0—47.x, 13.1	13.0—52.x, 13.1	13.0—58.x, 13.1
TLS1.2-DHE-RSA-AES128-GCM-SHA256	0x009e	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	13.0—47.x, 13.1	13.0—52.x, 13.1	13.0—58.x, 13.1
TLS1.2-AES-256-SHA256	0x003d	TLS_RSA_WITH_AES_256_CBC_SHA256	13.0—47.x, 13.1	13.0—52.x, 13.1	13.0—58.x, 13.1
TLS1.2-AES-128-SHA256	0x003c	TLS_RSA_WITH_AES_128_CBC_SHA256	13.0—47.x, 13.1	13.0—52.x, 13.1	13.0—58.x, 13.1
TLS1.2-ECDHE-RSA-AES-256-SHA384	0xc028	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	13.0—47.x, 13.1	13.0—52.x, 13.1	13.0—58.x, 13.1
TLS1.2-ECDHE-RSA-AES-128-SHA256	0xc027	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	13.0—47.x, 13.1	13.0—52.x, 13.1	13.0—58.x, 13.1
TLS1.2-DHE-RSA-AES-256-SHA256	0x006b	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	13.0—47.x, 13.1	13.0—52.x, 13.1	13.0—58.x, 13.1
TLS1.2-DHE-RSA-AES-128-SHA256	0x0067	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	13.0—47.x, 13.1	13.0—52.x, 13.1	13.0—58.x, 13.1
TLS1-ECDHE-ECDSA-AES128-SHA	0xc009	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	13.1–21.x	NA
TLS1-ECDHE-ECDSA-AES256-SHA	0xc00a	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	13.1–21.x	NA
TLS1-ECDHE-ECDSA-DES-CBC3-SHA	0xc008	TLS_ECDHE_ECDSA_WITH_3DES_CBC_SHA	13.1–21.x	NA
TLS1.2-ECDHE-ECDSA-AES128-GCM-SHA256	0xc02b	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	13.1–21.x	NA
TLS1.2-ECDHE-ECDSA-AES256-GCM-SHA384	0xc02c	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	13.1–21.x	NA
TLS1.2-ECDHE-ECDSA-AES128-SHA256	0xc023	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	13.1–

21.x|NA|
|TLS1.2-ECDHE-ECDSA-AES256-SHA384|0xc024|TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384|13.1–21.x|NA|

Compatibilidad con las plataformas basadas en chips Intel Coleto e Intel Lewisburg SSL

April 21, 2022

Los siguientes dispositivos se entregan con chips Intel Coleto:

- MPX 5900
- MPX/SDX 8900
- MPX/SDX 15000
- MPX/SDX 15000-50G
- MPX/SDX 26000
- MPX/SDX 26000-50
- MPX/SDX 26000-100G

El siguiente dispositivo se entrega con chips Intel Lewisburg:

- MPX/SDX 9100

Utilice el comando “show hardware” para identificar si su dispositivo tiene chips Coleto (COL) o Lewisburg (LBG).

```
> sh hardware

    Platform: NSMPX-8900 8\*CPU+4\*F1X+6\*E1K+1\*E1K+1*COL 8955 30010
    Manufactured on: 10/18/2016
    CPU: 2100MHZ
    Host Id: 0
    Serial no: CRAC5CR8UA
    Encoded serial no: CRAC5CR8UA
 Done
<!--NeedCopy-->
```

```
> sh hardware
        Platform: NSMPX-9100 10\*CPU+64GB+8\*F2X+E1K+1*LBG C627 35000
        Manufactured on: 10/1/2021
```



```
        CPU: 2300MHZ
        Host Id: 161644678
        Serial no: N2Z3ZD9S21
        Encoded serial no: N2Z3ZD9S21
        Netscaler UUID: 41a26261-227e-11ec-b4db-3cecef56f86b
        BMC Revision: 1.00
Done
<!--NeedCopy-->
```

Limitaciones

No se admiten los siguientes cifrados, protocolos y funciones:

- Cifrado DH 512
- Protocolo SSLv3
- Módulo de seguridad de hardware (HSM)
- GnuTLS
- Certificados ECDSA con curvas ECC P_224 y P521
- Descarga de DNSSEC (DNSSEC se admite en el software, pero no se admite la descarga al hardware).

Ver el uso de chips SSL en plataformas Citrix ADC MPX y SDX

A partir de la versión 13.1 compilación 21.x, se agregan contadores para ver más detalles sobre el uso del chip SSL en las siguientes plataformas:

- Plataformas MPX y SDX que se suministran con chips Intel Coleto.
- Plataformas MPX que se suministran con chips Intel Lewisburg.

Esta función no se admite en la plataforma SDX 9100.

En el símbolo del sistema, escriba:

```
> stat ssl

SSL Summary

1.  SSL cards present 4
2.  SSL cards UP 4
    SSL engine status 1
    SSL sessions (Rate) 19849
    SSL Crypto Utilization Asym (%) 88
    SSL Crypto Utilization Symm (%) 1
```



```
11
12 Crypto Utilization(%)
13 Asymmetric Crypto Utilization 86.30
14 Symmetric Crypto Utilization 0.97
15
16 System
17 Transactions Rate (/s) Total
18 SSL transactions 19849 45900312
19 SSLv2 transactions 0 0
20 SSLv3 transactions 0 0
21 TLSv1 transactions 0 0
22 TLSv1.1 transactions 0 0
23 TLSv1.2 transactions 19849 45900312
24 TLSv1.3 transactions 0 0
25 DTLSv1 transactions 0 0
26 DTLSv1.2 transactions 0 0
27
28 Front End
29 Sessions Rate (/s) Total
30 SSL sessions 19849 45937019
31 SSLv2 sessions 0 0
32 SSLv3 sessions 0 0
33 TLSv1 sessions 0 0
34 TLSv1.1 sessions 0 0
35 TLSv1.2 sessions 19849 45937019
36 TLSv1.3 sessions 0 0
37 DTLSv1 sessions 0 0
38 DTLSv1.2 sessions 0 0
39 New SSL sessions 19881 50722628
40 SSL session misses 0 0
41 SSL session hits 0 0
42
43 Back End
44 Sessions Rate (/s) Total
45 SSL sessions 0 137
46 SSLv3 sessions 0 0
47 TLSv1 sessions 0 0
48 TLSv1.1 sessions 0 0
49 TLSv1.2 sessions 0 137
50 DTLSv1 sessions 0 0
51 Session multiplex attempts 0 0
52 Session multiplex successes 0 0
53 Session multiplex failures 0 0
54
55 Encryption/Decryption statistics
```



```
Crypto Operation Rate (bytes/s) Total Bytes
Bytes encrypted 24338213 27705995030
Bytes decrypted 24664169 27942280990
Done
<!--NeedCopy-->
```

Los valores de los siguientes contadores se logran al sondear el hardware:

```
-  SSL Crypto Utilization Asym (%) 88
-  SSL Crypto Utilization Symm (%) 1
<!--NeedCopy-->
```

Los valores de los siguientes contadores se logran con el software. Los valores pueden variar ligeramente de los valores sondeados por hardware.

- Utilización de criptomonedas (%)
- Utilización criptográfica asimétrica 85.92
- Utilización criptográfica de RSA 11.43
  RSA_4K 0.00
  RSA_2K 11.43
  RSA_1K 0.00
  RSA_Otros 0.00
- Utilización criptográfica DH 74.50 Utilización criptográfica
  ECDH 0.00
  ECDH_P224 0.00
  ECDH_P256 0.00
  ECDH_P384 0.00
  ECDH_P521 0.00
- Utilización criptográfica ECDSA 0.00
  ECDSA_P224 0.00
  ECDSA_P256 0.00
  ECDSA_P384 0.00
  ECDSA_P521 0.00
- Utilización criptográfica simétrica 0.72

Para una utilización granular por cifrado, ejecute el siguiente comando.

```
> stat ssl -detail

SSL Offloading
```



```
1.  SSL cards present 4
2.  SSL cards UP 4
    SSL engine status 1
    SSL sessions (Rate) 19862
    SSL Crypto Utilization Asym (%) 88
    SSL Crypto Utilization Symm (%) 1

Crypto Utilization(%)

Asymmetric Crypto Utilization 85.92

RSA Crypto Utilization 11.43
RSA_4K 0.00
RSA_2K 11.43
RSA_1K 0.00
RSA_Others 0.00

DH Crypto Utilization 74.50

ECDH Crypto Utilization 0.00
ECDH_P224 0.00
ECDH_P256 0.00
ECDH_P384 0.00
ECDH_P521 0.00

ECDSA Crypto Utilization 0.00
ECDSA_P224 0.00
ECDSA_P256 0.00
ECDSA_P384 0.00
ECDSA_P521 0.00

Symmetric Crypto Utilization 0.72
System
Transactions Rate (/s) Total
SSL transactions 19861 46039342
SSLv2 transactions 0 0
SSLv3 transactions 0 0
TLSv1 transactions 0 0
TLSv1.1 transactions 0 0
TLSv1.2 transactions 19861 46039342
TLSv1.3 transactions 0 0
DTLSv1 transactions 0 0
DTLSv1.2 transactions 0 0
Server in record 117437 277622634
```



```
Front End
Sessions Rate (/s) Total
SSL sessions 19862 46076050
SSLv2 sessions 0 0
SSLv3 sessions 0 0
TLSv1 sessions 0 0
TLSv1.1 sessions 0 0
TLSv1.2 sessions 19862 46076050
TLSv1.3 sessions 0 0
DTLSv1 sessions 0 0
DTLSv1.2 sessions 0 0
New SSL sessions 19801 50861234
SSL session misses 0 0
SSL session hits 0 0
Session Renegotiation
SSL session renegotiations 0 0
SSLv3 session renegotiations 0 0
TLSv1 session renegotiations 0 0
TLSv1.1 session renegotiations 0 0
TLSv1.2 session renegotiations 0 0
DTLSv1 session renegotiations 0 0
DTLSv1.2 session renegotiations 0 0
Key Exchanges
RSA 512-bit key exchanges 0 0
RSA 1024-bit key exchanges 0 2032658
RSA 2048-bit key exchanges 0 143
RSA 3072-bit key exchanges 0 7757028
RSA 4096-bit key exchanges 0 2238698
DH 512-bit key exchanges 0 0
DH 1024-bit key exchanges 0 0
DH 2048-bit key exchanges 19862 5477702
DH 4096-bit key exchanges 0 0
ECDHE 521 curve key exchanges 0 0
ECDHE 384 curve key exchanges 0 0
ECDHE 256 curve key exchanges 0 28569821
ECDHE 224 curve key exchanges 0 0
Total ECDHE key exchanges 0 28569821
Ciphers Negotiated
RC4 40-bit encryptions 0 0
RC4 56-bit encryptions 0 0
RC4 64-bit encryptions 0 0
RC4 128-bit encryptions 0 0
DES 40-bit encryptions 0 0
DES 56-bit encryptions 0 0
3DES 168-bit encryptions 0 0
```



```
AES 128-bit encryptions 0 0
AES 256-bit encryptions 19862 17506229
RC2 40-bit encryptions 0 0
RC2 56-bit encryptions 0 0
RC2 128-bit encryptions 0 0
AES-GCM 128-bit encryptions 0 0
AES-GCM 256-bit encryptions 0 28569821
Null cipher encryptions 0 0
Hashes
MD5 hashes 0 0
SHA hashes 0 12028527
SHA256 hashes 19862 5477702
SHA384 hashes 0 0
Handshakes
SSLv2 SSL handshakes 0 0
SSLv3 SSL handshakes 0 0
TLSv1 SSL handshakes 0 0
TLSv1.1 SSL handshakes 0 0
TLSv1.2 SSL handshakes 19862 46076050
TLSv1.3 SSL handshakes 0 0
DTLSv1 SSL handshakes 0 0
DTLSv1.2 SSL handshakes 0 0
Client Authentications
SSLv2 client authentications 0 0
SSLv3 client authentications 0 0
TLSv1 client authentications 0 0
TLSv1.1 client authentications 0 0
TLSv1.2 client authentications 0 0
TLSv1.3 client authentications 0 0
DTLSv1 client authentications 0 0
DTLSv1.2 client authentications 0 0
Authentications
RSA authentications 19862 17506229
DH authentications 0 0
DSS (DSA) authentications 0 0
ECDSA authentications 0 28569821
Null authentications 0 0
Back End
Sessions Rate (/s) Total
SSL sessions 0 137
SSLv3 sessions 0 0
TLSv1 sessions 0 0
TLSv1.1 sessions 0 0
TLSv1.2 sessions 0 137
DTLSv1 sessions 0 0
```



```
Session multiplex attempts 0 0
Session multiplex successes 0 0
Session multiplex failures 0 0
Session Renegotiation
SSL session renegotiations 0 0
SSLv3 session renegotiations 0 0
TLSv1 session renegotiations 0 0
TLSv1.1 back-end session renegot 0 0
TLSv1.2 back-end session renegot 0 0
DTLSv1 session renegotiations 0 0
Key Exchanges
RSA 512-bit key exchanges 0 0
RSA 1024-bit key exchanges 0 0
RSA 2048-bit key exchanges 0 137
RSA 3072-bit key exchanges 0 0
RSA 4096-bit key exchanges 0 0
DH 512-bit key exchanges 0 0
DH 1024-bit key exchanges 0 0
DH 2048-bit key exchanges 0 0
DH 4096-bit key exchanges 0 0
ECDHE 521 curve key exchanges 0 0
ECDHE 384 curve key exchanges 0 0
ECDHE 256 curve key exchanges 0 0
ECDHE 224 curve key exchanges 0 0
Ciphers Negotiated
RC4 40-bit encryptions 0 0
RC4 56-bit encryptions 0 0
RC4 64-bit encryptions 0 0
RC4 128-bit encryptions 0 0
DES 40-bit encryptions 0 0
DES 56-bit encryptions 0 0
3DES 168-bit encryptions 0 0
AES 128-bit encryptions 0 0
AES 256-bit encryptions 0 137
RC2 40-bit encryptions 0 0
RC2 56-bit encryptions 0 0
RC2 128-bit encryptions 0 0
AES-GCM 128-bit encryptions 0 0
AES-GCM 256-bit encryptions 0 0
Null encryptions 0 0
Hashes
MD5 hashes 0 0
SHA hashes 0 137
SHA256 hashes 0 0
SHA384 hashes 0 0
```



```
Handshakes
SSLv3 handshakes 0 0
TLSv1 handshakes 0 0
TLSv1.1 handshakes 0 0
TLSv1.2 handshakes 0 137
DTLSv1 handshakes 0 0
Client Authentications
SSLv3 client authentications 0 0
TLSv1 client authentications 0 0
TLSv1.1 client authentications 0 0
TLSv1.2 client authentications 0 0
DTLSv1 client authentications 0 0
Authentications
RSA authentications 0 137
DH authentications 0 0
DSS authentications 0 0
ECDSA authentications 0 0
Null authentications 0 0
System Total
RSA key exchanges offloaded 0 0
RSA sign operations offloaded 0 0
DH key exchanges offloaded 19841 5481037
RC4 encryptions offloaded 0 0
DES encryptions offloaded 0 0
AES encryptions offloaded 0 0
AES-GCM 128-bit encryptions offl 0 0
AES-GCM 256-bit encryptions offl 0 0
Encryption/Decryption statistics
Crypto Operation Rate (bytes/s) Total Bytes
Bytes encrypted 12129801 27790903638
Bytes encrypted in hardware 12129801 27790903638
Bytes encrypted in software 0 0
Bytes encrypted on the front-end 5450907 13430410630
Bytes encrypted in hardware on t 5450907 13430410630
Bytes encrypted in software on t 0 0
Bytes encrypted on the back-end 6678894 14360493008
Bytes encrypted in hardware on t 6678894 14360493008
Bytes encrypted in software on t 0 0
Bytes decrypted 12449504 28029427518
Bytes decrypted in hardware 12449504 28029427518
Bytes decrypted in software 0 0
Bytes decrypted on the front-end 8190208 19876552670
Bytes decrypted in hardware on t 8190208 19876552670
Bytes decrypted in software on t 0 0
Bytes decrypted on the back-end 4259296 8152874848
```



```
Bytes decrypted in hardware on t 4259296 8152874848
Bytes decrypted in software on t 0 0
SSL
Rate (/s) Total
Total SPCB in use -87 84656
Active SSL sessions -30309 5615559
Current queue size -1 4153
CardQ
Rate (/s) Total
In Q count for current card -1 4153
In BulkQ count for current card 0 0
In KeyQ count for current card -1 4153
Done
<!--NeedCopy-->
```

Notas

- Se admite la partición de administración, pero la utilización de todas las particiones se muestra en la partición predeterminada. En particiones no predeterminadas, estos valores se muestran como 0.
- En una configuración de clúster, la dirección CLIP muestra el uso promedio de todos los nodos del clúster. Para un uso específico de nodos, ejecute el comando en la CLI de cada nodo. Estos datos pueden ser incorrectos para una plataforma SDX si los nodos del clúster están alojados en el mismo hardware.
- Para las instancias VPX en la plataforma SDX, se muestra el uso de cada instancia VPX.

Dispositivos FIPS MPX 14000

April 21, 2022

Importante:

- La plataforma FIPS MPX 9700/10500/12500/15500 ha llegado al final de su vida útil.
- Los pasos de configuración para los dispositivos FIPS NetScaler MPX 14000 y NetScaler MPX 9700/10500/12500/15500 son diferentes. Los dispositivos FIPS MPX 14000 no utilizan firmware v2.2. Una clave FIPS creada en el módulo de seguridad de hardware (HSM) de la plataforma MPX 9700 no se puede transferir al HSM de la plataforma MPX 14000. Tampoco se admite el revés. Sin embargo, si ha importado una clave RSA como clave FIPS, puede copiar la clave RSA en la plataforma MPX 14000. A continuación, importarlo como clave FIPS. Solo se admiten claves de 2048 bits y 3072 bits.

> - Las versiones de firmware enumeradas en “Citrix ADC versión 12.1-FIPS” y “Citrix ADC versión 12.1-ndcpp” en la página de descargas de Citrix ADC no son compatibles con las plataformas MPX 14000 FIPS o SDX 14000 FIPS. Estas plataformas pueden usar otras versiones más recientes del firmware de Citrix ADC disponibles en la página de descargas.

Un dispositivo FIPS está equipado con un módulo criptográfico a prueba de manipulaciones (a prueba de manipulaciones), Cavium CNN3560-NFBE-G, diseñado para cumplir con las especificaciones FIPS 140-2 Nivel 3 (de la versión 12.0 versión 56.x). Los parámetros de seguridad críticos (CSP), principalmente la clave privada del servidor, se almacenan y generan de forma segura dentro del módulo criptográfico, también denominado HSM. Nunca se accede a los CSP fuera de los límites del HSM. Solo el superusuario (`nsroot`) puede realizar operaciones con las claves almacenadas en el HSM.

Antes de configurar un dispositivo FIPS, debe comprobar el estado de la tarjeta FIPS y, a continuación, inicializarla. Cree una clave FIPS y un certificado de servidor, y agregue cualquier configuración SSL adicional.

Para obtener información sobre los cifrados FIPS compatibles, consulte Algoritmos y cifrados aprobados por FIPS.

Para obtener información sobre la configuración de dispositivos FIPS en una configuración de alta disponibilidad, consulte Configurar FIPS en dispositivos de una configuración de alta disponibilidad.

Limitaciones

1. La renegociación SSL mediante el protocolo SSLv3 no se admite en el back-end de un dispositivo MPX FIPS.
2. Las claves de 1024 bits y 4096 bits y el valor exponente de 3 no son compatibles.
3. No se admite el certificado de servidor de 4096 bits.
4. No se admite el certificado de cliente de 4096 bits (si la autenticación de cliente está habilitada en el servidor back-end).

Configurar el HSM

Antes de configurar el HSM en un dispositivo FIPS MPX 14000, compruebe el estado de la tarjeta FIPS para comprobar que el controlador se ha cargado correctamente. A continuación, inicialice la tarjeta.

En el símbolo del sistema, escriba:

```
1 show fips
2
3 FIPS Card is not configured
4 <!--NeedCopy-->
```


El mensaje “ERROR: No se permite el funcionamiento, no se permite ninguna tarjeta FIPS presente en el sistema” si el controlador no se ha cargado correctamente.

Inicializar la tarjeta FIPS

El dispositivo debe reiniciarse tres veces para que la tarjeta FIPS se inicialice correctamente.

> **Importante**
>
> - Compruebe que el directorio `/nsconfig/fips` se haya creado correctamente en el dispositivo.
> - No guarde la configuración antes de reiniciar el dispositivo por tercera vez.

Realice los siguientes pasos para inicializar la tarjeta FIPS:

1. Reinicie la tarjeta FIPS (`reset fips`).
2. Reinicie el dispositivo (`reboot`).
3. Establezca la contraseña del oficial de seguridad para las particiones 0 y 1, y la contraseña de usuario para la partición (`set fips -initHSM Level-2 <soPassword> <oldsoPassword> <userPassword> -hsmLabel NSFIPS`).

   Nota: El comando set or reset tarda más de 60 segundos en ejecutarse.
4. Guarde la configuración (`saveconfig`).
5. Compruebe que la clave cifrada con contraseña para la partición principal (master_pek.key) se haya creado en el directorio `/nsconfig/fips/`.
6. Reinicie el dispositivo (`reboot`).
7. Compruebe que la clave cifrada con contraseña para la partición predeterminada (default_pek.key) se haya creado en el directorio `/nsconfig/fips/`.
8. Reinicie el dispositivo (`reboot`).
9. Compruebe que la tarjeta FIPS esté UP (`show fips`).

Inicializar la tarjeta FIPS mediante la CLI

El comando `set fips` inicializa el módulo de seguridad de hardware (HSM) de la tarjeta FIPS y establece una nueva contraseña de responsable de seguridad y contraseña de usuario.

Precaución: Este comando borra todos los datos de la tarjeta FIPS. Se le preguntará antes de continuar con la ejecución del comando. Es necesario reiniciar antes y después de ejecutar este comando para que se apliquen los cambios. Guarde la configuración después de ejecutar este comando y antes de reiniciar el dispositivo.

En el símbolo del sistema, escriba los comandos siguientes:

```
reset fips

reboot

set fips -initHSM Level-2 so12345 so12345 user123 -hsmLabel NSFIPS

This command will erase all data on the FIPS card. You must save the
   configuration (saveconfig) after executing this command. Do you want
    to continue?(Y/N)y

<!--NeedCopy-->
```

Nota: Aparece el siguiente mensaje al ejecutar el `set fips` comando:

```
This command will erase all data on the FIPS card. You must save the
   configuration (saveconfig) after executing this command. [Note: On
   MPX/SDX 14xxx FIPS platform, the FIPS security is at Level-3 by
   default, and the -initHSM Level-2 option is internally converted to
   Level-3]  Do you want to continue?(Y/N)y

saveconfig

reboot

reboot

show fips

        FIPS HSM Info:
                HSM Label               : NetScaler FIPS
                Initialization          : FIPS-140-2 Level-3
                HSM Serial Number       : 3.1G1836-ICM000136
                HSM State               : 2
                HSM Model               : NITROX-III CNN35XX-NFBE
                Hardware Version        : 0.0-G
                Firmware Version        : 1.0
                Firmware Build          : NFBE-FW-1.0-48
                Max FIPS Key Memory     : 102235
                Free FIPS Key Memory    : 102231
                Total SRAM Memory       : 557396
```



```
23                  Free SRAM Memory        : 262780
24                  Total Crypto Cores      : 63
25                  Enabled Crypto Cores    : 63
26
27 <!--NeedCopy-->
```

Crear una clave FIPS

Puede crear una clave FIPS en el dispositivo MPX 14000 FIPS o importar una clave FIPS existente al dispositivo. El dispositivo FIPS MPX 14000 admite únicamente claves de 2048 bits y 3072 bits y un valor exponente de F4 (cuyo valor es 65537). En el caso de las claves PEM, no es necesario un exponente. Compruebe que la clave FIPS se ha creado correctamente. Cree una solicitud de firma de certificado y un certificado de servidor. Por último, agregue el par de claves de certificado a su dispositivo.

Especifique el tipo de clave (RSA o ECDSA). Para las claves ECDSA, especifique solo la curva. Se admite la creación de claves ECDSA con la curva P_256 y P_384.

> **Nota:**
>
> No se admiten claves de 1024 bits y 4096 bits ni un valor exponente de 3.

Crear una clave FIPS mediante la CLI

En el símbolo del sistema, escriba:

```
1 create ssl fipsKey <fipsKeyName> -keytype ( RSA | ECDSA ) [-exponent (
     3 | F4 )] [-modulus <positive_integer>] [-curve ( P_256 | P_384 )]
2 <!--NeedCopy-->
```

Ejemplo 1:

```
1 create fipsKey f1 -keytype RSA -modulus 2048 -exponent F4
2
3
4 show ssl fipskey f1
5
6 FIPS Key Name: f1  Key Type: RSA Modulus: 2048   Public Exponent: F4 (
     Hex: 0x10001)
7
8 <!--NeedCopy-->
```


Ejemplo 2:

```
> create fipskey f2 -keytype ECDSA -curve P_256


> sh fipskey f2
    FIPS Key Name: f2   Key Type: ECDSA Curve: P_256

<!--NeedCopy-->
```

Cree una clave FIPS mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > SSL > FIPS**.
2. En el panel de detalles, en la ficha Claves FIPS, haga clic en **Agregar**.
3. En el cuadro de diálogo Crear clave FIPS, especifique los valores de los siguientes parámetros:
   - Nombre de clave FIPS*: FIPSkeyName
   - Módulo*: módulo
   - Exponent*: exponente

   *Un parámetro requerido
4. Haga clic en **Crear** y, a continuación, en **Cerrar**.
5. En la ficha Claves FIPS, compruebe que la configuración mostrada para la clave FIPS creada sea correcta.

Importación de una clave FIPS

Para utilizar una clave FIPS existente con el dispositivo FIPS, debe transferir la clave FIPS desde el disco duro del dispositivo a su HSM.

Nota: Para evitar errores al importar una clave FIPS, asegúrese de que el nombre de la clave importada sea el mismo que el nombre de la clave original cuando se creó.

Importar una clave FIPS mediante la CLI

En el símbolo del sistema, escriba:

```
import ssl fipsKey <fipsKeyName> -key <string> [-inform <inform>] [-
    wrapKeyName <string>] [-iv<string>] -exponent  F4 ]
```



```
<!--NeedCopy-->
```

Ejemplo:

```
import fipskey Key-FIPS-2 -key Key-FIPS-2.key -inform SIM -exponent F4


import fipskey Key-FIPS-2 -key Key-FIPS-2.key -inform PEM

<!--NeedCopy-->
```

Compruebe que la clave FIPS se ha creado o importado correctamente ejecutando el comando `show fipskey`.

```
show fipskey
1)      FIPS Key Name: Key-FIPS-2

<!--NeedCopy-->
```

Importar una clave FIPS mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > SSL > FIPS**.
2. En el panel de detalles, en la ficha Claves FIPS, haga clic en **Importar**.
3. En el cuadro de diálogo Importar como clave FIPS, seleccione el archivo de claves FIPS y defina los valores para los siguientes parámetros:
   - Nombre de clave FIPS*
   - Nombre de archivo clave*: para colocar el archivo en una ubicación distinta de la predeterminada, especifique la ruta completa o haga clic en **Examinar** y navegue hasta una ubicación.
   - Exponente*

   *Un parámetro requerido
4. Haga clic en **Import** y, luego, en **Close**.
5. En la ficha Claves FIPS, compruebe que la configuración mostrada para la clave FIPS importada sea correcta.

Exportar una clave FIPS

Citrix recomienda crear una copia de seguridad de cualquier clave creada en FIPS HSM. Si se elimina una clave del HSM, no se puede volver a crear la misma clave y todos los certificados asociados se vuelven inútiles.

Además de exportar una clave como copia de seguridad, es posible que deba exportar una clave para transferirla a otro dispositivo.

El procedimiento siguiente proporciona instrucciones sobre cómo exportar una clave FIPS a la carpeta `/nsconfig/ssl` de CompactFlash del dispositivo y proteger la clave exportada mediante un método de cifrado de clave asimétrica segura.

Exportación de una clave FIPS mediante la CLI

En el símbolo del sistema, escriba:

```
export ssl fipsKey <fipsKeyName> -key <string>
<!--NeedCopy-->
```

Ejemplo:

```
export fipskey Key-FIPS-1 -key Key-FIPS-1.key
<!--NeedCopy-->
```

Exportación de una clave FIPS mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > SSL > FIPS**.
2. En el panel de detalles, en la ficha Claves FIPS, haga clic en **Exportar**.
3. En el cuadro de diálogo Exportar clave FIPS a un archivo, especifique los valores de los siguientes parámetros:
   - Nombre de clave FIPS*: FIPSkeyName
   - Nombre de archivo*: clave (Para colocar el archivo en una ubicación distinta a la predeterminada, puede especificar la ruta completa o hacer clic en el botón Examinar y desplazarse hasta una ubicación).

   *Un parámetro requerido
4. Haga clic en **Exportar** y, a continuación, en **Cerrar**.

Importar una clave externa

Puede transferir claves FIPS creadas dentro del HSM del dispositivo Citrix ADC. También puede transferir claves privadas externas (como claves creadas en un dispositivo Citrix ADC, Apache o IIS estándar) a un dispositivo Citrix ADC FIPS. Las claves externas se crean fuera del HSM mediante una herramienta como OpenSSL. Antes de importar una clave externa en el HSM, cópiela en la unidad flash del dispositivo en `/nsconfig/ssl`.

En los dispositivos FIPS MPX 14000, el parámetro -exponent del comando **`import`** `ssl fipskey` no es necesario al importar una clave externa. El exponente público correcto se detecta automáticamente cuando se importa la clave y se ignora el valor del parámetro -exponent.

El dispositivo Citrix ADC FIPS no admite claves externas con un exponente público distinto de 3 o F4.

No necesita una clave de envoltura en los dispositivos FIPS MPX 14000.

No se puede importar una clave FIPS externa cifrada directamente a un dispositivo FIPS MPX 14000. Para importar la clave, primero debe descifrar la clave y luego importarla. Para descifrar la clave, en el símbolo del shell, escriba:

```
1 openssl rsa -in <EncryptedKey.key> > <DecryptedKey.out>
2 <!--NeedCopy-->
```

Nota: Si importa una clave RSA como clave FIPS, Citrix recomienda eliminar la clave RSA del dispositivo por motivos de seguridad.

Importar una clave externa como clave FIPS mediante la CLI

1. Copie la clave externa en la unidad flash del dispositivo.
2. Si la clave está en formato.pfx, primero debe convertirla al formato PEM. En el símbolo del sistema, escriba:

```
1 convert ssl pkcs12 <output file> -import -pkcs12File <input .pfx
     file name> -password <password>
2 <!--NeedCopy-->
```

3. En el símbolo del sistema, escriba los siguientes comandos para importar la clave externa como clave FIPS y compruebe la configuración:

```
1 import ssl fipsKey <fipsKeyName> -key <string> -informPEM
2 show ssl fipskey<fipsKeyName>
```



```
<!--NeedCopy-->
```

Ejemplo:

```
convert ssl pkcs12 iis.pem -password 123456 -import -pkcs12File iis.pfx

import fipskey Key-FIPS-2 -key iis.pem -inform PEM

show ssl fipskey key-FIPS-2

FIPS Key Name: Key-FIPS-2 Modulus: 0   Public Exponent: F4 (Hex value 0
   x10001)
<!--NeedCopy-->
```

Importar una clave externa como clave FIPS mediante la GUI

1. Si la clave está en formato.pfx, primero debe convertirla al formato PEM.
   a) Vaya a **Administración del tráfico > SSL**.
   b) En el panel de detalles, en Herramientas, haga clic en **Importar PKCS #12**.
   c) En el cuadro de diálogo Importar archivo PKCS12, defina los siguientes parámetros:
      - Nombre del archivo de salida*
      - Nombre de archivo PKCS12*: especifique el nombre de archivo.pfx.
      - Importar contraseña*
      - Formato de codificación

      *Un parámetro obligatorio
2. Vaya a **Administración del tráfico > SSL > FIPS**.
3. En el panel de detalles, en la ficha Claves FIPS, haga clic en **Importar**.
4. En el cuadro de diálogo Importar como clave FIPS, seleccione el archivo PEM y defina los valores para los siguientes parámetros:
   - Nombre de clave FIPS*
   - Nombre del archivo de clave*: para colocar el archivo en una ubicación distinta a la predeterminada, puede especificar la ruta completa o hacer clic en Examinar y desplazarse hasta una ubicación.

   *Un parámetro requerido
5. Haga clic en **Import** y, luego, en **Close**.
6. En la ficha Claves FIPS, compruebe que la configuración mostrada para la clave FIPS importada sea correcta.

Configurar FIPS en dispositivos en una configuración de alta disponibilidad

Puede configurar dos dispositivos en un par HA como dispositivos FIPS.

Requisitos previos

- El módulo de seguridad de hardware (HSM) debe configurarse en ambos dispositivos. Para obtener más información, consulte Configurar el HSM.
- Cuando utilice la GUI, asegúrese de que los dispositivos ya están en una configuración de alta disponibilidad. Para obtener más información sobre cómo configurar una configuración de alta disponibilidad, consulte Alta disponibilidad.

> **Nota:**
>
> Citrix recomienda utilizar la utilidad de configuración (GUI) para este procedimiento. Si utiliza la línea de comandos (CLI), asegúrese de seguir cuidadosamente los pasos enumerados en el procedimiento. Cambiar el orden de los pasos o especificar un archivo de entrada incorrecto puede provocar una incoherencia que requiera reiniciar el dispositivo. Además, si utiliza la CLI, el comando `create ssl fipskey` no se propaga al nodo secundario. Cuando ejecuta el comando con los mismos valores de entrada para el tamaño del módulo y el exponente en dos dispositivos FIPS diferentes, las claves generadas no son las mismas. Cree la clave FIPS en uno de los nodos y, a continuación, transfiérala al otro nodo. Sin embargo, si utiliza la utilidad de configuración para configurar dispositivos FIPS en una configuración de alta disponibilidad, la clave FIPS que cree se transfiere automáticamente al nodo secundario. El proceso de administración y transferencia de las claves FIPS se conoce como gestión segura de la información (SIM).

Importante: La configuración de alta disponibilidad debe completarse en seis minutos. Si el procedimiento falla en algún paso, haga lo siguiente:

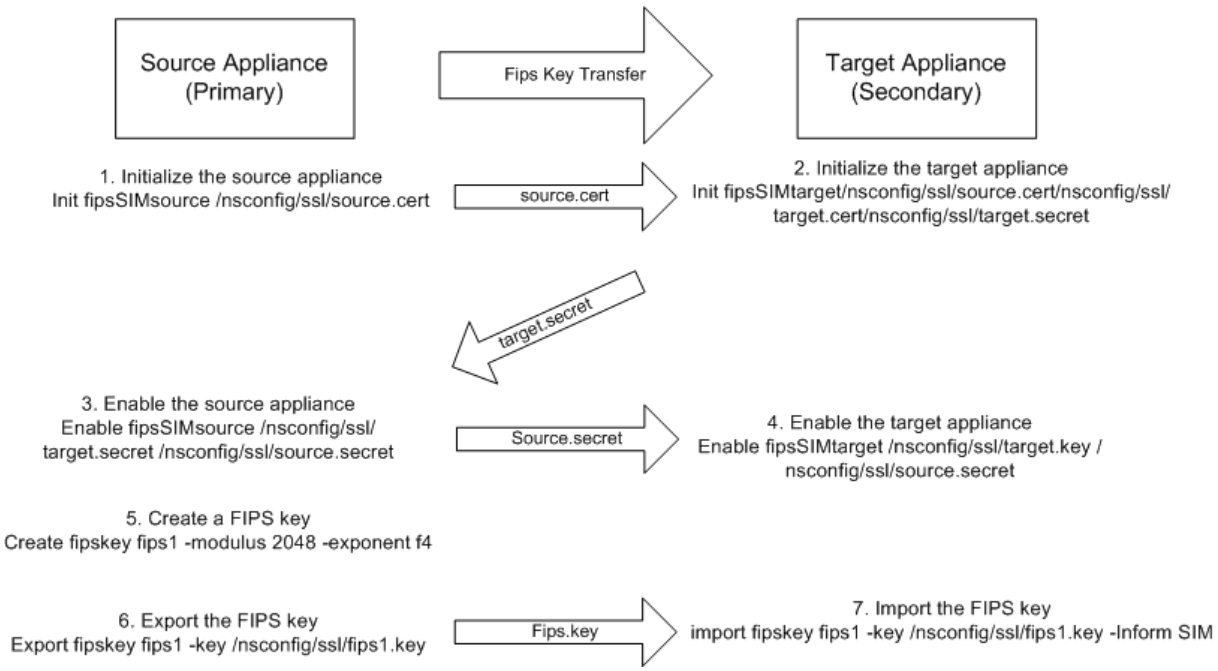
> 1. Reinicie el dispositivo o espere 10 minutos.
> 2. Elimine todos los archivos creados por el procedimiento.
> 3. Repita el procedimiento de configuración de HA.
>
> No vuelva a utilizar los nombres de archivo existentes.

En el procedimiento siguiente, el dispositivo A es el nodo principal y el dispositivo B es el nodo secundario.

Configurar FIPS en dispositivos en una configuración de alta disponibilidad mediante la CLI

El siguiente diagrama resume el proceso de transferencia en la CLI.

Ilustración 1. Transferir el resumen de claves FIPS



1. **En el dispositivo A**, abra una conexión SSH al dispositivo mediante un cliente SSH, como PuTTY.
2. Inicie sesión en el dispositivo con las credenciales de administrador.
3. Inicialice el dispositivo A como dispositivo de origen. En el símbolo del sistema, escriba:

```
init ssl fipsSIMsource <certFile>
<!--NeedCopy-->
```

Ejemplo:

```
init fipsSIMsource /nsconfig/ssl/nodeA.cert
```

4. Copie este archivo <certFile> en el dispositivo B, en la carpeta /nconfig/ssl.

Ejemplo:

```
scp /nsconfig/ssl/nodeA.cert nsroot@198.51.100.10:/nsconfig/ssl
```

5. **En el dispositivo B**, abra una conexión SSH con el dispositivo a través de un cliente SSH, como PuTTY.
6. Inicie sesión en el dispositivo con las credenciales de administrador.
7. Inicialice el dispositivo B como dispositivo de destino. En el símbolo del sistema, escriba:

```
init ssl fipsSIMtarget <certFile> <keyVector> <targetSecret>
<!--NeedCopy-->
```


Ejemplo:

```
init fipsSIMtarget /nsconfig/ssl/nodeA.cert /nsconfig/ssl/nodeB.key /
nsconfig/ssl/nodeB.secret
```

8. Copie este archivo <targetSecret> en el dispositivo A.

   Ejemplo:

   ```
   scp /nsconfig/ssl/fipslbdal0801b.secret nsroot@198.51.100.20:/nsconfig/
   ssl
   ```

9. **En el dispositivo A**, habilite el dispositivo A como dispositivo de origen. En el símbolo del sistema, escriba:

   ```
   1 enable ssl fipsSIMSource <targetSecret> <sourceSecret>
   2 <!--NeedCopy-->
   ```

   Ejemplo:

   ```
   enable fipsSIMsource /nsconfig/ssl/nodeB.secret /nsconfig/ssl/nodeA.
   secret
   ```

10. Copie este archivo <sourceSecret> en el dispositivo B.

    Ejemplo:

    ```
    scp /nsconfig/ssl/fipslbdal0801b.secret nsroot@198.51.100.10:/nsconfig/
    ssl
    ```

11. **En el dispositivo B**, habilite el dispositivo B como dispositivo de destino. En el símbolo del sistema, escriba:

    ```
    1 enable ssl fipsSIMtarget <keyVector> <sourceSecret>
    2 <!--NeedCopy-->
    ```

    Ejemplo:

    ```
    enable fipsSIMtarget /nsconfig/ssl/nodeB.key /nsconfig/ssl/nodeA.secret
    ```

12. **En el dispositivo A**, cree una clave FIPS, tal como se describe en Crear una clave FIPS.
13. Exporte la clave FIPS al disco duro del dispositivo, tal como se describe en Exportar una clave FIPS.
14. Copie la clave FIPS en el disco duro del dispositivo secundario mediante una utilidad de transferencia segura de archivos, como SCP.
15. **En el dispositivo B**, importe la clave FIPS del disco duro al HSM del dispositivo, tal como se describe en Importar una clave FIPS.

Configurar FIPS en dispositivos en una configuración de alta disponibilidad mediante la GUI

1. En el dispositivo que se configurará como dispositivo de origen (principal), vaya a **Administración del tráfico > SSL > FIPS**.
2. En el panel de detalles, en la ficha Información FIPS, haga clic en **Habilitar SIM**.
3. En el cuadro de diálogo **Habilitar SIM para par HA**, en el cuadro de texto **Nombre de archivo de certificado**, escriba el nombre del archivo. El nombre del archivo debe contener la ruta de acceso a la ubicación en la que se debe almacenar el certificado FIPS en el dispositivo de origen.
4. En el cuadro de texto **Nombre de archivo vectorial clave**, escriba el nombre del archivo. El nombre de archivo debe contener la ruta de acceso a la ubicación en la que se debe almacenar el vector de clave FIPS en el dispositivo de origen.
5. En el cuadro de texto **Nombre de archivo secreto de destino**, escriba la ubicación para almacenar los datos secretos en el dispositivo de destino.
6. En el cuadro de texto **Nombre de archivo secreto de origen**, escriba la ubicación para almacenar los datos secretos en el dispositivo de origen.
7. En **Credencial de inicio de sesión del sistema secundario**, introduzca los valores de **Nombre de usuario** y **Contraseña**.
8. Haga clic en **OK**. Los dispositivos FIPS ahora están configurados en modo HA.

Nota: Después de configurar los dispositivos en HA, cree una clave FIPS, tal como se describe en Crear una clave FIPS. La clave FIPS se transfiere automáticamente del dispositivo primario al secundario.

Crear una solicitud de firma de certificado mediante la CLI

En el símbolo del sistema, escriba:

```
create ssl certReq <reqFile> (-keyFile <input_filename> | -fipsKeyName
    <string>) [-keyform ( DER | PEM )  {
 -PEMPassPhrase  }
 ] -countryName <string> -stateName <string> -organizationName<string>
    [-organizationUnitName <string>] [-localityName <string>] [-
    commonName <string>] [-emailAddress <string>] {
 -challengePassword  }
  [-companyName <string>] [-digestMethod ( SHA1 | SHA256 )]
<!--NeedCopy-->
```

Ejemplo:

```
>create certreq f1.req  - fipsKeyName  f1 -countryName US  -stateName CA
    -organizationName Citrix -companyName Citrix -commonName ctx -
   emailAddress test@example.com
```



```
Done
<!--NeedCopy-->
```

Crear un certificado de servidor mediante la CLI

En el símbolo del sistema, escriba:

```
create ssl cert <certFile> <reqFile> <certType> [-keyFile <
    input_filename>] [-keyform ( DER | PEM ) {
 -PEMPassPhrase  }
 ] [-days <positive_integer>] [-certForm ( DER | PEM )] [-CAcert <
    input_filename>] [-CAcertForm ( DER | PEM )] [-CAkey <
    input_filename>][-CAkeyForm ( DER | PEM )] [-CAserial <
    output_filename>]
<!--NeedCopy-->
```

Ejemplo:

```
create cert f1.cert f1.req SRVR_CERT -CAcert ns-root.cert -CAkey ns-
    root.key -CAserial ns-root.srl -days 1000
Done
<!--NeedCopy-->
```

En el ejemplo anterior se crea un certificado de servidor mediante una CA raíz local del dispositivo.

Agregar un par de claves de certificado mediante la CLI

En el símbolo del sistema, escriba:

```
add ssl certKey <certkeyName> (-cert <string> [-password]) [-key <
    string> | -fipsKey <string> | -hsmKey <string>] [-inform <inform>][-
    expiryMonitor ( ENABLED | DISABLED ) [-notificationPeriod <
    positive_integer>]] [-bundle ( YES | NO )]
<!--NeedCopy-->
```

Ejemplo:


```
add certkey cert1 -cert f1.cert -fipsKey f1

<!--NeedCopy-->
```

Después de crear la clave FIPS y el certificado de servidor, puede agregar la configuración SSL genérica. Habilite las funciones necesarias para su implementación. Agregue servidores, servicios y servidores virtuales SSL. Enlazar el par de claves de certificado y el servicio al servidor virtual SSL. Guarde la configuración.

```
enable ns feature SSL LB

add server s1 10.217.2.5

add service sr1 s1 HTTP 80

add lb vserver v1 SSL 10.217.2.172 443

bind ssl vserver v1  - certkeyName cert1

bind lb vserver v1 sr1

saveconfig

<!--NeedCopy-->
```

Ya se ha completado la configuración básica de su dispositivo MPX 14000 FIPS.

Para obtener información sobre cómo configurar HTTPS seguro, haga clic en Configurar FIPS.

Para obtener información sobre cómo configurar RPC seguro, haga clic en Configurar FIPS por primera vez.

Actualizar la licencia en un dispositivo MPX 14000 FIPS

Cualquier actualización de la licencia en esta plataforma requiere dos reinicios.

1. Actualiza la licencia en la carpeta `/nsconfig/license`.
2. Reinicie el dispositivo.
3. Inicie sesión en el dispositivo.
4. Reinicie el dispositivo de nuevo.
   Nota: No agregue nuevos comandos, guarde la configuración ni compruebe el estado del sistema antes del segundo reinicio.

5. Inicie sesión en el dispositivo y asegúrese de que FIPS se inicializa mediante la ejecución del comando `show ssl fips`.

Compatibilidad con el modo FIPS híbrido en las plataformas FIPS MPX 14000 y SDX 14000 FIPS

> **Nota:**
>
> Esta función solo es compatible con la nueva plataforma FIPS MPX/SDX 14000 que contiene una tarjeta FIPS principal y una o más tarjetas secundarias. No es compatible con una plataforma VPX ni en una plataforma que contenga solo un tipo de tarjeta de hardware.

En una plataforma FIPS, el cifrado y el descifrado asimétricos y simétricos se realizan en la tarjeta FIPS por motivos de seguridad. Sin embargo, puede realizar parte de esta actividad (asimétrica) en una tarjeta FIPS y descargar el cifrado y descifrado masivo (simétrico) a otra tarjeta sin comprometer la seguridad de sus claves.

La nueva plataforma FIPS MPX/SDX 14000 contiene una tarjeta principal y una o más tarjetas secundarias. Si habilita el modo FIPS híbrido, los comandos de descifrado secreto pre-master se ejecutan en la tarjeta principal porque la clave privada se almacena en esta tarjeta. Sin embargo, el cifrado y el descifrado masivos se descargan en la tarjeta secundaria. Esta descarga aumenta significativamente el rendimiento del cifrado masivo en una plataforma FIPS MPX/SDX 14000 en comparación con el modo FIPS no híbrido y la plataforma FIPS MPX 9700/10500/12500/15000 existente. Habilitar el modo FIPS híbrido también mejora la transacción SSL por segundo en esta plataforma.

> **Notas:**
>
> - El modo FIPS híbrido está inhabilitado de forma predeterminada para cumplir con los estrictos requisitos de certificación, en los que todo el cálculo criptográfico debe realizarse dentro de un módulo certificado FIPS. Habilite el modo híbrido para descargar el cifrado y el descifrado masivos a la tarjeta secundaria.
> - En una plataforma FIPS SDX 14000, primero debe asignar un chip SSL a la instancia VPX antes de habilitar el modo híbrido.

Habilitar el modo FIPS híbrido mediante la CLI

En el símbolo del sistema, escriba:

```
set SSL parameter -hybridFIPSMode {
 ENABLED|DISABLED }


Arguments
```



```
6
7  hybridFIPSMode
8
9  When this mode is enabled, system will use additional crypto hardware
       to accelerate symmetric crypto operations.
10
11 Possible values: ENABLED, DISABLED
12
13 Default value: DISABLED
14 <!--NeedCopy-->
```

Ejemplo:

```
1      set SSL parameter -hybridFIPSMode ENABLED
2      show SSL parameter
3      Advanced SSL Parameters
4      ----------------------
5      . . . . . .
6      Hybrid FIPS Mode    : ENABLED
7      . . . . . .
8
9  <!--NeedCopy-->
```

Habilitar el modo FIPS híbrido mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > SSL**.
2. En el panel de detalles, en **Configuración**, haga clic en **Cambiar la configuración avanzada de SSL**.
3. En el cuadro de diálogo **Cambiar configuración SSL avanzada**, seleccione **Modo FIPS híbrido**.

Limitaciones:

1. No se admite la renegociación.
2. El comando `stat ssl parameter` de una plataforma SDX 14000 no muestra el porcentaje de utilización de la tarjeta secundaria correcto. Siempre muestra un 0,00% de utilización.

```
1  stat ssl
2
3  SSL Summary
4  # SSL cards present 1
5  # SSL cards UP  1
```



```
# Secondary SSL cards present   4
# Secondary SSL cards UP    4
SSL engine status      1
SSL sessions (Rate)     963
Secondary card utilization (%)     0.00
<!--NeedCopy-->
```

Dispositivos FIPS SDX 14000

April 21, 2022

> **Nota**
>
> Las versiones de firmware enumeradas en “Citrix ADC versión 12.1-FIPS” y “Citrix ADC versión 12.1-ndCPP” en la página de descargas de Citrix ADC no son compatibles con las plataformas MPX 14000 FIPS o SDX 14000 FIPS. Estas plataformas pueden usar otras versiones más recientes del firmware de Citrix ADC disponibles en la página de descargas.

Un dispositivo Citrix ADC SDX es una plataforma multiarrendatario en la que puede aprovisionar y administrar varias instancias virtuales de Citrix ADC. El dispositivo SDX aborda los requisitos de informática en la nube y de multiarrendamiento al permitir a un único administrador configurar y administrar el dispositivo y delegar la administración de cada instancia alojada en los arrendatarios.

Un dispositivo FIPS Citrix ADC SDX 14030/14060/14080 proporciona las capacidades de un dispositivo SDX con funcionalidad FIPS. Está equipado con un módulo criptográfico a prueba de manipulaciones (a prueba de manipulaciones), un Cavium CNN3560-NFBE-G, diseñado para cumplir con las especificaciones FIPS 140-2 nivel 3 (a partir de la versión 12.0 compilación 56.x). Los parámetros de seguridad críticos (CSP), principalmente la clave privada del servidor, se almacenan y generan de forma segura dentro del módulo criptográfico. Este módulo también se conoce como módulo de seguridad de hardware (HSM). Nunca se accede a los CSP fuera de los límites del HSM. Solo el superusuario (`nsroot`) puede realizar operaciones con las claves almacenadas en el HSM.

Un dispositivo FIPS Citrix ADC SDX 14030/14060/14080 contiene un módulo FIPS HSM con 63 núcleos. El módulo FIPS HSM se puede particionar hasta un máximo de 32 particiones. El administrador de SDX puede asignar almacenamiento de claves dedicado, recursos criptográficos y cantidad de núcleos FIPS SSL criptográficos a cada partición. Las claves y los recursos asignados a una partición son dedicados y seguros, y ninguna otra partición no puede acceder a ellos ni compartirlos.

La partición FIPS HSM que cree se puede asignar o adjuntar a una instancia VPX en el momento de aprovisionar la instancia o, posteriormente, modificando la instancia. La partición FIPS creada y conectada a una instancia actúa como un módulo HSM virtual para esa instancia.

A las instancias VPX de un dispositivo FIPS SDX 14030/14060/14080 se les asigna una partición de función virtual (VF) FIPS, que se trata como una tarjeta virtual FIPS aislada o HSM. Por lo tanto, los pasos para configurar una partición FIPS dentro de una instancia VPX son similares a los pasos para configurar un dispositivo FIPS MPX. Para obtener más información sobre el cumplimiento, consulte los detalles de la directiva de seguridad en el sitio web del Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos.

Para obtener información sobre la configuración de dispositivos FIPS en una configuración de alta disponibilidad, consulte Dispositivos FIPS en una configuración de alta disponibilidad.

> **Importante**
>
> Cada clave incluye una clave privada y una pública. Como resultado, ocupa dos espacios clave. Por lo tanto, el número máximo de llaves se limita a una menos de la mitad del tamaño del almacén de claves.

La plataforma FIPS SDX 14000 admite un modo FIPS híbrido. Este modo le permite descargar parte de la actividad de cifrado y descifrado a una tarjeta que no sea FIPS. Para obtener más información, consulte Modo FIPS híbrido.

Limitaciones

January 12, 2021

1. La renegociación SSL mediante el protocolo SSLv3 no se admite en el back-end de un dispositivo SDX FIPS.
2. No se admiten claves de 1024 bits y 4096 bits y un valor exponente de 3.
3. No se admiten copias de seguridad y restauración.
4. No se admiten dominios de clúster y administrativos.
5. Solo puede adjuntar una partición FIPS a una instancia.
6. A una instancia con una partición FIPS solo se le puede asignar un núcleo de CPU.
7. Puede asignar una partición FIPS o un núcleo SSL a una instancia, pero no ambas.
8. No se admite el certificado de servidor de 4096 bits.
9. No se admite el certificado de cliente de 4096 bits (si la autenticación de cliente está habilitada en el servidor back-end).

Terminología

February 16, 2021

Poner a cero: Restablecer el HSM. Se eliminan todos los datos del HSM. Este paso es obligatorio antes de inicializar el HSM.

Inicializar: Establezca las capacidades de HSM. El dispositivo Citrix ADC SDX FIPS cumple con el nivel 2 de FIPS-140-2. Puede crear particiones después de inicializar el chip.

Tamaño del almacén de claves: Número de claves que se pueden almacenar en una partición. Se puede especificar un máximo de 102235 teclas. El número máximo de claves que se pueden almacenar es menos de la mitad del número especificado. Por ejemplo, si especifica 100, solo puede crear 49 claves porque una de ellas es el par de claves RSA que consume 2 almacenes de claves.

Capacidad de Crypto Core: Número de núcleos criptográficos asignados a una partición. Hay un máximo de 63 núcleos disponibles.

Contexto SSL: Número de conexiones SSL simultáneas que se pueden crear en una partición.

Inicializar el HSM

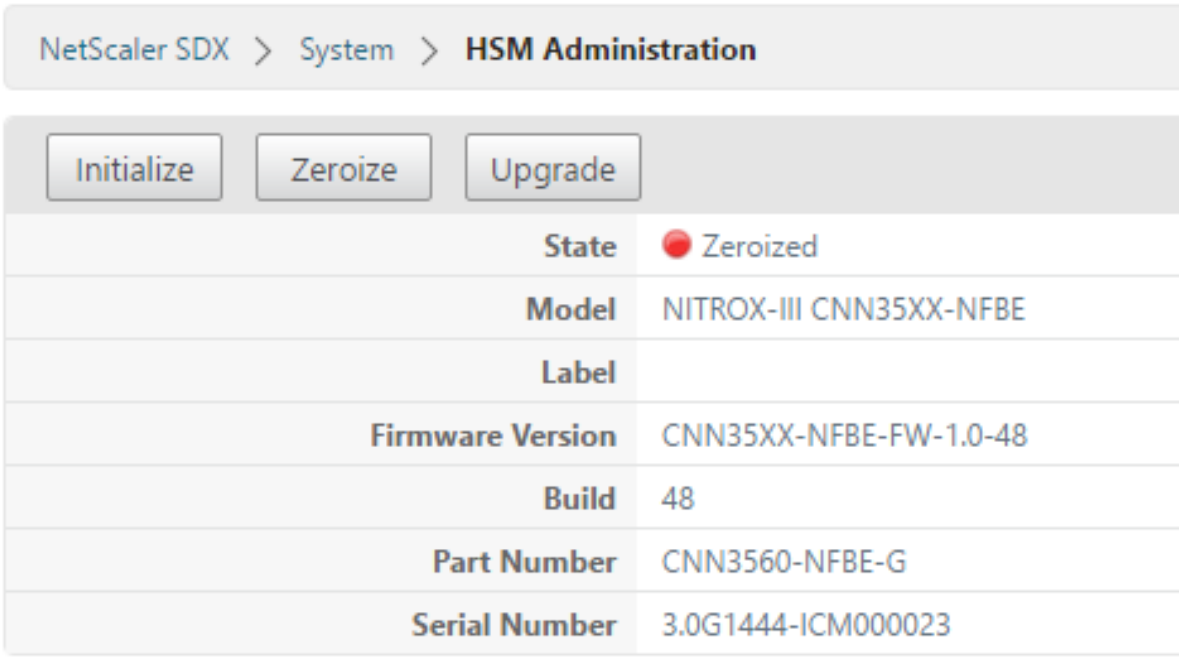
January 12, 2021

Antes de inicializar el HSM, primero debe poner a cero.

Poner a cero el HSM mediante el servicio de administración

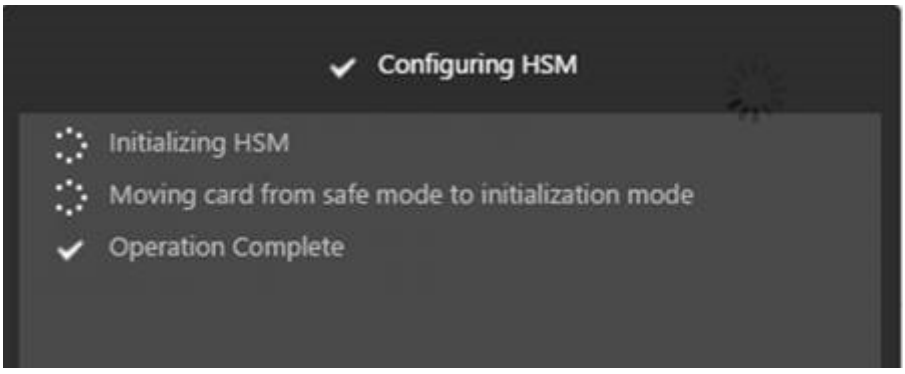
1. Abra un explorador e inicie sesión en el dispositivo.
2. En la ficha **Configuración**, vaya a **Sistema > Administración de HSM** y, en el plano de detalles, haga clic en **Zeroize**.

Todos los datos se borran del chip FIPS y el estado aparece como “Convertido en cero”. Se eliminan todas las particiones HSM creadas anteriormente.

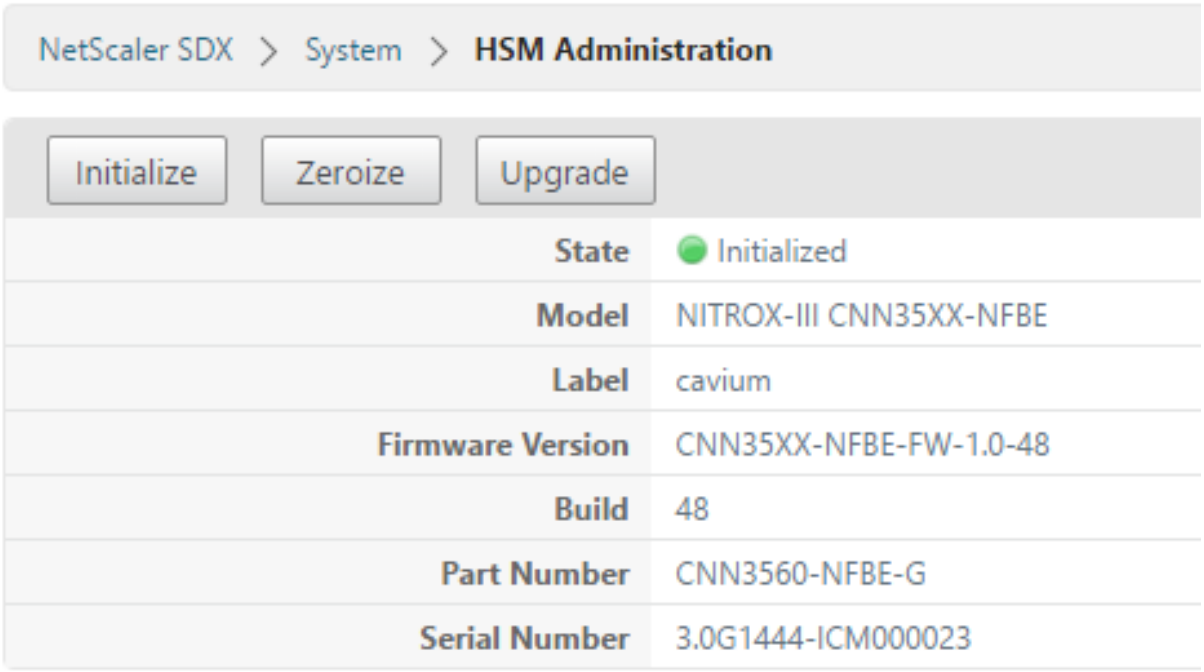


Inicializar el HSM mediante el servicio de administración

1. En la ficha **Configuración**, vaya a **Sistema > Administración de HSM** y, en el plano de detalles, haga clic en **Inicializar**.
2. Escriba un nuevo nombre de usuario, especifique una contraseña y haga clic en **Aceptar**.



El estado de la tarjeta aparece como “Inicializado”.



Crear particiones

January 12, 2021

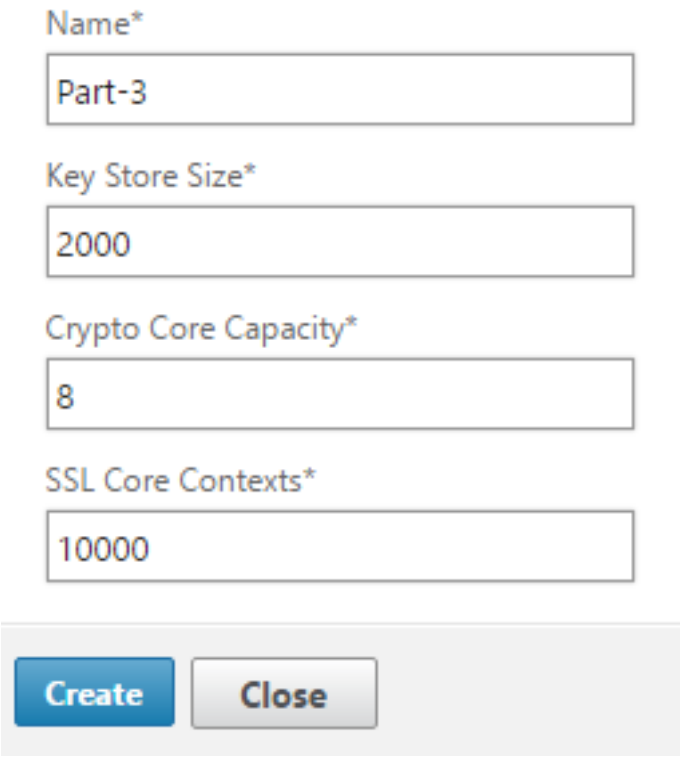
Cree particiones para diferentes arrendatarios y especifique los recursos criptográficos para cada partición. A cada instancia se le asigna una partición y una partición solo se puede asignar a una instancia. Al eliminar una instancia, se elimina la partición asignada a la instancia. Como resultado, los datos de partición también se eliminan y no se dejan sin seguridad o accesibles más tarde. El número de claves y la asignación de contexto SSL depende de su aplicación. Para obtener información sobre el número de núcleos que se deben asignar, consulte la hoja de datos de Citrix ADC.

> **Importante**
>
> Después de asignar un tamaño de almacén de claves y núcleos a una partición HSM, no puede cambiarlos en tiempo de ejecución. Primero separe la partición de la instancia.

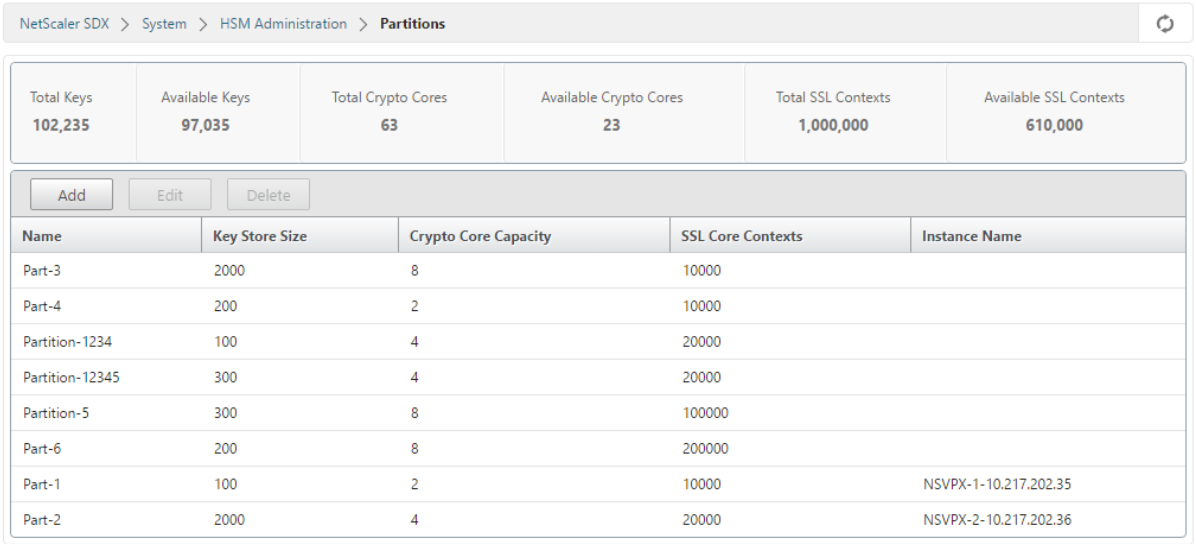
Crear una partición mediante el servicio de administración

1. En la ficha Configuración, vaya a **Sistema** > **Administración HSM** > **Particiones** y, en el plano de detalles, haga clic en **Agregar**.

2. Especifique un nombre para la partición y los recursos que se van a asignar a esta partición.
3. Haga clic en **Aceptar**.



La página de resumen muestra todas las particiones creadas. A algunas particiones se les asigna una instancia, mientras que otras son particiones libres.



Name	Key Store Size	Crypto Core Capacity	SSL Core Contexts	Instance Name
Part-3	2000	8	10000	
Part-4	200	2	10000	
Partition-1234	100	4	20000	
Partition-12345	300	4	20000	
Partition-5	300	8	100000	
Part-6	200	8	200000	
Part-1	100	2	10000	NSVPX-1-10.217.202.35
Part-2	2000	4	20000	NSVPX-2-10.217.202.36

Aprovisionar una nueva instancia o modificar una instancia existente y asignar una partición

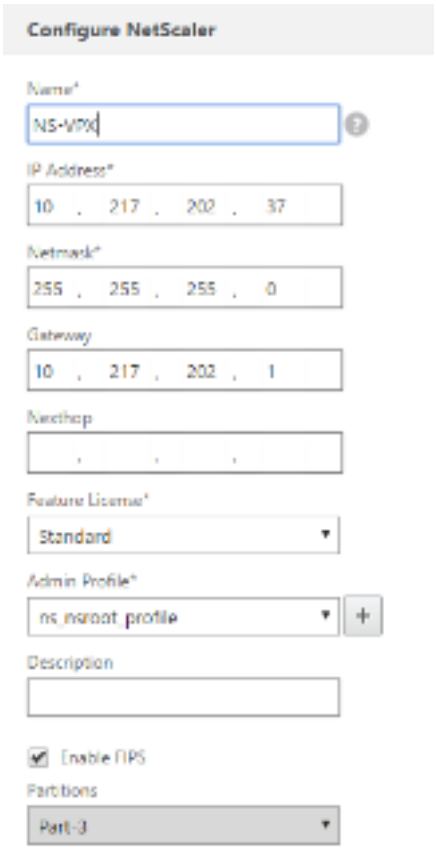
August 11, 2022

Después de crear las particiones, debe asignarlas a las instancias.

> **Importante:**
>
> - Solo puede adjuntar una partición FIPS a una instancia.
> - A una instancia con una partición FIPS solo se le puede asignar un núcleo de CPU.

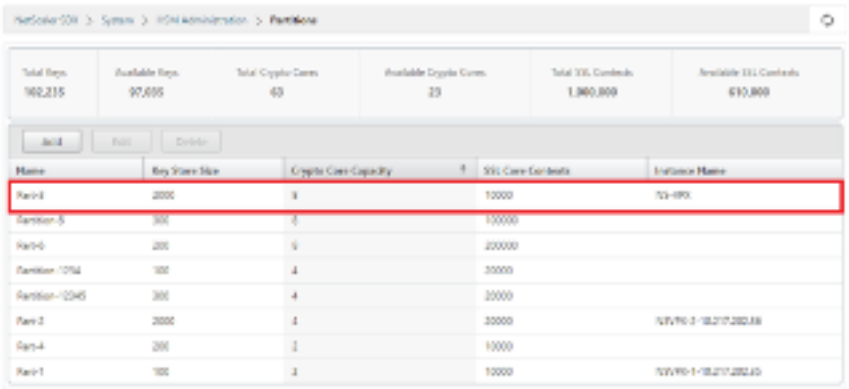
Aprovisionar una nueva instancia o modificar una instancia existente

1. En la ficha Configuración, vaya a **NetScaler** > **Instancias** y agregue o modifique una instancia.
2. Seleccione **Habilitar FIPS** y, en la lista **Particiones**, seleccione una partición para adjuntarla a esta instancia.



Puede verificar que la partición esté conectada a una instancia mediante la GUI o la CLI.

En la GUI, vaya a **Sistema** > **Administración de HSM** > **Particiones**. Se muestra el nombre de la instancia adjunta a la partición.



Para anular la asignación de una partición FIPS, vaya a **NetScaler** > **Instancias**. Modifique la instancia y desmarque la casilla **Habilitar FIPS**.

En la CLI, en el símbolo del sistema, escriba los siguientes comandos:

```
1 show fips
2
3 FIPS Card is not configured
4  Done
5 <!--NeedCopy-->
```

Si ve el siguiente resultado, consulte la sección de solución de problemas para la depuración.

ERROR: Operación no permitida; no hay ninguna tarjeta FIPS en el sistema

> Nota
>
> Cuando se separa una partición de cualquiera de las instancias VPX existentes, los datos de la partición se borran. Como resultado, se pierde cualquier configuración actual (por ejemplo, las claves FIPS). Después de desconectar o volver a conectar una partición a una instancia VPX nueva o previamente enlazada, se debe inicializar según las instrucciones de Configurar el HSM antes de poder usar la partición para cualquier conexión segura.
>
> Durante este tiempo (después de desconectar o volver a conectar la partición), se puede acceder a la instancia VPX correspondiente a través de la GUI mediante HTTP y a través de la CLI mediante SSH.

Configurar el HSM para una instancia en un dispositivo FIPS SDX 14030/14060/14080

December 2, 2021

Primero compruebe el estado de la tarjeta FIPS para verificar que el controlador se haya cargado correctamente y, a continuación, inicialice la tarjeta.

En el símbolo del sistema, escriba:

```
1 show fips
2
3 FIPS Card is not configured
4
5 Done
6 <!--NeedCopy-->
```

Si el controlador no está cargado correctamente, aparece el mensaje “ERROR: no se permite la operación, no hay tarjeta FIPS presente en el sistema”.

Inicializar la tarjeta FIPS

> **Importante:**
>
> Compruebe que el directorio `/nsconfig/fips` se haya creado correctamente en el dispositivo.

No guarde la configuración antes de reiniciar el dispositivo por tercera vez.

Realice los siguientes pasos para inicializar la tarjeta FIPS:

1. Reinicie la tarjeta FIPS (`reset fips`).
2. Reinicie el dispositivo (`reboot`).
3. Establezca la contraseña del oficial de seguridad para las particiones 0 y 1, y la contraseña de usuario para la partición (`set fips -initHSM Level-2 <soPassword> <oldsoPassword> <userPassword> -hsmLabel NSFIPS`).

   Nota: El comando set or reset tarda más de 60 segundos en ejecutarse.
4. Guarde la configuración (`saveconfig`).
5. Compruebe que la clave cifrada con contraseña para la partición principal (master_pek.key) se haya creado en el directorio /nsconfig/fips/.
6. Reinicie el dispositivo (`reboot`).
7. Compruebe que la tarjeta FIPS esté UP (`show fips`).

Inicializar la tarjeta FIPS mediante la CLI

En el símbolo del sistema, escriba los comandos siguientes:

```
reset fips

reboot

set fips -initHSM Level-2 <soPassword> <oldsoPassword> <userPassword> -
    hsmLabel <string>
<!--NeedCopy-->
```

> **Nota**: Aparece el siguiente mensaje al ejecutar el comando **set fips** :

```
This command will erase all data on the FIPS card. You must save the
    configuration (saveconfig) after executing this command. [Note: On
    MPX/SDX 14xxx FIPS platform, the FIPS security is at Level-3 by
    default, and the -initHSM Level-2 option is internally converted to
    Level-3]  Do you want to continue?(Y/N)y

saveconfig

reboot

show fips
<!--NeedCopy-->
```

Ejemplo:

```
reset fips

Done

reboot

set fips -initHSM Level-2 so12345 so12345 user123 -hsmLabel NSFIPS

This command will erase all data on the FIPS card. You must save the
    configuration (saveconfig) after executing this command. [Note: On
    MPX/SDX 14xxx FIPS platform, the FIPS security is at Level-3 by
```



```
      default, and the -initHSM Level-2 option is internally converted to
      Level-3]  Do you want to continue?(Y/N)y

Done

saveconfig

Done

reboot

show fips

    FIPS HSM Info:
    HSM Label : NSFIPS
    Initialization : FIPS-140-2 Level-2
    HSM Serial Number : 3.0G1532-ICM000228
    HSM State : 2
    HSM Model : NITROX-III CNN35XX-NFBE
    Hardware Version : 0.0-G
    Firmware Version : 1.0
    Firmware Build : NFBE-FW-1.0-48
    Max FIPS Key Memory : 1000
    Free FIPS Key Memory : 1000
    Total SRAM Memory : 557396
    Free SRAM Memory : 238088
    Total Crypto Cores : 4
    Enabled Crypto Cores : 4
Done
<!--NeedCopy-->
```

Crear una clave FIPS para una instancia en un dispositivo FIPS SDX 14030/14060/14080

August 20, 2021

Puede crear una clave FIPS en la instancia o importar una clave FIPS existente en la instancia. Un dispositivo FIPS SDX 14030/14060/14080 admite solo claves de 2048 bits y 3072 bits y un valor exponente de F4. Para las claves PEM, no se requiere un exponente. Verifique que la clave FIPS se haya creado correctamente. Cree una solicitud de firma de certificado y un certificado de servidor. Finalmente, agregue el par certificate-key a su instancia.

> **Nota:**
>
> No se admiten claves de 1024 bits y 4096 bits y un valor exponente de 3.

Crear una clave FIPS mediante la CLI

En el símbolo del sistema, escriba:

```
create ssl fipsKey <fipsKeyName> -keytype ( RSA | ECDSA ) [-exponent (3 | F4 )] [-modulus <positive_integer>] [-curve ( P_256 | P_384 )]
<!--NeedCopy-->
```

Ejemplo:

```
create fipsKey f1 -keytype RSA -modulus 2048 -exponent F4

Done

show ssl fipskey ddvws

FIPS Key Name: f1  Key Type: RSA Modulus: 2048   Public Exponent: F4 (Hex: 0x10001)

Done
<!--NeedCopy-->
```

Importar una clave FIPS mediante la CLI

En el símbolo del sistema, escriba:

```
import ssl fipsKey <fipsKeyName> -key <string> [-inform <inform>] [-wrapKeyName <string>] [-iv<string>] [-exponent F4 ]
<!--NeedCopy-->
```

Ejemplo:

```
import fipskey Key-FIPS-2 -key Key-FIPS-2.key -inform SIM -exponent F4
Done
```



```
3 import fipskey Key-FIPS-2 -key Key-FIPS-2.key -inform PEM
4 Done
5 <!--NeedCopy-->
```

Compruebe que la clave FIPS se ha creado o importado correctamente ejecutando el comando **show fipskey**.

```
1 show fipskey
2 1)      FIPS Key Name: Key-FIPS-2
3 Done
4 <!--NeedCopy-->
```

Crear una solicitud de firma de certificado mediante la CLI

En el símbolo del sistema, escriba:

```
1 create ssl certReq <reqFile> (-keyFile <input_filename> | -fipsKeyName
     <string>) [-keyform ( DER | PEM )  {
2  -PEMPassPhrase  }
3  ] -countryName <string> -stateName <string> -organizationName<string>
      [-organizationUnitName <string>] [-localityName <string>] [-
      commonName <string>] [-emailAddress <string>] {
4  -challengePassword  }
5   [-companyName <string>] [-digestMethod ( SHA1 | SHA256 )]
6 <!--NeedCopy-->
```

Ejemplo:

```
1 create certreq f1.req  - fipsKeyName f1 -countryName US -stateName CA -
     organizationName Citrix -companyName Citrix -commonName ctx -
     emailAddress test@example.com`
2 `Done
3 <!--NeedCopy-->
```

Crear un certificado de servidor mediante la CLI

En el símbolo del sistema, escriba:


```
create ssl cert <certFile> <reqFile> <certType> [-keyFile <
    input_filename>] [-keyform ( DER | PEM ) {
 -PEMPassPhrase  }
 ] [-days <positive_integer>] [-certForm ( DER | PEM )] [-CAcert <
    input_filename>] [-CAcertForm ( DER | PEM )] [-CAkey <
    input_filename>] [-CAkeyForm ( DER | PEM )] [-CAserial <
    output_filename>]
<!--NeedCopy-->
```

Ejemplo:

```
create cert f1.cert f1.req SRVR_CERT -CAcert ns-root.cert -CAkey ns-
    root.key -CAserial ns-root.srl -days 1000
Done
<!--NeedCopy-->
```

En el ejemplo anterior se crea un certificado de servidor mediante una CA raíz local en el dispositivo.

Agregar un par de claves de certificado mediante la CLI

En el símbolo del sistema, escriba:

```
add ssl certKey <certkeyName> (-cert <string> [-password]) [-key <
    string> | -fipsKey <string> | -hsmKey <string>] [-inform <inform>]
    [-expiryMonitor ( ENABLED | DISABLED ) [-notificationPeriod   <
    positive_integer>]] [-bundle ( YES | NO )]
<!--NeedCopy-->
```

Ejemplo:

```
add certkey cert1 -cert f1.cert -fipsKey f1
Done
<!--NeedCopy-->
```

Después de crear la clave FIPS y el certificado de servidor, puede agregar la configuración SSL genérica. Habilite las funciones necesarias para la implementación. Agregue servidores, servicios y servidores virtuales SSL. Enlace el par de claves de certificado y el servicio al servidor virtual SSL y guarde la configuración.


```
enable ns feature SSL LB
Done
add server s1 10.217.2.5
Done
add service sr1 s1 HTTP 80
Done
add lb vserver v1 SSL 10.217.2.172 443
Done
bind ssl vserver v1  -certkeyName cert1
Done
bind lb vserver v1 sr1
Done
saveconfig
Done
<!--NeedCopy-->
```

Para obtener información sobre cómo configurar HTTPS seguro y RPC seguro, haga clic aquí.

Actualizar el firmware de FIPS en una instancia VPX

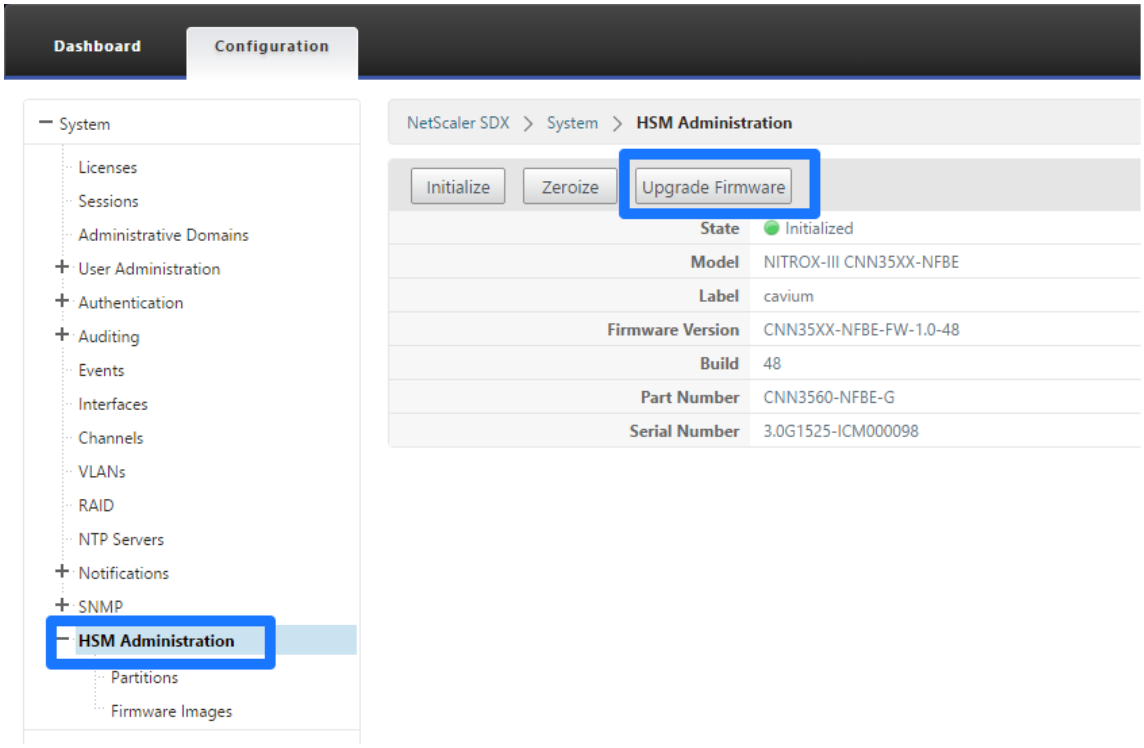
January 12, 2021

Las actualizaciones de firmware FIPS se lanzan de vez en cuando. Descargue el firmware más reciente de la página de descargas de Citrix y cárguelo en el dispositivo. El proceso de actualización puede tardar hasta 10 minutos en completarse. La instancia se reinicia después de la actualización.

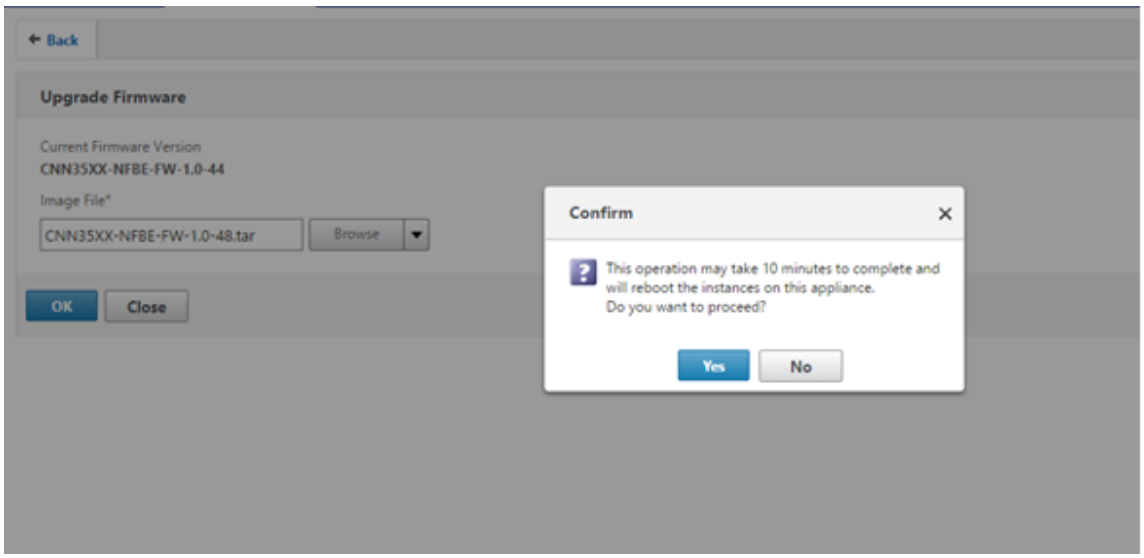
Actualizar el firmware de FIPS

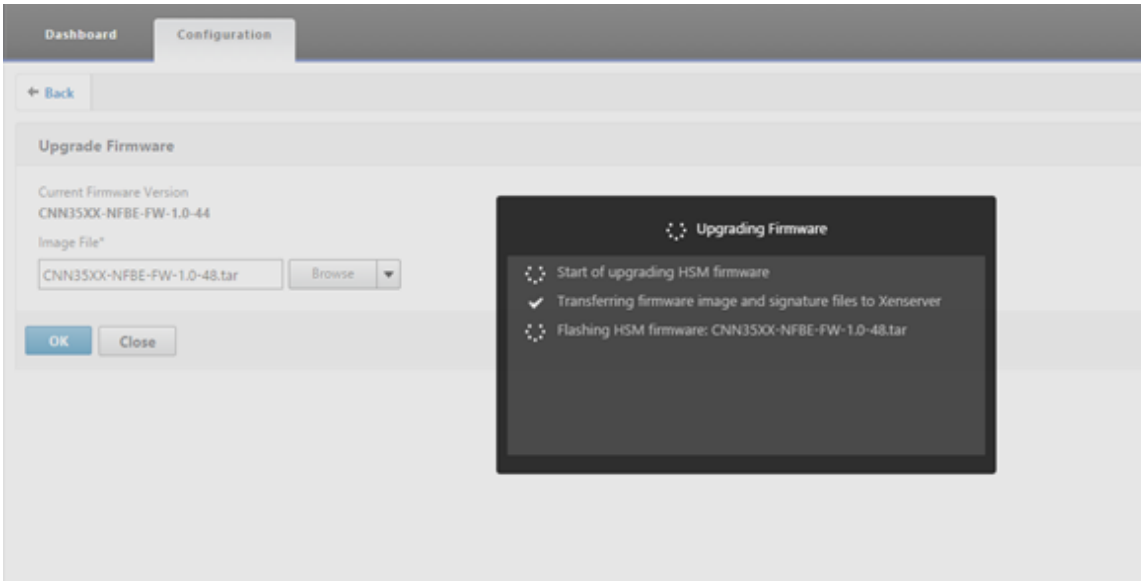
1. Vaya a **Sistema > Administración de HSM > Imágenes de firmware**.
2. Selecciona **Cargar**.

3. Vaya a la carpeta que contiene la imagen del firmware y seleccione el archivo.
4. Vaya a **Sistema > Administración de HSM**y seleccione **Actualizar firmware**.



5. Seleccione la imagen de firmware a la que quiere actualizar y haga clic en **Aceptar**.





Compatibilidad con el módulo de seguridad de hardware (HSM) de NShield Connect

August 20, 2021

Un dispositivo Citrix ADC que no sea FIPS almacena la clave privada del servidor en el disco duro. En un dispositivo FIPS, la clave se almacena en un módulo criptográfico conocido como HSM. El almacenamiento de una clave en el HSM la protege de ataques físicos y de software. Además, las claves se cifran mediante el uso de cifrados especiales aprobados por FIPS.

Solo los dispositivos Citrix ADC MPX 9700/10500/12500/15500 FIPS admiten una tarjeta FIPS. La compatibilidad con FIPS no está disponible en otros dispositivos MPX ni en los dispositivos SDX y VPX. Esta limitación se resuelve al admitir un HSM externo de NShield Connect en todos los dispositivos Citrix ADC MPX, SDX y VPX, excepto los dispositivos FIPS MPX 9700/10500/12500/15500.

NShield® Connect es un HSM externo conectado a red con certificación FIPS. Con un NShield HSM, las claves se almacenan de forma segura como tokens de clave de aplicación en un servidor de archivos remoto (RFS) y solo se pueden reconstituir dentro del NShield HSM.

Si ya está usando un NShield HSM, ahora puede utilizar un dispositivo Citrix ADC para optimizar, proteger y controlar la entrega de todos los servicios empresariales y en la nube.

Nota:

- Los HSM de NShield cumplen con las especificaciones FIPS 140-2 de nivel 3, mientras que los dispositivos FIPS MPX cumplen con las especificaciones de nivel 2.

- No se puede descifrar el seguimiento mientras utiliza NShield HSM. Solo el `hardserver` puede leer la respuesta del HSM al dispositivo Citrix ADC, ya que está cifrada.

Tabla de versiones compatibles

Versión Citrix ADC	Versión de cliente de NShield	`Hardserver` Versión	Versión del firmware de NShield
10.5e, 11.0, 11.1, 12.0, 12.1	11.70, 11.72	2.71.2	2.50.16, 2.51.10

Descripción de la arquitectura

August 20, 2021

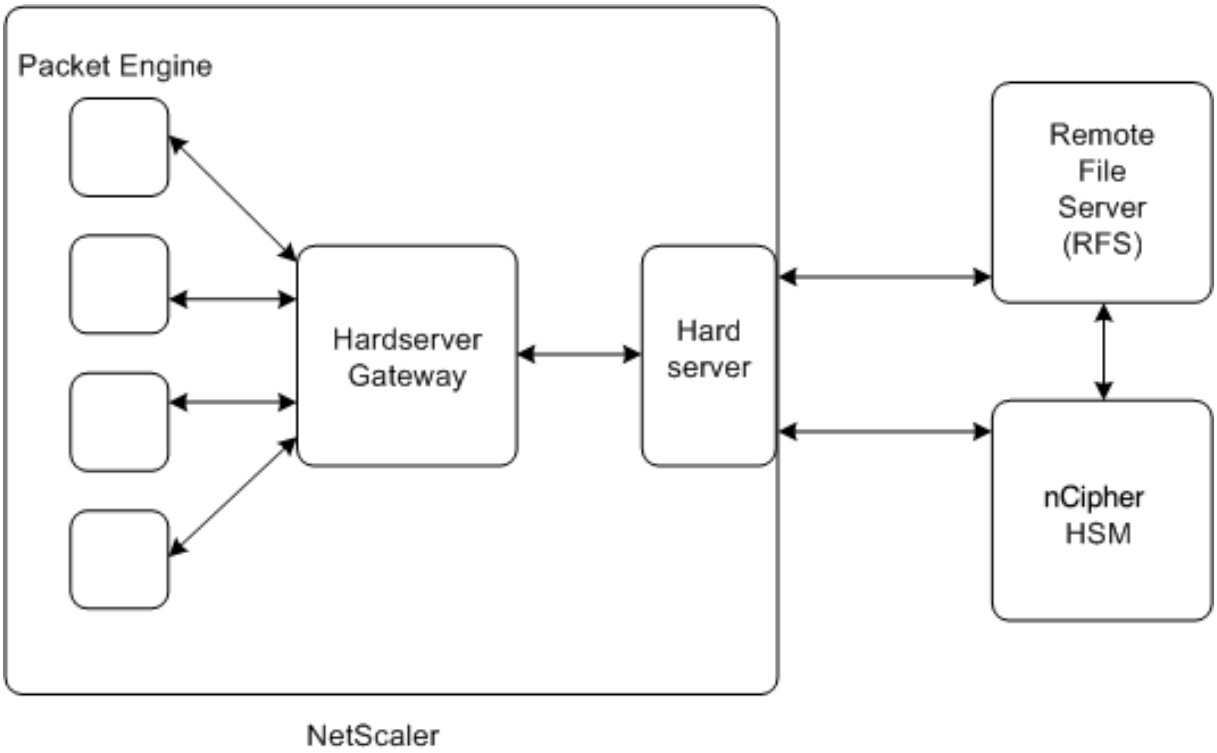
Las tres entidades que forman parte de una implementación de Citrix ADC-Entrust son un módulo Entrust nShield Connect, un servidor de archivos remoto (RFS) y un Citrix ADC.

Entrust nShield Connect es un módulo de seguridad de hardware conectado a la red. El RFS se utiliza para configurar el HSM y para almacenar los archivos de clave cifrada.

`Hardserver`, un demonio propietario proporcionado por Entrust, se utiliza para la comunicación entre el cliente (ADC), el HSM de Entrust y el RFS. Utiliza el protocolo de comunicación segura IMPATH. Un demonio de puerta de enlace, denominado `Hardserver Gateway`, se utiliza para comunicarse entre el motor de paquetes Citrix ADC y el `Hardserver`.

Nota: Los términos Entrust nShield Connect, Entrust HSM y HSM se utilizan indistintamente en esta documentación.

La siguiente ilustración ilustra la interacción entre los diferentes componentes.

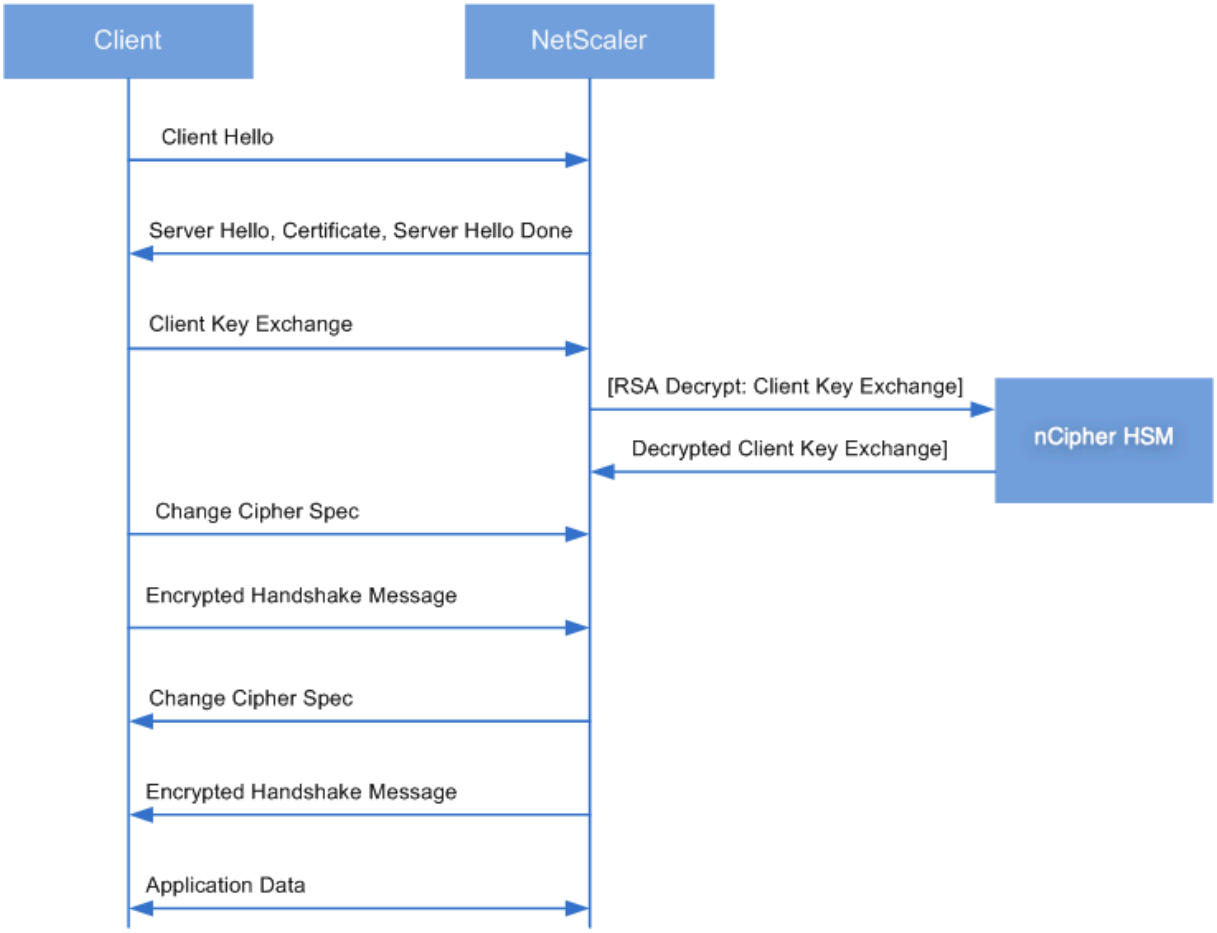


En una implementación típica, el RFS se utiliza para almacenar de forma segura las claves generadas por el HSM. Después de generar las claves, puede transferirlas de forma segura al ADC y, a continuación, utilizar la GUI o la línea de comandos para cargar las claves en el HSM. Un servidor virtual del ADC utiliza Entrust para descifrar el intercambio de claves de cliente y completar el protocolo de acceso SSL. A partir de entonces, todas las operaciones SSL se realizan en el ADC.

Nota: Los términos claves y tokens de clave de aplicación se utilizan indistintamente en esta documentación.

En la siguiente ilustración se ilustra el flujo de paquetes en el apretón de manos SSL con el HSM de Entrust.

Ilustración 1. Diagrama de flujo de paquetes de apretones de manos SSL con Citrix ADC mediante Entrust HSM



Nota: La comunicación entre el ADC y el HSM utiliza un protocolo de comunicación propietario de Entrust, denominado IMPATH.

Requisitos previos

August 20, 2021

Antes de poder utilizar un nShield Connect de Entrust con un Citrix ADC, asegúrese de que se cumplen los siguientes requisitos previos:

- Un dispositivo Entrust nShield Connect está instalado en la red, listo para usar y accesible para Citrix ADC. Es decir, la dirección NSIP se agrega como un cliente autorizado en el HSM.
- Existe un mundo de seguridad utilizable. Security World es una arquitectura única de administración de claves utilizada por la línea de HSM de Entrust nShield. Protege y administra las claves como tokens de clave de aplicación, lo que permite una capacidad de clave ilimitada y copia de seguridad y recuperación automáticas de claves. Para obtener más información sobre cómo crear un mundo de seguridad, consulte la Guía de inicio rápido de nShield Connect de

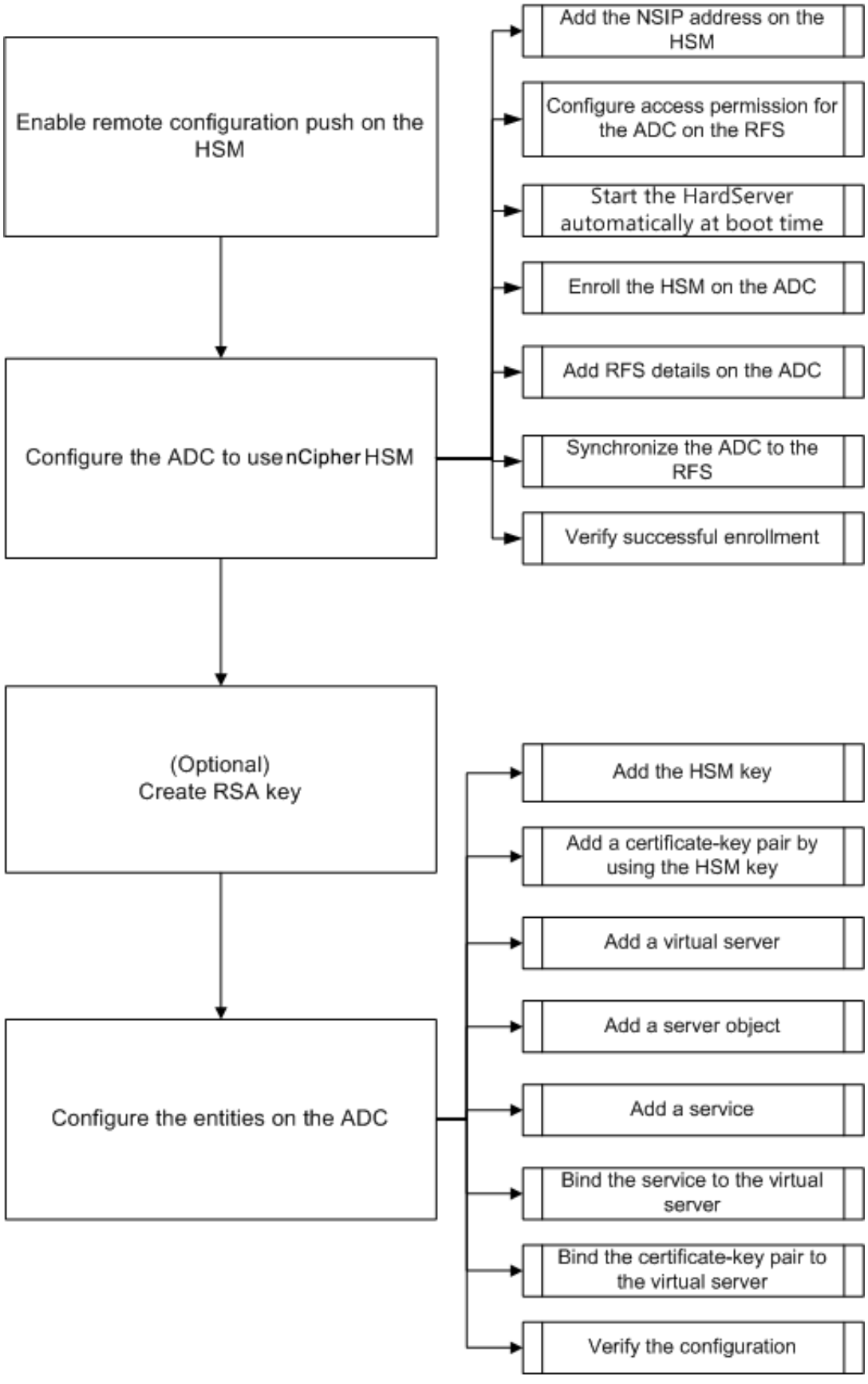
Entrust. También puede encontrar la guía en el CD suministrado con el módulo HSM de Entrust en CipherTools-Linux-DEV-XX.xx.xx/document/NSHIELD_Connect_QUICK_START_GUIDE.pdf.
Nota: `Softcard` las claves protegidas por Token/OCS no se admiten actualmente en Citrix ADC.

- Las licencias están disponibles para admitir el número de clientes que están conectados al HSM de Entrust. El ADC y el servidor de archivos remoto (RFS) son clientes del HSM.
- Se instala un RFS en la red y es accesible para Citrix ADC.
- El dispositivo Entrust nShield Connect, el RFS y el Citrix ADC pueden iniciar conexiones entre sí a través del puerto 9004.
- Está mediante NetScaler versión 10.5 build 52.1115.e o posterior.
- El dispositivo Citrix ADC no contiene una tarjeta FIPS Cavium.
  Importante: Entrust HSM no es compatible con los dispositivos FIPS MPX 9700/10500/12500/15500.

Configuración de la integración de ADC-Entrust

August 20, 2021

El siguiente diagrama de flujo muestra las tareas que debe realizar para utilizar Entrust HSM con Citrix ADC:



Como se muestra en el diagrama de flujo anterior, realice las siguientes tareas:

1. Habilite la inserción de configuración remota, en el HSM.
2. Configure el ADC para utilizar el HSM de Entrust.
    - Agregue la dirección NSIP en el HSM.
    - Configure el permiso de acceso para el ADC en el RFS.
    - Configure el inicio automático del `Hardserver` en el momento del arranque.
    - Inscriba el HSM en el ADC.
    - Agregue detalles de RFS en el ADC.
    - Sincronice el ADC con el RFS.
    - Compruebe que Entrust HSM se haya inscrito correctamente en el ADC.
3. (Opcional) Cree una clave HSM RSA.
4. Configure las entidades en Citrix ADC.
    - Agregue la clave HSM.
    - Agregue un par de claves de certificado mediante la clave HSM.
    - Agregue un servidor virtual.
    - Agregue un objeto de servidor.
    - Agregar un servicio.
    - Enlazar el servicio al servidor virtual.
    - Enlazar el par de claves de certificado al servidor virtual.
    - Verifique la configuración.

Configurar el HSM de Entrust

Especifique la dirección IP del RFS en el HSM de Entrust para que acepte la configuración que el RFS le envía. Utilice el panel frontal nShield Connect del HSM de Entrust para realizar el siguiente procedimiento.

Especificar la dirección IP de un equipo remoto en el HSM de Entrust

1. Vaya a **Configuración del sistema > Opciones de archivo de configuración > Permitir inserción automática**.
2. Seleccione **ON** y especifique la dirección IP del equipo (RFS) desde la que se aceptará la configuración.

Habilitar la inserción de la configuración remota en el HSM

Especifique la dirección IP del RFS en el HSM de Entrust para que acepte la configuración que el RFS le envía. Utilice el panel frontal nShield Connect del HSM de Entrust para realizar el siguiente procedimiento.

Especificar la dirección IP de un equipo remoto en el HSM de Entrust

1. Vaya a **Configuración del sistema > Opciones de archivo de configuración > Permitir inserción automática**.
2. Seleccione **ON** y especifique la dirección IP del equipo (RFS) desde la que se aceptará la configuración.

Configurar el ADC para utilizar el HSM de Entrust

Valores de ejemplo utilizados en esta documentación:

Dirección NSIP = 10.217.2.43

Dirección IP HSM de Entrust=10.217.2.112

Dirección IP RFS=10.217.2.6

Agregue la dirección NSIP en el HSM

Normalmente se utiliza el panel frontal de NShield Connect para agregar clientes al HSM. Para obtener más información, consulte la Guía de inicio rápido de nShield Connect.

Alternativamente, utilice el RFS para agregar el ADC como cliente al HSM. Para agregar el ADC, debe agregar la dirección NSIP en la configuración de HSM en el RFS y, a continuación, insertar la configuración en el HSM. Antes de poder presionar la configuración, debe conocer el número de serie electrónico (ESN) del HSM.

Para obtener el ESN de su HSM, ejecute el siguiente comando en el RFS:

```
root@ns# /opt/nfast/bin/anonkneti <Entrust HSM IP address>
<!--NeedCopy-->
```

Ejemplo:

```
root@ns# /opt/nfast/bin/anonkneti 10.217.2.112
BD17-C807-58D9 5e30a698f7bab3b2068ca90a9488dc4e6c78d822
<!--NeedCopy-->
```

El número ESN es BD17-C807-58D9.

Después de tener el número ESN, utilice un editor, como vi, para modificar el archivo de configuración HSM en el RFS.


```
vi /opt/nfast/kmdata/hsm-BD17-C807-58D9/config/config
<!--NeedCopy-->
```

En la `hs_clients` sección, agregue las siguientes entradas:

```
# Amount of data in bytes to encrypt with a session key before session
   key# renegotiation, or 0 for unlimitied. (default=1024\*1024\*8b=8Mb
   ).
#  datalimit=INT
addr=10.217.2.43
clientperm=unpriv
keyhash=0000000000000000000000000000000000000000
esn=
timelimit=86400
datalimit=8388608
-----
<!--NeedCopy-->
```

Nota: Incluya uno o más guiones como delimitadores para agregar varias entradas en la misma sección.

Para insertar la configuración en el HSM, ejecute el siguiente comando en el RFS:

```
/opt/nfast/bin/cfg-pushnethsm --address=<Entrust HSM IP address> --
   force /opt/nfast/kmdata/hsm-BD17-C807-58D9/config/config
<!--NeedCopy-->
```

Ejemplo:

```
/opt/nfast/bin/cfg-pushnethsm --address=10.217.2.112 --force
                /opt/nfast/kmdata/hsm-BD17-C807-58D9/config/config
<!--NeedCopy-->
```

Configurar el permiso de acceso para el ADC en el RFS

Para configurar el permiso de acceso para el ADC en el RFS, ejecute el siguiente comando en el RFS:


```
/opt/nfast/bin/rfs-setup --force -g --write-noauth <NetScaler IP
   address>
<!--NeedCopy-->
```

Ejemplo:

```
[root@localhost bin]# /opt/nfast/bin/rfs-setup --force -g --write-
   noauth 10.217.2.43
Adding read-only remote_file_system entries
Ensuring the directory /opt/nfast/kmdata/local exists
Adding new writable remote_file_system entries
Ensuring the directory /opt/nfast/kmdata/local/sync-store exists
Saving the new config file and configuring the hardserver
Done
<!--NeedCopy-->
```

Compruebe que el ADC puede llegar al HSM RFS y Entrust mediante el puerto 9004.

Configurar el `hardserver` inicio automático del

Cree un archivo y, a continuación, reinicie el dispositivo. Ahora, cada vez que reinicie el dispositivo y, si se encuentra este archivo, `Hardserver` se inicia automáticamente.

En el símbolo del shell, escriba:

```
touch /var/opt/nfast/bin/thales_hsm_is_enrolled
<!--NeedCopy-->
```

En el símbolo del sistema, escriba:

```
reboot
<!--NeedCopy-->
```

Inscribir el HSM en el ADC

Cambie el directorio a /var/opt/nfast/bin.

Para agregar detalles de HSM a la configuración de ADC, ejecute el siguiente comando en el ADC:

`nethsmenroll --force <Thales_nShield_Connect_ip_address> $(anonkneti <Thales_nShield_Connect_ip_address>)`

Ejemplo:

```
root@ns# ./nethsmenroll --force 10.217.2.112 $(anonkneti 10.217.2.112)
OK configuring hardserver's nethsm imports
<!--NeedCopy-->
```

Este paso agrega las siguientes entradas después de la línea # ntoken_esn=esn en la `nethsm_imports` sección del archivo /var/opt/nfast/kmdata/config/config.

```
...
local_module=0
remote_ip=10.217.2.112
remote_port=9004
remote_esn=BD17-C807-58D9
keyhash=5e30a698f7bab3b2068ca90a9488dc4e6c78d822
timelimit=86400
datalimit=8388608
privileged=0
privileged_use_high_port=0
ntoken_esn=
<!--NeedCopy-->
```

Cambie el directorio a /var/opt/nfast/bin y ejecute el siguiente comando en el ADC:

```
touch ”thales_hsm_is_enrolled”
<!--NeedCopy-->
```

Nota: Para quitar un HSM inscrito en el ADC, escriba:

```
./nethsmenroll - -remove <NETHSM-IP>
<!--NeedCopy-->
```

Agregar detalles de RFS en el ADC

Para agregar detalles de RFS, cambie el directorio a /var/opt/nfast/bin/ y, a continuación, ejecute el siguiente comando:


```
./rfs-sync --no-authenticate --setup <rfs_ip_address>
<!--NeedCopy-->
```

Ejemplo:

```
./rfs-sync --no-authenticate --setup 10.217.2.6
No current RFS synchronization configuration.
Configuration successfully written; new config details:
Using RFS at 10.217.2.6:9004: not authenticating.
<!--NeedCopy-->
```

Este paso agrega las siguientes entradas después de la línea # local_esn=esn en la `rfs_sync_client` sección del archivo /var/opt/nfast/kmdata/config/config.

```
… …
remote_ip=10.217.2.6
remote_port=9004
use_kneti=no
local_esn=
<!--NeedCopy-->
```

Nota: Para quitar un RFS inscrito en el ADC, escriba:

```
./rfs_sync - remove
<!--NeedCopy-->
```

Sincronizar el ADC con el RFS

Para sincronizar todos los archivos, cambie el directorio a /var/opt/nfast/bin y, a continuación, ejecute el siguiente comando en el ADC:

```
./rfs-sync - -update
<!--NeedCopy-->
```

Este comando recupera todos los archivos World, los archivos de módulo y los archivos de clave del directorio /opt/nfast/kmdata/local del RFS y los coloca en el directorio /var/opt/nfast/kmdata/local del

ADC. Citrix recomienda copiar manualmente los archivos World, los archivos Module_xxxx_xxxx_xxxx, donde XXXX_XXXXXX es el ESN del HSM inscrito y solo los archivos de clave RSA y certificado necesarios.

Verificar que el HSM de Entrust se haya inscrito correctamente en el ADC

Después de sincronizar el ADC con el RFS, haga lo siguiente:

- Compruebe que el local `Hardserver` esté activo y en funcionamiento. (Servidor de Entrust en ejecución).
- Obtenga el estado de los HSM configurados y verifique que los valores para el campo n_modules (número de módulos) y los campos de información km sean distintos de cero.
- Compruebe que el HSM está inscrito correctamente y que el ADC puede utilizar (estado 0x2 User).
- Cargar pruebas mediante`sigtest` ejecutar correctamente.

Cambie el directorio a /var/opt/nfast/bin y, en el símbolo del shell, ejecute los siguientes comandos:

```
1 root@ns# ./chkserv root@ns# ./nfkminfo root@ns# ./sigtest
2 <!--NeedCopy-->
```

Consulte el apéndice para ver un ejemplo.

Crear una clave RSA HSM

Solo se admiten claves RSA como claves HSM.

Nota: Omita este paso si las claves ya están presentes en la `/opt/nfast/kmdata/local` carpeta del RFS.

Cree una clave RSA, un certificado autofirmado y una solicitud de firma de certificados (CSR). Enviar la CSR a una entidad emisora de certificados para obtener un certificado de servidor.

En el ejemplo siguiente se crean los siguientes archivos:

- Insertar clave RSA: Key_embed_2ed5428aae1e159bdbd63f25292c7113ec2c78
- Certificado autofirmado: Example_selfcert
- Solicitud de firma de certificado: Example_req

Nota: El `generatekey` comando es compatible con el estricto mundo de seguridad FIPS 140-2 Nivel 3. Se necesita un conjunto de tarjetas de administrador (ACS) o un conjunto de tarjetas de operador (OCS) para controlar muchas operaciones, incluida la creación de claves y OCSs. Al ejecutar

el `generatekey` comando, se le pedirá que inserte una tarjeta ACS o OCS. Para obtener más información acerca del estricto mundo de seguridad FIPS 140-2 Level 3, consulte la Guía del usuario de nShield Connect.

En el ejemplo siguiente se utiliza Nivel 2 Security World. En el ejemplo, los comandos están en negrita.

Ejemplo:

```
[root@localhost bin]# ./generatekey embed
size: Key size? (bits, minimum 1024) [1024] > 2048
OPTIONAL: pubexp: Public exponent for RSA key (hex)? []
>
embedsavefile: Filename to write key to? []
> example
plainname: Key name? [] > example
x509country: Country code? [] > US
x509province: State or province? [] > CA
x509locality: City or locality? [] > Santa Clara
x509org: Organisation? [] > Citrix
x509orgunit: Organisation unit? [] > NS
x509dnscommon: Domain name? [] > www.citrix.com
x509email: Email address? [] > example@citrix.com
nvram: Blob in NVRAM (needs ACS)? (yes/no) [no] >
digest: Digest to sign cert req with? (md5, sha1, sha256, sha384,
   sha512)
  [default sha1] > sha512
key generation parameters:
 operation      Operation to perform              generate
 application    Application                       embed
 verify         Verify security of key            yes
 type           Key type                          RSA
 size           Key size                          2048
 pubexp         Public exponent for RSA key (hex)
 embedsavefile  Filename to write key to          example
 plainname      Key name                          example
 x509country    Country code                      US
 x509province   State or province                 CA
 x509locality   City or locality                  Santa Clara
 x509org        Organisation                      Citrix
 x509orgunit    Organisation unit                 NS
 x509dnscommon  Domain name                       www.citrix.com
 x509email      Email address                     example@citrix.com
 nvram          Blob in NVRAM (needs ACS)         no
 digest         Digest to sign cert req with      sha512
```



```
Key successfully generated.
Path to key: /opt/nfast/kmdata/local/
   key_embed_2ed5428aaeae1e159bdbd63f25292c7113ec2c78
You have new mail in /var/spool/mail/root
<!--NeedCopy-->
```

Resultado:

Ha creado un CSR (example_req), un certificado autofirmado (example_selfcert) y un archivo de token de clave de aplicación en formato embed (/opt/nfast/kmdata/local/key_embed_2ed5428aae1e159bdbd63f25292c

Dado que el ADC solo admite claves en formato simple, debe convertir la clave incrustada en una clave simple.

Para convertir la clave embed en una clave simple, ejecute el siguiente comando en el RFS:

```
[root@localhost bin]# ./generatekey -r simple
from-application: Source application? (embed, simple) [embed] > embed
from-ident: Source key identifier? (
   c6410ca00af7e394157518cb53b2db46ff18ce29,
                                    2
                                       ed5428aaeae1e159bdbd63f25292c7113ec2c78
                                       )
  [default c6410ca00af7e394157518cb53b2db46ff18ce29]
> 2ed5428aaeae1e159bdbd63f25292c7113ec2c78
ident: Key identifier? [] > examplersa2048key
plainname: Key name? [] > examplersa2048key
key generation parameters:
 operation         Operation to perform    retarget
 application       Application             simple
 verify            Verify security of key  yes
 from-application  Source application      embed
 from-ident        Source key identifier   2
    ed5428aaeae1e159bdbd63f25292c7113ec2c78
 ident             Key identifier          examplersa2048key
 plainname         Key name                examplersa2048key
Key successfully retargetted.
Path to key: /opt/nfast/kmdata/local/key_simple_examplersa2048key
<!--NeedCopy-->
```

> **Importante:**
>
> Cuando se le solicite el identificador de clave de origen, escriba **2ed5428aae1e159bdbd63f25292c7113ec2c78** como clave embed.

Resultado:

Se crea una clave con el prefijo key_simple (por ejemplo key_simple_examplersa2048key).

Nota: examplersa2048key es el identificador de clave (ident) y se conoce como el nombre de clave HSM en el ADC. Un identificador de clave es único. Todos los archivos simples tienen el prefijo key_simple.

Configurar las entidades en el ADC

Antes de que ADC pueda procesar el tráfico, debe hacer lo siguiente:

1. Habilitar funciones.
2. Agregue una dirección IP de subred (SNIP).
3. Agregue la clave HSM al ADC.
4. Agregue un par de claves de certificado mediante la clave HSM.
5. Agregue un servidor virtual.
6. Agregue un objeto de servidor.
7. Agregar un servicio.
8. Enlazar el servicio al servidor virtual.
9. Enlazar el par de claves de certificado al servidor virtual.
10. Verifique la configuración.

Habilitar funciones en el ADC

Las licencias deben estar presentes en el ADC para poder habilitar una función.

Habilitar una función mediante la CLI

En el símbolo del sistema, ejecute los siguientes comandos:

```
enable feature lb
enable feature ssl
<!--NeedCopy-->
```

Habilitar una función mediante la interfaz gráfica de usuario

Vaya a **Sistema** > **Configuración** y, en el grupo **Modos y funciones**, seleccione **Configurar funciones básicas** y, a continuación, seleccione **Descarga SSL**.

Agregar una dirección IP de subred

Para obtener más información sobre las direcciones IP de subred, consulte Configuración de direcciones IP de subred.

Agregue una dirección SNIP y verifique la configuración mediante la CLI

En el símbolo del sistema, ejecute los siguientes comandos:

```
add ns ip <IPAddress> <netmask> -type SNIP
show ns ip
<!--NeedCopy-->
```

Ejemplo:

```
add ns ip 192.168.17.253 255.255.248.0 -type SNIP
Done
show ns ip
        Ipaddress        Traffic Domain  Type             Mode     Arp
                 Icmp     Vserver  State
        ---------        --------------  ----             ----     ---
                 ----     -------  ------
1)      192.168.17.251   0               NetScaler IP     Active
   Enabled  Enabled  NA       Enabled
2)      192.168.17.252   0               VIP              Active
   Enabled  Enabled  Enabled  Enabled
3)      192.168.17.253   0               SNIP              Active
   Enabled  Enabled  NA       Enabled
 Done
<!--NeedCopy-->
```

Agregue una dirección SNIP y verifique la configuración mediante la interfaz gráfica de usuario

Vaya a **Sistema > Red > IP,**agregue una dirección IP y seleccione **Tipo de IP como IP de subred**.

Copie la clave HSM y el certificado en el ADC

Utilice una utilidad de transferencia segura de archivos para copiar de forma segura la clave (key_simple_examplersa2048key) en la `/var/opt/nfast/kmdata/local` carpeta y el certificado (example_selfcert) en la `/nsconfig/ssl` carpeta del ADC.

Agregar la clave en el ADC

Todas las teclas tienen un prefijo clave simple. Al agregar la clave al ADC, utilice el ident como nombre de clave HSM. Por ejemplo, si la clave que agregó es KEY_Simple_XXXX, el nombre de clave HSM es XXXX.

Importante:

- El nombre de clave HSM debe ser el mismo que el identificador que especificó al convertir una clave incrustada a un formato de clave simple.
- Las claves deben estar presentes en el `/var/opt/nfast/kmdata/local/` directorio del ADC.

Agregar una clave HSM mediante la CLI

En el símbolo del shell, ejecute el siguiente comando:

```
add ssl hsmKey <hsmKeyName> -key <string>
<!--NeedCopy-->
```

Ejemplo:

```
add ssl hsmKey examplersa2048key  - key key_simple_examplersa2048key
Done
<!--NeedCopy-->
```

Agregar una clave HSM mediante la interfaz gráfica de usuario

Vaya a **Administración del tráfico > SSL > HSM**y agregue una clave HSM.

Agregar un par de claves de certificado en el ADC

Para obtener información sobre los pares de claves de certificado, consulte Agregar o actualizar un par de claves de certificado.

Agregar un par de claves de certificado mediante la CLI

En el símbolo del sistema, ejecute el siguiente comando:

```
add ssl certKey <certkeyName> -cert <string> -hsmKey <string>
<!--NeedCopy-->
```


Ejemplo:

```
add ssl certKey key22 -cert example_selfcert -hsmKey examplersa2048key
Done
<!--NeedCopy-->
```

Agregue un par de claves de certificado mediante la interfaz gráfica de usuario

Vaya a **Traffic Management > SSL > Certificados** y agregue un par de claves de certificado.

Agregar un servidor virtual

Para obtener información sobre un servidor virtual, consulte Configuración del servidor virtual SSL.

Configurar un servidor virtual basado en SSL mediante la CLI

En el símbolo del sistema, ejecute el siguiente comando:

```
add lb vserver <name> <serviceType> <IPAddress> <port>
<!--NeedCopy-->
```

Ejemplo:

```
add lb vserver v1 SSL 192.168.17.252 443
<!--NeedCopy-->
```

Configurar un servidor virtual basado en SSL mediante la interfaz gráfica de usuario

Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**, cree un servidor virtual y especifique el protocolo como SSL.

Agregar un objeto de servidor

Antes de agregar un objeto de servidor en el ADC, asegúrese de haber creado un servidor back-end. En el siguiente ejemplo se utiliza el módulo integrado Python HTTP Server en un sistema Linux.

Ejemplo:


```
%python  -m SimpleHTTPServer 80
<!--NeedCopy-->
```

Agregar un objeto de servidor mediante la CLI

En el símbolo del sistema, ejecute el siguiente comando:

```
add server <name> <IPAddress>
<!--NeedCopy-->
```

Ejemplo:

```
add server s1 192.168.17.246
<!--NeedCopy-->
```

Agregar un objeto de servidor mediante la interfaz gráfica de usuario

Vaya a **Administración de tráfico > Equilibrio de carga > Servidores** y agregue un servidor.

Agregar un servicio

Para obtener más información, consulte Configuración de servicios.

Configurar un servicio mediante la CLI

En el símbolo del sistema, ejecute el siguiente comando:

```
add service <name> <serverName> <serviceType> <port>
<!--NeedCopy-->
```

Ejemplo:

```
add service sr1 s1 HTTP 80
<!--NeedCopy-->
```


Configurar un servicio mediante la interfaz gráfica de usuario

Vaya a **Administración del tráfico > Equilibrio de carga > Servicios**y cree un servicio.

Vincular el servicio al servidor virtual

Para obtener más información, consulte Vincular servicios al servidor virtual SSL.

Enlazar un servicio a un servidor virtual mediante la CLI

En el símbolo del sistema, ejecute el siguiente comando:

```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Ejemplo:

```
bind lb vserver v1 sr1
<!--NeedCopy-->
```

Enlazar un servicio a un servidor virtual mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. Abra un servidor virtual y haga clic en el panel Servicios para enlazar un servicio al servidor virtual.

Enlazar el par de claves de certificado al servidor virtual en el ADC

Para obtener más información, consulte Vincular el par de claves de certificado al servidor virtual SSL.

Enlazar un par de claves de certificado a un servidor virtual mediante la CLI

En el símbolo del sistema, ejecute el siguiente comando:

```
bind ssl vserver <vServerName> -certkeyName <string>
<!--NeedCopy-->
```

Ejemplo:


```
bind ssl vserver v1 -certkeyName key22
Warning: Current certificate replaces the previous binding
<!--NeedCopy-->
```

Enlazar un par de claves de certificado a un servidor virtual mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. Abra un servidor virtual SSL y, en **Configuración avanzada**, haga clic en **Certificado SSL**.
3. Enlazar un certificado de servidor al servidor virtual.

Verificar la configuración

Para ver la configuración mediante la CLI:

En el símbolo del sistema, ejecute los siguientes comandos:

```
show lb vserver <name>
show ssl vserver <vServerName>
<!--NeedCopy-->
```

Ejemplo:

```
show lb vserver v1
        v1 (192.168.17.252:443) - SSL   Type: ADDRESS
        State: UP
        Last state change was at Wed Oct 29 03:11:11 2014
        Time since last state change: 0 days, 00:01:25.220
        Effective State: UP
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Appflow logging: ENABLED
        No. of Bound Services :  1 (Total)       1 (Active)
        Configured Method: LEASTCONNECTION
        Current Method: Round Robin, Reason: Bound service's state
           changed to UP
        Mode: IP
        Persistence: NONE
        Vserver IP and Port insertion: OFF
```



```
        Push: DISABLED  Push VServer:
        Push Multi Clients: NO
        Push Label Rule: none
        L2Conn: OFF
        Skip Persistency: None
        IcmpResponse: PASSIVE
        RHIstate: PASSIVE
        New Service Startup Request Rate: 0 PER_SECOND, Increment
           Interval: 0
        Mac mode Retain Vlan: DISABLED
        DBS_LB: DISABLED
        Process Local: DISABLED
        Traffic Domain: 0

1) sr1 (192.168.17.246: 80) - HTTP State: UP    Weight: 1
Done
<!--NeedCopy-->
```

```
sh ssl vserver v1
        Advanced SSL configuration for VServer v1:
        DH: DISABLED
        Ephemeral RSA: ENABLED          Refresh Count: 0
        Session Reuse: ENABLED          Timeout: 120 seconds
        Cipher Redirect: DISABLED
        SSLv2 Redirect: DISABLED
        ClearText Port: 0
        Client Auth: DISABLED
        SSL Redirect: DISABLED
        Non FIPS Ciphers: DISABLED
        SNI: DISABLED
        SSLv2: DISABLED  SSLv3: DISABLED  TLSv1.0: ENABLED  TLSv1.1:
           DISABLED  TLSv1.2: DISABLED
        Push Encryption Trigger: Always
        Send Close-Notify: YES

        ECC Curve: P_256, P_384, P_224, P_521

1)      CertKey Name: key22       Server Certificate

1)      Cipher Name: DEFAULT
        Description: Predefined Cipher Alias
 Done
<!--NeedCopy-->
```


Para ver la configuración mediante la GUI:

Vaya a **Administración de tráfico > Equilibrio de carga > Servidores virtuales** y haga doble clic en un servidor virtual SSL para abrirlo y ver la configuración.

Limitaciones

August 20, 2021

- SSL versión 3 (SSLv3) no es compatible con un dispositivo MPX, pero sí con un dispositivo virtual VPX. Una instancia VPX aprovisionada en un dispositivo SDX admite SSLv3 solo si no se asigna un chip SSL a la instancia.
- No se admiten los cifrados de exportación.
- No se admite el intercambio de claves del servidor SSL mediante claves HSM.
- Si ha agregado o eliminado claves después de guardar la configuración por última vez, debe guardarla antes de realizar un reinicio en caliente. Si no guarda la configuración, hay una discrepancia de clave entre el ADC y el HSM.
- No puede enlazar una clave HSM a un servidor virtual DTLS.
- No puede enlazar un par de claves de certificado que se crea mediante una clave HSM a un servicio SSL.
- No puede utilizar la GUI para inscribir el ADC como cliente del HSM ni comprobar el estado del HSM desde la utilidad de configuración.
- Desde la versión 11, compilación 62.x, se admite la renegociación de SSL.
- No puede firmar solicitudes de OCSP mediante un par de claves de certificado que se crea mediante una clave HSM.
- No se admite un paquete de certificados con claves HSM.
- No aparece un error si la clave HSM y el certificado no coinciden. Por lo tanto, al agregar un par de claves de certificado, debe asegurarse de que la clave HSM y el certificado coinciden.
- Las particiones de administración y clústeres no son compatibles.

Apéndice

August 20, 2021

Ejemplo:

Nota: En el ejemplo siguiente, los comandos están en negrita.


```
root@ns# ./chkserv
nCipher server running
root@ns# ./nfkminfo
World
 generation  2
 state       0x17a70000 Initialised Usable Recovery PINRecovery !
    ExistingClient RTC NVRAM FTO !AlwaysUseStrongPrimes SEEDebug
 n_modules   1
 hknso       cbec8c0c56c6b5e76b73147ef02d34a661eaa044
 hkm     bbb8d4839da5782be4d092735a7535538834dc91 (type Rijndael)
 hkmwk       1d572201be533ebc89f30fdd8f3fac6ca3395bf0
 hkre        01f21ecf43933ffdd45e74c3883525176c5c439c
 hkra        ac8ec5ee6bce00991bd97adce2091d9739b9b452
 hkmc        cf1b509abaad91995ed202d8f36613fc99433155
 hkp         c20910b2ed1ca62d6a2b0db67052a05f7bbfeb43
 hkrtc       bd811020a7c2f8df435a481c3767a89c2e13bc4f
 hknv        278b8012e48910d518a9ee91cff57233fb0c9093
 hkdsee      12230b0e31e3cec66324c0815f782cfb9249edd5
 hkfto       89dd6250b3d6149bcd15606f4553085e2fd6271a
 hkmnull     0100000000000000000000000000000000000000
 ex.client   none
 k-out-of-n  1/2
 other quora m=1 r=1 p=1 nv=1 rtc=1 dsee=1 fto=1
 createtime  2014-02-28 21:05:32
 nso timeout 10 min
 ciphersuite DLf1024s160mRijndael

Module #1
 generation 2
 state      0x2 Usable
 flags      0x10000 ShareTarget
 n_slots    2
 esn        BD17-C807-58D9
 hkml       70289a6edba00ddc7e3f6d6f5a49edc963e822f2

Module #1 Slot #0 IC 0
 generation    1
 phystype      SmartCard
 slotlistflags 0x2 SupportsAuthentication
 state         0x2 Empty
 flags         0x0
 shareno       0
 shares
 error         OK
```



```
No Cardset

Module #1 Slot #1 IC 0
 generation    1
 phystype      SoftToken
 slotlistflags 0x0
 state         0x2 Empty
 flags         0x0
 shareno       0
 shares
 error         OK
No Cardset

No Pre-Loaded Objects

root@ns# ./sigtest
 Hardware module #1 speed index 5792 recommended minimum queue 19
Found 1 module; using 19 jobs
Making 1024-bit RSAPrivate key on module #1;
  using Mech_RSApPKCS1 and PlainTextType_Bignum.
Generated and exported key from module #1.
Imported keys on module #1
 1,       3059 1223.6, 3059 overall
 2,       8698 2989.76, 4349 overall
 3,      14396 4073.06, 4798.67 overall
 4,      20091 4721.83, 5022.75 overall
 5,      25799 5116.3, 5159.8 overall
 6,      31496 5348.58, 5249.33 overall
 7,      37192 5487.55, 5313.14 overall
 8,      42780 5527.73, 5347.5 overall
 9,      45777 4515.44, 5086.33 overall
 10,      51457 4981.26, 5145.7 overall
 11,      57151 5266.36, 5195.55 overall
 12,      62813 5424.61, 5234.42 overall
 13,      68496 5527.97, 5268.92 overall
 14,      74182 5591.18, 5298.71 overall
 15,      79832 5614.71, 5322.13 overall
 16,      85518 5643.23, 5344.88 overall
 17,      88412 4543.54, 5200.71 overall
 18,      94086 4995.72, 5227 overall
 19,      99778 5274.23, 5251.47 overall
 20,     105469 5440.94, 5273.45 overall
 21,     111133 5530.16, 5292.05 overall
 22,     116838 5600.1, 5310.82 overall
 23,     122522 5633.66, 5327.04 overall
```



```
 24,     128175 5641.4, 5340.62 overall
 25,     131072 4543.64, 5242.88 overall
 26,     136762 5002.18, 5260.08 overall
 27,     142415 5262.51, 5274.63 overall
 28,     148125 5441.51, 5290.18 overall
 29,     153816 5541.3, 5304 overall
 30,     159414 5563.98, 5313.8 overall
<!--NeedCopy-->
```

Compatibilidad con el módulo de seguridad de hardware Thales Luna Network

May 8, 2022

Un dispositivo Citrix ADC que no sea FIPS almacena la clave privada del servidor en el disco duro. En un dispositivo FIPS, la clave se almacena en un módulo criptográfico conocido como módulo de seguridad de hardware (HSM). El almacenamiento de una clave en el HSM la protege de ataques físicos y de software. Además, las claves se cifran con cifrados especiales aprobados por FIPS.

Solo los dispositivos FIPS Citrix ADC MPX/SDX 14000 admiten una tarjeta FIPS. La compatibilidad con FIPS no está disponible en otros dispositivos MPX/SDX ni en los dispositivos Citrix ADC VPX. Para solucionar esta limitación, se admite un HSM de red Thales Luna en todos los dispositivos Citrix ADC MPX, SDX y VPX, excepto los dispositivos FIPS MPX/SDX 14000 y los dispositivos enumerados en Compatibilidad con plataformas basadas en chips SSL Intel Coleto e Intel Lewisburg.

Una red HSM de Thales Luna está diseñada para proteger las claves criptográficas críticas y acelerar las operaciones criptográficas sensibles en una amplia gama de aplicaciones de seguridad.

Tabla de versiones compatibles

Versión de Citrix ADC	Versión del dispositivo de software	Versión de firmware	Versión del cliente
11.1, 12.0, 12.1	5.2.3-1	6.2.1	6.0.0
11.1, 12.0, 12.1	6.2.2-5	6.10.9	6.2.2
13.0	7.2.0-220	7.0.3	7.2.2 (7.2.0-220)
13.1	7.2.0-220	7.0.3	10.3.0

Requisitos previos

August 20, 2021

Antes de poder utilizar un HSM de red Thales Luna con Citrix ADC, asegúrese de que se cumplen los siguientes requisitos previos:

- Un HSM de red Thales Luna está instalado en la red, listo para usar y accesible para Citrix ADC. Es decir, la dirección NSIP o la dirección SNIP se agrega como un cliente autorizado en el HSM.
- Las licencias están disponibles para admitir el número necesario de particiones en el HSM.
- La red HSM de Thales Luna y Citrix ADC pueden iniciar conexiones entre sí a través del puerto 1792.
- Está mediante NetScaler versión 11.1 o posterior.
- El dispositivo Citrix ADC no contiene una tarjeta FIPS Cavium.

> **Importante**
>
> Los HSM de red Thales Luna no son compatibles con los dispositivos FIPS MPX 9700/10500/12500/15500.

Configurar un cliente de Thales Luna en el ADC

June 22, 2022

Después de configurar el HSM de Thales Luna y crear las particiones necesarias, debe crear clientes y asignarlos a particiones. Comience por configurar los clientes de Thales Luna en Citrix ADC y configurar los enlaces de confianza de red (NTLs) entre los clientes de Thales Luna y el HSM de Thales Luna. En el apéndicese proporciona una configuración de ejemplo.

1. Cambie el directorio a /var/safenet e instale el cliente Thales Luna. En el símbolo del shell, escriba:

```
cd /var/safenet
<!--NeedCopy-->
```

Para instalar el cliente Thales Luna, versión 6.0.0, escriba:

```
install_client.sh -v 600
<!--NeedCopy-->
```

Para instalar el cliente Thales Luna, versión 6.2.2, escriba:


```
install_client.sh -v 622
<!--NeedCopy-->
```

Para instalar el cliente Thales Luna, versión 7.2.2, escriba:

```
install_client.sh -v 722
<!--NeedCopy-->
```

2. Configure los NTLs entre el cliente Thales Luna (ADC) y HSM.

   Después de crear el directorio '/var/safenet/', realice las siguientes tareas en el ADC.

   a) Cambie el directorio a '/var/safenet/config/' y ejecute el script 'safenet_config '. En el símbolo del shell, escriba:

```
cd /var/safenet/config

sh safenet_config
<!--NeedCopy-->
```

   Este script copia el archivo "Chrystoki.conf" en el directorio /etc/. También genera un enlace simbólico 'libCryptoki2_64.so' en el directorio '/usr/lib/'.

   b) Cree y transfiera un certificado y una clave entre el ADC y el HSM de Thales Luna.

   Para comunicarse de forma segura, el ADC y el HSM deben intercambiar certificados. Cree un certificado y una clave en el ADC y, a continuación, transfiéralos al HSM. Copie el certificado de HSM en el ADC.

   i) Cambie el directorio a /var/safenet/safenet/lunaclient/bin.

   ii) Crear un certificado en el ADC. En el símbolo del shell, escriba:

```
./vtl createCert -n <ip address of Citrix ADC>
<!--NeedCopy-->
```

   Este comando también agrega la ruta del certificado y la clave al archivo "/etc/Chrystoki.conf".

   iii) Copie este certificado en el HSM. En el símbolo del shell, escriba:


```
scp /var/safenet/safenet/lunaclient/cert/client/<ip address of NS
   >.pem <LunaSA_HSM account>@<IP address of Luna SA>
<!--NeedCopy-->
```

iv) Copie el certificado de HSM en Citrix ADC. En el símbolo del shell, escriba:

```
scp <HSM account>@<HSM IP>:server.pem  /var/safenet/safenet/
   lunaclient/server_<HSM ip>.pem
<!--NeedCopy-->
```

3. Registre Citrix ADC como cliente y asígnele una partición en el HSM de Thales Luna.

   Inicie sesión en el HSM y cree un cliente. Introduzca el NSIP como IP del cliente. Esta dirección debe ser la dirección IP del ADC desde el que transfirió el certificado al HSM. Cuando el cliente se haya registrado correctamente, asígnele una partición. Ejecute los siguientes comandos en el HSM.

   a) Utilice SSH para conectarse al HSM de Thales Luna e introduzca la contraseña.

   b) Registre Citrix ADC en el HSM de Thales Luna. El cliente se crea en el HSM. La dirección IP es la dirección IP del cliente. Es decir, la dirección NSIP.

   En el símbolo del sistema, escriba:

```
client register  -client <client name> -ip <Citrix ADC ip>
<!--NeedCopy-->
```

   c) Asigne al cliente una partición de la lista de particiones. Para ver las particiones disponibles, escriba:

```
<luna_sh> partition list
<!--NeedCopy-->
```

   Asigne una partición de esta lista. Tipo:

```
<lunash:> client assignPartition -client <Client Name> -par <
   Partition Name>
<!--NeedCopy-->
```


4. Registre el HSM con su certificado en el Citrix ADC.

   En el ADC, cambie el directorio a "/var/safenet/safenet/lunaclient/bin" y, en el indicador del shell, escriba:

```
./vtl addserver -n <IP addr of HSM> -c /var/safenet/safenet/
   lunaclient/server_<HSM_IP>.pem
<!--NeedCopy-->
```

   Para eliminar el HSM que está inscrito en el ADC, escriba:

```
./vtl deleteServer -n <HSM IP> -c <cert path>
<!--NeedCopy-->
```

   Para enumerar los servidores HSM configurados en el ADC, escriba:

```
./vtl listServer
<!--NeedCopy-->
```

   > **Nota:**
   >
   > Antes de quitar el HSM mediante el uso `vtl`, asegúrese de que todas las claves de ese HSM se hayan eliminado manualmente del dispositivo. Las claves de HSM no se pueden eliminar después de quitar el servidor de HSM.

5. Verifique la conectividad de los enlaces de confianza de red (NTL) entre el ADC y el HSM. En el símbolo del shell, escriba:

```
./vtl verify
<!--NeedCopy-->
```

   Si la verificación falla, revise todos los pasos. Los errores se deben a una dirección IP incorrecta en los certificados de cliente.

6. Guarde la configuración.

   Los pasos anteriores actualizan el archivo de configuración "/etc/Chrystoki.conf". Este archivo se elimina cuando se inicia el ADC. Copie la configuración en el archivo de configuración predeterminado, que se utiliza cuando se reinicia un ADC.

   En el símbolo del shell, escriba:


```
root@ns# cp /etc/Chrystoki.conf /var/safenet/config/
<!--NeedCopy-->
```

La práctica recomendada es ejecutar este comando cada vez que se produce un cambio en la configuración relacionada con Thales Luna.

7. Inicie el proceso de puerta de enlace de Thales Luna.

   En el símbolo del shell, escriba:

```
sh /var/safenet/gateway/start_safenet_gw
<!--NeedCopy-->
```

8. Configure el inicio automático del daemon de Gateway en el momento del arranque.

   Cree el archivo “safenet_is_enrolled”, que indica que Thales Luna HSM está configurado en este ADC. Cada vez que el ADC se reinicia y se encuentra este archivo, la Gateway se inicia automáticamente.

   En el símbolo del shell, escriba:

```
touch /var/safenet/safenet_is_enrolled
<!--NeedCopy-->
```

9. Reinicie el dispositivo Citrix ADC. En el símbolo del sistema, escriba:

```
reboot
<!--NeedCopy-->
```

Configurar los HSM de Thales Luna en una configuración de alta disponibilidad en el ADC

August 20, 2021

La configuración de los HSM de Thales Luna en una alta disponibilidad (HA) garantiza un servicio ininterrumpido aunque todos, excepto uno de los dispositivos, no estén disponibles. En una configuración de alta disponibilidad, cada HSM se une a un grupo de alta disponibilidad en modo activo-activo. Los HSM de Thales Luna en una configuración de alta disponibilidad proporcionan equilibrio

de carga de todos los miembros del grupo para aumentar el rendimiento y el tiempo de respuesta a la vez que proporcionan la garantía de un servicio de alta disponibilidad. Para obtener más información, póngase en contacto con ventas y soporte técnico de Thales Luna.

Requisitos previos:

- Mínimo dos dispositivos HSM Thales Luna. Todos los dispositivos de un grupo de alta disponibilidad deben tener autenticación PED (ruta de confianza) o autenticación por contraseña. No se admite una combinación de autenticación de ruta de confianza y autenticación de contraseña en un grupo de alta disponibilidad.
- Las particiones de cada dispositivo HSM deben tener la misma contraseña aunque la etiqueta (nombre) sea diferente.
- Todas las particiones en HA deben asignarse al cliente (dispositivo Citrix ADC).

Después de configurar un cliente de Thales Luna en el ADC como se describe en Configurar un cliente de Thales Luna en el ADC, lleve a cabo los siguientes pasos para configurar los HSM de Thales Luna en HA:

1. En el símbolo del shell de Citrix ADC, inicie `lunacm` (/usr/safenet/lunaclient/bin)

   Ejemplo:

```
root@ns# cd /var/safenet/safenet/lunaclient/bin/

root@ns# ./lunacm
<!--NeedCopy-->
```

2. Identifique los ID de ranura de las particiones. Para enumerar las ranuras disponibles (particiones), escriba:

```
lunacm:> slot list
<!--NeedCopy-->
```

   Ejemplo:

```
    Slot Id ->              0
    HSM Label ->            trinity-p1
    HSM Serial Number ->    481681014
    HSM Model ->            LunaSA 6.2.1
    HSM Firmware Version -> 6.10.9
    HSM Configuration ->    Luna SA Slot (PED) Signing With
        Cloning Mode
```



```
7      HSM Status ->           OK
8
9      Slot Id ->              1
10     HSM Label ->            trinity-p2
11     HSM Serial Number ->    481681018
12     HSM Model ->            LunaSA 6.2.1
13     HSM Firmware Version -> 6.10.9
14     HSM Configuration ->    Luna SA Slot (PED) Signing With
          Cloning Mode
15     HSM Status ->           OK
16
17      Slot Id ->              2
18      HSM Label ->            neo-p1
19      HSM Serial Number ->    487298014
20      HSM Model ->            LunaSA 6.2.1
21      HSM Firmware Version -> 6.10.9
22      HSM Configuration ->    Luna SA Slot (PED) Signing With
           Cloning Mode
23     HSM Status ->           OK
24
25     Slot Id ->              3
26     HSM Label ->            neo-p2
27     HSM Serial Number ->    487298018
28     HSM Model ->            LunaSA 6.2.1
29     HSM Firmware Version -> 6.10.9
30     HSM Configuration ->    Luna SA Slot (PED) Signing With
          Cloning Mode
31     HSM Status ->           OK
32
33     Slot Id ->              7
34     HSM Label ->            hsmha
35     HSM Serial Number ->    1481681014
36     HSM Model ->            LunaVirtual
37     HSM Firmware Version -> 6.10.9
38     HSM Configuration ->    Luna Virtual HSM (PED) Signing With
          Cloning Mode
39     HSM Status ->           N/A - HA Group
40
41     Slot Id ->              8
42     HSM Label ->            newha
43     HSM Serial Number ->    1481681018
44     HSM Model ->            LunaVirtual
45     HSM Firmware Version -> 6.10.9
46     HSM Configuration ->    Luna Virtual HSM (PED) Signing With
          Cloning Mode
```



```
47      HSM Status ->            N/A - HA Group
48
49      Current Slot Id: 0
50  <!--NeedCopy-->
```

3. Cree el grupo HA. La primera partición se denomina partición primaria. Puede agregar más de una partición secundaria.

```
1  lunacm:> hagroup createGroup -slot <slot number of primary
       partition> -label <group name> -password <partition password >
2
3  lunacm:> hagroup createGroup -slot 1 -label gp12 -password ******
4  <!--NeedCopy-->
```

4. Agregue los miembros secundarios (particiones HSM). Repita este paso para todas las particiones que se agregarán al grupo HA.

```
1  lunacm:> hagroup addMember -slot <slot number of secondary
       partition to be added> -group <group name> -password <partition
        password>
2  <!--NeedCopy-->
```

Código:

```
1  lunacm:> hagroup addMember -slot 2 -group gp12 -password ******
2  <!--NeedCopy-->
```

5. Habilite el modo solo HA.

```
1  lunacm:> hagroup HAOnly  - enable
2  <!--NeedCopy-->
```

6. Habilitar el modo de recuperación activo.

```
1  lunacm:.>hagroup recoveryMode  - mode active
2  <!--NeedCopy-->
```


7. Establezca el tiempo de intervalo de recuperación automática (en segundos). El valor predeterminado es 60 segundos.

```
lunacm:.>hagroup interval  -interval <value in seconds>
<!--NeedCopy-->
```

Ejemplo:

```
lunacm:.>hagroup interval  -interval 120
<!--NeedCopy-->
```

8. Establecer el recuento de reintentos de recuperación. Un valor de -1 permite un número infinito de reintentos.

```
lunacm:> hagroup retry -count <xxx>
<!--NeedCopy-->
```

Ejemplo:

```
lunacm:> hagroup retry -count 2
<!--NeedCopy-->
```

9. Copie la configuración desde `Chrystoki.conf` en el directorio de configuración de SafeNet.

```
cp /etc/Chrystoki.conf /var/safenet/config/
<!--NeedCopy-->
```

10. Reinicie el dispositivo ADC.

```
reboot
<!--NeedCopy-->
```

Después de configurar Thales Luna HSM en HA, consulte Otra configuración de ADC para obtener más configuración en el ADC.

Otra configuración de ADC

August 20, 2021

1. Generar una clave en el HSM.

   Utilice herramientas de terceros para crear claves en el HSM.

2. Agregue una clave HSM en el ADC.

   Importante. El carácter # no se admite en un nombre de clave. Si el nombre de la clave incluye este carácter, se produce un error en la operación de clave de carga.

   Para agregar una clave HSM de Thales Luna mediante la CLI:

   En el símbolo del sistema, escriba:

   ```
   add ssl hsmkey <KeyName> -hsmType SAFENET -serialNum <serial #> -
       password
   <!--NeedCopy-->
   ```

   donde:

   -KeyName es la clave creada en el HSM mediante herramientas de terceros.

   -SerialNum es el número de serie de la partición en el HSM en el que se generan las claves.

   Nota: Para HSM en una configuración de alta disponibilidad, utilice el número de serie del grupo de alta disponibilidad.

   -password es la contraseña de la partición en la que están presentes las claves.

   Para agregar una clave HSM de Thales Luna mediante la GUI:

   Vaya a **Administración de tráfico** > **SSL** > **HSM** y agregue una clave de HSM. Debe especificar el tipo de HSM como **SAFENET**.

3. Agregue un par de claves de certificado en el ADC. Primero use una herramienta de terceros para generar un certificado asociado a la clave. A continuación, copie el certificado en el directorio /nsconfig/ssl/ del ADC.

   Nota: La clave debe ser una clave HSM.

   Para agregar un par de certkey en el ADC mediante la CLI:

   En el símbolo del sistema, escriba:


```
add ssl certkey <CertkeyName> -cert <cert name> -hsmkey <KeyName>
<!--NeedCopy-->
```

Para agregar un par de certkey en el ADC mediante la GUI:

a) Vaya a **Administración de Tráfico** > **SSL**.
b) En **Introducción**, seleccione **Instalar certificado (HSM)** y cree un par de clave de certificado mediante una clave de HSM.

4. Cree un servidor virtual y vincule el par de claves de certificado a este servidor virtual.

Para obtener información sobre cómo crear un servidor virtual, haga clic en Configuración del servidor virtual SSL.

Para obtener información sobre cómo agregar un par de claves de certificado, haga clic en Agregar o actualizar un par de claves de certificado.

Para obtener información sobre cómo vincular un par de claves de certificado a un servidor virtual SSL, haga clic en Vincular el par de claves de certificado al servidor virtual SSL.

Dispositivos Citrix ADC en una configuración de alta disponibilidad

August 20, 2021

Puede configurar una configuración de alta disponibilidad (HA) en los dispositivos Citrix ADC con una configuración HSM de Thales Luna de cualquiera de las dos formas siguientes:

- En primer lugar, configure un HSM Thales Luna en los dos nodos, mediante el mismo HSM y la misma partición. A continuación, cree un par HA. Por último, agregue la configuración de Citrix ADC, como claves, pares de certificados y servidores virtuales, en el nodo principal.
- Si un HSM de Thales Luna ya está configurado en un nodo con la configuración de Citrix ADC, agregue una configuración similar en el otro nodo. Copie "/var/safenet/sfgw_ident_file" del primer nodo al otro y reinicie el binario safenet_gw. Después de que la Gateway esté activa y en ejecución, agregue los nodos en una configuración de alta disponibilidad.

Limitaciones

October 5, 2021

1. Para cualquier cambio en la configuración relacionada con HSM en una configuración existente, como agregar o quitar un HSM o crear una configuración de alta disponibilidad, copie '/etc/Chrystoki.conf' en '/var/safenet/config'.

2. Después de agregar, quitar o reiniciar un HSM, debe reiniciar el binario '/var/safenet/gateway/safenet_gw'. Si no reinicia el binario de la puerta de enlace, el HSM no servirá ningún tráfico después de que se vuelva a agregar o después de reiniciarse.
3. Para reiniciar o detener el binario '/var/safenet/gateway/safenet_gw' actual, use

```
kill  - SIGTERM <PID>
kill  - SIGINT <PID>
<!--NeedCopy-->
```

¡**Importante**! No usar `kill -9 <PID>` ni `kill -6 <PID>`

4. Antes de quitar un HSM existente del ADC, quite del ADC todas las claves y pares de claves de certificado asociados a ese HSM. No se pueden eliminar estos archivos del ADC después de quitar el HSM.
5. En un dispositivo Citrix ADC independiente, los HSM de Thales Luna en HA son compatibles con Luna versión 6.2 y posteriores.
6. No se admiten los cifrados EXPORT.
7. No se admite la operación de actualización del par de claves de certificado.
8. Al generar una clave HSM en una herramienta de terceros, los nombres de clave privada y pública deben ser los mismos. Al agregar la clave HSM en el dispositivo, indique este nombre como nombre de clave.
9. El carácter ## no se admite en el nombre de clave ni en la contraseña de partición.
10. Las particiones de clúster y administración no son compatibles.

Apéndice

August 20, 2021

Comandos de ejemplo con sus salidas:

Ejecutar el script

```
     root@ns# pwd
    /var/safenet/config
    root@ns# sh safenet_config
<!--NeedCopy-->
```


Crear un certificado

```
1     root@ns# cd /var/safenet/safenet/lunaclient/bin
2     root@ns# ./vtl createcert -n 10.102.59.175
3     Private Key created and written to: /var/safenet/safenet/lunaclient
         /cert/client/10.102.59.175Key.pem
4     Certificate created and written to: /var/safenet/safenet/lunaclient
         /cert/client/10.102.59.175.pem
5  <!--NeedCopy-->
```

Copie el certificado en el HSM

```
1     root@ns# scp /var/safenet/safenet/lunaclient/cert/client
         /10.102.59.175.pem admin@10.217.2.7:
2     admin@10.217.2.7's password:
3
4     10.102.59.175.pem          100%  818     0.8KB/s   00:00
5  <!--NeedCopy-->
```

Copie el certificado y la clave del HSM en el dispositivo Citrix ADC

```
1     root@ns# scp admin@10.217.2.7:server.pem /var/Thales Luna/safenet/
         lunaclient/server.2.7.pem
2     admin@10.217.2.7's password:
3
4     server.pem            100% 1164     1.1KB/s   00:01
5  <!--NeedCopy-->
```

Utilice SSH para conectarse al HSM Thales Luna

```
1     ssh admin@10.217.2.7
2     Connecting to 10.217.2.7:22...
3     Connection established.
4     To escape to local shell, press 'Ctrl+Alt+]'.
5
6     Last login: Thu Jun 23 02:20:29 2016 from 10.252.243.11
7
8     Luna SA 5.2.3-1 Command Line Shell - Copyright (c) 2001-2014
         SafeNet, Inc. All rights reserved.
```



```
9
10      [Safenet1] lunash:>hsm login
11
12
13        Please enter the HSM Administrators' password:
14        > *******
15
16      'hsm login' successful.
17
18
19      Command Result : 0 (Success)
20      [Safenet1] lunash:>
21  <!--NeedCopy-->
```

Registre Citrix ADC en Thales Luna HSM

```
1       [Safenet1] lunash:>client register -client ns175 -ip 10.102.59.175
2
3       'client register' successful.
4
5
6       Command Result : 0 (Success)
7       [Safenet1] lunash:>
8   <!--NeedCopy-->
```

Asignar al cliente una partición de la lista de particiones

```
1       [Safenet1] lunash:>client assignPartition -client ns175 -partition
           p2
2
3       'client assignPartition' successful.
4
5
6       Command Result : 0 (Success)
7       [Safenet1] lunash:>
8   <!--NeedCopy-->
```

Registre el HSM con su certificado en el Citrix ADC


```
    root@ns# ./vtl addserver -n 10.217.2.7 -c /var/safenet/safenet/
       lunaclient/server.2.7.pem

    New server 10.217.2.7 successfully added to server list.
<!--NeedCopy-->
```

Comprobar la conectividad de enlaces de confianza de red (NTL) entre el ADC y HSM

```
    root@ns# ./vtl verify

    The following Luna SA Slots/Partitions were found:

    Slot        Serial #                  Label
    ====      ================          =====
       0              477877010          p2
<!--NeedCopy-->
```

Guardar la configuración

```
    root@ns# cp /etc/Chrystoki.conf /var/safenet/config/
<!--NeedCopy-->
```

Configurar el inicio automático del demonio de Gateway en el momento del arranque

```
    touch /var/safenet/safenet_is_enrolled
<!--NeedCopy-->
```

Preguntas frecuentes

August 20, 2021

- **¿Cómo compruebo que el proceso de Thales Luna se esté ejecutando?**

  En el símbolo del shell de Citrix ADC, escriba:


```
ps  - aux | grep safenet_gw
<!--NeedCopy-->
```

- **¿ Cómo verifico la conectividad de enlaces de confianza de red (NTL) entre el ADC y HSM?**

  Después de configurar Thales Luna, cambie el directorio a “/var/safenet/safenet/lunaclient/bin” y escriba:

```
./vtl verify
<!--NeedCopy-->
```

Compatibilidad con Azure Key Vault

December 2, 2021

El dispositivo Citrix ADC se integra con HSM externos (SafeNet y Thales) para implementaciones locales. Para implementaciones en la nube, el dispositivo ADC se integra con Azure Key Vault. El dispositivo almacena sus claves privadas en Key Vault para facilitar la administración y la seguridad de la clave privada en el dominio de la nube pública. Ya no tiene que almacenar y administrar claves en diferentes ubicaciones para los dispositivos ADC implementados en varios centros de datos y proveedores de nube.

El uso de ADC con el nivel de precios de Azure Key Vault Premium, que proporcionó claves admitidas por HSM, proporciona cumplimiento FIPS 140-2 de nivel 2.

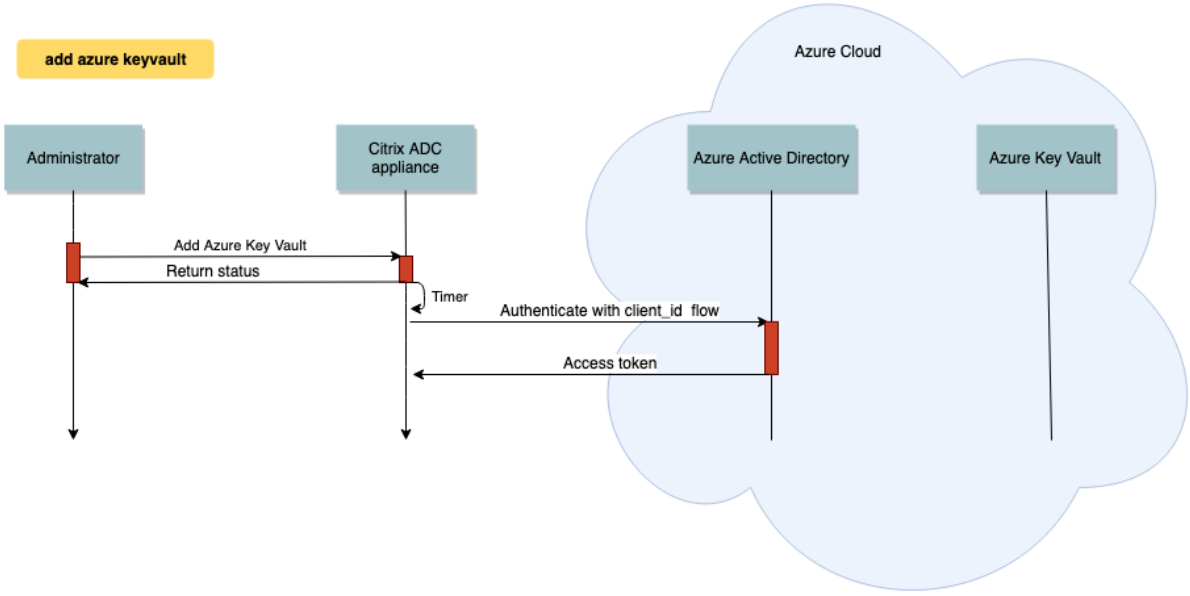
Azure Key Vault es una oferta estándar de Microsoft. Para obtener más información sobre Azure Key Vault, consulte la documentación de Microsoft Azure.

> **Nota:**
>
> La integración de Citrix ADC con Azure Key Vault se admite con el protocolo TLS 1.3.

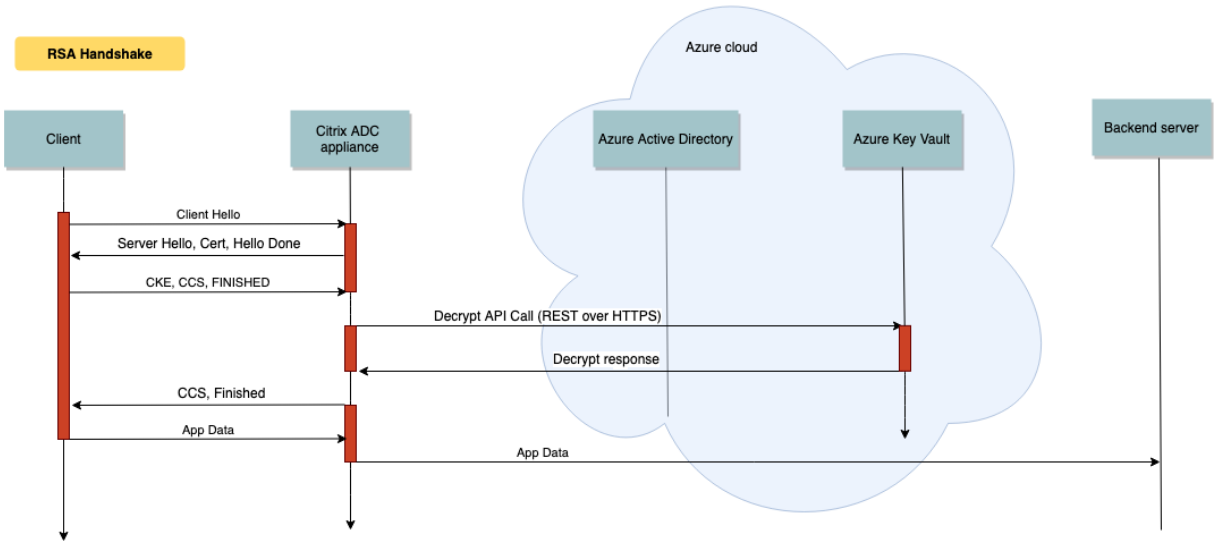
Descripción de la arquitectura

Azure Key Vault es un servicio para almacenar secretos de forma segura en la nube de Azure. Al guardar las llaves en Azure Key Vault, reduce las posibilidades de que se roben las llaves. Una vez que la bóveda de llaves esté configurada, podrás guardar las llaves en ella. Configure los servidores virtuales en el dispositivo ADC para realizar operaciones de clave privada en Key Vault. El dispositivo ADC accede a la clave de cada apretón de manos SSL.

El siguiente diagrama ilustra el proceso para obtener un token de acceso de Azure Active Directory después de la autenticación. Este token se usa con llamadas a la API REST para operaciones de cifrado mediante claves privadas.



El siguiente diagrama muestra un apretón de manos típico de RSA. El mensaje de intercambio de claves de cliente (CKE) que se cifra con la clave pública se descifra mediante la clave privada almacenada en Key Vault.



En un apretón de manos ECDHE, el mensaje de intercambio de claves de servidor (SKE) enviado por el dispositivo Citrix ADC se firma con la clave privada almacenada en Key Vault.

Requisitos previos

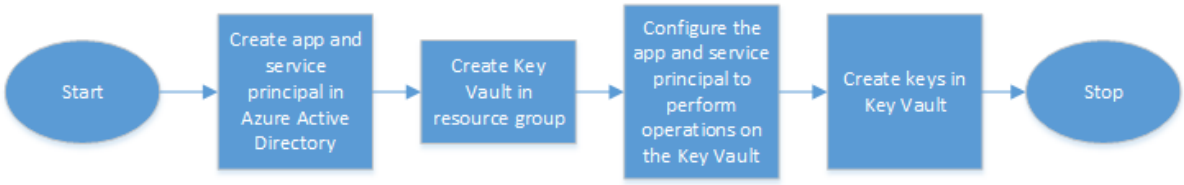
1. Debe tener una suscripción a Azure.
2. (Opcional) Instale la CLI de Azure en una máquina Linux. Para obtener instrucciones, consulte la documentación de Azure https://docs.microsoft.com/en-us/cli/azure/install-azure-cli-apt?view=azure-cli-latest.
3. Complete la configuración en el portal de Azure antes de configurar las entidades en el dispositivo ADC.

Configurar la integración de ADC Azure Key Vault

Primero realice la configuración en el portal de Azure, seguida de la configuración en el dispositivo ADC.

Realice los siguientes pasos en el portal de Azure

El siguiente diagrama de flujo muestra el flujo de alto nivel para la configuración requerida en el portal de Azure.

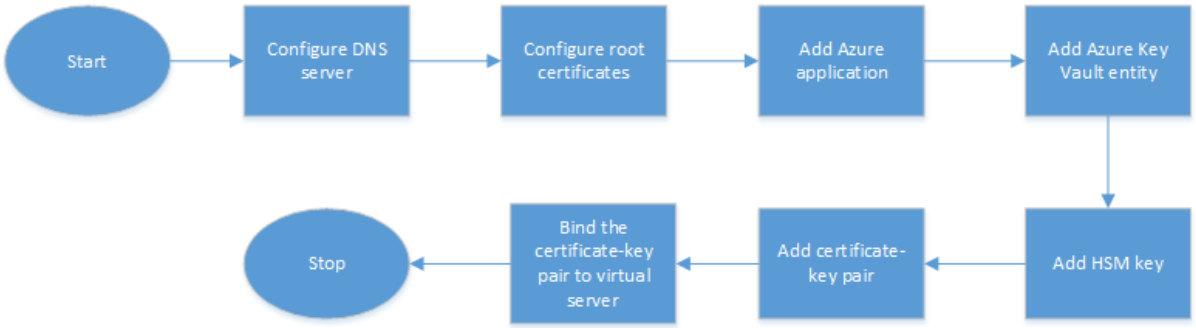


1. Cree una entidad de aplicación y servicio en Azure Active Directory.
2. Cree Key Vault en un grupo de recursos.
3. Configure la entidad principal de la aplicación y el servicio para que realice operaciones de firma y descifrado en Key Vault.
4. Cree llaves en el depósito de llaves de una de las siguientes maneras:
    a) Al importar un archivo de clave.
    b) Generando un certificado.

Para obtener información sobre los comandos para configurar los pasos anteriores, consulte la documentación de Azure en https://docs.microsoft.com/en-us/azure/active-directory/develop/app-objects-and-service-principals.

Realice los siguientes pasos en el dispositivo ADC

El siguiente diagrama de flujo muestra el flujo de alto nivel para la configuración requerida en el dispositivo ADC.



1. Configure un servidor DNS.
2. Configure los certificados raíz para verificar los certificados presentados por Azure.
3. Cree una aplicación de Azure.
4. Cree una entidad de Azure Key Vault.
5. Cree una clave HSM.
6. Cree un par de claves de certificado.
7. Enlace el par de claves de certificado a un servidor virtual.

Configurar un servidor DNS

Se requiere un servidor DNS para la resolución de nombres del host de Key Vault y el punto de conexión de Azure Active Directory.

Para configurar un servidor DNS mediante la CLI

En el símbolo del sistema, escriba:

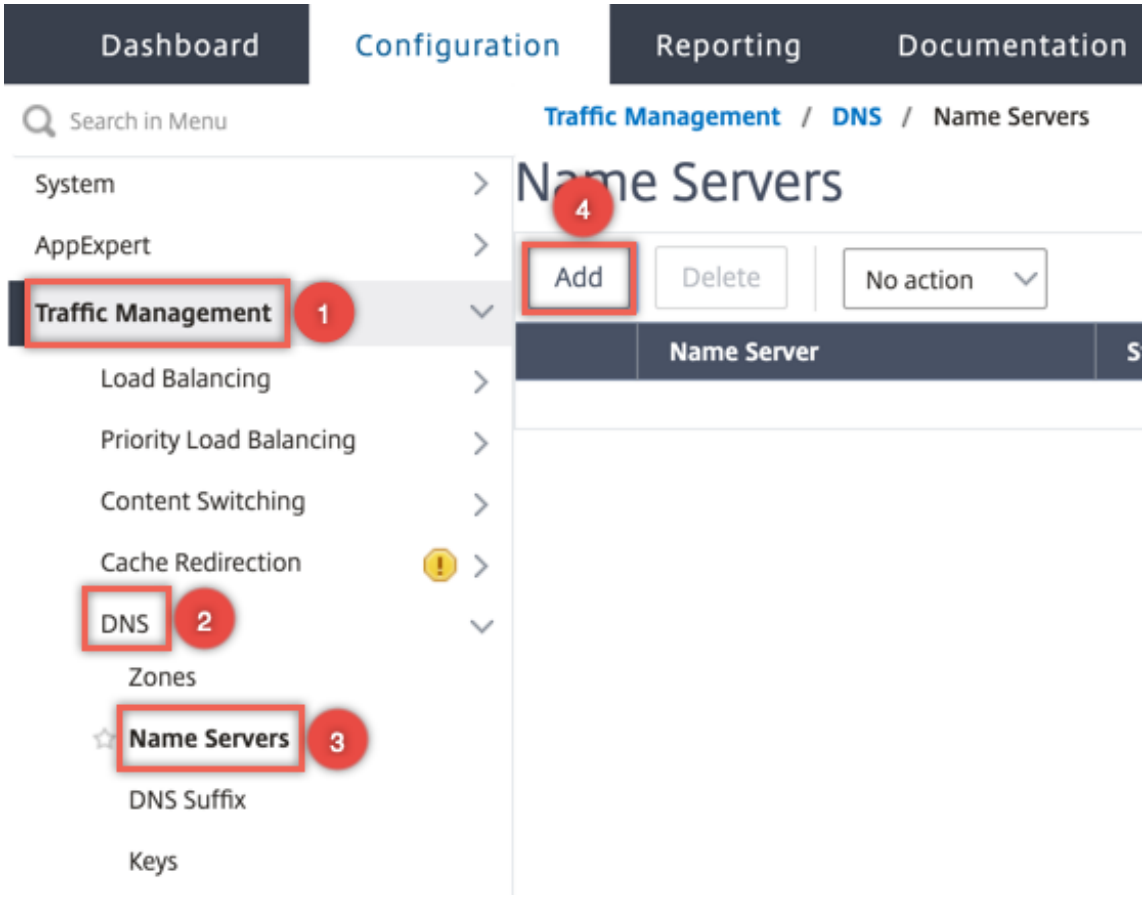
```
add dns nameserver <IP address>
<!--NeedCopy-->
```

Ejemplo:

```
add dns nameserver 192.0.2.150
<!--NeedCopy-->
```

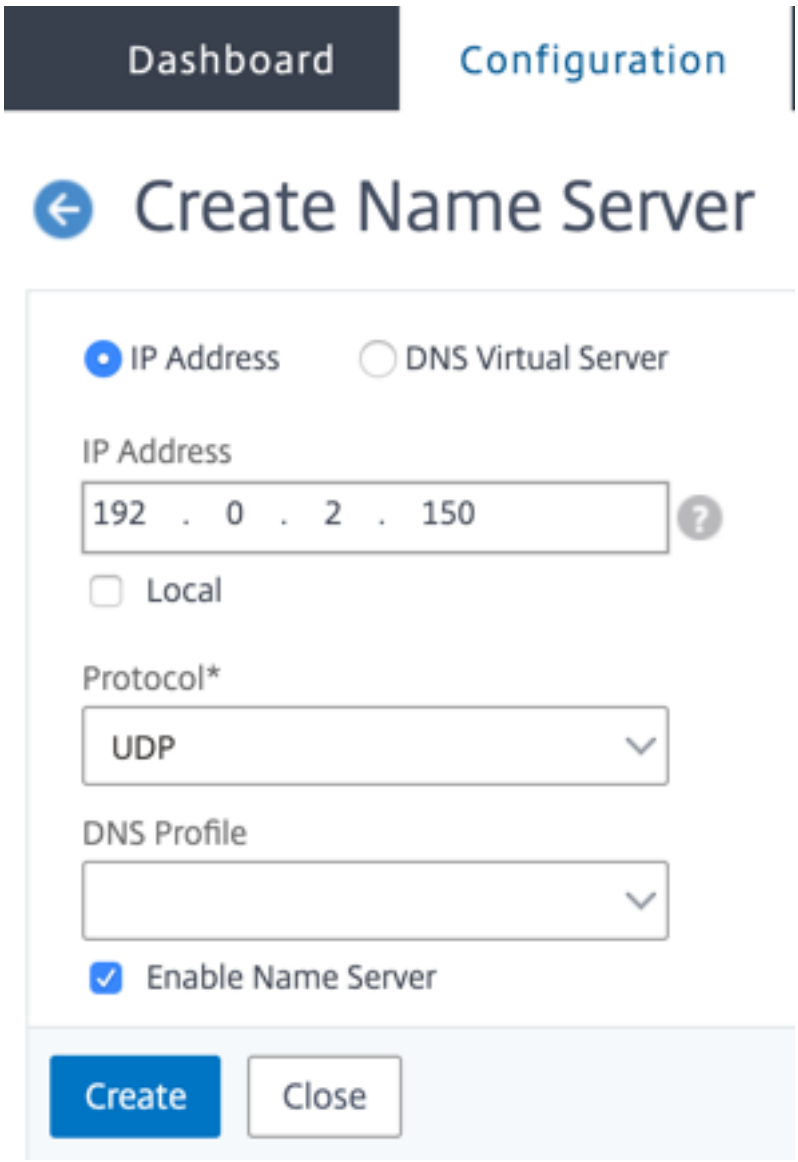
Para configurar un servidor DNS mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > DNS > Servidores de nombres**. Haga clic en **Agregar**.



2. Introduzca valores para los siguientes parámetros:

   - Dirección IP: dirección IP de un servidor de nombres externo o, si se establece el parámetro Local, dirección IP de un servidor DNS local (LDNS).
   - Protocolo: protocolo utilizado por el servidor de nombres. UDP_TCP no es válido si el servidor de nombres es un servidor virtual DNS configurado en el dispositivo.



3. Haga clic en **Crear**.

Agregar y vincular un certificado raíz

Descargue los certificados raíz del certificado presentado por Azure Key Vault `https://<vault_name>.vault.azure.net` y Azure Active Directory (AAD) https://login.microsoftonline.com y cárguelo en el dispositivo ADC. Estos certificados son necesarios para validar el certificado presentado por Azure Key Vault y AAD. Enlace uno o más certificados al grupo de certificados de CA `ns_callout_certs`.

Para agregar un certificado raíz mediante la CLI

En el símbolo del sistema, escriba:

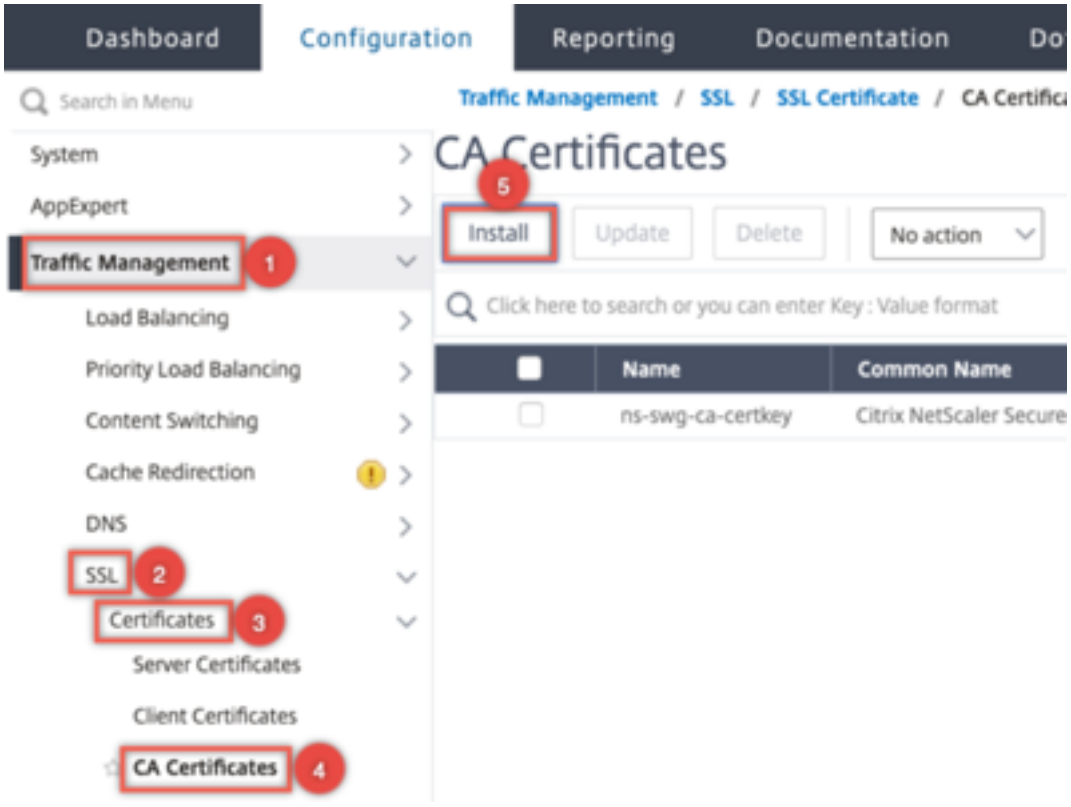

```
add ssl certkey <certkeyname> -cert <certname>
bind ssl caCertGroup <caCertGroupName> <certkeyName>
<!--NeedCopy-->
```

Ejemplo:
En el siguiente ejemplo, el certificado raíz presentado por Azure Key Vault y AAD es el mismo.

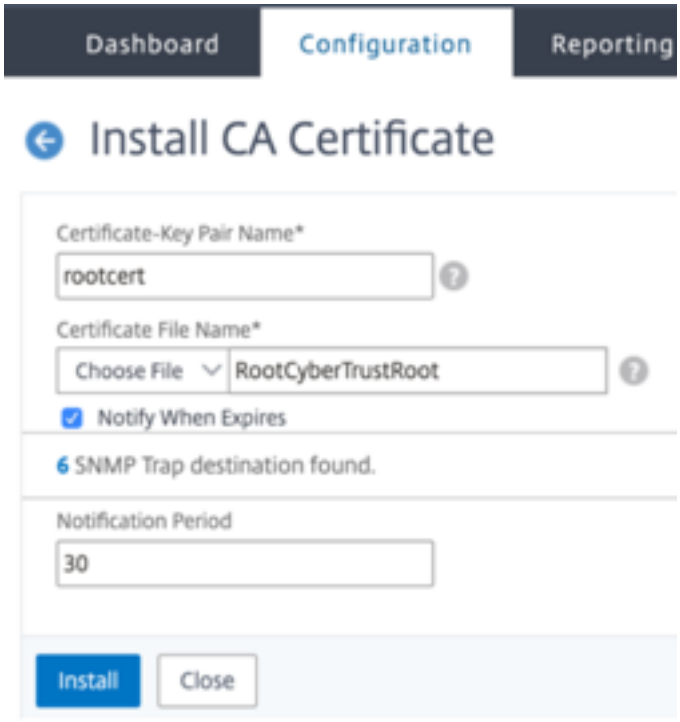
```
add ssl certKey rootcert -cert RootCyberTrustRoot.crt
bind ssl cacertGroup ns_callout_certs  rootcert
<!--NeedCopy-->
```

Para agregar un certificado raíz mediante la GUI

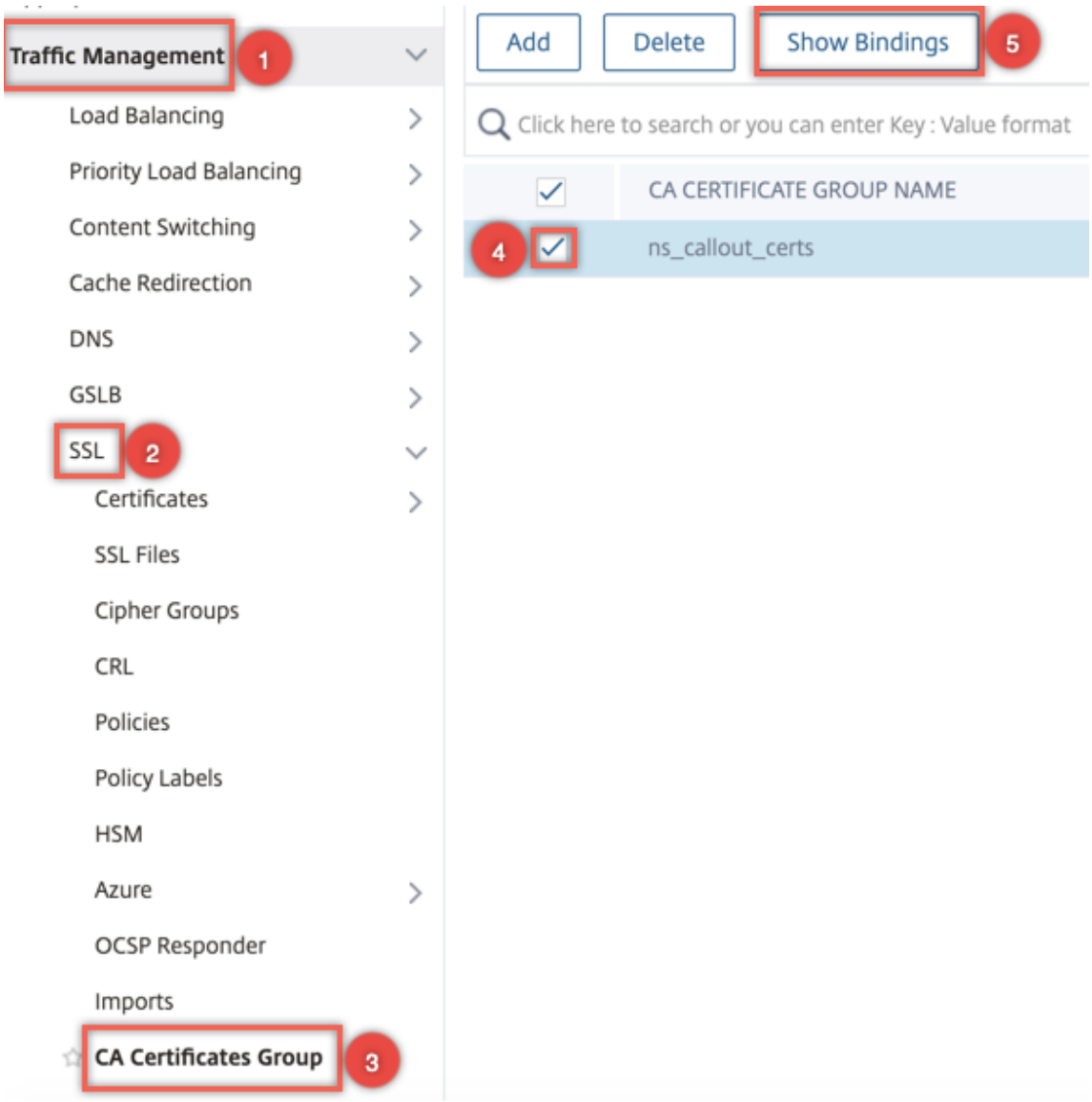
1. Vaya a **Administración del tráfico > SSL > Certificados > Certificados de CA**.



2. Introduzca valores para los siguientes parámetros:
    - Nombre del par de claves de certificado
    - Nombre del archivo de certificado



3. Haga clic en **Instalar**.
4. Vaya a **Administración del tráfico > SSL > Grupo de certificados de CA**.
5. Seleccione **ns_callout_certs** y haga clic en **Mostrar enlaces**.



6. Haga clic en **Bind**.
7. Seleccione el certificado de CA creado anteriormente y haga clic en **Seleccionar**.
8. Haga clic en **Vincular**y, a continuación, en **Cerrar**.

Configurar una aplicación de Azure

La entidad de aplicación de Azure contiene las credenciales necesarias para autenticarse en Azure Active Directory y obtener el token de acceso. Es decir, para obtener acceso de autorización a los recursos y API de Key Vault, agregue el ID de aplicación de Azure, el secreto (contraseña) y el ID de arrendatario en el dispositivo ADC.
Al configurar la entidad de aplicación de Azure mediante la CLI, debe introducir la contraseña. Si usa la GUI, la entidad de aplicación de Azure contiene las credenciales necesarias para autenticarse en

Azure Active Directory y obtener el token de acceso.

Para configurar una aplicación de Azure mediante la CLI

A partir de la versión 13.0-61.x, se agrega un parámetro, VaultResource, al comando `add azure application` para obtener el dominio del grupo de recursos antes de que se conceda el token de acceso a la aplicación. Este parámetro se agrega porque el nombre de dominio puede ser diferente para diferentes regiones. Por ejemplo, el dominio puede ser `vault.azure.net` o `vault.usgov.net`.

En el símbolo del sistema, escriba:

```
add azure application <name> -clientID <string> -clientSecret -tenantID
    <string> -vaultResource <string> [-tokenEndpoint <URL>]
show azure application
<!--NeedCopy-->
```

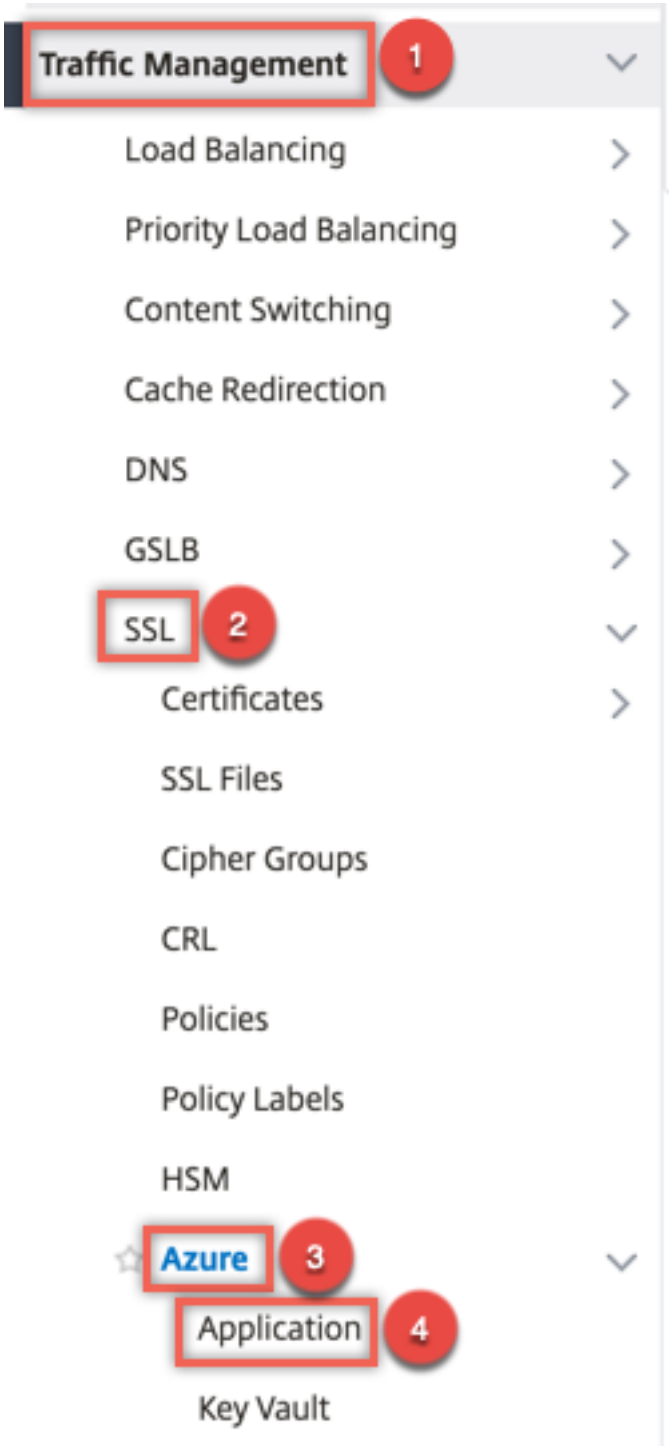
Ejemplo:

```
add azure application app10 -clientiD 12345t23aaa5 -clientsecret
   csHzOoEzmuY= -vaultResource example.vault.azure.net -tenantID 33583
   ee9ca5b
 Done
> sh azure application app10
1)  Name:  app10            ClientID:  12345t23aaa5
    TokenEndpoint:  ”https://login.microsoftonline.com/33583ee9ca5b/”
    TenantID:  33583ee9ca5b  VaultResource:  example.vault.azure.net
 Done

<!--NeedCopy-->
```

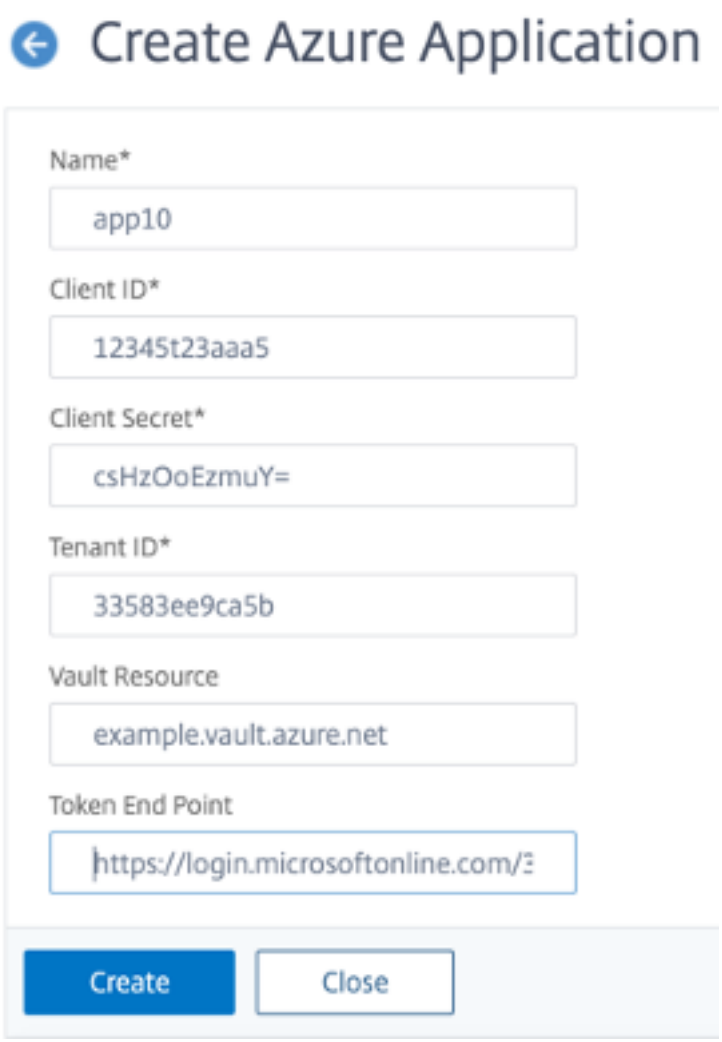
Para configurar una aplicación de Azure mediante la GUI

1. Vaya a **Administración del tráfico > SSL > Azure > Aplicación**.



2. En el panel de detalles, haga clic en **Agregar**.
3. Introduzca valores para los siguientes parámetros:
   - Nombre: nombre del objeto de aplicación del dispositivo Citrix ADC.
   - ID de cliente: ID de aplicación que se genera cuando se crea una aplicación en Azure Active Directory mediante la CLI de Azure o el portal de Azure (GUI).

- Secreto del cliente: contraseña para la aplicación configurada en Azure Active Directory. La contraseña se especifica en la CLI de Azure o se genera en el portal de Azure (GUI).
- ID de arrendatario: ID del directorio dentro de Azure Active Directory en el que se creó la aplicación.
- Vault Resource: recurso de la bóveda para el que se concede el token de acceso. Ejemplo `vault.azure.net`.
- Punto final del token: URL desde la que se puede obtener el token de acceso. Si no se especifica el punto final del token, el valor predeterminado es `https://login.microsoftonline.com/<tenant id>`.



Configurar Azure Key Vault

Cree un objeto de Azure Key Vault en el dispositivo ADC.

Para configurar Azure Key Vault mediante la CLI

En el símbolo del sistema, escriba:

```
add azure keyVault <name> -azureVaultName <string> -azureApplication
       <string>
show azure keyvault
<!--NeedCopy-->
```

Ejemplo:

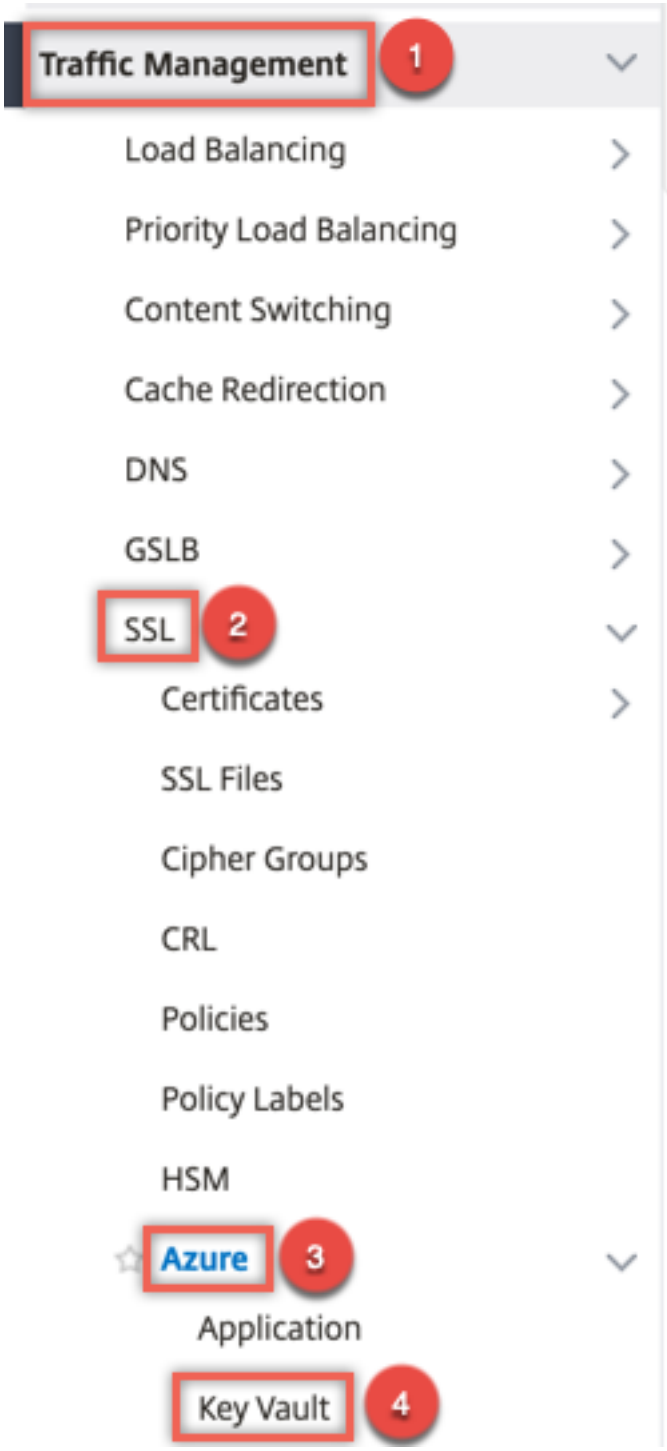
```
add azure keyvault kv1 -azureapplication app10 -azurevaultName pctest.
   vault.azure.net
> sh azure keyVault
1)  Name:  kv1               AzureVaultName:  pctest.vault.azure.net
  AzureApplication:  app10  State:  "Access token obtained"
 Done
<!--NeedCopy-->
```

En la siguiente tabla se enumeran los diferentes valores que el estado de Azure Key Vault puede tomar junto con una breve descripción de cada estado.

State	Descripción
`Created`	Estado inicial del objeto Key Vault. No se ha intentado la autenticación.
`Could not reach token end point`	Indica uno de los siguientes: servidor DNS no configurado, certificado del emisor no enlazado a un grupo de certificados de CA o problemas de red.
`Authorization failed`	Credenciales de aplicación incorrectas.
`Token parse error`	La respuesta de Azure Active Directory no tiene el formato esperado.
`Access token obtained`	Azure Active Directory se autenticó correctamente.

Para configurar Azure Key Vault mediante la interfaz gráfica de usuario

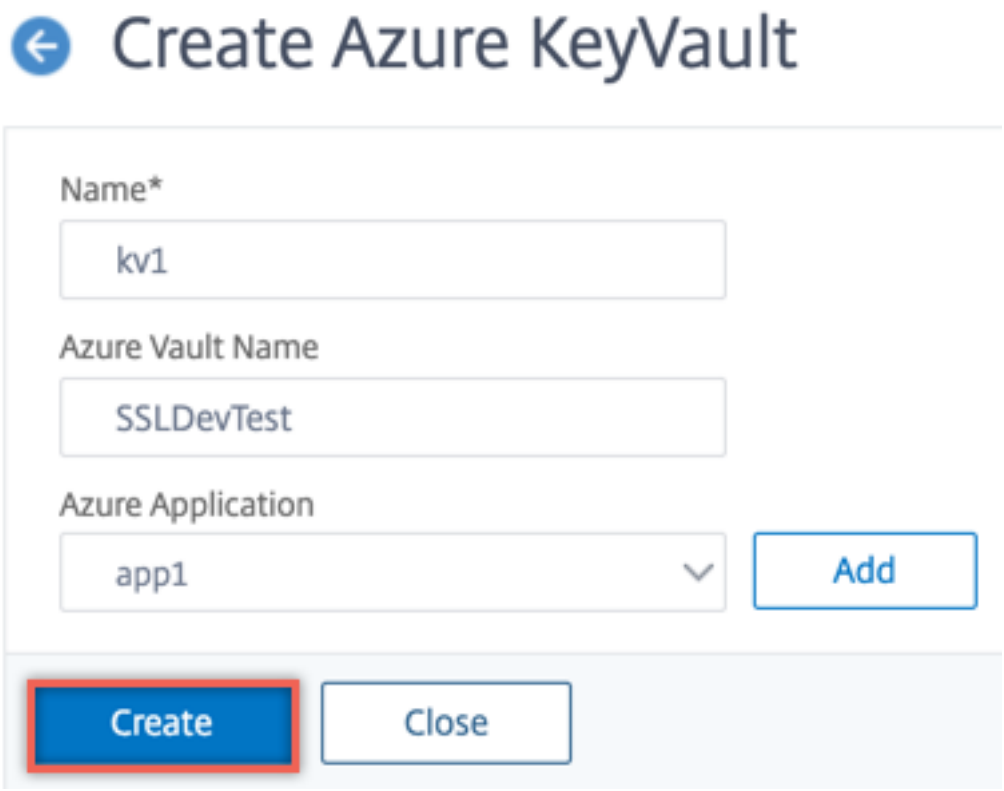
1. Vaya a **Administración del tráfico > SSL > Azure > Key Vault**.



2. Introduzca valores para los siguientes parámetros:

   - Nombre: Nombre de la bóveda de llaves.
   - Nombre de Azure Key Vault: Nombre del depósito de claves configurado en la nube de Azure mediante la CLI de Azure o el portal de Azure (GUI) con nombre de dominio.
   - Nombre de la aplicación de Azure: nombre del objeto de aplicación de Azure creado en

el dispositivo ADC. El objeto Application de Azure con este nombre se usa para la autenticación con Azure Active Directory.



Agregar clave HSM

Almacenar su clave privada en el HSM proporciona cumplimiento FIPS 140-2 nivel 2.

Para agregar una clave HSM mediante la CLI

En el símbolo del sistema, escriba:

```
add ssl hsmKey <hsmKeyName> [-hsmType <hsmType>] [-key <string> |
       -serialNum <string>] {
 -password  }
  [-keystore <string>]
<!--NeedCopy-->
```

Ejemplo:

```
add ssl hsmKey h1 -keystore kv1 -key san15key -hsmType KEYVAULT
```



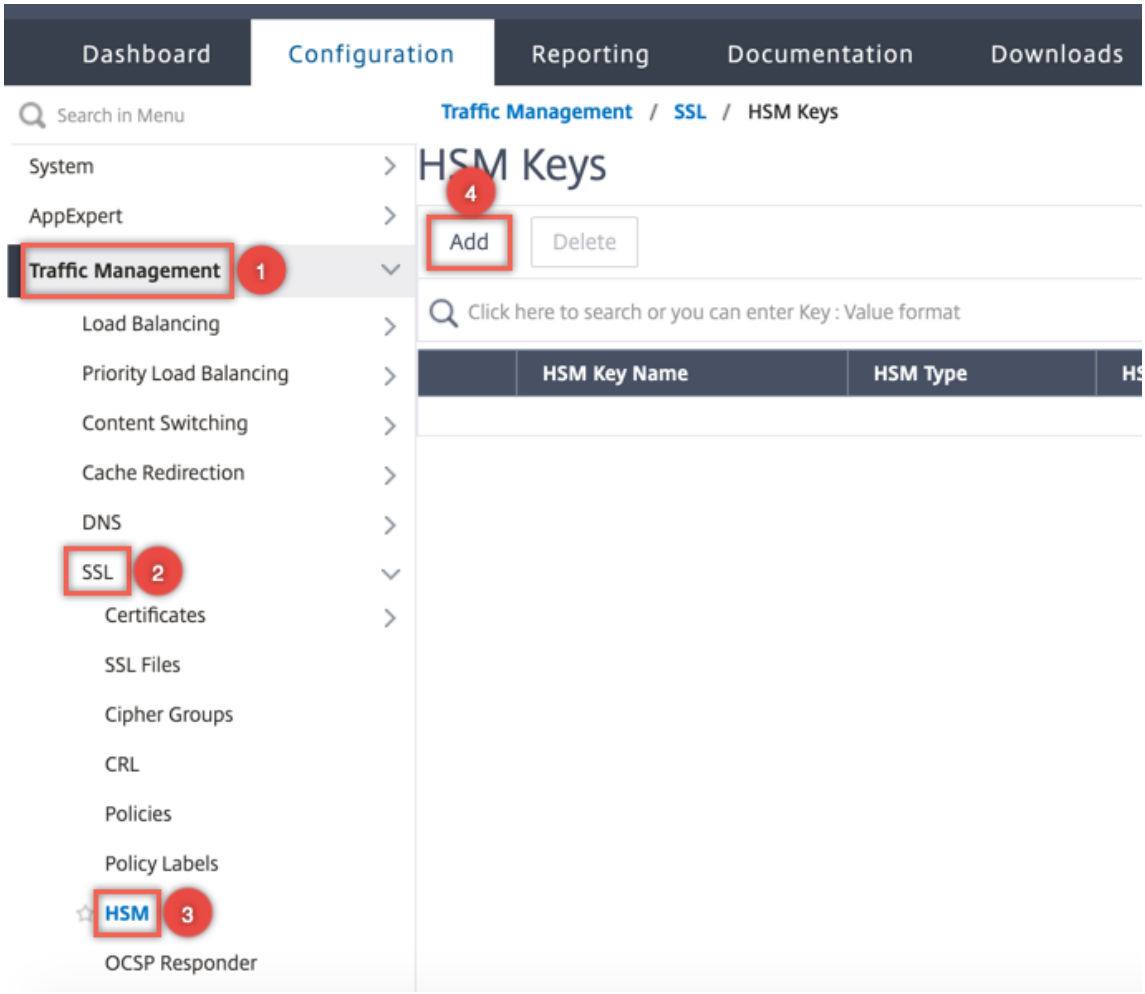
```
2
3
4 > sh ssl hsmKey h1
5     HSM Key Name: h1       Type: KEYVAULT
6     Key: san15key
7     Key store: kv1
8     State:  “Created”
9  Done
10 <!--NeedCopy-->
```

En la siguiente tabla se enumeran los diferentes valores que puede adoptar el estado de una clave HSM junto con una breve descripción de cada estado.

State	Descripción
Created	La clave HSM se agrega en el dispositivo ADC. Aún no se ha intentado realizar una operación clave.
Token de acceso no disponible	El token de acceso no está disponible cuando se intentó la operación de clave.
No autorizado	La aplicación Azure configurada no tiene permiso para realizar la operación clave.
No existe	La clave no existe en Azure Key Vault.
Inalcanzable	No se puede acceder al host de Key Vault en la red.
Marcado hacia abajo	La tecla HSM está marcada como ABAJO en el dispositivo ADC debido a errores de umbral durante la operación de la tecla.
Operaciones clave correctas	Se recibió una respuesta de éxito de Key Vault para la operación clave.
Las operaciones clave fallaron	Se recibió una respuesta de error de Key Vault para la operación clave.
Operación clave estrangulada	La solicitud de operación clave se ve regulada por Key Vault.

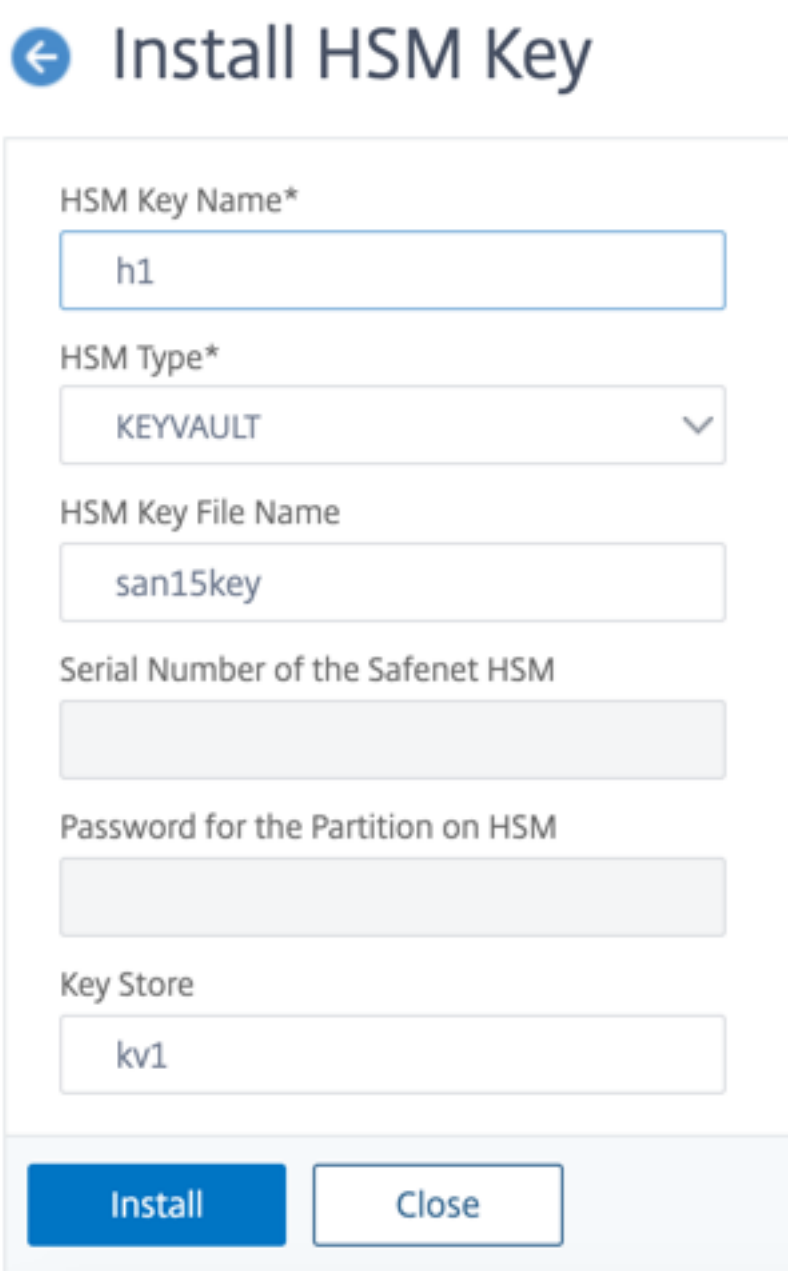
Para agregar una clave HSM mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > SSL > HSM**.



2. Introduzca valores para los siguientes parámetros.

   - Nombre de clave HSM: nombre de la clave.
   - Tipo de HSM: tipo de HSM.
   - Almacén de claves: nombre del objeto de almacenamiento de claves que representa el HSM donde se almacena la clave. Por ejemplo, nombre del objeto Key Vault o del objeto de autenticación de Azure Key Vault. Se aplica solo al tipo KEYVAULT de HSM.



3. Haga clic en **Agregar**

Agregar un par de claves de certificado

Agregue un par de claves de certificado con la clave HSM creada anteriormente.

Para agregar un par de claves de certificado mediante la CLI

En el símbolo del sistema, escriba:

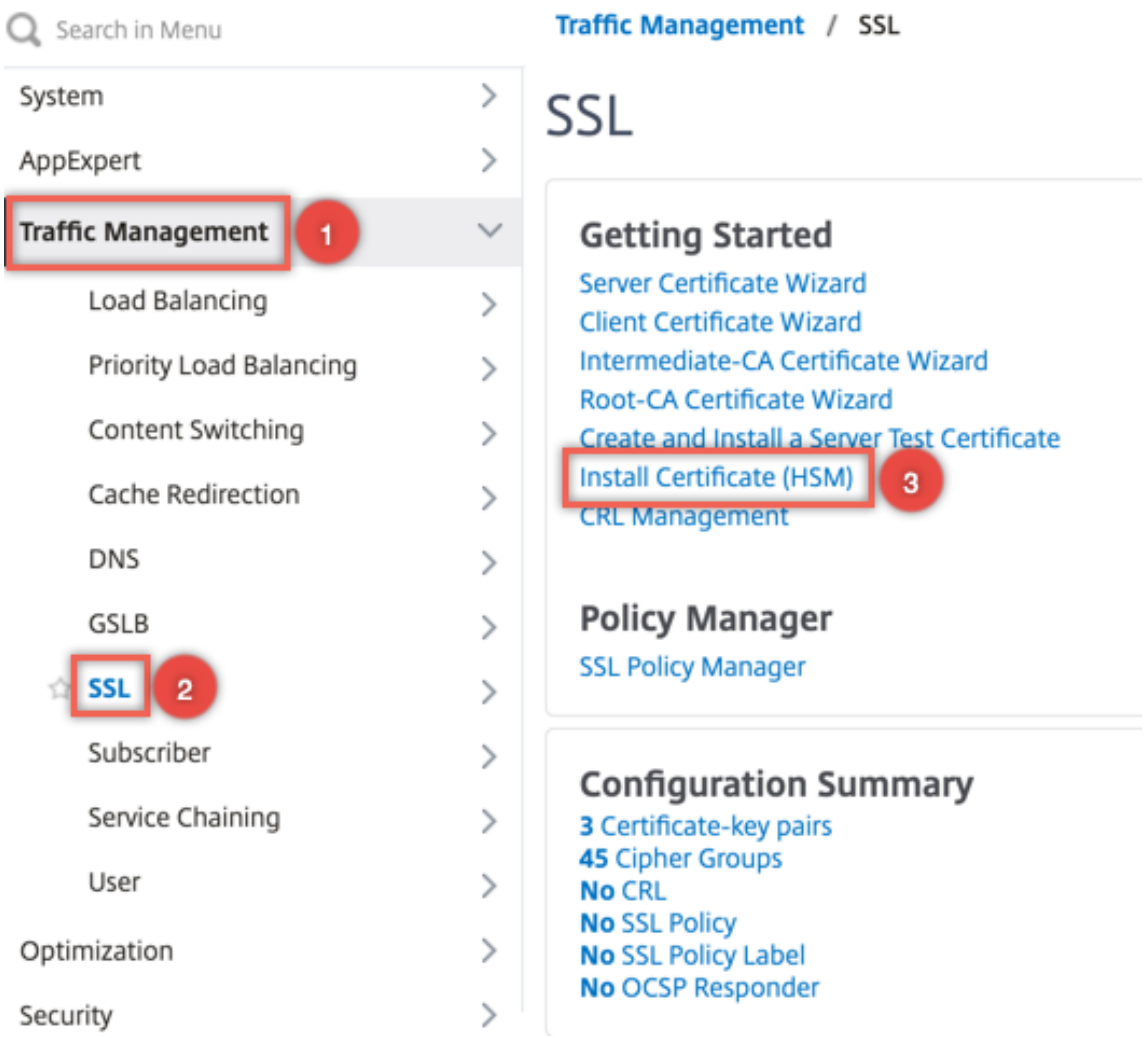

```
add ssl certKey <certkeyName> (-cert <string> [-password]) -hsmKey <
   string>]
show ssl certkey
<!--NeedCopy-->
```

Ejemplo:

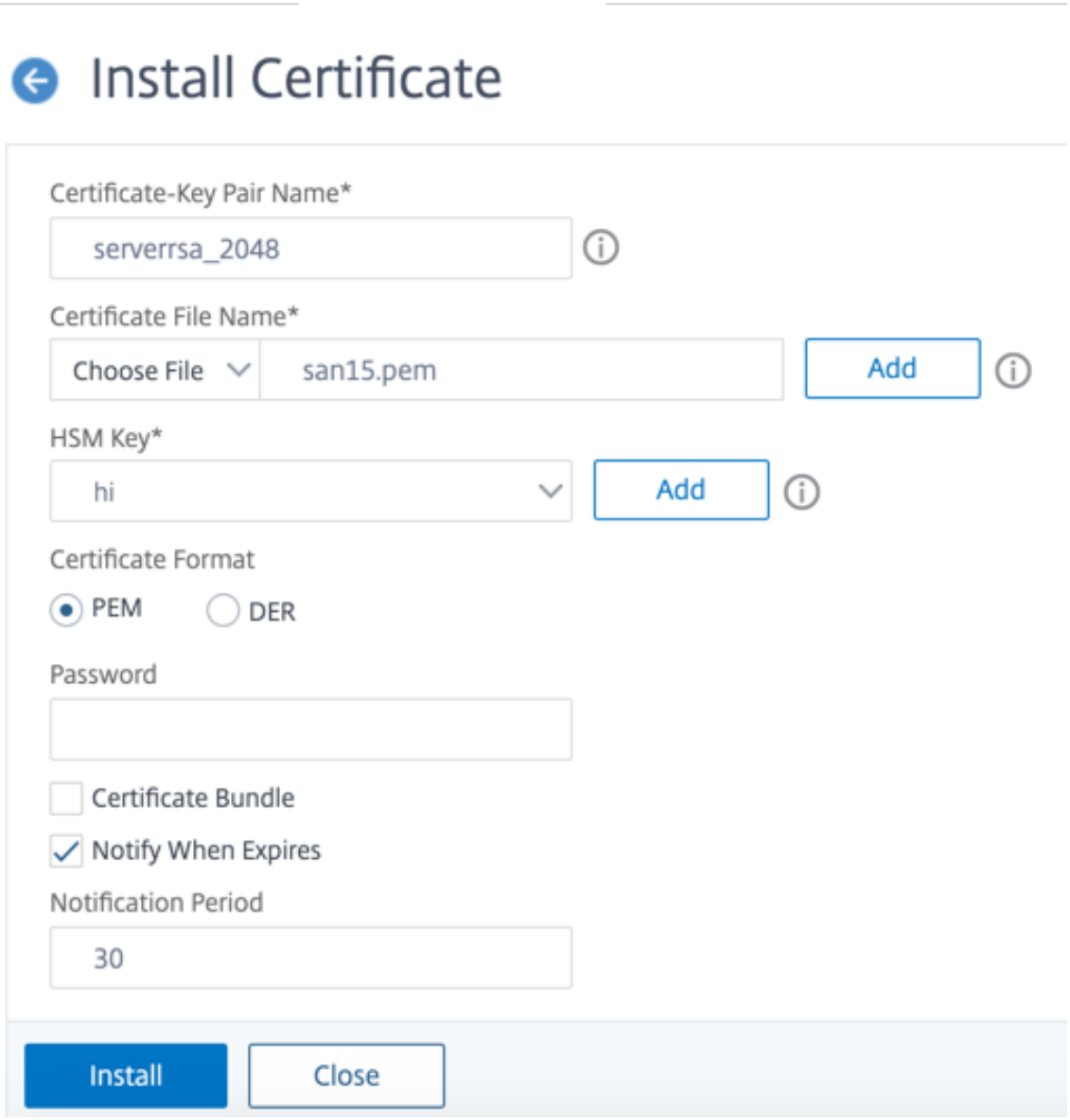
```
add ssl certKey serverrsa_2048 -cert /nsconfig/ssl/san_certs/san15.pem
   -hsmKey h1
> sh ssl certkey serverrsa_2048
    Name: serverrsa_2048        Status: Valid,   Days to expiration
       :9483
    Version: 3
    Serial Number: F5CFF9EF1E246022
    Signature Algorithm: sha256WithRSAEncryption
    Issuer:  C=in,O=citrix,CN=ca
    Validity
        Not Before: Mar 20 05:42:57 2015 GMT
        Not After : Mar 12 05:42:57 2045 GMT
    Certificate Type:   "Server Certificate"
    Subject:  C=in,O=citrix
    Public Key Algorithm: rsaEncryption
    Public Key size: 2048
    Ocsp Response Status: NONE
 Done
<!--NeedCopy-->
```

Para agregar un par de claves de certificado mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > SSL > Instalar certificado (HSM)**.



2. Introduzca valores para los siguientes parámetros:
   - Nombre del par de claves de certificado
   - Nombre del archivo de certificado
   - Clave HSM



3. Haga clic en **Instalar**.

Enlace el par de claves de certificado a un servidor virtual

El certificado utilizado para procesar transacciones SSL debe estar vinculado al servidor virtual que recibe los datos SSL.

Para enlazar el par de claves de certificado SSL a un servidor virtual mediante la CLI

En el símbolo del sistema, escriba:

```
1 bind ssl vserver <vServerName> -certkeyName <certificate-KeyPairName>
2 show ssl vserver <vServerName>
```



```
<!--NeedCopy-->
```

Ejemplo:

```
bind ssl vserver v1 -certkeyName serverrsa_2048

sh ssl vserver v1

    Advanced SSL configuration for VServer v1:
    DH: DISABLED
    DH Private-Key Exponent Size Limit: DISABLED    Ephemeral RSA:
       ENABLED      Refresh Count: 0
    Session Reuse: ENABLED      Timeout: 120 seconds
    Cipher Redirect: DISABLED
    ClearText Port: 0
    Client Auth: DISABLED
    SSL Redirect: DISABLED
    Non FIPS Ciphers: DISABLED
    SNI: DISABLED
    OCSP Stapling: DISABLED
    HSTS: DISABLED
    HSTS IncludeSubDomains: NO
    HSTS Max-Age: 0
    HSTS Preload: NO
    SSLv3: ENABLED  TLSv1.0: ENABLED  TLSv1.1: ENABLED  TLSv1.2:
       ENABLED  TLSv1.3: DISABLED
    Push Encryption Trigger: Always
    Send Close-Notify: YES
    Strict Sig-Digest Check: DISABLED
    Zero RTT Early Data: DISABLED
    DHE Key Exchange With PSK: NO
    Tickets Per Authentication Context: 1

    ECC Curve: P_256, P_384, P_224, P_521

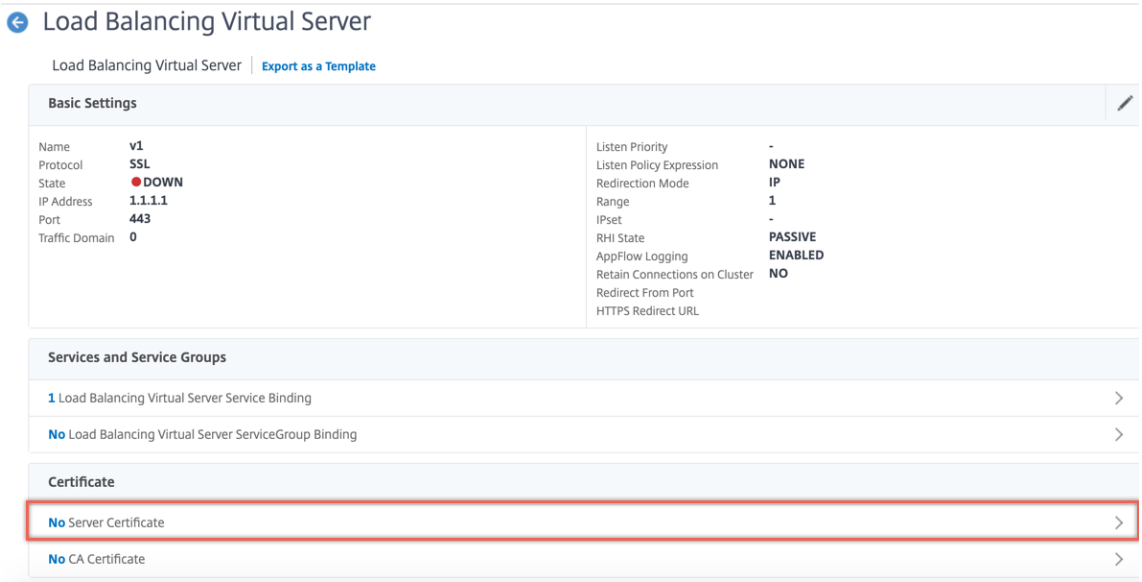
1)  CertKey Name: serverrsa_2048    Server Certificate



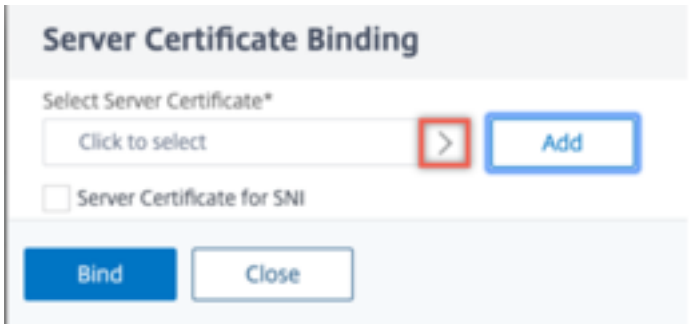
1)  Cipher Name: DEFAULT
    Description: Default cipher list with encryption strength >= 128bit
 Done
<!--NeedCopy-->
```


Para enlazar un par de claves de certificado SSL a un servidor virtual mediante la GUI

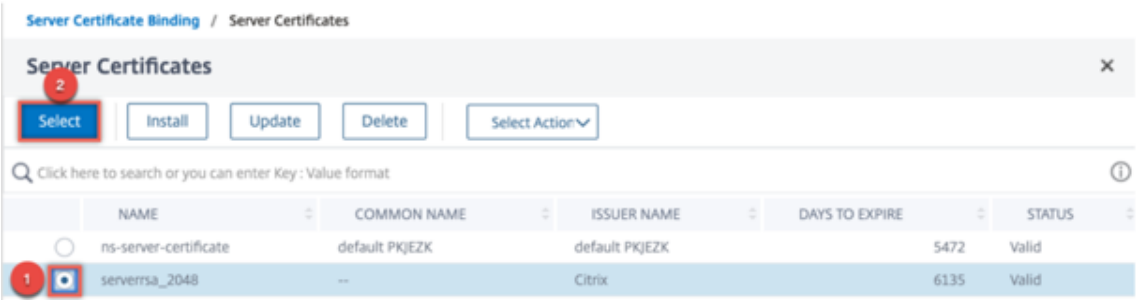
1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales** y abra un servidor virtual SSL. Haga clic en la sección Certificado.



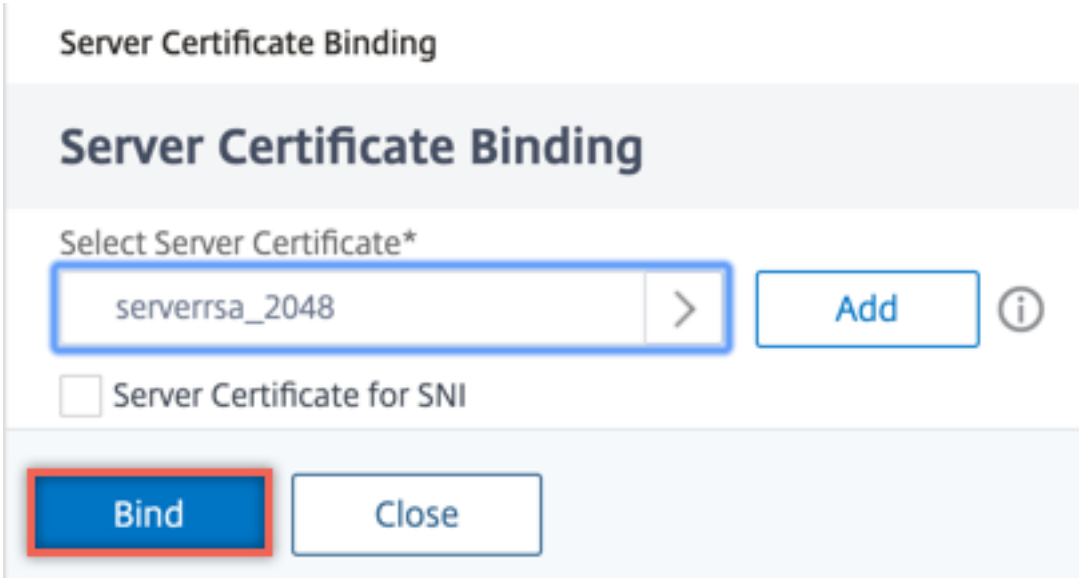
2. Haga clic en la flecha para seleccionar el par de claves de certificado.



3. Seleccione el par de claves de certificado de la lista.



4. Enlace el par de claves de certificado al servidor virtual.



Limitaciones

- El número de llamadas simultáneas a Azure Key Vault para operaciones clave es limitado. El rendimiento del dispositivo ADC depende de los límites de Key Vault. Para obtener más información, consulte la documentación de Microsoft Azure Key Vault.
- Las claves EC no son compatibles.
- No se admiten los protocolos EDT y DTLS.
- Los dispositivos ADC con chips SSL Intel Coleto no son compatibles.
- Las particiones de administración y clústeres no son compatibles.
- No puede actualizar la entidad de aplicación de Azure, el objeto Azure Key Vault y el par de claves de certificado HSM después de haberlos agregado al dispositivo ADC.
- No se admite un paquete de certificados con claves HSM.
- No aparece un error si la clave HSM y el certificado no coinciden. Al agregar un par de claves de certificado, asegúrese de que la clave HSM y el certificado coincidan.
- No se puede vincular una clave HSM a un servidor virtual DTLS.
- No puede firmar solicitudes de OCSP mediante un par de claves de certificado que se cree con una clave HSM.
- No puede vincular un par de claves de certificado a un servicio SSL si el par de claves de certificado se crea con una clave HSM.

Preguntas frecuentes

Cuando se integra con Azure Key Vault, ¿las claves privadas se almacenan en la memoria del dispositivo ADC?

No, las claves privadas no se almacenan en la memoria del dispositivo ADC. Para cada transacción SSL, el dispositivo envía una solicitud a Key Vault.

¿La integración cumple con FIPS 140-2 nivel 2?

Sí, la solución integrada permite usar FIPS 140-2 de nivel 2.

¿Qué tipos de clave se admiten?

Solo se admiten los tipos de clave RSA.

¿Qué tamaños de clave se admiten?

Se admiten claves RSA de 1024 bits, 2048 bits y 4096 bits.

¿Qué cifrados se admiten?

Se admiten todos los cifrados compatibles con el dispositivo ADC, incluidos los cifrados TLSv1.3 con ECDHE y SHA256.

¿Se registran las transacciones?

El dispositivo ADC registra cada transacción que realiza con Key Vault. Se registran detalles como la hora, la dirección IP de la bóveda, el puerto, el éxito o el fallo de la conexión y los errores.
A continuación se muestra una salida de registro SSL de ejemplo.

```
1 Apr  9 16:35:30 <local0.debug> 10.102.57.30 04/09/2019:16:35:30 GMT
      0-PPE-0 : default SSLLOG SSL_HANDSHAKE_SUCCESS 896 0 :
    Backend SPCBId 30894 - ServerIP 104.211.224.186 - ServerPort 443
     - ProtocolVersion TLSv1.2 - CipherSuite "ECDHE-RSA-AES256-GCM-
    SHA384 TLSv1.2 Non-Export 256-bit" - Session New -
    SERVER_AUTHENTICATED -SerialNumber "200005
    A75B04365827852D630000000005A75B" - SignatureAlgorithm "
    sha256WithRSAEncryption" - ValidFrom "Mar 17 03:28:42 2019 GMT"
    - ValidTo "Mar 17 03:28:42 2021 GMT" - HandshakeTime 40 ms
2 Apr  9 16:35:30 <local0.debug> 10.102.57.30 04/09/2019:16:35:30 GMT
```



```
        0-PPE-0 : default SSLLOG SSL_HANDSHAKE_ISSUERNAME 897 0 :
      SPCBId 30894 - IssuerName " C=US,ST=Washington,L=Redmond,O=
      Microsoft Corporation,OU=Microsoft IT,CN=Microsoft IT TLS CA 2"
3 Apr  9 16:35:30 <local0.debug> 10.102.57.30 04/09/2019:16:35:30 GMT
        0-PPE-0 : default SSLLOG SSL_HANDSHAKE_SUBJECTNAME 898 0 :
      SPCBId 30894 - SubjectName " CN=vault.azure.net"
4 <!--NeedCopy-->
```

Solucionar problemas

August 20, 2021

Si la función SSL no funciona como se esperaba después de la configuración, puede utilizar algunas herramientas comunes para acceder a los recursos de Citrix ADC y diagnosticar el problema.

Recursos para solucionar problemas

Para obtener los mejores resultados, utilice los siguientes recursos para solucionar un problema SSL en un dispositivo Citrix ADC:

- El archivo ns.log relevante
- El último archivo ns.conf
- El archivo de mensajes
- El archivo `newnslog` correspondiente
- Archivos de seguimiento
- Una copia de los archivos de certificado, si es posible
- Una copia del archivo de claves, si es posible
- El mensaje de error, si existe

Además de estos recursos, puede utilizar la aplicación Wireshark personalizada para los archivos de seguimiento Citrix ADC para agilizar la solución de problemas.

Solución de problemas de SSL

Para solucionar un problema SSL, proceda de la siguiente manera:

- Compruebe que el dispositivo Citrix ADC tiene licencia para descarga de SSL y equilibrio de carga.
- Compruebe que las funciones de descarga SSL y equilibrio de carga estén habilitadas en el dispositivo.
- Compruebe que el estado del servidor virtual SSL no se muestra como DOWN.

- Compruebe que el estado del servicio enlazado al servidor virtual no se muestra como DOWN.
- Compruebe que un certificado válido está enlazado al servidor virtual.
- Verifique que el servicio esté mediante un puerto apropiado, preferiblemente el puerto 443.

Descifrar el tráfico TLS1.3 del seguimiento de paquetes

Para solucionar problemas de protocolos que se ejecutan sobre TLS1.3, primero debe descifrar el tráfico TLS1.3. Para descifrar TLS 1.3 en Wireshark, los secretos deben exportarse en el formato de registro de claves de NSS. Para obtener más información sobre el formato de registro de claves, consulte Formato de registro de claves de NSS.

Para obtener información sobre cómo capturar un seguimiento de paquetes, consulte Captura de claves de sesión SSL durante un seguimiento.

Nota: Citrix ADC registra automáticamente los secretos de cada conexión en el formato adecuado para la versión del protocolo TLS/SSL en uso.

La actualización de CRL no ocurre en el nodo secundario en una configuración de HA

La actualización no se produce porque el servidor CRL solo es accesible para el nodo principal a través de una red privada.

Solución alternativa: Agregue un servicio en el nodo principal con la dirección IP del servidor CRL. Este servicio actúa como un proxy para el servidor CRL. Cuando la configuración se sincroniza entre los nodos, la actualización CRL funciona tanto para los nodos primario como secundario a través del servicio configurado en el nodo primario.

Preguntas frecuentes sobre SSL

September 8, 2021

Preguntas básicas

El acceso HTTPS a la GUI falla en una instancia VPX. ¿Cómo puedo obtener acceso?

Se necesita un par de claves de certificado para acceder HTTPS a la GUI. En un dispositivo Citrix ADC, un par de claves de certificado se enlaza automáticamente a los servicios internos. En un dispositivo MPX o SDX, el tamaño de clave predeterminado es de 1024 bytes y, en una instancia VPX, el tamaño de clave predeterminado es de 512 bytes. Sin embargo, la mayoría de los navegadores actuales no aceptan una clave inferior a 1024 bytes. Como resultado, el acceso HTTPS a la utilidad de configuración VPX está bloqueado.

Citrix recomienda instalar un par de claves de certificado de al menos 1024 bytes y vincularlo al servicio interno para obtener acceso HTTPS a la utilidad de configuración. Alternativamente, actualice el `ns-server-certificate` a 1024 bytes. Puede utilizar el acceso HTTP a la utilidad de configuración o a la CLI para instalar el certificado.

Si agrego una licencia a un dispositivo MPX, se pierde el enlace del par de claves de certificado. ¿Cómo soluciono este problema?

Si una licencia no está presente en un dispositivo MPX cuando se inicia y agrega una licencia más tarde y reinicia el dispositivo, podría perder el enlace de certificados. Vuelva a instalar el certificado y vincularlo al servicio interno

Citrix recomienda instalar una licencia adecuada antes de iniciar el dispositivo.

¿Cuáles son los distintos pasos necesarios para configurar un canal seguro para una transacción SSL?

La configuración de un canal seguro para una transacción SSL implica los siguientes pasos:

1. El cliente envía una solicitud HTTPS de un canal seguro al servidor.
2. Tras seleccionar el protocolo y el cifrado, el servidor envía su certificado al cliente.
3. El cliente comprueba la autenticidad del certificado de servidor.
4. Si falla alguna de las comprobaciones, el cliente muestra la valoración correspondiente.
5. Si los cheques pasan o el cliente decide continuar incluso si falla una comprobación, el cliente crea una clave desechable temporal. Esta clave se denomina *secreto previo al maestro* y el cliente cifra esta clave mediante la clave pública del certificado del servidor.
6. Al recibir el secreto previo al maestro, el servidor lo descifra utilizando la clave privada del servidor y genera las claves de sesión. El cliente también genera las claves de sesión a partir del secreto previo al maestro. Por lo tanto, tanto el cliente como el servidor tienen ahora una clave de sesión común, que se utiliza para cifrar y descifrar los datos de la aplicación.

Entiendo que SSL es un proceso intensivo de CPU. ¿Cuál es el coste de CPU asociado al proceso SSL?

Las dos etapas siguientes están asociadas al proceso SSL:

- El apretón de manos inicial y la configuración segura del canal mediante la tecnología de clave pública y privada.
- Cifrado masivo de datos mediante la tecnología de clave simétrica.

Ambas etapas anteriores pueden afectar al rendimiento del servidor y requieren un procesamiento intensivo de la CPU por los siguientes motivos:

1. El apretón de manos inicial implica la criptografía de clave público-privada, que requiere mucha CPU debido a los grandes tamaños de clave (1024 bits, 2048 bits, 4096 bits).
2. El cifrado/descifrado de datos también es caro desde el punto de vista computacional, dependiendo de la cantidad de datos que se deben cifrar o descifrar.

¿Cuáles son las distintas entidades de una configuración SSL?

Una configuración SSL tiene las siguientes entidades:

- Certificado de servidor
- Certificado de autoridad certificadora (CA)
- Conjunto de cifrado que especifica los protocolos para las siguientes tareas:
  - Intercambio de claves inicial
  - Autenticación de servidor y
  - algoritmo de cifrado masivo
  - autenticación de mensajes
- Client authentication
- CRL
- Herramienta de generación de claves de certificado SSL que permite crear los siguientes archivos:
  - Solicitud de certificado
  - Certificado autofirmado
  - Claves RSA
  - Parámetros DH

Quiero utilizar la función de descarga SSL del dispositivo Citrix ADC. ¿Cuáles son las distintas opciones para recibir un certificado SSL?

Debe recibir un certificado SSL para poder configurar la configuración SSL en el dispositivo Citrix ADC. Puede utilizar cualquiera de los siguientes métodos para recibir un certificado SSL:

- Solicite un certificado a una entidad de certificación (CA) autorizada.
- Utilice el certificado de servidor existente.
- Cree un par de claves de certificado en el dispositivo Citrix ADC.

Nota: Este certificado es un certificado de prueba firmado por la CA raíz de prueba generada por el dispositivo Citrix ADC. Los navegadores no aceptan certificados de prueba firmados por la CA raíz de prueba. El navegador emite un mensaje de advertencia que indica que el certificado del servidor no se puede autenticar.

- Para cualquier otra cosa que no sea una prueba, debe proporcionar un certificado de CA y una clave de CA válidos para firmar el certificado del servidor.

¿Cuáles son los requisitos mínimos para una configuración SSL?

Los requisitos mínimos para configurar una configuración SSL son los siguientes:

- Obtenga los certificados y las claves.
- Cree un servidor virtual SSL de equilibrio de carga.
- Enlazar servicios HTTP o SSL al servidor virtual SSL.
- Enlazar un par de claves de certificado al servidor virtual SSL.

¿Cuáles son los límites para los distintos componentes de SSL?

Los componentes SSL tienen los siguientes límites:

- Tamaño de bits de los certificados SSL: 4096.
- Número de certificados SSL: Depende de la memoria disponible en el dispositivo.
- Certificados SSL CA intermedios vinculados máximos: 9 por cadena.
- Revocaciones de CRL: depende de la memoria disponible en el dispositivo.

¿Cuáles son los distintos pasos del cifrado de datos de extremo a extremo en un dispositivo Citrix ADC?

Los pasos necesarios en el proceso de cifrado del lado del servidor en un dispositivo Citrix ADC son los siguientes:

1. El cliente se conecta al SSL VIP configurado en el dispositivo Citrix ADC en el sitio seguro.
2. Tras recibir la solicitud segura, el dispositivo descifra la solicitud y aplica técnicas de conmutación de contenido de capa 4 a 7 y políticas de equilibrio de carga. A continuación, selecciona el mejor servidor web back-end disponible para la solicitud.
3. El dispositivo Citrix ADC crea una sesión SSL con el servidor seleccionado.
4. Tras establecer la sesión SSL, el dispositivo cifra la solicitud del cliente y la envía al servidor Web mediante la sesión SSL segura.
5. Cuando el dispositivo recibe la respuesta cifrada del servidor, descifra y vuelve a cifrar los datos. A continuación, envía los datos al cliente mediante la sesión SSL del lado del cliente.

La técnica de multiplexación del dispositivo Citrix ADC permite al dispositivo reutilizar las sesiones SSL establecidas con los servidores web. Por lo tanto, el dispositivo evita el intercambio de claves intensivo de la CPU, conocido como *apretón de manos completo*. Este proceso reduce el número total de sesiones SSL en el servidor y mantiene la seguridad integral.

Certificados y claves

¿Puedo colocar los archivos de certificados y claves en cualquier ubicación? ¿Hay alguna ubicación recomendada para almacenar estos archivos?

Puede almacenar los archivos de certificado y clave en el dispositivo Citrix ADC o en un equipo local. Sin embargo, Citrix recomienda almacenar los archivos de certificados y claves en el `/nsconfig/ssl` directorio del dispositivo Citrix ADC. El `/etc` directorio existe en la memoria flash del dispositivo Citrix ADC. Esta acción proporciona portabilidad y facilita la copia de seguridad y la restauración de los archivos de certificado del dispositivo.

Nota: Asegúrese de que el certificado y los archivos clave estén almacenados en el mismo directorio.

¿Cuál es el tamaño máximo de la clave de certificado admitida en el dispositivo Citrix ADC?

Un dispositivo Citrix ADC que ejecuta una versión de software anterior a la versión 9.0 admite un tamaño máximo de clave de certificado de 2048 bits. La versión 9.0 y posterior admiten un tamaño máximo de clave de certificado de 4096 bits. Este límite se aplica a los certificados RSA.

Un dispositivo MPX admite certificados de 512 bits hasta los siguientes tamaños:

- Certificado de servidor de 4096 bits en el servidor virtual
- Certificado de cliente de 4096 bits en el servicio
- Certificado CA de 4096 bits (incluye certificados intermedios y raíz)
- Certificado de 4096 bits en el servidor back-end
- Certificado de cliente de 4096 bits (si la autenticación de cliente está habilitada en el servidor virtual)

Un dispositivo virtual admite certificados de 512 bits hasta los siguientes tamaños:

- Certificado de servidor de 4096 bits en el servidor virtual
- Certificado de cliente de 4096 bits en el servicio
- Certificado CA de 4096 bits (incluye certificados intermedios y raíz)
- Certificado de 4096 bits en el servidor back-end de la versión 12.0-56.x. Las versiones anteriores admiten certificados de 2048 bits.
- Certificado de cliente de 2048 bits (si la autenticación de cliente está habilitada en el servidor virtual) de la versión 12.0-56.x.

¿Cuál es el tamaño máximo del parámetro DH compatible con el dispositivo Citrix ADC?

El dispositivo Citrix ADC admite un parámetro DH de un máximo de 2048 bits.

¿Cuál es la longitud máxima de la cadena de certificados, es decir, el número máximo de certificados de una cadena compatible con un dispositivo Citrix ADC?

Un dispositivo Citrix ADC puede enviar un máximo de 10 certificados en una cadena al enviar un mensaje de certificado de servidor. Una cadena de la longitud máxima incluye el certificado de servidor y nueve certificados de CA intermedios.

¿Cuáles son los distintos formatos de certificado y clave admitidos en el dispositivo Citrix ADC?

El dispositivo Citrix ADC admite los siguientes formatos de certificado y clave:

- Correo mejorado de privacidad (PEM)
- Regla de codificación distinguida (DER)

¿Existe un límite para el número de certificados y claves que puedo instalar en el dispositivo Citrix ADC?

No. El número de certificados y claves que se pueden instalar está limitado únicamente por la memoria disponible en el dispositivo Citrix ADC.

He guardado el certificado y los archivos clave en el equipo local. Quiero transferir estos archivos al dispositivo Citrix ADC mediante el protocolo FTP. ¿Existe algún modo preferido para transferir estos archivos al dispositivo Citrix ADC?

Sí. Si utiliza el protocolo FTP, debe utilizar el modo binario para transferir el certificado y los archivos de clave al dispositivo Citrix ADC.

Nota: De forma predeterminada, FTP está deshabilitado. Citrix recomienda utilizar el protocolo SCP para transferir archivos de certificados y claves. La utilidad de configuración utiliza implícitamente SCP para conectarse al dispositivo.

¿Cuál es la ruta de directorio predeterminada para el certificado y la clave?

La ruta de directorio predeterminada para el certificado y la clave es '/nsconfig/ssl'.

Al agregar un par de certificados y claves, ¿qué ocurre si no especifico una ruta absoluta a los archivos de certificados y claves?

Al agregar un par de claves de certificado, especifique una ruta absoluta a los archivos de certificado y clave. Si no lo especifica, el dispositivo ADC busca estos archivos en el directorio predeterminado e intenta cargarlos en el kernel. El directorio predeterminado es `/nsconfig/ssl`. Por ejemplo, si los

archivos cert1024.pem y rsa1024.pem están disponibles en el `/nsconfig/ssl` directorio del dispositivo, los dos comandos siguientes se ejecutan correctamente:

```
add ssl certKey cert1 -cert cert1204.pem -key rsa1024.pem
<!--NeedCopy-->
```

```
add ssl certKey cert1 -cert /nsconfig/ssl/cert1204.pem -key /nsconfig/
   ssl/rsa1024.pem
<!--NeedCopy-->
```

He configurado una configuración de alta disponibilidad. Quiero implementar la función SSL en la configuración. ¿Cómo debo manejar los archivos de certificados y claves en una configuración de alta disponibilidad?

En una configuración de alta disponibilidad, debe almacenar los archivos de certificado y clave tanto en el dispositivo Citrix ADC principal como en el secundario. La ruta de directorio para los archivos de certificado y clave debe ser la misma en ambos dispositivos antes de agregar un par de claves de certificado SSL en el dispositivo principal.

nCipher nShield® HSM

Al integrarnos con nCipher nShield® HSM, ¿tenemos que tener en cuenta alguna configuración específica al agregar el dispositivo Citrix ADC a HA?

Configure los mismos dispositivos nCipher en ambos nodos de HA. Los comandos de configuración de nCipher no se sincronizan en HA. Para obtener información sobre los requisitos previos para nCipher nShield® HSM, consulte Requisitos previos.

¿Tenemos que integrar individualmente ambos dispositivos con NCipher NShield® HSM y RFS? ¿Necesitamos completar esta acción antes o después de la configuración de alta disponibilidad?

Puede completar la integración antes o después de la configuración de alta disponibilidad. Si la integración se realiza después de la configuración de alta disponibilidad, las claves importadas en el nodo principal antes de configurar el nodo secundario no se sincronizan con el nodo secundario. Por lo tanto, Citrix recomienda la integración de nCipher antes de la configuración de alta disponibilidad.

¿Necesitamos importar la clave en los dispositivos Citrix ADC primarios y secundarios, o las claves están sincronizadas desde el nodo principal al nodo secundario?

Si nCipher está integrado en ambos dispositivos antes de formar la HA, las claves se sincronizan automáticamente desde RFS durante el proceso de integración.

Dado que el HSM no está en el dispositivo Citrix ADC, sino en nCipher, ¿qué sucede con las claves y los certificados cuando un nodo falla y se reemplaza?

Si falla un nodo, puede sincronizar las claves y los certificados con el nuevo nodo, integrando nCipher en el nuevo nodo. A continuación, ejecute los siguientes comandos:

```
sync ha files ssl
force ha sync
<!--NeedCopy-->
```

Los certificados se sincronizan y agregan si las claves se sincronizan en el proceso de integración de nCipher.

Cifrados

¿Qué es un cifrado nulo?

Los cifrados sin cifrado se conocen como cifrados nulos. Por ejemplo, NULL-MD5 es un cifrado NULO.

¿Están habilitados los cifradores NULOS de forma predeterminada para un SSL VIP o un servicio SSL?

No. Los cifrados NULOS no están habilitados de forma predeterminada para un SSL VIP o un servicio SSL.

¿Cuál es el procedimiento para eliminar los cifrados nulos?

Para quitar los cifrados NULOS de un SSL VIP, ejecute el siguiente comando:

```
bind ssl cipher <SSL_VIP> REM NULL
<!--NeedCopy-->
```

Para quitar los cifrados NULOS de un servicio SSL, ejecute el siguiente comando:


```
bind ssl cipher <SSL_Service> REM NULL -service
<!--NeedCopy-->
```

¿Cuáles son los distintos alias de cifrado admitidos en el dispositivo Citrix ADC?

Para enumerar los alias de cifrado admitidos en el dispositivo, en el símbolo del sistema, escriba:

```
sh cipher
<!--NeedCopy-->
```

¿Cuál es el comando para mostrar todos los cifrados predefinidos del dispositivo Citrix ADC?

Para mostrar todos los cifrados predefinidos del dispositivo Citrix ADC, en la CLI, escriba:

```
show ssl cipher
<!--NeedCopy-->
```

¿Cuál es el comando para mostrar los detalles de un cifrado individual del dispositivo Citrix ADC?

Para mostrar los detalles de un cifrado individual del dispositivo Citrix ADC, en la CLI, escriba:

```
show ssl cipher <Cipher_Name/Cipher_Alias_Name/Cipher_Group_Name>
<!--NeedCopy-->
```

Ejemplo:

```
show cipher SSL3-RC4-SHA
     1) Cipher Name: SSL3-RC4-SHA
     Description: SSLv3 Kx=RSA Au=RSA Enc=RC4(128)
    Mac=SHA1
     Done
<!--NeedCopy-->
```


¿Cuál es la importancia de agregar los cifrados predefinidos del dispositivo Citrix ADC?

Al agregar los cifrados predefinidos del dispositivo Citrix ADC, los cifrados NULOS se agregan a un SSL VIP o a un servicio SSL SSL.

¿Es posible cambiar el pedido del cifrado sin desvincularlo de un grupo de cifrado en un dispositivo Citrix ADC?

Sí. Es posible cambiar el orden del cifrado sin desvincular los cifrados de un grupo de cifrado personalizado. Sin embargo, no se puede cambiar la prioridad en los grupos de cifrado incorporados. Para cambiar la prioridad de un cifrado enlazado a una entidad SSL, primero desvincule el cifrado del servidor virtual, el servicio o el grupo de servicios.

Nota: Si el grupo de cifrado enlazado a una entidad SSL está vacío, el protocolo de enlace SSL falla porque no hay ningún cifrado negociado. El grupo de cifrado debe contener al menos un cifrado.

¿Se admite ECDSA en el dispositivo Citrix ADC?

ECDSA es compatible con las siguientes plataformas Citrix ADC. Para obtener información detallada sobre las compilaciones compatibles, consulte la Tabla 1 y la Tabla 2 de Ciphers disponibles en los dispositivos Citrix ADC.

- Dispositivos Citrix ADC MPX y SDX con chips N3
- Citrix ADC MPX 5900/8900/15000/26000
- Citrix ADC SDX 8900/15000
- Dispositivos Citrix ADC VPX

¿El dispositivo Citrix ADC VPX admite los cifrados AES-GCM/SHA2 en el front-end?

Sí, los cifrados AES-GCM/SHA2 se admiten en el dispositivo Citrix ADC VPX. Para obtener información detallada sobre las compilaciones compatibles, consulte Cifrados disponibles en los dispositivos Citrix ADC.

Certificados

¿Está disponible el nombre distintivo de un certificado de cliente durante la duración de la sesión de usuario?

Sí. Puede acceder al nombre distintivo del certificado de cliente en las solicitudes posteriores durante la sesión de usuario. Es decir, incluso después de que se haya completado el apretón de manos SSL y el navegador no vuelva a enviar el certificado. Utilice una variable y una asignación tal y como se detalla en la siguiente configuración de ejemplo:

Ejemplo:

```
add ns variable v2 -type ”text(100)”

add ns assignment a1 -variable ”$v2” -set       ”CLIENT.SSL.CLIENT_CERT
   .SUBJECT.TYPECAST_NVLIST_T('=','/').VALUE(”CN”)”

add rewrite action act1 insert_http_header subject ”$v2”  // example:
   to insert the distinguished name in the header

add rewrite policy pol1 true a1

add rewrite policy pol2 true act1

bind rewrite global pol1 1 next -type RES_DEFAULT

bind rewrite global pol2 2 next -type RES_DEFAULT

set rewrite param -undefAction RESET
<!--NeedCopy-->
```

¿Por qué tengo que vincular el certificado de servidor?

Vincular los certificados de servidor es el requisito básico para permitir que la configuración SSL procese transacciones SSL.

Para vincular el certificado de servidor a una VIP SSL, en la CLI, escriba:

```
bind ssl vserver <vServerName> -certkeyName <cert_name>
<!--NeedCopy-->
```

Para vincular el certificado de servidor a un servicio SSL, en la CLI, escriba:

```
bind ssl service <serviceName> -certkeyName <cert_name>
<!--NeedCopy-->
```

¿Cuántos certificados puedo vincular a un SSL VIP o a un servicio SSL?

En un dispositivo FIPS Citrix ADC VPX, MPX/SDX (N3) y MPX/SDX 14000 FIPS, puede enlazar dos certificados a un servidor virtual SSL o a un servicio SSL si SNI está deshabilitado. Los certificados deben ser

uno de cada uno de los tipos RSA y ECDSA. Si SNI está habilitado, puede vincular varios certificados de servidor de tipo RSA o ECDSA. En un dispositivo FIPS Citrix ADC MPX (N2) o MPX 9700, si SNI está deshabilitado, solo puede enlazar un certificado de tipo RSA. Si SNI está habilitado, puede enlazar varios certificados de servidor de tipo RSA únicamente.

¿Qué ocurre si desvinculo o sobrescribo un certificado de servidor?

Cuando desvincula o sobrescribe un certificado de servidor, finalizan todas las conexiones y sesiones SSL creadas mediante el certificado existente. Al sobrescribir un certificado existente, aparece el siguiente mensaje:

```
ERROR:

Warning: Current certificate replaces the previous binding.
<!--NeedCopy-->
```

¿Cómo instalo un certificado intermedio en un dispositivo Citrix ADC y se vincula a un certificado de servidor?

Consulte el artículo en http://support.citrix.com/article/ctx114146 para obtener información sobre la instalación de un certificado intermedio.

¿Por qué aparece un error de «recurso ya existe» cuando intento instalar un certificado en Citrix ADC?

Consulte el artículo en http://support.citrix.com/article/CTX117284 para obtener instrucciones para resolver el error «el recurso ya existe».

Quiero crear un certificado de servidor en un dispositivo Citrix ADC para probar y evaluar el producto. ¿Cuál es el procedimiento para crear un certificado de servidor?

Realice el siguiente procedimiento para crear un certificado de prueba.

Nota: Un certificado creado con este procedimiento no se puede utilizar para autenticar a todos los usuarios y navegadores. Después de utilizar el certificado para realizar pruebas, debe obtener un certificado de servidor firmado por una entidad de certificación raíz autorizada.

Para crear un certificado de servidor autofirmado:

1. Para crear un certificado de CA raíz, en la CLI, escriba:


```
create ssl rsakey /nsconfig/ssl/test-ca.key 1024

create ssl certreq /nsconfig/ssl/test-ca.csr -keyfile /nsconfig/
   ssl/test-ca.key

Enter the required information when prompted, and then type the
   following command:

create ssl cert /nsconfig/ssl/test-ca.cer /nsconfig/ssl/test-ca.
   csr ROOT_CERT -keyfile /nsconfig/ssl/test-ca.key
<!--NeedCopy-->
```

2. Realice el siguiente procedimiento para crear un certificado de servidor y firmarlo con el certificado de CA raíz que acaba de crear.

   a) Para crear la solicitud y la clave, en la CLI, escriba:

```
create ssl rsakey /nsconfig/ssl/test-server.key 1024

    create ssl certreq /nsconfig/ssl/test-server.csr -keyfile
       /nsconfig/ssl/test-server.key
<!--NeedCopy-->
```

   b) Introduzca la información requerida cuando se le solicite.

   c) Para crear un archivo de número de serie, en la CLI, escriba:

```
shell
 # echo '01' >
/nsconfig/ssl/serial.txt
 # exit
<!--NeedCopy-->
```

   d) Para crear un certificado de servidor firmado por el certificado de CA raíz creado en el paso 1, en la CLI, escriba:

```
create ssl cert /nsconfig/ssl/test-server.cer /nsconfig/ssl/
   test-server.csr SRVR_CERT -CAcert /nsconfig/ssl/test-ca.cer
    -CAkey /nsconfig/ssl/test-ca.key -CAserial /nsconfig/ssl/
   serial.txt
<!--NeedCopy-->
```


e) Para crear un par de claves de certificado Citrix ADC, que es el objeto en memoria que contiene la información del certificado de servidor para los apretones de manos SSL y el cifrado masivo, en la CLI, escriba:

```
1 add ssl certkey test-certkey -cert /nsconfig/ssl/test-server.
     cer -key /nsconfig/ssl/test-server.key
2 <!--NeedCopy-->
```

f) Para vincular el par de claves de certificado al servidor virtual SSL, en la CLI, escriba:

```
1 bind ssl vserver <vServerName> -certkeyName <cert_name>
2 <!--NeedCopy-->
```

He recibido un dispositivo Citrix ADC en el que está instalado la versión 9.0 del software NetScaler. He notado un archivo de licencia adicional en el dispositivo. ¿Hay algún cambio en la política de licencias a partir de la versión 9.0 del software NetScaler?

Sí. A partir de la versión 9.0 del software Citrix NetScaler, es posible que el dispositivo no tenga un único archivo de licencia. El número de archivos de licencia depende de la edición de versión de software Citrix ADC. Por ejemplo, si ha instalado la edición avanzada, es posible que necesite archivos de licencia adicionales para la funcionalidad completa de las distintas funciones. Sin embargo, si ha instalado la edición Premium, el dispositivo solo tiene un archivo de licencia.

¿Cómo exporto el certificado desde Internet Information Service (IIS)?

Hay muchas formas, pero mediante el siguiente método se exportan el certificado y la clave privada apropiados para el sitio web. Este procedimiento debe realizarse en el servidor IIS real.

1. Abra la herramienta de administración del Administrador de Internet Information Services (IIS).
2. Expanda el nodo de sitios web y busque el sitio web habilitado para SSL que desea servir a través del dispositivo Citrix ADC.
3. Haga clic con el botón derecho en este sitio web y, a continuación
4. Haga clic en la pestaña Seguridad de directorios y, en la sección Comunicaciones seguras de la ventana, seleccione el cuadro Ver certificado.
5. Haga clic en la pestaña Detalles y, a continuación, en Copiar en archivo.
6. En la página Bienvenido al Asistente para exportación de certificados, haga clic en Siguiente.

7. Seleccione Sí, exporte la clave privada y haga clic en Siguiente.

   Nota: La clave privada DEBE exportarse para que la descarga SSL funcione en Citrix ADC.

8. Asegúrese de que el botón de opción Intercambio de información personal -PKCS #12 esté seleccionado y active *solo* la casilla de verificación Incluir todos los certificados en la ruta de certificación si es posible. Haga clic en Siguiente.

9. Introduzca una contraseña y haga clic en Siguiente.

10. Introduzca un nombre de archivo y una ubicación y, a continuación, haga clic en Siguiente. Proporcione al archivo una extensión de.PFX.

11. Haga clic en Finalizar.

¿Cómo convierto el certificado PKCS #12 e instalarlo en Citrix ADC?

1. Mueva el archivo de certificado .PFX exportado a una ubicación desde la que se puede copiar en el dispositivo Citrix ADC. Es decir, a una máquina que permite el acceso SSH a la interfaz de administración de un dispositivo Citrix ADC. Copie el certificado en el dispositivo mediante una utilidad de copia segura como SCP.

2. Acceda al shell BSD y convierta el certificado (por ejemplo, Cert.PFX) a formato.PEM:

```
root@ns# openssl pkcs12 -in cert.PFX -out cert.PEM
<!--NeedCopy-->
```

3. Para asegurarse de que el certificado convertido está en el formato x509 correcto, compruebe que el siguiente comando no produce ningún error:

```
root@ns# openssl x509 -in cert.PEM -text
<!--NeedCopy-->
```

4. Compruebe que el archivo de certificado contiene una clave privada. Comience por emitir el siguiente comando:

```
root@ns# cat cert.PEM

Verify that the output file includes an RSA PRIVATE KEY section.

-----BEGIN RSA PRIVATE KEY-----
Mkm^s9KMs9023pz/s...
```



```
-----END RSA PRIVATE KEY-----
<!--NeedCopy-->
```

A continuación se muestra otro ejemplo de una sección CLAVE PRIVADA RSA:

```
    Bag Attributes
    1.3.6.1.4.1.311.17.2: <No Values>
    localKeyID: 01 00 00 00
    Microsoft CSP Name: Microsoft RSA SChannel Cryptographic
    Provider
    friendlyName:
    4b9cef4cc8c9b849ff5c662fd3e0ef7e_76267e3e-6183-4d45-886e-6
       e067297b38f

    Key Attributes
    X509v3 Key Usage: 10
    -----BEGIN RSA PRIVATE KEY-----
    Proc-Type: 4,ENCRYPTED
    DEK-Info: DES-EDE3-CBC,43E7ACA5F4423968
    pZJ2SfsSVqMbRRf6ug37Clua5gY0Wld4frPIxFXyJquUHr31dilW5ta3hbIaQ+
       Rg

    ... (more random characters)
    v8dMugeRplkaH2Uwt/mWBk4t71Yv7GeHmcmjafK8H8iW80ooPO3D/ENV8X4U/
       tlh

    5eU6ky3WYZ1BTy6thxxLlwAullynVXZEflNLxq1oX+ZYl6djgjE3qg==
    -----END RSA PRIVATE KEY-----
<!--NeedCopy-->
```

A continuación se muestra una sección CERTIFICADO DE SERVIDOR:

```
    Bag Attributes
    localKeyID: 01 00 00 00
    friendlyName: AG Certificate
    subject=/C=AU/ST=NSW/L=Wanniassa/O=Dave Mother
    Asiapacific/OU=Support/CN=davemother.food.lan
    issuer=/DC=lan/DC=food/CN=hotdog
    -----BEGIN CERTIFICATE-----
    MIIFiTCCBHGgAwIBAgIKCGryDgAAAAAHzANBgkqhkiG9w0BAQUFADA8MRMwEQYK


```



```
10      ... (more random characters) 5
           pLDWYVHhLkA1pSxvFjNJHRSIydWHc5ltGyKqIUcBezVaXyel94pNSUYx07NpPV
           /
11
12      MY2ovQyQZM8gGe3+lGFum0VHbv/y/gB9HhFesog=
13      -----END CERTIFICATE-----
14  <!--NeedCopy-->
```

A continuación se muestra una sección CERTIFICADO DE CA INTERMEDIATE:

```
1       Bag Attributes: <Empty Attributes>
2       subject=/DC=lan/DC=food/CN=hotdog
3       issuer=/DC=lan/DC=food/CN=hotdog
4       -----BEGIN CERTIFICATE-----
5       MIIESDCCAzCgAwIBAgIQah20fCRYTY9LRXYMIRaKGjANBgkqhkiG9w0BAQUFADA8
6
7       ... (more random characters)
           Nt0nksawDnbKo86rQcNnY5xUs7c7pj2zxj/IOsgNHUp5W6dDI9pQoqFFaDk
           =
8
9       -----END CERTIFICATE-----
10  <!--NeedCopy-->
```

Pueden seguirse otros certificados de CA intermedia, según la ruta de certificación del certificado exportado.

5. Abrir el archivo.PEM en un editor de texto
6. Busque la primera línea del archivo.PEM y la primera instancia de la siguiente línea y copie esas dos líneas y todas las líneas entre ellas:

```
1   -----END CERTIFICATE-----
2
3   Note: Make sure that last copied line is the first
4   -----END CERTIFICATE----- line in the .PEM file.
5
6   <!--NeedCopy-->
```

7. Pegue las líneas copiadas en un nuevo archivo. Llame al nuevo archivo de forma intuitiva, como cert-key.pem. Este par de claves de certificado es para el servidor que aloja el servicio HTTPS.

Este archivo debe contener tanto la sección denominada CLAVE PRIVADA RSA como la sección denominada SERVER CERTIFICATE del ejemplo anterior.

Nota: El archivo par de claves de certificado contiene la clave privada y debe mantenerse seguro.

8. Busque cualquier sección posterior que empiece por —BEGIN CERTIFICATE— y termine con —END CERTIFICATE— y copie cada una de estas secciones en un nuevo archivo independiente.

   Estas secciones corresponden a certificados de CA de confianza que se han incluido en la ruta de certificación. Estas secciones deben copiarse y pegarse en nuevos archivos individuales para estos certificados. Por ejemplo, la sección CERTIFICADO DE CA INTERMEDIATE del ejemplo anterior debe copiarse y pegarse en un nuevo archivo).

   Para varios certificados de CA intermedios del archivo original, cree archivos para cada certificado de CA intermedia en el orden en que aparecen en el archivo. Realice un seguimiento (utilizando los nombres de archivo apropiados) del orden en que aparecen los certificados, ya que deben vincularse en el orden correcto en un paso posterior.

9. Copie el archivo de clave de certificado (cert-key.pem) y cualquier archivo de certificado de CA adicional en el directorio /nsconfig/ssl del dispositivo Citrix ADC.
10. Salga del shell BSD y acceda al mensaje de Citrix ADC.
11. Siga los pasos descritos en «Instalar los archivos de clave de certificado en el dispositivo» para instalar la clave/certificado una vez cargado en el dispositivo.

¿Cómo convierto el certificado PKCS #7 e instalarlo en el dispositivo Citrix ADC?

Puede utilizar OpenSSL para convertir un certificado PKCS #7 a un formato reconocible por el dispositivo Citrix ADC. El procedimiento es idéntico al procedimiento de los certificados PKCS #12, excepto que invoca OpenSSL con parámetros diferentes. Los pasos para convertir los certificados PKCS #7 son los siguientes:

1. Copie el certificado en el dispositivo mediante una utilidad de copia segura, como SCP.
2. Convierta el certificado (por ejemplo, Cert.p7b) a formato PEM:

```
1 openssl pkcs7 -inform DER -in cert.p7b -print_certs -text -out
     cert.pem
2 <!--NeedCopy-->
```

3. Siga los pasos 3 a 7 tal y como se describe en la respuesta de los certificados PKCS #12.
   Nota: Antes de cargar el certificado PKCS #7 convertido en el dispositivo, compruebe que contiene una clave privada, exactamente como se describe en el paso 3 del procedimiento PKCS

#12. Los certificados PKCS #7, en particular los certificados exportados desde IIS, no suelen contener una clave privada.

Cuando vinculo un cifrado a un servidor virtual o servicio mediante el comando bind cipher, veo el mensaje de error «Comando obsoleto. «?

El comando para vincular un cifrado a un servidor o servicio virtual ha cambiado.

Utilice el `bind ssl vserver <vsername> -ciphername <ciphername>` comando para vincular un cifrado SSL a un servidor virtual SSL.

Utilice el `bind ssl service <serviceName> -ciphername <ciphername>` comando para vincular un cifrado SSL a un servicio SSL.

Nota: Los nuevos cifrados y grupos de cifrado se añaden a la lista existente y no se reemplazan.

¿Por qué no puedo crear un grupo de cifrado y enlazar cifrados a él mediante el comando add cifrado?

La funcionalidad del comando add cipher ha cambiado en la versión 10. El comando solo crea un grupo de cifrado. Para añadir cifrados al grupo, utilice el comando de cifrado bind.

OpenSSL

¿Cómo uso OpenSSL para convertir certificados entre PEM y DER?

Para utilizar OpenSSL, debe tener una instalación funcional del software OpenSSL y poder ejecutar OpenSSL desde la línea de comandos.

Los certificados x509 y las claves RSA se pueden almacenar en varios formatos diferentes.

Dos formatos comunes son:

- DER (formato binario utilizado principalmente por las plataformas Java y Macintosh)
- PEM (representación base64 de DER con información de encabezado y pie de página, que se utiliza principalmente en las plataformas UNIX y Linux).

Una clave y el certificado correspondiente, además del certificado raíz y cualquier certificado intermedio, también se pueden almacenar en un único archivo PKCS #12 (.P12, .PFX).

Procedimiento

Utilice el comando **OpenSSL** para convertir entre formatos de la siguiente manera:

1. Para convertir un certificado de PEM a DER:


```
x509 -in input.crt -inform PEM -out output.crt -outform DER
<!--NeedCopy-->
```

2. Para convertir un certificado de DER a PEM:

```
x509 -in input.crt -inform DER -out output.crt -outform PEM
<!--NeedCopy-->
```

3. Para convertir una clave de PEM a DER:

```
rsa -in input.key -inform PEM -out output.key -outform DER
<!--NeedCopy-->
```

4. Para convertir una clave de DER a PEM:

```
rsa -in input.key -inform DER -out output.key -outform PEM
<!--NeedCopy-->
```

Nota: Si la clave que va a importar está cifrada con un cifrado simétrico compatible, se le pedirá que introduzca la frase de contraseña.

Nota: Para convertir una clave hacia o desde el formato NET obsoleto (servidor Netscape), sustituya NET por PEM o DER según corresponda. La clave almacenada se cifra en un cifrado simétrico RC4 débil sin sal, por lo que se solicita una frase de contraseña. Se acepta una frase de contraseña en blanco.

Límites del sistema

¿Cuáles son los números importantes que hay que recordar?

1. Crear solicitud de certificado:
   - Nombre de archivo de solicitud: máximo 63 caracteres
   - Nombre de archivo clave: máximo 63 caracteres
   - Frase de contraseña PEM (para clave cifrada): máximo 31 caracteres
   - Nombre común: máximo 63 caracteres
   - Ciudad: 127 caracteres como máximo
   - Nombre de la organización: máximo 63 caracteres
   - Nombre del estado/provincia: máximo 63 caracteres

- Dirección de correo electrónico: máximo 39 caracteres
- Unidad organizativa: 63 caracteres como máximo
- Contraseña de desafío: máximo 20 caracteres
- Nombre de la empresa: Maximum 127 characters

2. Crear certificado:

   - Nombre de archivo de certificado: 63 caracteres como máximo
   - Nombre del archivo de solicitud de certificado: máximo 63 caracteres
   - Nombre de archivo clave: máximo 63 caracteres
   - Frase de contraseña PEM: máximo 31 caracteres
   - Período de validez: Máximo 3650 días
   - Nombre de archivo de certificado de CA: máximo 63 caracteres
   - Nombre de archivo clave de CA: máximo 63 caracteres
   - Frase de contraseña PEM: máximo 31 caracteres
   - Archivo de número de serie de CA: máximo 63 caracteres

3. Crear e instalar un certificado de prueba de servidor:

   - Nombre de archivo de certificado: máximo 31 caracteres
   - Nombre de dominio completo: 63 caracteres como máximo

4. Crear clave Diffie-Hellman (DH):

   - Nombre de archivo DH (con ruta): máximo 63 caracteres
   - Tamaño del parámetro DH: máximo 2048 bits

5. Importar clave PKCS12:

   - Nombre de archivo de salida: 63 caracteres como máximo
   - Nombre de archivo PKCS12: Máximo 63 caracteres
   - Contraseña de importación: máximo 31 caracteres
   - Frase de contraseña PEM: máximo 31 caracteres
   - Verificar frase de contraseña PEM: máximo 31 caracteres

6. Exportar PKCS12

   - Nombre de archivo PKCS12: Máximo 63 caracteres
   - Nombre de archivo de certificado: 63 caracteres como máximo
   - Nombre de archivo clave: máximo 63 caracteres
   - Contraseña de exportación: máximo 31 caracteres
   - Frase de contraseña PEM: máximo 31 caracteres

7. Administración de CRL:

   - Nombre de archivo de certificado de CA: máximo 63 caracteres
   - Nombre de archivo clave de CA: máximo 63 caracteres

- Contraseña del archivo de clave de CA: máximo 31 caracteres
- Nombre del archivo de índice: 63 caracteres como máximo
- Nombre de archivo de certificado: 63 caracteres como máximo

8. Crear clave RSA:

   - Nombre de archivo clave: máximo 63 caracteres
   - Tamaño de clave: máximo 4096 bits
   - Frase de contraseña PEM: máximo 31 caracteres
   - Verificar frase de contraseña: máximo 31 caracteres

9. Cambiar la configuración SSL avanzada:

   - Tamaño máximo de memoria CRL: Máximo 1024 Mbytes
   - Tiempo de espera del activador de cifrado (ticks de 10 mS): máximo 200
   - Recuento de paquetes desencadenador de cifrado: máximo 50
   - Tamaño de caché OCSP: máximo 512 Mbytes

10. Certificado de instalación:

    - Nombre del par de claves de certificado: máximo 31 caracteres
    - Nombre de archivo de certificado: 63 caracteres como máximo
    - Nombre de archivo de clave privada: 63 caracteres como máximo
    - Contraseña: máximo 31 caracteres
    - Período de notificación: máximo 100

11. Crear grupo de cifrado:

    - Nombre del grupo de cifrado: máximo 39 caracteres

12. Crear CRL:

    - Nombre CRL: máximo 31 caracteres
    - Archivo CRL: máximo 63 caracteres
    - URL: 127 caracteres como máximo
    - DN base: 127 caracteres como máximo
    - DN de enlace: 127 caracteres como máximo
    - Contraseña: máximo 31 caracteres
    - Días: Máximo 31

13. Crear política SSL:

    - Nombre: Máximo 127 caracteres

14. Crear acción SSL:

    - Nombre: Máximo 127 caracteres

15. Crear respondedor OCSP:

- Nombre: Máximo 32 caracteres
- URL: 128 caracteres como máximo
- Profundidad de procesamiento por lotes: máximo 8
- Retardo de procesamiento por lotes: Máximo 10000
- Sesgo producido a tiempo: máximo 86400
- Tiempo de espera de solicitud: Máximo 120000

16. Crear servidor virtual:

    - Nombre: Máximo 127 caracteres
    - URL de redirección: 127 caracteres como máximo
    - Tiempo de espera del cliente: máximo 31536000 segundos

17. Crear servicio:

    - Nombre: Máximo 127 caracteres
    - Tiempo de espera de inactividad (segundos):
      Cliente: Máximo 31536000
      Servidor: Máximo 31536000

18. Crear grupo de servicios:

    - Nombre del grupo de servicios: 127 caracteres como máximo
    - ID del servidor: Máximo 4294967295
    - Tiempo de espera de inactividad (segundos):
      Cliente: Valor máximo 31536000
      Servidor: máximo 31536000

19. Crear monitor:

    - Nombre: Máximo 31 caracteres

20. Crear servidor:

    - Nombre del servidor: máximo 127 caracteres
    - Nombre de dominio: 255 caracteres como máximo
    - Resolver reintento: máximo 20939 segundos

Inspección de contenido

February 16, 2021

En los últimos tiempos, hay una expansión de tipos de dispositivos para mostrar varios contenidos multimedia. Los tipos de dispositivos pueden ser de teléfonos móviles a tabletas y escritorios. Los proveedores de infraestructura intermedia necesitan transformar el contenido original de un servidor

web a un formato adecuado para el dispositivo que solicita el contenido. Los dispositivos externos inspeccionan el contenido que transcodifica y lo envían de vuelta al cliente. El protocolo comúnmente utilizado para lograr esto es ICAP. ICAP permite que el dispositivo Citrix ADC se instale en varias implementaciones. ICAP utiliza la técnica de inspección de contenido que inspecciona los datos en busca de malware y problemas de seguridad.

> **Nota**
>
> HTTP/2 no es compatible con la inspección de contenido. Es posible que las aplicaciones que utilizan HTTP/2 no funcionen correctamente si el tráfico se envía a través de la inspección de contenido.

ICAP para inspección remota de contenido

May 8, 2022

El Protocolo de adaptación de contenido de Internet (ICAP) es un protocolo simple y ligero para ejecutar el servicio de transformación de valor agregado en mensajes HTTP. En un caso típico, un cliente ICAP reenvía las solicitudes y respuestas HTTP a uno o más servidores ICAP para su procesamiento. Los servidores ICAP realizan la transformación del contenido de las solicitudes y devuelven las respuestas con las medidas adecuadas para realizar la solicitud o respuesta.

ICAP en un dispositivo Citrix ADC

En una configuración de Citrix ADC, el dispositivo actúa como un cliente ICAP que interopera con servidores ICAP de terceros (como antimalware y Data Loss Protection [DLP]). Cuando el dispositivo recibe un tráfico web entrante, el dispositivo intercepta el tráfico y utiliza una directiva de inspección de contenido para evaluar si la solicitud HTTP necesita un procesamiento ICAP. En caso afirmativo, el dispositivo descifra y envía el mensaje como texto sin formato a los servidores ICAP. Los servidores ICAP ejecutan el servicio de transformación de contenido en el mensaje de solicitud y devuelven una respuesta al dispositivo. Los mensajes adaptados pueden ser una solicitud HTTP o una respuesta HTTP. Si el dispositivo interopera con varios servidores ICAP, el dispositivo realiza el equilibrio de carga de los servidores ICAP. Este caso ocurre cuando un servidor ICAP no es suficiente para gestionar toda la carga de tráfico. Una vez que los servidores ICAP devuelven un mensaje modificado, el dispositivo reenvía el mensaje modificado al servidor de origen back-end.

El dispositivo Citrix ADC también proporciona un servicio ICAP seguro si el tráfico entrante es de tipo HTTPS. El dispositivo utiliza un servicio TCP basado en SSL para establecer una conexión segura entre el dispositivo y los servidores ICAP.

Cómo funciona la modificación de solicitudes ICAP (REQMOD)

En el modo de modificación de solicitudes (REQMOD), el dispositivo Citrix ADC reenvía la solicitud HTTP recibida del cliente al servidor ICAP. El servidor ICAP realiza una de las siguientes acciones:

1. Devuelve una versión modificada de la solicitud y el dispositivo, a su vez, envía la solicitud modificada al servidor de origen back-end o canaliza la solicitud modificada a otro servidor ICAP.
2. Responde con un mensaje que indica que no se requiere adaptación.
3. Devuelve un error y el dispositivo, a su vez, devuelve el mensaje de error al usuario.

Cómo funciona la modificación de respuestas ICAP (RESPMOD)

En el modo de modificación de respuestas (RESPMOD), el dispositivo Citrix ADC envía una respuesta HTTP al servidor ICAP (la respuesta enviada por el dispositivo suele ser la respuesta enviada por el servidor de origen). El servidor ICAP realiza una de las siguientes acciones:

1. Envía una versión modificada de la respuesta y el dispositivo, a su vez, envía la respuesta al usuario o canaliza la respuesta a otro servidor ICAP.
2. Responde con un mensaje que indica que no se requiere adaptación.
3. Devuelve un error y el dispositivo, a su vez, envía el mensaje de error al usuario.

Licencia ICAP

La función ICAP funciona en una configuración independiente o de alta disponibilidad de Citrix ADC con la edición de licencia Citrix ADC Premium o Advanced.

Configurar ICAP para el servicio de transformación de contenido

Para utilizar ICAP para el servicio de transformación de contenido, primero debe habilitar las funciones de inspección de contenido y equilibrio de carga. Una vez que habilite las funciones, podrá completar las siguientes tareas

Para habilitar la inspección de contenido

Si desea que el dispositivo Citrix ADC actúe como cliente ICAP, primero debe habilitar las funciones de inspección de contenido y equilibrio de carga.

En el símbolo del sistema, escriba:

```
enable ns feature contentInspection LoadBalancing
<!--NeedCopy-->
```


Agregar perfil ICAP

Las configuraciones ICAP para un dispositivo Citrix ADC se especifican en una entidad denominada perfil ICAP. El perfil tiene una colección de configuraciones de ICAP. La configuración incluye parámetros para generar dinámicamente una solicitud ICAP, recibir la respuesta ICAP y registrar los datos de inspección de contenido.

Para generar dinámicamente una solicitud ICAP al servidor ICAP, se agrega un nuevo parámetro, "InsertHttpRequest", al perfil ICAP. Si se configura este parámetro, el dispositivo toma el valor configurado como expresión de directiva y evalúa la expresión e incluye el resultado como una solicitud o respuesta HTTP encapsulada y, a continuación, lo envía al servidor ICAP. Además, se puede configurar un nuevo parámetro "InserticAPHeaders" para evaluar e incluir dinámicamente los encabezados ICAP.

Cuando el dispositivo envía una solicitud ICAP y no recibe una respuesta al servidor ICAP, la conexión deja de responder. Ocurre hasta que el servidor ICAP envía una respuesta o se libera una sesión. El comportamiento se puede controlar configurando la opción de tiempo de espera de respuesta ICAP. Puede establecer un parámetro de tiempo de espera de solicitud para la acción si hay una respuesta ICAP retrasada. Si el dispositivo Citrix ADC no recibe una respuesta dentro del tiempo de espera de solicitud configurado, se lleva a cabo la acción de tiempo de espera de solicitud.

reqTimeoutAction: Los valores posibles son BYPASS, RESET, DROP.
BYPASS: Ignora la respuesta del servidor ICAP remoto y envía la solicitud/respuesta al cliente/servidor.
RESET (predeterminado): Para restablecer la conexión del cliente, ciérrela.
DROP: descarta la solicitud sin enviar una respuesta al usuario

Para evaluar una respuesta ICAP, se utiliza una nueva expresión de directiva `ICAP.RES` en la expresión de devolución de llamada de inspección de contenido. Esta expresión evalúa la respuesta ICAP de forma similar a la expresión `HTTP.RES` en una `HTTP_CALLOUT`.

Por ejemplo, cuando un dispositivo Citrix ADC recibe una solicitud HTTP para un servicio alojado detrás de la dirección IP virtual de Citrix ADC, es posible que el dispositivo tenga que comprobar la autenticación del cliente con un servidor externo y realizar una acción.

En el símbolo del sistema, escriba:

```
add ns icapProfile <name> [-preview ( ENABLED | DISABLED )][-previewLength
 <positive_integer>] -uri <string> [-hostHeader <string>] [-userAgent <
string>] -Mode ( REQMOD | RESPMOD )[-queryParams <string>] [-connectionKeepAlive
 ( ENABLED | DISABLED )][-allow204 ( ENABLED | DISABLED )] [-insertICAPHeaders
 <string>][-insertHTTPRequest <string>] [-reqTimeout <positive_integer>][-
reqTimeoutAction <reqTimeoutAction>] [-logAction <string>]
```

Ejemplo:


```
add icapprofile reqmod-profile -mode RESPMOD -uri “/req_scan” -hostHeader “Webroot.reqsca” -useragent “NS_SWG-Proxy”

add ns icapProfile icap_prof1 -uri ”/example”-Mode REQMOD -reqtimeout 4 -reqtimeoutaction BYPASS

> add icapProfile reqmode-profile -uri '/example'-mode REQMOD -insertHTTPRequest q{ HTTP.REQ.METHOD + ””+ HTTP.REQ.URL + ”HTTP/1.1\r\n”+ ”Host: ”+ HTTP.REQ.HOSTNAME + ”\r\n\r\n”}
```

Registrar acción de inspección de contenido ICAP

Para generar dinámicamente registros de flujo de registro de inspección de contenido o registros SYSLOG, puede usar la expresión de directiva basada en ICAP.RES en la respuesta ICAP. Este parámetro se puede configurar en el perfil ICAP para configurar la expresión de directiva a fin de generar los registros dinámicos.

En el símbolo del sistema, escriba:

```
add audit messageaction icap_log_expr INFORMATIONAL icap.res.full_header

set icapProfile reqmode-profile -logAction messageaction
```

Agregar el servicio ICAP como un servicio TCP o SSL_TCP

Después de habilitar la función de inspección de contenido, debe agregar un servicio ICAP para los servidores ICAP que formará parte de la configuración del equilibrio de carga. El servicio que agrega proporciona la conexión ICAP entre el dispositivo Citrix ADC y los servidores virtuales de equilibrio de carga.

Nota: Como administrador, puede agregar un servicio ICAP y configurar directamente la dirección IP del servidor ICAP en la acción Inspección de contenido.

En el símbolo del sistema, escriba lo siguiente:

```
1 add service <name> <IP> <serviceType> <port>
2 <!--NeedCopy-->
```

Ejemplo:

```
add service icapsv1 10.10.10.10 SSL_TCP 1345

add service icapsv2 10.10.10.11 SSL_TCP 1345
```


Agregar un servidor virtual de equilibrio de carga basado en TCP o SSL_TCP

Después de crear un servicio ICAP, debe crear un servidor virtual para aceptar el tráfico ICAP y equilibrar la carga de los servidores ICAP.

> **Nota:**
>
> También puede usar un servicio TCP basado en SSL a través de un canal seguro. Utiliza un servicio SSL_TCP y se vincula a la acción Inspección de contenido.

En el símbolo del sistema, escriba lo siguiente:

```
add lb vserver <name> <serviceType> <port>
<!--NeedCopy-->
```

Ejemplo:

```
add lb vserver vicap TCP 0.0.0.0.0 - persistenceType NONE -cltTimeout
    9000

add lb vserver vicap SSL_TCP 0.0.0.0 0 - persistenceType NONE -
    cltTimeout 9000
<!--NeedCopy-->
```

Vincular el servicio ICAP al servidor virtual de equilibrio de carga

Después de crear un servicio ICAP y un servidor virtual, debe vincular el servicio ICAP al servidor virtual.

En el símbolo del sistema, escriba lo siguiente:

```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Ejemplo:

```
bind lb vserver vicap icapsv1
<!--NeedCopy-->
```


Agregar acción de inspección de contenido

Después de habilitar la función de inspección de contenido, debe agregar una acción ICAP para gestionar la información de la solicitud ICAP. El perfil y los servicios ICAP o el servidor virtual de equilibrio de carga que se crean están vinculados a la acción ICAP. Si el servidor ICAP está inactivo, puede configurar el parámetro `ifserverdown` para que el dispositivo realice cualquiera de las siguientes acciones.

CONTINUAR: Si el usuario desea omitir la inspección de contenido cuando el servidor remoto está inactivo, puede elegir la acción "CONTINUAR" de forma predeterminada.
RESET (predeterminado): esta acción responde al cliente cerrando la conexión con RST.
DROP: Esta acción descarta silenciosamente los paquetes sin enviar una respuesta al usuario.

En el símbolo del sistema, escriba lo siguiente:

```
add contentInspection action <name> -type ICAP -serverName <string> -
    icapProfileName <string>

add ContentInspection action <name> -type ICAP -serverip <ip> -
    serverport <port> -icapProfileName <string>
<!--NeedCopy-->
```

> **Nota:**
>
> Si puede configurar el servicio ICAP en lugar de un servidor virtual de equilibrio de carga, puede mencionar el nombre del servicio en la opción `\<-serverip>`. Al agregar la acción de inspección de contenido, el servicio TCP se crea automáticamente para la dirección IP dada con el puerto 1344 y se utiliza para la comunicación ICAP.

Ejemplo:

```
add ContentInspection action ci_act_lb -type ICAP -serverName vicap -
    icapProfileName icap_reqmod

add ContentInspection action ci_act_svc -type ICAP -serverName icapsv1
    -icapProfileName icap_reqmod

add ContentInspection action ci_act_svc -type ICAP -serverip 1.1.1.1 -
    serverport 1344 -icapProfileName icap_reqmod
<!--NeedCopy-->
```


Agregar directivas de inspección de contenido

Después de crear una acción de inspección de contenido, debe crear directivas de inspección de contenido para evaluar las solicitudes de procesamiento ICAP y registro de auditoría. La directiva se basa en una regla que consiste en una o más expresiones. La regla está asociada a la acción de inspección de contenido que se asocia si una solicitud coincide con la regla.

En el símbolo del sistema, escriba lo siguiente:

```
add contentInspection policy <name> -rule <expression> -action <string>
<!--NeedCopy-->
```

Ejemplo:

```
add ContentInspection policy ci_pol_basic - rule true - action
    ci_act_svc

add ContentInspection policy ci_pol_HTTP - rule HTTP.REQ.URL.CONTAINS(
    "html" ) - action ci_act_svc
<!--NeedCopy-->
```

Vincular las directivas de inspección de contenido al servidor virtual de conmutación de contenido o equilibrio de carga

Para poner en práctica una directiva ICAP, debe vincularla globalmente o vincularla a un servidor virtual de conmutación de contenido o equilibrio de carga, que se encargue de la aplicación. Cuando vincula la directiva, debe asignarle una prioridad. La prioridad determina el orden en que se evalúan las directivas que defina.

> **Nota:**
>
> El servidor virtual de la aplicación debe ser de tipo: HTTP/SSL/CS-PROXY.

Para obtener información sobre cómo configurar una configuración de equilibrio de carga para reenviar el tráfico al servidor de origen back-end tras la transformación del contenido, consulte Equilibrio de carga.

Configurar el servicio ICAP seguro

Para establecer una conexión segura entre el dispositivo Citrix ADC y los servidores web ICAP, el dispositivo utiliza un servicio TCP basado en SSL o un servidor virtual de equilibrio de carga enlazado a una acción ICAP.

Para establecer una conexión ICAP segura, realice las siguientes tareas:

1. Agregue el servicio TCP basado en SSL.
2. Enlace el servicio TCP basado en SSL al servidor virtual de equilibrio de carga de tipo TCP o SSL_TCP.
3. Enlace el servicio TCP basado en SSL o el servidor virtual de equilibrio de carga a la acción de inspección de contenido.

Agregue el servicio TCP basado en SSL al servidor virtual de equilibrio de carga

Para establecer una conexión segura entre el dispositivo Citrix ADC y los servidores web ICAP, el dispositivo utiliza un servicio TCP basado en SSL o un servidor virtual de equilibrio de carga enlazado a una acción ICAP.

Para establecer una conexión ICAP segura, realice las siguientes tareas:

1. Agregue el servicio TCP basado en SSL.
2. Enlace el servicio TCP basado en SSL al servidor virtual de equilibrio de carga de tipo TCP o SSL_TCP.

Enlace el servicio TCP basado en SSL o el servidor virtual de equilibrio de carga a la acción de inspección de contenido

Agregue el servicio TCP basado en SSL al servidor virtual de equilibrio de carga

Después de habilitar la función de inspección de contenido, debe agregar un servicio ICAP seguro que formará parte de la configuración del equilibrio de carga. El servicio que agrega proporciona una conexión ICAP segura entre el dispositivo Citrix ADC y los servidores virtuales de equilibrio de carga.

En el símbolo del sistema, escriba lo siguiente:

```
add service <name> <IP> <serviceType> <port>
<!--NeedCopy-->
```

Ejemplo:

```
add service icapsv2 10.102.29.200 SSL_TCP 1344 -gslb NONE -maxclient
    0 -maxReq 0 -cip DISABLED -usip NO -useproxport YES -sp ON -
    cltTimeout 9000 -svrTimeout 9000 -CKA NO -TCPB NO -CMP NO
<!--NeedCopy-->
```


Enlace el servicio TCP basado en SSL al servidor virtual de equilibrio de carga SSL_TCP o TCP

Después de crear un servicio ICAP seguro, debe vincular el servicio al servidor virtual de equilibrio de carga. Es necesario si utiliza un servidor virtual de equilibrio de carga para equilibrar la carga de los servidores ICAP.

En el símbolo del sistema, escriba lo siguiente:

```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Ejemplo:

```
bind lb vserver vicap icapsv2
<!--NeedCopy-->
```

Vincular el servicio TCP basado en SSL o el servidor virtual de equilibrio de carga a la acción de inspección de contenido

Agregue una acción ICAP para gestionar la información de la solicitud ICAP y también vincular el servicio TCP basado en SSL a la acción.

En el símbolo del sistema, escriba lo siguiente:

```
add contentInspection action <name> -type ICAP -serverName <string> -
    icapProfileName <string>
<!--NeedCopy-->
```

Ejemplo:

```
add ContentInspection action ci_act_svc -type ICAP -serverName icapsv2
    -icapProfileName icap_reqmod

add ContentInspection action ci_act_svc -type ICAP -serverName vicap -
    icapProfileName icap_reqmod
<!--NeedCopy-->
```


Configurar el protocolo ICAP mediante la interfaz gráfica de usuario

1. Vaya a **Equilibrio de carga** > **Servicios** y haga clic en **Agregar**.
2. En la página **Servicios**, introduzca los detalles del servicio.
3. Vaya a **Equilibrio de carga** > **Servidores virtuales**. Agregue un servidor virtual de equilibrio de carga de tipo HTTP/SSL. O bien, puede seleccionar un servidor virtual y hacer clic en **Modificar**.
4. Después de introducir los detalles básicos del servidor, haga clic en **Continuar**.
5. En la sección **Configuración avanzada**, haga clic en **Directivas**.
6. Vaya a la sección **Directivas** y haga clic en el icono del **lápiz** para configurar la directiva de inspección de contenido.
7. En la página **Elegir directiva**, seleccione **Inspección de contenido**. Haga clic en **Continue**.
8. En la sección **Vinculación de directivas**, haga clic en **+** para agregar una directiva de inspección de contenido.
9. En la página **Crear directiva ICAP**, introduzca un nombre para la directiva.
10. En el campo **Acción**, haga clic en el signo "+" para agregar una acción ICAP.
11. En la página **Crear acción ICAP**, introduzca un nombre para la acción.
12. Introduzca un nombre para la acción.
13. En el campo **Nombre del servidor**, introduzca el nombre del servicio TCP ya creado.
14. En el campo **Perfil ICAP**, haga clic en el signo "+" para agregar un perfil ICAP.
15. En la página **Crear perfil ICAP**, introduzca un nombre de perfil, URI y MODE.
16. Haga clic en **Create**.
17. En la página **Crear acción ICAP**, haga clic en **Crear**.
18. En la página **Crear directiva ICAP**, escriba "true" en el **Editor de expresiones** y, a continuación, haga clic en **Crear**.
19. Haga clic en **Bind**.
20. Cuando se le pida que active la función de inspección de contenido, haga clic en **Sí**.
21. Haga clic en **Listo**.

Para obtener información sobre la configuración de la GUI de Citrix ADC para equilibrar la carga y reenviar el tráfico al servidor de origen back-end después de la transformación del contenido, consulte Equilibrio de carga.

Configure el protocolo ICAP seguro mediante la interfaz gráfica de usuario

1. Vaya a **Equilibrio de carga** > **Servicios** y haga clic en **Agregar**.
2. En la página **Servicios**, introduzca los detalles del servicio.
3. Vaya a **Equilibrio de carga** > **Servidores virtuales**. Agregue un servidor virtual de tipo HTTP/SSL. O bien, puede seleccionar un servidor virtual y hacer clic en **Modificar**.
4. Después de introducir los detalles básicos del servidor, haga clic en **Continuar**.
5. En la sección **Configuración avanzada**, haga clic en **Directivas**.

6. Vaya a la sección **Directivas** y haga clic en el icono del **lápiz** para configurar la directiva de inspección de contenido.
7. En la página **Elegir directiva**, seleccione **Inspección de contenido**. Haga clic en **Continue**.
8. En la sección **Vinculación de directivas**, haga clic en **+** para agregar una directiva de inspección de contenido.
9. En la página **Crear directiva ICAP**, introduzca un nombre para la directiva.
10. En el campo **Acción**, haga clic en el signo "+" para agregar una acción ICAP.
11. En la página **Crear acción ICAP**, introduzca un nombre para la acción.
12. Introduzca un nombre para la acción.
13. En el campo **Nombre del servidor**, introduzca el nombre del servicio TCP_SSL ya creado.
14. En el campo **Perfil ICAP**, haga clic en el signo "+" para agregar un perfil ICAP.
15. En la página **Crear perfil ICAP**, introduzca un nombre de perfil, URI y MODE.
16. Haga clic en **Create**.
17. En la página **Crear acción ICAP**, haga clic en **Crear**.
18. En la página **Crear directiva ICAP**, escriba "true" en el **Editor de expresiones** y, a continuación, haga clic en **Crear**.
19. Haga clic en **Bind**.
20. Cuando se le pida que active la función de inspección de contenido, haga clic en **Sí**.
21. Haga clic en **Listo**.

Soporte de registro de auditoría para la inspección remota de contenido

Si se inspecciona el contenido de una solicitud entrante o una respuesta saliente, el dispositivo Citrix ADC registra los detalles de ICAP. El dispositivo almacena los detalles como un mensaje de registro en el archivo ns.log.

Por lo general, cada mensaje de registro contiene los siguientes detalles:

```
<Source IP> <Destination IP> <Domain> <ICAP server IP><ICAP Mode> <
   Service URI> <ICAP response> <Policy action>
<!--NeedCopy-->
```

Limitación: el modo de transmisión de App Firewall no se admite con la función de inspección de contenido.

Ejemplo de mensaje de registro de solicitudes de contenido inspeccionado:

```
Apr 18 14:45:41 <local0.info> 10.106.97.104 04/18/2018:14:45:41 GMT 0-
   PPE-0 : default CI ICAP_LOG 788 0 : Source 10.102.1.98:39048 -
   Destination 10.106.97.89:8011 - Domain 10.106.97.89 - Content-Type
```



```
    application/x-www-form-urlencoded - ICAP Server 10.106.97.99:1344 -
    Mode REQMOD - Service /example - Response 204 - Action FORWARD
<!--NeedCopy-->
```

Ejemplo de mensaje de registro de respuesta inspeccionado por contenido:

```
Apr 18 12:34:08 <local0.info> 10.106.97.104 04/18/2018:12:34:08 GMT 0-
    PPE-0 : default CI ICAP_LOG 71 0 : Source 10.106.97.105:18552 -
    Destination 10.106.97.99:80 - Domain NA - Content-Type NA - ICAP
    Server 10.106.97.99:1344 - Mode RESPMOD - Service /example -
    Response 400 - Action Internal Error
<!--NeedCopy-->
```

Integración de dispositivos en línea con Citrix ADC

August 20, 2021

Los dispositivos de seguridad como el sistema de prevención de intrusiones (IPS) y el firewall de próxima generación (NGFW) protegen los servidores contra ataques de red. Estos dispositivos se implementan en modo inline de capa 2 y su función principal es proteger los servidores contra ataques de red e informar de amenazas de seguridad en la red.

Para evitar amenazas vulnerables y proporcionar protección de seguridad avanzada, un dispositivo Citrix ADC está integrado con uno o varios dispositivos en línea. Los dispositivos en línea pueden ser cualquier dispositivo de seguridad como IPS, NGFW.

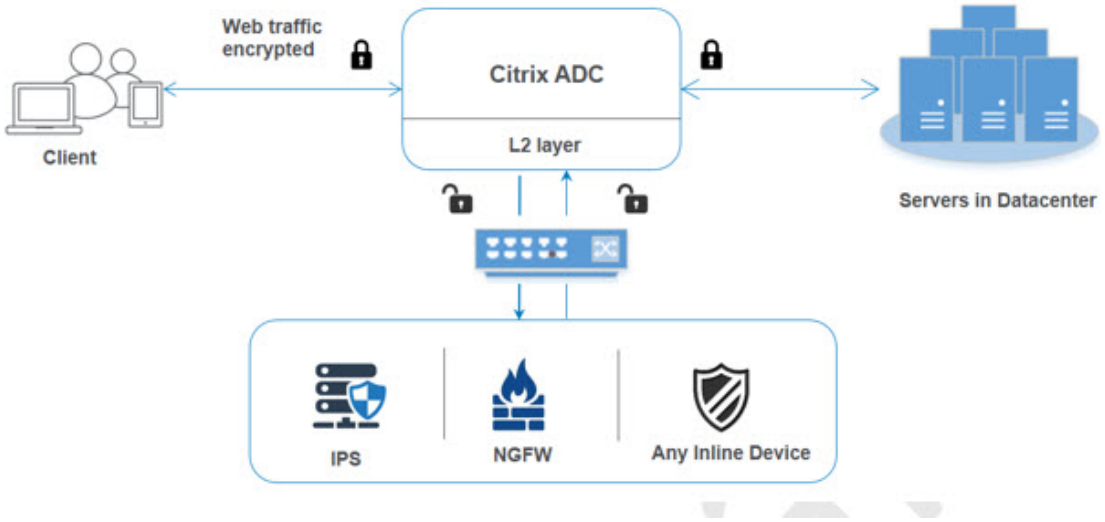
A continuación se presentan algunos de los casos de uso que se benefician de la integración de dispositivos en línea con el dispositivo Citrix ADC:

- **Inspeccionando el tráfico cifrado**. La mayoría de los dispositivos IPS y NGFW evitan el tráfico cifrado, lo que deja a los servidores vulnerables a los ataques. Un dispositivo Citrix ADC puede descifrar el tráfico y enviarlo a dispositivos en línea para su inspección. Mejora la seguridad de la red del cliente.
- **Descarga de dispositivos en línea del procesamiento TLS/SSL**. El procesamiento TLS/SSL es costoso y el problema puede dar lugar a una CPU del sistema alta en dispositivos IPS o NGFW si descifran el tráfico. Como el tráfico cifrado está creciendo a un ritmo rápido, estos sistemas no logran descifrar e inspeccionar el tráfico cifrado. Citrix ADC ayuda a descargar dispositivos en línea del procesamiento TLS/SSL. El resultado es que el dispositivo en línea admite un alto volumen de inspección de tráfico.

- **Carga de dispositivos en línea de equilibrio**. La carga del dispositivo Citrix ADC equilibra varios dispositivos en línea cuando hay un gran volumen de tráfico.
- **Selección inteligente de tráfico**. Es posible que se inspeccione el contenido de cada paquete que entra en el dispositivo, por ejemplo, la descarga de archivos de texto. El usuario puede configurar el dispositivo Citrix ADC para seleccionar tráfico específico (por ejemplo, archivos.exe) para su inspección y enviar el tráfico a dispositivos en línea para procesar los datos

Cómo se integra Citrix ADC con los dispositivos en línea

El siguiente diagrama muestra cómo se integra un dispositivo Citrix ADC con dispositivos de seguridad en línea.



Cuando integra dispositivos en línea con el dispositivo Citrix ADC, el componente interactúa según lo siguiente:

1. Un cliente envía una solicitud al dispositivo Citrix ADC.
2. El dispositivo recibe la solicitud y la envía a un dispositivo en línea basado en la evaluación de directivas.
   Nota: Si hay dos o más dispositivos en línea, la carga del dispositivo equilibra los dispositivos y envía el tráfico.
   Si el tráfico entrante es cifrado, el dispositivo descifra los datos y los envía como texto sin formato al dispositivo en línea para la inspección del contenido.
3. El dispositivo en línea inspecciona los datos en busca de amenazas y decide si quiere eliminar, restablecer o enviar los datos al dispositivo.
4. Si hay amenazas de seguridad, el dispositivo modifica los datos y los envía al dispositivo.
5. El Citrix ADC vuelve a cifrar los datos y reenvía la solicitud al servidor back-end.
6. El servidor back-end envía la respuesta al dispositivo Citrix ADC.
7. El dispositivo vuelve a descifrar los datos y los envía al dispositivo en línea para su inspección.

8. El dispositivo vuelve a cifrar los datos y envía la respuesta al cliente

Licencias de software

Para implementar la integración de dispositivos en línea, el dispositivo Citrix ADC debe aprovisionarse con una de las siguientes licencias:

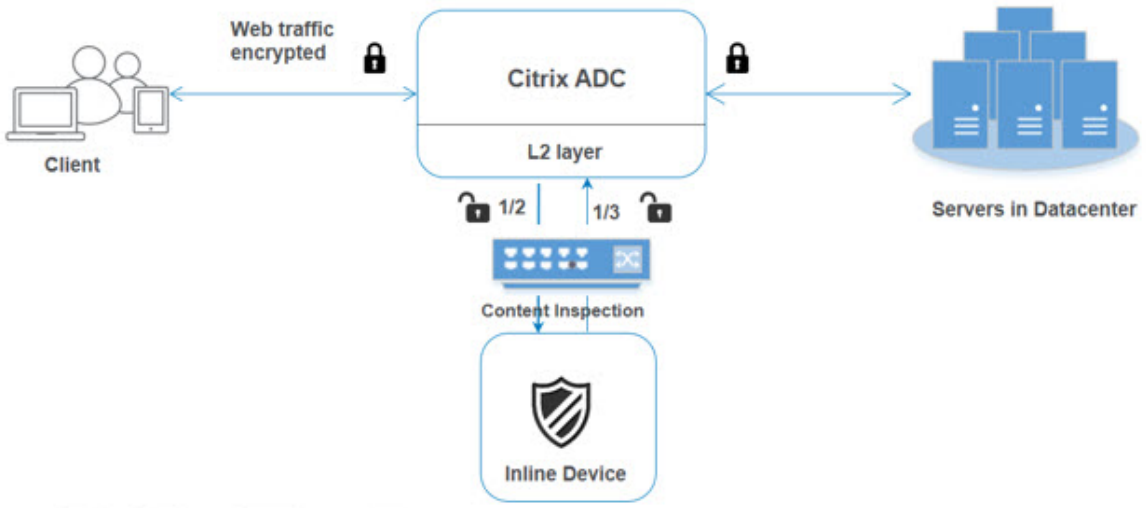
1. ADC Premium
2. ADC Avanzado
3. Telco avanzado
4. Telco Premium
5. Licencia SWG

Configuración de la integración de dispositivos en línea

Puede configurar un dispositivo Citrix ADC con un dispositivo en línea de tres maneras diferentes. Los casos de configuración son los siguientes.

Caso 1 para usar un único dispositivo en línea

Si desea integrar un dispositivo de seguridad (IPS o NGFW) en modo en línea, primero debe habilitar la función Inspección de contenido y habilitar Citrix ADC en MBF (reenvío basado en Mac) en modo global. Una vez habilitadas las funciones, debe agregar el perfil Inspección de contenido, agregar la acción Inspección de contenido para los dispositivos en línea para restablecer, bloquear o eliminar el tráfico según la inspección. A continuación, agregue la directiva de inspección de contenido para el dispositivo para decidir qué subconjunto de tráfico enviar a los dispositivos en línea. A continuación, configure el servidor virtual de equilibrio de carga con la conexión de capa 2 habilitada en el servidor. Finalmente, vincule la directiva de inspección de contenido al servidor virtual de equilibrio de carga.



Habilitar el modo MBF (reenvío basado en Mac)

Si quiere que el dispositivo Citrix ADC se integre en dispositivos integrados como IPS o firewalls, debe habilitar este modo. Para obtener más información acerca de MBF, vea el tema Configurar reenvío basado en Mac.

En el símbolo del sistema, escriba:

```
enable ns mode mbf
```

Habilitar inspección de contenido

Si desea que el dispositivo Citrix ADC descifrado y, a continuación, envíe el contenido para su inspección a los dispositivos en línea, debe habilitar las funciones Inspección de contenido y equilibrio de carga.

```
enable ns feature contentInspection LoadBalancing
```

Método de conexión Add Layer 2

Para gestionar la respuesta generada por dispositivos en línea, el dispositivo utiliza el canal VLAN como método de capa 2 (L2ConnMethod) de comunicación con dispositivos en línea.

En el símbolo del sistema, escriba:

```
set l4param -l2ConnMethod <l2ConnMethod>
```

Ejemplo

```
set l4param -l2ConnMethod VlanChannel
```

Agregar perfil de inspección de contenido para el servicio

La configuración de dispositivos en línea para un dispositivo Citrix ADC se puede especificar en una entidad denominada perfil de inspección de contenido. El perfil tiene una colección de configuraciones que explican cómo integrarse con un dispositivo en línea.

En el símbolo del sistema, escriba:

```
add contentInspection profile <name> -type InlineInspection -egressInterface
 <interface_name> -ingressInterface <interface_name>[-egressVlan <positive_integer
>] [-ingressVlan <positive_integer>]
```

Ejemplo:

```
add contentInspection profile Inline_profile1 -type InlineInspection -
ingressinterface “1/2” -egressInterface “1/3”
```


Agregar monitor IPS-TCP

Si quiere configurar monitores, agregue un monitor definido por el usuario.
Nota: Si quiere configurar monitores, debe usar un monitor personalizado. Al agregar un monitor, debe habilitar el parámetro transparente.

En el símbolo del sistema, escriba:

```
add lb monitor <monitorName> <type> [-destIP <ip_addr|ipv6_addr>] [-destPort
 <port>] [-transparent ( YES | NO )]
```

Ejemplo:

```
add lb monitor ips_tcp TCP -destIP 192.168.10.2 -destPort 80 -transparent
YES
```

Agregar un servicio

Agregar un servicio. Especifique una dirección IP ficticia que no sea propiedad de ninguno de los dispositivos, incluidos los dispositivos en línea. Establezca `use source IP address` (USIP) en YES. Ajuste `useproxyport` en NO. De forma predeterminada, la supervisión del estado está activada, enlaza el servicio a un monitor de estado y también establece la opción TRANSPARENTE en el monitor ON. En el símbolo del sistema, escriba:

```
add service <Service_name> <IP> TCP * - contentinspectionProfileName <Name>
 -healthMonitor YES -usip ON -useproxyport OFF
```

Ejemplo:

```
add service ips_service 192.168.10.2 TCP * -healthMonitor YES -usip YES -
useproxyport NO -contentInspectionProfileName ipsprof
```

Agregar un monitor de estado

De forma predeterminada, el monitor de estado está activado y también tiene la opción de desactivarlo, si es necesario. En el símbolo del sistema, escriba:

```
add lb monitor <name> TCP -destIP <ip address> -destPort 80 -transparent <
YES, NO>
```

Ejemplo:

```
add lb monitor ips_tcp TCP -destIP 192.168.10.2 -destPort 80 -transparent
YES
```


Vincular el servicio al monitor de estado

Después de configurar el monitor de estado, debe vincular el servicio al monitor de estado. En el símbolo del sistema, escriba:

```
bind service <name> -monitorName <name>
```

Ejemplo:

```
bind service ips_svc -monitorName ips_tcp
```

Agregar acción de inspección de contenido para el servicio

Después de habilitar la función Inspección de contenido y, a continuación, después de agregar el perfil y el servicio en línea, debe agregar la acción Inspección de contenido para gestionar la solicitud. En función de la acción de inspección de contenido, el dispositivo en línea puede soltar, restablecer o bloquear la acción después de inspeccionar los datos.

Si el servidor o servicio en línea está inactivo, puede configurar el `ifserverdown` parámetro en el dispositivo para realizar cualquiera de las siguientes acciones.

CONTINUAR: Si el usuario quiere omitir la inspección de contenido cuando el servidor remoto está inactivo, puede elegir la acción "CONTINUAR", como predeterminada.
RESET (predeterminado): esta acción responde al cliente cerrando la conexión con RST.
DROP: Esta acción deja caer silenciosamente los paquetes sin enviar una respuesta al usuario.

En el símbolo del sistema, escriba:

```
add contentInspection action <name> -type <type> (-serverName <string> [-
ifserverdown <ifserverdown>] [-reqTimeout <positive_integer>] [-reqTimeoutAction
 <reqTimeoutAction>]
```

```
add ContentInspection action <action_name> -type InlineINSPECTION -serverName
 Service_name/Vserver_name>
```

Ejemplo:

```
add ContentInspection action <Inline_action> -type InlineSPECTION -serverName
 Inline_service1
```

Agregar directiva de inspección de contenido para inspección

Después de crear una acción de inspección de contenido, debe agregar directivas de Inspección de contenido para evaluar las solicitudes de inspección. La directiva se basa en una regla que consta de una o más expresiones. La directiva evalúa y selecciona el tráfico para la inspección en función de la regla.

En el símbolo del sistema, escriba lo siguiente:


```
add contentInspection policy <policy_name> -rule <Rule> -action <action_name
>
```

Ejemplo

```
add contentInspection policy Inline_pol1 -rule true -action Inline_action
```

Agregar servidor virtual de cambio de contenido o equilibrio de carga de tipo HTTP/SSL

Para recibir el tráfico web, debe agregar un servidor virtual de equilibrio de carga. También debe habilitar la conexión layer2 en el servidor virtual.

En el símbolo del sistema, escriba:

```
add lb vserver <name> <vserver name> -l2Conn ON
```

Ejemplo:

```
add lb vserver HTTP_vserver HTTP 10.102.29.200 8080 -l2Conn ON
```

Vincular la directiva de inspección de contenido al servidor virtual de cambio de contenido o al servidor virtual de equilibrio de carga de tipo HTTP/SSL

Enlazar el servidor virtual de equilibrio de carga o el servidor virtual de cambio de contenido de tipo HTTP/SSL a la directiva Inspección de contenido.
En el símbolo del sistema, escriba lo siguiente:

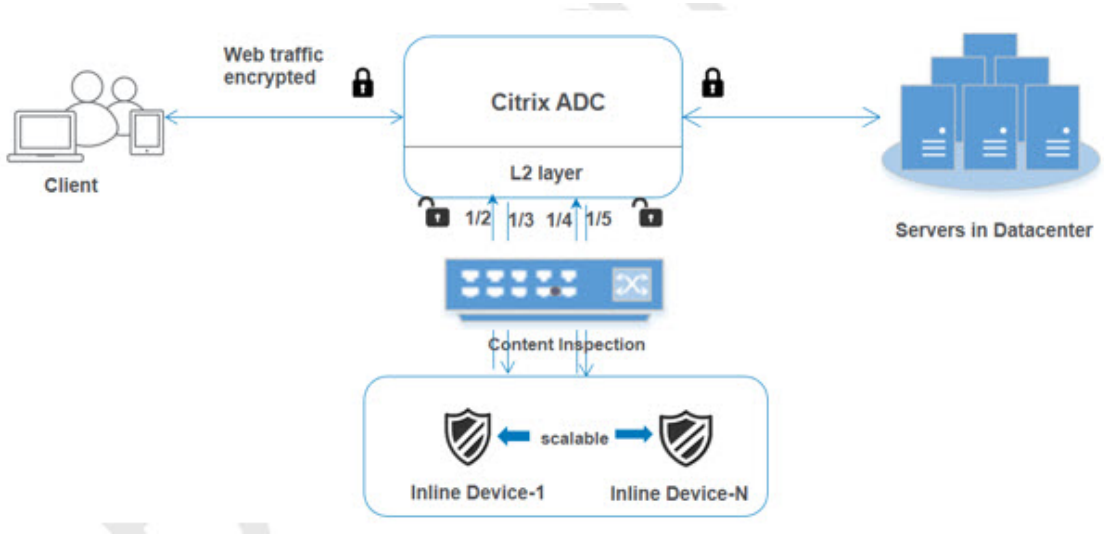
```
bind lb vserver <vserver name> -policyName < policy_name > -priority <
priority > -type <REQUEST>
```

Ejemplo:

```
bind lb vserver HTTP_vserver -policyName Inline_pol1 -priority 100 -type
REQUEST
```

Caso 2: Equilibrio de carga de varios dispositivos en línea mediante interfaces dedicadas

Si utiliza dos o más dispositivos en línea, debe equilibrar la carga de los dispositivos mediante diferentes servicios de inspección de contenido en una configuración de VLAN dedicada. En este caso, la carga del dispositivo Citrix ADC equilibra los dispositivos además de enviar un subconjunto de tráfico a cada dispositivo a través de una interfaz dedicada.
Para ver los pasos básicos de configuración, consulte el caso 1.



Agregar perfil de inspección de contenido1 para el servicio1

Las configuraciones en línea para un dispositivo Citrix ADC se pueden especificar en una entidad denominada perfil de inspección de contenido. El perfil tiene una colección de configuraciones del dispositivo. El perfil1 de inspección de contenido1 se crea para el servicio en línea 1 y la comunicación se realiza a través de interfaces dedicadas 1/2 y 1/3.

En el símbolo del sistema, escriba:

```
add contentInspection profile <name> -type InlineInspection -egressInterface
 <interface_name> -ingressInterface <interface_name>[-egressVlan <positive_integer
>] [-ingressVlan <positive_integer>]
```

Ejemplo:

```
add contentInspection profile Inline_profile1 -type InlineInspection -
ingressinterface “1/2” -egressInterface “1/3”
```

Agregar perfil de inspección de contenido2 para el servicio2

El perfil de inspección de contenido 2 se agrega para servicio2 y el dispositivo en línea se comunica con el dispositivo a través 1/4 de interfaces 1/5 dedicadas.
En el símbolo del sistema, escriba:

```
add contentInspection profile <name> -type InlineInspection -egressInterface
 <interface_name> -ingressInterface <interface_name>[-egressVlan <positive_integer
>] [-ingressVlan <positive_integer>]
```

Ejemplo:

```
add contentInspection profile Inline_profile2 -type InlineInspection -
ingressinterface “1/4” -egressInterface “1/5”
```


Agregar servicio 1 para el dispositivo en línea 1

Después de habilitar la función Inspección de contenido y agregar el perfil en línea, debe agregar un servicio en línea 1 para que el dispositivo en línea 1 forme parte de la configuración de equilibrio de carga. El servicio que se agrega proporciona todos los detalles de configuración en línea.

En el símbolo del sistema, escriba:

```
add service <Service_name_1> <Pvt_IP1> TCP * -contentInspectionProfileName
<Inline_Profile_1> -healthmonitor OFF -usip ON -useproxyport OFF
```

Ejemplo:

```
add service Inline_service1 10.102.29.200 TCP 80 -contentInspectionProfileName
 Inline_profile1 -healthmonitor OFF -usip ON -useproxyport OFF
```

Agregar servicio 2 para el dispositivo en línea 2

Después de habilitar la función Inspección de contenido y agregar el perfil en línea, debe agregar un servicio en línea 2 para el dispositivo en línea 2. El servicio que se agrega proporciona todos los detalles de configuración en línea.

En el símbolo del sistema, escriba:

```
add service <Service_name_1> <Pvt_IP1> TCP * -contentInspectionProfileName
<Inline_Profile_2> -healthmonitor OFF -usip ON -useproxyport OFF
```

Ejemplo:

```
add service Inline_service1 10.29.20.205 TCP 80 -contentInspectionProfileName
 Inline_profile2 -healthmonitor OFF -usip ON -useproxyport OFF
```

Agregar servidor virtual de equilibrio de carga

Después de agregar el perfil en línea y los servicios, debe agregar un servidor virtual de equilibrio de carga para equilibrar la carga de los servicios.

En el símbolo del sistema, escriba:

```
add lb vserver <vserver_name> TCP <Pvt_IP3> <port>
```

Ejemplo:

```
add lb vserver lb-Inline_vserver TCP *
```

Enlace el servicio 1 al servidor virtual de equilibrio de carga

Después de agregar el servidor virtual de equilibrio de carga, ahora vincule el servidor virtual de equilibrio de carga al primer servicio.

En el símbolo del sistema, escriba:

```
bind lb vserver <Vserver_name> <Service_name_1>
```

Ejemplo:

```
bind lb vserver lb-Inline_vserver Inline_service1
```

Enlace el servicio 2 al servidor virtual de equilibrio de carga

Después de agregar el servidor virtual de equilibrio de carga, ahora vincule el servidor al segundo servicio.

En el símbolo del sistema, escriba:

```
bind lb vserver <Vserver_name> <Service_name_1>
```

Ejemplo:

```
bind lb vserver lb-Inline_vserver Inline_service2
```

Agregar acción de inspección de contenido para el servicio

Después de habilitar la función Inspección de contenido, debe agregar la acción de inspección de contenido para gestionar la información de solicitud en línea. En función de la acción seleccionada, el dispositivo en línea cae, se restablece o bloquea después de examinar el subconjunto de tráfico dado.

En el símbolo del sistema, escriba:

```
add contentInspection action <name> -type <type> (-serverName <string> [-
ifserverdown <ifserverdown>] [-reqTimeout <positive_integer>] [-reqTimeoutAction
 <reqTimeoutAction>]
```

```
add ContentInspection action < action_name > -type InlineINSPECTION -
serverName Service_name/Vserver_name>
```

Ejemplo:

```
add ContentInspection action Inline_action -type InlineINSPECTION -serverName
 lb-Inline_vserver
```

Agregar directiva de inspección de contenido para inspección

Después de crear una acción Inspección de contenido, debe agregar la directiva Inspección de contenido para evaluar las solicitudes de servicio. La directiva se basa en una regla que consta de una o más expresiones. La regla está asociada a la acción de inspección de contenido asociada si una solicitud coincide con la regla.

En el símbolo del sistema, escriba lo siguiente:

```
add contentInspection policy <policy_name> -rule <Rule> -action <action_name
>
```

Ejemplo:

```
add contentInspection policy Inline_pol1 -rule true -action Inline_action
```

Agregar servidor virtual de cambio de contenido o equilibrio de carga de tipo HTTP/SSL

Agregue un servidor virtual de cambio de contenido o equilibrio de carga para aceptar tráfico web. También debe habilitar la conexión layer2 en el servidor virtual.
Para obtener más información sobre el equilibrio de cargas, consulte el tema Cómo funciona el equilibrio de cargas.

En el símbolo del sistema, escriba:

```
add lb vserver <name> <vserver name> -l2Conn ON
```

Ejemplo:

```
add lb vserver http_vserver HTTP 10.102.29.200 8080 -l2Conn ON
```

Vincular directiva de inspección de contenido al servidor virtual de equilibrio de carga de tipo HTTP/SSL

Debe vincular el servidor virtual de cambio de contenido o equilibrio de carga de tipo HTTP/SSL a la directiva de inspección de contenido.

En el símbolo del sistema, escriba lo siguiente:

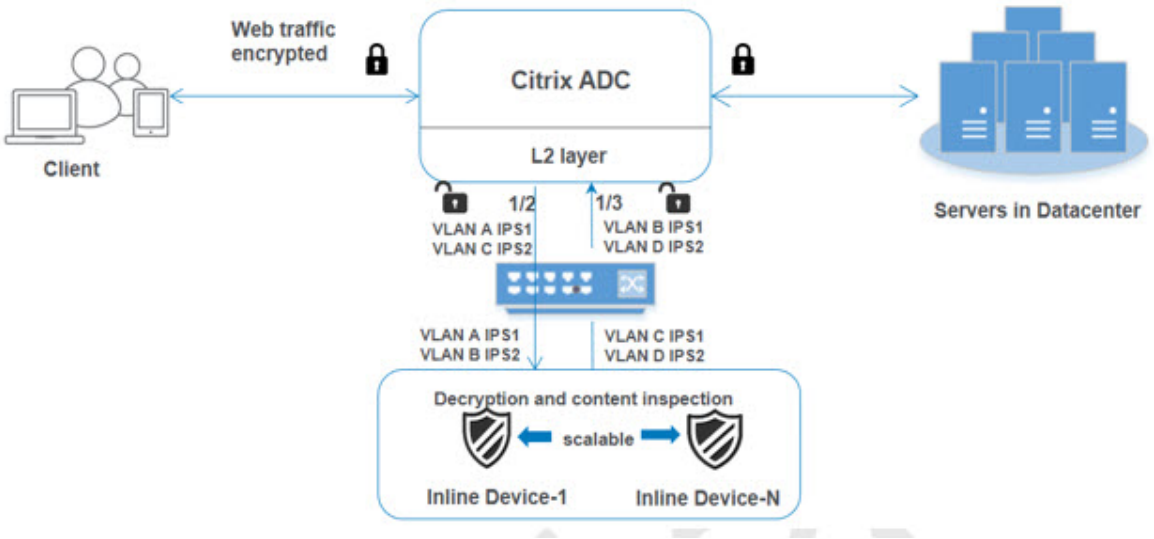
```
bind lb vserver <vserver name> -policyName < policy_name > -priority <> -
type <L7InlineREQUEST | L4Inline-REQUEST>
```

Ejemplo:

```
bind lb vserver http_vserver -policyName Inline_pol1 -priority 100 -type
REQUEST
```

Caso 3: Equilibrio de carga de varios dispositivos en línea mediante interfaces compartidas

Puede hacer referencia a esta configuración si está usando varios dispositivos en línea y si quiere equilibrar la carga de los dispositivos mediante diferentes servicios en una interfaz VLAN compartida. Esta configuración mediante interfaces VLAN compartidas es similar al caso 2. Para obtener información sobre la configuración básica, consulte el caso 2.



Vincular VLAN A con opción de uso compartido habilitada

En el símbolo del sistema, escriba lo siguiente:

```
bind vlan <id> -ifnum <interface> -tagged
```

Ejemplo:

```
bind vlan 100 -ifnum 1/2 tagged
```

Vincular VLAN B con opción de uso compartido habilitada

En el símbolo del sistema, escriba lo siguiente:

```
bind vlan <id> -ifnum <interface> -tagged
```

Ejemplo:

```
bind vlan 200 -ifnum 1/3 tagged
```

Vincular VLAN C con opción de uso compartido habilitada

En el símbolo del sistema, escriba lo siguiente:

```
bind vlan <id> -ifnum <interface> -tagged
```

Ejemplo:

```
bind vlan 300 -ifnum 1/2 tagged
```


Vincular VLAN D con opción de uso compartido habilitada

En el símbolo del sistema, escriba lo siguiente:

```
bind vlan <id> -ifnum <interface> -tagged
```

Ejemplo:

```
bind vlan 400 -ifnum 1/3 tagged
```

Agregar perfil de inspección de contenido1 para el servicio1

Las configuraciones en línea para un dispositivo Citrix ADC se pueden especificar en una entidad denominada perfil de inspección de contenido. El perfil tiene una colección de configuraciones del dispositivo. El perfil Inspección de contenido se crea para el servicio en línea 1 y la comunicación se realiza a través de 1/2 y 1/3 interfaces dedicadas.

En el símbolo del sistema, escriba:

```
add contentInspection profile <name> -type InlineInspection -egressInterface
 <interface_name> -ingressInterface <interface_name>[-egressVlan <positive_integer
>] [-ingressVlan <positive_integer>]
```

Ejemplo:

```
add contentInspection profile Inline_profile1 -type InlineInspection -
ingressinterface “1/2” -egressInterface “1/3” -egressVlan 100 -ingressVlan
 300
```

Agregar perfil de inspección de contenido2 para el servicio2

El perfil de inspección de contenido 2 se agrega para servicio2 y el dispositivo en línea se comunica con el dispositivo a través 1/2 de interfaces 1/3 dedicadas.

En el símbolo del sistema, escriba:

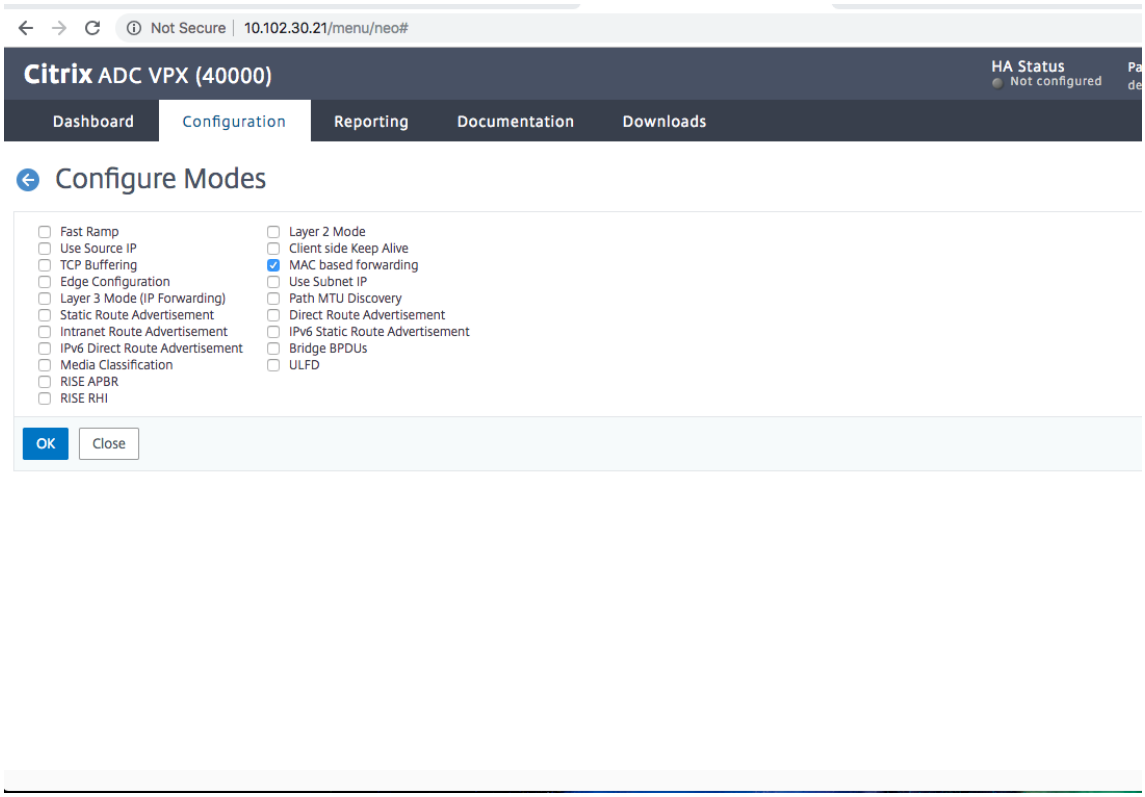
```
add contentInspection profile <name> -type InlineInspection -egressInterface
 <interface_name> -ingressInterface <interface_name>[-egressVlan <positive_integer
>] [-ingressVlan <positive_integer>]
```

Ejemplo:

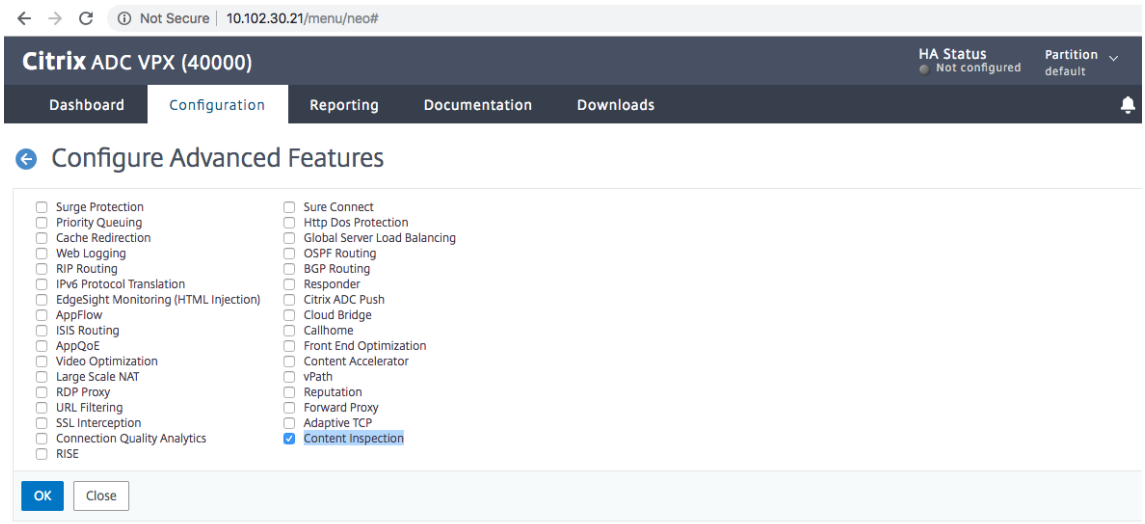
```
add contentInspection profile Inline_profile2 -type InlineInspection -
ingressinterface “1/2” -egressInterface “1/3” -egressVlan 200 -ingressVlan
 400
```


Configurar la integración de servicios en línea mediante la GUI de Citrix ADC

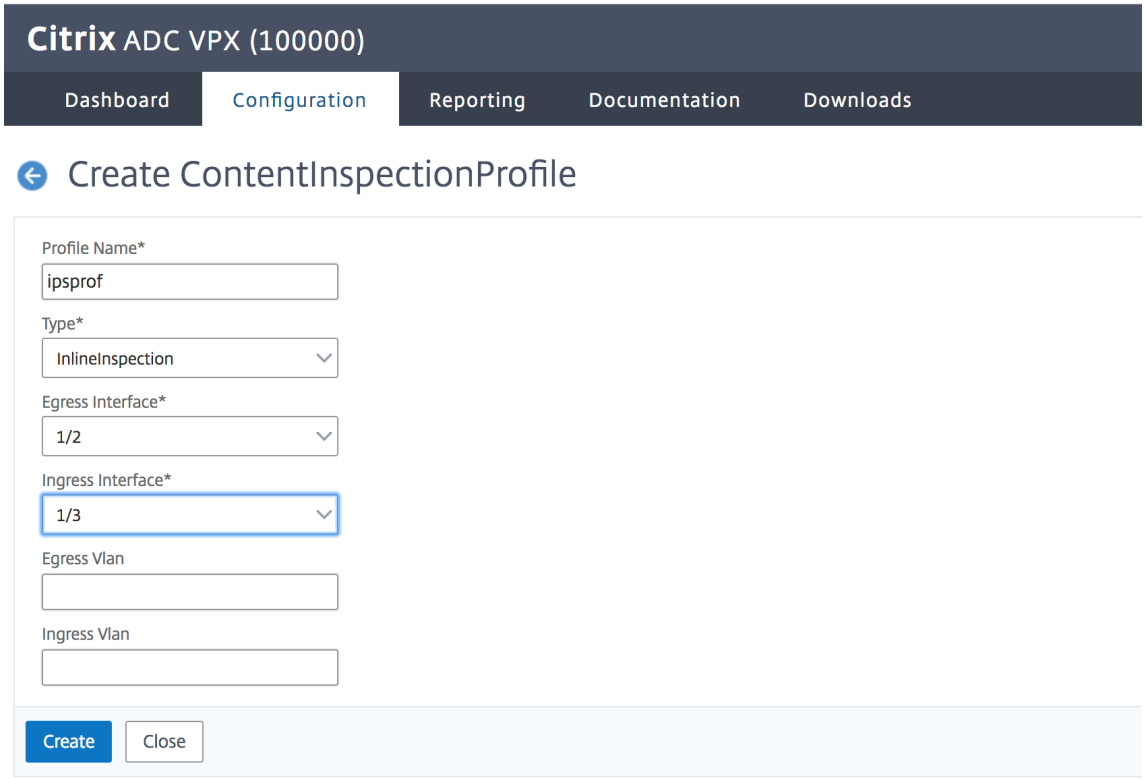
1. Inicie sesión en el dispositivo Citrix ADC y vaya a la página **de la ficha Configuración**.
2. Vaya a **Sistema** > **Configuración** > **Configurar modos**.
3. En la página **Configurar modos**, seleccione **Reenvío basado en Mac**.
4. Haga clic en **Aceptar** y **Cerrar**.



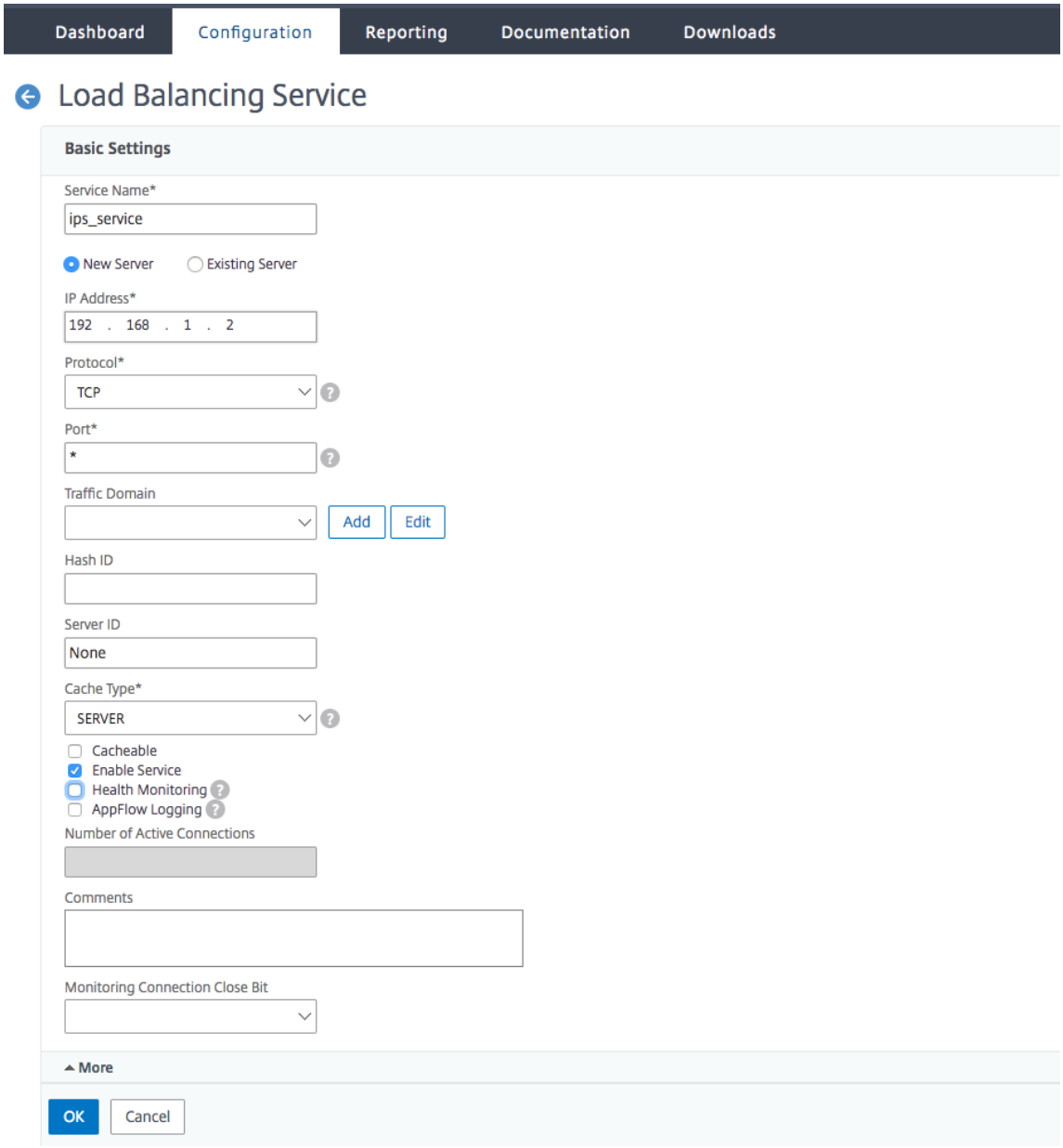
5. Vaya a **Sistema** > **Configuración** > **Configurar funciones avanzadas**.
6. En la página **Configurar función avanzada**, seleccione **Inspección de contenido**.
7. Haga clic en **Aceptar** y **Cerrar**.



8. Acceda a **Seguridad** > **Inspección de contenido** > **Perfiles de inspección de contenido**.
9. En la página **Perfiles de inspección de contenido**, haga clic en **Agregar**.
10. En la página **Crear perfiles de inspección de contenido**, defina los siguientes parámetros.
    a) Nombre del perfil. Nombre del perfil de inspección de contenido.
    b) Tipo. Seleccione el tipo de perfil como InlineInspection.
    c) Interfaz de salida. Interfaz a través de la cual el dispositivo envía tráfico desde Citrix ADC al dispositivo en línea.
    d) Interfaz de entrada. Interfaz a través de la cual el dispositivo recibe tráfico desde el dispositivo en línea al Citrix ADC.
    e) VLAN de salida. ID de VLAN de interfaz a través del cual se envía el tráfico al dispositivo Inline.
    f) Entrada de VLAN. ID de VLAN de interfaz a través del cual el dispositivo recibe tráfico de Inline a Citrix ADC (si está configurado).

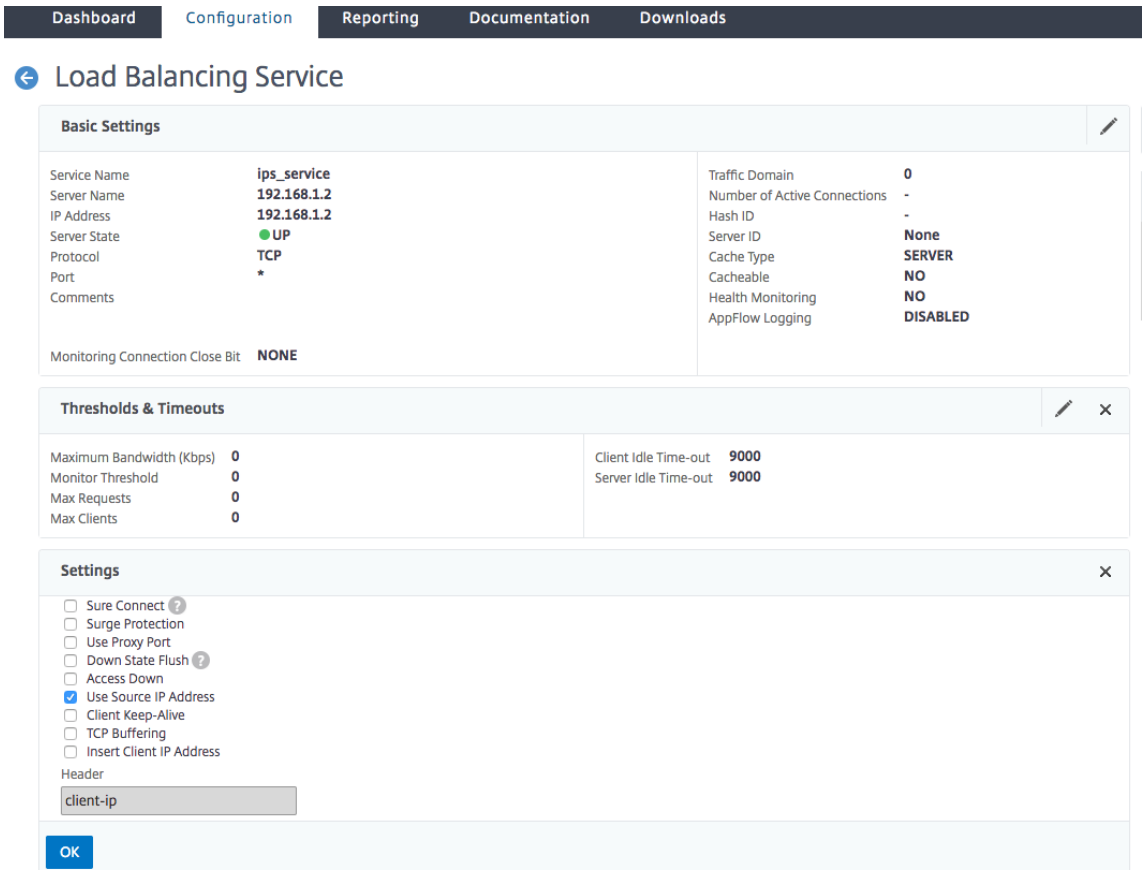


11. Haga clic en **Crear** y **cerrar**.
12. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servicios** y haga clic en **Agregar**.
13. En la página **Servicios**, establezca los siguientes parámetros:
    a) Nombre del servicio. Nombre del servicio de equilibrio de carga.
    b) Dirección IP. Utilice una dirección IP falsa. Nota: Ningún dispositivo debe poseer la dirección IP.
    c) Protocolo. Seleccione el tipo de protocolo como TCP.
    d) Puerto. Introducir *
    e) Monitorización de la salud. Desactive esta opción y habilite solo si desea enlazar el servicio al monitor de tipo TCP. Si desea enlazar un monitor al servicio, entonces la TRANSPARENT opción en el monitor debe estar ON. Consulte el paso 14 sobre cómo agregar monitor y cómo vincularlo al servicio.
    f) Haga clic en **Aceptar**.

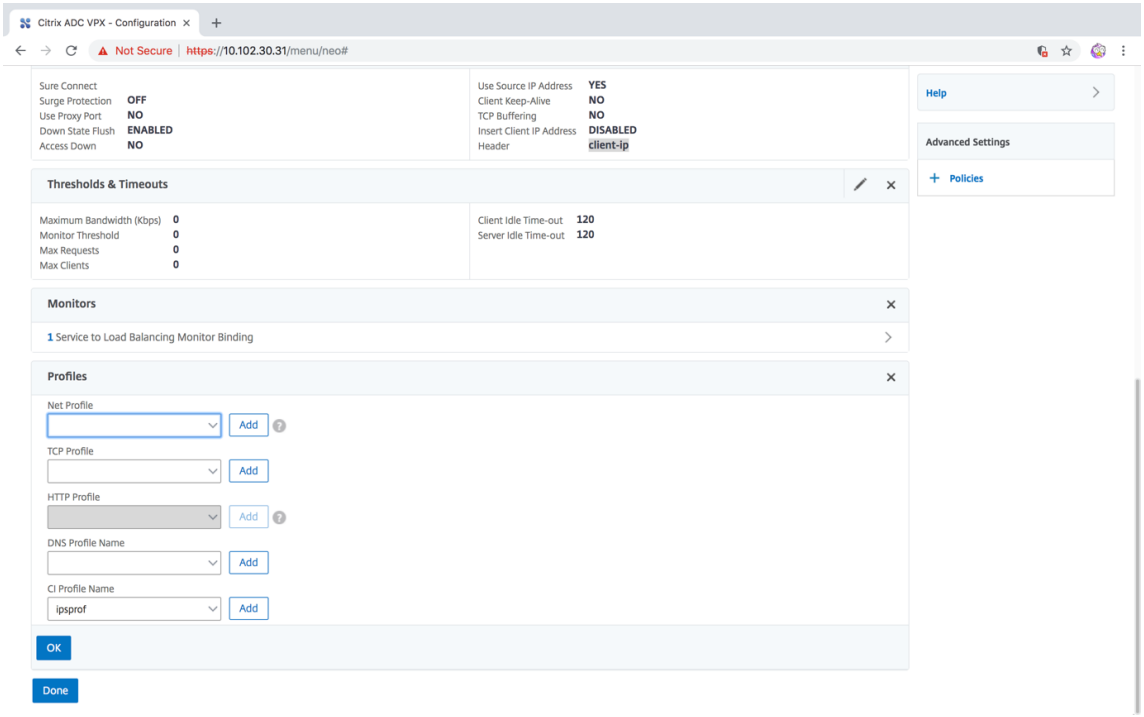


14. En la sección **Configuración**, modifique lo siguiente y haga clic en **Aceptar**.

    a) Usar Puerto Proxy: Desactivar
    b) Usar dirección IP de origen: Enciéndela



15. En la sección **Configuración avanzada**, haga clic en **Perfiles**.
16. Vaya a la sección **Perfiles**, agregue el perfil de inspección de contenido en línea y haga clic en **Aceptar**.

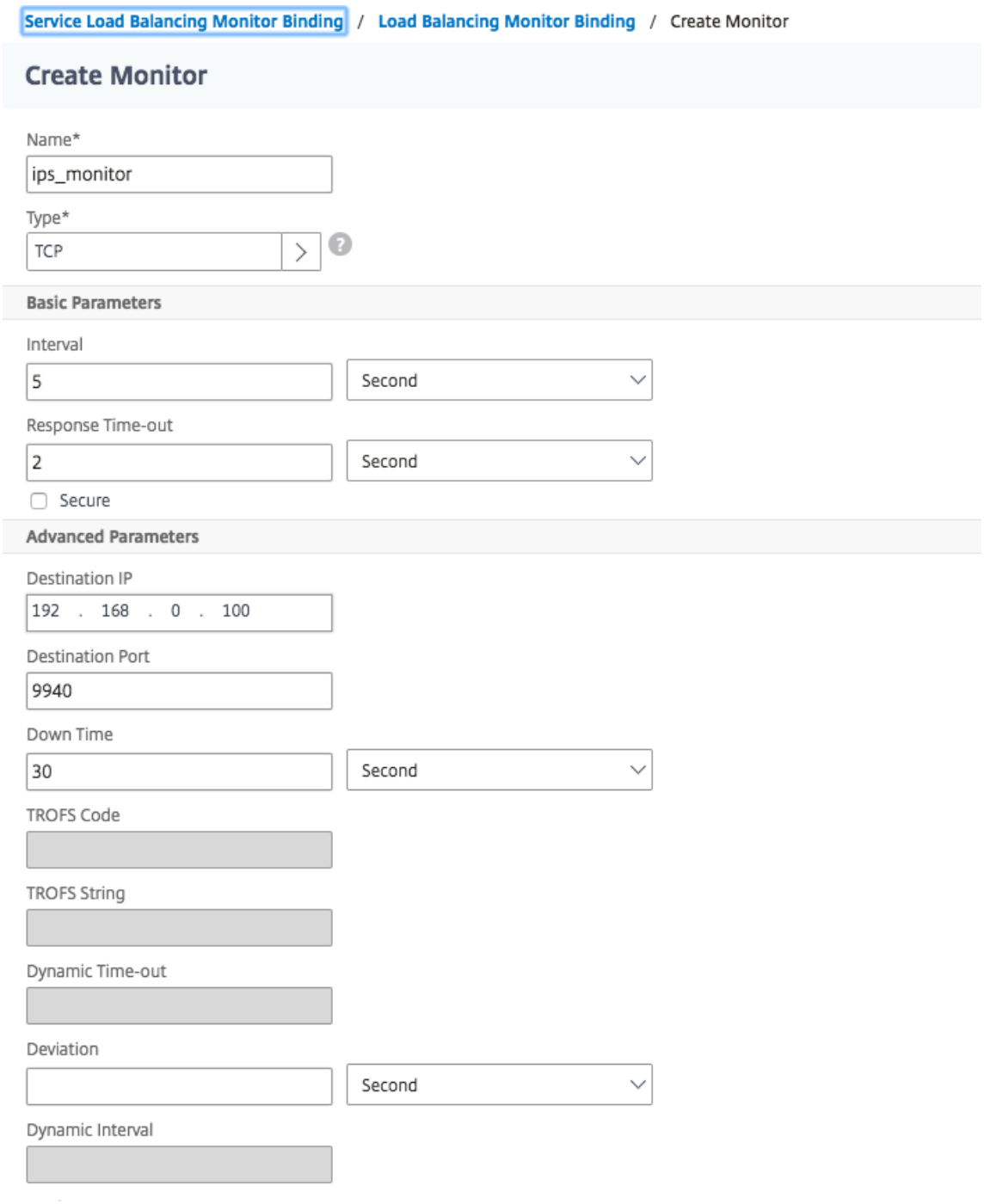


17. Vaya a la sección **Monitores**, **Agregar enlaces** > **Seleccione Monitor** > **Agregar**.

    a) Nombre: Nombre del monitor
    b) Tipo: Seleccione el tipo TCP
    c) IP de destino, PUERTO: Dirección IP de destino y puerto.
    d) Transparente: Encienda

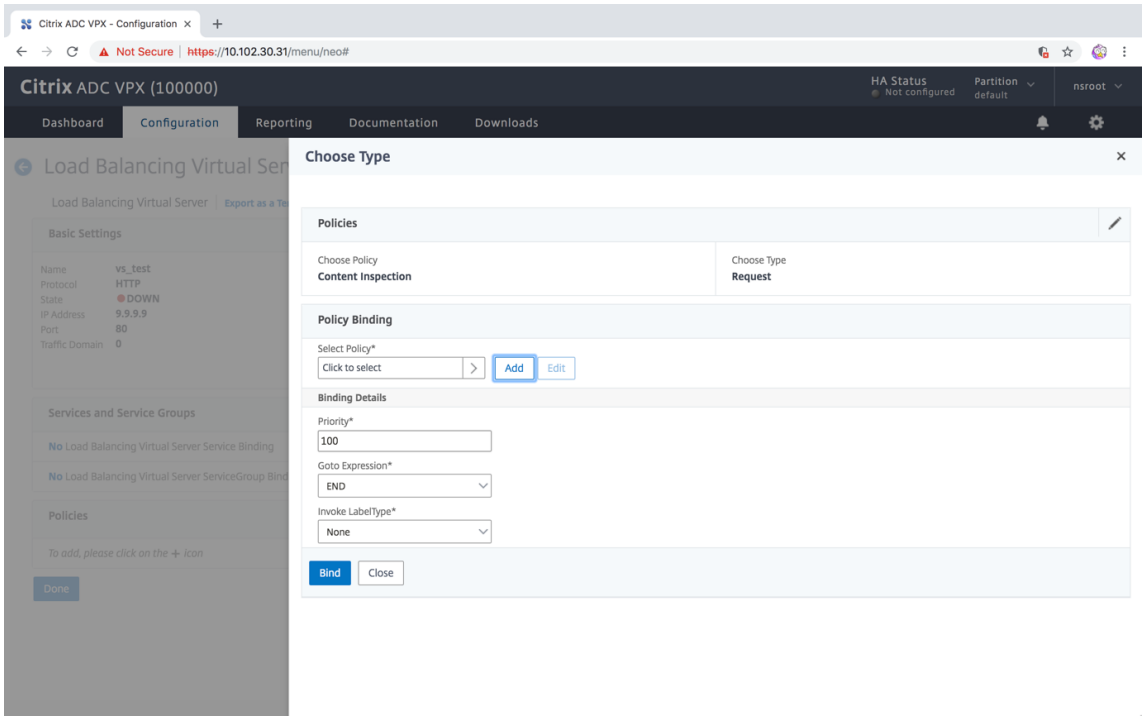
    Nota: Los paquetes del monitor deben fluir a través del dispositivo en línea para supervisar el estado del dispositivo en línea.

18. Haga clic en **Crear**.

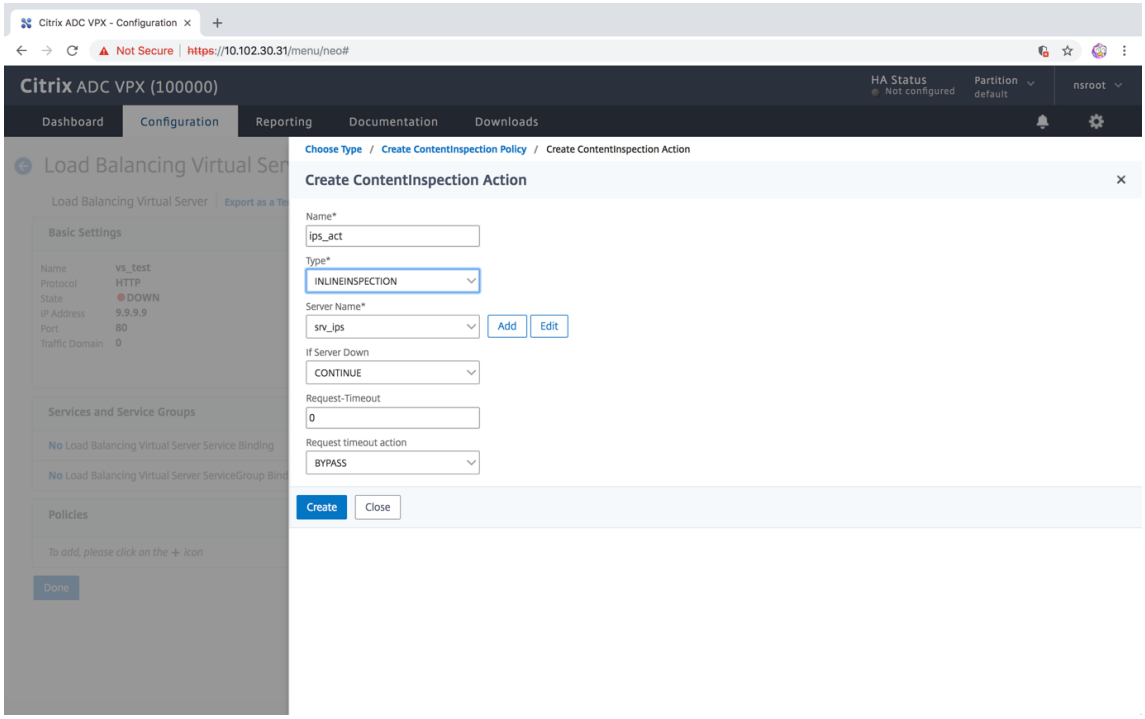


19. Haga clic en **Done**.
20. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**. Agregue un servidor virtual de tipo HTTP o SSL.
21. Después de introducir los detalles del servidor, haga clic en **Aceptar** y de nuevo en **Aceptar**.
22. En la sección **Configuración del tráfico** del Servidor virtual de equilibrio de carga, active los parámetros de capa 2.

23. En la sección **Configuración avanzada**, haga clic en **Directivas**.
24. Vaya a la sección **Directivas** y haga clic en el icono "+" para configurar la directiva de inspección de contenido.
25. En la página **Elegir directiva**, seleccione Inspección de contenido. Haga clic en **Continuar**.
26. En la sección **Enlace de directivas**, haga clic en **Agregar** para agregar una directiva de inspección de contenido.



27. En la página **Crear directiva de inspección de contenido**, escriba un nombre para la directiva de inspección de contenido en línea.
28. En el campo **Acción**, haga clic en **Agregar** para crear una acción de inspección de contenido en línea.
29. En la página **Crear Acción de CI**, establezca los siguientes parámetros:
    a) Name. Nombre de la directiva Inline de inspección de contenido.
    b) Tipo. Seleccione el tipo como InlineInspection.
    c) Servidor. Seleccione el servidor/servicio como dispositivos Inline.
    d) Si el servidor está inactivo. Seleccione una operación si el servidor se desactiva.
    e) Solicite tiempo de espera. Seleccione un valor de tiempo de espera. Puede utilizar valores predeterminados.
    f) Solicitar acción de tiempo de espera. Seleccione una acción de tiempo de espera. Puede utilizar valores predeterminados.
30. Haga clic en **Crear**.



31. Haga clic en **Crear**.
32. En la página **Crear Directiva de CI**, introduzca otros detalles:
33. Haga clic en **Aceptar** y **Cerrar**.

Integración con IPS o NGFW como dispositivos en línea mediante el proxy de reenvío SSL

August 20, 2021

Los dispositivos de seguridad como el sistema de prevención de intrusiones (IPS) y el firewall de próxima generación (NGFW) protegen los servidores contra ataques de red. Estos dispositivos pueden inspeccionar el tráfico en vivo y, por lo general, se implementan en el modo en línea de capa 2. El dispositivo proxy de reenvío SSL proporciona seguridad a los usuarios y a la red empresarial al acceder a los recursos de Internet.

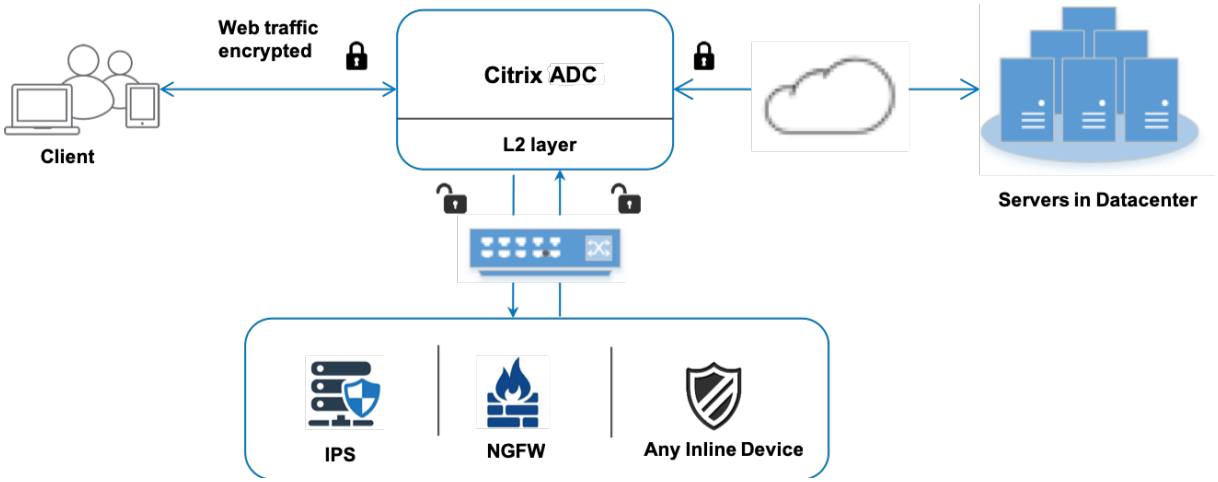
Un dispositivo proxy reenvío SSL se puede integrar con uno o más dispositivos en línea para evitar amenazas y proporcionar protección de seguridad avanzada. Los dispositivos en línea pueden ser cualquier dispositivo de seguridad, como IPS y NGFW.

Algunos casos de uso en los que puede beneficiarse mediante el dispositivo proxy de reenvío SSL y la integración de dispositivos en línea son:

- **Inspección del tráfico cifrado:** la mayoría de los dispositivos IPS y NGFW evitan el tráfico cifrado, lo que puede dejar a los servidores vulnerables a los ataques. Un dispositivo proxy de reenvío SSL puede descifrar el tráfico y enviarlo a los dispositivos en línea para su inspección. Esta integración mejora la seguridad de la red del cliente.
- **Descarga de dispositivos en línea del procesamiento TLS/SSL: El procesamiento** TLS/SSL es costoso, lo que puede resultar en una alta utilización de CPU en dispositivos IPS o NGFW si también descifran el tráfico. Un dispositivo proxy reenvío SSL ayuda a descargar el procesamiento TLS/SSL desde dispositivos en línea. Como resultado, los dispositivos en línea pueden inspeccionar un mayor volumen de tráfico.
- **Carga de dispositivos en línea de equilibrio:** si ha configurado varios dispositivos en línea para administrar el tráfico pesado, un dispositivo proxy de reenvío SSL puede equilibrar la carga y distribuir el tráfico de manera uniforme a estos dispositivos.
- **Selección inteligente del tráfico:** en lugar de enviar todo el tráfico al dispositivo en línea para su inspección, el dispositivo realiza una selección inteligente del tráfico. Por ejemplo, omite el envío de archivos de texto para su inspección a los dispositivos en línea.

Integración de proxy directo SSL con dispositivos en línea

El siguiente diagrama muestra cómo se integra un proxy de reenvío SSL con dispositivos de seguridad en línea.



Cuando integra dispositivos en línea con el dispositivo proxy de reenvío SSL, los componentes interactúan de la siguiente manera:

1. Un cliente envía una solicitud a un dispositivo proxy de reenvío SSL.
2. El dispositivo envía los datos al dispositivo en línea para la inspección de contenido en función de la evaluación de directivas. Para el tráfico HTTPS, el dispositivo descifra los datos y los envía en texto sin formato al dispositivo en línea para la inspección del contenido.

> **Nota**
>
> Si hay dos o más dispositivos en línea, la carga del dispositivo equilibra los dispositivos y envía el tráfico.

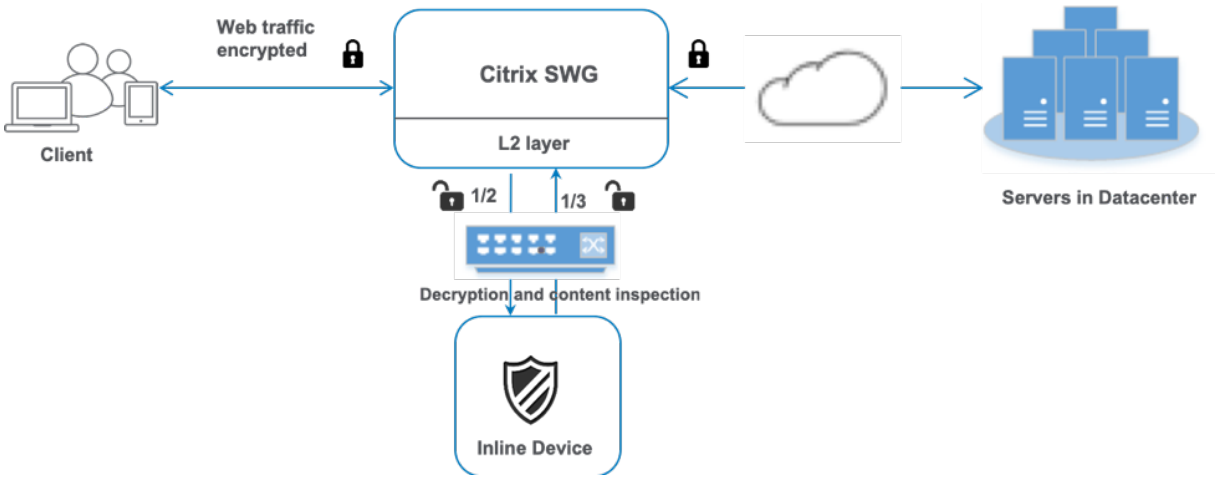
3. Agregue un cambio de contenido o un servidor virtual de equilibrio de carga HTTP/HTTPS.
4. El dispositivo en línea inspecciona los datos en busca de amenazas y decide si quiere eliminar, restablecer o enviar los datos al dispositivo.
5. Si hay amenazas de seguridad, el dispositivo modifica los datos y los envía al dispositivo.
6. Para el tráfico HTTPS, el dispositivo vuelve a cifrar los datos y reenvía la solicitud al servidor back-end.
7. El servidor back-end envía la respuesta al dispositivo.
8. El dispositivo vuelve a descifrar los datos y los envía al dispositivo en línea para su inspección.
9. El dispositivo en línea inspecciona los datos. Si hay amenazas de seguridad, el dispositivo modifica los datos y los envía al dispositivo.
10. El dispositivo vuelve a cifrar los datos y envía la respuesta al cliente.

Configuración de la integración de dispositivos en línea

Puede configurar un dispositivo proxy de reenvío SSL con un dispositivo en línea de tres maneras diferentes, como se indica a continuación:

Caso 1: Uso de un único dispositivo en línea

Para integrar un dispositivo de seguridad (IPS o NGFW) en modo inline, debe habilitar la inspección de contenido y el reenvío basado en MAC (MBF) en modo global en el dispositivo proxy de reenvío SSL. A continuación, agregue un perfil de inspección de contenido, un servicio TCP, una acción de inspección de contenido para que los dispositivos en línea restablezcan, bloqueen o descarten el tráfico basándose en la inspección. Agregue también una directiva de inspección de contenido que el dispositivo utiliza para decidir el subconjunto de tráfico que se va a enviar a los dispositivos en línea. Por último, configure el servidor virtual proxy con la conexión de capa 2 habilitada en el servidor y vincule la directiva de inspección de contenido a este servidor virtual proxy.



Siga estos pasos:

1. Habilite el modo de reenvío basado en Mac (MPF).
2. Habilite la función de inspección de contenido.
3. Agregue un perfil de inspección de contenido para el servicio. El perfil de inspección de contenido contiene la configuración del dispositivo en línea que integra el dispositivo proxy de reenvío SSL con un dispositivo en línea.
4. (Opcional) Agregue un monitor TCP.

   > **Nota:**
   >
   > Los dispositivos transparentes no tienen una dirección IP. Por lo tanto, para realizar comprobaciones de estado, debe vincular explícitamente un monitor.

5. Agregar un servicio. Un servicio representa un dispositivo en línea.
6. (Opcional) Enlazar el servicio al monitor TCP.
7. Agregue una acción de inspección de contenido para el servicio.
8. Agregue una directiva de inspección de contenido y especifique la acción.
9. Agregue un servidor virtual de proxy HTTP o HTTPS (cambio de contenido).
10. Enlazar la directiva de inspección de contenido al servidor virtual.

Configurar mediante la CLI

Escriba los siguientes comandos en el símbolo del sistema. Los ejemplos se dan después de la mayoría de los comandos.

1. Habilitar MBF.

```
enable ns mode mbf
```


1. Habilite la función.

```
enable ns feature contentInspection
```

1. Agregar un perfil de inspección de contenido.

```
add contentInspection profile <name> -type InlineInspection -egressInterface
 <interface_name> -ingressInterface <interface_name>[-egressVlan <positive_integer
>] [-ingressVlan <positive_integer>]
```

Ejemplo:

```
add contentInspection profile ipsprof -type InlineInspection -ingressinterface
 "1/2" -egressInterface "1/3"
```

1. Agregar un servicio. Especifique una dirección IP ficticia que no sea propiedad de ninguno de los dispositivos, incluidos los dispositivos en línea. Establezca `use source IP address` (USIP) en YES. Ajuste `useproxyport` en NO. De forma predeterminada, la supervisión del estado está activada, enlaza el servicio a un monitor de estado y también establece la opción TRANSPARENTE en el monitor ON.

```
add service <service_name> <IP> TCP * - contentinspectionProfileName <Name>
 -healthMonitor YES -usip YES -useproxyport NO
```

Ejemplo:

```
add service ips_service 198.51.100.2 TCP * -healthMonitor YES -usip YES -
useproxyport NO -contentInspectionProfileName ipsprof
```

1. Agregue un monitor de estado. De forma predeterminada, el monitor de estado está activado y también tiene la opción de desactivarlo, si es necesario. En el símbolo del sistema, escriba:

   ```
   add lb monitor <name> TCP -destIP <ip address> -destPort 80 -transparent
    <YES, NO>
   ```

Ejemplo:

```
add lb monitor ips_tcp TCP -destIP 192.168.10.2 -destPort 80 -transparent
YES
```

1. Vincular el servicio al monitor de estado

Después de configurar el monitor de estado, debe vincular el servicio al monitor de estado. En el símbolo del sistema, escriba:

```
bind service <name> -monitorName <name>
```

Ejemplo:

```
bind service ips_svc -monitorName ips_tcp
```

1. Agregar una acción de inspección de contenido.


```
add contentInspection action <name> -type INLINEINSPECTION -serverName <
string>
```

Ejemplo:

```
add contentInspection action ips_action -type INLINEINSPECTION -serverName
ips_service
```

1. Agregar una directiva de inspección de contenido.

```
add contentInspection policy <name> -rule <expression> -action <string>
```

Ejemplo:

```
add contentInspection policy ips_pol -rule "HTTP.REQ.METHOD.NE(\"CONNECT\")
"-action ips_action
```

1. Agregue un servidor virtual proxy.

```
add cs vserver <name> PROXY <IPAddress> <port> -cltTimeout <secs> -Listenpolicy
 <expression> -authn401 ( ON | OFF )-authnVsName <string> -l2Conn ON
```

> **Nota:**
>
> También se admiten servidores virtuales de equilibrio de carga de tipo HTTP/SSL.

Ejemplo:

```
add cs vserver transparentcs PROXY * * -cltTimeout 180 -Listenpolicy exp1 -
authn401 on -authnVsName swg-auth-vs-trans-http -l2Conn ON
```

1. Enlazar la directiva al servidor virtual.

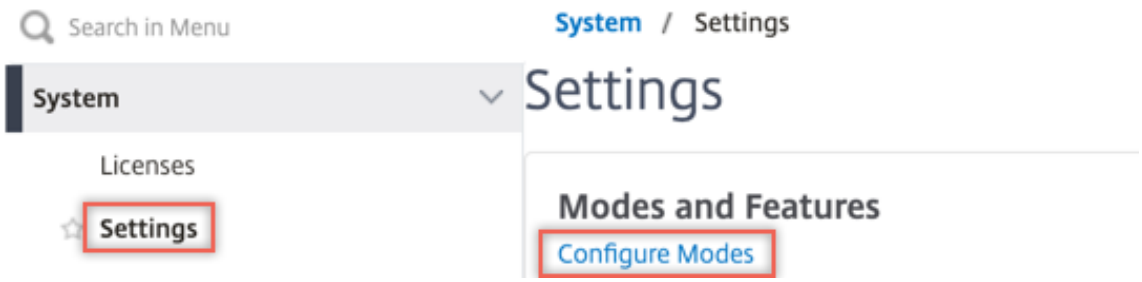
```
bind cs vserver <name> -policyName <string> -priority <positive_integer> -
gotoPriorityExpression <expression> -type REQUEST
```

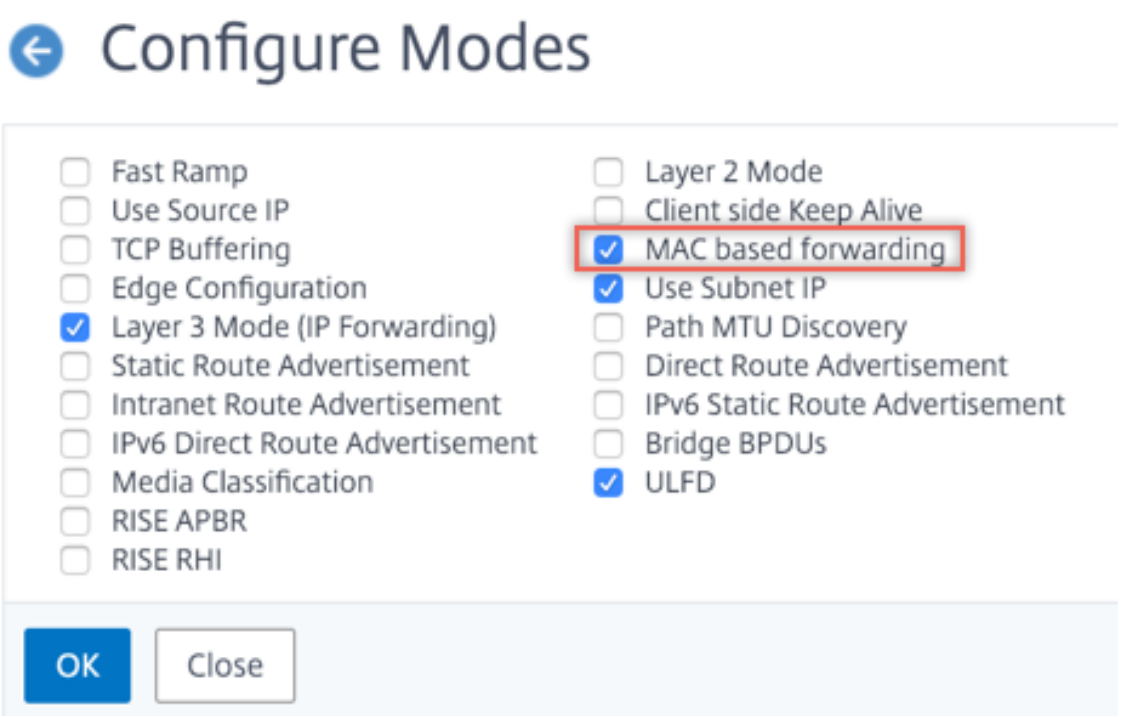
Ejemplo:

```
bind cs vserver explicitcs -policyName ips_pol -priority 1 -gotoPriorityExpression
 END -type REQUEST
```

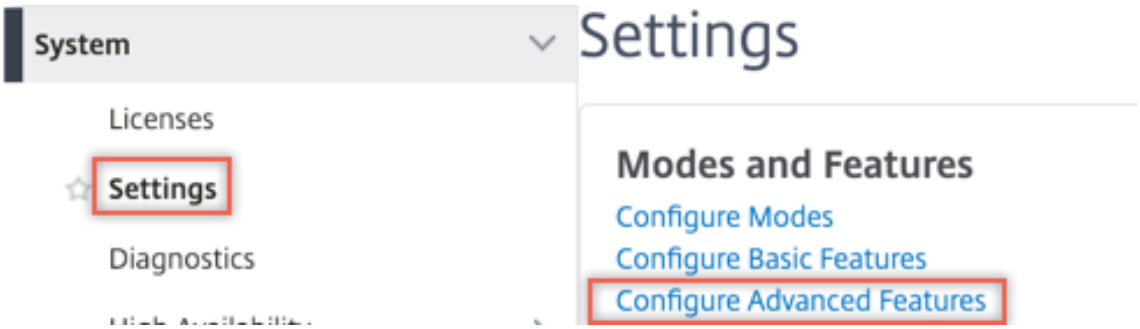
Configurar mediante la GUI

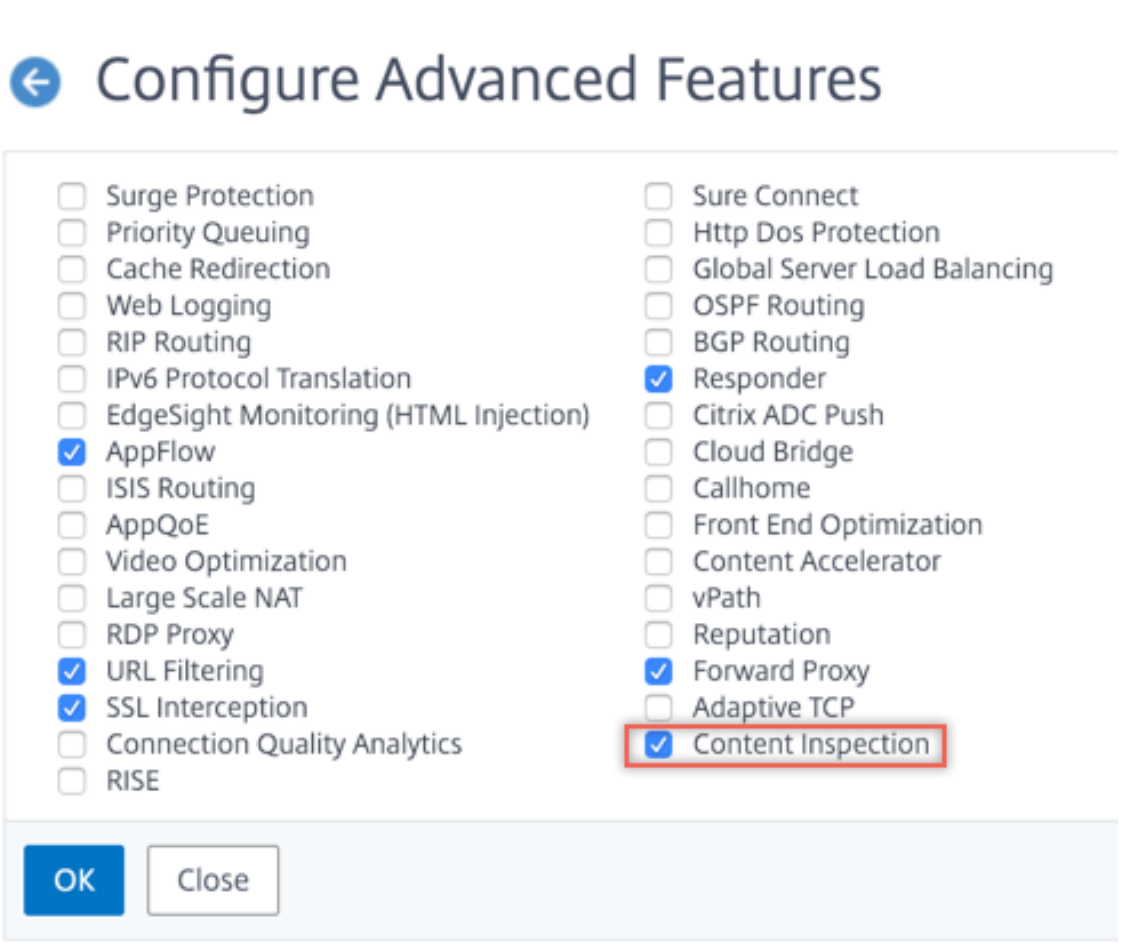
1. Vaya a **Sistema > Configuración**. En **Modos y funciones**, haga clic en **Configurar modos**.



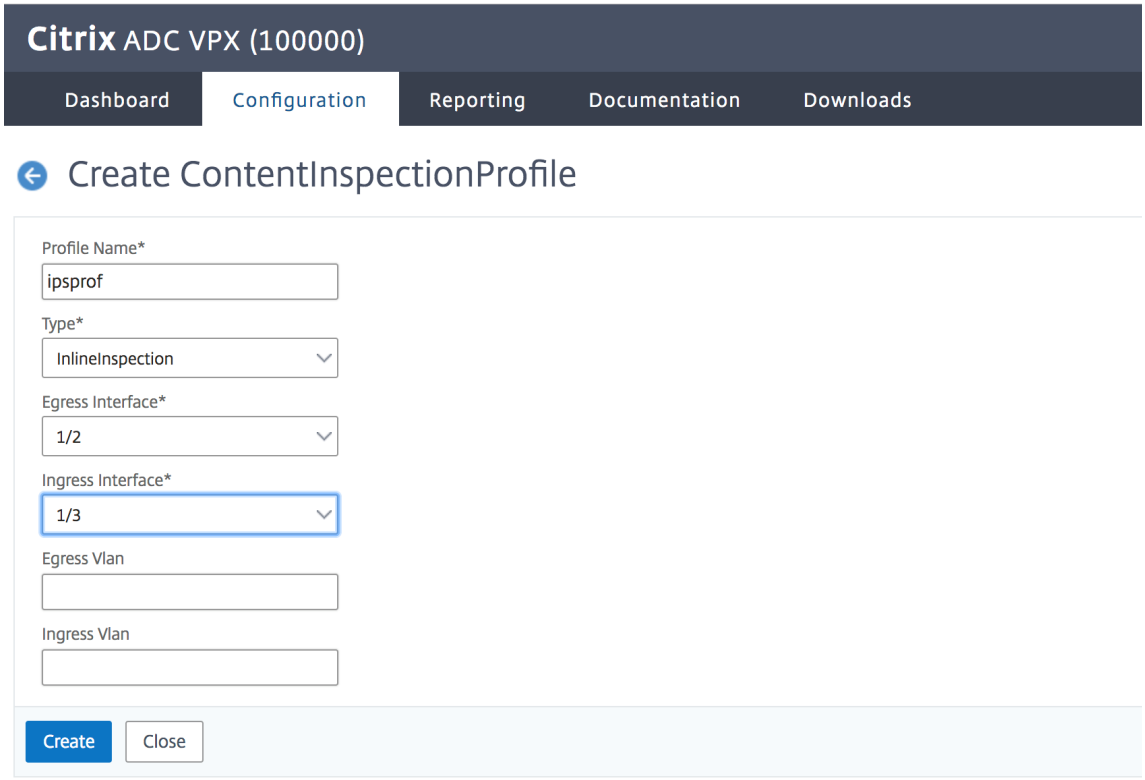


2. Vaya a **Sistema > Configuración**. En **Modos y funciones**, haga clic en **Configurar funciones avanzadas**.

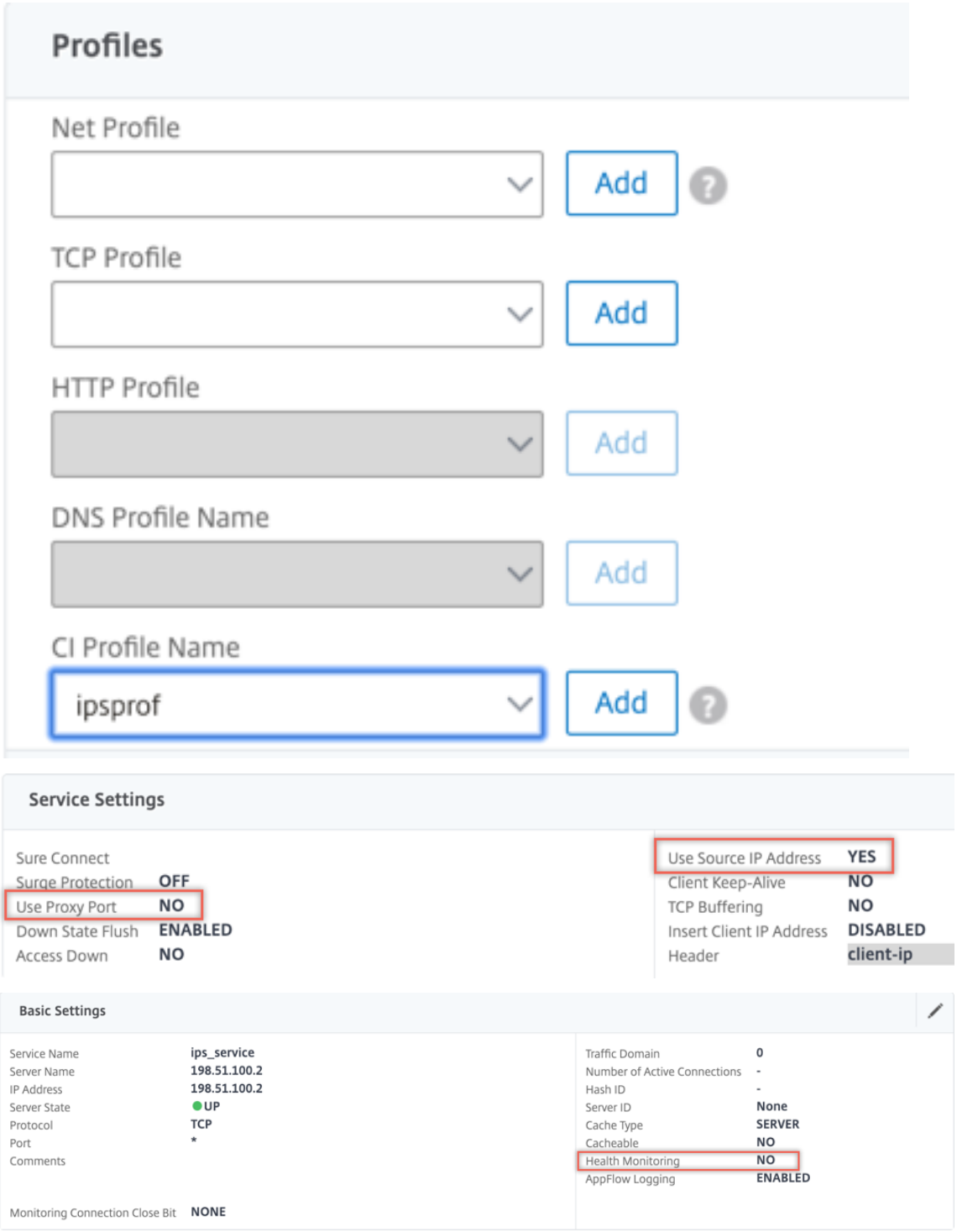




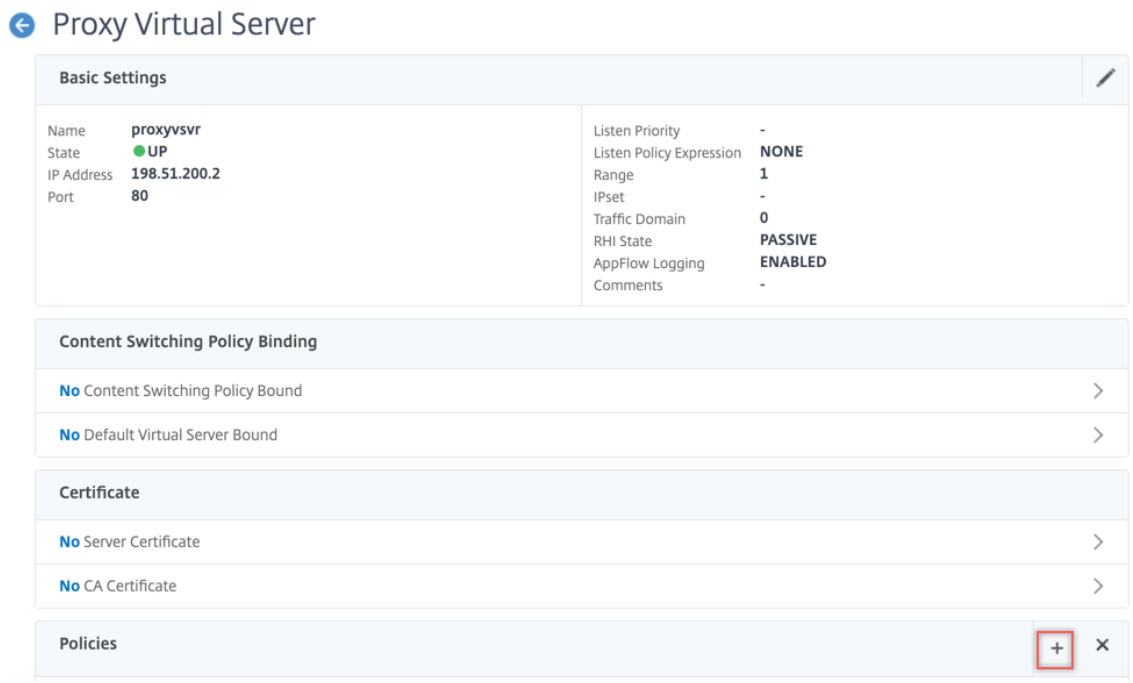
3. Vaya a **Secure Web Gateway > Inspección de contenido > Perfiles de inspección de contenido**. Haga clic en **Agregar**.



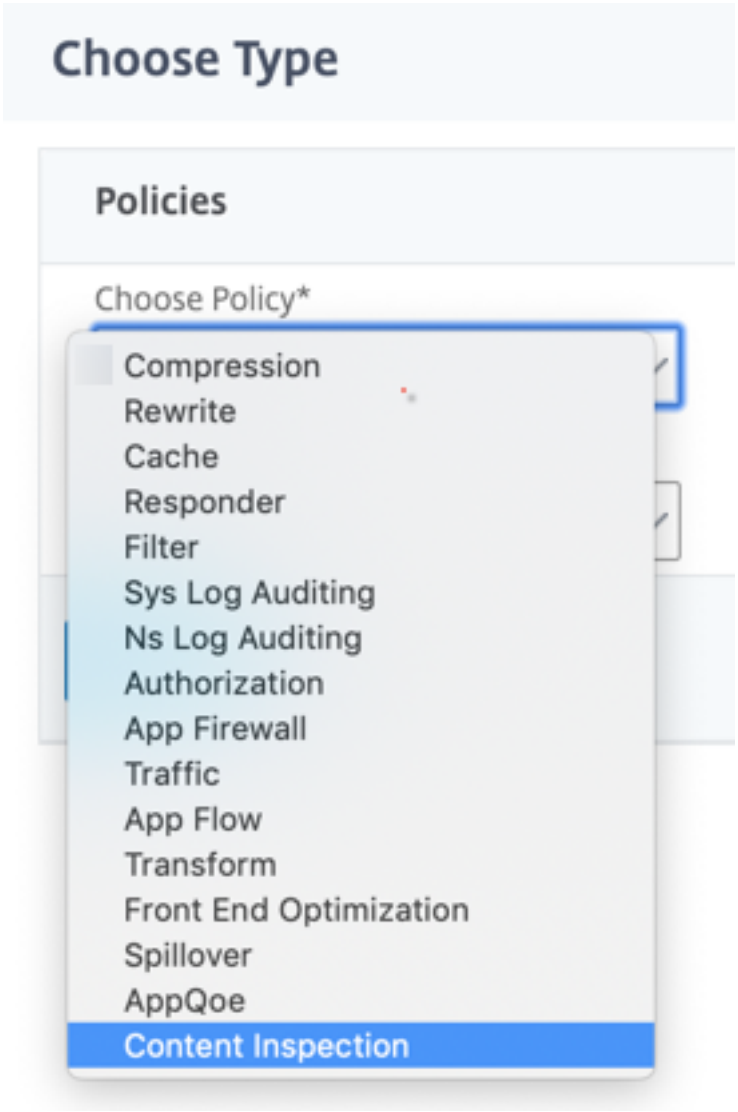
4. Desplácese hasta **Equilibrio de carga > Servicios > Agregar** y agregar un servicio. En **Configuración avanzada**, haga clic en **Perfiles**. En la lista **Nombre de perfil de CI**, seleccione el perfil de inspección de contenido creado anteriormente. En **Configuración del servicio**, establezca **Usar dirección IP de origen**en YES y **Usar puerto proxy**en No. En **Configuración básica**, establezca **Supervisión del estado**en NO. Active la supervisión de estado solo si vincula este servicio a un monitor TCP. Si vincula un monitor a un servicio, establezca la opción TRANSPARENTE del monitor en ON.



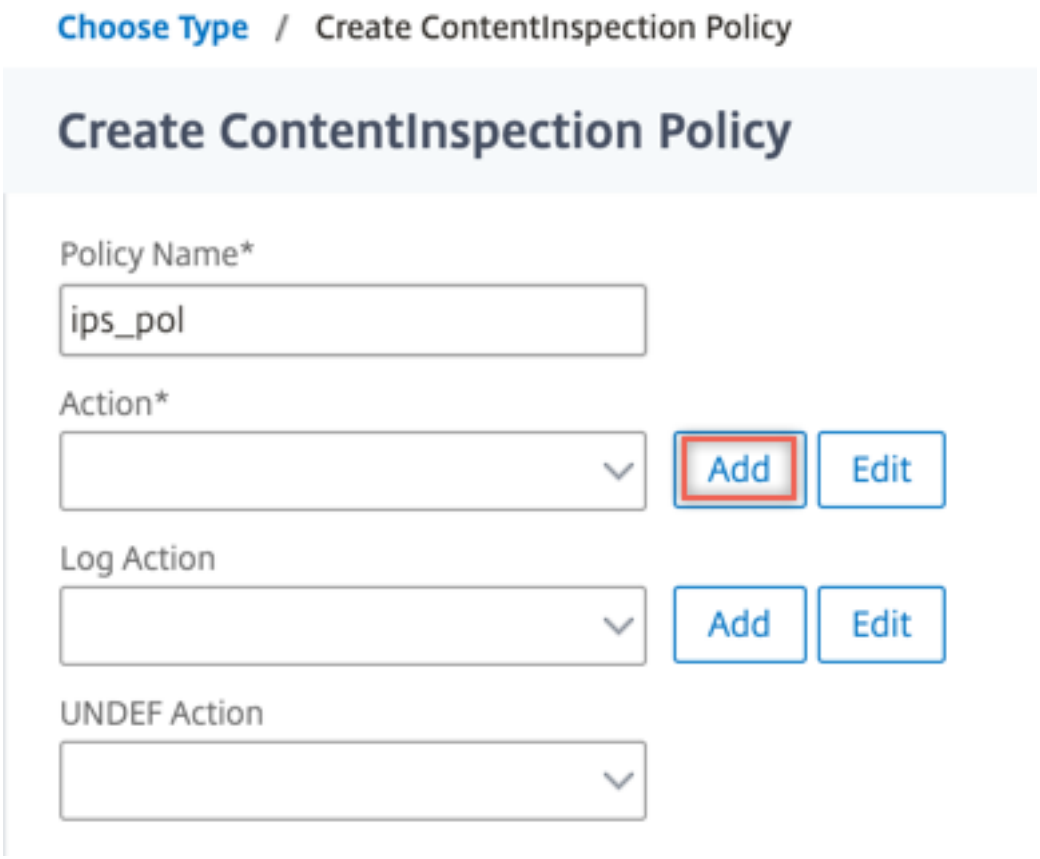
5. Vaya a **Secure Web Gateway > Servidores virtuales Proxy > Agregar**. Especifique un nombre, una dirección IP y un puerto. En **Configuración avanzada**, seleccione **Directivas**. Haga clic en el signo "+".



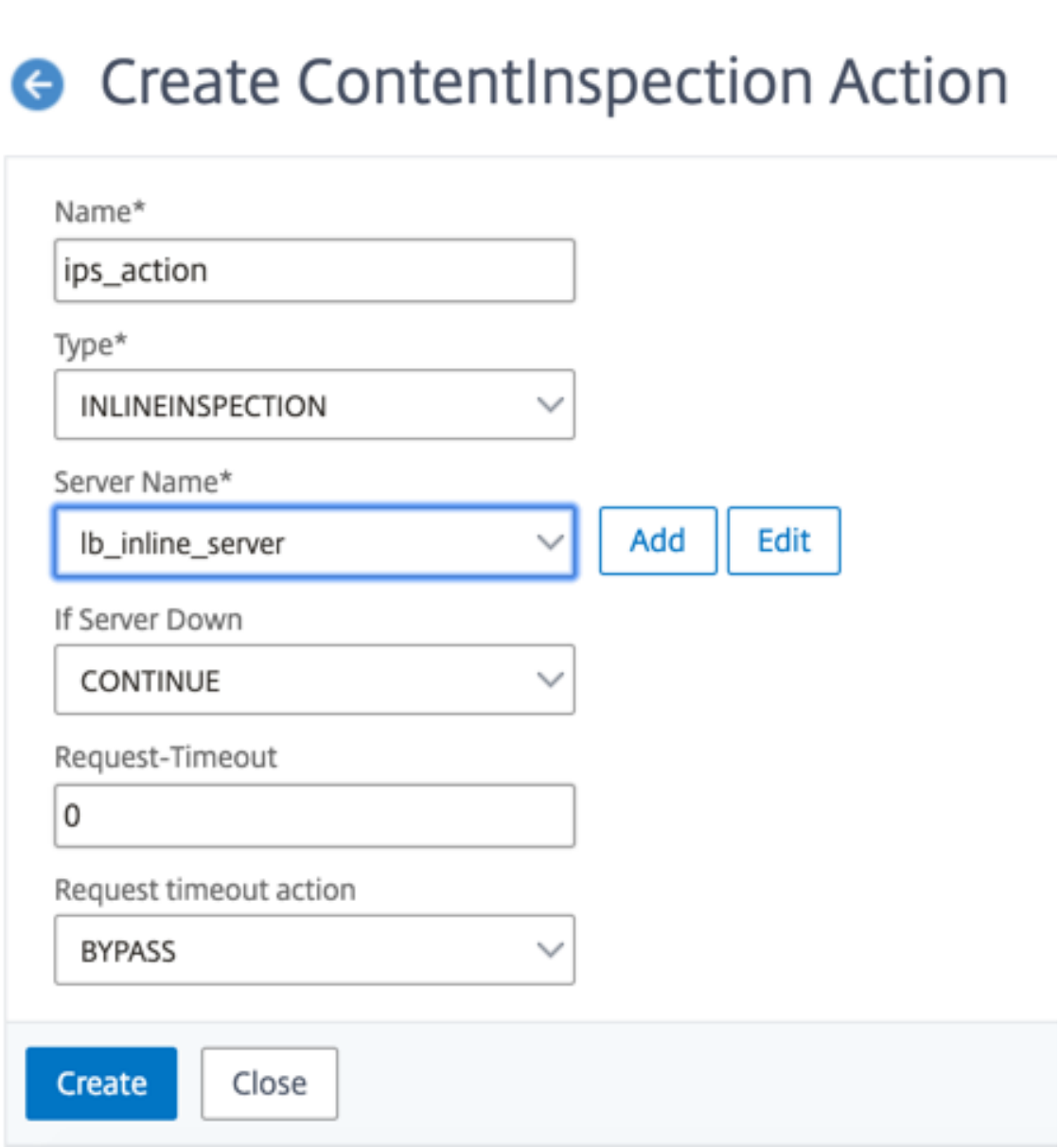
6. En **Elegir directiva**, seleccione **Inspección de contenido**. Haga clic en **Continuar**.



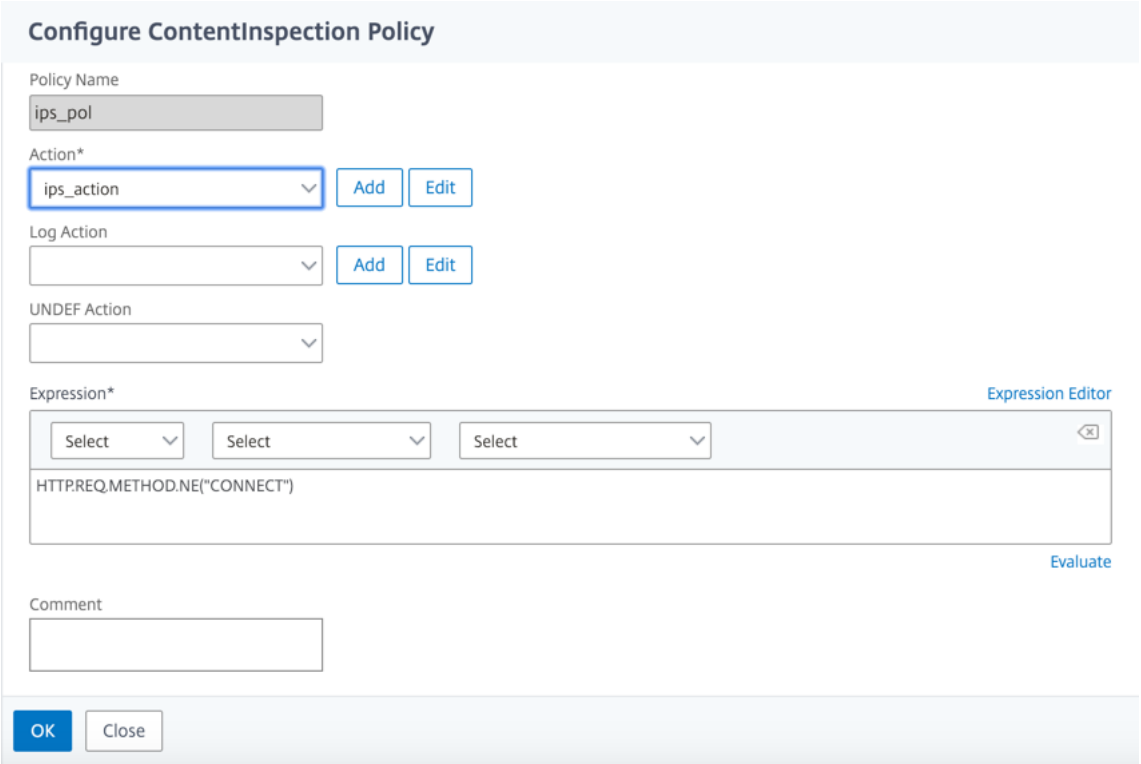
7. Haga clic en **Agregar**. Especifique un nombre. En **Acción**, haga clic en **Agregar**.



8. Especifique un nombre. En **Tipo**, seleccione **INLINEINSPECTION**. En **Nombre del servidor**, seleccione el servicio TCP creado anteriormente.



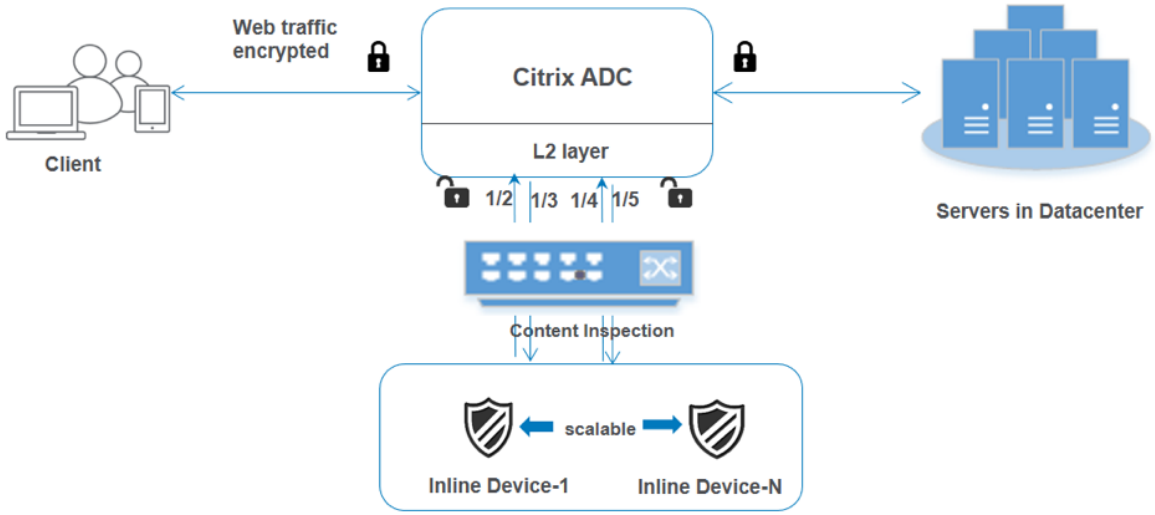
9. Haga clic en **Crear**. Especifique la regla y haga clic en **Crear**.



10. Haga clic en **Vincular**.
11. Haga clic en **Done**.

Caso 2: Equilibrio de carga de varios dispositivos en línea con interfaces dedicadas

Si utiliza dos o más dispositivos en línea, puede equilibrar la carga de los dispositivos mediante diferentes servicios de inspección de contenido con interfaces dedicadas. En este caso, la carga del dispositivo proxy de reenvío SSL equilibra el subconjunto de tráfico enviado a cada dispositivo a través de una interfaz dedicada. El subconjunto se decide en función de las directivas configuradas. Por ejemplo, es posible que los archivos TXT o de imagen no se envíen para su inspección a los dispositivos en línea.



La configuración básica sigue siendo la misma que en el caso 1. Sin embargo, debe crear un perfil de inspección de contenido para cada dispositivo en línea y especificar la interfaz de entrada y salida en cada perfil. Agregue un servicio para cada dispositivo en línea. Agregue un servidor virtual de equilibrio de carga y especifíquelo en la acción de inspección de contenido. Realice los siguientes pasos adicionales:

1. Agregue perfiles de inspección de contenido para cada servicio.
2. Agregue un servicio para cada dispositivo.
3. Agregue un servidor virtual de equilibrio de carga.
4. Especifique el servidor virtual de equilibrio de carga en la acción de inspección de contenido.

Configurar mediante la CLI

Escriba los siguientes comandos en el símbolo del sistema. Se dan ejemplos después de cada comando.

1. Habilitar MBF.

```
enable ns mode mbf
```

1. Habilite la función.

```
enable ns feature contentInspection
```

1. Agregar perfil 1 para el servicio 1.

```
add contentInspection profile <name> -type InlineInspection -egressInterface
 <interface_name> -ingressInterface <interface_name>[-egressVlan <positive_integer
>] [-ingressVlan <positive_integer>]
```

Ejemplo:


```
add contentInspection profile ipsprof1 -type InlineInspection -ingressInterface
 ”1/2”-egressInterface ”1/3”
```

1. Agregar perfil 2 para el servicio 2.

```
add contentInspection profile <name> -type InlineInspection -egressInterface
 <interface_name> -ingressInterface <interface_name>[-egressVlan <positive_integer
>] [-ingressVlan <positive_integer>]
```

Ejemplo:

```
add contentInspection profile ipsprof2 -type InlineInspection -ingressInterface
 ”1/4”-egressInterface ”1/5”
```

1. Agregar servicio 1. Especifique una dirección IP ficticia que no sea propiedad de ninguno de los dispositivos, incluidos los dispositivos en línea. Establezca `use source IP address` (USIP) en YES. Ajuste `useproxyport` en NO. Active la supervisión del estado con el monitor TCP con la opción TRANSPARENTE activada.

```
add service <service_name> <IP> TCP * - contentinspectionProfileName <Name>
 -healthMonitor NO -usip YES -useproxyport NO
```

Ejemplo:

```
add service ips_service1 192.168.10.2 TCP * -healthMonitor NO -usip YES -
useproxyport NO -contentInspectionProfileName ipsprof1
```

1. Agregar servicio 2. Especifique una dirección IP ficticia que no sea propiedad de ninguno de los dispositivos, incluidos los dispositivos en línea. Establezca `use source IP address` (USIP) en YES. Ajuste `useproxyport` en NO. Active la supervisión del estado con la opción TRANSPARENTE activada.

```
add service <service_name> <IP> TCP * - contentinspectionProfileName <Name>
 -healthMonitor NO -usip YES -useproxyport NO
```

Ejemplo:

```
add service ips_service2 192.168.10.3 TCP * -healthMonitor NO -usip YES -
useproxyport NO -contentInspectionProfileName ipsprof2
```

1. Agregue un servidor virtual de equilibrio de carga.

```
add lb vserver <LB_VSERVER_NAME> TCP <IP> <port>
```

Ejemplo:

```
add lb vserver lb_inline_vserver TCP 192.0.2.100 *
```

1. Enlazar los servicios al servidor virtual de equilibrio de carga.


```
bind lb vserver <LB_VSERVER_NAME> <service_name>
bind lb vserver <LB_VSERVER_NAME> <service_name>
```

Ejemplo:

```
bind lb vserver lb_inline_vserver ips_service1
bind lb vserver lb_inline_vserver ips_service2
```

1. Especifique el servidor virtual de equilibrio de carga en la acción de inspección de contenido.

```
add contentInspection action <name> -type INLINEINSPECTION -serverName <
string>
```

Ejemplo:

```
add contentInspection action ips_action -type INLINEINSPECTION -serverName
lb_inline_vserver
```

1. Agregar una directiva de inspección de contenido. Especifique la acción de inspección de contenido en la directiva.

```
add contentInspection policy <name> -rule <expression> -action <string>
```

Ejemplo:

```
add contentInspection policy ips_pol -rule "HTTP.REQ.METHOD.NE(\"CONNECT\")
"-action ips_action
```

1. Agregue un servidor virtual proxy.

```
add cs vserver <name> PROXY <IPAddress> <port> -l2Conn ON
```

Ejemplo:

```
add cs vserver transparentcs PROXY * * -l2Conn ON
```

1. Enlazar la directiva de inspección de contenido al servidor virtual.

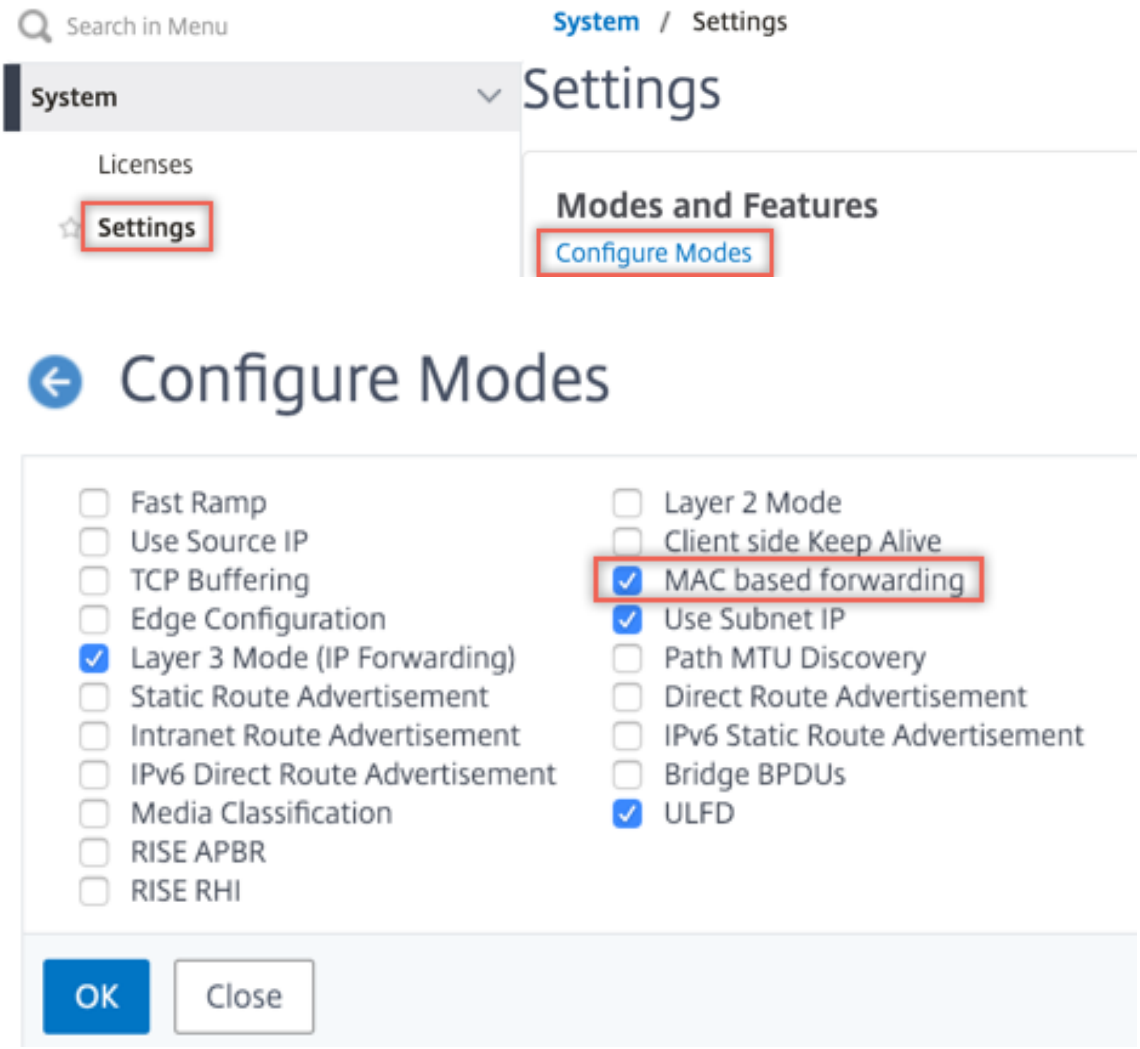
```
bind cs vserver <name> -policyName <string> -priority <positive_integer> -
gotoPriorityExpression <expression> -type REQUEST
```

Ejemplo:

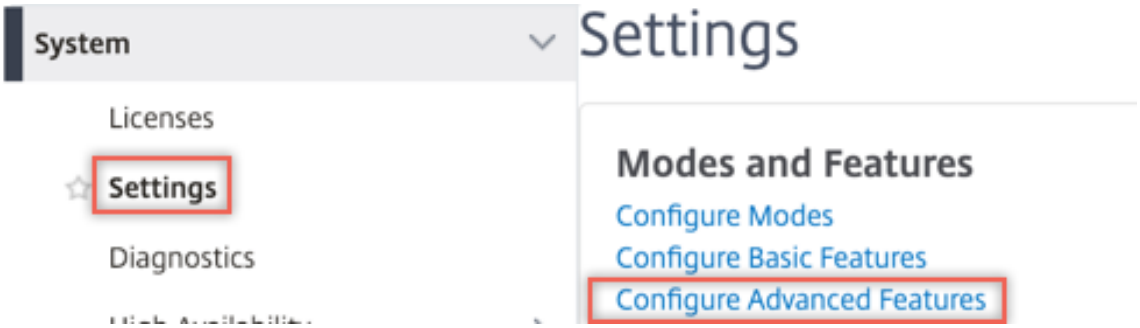
```
bind cs vserver explicitcs -policyName ips_pol -priority 1 -gotoPriorityExpression
 END -type REQUEST
```

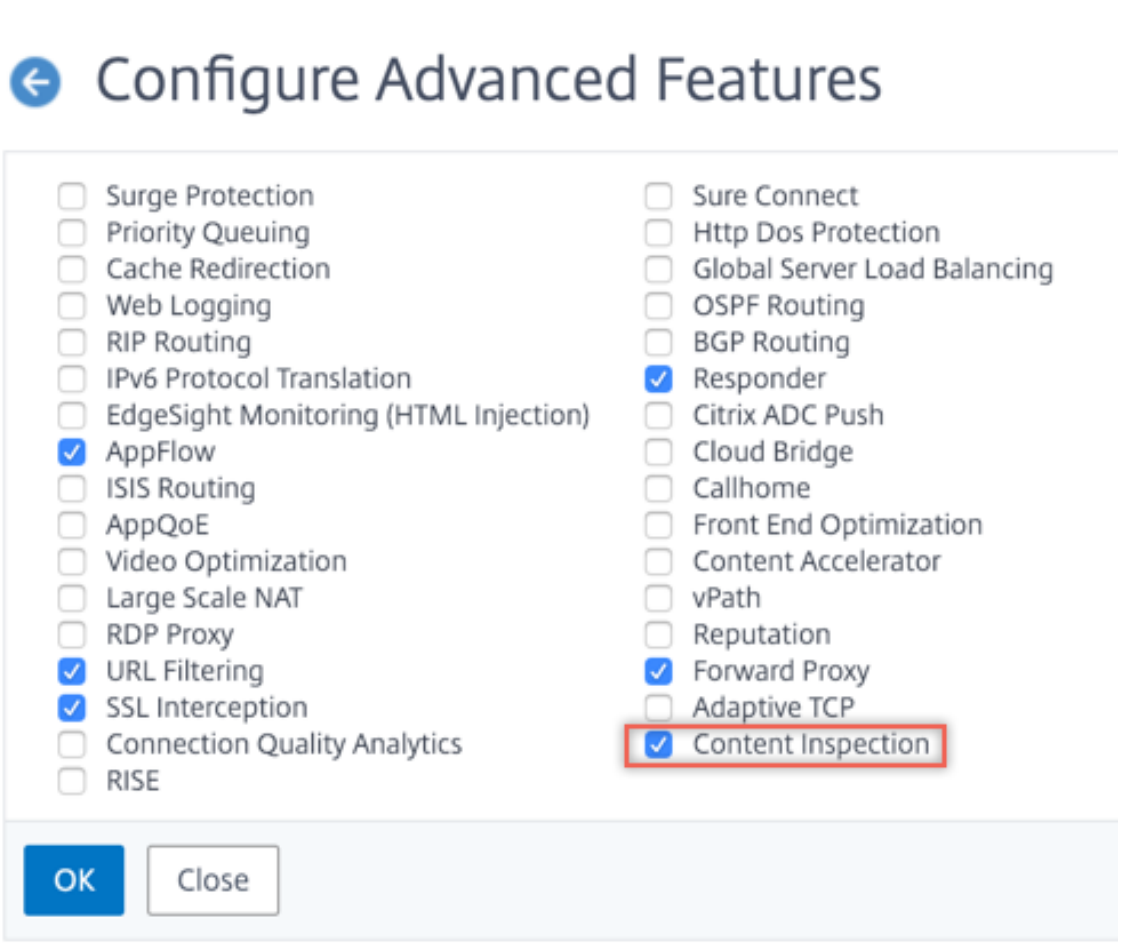
Configuración mediante la GUI

1. Vaya a **Sistema > Configuración**. En **Modos y funciones**, haga clic en **Configurar modos**.

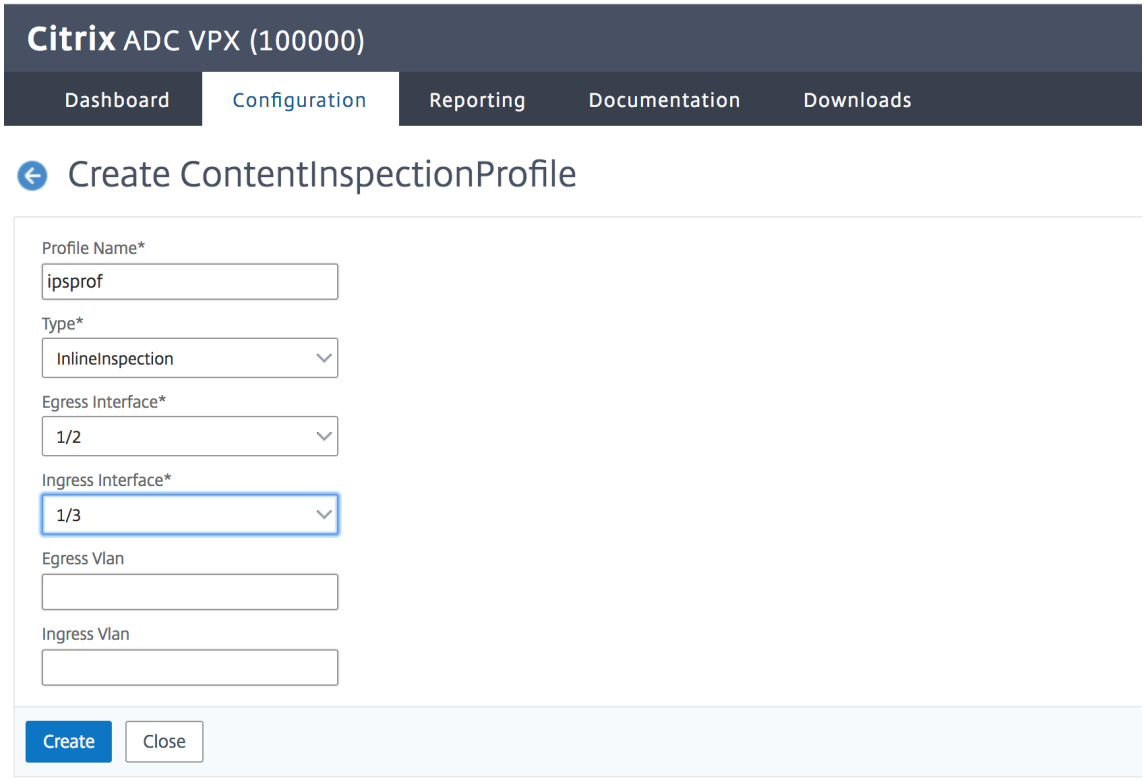


2. Vaya a **Sistema > Configuración**. En **Modos y funciones**, haga clic en **Configurar funciones avanzadas**.

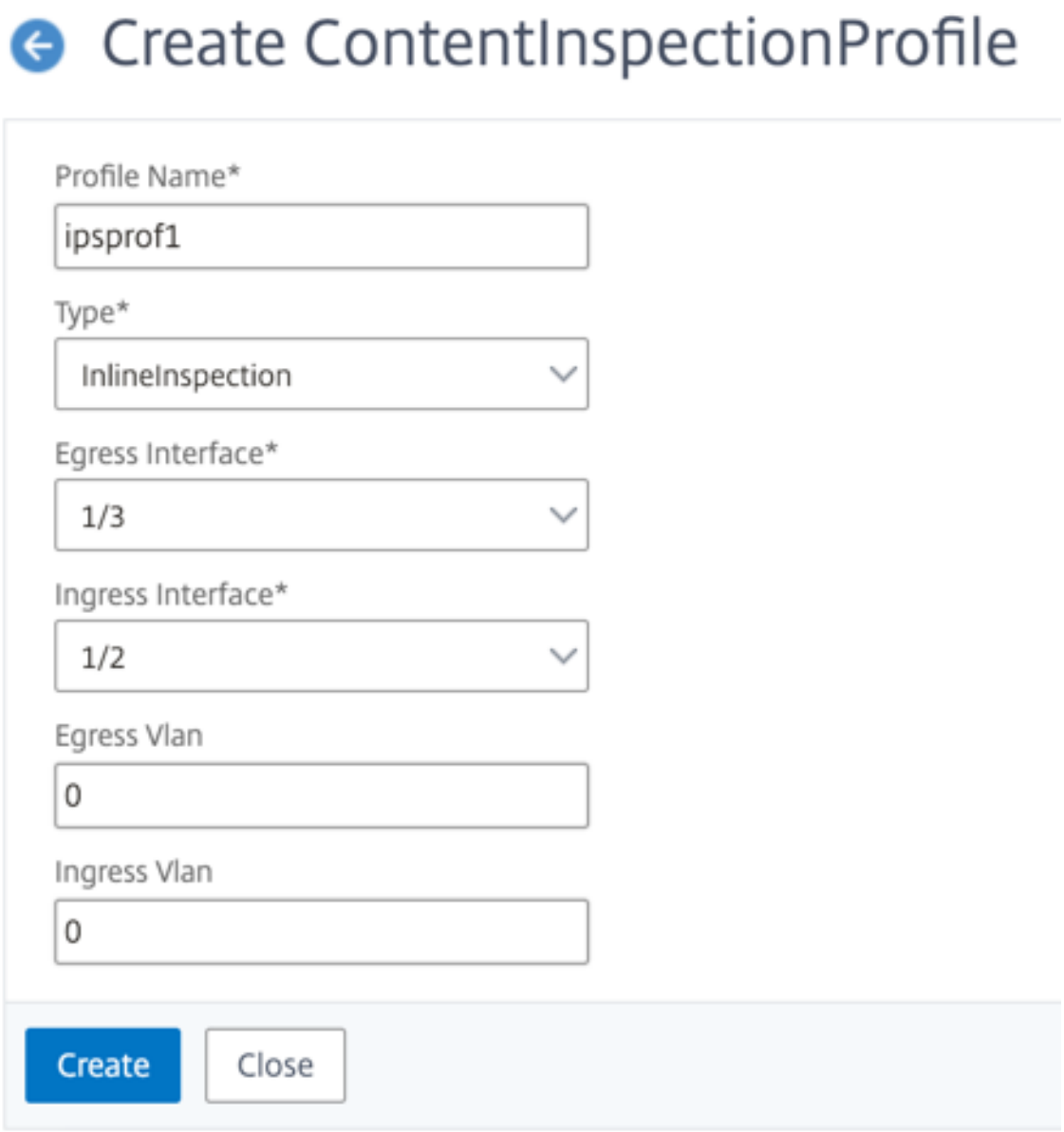




3. Vaya a **Secure Web Gateway > Inspección de contenido > Perfiles de inspección de contenido**. Haga clic en **Agregar**.

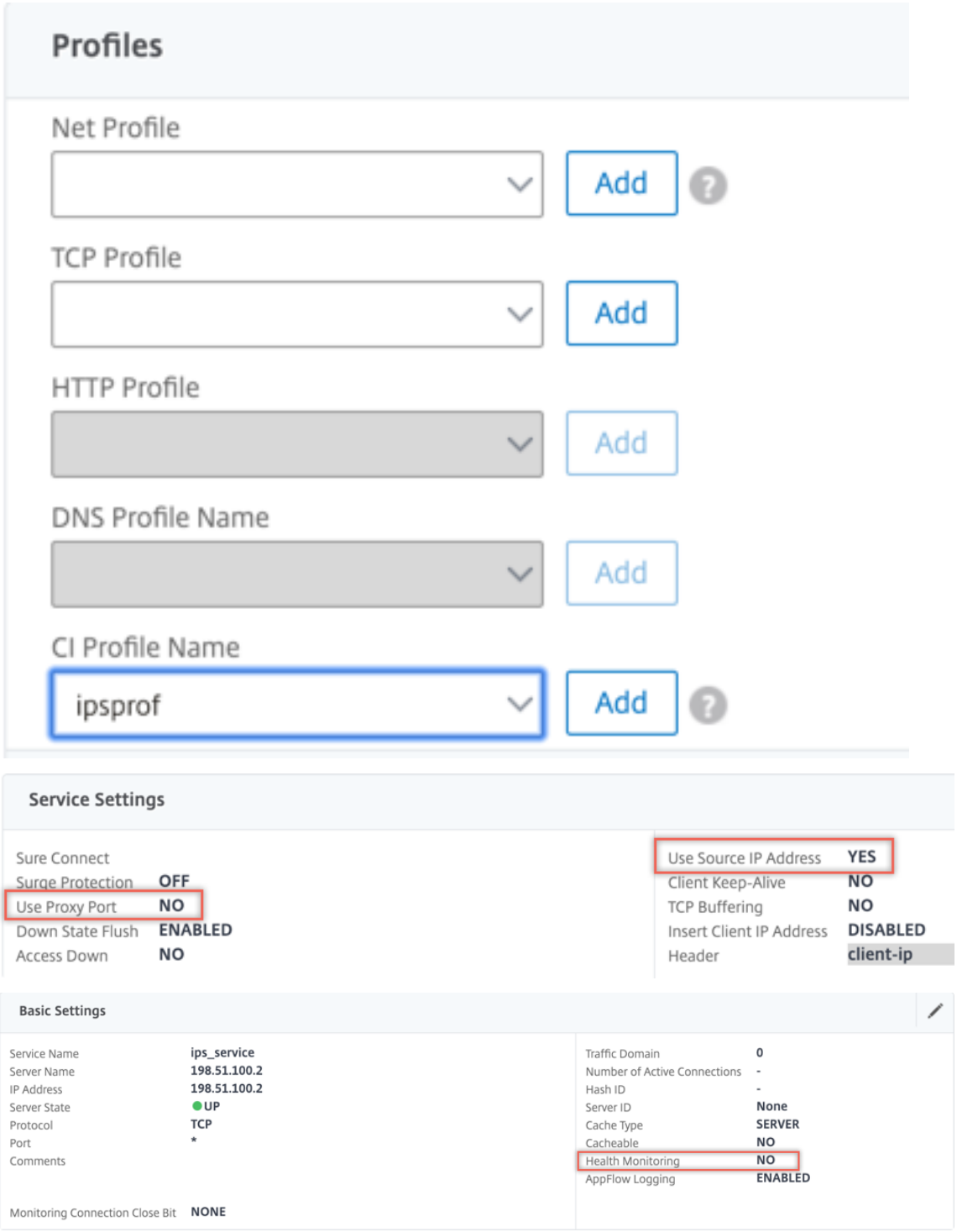


Especifique las interfaces de entrada y salida.



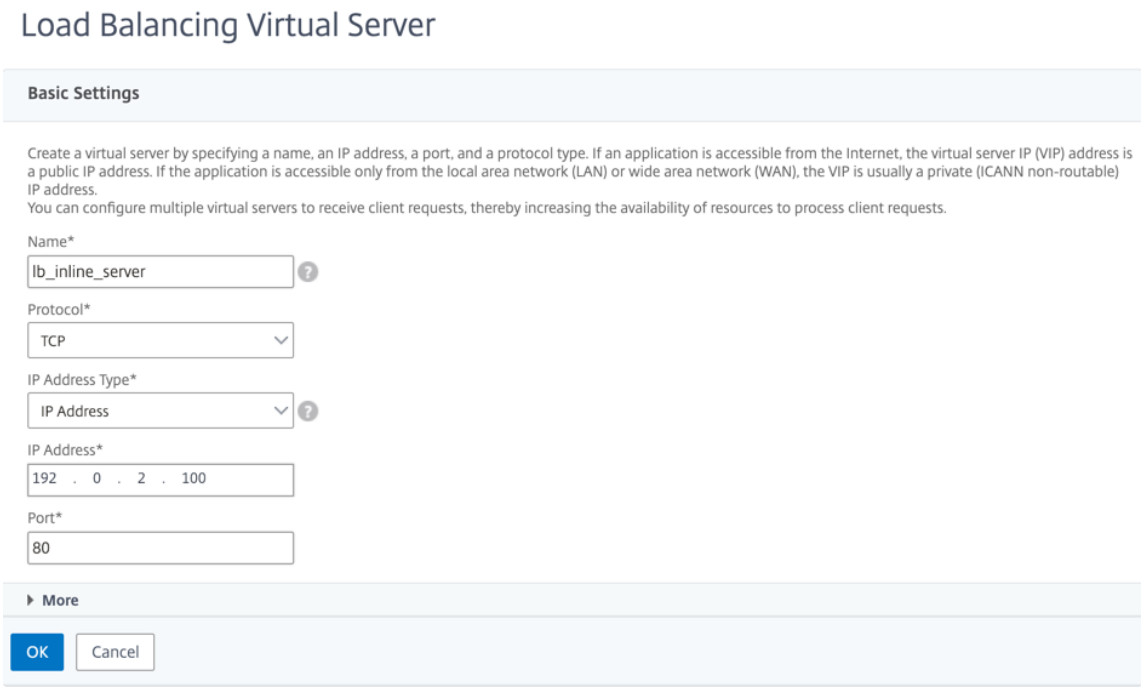
Cree dos perfiles. Especifique una interfaz de entrada y salida diferente en el segundo perfil.

4. Desplácese hasta **Equilibrio de carga > Servicios > Agregar** y agregar un servicio. En **Configuración avanzada**, haga clic en **Perfiles**. En la lista **Nombre de perfil de CI**, seleccione el perfil de inspección de contenido creado anteriormente. En **Configuración del servicio**, establezca **Usar dirección IP de origen**en YES y **Usar puerto proxy**en No. En **Configuración básica**, establezca **Supervisión del estado**en NO. Active la supervisión de estado solo si vincula este servicio a un monitor TCP. Si vincula un monitor a un servicio, establezca la opción TRANSPARENTE del monitor en ON.



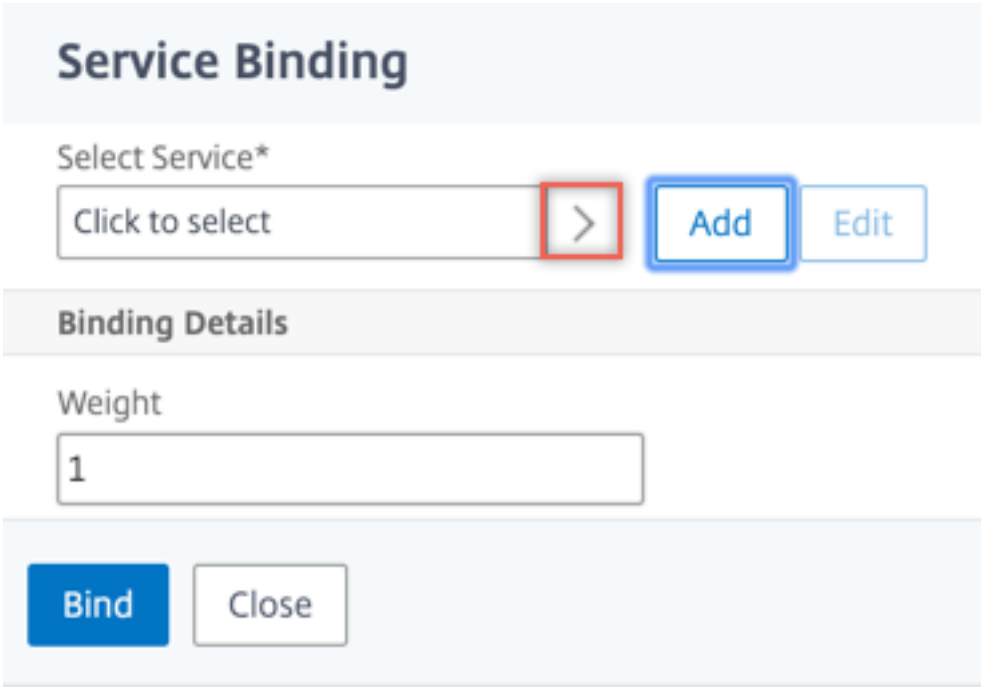
Cree dos servicios. Especifique direcciones IP ficticias que no pertenecen a ninguno de los dispositivos, incluidos los dispositivos en línea.

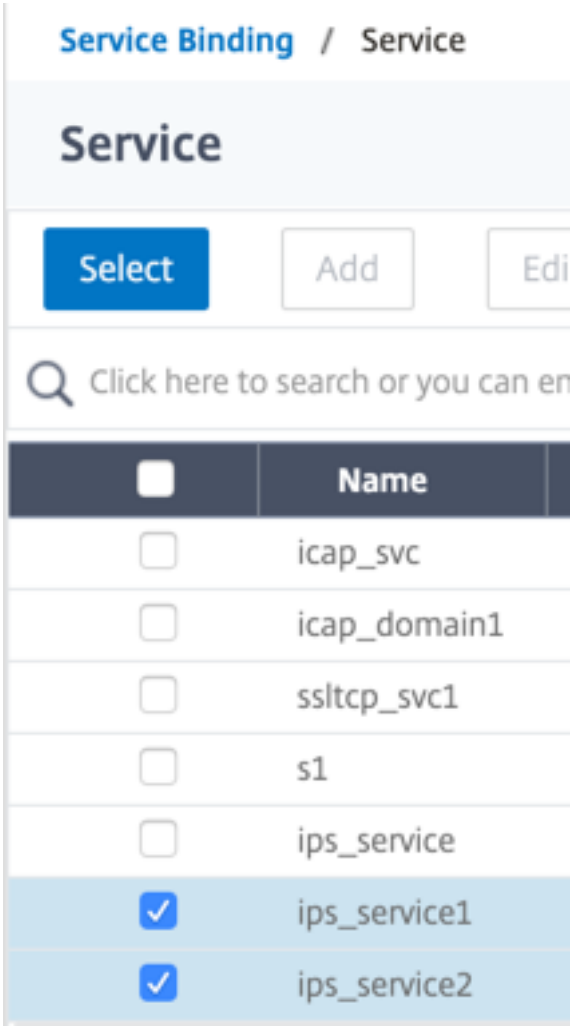
5. Desplácese hasta **Equilibrio de carga > Servidores virtuales > Agregar**. Cree un servidor virtual de equilibrio de carga TCP.

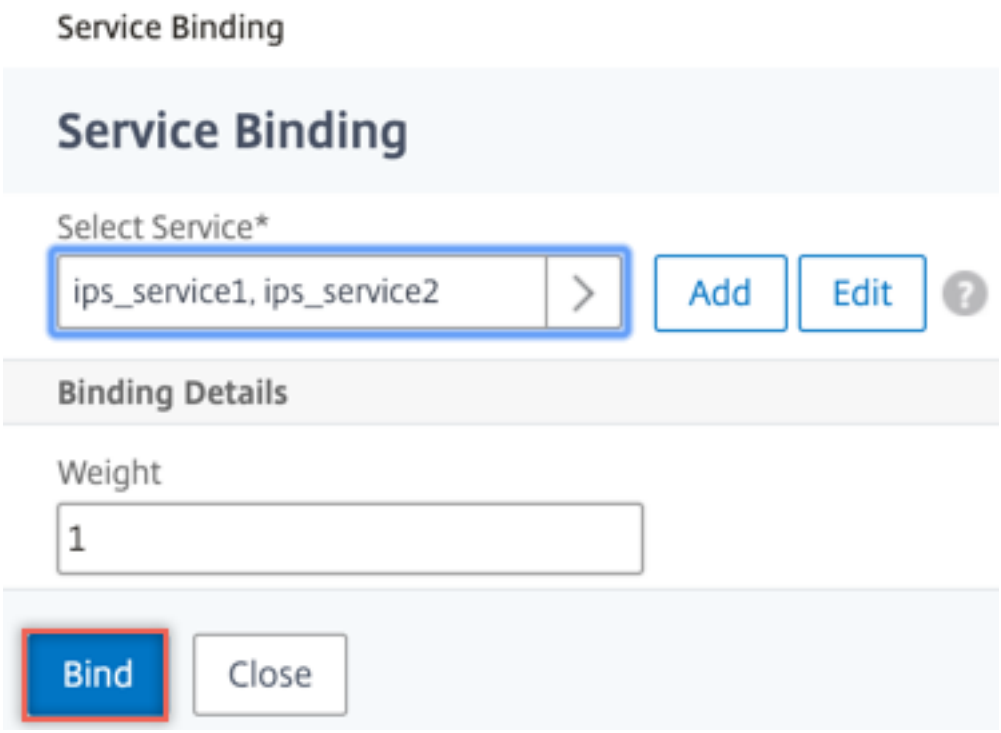


Haga clic en **Aceptar**.

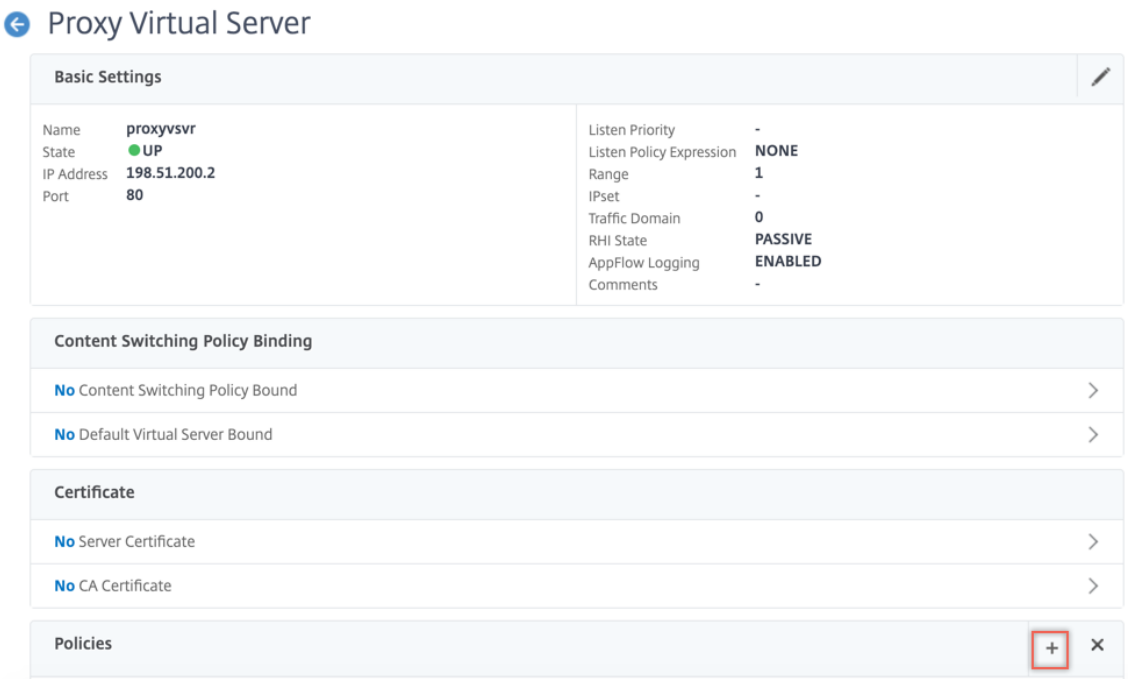
6. Haga clic dentro de la sección **Enlace del servicio de servidor virtual de equilibrio de carga**. En **Enlace de servicio**, haga clic en la flecha **de Seleccionar servicio**. Seleccione los dos servicios creados anteriormente y haga clic en **Seleccionar**. Haga clic en **Vincular**.



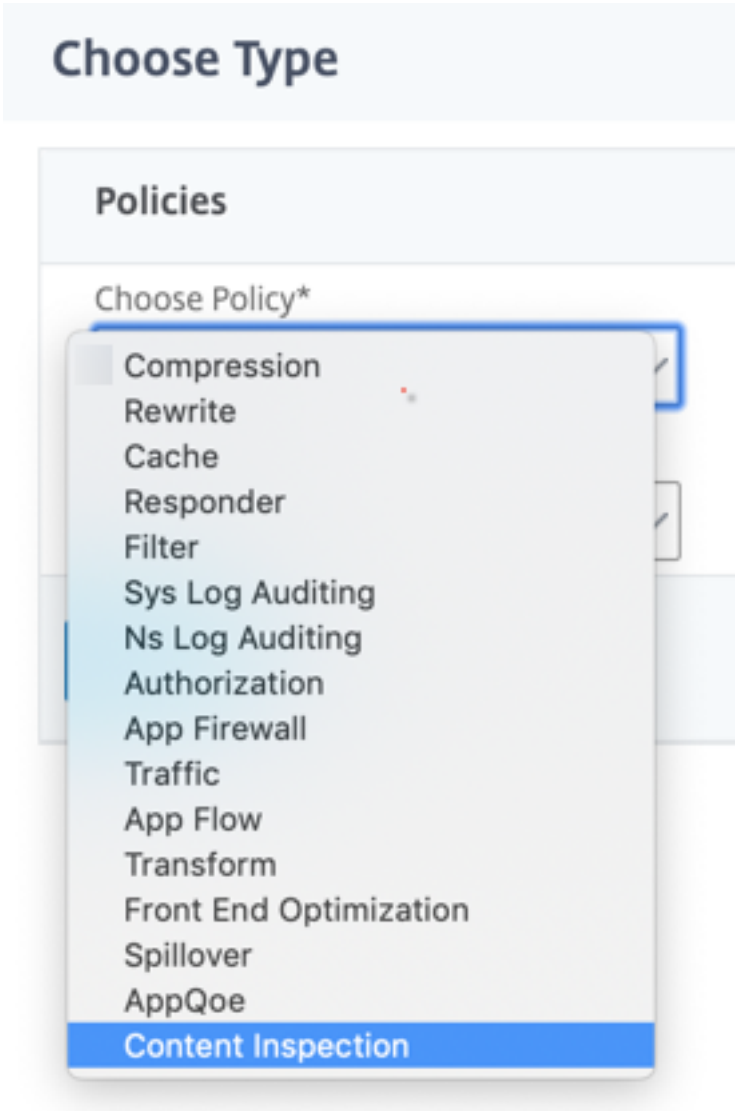




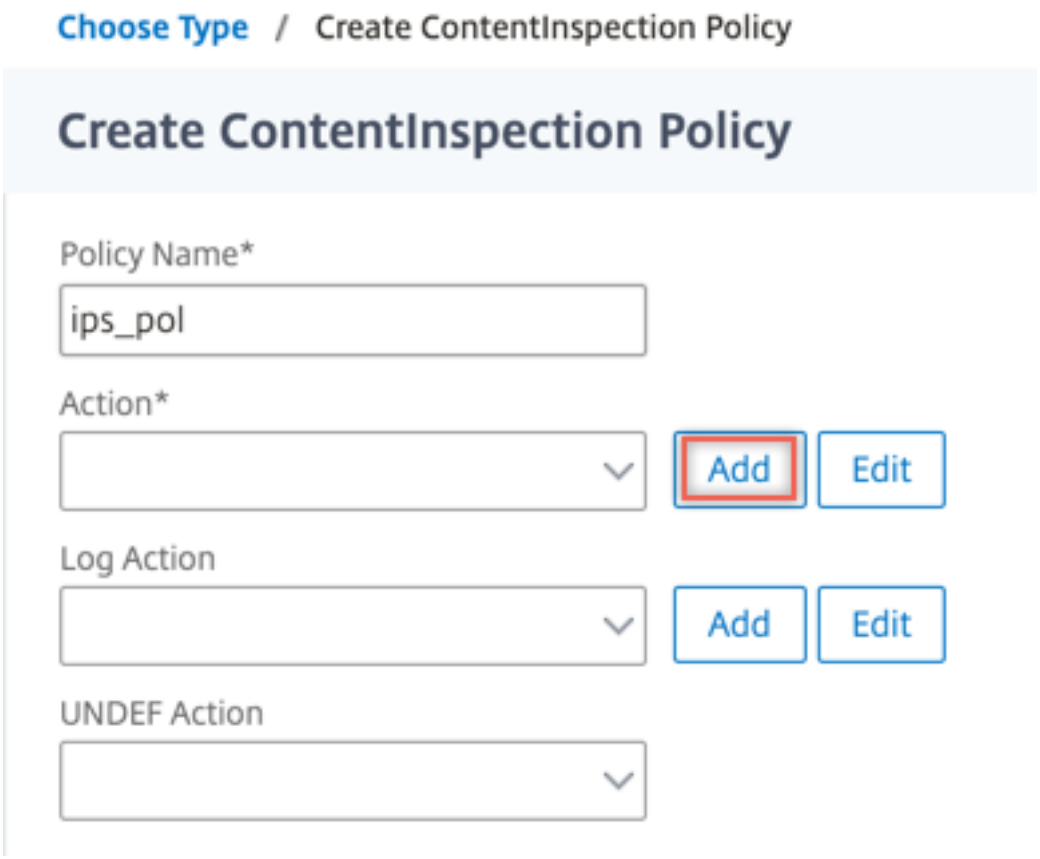
7. Vaya a **Secure Web Gateway > Servidores virtuales Proxy > Agregar**. Especifique un nombre, una dirección IP y un puerto. En **Configuración avanzada**, seleccione **Directivas**. Haga clic en el signo “+”.



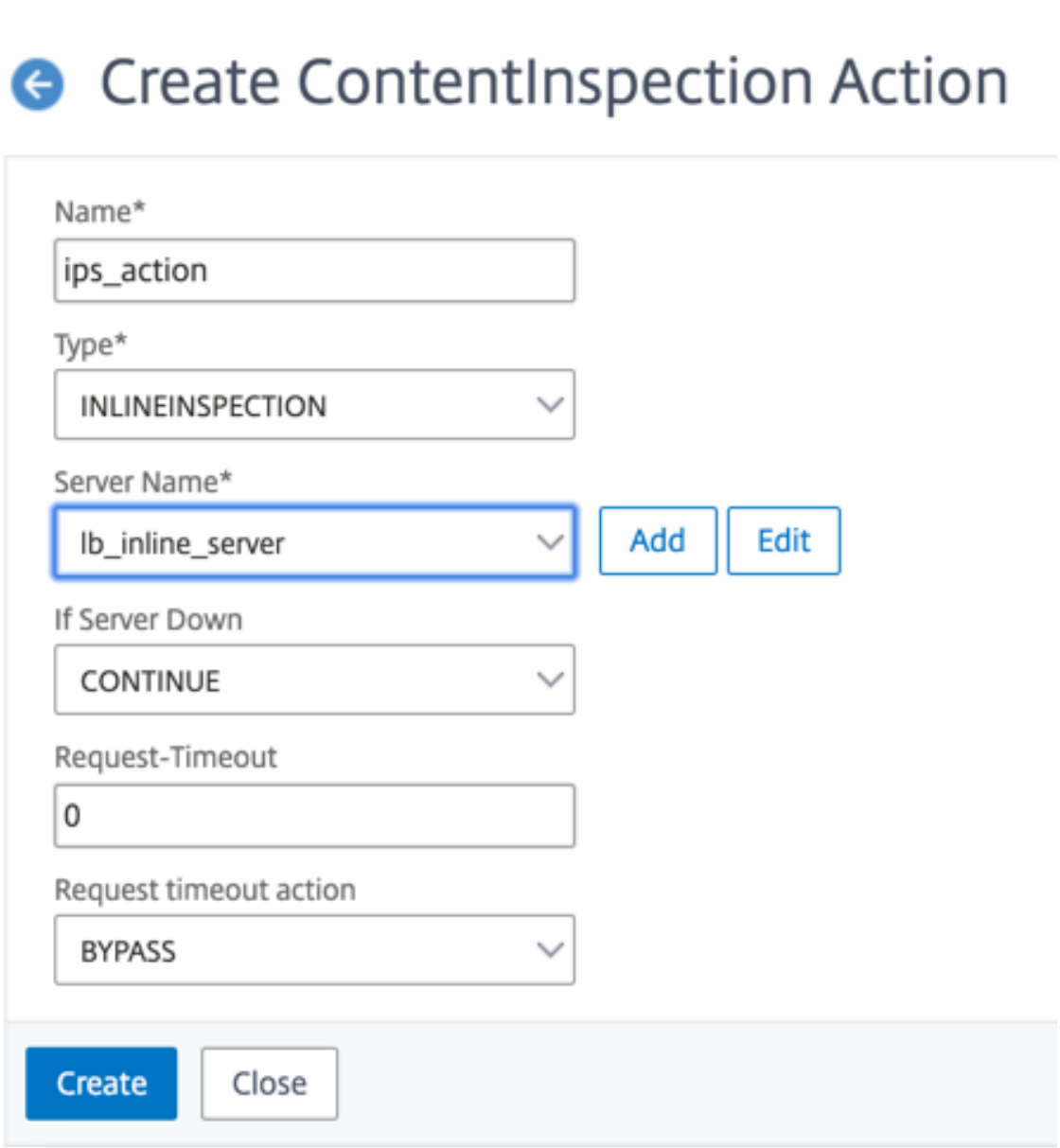
8. En **Elegir directiva**, seleccione **Inspección de contenido**. Haga clic en **Continuar**.



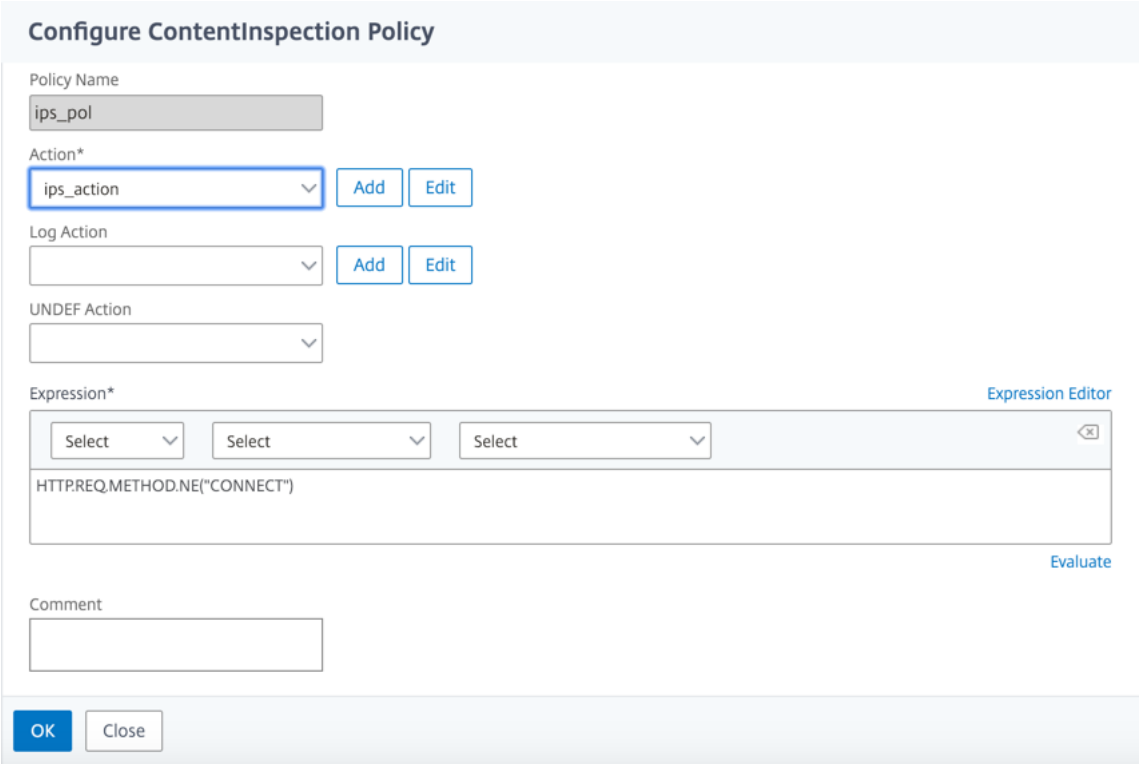
9. Haga clic en **Agregar**. Especifique un nombre. En **Acción**, haga clic en **Agregar**.



10. Especifique un nombre. En **Tipo**, seleccione **INLINEINSPECTION**. En **Nombre del servidor**, seleccione el servidor virtual de equilibrio de carga creado anteriormente.



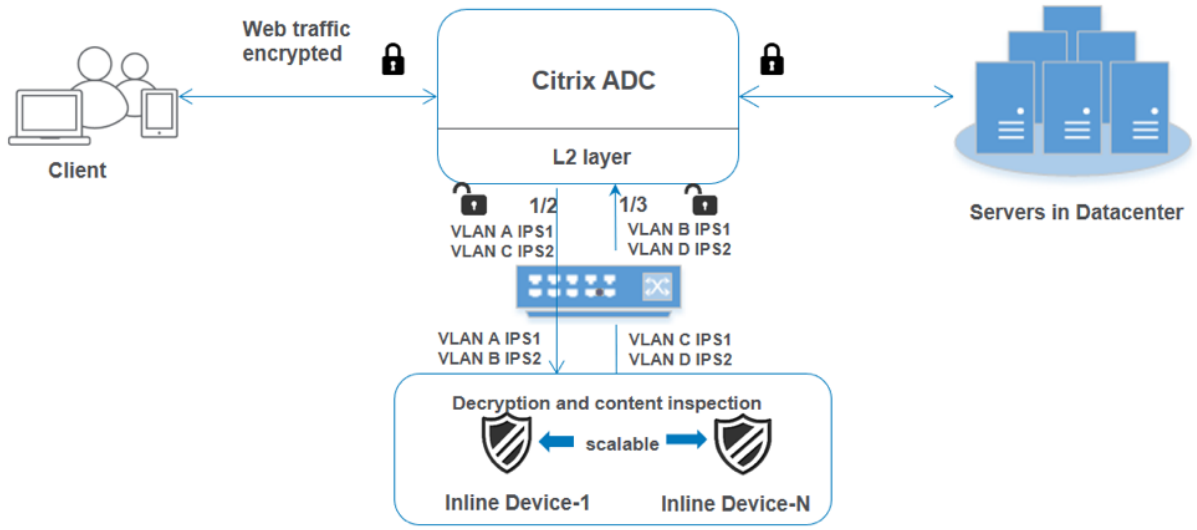
11. Haga clic en **Crear**. Especifique la regla y haga clic en **Crear**.



12. Haga clic en **Vincular**.
13. Haga clic en **Done**.

Caso 3: Equilibrio de carga de varios dispositivos en línea con interfaces compartidas

Si utiliza dos o más dispositivos en línea, puede equilibrar la carga de los dispositivos mediante diferentes servicios de inspección de contenido con interfaces compartidas. En este caso, la carga del dispositivo proxy de reenvío SSL equilibra el subconjunto de tráfico enviado a cada dispositivo a través de una interfaz compartida. El subconjunto se decide en función de las directivas configuradas. Por ejemplo, es posible que los archivos TXT o de imagen no se envíen para su inspección a los dispositivos en línea.



La configuración básica sigue siendo la misma que en el caso 2. Para este caso, vincule las interfaces a diferentes VLAN para segregar el tráfico de cada dispositivo en línea. Especifique las VLAN en los perfiles de inspección de contenido. Realice los siguientes pasos adicionales:

1. Enlazar las interfaces compartidas a diferentes VLAN.
2. Especifique las VLAN de entrada y salida en los perfiles de inspección de contenido.

Configuración mediante la CLI

Escriba los siguientes comandos en el símbolo del sistema. Se dan ejemplos después de cada comando.

1. Habilitar MBF.

```
enable ns mode mbf
```

1. Habilite la función.

```
enable ns feature contentInspection
```

1. Enlazar las interfaces compartidas a diferentes VLAN.

   ```
   bind vlan <id> -ifnum <interface> -tagged
   ```

Ejemplo:

```
1 bind vlan 100  - ifnum 1/2 tagged
2 bind vlan 200  - ifnum 1/3 tagged
3 bind vlan 300  - ifnum 1/2 tagged
```



```
4 bind vlan 400 -ifnum 1/3 tagged
5 <!--NeedCopy-->
```

1. Agregar perfil 1 para el servicio 1. Especifique las VLAN de entrada y salida en el perfil.

```
add contentInspection profile <name> -type InlineInspection -egressInterface
 <interface_name> -ingressInterface <interface_name>[-egressVlan <positive_integer
>] [-ingressVlan <positive_integer>]
```

Ejemplo:

```
add contentInspection profile ipsprof1 -type InlineInspection -egressInterface
 "1/3" -ingressinterface "1/2" -egressVlan 100 -ingressVlan 300
```

1. Agregar perfil 2 para el servicio 2. Especifique las VLAN de entrada y salida en el perfil.

```
add contentInspection profile <name> -type InlineInspection -egressInterface
 <interface_name> -ingressInterface <interface_name>[-egressVlan <positive_integer
>] [-ingressVlan <positive_integer>]
```

Ejemplo:

```
add contentInspection profile ipsprof2 -type InlineInspection -egressInterface
 "1/3" -ingressinterface "1/2" -egressVlan 200 -ingressVlan 400
```

1. Agregar servicio 1.

```
add service <service_name> <IP> TCP * - contentinspectionProfileName <Name>
 -healthMonitor NO -usip YES -useproxyport NO
```

Ejemplo:

```
add service ips_service1 192.168.10.2 TCP * -healthMonitor NO -usip YES -
useproxyport NO -contentInspectionProfileName ipsprof1
```

1. Agregar servicio 2.

```
add service <service_name> <IP> TCP * - contentinspectionProfileName <Name>
 -healthMonitor NO -usip YES -useproxyport NO
```

Ejemplo:

```
add service ips_service2 192.168.10.3 TCP * -healthMonitor NO -usip YES -
useproxyport NO -contentInspectionProfileName ipsprof2
```

1. Agregue un servidor virtual de equilibrio de carga.

```
add lb vserver <LB_VSERVER_NAME> TCP <IP> <port>
```

Ejemplo:

```
add lb vserver lb_inline_vserver TCP 192.0.2.100 *
```


1. Enlazar los servicios al servidor virtual de equilibrio de carga.

```
bind lb vserver <LB_VSERVER_NAME> <service_name>
bind lb vserver <LB_VSERVER_NAME> <service_name>
```

Ejemplo:

```
bind lb vserver lb_inline_vserver ips_service1
bind lb vserver lb_inline_vserver ips_service2
```

1. Especifique el servidor virtual de equilibrio de carga en la acción de inspección de contenido.

```
add contentInspection action <name> -type INLINEINSPECTION -serverName <
string>
```

Ejemplo:

```
add contentInspection action ips_action -type INLINEINSPECTION -serverName
lb_inline_vserver
```

1. Agregar una directiva de inspección de contenido. Especifique la acción de inspección de contenido en la directiva.

```
add contentInspection policy <name> -rule <expression> -action <string>
```

Ejemplo:

```
add contentInspection policy ips_pol -rule "HTTP.REQ.METHOD.NE(\"CONNECT\")
"-action ips_action
```

1. Agregue un servidor virtual proxy.

```
add cs vserver <name> PROXY <IPAddress> <port> -l2Conn ON
```

Ejemplo:

```
add cs vserver transparentcs PROXY * * -l2Conn ON
```

1. Enlazar la directiva de inspección de contenido al servidor virtual.

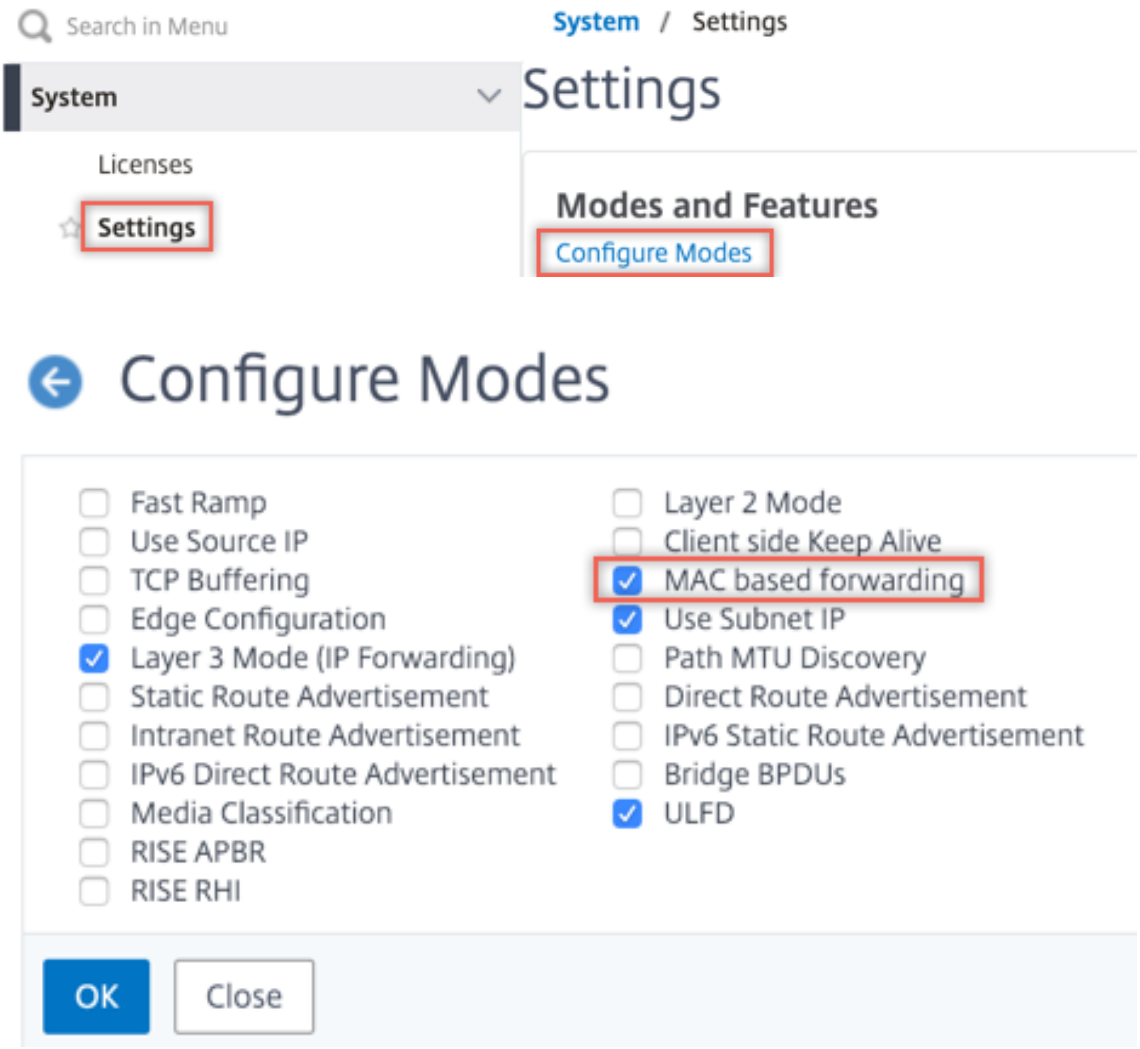
```
bind cs vserver <name> -policyName <string> -priority <positive_integer> -
gotoPriorityExpression <expression> -type REQUEST
```

Ejemplo:

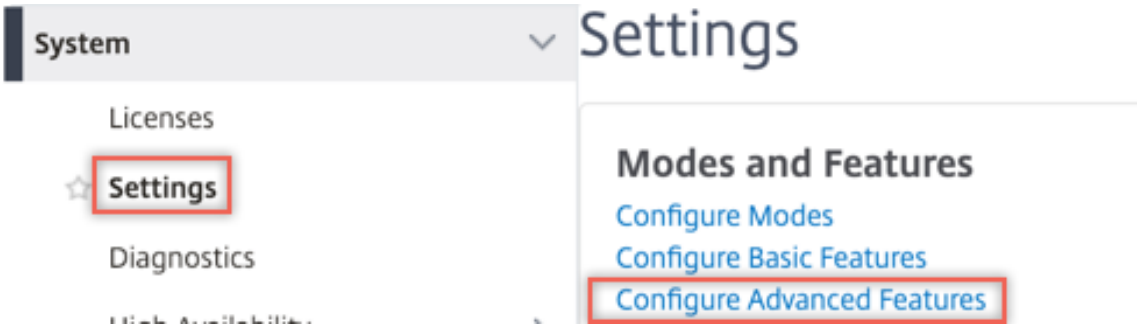
```
bind cs vserver explicitcs -policyName ips_pol -priority 1 -gotoPriorityExpression
 END -type REQUEST
```

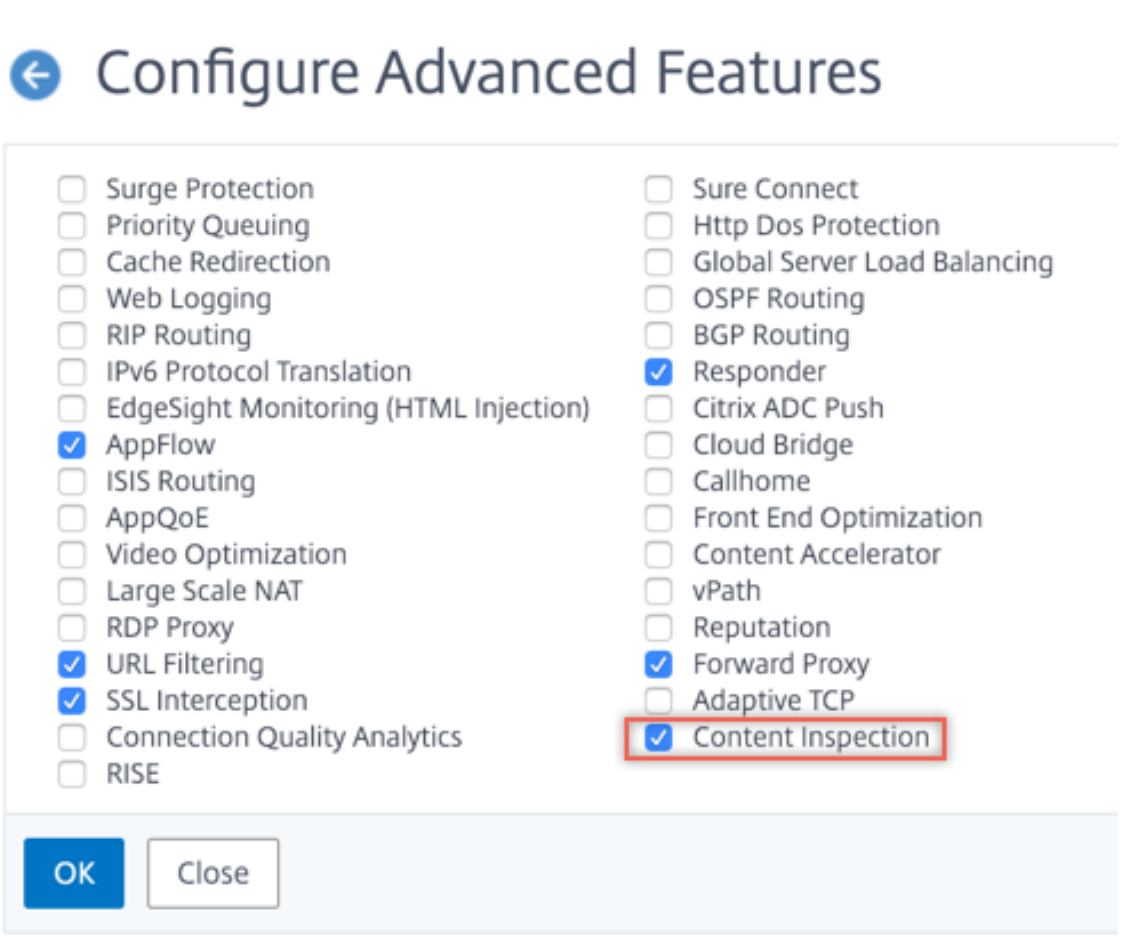
Configuración mediante la GUI

1. Vaya a **Sistema > Configuración**. En **Modos y funciones**, haga clic en **Configurar modos**.

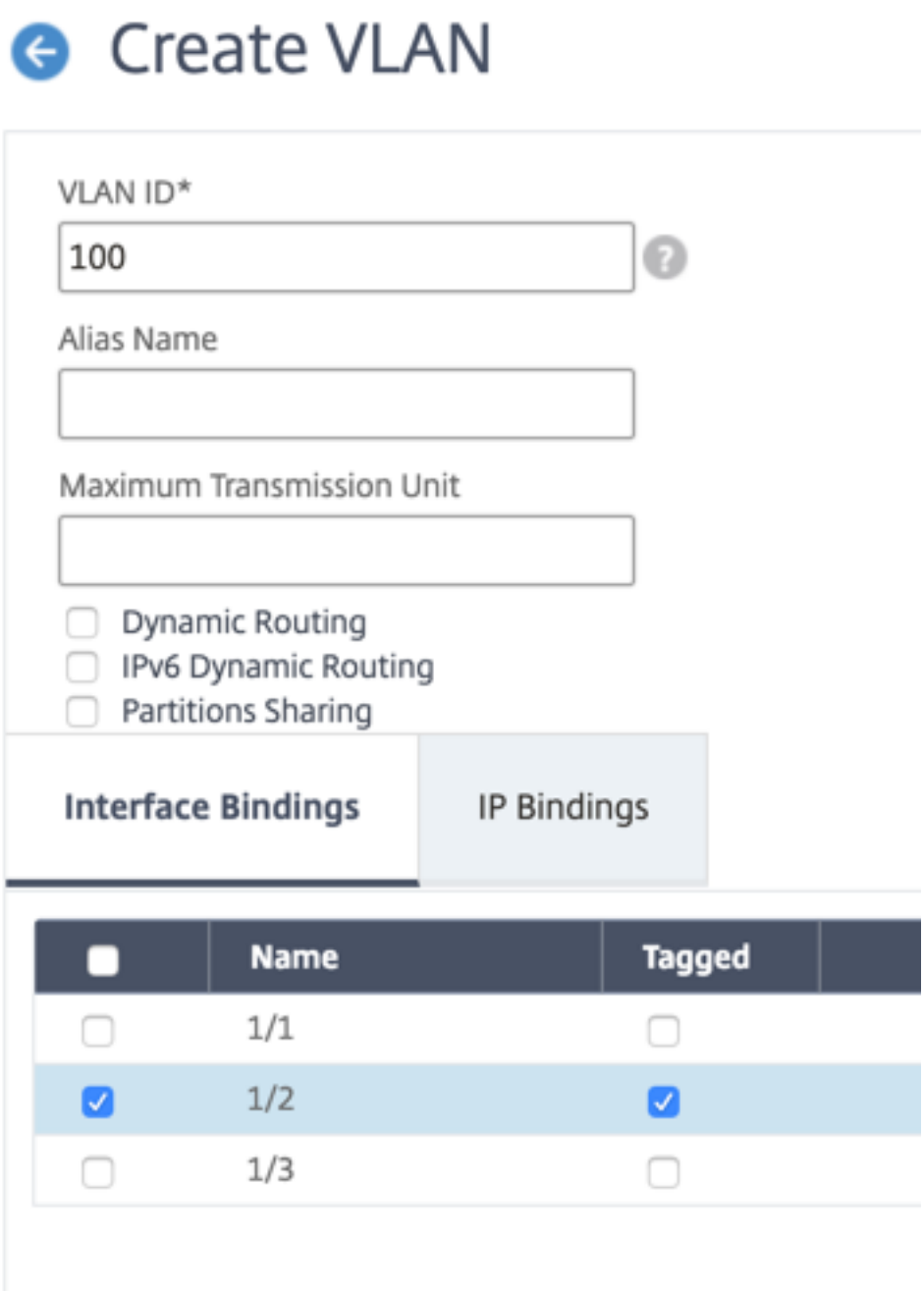


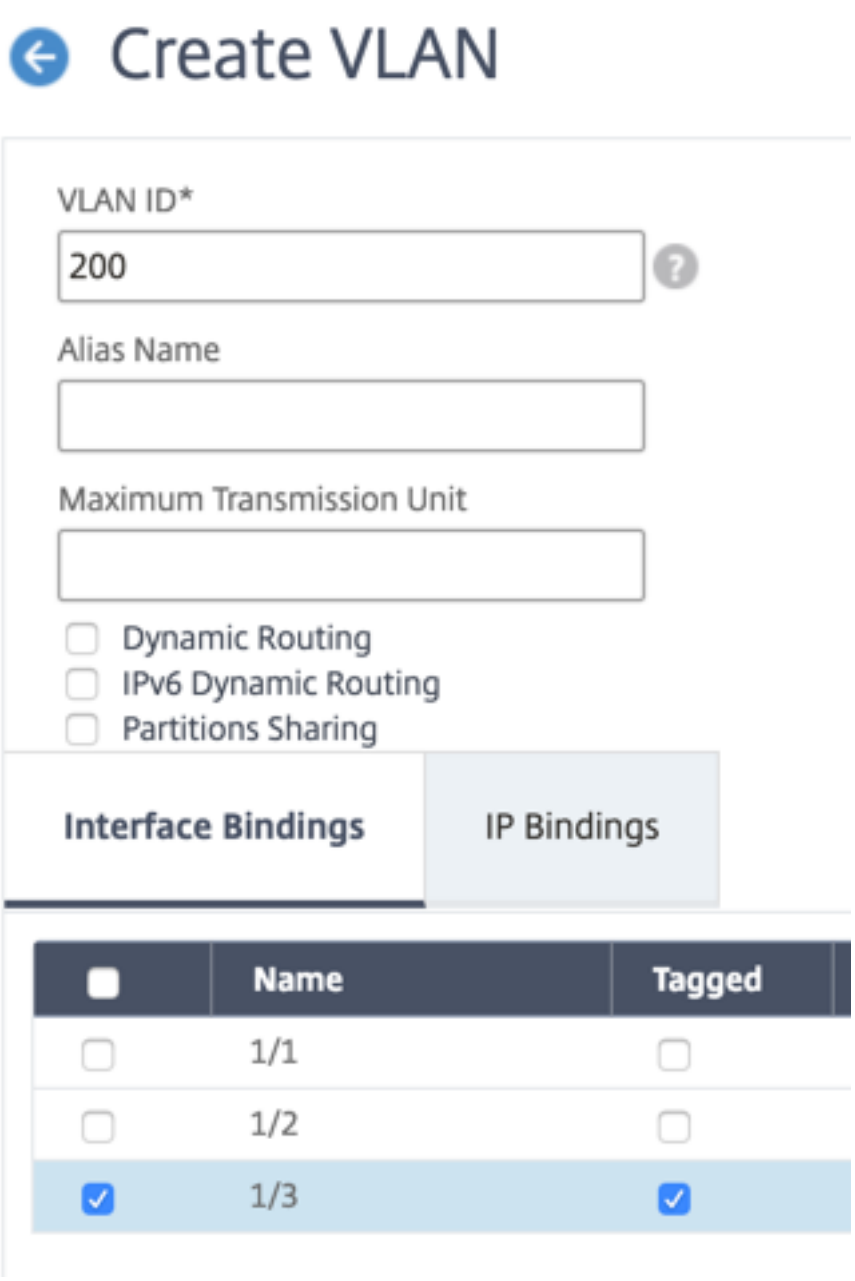
2. Vaya a **Sistema > Configuración**. En **Modos y funciones**, haga clic en **Configurar funciones avanzadas**.

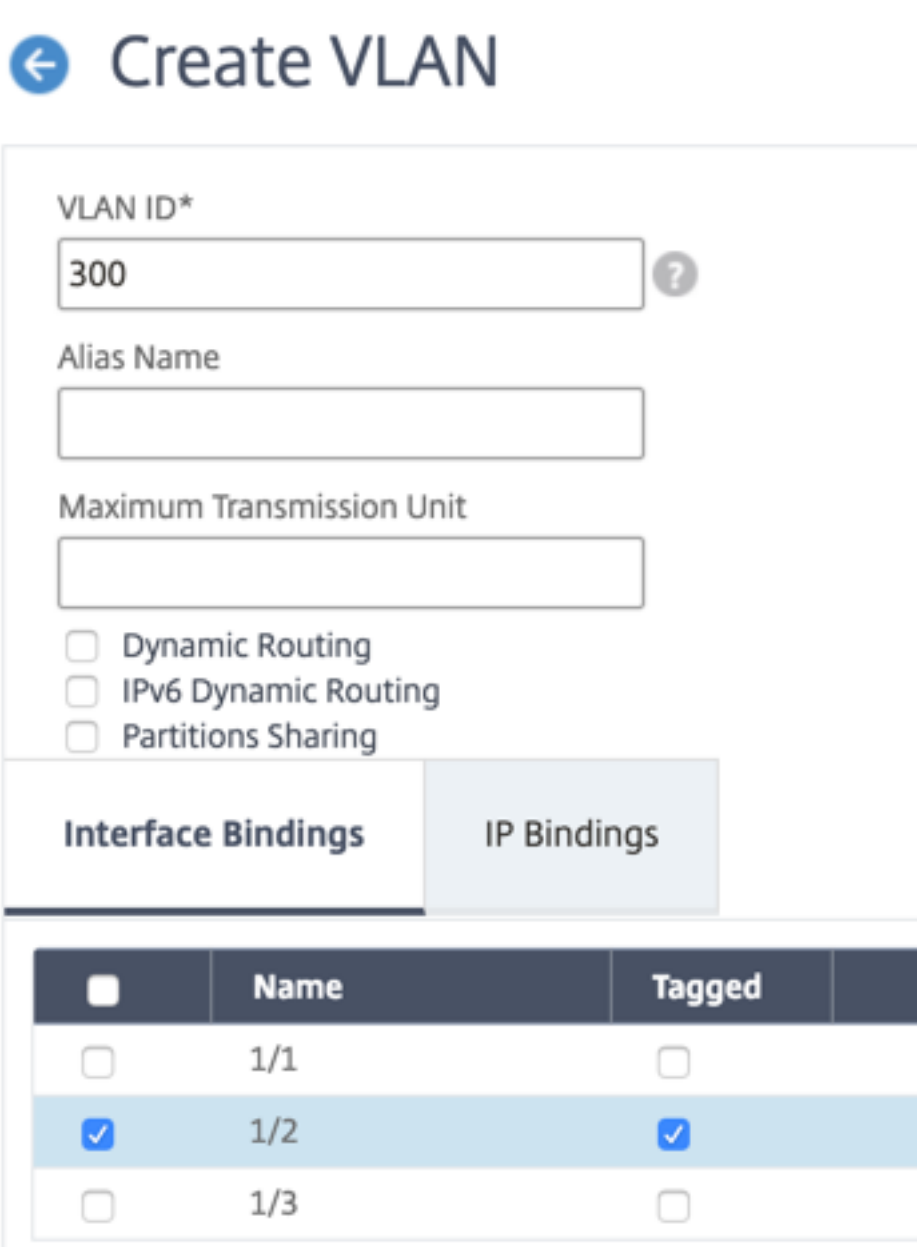


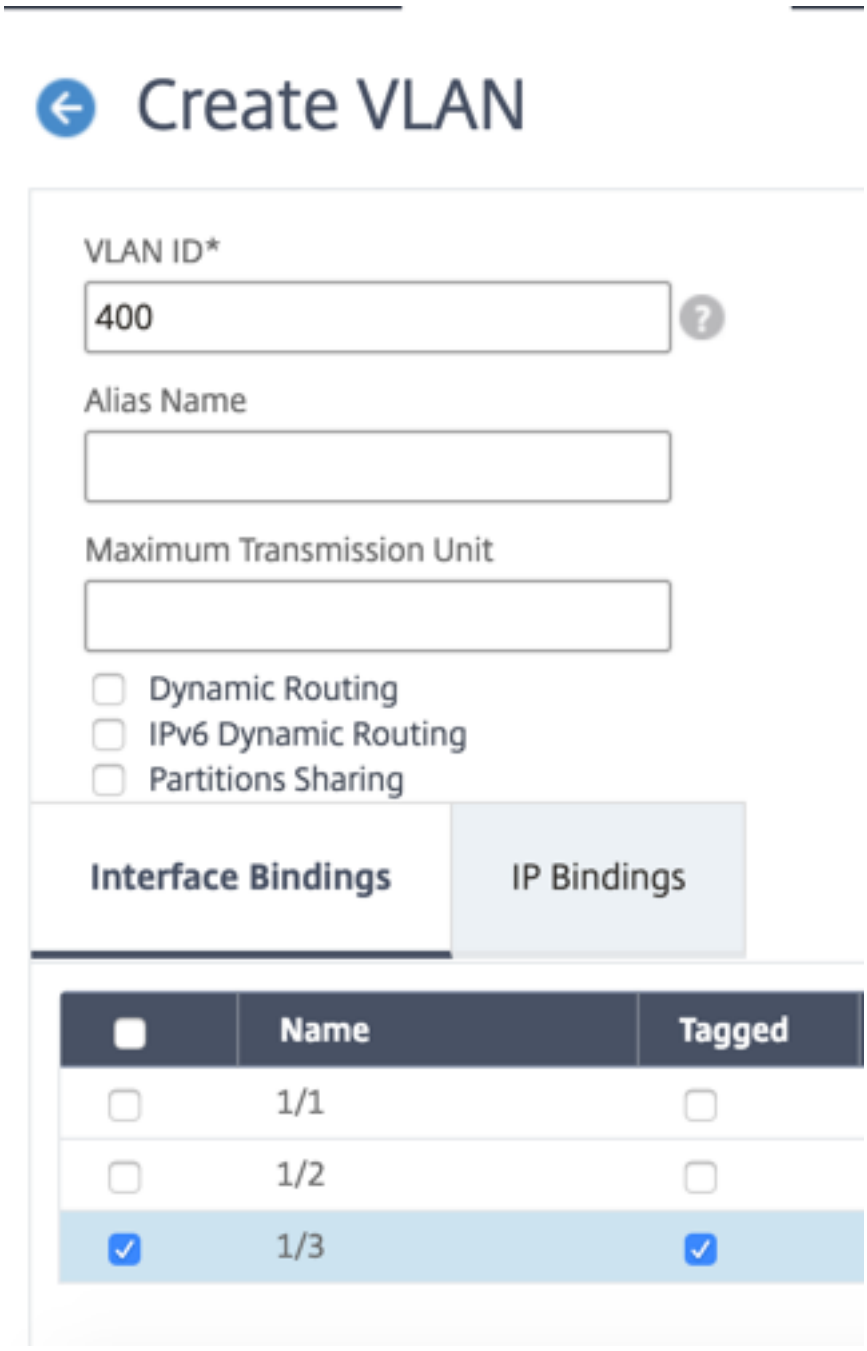


3. Vaya a **Sistema > Red > VLAN > Agregar**. Agregue cuatro VLAN y etiquetarlas a las interfaces.

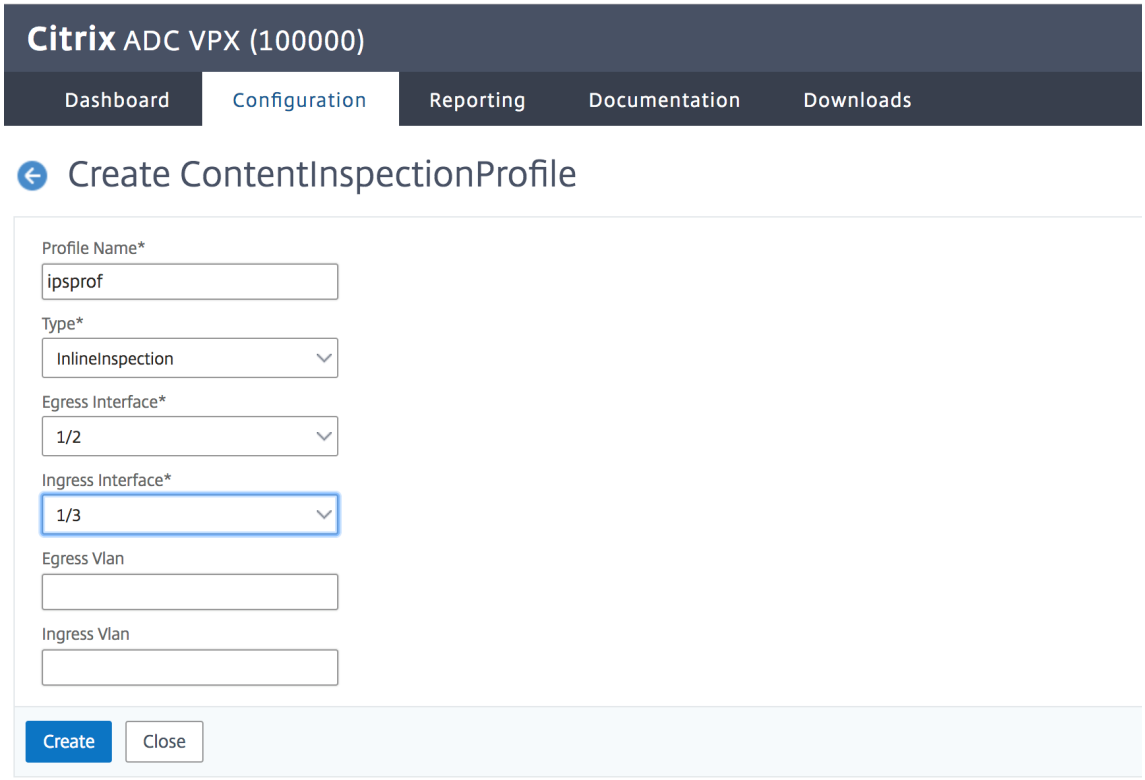




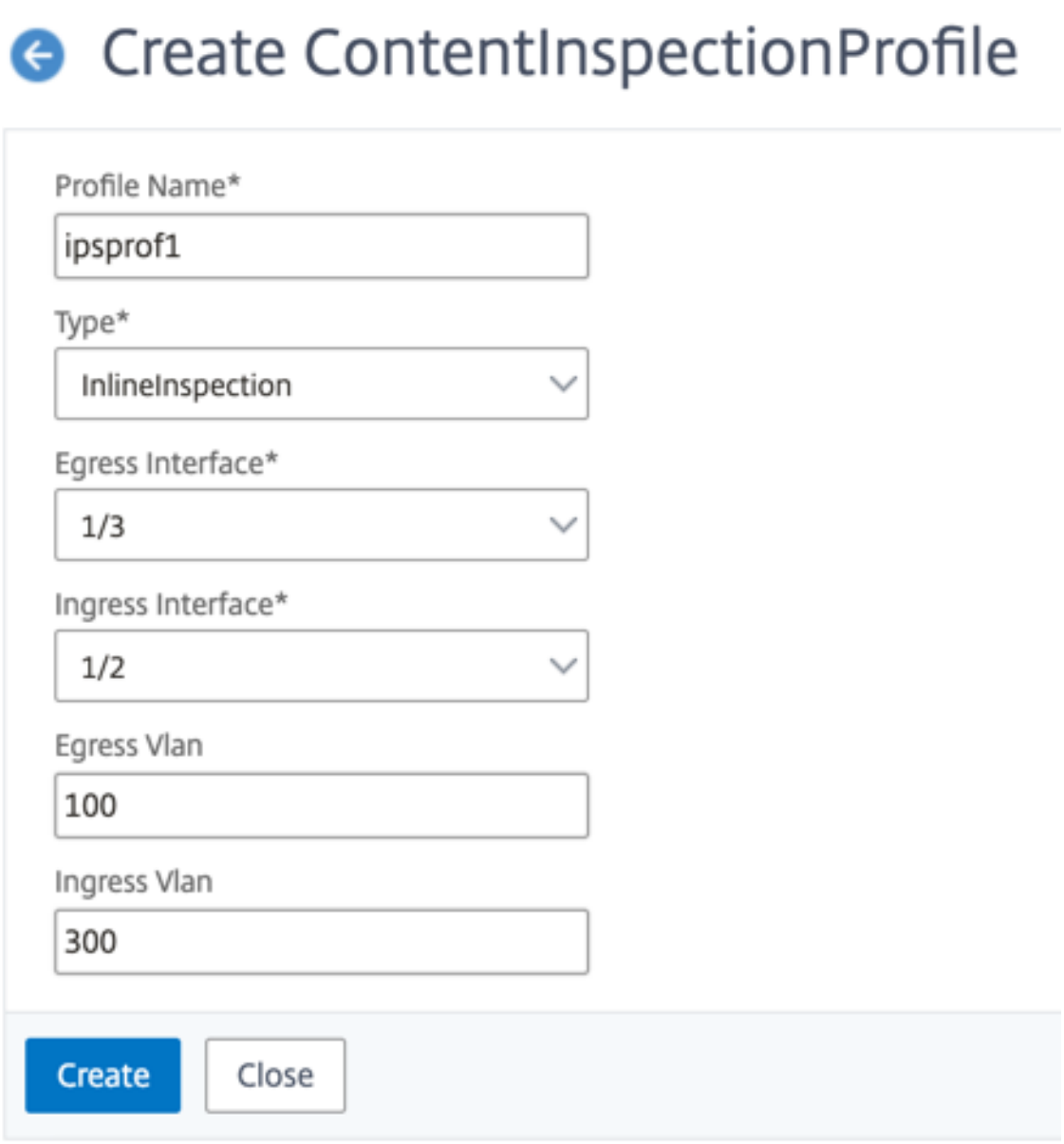




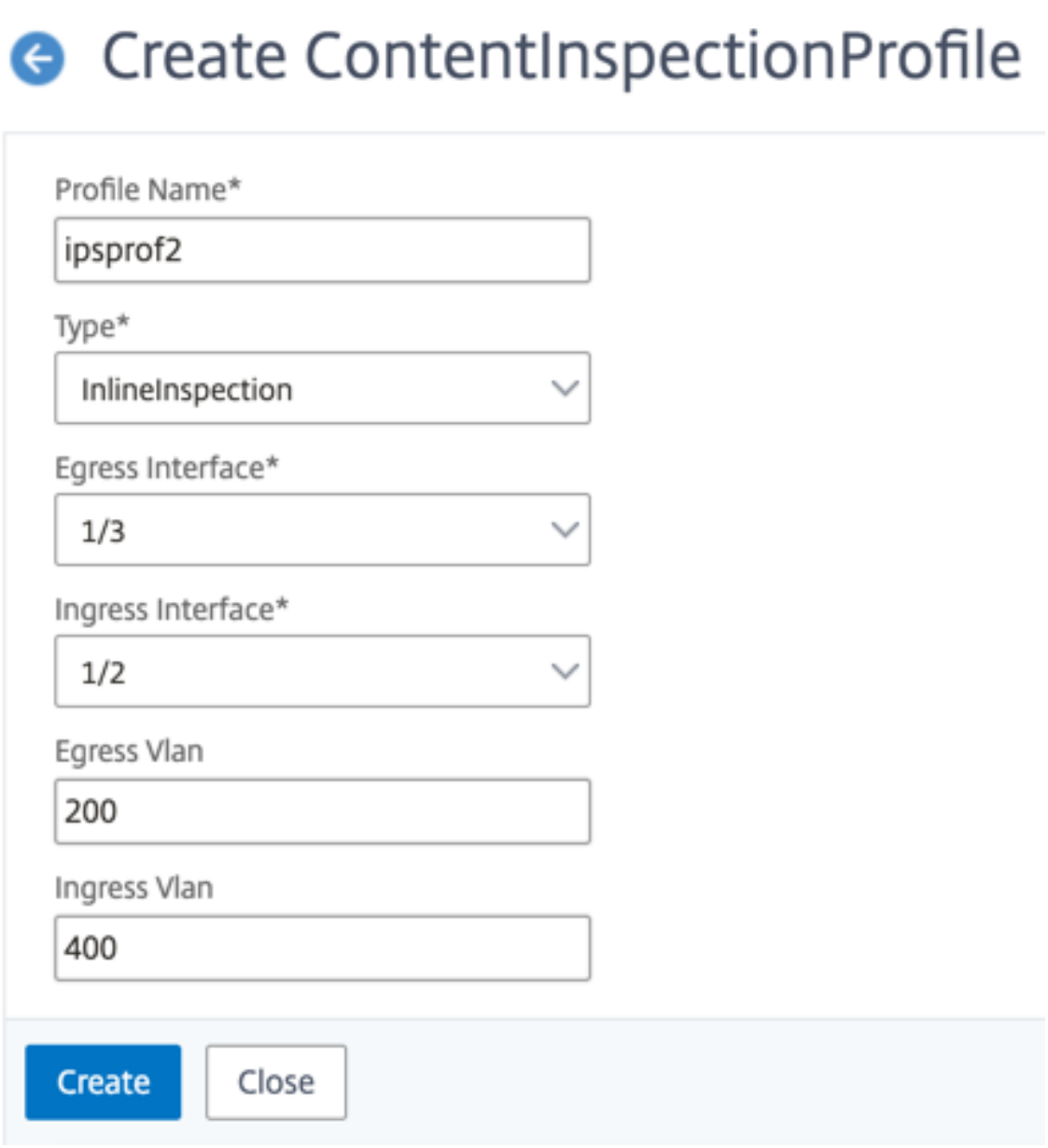
4. Vaya a **Secure Web Gateway > Inspección de contenido > Perfiles de inspección de contenido**. Haga clic en **Agregar**.



Especifique las VLAN de entrada y salida.

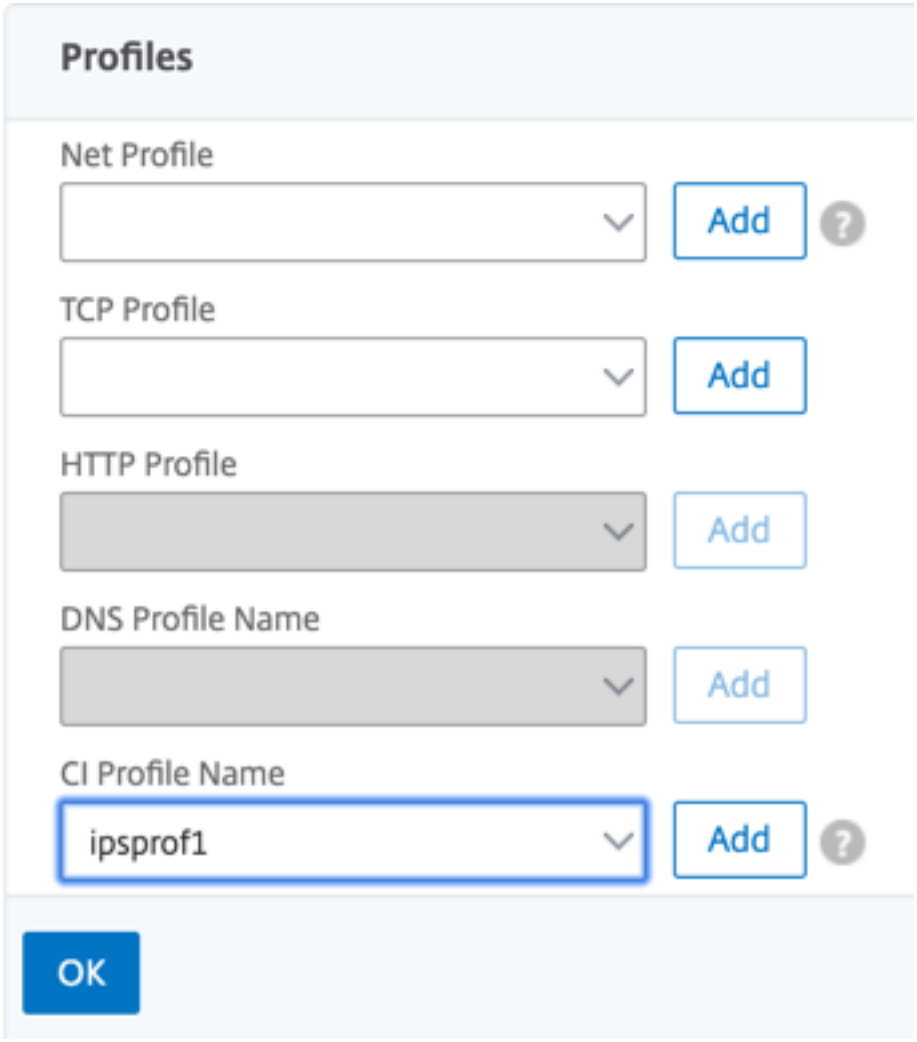


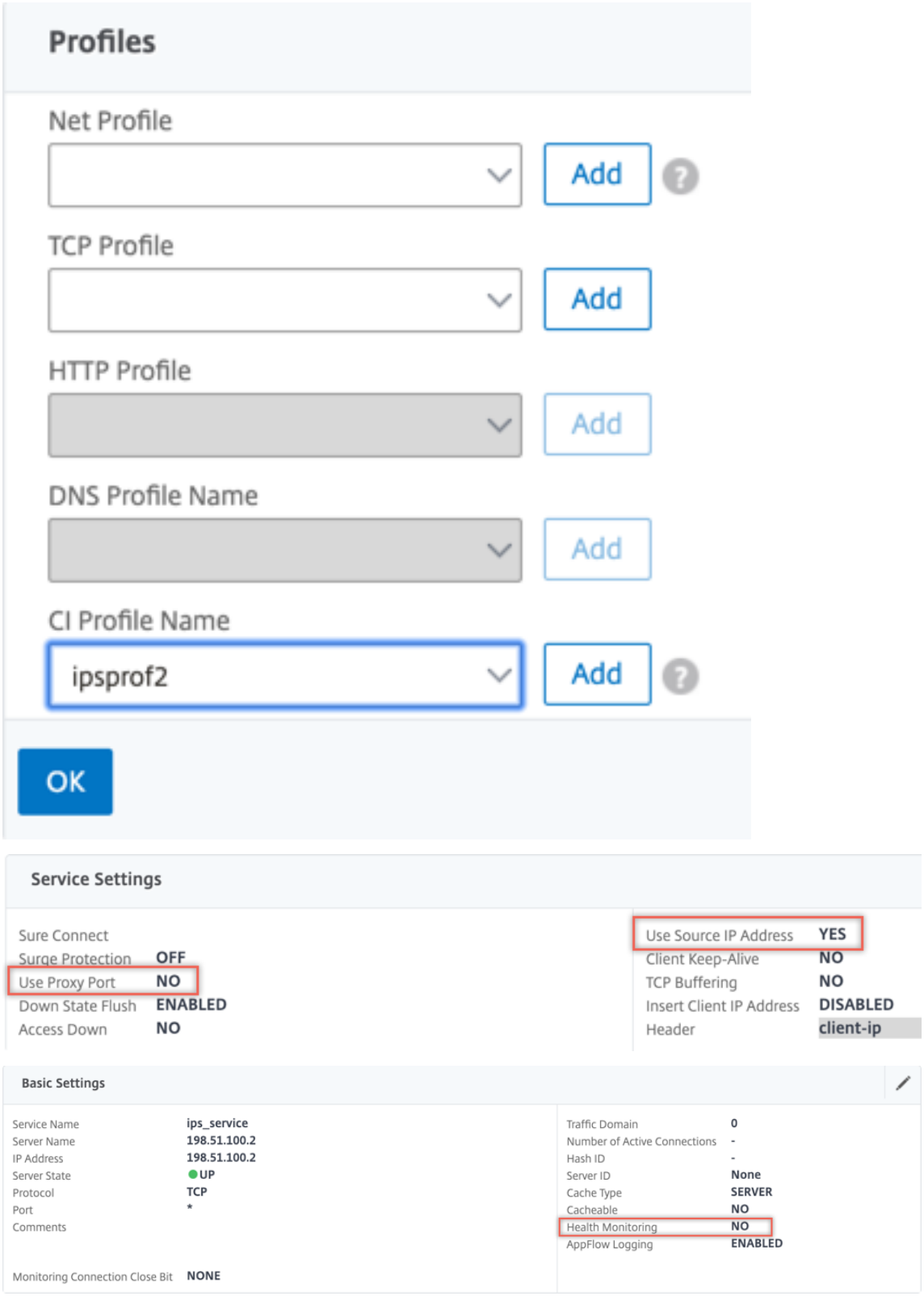
Cree otros perfiles. Especifique una VLAN de entrada y salida diferente en el segundo perfil.



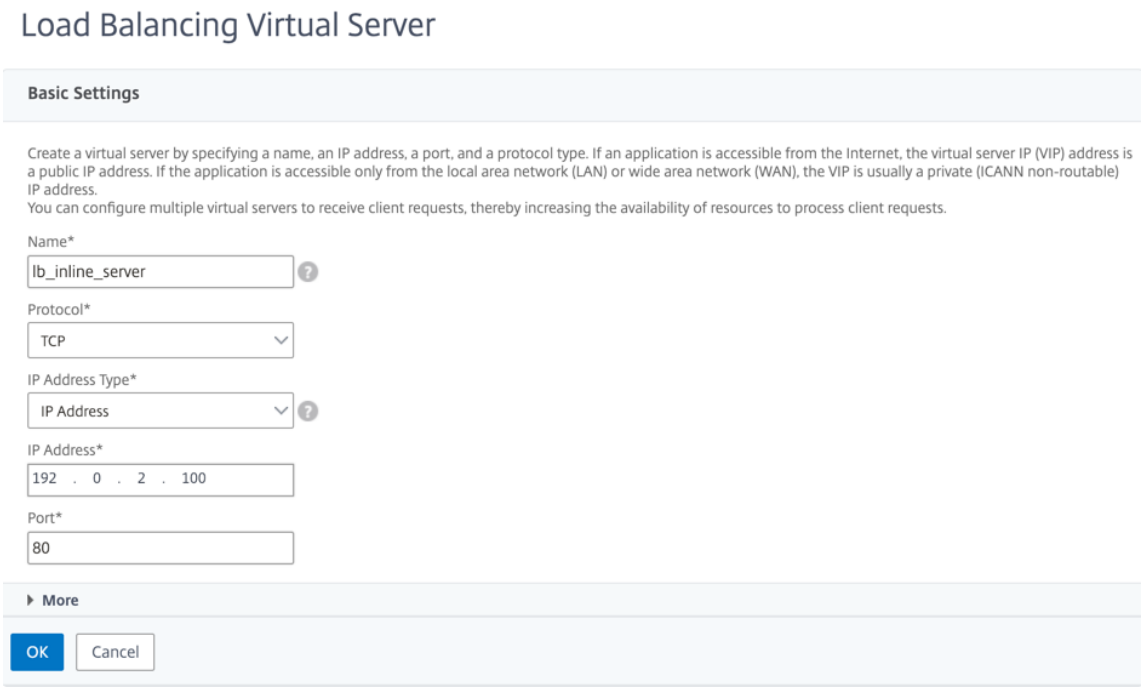
5. Desplácese hasta **Equilibrio de carga > Servicios > Agregar** y agregar un servicio. En **Configuración avanzada**, haga clic en **Perfiles**. En la lista **Nombre de perfil de CI**, seleccione el perfil de inspección de contenido creado anteriormente. En **Configuración del servicio**, establezca **Usar dirección IP de origen**en YES y **Usar puerto proxy**en No. En **Configuración básica**, establezca **Supervisión del estado**en NO.

   Cree dos servicios. Especifique direcciones IP ficticias que no pertenecen a ninguno de los dispositivos, incluidos los dispositivos en línea. Especifique el perfil 1 en el servicio 1 y el perfil 2 en el servicio 2.

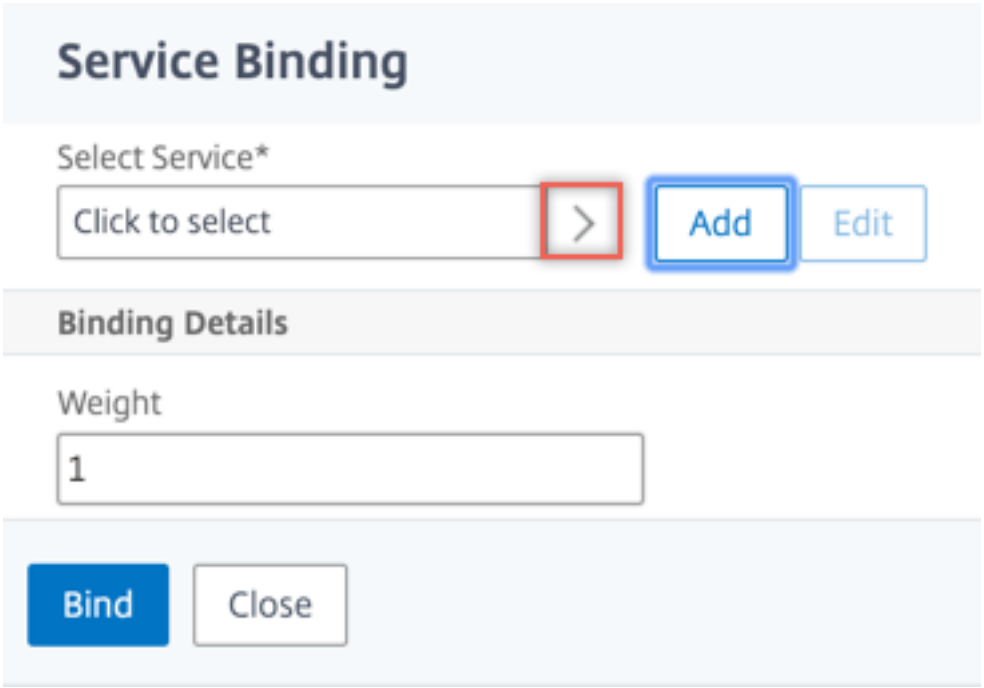


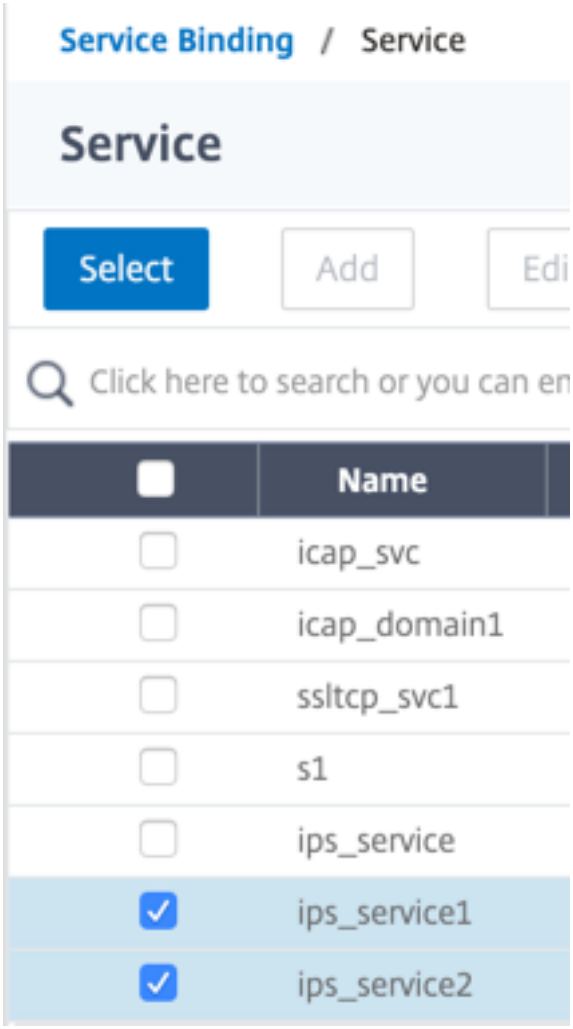


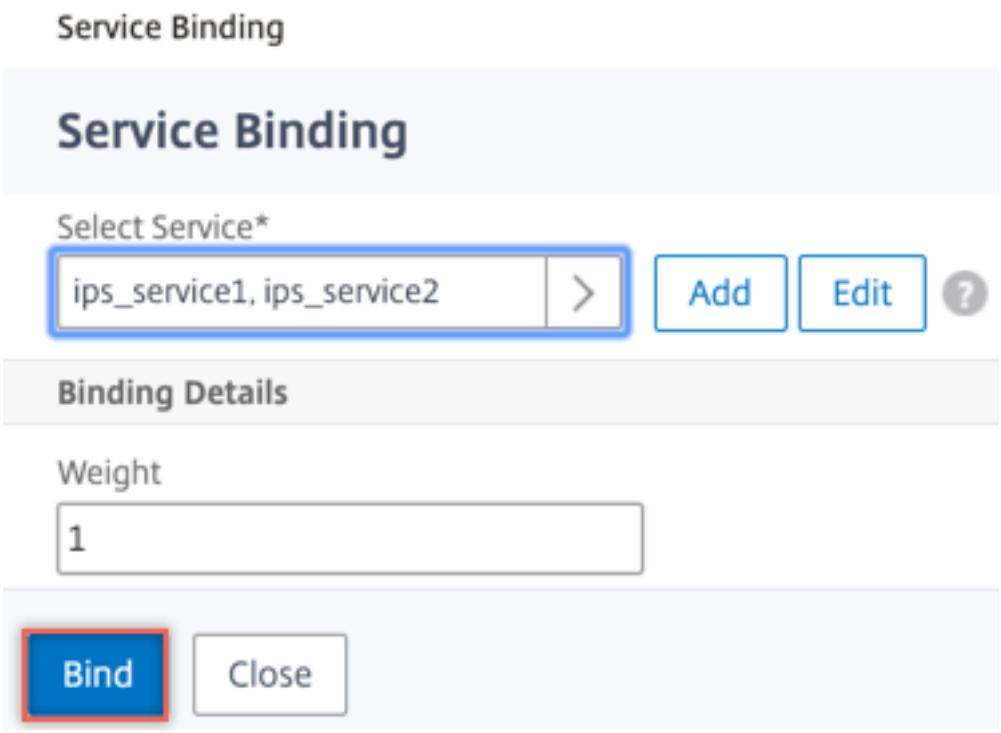
6. Desplácese hasta **Equilibrio de carga > Servidores virtuales > Agregar**. Cree un servidor virtual de equilibrio de carga TCP.



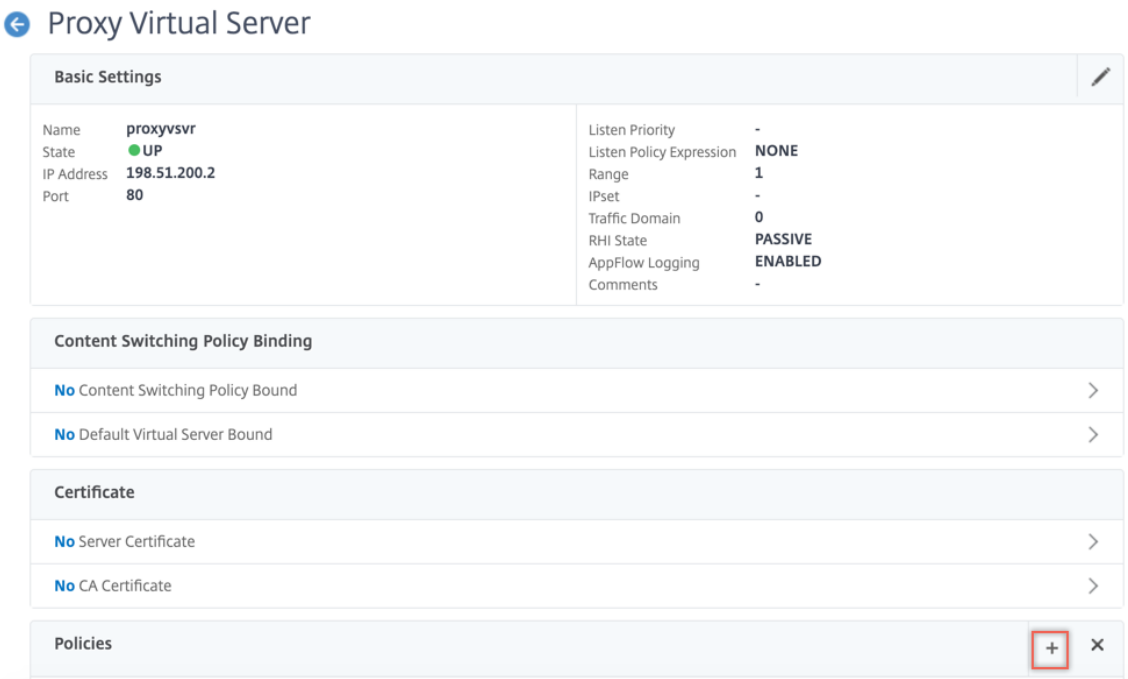
7. Haga clic en **Aceptar**.
8. Haga clic dentro de la sección **Enlace del servicio de servidor virtual de equilibrio de carga**. En **Enlace de servicio**, haga clic en la flecha **de Seleccionar servicio**. Seleccione los dos servicios creados anteriormente y haga clic en **Seleccionar**. Haga clic en **Vincular**.



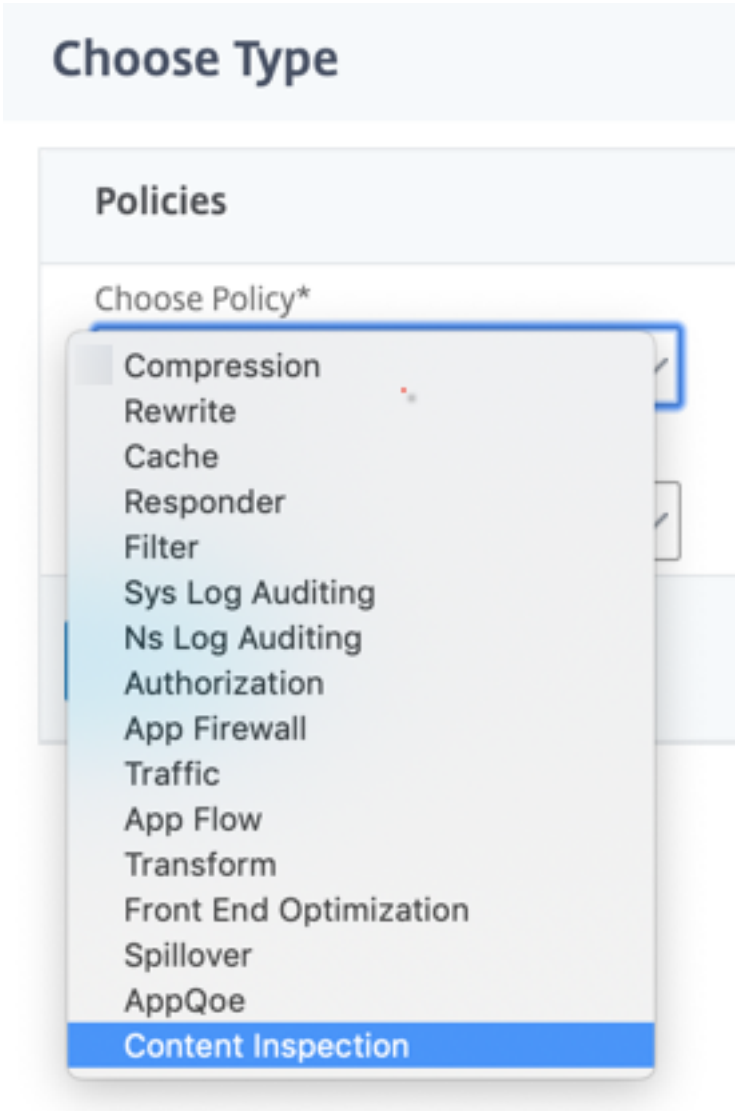




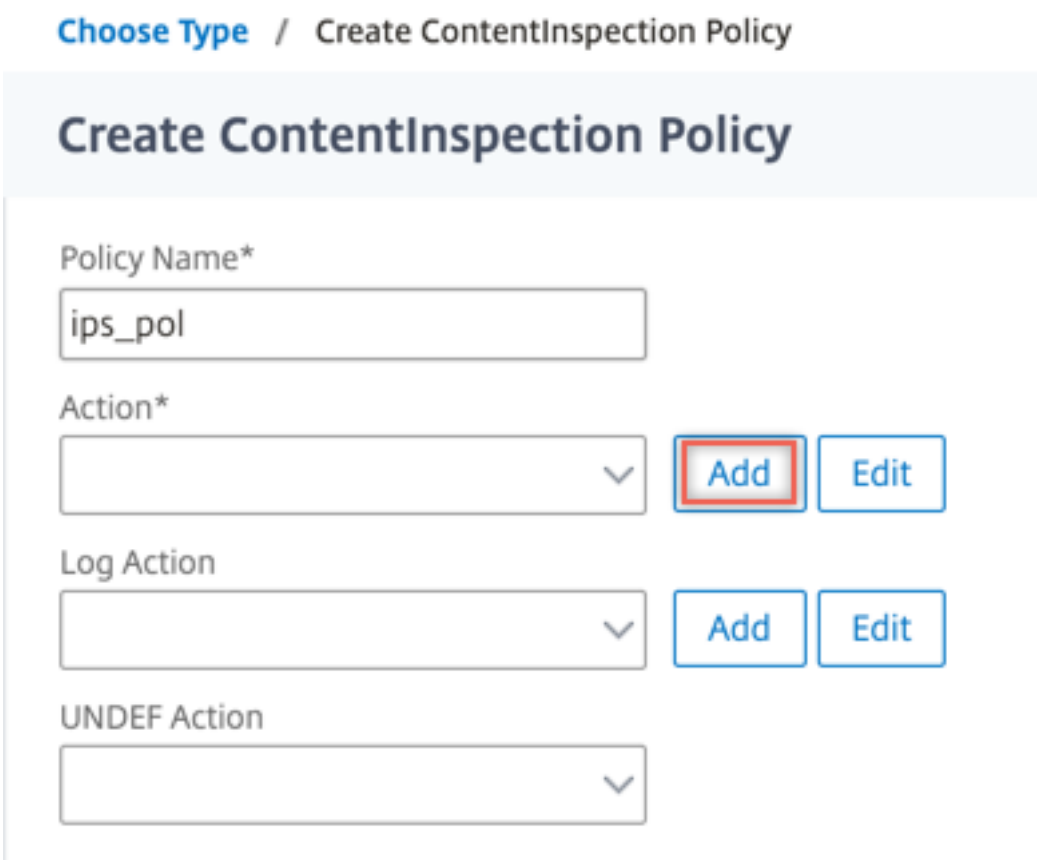
9. Vaya a **Secure Web Gateway > Servidores virtuales Proxy > Agregar**. Especifique un nombre, una dirección IP y un puerto. En **Configuración avanzada**, seleccione **Directivas**. Haga clic en el signo “+”.



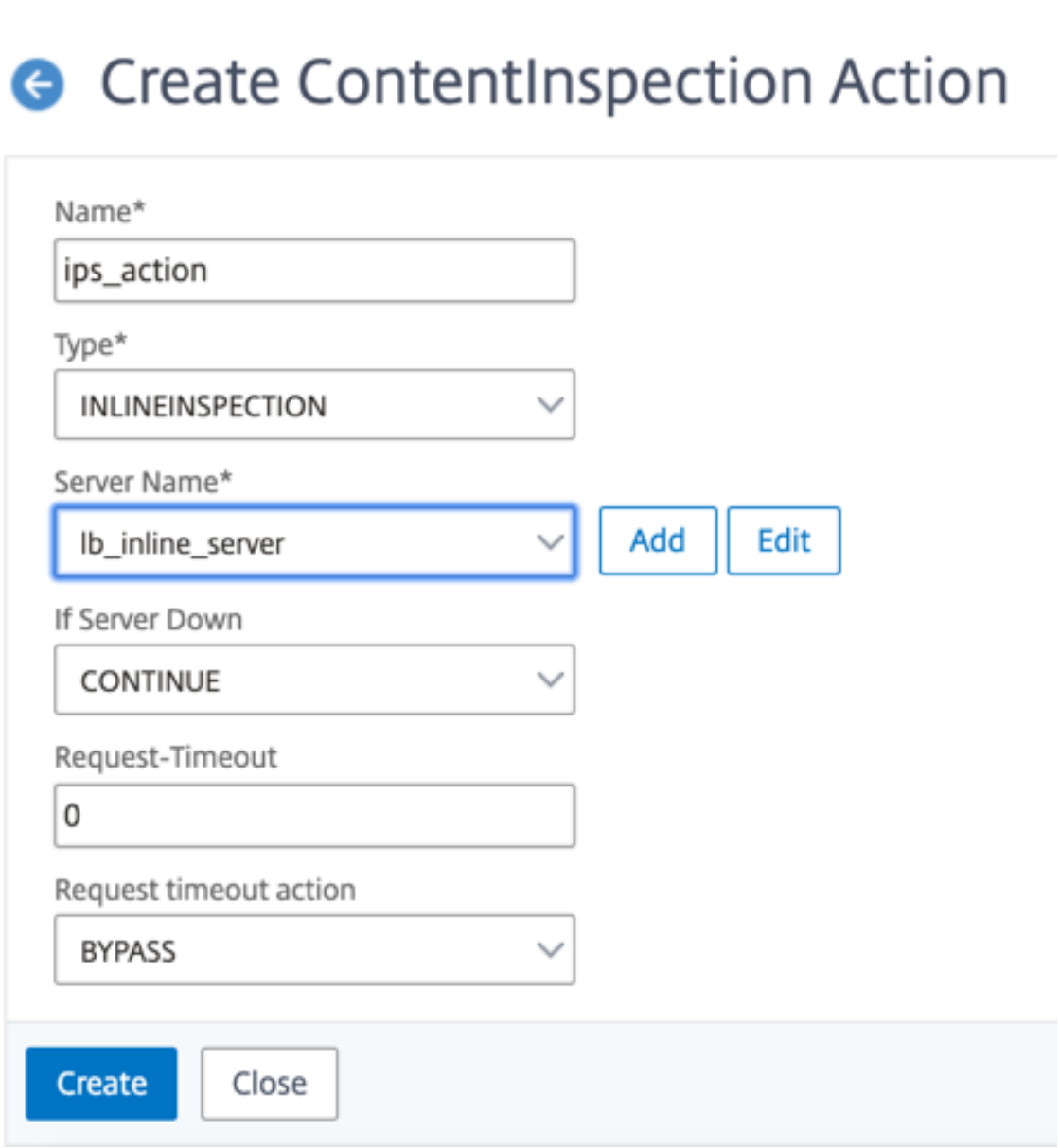
10. En **Elegir directiva**, seleccione **Inspección de contenido**. Haga clic en **Continuar**.



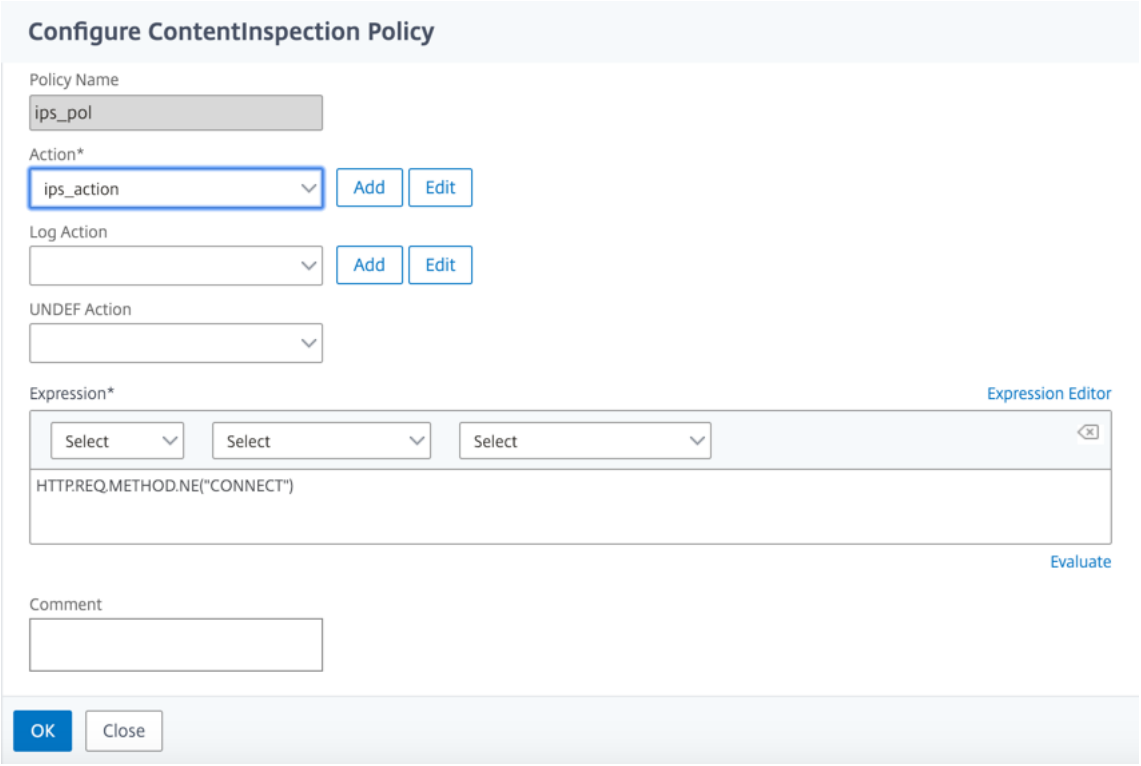
11. Haga clic en **Agregar**. Especifique un nombre. En **Acción**, haga clic en **Agregar**.



12. Especifique un nombre. En **Tipo**, seleccione **INLINEINSPECTION**. En **Nombre del servidor**, seleccione el servidor virtual de equilibrio de carga creado anteriormente.



13. Haga clic en **Crear**. Especifique la regla y haga clic en **Crear**.



14. Haga clic en **Vincular**.
15. Haga clic en **Done**.

Integración de Citrix ADC con dispositivos de seguridad pasivos (sistema de detección de intrusiones)

January 21, 2022

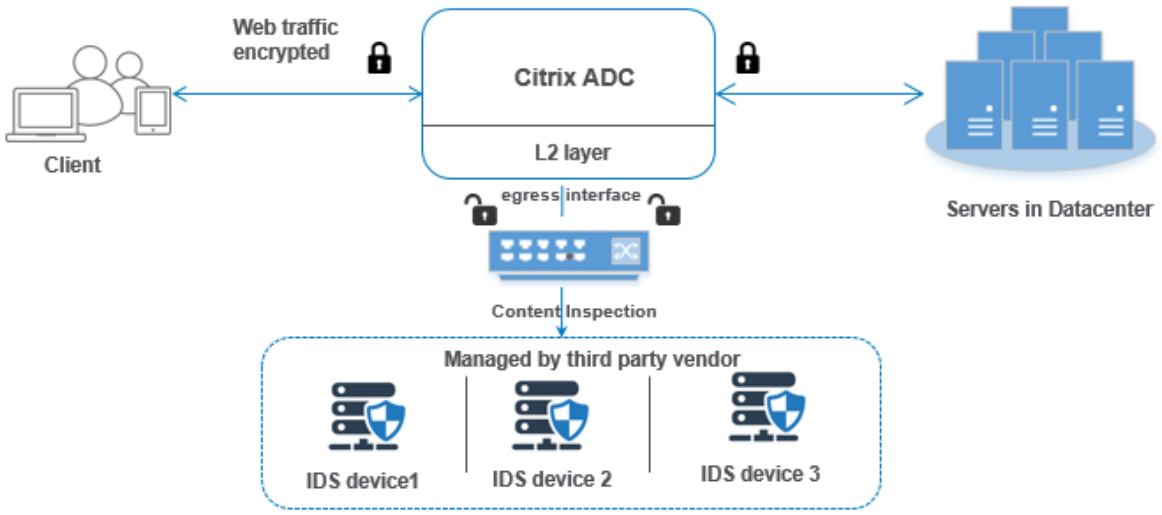
Un dispositivo Citrix ADC ahora se integra con dispositivos de seguridad pasivos, como el Sistema de detección de intrusiones (IDS). Estos dispositivos pasivos almacenan registros y activan alertas cuando detectan un tráfico incorrecto o no conforme. También genera informes para el propósito de cumplimiento. Si el dispositivo Citrix ADC está integrado con dos o más dispositivos IDS y cuando hay un gran volumen de tráfico, el dispositivo puede equilibrar la carga de los dispositivos clonando el tráfico en el nivel del servidor virtual.

Para una protección de seguridad avanzada, un dispositivo Citrix ADC se integra con dispositivos de seguridad pasivos, como IDS, implementados en modo de solo detección. Estos dispositivos almacenan registros y activan alertas cuando detectan un tráfico incorrecto o que no cumple con las normas. También genera informes para el propósito de cumplimiento. A continuación se presentan algunos de los beneficios de integrar Citrix ADC con un dispositivo IDS.

- **Inspeccionar el tráfico cifrado**. La mayoría de los dispositivos de seguridad eluden el tráfico cifrado, lo que deja a los servidores vulnerables a Un dispositivo Citrix ADC puede descifrar el tráfico y enviarlo a los dispositivos IDS para mejorar la seguridad de la red del cliente.
- **Descarga de dispositivos en línea del procesamiento TLS/SSL**. El procesamiento TLS/SSL es caro y da como resultado una CPU de sistema alta en los dispositivos de detección de intrusiones si descifran el tráfico. A medida que el tráfico cifrado crece a un ritmo acelerado, estos sistemas no pueden descifrar ni inspeccionar el tráfico cifrado. Citrix ADC ayuda a descargar el tráfico a los dispositivos IDS desde el procesamiento TLS/SSL. Esta forma de descargar datos da como resultado que un dispositivo IDS admita un alto volumen de inspección de tráfico.
- **Carga de dispositivos IDS de equilibrio**. La carga del dispositivo Citrix ADC equilibra la carga de varios dispositivos IDS cuando hay un gran volumen de tráfico al clonar el tráfico en el nivel del servidor virtual.
- **Replicar el tráfico en dispositivos pasivos**. El tráfico que fluye hacia el dispositivo se puede replicar en otros dispositivos pasivos para generar informes de cumplimiento. Por ejemplo, pocas agencias gubernamentales exigen que todas las transacciones se registren en algunos dispositivos pasivos.
- **Dirigir el tráfico a varios dispositivos pasivos**. Algunos clientes prefieren desplegarse o replicar el tráfico entrante en varios dispositivos pasivos.
- **Selección inteligente del tráfico**. Es posible que no se deba inspeccionar el contenido de todos los paquetes que fluyen hacia el dispositivo, por ejemplo, la descarga de archivos de texto. El usuario puede configurar el dispositivo Citrix ADC para seleccionar tráfico específico (por ejemplo, archivos.exe) para su inspección y enviar el tráfico a los dispositivos IDS para procesar los datos.

Cómo se integra Citrix ADC con el dispositivo IDS con conectividad L2

El siguiente diagrama muestra cómo se integra IDS con un dispositivo Citrix ADC.



La interacción de los componentes se da de la siguiente manera:

1. Un cliente envía una solicitud HTTP/HTTPS al dispositivo Citrix ADC.
2. El dispositivo intercepta el tráfico y lo replica en un dispositivo IDS en función de la evaluación de la directiva de inspección de contenido.
3. Si el tráfico está cifrado, el dispositivo descifra los datos y los envía como texto sin formato.
4. Según la evaluación de directivas, el dispositivo aplica una acción de inspección de contenido de tipo “ESPEJO”.
5. La acción tiene configurado el servicio IDS o el servicio de equilibrio de carga (para integraciones de varios dispositivos IDS).
6. El dispositivo IDS se configura como el tipo de servicio de inspección de contenido “Any” en el dispositivo. El servicio de inspección de contenido se asocia al perfil de inspección de contenido de tipo “MIRROR”, que especifica la interfaz de salida a través de la cual los datos deben enviarse al dispositivo IDS. De manera opcional, también puede configurar una etiqueta de VLAN en el perfil de inspección de contenido.

   > **Nota:**
   >
   > - La dirección IP utilizada para el servicio o servidor de IDS es una dirección ficticia.
   > - El dispositivo Citrix ADC no admite el canal LA para la interfaz de salida.

7. A continuación, el dispositivo replica los datos a través de la interfaz de salida en uno o más dispositivos IDS.
8. Del mismo modo, cuando el servidor back-end envía una respuesta al Citrix ADC, el dispositivo replica los datos y los reenvía al dispositivo IDS.

9. Si su dispositivo está integrado en uno o más dispositivos IDS y si prefiere equilibrar la carga de los dispositivos, puede usar el servidor virtual de equilibrio de carga.

Licencias de software

Para implementar la integración de dispositivos en línea, su dispositivo Citrix ADC debe aprovisionarse con una de las siguientes licencias:

1. ADC Premium
2. ADC Avanzado
3. Telco avanzado
4. Telco Premium

Configuración de la integración del sistema de detección de

Puede integrar el dispositivo IDS con Citrix ADC de dos maneras diferentes.

Caso 1: integración con un único dispositivo IDS

Los siguientes son los pasos que debe configurar mediante la interfaz de línea de comandos.

1. Permitir la inspección de contenido
2. Agregue un perfil de inspección de contenido de tipo MIRROR para el servicio que representa el dispositivo
3. Agregue el servicio IDS de tipo “ANY”
4. Agregar acción de inspección de contenido de tipo “MIRROR”
5. Agregar directiva de inspección de contenido para la inspección de IDS
6. Vincular la directiva de inspección de contenido al servicio virtual de cambio de contenido o equilibrio de carga de tipo HTTP/SSL

Habilitar inspección de contenido

Si quiere que el dispositivo Citrix ADC envíe el contenido para su inspección a los dispositivos IDS, debe habilitar las funciones de inspección de contenido y equilibrio de carga independientemente de realizar el descifrado.

En el símbolo del sistema, escriba:

```
enable ns feature contentInspection LoadBalancing
```

Agregar perfil de inspección de contenido de tipo “MIRROR

El perfil de inspección de contenido de tipo “MIRROR” explica cómo puede conectarse al dispositivo IDS.
En el símbolo del sistema, escriba.

```
add contentInspection profile <name> -type MIRROR -egressInterface <interface_name
> [-egressVlan <positive_integer>]
```

Ejemplo:

```
add contentInspection profile IDS_profile1 -type MIRROR -egressInterface
1/1 -egressVLAN 10
```

Agregar el servicio IDS

Debe configurar un servicio de tipo “ANY” para cada dispositivo IDS que esté integrado con el dispositivo. El servicio tiene los detalles de configuración del dispositivo IDS. El servicio representa el dispositivo IDS.

En el símbolo del sistema, escriba:

```
add service <Service_name> <IP> ANY <Port> - contentinspectionProfileName <
Name> -healthMonitor OFF -usip ON -useproxyport OFF
```

Ejemplo:

```
add service IDS_service 1.1.1.1 ANY 8080 -contentInspectionProfileName
IDS_profile1 -healthMonitor OFF
```

Agregar acción de inspección de contenido de tipo MIRROR para el servicio IDS

Después de habilitar la función Inspección de contenido y, a continuación, agregar el perfil y el servicio de IDS, debe agregar la acción Inspección de contenido para gestionar la solicitud. Según la acción de inspección de contenido, el dispositivo puede eliminar, restablecer, bloquear o enviar datos al dispositivo IDS.

En el símbolo del sistema, escriba:

```
add ContentInspection action < action_name > -type MIRROR -serverName
Service_name/Vserver_name>
```

Ejemplo:

```
add ContentInspection action IDS_action -type MIRROR -serverName IDS_service
```

Agregar directiva de inspección de contenido para la inspección de IDS

Después de crear una acción de inspección de contenido, debe agregar directivas de inspección de contenido para evaluar las solicitudes de inspección. La directiva se basa en una regla que consiste

en una o más expresiones. La directiva evalúa y selecciona el tráfico para su inspección en función de la regla.

En el símbolo del sistema, escriba lo siguiente:

```
add contentInspection policy < policy_name > -rule <Rule> -action <action_name
>
```

Ejemplo:

```
add contentInspection policy IDS_pol1 -rule true -action IDS_action
```

Vincular la directiva de inspección de contenido al servicio virtual de cambio de contenido o equilibrio de carga de tipo HTTP/SSL

Para recibir el tráfico web, debe agregar un servidor virtual de equilibrio de carga.
En el símbolo del sistema, escriba:

```
add lb vserver <name> <vserver name>
```

Ejemplo:

```
add lb vserver HTTP_vserver HTTP 1.1.1.3 8080
```

Enlace la directiva de inspección de contenido al servidor virtual de conmutación de contenido o al servidor virtual de equilibrio de carga de tipo HTTP/SSL

Debe vincular el servidor virtual de equilibrio de carga o el servidor virtual de conmutación de contenido de tipo HTTP/SSL a la directiva de inspección de contenido.

En el símbolo del sistema, escriba lo siguiente:

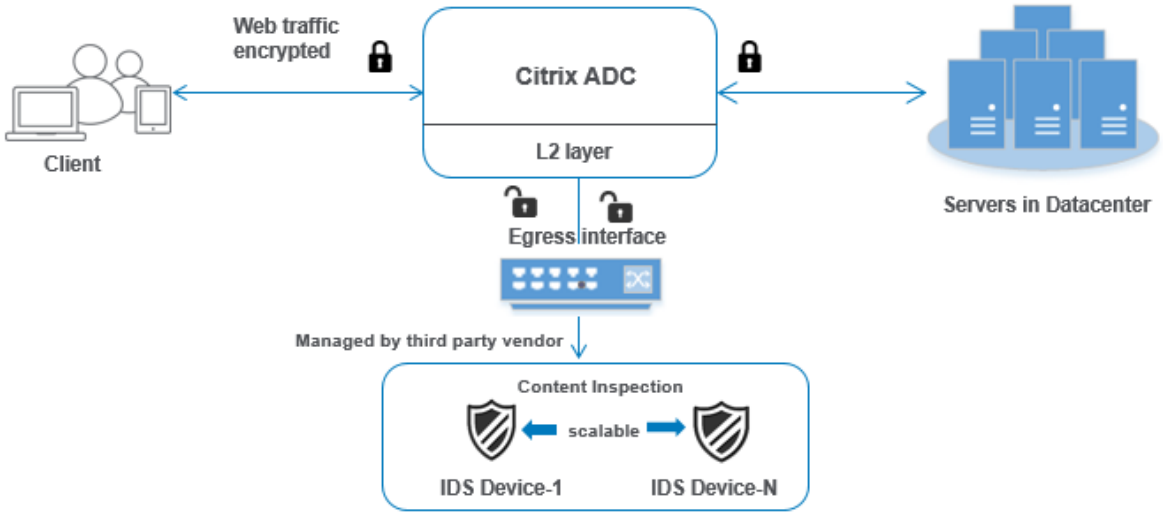
```
bind lb vserver <vserver name> -policyName < policy_name > -priority <
priority > -type <REQUEST>
```

Ejemplo:

```
bind lb vserver HTTP_vserver -policyName IDS_pol1 -priority 100 -type
REQUEST
```

Caso 2: equilibrio de carga de varios dispositivos IDS

Si utiliza dos o más dispositivos IDS, debe equilibrar la carga de los dispositivos mediante diferentes servicios de inspección de contenido. En este caso, la carga del dispositivo Citrix ADC equilibra los dispositivos además de enviar un subconjunto de tráfico a cada dispositivo.
Para ver los pasos de configuración básicos, consulte el caso 1.



Los siguientes son los pasos que debe configurar mediante la interfaz de línea de comandos.

1. Agregue el perfil de inspección de contenido 1 de tipo MIRROR para el servicio IDS 1
2. Agregue el perfil de inspección de contenido 2 de tipo MIRROR para el servicio IDS 2
3. Agregue el servicio IDS 1 de tipo ANY para el dispositivo IDS 1
4. Agregue el servicio IDS 2 de tipo ANY para el dispositivo IDS 2
5. Agregue un servidor virtual de equilibrio de carga de tipo ANY
6. Enlace el servicio IDS 1 al servidor virtual de equilibrio de carga
7. Enlace el servicio IDS 2 al servidor virtual de equilibrio de carga
8. Agregue una acción de inspección de contenido para el equilibrio de carga de los dispositivos IDS.
9. Agregar directiva de inspección de contenido para la inspección
10. Agregar un servidor virtual de conmutación de contenido o equilibrio de carga de tipo HTTP/SSL
11. Vincular la directiva de inspección de contenido al servidor virtual de equilibrio de carga de tipo HTTP/SSL

Agregue el perfil de inspección de contenido 1 de tipo MIRROR para el servicio IDS 1

La configuración de IDS se puede especificar en una entidad denominada perfil de inspección de contenido. El perfil tiene una colección de configuraciones del dispositivo. El perfil de inspección de contenido1 se crea para el servicio IDS 1.

En el símbolo del sistema, escriba:

```
add contentInspection profile <name> -type ANY -egressInterface <interface_name
> [-egressVlan <positive_integer>]
```

Ejemplo:


```
add contentInspection profile IDS_profile1 -type MIRROR -egressInterface
1/1 -egressVLAN 1
```

Agregue el perfil de inspección de contenido 2 para el tipo MIRROR para el servicio IDS

El perfil de inspección de contenido 2 se agrega para el servicio 2 y el dispositivo en línea se comunica con el dispositivo a través de la interfaz de salida 1/1.

En el símbolo del sistema, escriba:

```
add contentInspection profile <name> -type MIRROR -egressInterface -egressVlan
 <positive_integer>]
```

Ejemplo:

```
add contentInspection profile IDS_profile1 -type MIRROR -egressInterface
1/1 -egressVLAN 1
```

Agregue el servicio IDS 1 de tipo ANY para el dispositivo IDS 1

Después de habilitar la función de inspección de contenido y agregar el perfil en línea, debe agregar un servicio en línea 1 para que el dispositivo en línea 1 forme parte de la configuración de equilibrio de carga. El servicio que agrega proporciona todos los detalles de configuración en línea.

En el símbolo del sistema, escriba:

```
add service <Service_name_1> <Pvt_IP1> ANY <Port> -contentInspectionProfileName
 <IDS_Profile_1> -usip ON -useproxyport OFF
```

Ejemplo:

```
add service IDS_service1 1.1.1.1 ANY 80 -contentInspectionProfileName
IDS_profile1 -usip ON -useproxyport OFF
```

> **Nota**
>
> La dirección IP mencionada en el ejemplo es ficticia.

Agregue el servicio IDS 2 de tipo ANY para el dispositivo IDS 2

Después de habilitar la función de inspección de contenido y agregar el perfil en línea, debe agregar un servicio en línea 2 para el dispositivo en línea 2. El servicio que agrega proporciona todos los detalles de configuración en línea.

En el símbolo del sistema, escriba:

```
add service <Service_name_1> <Pvt_IP1> ANY -contentInspectionProfileName <
Inline_Profile_2> -healthmonitor OFF -usip ON -useproxyport OFF
```


Ejemplo:

```
add service IDS_service 1 1.1.2 ANY 80 -contentInspectionProfileName
IDS_profile2
```

> **Nota**
>
> La dirección IP mencionada en el ejemplo es ficticia.

Agregar un servidor virtual de equilibrio de carga

Después de agregar el perfil en línea y los servicios, debe agregar un servidor virtual de equilibrio de carga para equilibrar la carga de los servicios.

En el símbolo del sistema, escriba:

```
add lb vserver <vserver_name> ANY <Pvt_IP3> <port>
```

Ejemplo:

```
add lb vserver lb-IDS_vserver ANY 1.1.1.2
```

Enlace el servicio IDS 1 al servidor virtual de equilibrio de carga

Después de agregar el servidor virtual de equilibrio de carga, ahora vincule el servidor virtual de equilibrio de carga al primer servicio.

En el símbolo del sistema, escriba:

```
bind lb vserver <Vserver_name> <Service_name_1>
```

Ejemplo:

```
bind lb vserver lb-IDS_vserver IDS_service1
```

Enlace el servicio IDS 2 al servidor virtual de equilibrio de carga

Después de agregar el servidor virtual de equilibrio de carga, ahora vincule el servidor al segundo servicio.

En el símbolo del sistema, escriba:

```
bind lb vserver <Vserver_name> <Service_name_1>
```

Ejemplo:

```
bind lb vserver lb-IDS_vserver IDS_service2
```


Agregar acción de inspección de contenido para el servicio IDS

Después de habilitar la función Inspección de contenido, debe agregar la acción Inspección de contenido para gestionar la información de la solicitud en línea. Según la acción seleccionada, el dispositivo descarta, restablece, bloquea o envía tráfico al dispositivo IDS.

En el símbolo del sistema, escriba:

```
add contentInspection action <name> -type <type> (-serverName <string> [-
ifserverdown <ifserverdown>]
```

Ejemplo:

```
add ContentInspection action IDS_action -type MIRROR -serverName lb-IDS_vserver
```

Agregar directiva de inspección de contenido para la inspección

Después de crear una acción de inspección de contenido, debe agregar una directiva de inspección de contenido para evaluar las solicitudes de servicio.

En el símbolo del sistema, escriba lo siguiente:

```
add contentInspection policy <policy_name> -rule <Rule> -action <action_name
>
```

Ejemplo:

```
add contentInspection policy IDS_pol1 -rule true -action IDS_action
```

Agregar un servidor virtual de conmutación de contenido o equilibrio de carga de tipo HTTP/SSL

Agregue un servidor virtual de conmutación de contenido o equilibrio de carga para aceptar el tráfico web. También debe habilitar la conexión layer2 en el servidor virtual.

Para obtener más información sobre el equilibrio de cargas, consulte el tema **Cómo funciona el equilibrio** de cargas.

En el símbolo del sistema, escriba:

```
add lb vserver <name> <vserver name>
```

Ejemplo:

```
add lb vserver http_vserver HTTP 1.1.1.1 8080
```


Vincular la directiva de inspección de contenido al servidor virtual de equilibrio de carga de tipo HTTP/SSL

Debe vincular el servidor virtual de conmutación de contenido o equilibrio de carga de tipo HTTP/SSL a la directiva de inspección de contenido.

En el símbolo del sistema, escriba lo siguiente:

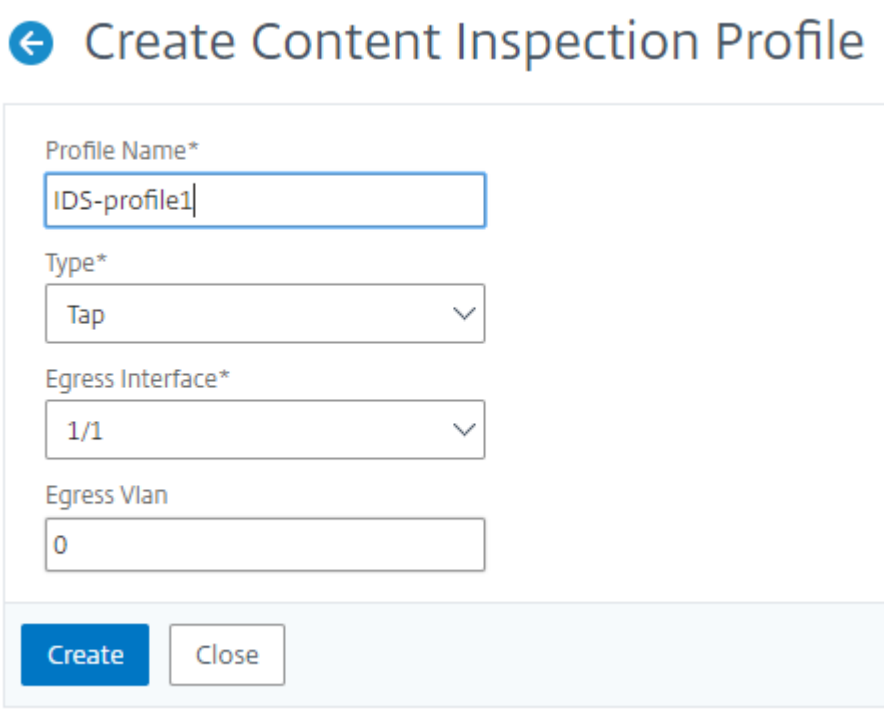
```
bind lb vserver <vserver name> -policyName < policy_name > -priority <> -
type <REQUEST>
```

Ejemplo:

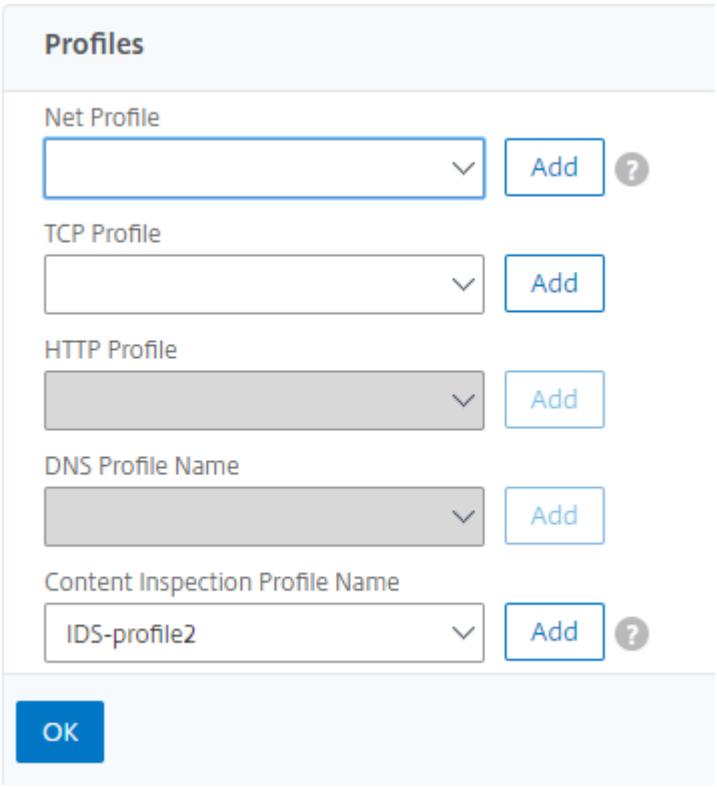
```
bind lb vserver http_vserver -policyName IDS_pol1 -priority 100 -type
REQUEST
```

Configurar la integración de servicios en línea mediante la GUI de Citrix ADC

1. Vaya a **Seguridad** > **Inspección de contenido** > **Perfiles de inspección de contenido**.
2. En la página **Perfil de inspección de contenido**, haga clic en **Agregar**.
3. En la página **Crear perfil de inspección de contenido**, defina los siguientes parámetros.
   a) Nombre del perfil. Nombre del perfil de inspección de contenido de IDS.
   b) Tipo. Seleccione los tipos de perfil como MIRROR.
   c) Interfaz de salida. La interfaz a través de la cual se envía el tráfico desde Citrix ADC al dispositivo IDS.
   d) VLAN de salida (opcional). El identificador de VLAN de interfaz a través del cual se envía el tráfico al dispositivo IDS.
4. Haga clic en **Crear**.



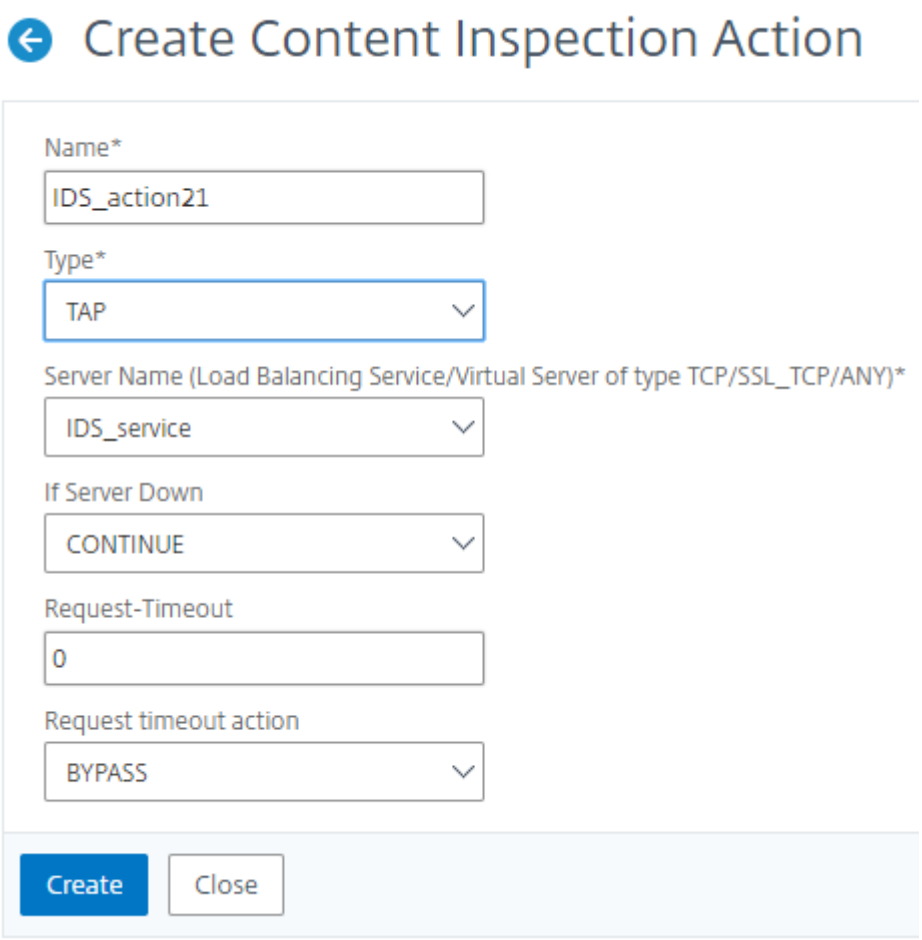
5. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servicios** y haga clic en **Agregar**.
6. En la página **Servicio de equilibrio de carga**, introduzca los detalles del servicio de inspección de contenido.
7. En la sección **Configuración avanzada**, haga clic en **Perfiles**.
8. Vaya a la sección **Perfiles** y haga clic en el icono de **lápiz** para agregar el perfil de inspección de contenido.
9. Haga clic en **OK**.



10. Vaya a **Equilibrio de carga** > **Servidores**. Agregue un servidor virtual de tipo HTTP o SSL.
11. Después de introducir los detalles del servidor, haga clic en **Aceptar** y de nuevo en **Aceptar**.
12. En la sección **Configuración avanzada**, haga clic en **Directivas**.
13. Vaya a la sección **Directivas** y haga clic en el icono de **lápiz** para configurar la directiva de inspección de contenido.
14. En la página **Elegir directiva**, seleccione **Inspección de contenido**. Haga clic en **Continuar**.
15. En la sección **Vinculación de directivas**, haga clic en "+" para agregar una directiva de inspección de contenido.
16. En la página **Crear directiva de CI**, introduzca un nombre para la directiva de inspección de contenido en línea.
17. En el campo **Acción**, haga clic en el signo "+" para crear una acción de inspección de contenido IDS de tipo MIRROR.
18. En la página **Crear acción de CI**, defina los siguientes parámetros.
    a) Nombre. Nombre de la directiva en línea de inspección de contenido.
    b) Tipo. Seleccione el tipo como ESPEJO.
    c) Nombre del servidor. Seleccione el nombre del servidor/servicio como dispositivos en línea.

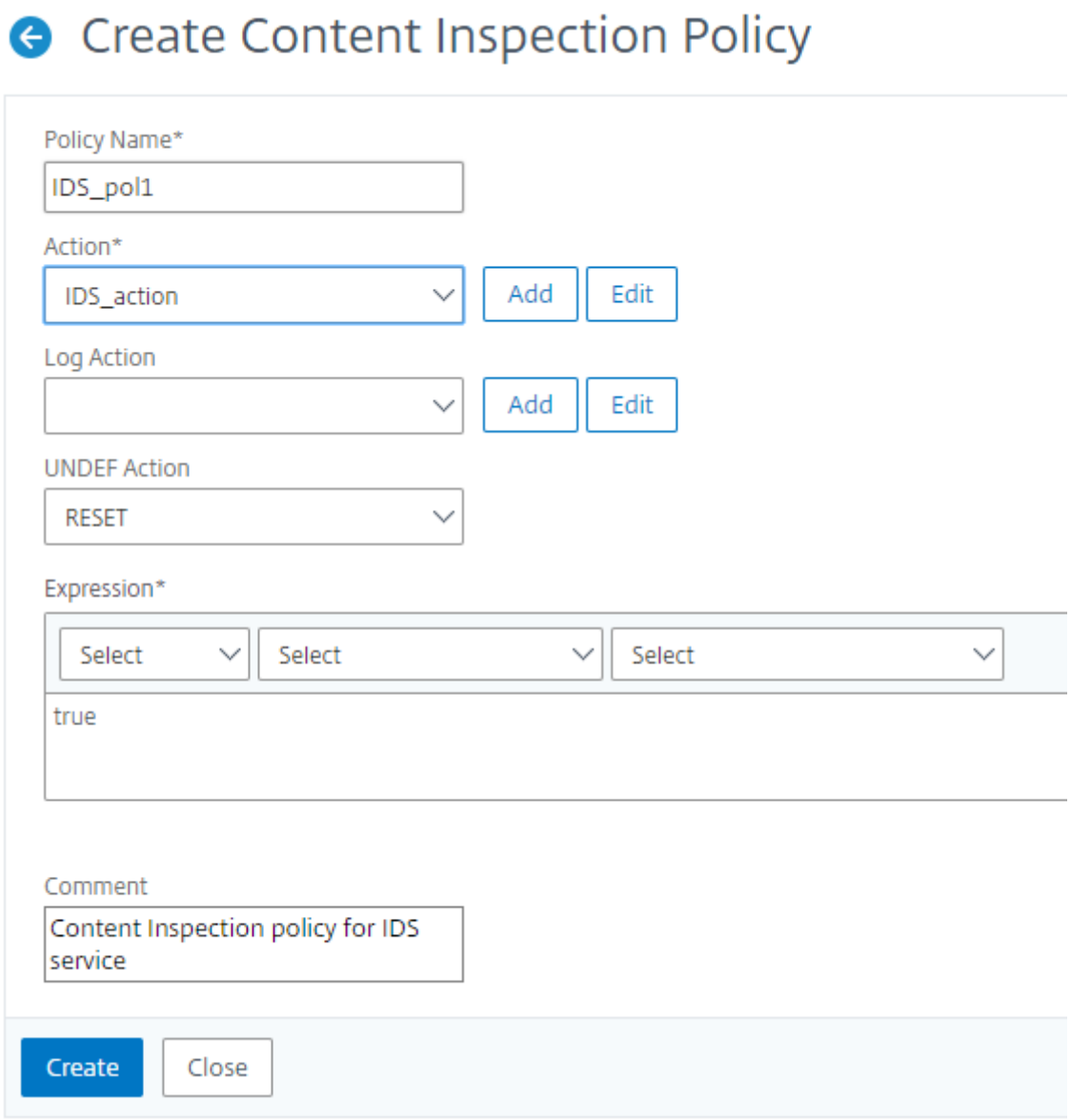
d) Si el servidor está inactivo. Seleccione una operación si el servidor deja de funcionar.
e) Solicitud de tiempo de espera. Seleccione un valor de tiempo de espera. Se pueden usar valores predeterminados.
f) Solicitud de acción de tiempo de espera. Seleccione una acción de tiempo de espera. Se pueden usar valores predeterminados.

19. Haga clic en **Crear**.



20. En la página **Crear directiva de CI**, introduzca otros detalles.
21. Haga clic en **Aceptar** y **cerrar**.

Para obtener información sobre la configuración de la GUI de Citrix ADC para equilibrar la carga y replicar el tráfico en dispositivos IDS, consulte Equilibrio de carga.



Para obtener información sobre la configuración de la GUI de Citrix ADC para equilibrar la carga y reenviar el tráfico al servidor de origen back-end después de la transformación del contenido, consulte el tema Equilibrio de carga.

Integración de Citrix ADC capa 3 con dispositivos de seguridad pasivos (sistema de detección de intrusiones)

August 20, 2021

Un dispositivo Citrix ADC ahora está integrado con dispositivos de seguridad pasiva, como el sistema

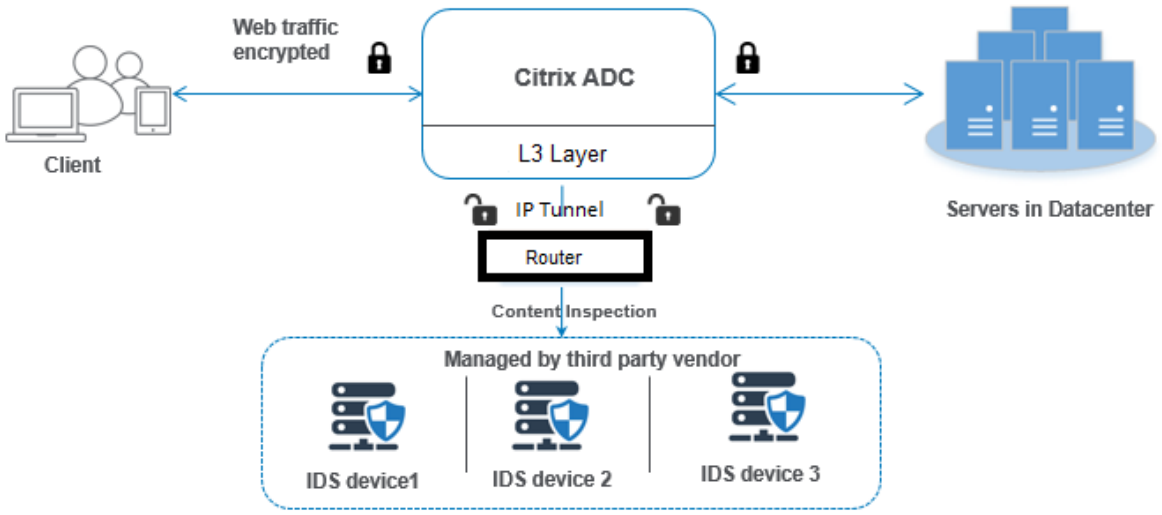
de detección de intrusiones (IDS). En esta configuración, el dispositivo envía una copia del tráfico original de forma segura a dispositivos IDS remotos. Estos dispositivos pasivos almacenan registros y activan alertas cuando detecta un tráfico incorrecto o no compatible. También genera informes para el propósito de cumplimiento. Si un dispositivo Citrix ADC está integrado con dos o más dispositivos IDS y cuando hay un gran volumen de tráfico, el dispositivo puede equilibrar la carga de los dispositivos mediante la clonación del tráfico en el nivel del servidor virtual.

Para una protección de seguridad avanzada, un dispositivo Citrix ADC se integra con dispositivos de seguridad pasiva, como IDS implementados en modo solo de detección. Estos dispositivos almacenan alertas de registro y activan cuando ve un tráfico incorrecto o no compatible. También genera informes para el propósito de cumplimiento. A continuación se presentan algunas de las ventajas de integrar Citrix ADC con un dispositivo IDS.

- **Inspeccionando el tráfico cifrado**. La mayoría de los dispositivos de seguridad omiten el tráfico cifrado, lo que deja a los servidores vulnerables a los ataques. Un dispositivo Citrix ADC puede descifrar el tráfico y enviarlo a dispositivos IDS para mejorar la seguridad de la red del cliente.
- **Descarga de dispositivos en línea del procesamiento TLS/SSL**. El procesamiento TLS/SSL es costoso y da como resultado una alta CPU del sistema en los dispositivos de detección de intrusiones si descifran el tráfico. Como el tráfico cifrado está creciendo a un ritmo rápido, estos sistemas no logran descifrar e inspeccionar el tráfico cifrado. Citrix ADC ayuda a descargar tráfico a dispositivos IDS desde el procesamiento TLS/SSL. Esta forma de descarga de datos resulta en un dispositivo IDS que admite un alto volumen de inspección de tráfico.
- **Carga de dispositivos IDS de equilibrio**. La carga del dispositivo Citrix ADC equilibra varios dispositivos IDS cuando hay un gran volumen de tráfico mediante la clonación del tráfico en el nivel del servidor virtual.
- **Replicando el tráfico a dispositivos pasivos**. El tráfico que fluye hacia el dispositivo se puede replicar a otros dispositivos pasivos para generar informes de conformidad. Por ejemplo, pocas agencias gubernamentales exigen que cada transacción se registre en algunos dispositivos pasivos.
- **Ventilando el tráfico a varios dispositivos pasivos**. Algunos clientes prefieren ventilar o replicar el tráfico entrante en varios dispositivos pasivos.
- **Selección inteligente de tráfico**. Es posible que cada paquete que fluya en el dispositivo no se debe inspeccionar el contenido, por ejemplo, la descarga de archivos de texto. El usuario puede configurar el dispositivo Citrix ADC para seleccionar tráfico específico (por ejemplo, archivos.exe) para su inspección y enviar el tráfico a dispositivos IDS para procesar datos.

Cómo se integra Citrix ADC con el dispositivo IDS con conectividad L3

El siguiente diagrama muestra cómo se integra el IDS con un dispositivo Citrix ADC.



La interacción de componentes se da de la siguiente manera:

1. Un cliente envía una solicitud HTTP/HTTPS al dispositivo Citrix ADC.
2. El dispositivo intercepta el tráfico y envía los datos a dispositivos IDS remotos a través de diferentes centros de datos o incluso en una nube. Esta integración se realiza a través de la capa 3 de túnel IP. Para obtener más información acerca de la tunelización IP en un dispositivo Citrix ADC, consulte el tema de túneles IP.
3. Si el tráfico es cifrado, el dispositivo descifra los datos y los envía como texto sin formato.
4. En función de la evaluación de directivas, el dispositivo aplica una acción de inspección de contenido de tipo “MIRROR”.
5. La acción tiene configurado un servicio IDS o un servicio de equilibrio de carga (para múltiples integraciones de dispositivos IDS) configurado en él.
6. El dispositivo IDS se configura como el tipo de servicio de inspección de contenido “Any” en el dispositivo. El servicio de inspección de contenido se asocia entonces al perfil de inspección de contenido del tipo “MIRROR” y al parámetro de túnel que especifica la interfaz de capa 3 con túnel IP a través de la cual se reenvían los datos al dispositivo IDS.

> **Nota** Opcionalmente, también puede configurar una etiqueta VLAN en el perfil de inspección de contenido.

1. Del mismo modo, cuando el servidor back-end envía una respuesta al Citrix ADC, el dispositivo replica los datos y los reenvía al dispositivo IDS.
2. Si el dispositivo está integrado en uno o varios dispositivos IDS y prefiere equilibrar la carga de los dispositivos, puede utilizar el servidor virtual de equilibrio de carga.

Licencias de software

Para implementar la integración de IDS, el dispositivo Citrix ADC debe aprovisionarse con una de las siguientes licencias:

1. ADC Premium
2. ADC Avanzado

Configuración de la integración del sistema de detección de intrusiones

Puede integrar un dispositivo IDS con un Citrix ADC de dos maneras diferentes.

Caso 1: Integración con un único dispositivo IDS

Los siguientes son los pasos que debe configurar mediante la interfaz de línea de comandos.

1. Habilitar inspección de contenido
2. Agregue el perfil de inspección de contenido de tipo MIRROR para el servicio que representa el dispositivo IDS.
3. Agregar servicio IDS de tipo “CUALQUIER”
4. Agregar acción de inspección de contenido del tipo “MIRROR”
5. Agregar directiva de inspección de contenido para la inspección de IDS
6. Vincular la directiva de inspección de contenido al servicio virtual de cambio de contenido o equilibrio de carga de tipo HTTP/SSL

Habilitar inspección de contenido

Si desea que el dispositivo Citrix ADC envíe el contenido para su inspección a los dispositivos IDS, debe habilitar las funciones Inspección de contenido y equilibrio de carga, independientemente de que se realice el descifrado.

En el símbolo del sistema, escriba:

```
enable ns feature contentInspection LoadBalancing
```

Agregar perfil de inspección de contenido del tipo “MIRROR”

El perfil de inspección de contenido del tipo “MIRROR” explica cómo puede conectarse al dispositivo IDS.
En el símbolo del sistema, escriba.

> **Nota**

> El parámetro de túnel IP solo se debe utilizar para la topología IDS de capa 3. De lo contrario, debe usar la interfaz de salida con la opción VLAN de salida.

```
add contentInspection profile <name> -type MIRROR -ipTunnel <iptunnel_name>
```

Ejemplo:

```
add contentInspection profile IDS_profile1 -type MIRROR -ipTunnel ipsect-
tunnel1
```

Agregar servicio IDS

Debe configurar un servicio de tipo “CUALQUIER” para cada dispositivo IDS integrado con el dispositivo. El servicio tiene los detalles de configuración del dispositivo IDS. El servicio representa el dispositivo IDS.

En el símbolo del sistema, escriba:

```
add service <Service_name> <IP> ANY <Port> - contentinspectionProfileName <
Name> -healthMonitor OFF -usip ON -useproxyport OFF
```

Ejemplo:

```
add service IDS_service 1.1.1.1 ANY 8080 -contentInspectionProfileName
IDS_profile1 -healthMonitor OFF
```

Agregar acción de inspección de contenido de tipo MIRROR para el servicio IDS

Después de habilitar la función Inspección de contenido y, a continuación, agregar el perfil y el servicio IDS, debe agregar la acción de inspección de contenido para gestionar la solicitud. Según la acción de inspección de contenido, el dispositivo puede eliminar, restablecer, bloquear o enviar datos al dispositivo IDS.

En el símbolo del sistema, escriba:

```
add ContentInspection action < action_name > -type MIRROR -serverName
Service_name/Vserver_name>
```

Ejemplo:

```
add ContentInspection action IDS_action -type MIRROR -serverName IDS_service
```

Agregar directiva de inspección de contenido para la inspección de IDS

Después de crear una acción de inspección de contenido, debe agregar directivas de Inspección de contenido para evaluar las solicitudes de inspección. La directiva se basa en una regla que consta de una o más expresiones. La directiva evalúa y selecciona el tráfico para la inspección en función de la regla.

En el símbolo del sistema, escriba lo siguiente:

```
add contentInspection policy < policy_name > -rule <Rule> -action <action_name
>
```

Ejemplo:

```
add contentInspection policy IDS_pol1 -rule true -action IDS_action
```

Vincular la directiva de inspección de contenido al servicio virtual de cambio de contenido o equilibrio de carga de tipo HTTP/SSL

Para recibir el tráfico web, debe agregar un servidor virtual de equilibrio de carga.
En el símbolo del sistema, escriba:

```
add lb vserver <name> <vserver name>
```

Ejemplo:

```
add lb vserver HTTP_vserver HTTP 1.1.1.3 8080
```

Vincular la directiva de inspección de contenido al servidor virtual de cambio de contenido o al servidor virtual de equilibrio de carga de tipo HTTP/SSL

Debe vincular el servidor virtual de equilibrio de carga o el servidor virtual de cambio de contenido de tipo HTTP/SSL a la directiva de inspección de contenido.

En el símbolo del sistema, escriba lo siguiente:

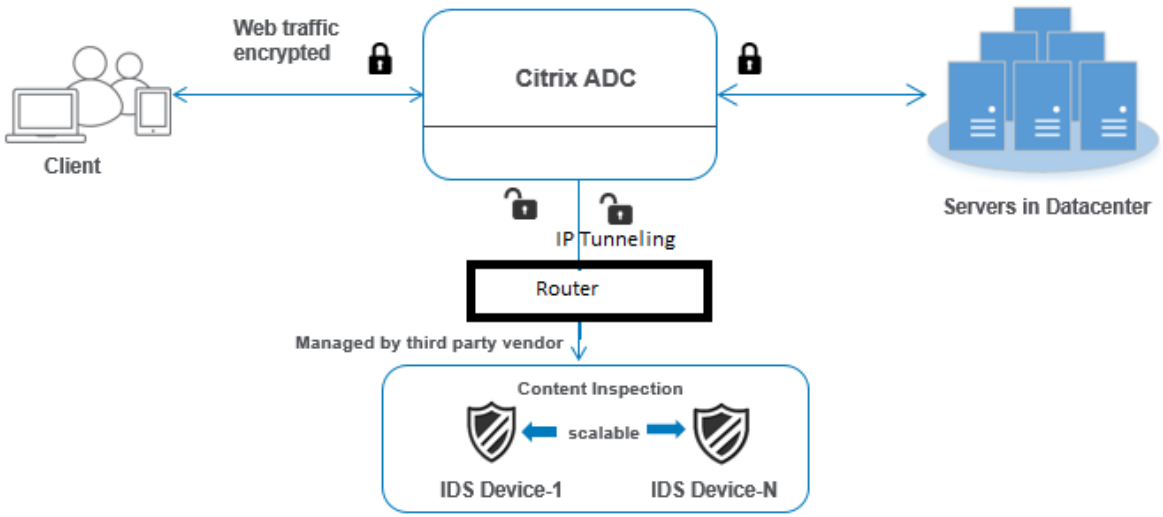
```
bind lb vserver <vserver name> -policyName < policy_name > -priority <
priority > -type <REQUEST>
```

Ejemplo:

```
bind lb vserver HTTP_vserver -policyName IDS_pol1 -priority 100 -type
REQUEST
```

Caso 2: Equilibrio de carga de varios dispositivos IDS

Si utiliza dos o más dispositivos IDS, debe equilibrar la carga de los dispositivos IDS mediante diferentes servicios de inspección de contenido. En este caso, la carga del dispositivo Citrix ADC equilibra los dispositivos además de enviar un subconjunto de tráfico a cada dispositivo.
Para ver los pasos básicos de configuración, consulte el caso 1.



Los siguientes son los pasos que debe configurar mediante la interfaz de línea de comandos.

1. Agregar perfil de inspección de contenido 1 de tipo MIRROR para el servicio IDS 1
2. Agregar el perfil de inspección de contenido 2 de tipo MIRROR para el servicio IDS 2
3. Agregar el servicio IDS 1 de tipo CUALQUIER para el dispositivo IDS 1
4. Agregar el servicio IDS 2 de tipo CUALQUIER para el dispositivo IDS 2
5. Agregar servidor virtual de equilibrio de carga de tipo ANI
6. Vincular el servicio 1 de IDS al servidor virtual de equilibrio de carga
7. Vincular el servicio IDS 2 al servidor virtual de equilibrio de carga
8. Agregue una acción de inspección de contenido para el equilibrio de carga de dispositivos IDS.
9. Agregar directiva de inspección de contenido para inspección
10. Agregar servidor virtual de cambio de contenido o equilibrio de carga de tipo HTTP/SSL
11. Vincular directiva de inspección de contenido al servidor virtual de equilibrio de carga de tipo HTTP/SSL

Agregar perfil de inspección de contenido1 de tipo MIRROR para el servicio IDS 1

La configuración de IDS se puede especificar en una entidad denominada perfil Inspección de contenido. El perfil tiene una colección de configuraciones del dispositivo. El perfil1 de inspección de contenido1 se crea para el servicio IDS 1.

> **Nota: El**parámetro de túnel
> IP solo debe utilizarse para topología IDS de capa 3. De lo contrario, debe usar la interfaz de salida con la opción VLAN de salida.

En el símbolo del sistema, escriba:

```
add contentInspection profile <name> -type ANY - ipTunnel <iptunnel_name>
```


Ejemplo:

```
add contentInspection profile IDS_profile1 -type MIRROR - ipTunnel ipsect_tunnel1
```

Agregar perfil de inspección de contenido 2 para el tipo MIRROR para el servicio IDS 2

El perfil de inspección de contenido 2 se agrega para el servicio 2 y el dispositivo en línea se comunica con el dispositivo a través de la interfaz 1/1 de salida.

En el símbolo del sistema, escriba:

```
add contentInspection profile <name> -type ANY - ipTunnel <iptunnel_name>
```

Ejemplo:

```
add contentInspection profile IDS_profile2 -type ANY - ipTunnel ipsect_tunnel2
```

Agregar el servicio IDS 1 de tipo CUALQUIER para el dispositivo IDS 1

Después de habilitar la función Inspección de contenido y agregar el perfil en línea, debe agregar un servicio en línea 1 para que el dispositivo en línea 1 forme parte de la configuración de equilibrio de carga. El servicio que se agrega proporciona todos los detalles de configuración en línea.

En el símbolo del sistema, escriba:

```
add service <Service_name_1> <Pvt_IP1> ANY <Port> -contentInspectionProfileName
 <IDS_Profile_1> -usip ON -useproxyport OFF
```

Ejemplo:

```
add service IDS_service1 1.1.1.1 ANY 80 -contentInspectionProfileName
IDS_profile1 -usip ON -useproxyport OFF
```

> **Nota**:
>
> La dirección IP mencionada en el ejemplo es falsa.

Agregar el servicio IDS 2 de tipo CUALQUIER para el dispositivo IDS 2

Después de habilitar la función Inspección de contenido y agregar el perfil en línea, debe agregar un servicio en línea 2 para el dispositivo en línea 2. El servicio que se agrega proporciona todos los detalles de configuración en línea.

En el símbolo del sistema, escriba:

```
add service <Service_name_1> <Pvt_IP1> ANY -contentInspectionProfileName <
Inline_Profile_2> -healthmonitor OFF -usip ON -useproxyport OFF
```


Ejemplo:

```
add service IDS_service 1 1.1.2 ANY 80 -contentInspectionProfileName
IDS_profile2
```

> **Nota**:
>
> La dirección IP mencionada en el ejemplo es falsa.

Agregar servidor virtual de equilibrio de carga

Después de agregar el perfil en línea y los servicios, debe agregar un servidor virtual de equilibrio de carga para equilibrar la carga de los servicios.

En el símbolo del sistema, escriba:

```
add lb vserver <vserver_name> ANY <Pvt_IP3> <port>
```

Ejemplo:

```
add lb vserver lb-IDS_vserver ANY 1.1.1.2
```

Vincular el servicio 1 de IDS al servidor virtual de equilibrio de carga

Después de agregar el servidor virtual de equilibrio de carga, ahora vincule el servidor virtual de equilibrio de carga al primer servicio.

En el símbolo del sistema, escriba:

```
bind lb vserver <Vserver_name> <Service_name_1>
```

Ejemplo:

```
bind lb vserver lb-IDS_vserver IDS_service1
```

Vincular el servicio IDS 2 al servidor virtual de equilibrio de carga

Después de agregar el servidor virtual de equilibrio de carga, ahora vincule el servidor al segundo servicio.

En el símbolo del sistema, escriba:

```
bind lb vserver <Vserver_name> <Service_name_1>
```

Ejemplo:

```
bind lb vserver lb-IDS_vserver IDS_service2
```


Agregar acción de inspección de contenido para el servicio IDS

Después de habilitar la función Inspección de contenido, debe agregar la acción de inspección de contenido para gestionar la información de solicitud en línea. Según la acción seleccionada, el dispositivo elimina, restablece, bloquea o envía tráfico al dispositivo IDS.

En el símbolo del sistema, escriba:

```
add contentInspection action <name> -type <type> (-serverName <string> [-
ifserverdown <ifserverdown>]
```

Ejemplo:

```
add ContentInspection action IDS_action -type MIRROR -serverName lb-IDS_vserver
```

Agregar directiva de inspección de contenido para inspección

Después de crear una acción Inspección de contenido, debe agregar la directiva Inspección de contenido para evaluar las solicitudes de servicio.

En el símbolo del sistema, escriba lo siguiente:

```
add contentInspection policy <policy_name> -rule <Rule> -action <action_name
>
```

Ejemplo:

```
add contentInspection policy IDS_pol1 -rule true -action IDS_action
```

Agregar servidor virtual de cambio de contenido o equilibrio de carga de tipo HTTP/SSL

Agregue un servidor virtual de cambio de contenido o equilibrio de carga para aceptar tráfico web. También debe habilitar la conexión layer2 en el servidor virtual.

Para obtener más información sobre el equilibrio de cargas, consulte el tema Cómo funciona el equilibrio de cargas.

En el símbolo del sistema, escriba:

```
add lb vserver <name> <vserver name>
```

Ejemplo:

```
add lb vserver http_vserver HTTP 1.1.1.1 8080
```

Vincular directiva de inspección de contenido al servidor virtual de equilibrio de carga de tipo HTTP/SSL

Debe vincular el servidor virtual de cambio de contenido o equilibrio de carga de tipo HTTP/SSL a la directiva de inspección de contenido.

En el símbolo del sistema, escriba lo siguiente:

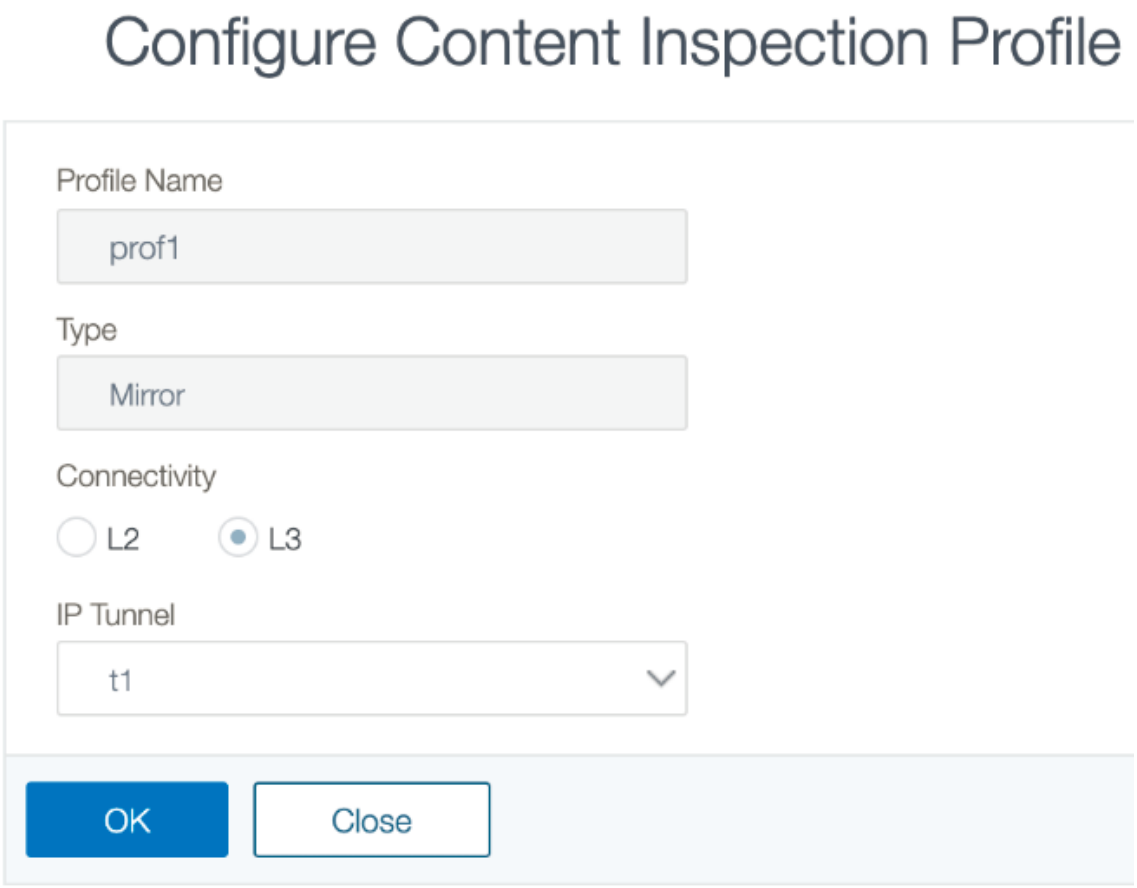
```
bind lb vserver <vserver name> -policyName < policy_name > -priority <> -
type <REQUEST>
```

Ejemplo:

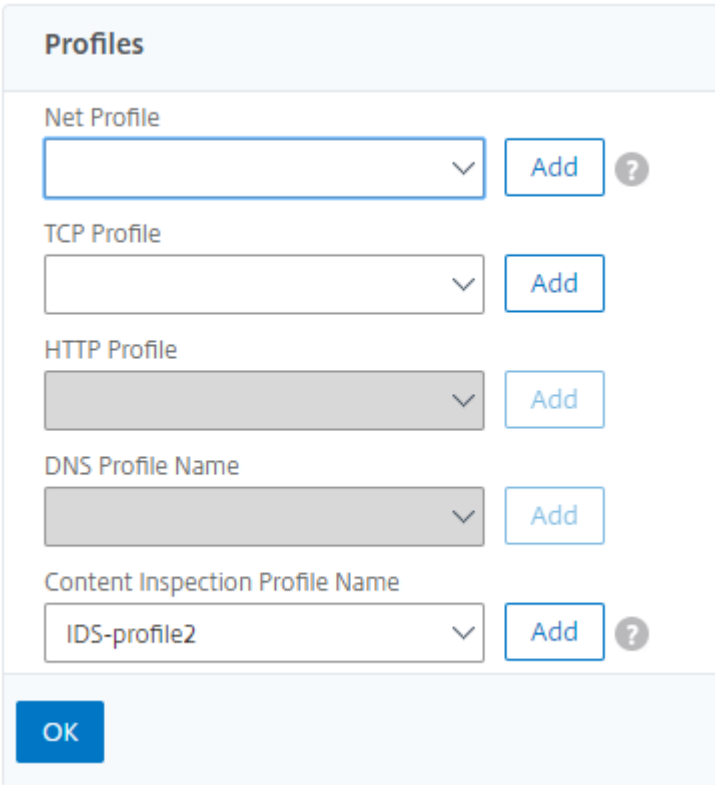
```
bind lb vserver http_vserver -policyName IDS_pol1 -priority 100 -type
REQUEST
```

Configurar la integración de servicios en línea mediante la GUI de Citrix ADC

1. Acceda a **Seguridad** > **Inspección de contenido** > **Perfiles de inspección de contenido**.
2. En la página **Perfil de inspección de contenido**, haga clic en **Agregar**.
3. En la página **Crear ContentInspectionProfile**, defina los siguientes parámetros.
    a) Nombre del perfil. Nombre del perfil de inspección de contenido para IDS.
    b) Tipo. Seleccione los tipos de perfil como MIRROR.
    c) Conectividad. Interfaz de capa 2 o capa 3.
    d) Túnel IP. Seleccione el canal de comunicación de red entre las dos redes.
4. Haga clic en **Crear**.



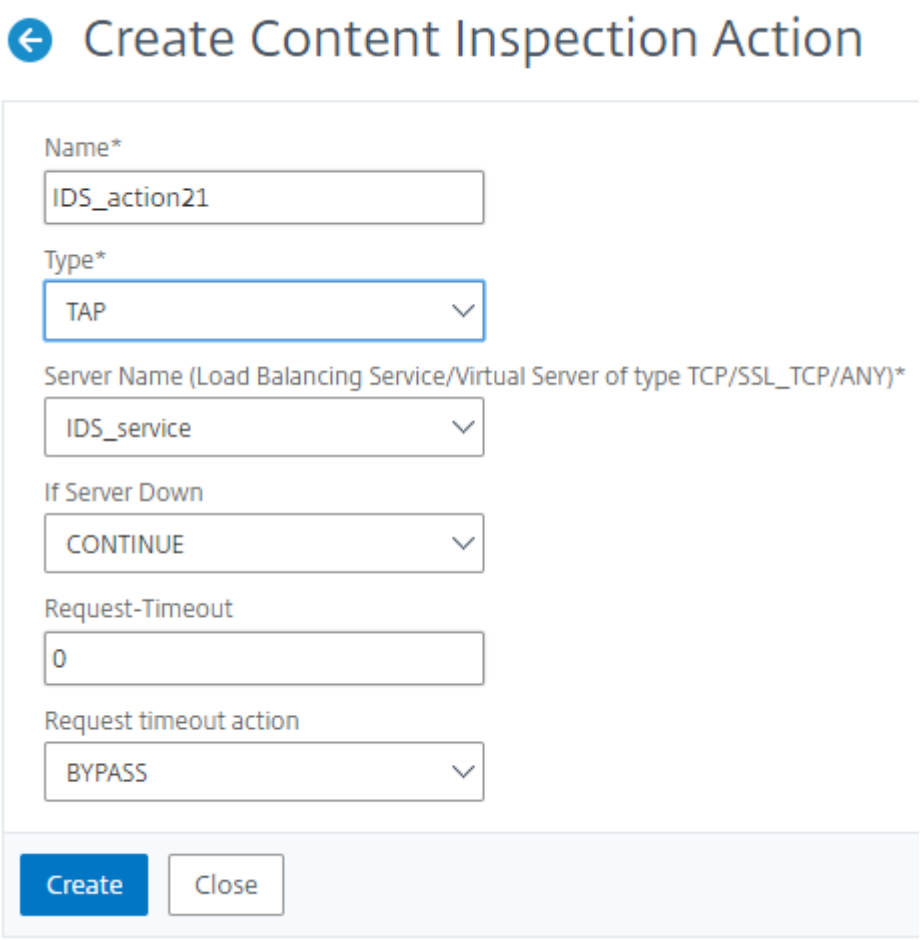
5. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servicios** y haga clic en **Agregar**.
6. En la página **Servicio de equilibrio de carga**, introduzca los detalles del servicio de inspección de contenido.
7. En la sección **Configuración avanzada**, haga clic en **Perfiles**.
8. Vaya a la sección **Perfiles** y haga clic en el icono **Lápiz** para agregar el perfil de inspección de contenido.
9. Haga clic en **Aceptar**.



10. Desplácese hasta **Equilibrio de carga** > **Servidores**. Agregue un servidor virtual de tipo HTTP o SSL.
11. Después de introducir los detalles del servidor, haga clic en **Aceptar** y de nuevo en **Aceptar**.
12. En la sección **Configuración avanzada**, haga clic en **Directivas**.
13. Vaya a la sección **Directivas** y haga clic en el icono **Lápiz** para configurar la directiva de inspección de contenido.
14. En la página **Elegir directiva**, seleccione **Inspección de contenido**. Haga clic en **Continuar**.
15. En la sección **Enlace de directivas**, haga clic en "+" para agregar una directiva de inspección de contenido.
16. En la página **Crear directiva de CI**, escriba un nombre para la directiva de inspección de contenido en línea.
17. En el campo **Acción**, haga clic en el signo "+" para crear una acción de inspección de contenido IDS de tipo MIRROR.
18. En la página **Crear Acción de CI**, establezca los siguientes parámetros.
    a) Name. Nombre de la directiva Inline de inspección de contenido.
    b) Tipo. Seleccione el tipo como MIRROR.
    c) Nombre del servidor. Seleccione el nombre del servidor/servicio como dispositivos Inline.

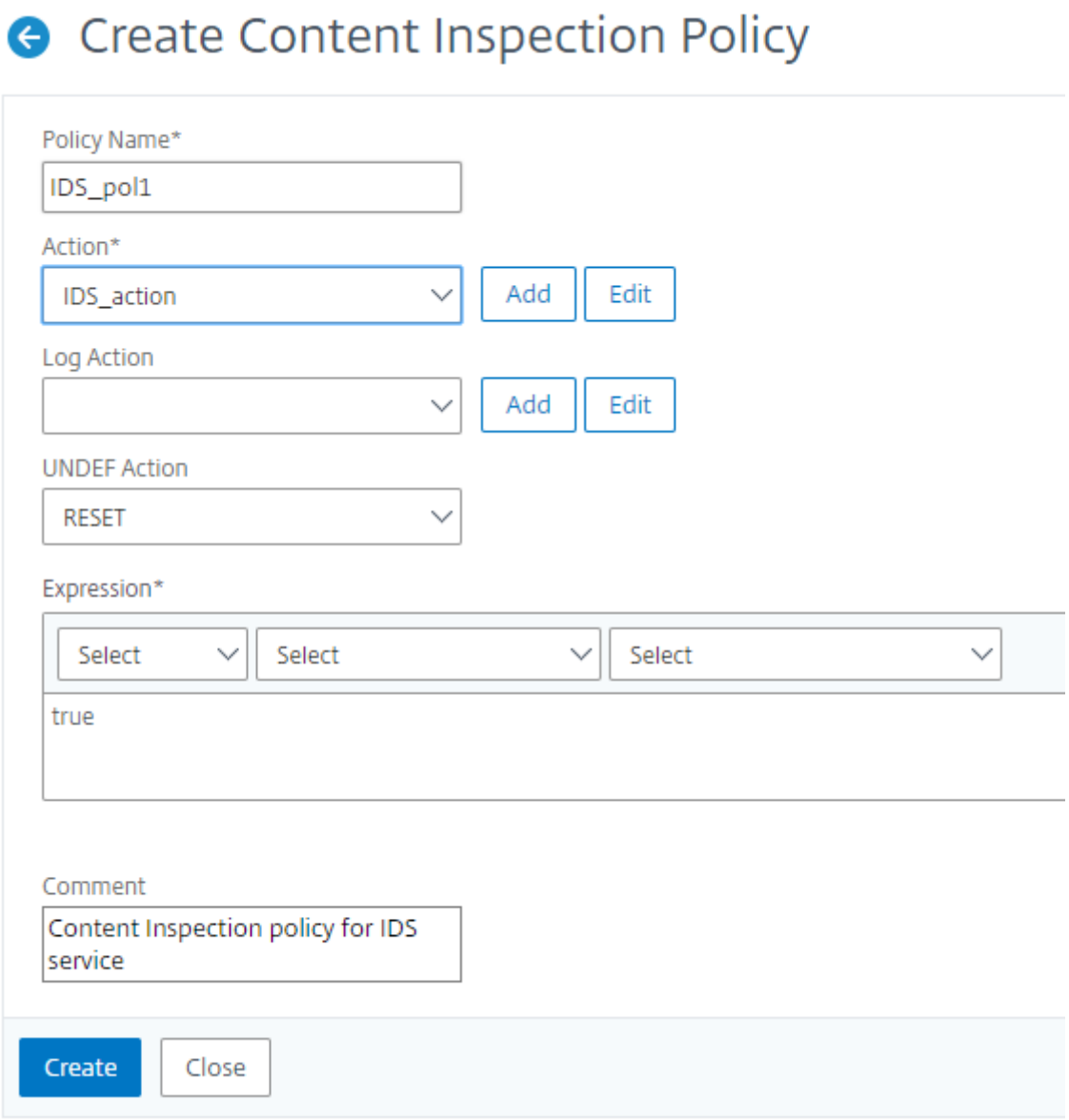
d) Si el servidor está inactivo. Seleccione una operación si el servidor se desactiva.
e) Solicite tiempo de espera. Seleccione un valor de tiempo de espera. Se pueden utilizar valores predeterminados.
f) Solicitar acción de tiempo de espera. Seleccione una acción de tiempo de espera. Se pueden utilizar valores predeterminados.

19. Haga clic en **Crear**.



20. En la página **Crear directiva de CI**, introduzca otros detalles.
21. Haga clic en **Aceptar** y **Cerrar**.

Para obtener información sobre la configuración de la GUI de Citrix ADC para equilibrar la carga y replicar el tráfico en dispositivos IDS, consulte Equilibrio de carga.



Para obtener información acerca de la configuración de la GUI de Citrix ADC para el equilibrio de carga y el reenvío del tráfico al servidor de origen back-end después de la transformación del contenido, consulte Equilibrio de carga.

Estadísticas de inspección de contenido para ICAP, IPS e IDS

February 16, 2021

Las estadísticas de inspección de contenido para los dispositivos ICAP, integración de dispositivos en línea (IDS) e Intrusion Prevention System (IPS) son una salida detallada (resumen) de los detalles de solicitud, respuesta y acción del servidor.

Las estadísticas de inspección de contenido son una recopilación de datos estadísticos que incluye la solicitud HTTP/HTTPS enviada para la inspección de contenido. Respuesta HTTP/HTTPS recibida de dispositivos IPS, IDS e ICAP y acción del servidor back-end.

Para mostrar las estadísticas de inspección de contenido mediante la CLI:

En el símbolo del sistema, escriba:

```
stat contentInspection
```

```
ContentInspection Stats

Inline Statistics
                                  Total
Requests                           10
Responses                           6
Request Bytes Sent                 3235
Request Bytes Received             2977
Response Bytes Sent                17302
Response Bytes Received            19681
Serverdown Reset Action taken       1
Serverdown Drop Action taken        0
Serverdown BYPASS Action taken      0
Inline device Generated Response    3

Mirror Statistics
                                  Total
Requests                           4
Responses                          4
Requests Bytes Sent               2763
Responses Bytes Sent              16732
Serverdown Reset Action taken      0
Serverdown Drop Action taken       0
Serverdown BYPASS Action taken     1

ICAP Statistics
                                  Total
REQMOD requests Sent                6
RESPMOD requests Sent               4
Preview requests                    1
204 Responses Received              6
100 Continue Responses Received     1
204 NO content Received             5
Adaptive Requests                   0
Adaptive Responses                  4
```



```
Callout requests Initiated          1
Callout requests completed          1
ICAP Req/Resp Errors handled        1
Serverdown Reset Action taken       1
Serverdown Drop Action taken        0
Serverdown BYPASS Action taken      1

Done
<!--NeedCopy-->
```

Proxy de reenvío SSL

August 20, 2021

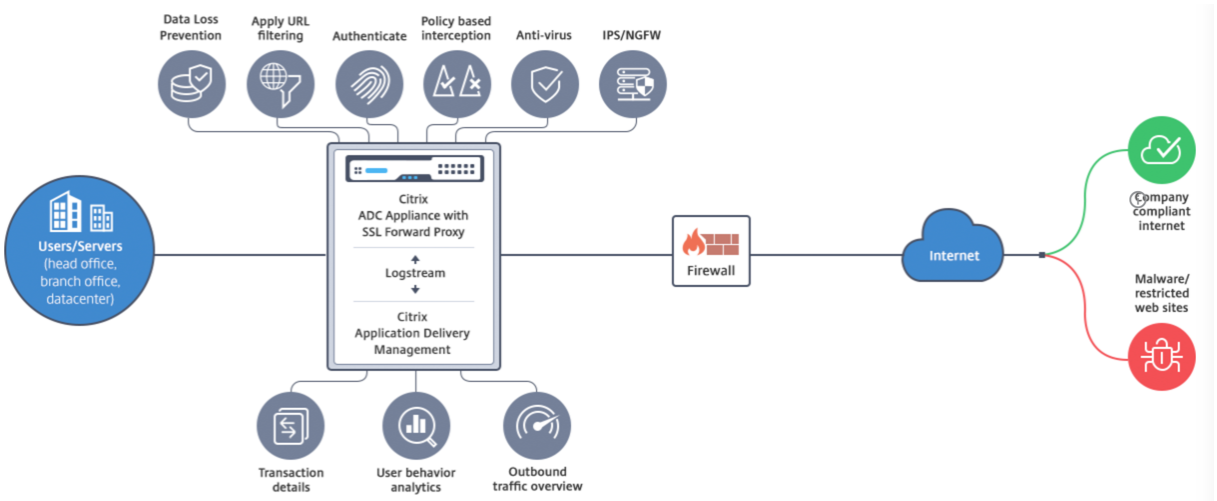
Nota: La función proxy de reenvío SSL está disponible con la licencia ADC Premium.

El tráfico web ha aumentado exponencialmente en los últimos años, y las empresas dependen cada vez más de Internet para sus operaciones diarias. Eso, combinado con la aparición de puntos finales más diversos, movilidad y BYOD, junto con una creciente base de atacantes, está haciendo que los usuarios sean blancos fáciles del malware moderno. Son cada vez más vulnerables al robo de identidad y a que sus datos se vean comprometidos. Tradicionalmente, las empresas han inspeccionado el tráfico HTTP en busca de malware y virus. Pasaron por alto el tráfico HTTPS/TLS, porque no era tan prominente. Se utilizó con moderación para el contenido que era confidencial y de confianza. Pero eso ha cambiado rápidamente, ya que la mayoría de los sitios web públicos de Internet ahora prefieren usar HTTPS para proteger la privacidad de los usuarios. Como resultado, la incapacidad de inspeccionar paquetes cifrados permite malware o intrusiones en la red empresarial. La solución de proxy directo SSL ofrece herramientas que las empresas pueden utilizar para proteger contra amenazas de Internet.

Un proxy es un servidor que controla todo el tráfico entre los usuarios y las aplicaciones de Internet o SaaS. Dado que todo el tráfico pasa a través de este proxy, realiza funciones relacionadas con la seguridad, como la autenticación de usuario y la categorización de URL.

La siguiente ilustración es una descripción general de la implementación del proxy de reenvío SSL. El tráfico fluye a través de la red empresarial desde la oficina central, las sucursales, el centro de datos y los empleados remotos. Un dispositivo Citrix ADC en el borde de la red actúa como proxy. El dispositivo puede funcionar en modo proxy transparente o modo proxy explícito y ofrece controles para interceptar el tráfico de Internet, incluido HTTPS. Las directivas configuradas en el dispositivo determinan si intercepta, omite o bloquea una solicitud concreta. El acceso a sitios restringidos se puede bloquear mediante el filtrado de URL. Un usuario se autentica antes de iniciar sesión en la red empresarial. Todas las solicitudes y respuestas se etiquetan para identificar al usuario, y el acceso al

sitio de Internet se clasifica. La actividad del usuario se registra y se utiliza para generar informes. Si se produce una infracción, los administradores pueden aislar el sistema infectado, determinar si los dispositivos de otros usuarios que visitaron ese sitio web están comprometidos y tomar las medidas apropiadas. Cuando se integra Citrix Application Delivery Management (ADM) con el proxy de reenvío SSL, la actividad del usuario registrado y los registros posteriores del dispositivo se exportan a Citrix ADM mediante `logstream`. Citrix ADM recopila y presenta información sobre las actividades de los usuarios, desde los sitios web visitados hasta el tiempo invertido en línea. También proporciona información sobre el uso del ancho de banda y las amenazas detectadas, como malware y sitios de phishing. Puede utilizar estas métricas clave para supervisar la red y utilizar la función proxy de reenvío SSL para realizar acciones correctivas.



El proxy de reenvío SSL permite a los directores de TI hacer lo siguiente:

- Obtenga visibilidad en el tráfico seguro que, de otro modo, no se pasaría.
- Bloquee el acceso a sitios maliciosos o desconocidos y evite infectar a los usuarios dentro de la empresa.
- Controle el acceso a algunos sitios web, como correo personal, redes sociales y sitios web de búsqueda de empleo, desde la red empresarial.
- Aplique directivas inteligentes de control de contenido para garantizar la máxima productividad del usuario.

Introducción a la función de proxy de reenvío SSL

August 11, 2022

Importante:

- La comprobación de OCSP requiere una conexión a Internet para comprobar la validez de los certificados. Si no se puede acceder a su dispositivo desde Internet mediante la dirección NSIP,

agregue listas de control de acceso (ACL) para realizar NAT desde la dirección NSIP a la dirección IP de subred (SNIP). El SNIP debe poder acceder a Internet. Por ejemplo:

```
add ns acl a1 ALLOW -srcIP = <NSIP> -destIP  “!=”
    10.0.0.0-10.255.255.255

add rnat RNAT-1 a1

bind rnat RNAT-1 <SNIP>

apply acls
<!--NeedCopy-->
```

- Especifique un servidor de nombres DNS para resolver los nombres de dominio.
- Asegúrese de que la fecha del dispositivo esté sincronizada con los servidores NTP. Si la fecha no está sincronizada, el dispositivo no puede verificar eficazmente si un certificado del servidor de origen está caducado.

Para usar la función de proxy de reenvío SSL, debe realizar las siguientes tareas:

- Agregue un servidor proxy en modo explícito o transparente.
- Habilite la intercepción de SSL.
  - Configure un perfil SSL.
  - Agregue y vincule directivas SSL al servidor proxy.
  - Agregue y vincule un par de claves de certificado de CA para la interceptación de SSL.

Nota:

Un dispositivo ADC configurado en modo proxy transparente puede interceptar solo los protocolos HTTP y HTTPS. Para omitir cualquier otro protocolo, como telnet, debe agregar la siguiente directiva de escucha en el servidor virtual proxy.

El servidor virtual ahora solo acepta tráfico entrante HTTP y HTTPS.

```
set cs vserver transparent-pxy1 PROXY * * -cltTimeout 180 -Listenpolicy
    ”CLIENT.TCP.DSTPORT.EQ(80) || CLIENT.TCP.DSTPORT.EQ(443)”`
<!--NeedCopy-->
```

Es posible que tenga que configurar las siguientes funciones, en función de su implementación:

- Servicio de autenticación (recomendado): para autenticar a los usuarios. Sin el servicio de autenticación, la actividad del usuario se basa en la dirección IP del cliente.
- Filtrado de URL: Para filtrar las URL por categorías, puntuación de reputación y listas de URL.

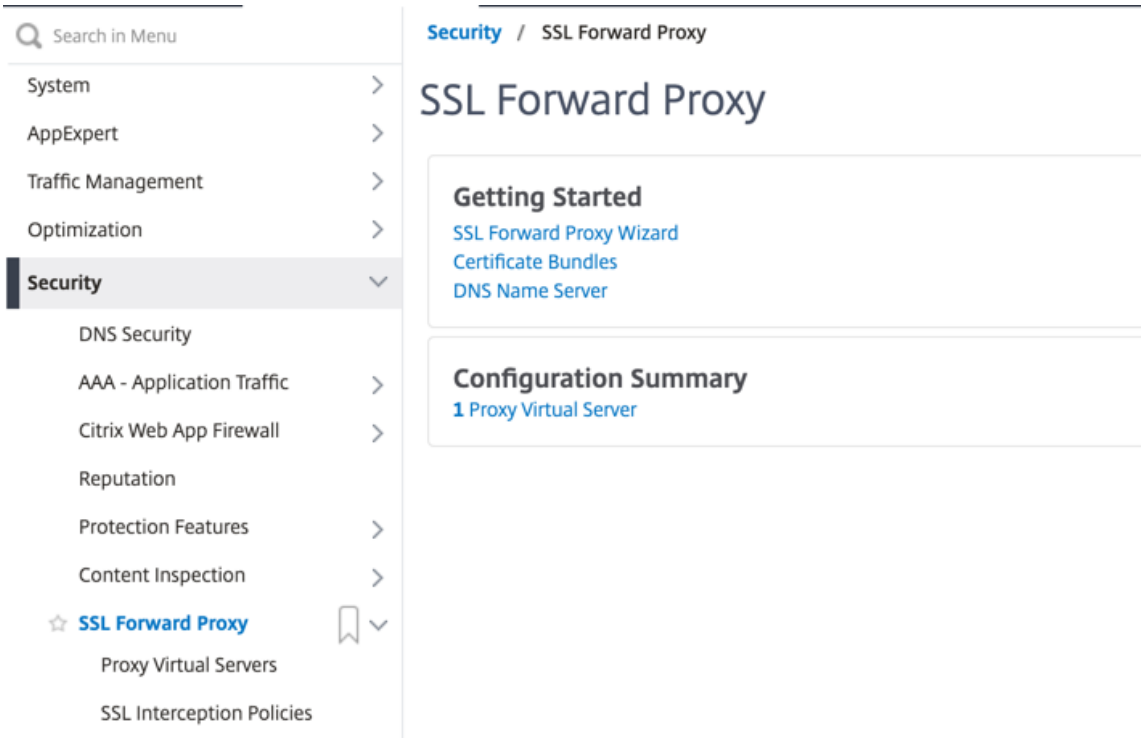
- Análisis: Para ver la actividad del usuario, los indicadores de riesgo del usuario, el consumo de ancho de banda y el desglose de las transacciones en Citrix Application Delivery Management (ADM).

Nota: El proxy de reenvío SSL implementa los estándares HTTP y HTTPS más comunes, seguidos de productos similares. Esta implementación se realiza sin tener en cuenta un explorador web específico y es compatible con los exploradores más comunes. SSL Forward Proxy se ha probado con exploradores comunes y versiones recientes de Google Chrome, Internet Explorer y Mozilla Firefox.

Asistente para proxy de reenvío SSL

El asistente de proxy de reenvío SSL proporciona a los administradores una herramienta para administrar toda la implementación del proxy de reenvío SSL mediante un explorador web. Ayuda a guiar a los clientes para que pongan en marcha un servicio de proxy de reenvío SSL rápidamente y ayuda a simplificar la configuración siguiendo una secuencia de pasos bien definidos.

1. Vaya a **Seguridad > Proxy de reenvío SSL**. En **Introducción**, haga clic en **Asistente para proxy de reenvío SSL**.



2. Siga los pasos del asistente para configurar la implementación.

Agregar una directiva de escucha al servidor proxy transparente

1. Vaya a **Seguridad > Proxy de reenvío SSL** > **Servidores virtuales proxy**. Seleccione el servidor proxy transparente y haga clic en **Modificar**.

2. Modifique **Configuración básica** y haga clic en **Más**.
3. En **Prioridad de escucha**, introduzca 1.
4. En **Expresión de directiva de escucha**, introduzca la siguiente expresión:

```
(CLIENT.TCP.DSTPORT.EQ(80)||CLIENT.TCP.DSTPORT.EQ(443))
<!--NeedCopy-->
```

Esta expresión supone puertos estándar para el tráfico HTTP y HTTPS. Si ha configurado puertos diferentes, por ejemplo, 8080 para HTTP u 8443 para HTTPS, modifique la expresión para reflejar esos puertos.

Limitaciones

El proxy de reenvío SSL no se admite en una configuración de clúster, en particiones administrativas ni en un dispositivo Citrix ADC FIPS.

Modos de proxy

January 12, 2021

El dispositivo Citrix ADC actúa como proxy de un cliente para conectarse a Internet y a las aplicaciones SaaS. Como proxy, acepta todo el tráfico y determina el protocolo del tráfico. A menos que el tráfico sea HTTP o SSL, se reenvía al destino tal como está. Cuando el dispositivo recibe una solicitud de un cliente, intercepta la solicitud y realiza algunas acciones, como la autenticación de usuarios, la categorización de sitios y la redirección. Utiliza directivas para determinar qué tráfico permitir y qué tráfico bloquear.

El dispositivo mantiene dos sesiones diferentes, una entre el cliente y el proxy y la otra entre el proxy y el servidor de origen. El proxy se basa en directivas definidas por el cliente para permitir o bloquear el tráfico HTTP y HTTPS. Por lo tanto, es importante que defina directivas para eludir los datos confidenciales, como la información financiera. El dispositivo ofrece un amplio conjunto de atributos de tráfico de capa 4 a capa 7 y atributos de identidad de usuario para crear directivas de administración de tráfico.

Para el tráfico SSL, el proxy verifica el certificado del servidor de origen y establece una conexión legítima con el servidor. A continuación, emula el certificado de servidor, lo firma con un certificado de CA instalado en Citrix ADC y presenta el certificado de servidor creado al cliente. Debe agregar el certificado de CA como certificado de confianza al explorador del cliente para que la sesión SSL se establezca correctamente.

El dispositivo admite modos proxy transparentes y explícitos. En el modo proxy explícito, el cliente debe especificar una dirección IP en su explorador, a menos que la organización inserte la configuración en el dispositivo del cliente. Esta dirección es la dirección IP de un servidor proxy configurado en el dispositivo ADC. Todas las solicitudes del cliente se envían a esta dirección IP. Para proxy explícito, debe configurar un servidor virtual de conmutación de contenido de tipo PROXY y especificar una dirección IP y un número de puerto válido.

Proxy transparente, como su nombre lo indica, es transparente para el cliente. Es decir, es posible que los clientes no sean conscientes de que un servidor proxy está mediando sus solicitudes. El dispositivo ADC está configurado en una implementación en línea y acepta de forma transparente todo el tráfico HTTP y HTTPS. Para proxy transparente, debe configurar un servidor virtual de conmutación de contenido de tipo PROXY, con asteriscos (*) como dirección IP y puerto. Al utilizar el **Asistente para proxy de reenvío SSL** en la GUI, no es necesario especificar una dirección IP y un puerto.

> **Nota**
>
> Para interceptar protocolos distintos de HTTP y HTTPS en modo proxy transparente, debe agregar una directiva de escucha y vincularla al servidor proxy.

Configurar proxy de reenvío SSL mediante la CLI

En el símbolo del sistema, escriba:

```
add cs vserver <name> PROXY <ipaddress> <port>
<!--NeedCopy-->
```

Argumentos:

Nombre:

Nombre del servidor proxy. Debe comenzar con un carácter alfanumérico o de subrayado (_) ASCII y debe contener solo caracteres alfanuméricos ASCII, guión bajo, hash (#), punto (.), espacio, dos puntos (:), en (@), igual (=) y guión (-). No se puede cambiar después de crear el servidor virtual CS.

El siguiente requisito solo se aplica a la CLI:

Si el nombre incluye uno o más espacios, enciérrelo entre comillas dobles o simples (por ejemplo, “mi servidor” o “mi servidor”).

Este argumento es obligatorio. Longitud máxima: 127

Dirección IP:

Dirección IP del servidor proxy.

Puerto:

Número de puerto para el servidor proxy. Valor mínimo: 1

Ejemplo de proxy explícito:

```
add cs vserver swgVS PROXY 192.0.2.100 80
<!--NeedCopy-->
```

Ejemplo de proxy transparente:

```
add cs vserver swgVS PROXY * *
<!--NeedCopy-->
```

Agregue una directiva de escucha al servidor proxy transparente mediante la interfaz gráfica de usuario

1. Vaya a **Seguridad** > **Proxy de reenvío SSL** > **Servidores virtuales proxy**. Seleccione el servidor proxy transparente y haga clic en **Modificar**.
2. Modifique **la configuración básica** y haga clic en **Más**.
3. En **Prioridad de escucha**, escriba 1.
4. En **Expresión de directiva de escucha**, escriba la siguiente expresión:

```
(CLIENT.TCP.DSTPORT.EQ(80)||CLIENT.TCP.DSTPORT.EQ(443))
<!--NeedCopy-->
```

> **Nota**
>
> Esta expresión asume puertos estándar para el tráfico HTTP y HTTPS. Si ha configurado puertos diferentes, por ejemplo 8080 para HTTP o 8443 para HTTPS, modifique la expresión anterior para especificar esos puertos.

Intercepción SSL

August 20, 2021

Un dispositivo Citrix ADC configurado para intercepción SSL actúa como un proxy. Puede interceptar y descifrar el tráfico SSL/TLS, inspeccionar la solicitud no cifrada y permitir que un administrador

aplique las reglas de cumplimiento y las comprobaciones de seguridad. La intercepción SSL utiliza una directiva que especifica el tráfico que interceptar, bloquear o permitir. Por ejemplo, el tráfico hacia y desde sitios web financieros, como bancos, no debe ser interceptado, pero se puede interceptar otro tráfico, y los sitios de la lista de prohibidos se pueden identificar y bloquear. Citrix recomienda configurar una directiva genérica para interceptar tráfico y directivas más específicas para omitir parte del tráfico.

El cliente y el proxy establecen un protocolo de enlace HTTS/TLS. El proxy establece otro protocolo de enlace HTTS/TLS con el servidor y recibe el certificado del servidor. El proxy comprueba el certificado del servidor en nombre del cliente y también comprueba la validez del certificado del servidor mediante el Protocolo de estado de certificado en línea (OCSP). Regenera el certificado de servidor, lo firma mediante la clave del certificado de CA instalado en el dispositivo y lo presenta al cliente. Por lo tanto, se utiliza un certificado entre el cliente y el dispositivo Citrix ADC, y otro certificado entre el dispositivo y el servidor back-end.

> **Importante**
>
> El certificado de CA que se utiliza para firmar el certificado de servidor debe estar preinstalado en todos los dispositivos cliente, de modo que el cliente confíe en el certificado de servidor regenerado.

Para el tráfico HTTPS interceptado, el servidor proxy descifra el tráfico saliente, accede a la solicitud HTTP de texto claro y puede usar cualquier aplicación de Capa 7 para procesar el tráfico, por ejemplo, mirando la URL de texto sin formato y permitiendo o bloqueando el acceso según la directiva corporativa y la reputación de URL. Si la decisión de directiva es permitir el acceso al servidor de origen, el servidor proxy reenvía la solicitud recifrada al servicio de destino (en el servidor de origen). El proxy descifra la respuesta del servidor de origen, accede a la respuesta HTTP de texto sin cifrar y, opcionalmente, aplica cualquier directiva a la respuesta. A continuación, el proxy vuelve a cifrar la respuesta y la reenvía al cliente. Si la decisión de directiva es bloquear la solicitud al servidor de origen, el proxy puede enviar una respuesta de error, como HTTP 403, al cliente.

Para realizar la interceptación SSL, además del servidor proxy configurado anteriormente, debe configurar lo siguiente en el dispositivo ADC:

- Perfil SSL
- Directiva SSL
- Almacén de certificados de CA
- Almacenamiento automático y almacenamiento en caché de errores SSL

> **Nota:**
>
> El tráfico HTTP/2 no es interceptado por la función de intercepción SSL.

Almacén de certificados de intercepción SSL

Un certificado SSL, que forma parte de cualquier transacción SSL, es un formulario de datos digitales (X509) que identifica a una empresa (dominio) o a un individuo. Una entidad emisora de certificados (CA) emite un certificado SSL. Una CA puede ser privada o pública. Las aplicaciones que llevan a cabo transacciones SSL confían en los certificados emitidos por las CA públicas, como Verisign. Estas aplicaciones mantienen una lista de CA en las que confían.

Como proxy de reenvío, el dispositivo ADC realiza el cifrado y el descifrado del tráfico entre un cliente y un servidor. Actúa como un servidor para el cliente (usuario) y como un cliente para el servidor. Antes de que un dispositivo pueda procesar el tráfico HTTPS, debe validar la identidad de un servidor para evitar transacciones fraudulentas. Por lo tanto, como cliente del servidor de origen, el dispositivo debe comprobar el certificado del servidor de origen antes de aceptarlo. Para verificar un certificado de servidor, todos los certificados (por ejemplo, certificados raíz e intermedios) que se utilizan para firmar y emitir el certificado de servidor deben estar presentes en el dispositivo. Un conjunto predeterminado de certificados de CA está preinstalado en un dispositivo. El dispositivo puede utilizar estos certificados para verificar casi todos los certificados de servidor de origen comunes. Este conjunto predeterminado no se puede modificar. Sin embargo, si la implementación requiere más certificados de CA, puede crear un paquete de dichos certificados e importarlo al dispositivo. Un paquete también puede contener un solo certificado.

Al importar un paquete de certificados al dispositivo, el dispositivo descarga el paquete desde la ubicación remota y, tras comprobar que el paquete contiene solo certificados, lo instala en el dispositivo. Debe aplicar un paquete de certificados antes de poder utilizarlo para validar un certificado de servidor. También puede exportar un paquete de certificados para modificarlo o almacenarlo en una ubicación sin conexión como copia de seguridad.

Importar y aplicar un paquete de certificados de CA en el dispositivo mediante la CLI

En el símbolo del sistema, escriba:

```
1 import ssl certBundle <name> <src>
2 apply ssl certBundle <name>
3 <!--NeedCopy-->
```

```
1 show ssl certBundle
2 <!--NeedCopy-->
```

ARGUMENTOS:

Nombre:

Nombre que se va a asignar al paquete de certificados importados. Debe comenzar con un carácter alfanumérico o de subrayado (_) ASCII y debe contener solo caracteres alfanuméricos ASCII, guión bajo, hash (#), punto (.), espacio, dos puntos (:), en (@), igual (=) y guión (-). El siguiente requisito solo se aplica a la CLI:

Si el nombre incluye uno o más espacios, enciérrelo entre comillas dobles o simples (por ejemplo, “mi archivo” o “mi archivo”).

Longitud máxima: 31

src:

URL que especifica el protocolo, el host y la ruta de acceso, incluido el nombre de archivo, al paquete de certificados que se va a importar o exportar. Por ejemplo, `http://www.example.com/cert_bundle_file`.

NOTA: La importación falla si el objeto que se va a importar está en un servidor HTTPS que requiere autenticación de certificado de cliente para el acceso.

Longitud máxima: 2047

Ejemplo:

```
import ssl certbundle swg-certbundle http://www.example.com/cert_bundle
apply ssl certBundle swg-certbundle
<!--NeedCopy-->
```

```
show ssl certbundle

            Name : swg-certbundle(Inuse)

            URL : http://www.example.com/cert_bundle

    Done
<!--NeedCopy-->
```

Importe y aplique un paquete de certificados de CA en el dispositivo mediante la interfaz gráfica de usuario

1. Vaya a **Seguridad > Proxy de reenvío SSL > Introducción > Paquetes de certificados**.
2. Lleve a cabo una de las siguientes acciones:

- Seleccione un paquete de certificados de la lista.
- Para agregar un paquete de certificados, haga clic en “+” y especifique un nombre y una URL de origen. Haga clic en **Aceptar**.

3. Haga clic en **Aceptar**.

Quitar un paquete de certificados de CA del dispositivo mediante la CLI

En el símbolo del sistema, escriba:

```
remove certBundle <cert bundle name>
<!--NeedCopy-->
```

Ejemplo:

```
remove certBundle mytest-cacert
<!--NeedCopy-->
```

Exportar un paquete de certificados de CA desde el dispositivo mediante la CLI

En el símbolo del sistema, escriba:

```
export certBundle <cert bundle name> <Path to export>
<!--NeedCopy-->
```

ARGUMENTOS:

Nombre:

Nombre que se va a asignar al paquete de certificados importados. Debe comenzar con un carácter alfanumérico o de subrayado (_) ASCII y debe contener solo caracteres alfanuméricos ASCII, guión bajo, hash (#), punto (.), espacio, dos puntos (:), en (@), igual (=) y guión (-). El siguiente requisito solo se aplica a la CLI:

Si el nombre incluye uno o más espacios, enciérrelo entre comillas dobles o simples (por ejemplo, “mi archivo” o “mi archivo”).

Longitud máxima: 31

src:

URL que especifica el protocolo, el host y la ruta de acceso, incluido el nombre de archivo, al paquete de certificados que se va a importar o exportar. Por ejemplo, `http://www.example.com/cert_bundle_file`.

NOTA: La importación falla si el objeto que se va a importar está en un servidor HTTPS que requiere autenticación de certificado de cliente para el acceso.

Longitud máxima: 2047

Ejemplo:

```
export certBundle mytest-cacert http://192.0.2.20/
<!--NeedCopy-->
```

Importar, aplicar y verificar un paquete de certificados de CA desde el almacén de certificados de CA de Mozilla

En el símbolo del sistema, escriba:

```
> import certbundle mozilla_public_ca https://curl.haxx.se/ca/cacert.
   pem
Done
<!--NeedCopy-->
```

Para aplicar el paquete, escriba:

```
> apply certbundle mozilla_public_ca
Done
<!--NeedCopy-->
```

Para verificar el paquete de certificados en uso, escriba:

```
> sh certbundle | grep mozilla
                Name : mozilla_public_ca (Inuse)
<!--NeedCopy-->
```


Limitaciones

- Los paquetes de certificados no se admiten en una instalación de clúster ni en un dispositivo con particiones.
- El protocolo TLSV1.3 no es compatible con Proxy de reenvío SSL.

Infraestructura de directivas SSL para interceptación SSL

Una directiva actúa como un filtro en el tráfico entrante. Las directivas del dispositivo ADC ayudan a definir cómo administrar las conexiones y las solicitudes proxy. El procesamiento se basa en las acciones configuradas para esa directiva. Es decir, los datos de las solicitudes de conexión se comparan con una regla especificada en la directiva y la acción se aplica a las conexiones que coinciden con la regla (expresión). Después de definir una acción para asignarla a la directiva y crearla, debe vincularla a un servidor proxy, de modo que se aplique al tráfico que fluye a través de ese servidor proxy.

Una directiva SSL para intercepción SSL evalúa el tráfico entrante y aplica una acción predefinida a las solicitudes que coinciden con una regla (expresión). La decisión de interceptar, omitir o restablecer una conexión se toma en función de la directiva SSL definida. Puede configurar una de las tres acciones para una directiva: Intercepción, BYPASS o RESET. Debe especificar una acción al crear una directiva. Para poner en práctica una directiva, debe vincularla a un servidor proxy del dispositivo. Para especificar que una directiva está destinada a la interceptación SSL, debe especificar el tipo (punto de enlace) como INTERCEPT_REQ cuando vincule la directiva a un servidor proxy. Al desvincular una directiva, debe especificar el tipo como INTERCEPT_REQ.

> **Nota**:
>
> El servidor proxy no puede tomar la decisión de interceptar a menos que especifique una directiva.

La interceptación de tráfico puede basarse en cualquier atributo de enlace SSL. El más utilizado es el dominio SSL. El dominio SSL suele ser indicado por los atributos del protocolo de enlace SSL. Puede ser el valor del indicador de nombre del servidor extraído del mensaje de saludo del cliente SSL, si está presente, o el valor del nombre alternativo del servidor (SAN) extraído del certificado del servidor de origen. La directiva de interceptación SSL presenta un atributo especial, DETECTED_DOMAIN. Este atributo facilita a los clientes crear directivas de interceptación basadas en el dominio SSL del certificado del servidor de origen. El cliente puede hacer coincidir el nombre de dominio con una cadena, una lista de direcciones URL (conjunto de direcciones URL o `patset`) o una categoría de URL derivada del dominio.

Crear una directiva SSL mediante la CLI

En el símbolo del sistema, escriba:


```
add ssl policy <name> -rule <expression> -action <string>
<!--NeedCopy-->
```

Ejemplos:

Los ejemplos siguientes son para directivas con expresiones que utilizan el atributo `detected_domain` para buscar un nombre de dominio.

No intercepte tráfico a una institución financiera, como XYZBANK

```
add ssl policy pol1 -rule client.ssl.detected_domain.contains("XYZBANK") -action BYPASS
<!--NeedCopy-->
```

No permitir que un usuario se conecte a YouTube desde la red corporativa

```
add ssl policy pol2 -rule client.ssl.client.ssl.detected_domain.url_categorize(0,0).category.eq ("YouTube") -action RESET
<!--NeedCopy-->
```

Interceptar todo el tráfico de usuario

```
add ssl policy pol3 -rule true -action INTERCEPT
<!--NeedCopy-->
```

Si el cliente no quiere utilizar detected_domain, puede utilizar cualquiera de los atributos de enlace SSL para extraer e inferir el dominio.

Por ejemplo, no se encuentra un nombre de dominio en la extensión SNI del mensaje de saludo del cliente. El nombre de dominio debe tomarse del certificado del servidor de origen. Los ejemplos siguientes son para directivas con expresiones que comprueban si hay un nombre de dominio en el nombre del sujeto del certificado del servidor de origen.

Interceptar todo el tráfico de usuarios a cualquier dominio de Yahoo

```
add ssl policy pol4 -rule client.ssl.origin_server_cert.subject.contains("yahoo") -action INTERCEPT
<!--NeedCopy-->
```


Interceptar todo el tráfico de usuarios de la categoría “Compras/Retail”

```
1 add ssl policy pol_url_category -rule client.ssl.origin_server_cert.
     subject.URL_CATEGORIZE(0,0).CATEGORY.eq(”Shopping/Retail”) -action
     INTERCEPT
2 <!--NeedCopy-->
```

Interceptar todo el tráfico de usuario a una URL no categorizada

```
1 add ssl policy pol_url_category -rule client.ssl.origin_server_cert.
     subject.url_categorize(0,0).category.eq(”Uncategorized”) -action
     INTERCEPT
2 <!--NeedCopy-->
```

Los siguientes ejemplos son para directivas que coinciden con el dominio con una entrada de un conjunto de direcciones URL.

Interceptar todo el tráfico de usuarios si el nombre de dominio en SNI coincide con una entrada del conjunto de URL “top100”

```
1 add ssl policy pol_url_set  -rule client.ssl.client_hello.SNI.
     URLSET_MATCHES_ANY(”top100”) -action INTERCEPT
2 <!--NeedCopy-->
```

Interceptar todo el tráfico de usuario del nombre de dominio si el certificado del servidor de origen coincide con una entrada del conjunto de URL “top100”

```
1 add ssl policy pol_url_set  -rule client.ssl.origin_server_cert.subject
     .URLSET_MATCHES_ANY(”top100”) -action INTERCEPT
2 <!--NeedCopy-->
```

Crear una directiva SSL en un servidor proxy mediante la interfaz gráfica de usuario

1. Vaya a **Administración de Tráfico > SSL > Directivas**.
2. En la ficha **Directivas SSL**, haga clic en **Agregar** y especifique los siguientes parámetros:
   - Nombre de directiva
   - Acción de directiva: Seleccione entre interceptar, omitir o restablecer.
   - Expresión

3. Haga clic en **Crear**.

Enlazar una directiva SSL a un servidor proxy mediante la CLI

En el símbolo del sistema, escriba:

```
bind ssl vserver <vServerName> -policyName <string> -priority <
   positive_integer> -type  INTERCEPT_REQ
<!--NeedCopy-->
```

Ejemplo:

```
bind ssl vserver <name> -policyName pol1 -priority 10 -type
   INTERCEPT_REQ
<!--NeedCopy-->
```

Enlazar una directiva SSL a un servidor proxy mediante la interfaz gráfica de usuario

1. Vaya a **Seguridad > Proxy de reenvío SSL > Servidores virtuales proxy**.
2. Seleccione un servidor virtual y haga clic en **Modificar**.
3. En **Configuración avanzada**, haga clic en **Directivas SSL**.
4. Haga clic dentro del cuadro **Directiva SSL**.
5. En **Seleccionar directiva**, seleccione una directiva para enlazar.
6. En **Tipo**, seleccione **INTERCEPT_REQ**.
7. Haga clic en **Vincular** y, a continuación, haga clic en **Aceptar**.

Desvincular una directiva SSL a un servidor proxy mediante la CLI

En el símbolo del sistema, escriba:

```
unbind ssl vserver <vServerName> -policyName <string> -type
   INTERCEPT_REQ
<!--NeedCopy-->
```

Expresiones SSL utilizadas en directivas SSL

Expresión	Descripción
`CLIENT.SSL.CLIENT_HELLO.SNI.*`	Devuelve la extensión SNI en un formato de cadena. Evalúe la cadena para ver si contiene el texto especificado. Ejemplo: Client.ssl.client_hello.sni.contains("xyz.com")
`CLIENT.SSL.ORIGIN_SERVER_CERT.*`	Devuelve un certificado, recibido de un servidor back-end, en un formato de cadena. Evalúe la cadena para ver si contiene el texto especificado. Ejemplo: Client.ssl.origin_server_cert.subject.contains("xyz.com")
`CLIENT.SSL.DETECTED_DOMAIN.*`	Devuelve un dominio, ya sea de la extensión SNI o del certificado del servidor de origen, en un formato de cadena. Evalúe la cadena para ver si contiene el texto especificado. Ejemplo: Client.ssl.detected_domain.contains("xyz.com")

Error SSL autoaprendizaje

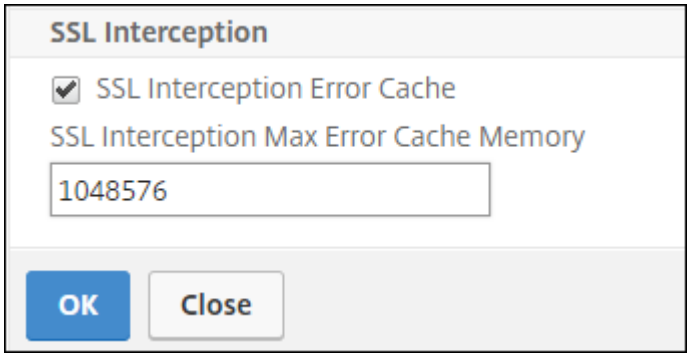
El dispositivo agrega un dominio a la lista de omisión de SSL si el modo de aprendizaje está activado. El modo de aprendizaje se basa en el mensaje de alerta SSL recibido de un cliente o de un servidor de origen. Es decir, el aprendizaje depende del cliente o servidor que envía un mensaje de alerta. No se aprende si no se envía un mensaje de alerta. El dispositivo se entera de si se cumple alguna de las condiciones siguientes:

1. Se recibe una solicitud de certificado de cliente del servidor.
2. Cualquiera de las siguientes alertas se recibe como parte del protocolo de enlace:
   - CERTIFICADO BAD_
   - UNSUPPORTED_CERTIFICATE
   - CERTIFICATE_REVOCADO
   - CERTIFICATE_CADUCADO
   - CERTIFICATE_UNKNOWN
   - UNKNOWN_CA (Si un cliente utiliza anclar, envía este mensaje de alerta si recibe un certificado de servidor).
   - HANDSHAKE_FAILURE

Para habilitar el aprendizaje, debe habilitar la caché de errores y especificar la memoria reservada para el aprendizaje.

Habilitar el aprendizaje mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > SSL**.
2. En **Configuración**, haga clic en **Cambiar la configuración avanzada de SSL**.
3. En **Intercepción SSL**, seleccione **Caché de Error de Intercepción SSL**.
4. En **SSL Interception Max Error Cache Memory**, especifique la memoria (en bytes) que quiere reservar.



5. Haga clic en **Aceptar**.

Habilitar el aprendizaje mediante la CLI

En el símbolo del sistema, escriba:

```
set ssl parameter -ssliErrorCache ( ENABLED | DISABLED ) -
    ssliMaxErrorCacheMem <positive_integer>
<!--NeedCopy-->
```

Argumentos:

SSLIErrorCache:

Habilite o inhabilite el aprendizaje dinámico y almacene en caché la información aprendida para tomar decisiones posteriores para interceptar u omitir solicitudes. Cuando se habilita, el dispositivo realiza una búsqueda en caché para decidir si se omite la solicitud.

Valores posibles: ENABLED, DISABLED

Valor predeterminado: DISABLED

sslimaxErrorcachemem:

Especifique la memoria máxima, en bytes, que se puede utilizar para almacenar en caché los datos aprendidos. Esta memoria se utiliza como caché LRU para que las entradas antiguas se sustituyan por entradas nuevas después de agotar el límite de memoria establecido. Un valor de 0 decide el límite automáticamente.

Valor predeterminado: 0

Valor mínimo: 0

Valor máximo: 4294967294

Perfil SSL

Un perfil SSL es una colección de configuraciones SSL, como cifrados y protocolos. Un perfil es útil si tiene una configuración común para diferentes servidores. En lugar de especificar la misma configuración para cada servidor, puede crear un perfil, especificar la configuración en el perfil y, a continuación, enlazar el perfil a diferentes servidores. Si no se crea un perfil SSL front-end personalizado, el perfil front-end predeterminado está enlazado a entidades del lado cliente. Este perfil le permite configurar los parámetros para administrar las conexiones del lado del cliente.

Para la intercepción SSL, debe crear un perfil SSL y habilitar la intercepción SSL en el perfil. Un grupo de cifrado predeterminado está enlazado a este perfil, pero puede configurar más cifrados para adaptarse a su implementación. Enlazar un certificado de CA de interceptación SSL a este perfil y, a continuación, enlazar el perfil a un servidor proxy. Para la intercepción SSL, los parámetros esenciales de un perfil son los utilizados para las siguientes acciones:

- Compruebe el estado OCSP del certificado del servidor de origen.
- Desencadena la renegociación del cliente si el servidor de origen solicita renegociación.
- Compruebe el certificado del servidor de origen antes de volver a utilizar la sesión SSL front-end.

Utilice el perfil back-end predeterminado cuando se comunique con los servidores de origen. Establezca cualquier parámetro del lado del servidor, como conjuntos de cifrado, en el perfil de back-end predeterminado. No se admite un perfil de back-end personalizado.

Para ver ejemplos de la configuración SSL más utilizada, consulte “Perfil de muestra” al final de esta sección.

El soporte de cifrado/protocolo difiere en la red interna y externa. En las tablas siguientes, la conexión entre los usuarios y un dispositivo ADC es la red interna. La red externa se encuentra entre el dispositivo e Internet.

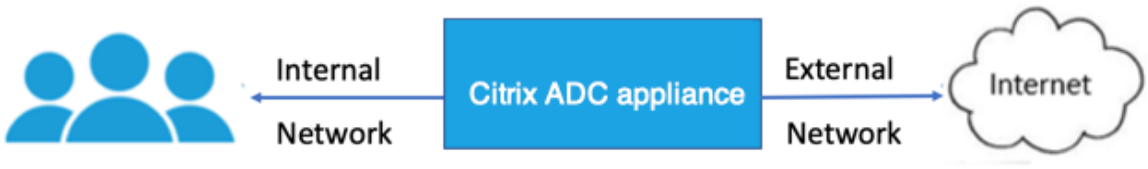


Tabla 1: Tabla de compatibilidad de cifrados/protocolos para la red interna

Consulte Tabla 1 Compatibilidad con servidor/servidor frontend virtual/servicio interno en Ciphers disponibles en los dispositivos Citrix ADC.

Tabla 2: Tabla de compatibilidad de cifrados/protocolos para la red externa

Consulte Tabla 2 Compatibilidad con servicios back-end en Ciphers disponibles en los dispositivos Citrix ADC.

Agregue un perfil SSL y habilite la interceptación SSL mediante la CLI

En el símbolo del sistema, escriba:

```
add ssl profile <name> -sslinterception ENABLED -ssliReneg ( ENABLED |
 DISABLED )-ssliOCSPCheck ( ENABLED | DISABLED )-ssliMaxSessPerServer <
positive_integer>
```

Argumentos:

Intercepción**SSLIntercepción**:

Habilitar o inhabilitar la interceptación de sesiones SSL.

Valores posibles: ENABLED, DISABLED

Valor predeterminado: DISABLED

SSLIreneg:

Habilitar o inhabilitar la activación de la renegociación del cliente cuando se recibe una solicitud de renegociación del servidor de origen.

Valores posibles: ENABLED, DISABLED

Valor predeterminado: ENABLED

Comprobación**SSLIOCSPCheck**:

Habilitar o inhabilitar la comprobación de OCSP para un certificado de servidor de origen.

Valores posibles: ENABLED, DISABLED

Valor predeterminado: ENABLED

sslimaxsessperServer:

Número máximo de sesiones SSL que se almacenarán en caché por servidor de origen dinámico. Se crea una sesión SSL única para cada extensión SNI recibida del cliente en un mensaje de saludo de cliente. La sesión coincidente se utiliza para la reutilización de la sesión del servidor.

Valor predeterminado: 10

Valor mínimo: 1

Valor máximo: 1000

Ejemplo:

```
add ssl profile swg_ssl_profile  -sslinterception ENABLED

Done

sh ssl profile swg_ssl_profile

1)    Name: swg_ssl_profile (Front-End)

                SSLv3: DISABLED               TLSv1.0: ENABLED  TLSv1
                    .1: ENABLED  TLSv1.2: ENABLED

                Client Auth: DISABLED

                Use only bound CA certificates: DISABLED

                Strict CA checks:                                NO

                Session Reuse: ENABLED
                    Timeout: 120 seconds

                DH: DISABLED

                DH Private-Key Exponent Size Limit: DISABLED
                    Ephemeral RSA: ENABLED
                    Refresh Count: 0

                Deny SSL Renegotiation
                    ALL

                Non FIPS Ciphers: DISABLED

                Cipher Redirect: DISABLED
```



```
28
29                  SSL Redirect: DISABLED
30
31                  Send Close-Notify: YES
32
33                  Strict Sig-Digest Check: DISABLED
34
35                  Push Encryption Trigger: Always
36
37                  PUSH encryption trigger timeout:             1 ms
38
39                  SNI: DISABLED
40
41                  OCSP Stapling: DISABLED
42
43                  Strict Host Header check for SNI enabled SSL sessions:
                                NO
44
45                  Push flag:            0x0 (Auto)
46
47                  SSL quantum size:                            8 kB
48
49                  Encryption trigger timeout           100 mS
50
51                  Encryption trigger packet count:               45
52
53                  Subject/Issuer Name Insertion Format: Unicode
54
55                  SSL Interception: ENABLED
56
57                  SSL Interception OCSP Check: ENABLED
58
59                  SSL Interception End to End Renegotiation: ENABLED
60
61                  SSL Interception Server Cert Verification for Client
                       Reuse: ENABLED
62
63                  SSL Interception Maximum Reuse Sessions per Server:  10
64
65                  Session Ticket: DISABLED              Session Ticket
                       Lifetime: 300 (secs)
66
67                  HSTS: DISABLED
68
69                  HSTS IncludeSubDomains: NO
```



```
70
71                  HSTS Max-Age: 0
72
73                  ECC Curve: P_256, P_384, P_224, P_521
74
75 1)             Cipher Name: DEFAULT Priority :1
76
77                  Description: Predefined Cipher Alias
78
79 Done
80 <!--NeedCopy-->
```

Enlazar un certificado de CA de interceptación SSL a un perfil SSL mediante la CLI

En el símbolo del sistema, escriba:

```
bind ssl profile <name> -ssliCACertkey <ssli-ca-cert>
```

Ejemplo:

```
1  bind ssl profile swg_ssl_profile -ssliCACertkey swg_ca_cert
2
3  Done
4
5  sh ssl profile swg_ssl_profile
6
7  1)             Name: swg_ssl_profile (Front-End)
8
9                   SSLv3: DISABLED               TLSv1.0: ENABLED  TLSv1
                       .1: ENABLED  TLSv1.2: ENABLED
10
11                  Client Auth: DISABLED
12
13                  Use only bound CA certificates: DISABLED
14
15                  Strict CA checks:                                NO
16
17                  Session Reuse: ENABLED
                       Timeout: 120 seconds
18
19                  DH: DISABLED
20
21                  DH Private-Key Exponent Size Limit: DISABLED
```



```
                    Ephemeral RSA: ENABLED
                    Refresh Count: 0
22
23                Deny SSL Renegotiation
                    ALL
24
25                Non FIPS Ciphers: DISABLED
26
27                Cipher Redirect: DISABLED
28
29                SSL Redirect: DISABLED
30
31                Send Close-Notify: YES
32
33                Strict Sig-Digest Check: DISABLED
34
35                Push Encryption Trigger: Always
36
37                PUSH encryption trigger timeout:             1 ms
38
39                SNI: DISABLED
40
41                OCSP Stapling: DISABLED
42
43                Strict Host Header check for SNI enabled SSL sessions:
                                        NO
44
45                Push flag:            0x0 (Auto)
46
47                SSL quantum size:                            8 kB
48
49                Encryption trigger timeout           100 mS
50
51                Encryption trigger packet count:               45
52
53                Subject/Issuer Name Insertion Format: Unicode
54
55                SSL Interception: ENABLED
56
57                SSL Interception OCSP Check: ENABLED
58
59                SSL Interception End to End Renegotiation: ENABLED
60
61                SSL Interception Server Cert Verification for Client
                    Reuse: ENABLED
```



```
62
63                  SSL Interception Maximum Reuse Sessions per Server:  10
64
65                  Session Ticket: DISABLED              Session Ticket
                       Lifetime: 300 (secs)
66
67                  HSTS: DISABLED
68
69                  HSTS IncludeSubDomains: NO
70
71                  HSTS Max-Age: 0
72
73                  ECC Curve: P_256, P_384, P_224, P_521
74
75 1)             Cipher Name: DEFAULT Priority :1
76
77                  Description: Predefined Cipher Alias
78
79 1)             SSL Interception CA CertKey Name: swg_ca_cert
80
81 Done
82 <!--NeedCopy-->
```

Enlazar un certificado de CA de interceptación SSL a un perfil SSL mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **Perfiles** > **Perfil SSL**.
2. Haga clic en **Agregar**.
3. Especifique un nombre para el perfil.
4. Habilite la **intercepción de sesiones SSL**.
5. Haga clic en **Aceptar**.
6. En **Configuración avanzada**, haga clic en **Clave de certificado**.
7. Especifique una clave de certificado de CA de intercepción SSL para enlazar al perfil.
8. Haga clic en **Seleccionar** y, a continuación, haga clic en **Vincular**.
9. Opcionalmente, configure los cifrados para que se adapten a su implementación.
    - Haga clic en el icono de edición y, a continuación, haga clic en **Agregar**.
    - Seleccione uno o más grupos de cifrado y haga clic en la flecha derecha.
    - Haga clic en **Aceptar**.

10. Haga clic en **Done**.

Enlazar un perfil SSL a un servidor proxy mediante la interfaz gráfica de usuario

1. Vaya a **Seguridad** >**Proxy de reenvío SSL** > **Servidores virtuales proxy** y agregue un servidor o seleccione un servidor para modificarlo.
2. En **Perfil SSL**, haga clic en el icono de edición.
3. En la lista **Perfil SSL**, seleccione el perfil SSL que creó anteriormente.
4. Haga clic en **Aceptar**.
5. Haga clic en **Done**.

Perfil de muestra:

```
Name: swg_ssl_profile (Front-End)

                SSLv3: DISABLED              TLSv1.0: ENABLED  TLSv1
                    .1: ENABLED  TLSv1.2: ENABLED

                Client Auth: DISABLED

                Use only bound CA certificates: DISABLED

                Strict CA checks:                                NO

                Session Reuse: ENABLED
                    Timeout: 120 seconds

                DH: DISABLED

                DH Private-Key Exponent Size Limit: DISABLED
                    Ephemeral RSA: ENABLED
                    Refresh Count: 0

                Deny SSL Renegotiation
                    ALL

                Non FIPS Ciphers: DISABLED

                Cipher Redirect: DISABLED

                SSL Redirect: DISABLED

                Send Close-Notify: YES
```



```
26
27                  Strict Sig-Digest Check: DISABLED
28
29                  Push Encryption Trigger: Always
30
31                  PUSH encryption trigger timeout:             1 ms
32
33                  SNI: DISABLED
34
35                  OCSP Stapling: DISABLED
36
37                  Strict Host Header check for SNI enabled SSL sessions:
                                NO
38
39                  Push flag:            0x0 (Auto)
40
41                  SSL quantum size:                            8 kB
42
43                  Encryption trigger timeout           100 mS
44
45                  Encryption trigger packet count:               45
46
47                  Subject/Issuer Name Insertion Format: Unicode
48
49                  SSL Interception: ENABLED
50
51                  SSL Interception OCSP Check: ENABLED
52
53                  SSL Interception End to End Renegotiation: ENABLED
54
55                  SSL Interception Maximum Reuse Sessions per Server:  10
56
57                  Session Ticket: DISABLED              Session Ticket
                       Lifetime: 300 (secs)
58
59                  HSTS: DISABLED
60
61                  HSTS IncludeSubDomains: NO
62
63                  HSTS Max-Age: 0
64
65                  ECC Curve: P_256, P_384, P_224, P_521
66
67  1)            Cipher Name: DEFAULT Priority :1
68
```



```
69                  Description: Predefined Cipher Alias
70
71 1)            SSL Interception CA CertKey Name: swg_ca_cert
72 <!--NeedCopy-->
```

Gestión de la identidad del usuario

February 19, 2022

El creciente número de infracciones de seguridad y la creciente popularidad de los dispositivos móviles han puesto de relieve la necesidad de garantizar que el uso de Internet externo cumpla con las directivas corporativas. Solo se debe permitir el acceso a los recursos externos proporcionados por el personal corporativo a los usuarios autorizados. La gestión de identidades lo hace posible mediante la verificación de la identidad de una persona o de un dispositivo. No determina qué tareas puede realizar el individuo ni qué archivos puede ver el individuo.

Una implementación de proxy de reenvío SSL identifica al usuario antes de permitir el acceso a Internet. Se inspeccionan todas las solicitudes y respuestas del usuario. La actividad del usuario se registra y los registros se exportan a Citrix Application Delivery Management (ADM) para generar informes. En Citrix ADM, puede ver las estadísticas sobre las actividades de los usuarios, las transacciones y el consumo de ancho de banda.

De forma predeterminada, solo se guarda la dirección IP del usuario, pero puede configurar la función para registrar más detalles sobre el usuario. Puede utilizar esta información de identidad para crear directivas de uso de Internet más eficaces para usuarios específicos.

El dispositivo Citrix ADC admite los siguientes modos de autenticación para una configuración de proxy explícito.

- **Protocolo ligero de acceso a directorios (LDAP)**. Autentica al usuario a través de un servidor de autenticación LDAP externo. Para obtener más información, consulte Directivas de autenticación LDAP.
- **RADIO**. Autentica al usuario a través de un servidor RADIUS externo. Para obtener más información, consulte Directivas de autenticación RADIUS.
- **TACACS+** Autentica al usuario a través de un servidor externo de autenticación del sistema de control de acceso de controlador de acceso de Terminal Access Controller (TACACS). Para obtener más información, consulte Directivas de autenticación.
- **Negociar**. Autentica al usuario mediante un servidor de autenticación Kerberos. Si hay un error en la autenticación Kerberos, el dispositivo utiliza la autenticación NTLM. Para obtener más información, consulte Negociación de directivas de autenticación.

Para proxy transparente, solo se admite la autenticación LDAP basada en IP. Cuando se recibe una solicitud de cliente, el proxy autentica al usuario mediante la comprobación de una entrada de la dirección IP del cliente en active directory. A continuación, crea una sesión basada en la dirección IP del usuario. Sin embargo, si configura el atributo ssonameAttribute en una acción LDAP, se crea una sesión utilizando el nombre de usuario en lugar de la dirección IP. Las directivas clásicas no son compatibles con la autenticación en una configuración de proxy transparente.

> **Nota**
>
> Para proxy explícito, debe establecer el nombre de inicio de sesión de LDAP en **sAMAccountName**. Para proxy transparente, debe establecer el nombre de inicio de sesión de LDAP en **networkAddress** y attribute1 en **sAMAccountName**.

Ejemplo de proxy explícito:

```
1 add authentication ldapAction swg-auth-action-explicit -serverIP
     10.105.157.116 -ldapBase "CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDn "
     CN=Administrator,CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDnPassword
     freebsd123$ -ldapLoginName sAMAccountName
2 <!--NeedCopy-->
```

Ejemplo de proxy transparente:

```
1 add authentication ldapAction swg-auth-action-explicit -serverIP
     10.105.157.116 -ldapBase "CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDn "
     CN=Administrator,CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDnPassword
     freebsd123$ -ldapLoginName networkAddress -authentication disable -
     Attribute1 sAMAccountName
2 <!--NeedCopy-->
```

Configurar la autenticación de usuarios mediante la CLI

En el símbolo del sistema, escriba:

```
1 add authentication vserver <vserver name> SSL
2
3 bind ssl vserver <vserver name> -certkeyName <certkey name>
4
5 add authentication ldapAction <action name> -serverIP <ip_addr> -
     ldapBase <string> -ldapBindDn <string> -ldapBindDnPassword -
     ldapLoginName <string>
```



```
6
7 add authentication Policy <policy name> -rule <expression> -action <
     string>
8
9 bind authentication vserver <vserver name> -policy <string> -priority <
     positive_integer>
10
11 set cs vserver <name> -authn401 ON -authnVsName <string>
12 <!--NeedCopy-->
```

Argumentos:

Nombre del servidor virtual:

Nombre del servidor virtual de autenticación al que se va a enlazar la directiva.

Longitud máxima: 127

Tipo de servicio:

Tipo de protocolo del servidor virtual de autenticación. Siempre SSL.

Valores posibles: SSL

Valor predeterminado: SSL

Nombre de la acción:

Nombre de la nueva acción LDAP. Debe comenzar con una letra, un número o un carácter de guión bajo (_) y debe contener solo letras, números y guión (-), punto (.), almohadilla (#), espacio ( ), en (@), igual a (=), dos puntos (:) y guión bajo. No se puede cambiar después de agregar la acción LDAP. El siguiente requisito solo se aplica a la CLI:

Si el nombre incluye uno o varios espacios, escriba el nombre entre comillas dobles o simples (por ejemplo, “mi acción de autenticación” o “mi acción de autenticación”).

Longitud máxima: 127

IP del servidor:

Dirección IP asignada al servidor LDAP.

Base LDAP:

Base (nodo) desde la que se inician las búsquedas LDAP. Si el servidor LDAP se ejecuta localmente, el valor predeterminado de base es dc=netscaler, dc=com. Longitud máxima: 127

DDN de enlace LDAP:

Nombre distintivo completo (DN) que se utiliza para enlazar con el servidor LDAP.

Predeterminado: cn=manager, dc=netscaler, dc=com

Longitud máxima: 127

Contraseña LDAP Binddn:

Contraseña utilizada para enlazar con el servidor LDAP.

Longitud máxima: 127

Nombre de inicio de sesión de LDAP:

Atributo de nombre de inicio de sesión LDAP. El dispositivo Citrix ADC utiliza el nombre de inicio de sesión LDAP para consultar servidores LDAP externos o Active Directories. Longitud máxima: 127

Nombre de la directiva:

Nombre de la directiva AUTENTICACIÓN avanzada. Debe comenzar con una letra, un número o un carácter de guión bajo (_) y debe contener solo letras, números y guión (-), punto (.), almohadilla (#), espacio ( ), en (@), igual a (=), dos puntos (:) y guión bajo. No se puede cambiar después de crear una directiva de AUTENTICACIÓN. El siguiente requisito solo se aplica a la CLI:

Si el nombre incluye uno o varios espacios, escriba el nombre entre comillas dobles o simples (por ejemplo, “mi directiva de autenticación” o “mi directiva de autenticación”).

Longitud máxima: 127

regla:

Nombre de la regla o expresión de directiva avanzada que utiliza la directiva para determinar si se intenta autenticar al usuario con el servidor AUTENTICATION.

Longitud máxima: 1499

acción:

Nombre de la acción de autenticación que se va a realizar si la directiva coincide.

Longitud máxima: 127

prioridad:

Entero positivo que especifica la prioridad de la directiva. Un número inferior especifica una prioridad más alta. Las directivas se evalúan en el orden de sus prioridades y se aplica la primera directiva que coincide con la solicitud. Debe ser único en la lista de directivas enlazadas al servidor virtual de autenticación.

Valor mínimo: 0

Valor máximo: 4294967295

Ejemplo:


```
add authentication vserver swg-auth-vs SSL

Done

bind ssl vserver explicit-auth-vs -certkeyName ns-swg-ca-certkey

Done

add authentication ldapAction swg-auth-action-explicit -serverIP
    192.0.2.116 -ldapBase "CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDn "CN=
    Administrator,CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDnPassword zzzzz
     -ldapLoginName sAMAccountName

Done

add authenticationpolicy swg-auth-policy -rule true -action swg-auth-
    action-explicit
Done

bind authentication vserver swg-auth-vs -policy swg-auth-policy -
    priority 1

Done

set cs vserver testswg -authn401 ON -authnVsName swg-auth-vs

Done
<!--NeedCopy-->
```

Habilitar el registro de nombres de usuario mediante la CLI

En el símbolo del sistema, escriba:

```
set appflow param -AAAUserName ENABLED
<!--NeedCopy-->
```

Argumentos:

Nombre de usuario AAAA

Habilite el registro de nombres de usuario de autenticación, autorización y auditoría de AppFlow.

Valores posibles: ENABLED, DISABLED

Valor predeterminado: DISABLED

Ejemplo:

```
set appflow param -AAAUserName ENABLED
<!--NeedCopy-->
```

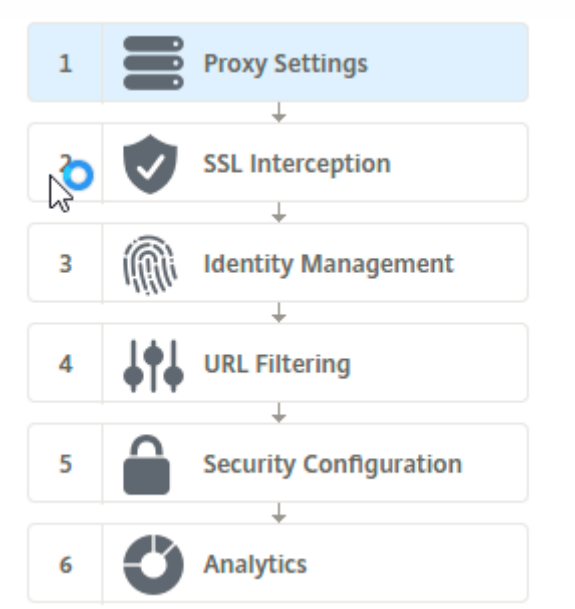
Filtrado de URL

August 20, 2021

El filtrado de URL proporciona un control basado en directivas de sitios web mediante el uso de la información contenida en las URL. Esta función ayuda a los administradores de red a supervisar y controlar el acceso de los usuarios a sitios web maliciosos de la red.

Introducción

Si es un usuario nuevo y quiere configurar el filtrado de URL, debe completar la configuración inicial del proxy de reenvío SSL. Para comenzar con el filtrado de URL, primero debe iniciar sesión en el asistente de proxy de reenvío SSL. El asistente le guiará por una serie de pasos de configuración antes de aplicar las directivas de filtrado de URL.



> **Nota**
>
> Antes de comenzar, asegúrese de que tiene instalada una licencia válida de función de URL Threat Intelligence en el dispositivo. Si utiliza una versión de prueba, asegúrese de adquirir una licencia válida para seguir mediante esta función en el dispositivo ADC.

Iniciar sesión en el asistente de proxy de reenvío SSL

El asistente de proxy de reenvío SSL le guía a través de una serie de tareas de configuración simplificadas y el panel derecho muestra la secuencia de flujo correspondiente. Puede utilizar este asistente para aplicar directivas de filtrado de URL a una lista de direcciones URL o a una lista predefinida de categorías.

Paso 1: Configurar la configuración del proxy

Primero configure un servidor proxy a través del cual el cliente accede a la puerta de enlace. Este servidor es de tipo SSL, y funciona en modo explícito o transparente. Para obtener más información sobre la configuración del servidor proxy, consulte Modos proxy.

Paso 2: Configurar la intercepción SSL

Después de configurar el servidor proxy, debe configurar el proxy de interceptación SSL para interceptar el tráfico cifrado en el dispositivo Citrix ADC. En el caso del filtrado de URL, el proxy SSL intercepta el tráfico y no permite URL bloqueadas, mientras que el resto del tráfico se puede omitir. Para obtener más información sobre cómo configurar la intercepción SSL, consulte Intercepción SSL.

Paso 3: Configurar la administración de identidades

Un usuario se autentica antes de que se le permita iniciar sesión en la red empresarial. La autenticación proporciona la flexibilidad necesaria para definir directivas específicas para un usuario o un grupo de usuarios, en función de sus funciones. Para obtener más información sobre la autenticación de usuarios, consulte Administración de identificación de usuarios.

Paso 4: Configurar el filtrado de URL

El administrador puede aplicar una directiva de filtrado de URL mediante la función Categorización de URL o mediante la función Lista de URL.

Categorización de URL. Controla el acceso a sitios web y páginas web filtrando el tráfico en función de una lista predefinida de categorías.

Lista de URL. Controla el acceso a sitios web y páginas web de la lista de prohibidos denegando el acceso a las direcciones URL que se encuentran en un conjunto de direcciones URL importadas al dispositivo.

Paso 5: Configurar la configuración de seguridad

Este paso le permite configurar una puntuación de reputación y permitir a los usuarios controlar el acceso a los sitios web denegando el acceso si la puntuación es demasiado baja. Su puntuación de reputación puede variar de uno a cuatro, y puede configurar el umbral en el que la puntuación se vuelve inaceptable. Para puntuaciones que superen el umbral, puede seleccionar una acción de directiva para permitir, bloquear o redirigir el tráfico. Para obtener más información, consulte Puntuación de reputación de URL.

Paso 6: Configurar el análisis de proxy directo SSL

Este paso le permite activar el análisis de proxy directo SSL para categorizar el tráfico web, registrar la categoría de URL en los registros de transacciones de usuario y ver análisis de tráfico. Para obtener más información sobre los análisis de proxy de reenvío SSL, consulte Analytics.

Paso 7: Haga clic en "Listo" para completar la configuración inicial y continuar administrando la configuración de filtrado de URL

Lista de URL

August 20, 2021

La función Lista de URL permite a los clientes empresariales controlar el acceso a sitios web específicos y categorías de sitios web. La función filtra sitios web aplicando una directiva de respuesta vinculada a un algoritmo de coincidencia de URL. El algoritmo hace coincidir la URL entrante con un conjunto de URL que consta de hasta un millón (1.000.000) de entradas. Si la solicitud de dirección URL entrante coincide con una entrada del conjunto, el dispositivo utiliza la directiva de respuesta para evaluar la solicitud (HTTP/HTTPS) y controlar el acceso a ella.

Tipos de conjuntos de direcciones URL

Cada entrada de un conjunto de URL puede incluir una URL y, opcionalmente, sus metadatos (categoría de URL, grupos de categorías o cualquier otro dato relacionado). Para las direcciones URL con metadatos, el dispositivo utiliza una expresión de directiva que evalúa los metadatos. Para obtener más información, consulte Conjunto de URL.

El proxy de reenvío SSL admite conjuntos de URL personalizados. También puede utilizar conjuntos de patrones para filtrar las URL.

Conjunto de URL personalizado. Puede crear un conjunto de direcciones URL personalizado con un máximo de 1.000.000 entradas de URL e importarlo como archivo de texto en el dispositivo.

Juego de patrones. Un dispositivo ADC puede utilizar conjuntos de patrones para filtrar direcciones URL antes de conceder acceso a sitios web. Un conjunto de patrones es un algoritmo de coincidencia de cadenas que busca una coincidencia exacta de cadenas entre una URL entrante y hasta 5000 entradas. Para obtener más información, consulte Conjunto de patrones.

Cada URL de un conjunto de URL importado puede tener una categoría personalizada en forma de metadatos de URL. La organización puede alojar el conjunto y configurar el dispositivo ADC para actualizarlo periódicamente sin necesidad de intervención manual.

Después de actualizar el conjunto, el dispositivo Citrix ADC detecta automáticamente los metadatos. La categoría ahora está disponible como expresión de directiva para evaluar la dirección URL y aplicar una acción como permitir, bloquear, redirigir o notificar al usuario.

Expresiones de directiva avanzadas utilizadas con conjuntos de direcciones URL

En la tabla siguiente se describen las expresiones básicas que puede utilizar para evaluar el tráfico entrante.

1. .URLSET_MATCHES_ANY: Evalúa como TRUE si la URL coincide exactamente con cualquier entrada en el conjunto de URL.
2. .GET_URLSET_METADATA (): La expresión GET_URLSET_METADATA () devuelve los metadatos asociados si la URL coincide exactamente con cualquier patrón dentro del conjunto de URL. Se devuelve una cadena vacía si no hay coincidencia.
3. `.GET_ URLSET_METADATA().EQ(<METADATA)- .GET_ URLSET_METADATA().EQ(<METADATA)`
4. .GET_URLSET_METADATA () .TYPECAST_LIST_T (‘,’) .GET (0) .EQ (): Evalúa como TRUE si los metadatos coincidentes están al principio de la categoría. Este patrón se puede utilizar para codificar campos separados dentro de los metadatos, pero solo coinciden con el primer campo.
5. HTTP.REQ.HOSTNAME.APPEND (HTTP.REQ.URL) - Une los parámetros host y URL, que luego se pueden usar para hacer coincidir.

Tipos de acción del respondedor

> **Nota:** En la tabla, HTTP.REQ.URL se generaliza como `<URL expression>`.

En la tabla siguiente se describen las acciones que se pueden aplicar al tráfico entrante de Internet.

Acción del Respondedor	Descripción
Permitir	Permitir que la solicitud acceda a la URL de destino.
Redirigir	Redirigir la solicitud a la URL especificada como destino.
Bloquear	Denegar la solicitud.

Requisitos previos

Configure un servidor DNS si importa un conjunto de URL desde una dirección URL de nombre de host. Esta configuración no es necesaria si utiliza una dirección IP.

En el símbolo del sistema, escriba:

```
add dns nameServer ((<IP> [-local])| <dnsVserverName>)[-state (ENABLED |
DISABLED )] [-type <type>] [-dnsProfileName <string>]
```

Ejemplo:

```
add dns nameServer 10.140.50.5
```

Configurar una lista de direcciones URL

Para configurar una lista de direcciones URL, puede utilizar el asistente de proxy de reenvío SSL de Citrix o la interfaz de línea de comandos (CLI) de Citrix ADC. En el dispositivo Citrix ADC, primero debe configurar la directiva de respondedor y, a continuación, enlazar la directiva a un conjunto de direcciones URL.

Citrix recomienda utilizar el asistente de proxy de reenvío SSL de Citrix como opción preferida para configurar una lista de direcciones URL. Utilice el asistente para enlazar una directiva de respondedor a un conjunto de direcciones URL. Alternativamente, puede enlazar la directiva a un conjunto de patrones.

Configurar una lista de direcciones URL mediante el asistente de proxy de reenvío SSL

Para configurar la lista de URL para el tráfico HTTPS mediante la GUI:

1. Vaya a la página **Seguridad** > **Proxy de reenvío SSL**.
2. En el panel de detalles, realice una de las acciones siguientes:
   a) Haga clic en **Asistente de proxy de reenvío SSL**.
   b) Seleccione una configuración existente y haga clic en **Modificar**.

3. En la sección **Filtrado de URL**, haga clic en **Modificar**.
4. Active la casilla **Lista de direcciones URL** para habilitar la función.
5. Seleccione una directiva de **lista de direcciones URL** y haga clic en **Enlazar**.
6. Haga clic en **Continuar** y, a continuación, en **Listo**.

Para obtener más información, consulte Cómo crear una directiva de lista de URL.

Configurar una lista de direcciones URL mediante la CLI

Para configurar una lista de direcciones URL, haga lo siguiente.

1. Configure un servidor virtual proxy para el tráfico HTTP y HTTPS.
2. Configure la intercepción SSL para interceptar el tráfico HTTPS.
3. Configure una lista de direcciones URL que contenga un conjunto de direcciones URL para el tráfico HTTP.
4. Configure la lista de direcciones URL que contiene el conjunto de direcciones URL para el tráfico HTTPS.
5. Configure un conjunto de direcciones URL privadas.

> **Nota**
>
> Si ya ha configurado un dispositivo ADC, puede omitir los pasos 1 y 2 y configurarlo con el paso 3.

Configuración de un servidor virtual proxy para el tráfico de Internet

El dispositivo Citrix ADC admite servidores virtuales proxy transparentes y explícitos. Para configurar un servidor virtual proxy para el tráfico de Internet en modo explícito, haga lo siguiente:

1. Agregue un servidor virtual SSL proxy.
2. Enlazar una directiva de respondedor al servidor virtual proxy.

Para agregar un servidor virtual proxy mediante la CLI:

En el símbolo del sistema, escriba:

```
add cs vserver <name> <serviceType> <IPAddress> <port>
<!--NeedCopy-->
```

Ejemplo:

```
add cs vserver starcs PROXY 10.102.107.121 80 -cltTimeout 180
<!--NeedCopy-->
```


Para enlazar una directiva de respondedor a un servidor virtual proxy mediante la CLI:

```
bind ssl vserver <vServerName> -policyName <string> [-priority <
    positive_integer>]
<!--NeedCopy-->
```

> **Nota**
>
> Si ya ha configurado el interceptor SSL como parte de la configuración de Citrix ADC, puede omitir el siguiente procedimiento.

Configurar la intercepción SSL para el tráfico HTTPS

Para configurar la intercepción SSL para el tráfico HTTPS, haga lo siguiente:

1. Enlazar un par de claves de certificado de CA al servidor virtual proxy.
2. Habilite el perfil SSL predeterminado.
3. Cree un perfil SSL front-end y enlaza al servidor virtual proxy y habilite la interceptación SSL en el perfil SSL front-end.

Para enlazar un par de claves de certificado de CA al servidor virtual proxy mediante la CLI:

En el símbolo del sistema, escriba:

```
bind ssl vserver <vServerName> -certkeyName <certificate-KeyPairName>
<!--NeedCopy-->
```

Para configurar un perfil SSL front-end mediante la CLI:

En el símbolo del sistema, escriba:

```
set ssl parameter -defaultProfile ENABLED

add ssl profile <name> -sslInterception ENABLED -ssliMaxSessPerServer <
    positive_integer>
<!--NeedCopy-->
```

Para enlazar un perfil SSL front-end a un servidor virtual proxy mediante la CLI

En el símbolo del sistema, escriba:


```
set ssl vserver <vServer name>  -sslProfile <name>
<!--NeedCopy-->
```

Configurar una lista de direcciones URL importando un conjunto de direcciones URL para el tráfico HTTP

Para obtener información sobre cómo configurar un conjunto de URL para el tráfico HTTP, consulte Conjunto de URL.

Realizar coincidencia explícita de subdominio

Ahora puede realizar una coincidencia explícita de subdominio para un conjunto de direcciones URL importadas. Se agrega un nuevo parámetro, "SubdomainExactMatch" al **import** policy URLset comando.

Al habilitar el parámetro, el algoritmo de filtrado de URL realiza una coincidencia explícita de subdominio. Por ejemplo, si la dirección URL entrante es news.example.com y si la entrada del conjunto de direcciones URL es example.com, el algoritmo no coincide con las direcciones URL.

En el símbolo del sistema, escriba:

```
import policy urlset <name> [-overwrite] [-delimiter <character>][-rowSeparator
 <character>] -url [-interval <secs>] [-privateSet][-subdomainExactMatch]
[-canaryUrl <URL>]
```

Ejemplo

```
import policy urlset test -url http://10.78.79.80/top-1k.csv -privateSet -
subdomainExactMatch -interval 900
```

Configurar un conjunto de direcciones URL para el tráfico HTTPS

Para configurar un conjunto de direcciones URL para el tráfico HTTPS mediante la CLI

En el símbolo del sistema, escriba:

```
add ssl policy <name> -rule <expression> -action <string> [-undefAction
    <string>] [-comment <string>]
<!--NeedCopy-->
```

Ejemplo:


```
add ssl policy pol1 -rule "client.ssl.client_hello.SNI.
    URLSET_MATCHES_ANY("top1m") -action INTERCEPT
<!--NeedCopy-->
```

Para configurar un conjunto de direcciones URL para el tráfico HTTPS mediante el asistente de proxy de reenvío SSL

Citrix recomienda utilizar el asistente de proxy de reenvío SSL como opción preferida para configurar una lista de direcciones URL. Utilice el asistente para importar un conjunto de direcciones URL personalizado y enlazar a una directiva de respondedor.

1. Vaya a **Seguridad > Proxy de reenvío SSL > Filtrado de URL > Listas de URL**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En la página **Directiva de lista de direcciones URL**, especifique el nombre de la directiva.
4. Seleccione una opción para importar un conjunto de direcciones URL.
5. En la página de separador **Directiva de lista de direcciones** URL, active la casilla de verificación **Importar conjunto de direcciones URL** y especifique los siguientes parámetros de conjunto de direcciones URL.
   a) Nombre de conjunto de direcciones URL: Nombre del conjunto de direcciones URL personalizado.
   b) URL: Dirección web de la ubicación en la que se accede al conjunto de direcciones URL.
   c) Sobrescribir (Overwrite): Sobrescribir un conjunto de direcciones URL importado previamente.
   d) Delimitador: Secuencia de caracteres que delimita un registro de archivo CSV.
   e) Separador de filas: Separador de filas utilizado en el archivo CSV.
   f) Intervalo: Intervalo en segundos, redondeado al número de segundos más cercano igual a 15 minutos, en el que se actualiza el conjunto de direcciones URL.
   g) Conjunto privado: Opción para impedir la exportación del conjunto de direcciones URL.
   h) URL Canary: URL interna para comprobar si el contenido del conjunto de URL debe mantenerse confidencial. La longitud máxima de la URL es de 2047 caracteres.
6. Seleccione una acción de respuesta en la lista desplegable.
7. Haga clic en **Crear** y **cerrar**.

Configurar un conjunto de direcciones URL privadas

Si configura un conjunto de direcciones URL privadas y mantiene su contenido confidencial, es posible que el administrador de red no conozca las direcciones URL incluidas en la lista de prohibidos del conjunto. En estos casos, puede configurar una URL Canary y agregarla al conjunto de direcciones URL. Mediante la URL Canary, el administrador puede solicitar que se utilice el conjunto de direcciones

URL privadas para cada solicitud de búsqueda. Puede consultar la sección del asistente para obtener descripciones de cada parámetro.

Para importar un conjunto de direcciones URL mediante la CLI:

En el símbolo del sistema, escriba:

```
1 import policy urlset <name> [-overwrite] [-delimiter <character>] [-
     rowSeparator <character>] -url <URL> [-interval <secs>] [-privateSet
     ] [-canaryUrl <URL>]
2 <!--NeedCopy-->
```

Ejemplo:

```
1 import policy urlset test1  - url http://10.78.79.80/alytra/top-1k.csv -
     private -canaryUrl http://www.in.gr
2 <!--NeedCopy-->
```

Mostrar conjunto de direcciones URL importadas

Ahora puede mostrar conjuntos de direcciones URL importados además de conjuntos de direcciones URL agregados. Se agrega un nuevo parámetro "importado" al `show urlset` comando. Si habilita esta opción, el dispositivo muestra todos los conjuntos de direcciones URL importados y distingue los conjuntos de direcciones URL importados de los conjuntos de direcciones URL agregados.

En el símbolo del sistema, escriba:

```
show policy urlset [<name>] [-imported]
```

Ejemplo

```
show policy urlset -imported
```

Configurar la mensajería del registro de auditoría

El registro de auditoría le permite revisar una condición o una situación en cualquier fase de un proceso de lista de URL. Cuando un dispositivo Citrix ADC recibe una dirección URL entrante, si la directiva de respuesta tiene una expresión de directiva avanzada Definir URL, la función de registro de auditoría recopila la información del conjunto de URL en la dirección URL. Almacena los detalles como un mensaje de registro para cualquier destino permitido por el registro de auditoría.

El mensaje de registro contiene la siguiente información:

1. Marca de tiempo.

2. Tipo de mensaje de registro.
3. Niveles de registro predefinidos (Crítico, Error, Aviso, Advertencia, Informativo, Depuración, Alerta y Emergencia).
4. Información del mensaje de registro, como el nombre del conjunto de direcciones URL, la acción de directiva o la dirección URL.

Para configurar el registro de auditoría para la función Lista de URL, debe completar las siguientes tareas:

1. Habilitar registros de auditoría.
2. Acción de mensaje Crear registro de auditoría.
3. Establecer la directiva de respuesta de lista de URL con la acción de mensaje Registro de auditoría.

Para obtener más información, consulte el tema Registro de auditoría .

Semántica de patrones de URL

August 20, 2021

En la tabla siguiente se muestran los patrones de URL utilizados para especificar la lista de páginas que quiere filtrar. Por ejemplo, el patrón www.example.com/bar solo coincide con una página en www.example.com/bar. Para que coincidan todas las páginas cuya URL comience por 'www.example.com/bar', agregue un asterisco (*) al final de la URL.

Semántica para el patrón de URL para que coincida con la asignación de metadatos

La semántica de coincidencia de patrones está disponible en formato de tabla. Para obtener más información, consulte la página PDF Semántica de patrones .

Asignación de categorías URL

August 20, 2021

Una lista de categorías y grupos de categorías de terceros. Para obtener más información, consulte la página Asignación de categorías de URL .

Caso práctico: filtrado de URL mediante el uso de un conjunto de URL personalizado

April 21, 2022

Si es un cliente empresarial que busca controlar el acceso a sitios web y categorías de sitios web específicos, utilice un conjunto de URL personalizado vinculado a una directiva de respuesta. La infraestructura de red de su organización puede usar un filtro de URL para bloquear el acceso a sitios web maliciosos o peligrosos. Por ejemplo, sitios web que presentan portales de adultos, violencia, juegos, drogas, directiva o empleo. Además de filtrar las URL, puede crear una lista personalizada de URL e importarla al dispositivo ADC. Por ejemplo, las directivas de su organización pueden exigir el bloqueo del acceso a ciertos sitios web, como las redes sociales, los portales de compras y los portales de empleo.

Cada URL de la lista puede tener una categoría personalizada en forma de metadatos. La organización puede alojar la lista de URL como una URL establecida en el dispositivo Citrix ADC. Configure el dispositivo para que actualice periódicamente el conjunto sin necesidad de intervención manual.

Una vez actualizado el conjunto, el dispositivo Citrix ADC detecta automáticamente los metadatos. La directiva de respuesta utiliza los metadatos de la URL (detalles de la categoría) para evaluar la URL entrante y aplicar una acción como permitir, bloquear, redirigir o notificar al usuario.

Para hacerlo, configure en su red, puede realizar las siguientes tareas:

1. Importar un conjunto de URL personalizado
2. Agregar un conjunto de URL personalizado
3. Configure una lista de URL personalizada en el asistente de proxy de reenvío SSL.

Importar un conjunto de URL personalizado mediante la CLI

En el símbolo del sistema, escriba:

```
import policy urlset <name> [-overwrite] [-delimiter <character>] [-
   rowSeparator <character>] -url <URL> [-interval <secs>] [-privateSet
   ] [-canaryUrl <URL>]

import policy urlset test1  -url http://10.78.79.80/alytra/top-1k.csv
<!--NeedCopy-->
```


Agregar un conjunto de URL personalizado mediante la CLI

En el símbolo del sistema, escriba:

```
add urlset <urlset_name>
```

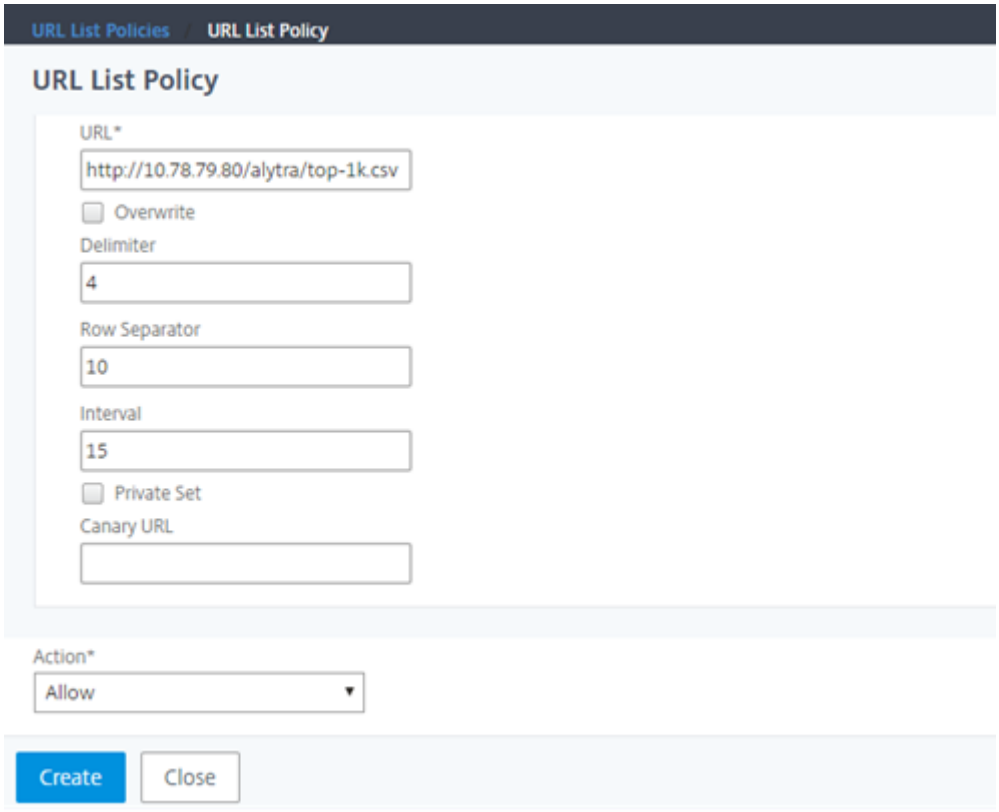
Ejemplo:

```
add urlset test1
```

Configurar una lista de URL mediante el asistente de proxy de reenvío SSL

Citrix recomienda utilizar el asistente de proxy de reenvío SSL como la opción preferida para configurar una lista de URL. Use el asistente para importar un conjunto de URL personalizado y vincularlo a una directiva de respuesta.

1. Vaya a **Seguridad > Proxy de reenvío SSL > Filtrado de URL > Listas de URL**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En la página **URL List Policy**, especifique el nombre de la directiva.
4. Seleccione una opción para importar un conjunto de URL.
5. En la página de la ficha **Directiva de lista de URL**, seleccione la casilla de verificación **Importar conjunto de URL** y especifique los siguientes parámetros de conjunto de URL.
   a) Nombre del conjunto de URL: nombre del conjunto de URL personalizado.
   b) URL: dirección web de la ubicación en la que se accede al conjunto de URL.
   c) Sobrescribir: sobrescribe un conjunto de URL importado anteriormente.
   d) Delimitador: secuencia de caracteres que delimita un registro de archivo CSV.
   e) Separador de filas: separador de filas utilizado en el archivo CSV.
   f) Intervalo: intervalo en segundos, redondeado a los 15 minutos más cercanos, en el que se actualiza el conjunto de URL.
   g) Conjunto privado: opción para evitar la exportación del conjunto de URL.
   h) URL Canary: URL interna para comprobar si el contenido del conjunto de URL debe mantenerse confidencial. La longitud máxima de la URL es de 2047 caracteres.
6. Seleccione una acción de respuesta de la lista desplegable.
7. Haga clic en **Crear** y **cerrar**.



Semántica de metadatos para conjuntos de URL personalizados

Para importar un conjunto de URL personalizado, agregue las URL a un archivo de texto y enlácelo a una directiva de respuesta para bloquear las URL de redes sociales.

A continuación se muestran ejemplos de URL que puede agregar al archivo de texto:

cnn.com, Noticias

bbc.com, Noticias

google.com, motor de búsqueda

yahoo.com, Motor de búsqueda

facebook.com, Redes sociales

twitter.com, Redes sociales

Configurar una directiva de respuesta para bloquear las URL de redes sociales mediante la CLI

```
1 add responder action act_url_unauthorized respondwith '"HTTP/1.1 451
     Unavailable For Legal Reasons\r\n\r\nURL is NOT authorized\n"'
```



```
2
3 add responder policy pol_url_meta_match 'HTTP.REQ.HOSTNAME.APPEND(HTTP.
     REQ.URL).GET_URLSET_METADATA(”u1”).EQ(”Social Media”)'
     act_url_unauthorized
4 <!--NeedCopy-->
```

categorización de URL

May 8, 2022

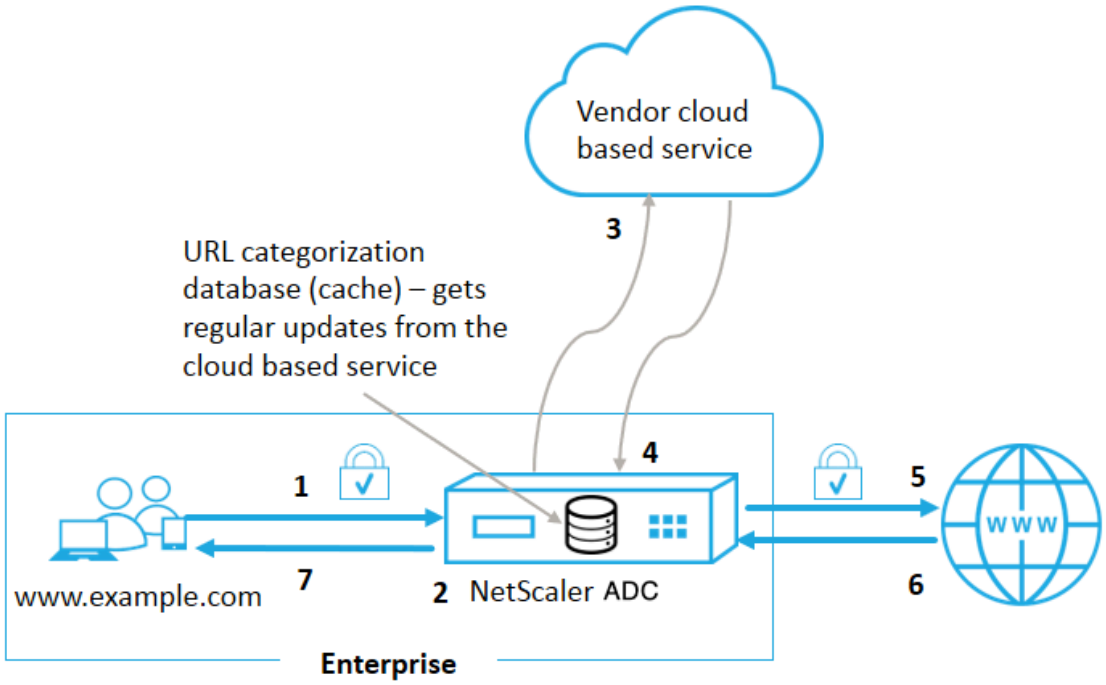
La categorización de URL restringe el acceso del usuario a sitios web y categorías de sitios web específicos. Como servicio suscrito en colaboración con NetSTAR, la función permite a los clientes empresariales filtrar el tráfico web mediante una base de datos de categorización comercial. La base de datos NetSTAR tiene una gran cantidad (miles de millones) de URL clasificadas en diferentes categorías, como redes sociales, juegos de azar, contenido para adultos, nuevos medios y compras. Además de la categorización, cada URL tiene una puntuación de reputación actualizada en función del perfil de riesgo histórico del sitio. Podemos utilizar datos de NetSTAR para filtrar el tráfico mediante la configuración de directivas avanzadas basadas en categorías, grupos de categorías (como terrorismo, drogas ilegales) o puntuaciones de reputación del sitio.

Por ejemplo, puede bloquear el acceso a sitios peligrosos, como los sitios que se sabe que están infectados con malware. También puede restringir selectivamente el acceso a contenido, como contenido para adultos o medios de transmisión de entretenimiento para usuarios empresariales. También puede capturar los detalles transaccionales y del tráfico saliente del usuario para supervisar el análisis del tráfico web en el servidor Citrix ADM.

Citrix ADC carga o descarga datos del dispositivo NetSTAR preconfigurado nsv10.netstar-inc.com y incompasshybridpc.netstar-inc.com se utiliza como host en la nube de forma predeterminada para las solicitudes de categorización en la nube. Se debe poder acceder a estas URL a través del firewall para que el filtrado de URL funcione correctamente. El dispositivo utiliza su dirección NSIP como dirección IP de origen y 443 como puerto de destino para la comunicación.

Cómo funciona la categorización de URL

La siguiente ilustración muestra cómo se integra un servicio de categorización de URL Citrix ADC con una base de datos comercial de categorización de URL y servicios en la nube para actualizaciones frecuentes.



Los componentes interactúan de la siguiente manera:

1. Un cliente envía una solicitud de URL enlazada a Internet.
2. El proxy de reenvío SSL aplica una directiva de cumplimiento a la solicitud en función de los detalles de la categoría, como la categoría, el grupo de categorías y la puntuación de reputación del sitio. Los detalles de la categoría se obtienen de la base de datos de categorización de URL. Si la base de datos devuelve los detalles de la categoría, el proceso salta al paso 5.
3. Si la base de datos omite los detalles de categorización, la solicitud se envía a un servicio de búsqueda basado en la nube mantenido por un proveedor de categorización de URL. Sin embargo, el dispositivo no espera una respuesta, sino que la URL se marca como sin categoría y se aplica una directiva (vaya al paso 5). El dispositivo continúa supervisando los comentarios de las consultas en la nube y actualiza la memoria caché para que las solicitudes futuras puedan beneficiarse de la búsqueda en la nube.
4. El dispositivo ADC recibe los detalles de la categoría de URL (categoría, grupo de categorías y puntuación de reputación) del servicio basado en la nube y los almacena en la base de datos de categorización.
5. La directiva permite la URL y la solicitud se envía al servidor de origen. De lo contrario, el dispositivo pierde, redirige o responde con una página HTML personalizada.
6. El servidor de origen responde con los datos solicitados al dispositivo ADC.
7. El dispositivo envía la respuesta al cliente.

Caso de uso: uso de Internet bajo cumplimiento corporativo para empresas

Puede utilizar la función de filtrado de URL para detectar e implementar directivas de cumplimiento para bloquear los sitios que infrinjan el cumplimiento corporativo. Por ejemplo, sitios como adultos, medios de transmisión, redes sociales que pueden considerarse no productivos o consumir un ancho de banda de Internet excesivo en una red empresarial. Bloquear el acceso a estos sitios web puede mejorar la productividad de los empleados, reducir los costes operativos para el uso del ancho de banda y reducir la sobrecarga del consumo de la red.

Requisitos previos

La función de categorización de URL funciona en una plataforma Citrix ADC solo si tiene un servicio de suscripción opcional con capacidades de filtrado de URL e inteligencia de amenazas para el proxy de reenvío SSL. La suscripción permite a los clientes descargar las últimas categorizaciones de amenazas para los sitios web y, a continuación, aplicar esas categorías al proxy de reenvío SSL. Antes de habilitar y configurar la función, debe instalar las siguientes licencias:

- `CNS_WEBF_SSERVER_Retail.lic`
- `CNS_XXXX_SERVER_PLT_Retail.lic`

Donde XXXXX es el tipo de plataforma, por ejemplo: V25000

Expresiones de la directiva

En la siguiente tabla se enumeran las diferentes expresiones de directiva que puede usar para verificar si una URL entrante debe permitirse, redirigirse o bloquearse.

1. `<text>. URL_CATEGORIZE (<min_reputation>, <max_reputation>)` - Devuelve un objeto URL_CATEGORY. Si `<min_reputation>` es mayor que 0, el objeto devuelto no contiene una categoría con una reputación inferior a `<min_reputation>`. Si `<max_reputation>` es mayor que 0, el objeto devuelto no contiene una categoría con una reputación superior a `<max_reputation>`. Si la categoría no se resuelve de manera oportuna, se devuelve el valor undef.
2. `<url_category>. CATEGORY()` - Devuelve la cadena de categoría de este objeto. Si la URL no tiene una categoría, o si la URL tiene un formato incorrecto, el valor devuelto es “Desconocido”.
3. `<url_category>. CATEGORY_GROUP()` - Devuelve una cadena que identifica el grupo de categorías del objeto. Esta agrupación es una agrupación de categorías de nivel superior, lo que resulta útil en operaciones que requieren información menos detallada sobre la categoría de URL. Si la URL no tiene una categoría, o si la URL tiene un formato incorrecto, el valor devuelto es “Desconocido”.
4. `<url_category>. REPUTATION()` - Devuelve la puntuación de reputación como un número del 0 al 5, donde 5 indica la reputación más arriesgada. Si existe la categoría “Desconocido”, el

valor de reputación es 1.

Tipos de directivas:

1. Directiva para seleccionar solicitudes de URL que están en la categoría de motores de búsqueda - `add responder policy p1 'HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGORIZE(0,0). CATEGORY().EQ( "Search Engine" )`
2. Directiva para seleccionar solicitudes de URL que están en el grupo de categoría Adultos - `add responder policy p1 'HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGORIZE(0,0). CATEGORY_GROUP().EQ( "Adult" )'`
3. Directiva para seleccionar solicitudes de URL de motores de búsqueda con una puntuación de reputación inferior a 4 - `add responder policy p2 'HTTP.REQ.HOSTNAME.APPEND (HTTP.REQ.URL).URL_CATEGORIZE(4,0).HAS_CATEGORY( "Search Engine" )`
4. Directiva para seleccionar solicitudes de URL de motor de búsqueda y de compras - `add responder policy p3 'HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGORIZE(0,0).CATEGORY().EQ ( "good_categories" )`
5. Directiva para seleccionar solicitudes de URL de motores de búsqueda con una puntuación de reputación igual o superior a 4 - `add responder policy p5 'CLIENT.SSL.DETECTED_DOMAIN.URL_CATEGORIZE(4,0). CATEGORY().EQ( "Search Engines" )`
6. Directiva para seleccionar solicitudes de URL que están en la categoría de motores de búsqueda y compararlas con un conjunto de URL - `'HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGORIZE(0,0). CATEGORY().EQ( "Search Engine" )&& HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URLSET_MATCHES_ANY( "u1" )'`

Tipos de directivas de respuesta

Hay dos tipos de directivas que se utilizan en una función de categorización de URL y cada uno de estos tipos de directivas se explica en la siguiente tabla:

Tipo de directiva	Descripción
URL Category	Clasifique el tráfico web y, en función de los resultados de la evaluación, bloquee, permita o redirija el tráfico.
Puntuación de reputación de URL	Determina la puntuación de reputación del sitio web y le permite controlar el acceso en función del nivel de umbral de puntuación de reputación establecido por el administrador.

Configurar la categorización de URL

Para configurar la categorización de URL en un dispositivo Citrix ADC, haga lo siguiente:

1. Habilite el filtrado de URL.
2. Configure un servidor proxy para el tráfico web.
3. Configure la interceptación SSL para el tráfico web en modo explícito.
4. Configure la memoria compartida para limitar la memoria caché.
5. Configure los parámetros de categorización de URL.
6. Configure la categorización de URL mediante el asistente de proxy de reenvío SSL de Citrix.
7. Configure los parámetros de categorización de URL mediante el asistente de proxy de reenvío SSL.
8. Configurar la ruta de la base de datos semilla y el nombre

Paso 1: Habilitar el filtrado de URL

Para habilitar la categorización de URL, habilite la función de filtrado de URL y habilite los modos de categorización de URL.

Para habilitar la categorización de URL mediante la CLI

En el símbolo del sistema, escriba:

```
enable ns feature URLFiltering
```

```
disable ns feature URLFiltering
```

Paso 2: Configurar un servidor proxy para el tráfico web en modo explícito

El dispositivo Citrix ADC admite servidores virtuales proxy transparentes y explícitos. Para configurar un servidor virtual proxy para el tráfico SSL en modo explícito, haga lo siguiente:

1. Agregue un servidor proxy.
2. Enlazar una directiva SSL al servidor proxy.

Para agregar un servidor proxy mediante la CLI

En el símbolo del sistema, escriba:

```
add cs vserver <name> [-td <positive_integer>] <serviceType> [-cltTimeout <
secs>]
```

Ejemplo:

```
add cs vserver starcs PROXY 10.102.107.121 80 -cltTimeout 180
```


Enlazar una directiva SSL a un servidor virtual proxy mediante la CLI

```
bind ssl vserver <vServerName> -policyName <string> [-priority <positive_integer
>]
```

Paso 3: Configurar la interceptación SSL para el tráfico HTTPS

Para configurar la interceptación SSL para el tráfico HTTPS, haga lo siguiente:

1. Enlace un par de claves de certificado de CA al servidor virtual proxy.
2. Configure el perfil SSL predeterminado con parámetros SSL.
3. Enlace un perfil SSL front-end al servidor virtual proxy y habilite la interceptación SSL en el perfil SSL front-end.

Para enlazar un par de claves de certificado de CA al servidor virtual proxy mediante la CLI

En el símbolo del sistema, escriba:

```
bind ssl vserver <vServerName> -certkeyName <certificate-KeyPairName> -CA -
skipCAName
```

Para configurar el perfil SSL predeterminado mediante la CLI

En el símbolo del sistema, escriba:

```
set ssl profile <name> -denySSLReneg <denySSLReneg> -sslInterception (
ENABLED | DISABLED)-ssliMaxSessPerServer positive_integer>
```

Enlazar un perfil SSL front-end a un servidor virtual proxy mediante la CLI

En el símbolo del sistema, escriba:

```
set ssl vserver <vServer name> -sslProfile ssl_profile_interception
```

Paso 4: configurar la memoria compartida para limitar la memoria caché

Para configurar la memoria compartida para limitar la memoria caché mediante la CLI

En el símbolo del sistema, escriba:

```
set cache parameter [-memLimit <megaBytes>]
```

Donde el límite de memoria configurado para el almacenamiento en caché se establece como 10 MB.

Paso 5: Configurar los parámetros de categorización de URL

Para configurar los parámetros de categorización de URL mediante la CLI

En el símbolo del sistema, escriba:

```
set urlfiltering parameter [-HoursBetweenDBUpdates <positive_integer>] [-
TimeOfDayToUpdateDB <HH:MM>]
```

Ejemplo:

```
set urlfiltering parameter -urlfilt_hours_betweenDB_updates 20
```

Paso 6: Configurar la categorización de URL mediante el asistente de proxy de reenvío SSL de Citrix

1. Inicie sesión en el dispositivo Citrix ADC y vaya a la página **Seguridad** > **Proxy de reenvío SSL**.
2. En el panel de detalles, realice una de las acciones siguientes:
   a) Haga clic en **Asistente de proxy de reenvío SSL** para crear una nueva configuración.
   b) Seleccione una configuración existente y haga clic en **Modificar**.
3. En la sección **Filtrado de URL**, haga clic en **Modificar**.
4. Seleccione la casilla de verificación **Categorización de URL** para habilitar la función.
5. Seleccione una directiva de **categorización de URL** y haga clic en **Vincular**.
6. Haga clic en **Continuar** y, a continuación, en **Listo**.

Para obtener más información sobre la directiva de categorización de URL, consulte Cómo crear una directiva de categorización de URL.

Paso 7: Configuración de los parámetros de categorización de URL mediante un Asistente de proxy de reenvío SSL

1. Inicie sesión en el dispositivo **Citrix ADC** y vaya a **Seguridad > Filtrado de URL**.
2. En la página **Filtro de URL**, haga clic en **el enlace Cambiar configuración de filtrado de URL**.
3. En la página **Configuración de parámetros de filtrado de URL**, especifique los siguientes parámetros.
   a) Horas entre actualizaciones de base de datos. Horas de filtrado de URL entre actualizaciones de bases de datos Valor mínimo: 0 y valor máximo: 720.
   b) Hora del día para actualizar la base de datos. Hora del día de filtrado de URL para actualizar la base de datos.
   c) Host en la nube. La ruta URL del servidor en la nube.
   d) Ruta de base de datos semilla. La ruta URL del servidor de búsqueda en la base de datos semilla.
4. Haga clic en **Aceptar** y **cerrar**.

Configuración de ejemplo:


```
enable ns feature LB CS SSL IC RESPONDER AppFlow URLFiltering

enable ns mode FR L3 Edge USNIP PMTUD

set ssl profile ns_default_ssl_profile_frontend -denySSLReneg NONSECURE
     -sslInterception ENABLED -ssliMaxSessPerServer 100

add ssl certKey swg_ca_cert -cert ns_swg_ca.crt -key ns_swg_ca.key

set cache parameter -memLimit 100

add cs vserver starcs PROXY 10.102.107.121 80 -cltTimeout 180

add responder action act1 respondwith ""HTTP/1.1 200 OK\r\n\r\n" + http
    .req.url.url_categorize(0,0).reputation + "\n""

add responder policy p1 "HTTP.REQ.URL.URL_CATEGORIZE(0,0).CATEGORY.eq("
    Shopping/Retail") || HTTP.REQ.URL.URL_CATEGORIZE(0,0).CATEGORY.eq("
    Search Engines & Portals

")" act1

bind cs vserver starcs_PROXY -policyName p1 -priority 10 -
    gotoPriorityExpression END -type REQUEST

add dns nameServer 10.140.50.5

set ssl parameter -denySSLReneg NONSECURE -defaultProfile ENABLED -
    sigDigestType RSA-MD5 RSA-SHA1 RSA-SHA224 RSA-SHA256 RSA-SHA384 RSA-
    SHA512 -ssliErrorCache ENABLED

-ssliMaxErrorCacheMem 100000000

add ssl policy pol1 -rule "client.ssl.origin_server_cert.subject.
    URL_CATEGORIZE(0,0).CATEGORY.eq("Search Engines & Portals")"" -
    action INTERCEPT

add ssl policy pol3 -rule "client.ssl.origin_server_cert.subject.ne("
    citrix")" -action INTERCEPT

add ssl policy swg_pol -rule "client.ssl.client_hello.SNI.
    URL_CATEGORIZE(0,0).CATEGORY.ne("Uncategorized")" -action INTERCEPT

set urlfiltering parameter -HoursBetweenDBUpdates 3 -
```



```
      TimeOfDayToUpdateDB 03:00
<!--NeedCopy-->
```

Configurar la ruta de la base de datos semilla y el nombre

Ahora puede configurar la ruta de la base de datos semilla y el nombre del servidor de búsqueda en la nube para la configuración manual del nombre del servidor de búsqueda en la nube y la ruta de la base de Para ello, se agregan dos nuevos parámetros, “CloudHost” y “SeedDBPath”, al parámetro de filtrado de URL.

En el símbolo del sistema, escriba:

```
set urlfiltering parameter [-HoursBetweenDBUpdates <positive_integer>] [-TimeOfDayToUpdateDB <HH:MM>] [-LocalDatabaseThreads <positive_integer>] [-CloudHost <string>] [-SeedDBPath <string>]
```

Ejemplo:

```
set urlfiltering parameter -HoursBetweenDBUpdates 3 -TimeOfDayToUpdateDB 03:00 -CloudHost localhost -SeedDBPath /mypath
```

La comunicación entre un dispositivo Citrix ADC y NetSTAR puede requerir un servidor de nombres de dominio. Puede realizar pruebas mediante una consola simple o una conexión telnet desde el dispositivo.

Ejemplo:

```
root@ns# telnet nsv10.netstar-inc.com 443
Trying 1.1.1.1...
Connected to nsv10.netstar-inc.com.
Escape character is '^]'.

root@ns# telnet incompasshybridpc.netstar-inc.com 443
Trying 10.10.10.10...
Connected to incompasshybridpc.netstar-inc.com.
Escape character is '^]'.
<!--NeedCopy-->
```

Configurar los mensajes del registro de auditoría

El registro de auditoría le permite revisar una condición o una situación en cualquier fase del proceso de categorización de URL. Cuando un dispositivo Citrix ADC recibe una URL entrante, si la directiva

de respuesta tiene una expresión de filtrado de URL, la función de registro de auditoría recopila información de conjunto de URL en la URL. Almacena la información como mensajes de registro para cualquier destino permitido por el registro de auditoría.

- Dirección IP de origen (la dirección IP del cliente que realizó la solicitud).
- Dirección IP de destino (la dirección IP del servidor solicitado).
- URL solicitada que contiene el esquema, el host y el nombre de dominio (http://www.example.com).
- Categoría de URL que devuelve el marco de filtrado de URL.
- Grupo de categorías de URL que devolvió el marco de filtrado de URL.
- Número de reputación de URL que devolvió el marco de filtrado de URL.
- Acción de registro de auditoría llevada a cabo por la directiva.

Para configurar el registro de auditoría para una función de lista de URL, debe completar las siguientes tareas:

1. Habilitar registros de auditoría.
2. Acción de mensaje Crear registro de auditoría.
3. Establecer la directiva de respuesta de lista de URL con la acción de mensaje Registro de auditoría.

Para obtener más información, consulte el tema Registro de auditoría.

Almacenamiento de errores mediante mensajería SYSLOG

En cualquier etapa del proceso de filtrado de URL, si se produce un error en el nivel del sistema, el dispositivo ADC utiliza el mecanismo de registro de auditoría para almacenar registros en el archivo ns.log. Los errores se almacenan como mensajes de texto en formato SYSLOG para que un administrador pueda verlos más adelante en un orden cronológico de ocurrencia del evento. Estos registros también se envían a un servidor SYSLOG externo para su archivado. Para obtener más información, consulte el artículo CTX229399.

Por ejemplo, si se produce un error al inicializar el SDK de filtrado de URL, el mensaje de error se almacena en el siguiente formato de mensajería.

```
Oct 3 15:43:40 <local0.err> ns URLFiltering[1349]: Error initializing
NetStar SDK (SDK error=-1). (status=1).
```

El dispositivo Citrix ADC almacena los mensajes de error en cuatro categorías de error diferentes:

- **Error en la descarga**. Si se produce un error al intentar descargar la base de datos de categorización.
- **Fallo de integración**. Si se produce un error al integrar una actualización en la base de datos de categorización existente.

- **Fallo de inicialización**. Si se produce un error al inicializar la función de categorización de URL, establecer los parámetros de categorización o finalizar un servicio de categorización.
- **Fallo en la recuperación**. Si se produce un error cuando el dispositivo recupera los detalles de categorización de la solicitud.

Configurar capturas SNMP para eventos de NetSTAR

La función de filtrado de URL genera capturas SNMP si se dan las siguientes condiciones:

- La actualización de la base de datos NetSTAR falla o se realiza correctamente.
- La inicialización del SDK de NetSTAR falla o se realiza correctamente.

El dispositivo tiene un conjunto de entidades condicionales denominadas alarmas SNMP. Cuando se cumple una condición en la alarma SNMP, el dispositivo genera capturas y las envía a un destino de captura especificado. Por ejemplo, si se produce un error en la inicialización del SDK de NetSTAR, se genera un OID SNMP 1.3.6.1.4.1.5951.1.1.0.183 y se envía al destino de captura.

Para que el dispositivo genere capturas, primero debe habilitar y configurar las alarmas SNMP. A continuación, especifique el destino de captura al que el dispositivo envía los mensajes de captura generados.

Habilitar una alarma SNMP

El dispositivo Citrix ADC genera capturas solo para las alarmas SNMP que están habilitadas. Algunas alarmas están habilitadas de forma predeterminada, pero puede desactivarlas.

Cuando se habilita una alarma SNMP, la función de filtrado de URL genera mensajes de captura cuando se produce un evento de éxito o error. Algunas alarmas están habilitadas de forma predeterminada.

Para habilitar una alarma SNMP mediante la interfaz de línea de comandos:

En el símbolo del sistema, escriba los siguientes comandos para establecer los parámetros y verificar la configuración:

```
enable snmp alarm <trapName>
show snmp alarm <trapName>
```

Para habilitar una alarma SNMP mediante la GUI de Citrix ADC

1. Vaya a **Sistema** > **SNMP** > **Alarmas**y seleccione la alarma.
2. Haga clic en **Acciones** y seleccione **Habilitar**.

Configurar la alarma SNMP mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para establecer los parámetros y verificar la configuración:


```
set snmp alarm <trapName> [-thresholdValue <positive_integer> [-normalValue
 <positive_integer>]] [-time <secs>] [-state ( ENABLED | DISABLED )] [-
severity <severity>] [-logging ( ENABLED | DISABLED )]
```

Ejemplo:

```
set snmp alarm URL-FIL-DB-UPDATE-STATUS -state ENABLED
set snmp alarm URL-FIL-INIT-SDK -state ENABLED
```

Configurar alarmas SNMP mediante la interfaz gráfica de usuario

Vaya a **Sistema** > **SNMP** > **Alarmas**, seleccione una alarma y configure los parámetros de la alarma.

Para obtener más información sobre las capturas SNMP, consulte el tema SNMP.

Puntuación de reputación de URL

October 5, 2021

La función Categorización de URL proporciona un control basado en directivas para restringir las direcciones URL incluidas en la lista de prohibidos. Puede controlar el acceso a los sitios web en función de la categoría de URL, la puntuación de reputación o la categoría de URL y la puntuación de reputación. Si los administradores de red supervisan a un usuario que accede a sitios web de alto riesgo, pueden utilizar una directiva de respuesta vinculada a la puntuación de reputación de URL para bloquear dichos sitios web peligrosos.

Al recibir una solicitud de URL entrante, el dispositivo recupera la puntuación de categoría y reputación de la base de datos de categorización de URL. Según la puntuación de reputación devuelta por la base de datos, el dispositivo asigna una calificación de reputación a los sitios web. El valor puede oscilar entre 1 y 4, donde 4 es el tipo de sitio web más riesgoso, como se muestra en la tabla siguiente.

Calificación de reputación de URL	Comentario de reputación
1	Sitio limpio
2	Sitio desconocido
3	Potencialmente peligroso o afiliado a un sitio peligroso
4	Sitio malicioso

Caso de uso: filtrado por puntuación de reputación de URL

Considere una organización empresarial con un administrador de red que supervisa las transacciones de los usuarios y el consumo de ancho de banda Si el malware puede entrar en la red, el administrador debe mejorar la seguridad de los datos y controlar el acceso a sitios web maliciosos y peligrosos que acceden a la red. Para proteger la red contra dichas amenazas, el administrador puede configurar la función de filtrado de URL para permitir o denegar el acceso por puntuación de reputación de URL.

Para obtener más información sobre la supervisión del tráfico saliente y las actividades de los usuarios en la red, consulte Analytics.

Si un empleado de la organización intenta acceder a un sitio web de redes sociales, el dispositivo ADC recibe una solicitud de URL. Consulta la base de datos de categorización de URL para recuperar la categoría URL como red social y un puntaje de reputación 3, lo que indica un sitio web potencialmente peligroso. A continuación, el dispositivo comprueba la directiva de seguridad configurada por el administrador, como bloquear el acceso a sitios con un índice de reputación de 3 o más. A continuación, aplica la acción directiva para controlar el acceso al sitio web.

Para implementar esta función, debe configurar la puntuación de reputación de URL y los niveles de umbral de seguridad mediante el asistente Proxy de reenvío SSL.

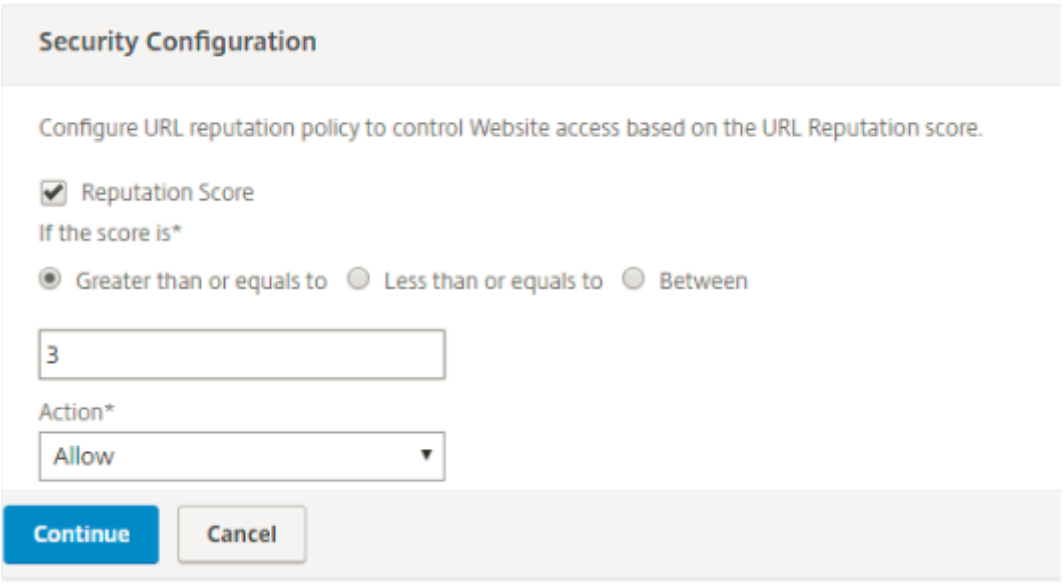
Configurar la puntuación de reputación mediante la interfaz gráfica de usuario

Citrix recomienda utilizar el asistente de proxy de reenvío SSL para configurar la puntuación de reputación y los niveles de seguridad. Según el umbral configurado, puede seleccionar una acción de directiva para permitir, bloquear o redirigir el tráfico.

1. Vaya a **Seguridad** > **Proxy de reenvío SSL**.
2. En el panel de detalles, haga clic en **Asistente para proxy de reenvío SSL**.
3. En la página de detalles, especifique la configuración del servidor proxy.
4. Haga clic en **Continuar** para especificar otros ajustes, como interceptación SSL y administración de identificaciones.
5. Haga clic en **Continuar** para acceder a la sección **Configuración de seguridad** .
6. En la sección **Configuración de seguridad**, active la casilla de verificación **Puntuación de reputación** para controlar el acceso en función de la puntuación de reputación de URL.
7. Seleccione el nivel de seguridad y especifique el valor umbral de puntuación de reputación:
   a) Mayor o igual que: permite o bloquea un sitio web si el valor del umbral es mayor o igual a N, donde N oscila entre uno y cuatro.
   b) Menor o igual que: permite o bloquea un sitio web si el valor del umbral es menor o igual a N, donde N oscila entre uno y cuatro.
   c) Entre medias: permite o bloquea un sitio web si el valor de umbral está entre N1 y N2 y el rango es de uno a cuatro.
8. Seleccione una acción de respuesta de la lista desplegable.

9. Haga clic en **Continuary cerrar**.

En la imagen siguiente se muestra la sección **Configuración de seguridad** del Asistente para proxy de reenvío SSL. Habilite la opción Puntuación de reputación de URL para configurar la configuración de la directiva.



Analytics

October 5, 2021

En el dispositivo Citrix ADC, se registran todos los registros de usuario y los registros posteriores. Al integrar Citrix Application Delivery Management (ADM) con el dispositivo Citrix ADC, la actividad del usuario registrado y los registros posteriores del dispositivo se exportan a Citrix ADM mediante la función `logstream`.

Citrix ADM recopila y presenta información sobre las actividades de los usuarios, como los sitios web visitados y el ancho de banda gastado. También informa sobre el uso del ancho de banda y las amenazas detectadas, como malware y sitios de phishing. Puede utilizar estas métricas clave para supervisar la red y realizar acciones correctivas con el dispositivo Citrix SWG. Para obtener más información, consulte Citrix SSL Forward Proxy Analytics.

Para integrar el dispositivo Citrix ADC con Citrix ADM:

1. En el dispositivo Citrix ADC, mientras configura la función de proxy de reenvío SSL, habilite Analytics y proporcione los detalles de la instancia de Citrix ADM que quiere utilizar para análisis.
2. En Citrix ADM, agregue el dispositivo Citrix ADC como instancia a Citrix ADM. Para obtener más información, consulte Agregar instancias a Citrix ADM.

Caso de uso: Hacer que una red empresarial sea segura mediante el uso de ICAP para la inspección remota de malware

August 20, 2021

El dispositivo Citrix ADC actúa como un proxy e intercepta todo el tráfico del cliente. El dispositivo utiliza directivas para evaluar el tráfico y reenvía las solicitudes de cliente al servidor de origen en el que reside el recurso. El dispositivo descifra la respuesta del servidor de origen y reenvía el contenido de texto sin formato al servidor ICAP para una comprobación antimalware. El servidor ICAP responde con un mensaje que indica "No se requiere adaptación", error o solicitud modificada. Dependiendo de la respuesta del servidor ICAP, el contenido solicitado se reenvía al cliente o se envía un mensaje apropiado.

Para este caso de uso, debe realizar alguna configuración general, configuración relacionada con proxy e intercepción SSL y configuración ICAP en el dispositivo Citrix ADC.

Configuración general

Configure las siguientes entidades:

- Dirección NSIP
- Dirección IP de subred (SNIP)
- Servidor de nombres DNS
- Par de claves de certificado de CA para firmar el certificado de servidor para la intercepción SSL

Configuración de servidor proxy e intercepción SSL

Configure las siguientes entidades:

- Servidor proxy en modo explícito para interceptar todo el tráfico HTTP y HTTPS saliente.
- Perfil SSL para definir la configuración SSL, como cifrados y parámetros, para las conexiones.
- Directiva SSL para definir reglas para interceptar tráfico. Establezca en true para interceptar todas las solicitudes del cliente.

Para obtener más información, consulte los siguientes temas:

- Modos de proxy
- Intercepción SSL

En la siguiente configuración de ejemplo, el servicio de detección de antimalware reside en `www.example.com`.

Ejemplo de configuración general:


```
add dns nameServer 203.0.113.2

add ssl certKey ns-swg-ca-certkey -cert ns_swg_ca.crt -key ns_swg_ca.
    key
<!--NeedCopy-->
```

Ejemplo de configuración de intercepción SSL y servidor proxy:

```
add cs vserver explicitswg PROXY 192.0.2.100 80  - Authn401 ENABLED  -
    authnVsName explicit-auth-vs

set ssl parameter -defaultProfile ENABLED

add ssl profile swg_profile -sslInterception ENABLED

bind ssl profile swg_profile -ssliCACertkey ns-swg-ca-certkey

set ssl vserver explicitswg -sslProfile swg_profile

add ssl policy ssli-pol_ssli -rule true -action INTERCEPT

bind ssl vserver explicitswg -policyName ssli-pol_ssli -priority 100 -
    type INTERCEPT_REQ
<!--NeedCopy-->
```

Ejemplo de configuración ICAP:

```
add service icap_svc 203.0.113.225 TCP 1344

enable ns feature contentinspection

add icapprofile icapprofile1 -uri /example.com -Mode RESMOD

add contentInspection action CiRemoteAction -type ICAP -serverName
    icap_svc -icapProfileName icapprofile1

add contentInspection policy CiPolicy -rule "HTTP.REQ.METHOD.NE("
    CONNECT")" -action CiRemoteAction

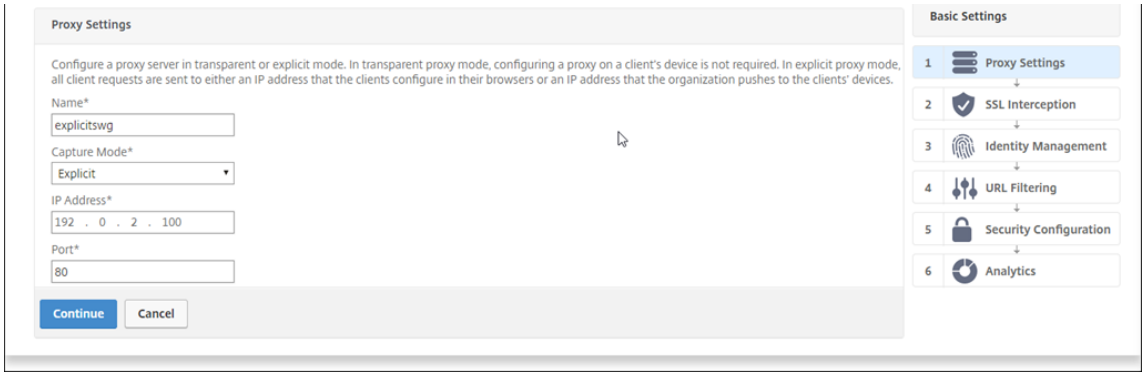
bind cs vserver explicitswg -policyName  CiPolicy -priority 200 -type
    response
```



```
12 <!--NeedCopy-->
```

Configurar la configuración del proxy

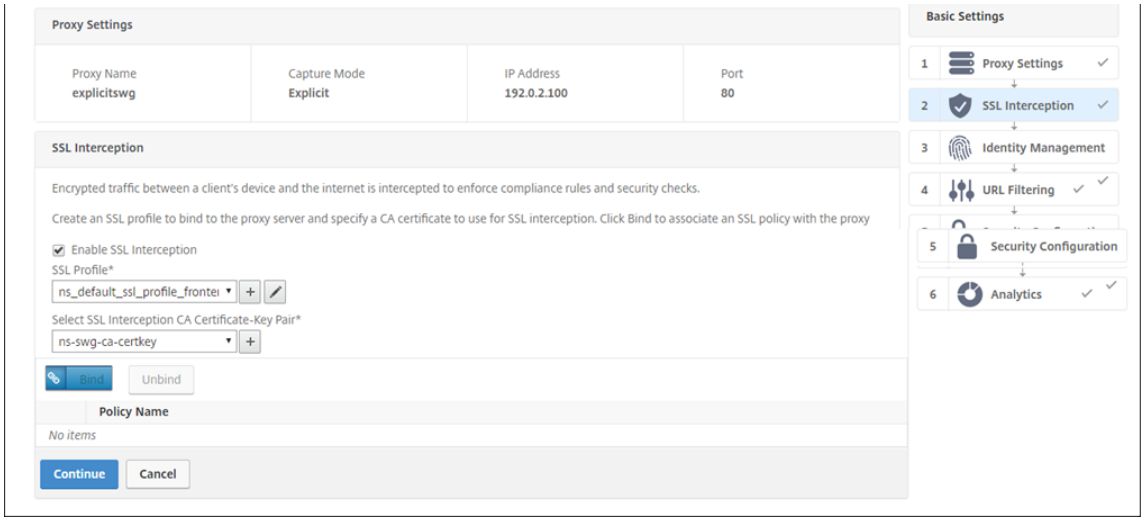
1. Vaya a **Seguridad** > **Proxy de reenvío SSL> Asistente de proxy** de reenvío SSL.
2. Haga clic en **Comenzar** y, a continuación, haga clic en **Continuar**.
3. En el cuadro de diálogo **Configuración de proxy**, escriba un nombre para el servidor proxy explícito.
4. En **Modo de captura,** seleccione **Explícito**.
5. Introduzca una dirección IP y un número de puerto.



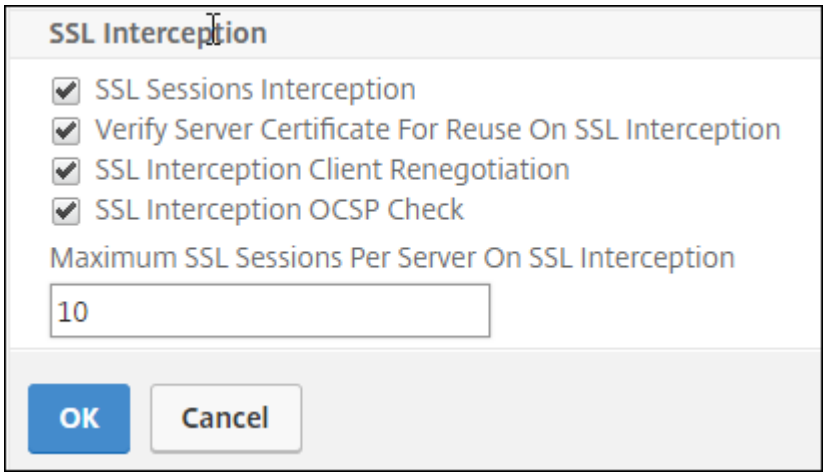
6. Haga clic en **Continuar**.

Configurar la configuración de intercepción SSL

1. Seleccione **Activar intercepción SSL**.

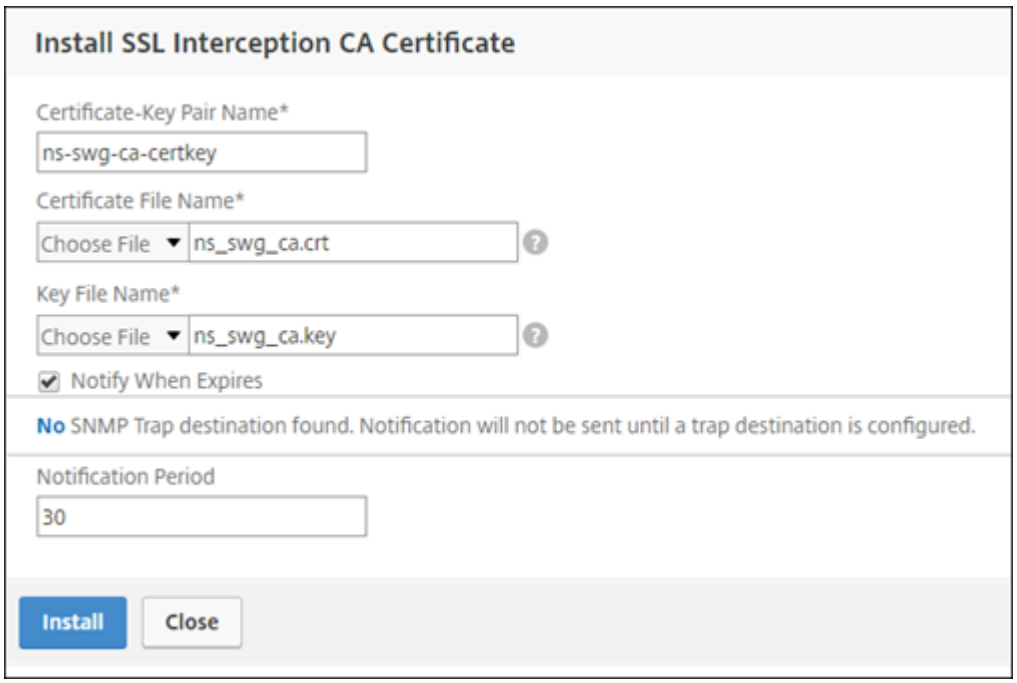


2. En **Perfil SSL**, seleccione un perfil existente o haga clic en "+" para agregar un nuevo perfil SSL front-end. Habilite la **intercepción de sesiones SSL** en este perfil. Si selecciona un perfil existente, omita el siguiente paso.



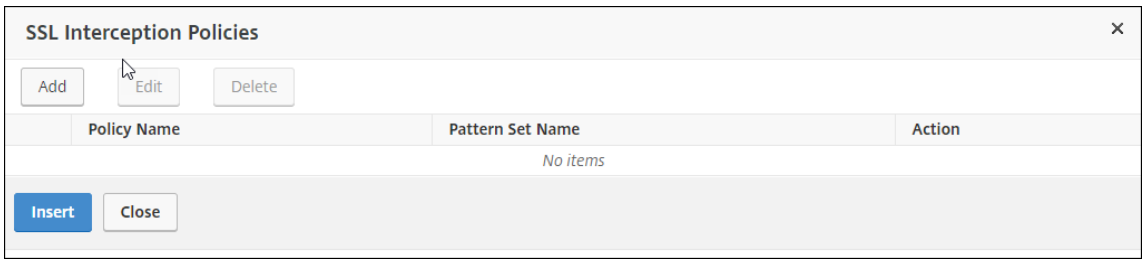
3. Haga clic en **Aceptar** y, a continuación, haga clic en **Listo**.

4. En **Seleccionar par de claves de certificado de CA de interceptación SSL**, seleccione un certificado existente o haga clic en "+" para instalar un par de claves de certificado de CA para la interceptación de SSL. Si selecciona un certificado existente, omita el siguiente paso.

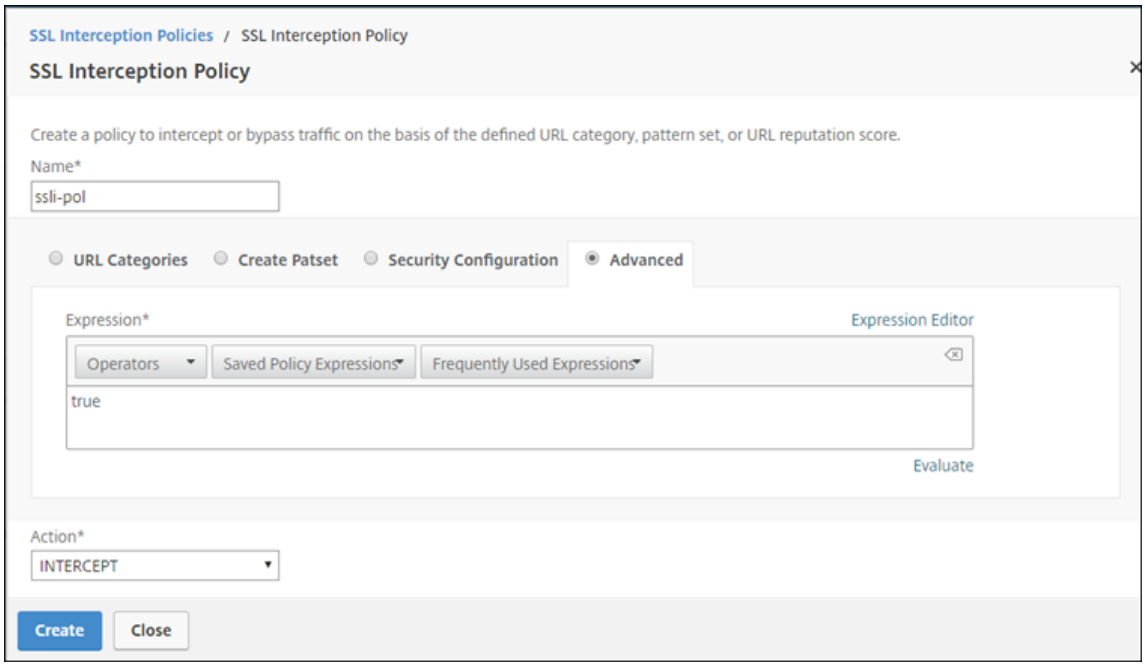


5. Haga clic en **Instalar** y, a continuación, haga clic en **Cerrar**.

6. Agregue una directiva para interceptar todo el tráfico. Haga clic en **Vincular**. Haga clic en **Agregar** para agregar una nueva directiva o seleccione una existente. Si selecciona una directiva existente, haga clic en **Insertar** y omita los tres pasos siguientes.



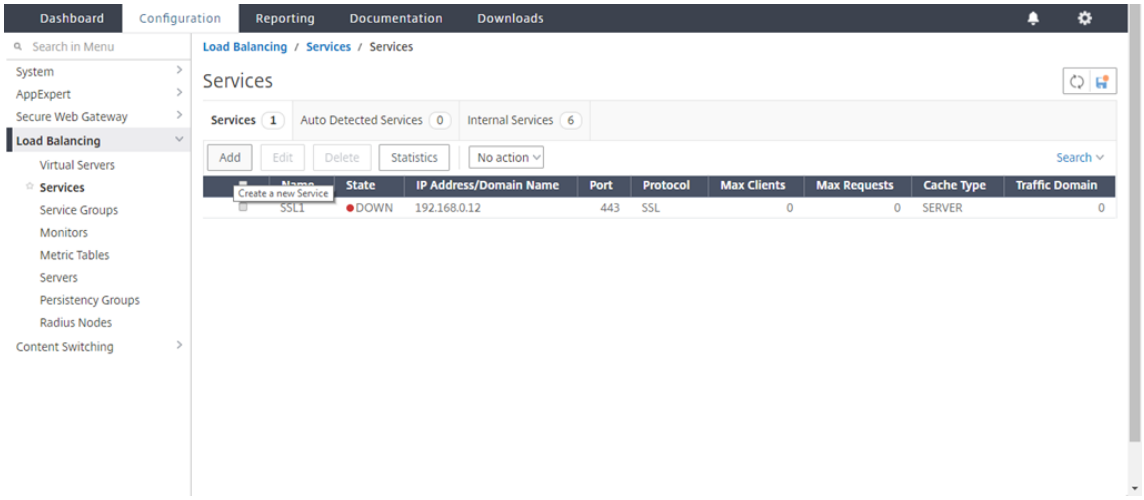
7. Escriba un nombre para la directiva y seleccione **Avanzadas**. En el editor de expresiones, escriba true.
8. En **Acción**, seleccione **INTERCEPCIÓN**.



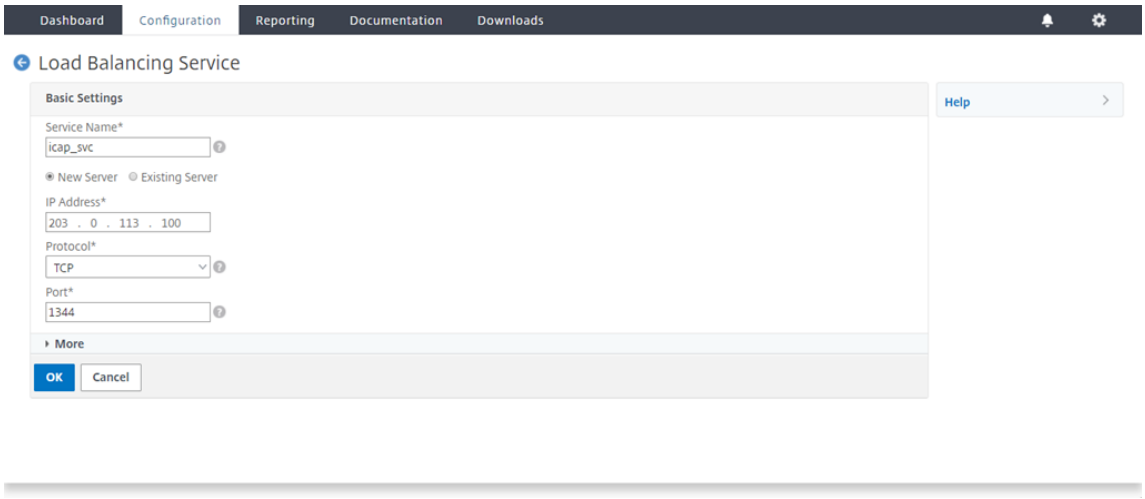
9. Haga clic en **Crear**.
10. Haga clic en **Continuar** cuatro veces y, a continuación, haga clic en **Listo**.

Configurar la configuración de ICAP

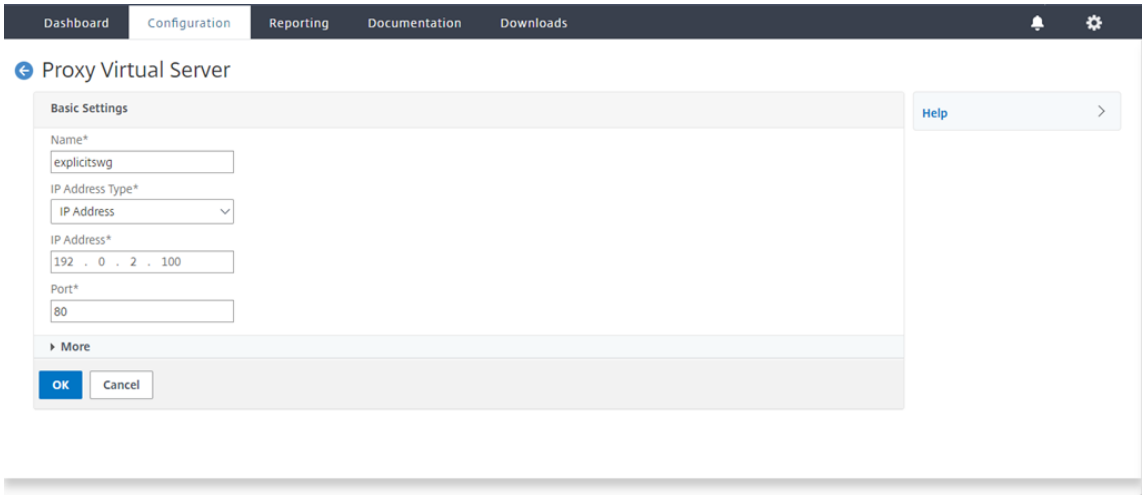
1. Desplácese hasta **Equilibrio de carga** > **Servicios** y haga clic en **Agregar**.



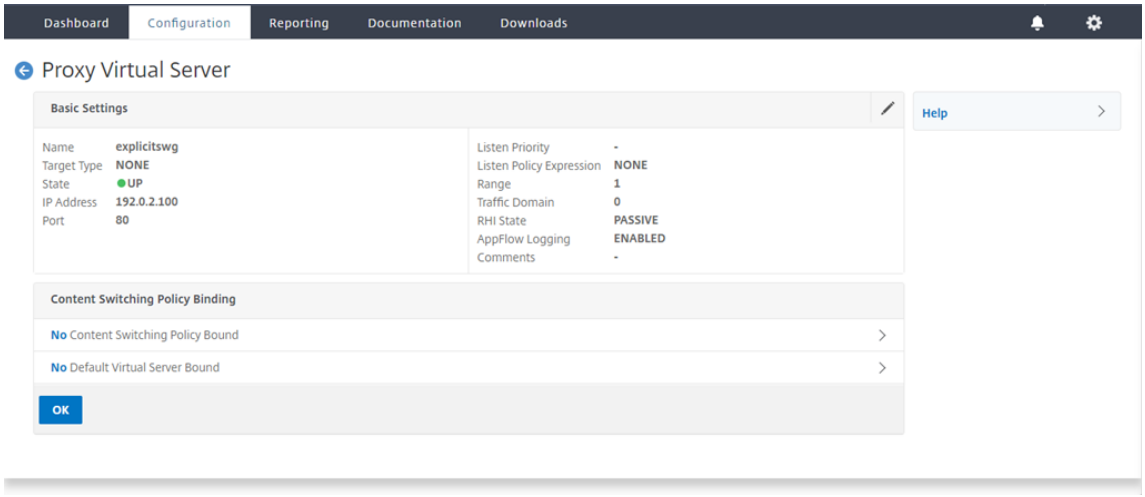
2. Escriba un nombre y una dirección IP. En **Protocolo**, seleccione **TCP**. En **Puerto**, escriba **1344**. Haga clic en **Aceptar**.



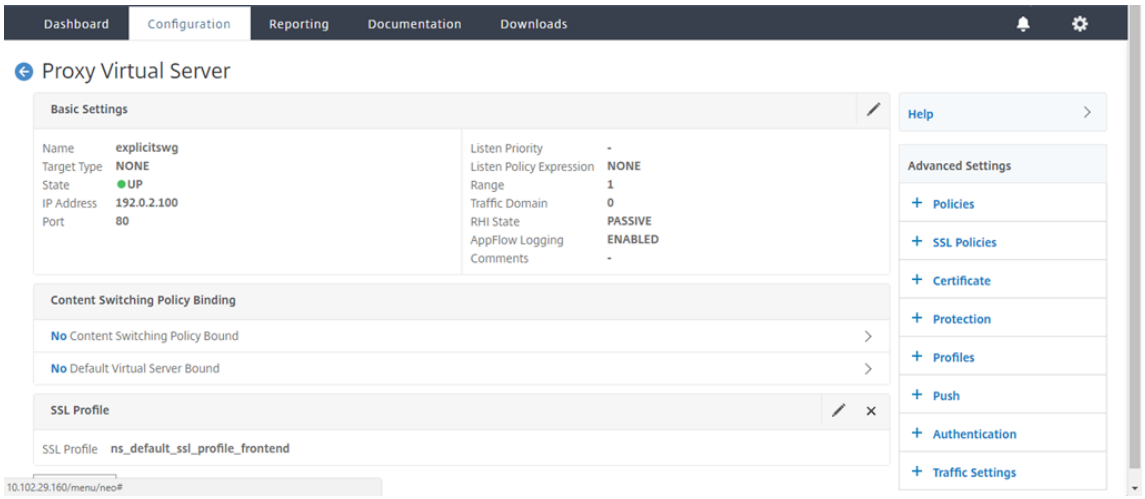
3. Desplácese hasta **Proxy de reenvío SSL** > **Servidores virtuales proxy**. Agregue un servidor virtual proxy o seleccione un servidor virtual y haga clic en **Modificar**. Después de introducir los detalles, haga clic en **Aceptar**.



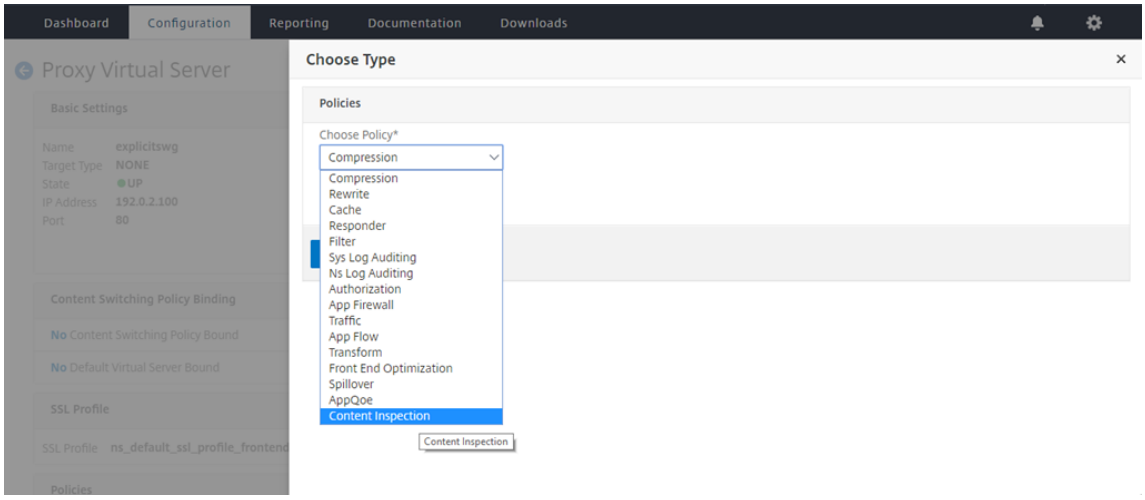
Vuelva a hacer clic en **Aceptar**.



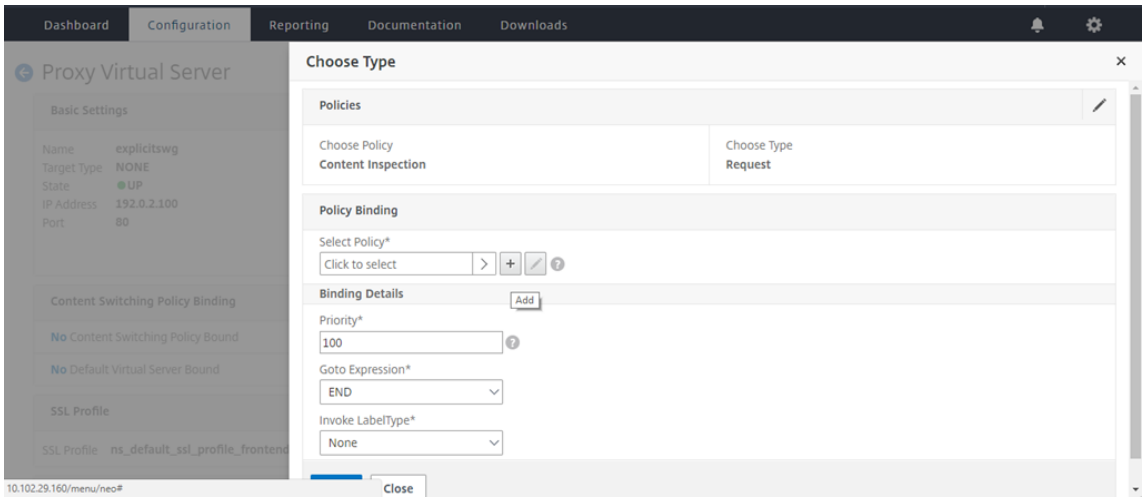
4. En **Configuración avanzada**, haga clic en **Directivas**.



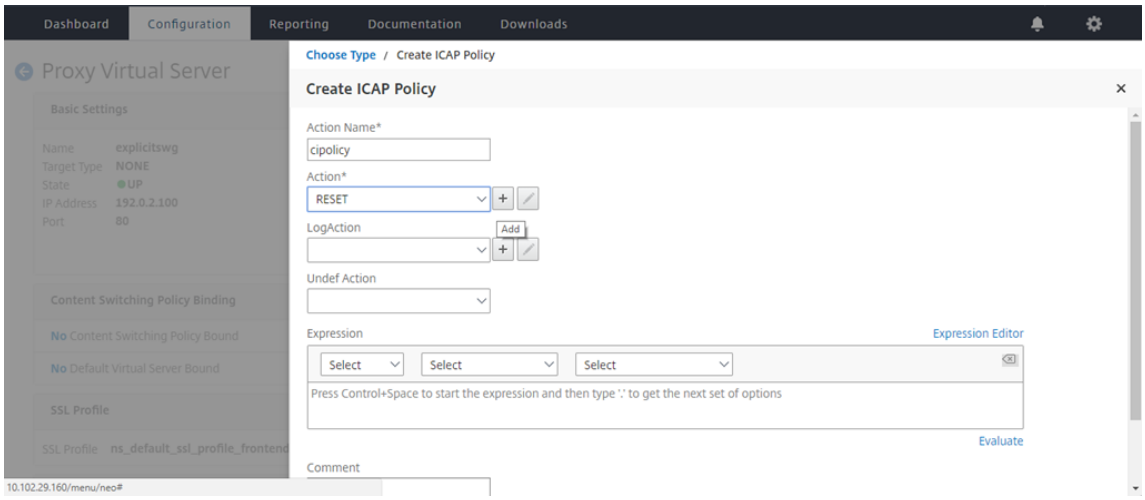
5. En **Elegir directiva**, seleccione **Inspección de contenido**. Haga clic en **Continuar**.



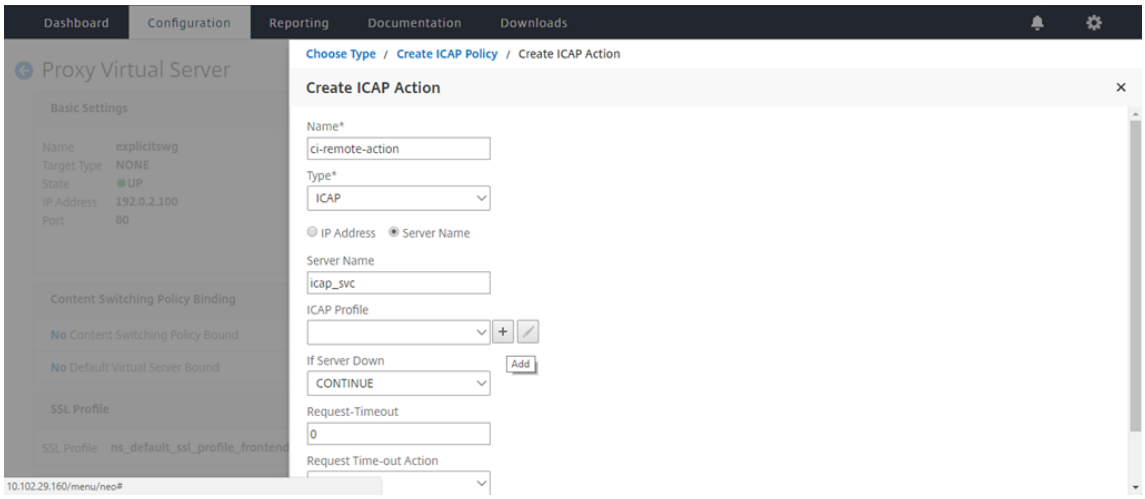
6. En **Seleccionar directiva**, haga clic en el signo “+” para agregar una directiva.



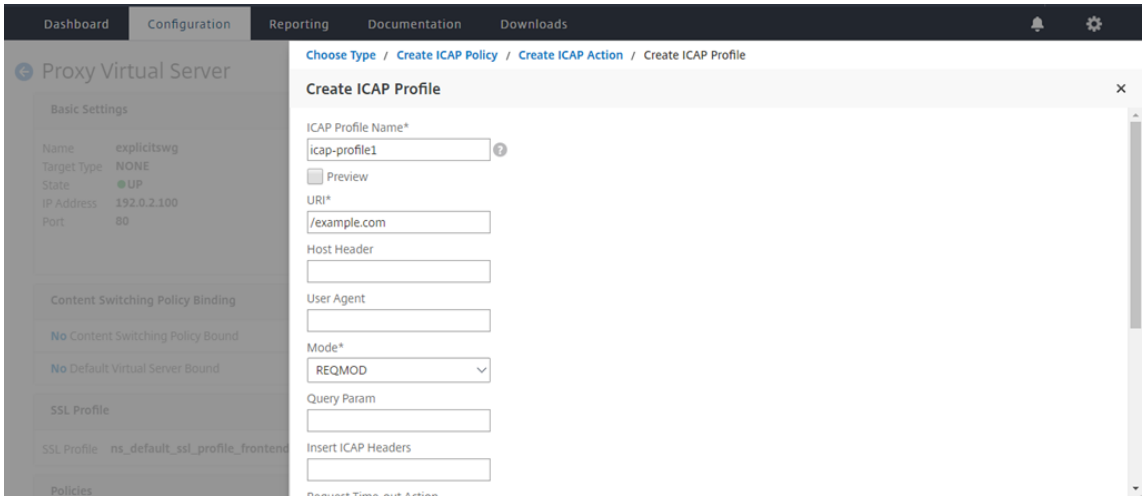
7. Introduzca un nombre para la directiva. En **Acción**, haga clic en el signo “+” para agregar una acción.



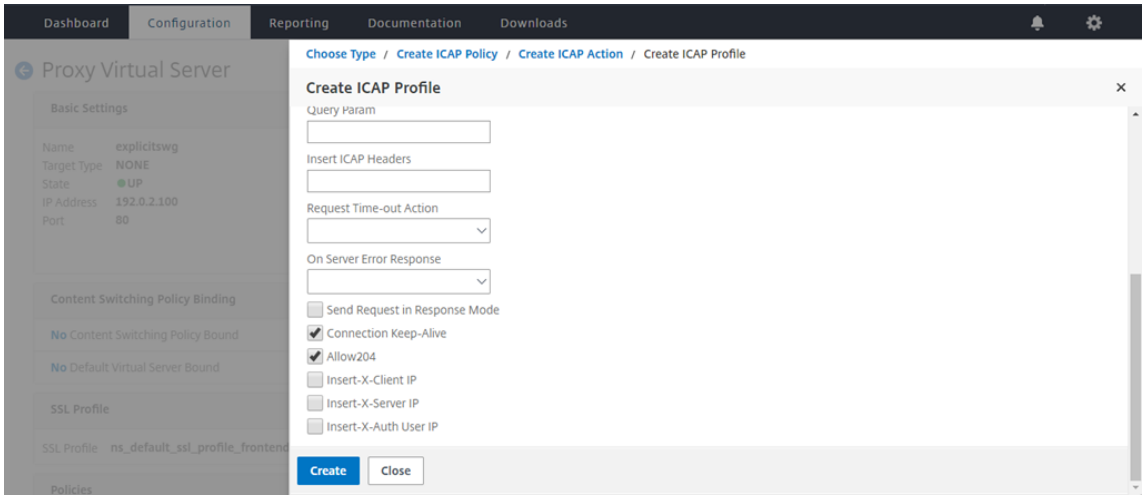
8. Escriba un nombre para la acción. En **Nombre del servidor**, escriba el nombre del servicio TCP creado anteriormente. En **Perfil ICAP**, haga clic en el signo "+" para agregar un perfil ICAP.



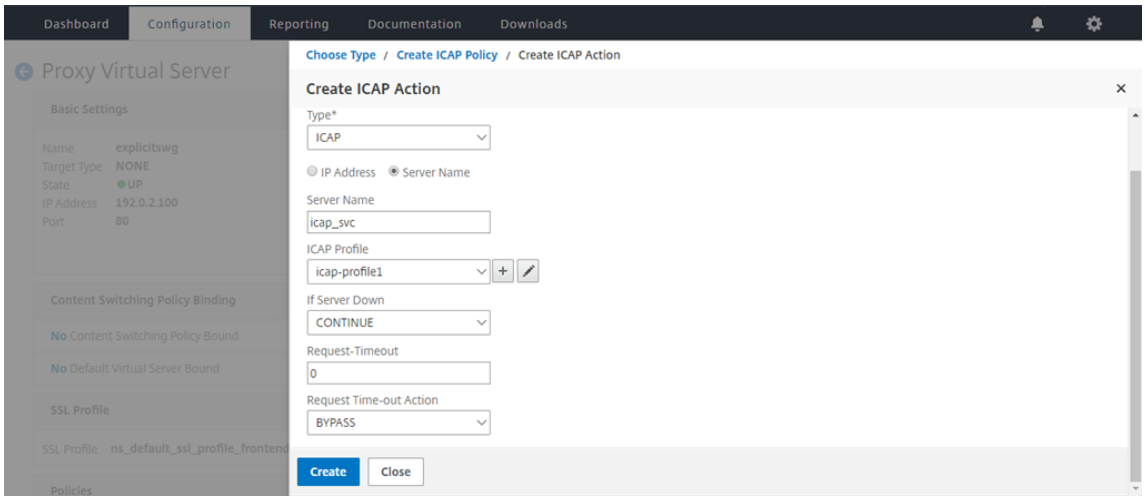
9. Escriba un nombre de perfil, URI. En **Modo**, seleccione **REQMOD**.



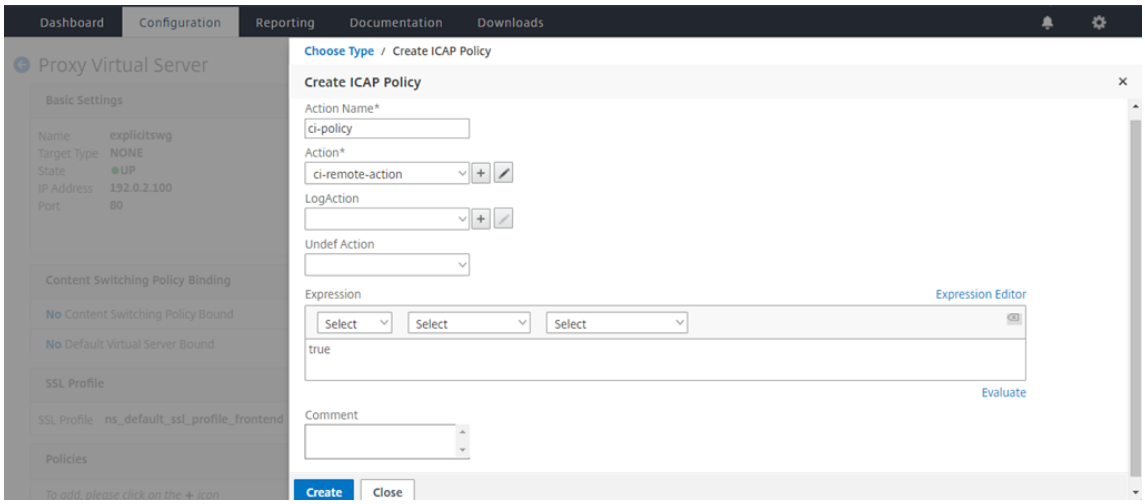
10. Haga clic en **Crear**.



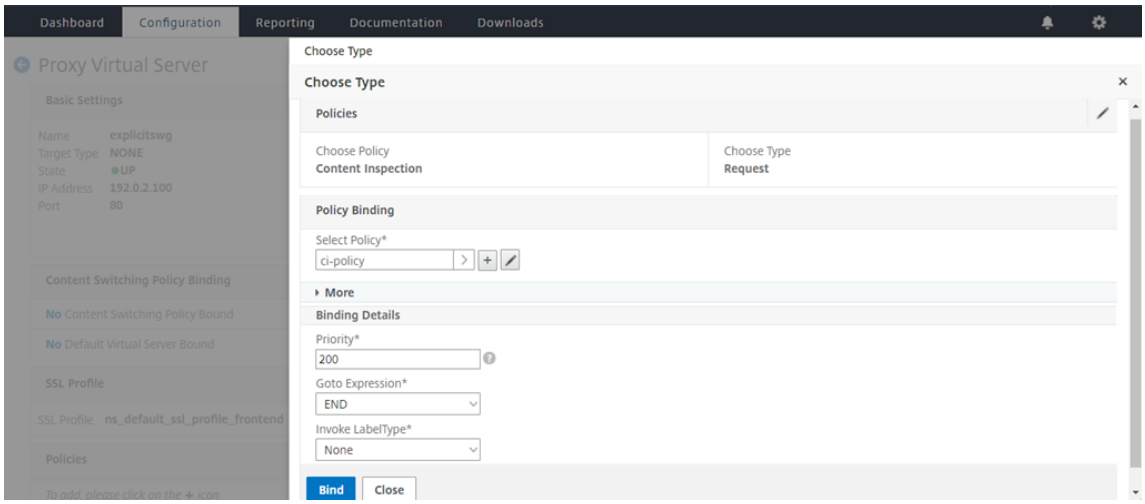
11. En la página **Crear acción ICAP**, haga clic en **Crear**.



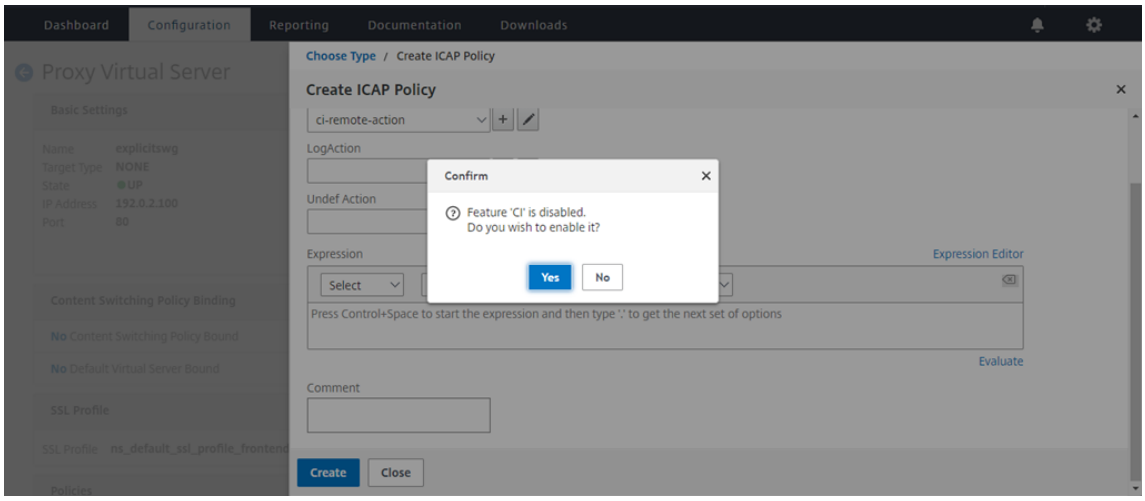
12. En la página **Crear directiva ICAP**, escriba true en el **Editor de expresiones**. A continuación, haga clic en **Crear**.



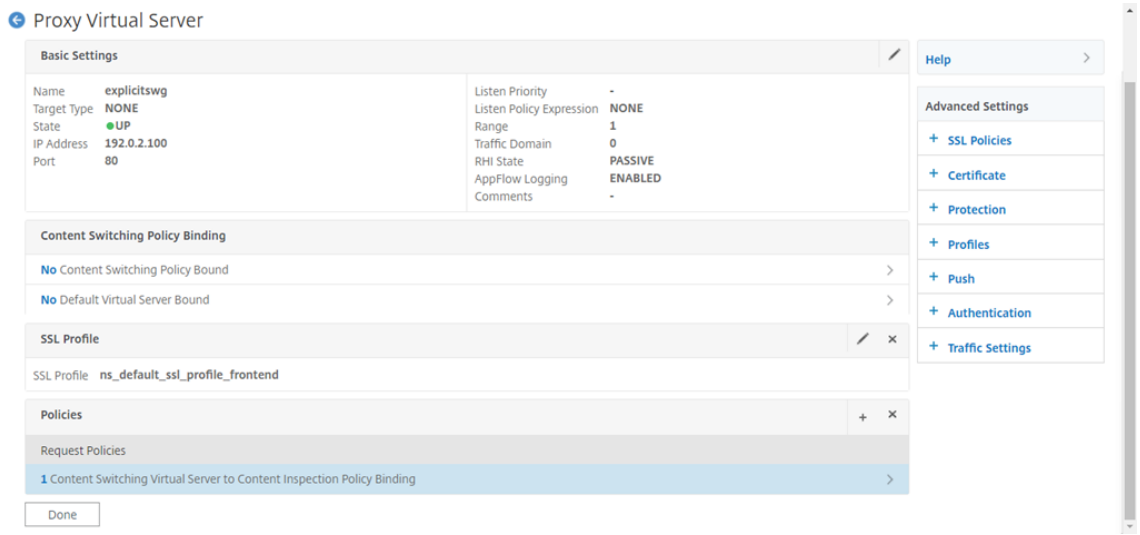
13. Haga clic en **Vincular**.



14. Cuando se le pida que active la función de inspección de contenido, seleccione **Sí**.



15. Haga clic en **Done**.



Transacciones ICAP de ejemplo entre el dispositivo Citrix ADC y el servidor ICAP en RESPMOD

Solicitud del dispositivo Citrix ADC al servidor ICAP:

```
RESPMOD icap://10.106.137.15:1344/resp ICAP/1.0

Host: 10.106.137.15

Connection: Keep-Alive

Encapsulated: res-hdr=0, res-body=282

HTTP/1.1 200 OK

Date: Fri, 01 Dec 2017 11:55:18 GMT

Server: Apache/2.2.21 (Fedora)

Last-Modified: Fri, 01 Dec 2017 11:16:16 GMT

ETag: ”20169-45-55f457f42aee4”

Accept-Ranges: bytes

Content-Length: 69

Keep-Alive: timeout=15, max=100
```



```
24
25 Content-Type: text/plain; charset=UTF-8
26
27 X5O!P%@AP[4PZX54(P^)7CC)7 }
28  $EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
29 <!--NeedCopy-->
```

Respuesta del servidor ICAP al dispositivo Citrix ADC:

```
1  ICAP/1.0 200 OK
2
3  Connection: keep-alive
4
5  Date: Fri, 01 Dec, 2017 11:40:42 GMT
6
7  Encapsulated: res-hdr=0, res-body=224
8
9  Server: IWSVA 6.5-SP1_Build_Linux_1080 $Date: 04/09/2015 01:19:26 AM$
10
11 ISTag: ”9.8-13.815.00-3.100.1027-1.0”
12
13 X-Virus-ID: Eicar_test_file
14
15 X-Infection-Found: Type=0; Resolution=2; Threat=Eicar_test_file;
16
17 HTTP/1.1 403 Forbidden
18
19 Date: Fri, 01 Dec, 2017 11:40:42 GMT
20
21 Cache-Control: no-cache
22
23 Content-Type: text/html; charset=UTF-8
24
25 Server: IWSVA 6.5-SP1_Build_Linux_1080 $Date: 04/09/2015 01:19:26 AM$
26
27 Content-Length: 5688
28
29 <html><head><META HTTP-EQUIV=”Content-Type” CONTENT=”text/html; charset
      =UTF-8”/>
30
31 …
32
33 …
```



```
34
35 </body></html>
36 <!--NeedCopy-->
```

Artículos de procedimientos

January 19, 2021

A continuación se presentan algunas instrucciones de configuración o casos de uso funcionales disponibles como artículos “Cómo” para ayudarle a administrar su implementación de proxy de reenvío SSL.

Filtrado de URL

Cómo crear una directiva de categorización de URL

Cómo crear una directiva de lista de direcciones URL

Cómo permitir una URL excepcional

Cómo bloquear sitios web de categorías de adultos

Seguridad

January 12, 2021

Los temas siguientes tratan la información de configuración e instalación de las funciones de seguridad de Citrix ADC. La mayoría de estas funciones se basan en directivas.

Filtrado de contenido	Bloquea las solicitudes HTML inapropiadas, evitando que las solicitudes lleguen a los servidores web.
Protección contra picos de tensión	Detecta cualquier aumento rápido en los intentos de conexión y ajusta la velocidad a la que se permite que las conexiones procedan al servidor, evitando la sobrecarga del servidor.

Opciones de seguridad DNS	Asistente de interfaz de usuario simplificado para crear directivas que protejan contra ataques DNS.

Protección contra picos de tensión

January 21, 2022

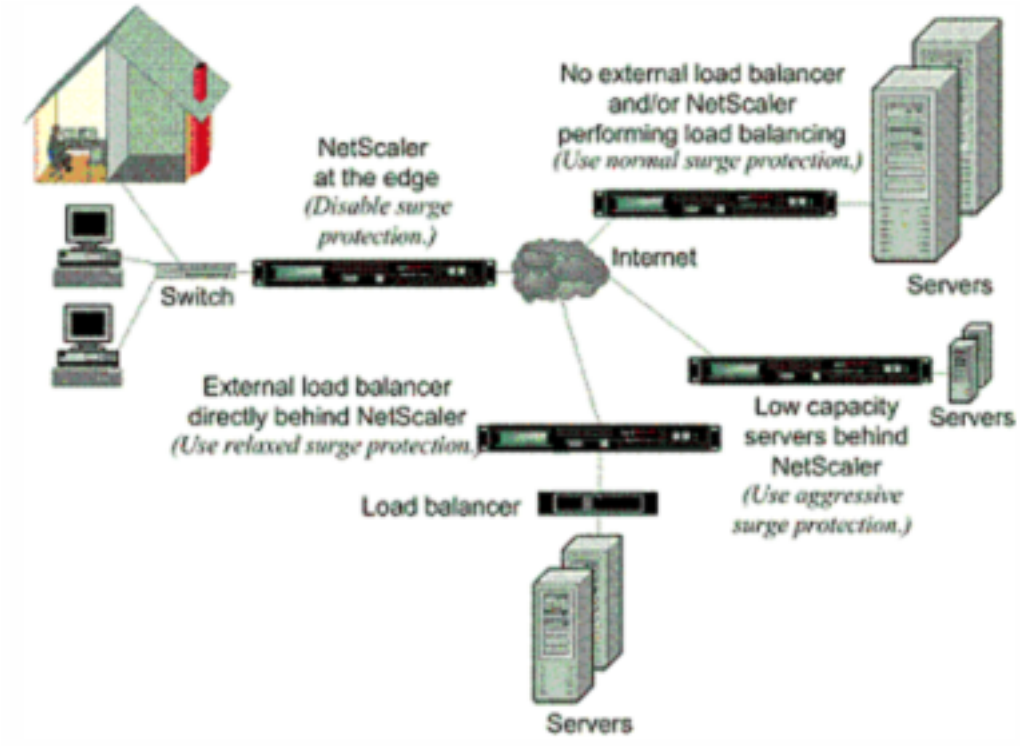
Cuando un aumento en las solicitudes de los clientes sobrecarga un servidor, la respuesta del servidor se vuelve lenta y el servidor no puede responder a las nuevas solicitudes. La función de protección contra sobretensiones garantiza que las conexiones al servidor se realicen a una velocidad que el servidor pueda manejar. La velocidad de respuesta depende de cómo se configure la protección contra sobretensiones. El dispositivo Citrix ADC también realiza un seguimiento de la cantidad de conexiones al servidor y utiliza esa información para ajustar la velocidad a la que abre nuevas conexiones del servidor.

La protección contra sobretensiones está habilitada de forma predeterminada. Si no quiere utilizar protección contra sobretensiones, como ocurre con algunas configuraciones especiales, debe desactivarla.

La configuración predeterminada de protección contra sobretensiones es suficiente para la mayoría de los usos, pero puede configurar la protección contra sobretensiones para ajustarla a sus necesidades. En primer lugar, puede establecer el valor del acelerador para indicarle la agresividad de administrar los intentos de conexión. En segundo lugar, puede establecer el valor umbral base para controlar el número máximo de conexiones simultáneas que permite el dispositivo Citrix ADC antes de activar la protección contra sobretensiones. (El valor del umbral base predeterminado se establece mediante el valor del acelerador, pero después de establecer el valor del acelerador puede cambiarlo a cualquier número que quiera.)

En la siguiente ilustración se ilustra cómo se configura la protección contra sobretensiones para gestionar el tráfico hacia un sitio web.

Ilustración 1. Una ilustración funcional de Citrix ADC Surge Protection



Nota

Si el dispositivo Citrix ADC está instalado en el borde de la red, donde interactúa con los dispositivos de red del lado cliente de Internet, debe inhabilitarse la función de protección contra sobretensiones. La protección contra sobretensiones también debe desactivarse si habilita el modo USIP (Using Source IP) en el dispositivo.

El siguiente ejemplo e ilustración muestran las tasas de solicitudes y respuestas para dos casos. En un caso, la protección contra sobretensiones está desactivada y, en el otro, está habilitada.

Cuando se inhabilita la protección contra sobretensiones y se produce un aumento en las solicitudes, el servidor acepta tantas solicitudes como pueda procesar al mismo tiempo y, a continuación, comienza a descartar solicitudes. A medida que el servidor se sobrecarga más, disminuye y la tasa de respuesta se reduce a cero. Cuando el servidor se recupera del fallo, varios minutos después, envía restablecimientos para todas las solicitudes pendientes, lo que es un comportamiento anormal, y también responde a nuevas solicitudes con restablecimientos. El proceso se repite para cada aumento de solicitudes. Por lo tanto, un servidor que esté bajo un ataque DDoS y reciba múltiples oleadas de solicitudes puede dejar de estar disponible para los usuarios legítimos.

Cuando la protección contra sobretensiones está habilitada y se produce un aumento en las solicitudes, la protección contra sobretensiones administra la tasa de solicitudes al servidor y envía solicitudes al servidor solo con la rapidez con la que el servidor puede gestionar esas solicitudes. Esto permite que el servidor responda a cada solicitud correctamente en el orden en que se recibió. Cuando termina el aumento, las solicitudes atrasadas se borran tan rápido como el servidor puede

gestionarlas, hasta que la tasa de solicitudes coincida con la tasa de respuesta.

Inhabilitar y volver a habilitar la protección contra sobre

October 5, 2021

La función de protección contra sobretensiones está activada de forma predeterminada. Cuando la protección contra sobretensiones está activada, está activa para cualquier servicio que agregue.

Inhabilitar o volver a activar la protección contra sobretensiones mediante la CLI

En el símbolo del sistema, escriba uno de los siguientes conjuntos de comandos para inhabilitar o volver a activar la protección contra sobretensiones y compruebe la configuración:

```
- disable ns feature SurgeProtection
- show ns feature
- enable ns feature SurgeProtection
- show ns feature
<!--NeedCopy-->
```

Ejemplo:

```
disable ns feature SurgeProtection
 Done show ns feature

        Feature                         Acronym             Status
        -------                         -------             ------
 1)     Web Logging                     WL                  ON
 2)     Surge Protection                SP                  OFF
 .
 .
 .
 24)    Citrix ADC Push                  push               OFF
 Done
<!--NeedCopy-->
```

```
 enable ns feature SurgeProtection
 Done
```



```
> show ns feature

        Feature                         Acronym             Status
        -------                         -------             ------
 1)     Web Logging                     WL                  ON
 2)     Surge Protection                SP                  ON
 .
 .
 .

 24)    Citrix ADC Push                  push                OFF
 Done
>
<!--NeedCopy-->
```

Inhabilitar o volver a activar la protección contra sobretensiones mediante la GUI

1. En el panel de navegación, expanda **Sistema**y, a continuación, seleccione **Configuración**.
2. En el panel de detalles, haga clic en **Cambiar funciones avanzadas**.
3. En el cuadro de diálogo **Configurar funciones avanzadas**, desactive la selección de la casilla **Protección contra sobretensiones** para inhabilitar la función de protección contra sobretensiones o active la casilla de verificación para habilitar la función.
4. Haga clic en **OK**.
5. En el cuadro de diálogo Habilitar/inhabilitar funciones, haga clic en Sí. Aparece un mensaje en la barra de estado que indica que la función se ha habilitado o inhabilitado.

Inhabilitar o volver a activar la protección contra sobretensiones para un servicio concreto mediante la interfaz gráfica de usuario

1. Vaya a **Traffic Management -> Load Balancing -> Services**. La lista de servicios configurados se muestra en el panel de detalles.
2. En el panel de detalles, seleccione el servicio para el que quiere inhabilitar o volver a activar la función de protección contra sobretensiones y, a continuación, haga clic en **Abrir**.
3. En el cuadro de diálogo **Configurar servicio**, haga clic en la **ficha Opciones avanzadas**y desplácese hacia abajo.
4. En el marco Otros, desactive la selección de la casilla de verificación **Protección contra sobretensiones** para desactivar la función de protección contra sobretensiones o seleccione la casilla de verificación para habilitar la función.
5. Haga clic en **OK**. Aparece un mensaje en la barra de estado que indica que la función se ha habilitado o inhabilitado.

Nota: La protección contra sobretensiones solo funciona cuando tanto la función como la configuración de servicio están activadas.

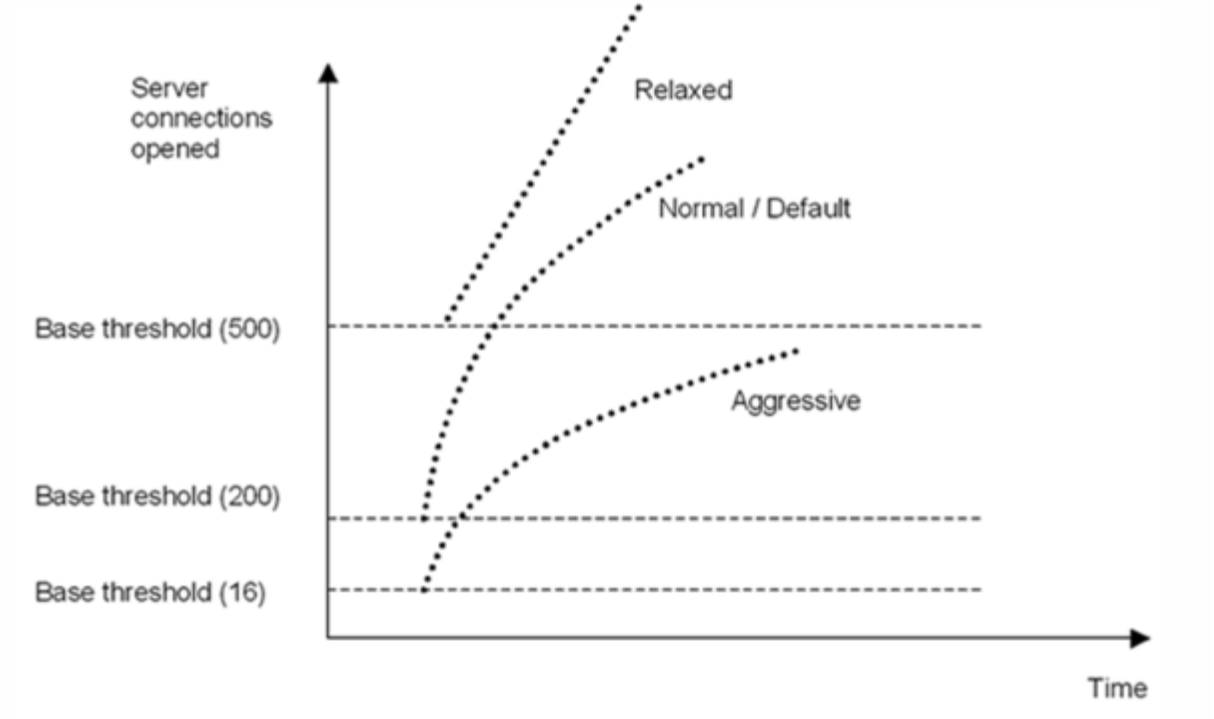
Establecer umbrales para la protección contra sobretensiones

August 20, 2021

Para establecer la velocidad a la que el dispositivo Citrix ADC abre conexiones al servidor, debe configurar los valores de umbral y aceleración para la protección contra sobretensiones.

La siguiente ilustración muestra las curvas de protección contra sobretensiones que resultan de ajustar la velocidad del acelerador a relajada, normal o agresiva. Dependiendo de la configuración de la capacidad del servidor, puede establecer valores de umbral base para generar curvas de protección contra sobretensiones adecuadas.

Ilustración 1. Curvas de protección contra sobretensiones



Los ajustes de configuración afectan al comportamiento de la protección contra sobretensiones de la siguiente manera:

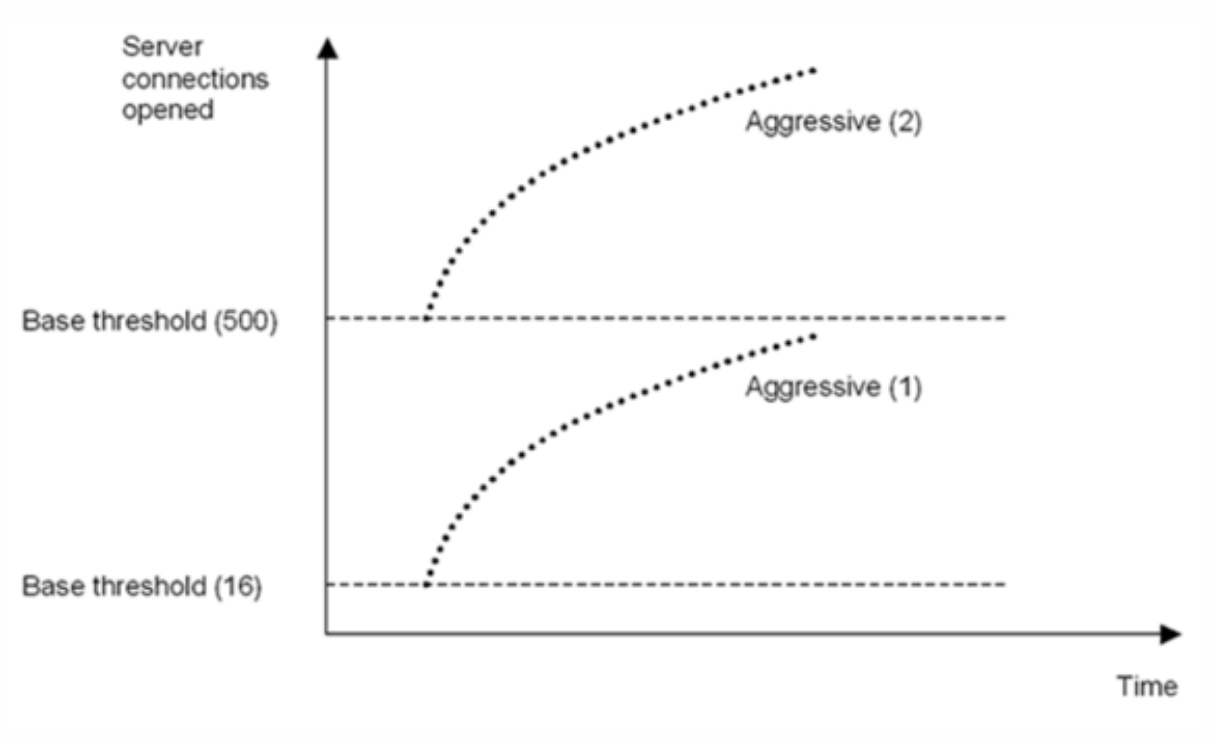
- Si no especifica una velocidad de aceleración, se establece en normal (el valor predeterminado) y el umbral base se establece en 200, como se muestra en la ilustración anterior.
- Si especifica una velocidad de aceleración (agresiva, normal o relajada) sin especificar un umbral base, la curva refleja los valores por defecto del umbral base para esa velocidad de acel-

eración. Por ejemplo, si establece la velocidad del acelerador en relajada, la curva resultante tendrá el valor umbral base de 500.

- Si solo especifica el umbral base, toda la curva de protección contra sobretensiones se desplaza hacia arriba o hacia abajo, dependiendo del valor especificado, como se muestra en la ilustración siguiente.
- Si especifica un umbral base y una velocidad de aceleración, la curva de protección contra sobretensiones resultante se basa en la velocidad de aceleración establecida y se ajusta de acuerdo con el valor establecido para el umbral base.

En la siguiente ilustración, la curva inferior (Agresivo 1) resulta cuando la velocidad del acelerador se establece en agresiva pero el umbral base no está establecido. La curva superior (Agresivo 2) resulta cuando el umbral base está establecido en 500, pero la velocidad del acelerador no está establecida. La segunda curva superior (Agresiva 2) también resulta cuando el umbral base se establece en 500 y la velocidad del acelerador se establece en agresiva.

Ilustración 2. Tasa agresiva con el valor predeterminado o un umbral base establecido



Establezca el umbral para la protección contra sobretensiones mediante la interfaz gráfica de usuario

1. En el panel de navegación, expanda Sistema y, a continuación, seleccione Configuración.
2. En el panel de detalles, haga clic en Configuración global del sistema.

3. Si quiere establecer un umbral base diferente del predeterminado para la velocidad de aceleración, en el cuadro de diálogo Configurar configuración global, umbral base, escriba el número máximo de conexiones simultáneas de servidor permitidas antes de que se active la protección contra sobretensiones. El umbral base es el número máximo de conexiones de servidor que se pueden abrir antes de activar la protección contra sobretensiones. El valor máximo para esta configuración es 32.767 conexiones de servidor. La configuración predeterminada para este valor se controla mediante la velocidad de aceleración que elija en el siguiente paso.

   Nota: Si no establece un valor explícito aquí, se utilizará el valor predeterminado.

4. En la lista desplegable Acelerador, seleccione una velocidad de aceleración. El acelerador es la velocidad a la que el dispositivo Citrix ADC permite abrir las conexiones con el servidor. El acelerador se puede ajustar a los siguientes valores:

   - **Agresivo:** elija esta opción cuando la capacidad de manejo de conexiones y manejo de sobretensiones del servidor sea baja y la conexión deba administrarse cuidadosamente. Cuando se establece el acelerador en agresivo, el umbral base se establece en un valor predeterminado de 16, lo que significa que la protección contra sobretensiones se activa siempre que haya 17 o más conexiones simultáneas con el servidor.
   - **Normal:** elija esta opción cuando no haya un equilibrador de carga externo detrás del dispositivo Citrix ADC o en el proceso descendente. El umbral base se establece en un valor de 200, lo que significa que la protección contra sobretensiones se activa siempre que haya 201 o más conexiones simultáneas al servidor. Normal es la opción predeterminada del acelerador.
   - **Relajado:** Elija esta opción cuando el dispositivo Citrix ADC esté realizando un equilibrio de carga entre un gran número de servidores web y, por lo tanto, pueda manejar un gran número de conexiones simultáneas. El umbral base se establece en un valor de 500, lo que significa que la protección contra sobretensiones se activa solo cuando hay 501 o más conexiones simultáneas al servidor.

5. Haga clic en Aceptar. Aparece un mensaje en la barra de estado que indica que la configuración global está configurada.

Vacíe la cola de sobretensiones

August 20, 2021

Cuando un servidor físico recibe un aumento de solicitudes, se vuelve lento para responder a los clientes que están conectados actualmente a él, lo que deja a los usuarios insatisfechos y descontentos. A menudo, la sobrecarga también hace que los clientes reciban páginas de error. Para evitar

tales sobrecargas, el dispositivo Citrix ADC proporciona funciones como la protección contra sobretensiones, que controla la velocidad a la que se pueden establecer nuevas conexiones a un servicio.

El dispositivo realiza multiplexación de conexión entre clientes y servidores físicos. Cuando recibe una solicitud de cliente para acceder a un servicio en un servidor, el dispositivo busca una conexión ya establecida con el servidor que sea gratuita. Si encuentra una conexión libre, utiliza esa conexión para establecer un vínculo virtual entre el cliente y el servidor. Si no encuentra una conexión gratuita existente, el dispositivo establece una nueva conexión con el servidor y establece un enlace virtual entre un cliente y el servidor. Sin embargo, si el dispositivo no puede establecer una nueva conexión con el servidor, envía la solicitud del cliente a una cola de sobretensiones. Si todos los servidores físicos vinculados al servidor virtual de equilibrio de carga o de cambio de contenido alcanzan el límite superior de las conexiones de cliente (valor máximo del cliente, umbral de protección contra sobretensiones o capacidad máxima del servicio), el dispositivo no podrá establecer una conexión con ningún servidor. La función de protección contra sobretensiones utiliza la cola de sobretensiones para regular la velocidad a la que se abren las conexiones con los servidores físicos. El dispositivo mantiene una cola de sobretensión diferente para cada servicio vinculado al servidor virtual.

La longitud de una cola de sobretensiones aumenta cada vez que llega una solicitud para la que el dispositivo no puede establecer una conexión, y la longitud disminuye cada vez que se envía una solicitud de la cola al servidor o se agana el tiempo de espera de una solicitud y se elimina de la cola.

Si la cola de sobretensión de un servicio o grupo de servicios se vuelve demasiado larga, es posible que quiera vaciarla. Puede vaciar la cola de sobretensiones de un servicio o grupo de servicios específico, o de todos los servicios y grupos de servicios vinculados a un servidor virtual de equilibrio de carga. El vaciado de una cola de sobretensión no afecta a las conexiones existentes. Solo se eliminan las solicitudes presentes en la cola de sobretensiones. Para esas solicitudes, el cliente tiene que hacer una nueva solicitud.

También puede vaciar la cola de sobretensiones de un servidor virtual de cambio de contenido. Si un servidor virtual de cambio de contenido reenvía algunas solicitudes a un servidor virtual de equilibrio de carga determinado y el servidor virtual de equilibrio de carga también recibe otras solicitudes, al vaciar la cola de sobretensión del servidor virtual de cambio de contenido, solo las solicitudes recibidas de esta cambio de contenido servidor virtual se vacían. Las demás solicitudes de la cola de sobretensión del servidor virtual de equilibrio de carga no se vacían.

Nota:

> - No puede vaciar las colas de sobretensión de redirección de caché, autenticación, servidores virtuales VPN o GSLB o servicios GSLB.
> - No utilice la función Protección contra sobretensiones si Usar IP de origen (USIP) está habilitada.

Vaciar una cola de sobretensiones mediante la CLI

El comando flush ns SurgeQ funciona de la siguiente manera:

- Puede especificar el nombre de un servicio, grupo de servicios o servidor virtual cuya cola de sobretensiones debe vaciarse.
- Si especifica un nombre mientras se ejecuta el comando, se vacía la cola de sobretensión de la entidad especificada. Si más de una entidad tiene el mismo nombre, el dispositivo vacía las colas de sobretensión de todas esas entidades.
- Si especifica el nombre de un grupo de servicios y un nombre de servidor y un puerto mientras ejecuta el comando, el dispositivo vacía la cola de sobretensión solo del miembro del grupo de servicio especificado.
- No puede especificar directamente un miembro del grupo de servicios <serverName> and <port> sin especificar el nombre del grupo de servicios <name> y no puede especificar <port> sin un <serverName>. Especifique <serverName> y <port> si quiere vaciar la cola de sobretensión para un miembro del grupo de servicios específico.
- Si ejecuta el comando sin especificar ningún nombre, el dispositivo vacía las colas de sobretensión de todas las entidades presentes en el dispositivo.
- Si un miembro del grupo de servicios se identifica con un nombre de servidor, debe especificar el nombre del servidor en este comando; no puede especificar su dirección IP.

En el símbolo del sistema, escriba:

```
flush ns surgeQ [-name <name>] [-serverName <serverName> <port>]
```

Ejemplos

1. `flush ns surgeQ -name SVC1ANZGB -serverName 10.10.10.1 80`

   El comando anterior vacía la cola de sobretensiones del servicio o servidor virtual denominado SVC1ANZGB y tiene una dirección IP como 10.10.10.

2. `flush ns surgeQ`

   El comando anterior vacía todas las colas de sobretensiones del dispositivo.

Vaciar una cola de sobretensiones mediante la interfaz gráfica de usuario

Vaya a Administración del tráfico > Cambio de contenido > Servidores virtuales, seleccione un servidor virtual y, en la lista Acción, seleccione Flush Surge Queue.

Opciones de seguridad DNS

August 20, 2021

Ahora puede configurar las opciones de seguridad DNS desde la página Agregar perfil de seguridad DNS en la GUI de Citrix ADC. Para configurar las opciones de seguridad DNS desde la CLI de Citrix ADC o la API NITRO, utilice los componentes AppExpert. Para obtener instrucciones, consulte la documentación de la API de NITRO y la Guía de referencia de comandos de Citrix ADC.

Una opción, la protección contra envenenamiento de caché, está habilitada de forma predeterminada y no se puede inhabilitar. Puede aplicar las otras opciones a todos los dispositivos de punto final DNS o a servidores virtuales DNS específicos de la implementación, como se muestra en la tabla siguiente:

Opción de seguridad	¿Se puede aplicar a todos los dispositivos de punto final DNS?	¿Se puede aplicar a servidores virtuales DNS específicos?
Protección DDoS DNS	Sí	Sí
Administrar excepciones: Servidores de lista de permitidos/lista de prohibidos	Sí	Sí
Evitar ataques aleatorios de subdominios	Sí	Sí
Omitir la caché	Sí	No
Aplicar transacciones DNS a través de TCP	Sí	Sí
Proporcionar detalles de raíz en la respuesta DNS	Sí	No

Protección contra envenenamiento por caché

Un ataque de envenenamiento de caché redirige a los usuarios de sitios legítimos a sitios web maliciosos.

Por ejemplo, el atacante reemplaza una dirección IP genuina en la caché DNS por una dirección IP falsa que controlan. Cuando el servidor responde a las solicitudes de estas direcciones IP, la caché se envenena. Las solicitudes posteriores de las direcciones del dominio se redirigen al sitio del atacante.

La opción Protección de envenenamiento de caché impide la inserción de datos dañados en la base de

datos que almacena en caché las solicitudes y respuestas del servidor DNS. Esta función está integrada en los dispositivos Citrix ADC y siempre está habilitada.

Protección DDoS DNS

Puede configurar la opción Protección DNS DDoS para cada tipo de solicitud que sospeche pueda utilizarse en un ataque DDoS. Para cada tipo, el dispositivo elimina cualquier solicitud recibida después de que se haya superado un valor umbral para el número de solicitudes recibidas en un período de tiempo determinado (intervalo de tiempo). También puede configurar esta opción para registrar una advertencia en el servidor SYSLOG. Por ejemplo:

- **DROP:** - Seleccione esta opción para las solicitudes DROP sin registrar. Supongamos que ha habilitado Protección de registros A con un valor umbral 15, un intervalo de tiempo de 1 segundo y ha elegido DROP. Cuando las solicitudes entrantes superan las 15 consultas en 1 segundo, los paquetes comienzan a descartarse.
- **ADVERTENCIA:** - Seleccione esta opción para las solicitudes LOG y DROP. Supongamos que ha habilitado la protección de registros A con un valor umbral 15, un intervalo de tiempo de 1 segundo y ha elegido WARN. Cuando las solicitudes entrantes superan las 15 consultas en 1 segundo, se registra un mensaje de advertencia que indica una amenaza y, a continuación, se descartan los paquetes. Citrix recomienda establecer valores de umbral para WARN menores que el valor umbral de DROP para un tipo de registro. Esta configuración ayuda a los administradores a identificar un ataque registrando un mensaje de advertencia antes de que ocurra el ataque real y Citrix ADC comience a eliminar las solicitudes entrantes.

Establezca un umbral para el tráfico entrante mediante la GUI

1. Vaya a **Configuración** > **Seguridad** > **Seguridad DNS**.
2. En la página **Perfil de seguridad DNS**, haga clic en **Agregar**.
3. En la página **Agregar perfil de seguridad DNS**, haga lo siguiente:
4. Expanda **Protección DDoS DNS**.
    a) Seleccione el tipo de registro e introduzca el límite de umbral y el valor del segmento temporal.
    b) Seleccione **DROP** o **WARN**.
    c) Repita los pasos a y b para cada uno de los otros tipos de registro contra los que quiera proteger.
5. Haga clic en **Enviar**.

Administrar excepciones: servidores de listas de permitidos/listas de bloqueo

Administrar excepciones le permite agregar excepciones a la lista de bloques o permitir nombres de dominio y direcciones IP de lista. Por ejemplo:

- Cuando se identifica una dirección IP concreta que publica un ataque, dicha dirección IP se puede agregar a la lista bloqueada.
- Cuando los administradores descubren que hay un número inesperadamente elevado de solicitudes de un nombre de dominio determinado, ese nombre de dominio se puede agregar a la lista bloqueada.
- `NXDomains` y algunos de los dominios existentes que pueden consumir los recursos del servidor pueden aparecer en la lista de prohibidos.
- Cuando los administradores permiten listas de nombres de dominio o direcciones IP, las consultas o solicitudes solo de estos dominios o direcciones IP se responden y se eliminan todos los demás.

Crear una lista de permitidos o una lista de bloqueos mediante la GUI

1. Vaya a **Configuración > Seguridad > Seguridad DNS**.
2. En la página **Perfiles de seguridad DNS**, haga clic en **Agregar**.
3. En la página **Agregar perfil de seguridad DNS**, haga lo siguiente:
   a) Expanda **Administrar excepciones: Servidores de lista de permitidos/lista de prohibidos**.
   b) Seleccione **Bloquear** para bloquear consultas de dominios/direcciones de la lista de prohibidos o seleccione **Permitir** solo para permitir consultas de dominios o direcciones de la lista de permitidos.
   c) En el cuadro **Nombre de dominio/Dirección IP**, escriba los nombres de dominio, direcciones IP o intervalos de direcciones IP. Utilice comas para separar las entradas.
   Nota: Si selecciona **Opción avanzada**, puede usar las opciones “empezar por”, “contiene” y “termina por” para establecer los criterios.
   Por ejemplo, puede establecer criterios para bloquear una consulta DNS que empieza por “imagen” o finaliza en “.co.ru” o que contiene “sitios móviles”. “
4. Haga clic en **Enviar**.

Evitar ataques aleatorios de subdominios

En los ataques de subdominio aleatorios, las consultas se envían a subdominios aleatorios e inexistentes de dominios legítimos. Esta acción aumenta la carga de los solucionadores y servidores DNS. Como resultado, pueden sobrecargarse y ralentizarse.

La opción Evitar ataques de subdominio aleatorios dirige al respondedor DNS a eliminar las consultas DNS que excedan una longitud especificada.

Supongamos que example.com es un nombre de dominio propiedad de usted y, por lo tanto, la solicitud de resolución llega a su servidor DNS. El atacante puede anexar un subdominio aleatorio a example.com y enviar una solicitud. Según la longitud de consulta especificada y el FQDN, se eliminan las

consultas aleatorias.

Por ejemplo, si la consulta es www.image987trending.example.com, se elimina si la longitud de la consulta se establece en 20.

Especificar una longitud de consulta DNS mediante la interfaz gráfica de usuario

1. Vaya a **Configuración > Seguridad > Seguridad DNS**.
2. En la página **Perfiles de seguridad DNS**, haga clic en **Agregar**.
3. En la página **Agregar perfil de seguridad DNS**, haga lo siguiente:
   a) Expanda **Evitar ataques aleatorios de subdominio**.
   b) Introduzca el valor numérico para la longitud de la consulta.
4. Haga clic en **Enviar**.

Omitir la caché

Durante un ataque, los datos que ya están almacenados en caché deben protegerse. Para proteger la caché, se pueden enviar nuevas solicitudes para determinados dominios o tipos de registro o códigos de respuesta a los servidores de origen en lugar de almacenarlas en caché.

La opción Evitar la caché indica al dispositivo Citrix ADC que omita la caché para dominios, tipos de registro o códigos de respuesta especificados cuando se detecta un ataque.

Omitir la caché para dominios o tipos de registro o tipos de respuesta especificados mediante la interfaz gráfica de usuario

1. Vaya a **Configuración > Seguridad > Seguridad DNS**.
2. En la página **Perfiles de seguridad DNS**, haga clic en **Agregar**.
3. En la página **Agregar perfil de seguridad DNS**, expanda **Omitir la caché** e introduzca los nombres de dominio. Opcionalmente, elija los tipos de registro o los tipos de respuesta para los que se debe omitir la caché.
   - Haga clic en **Dominios** e introduzca los nombres de dominio. Utilice comas para separar las entradas.
   - Haga clic en **Tipos de registro** y elija los tipos de registro.
   - Haga clic en **Tipos de respuesta** y elija el tipo de respuesta.
4. Haga clic en **Enviar**.

Aplicar transacciones DNS a través de TCP

Algunos ataques DNS se pueden evitar si las transacciones se ven forzadas a utilizar TCP en lugar de UDP. Por ejemplo, durante un ataque de bot, el cliente envía un flujo de consultas pero no puede

manejar las respuestas. Si se impone el uso de TCP para estas transacciones, los bots no pueden entender las respuestas y, por lo tanto, no pueden enviar solicitudes a través de TCP.

Forzar dominios o tipos de registro para que funcionen en el nivel TCP mediante la interfaz gráfica de usuario

1. Vaya a **Configuración > Seguridad > Seguridad DNS**.
2. En la página **Perfiles de seguridad DNS**, haga clic en **Agregar**.
3. En la página **Agregar perfil de seguridad DNS**, expanda **Aplicar transacciones DNS a través de TCP** e introduzca los nombres de dominio y/o elija los tipos de registro para los que se deben aplicar las transacciones DNS a través de TCP.
   - Haga clic en **Dominios** e introduzca los nombres de dominio. Utilice comas para separar las entradas.
   - Haga clic en **Tipos deregistro** y elija los tipos de registro.
4. Haga clic en **Enviar**.

Proporcionar detalles de raíz en la respuesta DNS

En algunos ataques, el atacante envía una serie de consultas para dominios no relacionados que no están configurados ni almacenados en caché en el dispositivo Citrix ADC. Si el `dnsRootReferral` parámetro está HABILITADO, expone todos los servidores raíz.

La opción Proporcionar detalles de raíz en la respuesta DNS indica al dispositivo Citrix ADC que restrinja el acceso a referencias raíz para una consulta que no esté configurada o almacenada en caché. El dispositivo envía una respuesta en blanco.

La opción Proporcionar detalles de raíz en la respuesta DNS también puede mitigar o bloquear los ataques de amplificación. Cuando el parámetro DNSRootReferral está DESHABILITADO, no hay referencias raíz en las respuestas de Citrix ADC y, por lo tanto, no se amplifican.

Habilitar o inhabilitar el acceso al servidor raíz mediante la interfaz gráfica de usuario

1. Vaya a **Configuración > Seguridad > Seguridad DNS**.
2. En la página **Perfiles de seguridad DNS**, haga clic en **Agregar**.
3. En la página **Agregar perfil de seguridad DNS**, haga lo siguiente:
   a) Expanda **Proporcionar detalles de raíz** en la **respuesta DNS**.
   b) Haga clic en **ON** u **OFF** para permitir o restringir el acceso al servidor raíz.
4. Haga clic en **Enviar**.

Sistema

January 19, 2021

En esta sección se proporciona información a nivel de sistema del Citrix ADC. Esto incluye una explicación detallada de las funciones de nivel del sistema, los casos en los que se pueden utilizar las entidades, los pasos de configuración y ejemplos que le ayudarán a comprender mejor las funciones.

- Operaciones básicas
- Autenticación y autorización
- Configuraciones TCP
- Configuraciones HTTP
- SNMP
- Registro de auditoría
- Registro del servidor web
- Call Home
- Herramienta de generación de informes
- Conector CloudBridge
- Alta disponibilidad
- Optimización TCP

Operaciones base del sistema

June 2, 2022

Las siguientes configuraciones permiten realizar operaciones básicas del sistema en un dispositivo Citrix ADC.

Cómo ver, guardar y borrar la configuración de Citrix ADC

Las configuraciones de Citrix ADC se almacenan en `/nsconfig/ns.conf directory`. Para que las configuraciones estén disponibles en todas las sesiones, debe guardar la configuración después de cada cambio de configuración.

Ver la configuración en ejecución mediante la interfaz de comandos

En el símbolo del sistema, escriba:


```
show ns runningConfig
<!--NeedCopy-->
```

Ver la configuración en ejecución mediante la interfaz gráfica de usuario

1. Desplácese hasta **Sistema** > **Diagnósticos** y, en el grupo **Ver configuración**, haga clic en **Ejecutar configuración**.

Ver la diferencia entre los dos archivos de configuración mediante la interfaz de comandos

En el símbolo del sistema, escriba:

```
diff ns config <configfile> <configfile2>
<!--NeedCopy-->
```

Ver la diferencia entre los dos archivos de configuración mediante la GUI

1. Vaya a **Sistema** > **Diagnósticos** y, en el grupo **Ver configuración**, haga clic en **Diferencia de configuración**.

Guardar configuraciones de Citrix ADC mediante la interfaz de comandos

En el símbolo del sistema, escriba:

```
save ns config
<!--NeedCopy-->
```

Guardar configuraciones de Citrix ADC mediante la interfaz gráfica de usuario

1. En la ficha **Configuración**, en la esquina superior derecha, haga clic en el icono **Guardar**.

Visualización de configuraciones guardadas mediante la interfaz de comandos

En el símbolo del sistema, escriba:


```
show ns ns.conf
<!--NeedCopy-->
```

Ver configuraciones guardadas mediante la interfaz gráfica de usuario

Vaya a **Sistema** > **Diagnóstico** y, en el grupo **Ver configuración**, haga clic en **Configuración guardada**.

Borrar la configuración de Citrix ADC mediante la interfaz de comandos

Dispones de las tres opciones siguientes para borrar la configuración de Citrix ADC.

Nivel básico. Al borrar la configuración en el nivel básico, se borran todos los ajustes excepto los siguientes:

- `Nsroot` contraseña
- Time Zone
- Servidor NTP
- Conexión de servidor ADM
- Información del archivo de licencia
- NSIP, MIP (s) y SNIP (s)
- Configuración de red (configuración predeterminada de puerta de enlace, VLAN, RHI, NTP y DNS)
- Definiciones de nodos HA
- Configuración de funciones y modos
- Contraseña de administrador predeterminada()`nsroot`

Nivel extendido. Al borrar la configuración en el nivel ampliado, se borran todos los ajustes excepto los siguientes:

- NSIP y SNIP (s)
- Configuración de red (configuración predeterminada de puerta de enlace, VLAN, RHI, NTP y DNS)
- Definiciones de nodos HA

La configuración de función y modo vuelve a sus valores predeterminados.

Nivel completo. Al borrar la configuración en todo el nivel, se devuelven todos los ajustes a sus valores predeterminados de fábrica. Sin embargo, el NSIP y la puerta de enlace predeterminada no cambian, porque cambiarlos puede provocar que el dispositivo pierda conectividad de red.

En el símbolo del sistema, escriba:


```
clear ns config -force
<!--NeedCopy-->
```

Ejemplo: Para borrar con fuerza las configuraciones básicas de un dispositivo.

```
clear ns config -force basic
<!--NeedCopy-->
```

Borrar la configuración de Citrix ADC mediante la interfaz gráfica de usuario

Vaya a **Sistema** > **Diagnóstico** y, en el grupo Mantenimiento, haga clic en **Borrar configuración** y seleccione el nivel de configuración que quiere borrar del dispositivo.

Cómo reiniciar o apagar el dispositivo para configuraciones de Citrix ADC no guardadas

El dispositivo Citrix ADC se puede reiniciar o apagar de forma remota desde las interfaces de usuario disponibles. Al reiniciar o apagar un dispositivo Citrix ADC independiente, se pierden las configuraciones no guardadas (configuraciones realizadas desde que se emitió el último comando save ns config).

En una configuración de alta disponibilidad, cuando el dispositivo principal se reinicia o se apaga, el dispositivo secundario asume el control y se convierte en el principal. Las configuraciones no guardadas del antiguo dispositivo principal están disponibles en el nuevo dispositivo principal.

También puede reiniciar el dispositivo reiniciando únicamente el software Citrix ADC y no reiniciando el sistema operativo subyacente. Esto se denomina reinicio en caliente. Por ejemplo, cuando agrega una nueva licencia o cambia la dirección IP, puede reiniciar en caliente el dispositivo Citrix ADC para que se realicen estos cambios.

> **Nota:**
>
> Solo puede realizar un reinicio en caliente en un dispositivo Citrix ADC independiente.

Reinicie el dispositivo mediante la interfaz de comandos

En el símbolo del sistema, escriba:

```
reboot [-warm]
<!--NeedCopy-->
```


Reinicie un dispositivo Citrix ADC mediante la interfaz gráfica de usuario

1. En la página de configuración, haga clic en **Reiniciar**.
2. Cuando se le pida que reinicie, seleccione **Guardar configuración** para asegurarse de que no pierde ninguna configuración.

> **Nota:**
>
> Puede realizar un reinicio en caliente seleccionando Reinicio en caliente.

Apague un dispositivo mediante la interfaz de comandos

En el símbolo del shell, escriba:

- `shutdown -p now`: Apaga el software y apaga el Citrix ADC. Para reiniciar Citrix ADC MPX, pulse el interruptor de alimentación de CA. Para reiniciar Citrix ADC VPX, reinicie la instancia VPX.
- `shutdown -h now`: Cierra el software y deja el Citrix ADC activado. Pulse cualquier tecla para reiniciar Citrix ADC. Este comando no desactiva Citrix ADC. Por lo tanto, no apague la alimentación de CA ni retire los cables de alimentación de CA.

> **Nota:**
>
> No se puede apagar un dispositivo mediante la GUI de Citrix ADC.

Cómo sincronizar el reloj del sistema con los servidores de la red

Puede configurar el dispositivo Citrix ADC para que sincronice su reloj local con un servidor de Protocolo de hora de red (NTP). Esto garantiza que su reloj tenga la misma configuración de fecha y hora que los demás servidores de la red.

Puede configurar la sincronización del reloj en el dispositivo agregando entradas del servidor NTP al archivo ntp.conf desde la GUI o la interfaz de línea de comandos, o modificando manualmente el archivo ntp.conf y, a continuación, iniciando el daemon NTP (NTPD). La configuración de sincronización del reloj no cambia si el dispositivo se reinicia, actualiza o baja de categoría. Sin embargo, la configuración no se propaga al Citrix ADC secundario en una configuración de alta disponibilidad.

La GUI de Citrix ADC le permite configurar la zona horaria y la dirección IP del servidor NTP necesarias para la sincronización del reloj en la pantalla del primer usuario (FTU).

> **Nota:**
>
> Si no tiene un servidor NTP local, puede encontrar una lista de servidores NTP públicos de acceso abierto en el sitio oficial de NTP <http://www.ntp.org>, en Lista de servidores de tiempo públicos. Antes de configurar el de Citrix ADC para que use un servidor NTP público, asegúrese de leer la página Reglas de interacción (enlace incluido en todas las páginas Servidores de tiempo

> público).
>
> En Citrix ADC versión 11, la versión NTP se ha actualizado de 4.2.6p3 a 4.2.8p2.

Requisito previo

Para configurar la sincronización del reloj, debe configurar las siguientes entidades:

1. Servidores NTP
2. Sincronización NTP.

Agregar un servidor NTP mediante la interfaz de comandos

En el símbolo del sistema, escriba los siguientes comandos para agregar un servidor NTP y compruebe la configuración:

- `add ntp server (<serverIP> | <serverName>)[-minpoll <positive_integer>] [-maxpoll <positive_integer>]`
- `show ntp server`

Ejemplo:

```
add ntp server 10.102.29.30 -minpoll 6 -maxpoll 11
<!--NeedCopy-->
```

Agregar un servidor NTP mediante la interfaz gráfica de usuario

Vaya a **Sistema** > **Servidores NTP**y cree el servidor NTP.

Habilitar la sincronización NTP mediante la interfaz de comandos

Al habilitar la sincronización NTP, Citrix ADC inicia el daemon NTP y utiliza las entradas del servidor NTP del archivo ntp.conf para sincronizar su configuración de hora local. Si no quiere sincronizar la hora del dispositivo con los demás servidores de la red, puede inhabilitar la sincronización NTP, lo que detiene el daemon NTP (NTPD).

En el símbolo del sistema, escriba uno de los siguientes comandos:

```
enable ntp sync
<!--NeedCopy-->
```


Habilitar la sincronización NTP mediante la interfaz gráfica de usuario

Vaya a **Sistema** > **Servidores NTP**, haga clic en **Acción** y seleccione **Sincronización NTP**.

Configurar la sincronización del reloj para modificar un archivo ntp.conf mediante la interfaz gráfica de usuario

1. Inicie sesión en la interfaz de línea de comandos.
2. Cambie a la solicitud del shell.
3. Copie el archivo `/etc/ntp.conf` en `/nsconfig/ntp.conf`, a menos que `/nsconfig directory` ya contenga un archivo `ntp.conf`.
4. Para cada servidor NTP que quiera agregar, debe agregar las dos líneas siguientes al `/nsconfig /ntp.conf` archivo:

```
server <IP address for NTP server> iburst

restrict <IP address for NTP server> mask <netmask> nomodify
   notrap nopeer noquery
<!--NeedCopy-->
```

> **Nota:**
>
> Por motivos de seguridad, debe haber una entrada restringida correspondiente para cada entrada del servidor.

Ejemplo

En el siguiente ejemplo, un administrador insertó caracteres # para “comentar” una entrada NTP existente y, a continuación, agregó una entrada:

```
#server 1.2.3.4 iburst

#restrict 1.2.3.4 mask 55.255.255.255 nomodify notrap nopeer
   noquery

server 10.102.29.160 iburst

restrict 10.102.29.160 mask 255.255.255.255 nomodify notrap nopeer
    noquery
<!--NeedCopy-->
```


5. Si el directorio /nsconfig no contiene un archivo denominado rc.netscaler, cree el archivo.
6. Agregue la siguiente entrada a /nsconfig/rc.netscaler: /bin/sh /etc/ntpd_ctl full_start

   Esta entrada inicia el servicio ntpd, comprueba el archivo ntp.conf y registra los mensajes en el directorio /var/log.

   Este proceso se ejecuta cada vez que se reinicia Citrix ADC.
7. Reinicie el dispositivo Citrix ADC para habilitar la sincronización del reloj. O bien, para iniciar el proceso de sincronización horaria sin reiniciar el dispositivo, introduzca los siguientes comandos en el símbolo del shell:

```
rm /etc/ntp.conf
ln -s /nsconfig/ntp.conf /etc/ntp.conf
/bin/sh /etc/ntpd_ctl full_start
<!--NeedCopy-->
```

Cómo configurar el tiempo de espera de sesión para conexiones de cliente inactivas

Se proporciona un intervalo de tiempo de espera de sesión para restringir el tiempo durante el que una sesión (GUI, CLI o API) permanece activa cuando no se está usando. Para Citrix ADC, el tiempo de espera de la sesión del sistema se puede configurar en los siguientes niveles:

- **Tiempo de espera a nivel de usuario.** Aplicable al usuario específico.

Tipo de interfaz	Configuración de tiempo de espera
Interfaz gráfica (GUI)	Vaya a **Sistema > Administración de usuarios > Usuarios**, seleccione un usuario y modifique la configuración del tiempo de espera del usuario.
CLI	En la solicitud de comando, escriba el siguiente comando: `set system user <name> -timeout <secs>`

- **Tiempo de espera a nivel de grupo de usuarios.** Aplicable a todos los usuarios del grupo.

Tipo de interfaz	Configuración de tiempo de espera
Interfaz gráfica (GUI)	Vaya a **Sistema > Administración de usuarios > Grupos**, seleccione un grupo y modifique la configuración del tiempo de espera del grupo.
CLI	En el símbolo del sistema, escriba el siguiente comando:`set system group <groupName> -timeout <secs>`

- **Tiempo de espera del sistema global.** Aplicable a todos los usuarios y usuarios de grupos que no tienen configurado un tiempo de espera.

Tipo de interfaz	Configuración de tiempo de espera
Interfaz gráfica (GUI)	Vaya a **Sistema > Configuración**, haga clic en **Cambiar la configuración global del sistema** y actualice el valor de tiempo de espera según sea necesario.
CLI	En la solicitud de comando, escriba el siguiente comando: `set system parameter -timeout <secs>`

El valor de tiempo de espera especificado para un usuario tiene la prioridad más alta. Si el tiempo de espera no está configurado para el usuario, se tiene en cuenta el tiempo de espera configurado para un grupo de miembros. Si no se especifica el tiempo de espera para un grupo (o el usuario no pertenece a un grupo), se tiene en cuenta el valor de tiempo de espera configurado globalmente. Si el tiempo de espera no se configura en ningún nivel, el valor predeterminado de 900 segundos se establece como el tiempo de espera de la sesión del sistema.

Además, puede especificar la duración del tiempo de espera para cada una de las interfaces a las que accede. Sin embargo, el valor de tiempo de espera especificado para una interfaz específica está restringido al valor de tiempo de espera configurado para el usuario que está accediendo a la interfaz. Por ejemplo, consideremos un usuario “publicadmin” que tiene un valor de tiempo de espera de 20 minutos. Ahora, al acceder a una interfaz, el usuario debe especificar un valor de tiempo de espera que esté dentro de los 20 minutos.

> **Nota:**
>
> Puede elegir mantener una comprobación de los valores de tiempo de espera mínimo y máximo especificando el tiempo de espera como restringido (en la CLI especificando

> el parámetro *restrictedTimeout*). Este parámetro se proporciona para dar cuenta de versiones anteriores de Citrix ADC en las que el valor de tiempo de espera no estaba restringido.

- Cuando está habilitado, el valor mínimo de tiempo de espera configurable es de 5 minutos (300 segundos) y el valor máximo es de 1 día (86400 segundos). Si el valor de tiempo de espera ya está configurado en un valor superior a 1 día, cuando este parámetro está habilitado, se le pedirá que lo cambie. Si no cambia el valor, el valor del tiempo de espera se reconfigurará automáticamente a la duración predeterminada del tiempo de espera de 15 minutos (900 segundos) en el próximo reinicio. Lo mismo sucederá si el valor de tiempo de espera configurado es inferior a 5 minutos.
- Cuando se inhabilita, se tienen en cuenta las duraciones de tiempo de espera configuradas.
- **Duración del tiempo de espera en cada interfaz:**

Tipo de interfaz	Configuración de tiempo de espera
CLI	Especifique el valor de tiempo de espera en el símbolo del sistema mediante el siguiente comando: `set cli mode -timeout <secs>`
API	Especifique el valor de tiempo de espera en la carga útil de inicio de sesión.

Cómo configurar la fecha y la hora del sistema para sincronizar el reloj con un servidor horario

Para cambiar la fecha y la hora del sistema, debe utilizar la interfaz del shell para el SO FreeBSD subyacente. Sin embargo, para ver la fecha y la hora del sistema, puede utilizar la interfaz de línea de comandos o la GUI.

Ver la fecha y la hora del sistema mediante la interfaz de comandos

En el símbolo del sistema, escriba:

```
1 show ns config
2 <!--NeedCopy-->
```


Ver la fecha y la hora del sistema mediante la interfaz gráfica de usuario

Vaya a **Sistema** y seleccione la ficha **Información del sistema** para ver la fecha del sistema.

Cómo configurar los puertos de administración HTTP y HTTPS para servicios internos

En una implementación en modo de IP única de un dispositivo Citrix ADC, se utiliza una única dirección IP como direcciones NSIP, SNIP y VIP. Esta dirección IP única utiliza diferentes números de puerto para funcionar como direcciones NSIP, SNIP y VIP.

Los números de puerto 80 y 443 son puertos conocidos para los servicios HTTP y HTTPS. Anteriormente, los puertos 80 y 443 de la dirección IP de Citrix ADC (NSIP) eran puertos dedicados para los servicios de administración HTTP y HTTPS internos. Dado que estos puertos estaban reservados para servicios internos, no puede utilizar estos puertos conocidos para proporcionar servicios de datos HTTP y HTTPS desde una dirección VIP, que tiene la misma dirección que la dirección NSIP en una implementación en modo IP única.

Para satisfacer este requisito, ahora puede configurar puertos para los servicios de administración HTTP y HTTPS internos (de la dirección NSIP) distintos de los puertos 80 y 443.

A continuación se enumeran los números de puerto predeterminados para los servicios de administración HTTP y HTTPS internos de los dispositivos Citrix ADC MPX, VPX y CPX:

- Dispositivos Citrix ADC MPX y VPX: 80 (HTTP) y 443 (HTTPS)
- Dispositivos Citrix ADC CPX: 9080 (HTTP) y 9443 (HTTPS)

Configurar los puertos de administración HTTP y HTTPS mediante la interfaz de comandos

Puede configurar un puerto HTTP y HTTPS en cualquier valor del dispositivo Citrix ADC para admitir el servicio de administración HTTP y HTTPS. Sin embargo, de forma predeterminada, el dispositivo Citrix ADC utiliza los puertos 80 y 443 para la conexión HTTP y HTTPS.

En el símbolo del sistema, escriba:

```
1 set ns param  - mgmtHttpPort<port>
2 <!--NeedCopy-->
```

Ejemplo:

```
1 set ns param -mgmtHttpPort 2000
2 <!--NeedCopy-->
```


Para configurar un puerto HTTPS mediante la interfaz de comandos

En el símbolo del sistema, escriba:

```
set ns param  - mgmtHttpsPort<port>
<!--NeedCopy-->
```

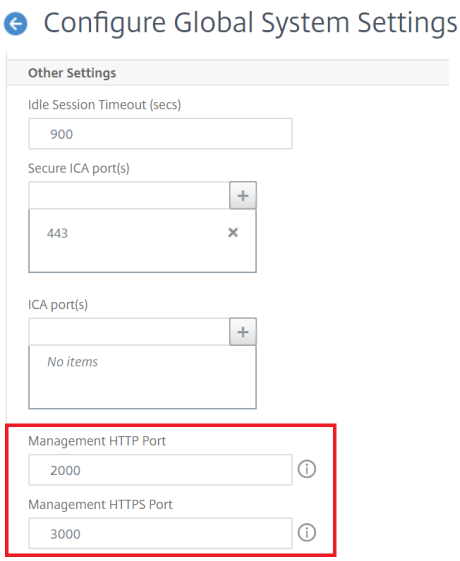
Ejemplo:

```
set ns param -mgmtHttpsPort 3000
<!--NeedCopy-->
```

Configurar los puertos de administración HTTP y HTTPS mediante la interfaz gráfica de usuario

Siga los pasos que se indican a continuación para configurar los valores de los puertos HTTP y HTTPS:

1. Vaya a **Sistema** > **configuración** > **Cambiar la configuración global del sistema**.
2. En la página **Configurar parámetros de configuración global del sistema**, en la sección **Otros ajustes**, defina los siguientes parámetros.
   a) Puerto HTTP de administración. Establezca el valor del puerto en 2000. Predeterminado = 80, Mín = 1, Máx = 65534.
   b) Puerto HTTPS de administración. Establezca el valor del puerto en 3000. Predeterminado = 443, Mín = 1, Máx = 65534.



Configurar el servicio GUI HTTP interno mediante la GUI de Citrix ADC, la CLI de Citrix ADC o las API de Citrix ADC NITRO

En un dispositivo Citrix ADC, `/etc/httpd.conf` es el archivo de configuración para el servicio GUI HTTP interno que administra las conexiones a la GUI de Citrix ADC.

En lugar de usar el archivo `httpd.conf` para configurar el servicio GUI HTTP interno, ahora puede usar la GUI de Citrix ADC, la CLI de Citrix ADC o las API de Citrix ADC NITRO. Por ejemplo, puede usar la CLI de Citrix ADC para modificar la cantidad máxima de clientes que pueden conectarse al servicio GUI HTTP interno a la vez.

El servicio GUI HTTP interno tiene el siguiente formato de nombre: **nshttpd-gui- -80**<loop back IP address>

Use las operaciones de comandos del servicio Citrix ADC para configurar el servicio GUI HTTP interno.

Para modificar el servicio GUI HTTP interno mediante la CLI:

- Use el comando `set service`. Para obtener más información, consulte set service.
- Use el comando `show service` para verificar la configuración. Para obtener más información, consulte show service.

Configuración de ejemplo:

En la siguiente configuración de ejemplo, el parámetro `maxClient` se establece en 300 para el servicio GUI HTTP interno.

```
> sh service nshttpd-gui-127.0.0.1-80
                nshttpd-gui-127.0.0.1-80 (127.0.0.1:80) - HTTP
                State: UP
                Last state change was at Wed Mar 16 20:16:16 2022
                Time since last state change: 0 days, 22:31:00.970
                Server Name: #ns-internal-127.0.0.1#
                Server ID : None                Monitor Threshold : 0
                Max Conn: 0       Max Req: 0          Max Bandwidth: 0
                   kbits
                Use Source IP: NO
                Client Keepalive(CKA): NO
                Monitoring Owner: 0
                Access Down Service: NO
                TCP Buffering(TCPB): NO
                HTTP Compression(CMP): NO
                Idle timeout: Client: 180 sec        Server: 360 sec
                Client IP: ENABLED cip-header
                Cacheable: NO
                SC: ???
```



```
                SP: OFF
                Down state flush: DISABLED
                Monitor Connection Close : NONE
                Appflow logging: DISABLED
                TCP profile name: nstcp_internal_apps
                HTTP profile name: nshttp_default_internal_apps
                Process Local: DISABLED
                Traffic Domain: 0

Done

> set service nshttpd-gui-127.0.0.1-80 -maxclient 300
Done

> sh service nshttpd-gui-127.0.0.1-80
                nshttpd-gui-127.0.0.1-80 (127.0.0.1:80) - HTTP
                State: UP

                ...

                Max Conn: 300  Max Req: 0          Max Bandwidth: 0
                   kbits

                ...

Done

<!--NeedCopy-->
```

Activar la recuperación de memoria mediante la interfaz de comandos

Puede activar la recuperación de memoria desde la interfaz de línea de comandos.

En el símbolo del sistema, escriba el siguiente comando:

```
start ns memrecovery [-percentage <positive_integer>]
```

Ejemplo:

```
start nsmemrecovery -percentage 30
```

Para comprobar la cantidad real de memoria recuperada, utilice el siguiente comando en el símbolo del sistema:

```
stat system memory
```


Cómo asignar una CPU de administración adicional para el procesamiento y la supervisión de datos

Si necesita un mejor rendimiento para la configuración y supervisión de un dispositivo Citrix ADC MPX, puede asignar una CPU de administración adicional del grupo de motores de paquetes del dispositivo. Esta función se admite en determinados modelos Citrix ADC MPX y en todos los modelos VPX, excepto en las instancias VPX que se ejecutan en dispositivos Citrix ADC SDX. Afecta a la salida de los comandos stat system CPU y stat system.

Modelos Citrix ADC MPX compatibles:

- 25xxx
- 22xxx
- 14xxx
- 115xx
- 15xxx
- 26xxx

> **Nota:**
>
> Para los modelos Citrix ADC MPX 26xxx con más de 20 núcleos, la función de CPU de administración adicional obligatoria está habilitada de forma predeterminada. Para los modelos Citrix ADC VPX, se necesita una licencia que admita al menos 12 vCPU para habilitar esta función.

Asignar una CPU de administración adicional mediante la interfaz de comandos

En el símbolo del sistema, escriba uno de los siguientes comandos:

- `enable extramgmtcpu`
- `disable extramgmtcpu`

> **Nota:**
>
> Después de habilitar y inhabilitar esta función, el dispositivo Citrix ADC muestra una advertencia para que se reinicie el dispositivo para que los cambios surtan efecto.

Mostrar el estado configurado y efectivo de una CPU de administración adicional.

En el símbolo del sistema, escriba:

```
1 show extramgmtcpu
2 <!--NeedCopy-->
```

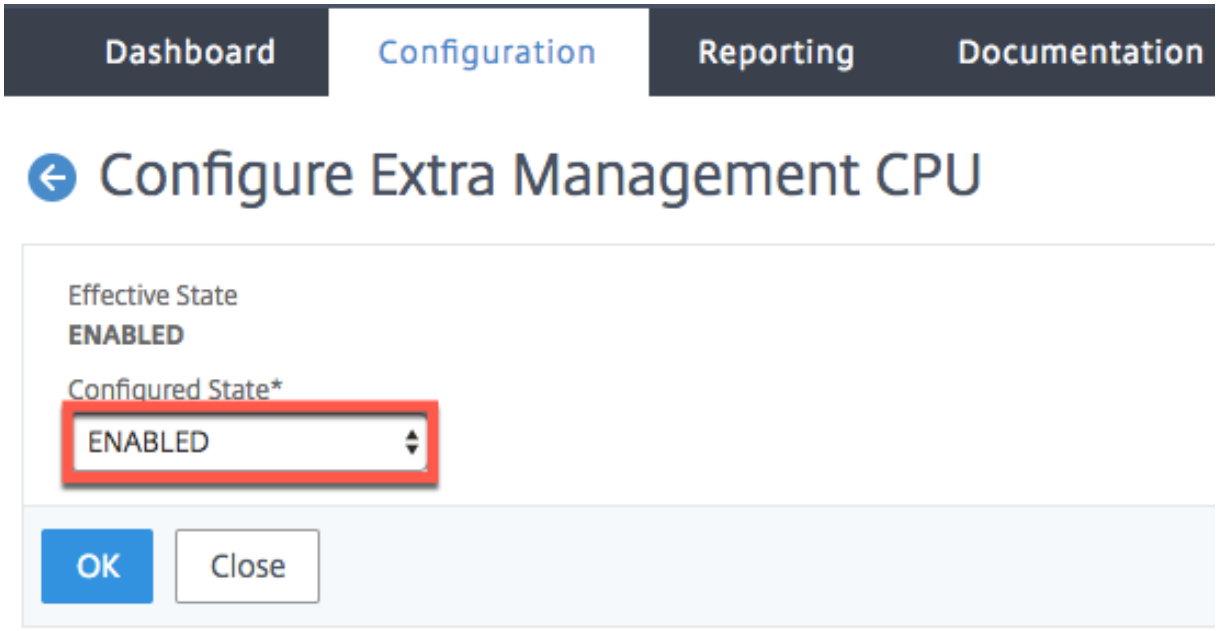
Ejemplo:


```
> show extramgmtcpu
ConfiguredState:  ENABLED EffectiveState:  ENABLED
<!--NeedCopy-->
```

> **Nota:**
>
> En este ejemplo, el comando show se introduce antes de reiniciar el dispositivo.

Asignar una CPU de administración adicional mediante la interfaz gráfica de usuario

Para asignar una CPU de administración adicional mediante la GUI, vaya a **Sistema** > **Configuración** y haga clic en **Configurar CPU de administración adicional**. En el menú desplegable **Estado configurado**, seleccione **Habilitado** y, a continuación, **Aceptar**.



Para comprobar el uso de la CPU, vaya a **Sistema** > **Configuración** > **Panel de control**.

Configurar una CPU de administración adicional mediante la API de NITRO

Utilice los siguientes métodos y formatos NITRO para habilitar, inhabilitar y mostrar una CPU de administración adicional.

Para habilitar una CPU de administración adicional:

```
HTTP Method: POST

URL: http://<NSIP>/nitro/v1/config/systemextramgmtcpu?action=enable
```



```
4
5  Payload: {
6   ”systemextramgmtcpu”:{
7    }
8    }
9
10
11 curl -v -X POST -H ”Content-Type: application/json” -u nsroot:nsroot
      http://10.102.201.92/nitro/v1/config/systemextramgmtcpu?action=
      enable -d '{
12  ”systemextramgmtcpu”:{
13   }
14   }
15  '
16 <!--NeedCopy-->
```

Para inhabilitar una CPU de administración adicional

```
1  HTTP Method: POST
2  URL: http://<NSIP>/nitro/v1/config/systemextramgmtcpu?action=disable
3  Payload: {
4   ”systemextramgmtcpu”:{
5    }
6    }
7
8  curl -v -X POST -H ”Content-Type: application/json” -u nsroot:nsroot
      http://10.102.201.92/nitro/v1/config/systemextramgmtcpu?action=
      disable -d '{
9   ”systemextramgmtcpu”:{
10   }
11   }
12  '
13 <!--NeedCopy-->
```

Para mostrar una CPU de administración adicional

```
1  HTTP Method: GET
2  URL: http://<NSIP>/nitro/v1/config/systemextramgmtcpu
3  <!--NeedCopy-->
```

Ejemplo:


```
curl -v -X GET -H "Content-Type: application/json" -u nsroot:nsroot
   http://10.102.201.92/nitro/v1/config/systemextramgmtcpu
<!--NeedCopy-->
```

Estadísticas y supervisión antes y después de agregar CPU de administración adicional

Los siguientes ejemplos muestran las diferencias en el resultado de los comandos stat system CPU y stat system antes y después de agregar una CPU de administración adicional.

```
stat system cpu
<!--NeedCopy-->
```

Este comando muestra estadísticas de las CPU.

A continuación se muestra un ejemplo de salida antes de agregar una CPU de administración adicional en uno de los modelos compatibles.

Ejemplo

```
> stat system cpu

    CPU statistics

    ID          Usage

    8               1

    7               1

    11              2

    1               1

    6               1

    9               1

    3               1

    5               1

```



```
    4               1

    10              1

    2               1
<!--NeedCopy-->
```

A continuación se muestra el resultado después de agregar una CPU de administración adicional en el mismo dispositivo MPX.

```
    > stat system cpu

    CPU statistics

    ID          Usage

    9               1

    7               1

    5               1

    8               1

    11              2

    10              1

    6               1

    4               1

    3               1

    2               1
<!--NeedCopy-->
```

```
stat system
<!--NeedCopy-->
```

Este comando muestra el uso de CPU. En el siguiente ejemplo, el resultado antes de agregar una CPU

de administración adicional en uno de los modelos compatibles es:

Administración Uso adicional de CPU (%) 0.00

Ejemplo

```
    > stat system

    Citrix ADC Executive View

    System Information:

    Up since        Wed Oct 11 11:17:54 2017

    /flash Used (%)                        0

    Packet CPU usage (%)                1.30

    Management CPU usage (%)            4.00

    Mgmt CPU0 usage (%)                 4.00

    Mgmt Additional-CPU  usage (%)      0.00

    Memory usage (MB)                   2167

    InUse Memory (%)                    5.76

    /var Used (%)                          0
<!--NeedCopy-->
```

En el ejemplo siguiente, el resultado después de agregar una CPU de administración adicional en el mismo dispositivo MPX es:

Administración Uso adicional de CPU (%) 0,80

```
> stat system


Citrix ADC Executive View

System Information:

```



```
Up since        Wed Oct 11 11:55:56 2017

/flash Used (%)                        0

Packet CPU usage (%)                1.20

Management CPU usage (%)            5.70

Mgmt CPU0 usage (%)                10.60

Mgmt Additional-CPU  usage (%)      0.80

Memory usage (MB)                   1970

InUse Memory (%)                    5.75

/var Used (%)                          0

<!--NeedCopy-->
```

Cómo realizar copias de seguridad y restaurar el dispositivo para recuperar la configuración perdida

Si el dispositivo se daña o necesita una actualización, puede hacer una copia de seguridad de la configuración del sistema. El procedimiento de copia de seguridad se realiza a través de la interfaz CLI o GUI de Citrix. El dispositivo también permite importar el archivo de copia de seguridad de un origen externo. Sin embargo, solo puede hacerlo a través de la interfaz GUI y no se puede hacer a través de la interfaz CLI.

Puntos que tener en cuenta

Debe recordar los siguientes puntos al realizar la copia de seguridad y restaurar el dispositivo.

- Debe haber configuración de red en una nueva plataforma.
- La nueva compilación de la plataforma debe ser la misma que la del archivo de copia de seguridad o una versión posterior.

Crear una copia de reserva de un dispositivo Citrix ADC

Según los requisitos de datos y reserva, puede crear una copia de seguridad “básica” o una copia de seguridad “completa”.

- **Backup básico.** Puede realizar este tipo de copia de seguridad si quiere hacer una copia de seguridad de los archivos que cambian constantemente. Los archivos de los que puede realizar una copia de seguridad se encuentran en la tabla siguiente.

Para obtener información sobre los detalles básicos de la copia de seguridad, consulte el tema Tabla.

- **Copia de seguridad completa.** Además de los archivos de los que se creó una copia de seguridad básica, una copia de seguridad completa contiene archivos que se actualizan con menos frecuencia. Los archivos de los que se realiza una copia de seguridad cuando se utiliza la opción de copia de seguridad "Completa" son:

Directorio	Subdirectorio o archivos
nsconfig	ssl*, licencia*, fips*
/var/	netscaler/ssl/*, wi/java_home/jre/lib/security/cacerts/*, wi/java_home/lib/security/cacerts/*

Los datos de la copia de seguridad se almacenan como un archivo TAR comprimido en el directorio `/var/ns_sys_backup/`. Para evitar problemas debido a la falta de disponibilidad de espacio en disco, puede almacenar hasta 50 archivos de copia de seguridad en este directorio. Puede utilizar el comando `rm system backup` para eliminar los archivos de copia de seguridad existentes y crear más copias de seguridad.

> **Nota:**
>
> Cuando la operación de copia de seguridad esté en curso, no ejecute comandos que afecten a la configuración.
>
> Si un archivo del que es necesario realizar una copia de seguridad no está disponible, la operación omite ese archivo.

Crear una copia de reserva de un dispositivo Citrix ADC mediante la interfaz de comandos

Siga el procedimiento que se indica a continuación para hacer una copia de seguridad de un dispositivo Citrix ADC mediante la interfaz de comandos de Citrix ADC.

En el símbolo del sistema, haga lo siguiente:

1. Guarde las configuraciones de Citrix ADC.

```
save ns config
<!--NeedCopy-->
```


1. Cree el archivo de copia de seguridad.

```
create system backup [<fileName>] -level <basic | full> -comment <
    string>
<!--NeedCopy-->
```

> **Nota:**
>
> Si no se especifica el nombre de archivo, el dispositivo crea un archivo TAR con la siguiente convención de nomenclatura:`backup_<level>_<nsip_address>_<date-timestamp>.tgz`.

Ejemplo: Para hacer una copia de seguridad de todo el dispositivo mediante la convención de nomenclatura predeterminada del archivo de copia de seguridad.

```
> create system backup -level full
<!--NeedCopy-->
```

1. Compruebe que se ha creado el archivo de copia de seguridad.

```
show system backup
<!--NeedCopy-->
```

Puede ver las propiedades de un archivo de copia de seguridad específico mediante el parámetro `fileName`.

Restaurar un dispositivo Citrix ADC mediante la interfaz de comandos

> **Importante:**
>
> No se puede restaurar correctamente el dispositivo si cambia el nombre o modifica el archivo de copia de seguridad.

Al restaurar el dispositivo, la operación de restauración desactiva el archivo de copia de seguridad del directorio `/var/ns_sys_backup/`. Una vez que los archivos están desbloqueados, los archivos se copian en los directorios respectivos.

Restaurar Citrix ADC desde un archivo de copia de seguridad local mediante la interfaz de comandos

> **Nota:**
>
> Citrix recomienda hacer una copia de seguridad de la configuración actual antes de restaurar una configuración anterior. Sin embargo, si no quiere que el comando restore cree automáticamente una copia de seguridad de la configuración actual, utilice el parámetro `-skipBackup`.

En el símbolo del sistema, haga lo siguiente:

1. Obtenga una lista de los archivos de copia de seguridad disponibles en el dispositivo.

```
show system backup
<!--NeedCopy-->
```

2. Restaure el dispositivo especificando uno de los archivos de copia de seguridad.

   `restore system backup <filename> [-skipBackup]`

   Ejemplo: Para restaurar mediante una copia de seguridad completa de un dispositivo

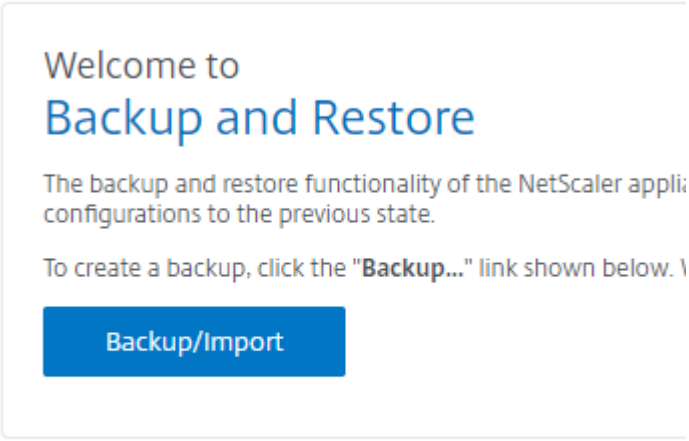
   `> restore system backup backup_full_<nsip_address>_<date-timestamp>.tgz`

3. Reinicie el dispositivo.

   `reboot`

Copia de seguridad y restauración de un dispositivo Citrix ADC mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **Copia de seguridad y restauración**.

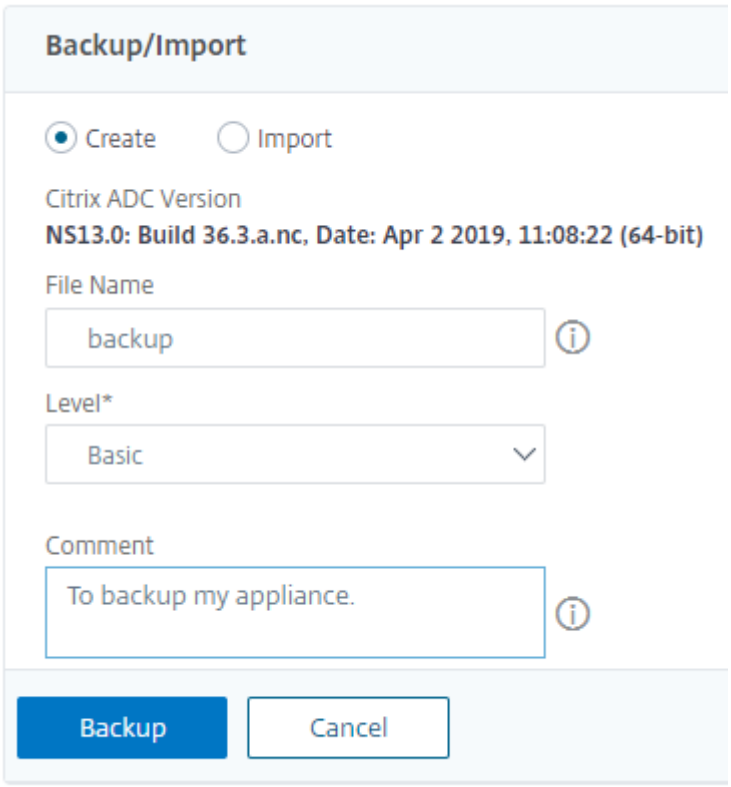


2. Haga clic en **Copia de seguridad/importación** para iniciar el proceso.

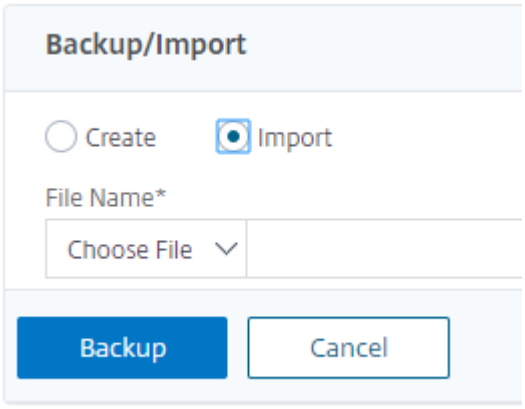
3. En la página **Copia de seguridad/importación**, seleccione **Crear** y defina los siguientes parámetros.

   a) Nombre del archivo. Nombre del archivo de copia de seguridad del dispositivo.
   b) Nivel. Seleccione un nivel de copia de seguridad como básico o completo.
   c) Comentar. Proporcione una breve descripción de la copia de seguridad.

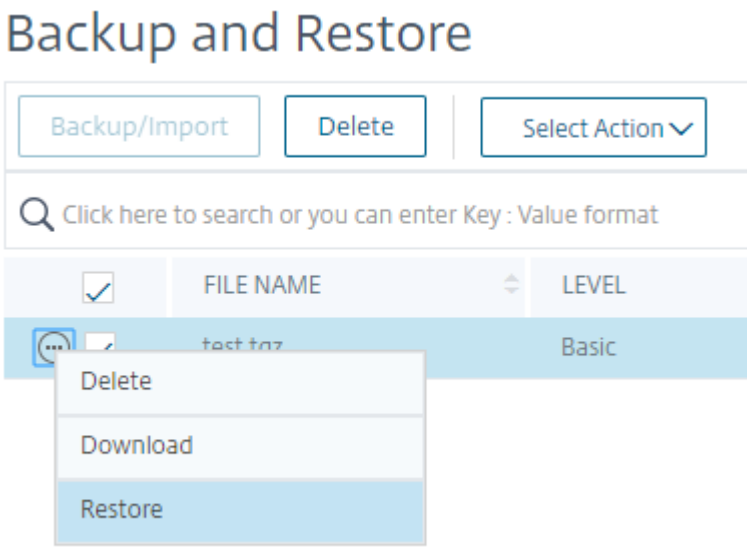
4. Haga clic en **Copia de seguridad**.



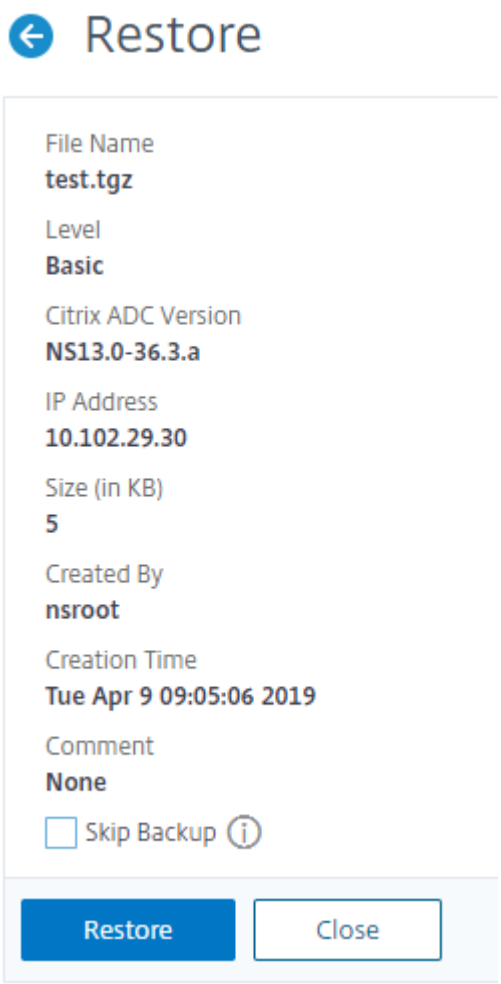
5. Si quieres importar una copia de seguridad, debes seleccionar **Importar**.



6. Una vez completada la copia de seguridad, puede seleccionar el archivo y hacer clic en **Descargar**.
7. Para restaurar, seleccione el archivo de copia de seguridad y haga clic en **Restaurar**.



8. En la página **Restaurar**, compruebe los detalles del archivo de reserva y haga clic en **Restaurar**.



9. Después de restaurar, debe reiniciar el dispositivo.

Para obtener más información sobre cómo hacer copias de seguridad y restaurar instancias de Citrix ADC, consulte el tema Copia de seguridad y restauración mediante Citrix ADM.

Para obtener más información sobre cómo hacer copias de seguridad y restaurar un dispositivo SDX, consulte Copia de seguridad y restauración del dispositivo SDX.

Para obtener información sobre las operaciones realizadas en el backup del sistema, consulte el tema Copia de seguridad del sistema.

Cómo generar un paquete de asistencia técnica para resolver problemas de dispositivos

Para obtener ayuda para analizar y resolver cualquier problema con un dispositivo Citrix ADC, puede generar un paquete de asistencia técnica en el dispositivo y enviarlo a la asistencia técnica de Citrix. El paquete de asistencia técnica de Citrix ADC es un archivo tar comprimido de datos y estadísticas de

configuración del sistema. Recopila los siguientes datos del dispositivo Citrix ADC en el que se genera el paquete:

- **Archivos de configuración**. Todos los archivos del directorio /flash/nsconfig.
- **Archivos Newnslog**. El newnslog actualmente en ejecución y algunos archivos anteriores. Para minimizar el tamaño del archivo, la recopilación `newnslog` está restringida a 500 MB, 6 archivos o 7 días, lo que ocurra primero. Si se necesitan datos antiguos, es posible que requiera la recopilación manual.
- **Archivos de registro**. Archivos en /var/log/messages, */var/log/ns.log* y otros archivos en /var/log y /var/nslog.
- **Archivos principales de la aplicación**. Archivos creados en el directorio /var/core durante la última semana, si los hubiera.
- **Salida de algunos comandos show de CLI**.
- **Salida de algunos comandos stat de CLI**.
- **Salida de comandos shell de BSD**.

Puede utilizar un solo comando para generar el paquete de asistencia técnica y cargarlo de forma segura en el servidor de asistencia técnica de Citrix. Para cargar, debe especificar sus credenciales de Citrix. Al generar el paquete, puede especificar el número de caso o solicitud de servicio que la asistencia técnica de Citrix le asignó. Si ya ha generado un paquete de asistencia técnica, puede cargar el archivo archivado existente en el servidor de asistencia técnica de Citrix especificando el nombre del archivo con la ruta completa.

El paquete de asistencia técnica se guarda en el dispositivo Citrix ADC en un archivo en la siguiente ubicación:

```
1 /var/tmp/support/support.tgz
2 <!--NeedCopy-->
```

La ruta es un enlace simbólico al recopilador más reciente para facilitar el acceso. El nombre completo del archivo varía en función de la topología de implementación, pero generalmente sigue un formato similar a:

```
1 collector_<P/S>\_<NS IP>\_<DateTime>.tgz.
2 <!--NeedCopy-->
```

Si el dispositivo Citrix ADC no tiene conectividad directa a Internet, puede utilizar un servidor proxy para cargar directamente el paquete de asistencia técnica en el servidor de asistencia técnica de Citrix. El formato básico de la cadena proxy es:


```
proxy_IP:<proxy_port>
<!--NeedCopy-->
```

Si el servidor proxy requiere autenticación, el formato es:

```
username:password@proxsy_IP:<proxy_port>
<!--NeedCopy-->
```

> **Nota:**
>
> Para los dispositivos Citrix ADC en un par de alta disponibilidad, debe generar el paquete de asistencia técnica en cada uno de los dos nodos.
>
> Para los dispositivos Citrix ADC en una configuración de clúster, puede generar el paquete de asistencia técnica en cada nodo de forma individual o puede generar archivos abreviados más pequeños para todos los nodos mediante la dirección IP del clúster.
>
> Para las particiones de administración de Citrix ADC, debe generar el paquete de asistencia técnica a partir de la partición de administración predeterminada. Para obtener el paquete de asistencia técnica para una partición específica, debe especificar el nombre de la partición para la que quiere generar el paquete de asistencia técnica. Si no especifica el nombre de la partición, los datos se recopilan de todas las particiones administrativas.

Genere el paquete de asistencia técnica de Citrix ADC mediante la interfaz de comandos

En el símbolo del sistema, escriba:

```
show techsupport [-scope <scope> <partitionName>] [-upload [-proxy <
    string>] [-casenumber <string>] [-file <string>] [-description <
    string>] [-userName <string> -password ]]
<!--NeedCopy-->
```

Sr. No	Tarea	Comando
1	Genere y cargue el paquete de asistencia técnica en el servidor de asistencia técnica de Citrix.	show techsupport –upload –userName account1 –password xxxxxxx

Sr. No	Tarea	Comando
2	Generar y cargar el paquete de asistencia técnica en el servidor de asistencia técnica de Citrix a través de un servidor proxy	show techsupport –upload –proxy 1.1.1.1:80 –userName account1 –password xxxxxxx
3	Cargue un paquete de asistencia técnica existente en el servidor de asistencia técnica de Citrix.	show techsupport –upload -file,/var/tmp/support/collector_P_10.102.29.1 –userName account1 –password xxxxxxx
4	Generar archivos pequeños y abreviados para todos los nodos de una configuración de clúster. Ejecute este comando mediante la dirección IP del clúster	show techsupport –scope CLUSTER
5	Genere un paquete de asistencia técnica específico para una partición de administración. Ejecute este comando en la partición de administración predeterminada.	show techsupport –scope PARTITION partition1

Cómo recopilar el paquete de asistencia técnica de los dispositivos SDX y VPX para el análisis de conocimientos

Un dispositivo Citrix ADC tiene un mecanismo integrado para recopilar archivos de registro. Los archivos de registro se envían a su vez a Citrix Insight Services para su análisis.

> **Nota:**
>
> Todos los procedimientos son aplicables a la versión 9.2 o posterior del software.

Descargue el paquete de asistencia técnica de los dispositivos Citrix ADC MPX y VPX

Para ejecutar un archivo recopilador mediante la GUI de Citrix ADC, debe completar el siguiente procedimiento:

> **Nota:**
>
> El procedimiento se aplica a la versión 9.2 o posterior del software.

1. Vaya a **Sistema** > **Diagnóstico**.
2. En la sección **Herramientas de asistencia técnica**, haga clic en el enlace **Generar archivo de asistencia**.
3. En la página **Asistencia técnica**, defina los siguientes parámetros:
   a) Alcance. Recopilar datos de uno o varios nodos.
   b) Partición. Nombre de la partición.
   c) Opciones de carga de la asistencia técnica de Citrix. Defina todas las opciones, como el servidor proxy, el número de caso de servicio, el nombre del archivo del recopilador y una breve descripción del archivo archivador para cargar el paquete de asistencia técnica.
   d) Cuenta Citrix. Introduzca sus credenciales de Citrix.
4. Haga clic en **Ejecutar**.
5. Se genera el paquete de asistencia técnica.
6. Haga clic en **Sí** para descargar el paquete de asistencia técnica en su escritorio local.

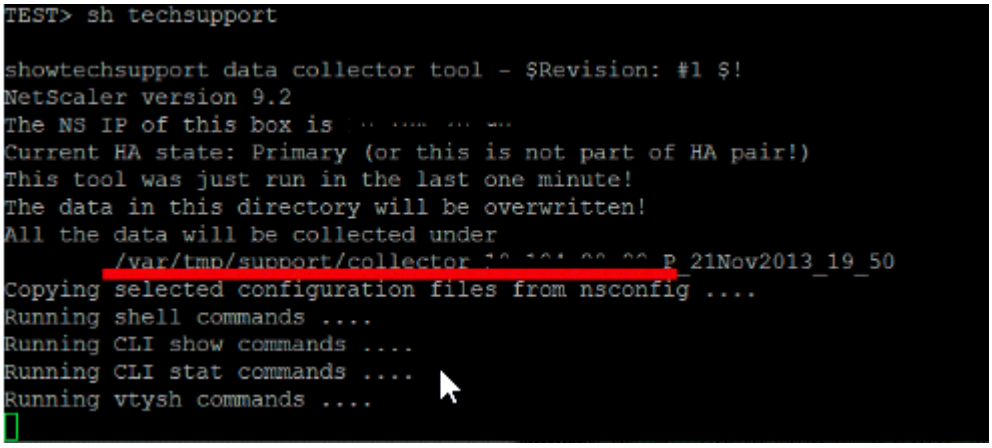
Obtenga el paquete de asistencia técnica mediante la interfaz de comandos

1. Descargue el archivo del dispositivo mediante una utilidad FTP segura (SFTP) o Secure Copy (SCP), como `WinSCP`, y cárguelo en Citrix Insight Services para su análisis.

> **Nota:**
>
> En la versión del software Citrix ADC anterior a la 9.0, el script del recopilador debe descargarse por separado y ejecutarse.

```
1 > show techsupport -scope CLUSTER
2 <!--NeedCopy-->
```

1. Esto recopila información de asistencia técnica de todos los nodos del clúster y comprime los archivos en un único archivo.
2. Una vez que el dispositivo genera el archivo recopilador, la ubicación del archivo se muestra como se muestra en la siguiente captura de pantalla.



El archivo se almacena en `/var/tmp/support` y puede comprobarlo iniciando sesión en un dispositivo Citrix ADC y ejecutando el siguiente comando desde un símbolo del shell.

```
root@NS# cd /var/tmp/support/
root@NS# ls -l
<!--NeedCopy-->
```

Obtener paquete de diagnóstico de Citrix ADC SDX mediante la interfaz gráfica de usuario

1. Abra la interfaz gráfica de usuario de Citrix SDX.
2. Expanda el nodo **Diagnóstico**.
3. Seleccione el nodo **Asistencia técnica**.
4. Haga clic en Generar archivo de asistencia técnica.
5. Seleccione **Equipo** (incluidas instancias) en el menú desplegable.
6. Haga clic en **Agregar**.
7. Seleccione una o varias instancias para agregarlas.
8. Haga clic en **Aceptar**. Espera a que se complete el proceso.
9. Seleccione el nombre del paquete que se generó y, a continuación, haga clic en **Descargar**
10. Cargue el archivo de paquete en Citrix Insight Services.

Más recursos

Vea un vídeo

Leer otro tema

Documento de referencia de comandos

Autenticación y autorización de los usuarios

August 20, 2021

Para configurar la autenticación y autorización de usuarios de Citrix ADC, primero debe definir los usuarios que tienen acceso al dispositivo Citrix ADC y, a continuación, puede organizar estos usuarios en grupos. Después de configurar usuarios y grupos, debe configurar directivas de comandos para definir tipos de acceso y asignarlas a usuarios y/o grupos.

Debe iniciar sesión como administrador para configurar usuarios, grupos y directivas de comandos. El nombre de usuario predeterminado del administrador de Citrix ADC es *nsroot*. Después de iniciar sesión como administrador predeterminado, debe cambiar la contraseña de la cuenta nsroot. Una vez que haya cambiado la contraseña, ningún usuario puede acceder al dispositivo Citrix ADC hasta que cree una cuenta para ese usuario. Si olvida la contraseña de administrador después de cambiarla de la predeterminada, puede restablecerla a nsroot.

> **Nota:**
>
> - Los usuarios locales pueden autenticarse en Citrix ADC incluso si están configurados servidores de autenticación externos. Para restringirlo, inhabilite el parámetro localAuth del comando set system parameter.
> - Para mejorar la seguridad, Citrix recomienda cambiar la contraseña nsroot. Es aconsejable cambiar la contraseña con frecuencia. Para obtener información sobre cómo cambiar la contraseña nsroot, consulte Restablecimiento de la contraseña de administrador predeterminada (nsroot) .

Directivas de usuarios, grupos de usuarios y comandos

August 20, 2021

Primero debe definir un usuario con una cuenta y, a continuación, organizar todos los usuarios en grupos. Puede crear directivas de comandos o utilizar directivas de comandos integradas para regular el acceso de los usuarios a los comandos.

> **Nota:**
>
> Si prefiere obtener más información sobre la configuración de grupos de usuarios y usuarios como parte de la configuración de autenticación y autorización de Citrix ADC para la administración del tráfico, consulte el tema Configurar usuarios y grupos .

También puede personalizar la línea de comandos de un usuario. Las solicitudes se pueden definir en la configuración de un usuario, en una configuración de grupo de usuarios y en la configuración global del sistema. La solicitud que se muestra para un usuario tiene el siguiente orden de prioridad:

1. Mostrar la solicitud tal como se define en la configuración del usuario.
2. Mostrar la solicitud tal como se define en la configuración de grupo para el grupo del usuario.
3. Mostrar la solicitud tal como se define en la configuración global del sistema.

Ahora puede especificar un valor de tiempo de espera para las sesiones de CLI inactivas para un usuario del sistema. Si la sesión de CLI de un usuario está inactiva durante un tiempo que excede el valor de tiempo de espera, el dispositivo Citrix ADC finaliza la conexión. El tiempo de espera se puede definir en una configuración de usuario, en una configuración de grupo de usuarios o en la configuración global del sistema. El tiempo de espera para las sesiones de CLI inactivas para un usuario se determina en el siguiente orden de prioridad:

1. Configuración de usuario.
2. Configuración de grupo para el grupo del usuario.
3. Configuración global del sistema.

Un administrador raíz de Citrix ADC puede configurar el límite máximo de sesiones simultáneas para los usuarios del sistema. Al restringir el límite, puede reducir el número de conexiones abiertas y mejorar el rendimiento del servidor. Siempre que el recuento de CLI esté dentro del límite configurado, los usuarios simultáneos pueden iniciar sesión en la GUI cualquier número de veces. Sin embargo, si el número de sesiones CLI alcanza el límite configurado, los usuarios ya no podrán iniciar sesión en la GUI. Por ejemplo, si el número de sesiones simultáneas está configurado en 20, los usuarios simultáneos pueden iniciar sesión en 19 sesiones de CLI. Pero si el usuario ha iniciado sesión en la sesión de `20<sup>th</sup>` CLI, cualquier intento de iniciar sesión en la GUI, CLI o NITRO da lugar a un mensaje de error (ERROR: se superó el límite de conexión a CFE).

> **Nota:**
>
> El número predeterminado de sesiones simultáneas se configura en 20 y el número máximo de sesiones simultáneas se configura en 40.

Configurar cuentas de usuario

Para configurar cuentas de usuario, solo tiene que especificar nombres de usuario y contraseñas. Puede cambiar contraseñas y eliminar cuentas de usuario en cualquier momento.

> **Nota:**
>
> No se aceptan todos los caracteres de una contraseña. Sin embargo, funciona si escribe los caracteres entre comillas.
>
> Además, la cadena no debe exceder una longitud máxima de 127 caracteres.

Para crear una cuenta de usuario mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para crear una cuenta de usuario y verificar la configuración:

- `add system user <username> [-externalAuth ( ENABLED | DISABLED )] [-promptString <string>] [-timeout \<secs>] [-logging ( ENABLED | DISABLED )] [-maxsession <positive_integer>]`
- `show system user <userName>`

Los usuarios externos pueden configurar el parámetro “log” para recopilar registros externos mediante el mecanismo de registro web o registro de auditoría. Si el parámetro está habilitado, el cliente de auditoría se autentica con el dispositivo Citrix ADC para recopilar registros.

Ejemplo:

```
> add system user johnd -promptString user-%u-at-%T
```

```
1 Enter password:
2 Confirm password:
3 > show system user johnd
4 user name: john
5      Timeout:900 Timeout Inherited From: Global
6      External Authentication: ENABLED
7      Logging: DISABLED
8      Maximum Client Sessions: 20
9 <!--NeedCopy-->
```

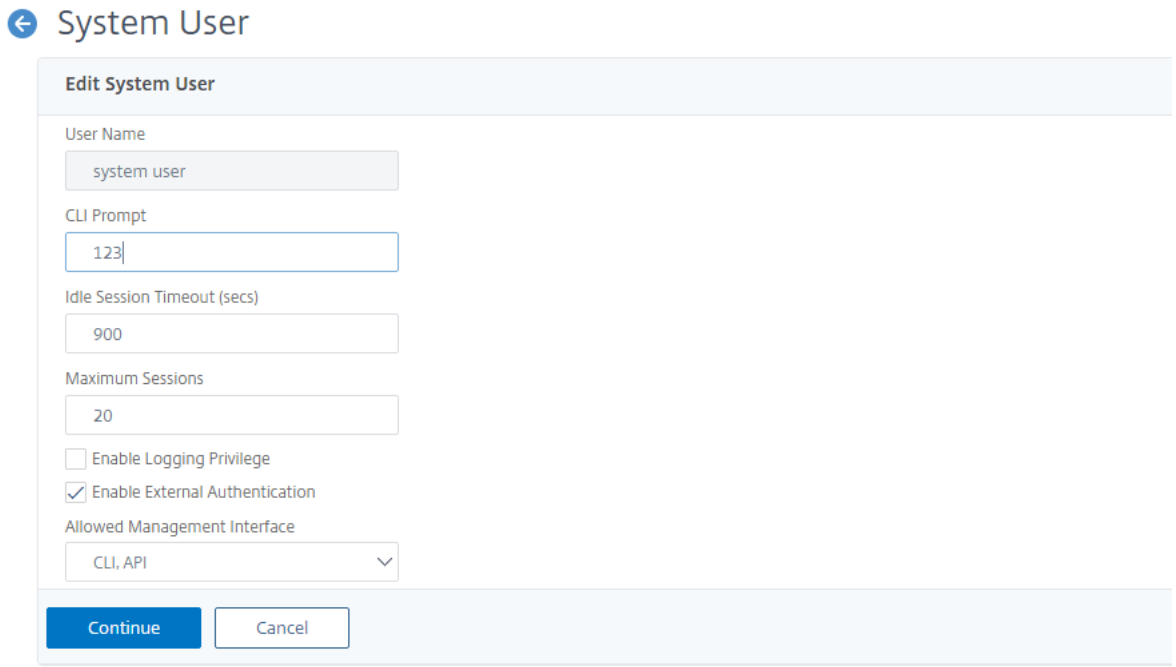
Para obtener una descripción de parámetros, consulte el tema de referencia de comandos de usuario de autenticación y autorización .

Configurar una cuenta de usuario mediante la GUI de Citrix ADC

1. Vaya a **Sistema** > **Administración** de **usuarios > Usuarios** y cree el usuario.
2. En el panel de detalles, haga clic en **Agregar** para crear un usuario del sistema.
3. En la página **Crear Grupo de Sistemas**, defina los siguientes parámetros:
   a) Nombre de usuario. Nombre del grupo de usuarios.

b) Indicador de CLI. El mensaje que prefiere establecer para el acceso a la interfaz CLI.
c) Tiempo de espera de sesión inactiva (segundos). Establezca la cantidad de tiempo que un usuario puede estar inactivo antes de que se agote el tiempo de espera y cierre la sesión.
d) Máximo de sesiones. Establezca el máximo de sesiones que un usuario puede probar.
e) Habilitar privilegio de registro. Habilitar el privilegio de registro para el usuario.
f) Habilite la autenticación externa. Seleccione la opción si quiere utilizar el servidor de autenticación externa para autenticar el usuario.
g) Interfaz de administración permitida. Seleccione las interfaces de Citrix ADC a las que se concede permiso para acceder al grupo de usuarios.
h) Directivas de comando. Enlazar directivas de comandos al grupo de usuarios.
i) Particiones. Enlazar particiones al grupo de usuarios.

4. Haga clic en **Crear** y **cerrar**.



Configurar grupos de usuarios

Después de configurar un grupo de usuarios, puede conceder fácilmente los mismos derechos de acceso a todos los miembros del grupo. Para configurar un grupo, cree el grupo y vincule usuarios al grupo. Puede enlazar cada cuenta de usuario a más de un grupo. La vinculación de cuentas de usuario a varios grupos puede permitir una mayor flexibilidad al aplicar directivas de comandos.

Para crear un grupo de usuarios mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para crear un grupo de usuarios y compruebe la configuración:

- `add system group <groupName> [-promptString <string>] [-timeout <secs>]`
- `show system group <groupName>`

Ejemplo:

```
> add system group Managers -promptString Group-Managers-at-%h
```

Vincular una cuenta de usuario a un grupo mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para enlazar una cuenta de usuario a un grupo y verificar la configuración:

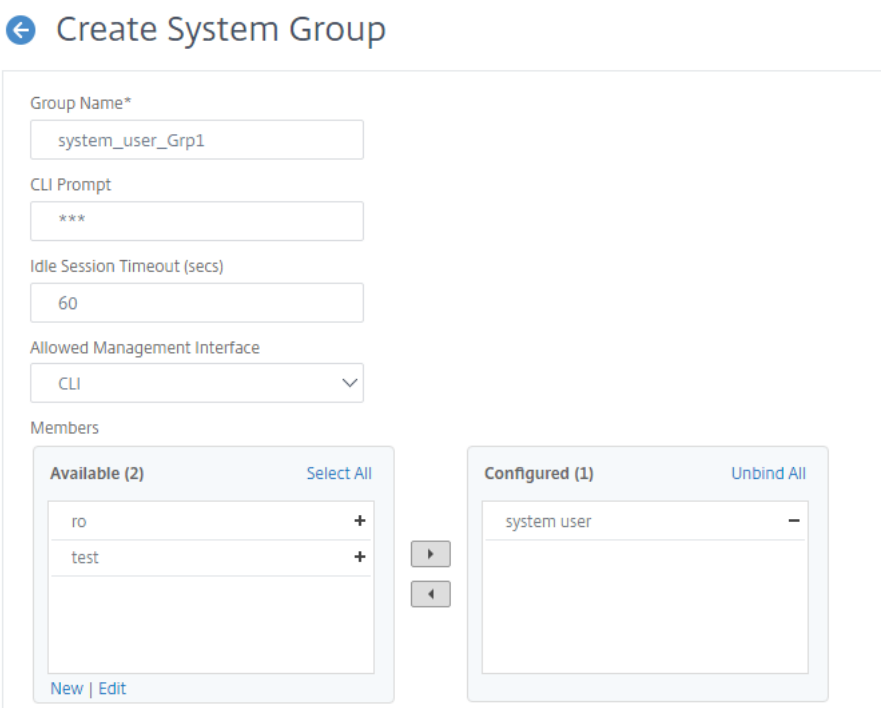
- `bind system group <groupName> -userName <userName>`
- `show system group <groupName>`

Ejemplo:

```
> bind system group Managers -userName user1
```

Configurar un grupo de usuarios mediante la GUI de Citrix ADC

1. Vaya a **Sistema** > **Administración de usuarios** > **Grupos** y cree el grupo de usuarios.
2. En el panel de detalles, haga clic en **Agregar** para crear un grupo de usuarios del sistema.
3. En la página **Crear Grupo de Sistemas**, defina los siguientes parámetros:
   a) Nombre del grupo. Nombre del grupo de usuarios.
   b) Indicador de CLI. El mensaje que prefiere establecer para el acceso a la interfaz CLI.
   c) Tiempo de espera de sesión inactiva (segundos). Establezca la cantidad de tiempo que un usuario puede estar inactivo antes de que se agote el tiempo de espera y cierre la sesión.
   d) Interfaz de administración permitida. Seleccione las interfaces de Citrix ADC a las que se concede permiso para acceder al grupo de usuarios.
   e) Miembros. Agregue cuentas de usuario al grupo.
   f) Directivas de comando. Enlazar directivas de comandos al grupo de usuarios.
   g) Particiones. Enlazar particiones al grupo de usuarios.
4. Haga clic en **Crear** y **cerrar**.



Nota:

Para agregar miembros al grupo, en la sección Miembros, haga clic en **Agregar**. Seleccione usuarios de la lista Disponibles y agréguelos a la lista Configurado.

Configurar directivas de comandos

Las directivas de comandos regulan qué comandos, grupos de comandos, servidores virtuales y otras entidades que los usuarios y grupos de usuarios pueden utilizar.

El dispositivo proporciona un conjunto de directivas de comandos integradas y puede configurar directivas personalizadas. Para aplicar las directivas, las vincula a usuarios o grupos.

Estos son los puntos clave a tener en cuenta al definir y aplicar directivas de comando.

- No se pueden crear directivas de comandos globales. Las directivas de comandos deben vincularse directamente a los usuarios y grupos del dispositivo.
- Los usuarios o grupos sin directivas de comandos asociadas están sujetos a la directiva de comandos predeterminada (DENY-ALL) y, por lo tanto, no pueden ejecutar ningún comando de configuración hasta que las directivas de comandos adecuadas estén enlazadas a sus cuentas.
- Todos los usuarios heredan las directivas de los grupos a los que pertenecen.
- Debe asignar una prioridad a una directiva de comandos cuando la vincule a una cuenta de usuario o a una cuenta de grupo. Esto permite al dispositivo determinar qué directiva tiene prioridad cuando dos o más directivas conflictivas se aplican al mismo usuario o grupo.

- Los siguientes comandos están disponibles de forma predeterminada para cualquier usuario y no se ven afectados por ningún comando que especifique:
- ayuda, mostrar atributo CLI, establecer símbolo de CLI, borrar símbolo de CLI, mostrar indicador de CLI, alias, desalias, historial, salir, whoami, config, establecer el modo CLI, unset CLI modo y mostrar el modo CLI.

En la tabla siguiente se describen las directivas integradas.

Nombre de directiva	Permite
solo lectura	Acceso de solo lectura a todos los comandos show excepto show ns runningConfig, show ns ns.conf y los comandos show para el grupo de comandos de Citrix ADC.
operator	Acceso de solo lectura y acceso a comandos para habilitar e inhabilitar servicios y servidores.
red	Acceso total, excepto a los comandos set y unset SSL, show ns ns.conf, show ns runningConfig y show gslb runningConfig.
administrador del sistema	[Incluido en Citrix ADC 12.0 y versiones posteriores] Un administrador del sistema es inferior a un superusuario si se permiten los términos de acceso en el dispositivo. Un usuario sysadmin puede realizar todas las operaciones de Citrix ADC con las siguientes excepciones: No tiene acceso al shell Citrix ADC, no puede realizar configuraciones de usuario, no puede realizar configuraciones de partición y algunas otras configuraciones como se indica en la directiva de comandos sysadmin.
superusuario	Acceso completo. Los mismos privilegios que el usuario nsroot.

Crear directivas de comandos personalizadas

Se ofrece compatibilidad con expresiones regulares para usuarios con recursos para mantener expresiones más personalizadas y para aquellas implementaciones que requieren la flexibilidad que ofre-

cen las expresiones regulares. Para la mayoría de los usuarios, las directivas de comando integradas son suficientes. Los usuarios que necesitan más niveles de control pero no están familiarizados con las expresiones regulares pueden querer usar solo expresiones simples, como las de los ejemplos proporcionados en esta sección, para mantener la legibilidad de las directivas.

Cuando utilice una expresión regular para crear una directiva de comandos, tenga en cuenta lo siguiente.

- Cuando se utilizan expresiones regulares para definir comandos que se ven afectados por una directiva de comandos, debe incluir los comandos entre comillas dobles. Por ejemplo, para crear una directiva de comandos que incluya todos los comandos que comiencen por show, escriba lo siguiente:
- "^mostrar. *$"
- Para crear una directiva de comandos que incluya todos los comandos que comiencen por rm, escriba lo siguiente:
- "^rm. *$"
- Las expresiones regulares utilizadas en las directivas de comando no distinguen entre mayúsculas y minúsculas.

En la tabla siguiente se enumeran ejemplos de expresiones regulares para Directivas de comandos:

Especificación de comandos	Coincide con estos comandos
"^rms+. *$"	Todas las acciones de eliminación, ya que todas las acciones de eliminación comienzan con la cadena rm, seguida de un espacio y más parámetros como grupos de comandos, tipos de objeto de comando y argumentos.
"^muestra+. *$"	Todos los comandos show, ya que todas las acciones show comienzan con la cadena show, seguido de un espacio y más parámetros como grupos de comandos, tipos de objeto de comando y argumentos.
"^shell$"	El comando shell solo, pero no combinado con ningún parámetro adicional, como grupos de comandos, tipos de objeto de comando y argumentos.

Especificación de comandos	Coincide con estos comandos
“^adds+vservers+. *$”	Todos crean acciones de servidor virtual, que consisten en agregar comando servidor virtual seguido de un espacio y más parámetros como grupos de comandos, tipos de objeto de comando y argumentos.
“^adds+ (lbs+vserver) s+. *”	Todos crean acciones de servidor virtual lb, que consisten en el comando add lb virtual server seguido de un espacio y más parámetros como grupos de comandos, tipos de objeto de comando y argumentos.

Para obtener información sobre las directivas de comandos integradas, consulte la tabla Tabla de directivas de comandos incorporada .

Para crear una directiva de comandos mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para crear una directiva de comandos y verificar la configuración:

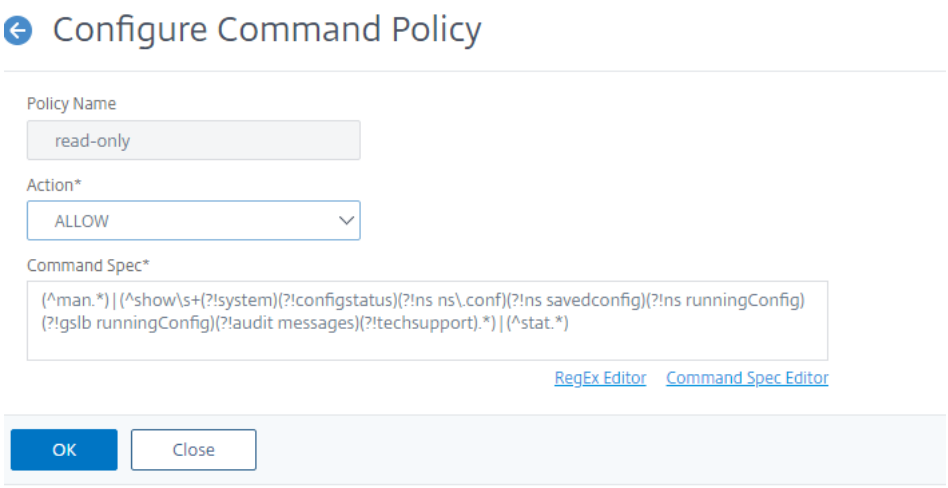
- `add system cmdPolicy <policyname> <action> <cmdspec>`
- `show system cmdPolicy <policyName>`

Ejemplo:

```
add system cmdPolicy USER-POLICY ALLOW (\ server\ )|(\ service(Group)*\ )
|(\ vserver\ )|(\ policy\ )|(\ policylabel\ )|(\ limitIdentifier\ )|(^show\
 (?!(system|ns\ (ns.conf|runningConfig)))|(save)|(stat\ .*serv)
```

Configurar una directiva de comandos mediante la GUI de Citrix ADC

1. Vaya a **Sistema** > **Administración de usuarios** > **Directivas de comandos**.
2. En el panel de detalles, haga clic en **Agregar** para crear una nueva directiva de comandos.
3. En la página **Configurar directiva de comandos**, establezca los siguientes parámetros:
   a) Nombre de directiva
   b) Action
   c) Especificación del comando.
4. Haga clic en **Aceptar**.



Vincular directivas de comandos a cuentas de usuario y grupos de usuarios

Una vez que haya definido las directivas de comandos, debe vincularlas a las cuentas de usuario y grupos apropiados. Cuando vincule una directiva, debe asignarle una prioridad para que el dispositivo pueda determinar qué directiva de comandos debe seguir cuando dos o más directivas de comandos aplicables estén en conflicto.

Las directivas de comando se evalúan en el siguiente orden:

- Las directivas de comandos enlazadas directamente a los usuarios y a los grupos correspondientes se evalúan según un número de prioridad. Una directiva de comando con un número de prioridad inferior se evalúa antes que una con un número de prioridad mayor. Por lo tanto, los privilegios que la directiva de comandos con números inferiores concede o deniega explícitamente no se anulan por una directiva de comandos con números superiores.
- Cuando dos directivas de comando, una vinculada a una cuenta de usuario y otra a un grupo, tienen el mismo número de prioridad, la directiva de comandos vinculada directamente a la cuenta de usuario se evalúa primero.

Para enlazar directivas de comandos a un usuario mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para enlazar una directiva de comandos a un usuario y verificar la configuración:

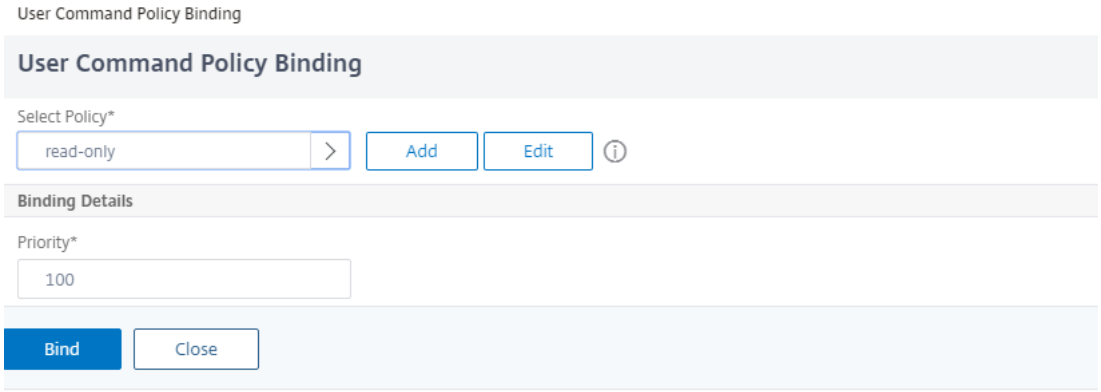
- `bind system user <userName> -policyName <policyName> <priority>`
- `show system user <userName>`

Ejemplo:

```
> bind system user user1 -policyName read_all 1
```


Vincular directivas de comandos a una cuenta de usuario mediante la GUI de Citrix ADC

Vaya a **Sistema** > **Administración** de **usuarios > Usuarios**, seleccione el usuario y enlazar directivas de comandos.



Opcionalmente, puede modificar la prioridad predeterminada para asegurarse de que la directiva se evalúa en el orden adecuado.

Para enlazar directivas de comandos a un grupo mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para enlazar una directiva de comandos a un grupo de usuarios y compruebe la configuración:

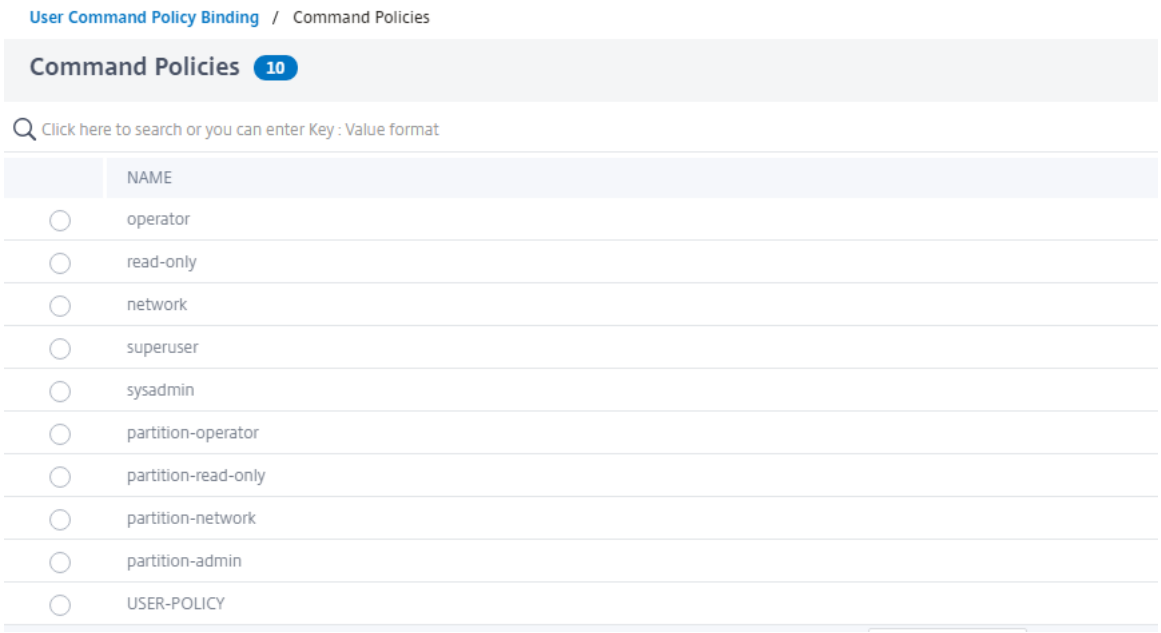
- `bind system group <groupName> -policyName <policyName> <priority>`
- `show system group <groupName>`

Ejemplo:

```
> bind system group Managers -policyName read_all 1
```

Vincular directivas de comandos a un grupo de usuarios mediante la GUI de Citrix ADC

Vaya a **Sistema** > **Administración de usuarios** > **Grupos**, seleccione el grupo y enlazar directivas de comando.



Opcionalmente, puede modificar la prioridad predeterminada para asegurarse de que la directiva se evalúa en el orden adecuado.

Ejemplo de caso de uso: Administrar cuentas de usuario, grupos de usuarios y directivas de comandos en una organización de fabricación

En el ejemplo siguiente se muestra cómo crear un conjunto completo de cuentas de usuario, grupos y directivas de comandos y vincular cada directiva a los grupos y usuarios adecuados. La empresa, Example Manufacturing, Inc., tiene tres usuarios que pueden acceder al dispositivo Citrix ADC:

- **John Doe.** El gerente de TI. John debe poder ver todas las partes de la configuración de Citrix ADC, pero no necesita modificar nada.
- **María Ramiez.** El administrador de TI principal. Maria debe poder ver y modificar todas las partes de la configuración de Citrix ADC excepto los comandos de Citrix ADC (los dictados de las directivas locales deben ejecutarse mientras inicia sesión como nsroot).
- **Michael Baldrock.** El administrador de TI encargado del equilibrio de carga. Michael debe poder ver todas las partes de la configuración de Citrix ADC, pero debe modificar únicamente las funciones de equilibrio de carga.

En la tabla siguiente se muestra el desglose de la información de red, los nombres de cuentas de usuario, los nombres de grupos y las directivas de comandos de la compañía de ejemplo.

Campo	Valor	Nota
Nombre de host de Citrix ADC	ns01.ejemplo.net	N/D

Campo	Valor	Nota
Cuentas de usuario	johnd, mariar y michaelb	John Doe, gerente de TI, Maria Ramírez, administrador de TI e Michael Baldrock, administrador de TI.
Grupos	Administradores y sistemas	Todos los administradores y todos los administradores de TI.
Directivas de comandos	read_all, modify_lb y modify_all	Permitir acceso completo de solo lectura, Permitir acceso de modificación al equilibrio de carga y Permitir acceso de modificación completo.

La siguiente descripción le guía por el proceso de creación de un conjunto completo de cuentas de usuario, grupos y directivas de comandos en el dispositivo Citrix ADC denominado ns01.example.net.

La descripción incluye procedimientos para vincular las cuentas de usuario y los grupos apropiados entre sí, y vincular las directivas de comando adecuadas a las cuentas y grupos de usuario.

En este ejemplo se ilustra cómo puede utilizar la priorización para conceder acceso y privilegios precisos a cada usuario del departamento de TI.

En el ejemplo se supone que la instalación y configuración iniciales ya se han realizado en Citrix ADC.

Configurar cuentas de usuario, grupos y directivas de comandos para una organización de ejemplo

1. Utilice el procedimiento descrito en la sección Configuración de cuentas de usuario para crear cuentas de usuario **johnd**, **mariar** y **michaelb**.
2. Utilice el procedimiento descrito en Configuración de grupos de usuarios para crear grupos de usuarios **Administradores** y **SysOP** y, a continuación, vincular los usuarios **mariar** y **michaelb** al grupo **SysOPS** y el usuario **johnd** al Grupo **de gerentes**.
3. Utilice el procedimiento descrito en Creación de directivas de comandos personalizadas para crear las siguientes directivas de comandos:
   - **read_all** con acción **Permitir** y especificación”`(^show\s+(?!system)(?!ns ns.conf )(?!ns runningConfig).*)|(^stat.*)`” de comandos
   - **modify_lb** con la acción como **Permitir** y la especificación”`^set\s+lb\s+.*$`” del comando

- modify_all con la acción como Permitir y la especificación”^\S+\s+(?!system).*”del comando

4. Utilice el procedimiento descrito en “Vinculación de directivas de comandos a usuarios y grupos” para vincular la directiva de comandos **read_all** al grupo **SysOPs**, con el valor de prioridad **1**.
5. Utilice el procedimiento descrito en “Vinculación de directivas de comandos a usuarios y grupos” para vincular la directiva de comandos **modify_lb** al usuario **michaelb**, con un valor de prioridad **5**.

La configuración que acaba de crear resulta en lo siguiente:

- John Doe, el administrador de TI, tiene acceso de solo lectura a toda la configuración de Citrix ADC, pero no puede realizar modificaciones.
- María Ramírez, responsable de TI, tiene acceso casi completo a todas las áreas de la configuración de Citrix ADC, y solo tiene que iniciar sesión para ejecutar comandos a nivel de Citrix ADC.
- Michael Baldrock, el administrador de TI responsable del equilibrio de carga, tiene acceso de solo lectura a la configuración de Citrix ADC y puede modificar las opciones de configuración para el equilibrio de carga.

El conjunto de directivas de comandos que se aplica a un usuario específico es una combinación de directivas de comandos aplicadas directamente a la cuenta del usuario y directivas de comandos aplicadas a uno o varios grupos de los que el usuario es miembro.

Cada vez que un usuario introduce un comando, el sistema operativo busca las directivas de comando para ese usuario hasta que encuentre una directiva con una acción Permitir o DENAR que coincida con el comando. Cuando encuentra una coincidencia, el sistema operativo detiene su búsqueda de directivas de comandos y permite o deniega el acceso al comando.

Si el sistema operativo no encuentra ninguna directiva de comandos coincidente, deniega al usuario el acceso al comando, de acuerdo con la directiva de denegación predeterminada del dispositivo Citrix ADC.

> **Nota:**
>
> Al colocar un usuario en varios grupos, tenga cuidado de no causar restricciones o privilegios de comandos de usuario no deseados. Para evitar estos conflictos, al organizar los usuarios en grupos, tenga en cuenta el procedimiento de búsqueda de directivas de comandos de Citrix ADC y las reglas de ordenación de directivas.

Gestión de cuentas de usuario y contraseñas

August 20, 2021

Citrix ADC le permite administrar cuentas de usuario y configuración de contraseñas. A continuación se indican algunas de las actividades que puede realizar para una cuenta de usuario del sistema o una cuenta de usuario `nsroot` administrativo en el dispositivo.

- Bloqueo de cuentas de usuario del sistema
- Bloquear cuenta de usuario del sistema para acceder a la administración
- Desbloquear una cuenta de usuario del sistema bloqueada para acceder a la administración
- Inhabilitar el acceso a la administración para la cuenta de usuario
- Forzar cambio de contraseña para usuarios `nsroot` administrativos
- Quitar archivos confidenciales de una cuenta de usuario del sistema
- Configuración segura de contraseñas para usuarios del sistema

Bloqueo de cuentas de usuario del sistema

Para evitar ataques de seguridad por fuerza bruta, puede configurar la configuración de bloqueo del usuario. La configuración permite que un administrador de red impida que un usuario del sistema inicie sesión en un dispositivo Citrix ADC. Y también desbloquea la cuenta de usuario antes de que caduque el periodo de bloqueo.

En el símbolo del sistema, escriba:

```
set aaa parameter -maxloginAttempts <value> -failedLoginTimeout <value> -
persistentLoginAttempts (ENABLED | DISABLED)
```

> **Nota**
>
> El parámetro “PersistentLoginIntts” debe estar ENABLED para obtener los detalles del almacenamiento persistente de intentos de inicio de sesión de usuario fallidos.

Ejemplo:

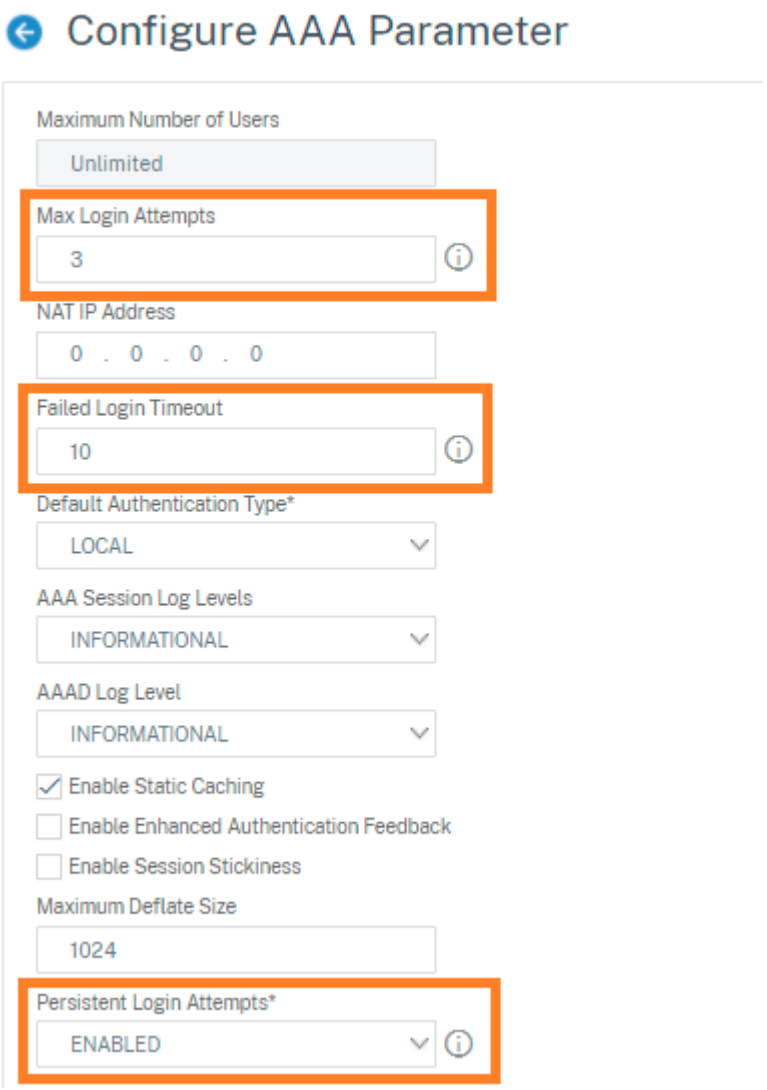
```
set aaa parameter -maxloginAttempts 3 -failedLoginTimeout 10 -persistentLoginAttempts
 ENABLED
```

Configurar el bloqueo de cuentas de usuario del sistema mediante la GUI

1. Vaya a **Configuración > Seguridad > Tráfico de aplicaciones AAA > Configuración de autenticación > Cambiar configuración AAA de autenticación**.
2. En la página **Configurar Parámetro AAA**, defina los siguientes parámetros:

a) Intentos de inicio de sesión máximo. El número máximo de intentos de inicio de sesión permitidos para que el usuario lo intente.
b) Error de tiempo de espera de inicio de sesión Número máximo de intentos de inicio de sesión no válidos por parte del usuario.
c) Intentos de inicio de sesión persistentes Almacenamiento persistente de intentos de inicio de sesión de usuario fallidos.

3. Haga clic en **Aceptar**.



Cuando establece los parámetros, la cuenta de usuario se bloquea durante 10 minutos para tres o más intentos de inicio de sesión no válidos. Además, el usuario no puede iniciar sesión incluso con credenciales válidas durante 10 minutos.

> **Nota**
>
> Si un usuario bloqueado intenta iniciar sesión en el dispositivo, aparece un mensaje de error


```
RBA Authentication Failure: maxlogin attempt reached for test..
```

Bloquear cuenta de usuario del sistema para acceder a la administración

El dispositivo Citrix ADC le permite bloquear a un usuario del sistema durante 24 horas y denegar el acceso al usuario.

El dispositivo Citrix ADC admite la configuración tanto para usuarios del sistema como para usuarios externos.

> **Nota**
>
> La función solo se admite si inhabilita la opción `persistentLoginAttempts` en el parámetro `aaa`.

En el símbolo del sistema, escriba:

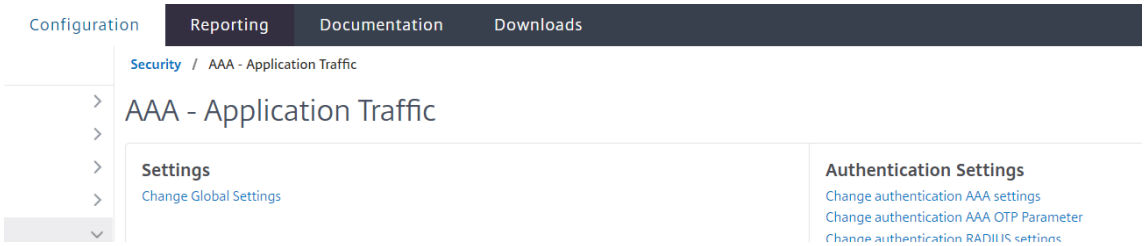
```
set aaa parameter -persistentLoginAttempts DISABLED
```

Ahora, para bloquear una cuenta de usuario, en el símbolo del sistema, escriba:

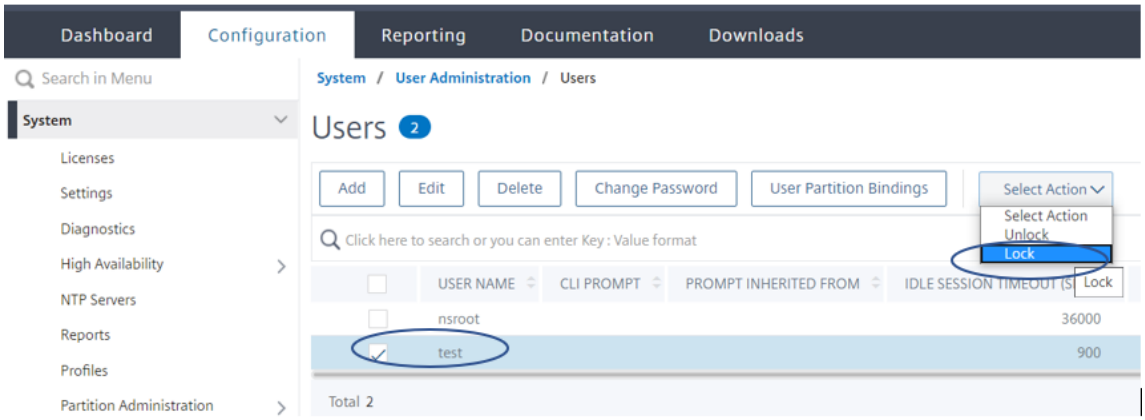
```
lock aaa user test
```

Bloquear una cuenta de usuario del sistema mediante la GUI

1. Vaya a **Configuración > Seguridad > Tráfico de aplicaciones AAA > Configuración de autenticación > Cambiar configuración AAA de autenticación**.



2. En **Configurar parámetro AAA**, en la lista **Intentos de inicio de sesión persistentes**, seleccione **INHABILITADO**.
3. Vaya a **Sistema > Administración de usuarios > Usuarios**.
4. Seleccione un usuario.
5. En la lista Seleccionar acción, seleccione **Bloquear**.



> **Nota**
>
> La GUI de Citrix ADC no tiene la opción de bloquear usuarios externos. Para bloquear un usuario externo, el administrador de ADC debe usar la CLI.
> Cuando un usuario del sistema bloqueado (bloqueado con el comando de usuario de autenticación de bloqueo, autorización y auditoría) intenta iniciar sesión en Citrix ADC, el dispositivo muestra un mensaje de error "Error de autenticación de RBA: prueba de usuario está bloqueada durante 24 horas".
>
> Cuando un usuario está bloqueado para iniciar sesión en el acceso de administración, el acceso a la consola está exento. El usuario bloqueado puede iniciar sesión en la consola.

Desbloquear una cuenta de usuario del sistema bloqueada para acceder a la administración

Los usuarios del sistema y los usuarios externos pueden bloquearse durante 24 horas mediante el comando de usuario de autenticación, autorización y auditoría de bloqueo.

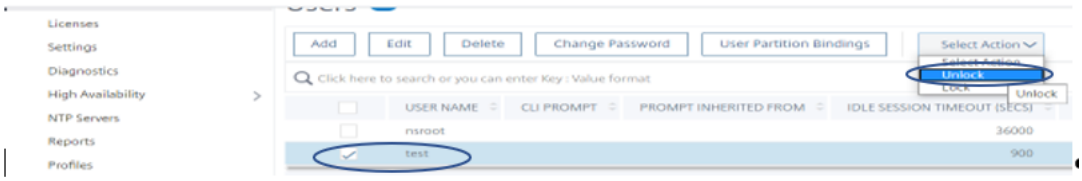
> **Nota**
>
> El dispositivo ADC permite a los administradores desbloquear al usuario bloqueado y la función no requiere ninguna configuración en el comando "PersistentLoginIntts".

En el símbolo del sistema, escriba:

```
unlock aaa user test
```

Configurar el desbloqueo del usuario del sistema mediante la GUI

1. Vaya a **Sistema > Administración de usuarios > Usuarios**.
2. Seleccione un usuario.
3. Haga clic en **Desbloquear**.



La GUI de Citrix ADC solo enumera los usuarios del sistema creados en el ADC, por lo que no hay opción en la GUI para desbloquear usuarios externos. Para desbloquear un usuario externo, el `nsroot` administrador debe usar la CLI.

Inhabilitar el acceso a la administración para la cuenta de usuario

Cuando la autenticación externa está configurada en el dispositivo y, como administrador, prefiere denegar el acceso a los usuarios del sistema para iniciar sesión en el acceso de administración, debe inhabilitar la opción LocalAuth en el parámetro del sistema.

En el símbolo del sistema, escriba lo siguiente:

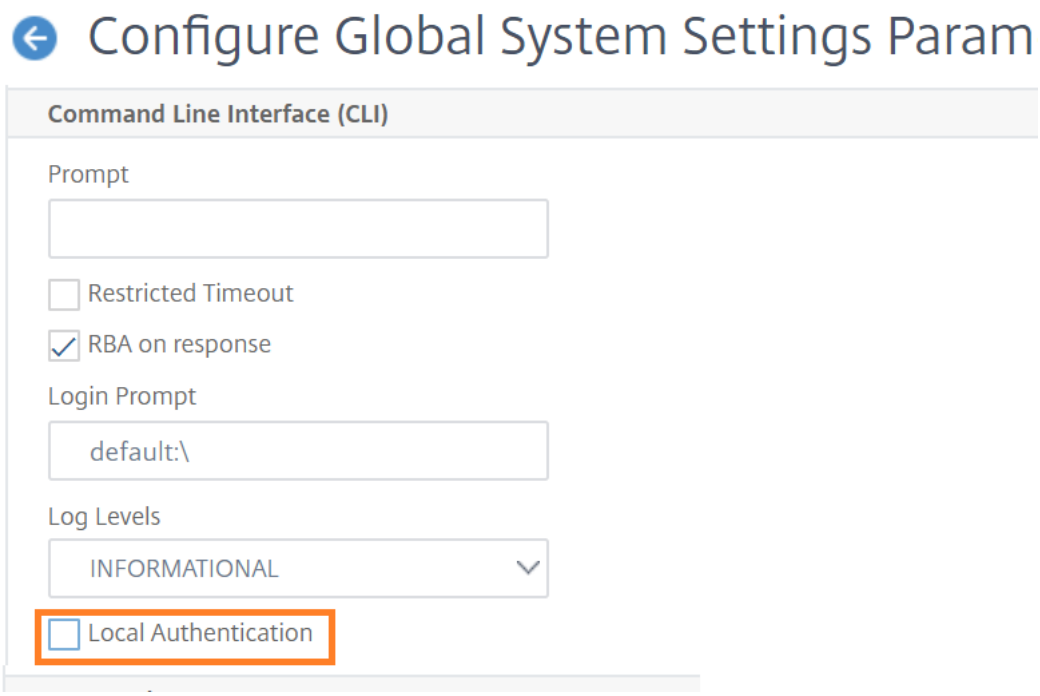
```
set system parameter localAuth <ENABLED|DISABLED>
```

Ejemplo:

```
set system parameter localAuth DISABLED
```

Inhabilitar el acceso de administración al usuario del sistema mediante la GUI

1. Vaya a **Configuración > Sistema > Configuración > Cambiar la configuración global del sistema**.
2. En la sección **Interfaz de línea de comandos (CLI)**, desactive la casilla **Autenticación local**.



Al inhabilitar la opción, los usuarios del sistema local no pueden iniciar sesión en el acceso de administración de ADC.

> **Nota**
>
> El servidor de autenticación externo debe estar configurado y accesible para no permitir la autenticación de usuario del sistema local en el parámetro del sistema. Si no se puede acceder al servidor externo configurado en ADC para el acceso de administración, los usuarios del sistema local pueden iniciar sesión en el dispositivo. El comportamiento se configura para fines de recuperación.

Forzar cambio de contraseña para usuarios administrativos

Para la autenticación`nsroot` segura, el dispositivo Citrix ADC solicita al usuario que cambie la contraseña predeterminada a una nueva si la `forcePasswordChange` opción está habilitada en el parámetro del sistema. Puede cambiar su `nsroot` contraseña desde CLI o GUI, en su primer inicio de sesión con las credenciales predeterminadas.

En el símbolo del sistema, escriba:

```
set system parameter -forcePasswordChange ( ENABLED | DISABLED )
```

Ejemplo de sesión SSH para NSIP:

```
1 ssh nsroot@1.1.1.1
```



```
Connecting to 1.1.1.1:22...
Connection established.
To escape to local shell, press Ctrl+Alt+].
###############################################################################

WARNING: Access to this system is for authorized users only #
Disconnect IMMEDIATELY if you are not an authorized user! #

###############################################################################

Please change the default NSROOT password.
Enter new password:
Please re-enter your password:
Done
<!--NeedCopy-->
```

Quitar archivos confidenciales de una cuenta de usuario del sistema

Para administrar datos confidenciales como claves autorizadas y claves públicas para una cuenta de usuario del sistema, debe habilitar la `removeSensitiveFiles` opción. Los comandos que eliminan archivos confidenciales cuando se habilita el parámetro del sistema son:

- rm cluster instance
- rm cluster node
- nodo de alta disponibilidad de rm
- borrar configuración completa
- unir clúster
- add cluster instance

En el símbolo del sistema, escriba:

```
set system parameter removeSensitiveFiles ( ENABLED | DISABLED )
```

Ejemplo:

```
set system parameter -removeSensitiveFiles ENABLED
```

Configuración segura de contraseñas para usuarios del sistema

Para la autenticación segura, el dispositivo Citrix ADC pide a los usuarios y administradores del sistema que establezcan contraseñas seguras para iniciar sesión en el dispositivo. La contraseña debe ser larga y debe ser una combinación de:

- Un carácter minúscula
- Un carácter mayúscula

- Un carácter numérico
- Un carácter especial

En el símbolo del sistema, escriba:

```
set system parameter -strongpassword <value> -minpasswordlen <value>
```

Donde:

`Strongpassword`. Después de habilitar la contraseña segura (`enable all` / `enablelocal`), todas las contraseñas o información confidencial deben tener lo siguiente:

- Al menos 1 carácter minúscula
- Al menos 1 carácter mayúscula
- Al menos 1 carácter numérico
- Al menos 1 carácter especial

Excluir la lista en `enablelocal` es - `NS_FIPS`, `NS_CRL`, `NS_RSAKEY`, `NS_PKCS12`, NS_PKCS8, NS_LDAP, `NS_TACACS`, `NS_TACACSACTION`, `NS_RADIUS`, `NS_RADIUSACTION`, `NS_ENCRYPTION_PARAMS`. Por lo tanto, no se realizan comprobaciones de contraseña segura en estos comandos ObjectType para el usuario del sistema.

Valores posibles: `enableall`, `enablelocal`, disabled
Valor predeterminado: disabled

`minpasswordlen`. Longitud mínima de la contraseña de usuario del sistema. Cuando la contraseña segura está habilitada de forma predeterminada, la longitud mínima es 4. El valor introducido por el usuario puede ser mayor o igual a 4. El valor mínimo predeterminado es 1 cuando la contraseña segura está inhabilitada. El valor máximo es 127 en ambos casos.

Valor mínimo: 1 Valor
máximo: 127

Ejemplo:

```
set system parameter -strongpassword enablelocal -minpasswordlen 6
```

Cuenta de usuario predeterminada

El administrador puede utilizar la cuenta de `nsrecover` usuario para recuperar el dispositivo Citrix ADC. Puede iniciar sesión en el dispositivo ADC `nsrecover` si los usuarios predeterminados del sistema (`nsroot`) no pueden iniciar sesión debido a problemas imprevistos. El `nsrecover` inicio de sesión es independiente de las configuraciones del usuario y le permite acceder directamente al mensaje del shell. Siempre se le permite iniciar sesión a través de `nsrecover` independientemente del límite máximo de configuración que se alcance.

Cómo restablecer la contraseña de administrador raíz (nsroot)

June 2, 2022

La cuenta de administrador raíz (`nsroot`) de Citrix ADC proporciona acceso completo a todas las funciones de ADC. Por lo tanto, para preservar la seguridad, la cuenta administrativa solo debe utilizarse si es necesario.

Como administrador, la recomendación es cambiar la contraseña. Si olvida su contraseña, primero debe restablecerla a la predeterminada y luego cambiarla a una nueva contraseña.

Como administrador `nsroot`, para restablecer la contraseña, debe iniciar sesión en el dispositivo y cambiarla. Sin embargo, si no recuerda la contraseña, puede reiniciar el dispositivo en modo de usuario único. Monte el sistema de archivos en modo de lectura/escritura y, a continuación, quite la entrada **Citrix ADC** del archivo ns.conf. Como último paso, reinicie e inicie sesión en el dispositivo con la predeterminada y, a continuación, establezca una nueva contraseña.

Complete los siguientes pasos para restablecer la contraseña de administrador raíz:

1. Conecte un equipo al puerto de consola del Citrix ADC e inicie sesión.

   > **Nota**
   >
   > No puede iniciar sesión mediante SSH para realizar este procedimiento; debe conectarse directamente al dispositivo.

2. Reinicie Citrix ADC.
3. Presione CTRL+C cuando aparezca el siguiente mensaje:

   ```
   Press [Ctrl-C] for command prompt, or any other key to boot immediately
   .
   Booting [kernel] in ## seconds.
   ```

   > **Nota**
   >
   > En una consola serie de Azure, el dispositivo Citrix ADC no admite un solo arranque hasta que se inicia el dispositivo ADC.

4. Ejecute el siguiente comando para iniciar Citrix ADC en un modo de usuario único:
   `boot -s`

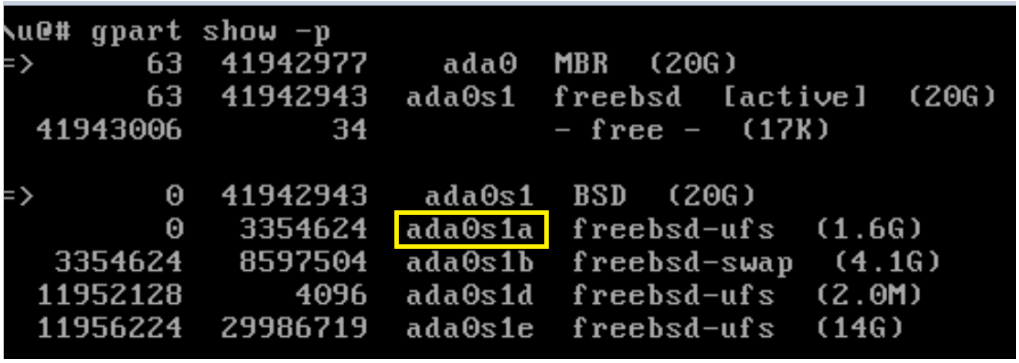
   Una vez arrancada el dispositivo, muestra el siguiente mensaje:

   Introduzca el nombre de ruta completo del shell o `RETURN for /bin/sh:`

5. Presione ENTRAR para mostrar el mensaje # y escriba los siguientes comandos para montar los sistemas de archivos:

a) Ejecute el siguiente comando para comprobar la coherencia del disco:

```
fsck_ufs /dev/ad0s1a
```

> **Nota**
>
> La unidad flash tiene un nombre de dispositivo específico según su Citrix ADC. Ejecute el siguiente comando en la CLI de ADC y copie el nombre que termina en "1a. "
>
> ```
> gpart show -p
> ```
>
> Por ejemplo,
>
> 
>

b) Acceda al directorio de desarrollo e introduzca 'ls' para comprobar los detalles de la unidad.

c) Ejecute el siguiente comando para mostrar las particiones montadas:

```
df
```

> **Nota**
>
> Si la partición flash no aparece en la lista, debe montarla manualmente.

d) Ejecute el siguiente comando para montar la unidad flash:

```
mount /dev/ad0s1a /flash
```

6. Ejecute el siguiente comando para cambiar al directorio `nsconfig`:

```
cd /flash/nsconfig
```

7. Ejecute los siguientes comandos para reescribir el archivo ns.conf y eliminar el conjunto de comandos del sistema por defecto para el administrador:

a) Ejecute el siguiente comando para crear un archivo de configuración que no tenga comandos predeterminados para el administrador:

```
grep -v "set system user nsroot" ns.conf > new.conf
```

b) Ejecute el siguiente comando para hacer una copia de seguridad del archivo de configuración existente:


```
mv ns.conf old.ns.conf
```

c) Ejecute el siguiente comando para cambiar el nombre del nuevo archivo .conf a ns.conf:

```
mv new.conf ns.conf
```

8. Ejecute el siguiente comando para reiniciar Citrix ADC:

```
reboot
```

9. Inicie sesión con las credenciales de administrador predeterminadas.
10. Ejecute el siguiente comando para restablecer la contraseña de administrador:

```
set system user nsroot <New_Password>
```

> **Nota**
>
> Para usar el carácter "?" en una cadena de contraseña, precede a este carácter por el carácter \.

Por ejemplo, `yourexamplepasswd?` se establece para la cuenta de administrador después de realizar la siguiente operación:

```
> set system user nsroot yourexamplepasswd\?
```

> **Nota**
>
> Para restablecer una contraseña olvidada (`nsroot`) en una configuración de alta disponibilidad, Citrix recomienda apagar el nodo de pares. Si el nodo del mismo nivel está activo, la contraseña se sobrescribe, ya que la sincronización de configuración se activa cuando el nodo aparece después del reinicio.

Además, lea el artículo de Citrix, CTX224027 para saber cómo funciona el acceso SSH seguro al dispositivo Citrix ADC.

Autenticación externa

August 11, 2022

El servicio de autenticación en un dispositivo Citrix ADC puede ser local o externo. En la autenticación de usuarios externos, el dispositivo utiliza un servidor externo, como LDAP, RADIUS o TACACS+, para autenticar al usuario. Para autenticar a un usuario externo y concederle acceso al dispositivo, debe aplicar una directiva de autenticación. La autenticación del sistema Citrix ADC utiliza directivas de autenticación avanzada con expresiones de directiva avanzadas. Las directivas de autenticación avanzada también se utilizan para la administración de usuarios del sistema en un dispositivo Citrix ADC con particiones.

> **Nota**
>
> Si el dispositivo sigue mediante directivas clásicas y sus expresiones, debe dejar de utilizarlas y migrar el uso de directivas clásicas a la infraestructura de directivas avanzadas.

Una vez que haya creado una directiva de autenticación, debe vincularla a la entidad global del sistema. Puede configurar un servidor de autenticación externo (por ejemplo, TACACS) vinculando una única directiva de autenticación a la entidad global del sistema. O bien, puede configurar una cascada de servidores de autenticación vinculando varias directivas a la entidad global del sistema.

> **Nota**
>
> Cuando un usuario externo inicia sesión en el dispositivo, el sistema genera un mensaje de error "El usuario no existe" en el archivo `ns.log`. Esto se debe a que el sistema ejecuta el comando systemuser_systemcmdpolicy_binding para inicializar la GUI del usuario.

Autenticación LDAP (mediante servidores LDAP externos)

Puede configurar el dispositivo Citrix ADC para autenticar el acceso de los usuarios con uno o más servidores LDAP. La autorización LDAP requiere nombres de grupo idénticos en Active Directory, en el servidor LDAP y en el dispositivo. Los caracteres y mayúsculas también deben ser los mismos.

Para obtener más información sobre las directivas de autenticación LDAP, consulte el tema Directivas de autenticación LDAP.

De forma predeterminada, la autenticación LDAP se protege mediante el protocolo SSL/TLS. Existen dos tipos de conexiones LDAP seguras. En el primer tipo, el servidor LDAP acepta la conexión SSL/TLS en un puerto independiente del puerto utilizado para aceptar conexiones LDAP claras. Después de que los usuarios establezcan la conexión SSL/TLS, el tráfico LDAP se puede enviar a través de la conexión. El segundo tipo permite conexiones LDAP no seguras y no seguras y el puerto único lo gestiona en el servidor. En este caso, para crear una conexión segura, el cliente establece primero una conexión LDAP clara. A continuación, el comando **LDAP** StartTLS se envía al servidor a través de la conexión. Si el servidor LDAP admite StartTLS, la conexión se convierte en una conexión LDAP segura mediante TLS.

Los números de puerto de las conexiones LDAP son:

- 389 para conexiones LDAP no seguras
- 636 para conexiones LDAP seguras
- 3268 para conexiones LDAP no seguras de Microsoft
- 3269 para conexiones LDAP seguras de Microsoft

Las conexiones LDAP que utilizan el comando StartTLS utilizan el número de puerto 389. Si los números de puerto 389 o 3268 están configurados en el dispositivo, intenta utilizar StartTLS para

establecer la conexión. Si se utiliza cualquier otro número de puerto, los intentos de conexión utilizan SSL/TLS. Si no se puede usar StartTLS o SSL/TLS, se produce un error en la conexión.

Al configurar el servidor LDAP, las mayúsculas y minúsculas de los caracteres alfabéticos deben coincidir con las del servidor y del dispositivo. Si se especifica el directorio raíz del servidor LDAP, también se buscará en todos los subdirectorios para encontrar el atributo de usuario. En directorios grandes, puede afectar al rendimiento. Por este motivo, Citrix recomienda utilizar una unidad organizativa (OU) específica.

En la tabla siguiente se muestran ejemplos del nombre distintivo (DN) base.

Servidor LDAP	DN base
Microsoft Active Directory	DC=Citrix, DC=local
Directorio electrónico de Novell	dc=Citrix, dc=net
Servidor IBM Directory	cn=usuarios
Lotus Domino	OU=City, O=Citrix, C=US
Directorio Sun ONE (anteriormente iPlanet)	ou=People, dc=Citrix, dc=com

La siguiente tabla muestra ejemplos del nombre distintivo (DN) de enlace.

Servidor LDAP	Vincular DN
Microsoft Active Directory	CN=Administrator, CN=Users, DC=Citrix, DC=local
Directorio electrónico de Novell	cn=admin, dc=Citrix, dc=net
Servidor IBM Directory	LDAP_dn
Lotus Domino	CN=Notes Administrator, O=Citrix, C=US
Directorio Sun ONE (anteriormente iPlanet)	uid=admin, ou=Administrators, ou=TopologyManagement, o=NetscapeRoot

Servidor LDAP	Vincular DN
Microsoft Active Directory	CN=Administrator, CN=Users, DC=Citrix, DC=local
Directorio electrónico de Novell	cn=admin, dc=Citrix, dc=net
Servidor IBM Directory	LDAP_dn

Servidor LDAP	Vincular DN
Lotus Domino	CN=Notes Administrator, O=Citrix, C=US
Directorio Sun ONE (anteriormente iPlanet)	uid=admin, ou=Administrators, ou=TopologyManagement, o=NetscapeRoot

Configurar la autenticación de usuarios LDAP mediante la CLI

Realice los siguientes pasos para configurar la autenticación LDAP para usuarios externos.

Configurar la directiva LDAP

En el símbolo del sistema, haga lo siguiente:

Paso 1: Cree una acción LDAP.

```
add authentication ldapAction <name> { -serverIP <ip_addr|ipv6_addr|*> | {
 -serverName <string> } } >] [-authTimeout <positive_integer>] [-ldapBase
<string>] [-ldapBindDn <string>] { -ldapBindDnPassword } [-ldapLoginName <
string>] [-groupAttrName <string>] [-subAttributeName <string>]
```

Ejemplo:

```
add authentication ldapAction ldap_act -serverIP <IP> -authTimeout 30 -
ldapBase "CN=xxxxx,DC=xxxx,DC=xxx"-ldapBindDn "CN=xxxxx,CN=xxxxx,DC=xxxx,DC
=xxx"-ldapBindDnPassword abcd -ldapLoginName sAMAccountName -groupattrName
memberOf -subAttributeName CN
```

Para obtener la descripción de los parámetros, consulte el tema de referencia de comandos de autenticación y autorización.

Paso 2: Cree una directiva LDAP clásica.

```
add authentication ldapPolicy <name> <rule> [<reqAction>]
```

Ejemplo:

```
add authentication ldappolicy ldap_pol_classic ns_true ldap_act
```

> **Nota**
>
> Puede configurar mediante una directiva LDAP clásica o avanzada, pero Citrix recomienda usar una directiva de autenticación avanzada porque las directivas clásicas están en desuso a partir de la versión 13.0 de Citrix ADC.

Paso 3: Cree una directiva LDAP avanzada


```
add authentication Policy <name> <rule> [<reqAction>]
```

Ejemplo:

```
add authentication policy ldap_pol_advance -rule true -action ldap_act
```

Paso 4: Vincule la directiva LDAP al sistema global

En el indicador de línea de comandos, haga lo siguiente:

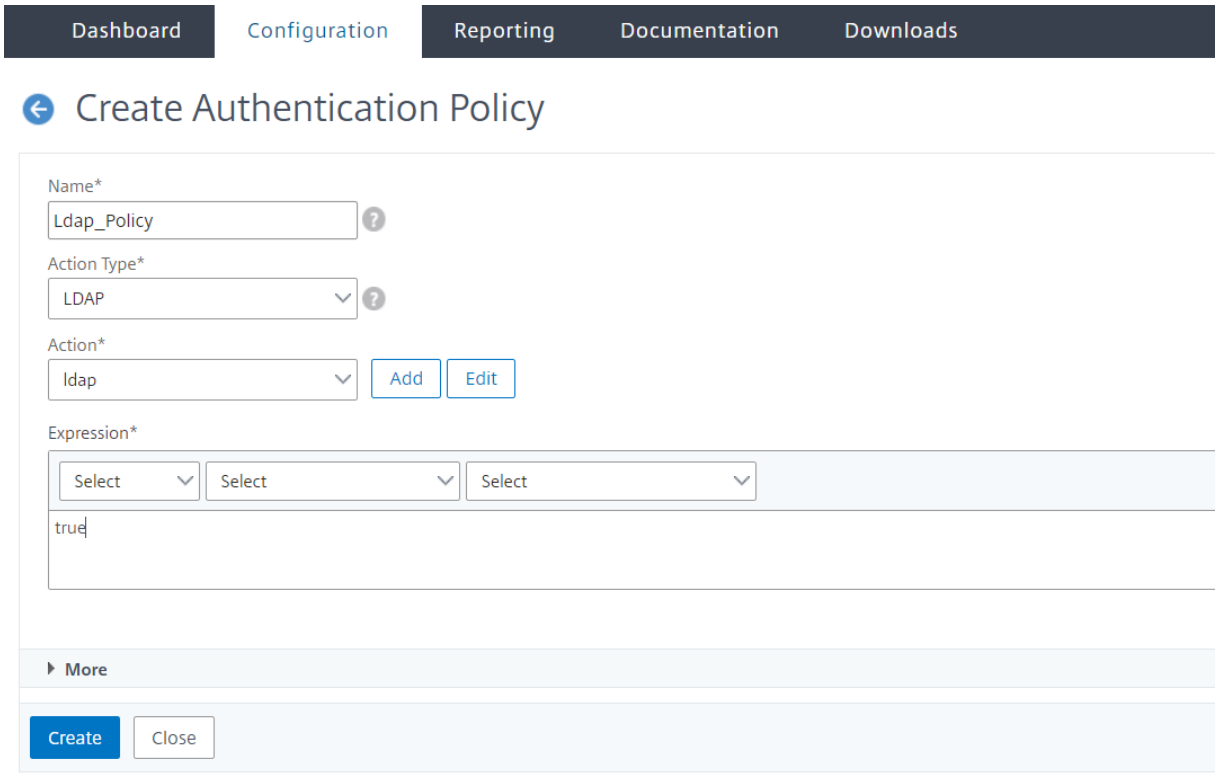
```
bind system global <policyName> [-priority <positive_integer]
```

Ejemplo:

```
bind system global ldap_pol_advanced -priority 10
```

Configurar la autenticación de usuarios LDAP mediante la GUI de Citrix ADC

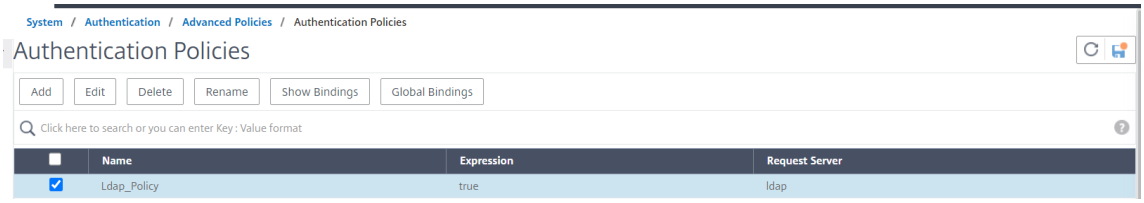
1. Vaya a **Sistema** > **Autenticación** > **Directivas avanzadas** > **Directiva**.
2. Haga clic en **Agregar** para crear una directiva de autenticación de tipo LDAP.
3. Haga clic en **Crear** y **cerrar**.



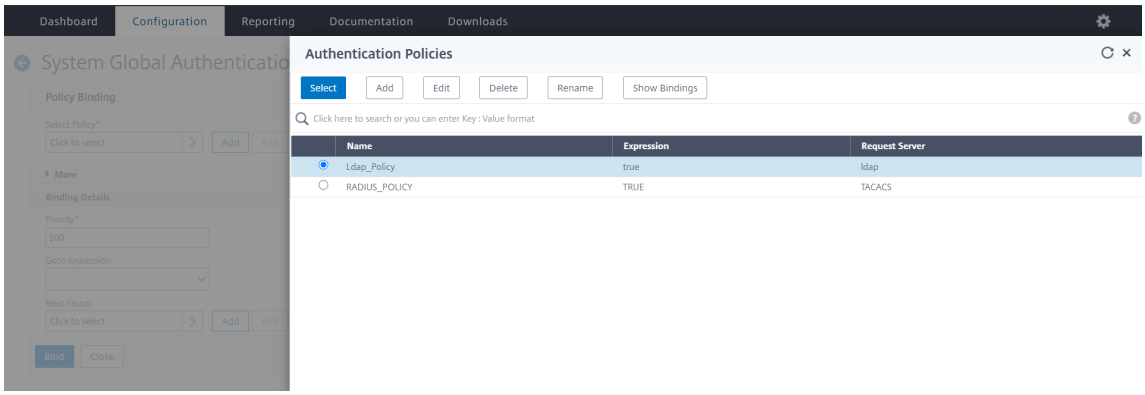
Vincular una directiva de autenticación al sistema global para la autenticación LDAP mediante la GUI de Citrix ADC

1. Vaya a **Sistema** > **Autenticación** > **Directivas avanzadas** > **Directiva de autenticación**.

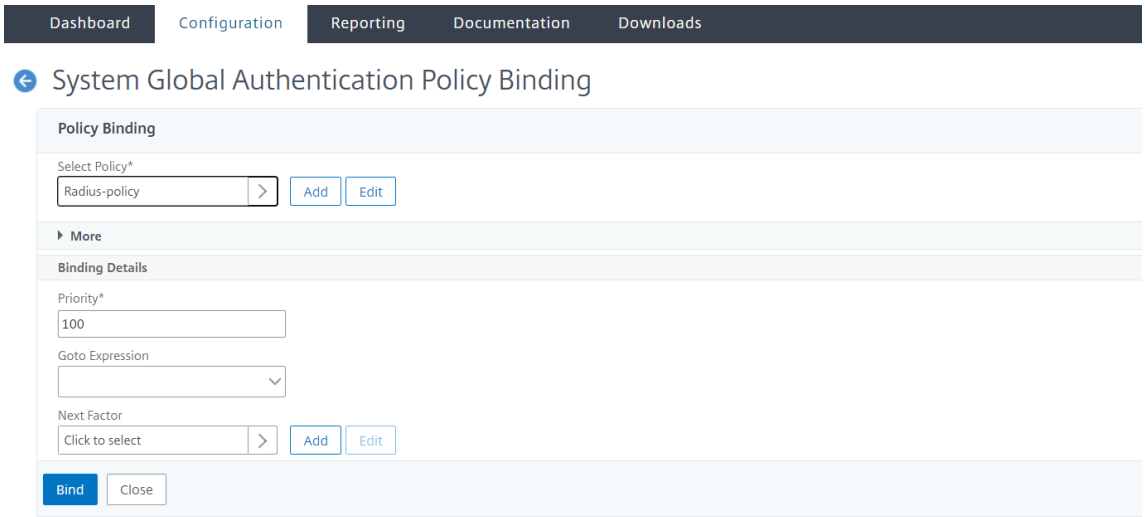
2. En el panel de detalles, haga clic en **Vínculos globales** para crear un vínculo de directiva de autenticación global del sistema.
3. Haga clic en **Vínculos globales**.



4. Seleccione un perfil de autenticación.

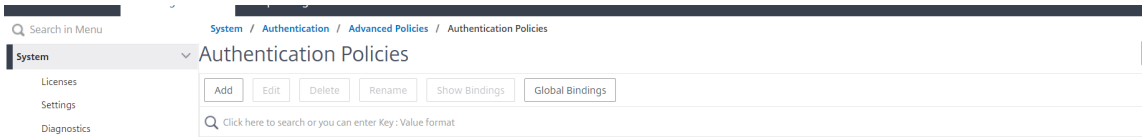


5. Seleccione la directiva LDAP.
6. En la página **Vinculación de directivas de autenticación global del sistema**, establezca los siguientes parámetros:
   a) Seleccione Directiva.
   b) Detalles de los vínculos



7. Haga clic en **Vincular** y **Listo**.

8. Haga clic en **Enlaces globales** para confirmar que la directiva está vinculada al sistema global.



Determinación de los atributos en el directorio LDAP

Si necesita ayuda para determinar los atributos de su directorio LDAP, puede buscarlos fácilmente con el explorador LDAP gratuito de Softerra.

Puede descargar el explorador LDAP desde el sitio web del administrador de LDAP de Softerra en < `http://www.ldapbrowser.com`>. Una vez instalado el explorador, defina los siguientes atributos:

- El nombre de host o la dirección IP del servidor LDAP.
- El puerto del servidor LDAP. El valor por defecto es 389.
- El campo DN base se puede dejar en blanco.
- La información proporcionada por el explorador LDAP puede ayudarle a determinar el DN base necesario para la ficha Autenticación.
- La comprobación de enlace anónimo determina si el servidor LDAP requiere credenciales de usuario para que el explorador se conecte a él. Si el servidor LDAP requiere credenciales, deje la casilla de verificación desactivada.

Después de completar la configuración, el explorador LDAP muestra el nombre del perfil en el panel izquierdo y se conecta al servidor LDAP.

Para obtener más información, consulte el tema LDAP.

Compatibilidad con autenticación basada en claves para usuarios LDAP

Con la autenticación basada en claves, ahora puede obtener la lista de claves públicas que se almacenan en el objeto de usuario en el servidor LDAP a través de SSH. El dispositivo Citrix ADC durante el proceso de autenticación basada en roles (RBA) debe extraer claves SSH públicas del servidor LDAP. La clave pública recuperada, que es compatible con SSH, debe permitirle iniciar sesión a través del método RBA.

Se introduce un nuevo atributo “sshPublicKey” en los comandos “add authentication ldapAction” y “set authentication ldapAction”. Al usar este atributo, puede obtener los siguientes beneficios:

- Puede almacenar la clave pública recuperada y la acción LDAP utiliza este atributo para recuperar la información de clave SSH del servidor LDAP.
- Puede extraer nombres de atributo de hasta 24 KB.

> **Nota**
>
> El servidor de autenticación externo, como LDAP, solo se usa para recuperar información de clave SSH. No se usa para fines de autenticación.

A continuación se muestra un ejemplo del flujo de eventos a través de SSH:

- El demonio SSH envía una solicitud AAA_AUTHENTICATE con el campo de contraseña vacío al puerto del demonio de autenticación, autorización y auditoría.
- Si LDAP está configurado para almacenar la clave pública SSH, la autenticación, la autorización y la auditoría responden con el atributo `sshPublicKey` junto con otros atributos.
- El demonio SSH verifica estas claves con las claves del cliente.
- El demonio SSH pasa el nombre de usuario en la carga útil de la solicitud, y la autenticación, la autorización y la auditoría devuelven las claves específicas de este usuario junto con las claves genéricas.

Para configurar el atributo sshPublicKey, en el símbolo del sistema, escriba los siguientes comandos:

- Con la operación add, puede agregar el atributo “sshPublicKey” mientras configura el comando `ldapAction`.

  ```
  add authentication ldapAction <name> { -serverIP <ip_addr|ipv6_addr
  |*> | { -serverName <string> } } [-serverPort <port>] … [-Attribute1 <
  string>] … [-Attribute16 <string>][-sshPublicKey <string>][-authentication
   off]<!--NeedCopy-->
  ```

- Con la operación set, puede configurar el atributo “sshPublicKey” en un comando ldapAction ya agregado.

  ```
  set authentication ldapAction <name> [-sshPublicKey <string>][-authentication
   off]<!--NeedCopy-->
  ```

Autenticación RADIUS (mediante servidores RADIUS)

Puede configurar el dispositivo Citrix ADC para autenticar el acceso de los usuarios con uno o más servidores RADIUS. Si utiliza productos RSA SecurID, SafeWord o Gemalto Protiva, utilice un servidor RADIUS.

Para obtener más información sobre las directivas de autenticación RADIUS, consulte el tema Directivas de autenticación RADIUS.

Es posible que su configuración requiera el uso de una dirección IP del servidor de acceso a la red (IP del NAS) o un identificador del servidor de acceso a la red (ID del NAS). Al configurar el dispositivo para que utilice un servidor de autenticación RADIUS, siga las siguientes instrucciones:

- Si habilita el uso de la IP del NAS, el dispositivo envía su dirección IP configurada al servidor RADIUS, en lugar de la dirección IP de origen utilizada para establecer la conexión RADIUS.
- Si configura el ID del NAS, el dispositivo envía el identificador al servidor RADIUS. Si no configura el ID del NAS, el dispositivo envía su nombre de host al servidor RADIUS.
- Cuando la dirección IP del NAS está habilitada, el dispositivo ignora cualquier ID de NAS que haya utilizado para comunicarse con el servidor RADIUS.

Configurar la autenticación de usuarios RADIUS mediante la CLI

En el símbolo del sistema, haga lo siguiente:

Paso 1: Crear una acción RADIUS

```
add authentication radiusaction <name> -serverip <ip> -radkey <key> -
radVendorID <id> -radattributetype <value>
```

Donde atributo ID de proveedor
`radVendorID` RADIUS, utilizado para la extracción de grupos RADIUS.
`radAttributeType` Tipo de atributo RADIUS, utilizado para la extracción de grupos RADIUS.

Ejemplo:

```
add authentication radiusaction RADserver531 rad_action -serverip 1.1.1.1 -
radkey key123 -radVendorID 66 -radattributetype 6
```

Paso 2: Cree una directiva RADIUS clásica.

```
add authentication radiusPolicy <name> <rule> [<reqAction>]
```

Ejemplo:

```
add authentication radiuspolicy radius_pol_classic ns_true radius_act
```

> **Nota**
>
> Puede configurar mediante una directiva RADIUS clásica o avanzada. Citrix recomienda utilizar la directiva de autenticación avanzada porque las directivas clásicas están obsoletas desde la versión de Citrix ADC 13.0 en adelante.

Paso 3: Crear una directiva RADIUS avanzada

```
add authentication policy <policyname> -rule true -action <radius action
name>
```

Ejemplo:

```
add authentication policy rad_pol_advanced -rule true -action radserver531rad_action
```

Paso 4: Enlazar la directiva RADIUS al sistema global.

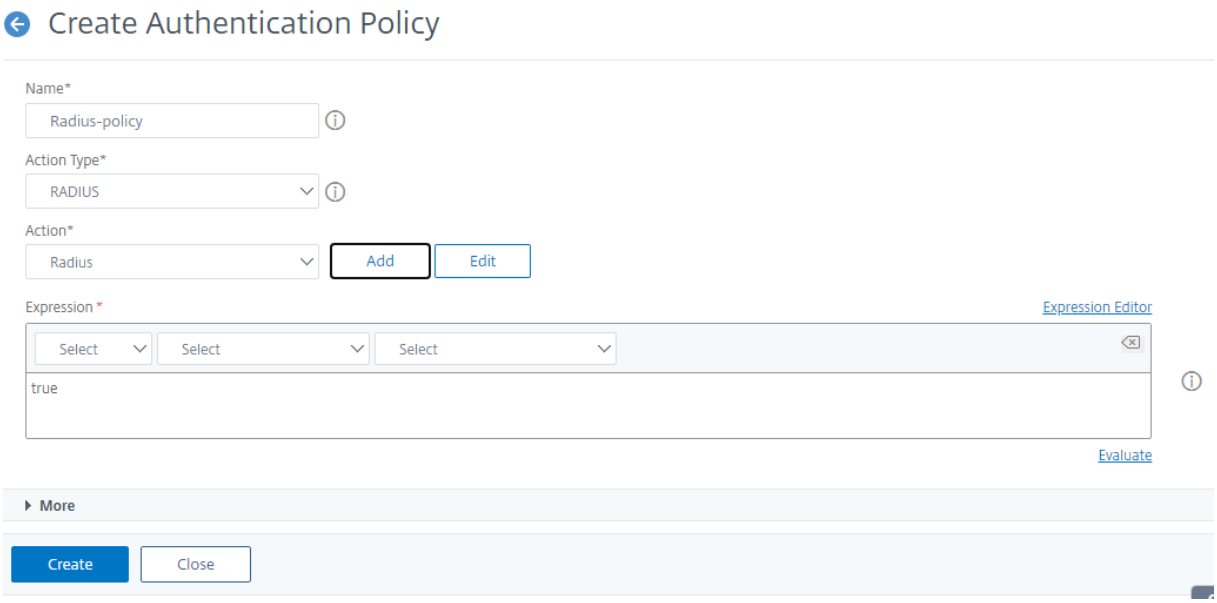

```
bind system global <policyName> -priority <positive_integer
```

Ejemplo:

```
bind system global radius_pol_advanced -priority 10
```

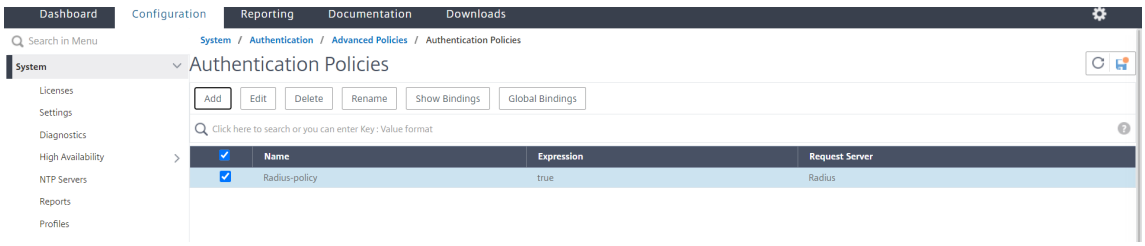
Configurar la autenticación de usuarios RADIUS mediante la GUI

1. Vaya a **Sistema** > **Autenticación** > **Directivas avanzadas** > **Directiva**.
2. Haga clic en **Agregar** para crear una directiva de autenticación de tipo RADIUS.
3. Haga clic en **Crear** y **cerrar**.



Enlazar la directiva de autenticación al sistema global para la autenticación RADIUS mediante la GUI

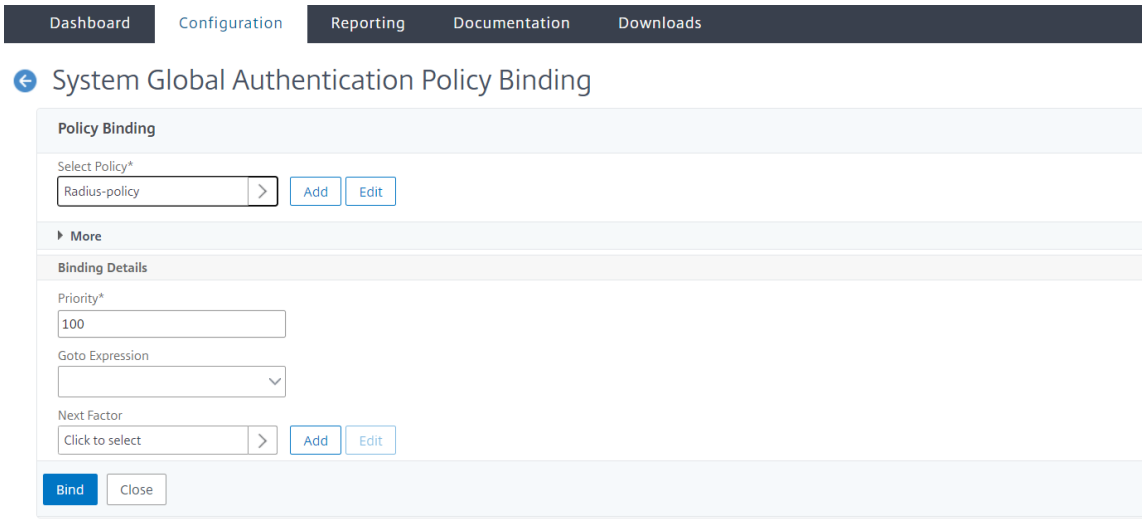
1. Vaya a **Sistema** > **Autenticación** > **Directivas avanzadas** > **Directiva**.
2. En el panel de detalles, haga clic en **Vínculos globales** para crear un vínculo de directiva de autenticación global del sistema.
3. Haga clic en **Vínculos globales**.



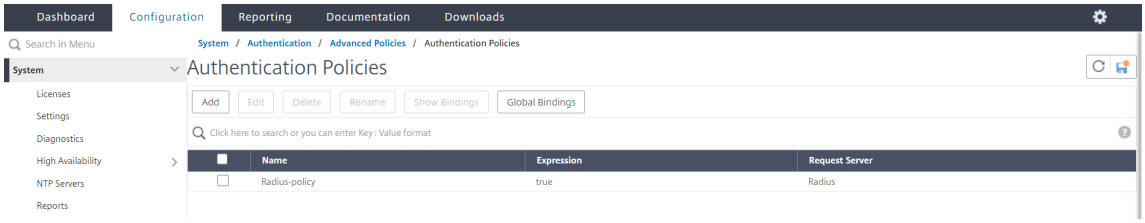
4. Selecciona RADIUS.

5. En la página **Vinculación de directivas de autenticación global del sistema**, establezca los siguientes parámetros:

   a) Seleccione una directiva.
   b) Detalles de unión.



6. Haga clic en **Vincular** y **Cerrar**.
7. Haga clic en **Enlaces globales** para confirmar que la directiva está vinculada al sistema global.



Elegir protocolos de autenticación de usuarios RADIUS

El dispositivo Citrix ADC admite implementaciones de RADIUS que están configuradas para usar cualquiera de varios protocolos para la autenticación de usuarios, incluidos:

- Protocolo de autenticación de contraseña
- Protocolo de autenticación por desafío mutuo (CHAP)
- Protocolo de autenticación Challenge Handshake de Microsoft (MS-CHAP versión 1 y versión 2)

Si la implementación está configurada para utilizar la autenticación RADIUS y el servidor RADIUS está configurado con un protocolo de autenticación de contraseña. Puede reforzar la autenticación de usuarios asignando un secreto compartido sólido al servidor RADIUS. Los secretos compartidos de RADIUS fuertes consisten en secuencias aleatorias de letras mayúsculas y minúsculas, números y signos de puntuación, y tienen una longitud mínima de 22 caracteres. Si es posible, utilice un programa de generación de caracteres aleatorios para determinar los secretos compartidos RADIUS.

Para proteger aún más el tráfico RADIUS, asigne un secreto compartido diferente a cada dispositivo o servidor virtual. Al definir clientes en el servidor RADIUS, también puede asignar un secreto compartido independiente a cada cliente. Además, debe configurar por separado cada directiva que utilice la autenticación RADIUS.

Configurar la extracción de direcciones IP

Puede configurar el dispositivo para que extraiga la dirección IP de un servidor RADIUS. Cuando un usuario se autentica con el servidor RADIUS, el servidor devuelve una dirección IP enmarcada asignada al usuario. Los siguientes son atributos para la extracción de direcciones IP:

- Permite que un servidor RADIUS remoto proporcione una dirección IP desde la red interna para un usuario que haya iniciado sesión en el dispositivo.
- Permite la configuración de cualquier atributo RADIUS mediante la dirección IP de tipo, incluidas las codificadas por el proveedor.

Al configurar el servidor RADIUS para la extracción de direcciones IP, configure el identificador de proveedor y el tipo de atributo.

El identificador de proveedor permite que el servidor RADIUS asigne una dirección IP al cliente desde un conjunto de direcciones IP que están configuradas en el servidor RADIUS. El ID de proveedor y los atributos se utilizan para establecer la asociación entre el cliente RADIUS y el servidor RADIUS. El ID de proveedor es el atributo de la respuesta RADIUS que proporciona la dirección IP de la red interna. Un valor de cero indica que el atributo no está codificado por el proveedor. El tipo de atributo es el atributo de dirección IP remota de una respuesta RADIUS. El valor mínimo es uno y el valor máximo es 255.

Una configuración común es extraer la *dirección IP en trama del atributo***RADIUS**. El ID del proveedor se establece en cero o no se especifica. El tipo de atributo se establece en ocho.

Extracción de grupos para RADIUS mediante la GUI

1. Vaya a **Sistema** > **Autenticación** > **Directivas avanzadas** > **Radius** y seleccione una directiva.
2. Seleccione o cree una directiva RADIUS.
3. En la página **Configurar servidor RADIUS de autenticación**, defina los siguientes parámetros.
    a) **Identificador de proveedor de**
    b) **Tipo de atributo de grupo**
4. Haga clic en **Aceptar** y **cerrar**.

Autenticación TACACS+ (mediante servidores TACACS+ externos)

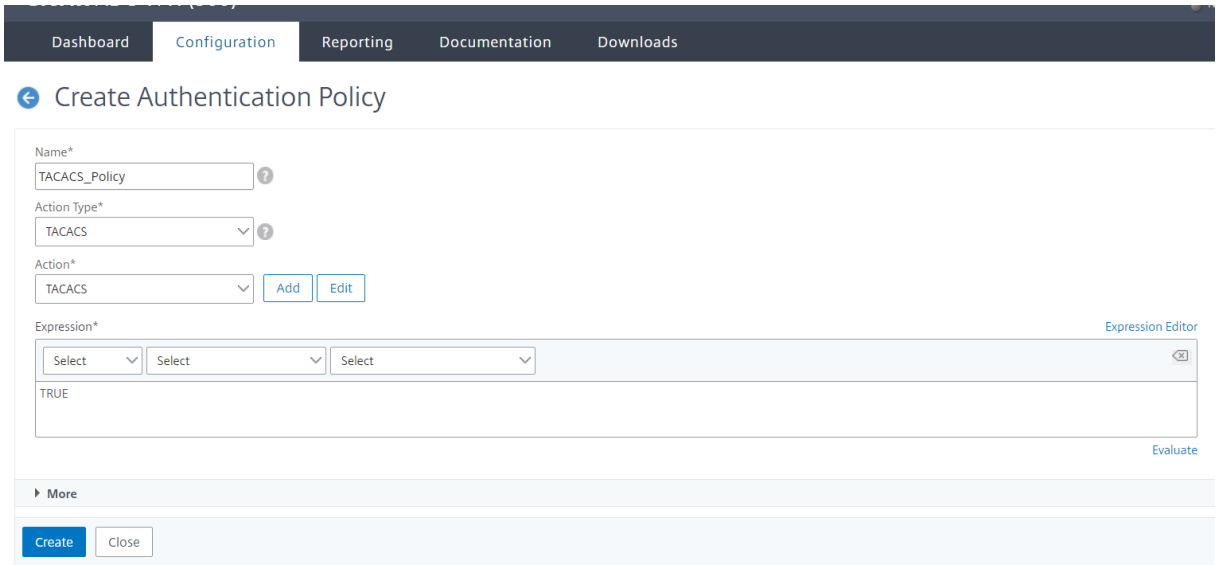
> **Importante**
>
> - Citrix recomienda no modificar ninguna configuración relacionada con TACACS cuando ejecuta un comando “clear ns config”.
> - La configuración relacionada con TACACS relacionada con las directivas avanzadas se borra y vuelve a aplicar cuando el `RBAconfig` parámetro se establece en NO en el comando “clear ns config” para directivas avanzadas.

Puede configurar un servidor TACACS+ para la autenticación. De forma similar a la autenticación RADIUS, TACACS+ utiliza una clave secreta, una dirección IP y el número de puerto. El número de puerto predeterminado es 49. Para configurar el dispositivo para que utilice un servidor TACACS+, proporcione la dirección IP del servidor y el secreto TACACS+. Debe especificar el puerto solo cuando el número de puerto del servidor en uso no sea el número de puerto predeterminado de 49.

Para obtener más información, consulte Autenticación TACACS.

Configurar la autenticación TACACS+ mediante la GUI

1. Vaya a **Sistema** > **Autenticación** > **Directivas avanzadas** > **Directiva**.
2. Haga clic en **Agregar** para crear una directiva de autenticación de tipo TACACS.
3. Haga clic en **Crear** y **cerrar**.



Una vez configurada la configuración del servidor TACACS+ en el dispositivo, vincule la directiva a la entidad global del sistema.

Enlazar las directivas de autenticación a la entidad global del sistema mediante la CLI

Cuando se hayan configurado las directivas de autenticación, vincule las directivas a la entidad global del sistema.

En el indicador de línea de comandos, haga lo siguiente:

```
bind system global <policyName> [-priority <positive_integer>]
```

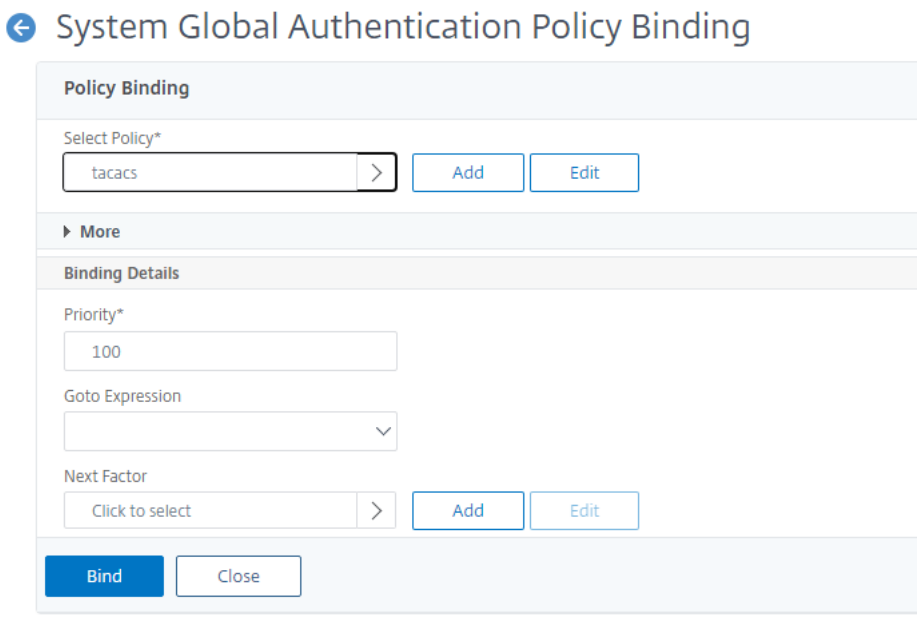
Ejemplo:

```
bind system global pol_classic -priority 10
```

Además, lea el artículo de Citrix CTX113820 para conocer la autenticación externa mediante TACACS.

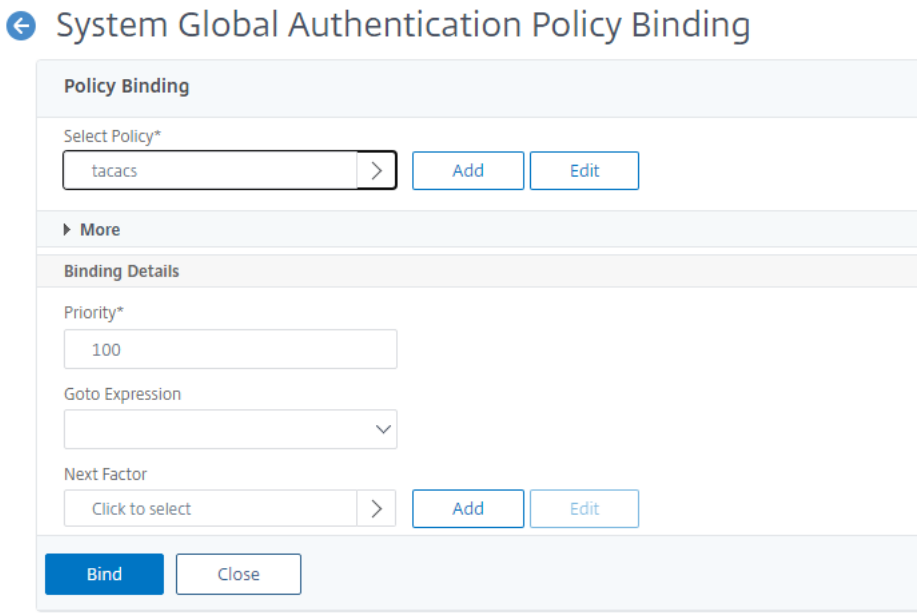
Vincular directivas de autenticación a la entidad global del sistema mediante la GUI

1. Vaya a **Sistema** > **Autenticación** > **Directivas avanzadas** > **Directivas de autenticación > Directiva**.
2. En el panel de detalles, haga clic en **Vínculos globales** para crear un vínculo de directiva de autenticación global del sistema.
3. Haga clic en **Vínculos globales**.

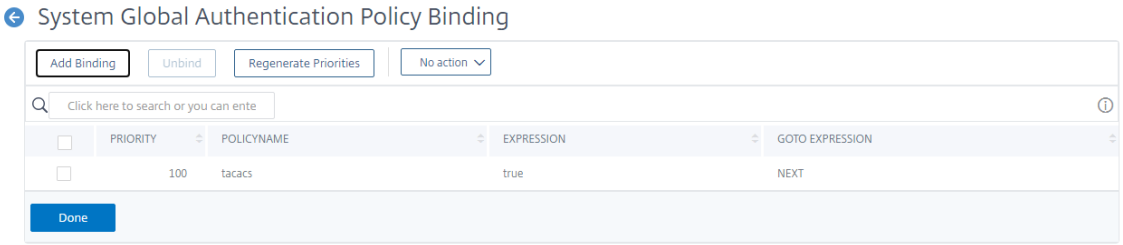


4. Seleccione la directiva TACACS.
5. En la página Vinculación de directivas de autenticación global del sistema, establezca los siguientes parámetros:
   a) Seleccione Directiva.

b) Detalles de los vínculos



6. Haga clic en **Vincular** y **Cerrar**.
7. Haga clic en **Enlaces globales** para confirmar la directiva vinculada al sistema global.



Para obtener más información sobre la extracción de grupos TACACS, lea el artículo CTX220024de Citrix.

Mostrar el número de intentos de inicio de sesión fallidos para usuarios externos

El dispositivo Citrix ADC muestra el número de intentos de inicio de sesión no válidos al usuario externo cuando intenta al menos un inicio de sesión fallido antes de iniciar sesión correctamente en la consola de administración de Citrix ADC.

> **Nota**
>
> Actualmente, Citrix solo admite la autenticación interactiva del teclado para usuarios externos con el parámetro “persistentLoginAttempts” habilitado en el parámetro del sistema.

En el símbolo del sistema, escriba:


```
set aaa parameter -maxloginAttempts <value> -failedLoginTimeout <value> -
persistentLoginAttempts (ENABLED | DISABLED )]
```

Ejemplo:

```
set aaa parameter -maxloginAttempts 5 -failedLoginTimeout 4 -persistentLoginAttempts
 ENABLED
```

```
Following msg will be seen to external user when he tries 1 invalid
    login attempt before successfully login to the ADC management access
    .

Connection established.
To escape to local shell, press 'Ctrl+Alt+]'.
###############################################################################

#

    #
#        WARNING: Access to this system is for authorized users only
            #
#         Disconnect IMMEDIATELY if you are not an authorized user!
             #
#

    #
###############################################################################


WARNING! The remote SSH server rejected X11 forwarding request.
Last login: Mon Aug 24 17:09:00 2020 from 10.10.10.10

The number of unsuccessful login attempts since the last successful
    login : 1
Done
>
The number of unsuccessful login attempts since the last successful
    login : 1
Done
>
<!--NeedCopy-->
```


Autenticación basada en clave SSH para usuarios del sistema local

August 20, 2021

Para tener un acceso de usuario seguro para el dispositivo Citrix ADC, puede tener la autenticación de clave pública del servidor SSH. La autenticación basada en clave SSH se prefiere sobre la autenticación basada en nombre de usuario o contraseña tradicional por las siguientes razones:

- Proporciona una mayor fortaleza criptográfica que las contraseñas de usuario.
- Elimina la necesidad de recordar contraseñas complicadas y evita ataques de navegación por hombros que son posibles si se usan contraseñas.
- Proporciona un inicio de sesión sin contraseña para hacer que los casos de automatización sean más seguros.

Citrix ADC admite la autenticación basada en claves SSH aplicando el concepto de clave pública y privada. La autenticación basada en claves SSH en Citrix ADC se puede habilitar para un usuario específico o para todos los usuarios locales.

> **Nota**
>
> La función solo se admite para usuarios locales de Citrix ADC y no para usuarios externos.

Autenticación basada en clave SSH para usuarios del sistema local

En un dispositivo Citrix ADC, un administrador puede configurar la autenticación basada en claves SSH para un acceso seguro al sistema. Cuando un usuario inicia sesión en Citrix ADC con una clave privada, el sistema autentica al usuario mediante la clave pública configurada en el dispositivo.

Configurar la autenticación basada en claves SSH para los usuarios del sistema local Citrix ADC mediante CLI

La siguiente configuración le ayuda a configurar la autenticación basada en clave para los usuarios del sistema local de Citrix ADC.

1. Inicie sesión en un dispositivo Citrix ADC mediante credenciales de administrador.
2. De forma predeterminada, `sshd_config` el archivo accede a esta ruta de acceso: **AuthorizedKeysFile /nsconfig/ssh/authorized_keys**.
3. Agregue la clave pública al archivo authorized_keys: **/nsconfig/ssh/authorized_keys**. La ruta de archivo para `sshd_config` es `/etc/sshd_config`.
4. Copie el `sshd_config` archivo en `/nsconfig` para asegurarse de que los cambios persisten incluso después de reiniciar el dispositivo.
5. Puede usar el siguiente comando para reiniciar el `sshd` proceso.


```
    kill -HUP `cat /var/run/sshd.pid`
<!--NeedCopy-->
```

> **Nota**
>
> Si el archivo authorized_keys no está disponible, primero debe crear uno y, a continuación, agregar la clave pública. **Asegúrese de que el archivo tiene el siguiente permiso para los keys authorized_keys**.
>
> `root@Citrix ADC## chmod 0644 authorized_keys`

```
> shell
Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993,
    1994
The Regents of the University of California. All rights reserved.
root@ns# cd /nsconfig/ssh
root@ns# vi authorized_keys
### Add public keys in authorized_keys file
<!--NeedCopy-->
```

Autenticación basada en clave SSH específica del usuario para usuarios del sistema local

En un dispositivo Citrix ADC, un administrador ahora puede configurar una autenticación basada en clave SSH específica del usuario para un acceso seguro al sistema. El administrador debe configurar primero la `Authorizedkeysfile` opción en el `sshd_config` archivo y, a continuación, agregar la clave pública en el `authorized_keys` archivo para un usuario del sistema.

> **Nota**
>
> Si el archivo authorized_keys no está disponible para un usuario, el administrador debe crear primero uno y luego agregarle la clave pública.

Configurar la autenticación basada en clave SSH específica del usuario mediante la CLI

El siguiente procedimiento le ayuda a configurar la autenticación basada en claves SSH específica del usuario para los usuarios del sistema local de Citrix ADC.

1. Inicie sesión en un dispositivo Citrix ADC mediante credenciales de administrador.

2. En el símbolo del shell, acceda al `sshd_config` archivo y agregue la siguiente línea de configuración:

   `AuthorizedKeysFile ~/.ssh/authorized_keys`

   > **Nota**
   >
   > El ~ es el directorio principal y difiere para los diferentes usuarios. Se expande a los diferentes directorios de inicio.

3. Cambie el directorio a la carpeta de usuario del sistema y agregue las claves públicas en el `authorized_keys` archivo.

   `/var/pubkey/<username>/.ssh/authorized_keys`

Una vez que haya completado los pasos anteriores, reinicie el `sshd` proceso en el dispositivo mediante el siguiente comando:

```
    kill -HUP `cat /var/run/sshd.pid`

<!--NeedCopy-->
```

> **Nota**
>
> Si el archivo authorized_keys no está disponible, primero debe crear uno y, a continuación, agregar la clave pública.

```
> shell
Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993,
    1994
The Regents of the University of California. All rights reserved.
root@ns# cd /var/pubkey/<username>/
root@ns# ls
.ssh
root@ns# cd .ssh
root@ns# vi authorized_keys
### Add public keys in authorized_keys file

<!--NeedCopy-->
```

Además, lea el artículo de Citrix, CTX109011 para saber cómo funciona el acceso SSH seguro al dispositivo Citrix ADC.

Autenticación de dos factores para usuarios del sistema y usuarios externos

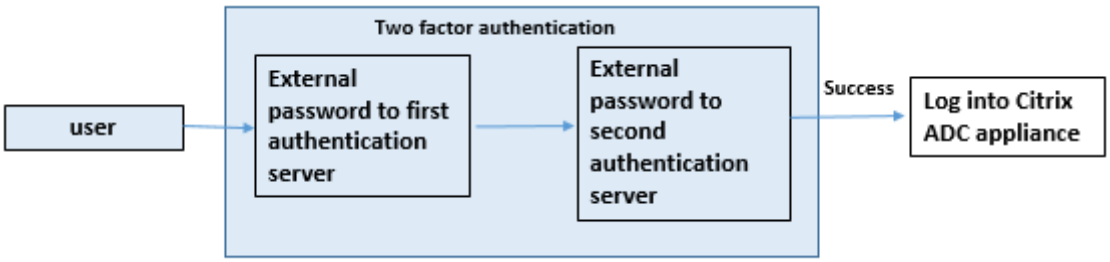
February 19, 2022

La autenticación de dos factores es un mecanismo de seguridad en el que un dispositivo Citrix ADC autentica a un usuario del sistema en dos niveles de autenticación. El dispositivo concede acceso al usuario solo después de la validación correcta de las contraseñas por ambos niveles de autenticación. Si un usuario se autentica localmente, el perfil de usuario debe crearse en la base de datos de Citrix ADC. Si el usuario se autentica externamente, entonces, el nombre de usuario y la contraseña deben coincidir con la identidad de usuario registrada en el servidor de autenticación externo.

> **Nota La**
>
> función de autenticación de dos factores solo funciona a partir de Citrix ADC 12.1 compilación 51.16 en adelante.

Cómo funciona la autenticación de dos factores

Considere un usuario que intenta iniciar sesión en un dispositivo Citrix ADC. El servidor de aplicaciones solicitado envía el nombre de usuario y la contraseña al primer servidor de autenticación externo (RADIUS, TACACS, LDAP o AD). Una vez validados el nombre de usuario y la contraseña, se le pedirá un segundo nivel de autenticación. Ahora el usuario puede proporcionar la segunda contraseña. Solo si ambas contraseñas son correctas, el usuario puede acceder al dispositivo Citrix ADC. El siguiente diagrama es una ilustración de cómo funciona la autenticación de dos factores para un dispositivo Citrix ADC.



Los siguientes son los diferentes casos de uso para configurar la autenticación de dos factores para los usuarios externos y del sistema.

Puede configurar la autenticación de dos factores en un dispositivo Citrix ADC de diferentes maneras. A continuación se presentan los diferentes casos de configuración para la autenticación de dos factores en un dispositivo Citrix ADC.

1. Autenticación de dos factores (2FA) en Citrix ADC, GUI, CLI, API y SSH.

2. Autenticación externa habilitada y autenticación local inhabilitada para los usuarios del sistema.
3. Autenticación externa habilitada con autenticación local basada en directivas para los usuarios del sistema.
4. Autenticación externa inhabilitada para usuarios del sistema con autenticación local habilitada.
5. Autenticación externa habilitada y autenticación local habilitada para los usuarios del sistema.
6. Autenticación externa habilitada para usuarios LDAP seleccionados

Caso de uso 1: Autenticación de dos factores (2FA) en las interfaces de Citrix ADC, GUI, CLI, API y SSH

La autenticación de dos factores está habilitada y está disponible en todos los accesos de administración de Citrix ADC para GUI, API y SSH.

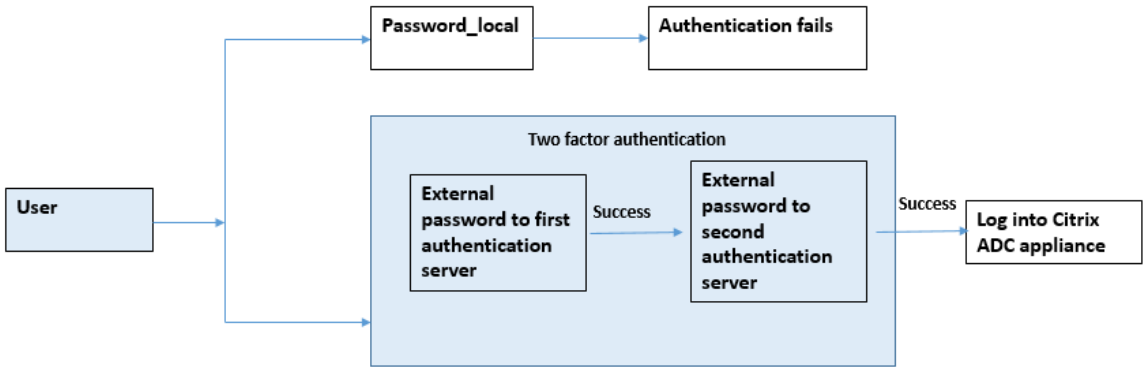
Caso de uso 2: Autenticación de dos factores admitida en servidores de autenticación externos como LDAP, RADIUS, Active Directory y TACACS

Puede configurar la autenticación de dos factores en los siguientes servidores de autenticación externos para la autenticación de usuario de primer nivel y segundo nivel.

- RADIUS
- LDAP
- Active Directory
- TACACS

Caso de uso 3: Autenticación externa habilitada y autenticación local inhabilitada para los usuarios del sistema

Para iniciar el proceso de autenticación, habilite la opción de autenticación externa e inhabilite la autenticación local para los usuarios del sistema.



Complete los siguientes pasos mediante la interfaz de línea de comandos:

1. Agregar acción de autenticación para la directiva LDAP
2. Agregar directiva de autenticación para directiva LDAP
3. Agregar acción de autenticación para la directiva RADIUS
4. Agregar directiva de autenticación para la directiva RADIUS
5. Agregar esquema de inicio de sesión de autenticación
6. Agregar y vincular la etiqueta de directiva de autenticación al servidor RADIUS
7. Enlazar autenticación global del sistema para la directiva LDAP
8. Inhabilitar la autenticación local en el parámetro del sistema

Agregar acción de autenticación para el servidor LDAP (autenticación de primer nivel)

En el símbolo del sistema, escriba:

```
add authentication ldapaction <ldap action name> -serverip <IP> -ldapbase
<> -ldapbinddn <binddn name> -ldapbinddnpassword <password>-ldaploginname <
loginname> -groupattrname <grp attribute name> -subAttributename <string>-
ssoNameAttribute <string>
```

Ejemplo:

```
add authentication ldapaction ldapact1 -serverip 1.1.1.1 -ldapbase base -
ldapbindDn name -ldapbindDNpassword password -ldapLoginName name -groupAttrName
 name -subAttributeName name -ssoNameAttribute name
```

Agregar directiva de autenticación para el servidor LDAP (autenticación de primer nivel)

En el símbolo del sistema, escriba:

```
add authentication policy <ldap policy name> -rule true -action <ldap
action name>
```

Ejemplo:

```
add authentication policy pol1 -rule true -action ldapact1
```

Agregar acción de autenticación para el servidor RADIUS (autenticación de segundo nivel)

En el símbolo del sistema, escriba:

```
add authentication radiusaction <rad action name> -serverip <rad server ip>
 -radkey <key> -radVendorID <ID >-radattributetype <rad attribute type>
```

Ejemplo:

```
add authentication radiusaction radact1 -serverip 1.1.1.1 -radkey 123 -
radVendorID 1234 -radAttributeType 2
```


Agregar directiva de autenticación para el servidor RADIUS (autenticación de segundo nivel)

En el símbolo del sistema, escriba:

```
add authentication policy <radius policy name> -rule true -action <rad
action name>
```

Ejemplo:

```
add authentication policy radpol11 -rule true -action radact1
```

Agregar esquema de inicio de sesión de autenticación

Puede utilizar el esquema de inicio de sesión “SingleAuth.xml” para que los usuarios del sistema proporcionen la segunda contraseña para el dispositivo Citrix ADC. En el símbolo del sistema, escriba:

```
add authentication loginSchema <login schema name> -authenticationSchema
LoginSchema/SingleAuth.xml
```

Ejemplo:

```
add authentication loginSchema radschema -authenticationSchema LoginSchema/
SingleAuth.xml
```

Agregar y vincular la etiqueta de directiva de autenticación al servidor RADIUS

En el símbolo del sistema, escriba:

```
add authentication policylabel <labelName> [-type ( AAATM_REQ | RBA_REQ )]
[-comment <string>][-loginSchema <string>]
```

```
bind authentication policylabel <labelName> -policyName <string> -priority
 <positive_integer> [-gotoPriorityExpression <expression>][-nextFactor <
string>]
```

Ejemplo:

```
add authentication policylabel label1 -type RBA_REQ -loginSchema radschema
```

```
bind authentication policylabel label1 -policyName radpol11 -priority 1
```

Sistema de autenticación de enlace global para la directiva LDAP

En el símbolo del sistema, escriba:

```
bind system global ldappolicy -priority <priority> -nextFactor <policy
label name>
```

Ejemplo:


```
bind system global pol11 -priority 1 -nextFactor label1
```

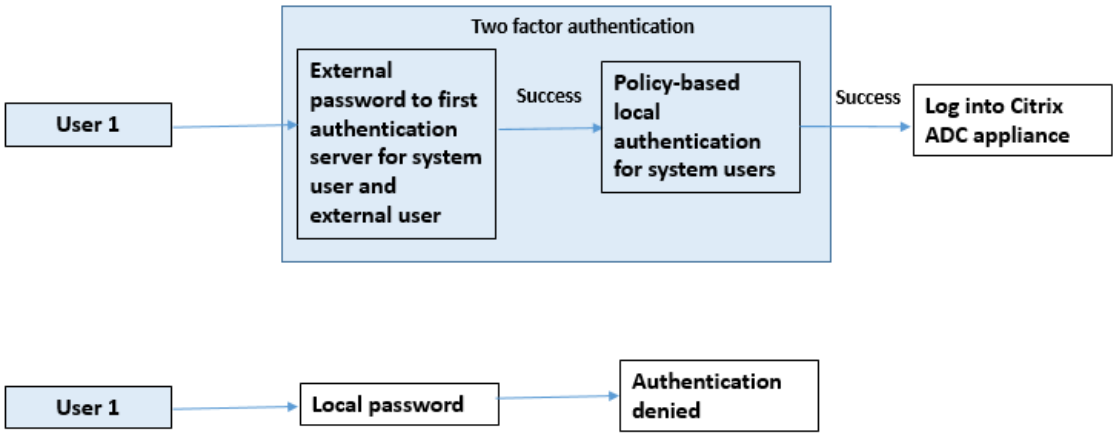
Inhabilitar la autenticación local en el parámetro del sistema

En el símbolo del sistema, escriba:

```
set system parameter -localauth disabled
```

Caso de uso 4: Autenticación externa habilitada para el usuario del sistema con directiva de autenticación local adjunta

En este caso, el usuario puede iniciar sesión en el dispositivo mediante autenticación de dos factores con evaluación de directivas de autenticación local en el segundo nivel de identificación de usuario.



Complete los pasos siguientes mediante la interfaz de línea de comandos.

1. Agregar acción de autenticación para el servidor LDAP
2. Agregar directiva de autenticación para directiva LDAP
3. Agregar directiva de autenticación local
4. Agregar etiqueta de directiva de autenticación
5. Enlazar la directiva LDAP como sistema global
6. Inhabilitar la autenticación local en el parámetro del sistema

Agregar acción de autenticación para el servidor LDAP (autenticación de primer nivel)

En el símbolo del sistema, escriba:

```
add authentication ldapaction <ldap action name> -serverip <IP> -ldapbase
<> -ldapbinddn <binddn name> -ldapbinddnpassword <password>-ldaploginname <
loginname> -groupattrname <grp attribute name> -subAttributename <string>-
ssoNameAttribute <string>
```


Ejemplo:

```
add authentication ldapaction ldapact1 -serverip 1.1.1.1 -ldapbase base -
ldapbindDn name -ldapbindDNpassword password -ldapLoginName name -groupAttrName
 name -subAttributeName name -ssoNameAttribute name -ssoNameAttribute name
```

Agregar directiva de autenticación para el servidor LDAP (autenticación de primer nivel)

En el símbolo del sistema, escriba:

```
add authentication policy <ldap policy name> -rule true -action <ldap
action name>
```

Ejemplo:

```
add authentication ldapaction ldapact1 -serverip 1.1.1.1 -ldapbase base -
ldapbindDn name -ldapbindDNpassword password -ldapLoginName name -groupAttrName
 name -subAttributeName name -ssoNameAttribute name
```

Agregar directiva de autenticación local para usuarios del sistema (autenticación de segundo nivel)

En el símbolo del sistema, escriba:

```
add authentication radiusaction <rad action name> -serverip <rad server ip>
 -radkey <key> -radVendorID <ID >-radattributetype <rad attribute type
```

Ejemplo:

```
add authentication radiusaction radact1 -serverip 1.1.1.1 -radkey 123 -
radVendorID 1234 -radAttributeType 2
```

Agregar y enlazar etiqueta de directiva de autenticación

En el símbolo del sistema, escriba:

```
add authentication policylabel <labelName> [-type ( AAATM_REQ | RBA_REQ )]
[-comment <string>][-loginSchema <string>]
bind authentication policylabel <labelName> -policyName <string> -priority
 <positive_integer> [-gotoPriorityExpression <expression>][-nextFactor <
string>]
```

Ejemplo:

```
add authentication policylabel label1 -type RBA_REQ -loginSchema radschema
bind authentication policylabel label1 -policyName radpol11 -priority 1 -
gotoPriorityExpression NEXT
```

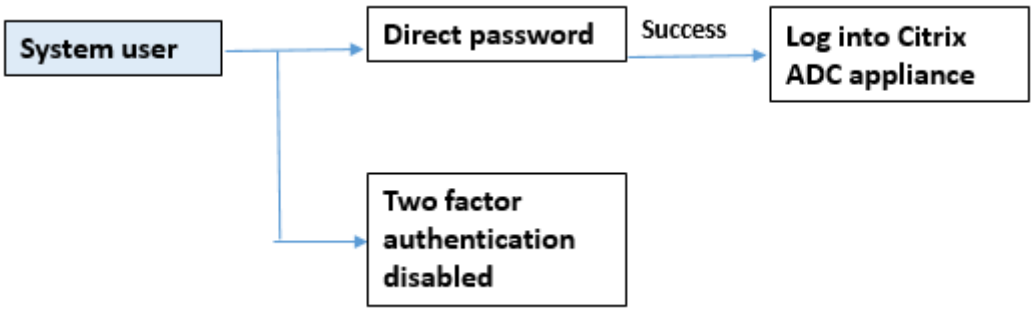

Inhabilitar la autenticación local en el parámetro del sistema

En el símbolo del sistema, escriba:

```
set system parameter -localauth disabled
```

Caso de uso 5: Autenticación externa inhabilitada y autenticación local habilitada para el usuario del sistema

Si el usuario tiene “externalAuth” inhabilitado, este usuario no existe en el servidor de autenticación. El usuario no se autentica con el servidor de autenticación externo aunque exista un usuario con el mismo nombre de usuario en el servidor autenticado externo. El usuario se autentica localmente.



Para habilitar la contraseña de usuario del sistema e inhabilitar la autenticación externa

En el símbolo del sistema, escriba lo siguiente:

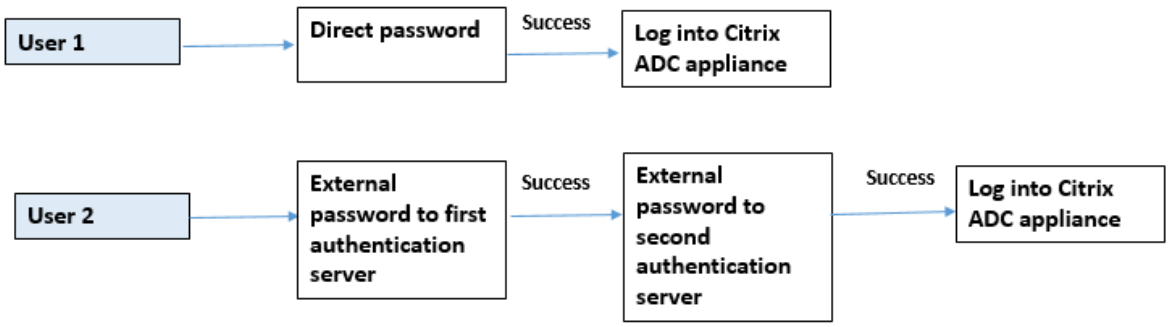
```
add system user <name> <password> -externalAuth DISABLED
```

Ejemplo:

```
add system user user1 password1 -externalAuth DISABLED
```

Caso de uso 6: Autenticación externa habilitada y autenticación local habilitada para usuarios del sistema

Para configurar el dispositivo para autenticar a los usuarios del sistema mediante una contraseña local. Si esta autenticación falla, el usuario se autentica mediante una contraseña de autenticación externa en los servidores de autenticación externos en dos niveles.



Configure los pasos siguientes mediante la CLI.

1. Agregar acción de autenticación para el servidor LDAP
2. Agregar directiva de autenticación para directiva LDAP
3. Agregar acción de autenticación para la directiva RADIUS
4. Agregar directiva de autenticación para la directiva RADIUS
5. Agregar esquema de inicio de sesión de autenticación
6. Agregar etiqueta de directiva de autenticación
7. Etiqueta de directiva de autenticación de enlace para el esquema de inicio de sesión
8. Sistema de autenticación de enlace global para la directiva RADIUS
9. Sistema de autenticación de enlace global para la directiva LDAP

Agregar acción de autenticación para el servidor LDAP

En el símbolo del sistema, escriba:

```
add authentication ldapaction <ldap action name> -serverip <IP> -ldapbase
<> -ldapbinddn <binddn name> -ldapbinddnpassword <password>-ldaploginname
 <loginname> -groupattrname <grp attribute name> -subAttributename <>-
ssoNameAttribute <>
```

Ejemplo:

```
add authentication ldapaction ldapact1 -serverip 1.1.1.1 -ldapbase base -
ldapbindDn name -ldapbindDNpassword password -ldapLoginName name -groupAttrName
 name -subAttributeName name -ssoNameAttribute name
```

Agregar directiva de autenticación para directiva LDAP

En el símbolo del sistema, escriba:

```
add authentication policy <policy name> --rule true -action <ldap action
name>
```


Ejemplo:

```
add authentication policy pol1 -rule true -action ldapact1
```

Agregar acción de autenticación para el servidor RADIUS

En el símbolo del sistema, escriba:

```
add authentication radiusaction <rad action name> -serverip <rad server ip>
 -radkey <key> -radVendorID <ID >-radattributetype <rad attribute type>
```

Ejemplo:

```
add authentication radiusaction radact1 -serverip 1.1.1.1 -radkey 123 -
radVendorID 1234 -radAttributeType 2
```

Agregar directiva de autenticación avanzada para el servidor RADIUS

En el símbolo del sistema, escriba:

```
add authentication policy <policy name> -rule true -action <rad action name
>
```

Ejemplo:

```
add authentication policy radpol11 -rule true -action radact1
```

Agregar esquema de inicio de sesión de autenticación

Puede utilizar el esquema de inicio de sesión SingleAuth.xml para mostrar la página de inicio de sesión y autenticar al usuario del sistema en la autenticación de segundo nivel.

En el símbolo del sistema, escriba:

```
add authentication loginSchema <name> -authenticationSchema <string>
```

Ejemplo:

```
add authentication loginSchema radschema -authenticationSchema LoginSchema/
SingleAuth.xml
```

Agregar y vincular la etiqueta de directiva de autenticación a la directiva de autenticación RADIUS para el inicio de sesión del usuario

En el símbolo del sistema, escriba:

```
add authentication policylabel <labelName> [-type ( AAATM_REQ | RBA_REQ )]
[-comment <string>][-loginSchema <string>]
```


Ejemplo:

```
add authentication policylabel label1 -type RBA_REQ -loginSchema radschema
bind authentication policylabel <labelName> -policyName <string> -priority
 <positive_integer> [-gotoPriorityExpression <expression>][-nextFactor <
string>]
```

Ejemplo:

```
bind authentication policylabel label1 -policyName rad pol11 -priority 1
```

Directiva de autenticación de enlace global

En el símbolo del sistema, escriba:

```
bind system global [<policyName> [-priority <positive_integer>] [-nextFactor
 <string>] [-gotoPriorityExpression <expression>]]
```

Ejemplo:

```
bind system global radpol11 -priority 1 -nextFactor label11
```

Caso de uso 7: Autenticación externa habilitada solo para usuarios externos seleccionados

Para configurar usuarios externos selectivos con autenticación de dos factores según el filtro de búsqueda configurado en la acción LDAP mientras que otros usuarios del sistema se autentican mediante autenticación de factor único.

Configure los pasos siguientes mediante la CLI.

1. Agregar acción de autenticación para el servidor LDAP
2. Agregar directiva de autenticación para directiva LDAP
3. Agregar acción de autenticación para la directiva RADIUS
4. Agregar directiva de autenticación para la directiva RADIUS
5. Agregar esquema de inicio de sesión de autenticación
6. Agregar etiqueta de directiva de autenticación
7. Etiqueta de directiva de autenticación de enlace para el esquema de inicio de sesión
8. Sistema de autenticación de enlace global para la directiva RADIUS

Agregar acción de autenticación para el servidor LDAP

En el símbolo del sistema, escriba:


```
add authentication ldapaction <ldap action name> -serverip <IP> -ldapbase
<> -ldapbinddn <binddn name> -ldapbinddnpassword <password>-ldaploginname
 <loginname> -groupattrname <grp attribute name> -subAttributename <>-
ssoNameAttribute <>
```

Ejemplo:

```
add authentication ldapaction ldapact1 -serverip 1.1.1.1 -ldapbase base -
ldapbindDn name -ldapbindDNpassword password -ldapLoginName name -groupAttrName
 name -subAttributeName name -ssoNameAttribute name
```

Agregar directiva de autenticación para directiva LDAP

En el símbolo del sistema, escriba:

```
add authentication policy <policy name> --rule true -action <ldap action
name>
```

Ejemplo:

```
add authentication policy pol1 -rule true -action ldapact1
```

Agregar acción de autenticación para el servidor RADIUS

En el símbolo del sistema, escriba:

```
add authentication radiusaction <rad action name> -serverip <rad server ip>
 -radkey <key> -radVendorID <ID >-radattributetype <rad attribute type>
```

Ejemplo:

```
add authentication radiusaction radact1 -serverip 1.1.1.1 -radkey 123 -
radVendorID 1234 -radAttributeType 2
```

Agregar directiva de autenticación avanzada para el servidor RADIUS

En el símbolo del sistema, escriba:

```
add authentication policy <policy name> -rule true -action <rad action name
>
```

Ejemplo:

```
add authentication policy radpol11 -rule true -action radact1
```


Agregar esquema de inicio de sesión de autenticación

Puede utilizar el esquema de inicio de sesión SingleAuth.xml para proporcionar la página de inicio de sesión para que el dispositivo autentique a un usuario del sistema en un segundo nivel de autenticación.

En el símbolo del sistema, escriba:

```
add authentication loginSchema <name> -authenticationSchema <string>
```

Ejemplo:

```
add authentication loginSchema radschema -authenticationSchema LoginSchema/
SingleAuth.xml
```

Agregar y vincular la etiqueta de directiva de autenticación a la directiva de autenticación RADIUS para el inicio de sesión del usuario

En el símbolo del sistema, escriba:

```
add authentication policylabel <labelName> [-type ( AAATM_REQ | RBA_REQ )]
[-comment <string>][-loginSchema <string>]
```

Ejemplo:

```
add authentication policylabel label1 -type RBA_REQ -loginSchema radschema
bind authentication policylabel <labelName> -policyName <string> -priority
 <positive_integer> [-gotoPriorityExpression <expression>][-nextFactor <
string>]
```

Ejemplo:

```
bind authentication policylabel label1 -policyName radpol11 -priority
```

Directiva de autenticación de enlace global

En el símbolo del sistema, escriba:

```
bind system global [<policyName> [-priority <positive_integer>] [-nextFactor
 <string>] [-gotoPriorityExpression <expression>]]
```

Ejemplo:

```
bind system global radpol11 -priority 1 -nextFactor label11
```

Para configurar sin autenticación de dos factores para usuarios de grupos mediante el filtro de búsqueda:

1. Agregar acción de autenticación para el servidor LDAP

2. Agregar directiva de autenticación para el servidor LDAP
3. Sistema de autenticación de enlace global para el servidor LDAP

Agregar acción de autenticación para el servidor LDAP

En el símbolo del sistema, escriba:

```
add authentication ldapaction <ldap action name> -serverip <IP> -ldapbase
<> -ldapbinddn <binddn name> -ldapbinddnpassword <password>-ldaploginname
 <loginname> -groupattrname <grp attribute name> -subAttributename <>-
searchFilter<>
```

Ejemplo:

```
add authentication ldapaction ldapact1 -serverip 1.1.1.1 -ldapbase base -
ldapbindDn name -ldapbindDNpassword password -ldapLoginName name -groupAttrName
 name -subAttributeName name - searchFilter "memberOf=CN=grp4,CN=Users,DC=
aaatm-test,DC=com"
```

Agregar directiva de autenticación para el servidor LDAP

En el símbolo del sistema, escriba:

```
add authentication policy <policy name> --rule true -action <ldap action
name>
```

Ejemplo:

```
add authentication policy pol1 -rule true -action ldapact1
```

Sistema de autenticación de enlace global para la directiva LDAP

En el símbolo del sistema, escriba:

```
bind system global ldappolicy -priority <priority> -nextFactor <policy
label name>
```

Ejemplo:

```
bind system global pol11 -priority 1 -nextFactor label11
```

Mostrar mensaje de solicitud personalizado para la autenticación de dos factores

Al configurar el campo de contraseña de dos factores con el archivo SingleAuth.xml en `/flash/nsconfig/loginschema/LoginSchema`

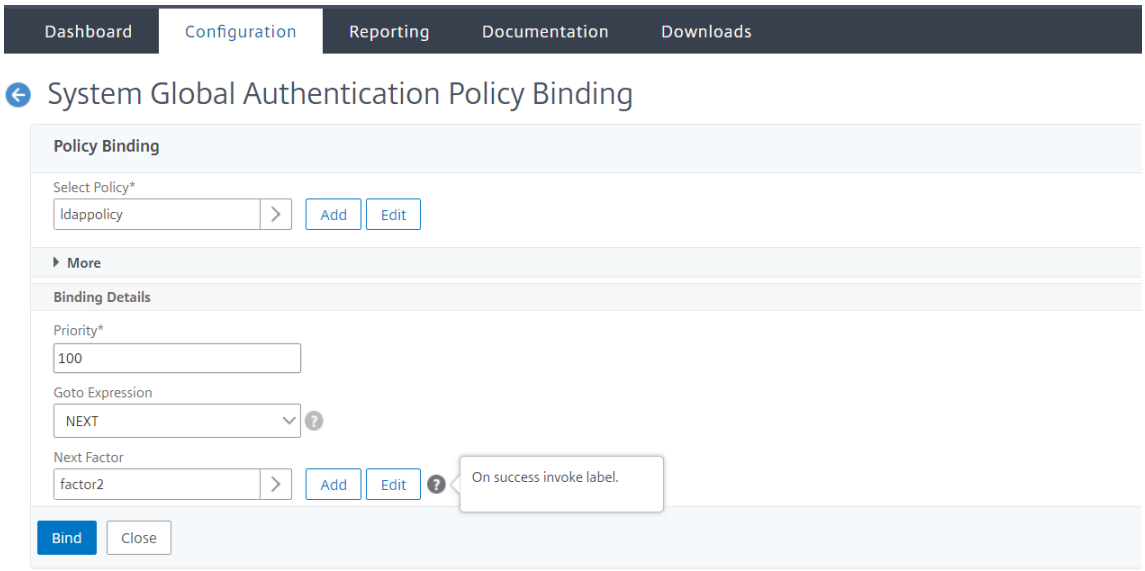
A continuación se presenta el fragmento de un archivo SingleAuth.xml donde 'SecondPassword: 'es el segundo nombre de campo de contraseña que se solicita al usuario que introduzca una segunda contraseña.

```
<?xml version="1.0" encoding="UTF-8"?>
<AuthenticateResponse xmlns="http://citrix.com/authentication/response/1">
<Status>success</Status>
<Result>more-info</Result>
<StateContext/>
<AuthenticationRequirements>
<PostBack>/nf/auth/doAuthentication.do</PostBack>
<CancelPostBack>/nf/auth/doLogoff.do</CancelPostBack>
<CancelButtonText>Cancel</CancelButtonText>
<Requirements>
<Requirement><Credential><ID>login</ID><SaveID>ExplicitForms-Username</SaveID><Type>username</Type></Credential><Label><Text>singleauth_user_name</Text><Type>nsg-login-label</Type></Label><Input><AssistiveText>singleauth_please_supply_either_domain\username_or_user@fully.qualified.domain</AssistiveText><Text><Secret>false</Secret><ReadOnly>false</ReadOnly><InitialValue/><Constraint>.+</Constraint></Text></Input></Requirement>
<Requirement><Credential><ID>passwd</ID><SaveID>ExplicitForms-Password</SaveID><Type>password</Type></Credential><Label><Text>SecondPassword:</Text><Type>nsg-login-label</Type></Label><Input><Text><Secret>true</Secret><ReadOnly>false</ReadOnly><InitialValue/><Constraint>.+</Constraint></Text></Input></Requirement>
<Requirement><Credential><Type>none</Type></Credential><Label><Text>singleauth_first_factor</Text><Type>nsg_confirmation</Type></Label><Input/></Requirement>
<Requirement><Credential><ID>saveCredentials</ID><Type>savecredentials</Type></Credential><Label><Text>singleauth_remember_my_password</Text><Type>nsg-login-label</Type></Label><Input><CheckBox><InitialValue>false</InitialValue></CheckBox></Input></Requirement>
<Requirement><Credential><ID>loginBtn</ID><Type>none</Type></Credential><Label><Type>none</Type></Label><Input><Button>singleauth_log_on</Button></Input></Requirement>
</Requirements>
</AuthenticationRequirements>
</AuthenticateResponse>
<!--NeedCopy-->
```


Configuración de la autenticación de dos factores mediante la GUI de Citrix ADC

1. Inicie sesión en el dispositivo Citrix ADC.
2. Vaya a **Sistema** > **Autenticación** > **Directivas avanzadas** > **Directiva**.
3. Haga clic en Agregar para crear la directiva de autenticación de primer nivel.
4. En la página **Crear directiva de autenticación**, establezca los siguientes parámetros.
    a) Name. Nombre de la directiva
    b) Tipo de acción. Seleccione el tipo de acción como LDAP, Active Directory, RADIUS, TACACS, etc.
    c) Acción. La acción de autenticación (perfil) que se va a asociar con la directiva. Puede elegir una acción de autenticación existente o hacer clic en el signo más y crear una acción del tipo adecuado.
    d) Expresión. Proporcione una expresión de directiva avanzada.
5. Haga clic en **Crear** y, a continuación, en **Cerrar**.
    a) Expresión. Proporcione una expresión de directiva avanzada.
6. Haga clic en **Crear**.
7. Haga clic en **Agregar** para crear la directiva de autenticación de segundo nivel.
8. En la página **Crear directiva de autenticación**, establezca los siguientes parámetros
    a) Name. Nombre de la directiva
    b) Tipo de acción. Seleccione el tipo de acción como LDAP, Active Directory, RADIUS, TACACS, etc.
    c) Acción. La acción de autenticación (perfil) que se va a asociar con la directiva. Puede elegir una acción de autenticación existente o hacer clic en el icono + para crear una acción del tipo adecuado.
    d) Expresión. Proporcionar una expresión de directiva avanzada
9. Haga clic en **Crear** y, a continuación, en **Cerrar**.
    a) Expresión. Proporcione una expresión de directiva avanzada.
10. Haga clic en **Crear**.
11. En la página **Directivas de autenticación**, haga clic en **Enlace global**.
12. En la página **Crear enlace de directiva de autenticación global**, seleccione la directiva de autenticación de primer nivel y haga clic en **Agregar enlace**.
13. En la página **Enlace de directivas**, seleccione la directiva de autenticación y establezca el siguiente parámetro de enlace de directivas.
    a) Siguiente factor. Seleccione la etiqueta de directiva de autenticación de segundo nivel.

14. Haga clic en **Aceptar** y **Cerrar**.



15. Haga clic en **Done**.
16. Inicie sesión en el dispositivo Citrix ADC para la autenticación de segundo nivel. Ahora el usuario puede proporcionar la segunda contraseña. Solo si ambas contraseñas son correctas, el usuario puede acceder al dispositivo Citrix ADC.

> **Nota**
>
> El TACACS configurado para una autenticación de segundo factor no admite la autorización y la contabilidad, incluso si lo habilita en el comando "TacacsAction". El segundo factor se utiliza únicamente para el propósito de autenticación.

Consulte también Autenticación de dos factores en el tema Autenticación nFactor de Citrix ADC .

Autenticación de usuario del sistema restringida a las interfaces de administración de Citrix ADC

August 20, 2021

Puede restringir el acceso de los usuarios del sistema a interfaces de administración específicas de Citrix ADC, como CLI o API. El `allowedManagementInterface` parámetro define la lista de interfaces de administración permitidas. Por ejemplo, si la interfaz de administración de un usuario o un grupo está establecida en API, todos los usuarios del grupo pueden acceder a Citrix ADC a través de API y no a través de CLI. Sin embargo, la GUI de Citrix ADC forma parte de la interfaz API y los usuarios con permiso de API también pueden acceder a la interfaz GUI.

> **Nota:**
>
> De forma predeterminada, los usuarios y grupos tienen acceso a todas las interfaces (CLI, API y GUI).

Puede configurar el parámetro en el nivel de usuario o en el nivel de grupo de usuarios. Cuando se configura a nivel de grupo, la configuración se aplica a todas las cuentas de usuario del grupo. Si un usuario está vinculado a varios grupos, el dispositivo permite el acceso a un conjunto agregado de interfaces de administración. Puede especificar la configuración de un usuario de un grupo configurando el parámetro a nivel de usuario. En este caso, la configuración de nivel de usuario está configurada para un grupo.
En determinados casos, cuando el cliente utiliza un servidor de autenticación externo para administrar cuentas de usuario, los detalles del servidor se configuran en el dispositivo. En este caso, el administrador puede crear un grupo de usuarios en el dispositivo Citrix ADC y agregar todos los usuarios (agrupados en el servidor externo) al grupo. Por ejemplo, todos los usuarios administrados en el servidor externo se agregan al grupo API_Users y el administrador puede configurar el grupo localmente en el dispositivo.

> **Nota:**
>
> El dispositivo Citrix ADC permite que solo el `nsroot` administrador (superusuario) configure el parámetro y no permite que ningún usuario del sistema cambie la configuración del parámetro.

Configurar el acceso de los usuarios a las interfaces de administración de Citrix ADC mediante la CLI

Para permitir el acceso de los usuarios a una interfaz de administración específica, debe establecer el parámetro de interfaz de administración permitida. En el símbolo del sistema, escriba:

```
set system group <groupName> [-allowedManagementInterface ( CLI | API )]
```

Ejemplo:

```
set system group network_usergroup -allowedManagementInterface CLI
```

Para obtener la descripción de los parámetros, consulte el tema de referencia de comandos de autenticación y autorización .

Para obtener información sobre las interfaces GUI y CLI de Citrix, consulte el tema Access Citrix ADC .

Configuraciones TCP

August 11, 2022

Las configuraciones TCP de un dispositivo Citrix ADC se pueden especificar en una entidad denominada perfil TCP, que es un conjunto de valores de configuración TCP. El perfil TCP se puede asociar a los servicios o servidores virtuales que quieran utilizar estas configuraciones TCP.

Se puede configurar un perfil TCP predeterminado para establecer las configuraciones TCP que se aplicarán de forma predeterminada, globalmente a todos los servicios y servidores virtuales.

> **Nota:**
>
> Cuando un parámetro TCP tiene valores diferentes para el servicio, el servidor virtual y globalmente, el valor de la entidad más específica (el servicio) tiene la prioridad más alta. El dispositivo Citrix ADC también proporciona otros enfoques para configurar TCP. Sigue leyendo para obtener más información.

Configuración TCP admitida

El dispositivo Citrix ADC admite las siguientes capacidades TCP:

Defender el TCP contra los ataques de suplantación

La **implementación de atenuación de ventanas de Citrix ADC** cumple con la norma RFC 4953.

Notificación explícita de congestión (ECN)

El dispositivo envía una notificación del estado de congestión de la red al remitente de los datos y toma medidas correctivas para la congestión de datos o la corrupción de datos. La implementación de ECN de Citrix ADC cumple con RFC 3168.

Medición del tiempo de ida y vuelta (RTTM) mediante la opción de marca de tiempo

Para que funcione la opción TimeStamp, al menos un lado de la conexión (cliente o servidor) debe admitirla. La implementación de Citrix ADC de la opción `TimeStamp` cumple con RFC 1323.

Detección de retransmisiones falsas

Esta detección se puede realizar mediante el reconocimiento selectivo duplicado de TCP (D-SACK) y la recuperación de RTO hacia adelante (F-RTO). Si hay retransmisiones falsas, las configuraciones de control de congestión se vuelven a su estado original. La implementación de Citrix ADC de D-SACK cumple con RFC 2883 y F-RTO cumple con RFC 5682.

Control de congestión

Esta funcionalidad utiliza algoritmos New-Reno, BIC, CUBIC, Nile y TCP Westwood.

Escalado de ventanas

Esto aumenta el tamaño de la ventana de **recepción de TCP** por encima de su valor máximo de 65.535 bytes.

Puntos a tener en cuenta antes de configurar el escalado de ventanas

- No se establece un valor alto para el factor de escala, ya que esto podría tener efectos adversos en el dispositivo y en la red.
- No configura el escalado de ventana a menos que sepa claramente por qué quiere cambiar el tamaño de la ventana.
- Ambos hosts de la conexión TCP envían una opción de escalado de ventana durante el establecimiento de la conexión. Si solo un lado de una conexión establece esta opción, no se utiliza la escala de la ventana para la conexión.
- Cada conexión de la misma sesión es una sesión de escalado de ventanas independiente. Por ejemplo, cuando la solicitud de un cliente y la respuesta del servidor fluyen a través del dispositivo, es posible tener escalado de ventana entre el cliente y el dispositivo sin escalarlo entre el dispositivo y el servidor.

Ventana Congestión máxima de TCP

El tamaño de la ventana es configurable por el usuario. El valor predeterminado es de 8190 bytes.

Reconocimiento selectivo (SACK)

Utiliza el receptor de datos (ya sea un dispositivo Citrix ADC o un cliente) que notifica al remitente todos los segmentos que se han recibido correctamente.

Reconocimiento directo (FACK)

Esta funcionalidad evita la congestión de TCP midiendo explícitamente el número total de bytes de datos pendientes en la red y ayudando al remitente (ya sea un Citrix ADC o un cliente) a controlar la cantidad de datos inyectados en la red durante los tiempos de espera de retransmisión.

Multiplexación de conexiones TCP

Esta funcionalidad permite reutilizar las conexiones TCP existentes. El dispositivo Citrix ADC almacena conexiones TCP establecidas al grupo de reutilización. Cada vez que se recibe una solicitud de cliente, el dispositivo comprueba si hay una conexión disponible en el grupo de reutilización y sirve al nuevo cliente si la conexión está disponible. Si no está disponible, el dispositivo crea una conexión para la solicitud del cliente y almacena la conexión en el grupo de reutilización. Citrix ADC admite la multiplexación de conexiones para los tipos de conexión HTTP, SSL y DataStream.

Almacenamiento en búfer de recepción dinámico

Esto permite que el búfer de recepción se ajuste dinámicamente en función de las condiciones de la memoria y de la red.

Conexión MPTCP

Conexiones MPTCP entre el cliente y Citrix ADC. Las conexiones MPTCP no se admiten entre Citrix ADC y el servidor back-end. La implementación de Citrix ADC de MPTCP cumple con RFC 6824.

Puede ver las estadísticas MPTCP, como las conexiones MPTCP activas y las conexiones de subflujo activas, mediante la interfaz de línea de comandos.

En el símbolo del sistema, escriba uno de los siguientes comandos para mostrar un resumen o un resumen detallado de las estadísticas MPTCP, o para borrar la visualización de estadísticas:

1. `Stat MPTCP`
2. `Stat mptcp -detail`
3. `Clearstats basic`

> **Nota:**
>
> Para establecer una conexión MPTCP, tanto el cliente como el dispositivo Citrix ADC deben admitir la misma versión MPTCP. Si utiliza el dispositivo Citrix ADC como puerta de enlace MPTCP para sus servidores, los servidores no tienen por qué ser compatibles con MPTCP. Cuando el cliente inicia una nueva conexión MPTCP, el dispositivo identifica la versión MPTPC del cliente en la opción MP_CAPABALE del paquete SYN. Si la versión del cliente es superior a la admitida en el dispositivo, el dispositivo indica su versión más alta en la opción MP_CAPABALE del paquete SYN-ACK. A continuación, el cliente vuelve a una versión inferior y envía el número de versión en la opción MP_CAPABALE del paquete ACK. Si esa versión es compatible, el dispositivo continúa con la conexión MPTCP. De lo contrario, el dispositivo recurriese a un TCP normal. El dispositivo Citrix ADC no inicia subflujos (MP_JOIN). El dispositivo espera que el cliente inicie subflujos.

Compatibilidad con anuncios de direcciones adicionales (ADD_ADDR) en MPTCP

En una implementación MPTCP, si tiene un servidor virtual vinculado con un conjunto de IP que tiene direcciones IP de servidor virtual adicionales, la funcionalidad de anuncio de direcciones adicional (ADD_ADDR) anuncia la dirección IP de los servidores virtuales enlazados al conjunto de IP. Los clientes pueden iniciar subflujos `MP-JOIN` adicionales a las direcciones IP anunciadas.

Puntos que debe recordar acerca de la funcionalidad MPTCP ADD_ADDR

- Puede enviar un máximo de 10 direcciones IP como parte de la opción ADD_ADDR. Si hay más de 10 direcciones IP con el parámetro mptcpAdvertise habilitado, después de anunciar la dirección IP 10, el dispositivo ignora el resto de las direcciones IP.
- Si el subflujo MP-CAPABLE se realiza en una de las direcciones IP del conjunto de IP en lugar de la dirección IP del servidor virtual principal, la dirección IP del servidor virtual se anuncia si el parámetro mptcpAdvertise está habilitado para la dirección IP del servidor virtual.

Configurar más publicidad de direcciones (ADD_ADDR) para anunciar direcciones VIP adicionales mediante la CLI

Puede configurar la funcionalidad MPTCP ADD_ADDR para los tipos de direcciones IPv4 e IPv6. En general, se pueden conectar varias IP IPv4 e IPv6 a un único conjunto de IP y el parámetro se puede habilitar en cualquier subconjunto de direcciones IP. En la función ADD_ADDR, solo se anuncian las direcciones IP que tienen activada la opción “mptcpAdvertise” y se ignoran las direcciones IP restantes del conjunto de IP.
Siga los siguientes pasos para configurar la función ADD_ADDR:

1. Agregue un conjunto de IP.
2. Agregue una dirección IP de tipo IP de servidor virtual (VIP) con la publicidad MPTCP habilitada.
3. Vincule la dirección IP con el conjunto de IP.
4. Configure el conjunto de IP con el servidor virtual de equilibrio de carga.

Agregar un conjunto de IP

En el símbolo del sistema, escriba:

```
add ipset <name> [-td <positive_integer>]
<!--NeedCopy-->
```

Ejemplo:

```
add ipset ipset_1
<!--NeedCopy-->
```

Agregar una dirección IP de tipo IP de servidor virtual (VIP) con la publicidad MPTCP habilitada

En el tipo de comando:


```
add ns ip <IPAddress>@ <netmask> [-mptcpAdvertise ( YES | NO )] -type <
    type>
<!--NeedCopy-->
```

Ejemplo:

```
add ns ip 10.10.10.10 255.255.255.255 -mptcpAdvertise YES -type VIP
```

Vincular direcciones IP al conjunto de IP

En el símbolo del sistema, escriba:

```
bind ipset <name> <IPAddress>
<!--NeedCopy-->
```

Ejemplo:

```
bind ipset ipset_1 10.10.10.10
```

Configurar el conjunto de IP para servidor virtual de equilibrio de carga

En el símbolo del sistema, escriba:

```
set lb vserver <name> [-ipset  <string>]
<!--NeedCopy-->
```

Ejemplo:

```
set lb vserver lb1 -ipset ipset_1
<!--NeedCopy-->
```

Configuración de ejemplo:

```
Add ipset ipset_1
add ns ip 10.10.10.10 255.255.255.255 -mptcpAdvertise YES -type VIP
bind ipset ipset_1 10.10.10.10
set lb vserver lb1 -ipset ipset_1
<!--NeedCopy-->
```


Configurar la dirección IP externa de publicidad mediante la funcionalidad ADD_ADDR

Si la dirección IP anunciada es propiedad de la entidad externa y el dispositivo Citrix ADC necesita anunciar la dirección IP, el parámetro “MPTCPAdvertise” debe habilitarse con los parámetros de estado y ARP inhabilitados.

Siga los siguientes pasos para configurar ADD_ADDR para publicitar la dirección IP externa.

1. Agregue una dirección IP de tipo IP de servidor virtual (VIP) con la publicidad MPTCP habilitada.
2. Vincule la dirección IP con el conjunto de IP.
3. Vincular conjunto de IP con el servidor virtual de equilibrio de carga

Agregar una dirección IP externa de tipo IP de servidor virtual (VIP) con la publicidad MPTCP habilitada

En el símbolo del sistema, escriba:

```
1 add ns ip <IPAddress>@ <External-IP-mask -type VIP> [-mptcpAdvertise (
     YES | NO )] -type <type> -state DISABLED -arp DISABLED
2 <!--NeedCopy-->
```

Ejemplo:

```
add ns ip 10.10.10.10 255.255.255.255 -mptcpAdvertise YES -type VIP -state
DISABLED -arp DISABLED
```

Vincular direcciones IP al conjunto de IP

En el símbolo del sistema, escriba:

```
1 bind ipset <name> <IPAddress>
2 <!--NeedCopy-->
```

Ejemplo:

```
bind ipset ipset_1 10.10.10.10
```

Configurar el conjunto de IP para servidor virtual de equilibrio de carga

En el símbolo del sistema, escriba:


```
set lb vserver <name> [-ipset  <string>]
<!--NeedCopy-->
```

Ejemplo:

```
set lb vserver lb1 -ipset ipset_1
```

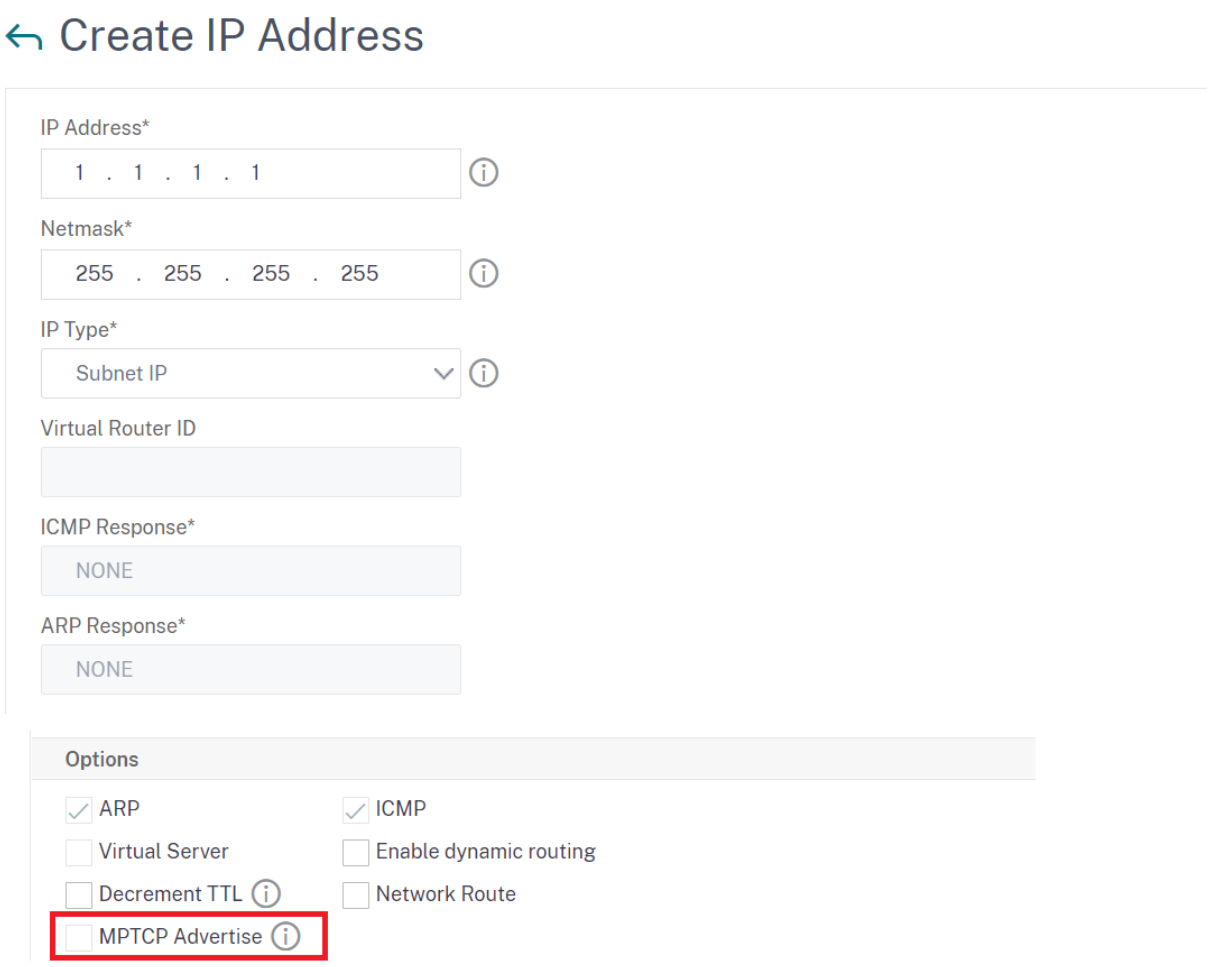
Configuración de ejemplo:

```
add ns ip 10.10.10.10 255.255.255.255 -mptcpAdvertise YES -type VIP
   state DISABLED -arp DISABLED
bind ipset ipset_1 10.10.10.10
set lb vserver lb1 -ipset ipset_1
<!--NeedCopy-->
```

Anunciar una dirección IP a los clientes habilitados para MPTCP mediante la GUI de Citrix ADC

Complete el siguiente paso para anunciar la dirección IP a los clientes habilitados para MPTCP:

1. Vaya a **Sistema > Red > IP**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En la página **Crear dirección IP**, active la casilla de verificación **Publicidad MPTCP** para establecer el parámetro. De forma predeterminada, está inhabilitada.



Extracción de la opción de superposición de ruta TCP/IP e inserción del encabezado HTTP Client-IP

Extracción de superposición de ruta TCP/IP e inserción de encabezado HTTP Client-IP. El transporte de datos a través de redes superpuestas suele utilizar la terminación de la conexión o la traducción de direcciones de red (NAT), en las que se pierde la dirección IP del cliente de origen. Para evitarlo, el dispositivo Citrix ADC extrae la opción de superposición de rutas TCP/IP e inserta la dirección IP del cliente de origen en el encabezado HTTP. Con la dirección IP en el encabezado, el servidor web puede identificar el cliente de origen que realizó la conexión. Los datos extraídos son válidos durante toda la vida de la conexión TCP y, por lo tanto, evita que el host de salto siguiente tenga que interpretar la opción de nuevo. Esta opción solo se aplica a los servicios web que tienen habilitada la opción de inserción de IP de cliente.

Descarga de segmentación TCP

Descarga la segmentación TCP a la NIC. Si establece la opción como “AUTOMÁTICO”, la segmentación TCP se descarga en la NIC, si se admite la NIC.

cookie de sincronización para el enlace TCP con los clientes

Esto se utiliza para resistir ataques de inundación SYN. Puede habilitar o inhabilitar el mecanismo `SYNCOOKIE` para el intercambio de manos TCP con los clientes. La desactivación de `SYNCOOKIE` evita la protección contra ataques `SYN` en el dispositivo Citrix ADC.

Aprendizaje de MSS para habilitar el aprendizaje de MSS para todos los servidores virtuales configurados en el dispositivo

Parámetros TCP compatibles

En la tabla siguiente se proporciona una lista de los parámetros TCP y su valor predeterminado configurado en un dispositivo Citrix ADC.

|Parámetro|Valor predeterminado|Descripción|
|— |— |— |
|Gestión de ventanas|
Temporizador TCP retrasado	100 miliseg	Tiempo de espera para TCP retrasado ACK, en milisegundos.
Tiempo de espera mínimo de retransmisión (RTO) TCP en millones de segundos	1000 millones seg	Tiempo de espera mínimo de retransmisión, en milisegundos, especificado en incrementos de 10 milisegundos (el valor debe generar un número entero si se divide por 10)
Tiempo de inactividad de la conexión antes de iniciar las sondas keep-alive	900 segundos	Desconecte silenciosamente las conexiones establecidas por TCP en tiempos de espera inactivos, conexiones establecidas en tiempo de espera por inactividad
Opción de marca de hora TCP	INHABILITADO	La opción de marca de tiempo permite una medición RTT precisa. Habilitar o inhabilitar la opción Marca de tiempo TCP.
Tiempo de espera de sesión TCP multiruta	0 segundos	Tiempo de espera de la sesión MPTCP en segundos. Si este valor no está establecido, inactivo. Las sesiones MPTCP se vacían después del tiempo de espera por inactividad del cliente del servidor virtual.
Suelte silenciosamente las conexiones semicerradas en tiempo de espera inactivo	0 segundos	Desconecte silenciosamente las conexiones TCP semicerradas en el tiempo de espera inactivo.
Suelta silenciosamente las conexiones establecidas en el tiempo de espera inactivo	INHABILITADO	Se eliminan silenciosamente las conexiones establecidas por TCP en el tiempo de espera inactivo
Administración de la memoria
Tamaño del búfer TCP	131072 octetos	El tamaño del búfer TCP es el tamaño del búfer de recepción

en Citrix ADC. Este tamaño de búfer se anuncia a clientes y servidores desde Citrix ADC y controla su capacidad para enviar datos a Citrix ADC. El tamaño del búfer predeterminado es de 8K y, por lo general, es seguro aumentarlo cuando se habla con comunidades de servidores internas. El tamaño del búfer también se vaya afectado por la capa de aplicación real de Citrix ADC, como en los casos de dispositivos de punto final SSL, se establece en 40 K y para Compresión en 96 K. **Nota:** El argumento de tamaño del búfer debe establecerse para que se realicen ajustes dinámicos.|
Tamaño del búfer de envío TCP	8190 bytes	Tamaño del búfer de envío TCP
Búfer de recepción dinámica TCP	INHABILITADO	Habilita o inhabilita el búfer de recepción dinámica. Cuando está habilitado, permite que el búfer de recepción se ajuste dinámicamente en función de las condiciones de la memoria y de la red. **Nota:** El argumento de tamaño del búfer debe establecerse para que se realicen ajustes dinámicos
Ventana de congestión TCP Max (CWND)	524288 bytes	Ventana Congestión máxima de TCP
Estado de escalado de ventana	HABILITADO	Habilita o inhabilita el escalado de ventanas.
Factor de escala de ventana	8	Factor utilizado para calcular el tamaño de la nueva ventana. Este argumento solo es necesario cuando el escalado de ventana está habilitado.
Configuración de conexión
Sondas Keep-alive	INHABILITADO	Envía sondeos de mantenimiento (KA) TCP periódicos para comprobar si el par sigue activo.
Tiempo de inactividad de la conexión antes de iniciar las sondas keep-alive	900 segundos	Duración, en segundos, para que la conexión esté inactiva, antes de enviar una sonda keep-alive (KA).
Intervalo de sonda Keep-alive	75 segundos	Intervalo de tiempo, en segundos, antes de la siguiente sonda keep-alive (KA), si el par no responde.
Sondeos keep-alive máximos que se deben omitir antes de interrumpir la conexión.	3	Número de sondeos keep-alive (KA) que se enviarán cuando no se reconozcan, antes de suponer que el par está inactivo.
Atenuación de ventana RST (protección contra falsificación).	INHABILITADO	Habilite o inhabilite la atenuación de la ventana de RST para protegerse contra la suplantación de identidad. Cuando está habilitada, la respuesta es con ACK correctivo cuando un número de secuencia no es válido.
Acepte RST con el último número de secuencia reconocido.	HABILITADO
Transferencia de datos
ACK inmediato en el paquete PUSH	HABILITADO	Envíe acuse de recibo positivo inmediato (ACK) al recibir paquetes TCP con el indicador PUSH.
Paquetes máximos por MSS	0	Número máximo de octetos permitidos en un segmento de datos TCP
Algoritmo de Nagle	INHABILITADO	El algoritmo de Nagle combate el problema de los paquetes pequeños en la transmisión TCP. Aplicaciones como Telnet y otros motores en tiempo real que requieren que cada pulsación de tecla se pase al otro lado suelen crear paquetes pequeños. Con el algoritmo de Nagle, Citrix ADC puede almacenar en búfer esos paquetes pequeños y enviarlos juntos para aumentar la eficiencia de la conexión. Este algoritmo debe funcionar junto con otras técnicas de optimización TCP en Citrix ADC.

|Máximo de segmentos TCP permitidos en una ráfaga|10 MSS|Número máximo de segmentos TCP permitidos en una ráfaga|
|Paquetes máximos fuera de servicio para poner en cola|300|Tamaño máximo de la cola de paquetes fuera de servicio. Un valor de 0 significa que no hay límite|
|Control de congestión|
Tipo de TCP	CUBIC
Configuración de la ventana de congestión inicial (cwnd)	4 MSS	Límite superior máximo inicial del número de paquetes TCP que pueden quedar pendientes en el enlace TCP al servidor
Notificación de congestión explícita de TCP (ECN)	INHABILITADO	La notificación explícita de congestión (ECN) proporciona una notificación de extremo a extremo de la congestión de la red sin perder paquetes.
Ventana de congestión TCP Max (CWND)	524288 bytes	TCP mantiene una ventana de congestión (CWND), lo que limita el número total de paquetes no reconocidos que pueden estar en tránsito de extremo a extremo. En TCP, la ventana de congestión es uno de los factores que determina el número de bytes que pueden estar pendientes en cualquier momento. La ventana de congestión es un medio para evitar que un enlace entre el remitente y el receptor se sobrecargue con demasiado tráfico. Se calcula calculando cuánta congestión hay en el enlace.
Inicio híbrido TCP (HyStart)	8 bytes
Tiempo de espera mínimo de retransmisión (RTO) TCP en millones de segundos	1000	Tiempo de espera mínimo de retransmisión, en milisegundos, especificado en incrementos de 10 milisegundos (el valor debe producir un número entero si se divide por 10).
Umbral de dupack TCP	INHABILITADO
Control de velocidad de ráfaga	3	Control de velocidad de ráfaga TCP DESACTIVADO/FIJO O DINÁMICO. FIJO requiere que se establezca una tasa TCP
Tasa TCP	INHABILITADO	Velocidad de envío de carga útil de conexión TCP en KB/s
Cola máxima de velocidad TCP	0	Tamaño máximo de cola de conexión en bytes, cuando se utiliza BurstRateControl.
MPTCP
TCP multitrayecto	INHABILITADO	TCP multirruta (MPTCP) es un conjunto de extensiones a TCP normal para proporcionar un servicio TCP multirruta, que permite que una conexión de transporte funcione a través de múltiples rutas simultáneamente.
Datos de caída de TCP multiruta en un subflujo preestablecido	INHABILITADO	Habilite o inhabilite la supresión silenciosa de los datos en el subflujo preestablecido. Cuando se habilita, los paquetes de datos DSS se descartan de forma silenciosa en lugar de interrumpir la conexión cuando se reciben datos en un subflujo preestablecido.
TCP multirruta de apertura rápida	INHABILITADO	Habilite o inhabilite la apertura rápida de TCP multiruta. Cuando se habilita, los paquetes de datos DSS se aceptan antes de recibir el tercer paquete de protocolo de enlace SYN.
Tiempo de espera de sesión TCP multiruta	0 segundos	Tiempo de espera de la sesión MPTCP en

segundos. Si no se establece este valor, las sesiones MPTCP inactivas se vacían después del tiempo de espera por inactividad del cliente del servidor virtual.|
|Seguridad|
|Protección contra la suplantación SYN|INHABILITADO|Habilite o inhabilite la suplantación de paquetes SYN no válidos para protegerse contra la suplantación de identidad. Cuando se inhabilita, las conexiones establecidas se restablecen cuando se recibe un paquete SYN.|
|Syncookie TCP|INHABILITADO|Esto se utiliza para resistir ataques de inundación SYN. Habilita o inhabilita el mecanismo SYNCOOKIE para el enlace TCP con los clientes. La desactivación de SYNCOOKIE impide la protección contra ataques SYN en el dispositivo Citrix ADC.|
|Detección y recuperación de pérdidas|
Reconocimiento selectivo duplicado (DSACK)	HABILITADO	Un dispositivo Citrix ADC utiliza el reconocimiento selectivo duplicado (DSACK) para determinar si una retransmisión se envió por error.
Recuperación de RTO hacia adelante (FRTO)	HABILITADO	Detecta tiempos de espera de retransmisión TCP falsos. Después de retransmitir el primer segmento no reconocido desencadenado por un tiempo de espera, el algoritmo del remitente TCP supervisa los acuses de recibo entrantes para determinar si el tiempo de espera fue falso. A continuación, decide si quiere enviar nuevos segmentos o retransmitir segmentos no confirmados. El algoritmo ayuda eficazmente a evitar otras retransmisiones innecesarias y, por lo tanto, mejora el rendimiento de TCP en caso de un tiempo de espera fúrico.
Reconocimiento de reenvío TCP (FACK)	HABILITADO	Activa o desactiva FACK (Forward ACK).
Estado de reconocimiento selectivo (SACK)	HABILITADO	TCP SACK soluciona el problema de pérdidas de varios paquetes, lo que reduce la capacidad de rendimiento general. Con un acuse de recibo selectivo, el receptor puede informar al remitente sobre todos los segmentos que se han recibido correctamente, lo que permite al remitente solo retransmitir los segmentos que se han perdido. Esta técnica ayuda a Citrix ADC a mejorar el rendimiento general y reducir la latencia de conexión.
Paquetes máximos por retransmisión	1	Permite a Citrix ADC controlar cuántos paquetes se retransmitirán en un intento. Cuando Citrix ADC recibe una ACK parcial y tiene que realizar una retransmisión, se tiene en cuenta esta configuración. Esto no afecta a las retransmisiones basadas en RTO.
Temporizador TCP retrasado	100 milisegundos	Tiempo de espera para ACK retrasado de TCP, en milisegundos
Optimización del TCO
Modo de optimización TCP	TRANSPARENT	Modos de optimización TCP TRANSPARENT/ENDPOINT
Aplicar optimizaciones TCP adaptativas	INHABILITADO	Aplicar optimizaciones TCP adaptativas
Descarga de segmentación TCP	AUTOMÁTICO	Descargue la segmentación TCP a la NIC. Si se establece en AUTOMATIC, la segmentación TCP se descarga a la NIC, si la NIC lo admite.
Agregación ACK	INHABILITADO	Habilitar o inhabilitar la agregación ACK
Tiempo de espera TCP (o Time_wait)	40 segundos	Tiempo transcurrido antes de liberar una conexión TCP cerrada
Desvincular cliente y servidor en RST	INHABILITADO	Desvincular la conexión cliente y servidor,

cuando hay
datos pendientes que se enviarán al otro lado. |

> **Nota:**
> Cuando HTTP/2 está habilitado, Citrix recomienda inhabilitar el parámetro Almacenamiento en búfer de recepción dinámica de TCP en el perfil TCP.

Configuración de parámetros TCP globales

El dispositivo Citrix ADC permite especificar valores para los parámetros TCP aplicables a todos los servicios y servidores virtuales de Citrix ADC. Esto se puede hacer mediante:

- Perfil TCP predeterminado
- Comando TCP global
- Función de almacenamiento en búfer TCP

> **Nota**:
>
> El parámetro `recvBuffSize` del comando set ns tcpParam queda obsoleto a partir de la versión 9.2. En versiones posteriores, establezca el tamaño del búfer mediante el parámetro `bufferSize` del comando set ns tcpProfile. Si actualiza a una versión en la que el parámetro `recvBuffSize` está obsoleto, el parámetro `bufferSize` se establece en su valor predeterminado.

Perfil TCP predeterminado

Un perfil TCP, denominado como `nstcp_default_profile`, se utiliza para especificar las configuraciones TCP que se utilizan si no se proporcionan configuraciones TCP a nivel de servicio o servidor virtual.

> **Notas:**
>
> - No todos los parámetros TCP se pueden configurar mediante el perfil TCP predeterminado. Algunas configuraciones deben realizarse mediante el comando TCP global (consulte la sección siguiente).
> - El perfil predeterminado no tiene que estar vinculado explícitamente a un servicio o servidor virtual.

Para configurar el perfil TCP predeterminado

- Mediante la interfaz de línea de comando, en la solicitud de comando escriba:

```
set ns tcpProfile nstcp_default_profile...
<!--NeedCopy-->
```


- En la GUI, vaya a **Sistema** > **Perfiles**, haga clic en **Perfiles TCP** y actualice nstcp_default_profile.

Comando TCP global

Otro enfoque que puede utilizar para configurar los parámetros TCP globales es el comando TCP global. Además de algunos parámetros únicos, este comando duplica algunos parámetros que se pueden establecer mediante un perfil TCP. Cualquier actualización realizada en estos parámetros duplicados se refleja en el parámetro correspondiente del perfil TCP predeterminado.

Por ejemplo, si el parámetro SACK se actualiza con este enfoque, el valor se refleja en el parámetro SACK del perfil TCP predeterminado (nstcp_default_profile).

> **Nota:**
>
> Citrix recomienda utilizar este enfoque solo para los parámetros TCP que no están disponibles en el perfil TCP predeterminado.

Para configurar el comando TCP global

- Mediante la interfaz de línea de comando, en la solicitud de comando escriba:

```
1 set ns tcpParam …
2 <!--NeedCopy-->
```

- En la GUI, vaya a **Sistema > Configuración**, haga clic en **Cambiar parámetros TCP** y, a continuación, actualice los parámetros TCP necesarios.

Función de almacenamiento en búfer TCP

Citrix ADC proporciona una función denominada búfer TCP que puede utilizar para especificar el tamaño del búfer TCP. La función se puede habilitar globalmente o a nivel de servicio.

> **Nota:**
>
> El tamaño del búfer también se puede configurar en el perfil TCP predeterminado. Si el tamaño del búfer tiene valores diferentes en la función de almacenamiento en búfer TCP y en el perfil TCP predeterminado, se aplica el valor mayor.

Configurar la función de almacenamiento en búfer TCP globalmente

- En la solicitud de comando escriba:

  habilitar el modo ns TCPB

  ```
  set ns tcpbufParam -size <positiveInteger> -memLimit <positiveInteger>
  ```


- En la GUI, vaya a **Sistema** > **Configuración**, haga clic en **Configurar modos** y, a continuación, seleccione **Almacenamiento en búfer TCP**.

  Además, vaya a **Sistema** > **Configuración**, haga clic en **Cambiar parámetros TCP**, especifique valores para **Tamaño de búfer** y **Límite de uso de memoria**.

Configuración de parámetros TCP específicos del servicio o del servidor virtual

Mediante los perfiles TCP, puede especificar parámetros TCP para servicios y servidores virtuales. Debe definir un perfil TCP (o utilizar un perfil TCP integrado) y asociarlo con el servicio y el servidor virtual adecuados.

> **Nota:**
>
> También puede modificar los parámetros TCP de los perfiles predeterminados según sus necesidades.

Puede especificar el tamaño del búfer TCP a nivel de servicio mediante los parámetros especificados por la función de almacenamiento en búfer TCP.

Para especificar configuraciones TCP a nivel de servicio o servidor virtual mediante la interfaz de línea de comandos

En el símbolo del sistema, realice lo siguiente:

1. Configure el perfil TCP.

```
set ns tcpProfile <profile-name>...
<!--NeedCopy-->
```

2. Enlazar el perfil TCP al servicio o al servidor virtual.

```
    set service <name> ....
    <!--NeedCopy-->
```

Ejemplo:

```
> set service service1 -tcpProfileName profile1
```

Para enlazar el perfil TCP al servidor virtual:

```
set lb vserver <name> ....
<!--NeedCopy-->
```


Ejemplo:

```
> set lb vserver lbvserver1 -tcpProfileName profile1
<!--NeedCopy-->
```

Para especificar configuraciones TCP de nivel de servidor virtual o de servicio mediante la interfaz gráfica de usuario

En la GUI, realice lo siguiente:

1. Configure el perfil TCP.

   Vaya a **Sistema** > **Perfiles** > **Perfiles TCP**y cree el perfil TCP.

2. Enlazar el perfil TCP al servicio o al servidor virtual.

   Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servicios/Servidores virtuales**y cree el perfil TCP, que debe estar vinculado al servicio o al servidor virtual.

Perfiles TCP incorporados

Para facilitar la configuración, Citrix ADC proporciona algunos perfiles TCP integrados. Revise los perfiles integrados que aparecen en la lista siguiente y seleccione un perfil y utilícelo tal como está o modifíquelo para cumplir con sus requisitos. Puede vincular estos perfiles a los servicios o servidores virtuales requeridos.

Perfil incorporado	Descripción
nstcp_default_profile	Representa la configuración TCP global predeterminada del dispositivo.
nstcp_default_tcp_lan	Útil para conexiones de servidor back-end, donde estos servidores residen en la misma LAN que el dispositivo.
nstcp_default_WAN	Útil para implementaciones WAN.
nstcp_default_tcp_lan_thin_stream	Similar al perfil nstcp_default_tcp_lan. Sin embargo, la configuración se ajusta a flujos de paquetes de tamaño pequeño.
nstcp_default_tcp_interactive_stream	Similar al perfil nstcp_default_tcp_lan. Sin embargo, tiene un temporizador ACK retardado reducido y ACK en la configuración de **paquetes PUSH**.

Perfil incorporado	Descripción
nstcp_default_tcp_lfp	Útil para redes de procesos gruesos y largos (WAN) del lado del cliente. Las redes de procesos largos y gruesos tienen líneas de larga demora y gran ancho de banda con mínimas caídas de paquetes.
nstcp_default_tcp_lfp_thin_stream	Similar al perfil nstcp_default_tcp_lfp. Sin embargo, la configuración está ajustada para flujos de paquetes de tamaño pequeño.
nstcp_default_tcp_lnp	Útil para redes de procesos largos y estrechos (WAN) del lado del cliente. Las redes de procesos largos y estrechos tienen pérdidas de paquetes considerables ocasionalmente.
nstcp_default_tcp_lnp_thin_stream	Similar al perfil nstcp_default_tcp_lnp. Sin embargo, la configuración está ajustada para flujos de paquetes de tamaño pequeño.
nstcp_internal_apps	Útil para aplicaciones internas del dispositivo (por ejemplo, sincronización de sitios GSLB). Contiene opciones de ajuste de escala de ventana y SACK para las aplicaciones deseadas. Este perfil no debe vincularse a aplicaciones distintas de las aplicaciones internas.
nstcp_default_mobile_profile	Útil para dispositivos móviles.
nstcp_default_XA_XD_profile	Útil para la implementación de Citrix Virtual Apps and Desktops.

Configuraciones TCP de ejemplo

Ejemplos de interfaz de línea de comandos de ejemplo para configurar lo siguiente:

Defender el TCP contra los ataques de suplantación

Permita que Citrix ADC defienda a TCP contra ataques de suplantación. De forma predeterminada, el parámetro “rstWindowAttenuation” está inhabilitado. Este parámetro está habilitado para proteger el dispositivo contra la suplantación de identidad. Si lo habilita, responde con acuse de recibo correctivo (ACK) para un número de secuencia no válido. Los valores posibles son habilitado o inhabilitado.

Donde el parámetro de atenuación de ventana RST protege el dispositivo contra la suplantación. Cuando esté habilitada, responda con ACK correctivo cuando un número de secuencia no es válido.

```
1      > set ns tcpProfile profile1 -rstWindowAttenuate ENABLED -
          spoofSynDrop ENABLED
2      Done
3      > set lb vserver lbvserver1 -tcpProfileName profile1
4      Done
5  <!--NeedCopy-->
```

Notificación explícita de congestión (ECN)

`Enable ECN on the required TCP profile`

```
1      > set ns tcpProfile profile1 -ECN ENABLED
2      Done
3      > set lb vserver lbvserver1 -tcpProfileName profile1
4      Done
5  <!--NeedCopy-->
```

Reconocimiento selectivo (SACK)

Habilite SACK en el perfil TCP requerido.

```
1      > set ns tcpProfile profile1 -SACK ENABLED
2      Done
3      > set lb vserver lbvserver1 -tcpProfileName profile1
4      Done
5  <!--NeedCopy-->
```

Reconocimiento directo (FACK)

Habilite FACK en el perfil TCP requerido.

```
1  > set ns tcpProfile profile1 -FACK ENABLED
2  > set lb vserver lbvserver1 -tcpProfileName profile1
3  <!--NeedCopy-->
```


Escalado de ventanas (WS)

Habilite el escalado de ventana y defina el factor de escala de ventana en el perfil TCP requerido.

```
set ns tcpProfile profile1  -WS ENABLED  -WSVal 9
Done
set lb vserver lbvserver1 -tcpProfileName profile1
Done
<!--NeedCopy-->
```

Tamaño máximo de segmento (MSS)

Actualice las configuraciones relacionadas con MSS.

```
> set ns tcpProfile profile1  -mss 1460 - maxPktPerMss 512
Done
> set lb vserver lbvserver1 -tcpProfileName profile1
Done
<!--NeedCopy-->
```

Citrix ADC para aprender el MSS de un servidor virtual

Habilite Citrix ADC para aprender el VSS y actualizar otras configuraciones relacionadas.

```
> set ns tcpParam -learnVsvrMSS ENABLED  -mssLearnInterval 180 -
   mssLearnDelay 3600
Done
<!--NeedCopy-->
```

TCP keep-alive

Habilite el mantenimiento activo de TCP y actualice otras configuraciones relacionadas.

```
> set ns tcpProfile profile1 -KA ENABLED -KaprobeUpdateLastactivity ENABLED
-KAconnIdleTime 900 -KAmaxProbes 3 -KaprobeInterval 75
Done
> set lb vserver lbvserver1 -tcpProfileName profile1
Done
```


Tamaño del búfer: uso del perfil TCP

Especifique el tamaño del búfer.

```
> set ns tcpProfile profile1 -bufferSize 8190
Done
> set lb vserver lbvserver1 -tcpProfileName profile1
Done
```

Tamaño del búfer: uso de la función de almacenamiento en búfer TCP

Habilite la función de almacenamiento en búfer TCP (globalmente o para un servicio) y, a continuación, especifique el tamaño del búfer y el límite de memoria.

```
> enable ns feature TCPB
Done
> set ns tcpbufParam -size 64 -memLimit 64
Done
```

MPTCP

Habilite MPTCP y, a continuación, establezca las configuraciones opcionales de MPTCP.

```
> set ns tcpProfile profile1 -mptcp ENABLED
Done
> set ns tcpProfile profile1 -mptcpDropDataOnPreEstSF ENABLED -mptcpFastOpen
 ENABLED -mptcpSessionTimeout 7200
Done
> set ns tcpparam -mptcpConCloseOnPassiveSF ENABLED -mptcpChecksum ENABLED
-mptcpSFtimeout 0 -mptcpSFReplaceTimeout 10
-mptcpMaxSF 4 -mptcpMaxPendingSF 4 -mptcpPendingJoinThreshold 0 -mptcpRTOsToSwitchSF
 2 -mptcpUseBackupOnDSS ENABLED
Done
```

Control de congestión

Defina el algoritmo de control de congestión TCP necesario.

```
set ns tcpProfile profile1 -flavor Westwood
Done
> set lb vserver lbvserver1 -tcpProfileName profile1
Done
```


Almacenamiento en búfer de recepción dinámico

Habilite el almacenamiento en búfer de recepción dinámica en el perfil TCP necesario.

```
> set ns tcpProfile profile1 -dynamicReceiveBuffering ENABLED
Done
> set lb vserver lbvserver1 -tcpProfileName profile1
Done
```

Admite para TCP Fast Open (TFO) en TCP Multipath (MPTCP)

Un dispositivo Citrix ADC ahora admite el mecanismo TCP Fast Open (TFO) para establecer conexiones TCP de múltiples rutas (MPTCP) y acelerar las transferencias de datos. El mecanismo permite que los datos de subflujo se transportan durante el enlace inicial de conexión MPTCP en paquetes SYN y SYN-ACK y también permite que los datos sean consumidos por el nodo receptor durante el establecimiento de la conexión MPTCP.

Para obtener más información, consulte el tema TCP Fast Open.

Compatibilidad con tamaño variable de cookie TFO para MPTCP

Un dispositivo Citrix ADC ahora permite configurar una cookie TCP Fast Open (TFO) de longitud variable con un tamaño mínimo de 4 bytes y un tamaño máximo de 16 bytes en un perfil TCP. Al hacerlo, el dispositivo puede responder al cliente con el tamaño de cookie TFO configurado en el paquete SYN-ACK.

Para configurar la cookie TCP Fast Open (TFO) en un perfil TCP mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
set tcpProfile nstcp_default_profile -tcpFastOpenCookieSize <positive_integer
>
```

Ejemplo

```
set tcpProfile nstcp_default_profile -tcpFastOpenCookieSize 8
```

Para configurar la cookie TCP Fast Open (TFO) en un perfil TCP mediante la GUI

1. Vaya a **Configuración** > **Sistema** > Perfiles.
2. En el panel de detalles, vaya a la ficha **Perfiles TCP** y seleccione un perfil TCP.
3. En la página **Configurar perfil TCP**, establezca el tamaño de la cookie **TCP Fast Open**.
4. Haga clic en **Aceptar** y **Listo**.

Intervalo de tiempo de espera de Syn Cookie

El parámetro `TCPSyncookie` está habilitado de forma predeterminada en los perfiles TCP para proporcionar una protección sólida (RFC 4987) contra ataques SYN. Si necesita acomodar clientes TCP personalizados que no son compatibles con esta protección pero que aún quieren garantizar una reserva en caso de ataque, `synAttackDetection` maneja activando automáticamente el comportamiento `SYNCookie` internamente durante un período de tiempo determinado por el parámetro `autosyncookietimeout`.

Para configurar el umbral máximo de retransmisión SYN ACK mediante la interfaz de línea de comandos:

En el símbolo del sistema, escriba:

```
1     set ns tcpparam [-maxSynAckRetx <positive_integer>]
2
3     Set ns tcpparam [-maxSynAckRetx 150]
4 <!--NeedCopy-->
```

Para configurar el intervalo de tiempo de espera automático de cookies SYN mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
set ns tcpparam [-autosyncookietimeout <positive_integer>]
```

```
Set ns tcpparam [-autosyncookietimeout 90]
```

Desvincular conexión cliente y servidor

Cuando está habilitado, el parámetro desvincula la conexión del cliente y del servidor cuando hay datos pendientes que se envían al otro lado. De forma predeterminada, el parámetro está inhabilitado.

```
1 set ns tcpparam -delinkClientServerOnRST ENABLED
2 Done
3
4 <!--NeedCopy-->
```

Configurar el parámetro umbral de inicio lento

Puede usar el parámetro `slowStartthreshold` de umbral de inicio lento para configurar el valor `tcp-slowstartthreshold` de la variante `Nile` del algoritmo de control de congestión. Los valores

aceptables para el parámetro son `min = 8190` y `max = 524288`. El valor predeterminado es `524288`. La variante TCP `Nile`, en el perfil TCP, ya no depende del parámetro `maxcwnd`. Debe configurar el parámetro `slowStartthreshold` de la variante `Nile`.

En el símbolo del sistema, escriba:

```
set tcpprofile nstcp_default_profile -slowstartthreshold 8190
Done

<!--NeedCopy-->
```

Configuraciones HTTP

August 11, 2022

> **Importante:**
>
> A partir de la versión 13.0 compilación 71.x de Citrix ADC, un dispositivo Citrix ADC puede gestionar solicitudes HTTP de gran tamaño de encabezado para acomodar las solicitudes de la aplicación L7. El tamaño del encabezado se puede configurar hasta 128 KB.

Las configuraciones HTTP para un dispositivo Citrix ADC se pueden especificar en una entidad llamada perfil HTTP, que es una colección de configuraciones HTTP. El perfil HTTP se puede asociar a servicios o servidores virtuales que deseen usar estas configuraciones HTTP.

Se puede configurar un perfil HTTP predeterminado para establecer las configuraciones HTTP que se aplican de forma predeterminada, de forma global a todos los servicios y servidores virtuales.

> **Nota:**
>
> Cuando un parámetro HTTP tiene valores diferentes para el servicio, el servidor virtual y de forma global, el valor de la entidad más específica (el servicio) recibe la mayor prioridad.

El dispositivo Citrix ADC también proporciona otros enfoques para configurar HTTP. Sigue leyendo para obtener más información.

Citrix ADC admite un protocolo WebSocket que permite a los exploradores web y otros clientes crear una conexión TCP bidireccional y dúplex completo a los servidores. La implementación de WebSocket de Citrix ADC cumple con RFC 6455.

> **Nota:**
>
> Un dispositivo Citrix ADC ahora admite la configuración de direcciones IP de origen de usuario

> (USIP) para los protocolos HTTP/1.1 y HTTP/2.

Configuración de parámetros HTTP globales

El dispositivo Citrix ADC le permite especificar valores para los parámetros HTTP que se aplican a todos los servicios Citrix ADC y servidores virtuales. Esto se puede hacer mediante:

- Perfil HTTP predeterminado
- Comando HTTP global

Perfil HTTP predeterminado

Un perfil HTTP, denominado nshttp_default_profile, se usa para especificar las configuraciones HTTP que se usan si no se proporcionan configuraciones HTTP en el nivel de servicio o servidor virtual.

> **Notas:**
>
> - No todos los parámetros HTTP se pueden configurar a través del perfil HTTP predeterminado. Algunas configuraciones se realizan mediante el comando HTTP global (consulte la siguiente sección).
> - El perfil predeterminado no tiene que estar vinculado explícitamente a un servicio o servidor virtual.

Para configurar el perfil HTTP predeterminado

- Mediante la interfaz de línea de comando, en la solicitud de comando escriba:

  ```
  set ns httpProfile nshttp_default_profile ...
  ```

- En la GUI, vaya a **Sistema** > **Perfiles**, haga clic en **Perfiles HTTP** y actualice nshttp_default_profile.

Comando HTTP global

Otro enfoque que puede utilizar para configurar los parámetros HTTP globales es el comando HTTP global. Además de algunos parámetros únicos, este comando duplica algunos parámetros que se pueden establecer mediante un perfil HTTP. Cualquier actualización realizada en estos parámetros duplicados se refleja en el parámetro correspondiente en el perfil HTTP predeterminado.

Por ejemplo, si el parámetro maxReusePool se actualiza con este enfoque, el valor se refleja en el parámetro maxReusePool del perfil HTTP predeterminado (nshttp_default_profile).

> **Nota:**
>
> Citrix recomienda utilizar este enfoque solo para los parámetros HTTP que no están disponibles en el perfil HTTP predeterminado.

Para configurar el comando HTTP global

- Mediante la interfaz de línea de comando, en la solicitud de comando escriba:

  ```
  set ns httpParam …
  ```

- En la GUI, vaya a **Sistema > Configuración**, haga clic en **Cambiar parámetros HTTP** y actualice los parámetros HTTP requeridos.

Para configurar un esquema de codificación ignorado para la solicitud de conexión

Para habilitar HTTP/2 y establecer los parámetros HTTP/2 para ignorar el esquema de codificación en la solicitud de conexión, en el símbolo del sistema, escriba:

```
set ns httpParam [-ignoreConnectCodingScheme ( ENABLED | DISABLED )]
```

Ejemplo:

```
set ns httpParam -ignoreConnectCodingScheme ENABLED
```

Para enlazar el perfil HTTP a un servidor virtual mediante la línea de comandos de Citrix ADC

Configurar el perfil HTTP para eliminar solicitudes no válidas TRACE o TRACK

Puede habilitar el parámetro markTraceReqInval para marcar las solicitudes TRACK y TRACK como no válidas. Cuando habilita esta opción junto con la opción dropInvalidReqs en la dirección IP virtual, puede restablecer un cliente que envía solicitudes TRACE o TRACK a un dispositivo Citrix ADC.

Para configurar el perfil HTTP mediante la CLI

En el símbolo del sistema, escriba:

```
set ns httpProfile <profile name> [-markTraceReqInval ENABLED | DISABLED ]
```

Ejemplo:

```
set ns httpProfile profile1 -markTraceReqInval ENABLED
```

Configurar el perfil HTTP para un grupo de servicios

En el símbolo del sistema, escriba:

```
1 add serviceGroup <serviceGroupName>@ <serviceType> [-cacheType <
    cacheType>] [-td <positive_integer>] [-maxClient <positive_integer>]
     [-maxReq <positive_integer>] [-cacheable ( YES | NO )] [-cip (
    ENABLED | DISABLED ) [<cipHeader>]] [-usip ( YES | NO )] [-
    pathMonitor ( YES | NO )] [-pathMonitorIndv ( YES | NO )] [-
    useproxyport ( YES | NO )] [-healthMonitor ( YES | NO )] [-sp ( ON |
     OFF )] [-rtspSessionidRemap ( ON | OFF )] [-cltTimeout <secs>] [-
```



```
    svrTimeout <secs>] [-CKA ( YES | NO )] [-TCPB ( YES | NO )] [-CMP (
    YES | NO )] [-maxBandwidth
2 <positive_integer>] [-monThreshold <positive_integer>] [-state ENABLED
    DISABLED )][-downStateFlush ( ENABLED | DISABLED )] [-tcpProfileName
     <string>] [-httpProfileName <string>] [-comment <string>] [-
    appflowLog ( ENABLED | DISABLED )] [-netProfile <string>] [-
    autoScale <autoScale> -memberPort <port> [-autoDisablegraceful ( YES
     | NO )] [-autoDisabledelay <secs>] ] [-monConnectionClose ( RESET |
     FIN )]
3
4 <!--NeedCopy-->
```

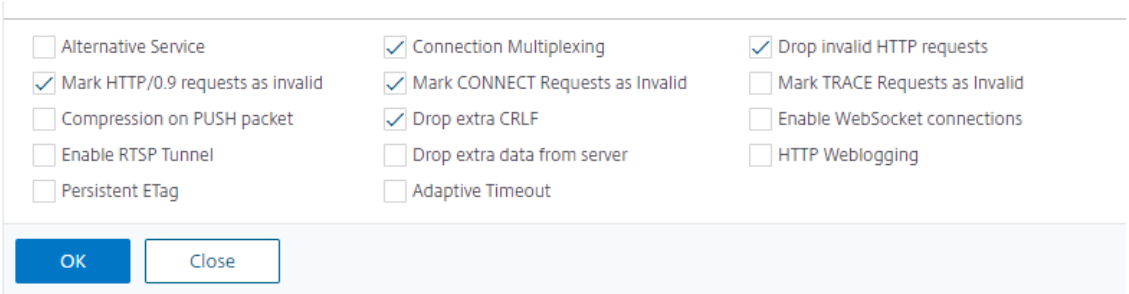
Ejemplo:

```
add serviceGroup Service-Group-1 HTTP -maxClient 0 -maxReq 0 -cip ENABLED -
usip NO -useproxyport YES -cltTimeout 200 -svrTimeout 300 -CKA NO -TCPB NO
-CMP NO -httpProfileName profile1
```

Configurar el perfil HTTP mediante la GUI de Citrix ADC

Para marcar solicitudes no válidas de TRACE o TRACK, complete el siguiente procedimiento.

1. Inicie sesión en el dispositivo Citrix ADC y vaya a **Configuración** > **Sistema** > **Perfiles**.
2. En la ficha **Perfiles HTTP**, haga clic en **Agregar**.
3. En la página **Crear perfil HTTP**, seleccione la opción **Marcar solicitudes TRACE como no válidas**.
4. Haga clic en **Crear**.



Configuración de parámetros HTTP específicos del servicio o del servidor virtual

Con los perfiles HTTP, puede especificar los parámetros HTTP para los servicios y los servidores virtuales. Debe definir un perfil HTTP (o usar un perfil HTTP integrado) y asociar el perfil con el servicio y el servidor virtual apropiados.

> **Nota:**
>
> También puede modificar los parámetros HTTP de los perfiles predeterminados según sus requisitos.

Para especificar configuraciones HTTP a nivel de servicio o servidor virtual mediante la interfaz de línea de comandos

En el símbolo del sistema, realice lo siguiente:

1. Configure el perfil HTTP.

   ```
   set ns httpProfile <profile-name>...
   ```

2. Enlaza el perfil HTTP al servicio o al servidor virtual.

   Para vincular el perfil HTTP al servicio:

```
set service <name> .....
```

Ejemplo:

```
1 > set service service1 -httpProfileName profile1
2 <!--NeedCopy-->
```

Para vincular el perfil HTTP al servidor virtual:

```
set lb vserver <name> .....
```

Ejemplo:

```
1 > set lb vserver lbvserver1 -httpProfileName profile1
2 <!--NeedCopy-->
```

Para especificar configuraciones HTTP a nivel de servicio o servidor virtual mediante la interfaz gráfica de usuario

En la GUI, realice lo siguiente:

1. Configure el perfil HTTP.

   Vaya a **Sistema** > **Perfiles** > **Perfiles HTTP**y cree el perfil HTTP.

2. Enlaza el perfil HTTP al servicio o al servidor virtual.

   Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servicios/Servidores virtuales**y cree el perfil HTTP, que debe estar enlazado al servicio/servidor virtual.

Perfiles HTTP incorporados

Para facilitar la configuración, Citrix ADC proporciona algunos perfiles HTTP integrados. Revise los perfiles enumerados y utilícelos tal cual o modifíquelos para cumplir con sus requisitos. Puede vincular estos perfiles a los servicios o servidores virtuales requeridos.

Perfil incorporado	Descripción
nshttp_default_profile	Representa la configuración HTTP global predeterminada del dispositivo.
nshttp_default_strict_validation	Configuración para implementaciones que requieren una validación estricta de las solicitudes y respuestas HTTP.

Configuraciones HTTP de ejemplo

Ejemplos de interfaz de línea de comandos de ejemplo para configurar lo siguiente:

- Estadísticas de banda HTTP
- Conexiones WebSocket

Estadísticas de banda HTTP

Especifique el tamaño de banda para las solicitudes y respuestas HTTP.

```
> set protocol httpBand reqBandSize 300 respBandSize 2048
Done
> show protocol httpband -type REQUEST
<!--NeedCopy-->
```

Conexiones WebSocket

Habilite WebSocket en el perfil HTTP requerido.

```
> set ns httpProfile http_profile1 -webSocket ENABLED
Done
> set lb vserver lbvserver1 -httpProfileName profile1
Done
<!--NeedCopy-->
```


Configuración HTTP/2

August 11, 2022

> **Nota:**
> La funcionalidad HTTP/2 es compatible con los modelos Citrix ADC MPX, VPX y SDX. En un dispositivo Citrix ADC VPX, la funcionalidad HTTP/2 se admite a partir de la versión 11.0 de Citrix ADC.

El problema del rendimiento de las aplicaciones web está directamente relacionado con la tendencia a aumentar el tamaño de la página y el número de objetos en las páginas web. HTTP/1.1 se desarrolló para admitir páginas web más pequeñas, conexiones a Internet más lentas y hardware de servidor más limitado que el habitual en la actualidad. No es adecuado para nuevas tecnologías como JavaScript y hojas de estilo en cascada (CSS) ni para nuevos tipos de medios como vídeos Flash e imágenes con gran cantidad de gráficos. Esto se debe a que solo puede solicitar un recurso por conexión al servidor. Esta limitación aumenta significativamente el número de viajes de ida y vuelta, lo que provoca una representación de páginas más prolongada y una reducción del rendimiento de la red.

El protocolo HTTP/2 aborda estas limitaciones al permitir que la comunicación se produzca con menos datos transmitidos a través de la red y ofrece la posibilidad de enviar varias solicitudes y respuestas a través de una sola conexión. En esencia, HTTP/2 aborda las limitaciones clave de HTTP/1.1 mediante el uso de las conexiones de red subyacentes de forma más eficiente. Cambia la forma en que las solicitudes y las respuestas viajan por la red.

HTTP/2 es un protocolo binario. Es más eficiente de analizar, más compacto en el cable, y lo más importante, es menos propenso a errores, en comparación con protocolos textuales como HTTP/1.1. El protocolo HTTP/2 utiliza una capa de encuadre binario que define el tipo de marco y cómo se encapsulan y transfieren los mensajes HTTP entre el cliente y el servidor. La funcionalidad HTTP/2 admite el uso del método CONNECT para establecer una conexión de túnel a través de un único flujo HTTP/2 a un host remoto.

El protocolo HTTP/2 incluye muchos cambios que mejoran el rendimiento y que mejoran significativamente el rendimiento, en particular para los clientes que se conectan a través de una red móvil.

La siguiente tabla enumera las principales mejoras en HTTP/2 sobre HTTP/1.1:

Funciones HTTP/2	Descripción
Compresión de encabezado	Los encabezados HTTP tienen mucha información repetitiva y, por lo tanto, consumen ancho de banda innecesario durante la transmisión de datos. HTTP/2 reduce los requisitos de ancho de banda al comprimir el encabezado y minimizar el requisito de transportar encabezados HTTP con cada solicitud y respuesta.
Multiplexación de conexiones	La latencia puede tener un gran impacto en los tiempos de carga de las páginas y en la experiencia del usuario final. La multiplexación de conexiones resuelve este problema mediante el envío de varias solicitudes y respuestas a través de una sola conexión.
Push de servidor	La inserción del servidor permite al servidor enviar contenido de forma proactiva al explorador del cliente, evitando retrasos de ida y vuelta. Esta función almacena en caché las respuestas que cree que necesita el cliente, reduce el número de viajes de ida y vuelta y mejora el tiempo de representación de la página. Importante: El dispositivo Citrix ADC no admite la funcionalidad de inserción del servidor.
Sin bloqueo de encabezamiento	En HTTP 1.1, los exploradores pueden descargar un recurso cada vez por conexión. Cuando un explorador tiene que descargar un recurso grande, bloquea la descarga de todos los demás recursos hasta que se complete la primera descarga. HTTP/2 resuelve este problema con un enfoque de multiplexación. Permite al explorador cliente descargar otros componentes web en paralelo a través de la misma conexión y mostrarlos a medida que estén disponibles.

Funciones HTTP/2	Descripción
Priorización de solicitudes	No todos los recursos tienen la misma prioridad cuando el explorador muestra una página web. Para acelerar el tiempo de carga, todos los exploradores modernos priorizan las solicitudes por tipo de activo, su ubicación en la página e incluso por prioridad aprendida de visitas anteriores. Con HTTP/1.1, el explorador tiene una capacidad limitada para utilizar los datos de prioridad, ya que este protocolo no admite la multiplexación y no hay forma de comunicar la priorización de solicitudes por parte del servidor. El resultado es una latencia de red innecesaria. HTTP/2 resuelve este problema permitiendo que el explorador envíe todas las solicitudes. El explorador puede comunicar su preferencia de priorización de transmisiones a través de dependencias y ponderaciones de transmisión, lo que permite a los servidores optimizar la entrega de respuestas. Importante: El dispositivo Citrix ADC no admite la funcionalidad de priorización de solicitudes.

Cómo funciona HTTP/2

Un dispositivo Citrix ADC admite HTTP/2 tanto en el lado del cliente como en el servidor. En el lado del cliente, el dispositivo Citrix ADC actúa como servidor que aloja un servidor virtual HTTP/HTTPS para HTTP/2. En el lado back-end, Citrix ADC actúa como cliente de los servidores enlazados al servidor virtual.

Por lo tanto, el dispositivo Citrix ADC mantiene conexiones independientes tanto en el lado del cliente como en el servidor. El dispositivo Citrix ADC tiene configuraciones HTTP/2 independientes para el lado del cliente y el lado del servidor.

Configuración de equilibrio de cargas HTTP/2 para HTTPS (SSL)

Para una configuración de equilibrio de carga HTTPS, el dispositivo Citrix ADC utiliza la extensión TLS ALPN (RFC 7301) para determinar si el cliente/servidor admite HTTP/2. Si lo hace, el dispositivo elige

HTTP/2 como protocolo de capa de aplicación para transmitir datos (como se describe en RFC 7540 - Sección 3.3) en el lado cliente/servidor.
El dispositivo utiliza el siguiente orden de preferencia al elegir el protocolo de capa de aplicación mediante la extensión ALPN de TLS:

- HTTP/2 (si está habilitado en el perfil HTTP)
- HTTP/1.1

HTTP/2 para configuración de equilibrio de cargas HTTP

Para una configuración de equilibrio de carga HTTP, el dispositivo Citrix ADC utiliza uno de los métodos siguientes para iniciar la comunicación con el cliente/servidor mediante HTTP/2.

> **Nota**
>
> En las descripciones de métodos siguientes, cliente y servidor son términos generales para una conexión HTTP/2. Por ejemplo, para una configuración de equilibrio de carga de un dispositivo Citrix ADC mediante HTTP/2, el dispositivo Citrix ADC actúa como servidor del lado del cliente y actúa como cliente del lado del servidor.

- **Actualización HTTP/2**. Un cliente envía una solicitud HTTP/1.1 a un servidor. La solicitud incluye un encabezado de actualización, que solicita al servidor que actualice la conexión a HTTP/2. Si el servidor admite HTTP/2, el servidor acepta la solicitud de actualización y se lo notifica en su respuesta. El cliente y el servidor comienzan a comunicarse mediante HTTP/2 después de que el cliente recibe la respuesta de confirmación de actualización.
- **HTTP/2 directo**. Un cliente comienza a comunicarse directamente con un servidor en HTTP/2 en lugar de utilizar el método de actualización HTTP/2. Si el servidor no admite HTTP/2 o no está configurado para aceptar directamente solicitudes HTTP/2, descarta los paquetes HTTP/2 del cliente. Este método resulta útil si el administrador del dispositivo cliente ya sabe que el servidor admite HTTP/2.
- **HTTP/2 directo mediante el servicio alternativo (ALT-SVC).** Un servidor anuncia que admite HTTP/2 para un cliente mediante la inclusión de un campo de servicio alternativo (ALT-SVC) en su respuesta HTTP/1.1. Si el cliente está configurado para comprender el campo ALT-SVC, el cliente y el servidor comienzan a comunicarse directamente mediante HTTP/2 una vez que el cliente recibe la respuesta.

El dispositivo Citrix ADC proporciona opciones configurables en un perfil HTTP para los métodos HTTP/2. Estas opciones HTTP/2 se pueden aplicar al lado del cliente, así como al lado del servidor de una configuración de equilibrio de carga HTTPS o HTTP. Para obtener más información sobre los métodos y opciones HTTP/2, consulte el PDF de opciones de HTTP/2.

Antes de comenzar

Antes de empezar a configurar HTTP/2 en un dispositivo Citrix ADC, tenga en cuenta los siguientes puntos:

- El dispositivo Citrix ADC admite HTTP/2 tanto en el lado del cliente como en el servidor.
- El dispositivo Citrix ADC no admite la funcionalidad de inserción del servidor HTTP/2.
- El dispositivo Citrix ADC no admite la funcionalidad de priorización de solicitudes HTTP/2.
- El dispositivo Citrix ADC no admite la renegociación SSL HTTP/2 para las configuraciones de equilibrio de carga HTTPS.
- El dispositivo Citrix ADC no admite la autenticación NTLM HTTP/2.
- Con HTTP/2 habilitado, la multiplexación de conexiones inhabilitada (como USIP habilitada) y el mapeo uno a uno de las conexiones TCP de cliente y servidor, los eventos de cierre como FIN, reinicio (RST) se reenvían desde la conexión del cliente o servidor a la conexión del par vinculado.

Configuración de HTTP/2

La configuración de HTTP/2 para una configuración de equilibrio de carga (HTTPS o HTTP) consiste en las siguientes tareas:

- **Habilite HTTP/2 y establezca parámetros HTTP/2 opcionales en un perfil HTTP**. Habilita HTTP/2 en un perfil HTTP. Cuando solo habilita HTTP/2 en un perfil HTTP, el dispositivo Citrix ADC utiliza únicamente el método de actualización (para HTTP) o el método ALPN de TLS (para HTTPS) para comunicarse en HTTP/2.

  Para que el dispositivo Citrix ADC utilice el método HTTP/2 **directo, la opción HTTP/2** directa debe estar habilitada en el perfil HTTP. Para que el dispositivo Citrix ADC utilice HTTP/2 directo mediante el método de servicio alternativo, la opción **Servicio alternativo (altsvc)** debe estar habilitada en el perfil HTTP.

- **Enlace el perfil HTTP a un servidor virtual o a un servicio**. Enlace el perfil HTTP a un servidor virtual para configurar HTTP/2 para el lado cliente de la configuración del equilibrio de carga. Enlaza el perfil HTTP a un servicio para configurar HTTP2 para el lado del servidor de la configuración del equilibrio de carga.

> **Nota**
>
> Citrix recomienda vincular perfiles HTTP independientes para el lado del cliente y el lado del servidor.

- **Habilite el parámetro global para la compatibilidad con el servidor HTTP/2**. Habilite el parámetro HTTP global del **lado del servicio HTTP/2(HTTP2Serverside**) para habilitar la compatibilidad con HTTP/2 en el lado del servidor de todas las configuraciones de equilibrio de carga que tengan configurado HTTP/2.

HTTP/2 no funciona en el lado del servidor de ninguna configuración de equilibrio de carga si **HTTP/2 Service Side** está inhabilitado aunque **HTTP/2** esté habilitado en el perfil HTTP enlazado a los servicios de equilibrio de carga relacionados.

Procedimientos de línea de comandos de Citrix ADC:

Para habilitar HTTP/2 y establecer parámetros HTTP/2 mediante la línea de comandos de Citrix ADC

- Para habilitar HTTP/2 y establecer los parámetros HTTP/2 mientras se agrega un perfil HTTP, en el símbolo del sistema, escriba:

```
add ns httpProfile <name> - http2 ( ENABLED | DISABLED )[-http2Direct (
ENABLED | DISABLED )] [-altsvc ( ENABLED | DISABLED )]
show ns httpProfile <name>
```

- Para habilitar HTTP/2 y establecer los parámetros HTTP/2 mientras se modifica un perfil HTTP, en el símbolo del sistema, escriba:

```
set ns httpProfile <name> -http2 ( ENABLED | DISABLED )[-http2Direct (
ENABLED | DISABLED)] [-altsvc (ENABLED | DISABLED )]
show ns httpProfile <name>
```

Para enlazar el perfil HTTP a un servidor virtual mediante la línea de comandos de Citrix ADC

En el símbolo del sistema, escriba:

```
set lb vserver <name> - httpProfileName <string>
show lb vserver <name>
```

Para enlazar el perfil HTTP a un servicio de equilibrio de carga mediante la línea de comandos de Citrix ADC

En el símbolo del sistema, escriba:

```
set service <name> -httpProfileName <string>
show service <name>
```

Para habilitar la compatibilidad con HTTP/2 de forma global en el servidor mediante la línea de comandos de Citrix ADC

En el símbolo del sistema, escriba:

```
set ns httpParam -HTTP2Serverside( ENABLED | DISABLED )
show ns httpParam
```

Para habilitar HTTP/2 y establecer parámetros HTTP/2 mediante la GUI de Citrix ADC

1. Vaya a **Sistema** > **Perfiles** y haga clic en la ficha **Perfiles HTTP**.
2. Habilite **HTTP/2** mientras agregas un perfil HTTP o modificas un perfil HTTP existente.

Para enlazar el perfil HTTP a un servidor virtual mediante la GUI de Citrix ADC

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**y abra el servidor virtual.
2. En **Configuración avanzada**, haga clic en **+ Perfil HTTP** para enlazar el perfil HTTP creado al servidor virtual.

Para enlazar el perfil HTTP a un servicio de equilibrio de carga mediante la GUI de Citrix ADC

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servicio**y abra el servicio.
2. En **Configuración avanzada**, haga clic en **+ Perfil HTTP** para enlazar el perfil HTTP creado al servicio.

Para habilitar la compatibilidad con HTTP/2 globalmente en el servidor mediante la interfaz gráfica de usuario

Vaya a **Sistema** > **Configuración**, haga clic en **Cambiar parámetros HTTP** y habilite **HTTP/2 Server Side**.

Configuraciones de ejemplo

En la siguiente configuración de ejemplo, HTTP/2 y HTTP/2 directo están habilitados en el perfil HTTP HTTP-PROFILE-HTTP2-CLIENT-SIDE. El perfil está enlazado al servidor virtual LB-VS-1.

```
set ns httpProfile HTTP-PROFILE-HTTP2-CLIENT-SIDE -http2 enabled -
   http2Direct enabled
Done

set lb vserver LB-VS-1 -httpProfileName HTTP-PROFILE-HTTP2-CLIENT-SIDE

Done
<!--NeedCopy-->
```

En la siguiente configuración de ejemplo, HTTP/2 y el servicio alternativo (ALT-SVC) están habilitados en el perfil HTTP HTTP-PROFILE-HTTP2-SERVER-SIDE. El perfil está vinculado al servicio LB-SERVICE-1.

```
set ns httpparam -HTTP2Serverside ENABLED
Done

set ns httpProfile HTTP-PROFILE-HTTP2-SERVER-SIDE -http2 ENABLED -
   altsvc ENABLED
Done

```



```
7 set service LB-SERVICE-1 -httpProfileName HTTP-PROFILE-HTTP2-SERVER-
     SIDE
8 Done
9 <!--NeedCopy-->
```

Configurar el tamaño de la ventana de conexión inicial HTTP/2

Según RFC 7540, la ventana de control de flujo para la transmisión y la conexión HTTP2 debe establecerse en 64 K (65535) octetos y cualquier cambio realizado en este valor debe comunicarse al par. El dispositivo ADC comunica el cambio en el tamaño de la ventana de control de flujo de la siguiente manera:

- Usar el marco `SETTINGS` para la transmisión.
- Usar el marco `WINDOW_UPDATE` para la conexión.

En un perfil HTTP, debe configurar el parámetro `http2InitialWindowSize` para establecer el tamaño de ventana inicial a nivel de transmisión. Debido a un error interno del sistema, el dispositivo ADC inicializa también la ventana de control de flujo para la conexión. Cuando se produce un cambio en la ventana de control de flujo configurada para la transmisión, el dispositivo ADC se comunica con el par mediante el marco SETTINGS. Sin embargo, el dispositivo ADC no comunica el cambio en la ventana de control de flujo para la conexión mediante el marco `WINDOW_UPDATE`. Esto lleva a una congelación de la conexión.

Para superar el problema, ahora se agrega el parámetro `http2InitialConnWindowSize` (en bytes) para controlar la ventana de control de flujo para la conexión. Mediante el uso de parámetros configurables independientes, ahora puede permitir que el dispositivo envíe actualizaciones para cambiar el tamaño de ventana, tanto en los niveles de transmisión como de conexión.

Configure el parámetro de tamaño de ventana de conexión inicial HTTP/2 mediante la CLI

En el símbolo del sistema, escriba:

```
1 set http profile p1 -http2InitialConnWindowSize 8290
2 Initial window size for stream level flow control, in bytes.
3 Default value: 65535
4 Minimum value: 8192
5 Maximum value: 20971520
6 <!--NeedCopy-->
```


> **Nota:**
> Cuando HTTP/2 está habilitado, Citrix recomienda inhabilitar el parámetro Almacenamiento en búfer de recepción dinámica de TCP en el perfil TCP.

HTTP/2 Mitigación de DoS

August 20, 2021

Los ataques de denegación de servicio (DoS) Http/2 ya no tienen ningún impacto en un dispositivo Citrix ADC. Si el dispositivo recibe tramas superiores al límite máximo, el dispositivo cierra silenciosamente la conexión.

Para mitigar los ataques, el perfil HTTP le permite cambiar la configuración predeterminada de tramas recibidas en una conexión HTTP/2.

La tabla de mitigación de DoS HTTP/2 muestra la lista de ataques DoS HTTP/2 y su mitigación.

Configure el límite máximo para tramas HTTP/2 para mitigar los ataques DoS mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba lo siguiente:

```
set ns httpprofile <profile_name> - http2MaxEmptyFramesPerMin <positive_integer
> -http2MaxPingFramesPerMin <positive_integer> -http2MaxSettingsFramesPerMin
 <positive_integer> -http2MaxResetFramesPerMin <positive_integer>
```

Ejemplo:

```
set ns httpprofile profile1 -http2MaxEmptyFramesPerMin 20 -http2MaxPingFramesPerMin
 20 -http2MaxSettingsFramesPerMin 20 -http2MaxResetFramesPerMin 20
```

Configure el límite máximo de tramas recibidas en una conexión HTTP/2 mediante la GUI de Citrix ADC

Siga los pasos que se indican a continuación para configurar el límite máximo de tramas recibidas en una conexión HTTP/2:

1. En el panel de navegación, expanda **Sistema** y, a continuación, haga clic en **Perfiles**.
2. En la página **Perfil**, seleccione la ficha **Perfiles HTTP**.
3. En la página de la ficha **Perfiles HTTP**, haga clic en **Agregar**.
4. En la página **Configurar perfil HTTP**, establezca el siguiente parámetro.

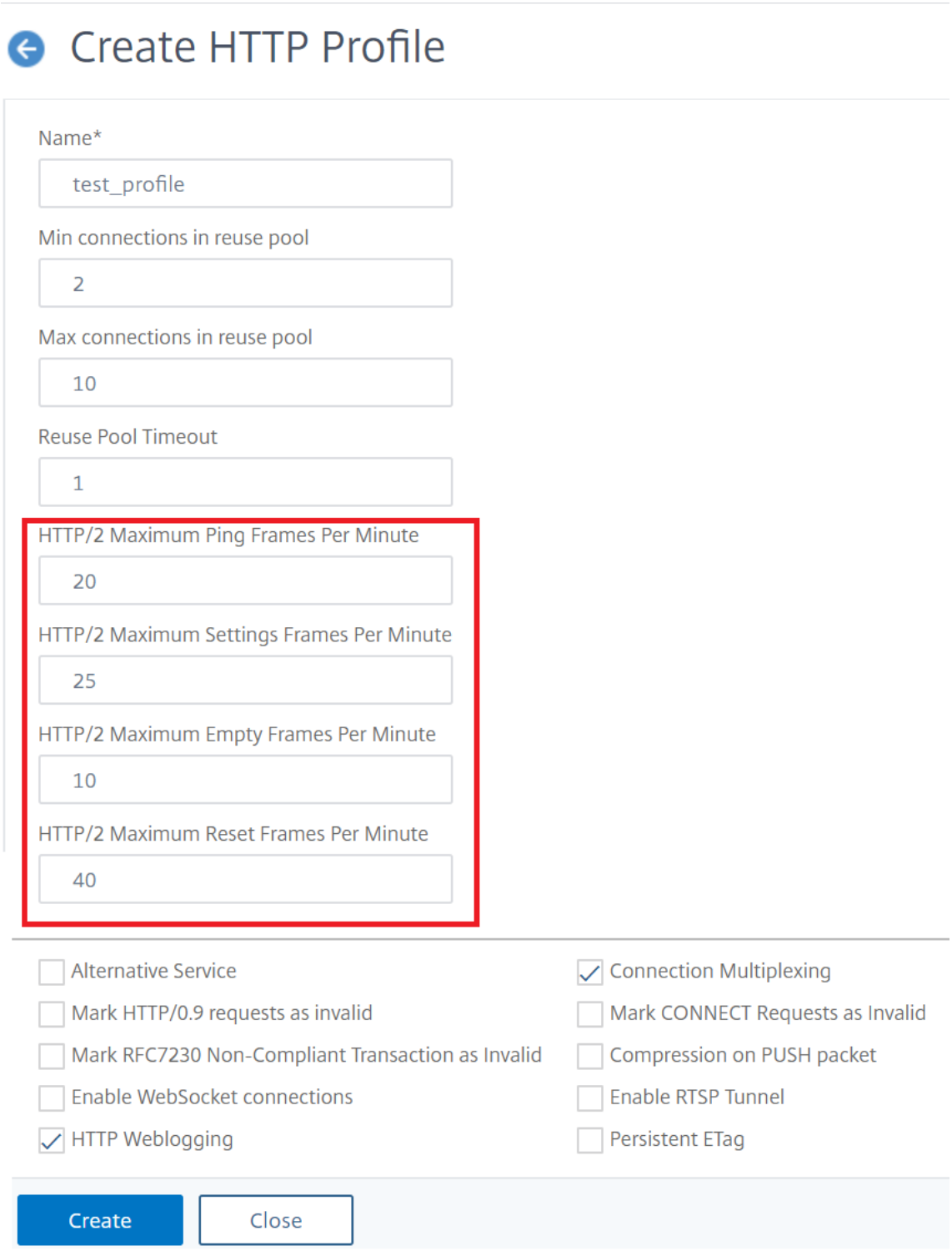
a) http2MaxPingFramesPerMin. Establezca el máximo de tramas PING recibidas por conexión en un minuto. Si el número de tramas PING supera el límite de configuración, el dispositivo descarta paquetes de forma silenciosa en la conexión.

b) http2MaxSettingsFramesPerMin. Establezca el máximo de tramas SETTINGS recibidas por conexión en un minuto. Si el número de tramas SETTINGS supera el límite de configuración, ADC descarta paquetes de forma silenciosa en la conexión.

c) http2MaxResetFramesPerMin. Establezca el máximo de tramas RESET enviadas por conexión en un minuto. Si el número de tramas RESET supera el límite de configuración, ADC descarta paquetes de forma silenciosa en la conexión.

d) http2MaxEmptyFramesPerMin. Establezca el máximo de tramas vacías enviadas por conexión en un minuto. Si el número de tramas vacías supera el límite de configuración, ADC descarta paquetes de forma silenciosa en la conexión.

5. Haga clic en **Aceptar** y **Cerrar**.



protocolo HTTP3 sobre QUIC

August 20, 2021

HTTP/2 a través de TCP es el estándar preferido para enviar múltiples secuencias de solicitudes HTTP a través de una única conexión. Sin embargo, en el mecanismo de transporte TCP existen ciertas limitaciones y problemas de latencia al acceder a sitios web y aplicaciones web. Cuando multiplex varias solicitudes a través de la misma conexión, están sujetas a la fiabilidad de la misma conexión. Si se pierde el paquete de una solicitud, todas las demás solicitudes multiplexadas se retrasan hasta que se detecta y se vuelve a transmitir el paquete perdido. Esto provoca retrasos en el bloqueo de cabecera de línea y problemas de latencia.

Para retrasos en la conexión y el transporte, HTTP/3 utiliza QUIC en lugar del protocolo TCP. El QUIC es un protocolo emergente que utiliza UDP en lugar de TCP como transporte base. En HTTP sobre quic, puede multiplexar varias solicitudes independientes sin depender de una sola conexión TCP. QUIC implementa una conexión fiable en la que puede transmitir varias solicitudes HTTP. QUIC también incorpora TLS como componente integrado y no como capa adicional como en HTTP/1.1 o HTTP/2.

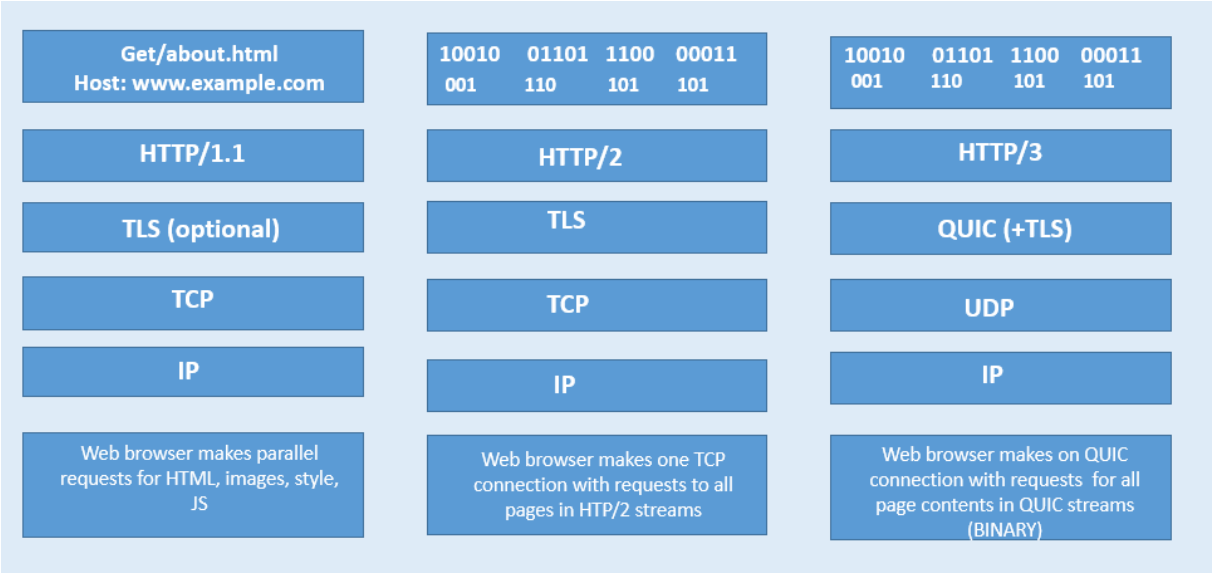
Ventaja de utilizar el protocolo HTTP/3

A continuación se presentan algunas de las ventajas importantes de utilizar el protocolo QUIC para el transporte de datos HTTP/3:

- Multiplexación de flujos
- Control de flujo a nivel de corriente y conexión
- Establecimiento de conexiones de baja latencia
- Migración de conexiones y resiliencia a la revinculación de NAT
- Encabezado y carga útil autenticados y cifrados

Pila de transporte en protocolos HTTP

La ilustración siguiente muestra la pila de transporte en los protocolos HTTP/1.1, HTTP/2 y HTTP/3.



Cómo funciona la administración de conexiones QUIC y HTTP/3 en Citrix ADC

En la siguiente ilustración se muestra cómo la administración de conexiones QUIC y HTTP/3 en un dispositivo Citrix ADC y cómo los componentes interactúan entre sí.

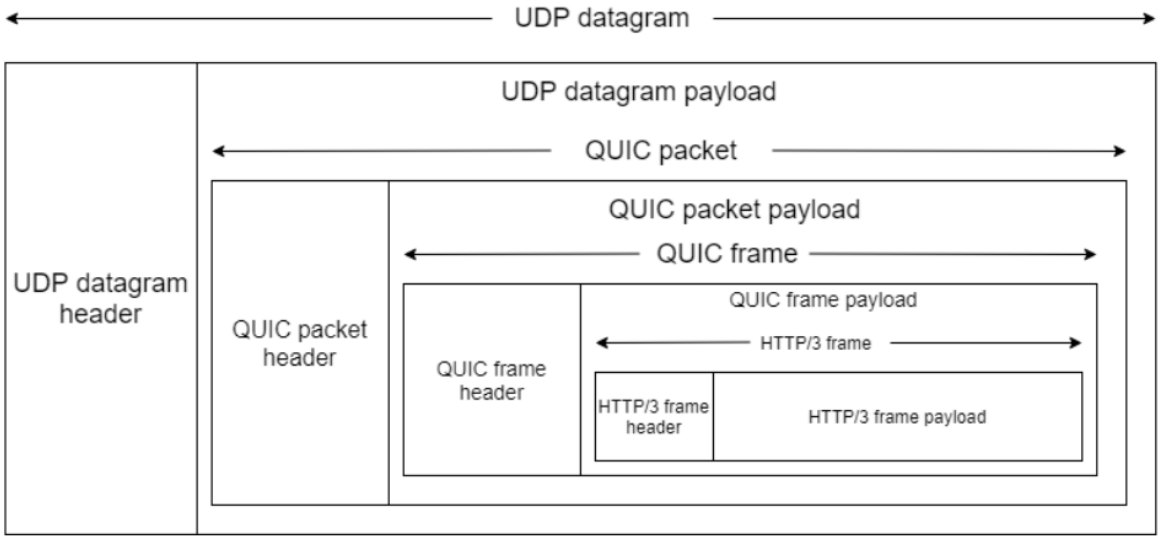
Paso 1: Solicitud HTTP/3 del lado del cliente a través del protocolo QUIC al dispositivo Citrix ADC.
Paso 2: Solicitud reenviada por Citrix ADC AS HTTP/1.1 o HTTP/2 según el soporte del servidor back-end.
Paso 3: Respuesta a través de HTTP/2 o HTTP/1.1 desde el servidor back-end a Citrix ADC.
Paso 4: ADC reenvía la respuesta como respuesta HTTP/3 al cliente.

Cómo funciona el protocolo HTTP/3

En HTTP/3, cuando un cliente sabe que existe un servidor HTTP/3 en un punto final determinado, abre una conexión QUIC. El protocolo QUIC proporciona multiplexación y control de flujo. Dentro de cada secuencia, la unidad básica de comunicación HTTP/3 es un marco. Cada tipo de marco tiene

un propósito diferente. Por ejemplo, los marcos HEADERS y DATA forman la base de las solicitudes y respuestas HTTP.

La multiplexación de solicitudes se realiza mediante la abstracción de flujo QUIC. Cada par de solicitudes de respuesta consume un único flujo QUIC. Las transmisiones son independientes entre sí, por lo que una transmisión que está bloqueada o sufre pérdida de paquetes no impide el progreso en otros flujos. La inserción del servidor es un modo de interacción introducido en HTTP/2 que permite a un servidor enviar un intercambio de solicitudes y respuestas a un cliente en previsión de que el cliente realicen la solicitud indicada. Esto cambia el uso de la red frente a una posible ganancia de latencia. Se utilizan varias tramas HTTP/3 para administrar la inserción del servidor, como PUSH_PROMISE, MAX_PUSH_ID y CANCEL_PUSH. Al igual que en HTTP/2, los campos de solicitud y respuesta se comprimen para su transmisión. Dado que HPACK se basa en la transmisión en orden de las secciones de campo comprimido (garantía no proporcionada por QUIC), HTTP/3 reemplaza a HPACK por QPACK. QPACK utiliza flujos unidireccionales independientes para modificar y rastrear el estado de la tabla de campos, mientras que las secciones de campo codificadas hacen referencia al estado de la tabla sin modificarla.



Configuración de HTTP/3 y resumen de estadísticas

July 8, 2022

Para configurar un protocolo HTTP/3 para enviar varios flujos de datos HTTP/3 mediante QUIC, debe completar los siguientes pasos:

1. Habilite las funciones SSL y de equilibrio de carga.

2. Agregue equilibrio de carga y conmutación de contenido (opcionales) servidores virtuales de tipo HTTP_QUIC.
3. Asocie los parámetros del protocolo QUIC al servidor virtual HTTP_QUIC.
4. Habilite HTTP/3 en el servidor virtual HTTP_QUIC.
5. Enlazar el par de claves de certificado SSL con el servidor virtual HTTP_QUIC.
6. Asocie los parámetros de protocolo SSL/TLS con el servidor virtual HTTP_QUIC.

Habilitar SSL y equilibrio de carga

Antes de empezar, asegúrese de que las funciones SSL y Equilibrio de carga estén habilitadas en el dispositivo. En el símbolo del sistema, escriba:

```
enable ns feature ssl lb
<!--NeedCopy-->
```

Agregar equilibrio de carga y conmutación de contenido (opcionales) servidores virtuales de tipo HTTP_QUIC para el servicio HTTP/3

Agregue un servidor virtual de equilibrio de carga para aceptar tráfico HTTP/3 a través de QUIC.
Nota: El servidor virtual de equilibrio de carga de tipo HTTP_QUIC tiene perfiles QUIC, SSL y HTTP3 integrados. Si prefiere crear perfiles definidos por el usuario, puede agregar nuevos perfiles y vincularlos al servidor virtual de equilibrio de carga.

```
add lb vserver <vserver-name> HTTP_QUIC <IP-address> <UDP-listening-
    port>

add cs vserver <vserver-name> HTTP_QUIC <IP-address> <UDP-listening-
    port>
<!--NeedCopy-->
```

Ejemplo:

```
add lb vserver lb-http3 HTTP_QUIC 1.1.1.1 443
add cs vserver cs-http3 HTTP_QUIC 10.10.10.10 443
```

Asociar parámetros de protocolo QUIC al servidor virtual HTTP_QUIC

Puede crear un perfil QUIC y especificar parámetros QUIC para el servicio QUIC y asociarlo al servidor virtual de equilibrio de carga. Debe crear un perfil definido por el usuario o utilizar el perfil QUIC

integrado y enlazar el perfil al servidor virtual de equilibrio de carga.

Paso 1: configurar un perfil QUIC definido por el usuario
En el símbolo del sistema, escriba:

```
set quic profile <profile_name> -transport_param <value>
<!--NeedCopy-->
```

Ejemplo:

```
set quic profile quic_http3 -ackDelayExponent 10 -activeConnectionIDlimit 4
```

Los distintos parámetros de transporte QUIC son los siguientes:

-ackDelayExponent. Valor entero anunciado por Citrix ADC en el extremo QUIC remoto, que indica un exponente que debe usar el dispositivo de punto final QUIC remoto, para decodificar el campo Demora ACK en tramas ACK de QUIC enviadas por Citrix ADC.

-activeConnectionIDlimit. Valor entero anunciado por Citrix ADC en el extremo QUIC remoto. Especifica el número máximo de ID de conexión QUIC desde el extremo QUIC remoto, que Citrix ADC está dispuesto a almacenar.

-activeConnectionMigration. Especifique si Citrix ADC debe permitir que el dispositivo de punto final QUIC remoto realice una migración de conexión QUIC activa.

-congestionCtrlAlgorithm. Especifique el algoritmo de control de congestión que se va a utilizar para las conexiones QUIC.

-initialMaxData. Valor entero anunciado por Citrix ADC en el extremo QUIC remoto, que especifica el valor inicial, en bytes, para la cantidad máxima de datos que se pueden enviar en una conexión QUIC.

-initialMaxStreamDataBidiLocal. Valor entero anunciado por Citrix ADC en el extremo QUIC remoto, que especifica el límite de control de flujo inicial, en bytes, para flujos QUIC bidireccionales iniciados por Citrix ADC.

-initialMaxStreamDataBidiRemote. Valor entero anunciado por Citrix ADC en el extremo QUIC remoto, que especifica el límite de control de flujo inicial, en bytes, para flujos QUIC bidireccionales iniciados por el dispositivo de punto final QUIC remoto.

-initialMaxStreamDataUni. Valor entero anunciado por Citrix ADC en el extremo QUIC remoto, que especifica el límite de control de flujo inicial, en bytes, para los flujos unidireccionales iniciados por el dispositivo de punto final QUIC remoto.

-initialMaxStreamsBidi. Valor entero anunciado por Citrix ADC en el extremo QUIC remoto, que especifica el número máximo inicial de flujos bidireccionales que debe iniciar el extremo QUIC remoto.

-initialMaxStreamsUni. Valor entero anunciado por Citrix ADC en el extremo QUIC remoto, que especifica el número máximo inicial de flujos unidireccionales que debe iniciar el dispositivo de punto final QUIC remoto.

-maxAckDelay. Valor entero anunciado por Citrix ADC en el extremo QUIC remoto, que especifica la cantidad máxima de tiempo, en milisegundos, mediante el cual Citrix ADC retrasa el envío de confirmaciones.

-maxIdleTimeout. Valor entero anunciado por Citrix ADC en el extremo QUIC remoto, que especifica el tiempo de espera máximo de inactividad, en segundos, para una conexión QUIC. Citrix ADC descartará silenciosamente una conexión QUIC que permanezca inactiva durante más tiempo de espera que el Citrix ADC y el punto final QUIC remoto anunciados por Citrix ADC y el triple del tiempo de espera de sonda (PTO) actual.

-maxUDPPayloadSize. Valor entero anunciado por Citrix ADC en el extremo QUIC remoto, que especifica el tamaño de la mayor carga útil de datagramas UDP, en bytes, que Citrix ADC está dispuesto a recibir en una conexión QUIC.

-newTokenValidityPeriod. Valor entero que especifica el período de validez, en segundos, de los tokens de validación de direcciones emitidos a través de tramas QUIC NEW_TOKEN enviadas por Citrix ADC.
-retryTokenValidityPeriod. Valor entero que especifica el período de validez, en segundos, de los tokens de validación de direcciones emitidos a través de paquetes de reintento QUIC enviados por Citrix ADC.
-statelessAddressValidation. Especifique si Citrix ADC debe llevar a cabo la validación de direcciones sin estado para clientes QUIC, enviando tokens en paquetes de reintento de QUIC durante el establecimiento de la conexión QUIC y enviando tokens en tramas de QUIC NEW_TOKEN después del establecimiento de la conexión QUIC.

Paso 2: Asociar el perfil QUIC definido por el usuario a un servidor virtual de equilibrio de carga de tipo http_quic

En el símbolo del sistema, escriba:

```
1 set lb vserver <name>@ [-IPAddress <ip_addr|ipv6_addr|*>@]  <
     serviceName>@] [-persistenceType <persistenceType>] [-
     quicProfileName <string>]
2 <!--NeedCopy-->
```

Ejemplo:

```
set lb vserver lb-http3 -quicProfileName quic_http3
```


Habilitar y enlazar HTTP/3 en un servidor virtual HTTP_QUIC

Para habilitar HTTP/3 en un servidor virtual HTTP_QUIC, se agrega un conjunto de parámetros de configuración a la configuración del perfil HTTP. Para facilitar la configuración, al agregar un servidor virtual HTTP_QUIC, hay disponible un nuevo perfil HTTP predeterminado o integrado en el dispositivo. El perfil tiene los parámetros de compatibilidad del protocolo HTTP/3 configurados en HABILITADO y también limitados a los servidores virtuales HTTP_QUIC (aplicable si decide no asociar el servidor virtual HTTP_QUIC con un perfil HTTP agregado por el usuario). El valor de los parámetros HTTP/3 del perfil HTTP decide si se selecciona el protocolo HTTP/3 y se anuncia al procesar la extensión TLS ALPN (Negociación de protocolo de capa de aplicación) durante el protocolo QUIC.

Puede crear un perfil HTTP/3 y especificar parámetros HTTP para el servicio HTTP/3 y el servidor virtual de equilibrio de carga. Debe crear un perfil definido por el usuario o utilizar el perfil HTTP/3 integrado y enlazar el perfil al servidor virtual de equilibrio de carga.

Paso 1: configurar un perfil HTTP/3 definido por el usuario
En el símbolo del sistema, escriba:

```
1 Add ns httpProfile <profile_name> -http3 ENABLED
2 <!--NeedCopy-->
```

Ejemplo:

```
add ns httpProfile http3_quic -http3 ENABLED
```

Paso 2: Vincular el perfil HTTP/3 definido por el usuario a un servidor virtual de equilibrio de carga de tipo http_quic
En el símbolo del sistema, escriba:

```
1 set lb vserver <name>@ [-IPAddress <ip_addr|ipv6_addr|*>@]  <
     serviceName>@] [-persistenceType <persistenceType>] [-
     httpProfileName <string>]
2 <!--NeedCopy-->
```

Ejemplo:

```
set lb vserver lb-http3 -httpProfileName http3_quic
```

Vincular par de claves de certificado SSL con el servidor virtual HTTP_QUIC

Para procesar el tráfico cifrado, debe agregar un par de claves de certificado SSL y vincularlo al servidor virtual HTTP_QUIC.

En el símbolo del sistema, escriba:

```
bind ssl vserver <vServerName> -certkeyName <certificate-KeyPairName>

<!--NeedCopy-->
```

Ejemplo:

```
bind ssl vserver lb-http3 -certkeyName rsa_certkeypair
```

Para obtener más información, consulte el tema Vincular certificado SSL .

Enlazar parámetros de protocolo SSL/TLS con un servidor virtual HTTP_QUIC

Los servidores virtuales de tipo HTTP_QUIC tienen funcionalidad de servidor TLS 1.3 incorporada porque el protocolo QUIC utiliza TLS 1.3 como componente de seguridad obligatorio. Para facilitar la configuración al agregar un servidor virtual HTTP_QUIC, se agrega un nuevo perfil SSL predeterminado o integrado de tipo: interfaz rápida. El perfil SSL tiene habilitada la versión TLS 1.3 con conjuntos de cifrado TLS 1.3 (y curvas elípticas) configurados. El perfil SSL debe enlazarse a los servidores virtuales HTTP_QUIC recientemente agregados.
Puede crear un perfil SSL y especificar parámetros de cifrado SSL para el servicio TLP 1.1 y el servidor virtual de equilibrio de carga. Debe crear un perfil definido por el usuario o utilizar el perfil SSL integrado y enlazar el perfil al servidor virtual de equilibrio de carga.

Paso 1: configurar un perfil SSL definido por el usuario
En el símbolo del sistema, escriba:

```
add ssl profile <name> -sslprofileType QUIC-FrontEnd
<!--NeedCopy-->
```

Ejemplo:

```
add ssl profile ssl_profile1 -sslprofileType QUIC-FrontEnd -tls13 ENABLED -
tls12 DISABLED -tls11 DISABLED -tls1 DISABLED
```

Paso 2: Vincular el perfil SSL definido por el usuario a un servidor virtual de equilibrio de carga de tipo HTTP_QUIC
En el símbolo del sistema, escriba:

```
set ssl vserver <name>@ [-sslProfile <string>]
<!--NeedCopy-->
```

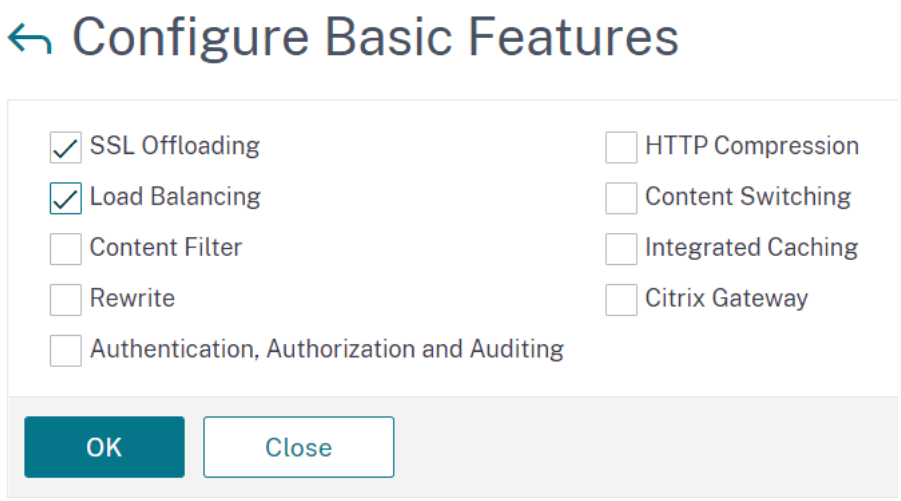

Ejemplo:

```
set ssl vserver lb-http3 -sslprofile ssl_profile1
```

Habilitar las funciones SSL y de equilibrio de carga mediante la GUI

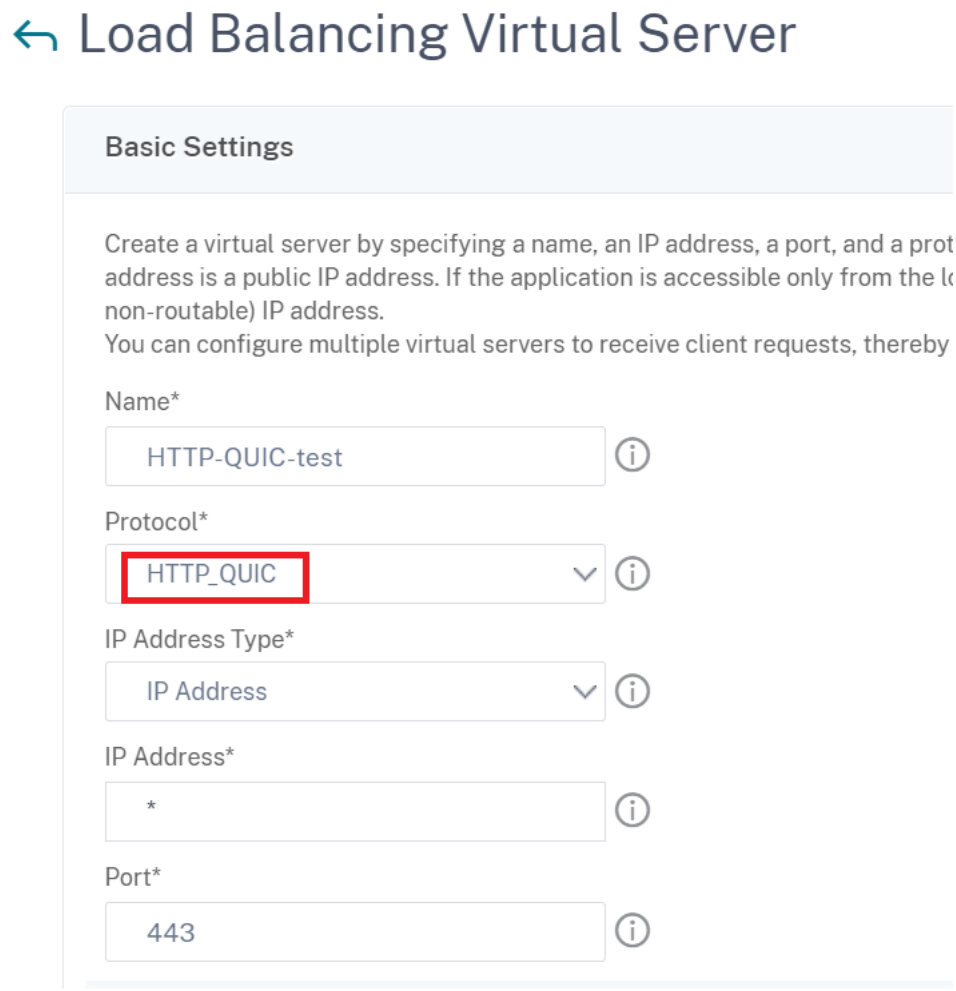
Complete los siguientes pasos para habilitar las funciones SSL y de equilibrio de carga:

1. En el panel de navegación, expanda **Sistema** y, a continuación, haga clic en **Configuración**.
2. En la página **Configurar funciones básicas**, seleccione **SSL** y **Equilibrio de carga**.
3. Haga clic en **Aceptar**y, a continuación, en **Cerrar**.



Agregar servidores virtuales de equilibrio de carga y conmutación de contenido (opcionales) de tipo HTTP_QUIC mediante la GUI

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. Haga clic en **Agregar** para crear un servidor virtual de equilibrio de carga de tipo HTTP_QUIC.
3. En la página **Servidor virtual de equilibrio de carga**, haga clic en **Perfiles**.
4. En la sección **Perfiles**, seleccione el tipo de perfil como QUIC. Nota: Los perfiles QUIC, HTTP/3 y SSL son integrados.
5. Haga clic en **Aceptar** y luego en **Listo**.

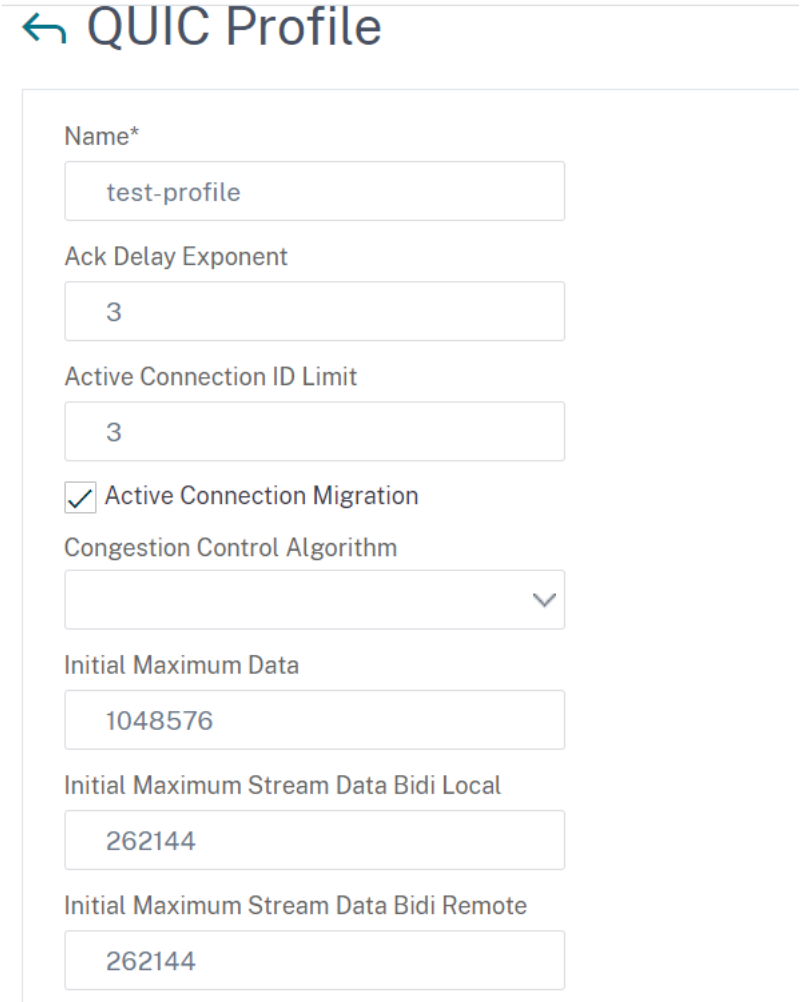


Asociar parámetros de protocolo QUIC al servidor virtual HTTP_QUIC mediante la GUI

Paso 1: Agregar perfil QUIC

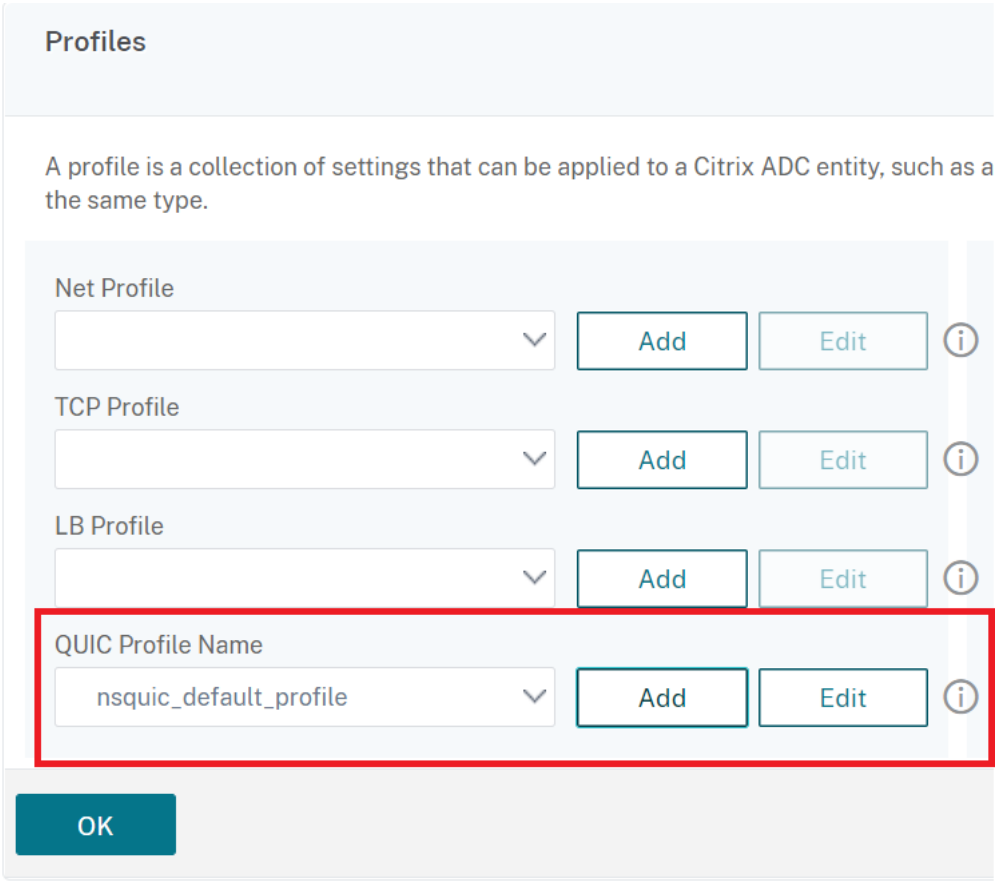
1. Vaya a **Sistema > Perfiles > Perfil QUIC**.
2. Haga clic en **Agregar**.
3. En la página Perfil QUIC, establezca los siguientes parámetros. Para obtener una descripción detallada de cada parámetro, consulte la sección de la CLI del protocolo QUIC Asociado.
   a) `Ack Delay` Exponente
   b) Active Connection ID Limit
   c) Active Connection Migration
   d) Congestion Control Algorithm
   e) Initial Maximum Data
   f) Initial Maximum Stream Data Bidi Local

g) Initial Maximum Stream Data Bidi Remote
h) Initial Maximum Stream Data Unit
i) Initial Maximum Stream bidi
j) Initial Maximum Stream Uni
k) Maximum Acknowledgment Delay
l) Maximum Idle Timeout
m) Maximum UDP Data GramsperBurst
n) New Token Validity Period
o) Retry Token Validity Period
p) Stateless Address Validation



Paso 2: Asociar el perfil QUIC con un servidor virtual de equilibrio de carga de tipo HTTP_QUIC

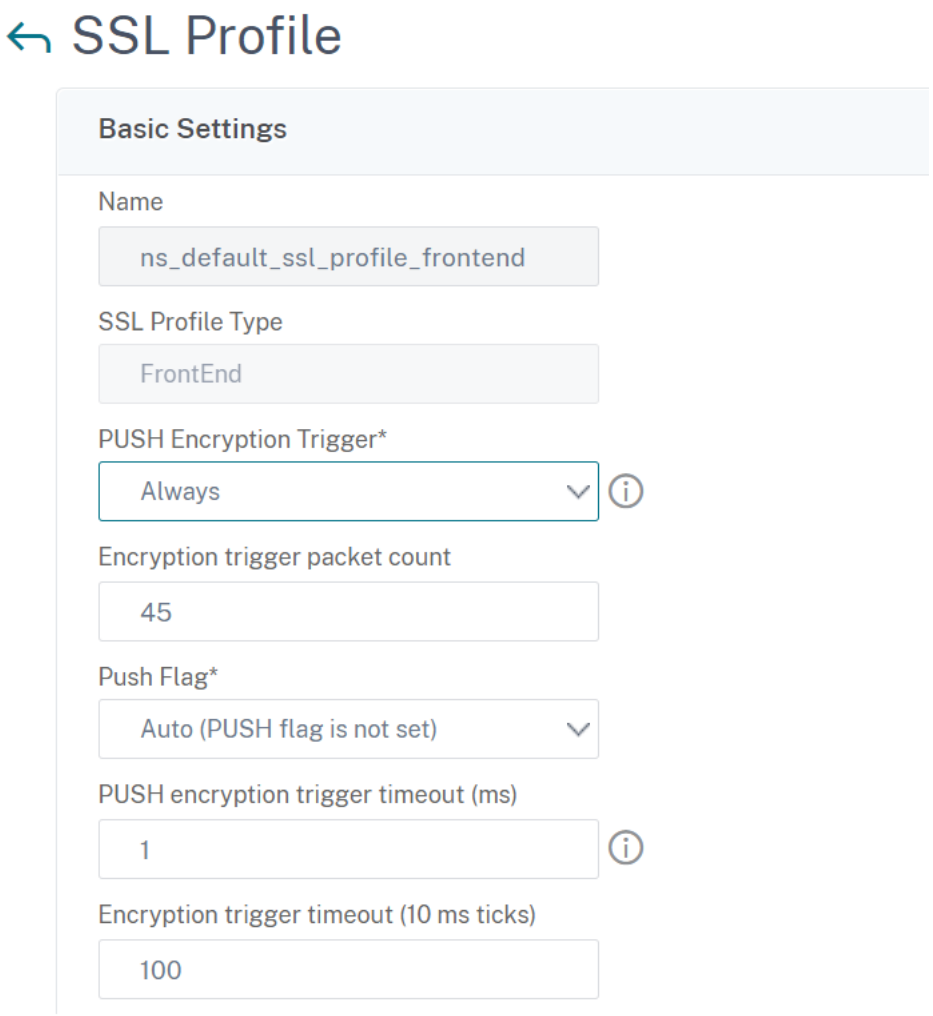
1. En la sección **Perfiles**, seleccione el perfil QUIC. Nota: Los perfiles QUIC, HTTP/3 y SSL son integrados.
2. Haga clic en **Aceptar** y luego en **Listo**.



Asociar parámetros de protocolo SSL/TLS con el servidor virtual de tipo SSL mediante la GUI

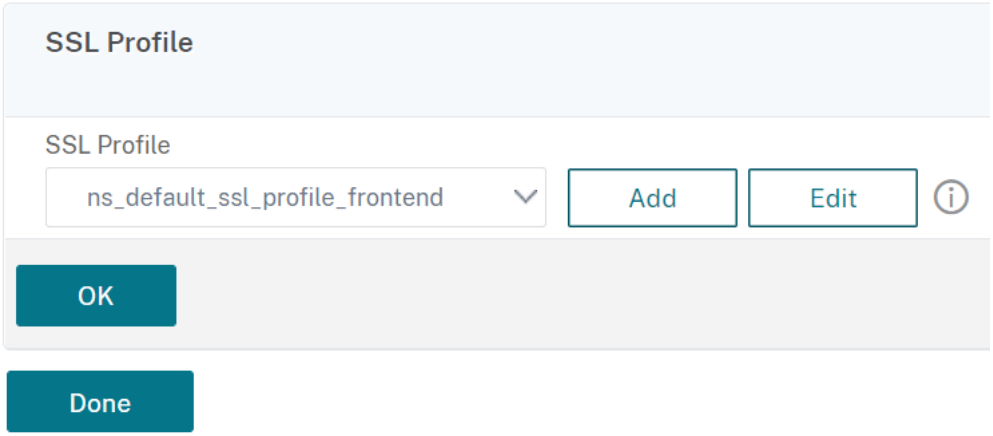
Paso 1: Agregar perfil SSL

1. Vaya a **Sistema > Perfiles > Perfil SSL**.
2. Haga clic en **Agregar**.
3. En la página **Perfil QUIC**, establezca los parámetros SSL. Para obtener una descripción detallada, consulte el tema de configuración del perfil SSL.
4. Haga clic en **Aceptar** y **cerrar**.



Paso 2: Asocie el perfil SSL con un servidor virtual de equilibrio de carga de tipo SSL.

1. En la sección **Perfiles**, seleccione el perfil SSL.
2. Haga clic en **Aceptar** y luego en **Listo**.



Ver estadísticas de QUIC y HTTP/3

Los siguientes comandos muestran un resumen detallado de QUIC y estadísticas HTTP3. En el símbolo del sistema, escriba lo siguiente:

```
> stat quic
> stat quic  - detail
<!--NeedCopy-->
```

Para borrar la visualización de estadísticas, escriba una de las siguientes opciones:

```
> stat quic -clearstats basic
> stat quic -clearstats full

<!--NeedCopy-->
```

Para mostrar un resumen detallado de las estadísticas HTTP/3:

```
> stat http3
> stat http3  - detail
<!--NeedCopy-->
```

Para borrar la visualización de estadísticas, escriba una de las siguientes opciones:

```
> stat http3 -clearstats basic
> stat http3 -clearstats full
<!--NeedCopy-->
```

Configuración de directivas para tráfico HTTP/3

October 5, 2021

HTTP/3 utiliza el transporte QUIC basado en UDP. Si ha definido una expresión de directiva para el servidor virtual HTTP o SSL que incluye expresiones de directiva TCP, ya no se puede utilizar con un servidor virtual HTTP_QUIC. Todas las demás directivas que no tienen expresiones TCP o clásicas se

pueden enlazar con un servidor virtual HTTP_QUIC. Para que las directivas surtan efecto, debe asegurarse de que las directivas de entidades estén vinculadas a los puntos de enlace globales recién agregados según lo siguiente.

- HTTPQUIC_REQ_DEFAULT
- HTTPQUIC_REQ_OVERRIDE
- HTTPQUIC_RES_DEFAULT
- HTTPQUIC_RES_OVERRIDE

O bien, las directivas se pueden vincular a puntos de enlace de servidores virtuales específicos:

- REQUEST
- RESPONSE

Para obtener más información, consulte el tema Vincular directiva mediante infraestructura de directivas avanzada.

A continuación se presentan las directivas admitidas para la configuración HTTP sobre QUIC:

- Responder
- Reescribe
- Compresión HTTP
- Almacenamiento en caché integrado
- Firewall de aplicaciones web
- Transformación de URL
- SSL
- Optimización de front-end (FEO)
- AppQoE

Configuración de la directiva de respuesta para el tráfico HTTP/3

Los servidores virtuales de tipo HTTP sobre QUIC tienen compatibilidad con directivas de respuesta. Sin embargo, dado que QUIC utiliza UDP como mecanismo de transporte, se excluyen las expresiones basadas en TCP y se incluyen expresiones basadas en UDP.

Las configuraciones de directivas nuevas o existentes con expresiones TCP no se pueden enlazar a servidores virtuales QUIC HTTP/3 o HTTP a través de puntos de enlace globales de QUIC. En lugar de expresiones TCP, las expresiones UDP se pueden incluir en las configuraciones de directivas vinculadas a servidores virtuales QUIC HTTP/3 o HTTP a través de puntos de enlace QUIC.

Agregar acción de respuesta para redirigir URL

Para agregar una acción de respuesta, en el símbolo del sistema, escriba:


```
add responder action <name> <type> (<target> | <htmlpage>) [-comment <
    string>] [-responseStatusCode <positive_integer>] [-reasonPhrase <
    expression>] [-headers <name(value)> ...]
<!--NeedCopy-->
```

Ejemplo:

```
add responder action redirectURL redirect "\"https://www.citrix.com/\""
```

Agregar directiva de Responder

Para agregar una directiva de respuesta, en el símbolo del sistema, escriba:

```
add responder policy <name> <rule> <action> [<undefAction>] [-comment <
    string>] [-logAction <string>] [-appflowAction <string>]
<!--NeedCopy-->
```

Ejemplo:

```
add responder policy res-pol "CLIENT.IP.SRC.IN_SUBNET(10.10.10.10/32)"
redirectURL
```

Agregar expresión UDP basada en directivas de respuesta

Para agregar una expresión UDP basada en directivas de respuesta, en el símbolo del sistema, escriba:

```
add responder policy <name> <rule> <action> [<undefAction>] [-comment <
    string>] [-logAction <string>] [-appflowAction <string>]
<!--NeedCopy-->
```

Ejemplo:

```
add responder policy redirectCitrixUdp "CLIENT.UDP.DSTPORT.EQ(443)"redirectURL
```

Enlazar expresión UDP basada en directivas de respuesta con servidor virtual de equilibrio de carga basado en HTTP/3 QUIC

Para vincular una expresión UDP basada en directivas de respuesta a un servidor virtual de equilibrio de carga, en el símbolo del sistema, escriba:


```
bind lb vserver <name>@ ((<serviceName>@   [-weight <positive_integer>]
     ) | <serviceGroupName>@ |         (-policyName <string>@  [-
    priority <positive_integer>]  [-gotoPriorityExpression <expression>]
      [-type <type>]  [-invoke  (<labelType>  <labelName>) ]  ) | -
    analyticsProfile <string>@)
<!--NeedCopy-->
```

Ejemplo:

```
bind lb vserver lb-http3 -policyName redirectCitrixUdp -priority 9 -gotoPriorityExpres
 END -type REQUEST
```

Directiva de respuesta de enlace con el servidor virtual de equilibrio de carga basado en HTTP/3 QUIC

Para vincular una directiva de respuesta a un servidor virtual de equilibrio de carga, en el símbolo del sistema, escriba:

```
bind lb vserver <name>@ ((<serviceName>@   [-weight <positive_integer>]
     ) | <serviceGroupName>@ |         (-policyName <string>@  [-
    priority <positive_integer>]  [-gotoPriorityExpression <expression>]
      [-type <type>]  [-invoke  (<labelType>  <labelName>) ]  ) | -
    analyticsProfile <string>@)
<!--NeedCopy-->
```

Ejemplo:

```
bind lb vserver lb-http3 -policyName redirectCitrixUdp -priority 10 -
gotoPriorityExpression END -type REQUEST
```

Vincular la directiva de respuesta al punto de enlace global HTTP/3

Para vincular una directiva de respuesta con el punto de enlace global HTTP/3, en el símbolo del sistema, escriba:

```
bind responder global <policyName> <priority>  [<gotoPriorityExpression
    >] [-type <type>] [-invoke (<labelType>  <labelName>) ] bind
    responder global redirectCitrixUdp 3 -type HTTPQUIC_REQ_DEFAULT
<!--NeedCopy-->
```


Ejemplo:

```
bind responder global redirectCitrixUdp 3 -type HTTPQUIC_REQ_DEFAULT
```

> **Nota:**
>
> Para obtener más información, consulte la documentación de la directiva de respuesta.

Reescritura de la configuración de directivas para el tráfico HTTP/3

Los servidores virtuales de tipo HTTP a través de QUIC tienen compatibilidad con directivas de reescritura. Sin embargo, dado que QUIC utiliza UDP como mecanismo de transporte, se excluyen las expresiones basadas en TCP y se incluyen expresiones basadas en UDP.

Las configuraciones de directivas nuevas o existentes con expresiones TCP no se pueden enlazar a servidores virtuales HTTP/3 ni a los puntos de enlace globales HTTP/3 recién agregados. En lugar de expresiones TCP, las expresiones UDP se pueden incluir en las configuraciones de directivas vinculadas a servidores virtuales QUIC HTTP/3 o HTTP a través de puntos de enlace QUIC.

A continuación se presentan los pasos de configuración para configurar la directiva de reescritura para HTTP3 a través de QUIC.

Agregar acción de reescritura para HTTP a través de QUIC

Para agregar una acción de reescritura, en el símbolo del sistema, escriba:

```
1 add rewrite action <name> <type> <target> [<stringBuilderExpr>] [-
     search <expression>] [-refineSearch <expression>] [-comment <string
     >]
2 <!--NeedCopy-->
```

Ejemplo:

```
add rewrite action http3-altsvc-action insert_http_header Alt-Svc q/"h3
-29=\":443\"; ma=3600; persist=1"/
```

Agregar directiva de reescritura para HTTP a través de QUIC

Para agregar una acción de escritura, en el símbolo del sistema, escriba:

```
1 add rewrite policy <name> <rule> <action> [<undefAction>] [-comment  <
     string>] [-logAction <string>]
2 <!--NeedCopy-->
```


Ejemplo:

```
add rewrite policy http3-altsvc-policy true http3-altsvc-action
```

Vincular directiva de reescritura al servidor virtual de equilibrio de carga de tipo HTTP/3_QUIC

Para vincular la directiva de reescritura al servidor virtual de equilibrio de carga, en el símbolo del sistema, escriba:

```
1 bind lb vserver <name>@ ((<serviceName>@ [-weight <positive_integer>] )
      | <serviceGroupName>@ | (-policyName <string>@ [-priority <
     positive_integer>] [-gotoPriorityExpression <expression>] [-type <
     type>] [-invoke (<labelType> <labelName>) ] ) | -analyticsProfile  <
     string>@)
2 <!--NeedCopy-->
```

Ejemplo:

```
bind lb vserver lb-http3 -policyName http3-altsvc-policy -priority 10 -type
 RESPONSE
```

Vincular directiva de reescritura al punto de enlace global HTTP/3

```
1 To bind a responder policy with HTTP/3 global bind point, at the
     command prompt, type:
2 bind rewrite global <policyName> <priority> [<gotoPriorityExpression>]
      [-type <type>] [-invoke (<labelType> <labelName>)]
3 <!--NeedCopy-->
```

Ejemplo:

```
bind rewrite global http3-altsvc-policy 3 -type HTTPQUIC_RES_DEFAULT
```

> **Nota:**
>
> Para obtener más información, consulte Reescritura de la documentación de directivas.

Configuración de directivas de compresión para tráfico HTTP/3

Cuando Citrix ADC recibe una respuesta HTTP de un servidor, evalúa las directivas de compresión integradas y las directivas de compresión personalizadas para determinar si se comprime la respuesta y, en caso afirmativo, el tipo de compresión que se va a aplicar. Las prioridades asignadas a las directivas determinan el orden en que se comparan las directivas con las solicitudes.

Los servidores virtuales de tipo HTTP sobre QUIC tienen compatibilidad con directivas de compresión. Sin embargo, dado que QUIC utiliza UDP como mecanismo de transporte, se excluyen las expresiones basadas en TCP y se incluyen expresiones basadas en UDP.
Las configuraciones de directivas nuevas o existentes con expresiones TCP no se pueden enlazar a servidores virtuales HTTP/3 ni a los puntos de enlace globales HTTP/3 recién agregados. En lugar de expresiones TCP, las expresiones UDP se pueden incluir en las configuraciones de directivas vinculadas a servidores virtuales QUIC HTTP/3 o HTTP a través de puntos de enlace QUIC.

Agregar directiva de compresión

Para agregar una directiva de compresión, en el símbolo del sistema, escriba:

```
1 add cmp policy <name> -rule <expression> -resAction <string>
2 <!--NeedCopy-->
```

Ejemplo:

```
add cmp policy udp_port_cmp_policy -rule "CLIENT.UDP.DSTPORT.EQ(443)"-
resAction COMPRESS
```

Directiva de compresión de enlace con servidor virtual de equilibrio de carga de tipo HTTP/3_QUIC

Para vincular la directiva de transformación de URL con un servidor virtual de equilibrio de carga de tipo HTTP/3_QUIC, en el símbolo del sistema, escriba:

```
1 bind lb vserver <name>@ ((<serviceName>@  [-weight <positive_integer>]
     ) | <serviceGroupName>@ |  (-policyName <string>@  [-priority <
     positive_integer>]  [-gotoPriorityExpression <expression>]  [-type (
      REQUEST | RESPONSE )] [-invoke  (<labelType>  <labelName>) ]  ) |
     -analyticsProfile <string>@)
2 <!--NeedCopy-->
```

Ejemplo:

```
bind lb vserver lb-http3 -policyName udp_port_cmp_policy -priority 10 -type
 RESPONSE
```


Compresión de enlace global a punto de enlace global HTTP/3

Para vincular una directiva de compresión con el punto de enlace global HTTP/3, en el símbolo del sistema, escriba:

```
bind compression global <policyName> <priority>  [<
    gotoPriorityExpression>] [-type <type>] [-invoke (<labelType>  <
    labelName>) ] bind responder global redirectCitrixUdp 3 -type
    HTTPQUIC_REQ_DEFAULT
<!--NeedCopy-->
```

Ejemplo:

```
bind cmp global udp_port_cmp_policy -priority 100 -type HTTPQUIC_RES_DEFAULT
 Global built-in compression policies
```

Después de actualizar el dispositivo a Citrix ADC versión 13.0 compilación 82.x, las siguientes directivas de compresión se enlazarán automáticamente al punto de enlace predeterminado de HTTP/3.

```
> sho cmp global -type HTTPQUIC_RES_DEFAULT
        Policy Name: ns_adv_nocmp_xml_ie
        Priority: 8700
        GotoPriorityExpression: END
        Type: HTTPQUIC_RES_DEFAULT

        Policy Name: ns_adv_nocmp_mozilla_47
        Priority: 8800
        GotoPriorityExpression: END
        Type: HTTPQUIC_RES_DEFAULT

        Policy Name: ns_adv_cmp_mscss
        Priority: 8900
        GotoPriorityExpression: END
        Type: HTTPQUIC_RES_DEFAULT

        Policy Name: ns_adv_cmp_msapp
        Priority: 9000
        GotoPriorityExpression: END
        Type: HTTPQUIC_RES_DEFAULT

        Policy Name: ns_adv_cmp_content_type
        Priority: 10000
        GotoPriorityExpression: END
```



```
25          Type: HTTPQUIC_RES_DEFAULT
26  <!--NeedCopy-->
```

Si no está vinculado, los siguientes comandos se pueden configurar mediante el símbolo del sistema y puede configurar en el dispositivo.

```
bind cmp global ns_adv_nocmp_xml_ie -priority 8700 -gotoPriorityExpression
END -type HTTPQUIC_RES_DEFAULT

bind cmp global ns_adv_nocmp_mozilla_47 -priority 8800 -gotoPriorityExpression
 END -type HTTPQUIC_RES_DEFAULT

bind cmp global ns_adv_cmp_mscss -priority 8900 -gotoPriorityExpression END
 -type HTTPQUIC_RES_DEFAULT

bind cmp global ns_adv_cmp_msapp -priority 9000 -gotoPriorityExpression END
 -type HTTPQUIC_RES_DEFAULT

bind cmp global ns_adv_cmp_content_type -priority 10000 -gotoPriorityExpression
 END -type HTTPQUIC_RES_DEFAULT
```

Para obtener más información, consulte Configuración de directivas de compresión.

Configuración de directivas de almacenamiento en caché para el tráfico HTTP/3

La caché integrada proporciona almacenamiento en memoria en el dispositivo Citrix ADC y ofrece contenido web a los usuarios sin necesidad de un viaje de ida y vuelta a un servidor de origen. En el caso del contenido estático, la memoria caché integrada requiere poca configuración inicial. Después de habilitar la función de caché integrada y realizar la configuración básica (por ejemplo, determinar la cantidad de memoria del dispositivo Citrix ADC que se permite utilizar la caché), la memoria caché integrada utiliza directivas integradas para almacenar y proporcionar tipos específicos de contenido estático, incluidas páginas web simples y archivos de imagen. También puede configurar la caché integrada para almacenar y servir contenido dinámico marcado como no almacenable en caché por servidores web y de aplicaciones (por ejemplo, registros de bases de datos y cotizaciones de stock). Los servidores virtuales de tipo HTTP sobre QUIC tienen compatibilidad con directivas de caché. Sin embargo, dado que QUIC utiliza UDP como mecanismo de transporte, se excluyen las expresiones basadas en TCP y se incluyen expresiones basadas en UDP.

Las configuraciones de directivas nuevas o existentes con expresiones TCP no se pueden enlazar a servidores virtuales HTTP/3 ni a los puntos de enlace globales HTTP/3 recién agregados. En lugar de expresiones TCP, las expresiones UDP se pueden incluir en las configuraciones de directivas vinculadas a servidores virtuales QUIC HTTP/3 o HTTP a través de puntos de enlace QUIC.

Agregar grupo de contenido de caché

Para agregar el grupo de contenido de caché, en el símbolo del sistema, escriba:

```
1 add cache contentGroup <name> [-weakPosRelExpiry <secs> | -relExpiry <
      secs> | -relExpiryMilliSec <msecs> | -absExpiry <HH:MM> ... | -
      absExpiryGMT <HH:MM> ...] [-heurExpiryParam <positive_integer>] [-
      weakNegRelExpiry <secs>] [-maxResSize <KBytes>] [-memLimit <MBytes>]
      ...
2 <!--NeedCopy-->
```

Ejemplo:

```
add cache contentGroup DEFAULT -maxResSize 500
```

Agregar directiva de caché

Para agregar una directiva de caché, en el símbolo del sistema, escriba:

```
1 add cache policy <policyName> -rule <expression> -action <action>  [-
      storeInGroup <string>] [-invalGroups <string> ...] [-invalObjects <
      string> ...] [-undefAction ( NOCACHE | RESET )] add cache policy <
      name> <rule> <profileName> [-comment <string>]  [-logAction <string
      >]
2 <!--NeedCopy-->
```

Ejemplo:

```
add cache policy ctx_doc_pdf -rule "HTTP.REQ.URL.ENDSWITH(\".pdf\")"-action
 CACHE -storeInGroup DEFAULT
```

Directiva de caché de enlace con servidor virtual de equilibrio de carga de tipo HTTP/3_QUIC

Para vincular la directiva de caché con un servidor virtual de equilibrio de carga de tipo HTTP/3_QUIC, en el símbolo del sistema, escriba:

```
1 bind lb vserver <name>@ ((<serviceName>@  [-weight <positive_integer>]
      ) | <serviceGroupName>@ |  (-policyName <string>@  [-priority <
      positive_integer>]  [-gotoPriorityExpression <expression>]  [-type (
       REQUEST | RESPONSE )] [-invoke  (<labelType>  <labelName>) ]  ) |
      -analyticsProfile <string>@)
```



```
<!--NeedCopy-->
```

Ejemplo:

```
bind lb vserver lb-http3 -policyName ctx_doc_pdf -priority 100 -type
REQUEST
```

Vincular directiva de caché global a punto de enlace global HTTP/3

Para vincular un punto de enlace global HTTP/3 de directiva de caché:

```
bind cache global <policy> -priority <positive_integer>  [-
    gotoPriorityExpression <expression>] [-type <type>] [-invoke (<
    labelType> <labelName>) ]
<!--NeedCopy-->
```

Ejemplo:

```
bind cache global ctx_doc_pdf -priority 3 -type HTTPQUIC_REQ_DEFAULT
```

Para obtener más información, consulte Configuración de directiva de caché integrada.

Directivas de caché integradas globales

Después de actualizar el dispositivo a Citrix ADC versión 13.0 compilación 82.x, las siguientes directivas de caché se enlazarán automáticamente al punto de enlace predeterminado de HTTP/3.

Al actualizar a la versión 13.0 82.x, las siguientes directivas de caché se enlazan automáticamente al punto de enlace predeterminado HTTP/3.

```
> sho cache global -type HTTPQUIC_REQ_DEFAULT
1)      Policy Name: NOPOLICY
        Priority: 185883
        GotoPriorityExpression: USE_INVOCATION_RESULT
        Invoke type: policylabel        Invoke name:
           _httpquicReqBuiltinDefaults
        Global bindpoint: HTTPQUIC_REQ_DEFAULT

 Done
> sho cache global -type HTTPQUIC_RES_DEFAULT
1)      Policy Name: NOPOLICY
        Priority: 185883
```



```
        GotoPriorityExpression: USE_INVOCATION_RESULT
        Invoke type: policylabel        Invoke name:
            _httpquicResBuiltinDefaults
        Global bindpoint: HTTPQUIC_RES_DEFAULT

<!--NeedCopy-->
```

Tras una actualización, si las directivas no están vinculadas, puede utilizar los siguientes comandos para enlazar y guardar manualmente la configuración.

```
add cache policylabel _httpquicReqBuiltinDefaults -evaluates
    HTTPQUIC_REQ

add cache policylabel _httpquicResBuiltinDefaults -evaluates
    HTTPQUIC_RES

bind cache policylabel _httpquicReqBuiltinDefaults -policyName
    _nonGetReq -priority 100

bind cache policylabel _httpquicReqBuiltinDefaults -policyName
    _advancedConditionalReq -priority 200

bind cache policylabel _httpquicReqBuiltinDefaults -policyName
    _personalizedReq -priority 300

bind cache policylabel _httpquicResBuiltinDefaults -policyName
    _uncacheableStatusRes -priority 100

bind cache policylabel _httpquicResBuiltinDefaults -policyName
    _uncacheableVaryRes -priority 200

bind cache policylabel _httpquicResBuiltinDefaults -policyName
    _uncacheableCacheControlRes -priority 300

bind cache policylabel _httpquicResBuiltinDefaults -policyName
    _cacheableCacheControlRes -priority 400

bind cache policylabel _httpquicResBuiltinDefaults -policyName
    _uncacheablePragmaRes -priority 500

bind cache policylabel _httpquicResBuiltinDefaults -policyName
    _cacheableExpiryRes -priority 600

```



```
23 bind cache policylabel _httpquicResBuiltinDefaults -policyName
       _imageRes -priority 700
24
25 bind cache policylabel _httpquicResBuiltinDefaults -policyName
       _personalizedRes -priority 800
26
27 bind cache global NOPOLICY -priority 185883 -gotoPriorityExpression
       USE_INVOCATION_RESULT -type HTTPQUIC_REQ_DEFAULT -invoke policylabel
        _httpquicReqBuiltinDefaults
28
29 bind cache global NOPOLICY -priority 185883 -gotoPriorityExpression
       USE_INVOCATION_RESULT -type HTTPQUIC_RES_DEFAULT -invoke policylabel
        _httpquicResBuiltinDefaults
30
31 <!--NeedCopy-->
```

> **Nota:**
>
> Los dos primeros comandos de la lista de comandos y los dos últimos comandos de la misma lista se incluyen en aras de su integridad. Es posible que se produzca un error al ejecutar los cuatro comandos, ya que los comandos ya se ejecutan en el momento del reinicio del dispositivo. Pero puede ignorar estos errores.

Configuración de directivas de transformación de URL para tráfico HTTP/3

La transformación de URL modifica todas las URL de las solicitudes designadas de una versión externa vista por usuarios externos a una URL interna que solo ven los servidores web y los administradores. Puede redirigir las solicitudes de los usuarios sin problemas, sin exponer su estructura de red a los usuarios. También puede modificar URL internas complejas que los usuarios pueden resultar difíciles de recordar en URL externas más sencillas y fáciles de recordar.
Los servidores virtuales de tipo HTTP sobre QUIC tienen compatibilidad con directivas de caché. Sin embargo, dado que QUIC utiliza UDP como mecanismo de transporte, se excluyen las expresiones basadas en TCP y se incluyen expresiones basadas en UDP.
Las configuraciones de directivas nuevas o existentes con expresiones TCP no se pueden enlazar a servidores virtuales HTTP/3 ni a los puntos de enlace globales HTTP/3 recién agregados. En lugar de expresiones TCP, las expresiones UDP se pueden incluir en las configuraciones de directivas vinculadas a servidores virtuales QUIC HTTP/3 o HTTP a través de puntos de enlace QUIC.

Agregar perfil de transformación de URL

Para agregar un perfil de transformación de URL, en el símbolo del sistema, escriba:


```
add transform profile <name> [-type URL]
<!--NeedCopy-->
```

Ejemplo:

```
add transform profile msapps
```

Acción de transformación Agregar URL

Para agregar una acción de transformación de URL, en el símbolo del sistema, escriba:

```
add transform action <name> <profileName> <priority> [-state ( ENABLED
    | DISABLED )]
<!--NeedCopy-->
```

Ejemplo:

```
add transform action docx2doc msapps 2
```

Acción de transformación Agregar URL

Para agregar una acción de transformación de URL para reemplazar URL, en el símbolo del sistema, escriba:

```
add transform action <name> <profileName> <priority> [-state ( ENABLED
    | DISABLED )]
<!--NeedCopy-->
```

Ejemplo:

```
add transform action docx2doc msapps 1
```

Agregar directiva de transformación de URL

Para agregar una directiva de transformación de URL, en el símbolo del sistema, escriba:

```
add transform policy <name> <rule> <profileName> [-comment <string>]
   [-logAction <string>]
<!--NeedCopy-->
```


Ejemplo:

```
add transform policy urltrans_udp ”CLIENT.UDP.DSTPORT.EQ(443)”msapps
```

Vincular URL Directiva de transformación con servidor virtual de equilibrio de carga de tipo HTTP/3_QUIC

Para vincular la directiva de transformación de URL con un servidor virtual de equilibrio de carga de tipo HTTP/3_QUIC, en el símbolo del sistema, escriba:

```
bind lb vserver <name>@ ((<serviceName>@  [-weight <positive_integer>]
    ) | <serviceGroupName>@ |  (-policyName <string>@  [-priority <
    positive_integer>]  [-gotoPriorityExpression <expression>]  [-type (
     REQUEST | RESPONSE )] [-invoke  (<labelType>  <labelName>) ]  ) |
    -analyticsProfile <string>@)
<!--NeedCopy-->
```

Ejemplo:

```
bind lb vs lb-http3 -policyName urltrans_udp -type REQUEST -priority 8
```

Directiva de transformación de URL de enlace global con servidor virtual de equilibrio de carga basado en HTTP/3 QUIC

Para vincular una directiva de transformación de URL punto de enlace global HTTP/3, en el símbolo del sistema, escriba:

```
bind transform global <policyName> <priority>  [<gotoPriorityExpression
    >] [-type <type>] [-invoke (<labelType>  <labelName>) ]
<!--NeedCopy-->
```

Ejemplo:

```
bind transform global urltrans_udp 100 -type HTTPQUIC_REQ_DEFAULT
```

Para obtener más información, consulte Configuración de directivas de transformación de URL.

Configuración de directivas de optimización front-end (FEO) para el tráfico HTTP/3

Los protocolos HTTP que subyacen a las aplicaciones web se desarrollaron originalmente para admitir la transmisión y representación de páginas web simples. Las nuevas tecnologías, como JavaScript y

hojas de estilo en cascada (CSS), y los nuevos tipos de medios, como los vídeos Flash y las imágenes ricas en gráficos, imponen grandes exigencias al rendimiento front-end, es decir, al rendimiento a nivel del explorador. La función de optimización front-end (FEO) de Citrix ADC soluciona estos problemas y reduce el tiempo de carga y el tiempo de procesamiento de las páginas web.

> **Nota:**
>
> `HTTP_QUIC _Override/Default_Request` El tipo no se admite para la vinculación global de directivas FEO.

Acción Agregar optimización front-end (FEO)

Para agregar una acción FEO, en el símbolo del sistema, escriba:

```
1 add feo action <name> [-pageExtendCache] [<cacheMaxage>][-
      imgShrinkToAttrib] [-imgGifToPng] [-imgToWebp] [-imgToJpegXR] [-
      imgInline] [-cssImgInline] [-jpgOptimize] [-imgLazyLoad] [-cssMinify
      ] [-cssInline] [-cssCombine] [-convertImportToLink] [-jsMinify] [-
      jsInline] [-htmlMinify] [-cssMoveToHead] [-jsMoveToEND][-
      domainSharding <string> <dnsShards> ...] [-clientSideMeasurements]
2
3 <!--NeedCopy-->
```

Ejemplo:

```
add feo action feoact -imgGifToPng -pageExtendCache
```

Agregar directiva de optimización de front-end (FEO)

Para agregar una directiva FEO, en el símbolo del sistema, escriba:

```
add feo policy <name> <rule> <action>
```

Ejemplo:

```
add feo policy udp_feo_img ”CLIENT.UDP.DSTPORT.EQ(443)”IMG_OPTIMIZE
```

Vincular la directiva FEO con un servidor virtual de equilibrio de carga de tipo HTTP/3_QUIC

Para vincular la directiva FEO con un servidor virtual de equilibrio de carga de tipo HTTP/3_QUIC, en el símbolo del sistema, escriba:


```
bind lb vserver <name>@ ((<serviceName>@   [-weight <positive_integer>]
     ) | <serviceGroupName>@ |         (-policyName <string>@  [-
    priority <positive_integer>]  [-gotoPriorityExpression <expression>]
      [-type <type>]  [-invoke  (<labelType>  <labelName>) ]  ) | -
    analyticsProfile <string>@)
<!--NeedCopy-->
```

Ejemplo:

```
bind lb vserver lb-http3 -policyName udp_feo_img -priority 4 -gotoPriorityExpression
 END -type REQUEST
```

Vincular la directiva FEO al punto de enlace global HTTP/3

Para vincular una directiva de caché al punto de enlace global HTTP/3, en el símbolo del sistema, escriba:

```
bind cache global <policy> -priority <positive_integer>  [-
    gotoPriorityExpression <expression>] [-type <type>] [-invoke (<
    labelType> <labelName>) ]
<!--NeedCopy-->
```

Ejemplo:

```
bind cache global ctx_doc_pdf -priority 3 -type HTTPQUIC_REQ_DEFAULT
```

Para obtener más información, consulte Configuración de directivas de optimización de front-end.

Configuración de directivas SSL para tráfico HTTP/3

Los servidores virtuales de tipo HTTP sobre QUIC tienen compatibilidad con directivas SSL. Sin embargo, dado que QUIC utiliza UDP como mecanismo de transporte, se excluyen las expresiones basadas en TCP y se incluyen expresiones basadas en UDP.

Las configuraciones de directivas nuevas o existentes con expresiones TCP no se pueden enlazar a servidores virtuales HTTP/3 ni a los puntos de enlace globales HTTP/3 recién agregados. En lugar de expresiones TCP, las expresiones UDP se pueden incluir en las configuraciones de directivas vinculadas a servidores virtuales QUIC HTTP/3 o HTTP a través de puntos de enlace QUIC.

Las directivas SSL con acciones compatibles con TLSv1.3 solo se aplican a los puntos de enlace HTTP/3 o servidores virtuales.

Agregar directiva SSL

Para agregar una directiva FEO, en el símbolo del sistema, escriba:

```
1 add ssl policy <name> -rule <expression> [-action <string>] [-
     undefAction <string>] [-comment <string>]
2 <!--NeedCopy-->
```

Ejemplo:

```
add ssl policy ssl-pol -rule CLIENT.SSL.IS_SSL -action NOOP
```

Vincular directiva SSL al servidor virtual HTTP/3

Para vincular una directiva SSL al servidor virtual HTTP/3, en el símbolo del sistema:

```
1 bind ssl policylabel <labelName> <policyName> <priority> [<
     gotoPriorityExpression>] [-invoke (<labelType> <labelName>)
2 <!--NeedCopy-->
```

Ejemplo:

```
bind ssl vserver lb-http3 -policyName ssl-pol -priority 4 -type REQUEST
```

Agregar directiva SSL con expresión UDP para directiva SSL

Para agregar una directiva SSL con expresión UDP, en el símbolo del sistema:

```
1 add ssl policy <name> -rule <expression> [-action <string>] [-
     undefAction <string>] [-comment <string>]
2 <!--NeedCopy-->
```

Ejemplo:

```
add ssl policy ssl_udp_clnt -rule "CLIENT.UDP.DSTPORT.EQ(443)"-action NOOP
```

Vincular directiva SSL con expresión UDP al servidor virtual HTTP/3

Para vincular una directiva SSL con expresión UDP al servidor virtual HTTP/3, en el símbolo del sistema, escriba


```
1 bind ssl policylabel <labelName> <policyName> <priority> [<
      gotoPriorityExpression>] [-invoke (<labelType> <labelName>)
2 <!--NeedCopy-->
```

Ejemplo:

```
bind ssl vs lb-http3 -policyName ssl_udp_clnt -priority 8 -type REQUEST
```

Agregar directiva SSL para el punto de enlace CLIENTHELLO para el tráfico HTTP/3

Para vincular la directiva SSL para el punto de enlace CLIENTHELLO para el tráfico HTTP/3, en el símbolo del sistema, escriba:

```
1 bind ssl policylabel <labelName> <policyName> <priority> [<
      gotoPriorityExpression>] [-invoke (<labelType> <labelName>)
2 <!--NeedCopy-->
```

Ejemplo:

```
add ssl policy ssl-pol-ch -rule ”CLIENT.SSL.CLIENT_HELLO.CIPHERS.HAS_HEXCODE
(0x1301)”-action RESET
```

Vincular directiva SSL al punto de enlace CLIENTHELLO

Para vincular una directiva SSL al punto de enlace CLIENTHELLO, en el símbolo del sistema, escriba:

```
1 bind ssl policylabel <labelName> <policyName> <priority> [<
      gotoPriorityExpression>] [-invoke (<labelType> <labelName>)
2 <!--NeedCopy-->
```

Ejemplo:

```
bind ssl vs lb-http3 -policyName ssl-pol-ch -type CLIENTHELLO_REQ -priority
 100
```

Vincular directiva SSL al punto de enlace global HTTP/3

Para vincular una directiva SSL al punto de enlace global HTTP/3, en el símbolo del sistema, escriba:

```
bind cache global <policy> -priority <positive_integer> [-gotoPriorityExpression
 <expression>] [-type <type>] [-invoke (<labelType> <labelName>)]
```


Ejemplo:

A continuación se muestra un ejemplo de una directiva DATA vinculada a un punto de enlace global HTTP/3:

```
Bind ssl global -policyName ssl-pol-ch -priority 7 -type HTTPQUIC_DATA_DEFAULT
```

> **Nota:**
>
> La acción de reenvío que se puede establecer para el punto de enlace CLIENTHELLO para servidores virtuales SSL no se admite actualmente para los servidores virtuales de tipo HTTP_QUIC.

Configuración de la directiva de firewall de aplicaciones para el tráfico HTTP/3

Los servidores virtuales de tipo HTTP sobre QUIC tienen compatibilidad con directivas de firewall de aplicaciones web. Sin embargo, dado que QUIC utiliza UDP como mecanismo de transporte, se excluyen las expresiones basadas en TCP y se incluyen expresiones basadas en UDP.
Las configuraciones de directivas nuevas o existentes con expresiones TCP no se pueden enlazar a servidores virtuales HTTP/3 ni a los puntos de enlace globales HTTP/3 recién agregados. En lugar de expresiones TCP, las expresiones UDP se pueden incluir en las configuraciones de directivas vinculadas a servidores virtuales QUIC HTTP/3 o HTTP a través de puntos de enlace QUIC.

Agregar directiva Firewall de aplicaciones web con expresión UDP

Para agregar la directiva de Web Application Firewall con expresión UDP, en el símbolo del sistema:

```
1 add appfw policy <name> <rule> <profileName> [-comment <string>] [-
     logAction <string>]
2 <!--NeedCopy-->
```

Ejemplo:

```
add appfw policy appfw_udp ”CLIENT.UDP.DSTPORT.EQ(443)”APPFW_BYPASS
```

Enlazar expresiones de registro con una expresión basada en UDP para el perfil de Web Application Firewall

Para enlazar expresiones de registro con el perfil UDP for Web Application Firewall, en el símbolo del sistema:

Ejemplo:


```
bind appfw profile APPFW_BLOCK -logExpression logexp-1 "CLIENT.UDP.DSTPORT.
EQ(443)"
```

Vincular directiva de firewall de aplicaciones con el servidor virtual HTTP/3

Para vincular la directiva Firewall de aplicaciones web con el servidor virtual HTTP/3, en el símbolo del sistema:

```
1 bind appfw policylabel <labelName> <policyName> <priority> [<
     gotoPriorityExpression>] [-invoke (<labelType> <labelName>)
2 <!--NeedCopy-->
```

Ejemplo:

```
bind lb vs lb-http3 -policyName appfw_udp -priority 3 -type REQUEST
```

Vincular la directiva Firewall de aplicaciones web al punto de enlace global HTTP/3

Para vincular una directiva Firewall de aplicaciones web al punto de enlace global HTTP/3, en el símbolo del sistema, escriba:

```
1 bind appfw global <policy> -priority <positive_integer>  [-
     gotoPriorityExpression <expression>] [-type <type>] [-invoke (<
     labelType> <labelName>) ]
2 <!--NeedCopy-->
```

Ejemplo:

```
bind appfw global appfw_udp 100 -type HTTPQUIC_REQ_DEFAULT
```

Configuración de la directiva de AppQoe para el tráfico HTTP/3

Los servidores virtuales de tipo HTTP sobre QUIC tienen compatibilidad con directivas de AppQoE. Sin embargo, dado que QUIC utiliza UDP como mecanismo de transporte, se excluyen las expresiones basadas en TCP y se incluyen expresiones basadas en UDP.
Las configuraciones de directivas nuevas o existentes con expresiones TCP no se pueden enlazar a servidores virtuales HTTP/3 ni a los puntos de enlace globales HTTP/3 recién agregados. En lugar de expresiones TCP, las expresiones UDP se pueden incluir en las configuraciones de directivas vinculadas a servidores virtuales QUIC HTTP/3 o HTTP a través de puntos de enlace QUIC.

Agregar directiva de AppQoE con expresión basada en UDP

Para agregar una directiva de AppQOE con expresión UDP, en el símbolo del sistema:

```
1 add AppQoE policy <name> <rule> <profileName> [-comment <string>] [-
     logAction <string>]
2 <!--NeedCopy-->
```

Ejemplo:

```
add appqoe policy appqoe-pol-udp -rule ”CLIENT.UDP.DSTPORT.EQ(443)”-action
appqoe-act-basic-prhigh
```

Vincular la directiva de AppQoE con el servidor virtual HTTP/3

Para vincular la directiva de AppQoE con el servidor virtual HTTP/3, en el símbolo del sistema, escriba:

```
1 bind appqoe policylabel <labelName> <policyName> <priority> [<
     gotoPriorityExpression>] [-invoke (<labelType> <labelName>)
2 <!--NeedCopy-->
```

Ejemplo:

```
bind lb vs lb-http3 -policyName appqoe-pol-udp -type REQUEST -priority 3
```

Vincular la directiva de AppQOE al servidor virtual HTTP_QUIC

Para vincular la directiva de AppQoe al servidor `HTTP_QUIC` virtual, en el símbolo del sistema, escriba:

```
1 bind appqoe <policy> -priority <positive_integer>  [-
     gotoPriorityExpression <expression>] [-type <type>] [-invoke (<
     labelType> <labelName>) ]
2 <!--NeedCopy-->
```

Ejemplo:

```
bind lb vs lb-http3 -policyName appqoe-pol-primd -priority 8 -type REQUEST
```


Detección de servicios HTTP/3

August 20, 2021

El protocolo HTTP se basa en el uso de servicios alternativos HTTP para el servidor de origen para anunciar la disponibilidad de un servicio equivalente. La detección de servicios HTTP/3 también utiliza el mismo principio. Se puede anunciar un endpoint HTTP/3 alternativo mediante cualquiera de los siguientes métodos:

- Encabezado de respuesta HTTP Alt-Svc
- Marco HTTP/2 Alt-Svc en la respuesta
- Negociación de protocolos de capa de aplicación (ALPN)

El servicio alternativo anuncia el uso de un encabezado de respuesta HTTP Alt-Svc y el marco HTTP/2 Alt-Svc como endpoint HTTP/3. Los servidores pueden servir HTTP/3 en cualquier puerto UDP. Un anuncio de servicio alternativo incluye un puerto explícito y las URL contienen un puerto explícito o un puerto predeterminado asociado al esquema.

Los clientes que reciben encabezados o tramas de servicio alternativos no están obligados a usarlos. El cliente, si se informa de un servicio alternativo y si es compatible con el mecanismo de servicio alternativo, debe utilizar el servicio alternativo adecuado anunciado. En otras palabras, un servicio HTTP/1.1 o un servicio HTTP/2 pueden anunciar un endpoint equivalente compatible con el protocolo HTTP/3. El cliente al recibir esta información de servicio alternativo puede elegir establecer una conexión QUIC con el servicio alternativo especificado y, una vez disponible, esta conexión se puede utilizar para cualquier solicitud posterior. Si falla el establecimiento de la conexión con el servicio alternativo seleccionado, el cliente puede volver al punto final original. Cuando el cliente comience a utilizar el servicio alternativo anunciado, lo indicará incluyendo un encabezado Alt-Used.

Citrix ADC admite puntos finales HTTP/3 equivalentes de publicidad en servidores virtuales de tipo HTTP y SSL.

Configurar la detección de servicios HTTP/3

Siga los siguientes pasos para configurar la detección de servicios HTTP/3:

1. Configurar el endpoint de servicio alternativo HTTP/3 mediante un encabezado HTTP Alt-Svc
2. Configure el endpoint de servicio alternativo HTTP/3 mediante un marco HTTP/2 Alt-Svc
   Configurar el endpoint de servicio alternativo HTTP/3 mediante un encabezado HTTP Alt-Svc
   Para anunciar un endpoint HTTP/3 mediante un encabezado HTTP Alt-Svc, escriba el siguiente comando:

Nota: El objetivo principal del servicio alternativo publicitario es informar al usuario que se puede acceder a la capacidad HTTP/3 en el servicio HTTP/1.1 o HTTP/2 también en a.b.c.d:443.


```
1 add ns httpProfile <name> -custom -altsvc [ ENABLED | DISABLED ]
2 <!--NeedCopy-->
```

Ejemplo:

```
1 add ns httpProfile http-profile -altsvc ENABLED -altSvcValue  ”h3-29=”
     :443”; ma=3600; persist=1”
2 <!--NeedCopy-->
```

O bien:

```
1 set ns httpProfile http-custom -altsvc ENABLED -altSvcValue  ”h3-29=”
     :443”; ma=3600; persist=1”
2 <!--NeedCopy-->
```

Configurar el endpoint de servicio alternativo HTTP/3 mediante un marco HTTP/2 Alt-Svc

Para anunciar un endpoint HTTP/3 mediante un marco HTTP/2 Alt-SVC, escriba el siguiente comando:

```
1 add ns httpProfile <name> -custom -altsvc [ ENABLED | DISABLED ] -
     http2AltSvcFrame [ ENABLED | DISABLED ]
2 <!--NeedCopy-->
```

Ejemplo:

```
add ns httpProfile http-custom -http2 ENABLED -http2Direct ENABLED -http2AltSvcFrame
 ENABLED -altsvc ENABLED -altSvcValue ”h3-29=\”:443\”; ma=3600; persist=1”
```

O bien:

```
set ns httpProfile http-custom -http2 ENABLED -http2Direct ENABLED -http2AltSvcFrame
 ENABLED -altsvc ENABLED -altSvcValue ”h3-29=\”:443\”; ma=3600; persist=1”
```

Configurar el servicio alternativo HTTP/3 con el valor de encabezado HTTP Alt-Svc mediante GUI

1. Vaya a **Sistema > Perfiles > Perfiles HTTP**.

2. Haga clic en **Add**.
3. En la página **Crear perfil HTTP**, vaya a la sección HTTP/3 y active la casilla de verificación **Servicio alternativo** .
4. El sistema muestra el cuadro de texto **Valor de servicio alternativo** en la sección http2.
5. Introduzca el valor de servicio alternativo como “h3-29=” :443”; ma=3600; persist=1”
6. Haga clic en **Aceptar** y **Cerrar**.

gRPC

August 20, 2021

GRPC en un dispositivo Citrix ADC es un marco de llamada a procedimiento remoto (RPC) universal de código abierto, ligero y de alto rendimiento. El marco es óptimo para trabajar en varios idiomas que se ejecutan en cualquier sistema operativo. Además, cuando se compara con otros protocolos, GRPC ofrece un mejor rendimiento y seguridad.

Se prefiere GRPC para Citrix ADC por las siguientes razones:

- Cree aplicaciones distribuidas para infraestructura de nube público-privada y de centros de datos.
- Proporcione comunicación cliente-servidor para dispositivos móviles, web o en la nube.
- Acceda a servicios y aplicaciones en la nube
- Implementaciones de microservicios

Por qué GRPC en Citrix ADC

GRPC en Citrix ADC se implementa a través de HTTP/2 para admitir API escalables y de alto rendimiento. El uso de binario que texto mantiene la carga útil compacta y eficiente. En Citrix ADC, las solicitudes HTTP/2 se multiplexan a través de una única conexión TCP, lo que permite que varios

mensajes simultáneos estén en vuelo sin comprometer el uso de recursos de red. También utiliza compresión de encabezado para reducir el tamaño de las solicitudes y respuestas.

grPC admite los siguientes tipos de métodos de servicio para que un cliente invoque de forma remota parámetros y tipos de devolución.

1. **RPC unario**. El cliente envía una sola solicitud al servidor GRPC y obtiene una única respuesta de vuelta.

   Ejemplo:
   ```
   rpc SayHello(HelloRequest)returns (HelloResponse);
   ```

2. **RPC de transmisión del servidor**. El cliente envía una sola solicitud al servidor GRPC y obtiene una respuesta de flujo.

   Ejemplo:
   ```
   rpc StreamingResponse(HelloRequest)returns (HelloResponse);
   ```

3. **RPC de transmisión de clientes**. El cliente envía una secuencia de mensajes y espera a que el servidor lea y devuelva su respuesta.

   Ejemplo:
   ```
   rpc IntroduceYourself(stream HelloRequest)returns (HelloResponse)
   ```

4. **RPC de transmisión bidireccional**. Tanto el cliente como el servidor de ambos lados envían una secuencia de mensajes mediante la secuencia de lectura-escritura. Las dos corrientes funcionan de forma independiente.

   Ejemplo:
   ```
   rpc ChatSession (stream HelloRequest)returns (stream HelloResponse)
   ```

Citrix ADC admite las siguientes capacidades para sus servicios con endpoints de GRPC:

- Equilibrio de carga
- Cambio de contenido
- Servicios de punto final seguros como Web Application Firewall, autenticación.
- Configuración de directivas
- Estadísticas y registro
- Reescritura de contenido, filtrado de contenido
- Optimizaciones de capa 4 y capa 7, oferta TLS
- Soluciones de gateway para traducciones de protocolos

Configuración integral de GRPC

August 20, 2021

La configuración integral de GRPC funciona enviando una solicitud de GRPC desde un cliente a través del protocolo HTTP/2 y reenviando de nuevo los mensajes de GRPC respondidos por el servidor de GRPC.

Cómo funciona la configuración integral de GRPC

En el siguiente diagrama se muestra una configuración de GRPC funciona en un dispositivo Citrix ADC.

1. Para implementar la configuración de GRPC, primero debe habilitar HTTP/2 en el perfil HTTP y también habilitar la compatibilidad con HTTP/2 globalmente en el lado del servidor.
2. Cuando un cliente envía una solicitud de GRPC, el servidor virtual de equilibrio de carga evalúa el tráfico de GRPC mediante directivas.
3. Basado en la evaluación de directivas, el servidor virtual de equilibrio de carga (con el servicio GrPC vinculado a él) finaliza la solicitud y la reenvía como una solicitud GRPC al servidor GRPC back-end.
4. Del mismo modo, cuando el servidor de GRPC responde al cliente, el dispositivo finaliza la respuesta y la reenvía como una respuesta de GRPC al cliente.

Ejemplo de solicitud de GRPC enviada al servidor de GRPC

El encabezado de solicitud se envía como encabezados HTTP/2 en ENCABEZADERS+CONTINUACIÓN Frames.

```
```
HEADERS (flags = END_HEADERS)
: method = POST
: scheme = http
: path = /helloworld.citrix-adc/SayHello
: authority = 10.10.10.10.:80
grpc-timeout = 15
content-type = application/grpc+proto
```

 
```

```
grpc-encoding = gzip
DATA (flags = END_STREAM)
<Length-Prefixed Message>
<!--NeedCopy--> ```
```

Ejemplo de encabezado de respuesta de GRPC del servidor GRPC al dispositivo Citrix ADC

Solo cabeceras de respuesta y remolques se entregan en un único bloque de tramas HTTP/2 HEADERS. Se espera que la mayoría de las respuestas tengan encabezados y tráilers, pero solo Trailers está permitido para llamadas que produzcan un error inmediato. El estado debe enviarse en Trailers incluso si el código de estado HTTP es correcto.

```
```
HEADERS (flags = END_HEADERS)
: status = 200
Grpc-encoding= gzip
Content-type = application/grpc+proto
DATA
<Length-Prefixed Message>
HEADERS (flags = END_STREAM, END_HEADERS)
grpc-status = 0 # OK

<!--NeedCopy--> ```
```

### Configurar GRPC mediante la CLI

Para configurar una implementación integral de GRPC, debe completar lo siguiente:

- Agregar perfil HTTP con HTTP/2 y HTTP/2 directo habilitados.
- Habilitar el soporte global de back-end HTTP/2 en el parámetro HTTP
- Agregar servidor virtual de equilibrio de carga de tipo SSL/HTTP y establecer el perfil HTTP
- Agregar servicio para endpoint de GRPC y establecer el perfil HTTP
- Enlazar el servicio de punto final de GRPC al servidor virtual de equilibrio de carga

#### Agregar perfil HTTP con HTTP/2 y HTTP/2 habilitados directamente

Debe habilitar los parámetros directos HTTP/2 y HTTP/2 en el perfil HTTP. Además, debe habilitar el parámetro HTTP/2 direct si se requiere GRPC sobre HTTP/2.

En el símbolo del sistema, escriba:

 
```

```
add ns httpProfile <name> - http2 ( ENABLED | DISABLED )[-http2Direct (
ENABLED | DISABLED )]
```

Ejemplo:

```
add ns httpProfile http2gRPC -http2Direct ENABLED -http2 ENABLED
```

Habilitar el soporte global HTTP/2 de back-end a través del parámetro HTTP

Para habilitar el soporte HTTP/2 globalmente en el servidor mediante la línea de comandos de Citrix ADC.

En el símbolo del sistema, escriba:

```
set ns httpParam -http2ServerSide( ON | OFF )
```

Ejemplo:

```
set ns httpParam -http2ServerSide ON
```

Agregar servidor virtual de equilibrio de carga de tipo SSL/HTTP y establecer el perfil HTTP

Para agregar un servidor virtual de equilibrio de carga mediante la interfaz de comandos de **Citrix ADC** :

En el símbolo del sistema, escriba:

```
add lb vserver <name> <service type> [(<IP address>@ <port>)] [-httpProfileName
 <string>]
```

Ejemplo:

```
add lb vserver lb-grpc HTTP 10.10.10.11 80 -httpProfileName http2gRPC
```

> **Nota:**
>
> Si utiliza un servidor virtual de equilibrio de carga de tipo SSL, debe enlazar el certificado del servidor. Consulte el tema Enlazar certificado de servidor para obtener más información.

Agregar servicio para endpoint de GRPC y establecer el perfil HTTP

Para agregar un servicio GRPC con perfil HTTP mediante la interfaz de comandos de **Citrix ADC** :
En el símbolo del sistema, escriba:

```
add service <name> (<IP> | <serverName> )<serviceType> <port> [-httpProfileName
 <string>]
```

Ejemplo:

```
add service svc-grpc 10.10.10.10 HTTP 80 -httpProfileName http2gRPC
```


Enlazar el servicio de punto final de GRPC al servidor virtual de equilibrio de carga

Para enlazar un servicio GRPC al servidor virtual de equilibrio de carga mediante la interfaz de comandos de **Citrix ADC** :

En la interfaz de comandos, escriba:

```
bind lb vserver <name> <serviceName>
```

Ejemplo:

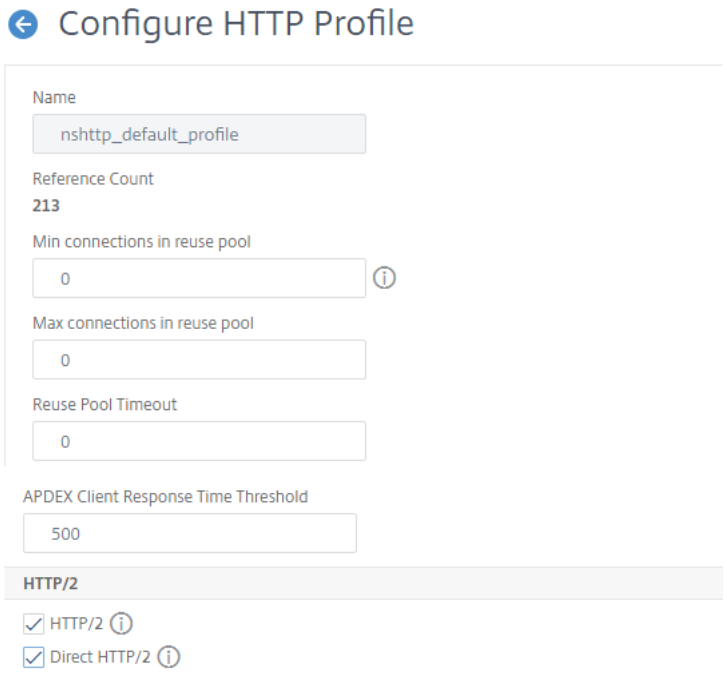
```
bind lb vserver lb-grpc svc-grpc
```

Configurar la implementación integral de GRPC mediante la interfaz gráfica de usuario

Complete los siguientes pasos para configurar GRPC mediante la GUI.

Agregar perfil HTTP con HTTP/2 y HTTP/2 habilitados directamente

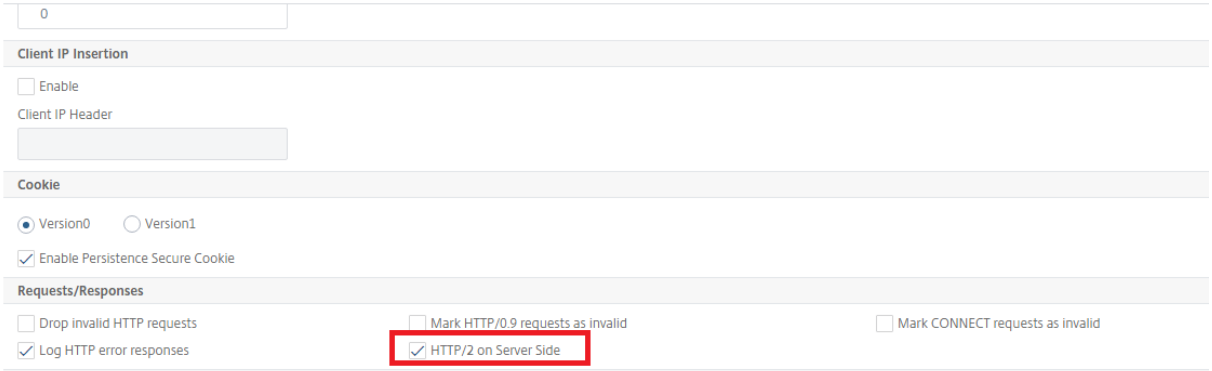
1. Vaya a **Sistema > Perfiles** y haga clic en **Perfiles HTTP**.
2. Habilitar la opción HTTP/2 en un nuevo perfil HTTP o un perfil HTTP existente



Habilitar el soporte global de back-end HTTP/2 en el parámetro HTTP

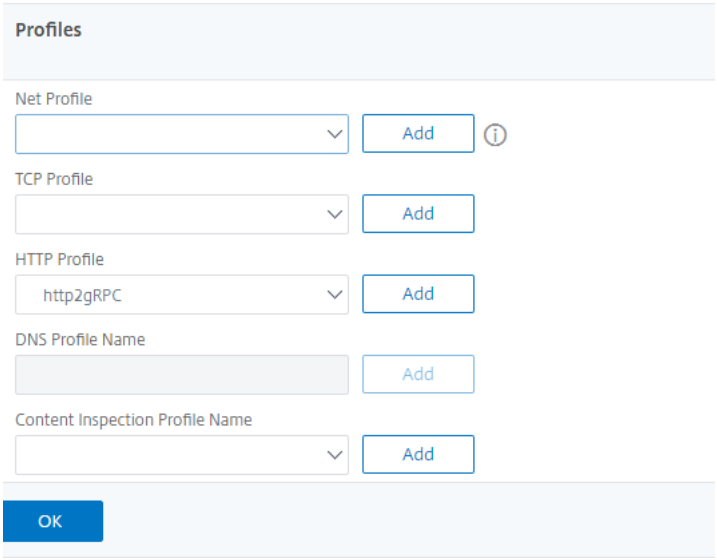
1. Vaya a **Sistema > Configuración > Parámetros HTTP**.
2. En la página Configurar parámetros HTTP, seleccione HTTP/2 en el lado del servidor.

3. Haga clic en **Aceptar**.



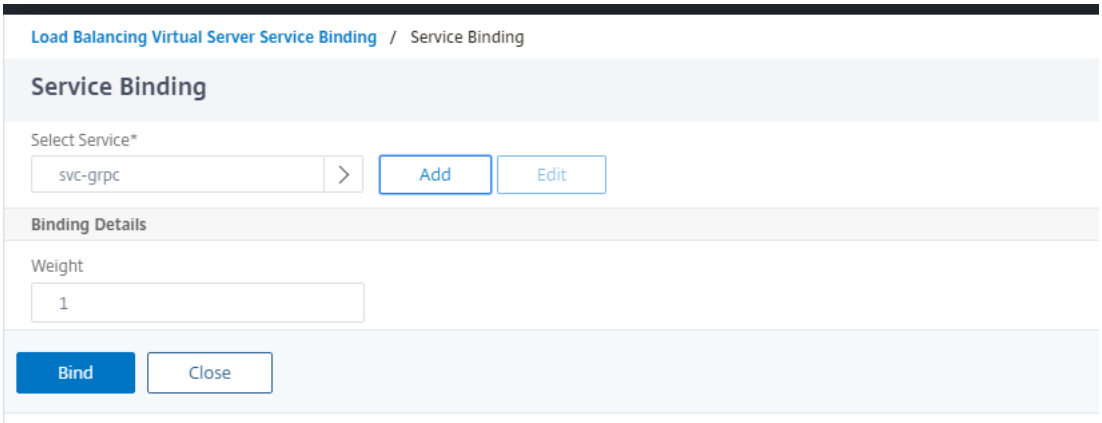
Agregar servidor virtual de equilibrio de carga de tipo SSL/HTTP y establecer el perfil HTTP

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. Haga clic en Agregar para crear un servidor virtual de equilibrio de carga para el tráfico de GRPC.
3. En la página Servidor virtual de equilibrio de carga, haga clic en Perfiles.
4. En la sección Perfiles, seleccione el tipo de perfil como HTTP.
5. Haga clic en Aceptar y, a continuación, Listo.



Agregar servicio para endpoint de GRPC y establecer el perfil HTTP

1. Vaya a **Administración de Tráfico > Equilibrio de carga > Servicios**.
2. Haga clic en Agregar para crear un servidor de aplicaciones para el tráfico de GRPC.
3. En la página Servicio de Equilibrio de carga, vaya a la sección Perfil.
4. En Perfiles, agregue perfil HTTP para el extremo de GRPC.
5. Haga clic en Aceptar y, a continuación, Listo.



Para obtener procedimientos de GUI detallados relacionados con el equilibrio de carga, consulte el tema Equilibrio de carga.

Puente de GRPC

August 20, 2021

Cuando un cliente envía una solicitud a través del protocolo HTTP/1.1, el dispositivo Citrix ADC admite la conexión en puente de las solicitudes de GRPC a través del protocolo HTTP/1.1, que cumple con el servidor GRPC sobre el protocolo HTTP/2. Del mismo modo, en el puente inverso, el dispositivo recibe la solicitud GRPC del cliente a través del protocolo HTTP/2 y realiza un puente inverso para las solicitudes de GRPC de conformidad con el servidor GRPC del protocolo HTTP/1.1.

Cómo funciona el puente de GRPC

En este caso, el dispositivo Citrix ADC conecta sin problemas el contenido grPC recibido en una conexión HTTP/1.1 y lo reenvía al servidor GRPC back-end a través de HTTP/2.

El siguiente diagrama muestra cómo los componentes interactúan entre sí en una configuración de puente de GRPC.

1. Cuando se envía una solicitud de GRPC, el dispositivo Citrix ADC comprueba si la conexión es HTTP/1.1 y el tipo de contenido es application/grpc. Las solicitudes HTTP/1.1 se traducen a los siguientes pseudo encabezados.
2. Al recibir una solicitud de GRPC en la conexión HTTP/1.1. como se indica en el encabezado Content-Type, el dispositivo ADC transforma la solicitud en GRPC a través de HTTP/2 como se indica a continuación:

```
    :method: Method-name in HTTP/1.1 request
    :path: Path is HTTP/1.1 request
    content-type: application/grpc
<!--NeedCopy-->
```

1. Basado en la evaluación de directivas, el servidor virtual de equilibrio de carga (con el servicio GRPC vinculado a él) finaliza la solicitud o la reenvía a través de tramas HTTP/2 al servidor GRPC back-end.
2. Al recibir la respuesta en una conexión HTTP/2 desde el servidor GRPC, el dispositivo almacena en búfer hasta que recibe el tráiler HTTP/2 y, a continuación, comprueba el código de estado GRPC. Si no es un estado de error de GRPC distinto de cero, el dispositivo busca el código de estado HTTP de asignación y envía una respuesta de error HTTP/1.1 adecuada.

Configurar el puente de GRPC mediante la CLI

Para configurar el puente de GRPC, debe realizar los siguientes pasos:

1. Agregar perfil HTTP con HTTP/2 y HTTP/2 habilitados directamente
2. Habilitar el soporte global HTTP/2 de back-end en el parámetro HTTP
3. Agregar servidor virtual de equilibrio de carga de tipo SSL/HTTP y establecer el perfil HTTP
4. Agregar servicio para el extremo de GRPC y establecer el perfil HTTP
5. Enlazar el servicio de punto final de GRPC al servidor virtual de equilibrio de carga
6. Asignar código de estado de GRPC a la respuesta HTTP para el estado de GRPC distinto de cero
7. Configurar el almacenamiento en búfer de GRPC por tiempo y/o tamaño

Agregar perfil HTTP con HTTP/2 y HTTP/2 Direct habilitados

Para comenzar la configuración, debe habilitar la función HTTP/2 en el perfil HTTP. Si el cliente envía las solicitudes HTTP 1.1, el dispositivo enlaza la solicitud y la reenvía al servidor back-end.

En el símbolo del sistema, escriba:

```
add ns httpProfile <name> - http2 ( ENABLED | DISABLED )[-http2Direct (
ENABLED | DISABLED )]
```


Ejemplo:

```
add ns httpProfile http2gRPC -http2Direct ENABLED -http2 ENABLED
```

Habilitar el soporte global HTTP/2 de back-end en el parámetro HTTP

Para habilitar el soporte HTTP/2 globalmente en el servidor mediante la línea de comandos de Citrix ADC.

En el símbolo del sistema, escriba:

```
set ns httpParam -http2ServerSide( ON | OFF )
```

Ejemplo:

```
set ns httpParam -http2ServerSide ON
```

Agregar servidor virtual de equilibrio de carga de tipo SSL/HTTP y establecer el perfil HTTP

Para agregar un servidor virtual de equilibrio de carga mediante la interfaz de comandos de **Citrix ADC**

En el símbolo del sistema, escriba:

```
add lb vserver <name> <service type> [(<IP address>@ <port>)] [-httpProfileName
 <string>]
```

Ejemplo:

```
add lb vserver lb-grpc HTTP 10.10.10.10 80 -httpProfileName http2gRPC
```

> **Nota:**
>
> Si utiliza un servidor virtual de equilibrio de carga de tipo SSL, debe enlazar el certificado del servidor. Consulte el tema Vincular certificado de servidor para obtener más información.

Agregar servicio para el extremo de GRPC y establecer el perfil HTTP

Para agregar un servicio GRPC con el perfil HTTP mediante la interfaz de comandos de **Citrix ADC**.

En el símbolo del sistema, escriba:

```
add service <name> (<IP> | <serverName> )<serviceType> <port> [-httpProfileName
 <string>]
```

Ejemplo:

```
add service svc-grpc 10.10.10.10 HTTP 80 -httpProfileName http2gRPC
```


Enlazar el servicio de punto final de GRPC al servidor virtual de equilibrio de carga

Para enlazar un servicio de punto final de GRPC al servidor virtual de equilibrio de carga mediante la CLI.

En la interfaz de comandos, escriba:

```
bind lb vserver <name> <serviceName>
```

Ejemplo:

```
bind lb vserver lb-grpc svc-grpc
```

Asignar código de estado de GRPC al código de estado HTTP en la respuesta HTTP/1.1

En el caso de puente de GRPC, el servicio GRPC responde a la solicitud con un código de estado de GRPC. El dispositivo asigna el código de estado de GRPC a un código de respuesta HTTP y una frase de motivo correspondientes. El mapeo se realiza sobre la base de la tabla que se proporciona a continuación. El dispositivo Citrix ADC al enviar la respuesta HTTP/1.1 al cliente envía el código de estado HTTP y la frase de motivo.

Código de estado de GRPC	Código de estado de respuesta HTTP	Frase de razón de respuesta HTTP
OK = 0	200	Aceptar
CANCELADO = 1	499	*
DESCONOCIDO = 2	500	Error interno del servidor
ARGUMENTO INVALID_= 3	400	Solicitud incorrecta.
DEADLINE_EXCEEDED = 4	504	Tiempo de espera de gateway
NOT_FOUND = 5	404	*
ALREADY_EXISTS = 6	409	Conflicto
PERMISSION_DENIED = 7	403	Si están prohibidas
SIN AUTENTICAR = 16	401	No autorizado
RESOURCE_AGOTADO = 8	429	*
FAILED_PRECONDITION = 9	400	Solicitud incorrecta.
ABORTADO = 10	409	Conflicto
OUT_OF_RANGE = 11	400	Solicitud incorrecta.
NO EJECUTADOS = 12	501	No implementado
INTERNO = 13	500	Error interno del servidor

Código de estado de GRPC	Código de estado de respuesta HTTP	Frase de razón de respuesta HTTP
NO DISPONIBLE = 14	503	Servicio no disponible
DATA_LOSS = 15	500	Error interno del servidor

Configurar el almacenamiento en búfer de GRPC por tiempo y/o tamaño

El dispositivo Citrix ADC almacena en búfer la respuesta de GRPC desde el servidor back-end hasta que se recibe el tráiler de respuesta. Esto rompe las llamadas de GRPC bidireccionales. Además, si la respuesta de GRPC es enorme, consume una cantidad significativa de memoria para almacenar en búfer la respuesta por completo. Para resolver el problema, se ha mejorado la configuración de puente de GRPC para limitar el almacenamiento en búfer por tiempo y/o tamaño. Si el tamaño del búfer o el límite de tiempo exceden el umbral, el dispositivo detiene el almacenamiento en búfer y reenvía la respuesta al cliente incluso cuando cualquiera de las limitaciones se desencadena (o bien el tráiler no se recibe dentro del tamaño del búfer configurado o si se produce el tiempo de espera configurado). Como resultado, las directivas configuradas y sus expresiones (basadas en el código grpc-status) no funcionan como se esperaba.

Para limitar el almacenamiento en búfer de GRPC por tiempo y/o tamaño por la CLI, puede configurar cuando agrega un nuevo perfil HTTP o cuando modifica un perfil existente.

En el símbolo del sistema, escriba:

```
add ns httpProfile http2gRPC [-grpcHoldLimit <positive_integer>] [-grpcHoldTimeout
 <positive_integer>]
```

O

```
set ns httpProfile http2gRPC [-grpcHoldLimit <positive_integer>] [-grpcHoldTimeout
 <positive_integer>]
```

Donde:

`grpcholdlimit`. Se permite el tamaño máximo en bytes para almacenar en búfer los paquetes de GRPC hasta que se reciba el remolque. Puede configurar tanto los parámetros como cualquiera.

Valor predeterminado: 131072 Valor
mínimo: 0 Valor
máximo: 33554432

`grpcholdtimeout`. Tiempo máximo en milisegundos permitido para almacenar en búfer los paquetes de GRPC hasta que se reciba el remolque. El valor debe estar en múltiplos de 100.
Valor predeterminado: 1000 Valor

mínimo: 0 Valor
máximo: 180000

Ejemplo:

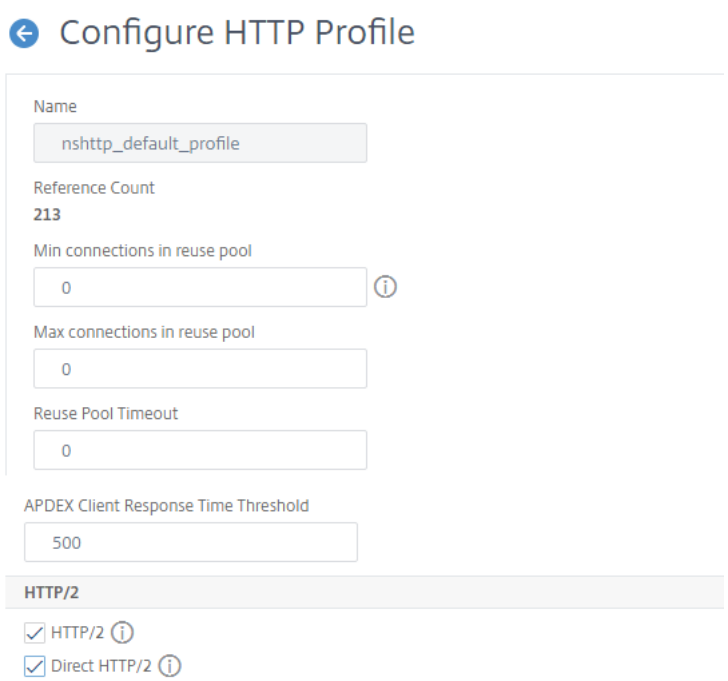
```
add httpprofile http2gRPC -grpcholdlimit 1048576 -grpcholdtimeout 5000
set httpprofile http2gRPC -grpcholdlimit 1048576 -grpcholdtimeout 5000
```

Configurar el puente de GRPC mediante la interfaz gráfica de usuario

Complete los siguientes pasos para configurar el puente de GRPC mediante la GUI de Citrix ADC.

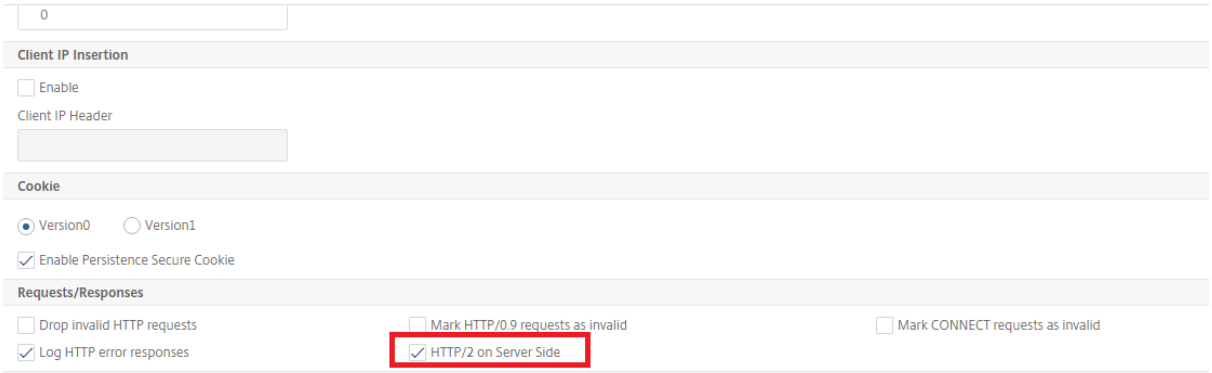
Agregar perfil HTTP con HTTP/2 y HTTP/2 habilitados directamente

1. Vaya a **Sistema > Perfiles** y haga clic en **Perfiles HTTP**.
2. Seleccione **HTTP/2** en el perfil HTTP.



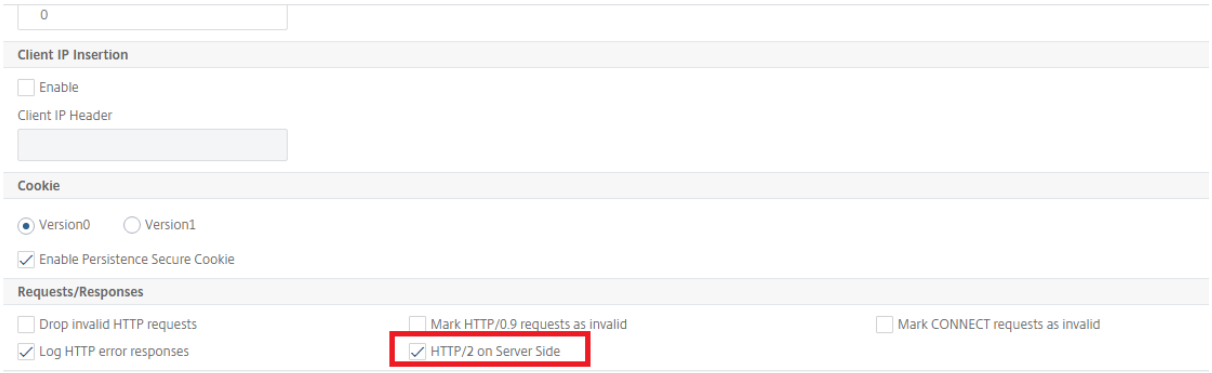
Habilitar el soporte global HTTP/2 de back-end en el parámetro HTTP

1. Vaya a **Sistema > Configuración > Parámetros HTTP**.
2. En la página **Configurar parámetros HTTP**, seleccione la opción **HTTP/2 en el lado del servidor**.
3. Haga clic en **Aceptar**.



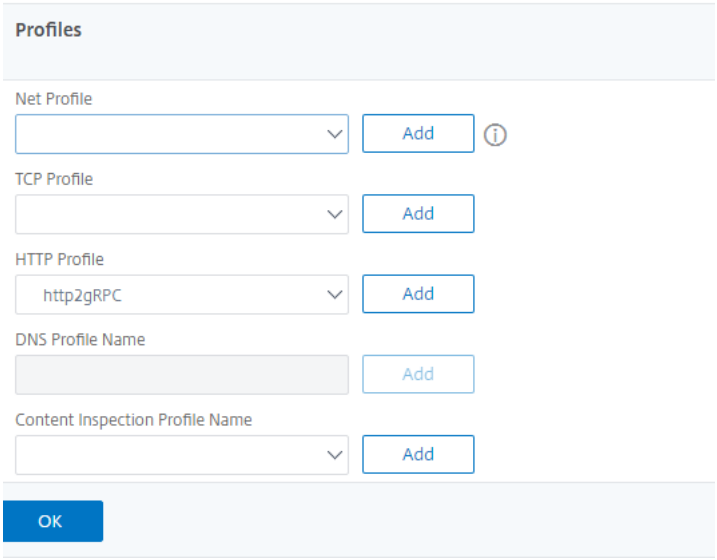
Agregar servidor virtual de equilibrio de carga de tipo SSL/HTTP y establecer el perfil HTTP

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. Haga clic en **Agregar** para crear un servidor virtual de equilibrio de carga para el tráfico de GRPC.
3. En la página **Servidor virtual de equilibrio de carga**, haga clic en **Perfiles**.
4. En la sección **Perfiles**, seleccione el tipo de perfil como HTTP.
5. Haga clic en **Aceptar** y, a continuación, **Listo**.



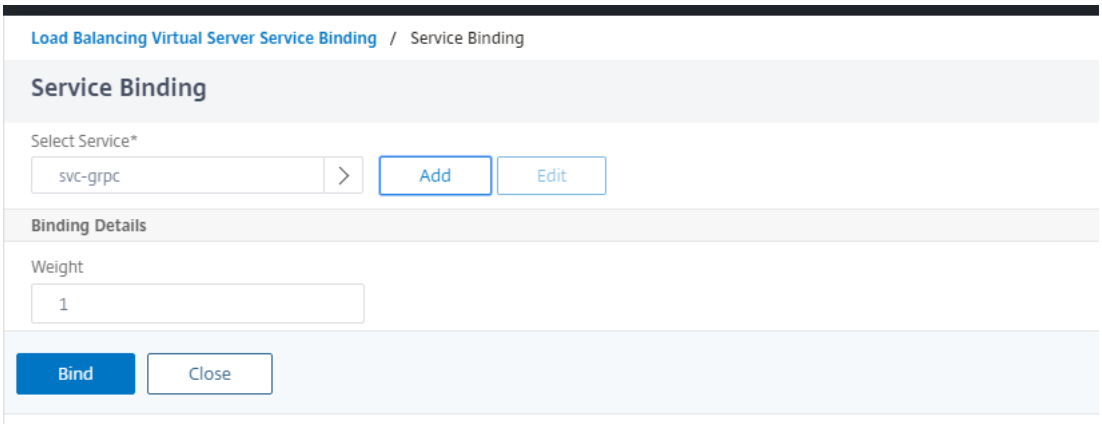
Agregar servicio para endpoint de GRPC y establecer el perfil HTTP

1. Vaya a **Administración de Tráfico > Equilibrio de carga > Servicios**.
2. Haga clic en **Agregar** para crear un servidor de aplicaciones para el tráfico de GRPC.
3. En la página **Servicio de Equilibrio de carga**, vaya a la sección **Perfil**.
4. En **Perfiles**, agregue **perfil HTTP** para el extremo de GRPC.
5. Haga clic en **Aceptar** y, a continuación, **Listo**.



Servicio de enlace para endpoint de GRPC al servidor virtual de equilibrio de carga

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. Haga clic en **Agregar** para crear un servidor virtual de equilibrio de carga para el tráfico de GRPC.
3. En la página **Servidor virtual de equilibrio de carga**, haga clic en la sección **Servicios y grupos de servicios**.
4. En la página **Enlace de Servicio de Servidor Virtual de Equilibrio de Carga**, seleccione el servicio GRPC que quiere enlazar.
5. Haga clic en **Cerrar** y luego en **Listo**.

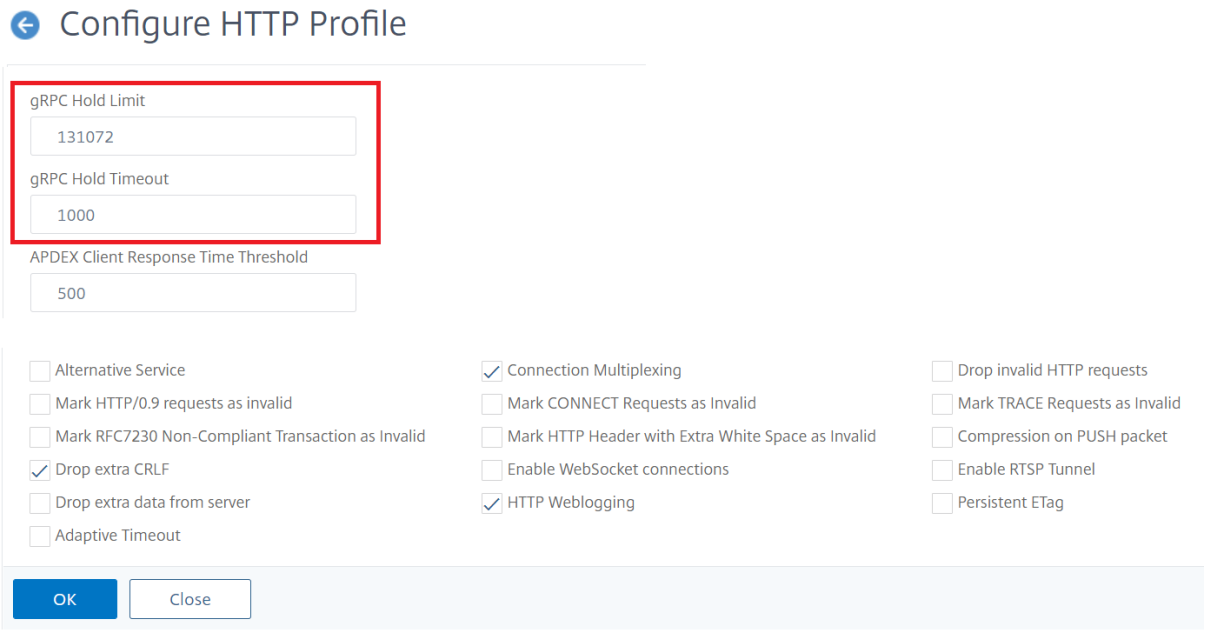


Configurar el almacenamiento en búfer de GRPC por tiempo y tamaño mediante la GUI

1. Vaya a **Sistema > Perfiles** y haga clic en **Perfiles HTTP**.
2. Seleccione **HTTP/2** en el perfil HTTP.
3. En la página **Configurar Perfil HTTP**, defina los siguientes parámetros:

a) grpCholdTimeout. Introduzca el tiempo en milisegundos para almacenar en búfer los paquetes de GRPC hasta que se reciba el remolque.
b) GrpCholdLimit. Introduzca el tamaño máximo en bytes para almacenar en búfer los paquetes de GRPC hasta que se reciba el remolque.

4. Haga clic en **Aceptar** y **Cerrar**.



Para obtener procedimientos de GUI detallados para servicios de enlace y servidores virtuales de equilibrio de carga, consulte el tema Equilibrio de carga.

Puente inverso de GRPC

August 20, 2021

En este caso, el dispositivo Citrix ADC conecta sin problemas el contenido grPC recibido en una conexión HTTP/2 y lo reenvía al servidor GRPC back-end a través de HTTP/1,1.

Cómo funciona el puente inverso

El siguiente diagrama muestra cómo los componentes interactúan entre sí en una configuración de puente de GRPC.

1. El cliente envía una solicitud de GRPC en conexión HTTP/2 con encabezados GRPC en tramas HTTP/2 y proto-buf carga útil.
2. Basado en la evaluación de directivas, el servidor virtual de equilibrio de carga (con el servicio GRPC vinculado a él) traduce y reenvía la solicitud a través de la conexión HTTP/1.1 al servidor backend.
3. Al recibir la respuesta HTTP/1.1, si no hay ningún código grpc-status en la respuesta, ADC deriva un caso de estado grpc del código de respuesta HTTP.
4. A continuación, el dispositivo inserta los encabezados de GRPC en el tráiler HTTP/2 antes de reenviar la respuesta al cliente.

Configurar el puente inverso de GRPC mediante la CLI

Para configurar el puente inverso de GRPC, debe realizar los siguientes pasos:

- Agregar perfil HTTP 1 con HTTP/2 y HTTP/2 habilitado directo para el servidor virtual de equilibrio de carga
- Agregar perfil HTTP 2 con HTTP/2 inhabilitado para el servidor back-end
- Agregar servidor virtual de equilibrio de carga de tipo SSL/HTTP y configurado en perfil HTTP 1
- Agregar servicio para el punto final de GRPC y establecer el perfil HTTP 2
- Servicio de enlace para endpoint de GRPC al servidor virtual de equilibrio de carga
- Asignar código de estado HTTP al código de estado de GRPC si la respuesta no tiene un código de estado grpc

Agregar perfil HTTP 1 con HTTP/2 y HTTP/2 habilitado directo para el servidor virtual de equilibrio de carga

Para iniciar la configuración de puente inverso, debe agregar dos perfiles HTTP. Un perfil para habilitar HTTP/2 para solicitudes de cliente de GRPC y otro perfil para inhabilitar HTTP/2 para respuesta de servidor que no sea GRPC.

En el símbolo del sistema, escriba:

```
add ns httpProfile <name> - http2 ( ENABLED | DISABLED )[-http2Direct (
ENABLED | DISABLED )]
```


Ejemplo:

add ns HttpProfile1 —http2 ENABLED -http2Direct HABILITADO

Agregar perfil HTTP 2 con HTTP/2 inhabilitado para el servidor back-end

Para inhabilitar la compatibilidad con HTTP/2 en el perfil HTTP para la respuesta del servidor back-end mediante la línea de comandos de Citrix ADC.

En el símbolo del sistema, escriba:

```
add ns httpProfile <name> - http2 ( ENABLED | DISABLED )[-http2Direct (
ENABLED | DISABLED )]
```

Ejemplo:

add ns HttpProfile2 —http2 DESHABILITADO Http2Direct DESHABILITADO

Agregar servidor virtual de equilibrio de carga de tipo SSL/HTTP y configurado en perfil HTTP 1

Para agregar un servidor virtual de equilibrio de carga mediante la interfaz de comandos de Citrix ADC.

En el símbolo del sistema, escriba:

```
add lb vserver <name> <service type> [(<IP address>@ <port>)] [-httpProfileName
 <string>]
```

Ejemplo:

agregar lb vserver lb-grpc HTTP 10.10.10.10 80 -HTTPProfileName profile1

> **Nota:**
>
> Si utiliza un servidor virtual de equilibrio de carga de tipo SSL, debe enlazar el certificado del servidor. Consulte el tema Enlazar certificado de servidor para obtener más información.

Agregar servicio para el punto final de GRPC y establecer el perfil HTTP 2

Para agregar un servicio con endpoint de GRPC y establecer el perfil HTTP 2 mediante la interfaz de comandos de Citrix ADC.

En el símbolo del sistema, escriba:

```
add service <name> (<IP> | <serverName> )<serviceType> <port> [-httpProfileName
 <string>]
```

Ejemplo:

```
add service svc-grpc 10.10.10.11 HTTP 80 -httpProfileName profile2
```


Servicio de enlace para el punto final de GRPC al servidor virtual de equilibrio de carga

Para enlazar un servicio GRPC al servidor virtual de equilibrio de carga mediante la interfaz de comandos de Citrix ADC.

En la interfaz de comandos, escriba:

```
bind lb vserver <name> <serviceName>
```

Ejemplo:

```
bind lb vserver lb-grpc svc-grpc
```

Asignar código de respuesta HTTP al código de estado de GrPC

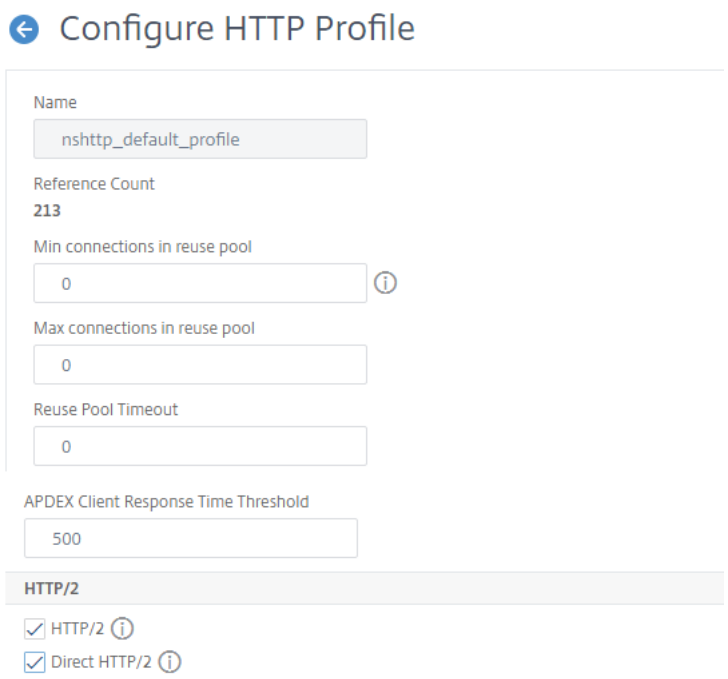
Si el servidor no genera un código de estado GRPC, el dispositivo Citrix ADC genera un código de estado GrPC adecuado basado en la respuesta HTTP recibida. Los códigos de estado se enumeran en la siguiente tabla de asignación.

Código de estado de respuesta HTTP	Código de estado de GRPC
200	Aceptar
400	INTERNO = 13
403	PERMISSION_DENIED = 7
401	SIN AUTENTICAR = 16
429, 502, 503, 504	NO DISPONIBLE = 14
404	NO EJECUTADOS = 12

Configurar el puente inverso de GRPC mediante la GUI

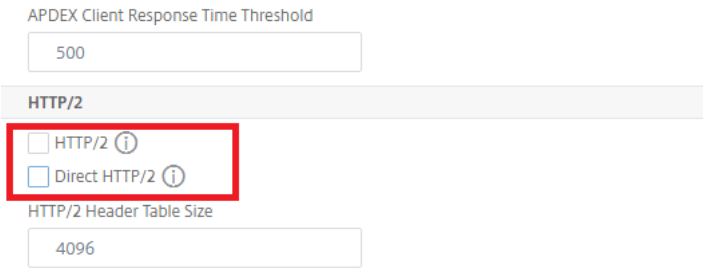
Agregar perfil HTTP 1 con HTTP/2 y HTTP/2 habilitado directo para el servidor virtual de equilibrio de carga

1. Vaya a Sistema > Perfiles y haga clic en Perfiles HTTP.
2. Habilite la opción HTTP/2 en un perfil HTTP 1.



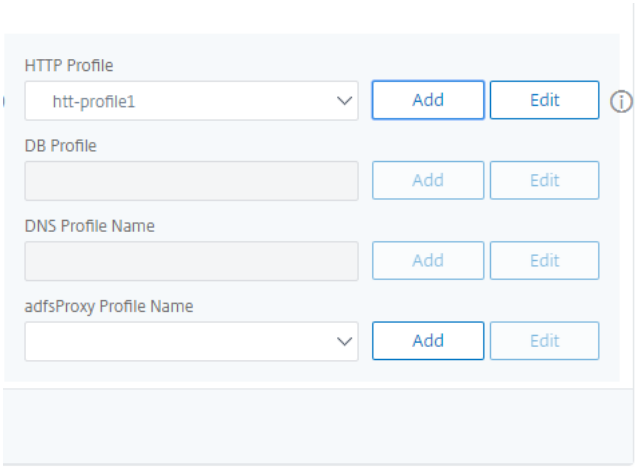
Agregar perfil HTTP 2 con HTTP/2 inhabilitado para el servidor back-end

1. Vaya a **Sistema > Perfiles** y haga clic en **Perfiles HTTP**.
2. Habilite la opción **HTTP/2** en un perfil HTTP 2.
3. Haga clic en **Aceptar**.



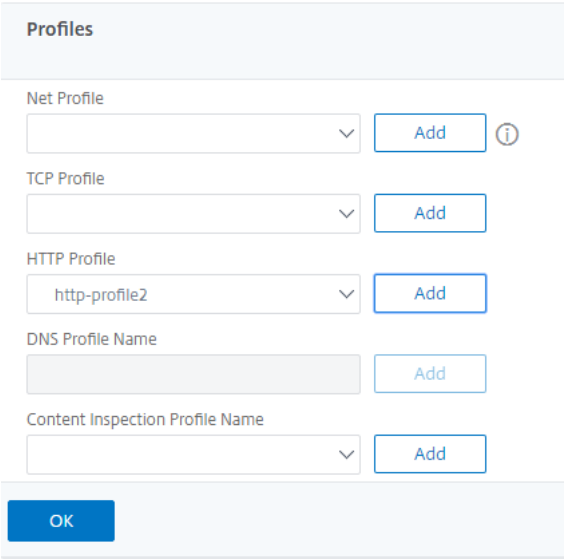
Agregar servidor virtual de equilibrio de carga de tipo SSL/HTTP y configurado en perfil HTTP 1

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. Haga clic en **Agregar** para crear un servidor virtual de equilibrio de carga para el tráfico de GRPC.
3. En la página **Servidor virtual de equilibrio de carga**, haga clic en **Perfiles**.
4. En la sección **Perfiles**, seleccione el tipo de perfil como HTTP.
5. Haga clic en **Aceptar** y, a continuación, **Listo**.



Agregar servicio con endpoint de GRPC y establecer el perfil HTTP 2

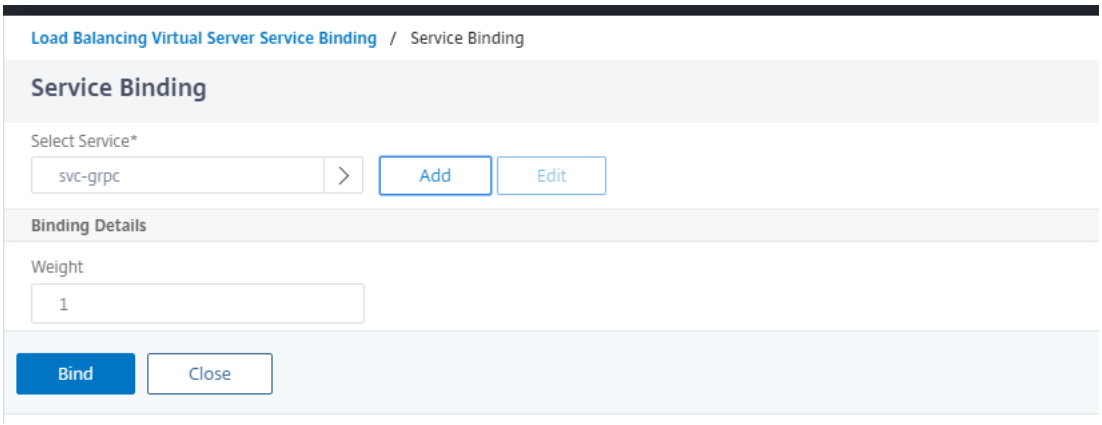
1. Vaya a **Administración de Tráfico > Equilibrio de carga > Servicios**.
2. Haga clic en **Agregar** para crear un servidor de aplicaciones para el tráfico de GRPC.
3. En la página **Servicio de Equilibrio de carga**, vaya a la sección **Perfil**.
4. En **Perfiles**, agregue **perfil HTTP** para el extremo de GRPC.
5. Haga clic en **Aceptar** y, a continuación, **Listo**.



Servicio de enlace para endpoint de GRPC al servidor virtual de equilibrio de carga

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. Haga clic en **Agregar** para crear un servidor virtual de equilibrio de carga para el tráfico de GRPC.

3. En la página **Servidor virtual de equilibrio de carga**, haga clic en la sección **Grupos de**servicios**y servicios** .
4. En la página **Enlace de Servicio de Servidor Virtual de Equilibrio de Carga**, seleccione el servicio GRPC que quiere enlazar.
5. Haga clic en **Cerrar** y luego en **Listo**.



Para obtener procedimientos de GUI detallados, consulte el tema Equilibrio de carga .

Terminación de llamada de GRPC

January 12, 2021

Cuando un dispositivo Citrix ADC tiene directivas como la limitación de velocidad, la seguridad de Web App Firewall configurada y si una directiva se evalúa como true, el dispositivo puede finalizar la llamada y responder con un mensaje de error de GRPC computable al cliente.

GRPC con directiva de reescritura

January 12, 2021

El caso de uso de la directiva GRPC con reescritura explica cómo funciona el dispositivo Citrix ADC para reescribir información en las solicitudes o respuestas de GRPC. El siguiente diagrama muestra los componentes interactúan.

El siguiente diagrama muestra cómo interactúan los componentes entre sí en un GRPC con configuración de directiva de reescritura.

1. Habilitar la función de reescritura en el dispositivo.
2. Configure la acción de reescritura para modificar, agregar o eliminar encabezados de GRPC.
3. Configure la directiva de reescritura para determinar las solicitudes de GRPC (tráfico) en las que se debe realizar una acción.
4. Enlazar la directiva de reescritura al servidor virtual de equilibrio de carga para examinar si el tráfico coincide con la expresión de directiva.
5. Mediante el uso de una directiva de reescritura, puede realizar lo siguiente según el código de estado de GrPC.
   a) Modificar las respuestas del servidor web de GRPC.
   b) Modificar, agregar o eliminar encabezados de GRPC.
   c) Modifique la URL de la solicitud al servidor grRC.

Configurar la terminación de llamadas de GRPC con directiva de reescritura

Para configurar la terminación de llamadas de GRPC con directiva de reescritura, debe realizar los siguientes pasos:

1. Activar función de reescritura
2. Agregar directiva de reescritura
3. Enlazar la directiva de reescritura al servidor virtual de equilibrio de carga

Activar función de reescritura

Para utilizar la función de reescritura, primero debe habilitarla.

En el símbolo del sistema, escriba:

```
enable ns rewrite
```

Agregar directiva de reescritura

Después de configurar una acción de reescritura, debe configurar una directiva de reescritura para seleccionar las solicitudes de GRPC en las que debe volver a escribir el dispositivo Citrix ADC.

En el símbolo del sistema, escriba:

```
add rewrite policy <name> <expression> <action> [<undefaction>]-appFlowaction
 <actionName>
```

Ejemplo:

```
add rewrite policy grpc-rewr_pol1 ”http.res.header(\”grpc-status\”).NE
(\”0\”)”RESET
```

Enlazar la directiva de reescritura al servidor virtual de equilibrio de carga

Para poner en práctica una directiva, debe vincularla al servidor virtual de equilibrio de carga con el servicio GRPC.

En el símbolo del sistema, escriba:

```
bind rewrite global <policyName> <priority> [<gotoPriorityExpression> [-
type <type>] [-invoke (<labelType> <labelName>)]
```

Ejemplo:

```
bind lb vserver lb-grpc -policyName grpc-rewr_pol1 -priority 100
```

gRPC con la directiva de respuesta

August 20, 2021

La configuración de directiva de gRPC con respuesta explica cómo un dispositivo Citrix ADC proporciona respuestas diferentes a las solicitudes de gRPC a través del protocolo HTTP/2. Cuando los usuarios solicitan una página principal del sitio web, es posible que quiera proporcionar una página principal diferente dependiendo de dónde se encuentre cada usuario o del explorador que esté mediante el usuario.

En el siguiente diagrama se muestran los componentes que interactúan.

1. Habilite la función de respuesta en el dispositivo.
2. Configure la acción de respuesta para generar una respuesta personalizada, redirigir una solicitud a una página web diferente o restablecer una conexión.
3. Configure la directiva de respuesta para determinar las solicitudes de GRPC (tráfico) en las que se debe realizar una acción.
4. Enlazar la directiva de respuesta al servidor virtual de equilibrio de carga para examinar si el tráfico coincide con la expresión de directiva.
5. Mediante una directiva de respuesta, puede realizar lo siguiente en función del código de estado de gRPC.

Configurar la finalización de llamadas de gRPC con la directiva de respuesta mediante la CLI

Para configurar la terminación de llamadas de GRPC con la directiva de respuesta, debe completar los siguientes pasos:

1. Habilitar la función de respuesta
2. Agregar una acción de respuesta
3. Agregar una directiva de respuesta y una acción de respuesta asociada
4. Vincular la directiva de respuesta al servidor virtual de equilibrio de carga

Habilitar la función de respuesta

Para utilizar la función respondedor, primero debe habilitarla.

En el símbolo del sistema, escriba:

```
enable ns responder
```

Agregar la acción de respuesta

Después de habilitar la función, debe configurar la acción del respondedor para gestionar la respuesta de GRPC en función del código de estado devuelto por el servidor back-end.

En el símbolo del sistema, escriba:

```
add responder action <name> <type>
```

Ejemplo:

```
add responder action grpc-act respondwith "HTTP/1.1 200 OK\r\nServer: NS
-Responder\r\nContent-Type:application/grpc\r\ngrpc-status: 12\r\ngrpc
-message: Not Implemented\r\n\r\n"+ "Method: "+ HTTP.REQ.URL+ "is not
implemented."
```


Agregar directiva de respondedor

Después de configurar una acción de respuesta, debe configurar una directiva de respuesta para seleccionar la solicitud GRPC a la que debe responder el dispositivo Citrix ADC.

En el símbolo del sistema, escriba:

```
add responder policy <name> <expression> <action> [<undefaction>]-appFlowaction
 <actionName>
```

Ejemplo:

```
add responder policy grpc-resp-pol1 HTTP.REQ.URL.NE( "/helloworld.Greeter/
SayHello" )grpc-act
```

Enlazar la directiva de respuesta al servidor virtual de equilibrio de carga

Para poner en práctica una directiva, debe vincularla al servidor virtual de equilibrio de carga con el servicio GRPC.

En el símbolo del sistema, escriba:

```
bind responder global <policyName> <priority> [<gotoPriorityExpression> [-
type <type>] [-invoke (<labelType> <labelName>)]
```

Ejemplo:

```
bind lb vserver lb-grpc svc-grpc -policyName grpc-resp-pol1 -priority 100
```

Para obtener más información sobre la directiva de respuesta, consulte el tema Directiva de respuesta
.

Expresiones de directiva para coincidir los campos de búfer de protocolo de gRPC

El dispositivo Citrix ADC admite las siguientes expresiones de directiva en la configuración de gRPC:

- **Acceso a campo de búfer de protocolo gRPC.** La llamada arbitraria a la API de gRPC coincide con el número de campo de mensaje con las nuevas expresiones de directiva. En una configuración de PI, las coincidencias se realizan mediante solo los "números de campo" y la "ruta API".
- **Filtrado de encabezados gRPC.** Los parámetros "HttpProfile" para gRPC se utilizan para ajustar el comportamiento predeterminado del análisis de gRPC (incluidas las expresiones de directivas de gRPC). Los siguientes parámetros se aplican a las expresiones de directivas de gRPC:
  - **Delimitación de longitud de GRP.** Está habilitado de forma predeterminada y espera que los búferes de protocolo se presenten con un mensaje delimitado por longitud.

- **Límite de Refía de GRP.** El valor predeterminado es 131072. Es el tamaño máximo del mensaje de búfer de protocolo en bytes. También es la longitud máxima de cadena y la longitud máxima de campo de “byte” también.

Configurar expresiones de directivas avanzadas de gRPC mediante la CLI

En el símbolo del sistema, escriba:

```
set ns httpProfile <name> -http2 ( ENABLED | DISABLED ) -
    gRPCLengthDelimitation ( ENABLED | DISABLED ) -gRPCHoldLimit <int>
```

Ejemplo:

```
set ns httpProfile http2gRPC -http2 ENABLED -gRPCLengthDelimitation
    ENABLED -gRPCHoldLimit 131072
```

Configurar los parámetros de filtrado de encabezados de gRPC mediante la GUI

1. Vaya a **Sistema > Perfiles** y haga clic en **Perfiles HTTP**.
2. En la página **Crear perfil HTTP**, desplácese hacia abajo hasta la sección **HTTP/3** y seleccione **Delimitación de longitud de gRPC**.

En el siguiente ejemplo de expresión de directiva se muestra un valor en el mensaje 5, el submensaje 4 y el campo 3. Es un int de 32 bits igual a 2.

```
http.req.body(1000).grpc.message(5).message(4).int32(3).eq(2)
```

Se añaden las siguientes expresiones de directiva para que coincidan los campos de mensajes de búfer de protocolo de gRPC por número:

- message
- doble
- flotar
- int32
- int64
- uint32
- uint64
- sint64

- sint32
- fixed32
- fixed64
- sfixed32
- sfixed64
- Bool
- cadena
- enum
- bytes

Coincidencia de rutas API

La coincidencia de rutas de API se utiliza para coincidir con la llamada a la API de gRPC correcta cuando se utiliza más de una API. Haga coincidir la ruta de la API, que se encuentra en el pseudo encabezado ': path' de la solicitud HTTP.

Ejemplo:

```
http.req.header(":path").eq("acme.inventory.v1/ListBooks")
```

Monitor de verificación de estado gRPC

December 2, 2021

El monitor de estado gRPC sondea los servidores gRPC para comprobar su estado de salud. El monitor de estado gRPC comprueba el estado general del servicio gRPC o el estado de un servicio en particular. Actualmente, el dispositivo Citrix ADC solo admite el método de comprobación.

En el dispositivo Citrix ADC, el monitor de comprobación de estado se configura al establecer parámetros gRPC, como gRPCHealthCheck gRPCStatusCode, gRPCServiceName y httprequest en la configuración del monitor HTTP2. Un cliente que implementa el protocolo consulta al servidor por su estado (correcto, no correcto, desconocido o servicio no implementado) y espera la respuesta de estado del servicio.

En la siguiente tabla se proporcionan detalles sobre los nuevos parámetros gRPC y su descripción:

parámetros de gRPC	Valor	Descripción
Comprobación de la salud de GRP	Sí/No	Active o inhabilite la sonda de comprobación de estado

parámetros de gRPC	Valor	Descripción
Código de estado GRPC	unsigned int (0-65535), predeterminado: 12	Configure hasta 16 códigos de estado gRPC. El dispositivo busca el código de estado 0 en la respuesta de estado. Si no recibe 0, el servicio puede configurarse si alguno de los 16 códigos coincide con el estado del servicio.
Nombre del servicio GRPC	Nombre del servicio entre comillas dobles, Default = “” (cadena vacía)	Compruebe el estado del servicio en particular.

Configure el monitor de estado de gRPC en HTTP/2 mediante la interfaz de comandos

Para realizar una sonda de comprobación de estado gRPC, debe habilitar el servicio de verificación de estado, configurar el código de estado gRPC y proporcionar el nombre del servicio gRPC para el que se debe realizar la comprobación de estado gRPC. En el símbolo del sistema, escriba:

```
add lb monitor <monitor_name> HTTP2 -httpRequest <string> -grpcHealthCheck
( YES | NO )- grpcStatusCode <positive_integer> - grpcServiceName string>]
```

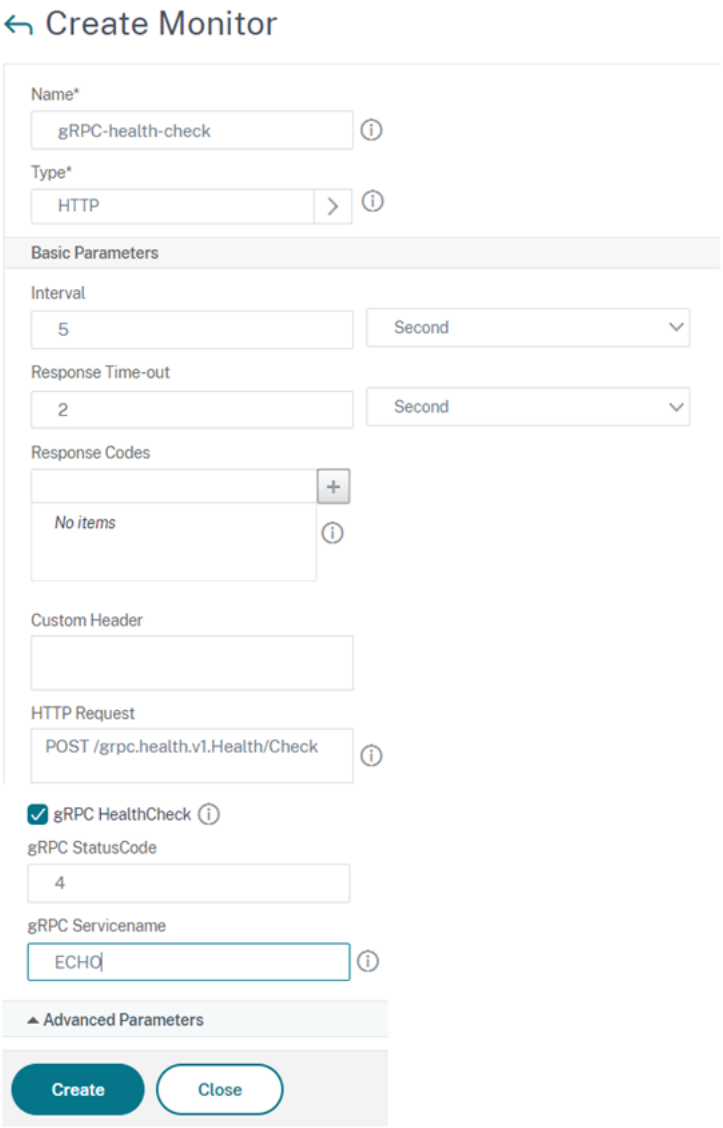
Ejemplo:

```
add lb monitor http2 HTTP2 -httprequest  “POST /grpc.health.v1.Health/Check”
 - gRPCHealthCheck Yes -gRPCStatusCode 0 -grpcServiceName ”ECHO”
```

Configure el monitor de estado gRPC en HTTP/2 mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Monitores**.
2. Haga clic en **Agregar**.
3. En la página **Crear monitor**, defina los siguientes parámetros:
   a) Nombre. Nombre del monitor estado gRPC.
   b) Tipo. Seleccione el tipo de servicio como HTTP/2.
   c) Comprobación de salud de gRPC. Habilite la sonda de verificación de estado gRPC.
   d) Código de estado de gRPC. El estado del servicio gRPC es “UP” solo si el código de estado gRPC es cero o el valor configurado. El estado desciende si el código de estado es un valor distinto de cero o el valor configurado.
   e) gRPC Nombre del servicio. Servicio para el que se realiza la comprobación de estado.

4. Crear **Crear**.



QUIC

August 20, 2021

El protocolo rápido de Internet UDP (QUIC) es una combinación de protocolos (TCP+TLS+HTTP/2) implementados en UDP. El protocolo de transporte QUIC multiplexa las conexiones entre dos extremos mediante UDP. Además, en comparación con otros protocolos, QUIC proporciona un alto rendimiento en términos de seguridad, entrega rápida de tráfico y menor latencia.

Se configura un puente QUIC en un dispositivo Citrix ADC para equilibrar la carga del tráfico QUIC

entre un cliente QUIC y un servidor back-end QUIC. El puente QUIC le permite tener conexiones QUIC persistentes entre el cliente y el servidor si hay un reenlace NAT o una migración de conexión. Sin embargo, esta configuración no procesa datos. Solo se utiliza para equilibrar la carga del tráfico QUIC a través del dispositivo Citrix ADC.

Los paquetes QUIC contienen ID de conexión para permitir que los endpoints asocien los paquetes con una dirección diferente o 4 tuplas a la misma conexión. El ID de conexión contiene los detalles del ID de servidor que se comparte en el dispositivo Citrix ADC y en los servidores back-end. El dispositivo Citrix ADC extrae los detalles del ID de conexión del ID de servidor y envía el tráfico de vuelta al servidor back-end. Los ID de conexión se encuentran en paquetes protegidos que hacen que las conexiones sean sólidas en caso de migración de la conexión.

> **Importante**
>
> Los servidores back-end deben tener soporte para codificar el ID de servidor en el ID de conexión QUIC.

Beneficios del puente QUIC

El puente QUIC para el dispositivo Citrix ADC se prefiere por los siguientes motivos:

- Sin operaciones criptográficas costosas.
- Es posible la redirección sin estado (no hay equilibrio de carga basado en 4 tuplas).

Configuración de puentes QUIC

October 5, 2021

Para configurar el puente QUIC, debe completar lo siguiente:

- Agregar perfil de puente QUIC
- Agregar servidores back-end QUIC
- Agregar servicio QUIC en el dispositivo
- Agregar servidor virtual de equilibrio de carga de tipo puente QUIC
- Vincular puente QUIC al servidor virtual de equilibrio de carga de tipo puente QUIC

> **Importante**
>
> Antes de configurar el puente QUIC, asegúrese de habilitar primero la función de equilibrio de carga en el dispositivo. Para obtener más información, consulte Configurar el equilibrio de carga básico.

Configurar puente QUIC mediante la CLI

Las siguientes secciones deben configurarse mediante la CLI.

Agregar un perfil de puente QUIC

Agregue un perfil de puente QUIC.

En el símbolo del sistema, escriba:

```
add quicBridge profile <name> -routingAlgorithm <PLAINTEXT> -
    serveridlen <value>
```

Ejemplo:

```
add quicBridge profile q1 -routingAlgorithm PLAINTEXT -serveridlen 6
```

> **Nota**
>
> El parámetro `serveridlen` configurado en el ejemplo es la longitud de un ID de servidor personalizado, que es la cadena hexadecimal de IP y PORT.

Agregar servidor de aplicaciones back-end QUIC

Agregue servidores de aplicaciones back-end QUIC.

En el símbolo del sistema, escriba:

```
-  add server <name> (<IPAddress>)
-  add server <name> (<IPAddress>)
```

Ejemplo:

```
-  add server s1 192.0.2.20
-  add server s2 192.0.2.30
```


Agregar servicio puente QUIC

Debe agregar el servicio puente QUIC a los servidores de aplicaciones.

En el símbolo del sistema, escriba:

```
1 - add service  <name>  (<IP> | <serverName>) <serviceType> <port> [-
    CustomServerID <string>]
2
3 - add service  <name>  (<IP> | <serverName>) <serviceType> <port> [-
    CustomServerID <string>]
```

Ejemplo:

```
1 - add service src1 s1 QUIC_BRIDGE 443 -CUSTOMSERVERID C0A8026401BB
2
3 - add service src2 s2 QUIC_BRIDGE 443 -CUSTOMSERVERID C0A802C801BB
```

> **Nota**
>
> Los parámetros `CustomServerID` configurados en el ejemplo anterior son la cadena hexadecimal de una IP correspondiente y el PORT del servidor (s1 y s2). Para la función puente QUIC, Citrix recomienda configurar el parámetro `CustomServerID` solo en formato de cadena hexadecimal.

Agregar un servidor virtual de equilibrio de carga de tipo puente QUIC

Debe agregar un servidor virtual de equilibrio de carga de tipo puente QUIC.

En el símbolo del sistema, escriba:

```
1 add lb vserver <name> [<IPAddress>@ <port> [-persistenceType <
    persistenceType >] [-lbMethod < lbMethod > [-cltTimeout <secs>] [-
    quickBridgeProfilename <name>]
```

Ejemplo:

```
1 add lb vserver quic_bridge_vip QUIC_BRIDGE 192.0.2.10 443 -
    persistenceType CUSTOMSERVERID -lbMethod TOKEN -cltTimeout 120 -
    quicBridgeProfilename q1
```


> **Nota**
>
> Al configurar el servidor virtual puente QUIC, debe configurar un parámetro `persistenceType` como `CUSTOMSERVERID` y un parámetro "LbMethod" como `TOKEN`.

Vincular el servicio puente QUIC al servidor virtual de equilibrio de carga de tipo puente QUIC

Debe vincular el servicio puente QUIC al servidor virtual de equilibrio de carga de tipo puente QUIC.

En el símbolo del sistema, escriba:

```
1 - bind lb vserver <name> (<serviceName>)
2
3 - bind lb vserver <name> (<serviceName>)
```

Ejemplo:

```
1 - bind lb vserver quic_bridge_vip src1
2
3 - bind lb vserver quic_bridge_vip src2
```

Configurar puente QUIC para grupos de servicios

También puede configurar las capacidades de puente QUIC para grupos de servicios. Los siguientes pasos le guían para configurar el puente QUIC para grupos de servicios.

Para configurar el puente QUIC para grupos de servicios, debe completar lo siguiente:

Agregar perfil de puente QUIC

En el símbolo del sistema, escriba:

```
1 add quicBridge profile <name> -routingAlgorithm <PLAINTEXT> -
      serveridlen <value>
```

Ejemplo:

```
1 add quicBridge profile q1 -routingAlgorithm PLAINTEXT -serveridlen 6
```


Agregar servidor de tipo QUIC

En el símbolo del sistema, escriba:

```
1 - add server <name> (<IPAddress>)
2 - add server <name> (<IPAddress>)
```

Ejemplo:

```
1 - add server s1 192.0.2.20
2 - add server s2 192.0.2.30
```

Agregar grupo de servicios puente QUIC

En el símbolo del sistema, escriba:

```
1 add serviceGroup <serviceGroupName> (<IP> | <serverName>) <serviceType>
```

Ejemplo:

```
1 add serviceGroup svg1 QUIC_BRIDGE
```

Vincular los servidores QUIC al grupo de servicios

En el símbolo del sistema, escriba:

```
1 - bind serviceGroup <serviceGroupName> (<IP>@ | (<serverName>) [-
    CustomServerID <string>]
2 - bind serviceGroup <serviceGroupName> (<IP>@ | (<serverName>) [-
    CustomServerID <string>]
```

Ejemplo:

```
1 - bind serviceGroup svg1 s1 443 -customServerID C0A8026401BB
2 - bind serviceGroup svg1 s2 443 -customServerID C0A802C801BB
```


Agregar servidor virtual de equilibrio de carga de tipo puente QUIC

En el símbolo del sistema, escriba:

```
add lb vserver <name> [<IPAddress>@ <port> [-persistenceType <
    persistenceType >] [-lbMethod < lbMethod > [-cltTimeout <secs>] [-
    quickBridgeProfilename <name>]
```

Ejemplo:

```
add lb vserver quic_bridge_vip QUIC_BRIDGE 192.0.2.10 443 -
    persistenceType CUSTOMSERVERID -lbMethod TOKEN -cltTimeout 120 -
    quicBridgeProfilename q1
```

Vincular el servidor virtual de equilibrio de carga de tipo QUIC bridge al grupo de servicios

En el símbolo del sistema, escriba:

```
bind lb vserver <name>@ (<serviceName>@ <serviceGroupName>
```

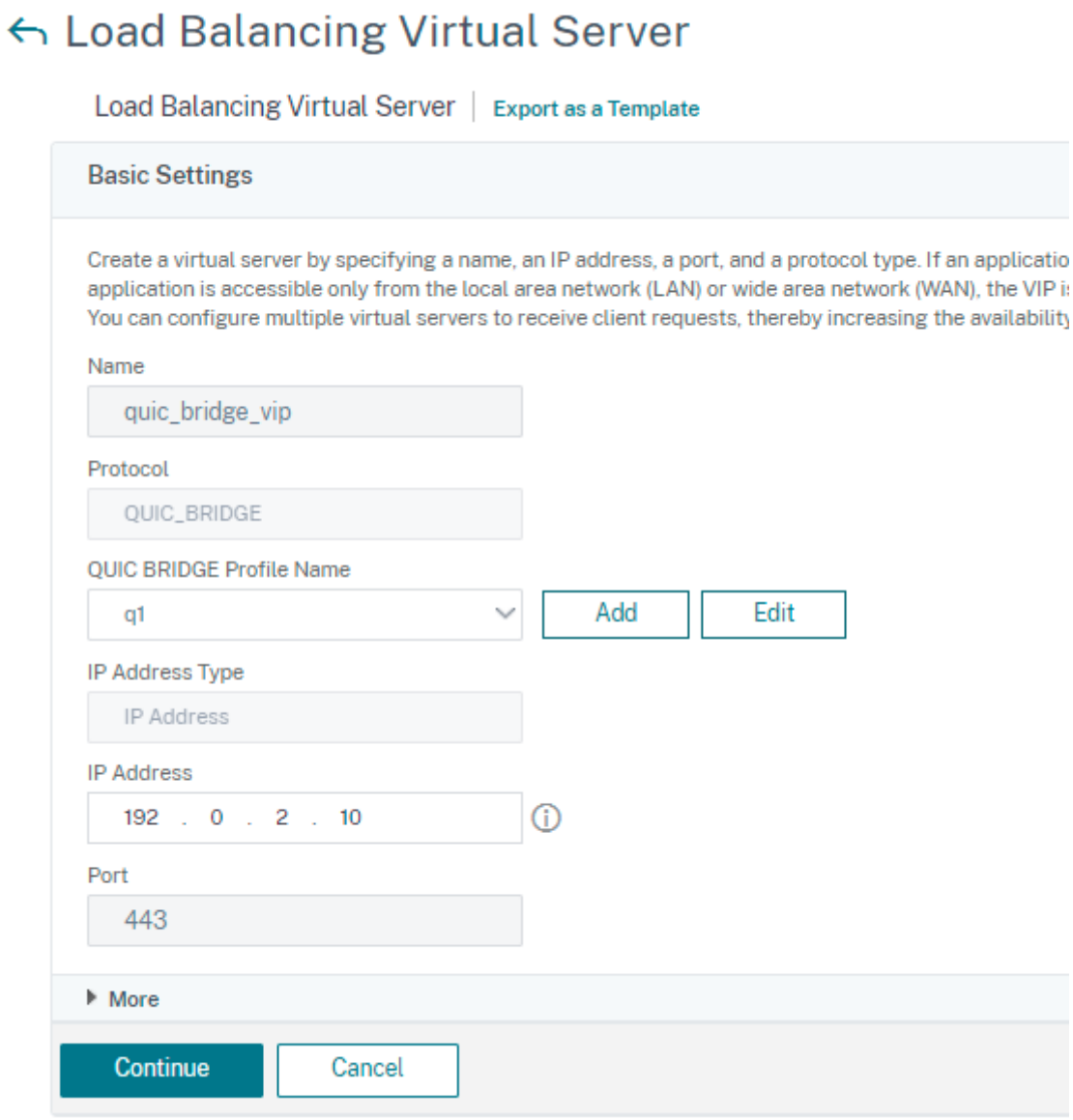
Ejemplo:

```
bind lb vserver quic_bridge_vip svg1
```

Configurar puente QUIC mediante la GUI

Siga los siguientes pasos para configurar el puente QUIC mediante la GUI.

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. En la página **Servidores virtuales**, haga clic en **Agregar**.
3. En la página **Servidor virtual de equilibrio de carga**, seleccione el Protocolo como QUIC_BRIDGE e introduzca los detalles. Haga clic en **OK**.

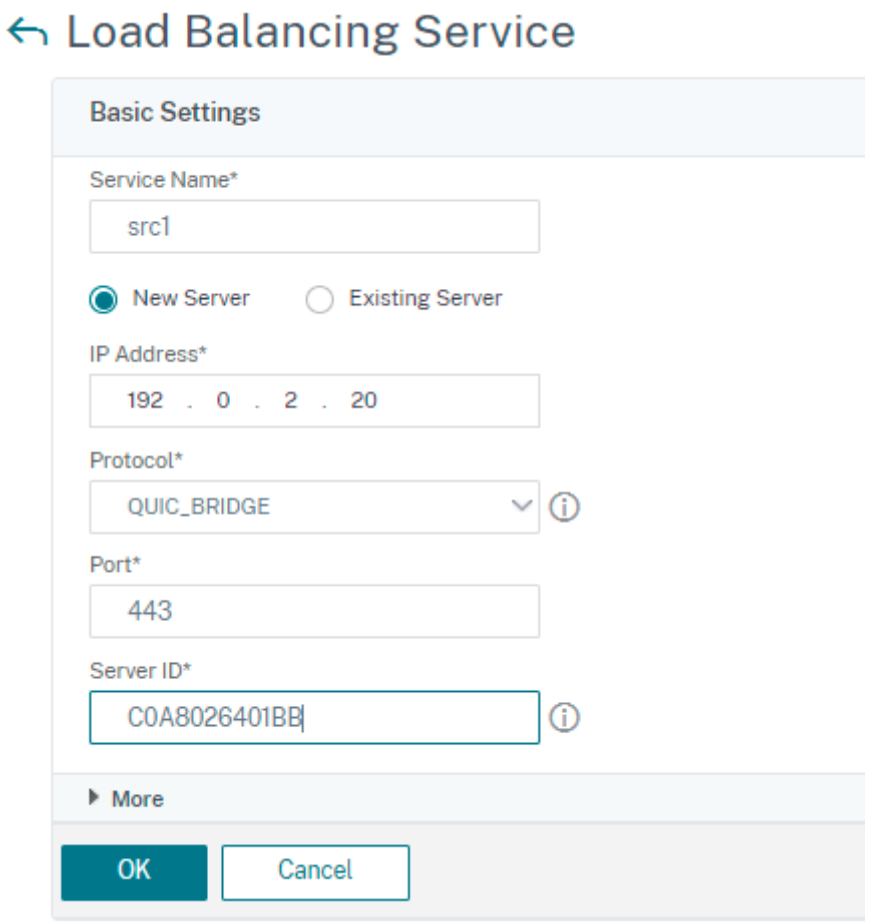


4. En la página **Servidor virtual de equilibrio de carga**, haga clic en **Continuar** y **Listo**.

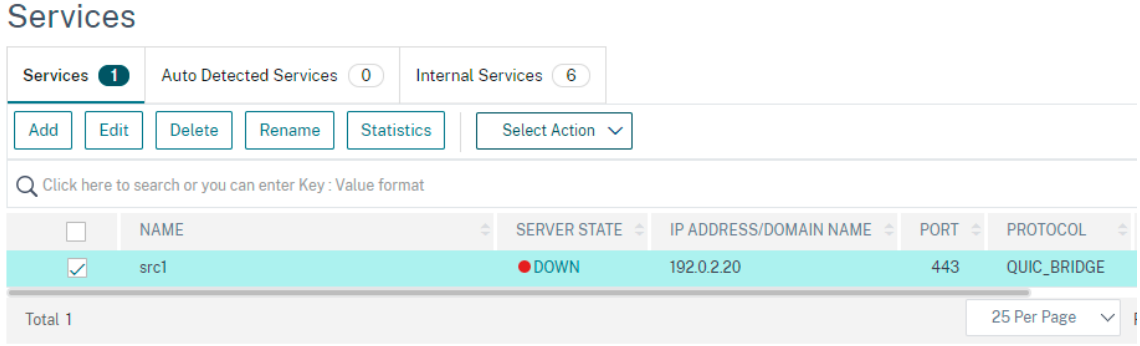
Configurar el equilibrio de carga de los servicios mediante la GUI

Complete los siguientes pasos para configurar el equilibrio de carga de los servicios mediante la GUI.

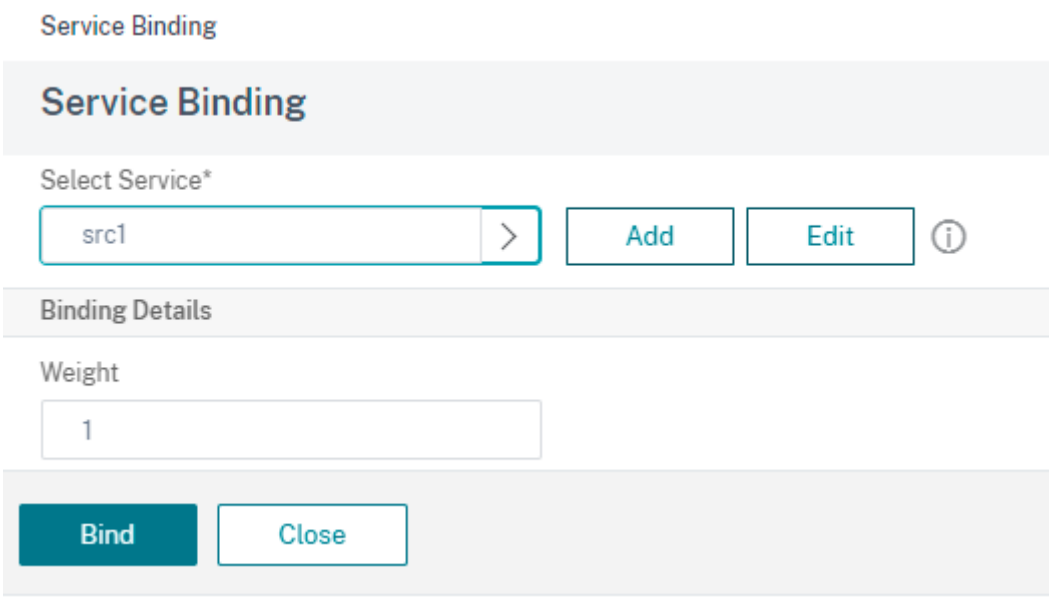
1. Vaya a **Traffic Management -> Load Balancing -> Services**. En la página **Servicios**, haga clic en **Agregar**.
2. En la página **Servicio de equilibrio de carga**, introduzca los detalles y haga clic en **Aceptar**.



3. En la página **Servidores virtuales**, seleccione el servidor virtual creado para enlazar el servicio.
4. Vaya hacia abajo en la página **Servidor virtual de equilibrio de carga** y seleccione **Servicios y grupos de servicios**.
5. En la pantalla **Enlace de servicios**, haga clic en **el campo Seleccionar servicio**.
6. En la pantalla **Servicio**, seleccione el servicio que quiere enlazar al servidor virtual de equilibrio de carga y haga clic en **Seleccionar**.



7. Se selecciona el servicio src1 y, en la pantalla **Enlace de servicios**, haga clic en **Enlazar**.



8. En la página **Servidor virtual de equilibrio de carga**, haga clic en **Listo**.

Ver las estadísticas de QUIC bridge

El puente QUIC admite el comando statistics para ver un resumen detallado de las estadísticas del puente QUIC.

Los siguientes comandos muestran un resumen detallado de las estadísticas del puente QUIC. En el símbolo del sistema, escriba lo siguiente:

- `stat quicbridge`
- `stat quicbridge -detail`

Para borrar la visualización de estadísticas, escriba una de las siguientes opciones:

- `stat quicbridge -clearstats basic`
- `stat quicbridge -clearstats full`

Ver las estadísticas del puente QUIC mediante la interfaz gráfica de usuario

Complete los siguientes pasos para ver las estadísticas del puente QUIC.

1. En la ficha **Panel** de control, desplace el ratón hasta la sección **Descripción general del sistema** .
2. Haga clic en **Descripción general del sistema** y seleccione QUIC BRIDGE en la lista desplegable.

Protocolo proxy

June 2, 2022

El protocolo proxy transporta de forma segura los detalles del cliente al servidor en todos los dispositivos Citrix ADC. El dispositivo agrega un encabezado de protocolo proxy con los detalles del cliente y lo reenvía al servidor back-end. A continuación se presentan algunos de los casos de uso del protocolo proxy en un dispositivo Citrix ADC.

- Aprendizaje de la dirección IP original del cliente
- Selección de un idioma para un sitio web
- Bloquear lista de direcciones IP seleccionadas
- Registro y recopilación de estadísticas.

A continuación se presentan los tres modos de funcionamiento:

- Insertar. El dispositivo inserta los datos del cliente y los envía al servidor back-end.
- Adelante. El dispositivo reenvía los datos del cliente al servidor back-end.
- Despojado. El dispositivo almacena los detalles del cliente para fines de registro. Además, si el servidor back-end no admite el protocolo proxy, envía los detalles del cliente al servidor mediante la configuración de directiva de reescritura

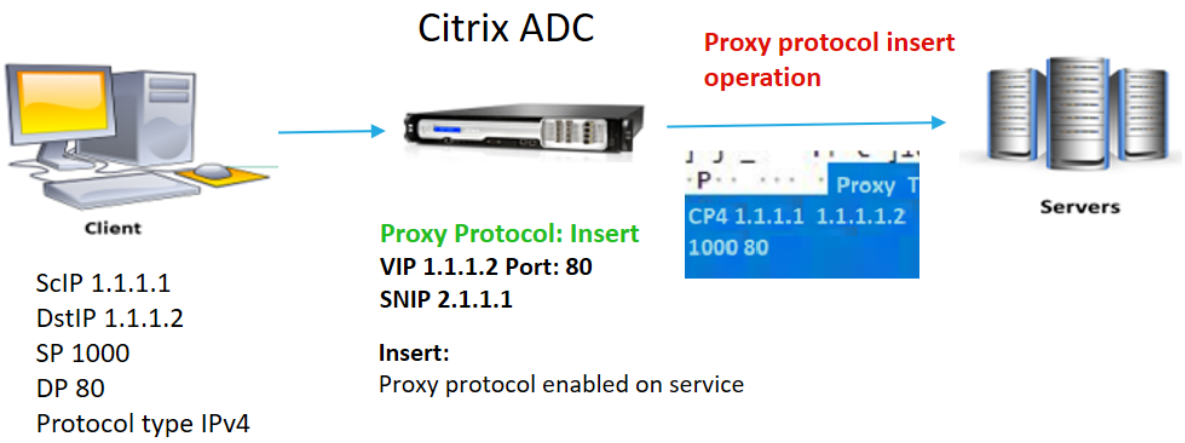
Limitaciones

El protocolo proxy no es compatible con las funciones TCP Fast Open (TFO) y MultiPath TCP. La función solo se admite para los servicios para los que el dispositivo Citrix ADC realiza la terminación de la conexión TCP. No es compatible con otros servicios; por ejemplo, “ANY”.

Cómo funciona el protocolo proxy en un dispositivo Citrix ADC

Los diagramas de flujo siguientes muestran cómo configurar el protocolo proxy en los dispositivos Citrix ADC para las operaciones Insertar, Reenviar y Despojar:

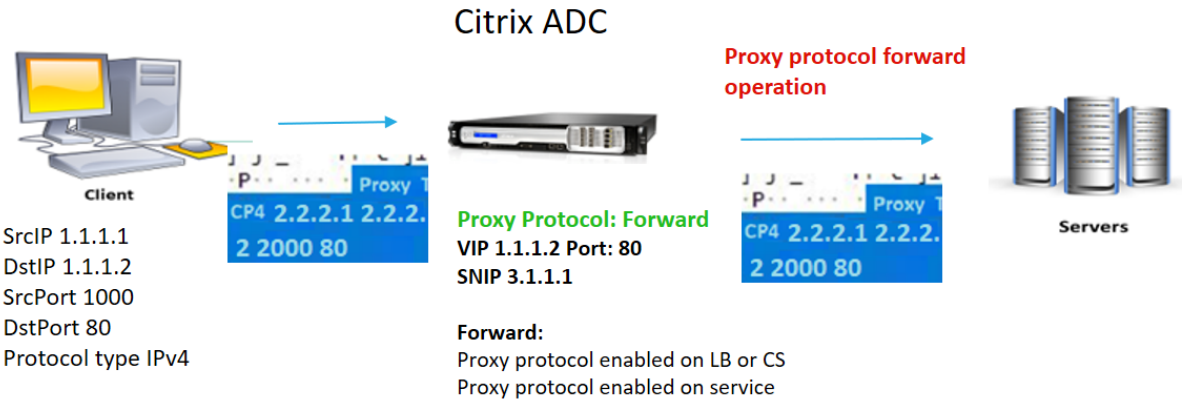
operación de inserción



El componente interact es el siguiente:

- En la instancia de Citrix ADC, debe habilitar el protocolo proxy en el perfil de red y vincularlo al servicio.
- En la operación Insertar, Citrix ADC agrega un encabezado proxy con los detalles de conexión del cliente y lo reenvía al servidor back-end.
- En el lado del envío, el dispositivo decide la versión del protocolo proxy en función de la configuración de la CLI.

Operación de avance



*** The original client details 2.2.2.1, 2.2.2.2, 2000, 80 in the proxy header is forwarded to the back-end server**

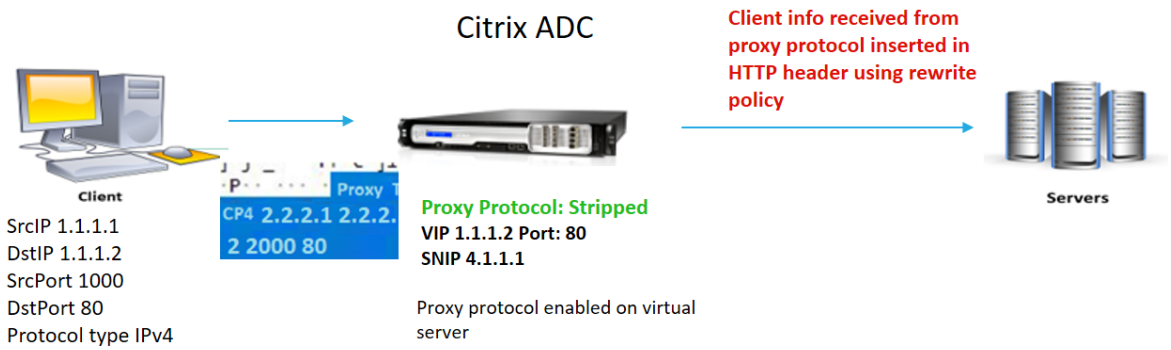
El componente interact es el siguiente:

- Un cliente envía una solicitud junto con el encabezado proxy a Citrix ADC. El dispositivo identi-

fica dinámicamente la versión.

- En el dispositivo Citrix ADC, es una operación de reenvío. El protocolo proxy se habilita en el servidor virtual de equilibrio de carga o en el servidor virtual de conmutación de contenido y se habilita en el servicio. El dispositivo recibe el encabezado proxy y reenvía los detalles del encabezado al servidor back-end.
- Si los detalles del encabezado del proxy no tienen un formato válido, el dispositivo restablece la conexión.
- En el lado del envío, el dispositivo decide la versión del protocolo proxy en función de la configuración de la CLI.

Operación despojada



El componente interact es el siguiente:

- Un cliente envía una solicitud junto con un encabezado proxy al dispositivo Citrix ADC.
- En el dispositivo Citrix ADC, si se trata de una operación de eliminación, el dispositivo reenvía la información del cliente obtenida del protocolo proxy y la inserta en el encabezado HTTP mediante expresiones de directiva de reescritura.
- Los detalles del cliente, como la dirección IP de origen, la dirección IP de destino, el puerto de origen y el puerto de destino, se agregan en un encabezado HTTP mediante expresiones de directiva de reescritura. La directiva de reescritura evalúa la expresión y, si es “true”, se desencadena la acción de directiva de reescritura correspondiente. Y los detalles del cliente se reenvían al servidor back-end en un encabezado HTTP.
- Si los detalles del encabezado del proxy no tienen un formato válido, el dispositivo restablece la conexión.

Formatos de versión de protocolo

La versión del protocolo proxy está disponible en dos formatos. El dispositivo decide utilizar un formato basado en la longitud de los datos entrantes. Para obtener información detallada, consulte RFP

de protocolo proxy.

1. Formato de la versión 1 del protocolo proxy

   ```
   PROXY TCP4/TCP6/UNKNOWN <SRC IP> <DST IP> <SRC PORT> <DST PORT>
   ```

   - PROXY -> Formato de cadena único para encabezado Proxy versión -1.
   - Admite protocolos TCP sobre IPv4 y TCP sobre IPv6. Para los protocolos restantes, esto es DESCONOCIDO.
   - IP de SRC: dirección IP de origen (IP del cliente original) de un paquete.
   - IP de DST: dirección IP de destino de un paquete.
   - Puerto SRC: puerto de origen de un paquete.
   - Puerto DST: puerto de destino de un paquete.

2. Formato de la versión 2 del protocolo proxy

   ```
   0D 0A 0D 0A 00 0D 0A 51 55 49 54 0A <13th byte> <14th byte> <15-16th byte> <17th byte onwards>
   ```

   - D 0A 0D 0A 00 0D 0A 51 55 49 54 0A -> Cadena binaria única para encabezado Proxy versión -2.
   - Admite protocolos TCP sobre IPv4 y TCP sobre IPv6. Para los protocolos restantes, esto es DESCONOCIDO.
   - Decimotercer byte: versión y comando del protocolo.
   - Decimocuarto byte: familia de direcciones y protocolos.
   - 15-16th byte: longitud de la dirección en orden de red.
   - Decimoséptimo byte en adelante: información de direcciones presente en el orden de red: IP src, ip dst, puerto src, puerto dst.

Configurar el protocolo proxy en el dispositivo Citrix ADC

Realice los siguientes pasos para configurar el protocolo Proxy en su dispositivo Citrix ADC.

1. Habilite el protocolo proxy como global.
2. Configurar el protocolo proxy para la operación Insertar
3. Configurar el protocolo proxy para la operación Forward
4. Configurar el protocolo proxy para la operación Strip
5. Configurar el protocolo proxy sin ninguna operación

Habilitar el protocolo proxy como global

En el símbolo del sistema, escriba lo siguiente:

```
set ns param -proxyProtocol ENABLED
```


Configurar el protocolo proxy para la operación Insertar

Para configurar el protocolo proxy para la operación Insertar, debe habilitar o inhabilitar el protocolo en el servidor virtual de equilibrio de carga y habilitarlo en el servicio.

Agregar perfil de red con el protocolo proxy inhabilitado para el servidor virtual de equilibrio de carga

En el símbolo del sistema, escriba lo siguiente:

```
add netprofile <name> -proxyProtocol ENABLED/DISABLED> -proxyprotocoltxversion
 <V1/V2>
```

Ejemplo:

```
Add netprofile proxyprofile-1 -proxyProtocol ENABLED -proxyprotocoltxversion
 V1
```

> **Nota:**
>
> Si inhabilita el protocolo proxy en el dispositivo, no es necesario establecer el parámetro de versión del protocolo.

Agregar perfil de red con un protocolo proxy habilitado para el servicio

En el símbolo del sistema, escriba lo siguiente:

```
add netprofile <name> -proxyProtocol ENABLED/DISABLED> -proxyprotocoltxversion
 <V1/V2>
```

Ejemplo:

```
add netprofile proxyprofile-2 -proxyProtocol ENABLED -proxyprotocoltxversion
 V1
```

Agregar servidor virtual de equilibrio de carga para el dispositivo Citrix ADC en la capa proxy

En el símbolo del sistema, escriba lo siguiente:

```
add lb vserver <name>@ <serviceType> [(<IPAddress>@ <port>)]
```

Ejemplo:

```
add lb vserver lbvserver-1 http 1.1.1.1 80
```


Agregar servicio HTTP para el dispositivo Citrix ADC en la capa proxy

En el símbolo del sistema, escriba lo siguiente:

```
add service <name>@ (<IP>@ | <serverName>@)<serviceType> <port>
```

Ejemplo:

```
Add service http-service-1 2.2.2.1 http 80
```

Establecer el perfil de red con el servidor virtual de equilibrio de carga en el dispositivo Citrix ADC

En el símbolo del sistema, escriba lo siguiente:

```
set lb vserver <vserver name> -netprofile <name>
```

Ejemplo:

```
set lb vserver lbvserver-1 -netprofile proxyProfile-1
```

Establecer el perfil de red con el servicio HTTP en el dispositivo Citrix ADC

En el símbolo del sistema, escriba lo siguiente:

```
set service <service name> -netprofile <name>
```

Ejemplo:

```
set service http-service-1 -netprofile proxyProfile-1
```

Configurar el protocolo proxy para operaciones de reenvío

Configurar el protocolo proxy para la operación de reenvío de la siguiente instancia de Citrix ADC de la capa de proxy. Debe habilitar o inhabilitar el protocolo y vincularlo al servidor o servicio virtual.

Agregar perfil de red con el protocolo proxy habilitado para el servidor virtual de equilibrio de carga

En el símbolo del sistema, escriba lo siguiente:

```
add netprofile <name> -proxyProtocol ENABLED/DISABLED> -proxyprotocoltxversion
 <V1/V2>
```

Ejemplo:

```
add netprofile proxyprofile-3 -proxyProtocol ENABLED -proxyprotocoltxversion
 V1
```


Agregar perfil de red con el protocolo proxy habilitado para el servicio

En el símbolo del sistema, escriba lo siguiente:

```
add netprofile <name> -proxyProtocol ENABLED/DISABLED> -proxyprotocoltxversion
 <V1/V2>
```

Ejemplo:

```
add netprofile proxyprofile-4 -proxyProtocol ENABLED -proxyprotocoltxversion
 V1
```

Agregar servidor virtual de equilibrio de carga para el dispositivo Citrix ADC en la capa proxy

En el símbolo del sistema, escriba lo siguiente:

```
add lb vserver <name>@ <serviceType> [(<IPAddress>@ <port>)]
```

Ejemplo:

```
add lb vserver lbvserver-2 http 2.2.2.2 80
```

Agregar servicio HTTP para el dispositivo Citrix ADC en la capa proxy

En el símbolo del sistema, escriba lo siguiente:

```
add service <name>@ (<IP>@ | <serverName>@)<serviceType> <port>
```

Ejemplo:

```
Add service http-service-2 3.3.3.1 http 80
```

Establecer el perfil de red con el servidor virtual de equilibrio de carga en el dispositivo Citrix ADC

En el símbolo del sistema, escriba lo siguiente:

```
set lb vserver <vserver name> -netprofile <name>
```

Ejemplo:

```
set lb vserver lbvserver-2 -netprofile proxyProfile-3
```

Establecer el perfil de red con el servicio HTTP en el dispositivo Citrix ADC

En el símbolo del sistema, escriba lo siguiente:

```
set service <service name> -netprofile <name>
```

Ejemplo:

```
set service http-service-2 -netprofile proxyProfile-4
```


Configurar el protocolo proxy para la operación strip

Para configurar el protocolo proxy para la operación strip, debe habilitar el protocolo proxy en el servidor virtual de equilibrio de carga y inhabilitar el protocolo proxy en el servicio.

Agregar perfil de red con el protocolo proxy habilitado para el servidor virtual

En el símbolo del sistema, escriba lo siguiente:

```
add netprofile <name> -proxyProtocol ENABLED> -proxyprotocoltxversion <V1/
V2>
```

Ejemplo:

```
add netprofile proxyprofile-5 -proxyProtocol ENABLED -proxyprotocoltxversion
 V1
```

Agregar un servidor virtual de equilibrio de carga o conmutación de contenido para el dispositivo Citrix ADC en la capa proxy

En el símbolo del sistema, escriba lo siguiente:

```
add lb vserver <name>@ <serviceType> [(<IPAddress>@ <port>)]
```

Ejemplo:

```
add lb vserver lbvserver-3 http 2.2.2.2 80
```

Agregar servicio HTTP para el dispositivo Citrix ADC en la capa proxy

En el símbolo del sistema, escriba lo siguiente:

```
add service <name>@ (<IP>@ | <serverName>@)<serviceType> <port>
```

Ejemplo:

```
Add service http-service-3 3.3.3.1 http 80
```

Establecer el perfil de red con el servidor virtual de equilibrio de carga o conmutación de contenido en el dispositivo Citrix ADC

En el símbolo del sistema, escriba lo siguiente:

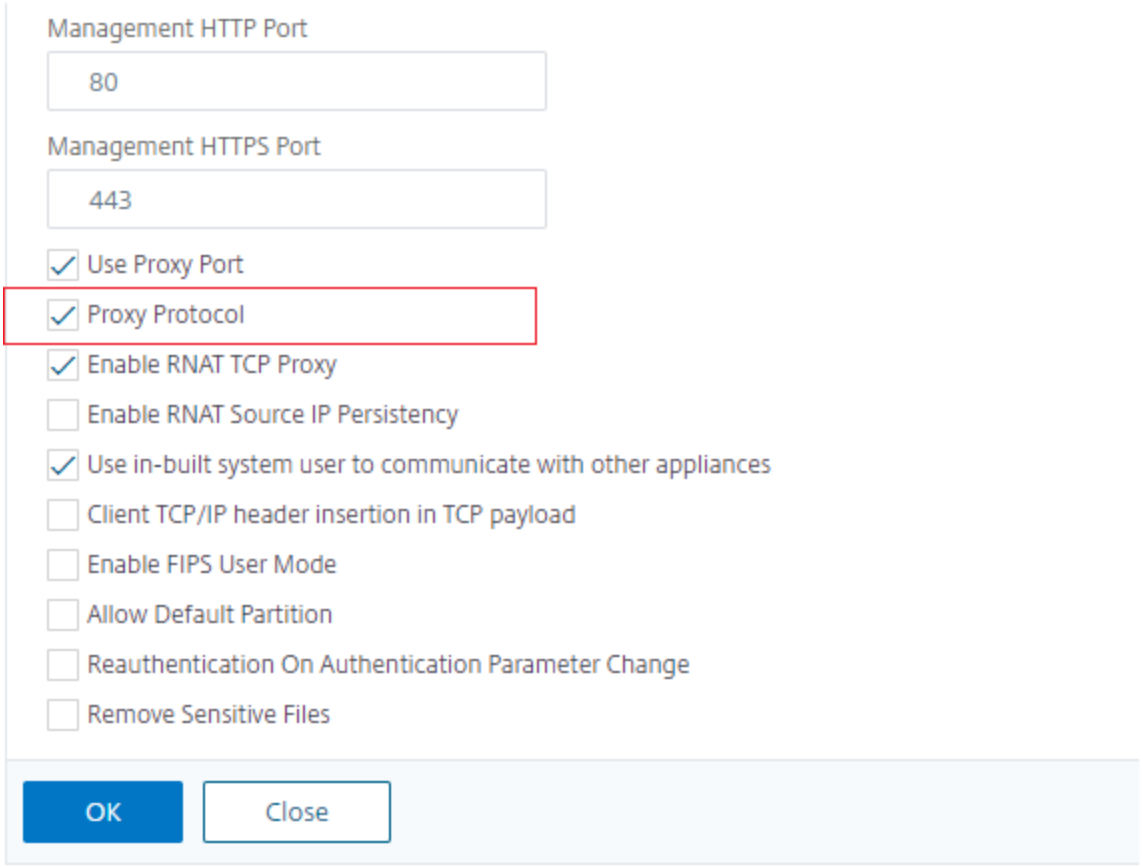
```
set lb vserver <vserver name> -netprofile <name>
```

Ejemplo:

```
set lb vserver lbvserver-3 -netprofile proxyProfile-5
```

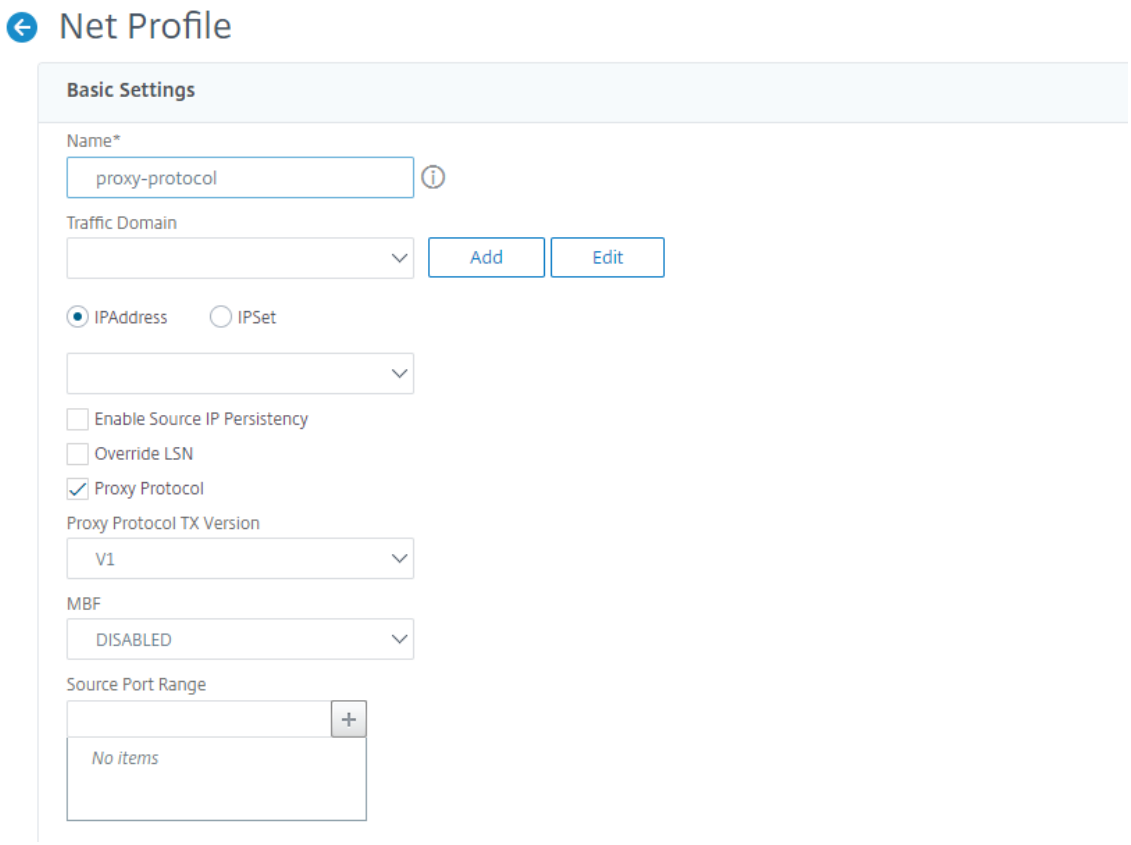

Configurar el protocolo proxy mediante la interfaz gráfica de usuario de Citrix ADC

1. Vaya a **Sistema** > **Configuración** > **Cambiar configuración global del sistema**.
2. En la página **Configurar parámetros de configuración global del sistema**, seleccione la casilla de verificación **Protocolo proxy**.
3. Haga clic en **Aceptar** y **cerrar**.

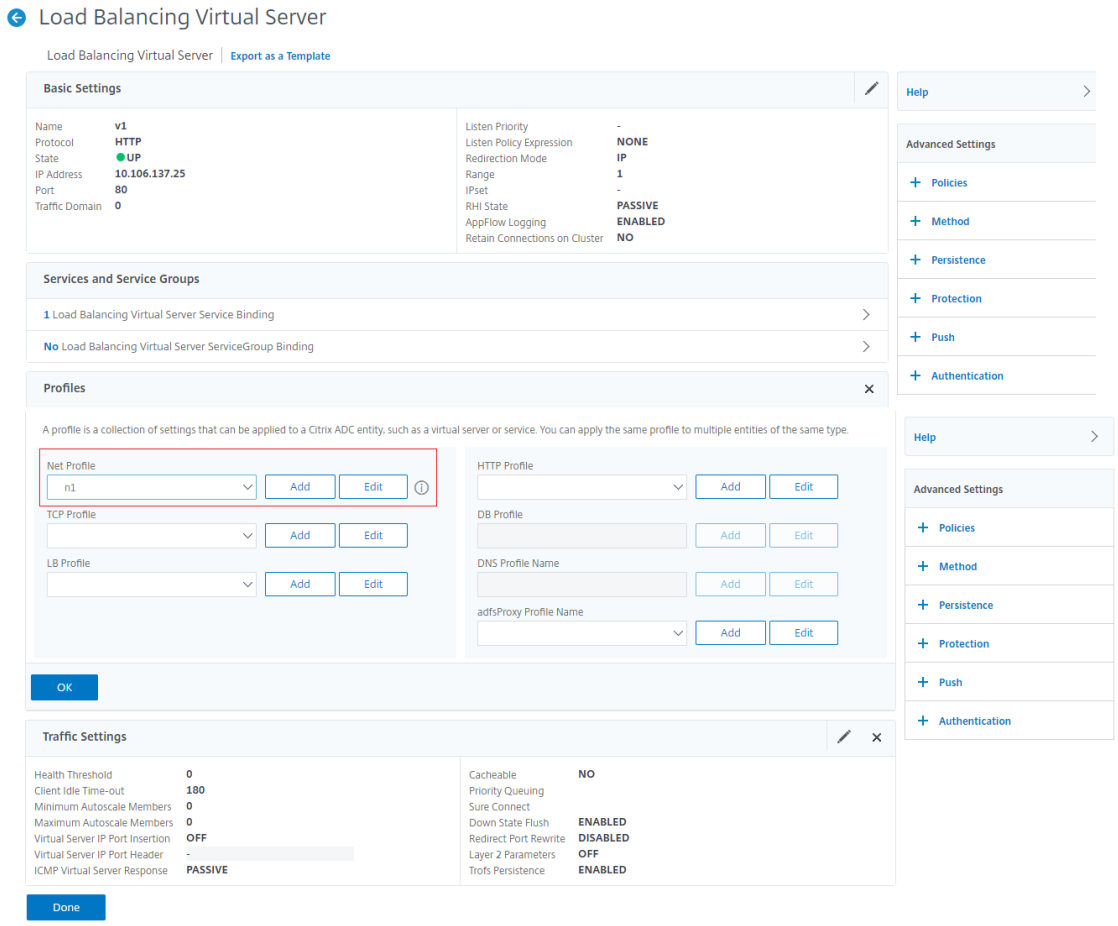


4. Vaya a **Sistema** > **Red** > **Perfiles de red**.
5. En el panel de detalles, haga clic en **Agregar** para crear un perfil de red para el servidor virtual de equilibrio de carga.
6. En la página **Perfil de red**, defina los siguientes parámetros:
   a) Nombre. Nombre del perfil de red.
   b) Protocolo proxy. Habilite o inhabilite el protocolo proxy para el servidor virtual de equilibrio de carga.
   c) Versión TX del protocolo proxy. Establezca la versión del protocolo proxy como V1 o V2 según el formato de datos entrantes.

7. Haga clic en **Aceptar**.

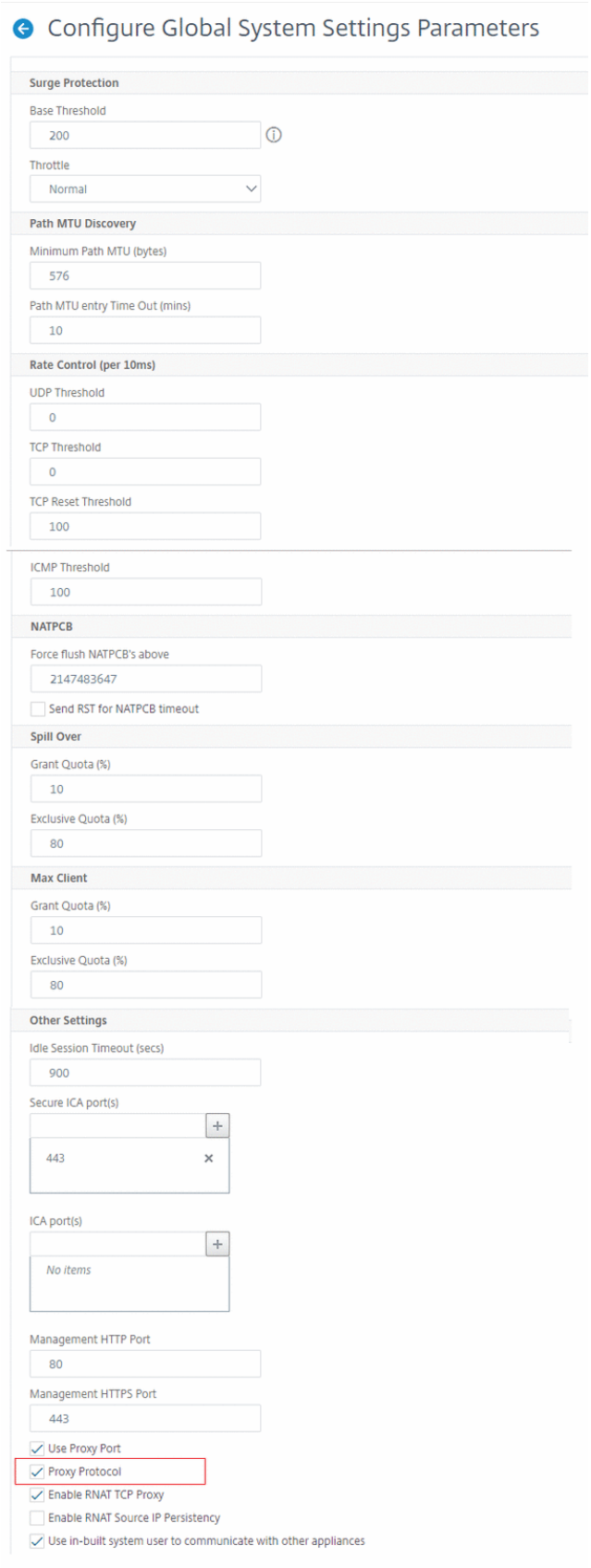


8. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**.
9. En el panel de detalles, haga clic en **Agregar**.
10. En la página **Servidor virtual de equilibrio de carga**, establezca los parámetros básicos.
11. En la sección **Configuración avanzada**, seleccione **Perfiles**.
12. En la sección **Perfiles**, haga clic en el icono del lápiz.
13. Seleccione un perfil de red y haga clic en **Aceptar**.
14. Haga clic en **Listo**.



15. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servicios**.
16. En el panel de detalles, haga clic en **Agregar**.
17. En la página **Servicio de equilibrio de carga**, defina los parámetros básicos.
18. En la sección **Configuración avanzada**, seleccione **Perfiles**.
19. En la sección **Perfiles**, haga clic en el icono del lápiz.
20. Seleccione un perfil de red y haga clic en **Aceptar**.
21. Haga clic en **Listo**.

> **Nota:**
>
> Si tiene más de un dispositivo Citrix ADC como parte de la capa de proxy, debe establecer la configuración del protocolo proxy en cada dispositivo para la operación de reenvío.



Dirección IP del cliente en la opción TCP

April 21, 2022

El dispositivo Citrix ADC utiliza muchas formas de enviar la información del cliente al servidor back-end. Uno de estos métodos consiste en enviar la dirección IP del cliente en la opción TCP. El dispositivo utiliza el número de opción TCP en el perfil TCP, si el servidor back-end utiliza la opción TCP para leer la dirección IP del cliente.

El dispositivo Citrix ADC envía la dirección IP del cliente, en el encabezado de la opción TCP, solo en los siguientes paquetes:

- paquete ACK final del apretón de manos de tres vías
- primer paquete de datos.

A continuación se presentan algunos de los escenarios de uso de la configuración de opciones TCP en un dispositivo Citrix ADC.

- Aprendizaje de la dirección IP original del cliente
- Selección de un idioma para un sitio web
- Bloquear la lista de las direcciones IP seleccionadas

A continuación se presentan los dos modos de operación para enviar la dirección IP del cliente en la opción TCP:

- **Insertar**. En el modo de inserción, el dispositivo agrega los detalles del cliente en el campo de la opción TCP 28 (configurable pero el valor preferible es 28) y los envía al servidor back-end.
- **Adelante**. En el modo de reenvío, el servidor virtual recibe los detalles de IP del cliente en la opción TCP desde un dispositivo proxy. Para el servidor virtual, debe configurar la misma opción TCP, que el dispositivo proxy ha utilizado para enviar los detalles de la IP del cliente.

  A continuación, el dispositivo envía los detalles del cliente en el campo de opción TCP al servidor back-end. Para el servicio que representa el servidor back-end, puede establecer cualquier opción TCP, pero el valor preferible es 28.

El dispositivo Citrix ADC también admite el envío del puerto cliente en la opción TCP para la configuración del modo de inserción.

> **Notas:**
>
> - La multiplexación no se admite para el tráfico recibido en un servidor virtual si la opción TCP IP de cliente está habilitada en el perfil TCP enlazado.
> - Para un servidor virtual TCP o HTTP, el número de opción TCP se reenvía con o sin esta función habilitada en modo transparente.

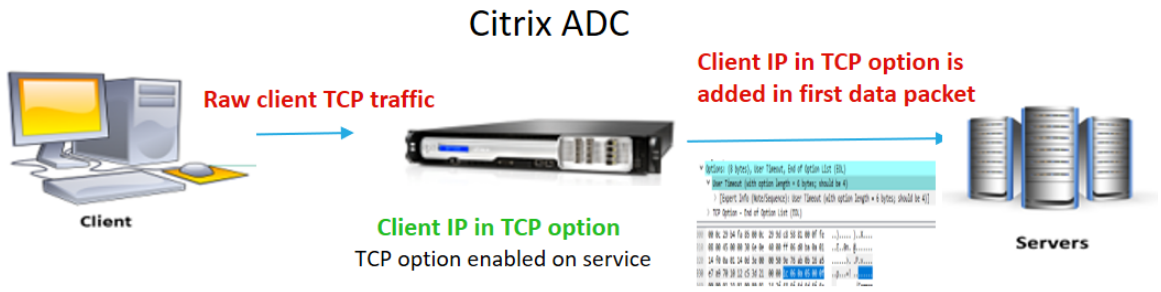
Limitaciones

La función de configuración de opciones TCP no se admite en las funciones TFO, TCP MultiPath y HTTP2.

Cómo configurar las opciones TCP en un dispositivo Citrix ADC

Los siguientes diagramas de flujo muestran cómo puede configurar la opción TCP en los dispositivos Citrix ADC para las operaciones de inserción y reenvío.

Operación de inserción:

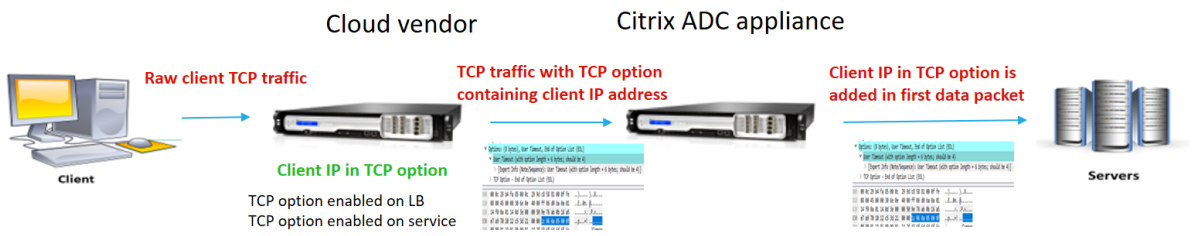


El componente interact es el siguiente:

- Un cliente envía una solicitud a Citrix ADC.
- En la operación Insertar, el dispositivo Citrix ADC inserta la dirección IP y el puerto del cliente en la opción TCP configurada de los siguientes paquetes en el servidor back-end.
  - paquete ACK final del apretón de manos de tres vías
  - primer paquete de datos

> **Nota:**
>
> Si el tráfico entrante es HTTPS, la dirección IP del cliente y el puerto del cliente en la opción TCP se envían en el mensaje de saludo del cliente SSL, que es el primer paquete de datos en el nivel TCP.

Operación hacia adelante:



El componente interact es el siguiente:

- Un cliente envía una solicitud HTTP/HTTPS al dispositivo Citrix ADC.
- Para la operación de reenvío, la opción TCP se habilita en un servidor virtual de equilibrio de carga o en un servidor virtual de conmutación de contenido y también se habilita en el servicio. El dispositivo recibe los detalles del cliente en el número de opción TCP especificado en el servidor virtual.
- A continuación, el dispositivo Citrix ADC inserta la dirección IP y el puerto del cliente en la opción TCP configurada (para el servicio) de los siguientes paquetes en el servidor back-end.
  - paquete ACK final del apretón de manos de tres vías
  - primer paquete de datos

Configurar la opción TCP para la operación Insertar

La configuración de la opción TCP para la operación Insertar consiste en los siguientes pasos:

1. Configure un perfil TCP. Habilite la opción TCP de IP de cliente (`clientIpTcpOption`) y especifique el número de opción TCP (`clientIpTcpOptionNumber`). Si lo quiere, habilite `sendClientPortInTcpOption` para enviar el puerto del cliente en el encabezado de la opción TCP.

   > **Nota:**
   >
   > Citrix recomienda configurar el número de opción TCP como 28 en el perfil TCP.

2. Enlazar el perfil TCP a un servicio

Para configurar un perfil TCP mediante la CLI:

En el símbolo del sistema, escriba:

- `add tcpprofile <name> -clientIpTcpOption (ENABLED | DISABLED)-clientIpTcpOptionNu <positive_integer> -sendClientPortInTcpOption (ENABLED | DISABLED)`
- `show tcpprofile <name>`

Para vincular el perfil TCP al servicio mediante la CLI:

En el símbolo del sistema, escriba:

- `set service <name> -tcpprofileName <name>`
- `show service <name>`

Configuración de ejemplo


```
1 add tcpprofile TCP-PROFILE-1 -clientIpTcpOption ENABLED -
     clientIpTcpOptionNumber 28 -sendClientPortInTcpOption ENABLED
2 set service SERVICE-1  - tcpprofileName TCP-PROFILE-1
3 <!--NeedCopy-->
```

Configurar la opción TCP para la operación de reenvío

La configuración de la opción TCP para la operación de reenvío consiste en los siguientes pasos:

1. Configure un perfil TCP. Habilite la opción TCP de IP de cliente (`clientIpTcpOption`) y especifique el número de opción TCP (`clientIpTcpOptionNumber`).
2. Enlazar el perfil TCP a un servidor virtual de equilibrio de carga o conmutación de contenido
3. Enlaza el perfil TCP a los servicios.

Para configurar un perfil TCP mediante la CLI:

En el símbolo del sistema, escriba:

- `add tcpprofile <name> -clientIpTcpOption (ENABLED | DISABLED)-clientIpTcpOptionNu <positive_integer>`
- `show tcpprofile <name>`

Para vincular el perfil TCP a un servidor virtual de equilibrio de carga o conmutación de contenido mediante la CLI:

En el símbolo del sistema, escriba:

- `set lb vserver <name> -tcpprofileName <name>`
- `show lb vserver <name>`

Para vincular el perfil TCP al servicio mediante la CLI:

En el símbolo del sistema, escriba:

- `set service <name> -tcpprofileName p1`
- `show service <name>`

Configuración de ejemplo

```
1 add tcpprofile TCP-PROFILE-2 -clientIpTcpOption ENABLED -
     clientIpTcpOptionNumber 29
2 set lb vserver LBVS-2  - tcpprofileName TCP-PROFILE-2
3 set service SERVICE-2 -tcpprofileName TCP-PROFILE-2
4 <!--NeedCopy-->
```


Configurar la opción TCP mediante la GUI de Citrix ADC

1. Vaya a **Sistema** > **Perfiles**.
2. En la página de la ficha **Perfil TCP**, haga clic en **Agregar**.
3. En la página **Configurar perfil TCP**, configure los siguientes parámetros:
   - **Opción IPTCP del cliente**. Permite que la opción TCP envíe o reciba la dirección IP del cliente.
   - **número de opción iptcp del cliente**. Establece el número de opción TCP.
   - **SendClientPortInTCPOption** Envía el puerto del cliente en la opción TCP para la configuración del modo de inserción.
4. Haga clic en **Aceptar** y **cerrar**.

SNMP

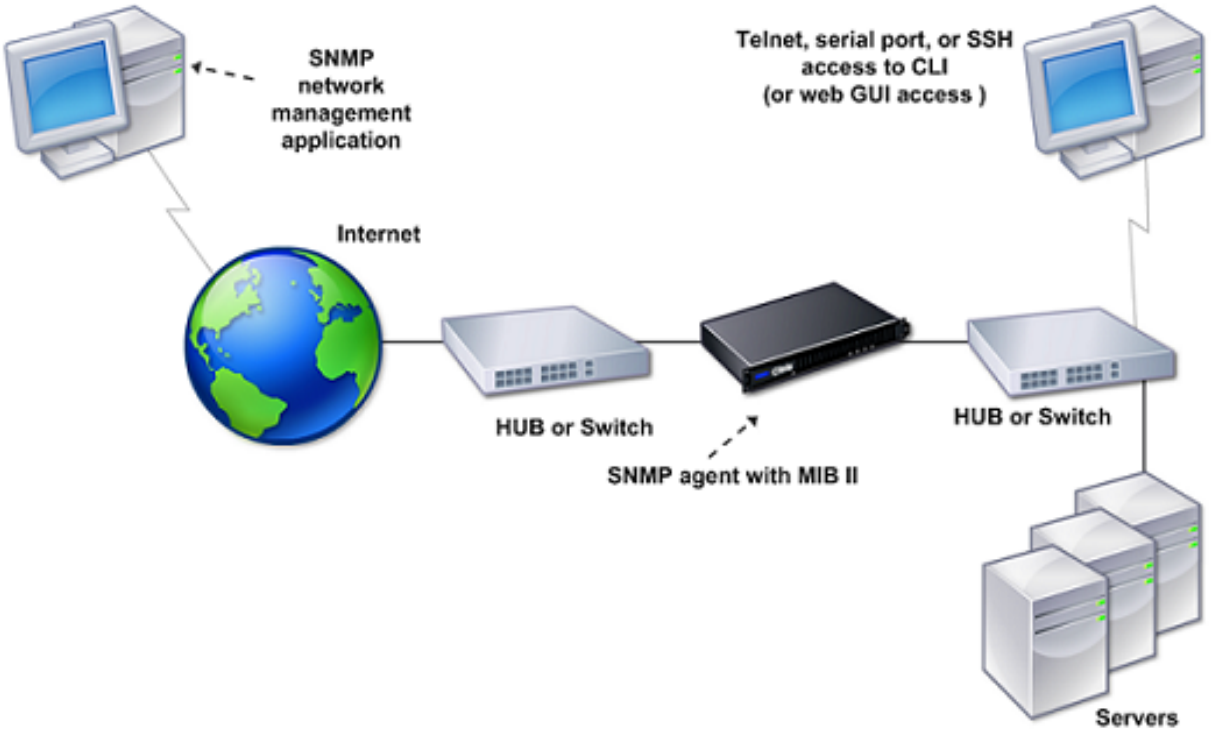
August 20, 2021

Puede utilizar el Protocolo simple de administración de redes (SNMP) para configurar el agente SNMP en el dispositivo Citrix ADC para generar eventos asincrónicos, que se denominan *trampas*. Las trampas se generan siempre que hay condiciones anormales en el Citrix ADC. A continuación, las capturas se envían a un dispositivo remoto denominado *detector de capturas*, que indica la condición anormal en el dispositivo Citrix ADC. O bien, puede consultar al agente SNMP para obtener información específica del sistema desde un dispositivo remoto denominado *administrador SNMP*. A continuación, el agente busca en la base de información de administración (MIB) los datos solicitados y los envía al administrador de SNMP.

El agente SNMP en Citrix ADC puede generar capturas compatibles con SNMPv1, SNMPv2 y SNMPv3. Para realizar consultas, el agente SNMP admite SNMP versión 1 (SNMPv1), SNMP versión 2 (SNMPv2) y SNMP versión 3 (SNMPv3).

Para obtener información sobre los parámetros SNMP, las capturas y sus descripciones, consulte Referencia de OID SNMP de Citrix ADC.

La siguiente ilustración ilustra una red con un dispositivo Citrix ADC que tiene SNMP habilitado y configurado. En la ilustración, cada aplicación de administración de red SNMP utiliza SNMP para comunicarse con el agente SNMP en Citrix ADC. El agente SNMP busca en su base de información de administración (MIB) para recopilar los datos solicitados por SNMP Manager y proporciona la información a la aplicación.



> **Importante**
>
> El módulo SNMP de un dispositivo Citrix ADC admite una longitud máxima de 128 bytes (conforme a RFC 3416) para un OID SNMP. Un nombre de variable de índice largo para un objeto puede dar como resultado un OID SNMP de más de 128 bytes de longitud.
>
> Para resolver este problema, el módulo SNMP de Citrix ADC admite una longitud máxima de 31 caracteres para un nombre de variable de índice. Si el nombre de una variable de índice supera los 31 caracteres de longitud, el módulo SNMP que utiliza un algoritmo hash convierte el nombre en un valor hash de 31 caracteres. Este valor hash se utiliza en el OID SNMP para esa variable.
>
> El nombre de la variable de índice original se almacena en otra variable, que tiene el siguiente formato de nombre: `<variable type>FullName`. Por ejemplo, cuando el nombre de un servidor virtual de equilibrio de carga tiene más de 31 caracteres, `vserverName` SNMP OID contiene el valor hash y `vsvrFullName` SNMP OID contiene el nombre completo (original) del servidor virtual.
>
> Del mismo modo, para las capturas SNMP, la variable de índice muestra un valor hash valorado. `<variable type>FullName`, que almacena el nombre completo del nombre de la variable de índice original, también forma parte de los mensajes de captura.

Importación de archivos MIB a SNMP Manager y Listener de captura

Para supervisar un dispositivo Citrix ADC, debe descargar los archivos de definición de objetos MIB. El dispositivo Citrix ADC admite las siguientes MIB específicas de la empresa:

- **Subconjunto de grupos MIB-2 estándar**. Proporciona grupos MIB-2 SYSTEM, IF, ICMP, UDP y SNMP.
- **MIB empresarial del sistema**. Proporciona configuración y estadísticas específicas del sistema.

Puede obtener los archivos de definición de objetos MIB desde el directorio /netscaler/snmp o desde la ficha Descargas de la GUI.

Configuración del Citrix ADC para generar capturas SNMP

August 20, 2021

Puede configurar el dispositivo Citrix ADC para generar eventos asincrónicos, que se denominan *trampas*. Las trampas se generan siempre que hay condiciones anormales en el dispositivo. Las trampas se envían a un dispositivo remoto llamado *detector de trampas*. Ayuda a los administradores a supervisar el dispositivo y responder rápidamente a cualquier problema.

El dispositivo Citrix ADC proporciona un conjunto de entidades de condición denominadas *alarmas SNMP*. Cuando se cumple la condición de cualquier alarma SNMP, el dispositivo genera mensajes de captura SNMP que se envían a los detectores de captura configurados. Por ejemplo, cuando se habilita la alarma LOGIN-Failure, se genera un mensaje de captura y se envía al agente de escucha de captura cada vez que se produce un error de inicio de sesión en el dispositivo.

Para configurar el dispositivo Citrix ADC para generar capturas, debe habilitar y configurar alarmas. A continuación, se especifican los detectores de capturas a los que el dispositivo envía los mensajes de captura generados.

Activación de una alarma SNMP

El dispositivo Citrix ADC genera capturas solo para las alarmas SNMP habilitadas. Algunas alarmas están habilitadas de forma predeterminada, pero puede desactivarlas.

Cuando habilita una alarma SNMP, el dispositivo genera los mensajes de captura correspondientes cuando se producen algunos eventos. Algunas alarmas están habilitadas de forma predeterminada.

Para habilitar una alarma SNMP mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para establecer los parámetros y verificar la configuración:

- `enable snmp alarm <trapName>`
- `show snmp alarm <trapName>`

Para habilitar una alarma SNMP mediante la interfaz gráfica de usuario

1. Vaya a **Sistema > SNMP > Alarmas**y seleccione la alarma.
2. Haga clic en **Acciones** y seleccione **Habilitar**.

Configuración de alarmas

El dispositivo Citrix ADC proporciona un conjunto de entidades de condición denominadas *alarmas SNMP*. Cuando se cumple la condición establecida para una alarma SNMP, el dispositivo genera mensajes de capturas SNMP que se envían a los detectores de capturas configurados. Por ejemplo, cuando se habilita la alarma LOGIN-Failure, se genera un mensaje de captura y se envía al agente de escucha de captura cada vez que se produce un error de inicio de sesión en el dispositivo.

Puede asignar una alarma SNMP con un nivel de gravedad. Al hacerlo, se asigna ese nivel de gravedad a los mensajes de captura correspondientes.

A continuación se indican los niveles de gravedad, definidos en el dispositivo, en orden decreciente de gravedad.

- Grave
- Mayor
- Leves
- Advertencia
- Informativo

Por ejemplo, si establece un nivel de gravedad de advertencia para la alarma SNMP denominada LOGIN-FAILURE, los mensajes de captura generados cuando se produce un error de inicio de sesión se asignan con el nivel de gravedad de la advertencia.

> **Nota**
>
> Citrix ADC admite varias alarmas SNMP. Para obtener más información, consulte Alarmas SNMP.

También puede configurar una alarma SNMP para registrar los mensajes de captura correspondientes generados siempre que se cumpla la condición de dicha alarma.

Para configurar una alarma SNMP mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para configurar una alarma SNMP y verificar la configuración:

- `set snmp alarm <trapName> [-thresholdValue <positive_integer> [-normalValue <positive_integer>]] [-time <secs>] [-state ( ENABLED | DISABLED )] [-severity <severity>] [-logging ( ENABLED | DISABLED )]`
- `show snmp alarm <trapName>`

Donde:

ThresholdValue: Valor para el umbral alto. El dispositivo Citrix ADC genera un mensaje de captura SNMP cuando el valor del atributo asociado a la alarma es mayor o igual que el valor de umbral alto especificado.

NormalValue: Valor para el umbral normal. Se genera un mensaje de captura si el valor del atributo respectivo cae o por debajo de este valor después de superar el umbral alto.

Para configurar alarmas SNMP mediante la interfaz gráfica de usuario

Vaya a **Sistema > SNMP > Alarmas**, seleccione una alarma y configure los parámetros de alarma.

Configuración de capturas SNMPv1 o SNMPv2

Después de configurar las alarmas, debe especificar el detector de captura al que el dispositivo envía los mensajes de captura. Además de especificar parámetros como la dirección IP o IPv6 y el puerto de destino del listener de captura, puede especificar el tipo de captura (genérico o específico) y la versión SNMP.

Puede configurar un máximo de 20 detectores de captura para recibir capturas genéricas o específicas.

También puede configurar el dispositivo para que envíe mensajes de captura SNMP con una dirección IP de origen distinta de la dirección IP de Citrix ADC (NSIP o NSIP6) a un detector de captura determinado. Para un agente de escucha de captura que tiene una dirección IPv4, puede establecer la IP de origen en una dirección IP asignada (MIP) o una dirección IP de subred (SNIP) configurada en el dispositivo. Para un detector de capchas que tiene una dirección IPv6, puede configurar la IP de origen en una dirección IPv6 de subred (SNIP6) configurada en el dispositivo.

También puede configurar el dispositivo para que envíe mensajes de captura a un detector de trampa en función de un nivel de gravedad. Por ejemplo, si establece el nivel de gravedad como Menor para un detector de captura, todos los mensajes de captura del nivel de gravedad igual o mayor que Menor (Menor, Mayor y Crítico) se envían al agente de escucha de captura.

Si ha definido una cadena de comunidad para el agente de escucha de captura, también debe especificar una cadena de comunidad para cada captura que se va a enviar al agente de escucha. Un detector de captura para el que se ha definido una cadena de comunidad acepta solo mensajes de captura que incluyan una cadena de comunidad que coincida con la cadena de comunidad definida en el detector de captura. Se descartan otros mensajes de captura.

Para agregar una captura SNMP mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para establecer los parámetros y verificar la configuración:

- `add snmp trap <trapClass> <trapDestination> -version ( V1 | V2 )-destPort <port> -communityName <string> -srcIP <ip_addr> -severity <severity>`
- `show snmp trap`

Ejemplo:

```
> `add snmp trap specific 192.0.2.10 -version V2 -destPort 80 -communityName com1 -severity Major`
<!--NeedCopy-->
```

Para configurar capturas SNMP mediante la interfaz gráfica de usuario

Vaya a **Sistema > SNMP > Capturas**y cree la captura SNMP.

Configuración de capturas SNMPv3

SNMPv3 proporciona funciones de seguridad como autenticación y cifrado mediante el uso de las credenciales de los usuarios SNMP. Un administrador SNMP solo puede recibir mensajes de captura SNMPv3 si su configuración incluye la contraseña asignada al usuario SNMP.

El destino de captura ahora puede recibir mensajes de captura SNMPv1, SNMPv2 y SNMPv3.

Para configurar una captura SNMPv3 mediante la CLI

En el símbolo del sistema, haga lo siguiente:

1. Agregue una captura SNMPv3.

   `add snmp trap <trapClass> <trapDestination> -version ( V1 | V2 | V3) -destPort <port> -communityName <string> -srcIP <ip_addr> -severity <severity>`

   > **Nota**
   >
   > Una vez establecida, la versión de captura SNMP no se puede modificar.

   Ejemplo

   ```
   > add snmp trap specific 192.0.2.10 -version V3 -destPort 80 -communityName com1 -severity Major
   <!--NeedCopy-->
   ```


2. Agregue un usuario SNMP.

   ```
   add snmp user <name> -group <string> [ -authType ( MD5 | SHA ){ -
   authPasswd } [-privType ( DES | AES ){ -privPasswd } ]]
   ```

   Ejemplo

   ```
   1 > add snmp user edocs_user -group edocs_group
   2 <!--NeedCopy-->
   ```

3. Enlace la captura SNMPv3 al usuario SNMP.

```
bind snmp trap <trapClass> <trapDestination> [-version <version>] (-userName
 <string> [-securityLevel <securityLevel>])
```

Ejemplo

```
1     > bind snmp trap specific 192.0.2.10 -version V3 -userName
         edocs_user -securityLevel authPriv
2 <!--NeedCopy-->
```

Para configurar una captura SNMPv3 mediante la interfaz gráfica de usuario

1. Agregue una captura SNMPv3.

   Vaya a **Sistema > SNMP > Capturas**y cree la captura SNMP seleccionando V3 como versión SNMP.

2. Agregue un usuario SNMP.

   Vaya a **Sistema > SNMP > Usuarios** y cree el usuario SNMP.

3. Enlace la captura SNMPv3 al usuario SNMP.

   - Vaya a **Sistema > SNMP > Capturas**y seleccione la captura SNMP versión 3.
   - Seleccione el usuario al que debe enlazarse la captura y defina el nivel de seguridad adecuado.

Registro de capturas SNMP

Un dispositivo Citrix ADC puede registrar mensajes de captura SNMP (para alarmas SNMP en las que la capacidad de registro está habilitada) cuando se habilita la opción de registro de capturas SNMP y se configura al menos un detector de capturas en el dispositivo. Ahora, puede especificar el nivel de registro de auditoría de los mensajes de captura enviados a un servidor de registro externo. El nivel

de registro predeterminado es Informativo. Los valores posibles son Emergency, Alert, Critical, Error, Warning, Debug y Notice.

Por ejemplo, puede establecer el nivel de registro de auditoría en Crítico para un mensaje de captura SNMP generado por un error de inicio de sesión. Esa información está disponible en el servidor NSLOG o SYSLOG para la solución de problemas.

Para habilitar el registro de capturas SNMP y configurar el nivel de registro de capturas mediante la CLI

En el símbolo del sistema, escriba los siguientes comandos para configurar el registro de capturas SNMP y verificar la configuración:

- `set snmp option [-snmpTrapLogging (ENABLED | DISABLED)][-snmpTrapLoggingLevel <snmpTrapLoggingLevel>]`
- `show snmp option`

Para habilitar el registro de capturas SNMP y configurar el nivel de registro de capturas SNMP mediante la interfaz gráfica de usuario

Vaya a **Sistema > SNMP**, haga clic en Cambiar opciones SNMP y establezca los siguientes parámetros:

1. Registro de capturas SNMP: Active esta casilla de verificación para habilitar el registro de capturas SNMP cuando se haya configurado al menos un detector de capturas en el dispositivo.
2. Nivel de registro de capturas SNMP: Seleccione un nivel de registro de auditoría para la captura SNMP. De forma predeterminada, el nivel de auditoría de una captura SNMP se establece en “Informativo. “

Configuración de Citrix ADC para consultas SNMP v1 y v2

August 20, 2021

Puede consultar al agente SNMP de Citrix ADC para obtener información específica del sistema desde un dispositivo remoto denominado *administradores SNMP*. A continuación, el agente busca en la base de información de administración (MIB) los datos solicitados y los envía al administrador de SNMP.

El agente SNMP admite los siguientes tipos de consultas SNMP v1 y v2:

- GET
- GET NEXT
- ALL
- GET BULK

Puede crear cadenas denominadas cadenas de comunidad y asociar cada una de ellas a tipos de consulta. Puede asociar una o más cadenas de comunidad a cada tipo de consulta. Las cadenas de comunidad son contraseñas y se utilizan para autenticar consultas SNMP de administradores SNMP.

Por ejemplo, si asocia dos cadenas de comunidad, como **abc** y **bcd**, al tipo de consulta GET NEXT, el agente SNMP del dispositivo Citrix ADC solo tiene en cuenta los paquetes de consulta GET NEXT SNMP que contienen **abc** o **bcd** como cadena de comunidad.

Especificación de un administrador SNMP

Debe configurar el dispositivo Citrix ADC para permitir que los administradores SNMP apropiados lo consulten. También debe proporcionar al administrador SNMP la información específica de Citrix ADC requerida. Puede agregar hasta un máximo de 100 administradores o redes SNMP.

Para un administrador SNMP IPv4, puede especificar un nombre de host en lugar de la dirección IP del administrador. Si lo hace, debe agregar un servidor de nombres DNS que resuelva el nombre de host del administrador SNMP a su dirección IP. Puede agregar hasta un máximo de cinco administradores SNMP basados en nombres de host.

> **Nota**:
> El dispositivo no admite el uso de nombres de host para administradores SNMP que tienen direcciones IPv6. Debe especificar la dirección IPv6.

Si no configura al menos un administrador SNMP, el dispositivo acepta y responde a las consultas SNMP de todas las direcciones IP de la red. Si configura uno o varios administradores SNMP, el dispositivo acepta y responde a las consultas SNMP solo desde esas direcciones IP específicas.

Si quita un administrador SNMP de la configuración, ese administrador ya no podrá consultar el dispositivo.

Para agregar administradores SNMP especificando direcciones IP mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para establecer los parámetros y verificar la configuración:

- `add snmp manager <IPAddress> ... [-netmask <netmask>]`
- `show snmp manager`

Ejemplo

```
> add snmp manager 10.102.29.10 10.102.29.15 10.102.29.30
```


Para agregar un administrador SNMP especificando su nombre de host mediante la interfaz de línea de comandos

Importante: Si especifica el nombre de host del administrador SNMP en lugar de su dirección IP, debe configurar un servidor de nombres DNS para resolver el nombre de host en la dirección IP del administrador SNMP. Para obtener más información, consulte "Adición de un servidor de nombres. "

En el símbolo del sistema, escriba los siguientes comandos para establecer los parámetros y verificar la configuración:

- `add snmp manager <IPAddress> [-domainResolveRetry ****<integer>]`
- `show snmp manager`

Ejemplo

```
add nameserver 10.103.128.15
add snmp manager engwiki.eng.example.net -domainResolveRetry 10
```

Para agregar un administrador SNMP mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **SNMP** > **Administradores** y cree el administrador SNMP.

   > **Importante**:
   >
   > Si especifica el nombre de host del administrador SNMP en lugar de su dirección IPv4, debe configurar un servidor de nombres DNS para resolver el nombre de host en la dirección IP del administrador SNMP.

> **Nota**:
> El dispositivo no admite nombres de host para administradores SNMP que tienen direcciones IPv6.

Especificación de una comunidad SNMP

Puede crear cadenas denominadas cadenas de comunidad y asociarlas con los siguientes tipos de consulta SNMP en el dispositivo:

- GET
- GET NEXT
- ALL
- GET BULK

Puede asociar una o más cadenas de comunidad a cada tipo de consulta. Por ejemplo, cuando asocia dos cadenas de comunidad, como **abc** y **bcd**, al tipo de consulta GET NEXT, el agente SNMP del

dispositivo solo tiene en cuenta los paquetes de consulta GET NEXT SNMP que contienen **abc** o **bcd** como cadena de comunidad.

Si no asocia ninguna cadena de comunidad a un tipo de consulta, el agente SNMP responderá a todas las consultas SNMP de ese tipo.

Para especificar una comunidad SNMP mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para establecer los parámetros y verificar la configuración:

- `add snmp community <communityName> <permissions>`
- `show snmp community`

Ejemplo

```
> add snmp community com all
```

Para configurar una cadena de comunidad SNMP mediante la interfaz gráfica de usuario

Vaya a **Sistema** > **SNMP** > **Comunidad** y cree la comunidad SNMP.

Configuración de Citrix ADC para consultas SNMPv3

August 20, 2021

Simple Network Management Protocol Version 3 (SNMPv3) se basa en la estructura y arquitectura básicas de SNMPv1 y SNMPv2. Sin embargo, SNMPv3 mejora la arquitectura básica para incorporar capacidades de administración y seguridad, como autenticación, control de acceso, verificación de integridad de datos, verificación de origen de datos, verificación de puntualidad de mensajes y confidencialidad de datos.

Para implementar la seguridad y el control de acceso a nivel de mensajes, SNMPv3 introduce el modelo de seguridad basado en el usuario (USM) y el modelo de control de acceso basado en la vista (VACM).

- **Modelo de seguridad basado en el usuario.** El modelo de seguridad basado en el usuario (USM) proporciona seguridad a nivel de mensajes. Permite configurar usuarios y parámetros de seguridad para el agente SNMP y el administrador SNMP. USM ofrece las siguientes funciones:
  - **Integridad de datos:** Para proteger los mensajes de modificación durante la transmisión a través de la red.

  - **Verificación de origen de datos:** para autenticar al usuario que envió la solicitud de mensaje.
  - **Puntualidad del mensaje:** Para proteger contra retrasos o repeticiones de mensajes.
  - **Confidencialidad de los datos:** Para proteger el contenido de los mensajes de ser divulgado a entidades o personas no autorizadas.
- **Modelo de control de acceso basado en vista.** El modelo de control de acceso basado en vista (VACM) permite configurar derechos de acceso a un subárbol específico de la MIB basándose en varios parámetros, como el nivel de seguridad, el modelo de seguridad, el nombre de usuario y el tipo de vista. Permite configurar agentes para proporcionar diferentes niveles de acceso a la MIB a diferentes administradores.

Citrix ADC admite las siguientes entidades que le permiten implementar las funciones de seguridad de SNMPv3:

- Motores SNMP
- Vistas SNMP
- Grupos SNMP
- Usuarios SNMP

Estas entidades funcionan juntas para implementar las funciones de seguridad de SNMPv3. Las vistas se crean para permitir el acceso a los subárboles de la MIB. A continuación, se crean grupos con el nivel de seguridad requerido y acceso a las vistas definidas. Finalmente, los usuarios se crean y asignan a los grupos.

> **Nota**:
>
> La configuración de vista, grupo y usuario se sincronizan y propagan al nodo secundario en un par de alta disponibilidad (HA). Sin embargo, el ID del motor no se propaga ni sincroniza, ya que es exclusivo de cada dispositivo Citrix ADC.

Para implementar la autenticación de mensajes y el control de acceso, debe hacer lo siguiente:

Configuración del ID del motor

Los motores SNMP son proveedores de servicios que residen en el agente SNMP. Proporcionan servicios como el envío, recepción y autenticación de mensajes. Los motores SNMP se identifican de forma única mediante ID de motor.

El dispositivo Citrix ADC tiene un EngineID único basado en la dirección MAC de una de sus interfaces. No es necesario anular el EngineID. Sin embargo, si quiere cambiar el ID del motor, puede restablecerlo.

Para establecer el ID del motor mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para establecer los parámetros y verificar la configuración:

- `set snmp engineId <engineID>`
- `show snmp engineId`

Ejemplo

```
> set snmp engineId 8000173f0300c095f80c68
```

Para establecer el ID del motor mediante GUI

Vaya a **Sistema** > **SNMP** > **Usuarios**, haga clic en **Configurar ID de motor** y escriba un ID de motor.

Configurar una vista

Las vistas SNMP restringen el acceso del usuario a partes específicas de la MIB. Las vistas SNMP se utilizan para implementar el control de acceso.

Para agregar una vista SNMP mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para establecer los parámetros y verificar la configuración:

- `add snmp view <name> <subtree> -type ( included | excluded )`
- `show snmp view <name>`
- `rm snmp view <name> <subtree>`

Donde:

Name. Nombre de la vista SNMPv3. Puede constar de 1 a 31 caracteres que incluyen letras mayúsculas y minúsculas, números y los caracteres de guión (-), punto (.) libra (#), espacio (), signo (@), igual a (=), dos puntos (:) y guión bajo (_). Debe elegir un nombre que ayude a identificar la vista SNMPv3.

Subárbol. Una rama determinada (subárbol) del árbol MIB que quiere asociar a esta vista SNMPv3. Debe especificar el subárbol como un OID SNMP. Este es un argumento de longitud máxima: 99.

tipo. Incluya o excluya el subárbol, especificado por el parámetro de subárbol, en o desde esta vista. Esta configuración puede resultar útil cuando se ha incluido un árbol secundario, como A, en una vista SNMPv3 y se quiere excluir un árbol secundario específico de A, como B, de la vista SNMPv3. Este es un argumento obligatorio. Valores posibles: Incluidos, excluidos.

Ejemplos

add snmp view snmpv3Test 1.1.1.1 -type included
sh snmp view snmpv3Test
rm snmp view snmpv3Test 1.1.1.1

Para configurar una vista SNMP mediante la interfaz gráfica de usuario

Vaya a **Sistema** > **SNMP** > **Vistas** y cree la vista SNMP.

Configurar un grupo

Los grupos SNMP son agregaciones lógicas de usuarios SNMP. Se utilizan para implementar el control de acceso y para definir los niveles de seguridad. Puede configurar un grupo SNMP para que establezca derechos de acceso para los usuarios asignados a ese grupo, restringiendo así los usuarios a vistas específicas.

Debe configurar un grupo SNMP para establecer derechos de acceso para los usuarios asignados a ese grupo.

Para agregar un grupo SNMP mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para establecer los parámetros y verificar la configuración:

- `add snmp group <name> <securityLevel> -readViewName <string>`
- `show snmp group <name> <securityLevel>`

Donde:

Name. Nombre del grupo SNMPv3. Puede constar de 1 a 31 caracteres que incluyan letras mayúsculas y minúsculas, números y los caracteres de guión (-), punto (.) libra (#), espacio (), signo en (@), igual a (=), dos puntos (:) y guión bajo (_). Debe elegir un nombre que ayude a identificar el grupo SNMPv3.

Nivel de seguridad. Nivel de seguridad necesario para la comunicación entre el dispositivo Citrix ADC y los usuarios SNMPv3 que pertenecen al grupo. Especifique una de las siguientes opciones:

NoAuthNopriv. No requieren autenticación ni cifrado.

AuthNoPriv. Requiere autenticación pero no cifrado.

AuthPriv. Requiere autenticación y cifrado. Nota: Si especifica la autenticación, debe especificar un algoritmo de cifrado al asignar un usuario SNMPv3 al grupo. Si también especifica el cifrado, debe asignar tanto una autenticación como un algoritmo de cifrado para cada miembro del grupo. Este es un argumento obligatorio. Valores posibles: NoAuthNoPriv, AuthNoPriv, AuthPriv.

ReadViewName. Nombre de la vista SNMPv3 configurada que quiere enlazar a este grupo SNMPv3. Un usuario SNMPv3 vinculado a este grupo puede acceder a los subárboles que están enlazados a esta vista SNMPv3 como tipo INCLUIDO, pero no puede acceder a los que son de tipo EXCLUIDO. Si el dispositivo Citrix ADC tiene varias entradas de vista SNMPv3 con el mismo nombre, todas estas entradas están asociadas al grupo SNMPv3. Este es un argumento obligatorio. Longitud máxima: 31

Para configurar un grupo SNMP mediante la interfaz gráfica de usuario

Vaya a **Sistema** > **SNMP** > **Grupos** y cree el grupo SNMP.

Configuración de un usuario

Los usuarios SNMP son los administradores SNMP que los agentes permiten acceder a las MIB. Cada usuario SNMP se asigna a un grupo SNMP.

Debe configurar usuarios en el agente y asignar cada usuario a un grupo.

Para configurar un usuario mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para establecer los parámetros y verificar la configuración:

- `add snmp user <name> -group <string> [-authType ( MD5 | SHA ){ -authPasswd } [-privType ( DES | AES ){ -privPasswd } ]]`
- `show snmp user <name>`

Donde:

AuthType es la opción de autenticación disponible durante la configuración de un usuario. Hay dos tipos de autenticación, como MD5 y SHA.

PrivType es la opción de cifrado disponible durante la configuración de un usuario. Hay dos tipos de cifrado, como DES de tamaño de clave 128 bits y AES de tamaño de clave 128 bits.

Ejemplo

```
1 > add snmp user edocs_user -group edocs_group
2 <!--NeedCopy-->
```

Para configurar un usuario SNMP mediante la interfaz gráfica de usuario

Vaya a **Sistema** > **SNMP** > **Usuarios** y cree el usuario SNMP.

Configuración de alarmas SNMP para limitación de velocidad

August 20, 2021

Los dispositivos Citrix ADC, como Citrix ADC MPX 10500, 12500 y 15500, tienen una tarifa limitada. El rendimiento máximo (Mbps) y los paquetes por segundo (PPS) están determinados por la licencia adquirida para el dispositivo. Para las plataformas de tasa limitada, puede configurar capturas SNMP para enviar notificaciones cuando el rendimiento y PPS se aproximen a sus límites y cuando vuelvan a la normalidad.

El rendimiento y el PPS se supervisan cada siete segundos. Puede configurar capturas con valores de umbral alto y umbral normal, que se expresan como un porcentaje de los límites con licencia. A continuación, el dispositivo genera una captura cuando el rendimiento o PPS supera el umbral alto, y una segunda captura cuando el parámetro supervisado cae al umbral normal. Además de enviar las capturas al dispositivo de destino configurado, Citrix ADC registra los eventos asociados con las capturas en el archivo /var/log/ns.log como EVENT ALERTStarted y EVENT ALERTTED.

Superar el límite de rendimiento puede provocar la pérdida de paquetes. Puede configurar alarmas SNMP para informar sobre la pérdida de paquetes.

Para obtener más información sobre alarmas y capturas SNMP, consulte "Configuración de Citrix ADC para generar capturas SNMP v1 y v2. "

Este documento incluye los siguientes detalles:

- Configuración de una alarma SNMP para rendimiento o PPS
- Configuración de la alarma SNMP para paquetes descartados

Configuración de una alarma SNMP para rendimiento o PPS

Para supervisar tanto en todo como en PPS, debe configurar alarmas separadas y establecer el valor pps umbral en Mbps.

Para configurar una alarma SNMP para la velocidad de rendimiento mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para configurar la alarma SNMP, establecer el valor umbral en Mbps y verificar la configuración:

- `set snmp alarm PF-RL-RATE-THRESHOLD [-thresholdValue <positive_integer> [-normalValue <positive_integer>]] [-state ( **ENABLED** | **DISABLED** )] [-severity <severity>] [-logging ( **ENABLED** | **DISABLED** )]`
- `show snmp alarm PF-RL-RATE-THRESHOLD`

Ejemplo

```
> set snmp alarm PF-RL-RATE-THRESHOLD -thresholdValue 70 -normalValue
   50
<!--NeedCopy-->
```

Para configurar una alarma SNMP para PPS mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para configurar la alarma SNMP para PPS y compruebe la configuración:

- `set snmp alarm PF-RL-PPS-THRESHOLD [-thresholdValue <positive_integer> [-normalValue <positive_integer>]] [-state ( **ENABLED** | **DISABLED** )] [-severity <severity>] [-logging ( **ENABLED** | **DISABLED** )]`
- `show snmp alarm PF-RL-PPS-THRESHOLD`

Ejemplo

```
> set snmp alarm PF-RL-PPS-THRESHOLD -thresholdValue 70 -normalValue 50
<!--NeedCopy-->
```

Para configurar una alarma SNMP para rendimiento o PPS mediante la interfaz gráfica de usuario

1. Desplácese hasta **Sistema** > **SNMP** > **Alarmas** y seleccione **PF-RL-RATE-THRESH** (para velocidad de rendimiento) o **PF-RL-PPS-THRESH** (para paquetes por segundo).
2. Establezca los parámetros de alarma y active la alarma SNMP seleccionada.

Configuración de la alarma SNMP para paquetes descartados

Puede configurar una alarma para los paquetes descartados como resultado de exceder el límite de rendimiento y una alarma para los paquetes descartados como resultado de exceder el límite de PPS.

Para configurar una alarma SNMP para paquetes descartados debido a un rendimiento excesivo, mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:


```
set snmp alarm PF-RL-RATE-PKTS-DROPPED [-state (ENABLED | DISABLED)] [-
severity <severity>] [-logging ( ENABLED | DISABLED )]
```

Para configurar una alarma SNMP para paquetes descartados debido a un PPS excesivo, mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
set snmp alarm PF-RL-PPS-PKTS-DROPPED [-state (ENABLED | DISABLED)] [-
severity <severity>] [-logging ( ENABLED | DISABLED )]
```

Para configurar una alarma SNMP para paquetes descartados mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **SNMP** > **Alarmas** y seleccione **PF-RL-RATE-PKTS-DRAWD** (para paquetes descartados debido a un rendimiento excesivo) o **PF-RL-PPS-PKTS-DROPS** (para paquetes descartados debido a un PPS excesivo).
2. Establezca los parámetros de alarma y active la alarma SNMP seleccionada.

Configuración de SNMP en modo FIPS

August 20, 2021

El modo FIPS requiere Simple Network Management Protocol versión 3 (SNMPv3) con la opción de autenticación y privacidad (AuthPriv). Las versiones 1 y 2 de SNMP utilizan un mecanismo de cadena de comunidad para proporcionar acceso seguro a los datos de administración. La cadena de comunidad se envía como texto claro entre un administrador SNMP y un agente SNMP. Este tipo de comunicación no es segura, lo que permite a los intrusos acceder a la información SNMP en la red.

El protocolo SNMPv3 utiliza el modelo de seguridad basado en usuario (USM) y el modelo de control de acceso basado en vista (VACM) para autenticar y controlar el acceso de administración a los datos de mensajería SNMP. SNMPv3 tiene tres niveles de seguridad: Sin autenticación sin privacidad (NoAuthNoPriv), autenticación y sin privacidad (AuthNoPriv), y autenticación y privacidad (AuthPriv).

Al habilitar el modo FIPS y reiniciar el dispositivo Citrix ADC se eliminan las siguientes configuraciones SNMP del dispositivo:

1. Configuración de la comunidad para los protocolos SNMPv1 y SNMPv2.
2. Grupos SNMPv3 configurados con la opción de nivel de seguridad NoAuthNoPriv o AuthNoPriv.
3. Trampas configuradas para SNMPv1 o SNMPv2 o SNMPv3 con la opción NoAuthNoPriv nivel de seguridad.

Después de reiniciar el dispositivo, configure SNMPv3 con la opción AuthPriv. Para obtener más información sobre la configuración de la opción AuthPriv en SMNP v3, consulte el tema SNMPV3.

> **Nota**:
>
> La activación del modo FIPS y el reinicio del dispositivo bloquea la ejecución de los siguientes comandos de captura y grupo SNMP:

```
1     1.  add snmp community <communityName> <permissions>
2
3     2.  add snmp trap <trapClass> <trapDestination> ... [-version: v1/
          v2]   [-td <positive_integer>] [-destPort <port>] [-
          communityName <string>] [-srcIP <ip_addr|ipv6_addr>] [-severity
          <severity>] [-allPartitions ( ENABLED | DISABLED )]
4
5     3.  add snmp group <name> <securityLevel : noAuthNoPriv/ authNoPriv
           > -readViewName <string>
6
7     4.  bind snmp trap specific <TrapIp>-userName <v3 user name> -
          securityLevel <noAuthNoPriv/ authNoPriv>
8 <!--NeedCopy-->
```

Registro de auditoría

January 12, 2021

> **Importante**
>
> Citrix recomienda actualizar una configuración SYSLOG o NSLOG solo durante el mantenimiento o el tiempo de inactividad. Si actualiza una configuración después de crear una sesión, los cambios no se aplican a los registros de sesión existentes.

La auditoría es un examen metódico o revisión de una condición o situación. La función de registro de auditoría permite registrar los estados de Citrix ADC y la información de estado recopilada por varios módulos. La información de registro puede estar en el kernel y en los demonios de nivel de usuario. Para el registro de auditoría, puede utilizar el protocolo SYSLOG, el protocolo NSLOG nativo o ambos.

SYSLOG es un protocolo estándar para el registro. Tiene dos componentes:

- **Módulo de auditoría SYSLOG.** Se ejecuta en el dispositivo Citrix ADC.
- **Servidor SYSLOG.** Se ejecuta en el sistema operativo (SO) FreeBSD subyacente del dispositivo Citrix ADC o en un sistema remoto.

SYSLOG utiliza un protocolo de datos de usuario (UDP) para la transferencia de datos.

Del mismo modo, el protocolo NSLOG nativo tiene dos componentes:

- **Módulo de auditoría NSLOG.** Se ejecuta en el dispositivo Citrix ADC.
- **Servidor NSLOG.** Se ejecuta en el sistema operativo FreeBSD subyacente del dispositivo Citrix ADC o en un sistema remoto.

NSLOG utiliza TCP para la transferencia de datos.

Cuando ejecuta un servidor SYSLOG o NSLOG, éste se conecta al dispositivo Citrix ADC. A continuación, el dispositivo Citrix ADC comienza a enviar toda la información de registro al servidor SYSLOG o NSLOG. Y el servidor filtra las entradas de registro antes de almacenarlas en un archivo de registro. Un servidor NSLOG o SYSLOG recibe información de registro de más de un dispositivo Citrix ADC. El dispositivo Citrix ADC envía información de registro a más de un servidor SYSLOG o servidor NSLOG.

Si se configuran varios servidores SYSLOG, el dispositivo Citrix ADC envía sus mensajes y eventos SYSLOG a todos los servidores de registro externos configurados. Resulta en el almacenamiento de mensajes redundantes y dificulta la supervisión para los administradores del sistema. Para solucionar este problema, el dispositivo Citrix ADC ofrece algoritmos de equilibrio de carga. El dispositivo puede equilibrar la carga de los mensajes SYSLOG entre los servidores de registro externos para mejorar el mantenimiento y el rendimiento. Los algoritmos de equilibrio de carga soportados incluyen RoundRobin, LeastBandwidth, CustomLoad, LeastPackets y AuditLogHash.

> **Nota**
>
> El dispositivo Citrix ADC puede enviar mensajes de registro de auditoría de hasta 16 KB a un servidor SYSLOG externo.

La información de registro que un servidor SYSLOG o NSLOG recopila de un dispositivo Citrix ADC se almacena en un archivo de registro en forma de mensajes. Por regla general, estos mensajes contienen la siguiente información:

- La dirección IP de un dispositivo Citrix ADC que generó el mensaje de registro.
- Una marca de tiempo
- El tipo de mensaje
- Los niveles de registro predefinidos (Crítico, Error, Aviso, Advertencia, Informativo, Depuración, Alerta y Emergencia)
- La información del mensaje

Para configurar el registro de auditoría, primero debe configurar los módulos de auditoría en el dispositivo Citrix ADC. El dispositivo implica la creación de directivas de auditoría y la especificación de la información del servidor NSLOG o del servidor SYSLOG. A continuación, instale y configure el servidor SYSLOG o NSLOG en el SO FreeBSD subyacente del dispositivo Citrix ADC o en un sistema remoto.

> **Nota**
>
> SYSLOG es un estándar de la industria para registrar mensajes de programas, y varios proveedores proporcionan soporte técnico. La documentación no incluye información de configuración del servidor SYSLOG.

El servidor NSLOG tiene su propio archivo de configuración (auditlog.conf). Puede personalizar el registro en el sistema del servidor NSLOG realizando modificaciones adicionales en el archivo de configuración (auditlog.conf).

Configuración del dispositivo Citrix ADC para el registro de auditoría

January 21, 2022

> **Advertencia:**
>
> Las expresiones de directivas clásicas y su uso están en desuso (se desaconseja su uso, pero aún se admite) a partir de Citrix ADC 12.0 compilación 56.20 y, como alternativa, Citrix recomienda usar directivas avanzadas. Para obtener más información, consulte Directivas avanzadas.

El registro de auditoría muestra la información de estado de los distintos módulos para que un administrador pueda ver el historial de eventos en orden cronológico. Los componentes principales de un marco de auditoría son la “acción de auditoría” y la “directiva de auditoría”. La “acción de auditoría” describe la información de configuración del servidor de auditoría, mientras que la “directiva de auditoría” vincula una entidad vinculante a una “acción de auditoría”. Las directivas de auditoría utilizan el marco “Motor de directivas clásico” (CPE) o el marco de integración de progreso (PI) para vincular la “acción de auditoría” con las “entidades vinculantes globales del sistema”.

Sin embargo, los marcos de directivas difieren entre sí en la vinculación de directivas de registro de auditoría a entidades globales. Anteriormente, el módulo de auditoría solo admitía la expresión clásica, pero ahora admite expresiones de directivas clásicas y avanzadas. Actualmente, la expresión Advanced solo puede enlazar directivas de registro de auditoría a entidades globales del sistema.

> **Nota**
>
> Al enlazar una directiva a entidades globales, debe vincularla a una entidad global del sistema de la misma expresión. Por ejemplo, no se puede enlazar una directiva clásica a una entidad global avanzada ni enlazar una directiva avanzada a una entidad global clásica.
>
> Además, no puede vincular tanto la directiva de registro de auditoría clásica como la directiva de registro de auditoría avanzada a un servidor virtual de equilibrio de carga.

Configuración de directivas de registro de auditoría en una expresión de directiva clásica

La configuración del registro de auditoría en la directiva Classic consiste en los siguientes pasos:

1. **Configuración de una acción de registro de auditoría**. Puede configurar una acción de auditoría para distintos servidores y para distintos niveles de registro. La "acción de auditoría" describe la información de configuración del servidor de auditoría, mientras que la "directiva de auditoría" vincula una entidad vinculante a una "acción de auditoría". De forma predeterminada, SYSLOG y NSLOG utilizan únicamente TCP para transferir información de registro a los servidores de registro. TCP es más fiable que UDP para transferir datos completos. Al utilizar TCP para SYSLOG, puede establecer el límite de búfer en el dispositivo Citrix ADC para almacenar los registros. Después de lo cual los registros se envían al servidor SYSLOG.
2. **Configuración de la directiva de registro de auditoría**. Puede configurar directivas SYSLOG para registrar mensajes en un servidor SYSLOG o directiva NSLOG para registrar mensajes en un servidor NSLOG. Cada directiva incluye una regla que identifica los mensajes que se van a registrar y una acción SYSLOG o NS LOG.
3. **Vinculación de directivas de registro de auditoría a entidades globales**. Debe enlazar globalmente las directivas de registro de auditoría a entidades globales como SYSTEM, VPN, Citrix ADC AAA, etc. Puede hacerlo para habilitar el registro de todos los sucesos del sistema Citrix ADC. Al definir el nivel de prioridad, puede establecer el orden de evaluación del registro del servidor de auditoría. La prioridad 0 es la más alta y se evalúa primero. Cuanto mayor sea el número de prioridad, menor será la prioridad de la evaluación.

Cada uno de estos pasos se explica en las secciones siguientes.

Configuración de la acción audit-log

Para configurar la acción SYSLOG en la infraestructura de directivas avanzadas mediante la interfaz de línea de comandos.

> **Nota**
>
> El dispositivo Citrix ADC permite configurar solo una acción SYSLOG en la dirección IP y el puerto del servidor SYSLOG. El dispositivo no permite configurar varias acciones SYSLOG en la misma dirección IP y puerto del servidor.

Una acción syslog contiene una referencia a un servidor syslog. Especifica qué información se va a registrar y menciona cómo registrar esa información.

En el símbolo del sistema, escriba los siguientes comandos para establecer los parámetros y verificar la configuración:


```
- add audit syslogAction <name> <serverIP> [-serverPort <port>] -
  logLevel <logLevel> [-dateFormat ( MMDDYYYY | DDMMYYYY )] [-
  transport ( TCP | UDP )]`
- show audit syslogAction [<name>]

<!--NeedCopy-->
```

Para configurar la acción NSLOG en la infraestructura de directivas avanzadas mediante la interfaz de línea de comandos

Una acción ns log contiene una referencia a un servidor nslog. Especifica qué información se va a registrar y menciona cómo registrar esa información.

En el símbolo del sistema, escriba los siguientes comandos para establecer los parámetros y verificar la configuración:

```
- add audit nslogAction <name> <serverIP> [-serverPort <port>] -
  logLevel <logLevel> [-dateFormat ( MMDDYYYY | DDMMYYYY )]
- show audit nslogAction [<name>]
<!--NeedCopy-->
```

Configuración de directivas de registro de auditoría

Para configurar directivas de registro de auditoría en la infraestructura de directivas clásica mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
- add audit syslogpolicy <name> <-rule> <action>
- add audit nslogpolicy <name> < rule> <action>rm audit nslogpolicy <
  name>show audit nslogpolicy [<name>]set audit nslogpolicy <name>  [-
  rule <expression>] [-action <name>]
<!--NeedCopy-->
```

Vinculación de directivas syslog de auditoría a syslog global de auditoría

Para enlazar la directiva de registro de auditoría en el marco de directivas clásico mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:


```
bind audit syslogGlobal <policyName> [-globalBindType <globalBindType
unbind audit syslogGlobal <policyName>[-globalBindType <globalBindType>]
```

Configuración de directivas de registro de auditoría mediante expresiones de directivas avanzadas

La configuración del registro de auditoría en la directiva Avanzada consiste en los siguientes pasos:

1. **Configuración de una acción de registro de auditoría**. Puede configurar una acción de auditoría para distintos servidores y para distintos niveles de registro. La "acción de auditoría" describe la información de configuración del servidor de auditoría, mientras que la "directiva de auditoría" vincula una entidad vinculante a una "acción de auditoría". De forma predeterminada, SYSLOG y NSLOG utilizan únicamente TCP para transferir información de registro a los servidores de registro. TCP es más fiable que UDP para transferir datos completos. Al utilizar TCP para SYSLOG, puede establecer el límite de búfer en el dispositivo Citrix ADC para almacenar los registros. Después de lo cual los registros se envían al servidor SYSLOG.
2. **Configuración de la directiva de registro de auditoría**. Puede configurar directivas SYSLOG para registrar mensajes en un servidor SYSLOG o directiva NSLOG para registrar mensajes en un servidor NSLOG. Cada directiva incluye una regla que identifica los mensajes que se van a registrar y una acción SYSLOG o NS LOG.
3. **Vinculación de directivas de registro de auditoría a entidades globales**. Debe enlazar globalmente las directivas de registro de auditoría a la entidad global SYSTEM para habilitar el registro de todos los sucesos del sistema Citrix ADC. Al definir el nivel de prioridad, puede establecer el orden de evaluación del registro del servidor de auditoría. La prioridad 0 es la más alta y se evalúa primero. Cuanto mayor sea el número de prioridad, menor será la prioridad de la evaluación.

> **Nota**
>
> El dispositivo Citrix ADC evalúa todas las directivas vinculadas a true.

Configuración de la acción audit-log

Para configurar la acción syslog en la infraestructura de directivas avanzadas mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para establecer los parámetros y verificar la configuración:

```
1 -  add audit syslogAction <name> <serverIP> [-serverPort <port>] -
     logLevel <logLevel> [-dateFormat ( MMDDYYYY | DDMMYYYY )] [-
     transport ( TCP | UDP )]
```



```
2 -  show audit syslogAction [<name>]
3 <!--NeedCopy-->
```

Para configurar la acción NSLOG en la infraestructura de directivas avanzadas mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para establecer los parámetros y verificar la configuración:

```
1 -  add audit nslogAction <name> <serverIP> [-serverPort <port>] -
     logLevel <logLevel> [-dateFormat ( MMDDYYYY | DDMMYYYY )]
2 -  show audit nslogAction [<name>]
3 <!--NeedCopy-->
```

Configuración de directivas de registro de auditoría

Para agregar una acción de auditoría syslog mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
1     add audit syslogAction <name> (<serverIP> | ((<serverDomainName>[-
         domainResolveRetry <integer>])
2     | -lbVserverName <string>))[-serverPort <port>] -logLevel <logLevel
         >[-dateFormat <dateFormat>]
3      [-logFacility <logFacility>][-tcp ( NONE | ALL )] [-acl ( ENABLED
          | DISABLED )]
4     [-timeZone ( GMT_TIME | LOCAL_TIME )][-userDefinedAuditlog ( YES |
         NO )]
5      [-appflowExport ( ENABLED | DISABLED )] [-lsn ( ENABLED | DISABLED
           )][-alg ( ENABLED | DISABLED )]
6     [-subscriberLog ( ENABLED | DISABLED )][-transport ( TCP | UDP )]
         [-tcpProfileName <string>][-maxLogDataSizeToHold
7 <!--NeedCopy-->
```

Ejemplo

```
1     > add audit syslogaction audit-action1 10.102.1.1 -loglevel
         INFORMATIONAL -dateformat MMDDYYYY
2     > add audit nslogAction nslog-action1 10.102.1.3 -serverport 520 -
         loglevel INFORMATIONAL -dateFormat MMDDYYYY
```



```
    > add audit syslogpolicy syslog-pol1 TRUE audit-action1
    > add audit nslogPolicy nslog-pol1 TRUE nslog-action1
    > bind system global nslog-pol1 -priority 20
<!--NeedCopy-->
```

Para agregar una acción de auditoría nslog mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
    add audit nslogAction <name> (<serverIP> | (<serverDomainName>[-
        domainResolveRetry <integer>])) [-serverPort <port>]       -
        logLevel <logLevel> ... [-dateFormat <dateFormat>][-logFacility
        <logFacility>] [-tcp ( NONE | ALL )][-acl ( ENABLED | DISABLED )
        ] [-timeZone ( GMT_TIME | LOCAL_TIME )][-userDefinedAuditlog (
        YES | NO )][-appflowExport ( ENABLED | DISABLED )] [-lsn (
        ENABLED | DISABLED )][-alg ( ENABLED | DISABLED )] [-
        subscriberLog ( ENABLED | DISABLED )]`
<!--NeedCopy-->
```

Vinculación de directivas de registro de auditoría a entidades globales

Para enlazar la directiva de registro de auditoría de syslog en el marco de directivas avanzado mediante la interfaz de línea de comandos

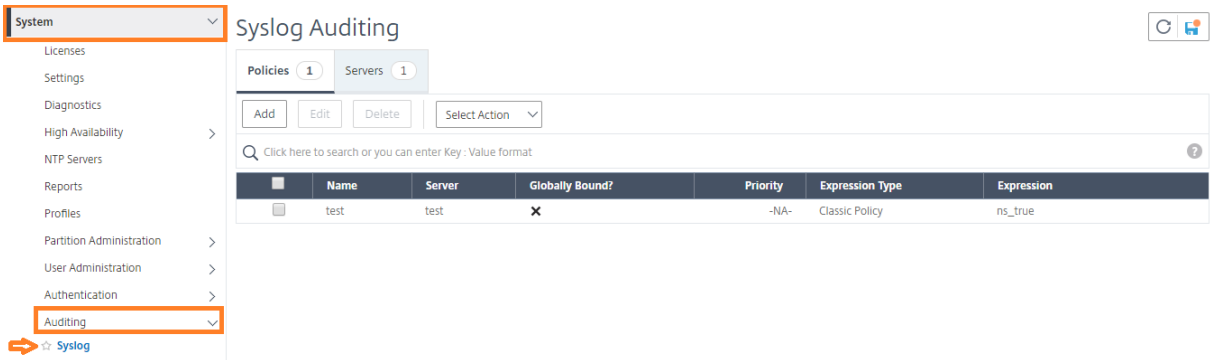
En el símbolo del sistema, escriba:

```
bind audit syslogGlobal <policyName> [-globalBindType <globalBindType
```

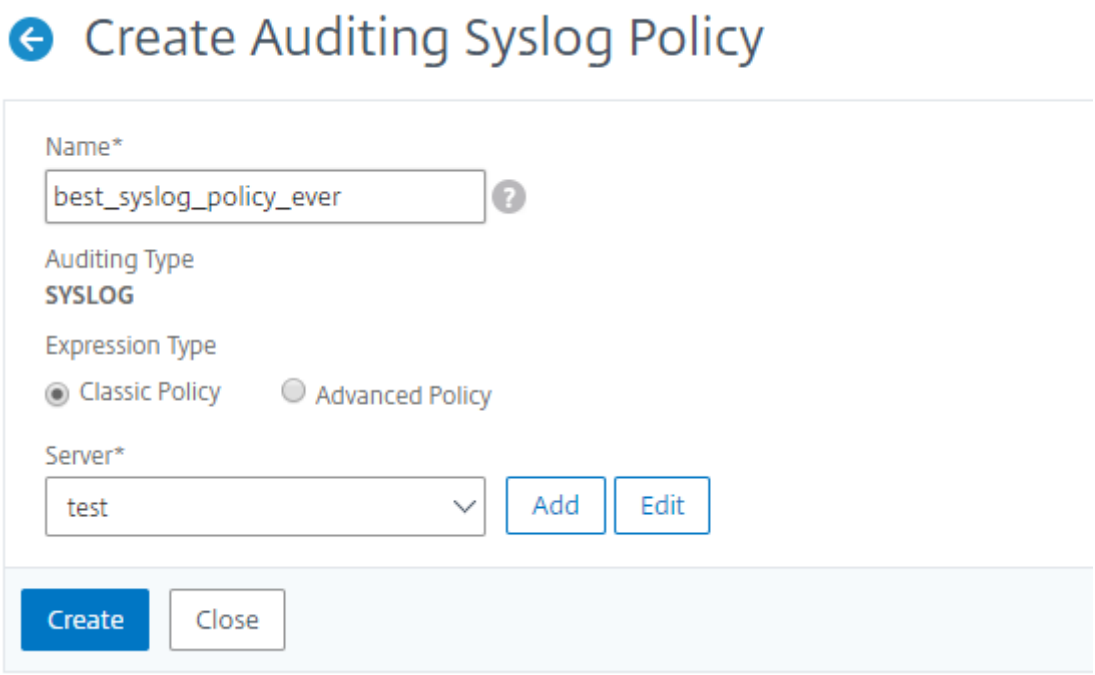
```
unbind audit syslogGlobal <policyName>[-globalBindType <globalBindType>]
```

Configuración de la directiva de registro de auditoría mediante la interfaz gráfica de usuario

1. Vaya a **Configuración** > **Sistema** > **Auditoría** > **Syslog**.



1. Seleccione la ficha **Servidores**.
2. Haga clic en **Agregar**.
3. En la página **Crear servidor de auditoría**, rellene los campos correspondientes y haga clic en **Crear**.
4. Para agregar la directiva, seleccione la ficha **Directivas** y haga clic en **Agregar**.
5. En la página **Crear directiva de syslog de auditoría**, rellene los campos pertinentes y haga clic en **Crear**.



6. Para enlazar la directiva de forma global, seleccione **Enlaces globales de directivas avanzadas** en la lista desplegable. Seleccione la directiva **best_syslog_policy_ever**. Haga clic en **Seleccionar**.
7. En la lista desplegable, seleccione el punto de enlace como **SYSTEM_GLOBAL**, haga clic en **Enlazar**y, a continuación, haga clic en **Listo**.

Configuración del registro basado en directivas

Puede configurar el registro basado en directivas para las directivas de reescritura y respuesta. Los mensajes de auditoría se registran en un formato definido cuando la regla de una directiva se evalúa como TRUE. Para configurar el registro basado en directivas, debe configurar una acción de mensaje de auditoría que utiliza expresiones de directivas avanzadas para especificar el formato de los mensajes de auditoría. Y asocie la acción con una directiva. La directiva se puede enlazar de forma global o a un servidor virtual de equilibrio de carga o conmutación de contenido. Puede utilizar acciones

de mensajes de auditoría para registrar mensajes en varios niveles de registro, ya sea solo en formato syslog o tanto en formato syslog como en formato nslog nuevo

Requisitos previos

- La opción Mensajes de registro configurables por el usuario (UserDefinedAuditLog) está habilitada para configurar el servidor de acciones de auditoría al que quiere enviar los registros en un formato definido.
- La directiva de auditoría relacionada está vinculada al sistema global.

Configuración de una acción de mensaje de auditoría

Puede configurar acciones de mensajes de auditoría para registrar mensajes en varios niveles de registro, ya sea solo en formato syslog o en formatos de registro syslog y ns nuevos. Las acciones de mensajes de auditoría utilizan expresiones para especificar el formato de los mensajes de auditoría.

Para crear una acción de mensaje de auditoría mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
1 add audit messageaction <name> <logLevel> <stringBuilderExpr> [-
     logtoNewnslog (YES|NO)]
2 <!--NeedCopy-->
```

```
1 add audit messageaction log-act1 CRITICAL '"Client:"+CLIENT.IP.SRC+"
     accessed "+HTTP.REQ.URL'
2 <!--NeedCopy-->
```

Para configurar una acción de mensaje de auditoría mediante la interfaz gráfica de usuario

Vaya a **Sistema > Auditoría > Acciones de mensajes**y cree la acción del mensaje de auditoría.

Enlazar acción de mensaje de auditoría a una directiva

Después de crear una acción de mensaje de auditoría, debe vincularla a una directiva de reescritura o respuesta. Para obtener más información sobre cómo vincular acciones de mensajes de registro a una directiva de reescritura o respuesta, consulte Reescritura o Respondedor.

Instalación y configuración del servidor NSLOG

August 20, 2021

Durante la instalación, el archivo ejecutable del servidor NSLOG (auditserver) se instala junto con otros archivos. El archivo ejecutable auditserver incluye opciones para realizar varias acciones en el servidor NSLOG, incluida la ejecución y detención del servidor NSLOG. Además, se utiliza el ejecutable auditserver para configurar el servidor NSLOG con las direcciones IP de los dispositivos Citrix ADC desde los que el servidor NSLOG comenzará a recopilar registros. Los valores de configuración se aplican en el archivo de configuración del servidor NSLOG (auditlog.conf).

A continuación, inicie el servidor NSLOG ejecutando el ejecutable auditserver. La configuración del servidor NSLOG se basa en la configuración del archivo de configuración. Puede personalizar aún más el registro en el sistema del servidor NSLOG realizando modificaciones adicionales en el archivo de configuración del servidor NSLOG (auditlog.conf).

> **Atención**:
>
> La versión del paquete de servidor NSLOG debe ser la misma que la del Citrix ADC. Por ejemplo, si la versión del Citrix ADC es 10.1 Build 125.9, el servidor NSLOG también debe ser de la misma versión.

En la tabla siguiente se enumeran los sistemas operativos en los que se admite el servidor NSLOG.

Sistema operativo	Requisitos de software	Observaciones
Windows	Windows XP Professional, Windows Server 2003, Windows 2000/NT, Windows Server 2008, Windows Server 2008 R2	
Linux	RedHat Linux 4 o posterior, SUSE Linux Enterprise 9.3 o posterior	
FreeBSD	FreeBSD 6.3 o posterior	Para Citrix ADC 10.5, utilice solo FreeBSD 8.4.
Mac OS	Mac OS 8.6 o posterior	No se admite en Citrix ADC 10.1 y versiones posteriores.

Las especificaciones mínimas de hardware para la plataforma que ejecuta el servidor NSLOG son las siguientes:

- Procesador: Intel x86 ~ 501 megahercios (MHz)
- RAM: 512 megabytes (MB)
- Controlador: SCSI

Instalación del servidor NSLOG en el sistema operativo Linux

Inicie sesión en el sistema Linux como administrador. Utilice el procedimiento siguiente para instalar los archivos ejecutables del servidor NSLOG en el sistema.

Para instalar el paquete de servidor NSLOG en un sistema operativo Linux

1. En un símbolo del sistema de Linux, escriba el siguiente comando para copiar el archivo NSAuditServer.rpm en un directorio temporal:

   ```
   cp <path_to_cd>/Utilities/auditserver/Linux/NSauditserver.rpm /tmp
   ```

2. Escriba el siguiente comando para instalar el archivo NSAuditServer.rpm.

   rpm -i NSAuditServer.rpm

   Este comando extrae los archivos y los instala en los directorios siguientes:

   - /usr/local/netscaler/etc
   - /usr/local/netscaler/bin
   - /usr/local/netscaler/samples

Para desinstalar el paquete de servidor NSLOG en un sistema operativo Linux

1. En el símbolo del sistema, escriba el comando siguiente para desinstalar la función de registro del servidor de auditoría:

   ```
   rpm -e NSauditserver
   ```

2. Para obtener más información acerca del archivo RPM NSAuditServer, utilice el siguiente comando:

   ```
   rpm -qpi \*.rpm
   ```

3. Para ver los archivos del servidor de auditoría instalados, utilice el siguiente comando:

   ```
   rpm -qpl *.rpm
   ```

   *.rpm: Especifica el nombre del archivo.

Instalación del servidor NSLOG en el sistema operativo FreeBSD

Antes de poder instalar el servidor NSLOG, debe copiar el paquete NSLOG del CD del producto Citrix ADC o descargarlo desde www.citrix.com. El paquete NSLOG tiene el siguiente formato de nombre:

`AuditServer_<release number>-<build number>.zip`

Por ejemplo: `AuditServer_10.5-58.11.zip`

Este paquete contiene archivos para todas las plataformas compatibles: Linux, Windows y FreeBSD. En un sistema operativo FreeBSD, instale el paquete NSLOG que tiene el siguiente formato de nombre:

`audserver_bsd-<release number>-<build number>.tgz`

Por ejemplo: `audserver_bsd-10.5-58.11.tgz`

Para descargar el paquete NSLOG desde www.citrix.com:

1. En un explorador web, vaya a www.citrix.com.
2. En la barra de menús, haga clic **en Iniciar sesión**.
3. Escriba sus credenciales de inicio de sesión y, a continuación, haga clic **en Iniciar sesión**.
4. En la barra de menús, haga clic en **Descargas**.
5. En la lista **Seleccionar un producto**, seleccione **Citrix ADC**.
6. En la página **Citrix ADC**, seleccione la versión para la que quiere descargar el paquete NSLOG (por ejemplo, versión 10.5) y, a continuación, seleccione **Firmware**.
7. En **Firmware**, seleccione el firmware de Citrix ADC para el número de compilación para el que quiere descargar el paquete NSLOG.
8. En la página que aparece, desplácese hacia abajo, seleccione **Servidores de auditoría** y haga clic en **Descargar archivo**junto al paquete que quiere descargar.

Para instalar el paquete de servidor NSLOG en un sistema operativo FreeBSD

1. En el sistema al que ha descargado el paquete NSLOG`AuditServer_<release number>-<build number>.zip` (por ejemplo, `AuditServer_9.3-51.5.zip`), extraiga el `FreeBSD NSLOG server package audserver_bsd-<release number>-<build number>.tgz` (por ejemplo, `audserver_bsd-9.3-51.5.tgz`) del paquete.
2. Copie el paquete de servidor FreeBSD NSLOG`audserver_bsd-<release number>-<build number>.tgz` (por ejemplo, `audserver_bsd-9.3-51.5.tgz`) a un directorio en un sistema que ejecute FreeBSD OS.
3. En un símbolo del sistema para el directorio en el que se copió el paquete del servidor FreeBSD NSLOG, ejecute el siguiente comando para instalar el paquete:

   `pkg_add audserver_bsd-<release number>-<build number>.tgz`

   Ejemplo:


```
pkg_add audserver_bsd-9.3-51.5.tgz
<!--NeedCopy-->
```

Se extraen los siguientes directorios:

- <root directory extracted from the FreeBSD NSLOG server package tgz file>Citrix ADCbin (por ejemplo, /var/auditserver/netscaler/bin)
- <root directory extracted from the FreeBSD NSLOG server package tgz file>netscaler/etc (por ejemplo, /var/auditserver/netscaler/etc)
- <root directory extracted from the FreeBSD NSLOG server package tgz file>\netscaler\samples (por ejemplo, /var/auditserver/samples)

4. En el símbolo del sistema, escriba el comando siguiente para comprobar que el paquete está instalado:

   ```
   pkg_info | grep NSaudserver
   ```

Para desinstalar el paquete de servidor NSLOG en un sistema operativo FreeBSD

Escriba lo siguiente en una interfaz de comandos:

```
pkg_delete NSaudserver
```

Instalación de archivos de servidor NSLOG en el sistema operativo Windows

Antes de poder instalar el servidor NSLOG, debe copiar el paquete NSLOG del CD del producto Citrix ADC o descargarlo desde www.citrix.com. El paquete NSLOG tiene el siguiente formato de nombre AuditServer _<release number>-<build number>.zip (por ejemplo, AuditServer_9.3-51.5.zip). Este paquete contiene paquetes de instalación de NSLOG para todas las plataformas compatibles.

Para descargar el paquete NSLOG desde www.Citrix.com

1. En un explorador web, vaya a www.citrix.com.
2. En la barra de menús, haga clic en Iniciar sesión.
3. Escriba sus credenciales de inicio de sesión y, a continuación, haga clic en Iniciar sesión.
4. En la barra de menús, haga clic en Descargas.
5. Busque la página que proporciona el número de versión apropiado y la compilación.
6. En esa página, en Servidores de auditoría, haga clic en Descargar para descargar el paquete NSLOG, que tiene el formato AuditServer_<release number>-<build number>.zip, en el sistema local (por ejemplo, AuditServer_9.3-51.5.zip).

Para instalar el servidor NSLOG en un sistema operativo Windows

1. En el sistema, donde ha descargado el paquete NSLOG AuditServer_<release number>-<build number>.zip (por ejemplo, AuditServer_9.3-51.5.zip), extraiga audserver_win-<release number>-<build number>.zip (por ejemplo, audserver_win-9.3-51.5.zip) del paquete.
2. Copie el archivo extraído audserver_<release number>-<build number>.zip (por ejemplo, audserver_win-9.3-51.5.zip) en un sistema Windows en el que instalar el servidor NSLOG.
3. Descomprima el audserver_<release number>-<build number>.zip archivo (por ejemplo, audserver_win-9.3-51.5.zip).
4. Se extraen los siguientes directorios:
   a) <root directory extracted from the Windows NSLOG server **package** zip file>\bin(por ejemplo, C:\audserver_win-9.3-51.5\bin)
   b) <root directory extracted from the Windows NSLOG server **package** zip file>\etc (por ejemplo, C:\audserver_win-9.3-51.5\etc)
   c) <root directory extracted from the Windows NSLOG server **package** zip file>\samples (por ejemplo, C:\audserver_win-9.3-51.5\samples)
5. En un símbolo del sistema, ejecute el siguiente comando desde el menú <root directory extracted from the Windows NSLOG server **package** zip file>\bin path

   ```
   audserver -install -f <directorypath>\auditlog.conf
   ```

   <directorypath>: Especifica la ruta de acceso al archivo de configuración (auditlog.conf). De forma predeterminada, log.conf está en el directorio \<root directory extracted from Windows NSLOG server **package** zip file\>\samples. Pero puede copiar auditlog.conf en el directorio deseado.

Para desinstalar el servidor NSLOG en un sistema operativo Windows

En el símbolo del sistema, ejecute lo siguiente desde la ruta de acceso <root directory extracted from Windows NSLOG server **package** zip file>\bin:

```
audserver -remove
```

Opciones de comandos del servidor NSLOG

Para obtener información sobre los comandos del servidor NSLOG, consulte Opciones del servidor de auditoría.

Ejecute el comando audserver desde el directorio en el que está presente el ejecutable del servidor de auditoría:

- En Windows: \ns\bin
- En Solaris y Linux: \usr\local\netscaler\bin

Los archivos de configuración del servidor de auditoría están presentes en los directorios siguientes:

- En Windows: \ns\etc
- En Linux: \usr\local\netscaler\etc

El ejecutable del servidor de auditoría se inicia como ./auditserver en Linux y FreeBSD.

Adición de las direcciones IP de Citrix ADC Appliance en el servidor NSLOG

En el archivo de configuración (
auditlog.conf), agregue las direcciones IP de los dispositivos Citrix ADC cuyos eventos deben registrarse.

Para agregar las direcciones IP del dispositivo Citrix ADC

En el símbolo del sistema, escriba el siguiente comando:

```
audserver -addns -f <directorypath\>\auditlog.conf
```

<directorypath>: Especifica la ruta al archivo de configuración (auditlog.conf).

Se le pedirá que introduzca la información para los siguientes parámetros:

NSIP: Especifica la dirección IP del dispositivo Citrix ADC, por ejemplo, 10.102.29.1.

ID de usuario: Especifica el nombre de usuario, por ejemplo, nsroot.

Contraseña: Especifica la contraseña, por ejemplo, nsroot.

Si agrega varias direcciones IP de Citrix ADC (NSIP) y, posteriormente, no quiere registrar todos los detalles del evento del dispositivo Citrix ADC, puede eliminar los NSIP manualmente quitando la instrucción NSIP al final del archivo auditlog.conf. Para una configuración de alta disponibilidad (HA), debe agregar direcciones IP de Citrix ADC primarias y secundarias a auditlog.conf mediante el comando audserver. Antes de agregar la dirección IP, asegúrese de que el nombre de usuario y la contraseña existan en el sistema.

Verificación del archivo de configuración del servidor NSLOG

Compruebe la corrección de sintaxis en el fichero de configuración (audit log.conf) para permitir que el registro se inicie y funcione correctamente.

Para verificar la configuración, en el símbolo del sistema, escriba el siguiente comando:

```
audserver -verify -f <directorypath>\auditlog.conf
```


<directorypath>: Specifies the path to the configuration file (audit log.conf).

Ejecución del servidor NSLOG

January 12, 2021

Para iniciar el registro del servidor de auditoría

Escriba el comando siguiente en el símbolo del sistema:

audserver -start -f <directorypath>\auditlog.conf

<directorypath>: Especifica la ruta al archivo de configuración (audit log.conf).

Para detener el registro del servidor de auditoría que se inicia como un proceso en segundo plano en FreeBSD o Linux

Escriba el siguiente comando:

```
audserver -stop
```

Para detener el registro del servidor de auditoría que se inicia como un servicio en Windows

Escriba el siguiente comando:

```
audserver -stopservice
```

Personalizar el registro en el servidor NSLOG

January 12, 2021

Puede personalizar el registro en el servidor NSLOG realizando modificaciones adicionales en el archivo de configuración del servidor NSLOG (log.conf). Utilice un editor de texto para modificar el archivo de configuración log.conf en el sistema del servidor.

Para personalizar el registro, utilice el archivo de configuración para definir filtros y propiedades de registro.

- **Filtros de registro.** Filtrar la información de registro de un dispositivo Citrix ADC o de un conjunto de dispositivos Citrix ADC.
- **Propiedades de registro.** Cada filtro tiene un conjunto asociado de propiedades de registro. Las propiedades de registro definen cómo almacenar la información de registro filtrada.

Este documento incluye los siguientes detalles:

- Creación de filtros
- Especificación de propiedades de registro

Creación de filtros

Puede utilizar la definición de filtro predeterminada ubicada en el archivo de configuración (audit log.conf), o bien puede modificar el filtro o crear un nuevo filtro. Puede crear más de un filtro de registro.

> Nota:
> Para el registro consolidado, si se produce una transacción de registro para la que no existe una definición de filtro, se utiliza el filtro predeterminado (si está activado). La única forma de configurar el registro consolidado de todos los dispositivos Citrix ADC es definiendo el filtro predeterminado.

Para crear un filtro

En el símbolo del sistema, escriba el siguiente comando en el archivo de configuración (auditlog.conf):

```
filter <filterName> [IP <ip>] [NETMASK <mask>] ON | OFF]
<!--NeedCopy-->
```

FilterName: Especifique el nombre del filtro (máximo de 64 caracteres alfanuméricos).

ip: Especifique las direcciones IP.

máscara: Especifique la máscara de subred que se va a utilizar en una subred.

Especifique ON para habilitar el filtro para registrar transacciones, o bien OFF para inhabilitar el filtro. Si no se especifica ningún argumento, el filtro está activado.

Ejemplos:

```
filter F1 IP 192.168.100.151 ON
<!--NeedCopy-->
```


Para aplicar el filtro F2 a las direcciones IP 192.250.100.1 a 192.250.100.254:

```
filter F2 IP 192.250.100.0 NETMASK 255.255.255.0 ON
<!--NeedCopy-->
```

FilterName es un parámetro obligatorio si está definiendo un filtro con otros parámetros opcionales, como dirección IP, o la combinación de dirección IP y máscara de red.

Especificación de propiedades de registro

Las propiedades de registro asociadas con el filtro se aplican a todas las entradas de registro presentes en el filtro. La definición de propiedad de registro comienza con la palabra clave BEGIN y termina con END, como se ilustra en el siguiente ejemplo:

```
BEGIN <filtername>
    logFilenameFormat ...
    logDirectory ...
    logInterval ...
    logFileSizeLimit ....
END
<!--NeedCopy-->
```

Las entradas de la definición pueden incluir lo siguiente:

- **LogFileNameFormat** especifica el formato de nombre de archivo del archivo de registro. El nombre del archivo puede ser de los siguientes tipos:
  - Estático: Cadena constante que especifica la ruta absoluta y el nombre del archivo.
  - Dinámico: Expresión que incluye los siguientes especificadores de formato:
    - Date (%{format}t)
    - crea un nombre de archivo con NSIP

  Ejemplo:

  ```
  LogFileNameFormat Ex%`{
  `%m%d%y }
  t.log
  <!--NeedCopy-->
  ```

  Esto crea el primer nombre de archivo como Exmmddyy.log. Los nuevos archivos se denominan:

exmmddyy.log.0, exmmddyy.log.1, etc. En el ejemplo siguiente, los nuevos archivos se crean cuando el tamaño del archivo alcanza los 100 MB.

Ejemplo:

```
LogInterval size
LogFileSize 100
LogFileNameFormat Ex%`{
`%m%d%y }
t
<!--NeedCopy-->
```

> **Precaución**
>
> El formato de fecha%t especificado en el parámetro LogFileNameFormat reemplaza la propiedad de intervalo de registro para ese filtro. Para evitar que se cree un nuevo archivo todos los días en lugar de cuando se alcance el tamaño del archivo de registro especificado, no use %t en el parámetro LogFileNameFormat.

- **LogDirectory** especifica el formato de nombre de directorio del archivo de registro. El nombre del archivo puede ser uno de los siguientes:
  - Estático: Es una cadena constante que especifica la ruta absoluta y el nombre de archivo.
  - Dinámico: Es una expresión que contiene los siguientes especificadores de formato:
    - Date (%{format}t)
    - crea directorio con NSIP

  El separador de directorios depende del sistema operativo. En Windows, utilice el separador de directorios.

  Ejemplo:

  ```
  LogDirectory dir1\dir2\dir3
  <!--NeedCopy-->
  ```

  En los demás sistemas operativos (Linux, FreeBSD, etc.), utilice el separador de directorios.

- **LogInterval** especifica el intervalo en el que se crean nuevos archivos de registro. Utilice uno de los siguientes valores:
  - Cada hora: Se crea un archivo cada hora. Este es el valor predeterminado.
  - Diariamente: Un archivo se crea el día mismo a la medianoche.
  - Semanal: Cada domingo a medianoche se crea un archivo.
  - Mensual: Se crea un archivo el primer día del mes a medianoche.

- Ninguno: Un archivo se crea una sola vez, cuando se inicia el registro del servidor de auditoría.
- Tamaño: Solo se crea un archivo cuando se alcanza el límite de tamaño del archivo de registro.

Ejemplo:

```
LogInterval Hourly
<!--NeedCopy-->
```

- **LogFileSizelimit** especifica el tamaño máximo (en MB) del archivo de registro. Se crea un nuevo archivo cuando se alcanza el límite.

> **Nota**
>
> Puede anular la propiedad loginterval asignando tamaño como valor.

El valor predeterminado de LogFileSizelimit es de 10 MB.

Ejemplo:

```
LogFileSizeLimit 35
<!--NeedCopy-->
```

SYSLOG a través de TCP

May 8, 2022

Syslog es un estándar para enviar mensajes de notificación de eventos. Estos mensajes se pueden almacenar localmente o en un servidor de registro externo. Syslog permite a los administradores de red consolidar los mensajes de registro y obtener información de los datos recopilados.

Syslog se diseñó originalmente para funcionar a través de UDP, que puede transmitir una enorme cantidad de datos dentro de la misma red con una pérdida mínima de paquetes. Sin embargo, los operadores de telecomunicaciones prefieren transmitir datos de syslog a través de TCP, porque necesitan una transmisión de datos fiable y ordenada entre redes. Por ejemplo, la empresa de telecomunicaciones rastrea las actividades de los usuarios y TCP proporciona retransmisión en caso de error de la red.

Cómo funciona Syslog over TCP

Para entender cómo funciona syslog over TCP, considere dos casos hipotéticos:

Sam, un administrador de red, desea registrar eventos importantes en un servidor syslog externo.

XYZ Telecom, un ISP, tiene que transmitir y almacenar una cantidad significativa de datos en servidores syslog para cumplir con las regulaciones gubernamentales.

En ambos casos, los mensajes de registro deben transmitirse a través de un canal fiable y almacenarse de forma segura en un servidor syslog externo. A diferencia de UDP, TCP establece una conexión, transmite mensajes de forma segura y retransmite (del remitente al receptor) cualquier dato que esté dañado o perdido debido a un error de la red.

El dispositivo Citrix ADC envía mensajes de registro por UDP al demonio syslog local y envía mensajes de registro por TCP o UDP a servidores syslog externos.

Soporte de SNIP para Syslog

Cuando el módulo audit-log genera mensajes syslog, utiliza una dirección IP de Citrix ADC (NSIP) como dirección de origen para enviar los mensajes a un servidor syslog externo. Para configurar un SNIP como dirección de origen, debe hacerlo parte de la opción netProfile y vincular netProfile a la acción syslog.

> **Nota**
>
> TCP usa SNIP para enviar sondeos de supervisión para verificar la conectividad y luego envía los registros a través de NSIP. Por lo tanto, se debe poder acceder al servidor syslog a través de SNIP. Los perfiles de red se pueden usar para redirigir todo el tráfico de syslog TCP a través de SNIP por completo.

El uso de una dirección SNIP no se admite en el registro interno.

Nombre de dominio totalmente cualificado Soporte para registro de auditoría

Anteriormente, el módulo audit-log se configuraba con la dirección IP de destino del servidor syslog externo al que se enviaban los mensajes de registro. Ahora, el servidor de registro de auditoría utiliza un nombre de dominio completo (FQDN) en lugar de la dirección IP de destino. La configuración de FQDN resuelve el nombre de dominio configurado del servidor syslog en la dirección IP de destino correspondiente para enviar los mensajes de registro desde el módulo audit-log. El servidor de nombres debe estar configurado correctamente para resolver el nombre de dominio y evitar problemas de servicio basados en el dominio.

> **Nota**
>
> Al configurar un FQDN, no se admite la configuración del nombre de dominio del servidor del mismo dispositivo Citrix ADC en la acción syslog o la acción nslog.

Configuración de Syslog sobre TCP mediante la interfaz de línea de comandos

Para configurar un dispositivo Citrix ADC para enviar mensajes de syslog a través de TCP mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
1     add audit syslogAction <name> (<serverIP> | ((<serverDomainName>[-
          domainResolveRetry <integer>]) | -lbVserverName<string>))[-
          serverPort <port>] -logLevel <logLevel>[-dateFormat <dateFormat
          >] [-logFacility <logFacility>]   [-tcp ( NONE | ALL )] [-acl (
          ENABLED | DISABLED )][-timeZone ( GMT_TIME | LOCAL_TIME )][-
          userDefinedAuditlog ( YES | NO )][-appflowExport ( ENABLED |
          DISABLED )] [-lsn ( ENABLED | DISABLED )][-alg ( ENABLED |
          DISABLED )] [-subscriberLog ( ENABLED | DISABLED )][-transport (
           TCP | UDP )] [-tcpProfileName <string>][-maxLogDataSizeToHold <
          positive_integer>][-dns ( ENABLED | DISABLED )] [-netProfile <
          string>]
2 <!--NeedCopy-->
```

```
1     add audit syslogaction audit-action1 10.102.1.1 -loglevel
          INFORMATIONAL -dateformat MMDDYYYY -transport TCP
2 <!--NeedCopy-->
```

Agregar la dirección IP SNIP a la opción de perfil de red mediante la interfaz de línea de comandos

Para agregar una dirección IP SNIP al perfil de red mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
1     add netProfile <name> [-td <positive_integer>] [-srcIP <string>][-
          srcippersistency ( ENABLED | DISABLED )][-overrideLsn ( ENABLED
          | DISABLED )]add syslogaction <name> <serverIP>  -loglevel all
          -netprofile net1
```



```
<!--NeedCopy-->
```

```
    add netprofile net1  -srcip 10.102.147.204`
<!--NeedCopy-->
```

Donde srCip es el SNIP.

Agregar perfil de red en una acción de syslog mediante la interfaz de línea de comandos

Para agregar una opción netProfile en una acción de syslog mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
     add audit syslogaction <name> (<serverIP> | -lbVserverName <string
        >)  -logLevel <logLevel>
    -netProfile <string>  ...

<!--NeedCopy-->
```

```
    add syslogaction sys_act1 10.102.147.36  -loglevel all  -netprofile
        net1
<!--NeedCopy-->
```

Donde -netprofile especifica el nombre del perfil de red configurado. La dirección SNIP se configura como parte de netProfile y esta opción netProfile está enlazada a la acción syslog.

> **Nota**
>
> Siempre debe vincular netProfile a los servicios SYSLOGUDP o SYSLOGTCP que están enlazados al servidor virtual de equilibrio de carga SYSLOGUDP o SYSLOGTCP.

Configuración de la compatibilidad con FQDN mediante la interfaz de línea de comandos

Para agregar un nombre de dominio de servidor a una acción de Syslog mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:


```
1 add audit syslogAction <name> (<serverIP> | ((<serverDomainName>[-
     domainResolveRetry <integer>]) | -lbVserverName <string>)) -logLevel
      <logLevel> ...
2     set audit syslogAction <name> [-serverIP <ip_addr|ipv6_addr|*>]-
        serverDomainName <string>] [-lbVserverName <string>]-
        domainResolveRetry <integer>] [-domainResolveNow]
3 <!--NeedCopy-->
```

Agregar un nombre de dominio de servidor a una acción Nslog mediante la interfaz de línea de comandos.

En el símbolo del sistema, escriba:

```
1     add audit nslogAction <name> (<serverIP> | (<serverDomainName>[-
        domainResolveRetry <integer>]))  -logLevel <logLevel> ...
2     set audit nslogAction <name> [-serverIP <ip_addr|ipv6_addr|*>][-
        serverDomainName <string>] [-domainResolveRetry <integer>][-
        domainResolveNow]
3 <!--NeedCopy-->
```

Donde ServerDomainName. Nombre de dominio del servidor de registro. Es mutuamente excluyente con ServerIP/ LBVServerName.

DomainResolveRetry entero. Tiempo (en segundos) que espera el dispositivo Citrix ADC, después de que se produzca un error en la resolución de DNS, antes de enviar la siguiente consulta de DNS para resolver el nombre de dominio.

Domain Resolve ahora. Se incluye si la consulta DNS debe enviarse inmediatamente para resolver el nombre de dominio del servidor.

Configuración de Syslog sobre TCP mediante la GUI

Para configurar el dispositivo Citrix ADC para que envíe mensajes de syslog a través de TCP mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **Auditoría** > **Syslog** y seleccione la ficha **Servidores** .
2. Haga clic en **Agregar** y seleccione Tipo de transporte como **TCP**.

Configuración de un perfil de red para la compatibilidad con SNIP mediante la GUI

Para configurar el perfil de red para la compatibilidad con SNIP mediante la GUI

1. Vaya a **Sistema > Auditoría > Syslog** y seleccione la ficha **Servidores** .
2. Haga clic en **Agregar** y seleccione un perfil de red de la lista.

Configuración de FQDN mediante la GUI

Para configurar el FQDN mediante la GUI

1. Vaya a **Sistema** > **Auditoría** > **Syslog** y seleccione la ficha **Servidores** .
2. Haga clic en **Agregar** y seleccione un tipo de servidor y un nombre de dominio de servidor de la lista.

Servidores SYSLOG de equilibrio de carga

January 12, 2021

El dispositivo Citrix ADC envía sus eventos SYSLOG y mensajes a todos los servidores de registro externos configurados. Esto da como resultado el almacenamiento de mensajes redundantes y dificulta la supervisión para los administradores del sistema. Para solucionar este problema, el dispositivo Citrix ADC ofrece algoritmos de equilibrio de carga que pueden equilibrar la carga de los mensajes SYSLOG entre los servidores de registro externos para mejorar el mantenimiento y el rendimiento. Los algoritmos de equilibrio de carga compatibles incluyen RoundRobin, LeastBandwidth, CustomLoad, LeastConnection, LeastPackets y AuditLogHash.

Equilibrio de carga de servidores SYSLOG mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

1. Agregue un servicio y especifique el tipo de servicio como SYSLOGTCP o SYSLOGUDP.

   ```
   add service <name>(<IP> | <serverName>)<serviceType (SYSLOGTCP |
   SYSLOGUDP)> <port>
   ```

2. Agregue un servidor virtual de equilibrio de carga, especifique el tipo de servicio como SYSLOGTCP o SYSLOGUDP y el método de equilibrio de carga como AUDITLOGHASH.

   ```
   add lb vserver <name> <serviceType (SYSLOGTCP | SYSLOGUDP)> [-lbMethod
   <AUDITLOGHASH>]
   ```

3. Bing el servicio al servidor virtual de equilibrio de carga.

   ```
   Bind lb vserver <name> <serviceName>
   ```

4. Agregue una acción SYSLOG y especifique el nombre del servidor de equilibrio de carga que tiene SYSLOGTCP o SYSLOGUDP como tipo de servicio.

   ```
   add syslogaction <name> <serverIP> [-lbVserverName <string>] [-logLevel
    <logLevel>]
   ```

5. Agregue una directiva SYSLOG especificando la regla y la acción.

   ```
   add syslogpolicy <name> <rule> <action>
   ```


6. Enlace la directiva SYSLOG al global del sistema para que la directiva surta efecto.

   ```
   bind system global <policyName>
   ```

Equilibrio de carga de servidores SYSLOG desde la GUI

1. Agregue un servicio y especifique el tipo de servicio como SYSLOGTCP o SYSLOGUDP.

   Vaya a **Administración de Tráfico** > **Servicios**, haga clic en **Agregar** y seleccione **SYLOGTCP** o **SYSLOGUDP** como protocolo.

2. Agregue un servidor virtual de equilibrio de carga, especifique el tipo de servicio como SYSLOGTCP o SYSLOGTCP y el método de equilibrio de carga como AUDITLOGHASH.

   Vaya a **Administración del tráfico** > **Servidores virtuales**, haga clic en **Agregar** y seleccione **SYLOGTCP** o **SYSLOGUDP** como protocolo.

3. Bing el servicio al servidor virtual de equilibrio de carga al servicio.

   Bing el servicio al servidor virtual de equilibrio de carga.

   Vaya a **Administración del tráfico** > **Servidores virtuales**, seleccione un servidor virtual y, a continuación, seleccione **AUDITLOGHASH** en el **método de equilibrio de carga**.

4. Agregue una acción SYSLOG y especifique el nombre del servidor de equilibrio de carga que tiene SYSLOGTCP o SYSLOGUDP como tipo de servicio.

   Vaya a **Sistema** > **Auditoría**, haga clic en **Servidores** y agregue un servidor seleccionando la opción **LB Vserver** en **Servidores**.

5. Agregue una directiva SYSLOG especificando la regla y la acción.

   Vaya a **Sistema** > **Syslog**, haga clic en **Directivas** y agregue una directiva SYSLOG.

6. Enlace la directiva SYSLOG al global del sistema para que la directiva surta efecto.

   Vaya a **Sistema** > **Syslog**, seleccione una directiva SYSLOG y haga clic en **Acción** y, a continuación, haga clic en **Enlaces globales** y vincule la directiva a global del sistema.

Ejemplo:

La siguiente configuración especifica el equilibrio de carga de los mensajes SYSLOG entre los servidores de registro externos mediante AUDITLOGHASH como método de equilibrio de carga. La carga del método AUDITLOGHASH equilibra el tráfico en función del valor hash de entrada de los agentes de auditoría. Los agentes son los módulos que generan auditlog en un dispositivo Citrix ADC. Por ejemplo, si un agente LSN quiere equilibrar la carga auditlogs basados en la dirección IP del cliente, el módulo LSN genera el valor hash basado en ClientIP y pasa el valor hash al módulo auditlog. El módulo auditlog envía los mensajes auditlog que tienen el mismo valor hash al servidor syslog externo.

El dispositivo Citrix ADC genera eventos SYSLOG y mensajes equilibrados de carga entre los servicios, service1, service2 y service 3.


```
add service service1 192.0.2.10 SYSLOGUDP 514
add service service2 192.0.2.11 SYSLOGUDP 514
add service service3 192.0.2.11 SYSLOGUDP 514
add lb vserver lbvserver1 SYSLOGUDP -lbMethod AUDITLOGHASH
bind lb vserver lbvserver1 service1
bind lb vserver lbvserver1 service2
bind lb vserver lbvserver1 service3
add syslogaction sysaction1 -lbVserverName lbvserver1 -logLevel All
add syslogpolicy syspol1 ns_true sysaction1
bind system global syspol1
<!--NeedCopy-->
```

Limitaciones:

- El dispositivo Citrix ADC no admite un servidor virtual de equilibrio de carga externo que equilibra la carga de los mensajes SYSLOG entre los servidores de registro.

Configuración predeterminada para las propiedades de registro

January 12, 2021

A continuación se muestra un ejemplo del filtro predeterminado con la configuración predeterminada para las propiedades del registro:

```
begin default
 logInterval Hourly
 logFileSizeLimit 10
 logFilenameFormat  auditlog%`{
 `%y%m%d }
 t.log
 end default
<!--NeedCopy-->
```

A continuación se presentan dos ejemplos de definición de los filtros predeterminados:

Ejemplo 1:

```
Filter f1 IP 192.168.10.1
<!--NeedCopy-->
```


Esto crea un archivo de registro para NSI 192.168.10.1 con los valores predeterminados del efecto de inicio de sesión.

Ejemplo 2:

```
Filter f1 IP 192.168.10.1
begin f1
    logFilenameFormat logfiles.log
end f1
<!--NeedCopy-->
```

Esto crea un archivo de registro para NSIP 192.168.10.1. Dado que se especifica el formato de nombre de archivo de registro, los valores predeterminados de las otras propiedades de registro están en vigor.

Archivo de configuración de ejemplo (audit.conf)

August 20, 2021

A continuación se muestra un archivo de configuración de ejemplo:

```
##############################
# This is the Auditserver configuration file
# Only the default filter is active
# Remove leading # to activate other filters
##############################
MYIP <NSAuditserverIP>
MYPORT 3023
#   Filter filter_nsip  IP <Specify the Citrix ADC IP address to filter
    on > ON
#   begin filter_nsip
#       logInterval         Hourly
#       logFileSizeLimit    10
#       logDirectory         logdir\%A\
#       logFilenameFormat   nsip%\\{
 \\%d%m%Y }
 t.log
#   end filter_nsip
Filter default
begin default
    logInterval      Hourly
    logFileSizeLimit    10
```



```
21     logFilenameFormat   auditlog%\{
22  \%y%m%d }
23  t.log
24 end default
25 <!--NeedCopy-->
```

Registro del servidor web

January 12, 2021

Puede utilizar la función de registro del servidor web para enviar registros de solicitudes HTTP y HTTPS a un sistema cliente para su almacenamiento y recuperación. Esta función tiene dos componentes:

- El servidor de registro web, que se ejecuta en Citrix ADC.
- El cliente Citrix ADC Web Logging (NSWL), que se ejecuta en el sistema cliente.

Cuando ejecuta el cliente Citrix ADC Web Logging (NSWL):

1. Se conecta al Citrix ADC.
2. Citrix ADC almacena en búfer las entradas del registro de solicitudes HTTP y HTTPS antes de enviarlas al cliente.
3. El cliente puede filtrar las entradas antes de almacenarlas.

Para configurar el registro del servidor web, primero habilite la función de registro web en Citrix ADC y configure el tamaño del búfer para almacenar temporalmente las entradas de registro. A continuación, instala NSWL en el sistema cliente. A continuación, agregue la dirección IP de Citrix ADC (NSIP) al archivo de configuración de NSWL. Ahora está listo para iniciar el cliente NSWL para iniciar el registro. Puede personalizar el registro del servidor web realizando modificaciones adicionales en el archivo de configuración de NSWL (log.conf).

Configuración del Citrix ADC para el registro de servidores web

August 20, 2021

Para configurar Citrix ADC para el registro de servidores web, solo debe habilitar la función Registro de servidores web. Opcionalmente, puede realizar las siguientes configuraciones:

- Modifique el tamaño del búfer (el tamaño predeterminado es 16 MB) que almacena la información registrada antes de enviarla al cliente de Citrix ADC Web Logging (NSWL).

- Especifique los encabezados HTTP personalizados que quiere exportar al cliente NSWL. Puede configurar un máximo de dos nombres de encabezado de solicitud HTTP y dos de respuesta HTTP.

Para configurar el registro del servidor web mediante la interfaz de línea de comandos

En el símbolo del sistema, realice las siguientes operaciones:

- Habilite la función de registro del servidor web.

  ```
  enable ns feature WL
  ```

- [Opcional] Modifique el tamaño del búfer para almacenar la información registrada.

  ```
  set ns weblogparam -bufferSizeMB <size>
  ```

  > **Nota**:
  >
  > Para activar la modificación, debe inhabilitar y volver a habilitar la función de registro del servidor web.

- [Opcional] Especifique los nombres de encabezado HTTP personalizados que quiere exportar.

  ```
  set ns weblogparam [-customReqHdrs <string> ...] [-customRspHdrs <
  string> ...]
  ```

```
1     > enable ns feature WL
2     Done
3     > set ns weblogparam -bufferSizeMB 60
4     Done
5     > show ns weblogparam
6         Web Logging parameters:
7         Log buffer size:  60MB
8         Custom HTTP request headers: (none)
9         Custom HTTP response headers: (none)
10    Done
11    > set ns weblogparam -customReqHdrs req1 req2 -customRspHdrs res1
          res2
12    Done
13    > show ns weblogparam
14        Web Logging parameters:
15        Log buffer size:  60MB
16        Custom HTTP request headers: req1, req2
17        Custom HTTP response headers: res1, res2
18    Done
19 <!--NeedCopy-->
```


Para configurar el registro del servidor web mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **Configuración** y realice las siguientes operaciones:
    a) Para habilitar la función de registro del servidor web, haga clic en **Cambiar funciones avanzadas** y seleccione **Registro web**.
    b) Para modificar el tamaño del búfer, haga clic en **Cambiar configuración global del sistema** y, en **Registro web**, introduzca el tamaño del búfer.
    c) Para especificar los encabezados HTTP personalizados que se van a exportar, haga clic en **Cambiar configuración global del sistema** y, en **Registro web**, especifique los valores de encabezado.

Instalación del cliente de registro web (NSWL) de Citrix ADC

October 5, 2021

Al instalar NSWL, el archivo ejecutable del cliente (NSWL) se instala junto con otros archivos. El archivo ejecutable de NSWL proporciona una lista de opciones que puede utilizar. Para obtener más información, consulte Configuración del cliente NSWL.

> **Atención**
>
> La versión del cliente NSWL debe ser la misma que Citrix ADC. Por ejemplo, si la versión del Citrix ADC es 10.1 Build 125.9, el cliente NSWL también debe ser de la misma versión. Además, el cliente de registro web (NSWL) funciona tanto en equipos de 32 bits como en servidores de 64 bits. La página de descarga solo tiene un cliente weblog de 32 bits. El cliente weblog de 64 bits está disponible bajo petición y le recomienda que se ponga en contacto con el soporte de Citrix para obtener más información.

En la tabla siguiente se enumeran los sistemas operativos en los que se puede instalar el cliente NSWL.

Sistema operativo	Versión	Requisitos de hardware	Observaciones
Windows	Windows Server 2016 o posterior	Procesador: CPU x86/amd64 (1 GHz o superior), RAM - 4 GB (o superior)	
macOS	macOS 8.6 o posterior	No se admite en Citrix ADC 10.1 y versiones posteriores.	

Sistema operativo	Versión	Requisitos de hardware	Observaciones
Linux	Ubuntu, SUSE Linux, CentOS, Red Hat Enterprise Linux lanzado en 2016 o posterior	Procesador - CPU x86/amd64 (1 GHz o superior), RAM - 4 GB (o superior)	
Solaris	Solaris Sun OS 5.6 o posterior	Procesador - UltraSPARC-III 400 MHz, RAM - 512 MB, Controlador - SCSI	No compatible con Citrix ADC 10.5 y versiones posteriores.
FreeBSD	FreeBSD 6.3 o posterior	Procesador - x86/amd64 CPU (1 GHz o superior), RAM - 4 GB (o superior)	Para Citrix ADC 10.5, utilice solo FreeBSD 8.4.
AIX	AIX 6.1	-	No es compatible con Citrix ADC 10.5 y versiones posteriores.

Si el sistema cliente NSWL no puede procesar la transacción de registro debido a una limitación de CPU, el búfer de registro web se sobrepasa y se reinicia el proceso de registro.

> **Precaución**
>
> La reiniciación del registro puede provocar la pérdida de transacciones de registro.

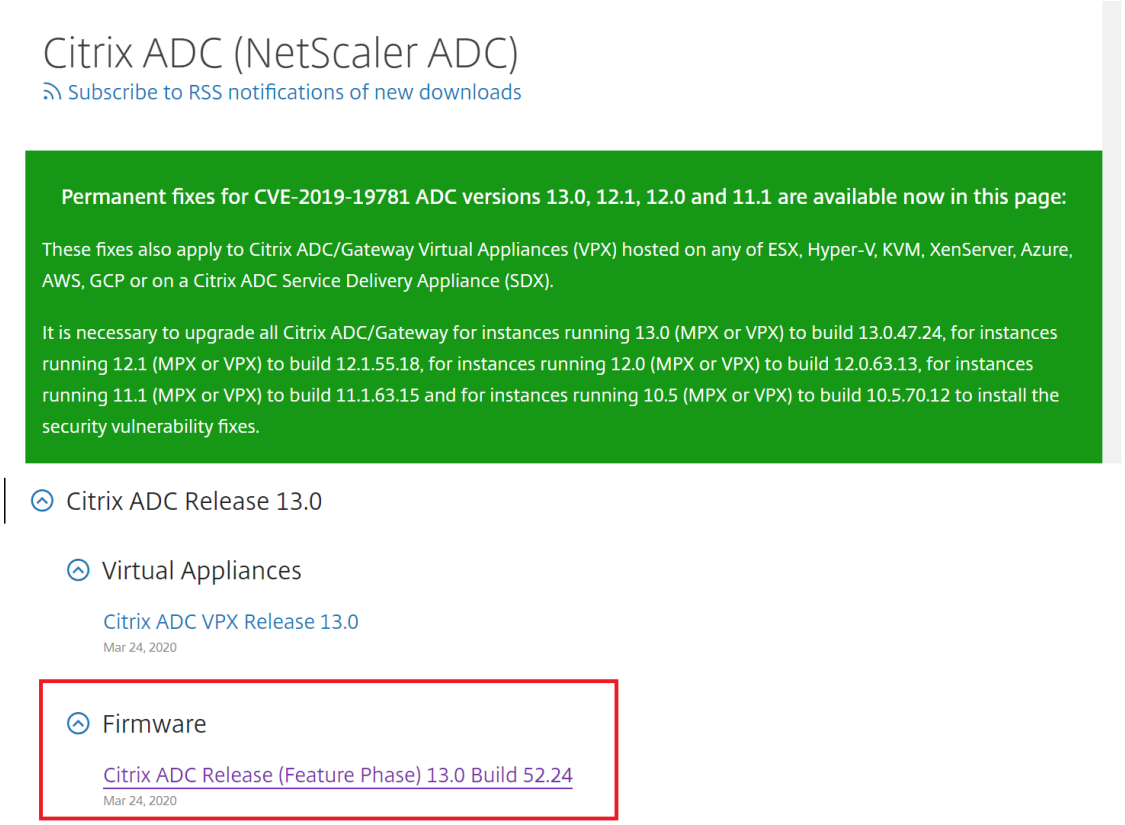
Para resolver temporalmente un cuello de botella del sistema cliente NSWL causado por una limitación de CPU, puede ajustar el tamaño del búfer de registro del servidor web en el dispositivo Citrix ADC. Para resolver el problema, necesita un sistema cliente que pueda manejar el rendimiento del sitio.

Descargar cliente NSWL

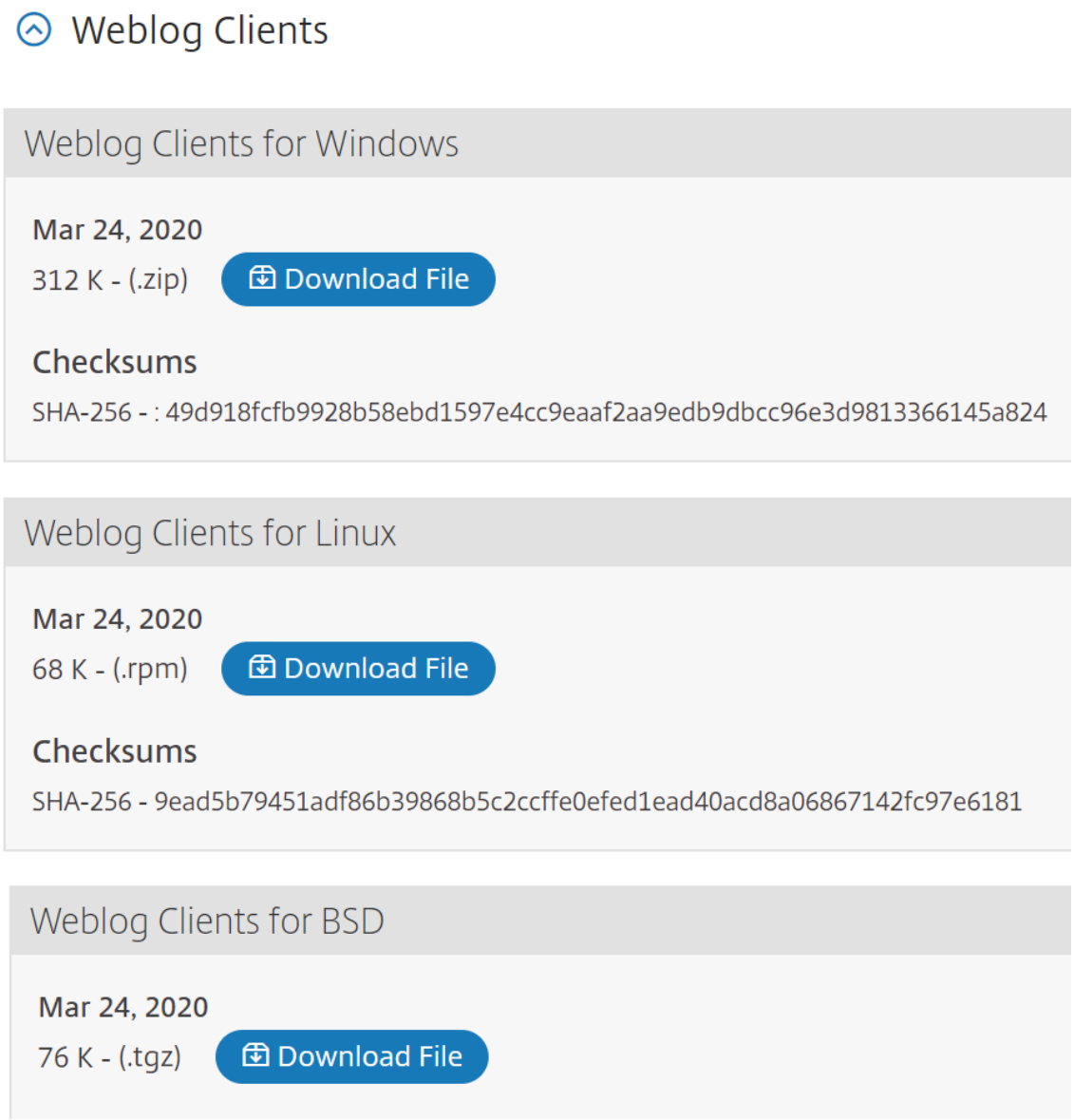
Puede obtener el paquete de cliente NSWL desde el CD del producto Citrix ADC o desde el sitio de descargas de Citrix. Dentro del paquete hay paquetes de instalación separados para cada plataforma soportada.

Para descargar el cliente NSWL desde el sitio web de Citrix

1. Inicie sesión en Citrix accediendo a la URL `https://www.citrix.com/downloads/citrix-adc/`.
2. Vaya a una versión concreta de Citrix ADC y busque su firmware.
3. Haga clic en **Firmware** (por ejemplo, Citrix ADC Release (Feature Phase) 13.0 Build 52.24).



4. En la página **Generación de Citrix ADC Release (Feature Phase)**, vaya a la sección **Clientes de Weblog**.
5. La sección le permite descargar clientes de Weblog para Windows, Linux y BSD.



Instalar cliente NSWL en Solaris

Para instalar el cliente NSWL, realice las siguientes operaciones en el sistema donde descargó el paquete.

1. Extraiga el `nswl_solaris-<release number>-<build number>.tar file` del paquete.
2. Copie el archivo extraído en un sistema Solaris en el que quiera instalar el cliente NSWL.
3. Extraiga los archivos del archivo tar con el siguiente comando:

   ```
   tar xvf nswl_solaris-9.3-51.5.tar
   ```


Un directorio weblog se crea en el directorio temporal, y los archivos se extraen en el directorio weblog.

- Instale el paquete con el siguiente comando:

  ```
  pkgadd -d
  ```

- Aparece la lista de paquetes disponibles. En el siguiente ejemplo, se muestra un paquete de Weblog:

  ```
  1 NSweblog Citrix ADC Weblogging (SunOS,sparc)7.0
  ```

Se le pedirá que seleccione los paquetes. Seleccione el número de paquete del Weblog que se va a instalar.

Después de seleccionar el número de paquete y presionar **Intro**, los archivos se extraen e instalan en los siguientes directorios:

- /usr/local/netscaler/etc
- /usr/local/netscaler/bin
- /usr/local/netscaler/samples

1. Para comprobar si el paquete NSWL está instalado, ejecute el siguiente comando:

   ```
   pkginfo | grep NSweblog
   ```

2. Para desinstalar el paquete NSWL, ejecute el siguiente comando:

   ```
   pkgrm NSweblog
   ```

Instalar cliente NSWL en Linux

> **Importante**
>
> La instalación de un cliente NSWL en Linux reemplaza al archivo de configuración. Debe realizar una copia de seguridad antes de instalarla.

Para instalar el cliente NSWL, realice las siguientes operaciones en el sistema donde descargó el paquete.

1. Extraiga el archivo nswl_linux-<release number>-<build number>.rpm del paquete.
2. Copie el archivo extraído en un sistema que ejecute el sistema operativo Linux, en el que quiera instalar el cliente NSWL.
3. Para instalar el paquete NSWL, ejecute el siguiente comando:

   ```
   rpm -i nswl_linux-9.3-51.5.rpm
   ```

Este comando extrae los archivos y los instala en los directorios siguientes.

- /usr/local/netscaler/etc

- /usr/local/netscaler/bin
- /usr/local/netscaler/samples

1. Para desinstalar el paquete NSWL, ejecute el siguiente comando:

   ```
   rpm -e NSweblog
   ```

2. Para obtener más información sobre el archivo RPM de Weblog, ejecute el siguiente comando:

   ```
   rpm -qpi *.rpm
   ```

3. Para ver los archivos de registro del servidor web instalados, ejecute el siguiente comando:

   ```
   rpm -qpl *.rpm
   ```

Instalar el cliente NSWL en FreeBSD

Para instalar el cliente NSWL, realice las siguientes operaciones en el sistema donde descargó el paquete.

1. Extraiga el archivo `nswl_bsd-<release number>-<build number>.tgz` del paquete.
2. Copie el archivo extraído en un sistema, ejecutando FreeBSD OS, en el que quiere instalar el cliente NSWL.
3. Para instalar el paquete NSWL, ejecute el siguiente comando:

   ```
   pkg_add nswl_bsd-9.3-51.5.tgz
   ```

Este comando extrae los archivos y los instala en los directorios siguientes.

```
1 -  /usr/local/netscaler/etc
2 -  /usr/local/netscaler/bin
3 -  /usr/local/netscaler/samples
```

1. Para desinstalar el paquete NSWL, ejecute el siguiente comando:

   ```
   pkg_delete NSweblog
   ```

2. Para comprobar que el paquete está instalado, ejecute el siguiente comando:

   ```
   pkg_info | grep NSweblog
   ```

Instalar el cliente NSWL en Mac

Para instalar el cliente NSWL, realice las siguientes operaciones en el sistema donde descargó el paquete.

1. Extraiga el archivo `nswl_macos-<release number>-<build number>.tgz` del paquete.

2. Copie el archivo extraído en un sistema que ejecute macOS, en el que quiera instalar el cliente NSWL.
3. Para instalar el paquete NSWL, ejecute el siguiente comando:

   ```
   pkg_add nswl_macos-9.3-51.5.tgz
   ```

Este comando extrae los archivos y los instala en los directorios siguientes:

- /usr/local/netscaler/etc
- /usr/local/netscaler/bin
- /usr/local/netscaler/samples

1. Para desinstalar el paquete NSWL, ejecute el siguiente comando:

   ```
   pkg_delete NSweblog
   ```

2. Para comprobar que el paquete está instalado, ejecute el siguiente comando:

   ```
   pkg_info | grep NSweblog
   ```

Instalar cliente NSWL en Windows

Para instalar el cliente NSWL, realice las siguientes operaciones en el sistema donde descargó el paquete.

1. Extraiga el archivo `nswl_win-<release number>-<build number>.zip` del paquete.
2. Copie el archivo extraído en un sistema Windows en el que quiera instalar el cliente NSWL.
3. En el sistema Windows, descomprima el archivo en un directorio (denominado `<NSWL-HOME>`). Se extraen los siguientes directorios: `/bin`, `/etc` y `/samples`.
4. En el símbolo del sistema, ejecute el siguiente comando desde el menú `<NSWL-HOME>\bin directory`:

   ```
   nswl -install -f <directorypath>\log.conf
   ```

Donde:

Ruta de acceso del directorio hace referencia a la ruta del archivo de configuración (log.conf). De forma predeterminada, el archivo está en el `<NSWL-HOME>` directorio `/etc` y. Puede copiar el archivo de configuración en cualquier otro directorio.

> **Nota**
>
> Para desinstalar el cliente NSWL, en el símbolo del sistema, ejecute el siguiente comando desde el `<NSWL-HOME>\bin directory`:

```
1 > nswl -remove
```


Instalar el cliente NSWL en el sistema AIX

Para instalar el cliente NSWL, realice las siguientes operaciones en el sistema donde descargó el paquete.

1. Extraiga el archivo `nswl_aix-<release number>-<build number>.rpm` del paquete.
2. Copie el archivo extraído en un sistema que ejecute AIX OS, en el que quiera instalar el cliente NSWL.
3. Para instalar el paquete NSWL, ejecute el siguiente comando:

   ```
   rpm -i nswl_aix-9.3-51.5.rpm
   ```

Este comando extrae los archivos y los instala en los directorios siguientes.

- `/usr/local/netscaler/etc`
- `/usr/local/netscaler/`
- `usr/local/netscaler/samples`

1. Para desinstalar el paquete NSWL, ejecute el siguiente comando:

   ```
   rpm -e NSweblog
   ```

2. Para obtener más información sobre el archivo RPM de Weblog, ejecute el siguiente comando:

   ```
   rpm -qpi *.rpm
   ```

3. Para ver los archivos de registro del servidor web instalados, ejecute el siguiente comando:

   ```
   rpm -qpl *.rpm
   ```

Configurar el cliente NSWL

July 8, 2022

Después de instalar el cliente NSWL, puede configurar el cliente NSWL mediante el ejecutable nswl. Estas configuraciones se almacenan en el archivo de configuración del cliente NSWL (log.conf).

> **Nota:**
>
> Puede personalizar aún más el registro en el cliente NSWL realizando más modificaciones en el archivo de configuración de NSWL (log.conf). Para obtener más información, consulte Personalización del registro en el sistema cliente NSWL.

En la tabla siguiente se describen los comandos que puede utilizar para configurar el cliente NSWL.

Comando NSWL	Qué especifica
nswl -ayuda	Las opciones de ayuda de NSWL disponibles.
nswl -complementos -f <path-to-configuration-file>	El sistema que recopila los datos de transacciones de registro. Se le pedirá que introduzca la dirección IP del dispositivo Citrix ADC. Introduzca un nombre de usuario y una contraseña válidos.
nswl -verificar -f <path-to-configuration-file>	Compruebe si hay errores semánticos o sintácticos en el archivo de configuración.
nswl -start -f <path-to-configuration-file>	Inicie el cliente NSWL según la configuración del archivo de configuración. Nota: Para Solaris y Linux: Para iniciar el registro del servidor web como un proceso en segundo plano, escriba el signo de ampersand (&) al final del comando.
nswl -stop (solo Solaris y Linux)	Detenga el cliente NSWL si se inició como un proceso en segundo plano; de lo contrario, use CTRL+C para detener el registro del servidor web.
nswl -install -f <path-to-configuration-file> (solo Windows)	Instale el cliente NSWL como servicio en Windows.
nswl -startservice (solo Windows)	Inicie el cliente NSWL mediante la configuración del archivo de configuración especificado en la opción de instalación nswl. También puede iniciar el cliente NSWL desde **Inicio > Panel de control > Servicios**. Nota: Los archivos de registro de NSWL se crean en C:\Windows\SysWOW64.
nswl -stopservice (solo Windows)	Detiene el cliente NSWL.
nswl -eliminar	Elimine el servicio de cliente NSWL del registro.

Ejecute los siguientes comandos desde el directorio en el que se encuentra el ejecutable de NSWL:

- Windows: \ns\bin
- Solaris and Linux: \usr\local\netscaler\bin

Los archivos de configuración de registro del servidor web se encuentran en la siguiente ruta de directorio:

- `Windows: \ns\etc`
- `Solaris and Linux: \usr\local\netscaler\etc`

El ejecutable de NSWL se inicia como. \ nswl en Linux y Solaris.

Agregue las direcciones IP del dispositivo Citrix ADC

En el archivo de configuración del cliente NSWL (log.conf), agregue la dirección IP de Citrix ADC (NSIP) desde la que el cliente NSWL comienza a recopilar registros.

Para agregar la dirección NSIP del dispositivo Citrix ADC

1. En el símbolo del sistema cliente, escriba:

   ```
   nswl -addns -f < directorypath > \log.conf
   < directorypath >: Specifies the path to the configuration file (log.
   conf).
   ```

2. En el siguiente mensaje, introduzca la siguiente información:
   - **NSIP**: especifique la dirección IP del dispositivo Citrix ADC.
   - Nombre de usuario y contraseña: especifique las credenciales de usuario nsroot del dispositivo Citrix ADC.

     > **Nota:**
     >
     > Cualquier usuario del sistema con el privilegio de registro habilitado admite esta función.

> **Nota:**
>
> Si agrega varias direcciones IP de Citrix ADC (NSIP) y, posteriormente, no quiere registrar todos los detalles del registro del sistema Citrix ADC, puede eliminar los NSIP manualmente quitando la instrucción NSIP al final del archivo log.conf. Durante una configuración de conmutación por error, debe agregar direcciones IP de Citrix ADC principales y secundarias a log.conf mediante el comando. Antes de agregar la dirección IP, asegúrese de que el nombre de usuario y la contraseña existan en los dispositivos Citrix ADC.

Comprobar el archivo de configuración de NSWL

Para asegurarse de que el registro funciona correctamente, revise el archivo de configuración de NSWL (log.conf) en el sistema cliente para ver si hay errores de sintaxis.

Para verificar la configuración en el archivo de configuración NSWL

En el símbolo del sistema cliente, escriba:

```
nswl -verify -f <directorypath>\log.conf
```

< directorypath>: especifica la ruta al archivo de configuración (log.conf).

Ejecutar cliente NSWL

Iniciar registro del servidor web

En el símbolo del sistema cliente, escriba:

```
nswl -start -f <directorypath>\log.conf
```

<directorypath>: especifica la ruta al archivo de configuración (log.conf).

Detener el registro del servidor web iniciado como un proceso en segundo plano en los sistemas operativos Solaris o Linux

En el símbolo del sistema, escriba:

```
nswl -stop
```

Para detener el registro del servidor web iniciado como un servicio en el sistema operativo Windows

En el símbolo del sistema, escriba:

```
nswl -stopservice
```

Personalizar el registro en el sistema cliente NSWL

May 8, 2022

Puede personalizar el registro en el sistema cliente Citrix ADC Web Logging (NSWL) realizando más modificaciones en el archivo de configuración del cliente NSWL (log.conf). Utilice un editor de texto para modificar el archivo de configuración log.conf en el sistema cliente.

Para personalizar el registro, use el archivo de configuración para definir los filtros y las propiedades del registro.

- **Filtros de registro.** Filtre la información de registro en función de la dirección IP del host, el nombre de dominio y el nombre de host de los servidores web.
- **Propiedades de registro.** Cada filtro tiene un conjunto asociado de propiedades de registro. Las propiedades de registro definen cómo almacenar la información de registro filtrada.

Archivo de configuración de ejemplo

A continuación se muestra un archivo de configuración de ejemplo:

```
##########
# This is the NSWL configuration file
# Only the default filter is active
# Remove leading # to activate other filters
##########
##########
# Default filter (default on)
# W3C Format logging, new file is created every hour or on reaching 10 MB file size,
# and the file name is Exyymmdd.log
##########
Filter default
begin default
        logFormat               W3C
        logInterval             Hourly
        logFileSizeLimit        10
        logFilenameFormat       Ex%`{
 `%y%m%d }
 t.log
end default
##########
# Citrix ADC caches example
# CACHE_F filter covers all the transaction with HOST name www.netscaler.com and the listed server ip's
##########
#Filter CACHE_F HOST www.netscaler.com IP 192.168.100.89 192.168.100.95 192.168.100.52 192.168.100.53 ON
##########
# netscaler origin server example
# Not interested in Origin server to Cache traffic transaction logging
##########
#Filter ORIGIN_SERVERS IP 192.168.100.64 192.168.100.65 192.168.100.66 192.168.100.67 192.168.100.225 192.168.100.226 192.168.
100.227 192.168.100.228 OFF
##########
# netscaler image server example
# all the image server logging.
##########
#Filter IMAGE_SERVER HOST www.netscaler.images.com IP 192.168.100.71 192.168.100.72 192.168.100.169 192.168.100.170 192.168.10
```



```
0.171 ON
##########
# NCSA Format logging, new file is created every day midnight or on reaching 20MB file size,
# and the file name is /datadisk5/netscaler/log/NS<hostname>/Nsmmddyy.log.
# Exclude objects that ends with .png .jpg .jar.
##########
#begin ORIGIN_SERVERS
#       logFormat               NCSA
#       logInterval             Daily
#       logFileSizeLimit        40
#       logFilenameFormat       /datadisk5/ORGIN/log/%v/NS%`{ `%m%d%y }t.log
#       logExclude              .png .jpg .jar
#end ORIGIN_SERVERS

##########
# NCSA Format logging, new file is created every day midnight or on reaching 20MB file size,
# and the file name is /datadisk5/netscaler/log/NS<hostname>/Nsmmddyy.log with log record timestamp as GMT.
##########
#begin CACHE_F
#       logFormat               NCSA
#       logInterval             Daily
#       logFileSizeLimit        20
#       logFilenameFormat /datadisk5/netscaler/log/%v/NS%`{ `%m%d%y }t.log
#       logtime                 GMT
#end CACHE_F

##########
# W3C Format logging, new file on reaching 20MB and the log file path name is
# atadisk6/netscaler/log/server's ip/Exmmyydd.log with log record timestamp as LOCAL.
##########
#begin IMAGE_SERVER
#       logFormat               W3C
#       logInterval             Size
#       logFileSizeLimit        20
#       logFilenameFormat /datadisk6/netscaler/log/%AEx%`{
```



```
 `%m%d%y }
 t
#       logtime                 LOCAL
#end IMAGE_SERVER

##########
# Virtual Host by Name firm, can filter out the logging based on the
   host name by,
##########

#Filter VHOST_F IP 10.101.2.151 NETMASK 255.255.255.0
#begin VHOST_F
#       logFormat               W3C
#       logInterval             Daily
#       logFileSizeLimit        10
logFilenameFormat /ns/prod/vhost/%v/Ex%`{
 `%m%d%y }
 t
#end VHOST_F

########## END FILTER CONFIGURATION ##########
<!--NeedCopy-->
```

Creación de filtros

Puede utilizar la definición de filtro predeterminada en el archivo de configuración (log.conf) o bien modificar el filtro o crear un filtro. Puede crear más de un filtro de registro.

> **Nota:**
>
> El registro consolidado, que registra las transacciones para las que no se ha definido ningún filtro, utiliza el filtro predeterminado si está habilitado. El registro consolidado de todos los servidores se puede realizar al definir solo el filtro predeterminado.

Si el servidor aloja varios sitios web y cada sitio web tiene su propio nombre de dominio y cada dominio está asociado a un servidor virtual, puede configurar el registro del servidor web para crear un directorio de registro independiente para cada sitio web. En la siguiente tabla se muestran los parámetros para crear un filtro.

Tabla 1. Parámetros para crear un filtro

Parámetro	Especifica
Nombre del filtro	Nombre del filtro. El nombre del filtro puede incluir caracteres alfanuméricos y no puede tener más de 59 caracteres. Los nombres de filtro de más de 59 caracteres se truncan a 59 caracteres.
Nombre de host	Nombre de host del servidor para el que se registran las transacciones.
IP `ip`	Dirección IP del servidor para el que se van a registrar las transacciones (por ejemplo, si el servidor tiene varios dominios que tienen una dirección IP).
IP `ip 2...ip` n:	Varias direcciones IP (por ejemplo, si el dominio del servidor tiene varias direcciones IP).
ip6 IP	Dirección IPv6 del servidor para el que se van a registrar las transacciones.
IP ip NETMASK mask	Combinación de direcciones IP y máscara de red que se utilizará en una subred.
`ON | OFF`	Habilite o inhabilite el filtro para registrar transacciones. Si no se selecciona ningún argumento, el filtro se habilita (ACTIVADO).

Para crear un filtro, introduzca el siguiente comando en el archivo log.conf:

- `filter <filterName> <HOST name> | [IP<ip> ] | [IP<ip 2...ip n> ] | <IP ip NETMASK mask> [ON | OFF]`
- `filter <filterName> <HOST name> | [IP6 ip/<prefix length>] [ON | OFF]`

Crear un filtro para un servidor virtual

Para crear un filtro para un servidor virtual, introduzca el siguiente comando en el archivo log.conf:

`filter <filterName> <VirtualServer IP address>`

Ejemplo

En el siguiente ejemplo, especifica una dirección IP de 192.168.100.0 y una máscara de red de 255.255.255.0. El filtro se aplica a las direcciones IP 192.168.100.1 a 192.168.100.254.


```
Filter F1 HOST www.netscaler.com ON
Filter F2 HOST www.netscaler.com IP 192.168.100.151 ON
Filter F3 HOST www.netscaler.com IP 192.168.100.151 192.165.100.152 ON
Filter F4 IP 192.168.100.151
Filter F5 IP 192.168.100.151 HOST www.netscaler.com OFF
Filter F6 HOST www.netscaler.com HOST www.xyz.com HOST www.abcxyz.com
    IP 192.168.100.200 ON
Filter F7 IP 192.250.100.0 NETMASK 255.255.255.0
Filter F8 HOST www.xyz.com IP 192.250.100.0 NETMASK 255.255.255.0 OFF
For creating filters for servers having IPv6 addresses.
Filter F9 2002::8/112 ON
Filter F10 HOST www.abcd.com IP6 2002::8 ON

<!--NeedCopy-->
```

Especificar propiedades de registro

Las propiedades de registro se aplican a todas las entradas de registro asociadas al filtro. La definición de la propiedad log comienza con la palabra clave `BEGIN` y termina en `END`, como se ilustra en el siguiente ejemplo:

```
BEGIN <filtername>
 logFormat ...
 logFilenameFormat ...
 logInterval ...
 logFileSize ....
 logExclude ....
 logTime ….
 END
<!--NeedCopy-->
```

Las entradas de la definición pueden incluir lo siguiente:

- **LogFormat** especifica la función de registro del servidor web que admite NCSA, W3C Extended y formatos de archivo de registros personalizados.

De forma predeterminada, la propiedad `logformat` es w3c. Para sustituir, introduzca personalizado o NCSA en el archivo de configuración, por ejemplo:

```
LogFormat NCSA
```



```
<!--NeedCopy-->
```

> **Nota:**
>
> Para los formatos de registro NCSA y personalizados, la hora local se utiliza para las transacciones de marca de tiempo y para la rotación de archivos.

- **LogInterval** especifica los intervalos en los que se crean los nuevos archivos de registros. Use uno de los valores siguientes:
  - Cada hora: se crea un archivo cada hora.
  - Diariamente: se crea un archivo todos los días a medianoche. Este es el valor predeterminado.
  - Semanalmente: se crea un archivo todos los domingos a medianoche.
  - Mensualmente: se crea un archivo el primer día del mes a medianoche.
  - Ninguno: un archivo se crea solo una vez, cuando se inicia el registro del servidor web.

Ejemplo:

```
LogInterval Daily
<!--NeedCopy-->
```

LogFileSizeLimit especifica el tamaño máximo del archivo de registros en MB. Se puede usar con cualquier intervalo de registro (semanal, mensual, etc.). Un archivo se crea cuando se alcanza el límite máximo de tamaño de archivo o cuando transcurre el tiempo del intervalo de registro definido.

Para anular este comportamiento, especifique el tamaño como propiedad `loginterval` de modo que se cree un archivo solo cuando se alcanza el límite de tamaño del archivo de registros.

El valor predeterminado de `LogFileSizeLimit` es de 10 MB.

Ejemplo:

```
LogFileSizeLimit 35
<!--NeedCopy-->
```

- **LogFilenameFormat** especifica el formato de nombre de archivo del archivo de registros. El nombre del archivo puede ser de los siguientes tipos:
  - Estático: especifica una cadena constante que contiene la ruta absoluta y el nombre del archivo.

    Dinámico: especifica una expresión que contiene el siguiente formato:

* Dirección IP del servidor
* Fecha (% {format} t)
* Sufijo de URL (%x)
* Nombre de host (%v)

Ejemplo:

```
LogFileNameFormat Ex%`{
 `%m%d%y }
 t.log
<!--NeedCopy-->
```

Este comando crea el primer nombre de archivo como Exmmddyy.log y, a continuación, cada hora crea un archivo con un nombre de archivo: Exmmddyy.log.0, Exmmddyy.log.1,…, Exmmddyy.log.n.

Ejemplo:

```
      LogInterval size
      LogFileSize 100
      LogFileNameFormat Ex%`{
 `%m%d%y }
 t
<!--NeedCopy-->
```

> **Precaución:**
>
> El formato de fecha%t especificado en el comando LogFilenameFormat reemplaza la propiedad de intervalo de registro para ese filtro. Para evitar que se cree un nuevo archivo todos los días en lugar de cuando se alcance el tamaño del archivo de registros especificado, no util%t en LogFilenameFormat.

- **LogExclude** evita el registro de transacciones con las extensiones de nombre de archivo especificadas.

Ejemplo:

```
LogExclude.html
<!--NeedCopy-->
```

Este comando crea un archivo de registros que excluye las transacciones de registro de los archivos*.html.

LogTime especifica el tiempo de registro como GMT o LOCAL.

Los valores predeterminados son:

- Formato de archivo de registros NCSA: LOCAL
- Formato del archivo de registros del W3C: GMT.

Comprender los formatos de registro NCSA y W3C

Citrix ADC admite los siguientes formatos de archivo de registros estándar:

- Formato de registro común de NCSA
- Formato de registro extendido del W3C

Formato de registro común de NCSA

Si el formato del archivo de registros es NCSA, el archivo de registros muestra la información de registro en el siguiente formato:

```
1 Client_IP_address -User_Name [Date:Time -TimeZone] ”Method Object
     HTTP_version” HTTP_StatusCode BytesSent
2 <!--NeedCopy-->
```

Para utilizar el formato de registro común de NCSA, introduzca **NCSA** en el argumento LogFormat del archivo `log.conf`.

En la siguiente tabla se describe el formato de registro común de NCSA.

Argumento	Qué especifica
Client_IP_address	La dirección IP del equipo cliente.
User Name	El nombre de usuario.
Date	La fecha de la transacción.
Time	La hora en que se completó la transacción.
Time Zone	La zona horaria (hora del meridiano de Greenwich u hora local).
Method	El método de solicitud (por ejemplo, GET, POST).
Object	La URL.
HTTP_version	La versión de HTTP que utiliza el cliente.

Argumento	Qué especifica
HTTP_StatusCode	El código de estado de la respuesta.
Bytes Sent	La cantidad de bytes enviados desde el servidor.

Formato de registro extendido del W3C

Un archivo de registros extendido contiene una secuencia de líneas que contienen caracteres ASCII terminados por un salto de línea (LF) o la secuencia Avance de línea de retorno de carro (CRLF). Los generadores de archivos de registros deben seguir la convención de terminación de línea para la plataforma en la que se ejecutan.

Los analizadores de troncos deben aceptar el formulario LF o CRLF. Cada línea puede contener una directiva o una entrada. Si quiere utilizar el formato de registro extendido de W3C, escriba W3C como argumento Log-Format en el archivo log.conf.

De forma predeterminada, el formato de registro estándar del W3C se define internamente como el formato de registro personalizado, que se muestra a continuación:

```
%`{
 `%Y-%m-%d%H:%M:%S }
 t %a %u %S %A %p %m %U %q %s %j %J %T %H %+{
 user-agent }
 i %+{
 cookie }
  i%+{
 referer }
 i
<!--NeedCopy-->
```

También puede cambiar el orden o eliminar algunos campos en este formato de registro del W3C. Por ejemplo:

```
logFormat W3C %`{
 `%Y-%m-%d%H:%M:%S }
 t %m %U
<!--NeedCopy-->
```

Las entradas de registro del W3C se crean con el siguiente formato:


```
#Version: 1.0
#Fields: date time cs-method cs-uri
#Date: 12-Jun-2001 12:34
2001-06-12 12:34:23 GET /sports/football.html 2001-06-12 12:34:30
GET /sports/football.html
<!--NeedCopy-->
```

Entradas

Las entradas consisten en una secuencia de campos relacionados con una única transacción HTTP. Los campos están separados por espacios en blanco. Citrix recomienda el uso de caracteres de tabulación. Si no se utiliza un campo de una entrada determinada, un guión (-) marca el campo omitido.

Directivas

Consulte la tabla Directivas para obtener información sobre el proceso de registro. Las líneas que comienzan con almohadillas (#) contienen directivas.

Ejemplo:

El siguiente archivo de registros de ejemplo muestra las entradas de registro en formato de registro extendido W3C:

```
#Version: 1.0
#Fields: time cs-method cs-uri
#Date: 12-Jan-1996 00:00:00
00:34:23 GET /sports/football.html
12:21:16 GET /sports/football.html
12:45:52 GET /sports/football.html
12:57:34 GET /sports/football.html
<!--NeedCopy-->
```

Campos

La directiva Fields muestra una secuencia de identificadores de campo que especifican la información registrada en cada entrada. Los identificadores de campo pueden tener uno de los siguientes formularios:

- **identificador:** se relaciona con la transacción en su conjunto.

- **prefijo-identificador:** se refiere a la transferencia de información entre partes definida por el prefijo de valor.
- **prefijo (encabezado):** especifica el valor del encabezado del campo de encabezado HTTP para la transferencia entre partes definido por el prefijo de valor. Los campos especificados de esta manera siempre tienen el tipo.

En la siguiente tabla se describen los prefijos definidos.

Prefix	Especifica
c	Cliente
s	Servidor
r	Remota
cs	De cliente a servidor
sc	De servidor a cliente
sr	De servidor a servidor remoto (prefijo utilizado por los proxies)
rs	De servidor a servidor remoto (prefijo utilizado por los proxies)
x	Identificador específico de la aplicación

Ejemplos:

Los siguientes ejemplos son identificadores definidos que usan prefijos:

cs-method: El método en la solicitud enviada por el cliente al servidor.

sc(Referer): El campo `Referer` de la respuesta.

c-ip: La dirección IP del cliente.

Identificadores

En la siguiente tabla se describen los identificadores de formato de registro extendido del W3C que no requieren un prefijo.

Identificador	Descripción
fecha	Fecha en la que se realizó la transacción.
tiempo	La hora en que se realiza la transacción.

Identificador	Descripción
tomado el tiempo	El tiempo que tarda (en segundos) la transacción en completarse.
bytes	El número de bytes transferidos.
en caché	Registra si se ha producido una coincidencia en la caché. Un cero indica que falta un caché.

En la siguiente tabla se describen los identificadores de formato de registro extendido del W3C que requieren un prefijo.

Identificador	Descripción
IP	La dirección IP y el número de puerto.
DNS	El nombre DNS.
estado	El código de estado.
comentario	El comentario se ha devuelto con un código de estado.
método	El método.
url	La URL.
url-tallo	La parte principal de la URL.
url-consulta	La parte de consulta de la URL.

El formato de archivo de registros extendido del W3C le permite elegir campos de registro. Estos campos se muestran en la siguiente tabla.

Campo	Descripción
Fecha	Fecha en la que se realiza la transacción.
Hora	La hora en que se realiza la transacción.
Client IP	La dirección IP del cliente.
Nombre de usuario	El nombre de usuario.
Nombre del servicio	El nombre del servicio, que siempre es HTTP.
IP de servidor	La dirección IP del servidor.
Puerto del servidor	El número de puerto del servidor

Campo	Descripción
Método	El método de solicitud (por ejemplo, GET, POST).
Vástago URL	La raíz de la URL.
Consulta de URL	La parte de consulta de la URL.
Estado HTTP	El código de estado de la respuesta.
Bytes enviados	La cantidad de bytes enviados al servidor (tamaño de la solicitud, incluidos los encabezados HTTP).
Bytes recibidos	La cantidad de bytes recibidos del servidor (tamaño de respuesta, incluidos los encabezados HTTP).
Tiempo tomado	El tiempo que tarda una transacción en completarse, en segundos.
Versión del protocolo	El número de versión de HTTP que utiliza el cliente.
Agente de usuario	El campo **User-Agent** del protocolo HTTP.
Cookie	El campo **Cookie** del protocolo HTTP.
`Referer`	El campo `Referer` del protocolo HTTP.

Crear un formato de registro personalizado

Puede personalizar el formato de visualización de los datos del archivo de registros manualmente o mediante la biblioteca NSWL. Al usar el formato de registro personalizado, puede derivar la mayoría de los formatos de registro que Apache admite actualmente.

Crear un formato de registro personalizado mediante la biblioteca NSWL

Utilice una de las siguientes bibliotecas NSWL dependiendo de si el ejecutable NSWL se ha instalado en un equipo host Windows o Solaris:

- **Windows:** La biblioteca nswl.lib en el directorio `\ns\bin` del equipo host del administrador del sistema.
- **Solaris:** La biblioteca `libnswl.a` en `usr/local/netscaler/bin`.

1. Agregue las siguientes dos funciones C definidas por el sistema en un archivo fuente C:

NS_userDeffieldName (): Esta función devuelve la cadena que debe agregarse como nombre de campo personalizado en el registro de registro.

NS_userDeffieldVal (): Esta función implementa el valor de campo personalizado y, a continuación, lo devuelve como una cadena que debe agregarse al final del registro de registro.

2. Compilar el archivo en un archivo de objeto.
3. Vincule el archivo objeto con la biblioteca NSWL (y, opcionalmente, con bibliotecas de terceros) para formar un nuevo ejecutable NSWL.
4. Agregue una cadena %d al final de la cadena LogFormat en el archivo de configuración (log.conf).

Ejemplo:

```
##########
# A new file is created every midnight or on reaching 20MB file size,
# and the file name is
/datadisk5/netscaler/log/NS<hostname>/Nsmmddyy.log and create
digital
#signature field for each record.
BEGIN CACHE_F
    logFormat custom "%a - "%{
 user-agent }
 i" [%d/%B/%Y %T -%g] "%x"
%s %b%{
 referrer }
 i "%{
 user-agent }
 i" "%{
 cookie }
 i" %d "
    logInterval Daily
    logFileSizeLimit 20
    logFilenameFormat
/datadisk5/netscaler/log/%v/NS%`{
 `%m%d%y }
 t.log
END CACHE_F
<!--NeedCopy-->
```


Crear un formato de registro personalizado manualmente

Para personalizar el formato en el que deben aparecer los datos del archivo de registro, especifique una cadena de caracteres como argumento de la definición de la propiedad de **registro LogFormat** . A continuación se muestra un ejemplo en el que se utilizan cadenas de caracteres para crear un formato de registro:

```
LogFormat Custom ""%a - "%{
 user-agent }
 i" %[%d/%m/%Y]t %U %s %b %T"
<!--NeedCopy-->
```

- La cadena puede contener los caracteres de control de tipo “c”\ n y\ t para representar nuevas líneas y fichas.
- Use la tecla Esc con comillas literales y barras invertidas.

Las funciones de la solicitud se registran colocando directivas % en la cadena de formato, que se sustituyen en el archivo de registros por los valores.

Si el especificador de formato%v (nombre de host) o%x (sufijo de URL) está presente en una cadena de formato de nombre de archivo de registros, los siguientes caracteres del nombre de archivo se sustituyen por un símbolo de subrayado en el nombre del archivo de configuración de registro:

```
" *. /: < > ? \ |
```

Los caracteres cuyos valores ASCII se encuentran en el intervalo de 0 a 31 se sustituyen por los siguientes:

```
%<ASCII value of character in hexadecimal>.
```

Por ejemplo, el carácter con el valor ASCII 22 se reemplaza por%16.

> **Precaución:**
>
> Si el especificador de formato%v está presente en una cadena de formato de nombre de archivo de registros, se abre un archivo independiente para cada host virtual. Para garantizar el registro continuo, el número máximo de archivos que un proceso puede tener abierto debe ser lo suficientemente grande. Consulte la documentación del sistema operativo para ver un procedimiento para cambiar el número de archivos que se pueden abrir.

Crear formatos de registro de Apache

Puede derivar de los registros personalizados la mayoría de los formatos de registro que Apache admite actualmente. Los formatos de registro personalizados que coinciden con los formatos de registro de Apache son:

NCSA/Combinado: LogFormat personalizado%h%l%u [%t] “%r” %s%b “% {referer} i” “% {user-agent} i”

NCSA/Common: LogFormat personalizado%h%l%u [%t] “%r” %s%b

Referer Registro: LogFormat personalizado “% {referer} i” ->%U

Agente de usuario: LogFormat custom% {user-agent} i

Del mismo modo, puede derivar los otros formatos de registro del servidor a partir de los formatos personalizados.

Argumentos para definir un formato de registro personalizado

En la siguiente tabla se describe el formato de registro personalizado.

Argumento	Especifica
%a	Dirección IPv4 remota.
%A	Dirección IPv4 local.
%a6	Dirección IPv6 remota.
%A6	Dirección IPv6 local.
%B	Bytes enviados, excluidos los encabezados HTTP (tamaño de la respuesta).
%b	Bytes recibidos, excluidos los encabezados HTTP (tamaño de la solicitud).
%d	Campo definido por el usuario.
%K	Información del puerto del cliente.
%e1	Valor del primer encabezado de solicitud HTTP personalizado.
%e2	Valor del segundo encabezado de solicitud HTTP personalizado.
%E1	Valor del primer encabezado de respuesta HTTP personalizado.
%E2	Valor del segundo encabezado de respuesta HTTP personalizado. Nota: Para obtener instrucciones sobre cómo exportar encabezados HTTP personalizados, consulte Configuración de NetScaler para el registro del servidor web

Argumento	Especifica
%g	Compensación de la hora del meridiano de Greenwich (por ejemplo, -0800 para la hora estándar del Pacífico).
%h	Dirección IPv4 de un host remoto.
%h6	Dirección IPv6 de un host remoto.
H	Protocolo de solicitud.
% {Foobar} i	Contenido de Foobar: línea (s) de encabezado en la solicitud enviada al servidor. El sistema admite los encabezados User -Agent, Referer y cookie. El signo + después del% en este formato informa al cliente de registro que debe usar el signo + como separador de palabras.
%j	Bytes recibidos, incluidos los encabezados (tamaño de la solicitud).
%J	Bytes enviados, incluidos los encabezados (tamaño de la respuesta).
%l	Nombre del registro remoto (de identd, si se proporciona).
%m	Método de solicitud.
%M	Tiempo necesario para atender la solicitud (en microsegundos).
% {Foobar}	Contenido de Foobar: línea (s) de encabezado en la respuesta. Se admiten los encabezados USER -AGENT, Referrer y cookie (incluidos los encabezados de cookie establecidos).
%p	Puerto canónico del servidor que atiende la solicitud.
%P	La partición admin.
%q	Cadena de consulta (con el prefijo de un signo de interrogación (?) si existe una cadena de consulta).
%r	Primera línea de la solicitud.
%s	Solicitudes que se redirigieron internamente, este es el estado de la solicitud original.

Argumento	Especifica
%t	Hora, en formato de registro común (formato de hora estándar en inglés).
% {format} t	La hora, en la forma dada por format, debe estar en el formato strftime (3). Para ver las descripciones de los formatos, consulte Definición de formato de hora
%T	Tiempo necesario para tramitar la solicitud, en segundos.
%u	Usuario remoto (de autenticación; puede ser falso si el estado de devolución (%s) es 401).
%U	Se ha solicitado la ruta URL.
%v	Nombre canónico del servidor que atiende la solicitud.
%V6	Dirección IPv6 del servidor virtual en el sistema, si se utiliza el equilibrio de carga, la conmutación de contenido o la redirección de caché.
%D	Imprime el ID de transacción HTTP.
%L	Tiempo de transacción en milisegundos.
%R	Cadena de motivo HTTP asignada al código de estado.
%f	Registro del puerto de origen.
%V	Dirección IPv4 del servidor virtual.

> **Nota**
>
> Para obtener instrucciones sobre cómo exportar encabezados HTTP personalizados, consulte Configuración de Citrix ADC para el registro del servidor web

Por ejemplo, si define el formato de registro como `%+{ user-agent } i`y si el valor del agente de usuario es Citrix ADC system Web Client, la información se registra como Citrix ADC System+Web+Client. Una alternativa es usar comillas dobles. Por ejemplo, "% {user-agent} i" lo registra como "Cliente web del sistema Citrix ADC. " No utilice la clave `\<Esc\>` en cadenas de %.. .r, %. . .i y %. . .o. Cumple con los requisitos del formato de registro común. Los clientes pueden insertar caracteres de control en el registro. Por lo tanto, debe tener cuidado al trabajar con archivos de registros sin procesar.

Definición de formato de hora

En la tabla siguiente se describe la definición del formato de hora para conocer la parte de formato de la cadena `%{ format } t` descrita en la tabla Formato de registro personalizado. Los valores entre corchetes ([ ]) muestran el rango de valores que aparecen. Por ejemplo, [1,31] en la descripción %d de la siguiente tabla muestra %d rangos de 1 a 31.

Argumento	Especifica
————	———-
%%	Igual que%.
%a	El nombre abreviado del día de la semana de la configuración regional.
%A	El nombre completo del día de la semana de la localidad
%b	El nombre abreviado del mes de la configuración regional.
%B	El nombre completo del mes de la configuración regional.
%C	El número del siglo (el año dividido por 100 y truncado a un número entero como número decimal `[1,99]`); los dígitos simples van precedidos de un 0.
%d	Campo definido por el usuario.
%K	El número del siglo (el año dividido por 100 y truncado a un número entero como número decimal `[1,99]`); los dígitos simples van precedidos de un 0.
%e	El día del mes `[1,31]`; un solo dígito va precedido de un espacio en blanco.
%h	El nombre abreviado del mes de la configuración regional.
%H	La hora (reloj de 24 horas) `[0,23]`; un solo dígito va precedido de un 0.
%I	La hora (reloj de 12 horas) `[1,12]`; un solo dígito va precedido de un 0.
%j	El número del día del año `[1,366]`; un dígito va precedido de 0.
%k	La hora (reloj de 24 horas) `[0,23]`; un solo dígito va precedido de un espacio en blanco.
%l	La hora (reloj de 12 horas) `[1,12]`; un solo dígito va precedido de un espacio en blanco.
%m	El número del mes del año `[1,12]`; un solo dígito va precedido de un 0.
%M	El minuto `[00,59]`; el 0 inicial está permitido pero no es obligatorio.
%n	Inserta una línea nueva.
%p	El equivalente de a.m. o p.m. para la configuración regional.
%r	La representación de hora adecuada en formato de reloj de 12 horas con %p
%S	Los segundos `[00,61]`; el intervalo de valores es `[00,61]` en lugar de `[00,59]` para permitir el segundo ocasional siguiente y el segundo subsiguiente.
%3	Los milisegundos `[000,999]`; el rango de valores es `[000,999]`.
%6	Los microsegundos `[000000,999999]`; el rango de valores es `[000000,999999]`.
%9	Los nanosegundos `[000000000,999999999]`; el rango de valores es `[000000000,999999999]` .
%t	Inserta una ficha.
%u	El día de la semana como número decimal `[1,7]`. 1 representa Domingo, 2 representa el martes y así sucesivamente.
%U	El número de la semana del año como número decimal `[00,53]`, con el domingo como el

primer día de la semana 1. |

> **Nota:**
>
> Si especifica una conversión que no corresponde a ninguna de las descritas en la tabla anterior o a ninguna de las especificaciones de conversión modificadas enumeradas en el párrafo siguiente, el comportamiento no está definido y devuelve 0.

La diferencia entre `%U` y `%W` (y también entre las conversiones modificadas `%OU` y `%OW`) es el día que se considera el primer día de la semana. La semana número 1 es la primera semana de enero (comienza con un domingo para `%U`o un lunes para `%W`). La semana número 0 contiene los días anteriores al primer domingo o lunes de enero para `%U` y `%W`.

Mostrar registros del servidor

Puede configurar una función NSWL para mostrar los registros del servidor en la consola o redirigir los registros del servidor a un directorio del dispositivo Citrix ADC.

Hay dos formas de mostrar los registros en la consola (salida estándar):
Opción 1: Mostrar todos los registros en la consola.
Opción 2: Mostrar solo los registros seleccionados en la consola con filtros con `logfilenameformat` como `STDOUT`.

Call Home

February 19, 2022

A veces, es posible que los dispositivos no funcionen bien debido a problemas de software o hardware. En tales casos, Citrix necesita recopilar datos y resolver problemas antes de que pueda producirse un impacto potencial en el sitio del cliente. Al habilitar Call Home en su dispositivo Citrix ADC, puede automatizar el proceso de notificación de errores. No solo evita llamar a la asistencia técnica de Citrix, generar una solicitud de servicio y cargar datos del sistema antes de que el equipo de asistencia pueda solucionar el problema, sino que la asistencia puede identificar y solucionar un problema antes de que ocurra. Call Home supervisa periódicamente el dispositivo y carga automáticamente los datos en el servidor de asistencia técnica de Citrix. Además, los datos entrantes de Call Home proporcionan información sobre el uso de Citrix ADC. Varios equipos de Citrix pueden utilizar estos datos para diseñar, admitir e implementar Citrix ADC mejor.

De forma predeterminada, Call Home está habilitado en todas las plataformas y todos los tipos de Citrix ADC (MPX, VPX, SDX). Al tener habilitada esta función, permite que Citrix recopile datos de telemetría e implementación de Citrix ADC para mejorar la implementación y el servicio de asistencia técnica.

> **Nota**
>
> También puede consultar la página de preguntas frecuentes de Call Home para obtener información relacionada con Call Home.

Ventajas

Call Home proporciona los siguientes beneficios.

- Supervisar las condiciones de error de hardware y software. Para obtener más información, consulte la sección Supervisar condiciones de error críticas.
- Notificar eventos críticos que afecten a su red.
- Envíe datos de rendimiento y detalles de uso del sistema a Citrix a:
  - Analizar y mejorar la calidad del producto.
  - Proporcione información de solución de problemas en tiempo real para la identificación proactiva de problemas y una resolución más rápida de problemas.

Plataformas compatibles

La función Call Home se admite en todas las plataformas Citrix ADC y en todos los modelos de dispositivos (MPX, VPX y SDX).

- Citrix ADC MPX: Todos los modelos MPX.
- Citrix ADC VPX: Todos los modelos VPX, incluidos los dispositivos VPX que obtienen su licencia de grupos de licencias externos o centrales.
- Citrix ADC SDX: Supervisa la unidad de disco y los chips SSL asignados en busca de errores o fallas. Sin embargo, las instancias VPX no tienen acceso a la unidad de fuente de alimentación (PSU) y, por lo tanto, su estado no se supervisa. En una plataforma SDX, puede configurar Call Home directamente en una instancia individual o a través del SVM.

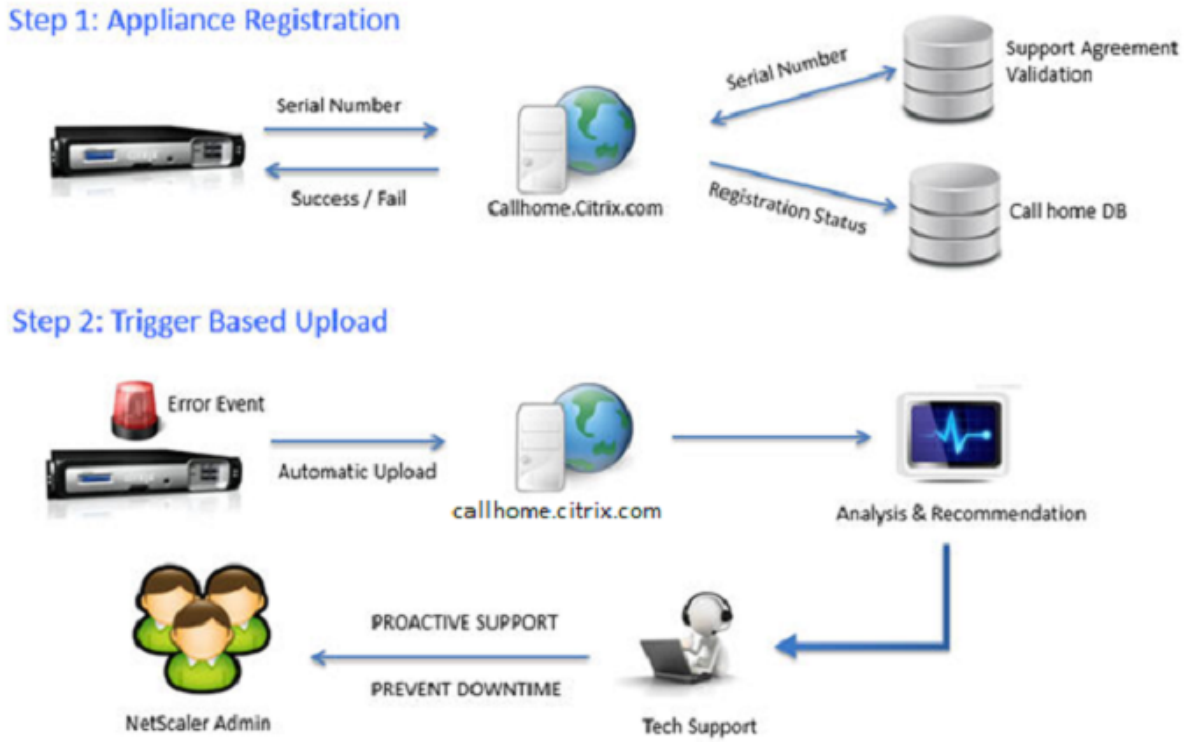
Requisitos previos

Para utilizar Call Home, el dispositivo Citrix ADC debe tener lo siguiente:

- **Conexión a Internet.** Call Home requiere una conexión a Internet para que Citrix ADC se conecte al servidor de asistencia de Citrix para cargar un archivo de datos.
- **URL.** Call Home funciona intercambiando tráfico con `callhome.citrix.com` mediante el protocolo SSL/TLS con el puerto 443 para el tráfico bidireccional.

Cómo funciona Call Home

La siguiente ilustración muestra un flujo de trabajo básico de Call Home en un dispositivo Citrix ADC implementado en un sitio del cliente.



A continuación se muestra el flujo de trabajo de un Call Home:

1. Configurar la conectividad a Internet. Para que Call Home cargue los datos del sistema, el dispositivo debe tener conexión a Internet. Si no lo hace, puede configurar una configuración de servidor proxy para proporcionar conectividad a Internet. Para obtener más información, consulte la sección Configuración del Call Home.

2. Habilite Call Home. Al actualizar el dispositivo al software más reciente a través de la interfaz de comandos de Citrix ADC o de la GUI, Call Home está habilitado de forma predeterminada y el sistema retrasa el proceso de registro 24 horas. Durante este período, puede optar por inhabilitar manualmente la función, pero Citrix recomienda que la habilite.

> **Nota**
>
> Si va a actualizar el dispositivo desde una versión anterior que explícitamente tiene inhabilitada Call Home, el sistema seguirá habilitando la función de forma predeterminada y mostrará un mensaje de notificación en el primer inicio de sesión.

Además, si va a realizar cambios de configuración para una conectividad a Internet, debe inhabilitar y habilitar Call Home. Permite que Call Home se registre en el servidor Citrix Insight Services (CIS) sin

errores de error.

3. Registre el dispositivo Citrix ADC en el servidor de asistencia técnica de Citrix. Cuando Call Home registra el dispositivo con el servidor Citrix Support, el servidor comprueba la validez del número de serie del dispositivo en la base de datos. Si el número de serie es válido, el servidor registra el dispositivo para el servicio Call Home y envía una respuesta de registro correcta. De lo contrario, el servidor devuelve un mensaje de error de registro. La información básica del sistema se envía como un mensaje separado. Los datos incluyen detalles de uso de memoria y CPU junto con los números de rendimiento. Los datos se envían periódicamente como parte del mensaje de latido cada 7 días, de forma predeterminada. Sin embargo, no se recomienda un valor inferior a 5 días, ya que las cargas frecuentes no son útiles.

4. Supervise las condiciones críticas de error. Una vez registrado, Call Home comienza a supervisar el dispositivo. En la tabla siguiente se enumeran las condiciones que Call Home puede supervisar en el dispositivo.

Condición de error crítico	Descripción	Intervalo de supervisión de Call Home	Nombre de alarma SNMP correspondiente
Errores de unidad flash compacta	La unidad flash compacta del dispositivo detectó errores de lectura o escritura.	24 horas	COMPACT-FLASH-ERRORS
Errores de la unidad de disco duro	Las unidades de disco duro del dispositivo detectaban errores de lectura o escritura.	24 horas	HARD-DISK-DRIVE-ERRORS
Fallo de la unidad de alimentación	Error en una de las unidades de fuente de alimentación del dispositivo Citrix ADC.	7 segundos	POWER-SUPPLY-FAILURE
Error en la tarjeta SSL	Error en una de las tarjetas SSL del dispositivo Citrix ADC.	7 segundos	SSL-CARD-FAILED
Reinicio en caliente	El dispositivo se ha reiniciado en caliente debido a un fallo de un proceso del sistema.	Después de cada reinicio del dispositivo Citrix ADC.	WARM-RESTART-EVENT

Condición de error crítico	Descripción	Intervalo de supervisión de Call Home	Nombre de alarma SNMP correspondiente
Error de anomalía de memoria	La utilización de la memoria aumenta progresivamente por encima de su límite normal y excede el umbral.	1 día	Sin alarma SNMP
Límite de velocidad de caída de paquetes	Se alcanzan los límites de rendimiento o los límites de paquetes por segundo (pps).	7 segundos	PF-RL-PPS-PKTS-DROPPED, PF-RL-RATE-PKTS-DROPPED

5. Cargar datos de Call Home. Si se identifica alguna de las condiciones críticas anteriores en el dispositivo, la función Call Home notifica automáticamente a la asistencia de Citrix. Los archivos de asistencia se cargan en el servidor de asistencia de Citrix. Además, puede configurar la alarma SNMP CALLHOME-UPLOAD-EVENT para generar una alerta SNMP cada vez que se suceda la carga de Call Home. La alerta SNMP notifica al administrador local sobre el evento crítico.

> **Nota**
>
> Call Home crea el archivo tar de Call Home y lo carga en el servidor de asistencia técnica de Citrix solo para la primera aparición de una condición de error particular desde el último reinicio. Si quiere que el dispositivo envíe alertas cada vez que se produzca una condición de error concreta, configure la alarma SNMP correspondiente para la condición de error.

6. Crear solicitud de servicio. Call Home crea automáticamente una solicitud de servicio para todos los eventos críticos relacionados con el hardware. Los eventos se clasifican como; fallo de la fuente de alimentación, falla de la tarjeta SSL, errores de unidad de disco duro y errores compactos de flash. Para otros errores, después de revisar los registros del sistema, puede ponerse en contacto con el equipo de asistencia técnica de Citrix para presentar una solicitud de servicio para su investigación.

Configuración de Call Home

Para configurar Call Home, compruebe la conectividad a Internet en el dispositivo y asegúrese de que esté configurado un servidor de nombres DNS. Si no hay conexión a Internet, configure un servidor o servicio proxy. A continuación, habilite Call Home en el dispositivo y verifique el estado de registro del dispositivo con el servidor de asistencia de Citrix. Una vez registrado, Call Home puede supervisar

y subir datos. Además, puede configurar alarmas SNMP para notificar al administrador en el sitio del cliente.

Para configurar Call Home, puede utilizar la interfaz de comandos de Citrix ADC o la GUI para realizar las siguientes tareas:

- Habilite Call Home.
- Configure Call Home para los parámetros opcionales del servidor proxy.
- Verifique el estado de registro de Call Home.
- Ver los errores y los detalles de la marca de tiempo.
- Configurar alarmas SNMP.

Para configurar Call Home mediante la interfaz de comandos de Citrix ADC

La interfaz de comandos de Citrix ADC le permite hacer lo siguiente:

```
Enabling Call Home
```

En el símbolo del sistema, escriba:

```
enable ns feature callhome
```

Configuración de Call Home para parámetros opcionales del servidor proxy

Call Home le permite configurar el servidor proxy opcional para la conectividad a Internet. Puede configurar un servidor proxy con dirección IP y puerto o configurar un servicio de autenticación proxy con autenticación unidireccional o bidireccional.

```
To configure optional proxy server with IP address and port
```

En el símbolo del sistema, escriba:

```
set callhome -proxyMode ( YES | NO )[-IPAddress <ip_addr|ipv6_addr|*>] [-
port <port |*>]
```

```
1 set callhome -proxyMode YES -IPAddress 10.102.167.33 -port 80
2 <!--NeedCopy-->
```

> **Nota**
>
> Call Home utiliza el servidor proxy solo cuando se establece el parámetro modo proxy-mode en YES. Si lo establece en NO, la funcionalidad del proxy no funciona, incluso si la dirección IP y el puerto están configurados. El número de puerto debe ser para un servicio HTTP, no para un servicio HTTPS.

Para configurar el servicio de autenticación proxy opcional

Este modo proporciona dos tipos de autenticación de seguridad: Unidireccional y bidireccional. Para configurar cualquiera de los tipos, debe configurar un servicio SSL. Para obtener más información, consulte el tema Configuración de un servicio SSL.

En la autenticación unidireccional, solo el dispositivo Citrix ADC autentica el servidor proxy. En la autenticación bidireccional, el dispositivo Citrix ADC autentica el servidor proxy y el servidor proxy, a su vez, autentica el dispositivo.

Para configurar el servicio de autenticación de proxy

En el símbolo del sistema, escriba:

```
set callhome -proxyMode ( YES | NO )[-proxyAuthService <string>]
```

```
1 set callhome  - proxyMode YES  - proxyAuthService callhome_proxy
2 <!--NeedCopy-->
```

Para configurar la autenticación de servidor proxy unidireccional

Realice las siguientes tareas para configurar la autenticación de servidor proxy unidireccional.

1. Cree un servicio SSL.
2. Enlazar un certificado de CA al servicio.
3. Enlazar un monitor HTTPS al servicio.
4. Configure Call Home para usar el servicio SSL.

Para configurar la autenticación de servidor proxy bidireccional

Realice las siguientes tareas para configurar la autenticación de servidor proxy bidireccional.

1. Crear un servicio SSL
2. Enlazar un certificado de CA al servicio.
3. Enlazar un certificado de cliente.
4. Enlazar un monitor HTTPS al servicio.
5. Configure Call Home para usar el servicio SSL.

Verificación del estado de registro de Call Home

En el símbolo del sistema, escriba:

```
1 show callhome
2
3     show callhome
4
5      Registration with Citrix upload server SUCCESSFUL
6
```



```
7       Mode: Default
8
9       Contact email address: exampleadmin@example.com
10
11      Heartbeat Custom Interval (days): 7
12
13      Proxy Mode: Yes
14
15         Proxy IP Address:10.102.29.200
16
17         Proxy Authentication Service:
18
19         Proxy Port: 80
20
21     Trigger event                   State   First occurrence
                      Latest occurrence
22
23      -------------                   -----   ----------------
                       -----------------
24
25      1) Warm boot                    Enabled N/A
                                        ..
26
27      2) Compact flash errors         Enabled ..
                                          ..
28
29      3) Hard disk drive errors       Enabled ..
                                          ..
30
31      4) SSL card failure             N/A     N/A
                                        N/A
32
33      5) Power supply unit failure    N/A     N/A
                                        N/A
34
35      6) Rate limit packet drops      Enabled ..
                                          ..
36
37      7) Memory anomaly               Enabled ..
                                          ..
38
39      Done
40 <!--NeedCopy-->
```


> **Nota**
>
> Si Call Home no se registra en CIS, el dispositivo muestra un mensaje de error.

Activación de alarmas SNMP

El dispositivo Citrix ADC proporciona un conjunto de entidades de condición de error denominadas *alarmas SNMP*. Cuando se cumple una condición de error en una alarma SNMP, el dispositivo genera mensajes de captura SNMP que se envían a los detectores de capturas configurados. Por ejemplo, cuando la alarma SSL-CARD-FAILED está habilitada, se genera un mensaje de captura y se envía al detector de captura. El mensaje de captura se envía cada vez que se produce un error en la tarjeta SSL en el dispositivo. Para obtener más información, consulte SNMP.

En el símbolo del sistema, escriba:

```
enable snmp alarm <trapName>
```

```
show snmp alarm <trapName>
```

Para configurar Call Home mediante GUI

Para verificar si la función Call Home está habilitada de forma predeterminada en la GUI

1. Vaya a **Configuración** > **Sistema** > **Configuración**.
2. En el panel de **detalles**, haga clic en el vínculo **Configurar funciones avanzadas**.
3. En la página **Configurar funciones avanzadas**, la opción **Call Home** debe aparecer habilitada.

Para habilitar Call Home mediante GUI

1. Vaya a **Configuración** > **Sistema** > **Configuración**.
2. En el **panel de detalles**, haga clic en el vínculo **Configurar funciones avanzadas** y seleccione la opción **Callhome**.

Para configurar Call Home para la autenticación de modo proxy opcional mediante GUI

1. Puede utilizar cualquiera de las dos formas de acceder a la página Call Home:
   a) Vaya a **Sistema** > **Información del sistema**.
   b) Vaya a **Sistema** > **Diagnósticos**.
      i. En el panel de detalles, en **Herramientas de asistencia técnica**, seleccione **Call Home**.
2. En la página **Configurar Call Home**, establezca los siguientes parámetros.
   a) **Modo**. Modo de operación Call Home. Tipos posibles: Implementación predeterminada de Citrix Service Provider (CSP).

      > **Nota**
      >
      > Esta opción no es configurable por el usuario. El modo se determina y establece automáticamente en función del tipo de implementación de Citrix ADC.

b) **Dirección de correo electrónico**. Dirección de correo electrónico del administrador de contacto en el sitio del cliente.
c) **Intervalo de latidos del corazón de CallHome (días).** Intervalo de monitorización (en días) entre los latidos del corazón de Call Home. Mínimo = 1 y Máximo = = 7.
d) **Habilite Call Home**. Habilite o inhabilite la función Call Home para ver el estado del registro del dispositivo en el servidor de asistencia de Citrix.
e) **Modo Proxy**. Si no tiene conectividad a Internet, habilite el modo proxy y establezca los parámetros de proxy opcionales.
f) **Servidor proxy**. Si establece el modo proxy mediante un servidor proxy, especifique la dirección IP del servidor.
    i. **Servicio proxy**. Si establece el modo proxy mediante un servicio proxy, especifique el nombre del servicio.
    ii. **Dirección IP**. Dirección IP del servidor proxy.
    iii. **Puerto**. Número de puerto del servidor proxy.
    iv. **Servicio SSL de autenticación de proxy**. Nombre del servicio proxy que proporciona autenticación en modo proxy.

3. Haga clic en **Aceptar** y **Listo**.

Para configurar el servicio SSL para la autenticación del servidor proxy mediante GUI

Para obtener información sobre cómo configurar el servicio SSL mediante la GUI, consulte el tema Configuración de un servicio SSL.

Para verificar el estado de registro de Call Home mediante la GUI

1. Puede utilizar cualquiera de las dos formas de acceder a la página **Call Home**:
    a) Vaya a **Sistema** > **Información del sistema**.
    b) Vaya a **Sistema** > **Diagnósticos**.
        i. En el panel de detalles, en **Herramientas de asistencia técnica**, seleccione **Call Home**.
2. En la página **Configurar Call Home**, el campo **Registro con servidor de carga de Citrix** muestra el estado del registro.

Para configurar una alarma SNMP

1. Vaya a **Sistema** > **SNMP** > **Alarmas**.
2. En el panel de detalles, seleccione una alarma y configure sus parámetros.
3. Haga clic en **Aceptar** y **cerrar**.

Compatibilidad con la implementación de Citrix Service Provider (CSP)

En un entorno de Citrix Service Provider (CSP) donde los servicios Citrix ADC se implementan en instancias VPX, Call Home puede supervisar y realizar un seguimiento de la información específica de la

licencia y enviar la información de forma segura a Citrix Insight Services (CIS). CIS a su vez envía la información al portal License Usage Insights (LUI) para fines contables y para que los clientes CSP revisen el uso de licencias. Actualmente, los entornos CSP admiten servicios Citrix ADC solo en instancias VPX, no en dispositivos MPX o SDX. Las instancias VPX se pueden implementar en modo independiente o de alta disponibilidad.

Herramienta de generación de informes

August 20, 2021

Utilice la herramienta Citrix® Citrix ADC® Reporting para ver los datos de estadísticas de rendimiento de Citrix ADC como informes. La `nscollect` utilidad recopila los datos estadísticos y se almacenan en una base de datos. Cuando desea ver determinados datos de rendimiento durante un período, la herramienta Informes extrae datos específicos de la base de datos y los muestra en gráficos.

Los informes son una colección de gráficos. La herramienta Informes proporciona informes integrados y la opción de crear informes personalizados. En un informe, puede modificar los gráficos y agregar nuevos gráficos. También puede modificar el funcionamiento de la utilidad de recopilación de datos y detener o iniciar su operación. `nscollect`

Uso de la herramienta de informes

La herramienta Reporting es una interfaz basada en web a la que se accede desde el dispositivo Citrix® Citrix ADC®. Utilice la herramienta Informes para mostrar los datos de estadísticas de rendimiento como informes que contienen gráficos. Además de utilizar los informes integrados, puede crear informes personalizados, que puede modificar en cualquier momento. Los informes pueden tener entre uno y cuatro gráficos. Puede crear hasta 256 informes personalizados. Puede crear un informe personalizado para cualquier número de entidades.

Para invocar la herramienta de informes

1. Utilice el explorador web de su elección para conectarse a la dirección IP del Citrix ADC (por ejemplo, `http://10.102.29.170/`). Aparecerá la pantalla Inicio de sesión en web.
2. En el cuadro de texto Nombre de usuario, escriba el nombre de usuario asignado al Citrix ADC.
3. En el cuadro de texto Contraseña, escriba la contraseña.
4. En el cuadro de lista desplegable Empezar en, seleccione Informes. Haga clic en Iniciar sesión.

Las capturas de pantalla siguientes muestran la barra de herramientas del informe y la barra de herramientas del gráfico, a las que se hace referencia con frecuencia en esta documentación.

Ilustración 1. *Barra de herramientas Informes*

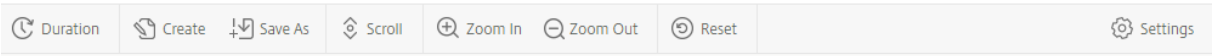
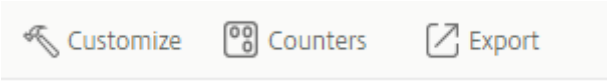


Ilustración 2. *Barra de herramientas Gráfico*



Trabajar con informes

Puede trazar y supervisar las estadísticas de los diversos grupos funcionales configurados en Citrix ADC durante un intervalo de tiempo especificado. Los informes le permiten solucionar problemas o analizar el comportamiento del dispositivo. Hay dos tipos de informes: Informes integrados e informes personalizados. El contenido del informe para los informes integrados o personalizados se puede ver en formato gráfico o tabular. La vista gráfica consta de gráficos de líneas, áreas y barras que pueden mostrar hasta 32 conjuntos de datos (contadores). La vista tabular muestra los datos en columnas y filas. Esta vista es útil para depurar contadores de errores.

El informe predeterminado que se muestra en la herramienta Informes es CPU frente a Uso de memoria y frecuencia de solicitudes HTTP. Puede cambiar la vista Informes predeterminada mostrando el informe que quiera como vista predeterminada y, a continuación, haciendo clic en Informe predeterminado.

Los informes se pueden generar para la última hora, el último día, la última semana, el último mes, el último año, o puede personalizar la duración.

Puede hacer lo siguiente con los informes:

- Alternar entre una vista tabular de datos y una vista gráfica de datos.
- Cambie el tipo de visualización gráfica, como gráfico de barras o gráfico de líneas.
- Personalizar gráficos en un informe.
- Exporte el gráfico como un archivo de valores separados por comas (CSV) de Excel.
- Vea los gráficos en detalle ampliando, alejando o mediante una operación de arrastre (desplazamiento).
- Establezca un informe como el informe predeterminado para verlo cada vez que inicie sesión.
- Agregar o quitar contadores.
- Imprimir informes.
- Actualice los informes para ver los datos de rendimiento más recientes.

Uso de informes integrados

La herramienta Informes proporciona informes integrados para los datos que se ven con frecuencia. Los informes integrados están disponibles para los siguientes grupos funcionales: System, Network, SSL, Compression, Integrated Cache, Citrix ADC Gateway y Citrix ADC Application Firewall. De forma

predeterminada, los informes integrados se muestran para el último día. Sin embargo, puede ver los informes de la última hora, la semana pasada, el mes pasado o el año pasado.

> **Nota**:
>
> No puede guardar los cambios en los informes integrados, pero puede guardar un informe integrado modificado como un informe personalizado.

Para mostrar un informe integrado

1. En el panel izquierdo de la herramienta Informes, en Informes integrados, expanda un grupo (por ejemplo, SSL).
2. Haga clic en un informe (por ejemplo, **SSL > Todos los cifrados backend)**.

Creación y eliminación de informes

Puede crear sus propios informes personalizados y guardarlos con nombres definidos por el usuario para su reutilización. Puede trazar diferentes contadores para diferentes grupos según sus necesidades. Puede crear hasta 256 informes personalizados.

Puede crear un informe nuevo o guardar un informe integrado como un informe personalizado. De forma predeterminada, un informe personalizado recién creado contiene un gráfico denominado Descripción general del sistema, que muestra el contador Uso de CPU trazado para el último día. Puede personalizar el intervalo y establecer el origen de datos y la zona horaria desde la barra de herramientas del informe.

Para crear un informe personalizado

1. En la herramienta **Informes**, en la barra de herramientas del informe, haga clic en **Crear** o, si quiere crear un nuevo informe personalizado basado en un informe existente, abra el informe existente y, a continuación, haga clic en **Guardar como**.
2. En el cuadro **Nombre del informe**, escriba un nombre para el informe personalizado.
3. Lleve a cabo una de las siguientes acciones:
   - Para agregar el informe a una carpeta existente, en Crear en o Guardar en, haga clic en la flecha hacia abajo para elegir una carpeta existente y, a continuación, haga clic en **Aceptar**.
   - Para crear una carpeta nueva para almacenar el informe, haga clic en el icono Haga clic para agregar carpeta, en Nombre de carpeta, escriba el nombre de la carpeta y, en Crear en, especifique dónde quiere que resida la nueva carpeta en la jerarquía y, a continuación, haga clic en **Aceptar**.

> **Nota**:
> Puede crear hasta 128 carpetas.

Para eliminar un informe personalizado

1. En el panel izquierdo de la herramienta Informes, junto a Informes personalizados, haga clic en el icono Haga clic para administrar los informes personalizados.
2. Active la casilla de verificación correspondiente al informe que quiere eliminar y, a continuación, haga clic en Eliminar.

> **Nota**:
>
> Cuando se elimina una carpeta, se elimina todo el contenido de esa carpeta.

Modificación del intervalo de tiempo

De forma predeterminada, los informes integrados muestran los datos del último día. Sin embargo, si quiere cambiar el intervalo de tiempo de un informe integrado, puede guardarlo como un informe personalizado. El nuevo intervalo se aplica a todos los gráficos del informe. En la siguiente tabla se describen las opciones de intervalo de tiempo.

Para modificar el intervalo de tiempo

1. En el panel izquierdo de la herramienta Informes, haga clic en un informe.
2. En la barra de herramientas del informe, haga clic en **Duración** y, a continuación, en un intervalo de tiempo.

Configuración del origen de datos y la zona horaria

Puede recuperar datos de diferentes orígenes de datos para mostrarlos en los informes. También puede definir la zona horaria de los informes y aplicar la selección de hora del informe que se muestra actualmente a todos los informes, incluidos los informes integrados.

Para establecer el origen de datos y la zona horaria

1. En la **herramienta Informes**, en la barra de herramientas Informe, haga clic en **Configuración**.
2. En el cuadro de diálogo **Configuración**, en Origen de datos, seleccione el origen de datos desde el que quiere recuperar la información del contador.
3. Realice una de las siguientes acciones o ambas:
   - Si quiere que la herramienta recuerde el período de tiempo para el que se traza un gráfico, active la casilla de verificación **Recordar selección de hora para gráficos**.
   - Si quiere que los informes utilicen la configuración de hora de su dispositivo Citrix ADC, active la casilla de verificación **Usar zona horaria del dispositivo**.

Exportación e importación de informes personalizados

Puede compartir informes con otros administradores de Citrix ADC exportando informes. También puede importar informes.

Para exportar o importar informes personalizados

1. En el panel izquierdo de la herramienta Informes, junto a Informes personalizados, haga clic en el icono **Haga clic para administrar informes personalizados**.
2. Active la casilla de verificación correspondiente al informe que quiere exportar o importar y, a continuación, haga clic en **Exportar** o **Importar**.

   > **Nota**:
   >
   > Al exportar el archivo, se exporta en un formato de archivo.gz.

Trabajar con gráficos

Utilice gráficos para trazar y supervisar contadores o grupos de contadores. Puede incluir hasta cuatro gráficos en un informe. En cada gráfico, puede trazar hasta 32 contadores. Los gráficos pueden utilizar diferentes formatos gráficos (por ejemplo, área y barra). Puede mover los gráficos hacia arriba o hacia abajo dentro del informe, personalizar los colores y la visualización visual de cada contador de un gráfico y eliminar un gráfico cuando no quiera supervisarlo.

En todos los gráficos de informe, el eje horizontal representa el tiempo y el eje vertical representa el valor del contador.

Agregar un gráfico

Cuando agrega un gráfico a un informe, aparece el gráfico Descripción general del sistema con el contador Uso de CPU trazado durante el último día.

> **Nota**:
>
> Si agrega gráficos a un informe integrado y quiere conservar el informe, debe guardarlo como un informe personalizado.

Utilice el procedimiento siguiente para agregar un gráfico a un informe.

Para agregar un gráfico a un informe

1. En el panel izquierdo de la herramienta Informes, haga clic en un informe.
2. Debajo del gráfico en el que quiere agregar el nuevo gráfico, haga clic en el icono Agregar.

Modificación de un gráfico

Puede modificar un gráfico cambiando el grupo funcional para el que se muestran las estadísticas y seleccionando diferentes contadores.

Para modificar un gráfico

1. En el panel izquierdo de la herramienta Informes, haga clic en un informe.
2. En el gráfico que quiere modificar, haga clic en Contadores.
3. En el cuadro de diálogo que aparece, en el cuadro Título, escriba un nombre para el gráfico.
4. Junto al gráfico de trazado de, siga uno de estos procedimientos:
    - Para trazar contadores para contadores globales, como Caché integrada y compresión, haga clic en Estadísticas globales del sistema.
    - Para trazar contadores de entidad para tipos de entidad, como Equilibrio de carga y GSLB, haga clic en Estadísticas de entidades del sistema.
5. En el grupo Seleccionar, haga clic en la entidad deseada.
6. En Contadores, en Disponible, haga clic en uno o varios nombres de contadores que desee trazar y, a continuación, haga clic en el botón >.
7. Si ha seleccionado Estadísticas de entidades del sistema en el paso 4, en la ficha Entidades, en Disponible, haga clic en uno o varios nombres de instancia de entidad que desee trazar y, a continuación, haga clic en el botón >.
8. Haga clic en Aceptar.

Visualización de un gráfico

Puede especificar los formatos gráficos de los contadores trazados en un gráfico. Los gráficos se pueden ver como gráficos de líneas, gráficos splines, gráficos de líneas escalonadas, gráficos de dispersión, gráficos de áreas, gráficos de barras, gráficos de áreas apiladas y gráficos de barras apiladas. También puede acercar, alejar o desplazarse dentro del área de trazado de un gráfico. Puede acercar o alejar todos los orígenes de datos durante 1 hora, 1 día, 1 semana, 1 mes, 1 año y 3 años.

Otras opciones para personalizar la vista de un gráfico incluyen personalizar los ejes de los gráficos, cambiar el color de fondo y borde del área de trazado, personalizar el color y el tamaño de las cuadrículas y personalizar la visualización de cada conjunto de datos (contador) de un gráfico.

Los números del conjunto de datos, como el conjunto de datos 1, corresponden al orden en que se muestran los contadores del gráfico en la parte inferior del gráfico. Por ejemplo, si el uso de CPU y el uso de memoria se muestran en primer y segundo orden en la parte inferior del gráfico, el uso de CPU es igual al conjunto de datos 1 y el uso de memoria es igual al conjunto de datos 2.

Siempre que modifique un informe integrado, deberá guardarlo como un informe personalizado para conservar los cambios.

Para cambiar el tipo de gráfico de un gráfico

1. En el panel izquierdo de la herramienta Informes, seleccione un informe.
2. En el panel derecho, debajo del gráfico que quiere ver, en la barra de herramientas del gráfico, haga clic en **Personalizar**.
3. En la ficha **Gráfico**, en **Categoría**, haga clic en **Tipo de trazado** y, a continuación, haga clic en el tipo de gráfico que quiera mostrar para el gráfico. Si quiere mostrar el gráfico es 3D, active la casilla de verificación Usar 3D.

Para volver a enfocar un gráfico con datos detallados

1. En el panel izquierdo de la herramienta Informes, seleccione un informe.
2. En el panel derecho, en la barra de herramientas del informe, haga clic **en Acercar** y realice una de las acciones siguientes o ambas:
   - Para volver a enfocar el gráfico para mostrar los datos de una ventana de tiempo específica, arrastre el cursor desde la hora de inicio hasta la hora de finalización. Por ejemplo, puede ver datos durante un período de una hora en un día determinado.
   - Para volver a orientar el gráfico para mostrar los datos de un punto de datos, simplemente haga clic una vez en el gráfico en el que desea ampliar y obtener información más detallada.
3. Una vez que tenga el intervalo de tiempo deseado para el que quiere ver datos detallados, en la barra de herramientas del informe, haga clic en Vista tabular. La vista tabular muestra los datos en forma numérica en filas y columnas.

Para ver datos numéricos de un gráfico

1. En el panel izquierdo de la herramienta Informes, seleccione un informe.
2. En el panel derecho, en la barra de herramientas del informe, haga clic en Vista tabular. Para volver a la vista gráfica, haga clic en **Vista gráfica**.

> **Nota**: También puede ver los datos numéricos en la vista gráfica desplazando el cursor sobre las muescas de las líneas de cuadrícula.

Para desplazarse por el tiempo en un gráfico

1. En el panel izquierdo de la herramienta Informes, seleccione un informe.
2. En el panel derecho, en la barra de herramientas del informe, haga clic en **Desplazarse** y, a continuación, haga clic dentro del gráfico y arrastre el cursor en la dirección en la que quiere ver los datos para un nuevo período de tiempo. Por ejemplo, si quieres ver datos en el pasado, arrastra hacia la izquierda.

Para cambiar el color de fondo y el color del texto de un gráfico

1. En el panel izquierdo de la herramienta Informes, seleccione un informe.
2. En el panel derecho, en el gráfico para el que quiere personalizar los ejes, haga clic en **Personalizar**.
3. En la ficha **Gráfico**, en **Categoría**, haga clic en una o varias de las opciones siguientes:
   - Para cambiar el color de fondo, haga clic en **Color de fondo** y, a continuación, seleccione las opciones de color, transparencia y efectos.
   - Para cambiar el color del texto, haga clic en **Color**del texto y, a continuación, seleccione las opciones de color, transparencia y efectos.

Para personalizar los ejes de un gráfico

1. En el panel izquierdo de la herramienta Informes, seleccione un informe.
2. En el panel derecho, en el gráfico para el que quiere personalizar los ejes, haga clic en **Personalizar**.
3. En la ficha **Gráfico**, en Categoría, haga clic en uno o varios de los siguientes elementos:
   - Para cambiar la escala del eje Y izquierdo, haga clic en **Eje Y izquierdo** y, a continuación, seleccione la escala que quiera.
   - Para cambiar la escala del eje y derecho, haga clic en Eje Y derecho, en el conjunto de datos que desea trazar, seleccione el conjunto de fechas y, a continuación, seleccione la escala que desee.

     > Nota:
     > Los números del conjunto de datos, como el conjunto de datos 1, corresponden al orden en que se muestran los contadores del gráfico en la parte inferior del gráfico. Por ejemplo, si el uso de CPU y el uso de memoria se muestran en primer y segundo orden en la parte inferior del gráfico, el uso de CPU es igual al conjunto de datos 1 y el uso de memoria es igual al conjunto de datos 2.

   - Para trazar cada conjunto de datos en su propio eje Y oculto, haga clic en Varios ejes y, a continuación, haga clic en Habilitar.

Para cambiar el color de fondo, el color de borde y las líneas de cuadrícula de un área de trazado de un gráfico

1. En el panel izquierdo de la herramienta Informes, seleccione un informe.
2. En el panel derecho, en el gráfico para el que quiere personalizar el área de trazado, haga clic en **Personalizar**.
3. En la ficha **Área de trazado**, en Categoría, haga clic en una o varias de las opciones siguientes:
   - Para cambiar el color de fondo y el color de borde del gráfico, haga clic en **Color de fondo y Color de borde** y, a continuación, seleccione las opciones de color, transparencia y efectos.

- Para cambiar las rejillas horizontales o verticales del gráfico, haga clic en **Rejillas horizontales** o **Rejillas verticales** y, a continuación, seleccione las opciones para mostrar las rejillas, el ancho de la cuadrícula, el color de la cuadrícula, la transparencia y los efectos.

Para cambiar el color y el tipo de gráfico de un conjunto de datos

1. En el panel izquierdo de la herramienta Informes, seleccione un informe.
2. En el panel derecho, en el gráfico para el que quiere personalizar la visualización del conjunto de datos (contadores), haga clic en **Personalizar**.
3. En la ficha **Conjunto de datos**, en Seleccionar conjunto de datos, seleccione el conjunto de datos (contador) para el que quiere personalizar la visualización gráfica.
   Nota: Los números del conjunto de datos, como el conjunto de datos 1, corresponden al orden en que se muestran los contadores del gráfico en la parte inferior del gráfico. Por ejemplo, si el uso de
   CPU y el uso de
   memoria se muestran en primer y segundo orden en la parte inferior del gráfico, el uso de CPU es igual al conjunto de
   datos 1 y el uso de
   memoria es igual al conjunto de
   datos 2.
4. En Categoría, realice una de las siguientes acciones:
   - Para cambiar el color de fondo, haga clic en **Color** y, a continuación, seleccione las opciones de color, transparencia y efectos.
   - Para cambiar el tipo de gráfico, haga clic en **Tipo de trazado** y, a continuación, seleccione el tipo de gráfico que quiere mostrar para el conjunto de datos. Si quiere mostrar el gráfico como 3D, active la casilla de verificación Usar 3D.

Exportar datos de gráficos a Excel

Para más análisis de datos, puede exportar gráficos a Excel en un formato de valores separados por comas (CSV).

Para exportar datos de gráficos a Excel

1. En el panel izquierdo de la herramienta Informes, seleccione un informe.
2. En el panel derecho, en el gráfico con los datos que quiere exportar a Excel, haga clic en **Exportar**.

Eliminación de un gráfico

Si no quiere utilizar un gráfico, puede eliminarlo del informe. Solo se pueden quitar gráficos de los informes personalizados de forma permanente. Si elimina un gráfico de un informe integrado y quiere

conservar los cambios, debe guardar el informe como un informe personalizado.

Para eliminar un gráfico

1. En el panel izquierdo de la herramienta Informes, seleccione un informe.
2. En el panel derecho, debajo del gráfico que quiere eliminar, haga clic en el icono **Eliminar**.

Ejemplos

Para mostrar el informe de tendencias para el uso de la CPU y el uso de memoria durante la última semana

1. En el panel izquierdo de la herramienta Informes, en Informes integrados, expanda Sistema.
2. Haga clic en el informe CPU frente a Uso de memoria y frecuencia de solicitudes HTTP.
3. En el panel derecho, en la barra de herramientas del informe, haga clic en **Duración** y, a continuación, haga clic en **Última semana**.

Para comparar la velocidad de recepción de bytes y la velocidad de transmisión de bytes entre las dos interfaces de la última semana

1. En el panel derecho, en la barra de herramientas del informe, haga clic en Crear.
2. En el cuadro **Nombre del informe**, escriba un nombre para el informe personalizado (por ejemplo, Custom_Interfaces) y, a continuación, haga clic en **Aceptar**. El informe se crea con el gráfico Descripción general del sistema predeterminado, que muestra el contador Uso de CPU trazado durante la última hora.
3. En Información general del sistema, en la barra de herramientas del gráfico, haga clic en Contadores.
4. En el panel de selección de contadores, en Título, escriba un nombre para el gráfico (por ejemplo, Interfaces bytes data).
5. En Gráfico de trazado para, haga clic en Estadísticas de entidades del sistema y, a continuación, en Seleccionar grupo, seleccione Interfaz.
6. En la ficha **Entidades**, haga clic en uno o varios nombres de interfaz que desee trazar (por ejemplo, 1/1 y 1/2) y, a continuación, haga clic en el botón >.
7. En la ficha Contadores, haga clic en Bytes recibidos (Tasa) y Bytes transmitidos (Tasa) y, a continuación, haga clic en el botón >.
8. Haga clic en **Aceptar**.
9. En la barra de herramientas del informe, haga clic en **Duración** y, a continuación, haga clic en **Última semana**.

Detener e iniciar la utilidad de recopilación de datos

La utilidad de recopilación de datos `nscollect`, se ejecuta automáticamente al iniciar Citrix ADC. Esta utilidad recupera los datos de rendimiento de la aplicación y los almacena en forma de orígenes de datos en el ADC. Puede crear hasta 32 orígenes de datos. El origen de datos predeterminado es `/var/log/db/default`.

La utilidad de recopilación de datos crea bases de datos para contadores globales y contadores específicos de entidad, y utiliza estos datos para generar informes. Las bases de datos de contador global se crean en `/var/log/db/<DataSourceName>`. Las bases de datos específicas de la entidad se crean en función de las entidades configuradas en Citrix ADC, y se crea una carpeta independiente para cada tipo de entidad en `/var/log/db/<DataSourceName/EntityNameDB>`.

`nscollect` Recupera datos una vez cada 5 minutos. Conserva los datos en granularidad de 5 minutos durante un día, por hora durante los últimos 30 días y diariamente durante tres años.

Es posible que tenga que detener y reiniciar la utilidad de recopilación de datos si los datos no se actualizan con precisión o si los informes muestran datos dañados.

Para parar `nscollect`

En el símbolo del sistema, escriba:

```
/netscaler/nscollect stop
```

Para iniciar nscollect en la sesión SSH actual en Citrix ADC:

En el símbolo del sistema, escriba:

```
/netscaler/nscollect start
```

Para iniciar nscollect en el sistema local:

En el símbolo del sistema, escriba:

```
/netscaler/nscollect start &
```

Conector CloudBridge

August 20, 2021

Nota: La versión actual de Citrix ADC 1000V no admite esta función.

La función CloudBridge Connector del dispositivo Citrix ADC conecta centros de datos empresariales a nubes externas y entornos de alojamiento, lo que convierte a la nube en una extensión segura de la red empresarial. Las aplicaciones alojadas en la nube aparecen como si se estuvieran ejecutando

en una red empresarial contigua. Con Citrix CloudBridge Connector, puede aumentar sus centros de datos con la capacidad y eficiencia disponibles en los proveedores de la nube.

CloudBridge Connector le permite mover sus aplicaciones a la nube para reducir costes y aumentar la fiabilidad.

Además de utilizar CloudBridge Connector entre un centro de datos y una nube, puede utilizarlo para conectar dos centros de datos para crear un enlace seguro y acelerado de alta capacidad.

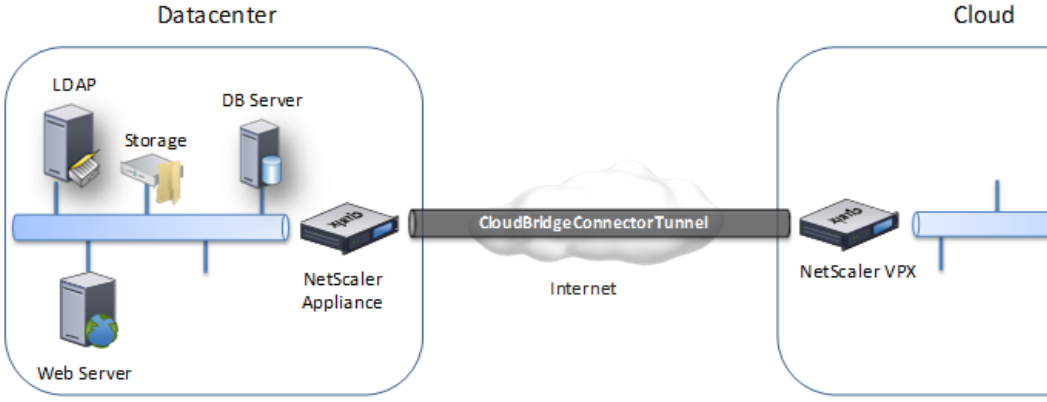
Descripción de CloudBridge Connector

Para implementar la solución Citrix CloudBridge Connector, conecte un centro de datos a otro centro de datos o a una nube externa configurando un túnel denominado túnel CloudBridge Connector.

Para conectar un centro de datos a otro centro de datos, configure un túnel de CloudBridge Connector entre dos dispositivos Citrix ADC, uno en cada centro de datos.

Para conectar un centro de datos a una nube externa (por ejemplo, la nube de Amazon AWS), debe configurar un túnel de CloudBridge Connector entre un dispositivo Citrix ADC en el centro de datos y un dispositivo virtual (VPX) que reside en la nube. El punto final remoto puede ser CloudBridge Connector o Citrix ADC VPX con licencia Premium.

La siguiente ilustración muestra un túnel de CloudBridge Connector configurado entre un centro de datos y una nube externa.



Los dispositivos entre los que se configura un túnel de CloudBridge Connector se denominan *puntos finales* o *pares* del túnel de CloudBridge Connector.

Un túnel de CloudBridge Connector utiliza los siguientes protocolos:

- Protocolo de encapsulación de redirección genérica (GRE)
- Conjunto de protocolos IPSec estándar abierto, en modo de transporte

El protocolo GRE proporciona un mecanismo para encapsular paquetes, de una amplia variedad de protocolos de red, para ser reenviados a través de otro protocolo. GRE se utiliza para:

- Conecte redes que ejecutan protocolos no IP y no enrutables.

- Puente a través de una red de área amplia (WAN).
- Cree un túnel de transporte para cualquier tipo de tráfico que deba enviarse sin cambios a través de una red diferente.

El protocolo GRE encapsula los paquetes agregando un encabezado GRE y un encabezado IP GRE a los paquetes.

El conjunto de protocolos de seguridad del protocolo Internet (IPSec) protege la comunicación entre pares en el túnel de CloudBridge Connector.

En un túnel de CloudBridge Connector, IPSec garantiza:

- Integridad de los datos
- Autenticación de origen de datos
- Confidencialidad de los datos (cifrado)
- Protección contra ataques de repetición

IPSec utiliza el modo de transporte en el que se cifra el paquete encapsulado GRE. El cifrado se realiza mediante el protocolo Encapsulating Security Payload (ESP). El protocolo ESP garantiza la integridad del paquete mediante el uso de una función hash HMAC y garantiza la confidencialidad mediante el uso de un algoritmo de cifrado. Después de que el paquete se cifra y se calcula el HMAC, se genera un encabezado ESP. El encabezado ESP se inserta después del encabezado IP GRE y se inserta un remolque ESP al final de la carga útil cifrada.

Los pares del túnel de CloudBridge Connector utilizan el protocolo de la versión de intercambio de claves de Internet (IKE) (parte del conjunto de protocolos IPSec) para negociar la comunicación segura, como se indica a continuación:

- Los dos pares se autentican mutuamente mediante uno de los siguientes métodos de autenticación:
  - **Autenticación de clave previamente compartida**. Una cadena de texto denominada clave previamente compartida se configura manualmente en cada par. Las claves previamente compartidas de los pares se comparan entre sí para la autenticación. Por lo tanto, para que la autenticación sea correcta, debe configurar la misma clave previamente compartida en cada uno de los pares.
  - **Autenticación de certificados digitales**. El par iniciador (remitente) firma los datos de intercambio de mensajes mediante su clave privada y el otro par receptor utiliza la clave pública del remitente para verificar la firma. Normalmente, la clave pública se intercambia en mensajes que contienen un certificado X.509v3. Este certificado proporciona un nivel de seguridad de que la identidad de un par tal y como se representa en el certificado está asociada a una clave pública determinada.
- A continuación, los pares negocian para llegar a un acuerdo sobre:

- Un algoritmo de cifrado.
- Claves criptográficas para cifrar datos en un par y descifrar los datos en el otro.

Este acuerdo sobre el protocolo de seguridad, el algoritmo de cifrado y las claves criptográficas se denomina Asociación de Seguridad (SA). Las SA son unidireccionales (simplex). Por ejemplo, cuando dos pares, CB1 y CB2, se comunican a través de un túnel Connector, CB1 tiene dos asociaciones de seguridad. Una SA se utiliza para procesar paquetes de salida y la otra SA se utiliza para procesar paquetes de entrada.

Las SA caducan después de un período de tiempo especificado, que se denomina *duración*. Los dos pares utilizan el protocolo de intercambio de claves de Internet (IKE) (parte del conjunto de protocolos IPSec) para negociar nuevas claves criptográficas y establecer nuevas SA. El propósito de la duración limitada es evitar que los atacantes rompan una clave.

En la tabla siguiente se enumeran algunas funciones IPSec admitidas por un dispositivo Citrix ADC:

Propiedades IPSec	Tipos admitidos
Versiones IKE	V1, V2
Grupo IKE DH	Un dispositivo Citrix ADC solo admite el grupo DH 2 (algoritmo MODP de 1024 bits) para IKEv1 e IKEv2.
Métodos de autenticación IKE	Autenticación de clave previamente compartida, Autenticación de certificados digitales
Algoritmo de cifrado	AES (128 bits), AES 256 (256 bits), 3DES
Algoritmo hash	HMAC SHA1, HMAC SHA256, HMAC SHA384, HMAC SHA512, HMAC MD5

Supervisión de túneles de CloudBridge Connector

January 12, 2021

Puede mostrar las estadísticas para supervisar el rendimiento de un túnel de CloudBridge Connector. Para mostrar las estadísticas del túnel de CloudBridge Connector en un dispositivo Citrix ADC, utilice la GUI o la línea de comandos Citrix ADC.

En la siguiente tabla se enumeran los contadores estadísticos disponibles para supervisar los túneles de CloudBridge Connector en un dispositivo Citrix ADC.

Contador estadístico	Especifica
Bytes recibidos	Número total de bytes recibidos por el dispositivo Citrix ADC a través de todos los túneles configurados de CloudBridge Connector desde la última vez que se inició el dispositivo.
Bytes enviados	Número total de bytes enviados por el dispositivo Citrix ADC a través de todos los túneles configurados de CloudBridge Connector desde la última vez que se inició el dispositivo.
Paquetes recibidos	Número total de paquetes recibidos por el dispositivo Citrix ADC a través de todos los túneles configurados de CloudBridge Connector desde la última vez que se inició el dispositivo.
Paquetes enviados	Número total de paquetes enviados por el dispositivo Citrix ADC a través de todos los túneles configurados de CloudBridge Connector desde la última vez que se inició el dispositivo.
Tasa de bytes recibidos	Número de bytes por segundo recibidos por el dispositivo Citrix ADC a través de todos los túneles configurados de CloudBridge Connector.
Velocidad de envío de bytes	Número de bytes por segundo enviados por el dispositivo Citrix ADC a través de todos los túneles configurados de CloudBridge Connector
Velocidad de recepción de paquetes	Número de bytes por segundo recibidos por el dispositivo Citrix ADC a través de todos los túneles configurados de CloudBridge Connector

Contador estadístico	Especifica
Velocidad de envío de paquetes	Número de bytes por segundo recibidos por el dispositivo Citrix ADC a través de todos los túneles configurados de CloudBridge Connector

Todos estos contadores se restablecen a 0 cuando se reinicia el dispositivo Citrix ADC. No se incrementan durante las siguientes fases:

- Fase de autenticación de Intercambio de claves de Internet (IKE) (clave previamente compartida) en cualquier túnel configurado de CloudBridge Connector.
- Fase de establecimiento de IKE Security Association (SA) en cualquier túnel de CloudBridge Connector configurado.

Para mostrar las estadísticas del túnel de CloudBridge Connector mediante la línea de comandos de Citrix ADC

En el símbolo del sistema, escriba:

- **contadores ipsec stat**

Para mostrar las estadísticas del túnel de CloudBridge Connector mediante la interfaz gráfica de usuario

1. Acceda a la GUI mediante un explorador web para conectarse a la dirección IP del dispositivo Citrix ADC.
2. En la ficha **Configuation**, vaya a **Sistema** > **CloudBridge Connector**.
3. En la página Conector de CloudBridge, haga clic en **Crear/Supervisar Conector de CloudBridge**. Los gráficos **Bytes IPSec** y **Paquetes IPSec** muestran la velocidad de recepción de bytes, la velocidad de envío de bytes, la velocidad de recepción de paquetes y la velocidad de envío de paquetes de todos los túneles de CloudBridge Connector configurados en el dispositivo Citrix ADC.

```
1     > stat ipsec counters
2     Secure tunnel(s) summary
3                          Rate (/s)        Total
4     Bytes Received    0    2811248
5     Bytes Sent           0    157460630
6     Packets Received    0    56787
7     Packets Sent        0    200910
8     Done
9     >
```



```
<!--NeedCopy-->
```

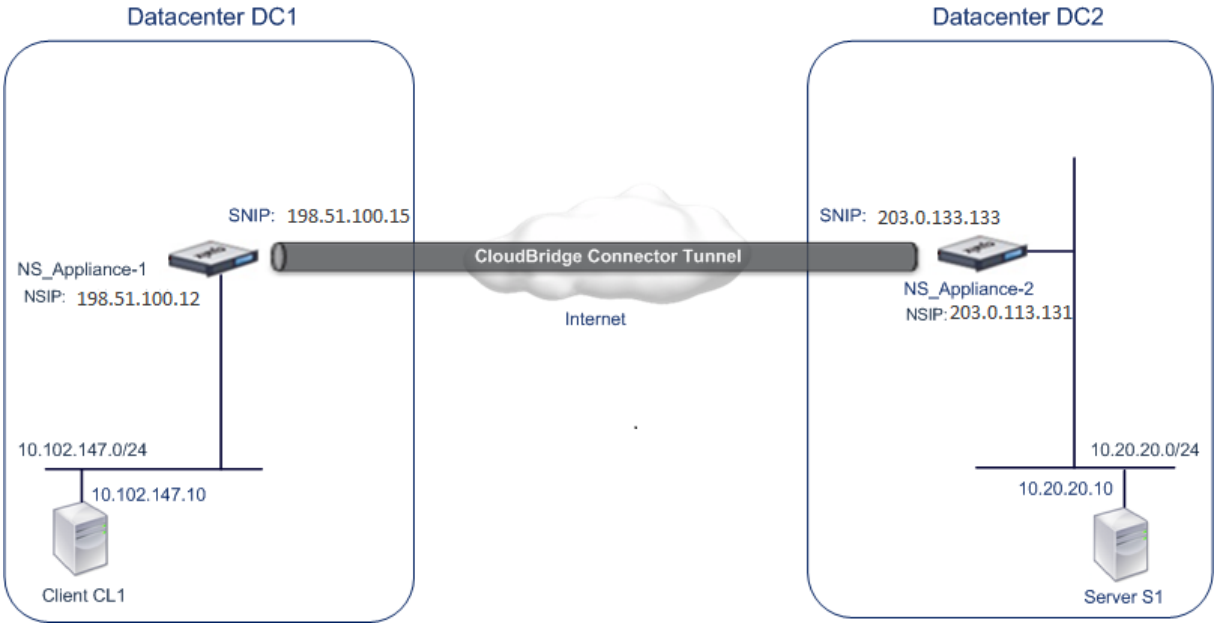
Configuración de un túnel de CloudBridge Connector entre dos centros de datos

August 20, 2021

Puede configurar un túnel de CloudBridge Connector entre dos centros de datos diferentes para ampliar la red sin reconfigurarla y aprovechar las capacidades de los dos centros de datos. Un túnel de CloudBridge Connector entre los dos centros de datos separados geográficamente le permite implementar redundancia y proteger su configuración de fallos. El túnel CloudBridge Connector ayuda a lograr una utilización óptima de la infraestructura y los recursos en todos los centros de datos. Las aplicaciones disponibles en los dos centros de datos aparecen como locales para el usuario.

Para conectar un centro de datos a otro centro de datos, configure un túnel de CloudBridge Connector entre un dispositivo Citrix ADC en un centro de datos y un dispositivo Citrix ADC en el otro centro de datos.

Como ilustración del túnel de CloudBridge Connector entre centros de datos, considere un ejemplo en el que se configura un túnel de CloudBridge Connector entre el dispositivo Citrix ADC NS_Appliance-1 en el centro de datos DC1 y el dispositivo Citrix ADC NS_Appliance-2 en el centro de datos DC2.



Ambos NS_Appliance-1 y NS_Appliance-2 funcionan en modo L2 y L3. Permiten la comunicación entre redes privadas en centros de datos DC1 y DC2. En el modo L3, NS_Appliance-1 y NS_Appliance-2 habilitan la comunicación entre el cliente CL1 en el centro de datos DC1 y el servidor S1 en el centro de

datos DC2 a través del túnel CloudBridge Connector. El cliente CL1 y el servidor S1 están en diferentes redes privadas.

Dado que el cliente CL1 y el servidor S1 están en diferentes redes privadas, el modo L3 está habilitado en NS_Appliance-1 y NS_Appliance-2, y las rutas se actualizan de la siguiente manera:

- CL1 tiene una ruta a NS_Appliance-1 para llegar a S1.
- NS_appliance-1 tiene una ruta a NS_appliance-2 para llegar a S1.
- S1 tiene una ruta a NS_Appliance-2 para llegar a CL1.
- NS_Appliance-2 tiene una ruta a NS_Appliance-1 para llegar a CL1.

En la tabla siguiente se enumeran las opciones de configuración del dispositivo Citrix ADC NS_Appliance-1 en el centro de datos DC1.

En la tabla siguiente se enumeran las opciones de configuración del dispositivo Citrix ADC NS_Appliance-2 en el centro de datos DC2.

Entidad	Nombre	Detalles
La dirección NSIP		198.51.100.12
Dirección SNIP		198.51.100.15
Túnel del conector CloudBridge	Cloud_Connector_DC1-DC2	1. Dirección IP del extremo local del túnel CloudBridge Connector: 198.51.100.15, 2. Dirección IP del extremo remoto del túnel CloudBridge Connector: 203.0.113.133. Detalles del túnel GRE Nombre = Cloud_Connector_DC1-DC2, Detalles del perfil IPSec Nombre = Cloud_Connector_DC1-DC2, Algoritmo de cifrado = AES, Algoritmo de hash = HMAC SHA1

Puntos a tener en cuenta para configurar el túnel de CloudBridge Connector

Antes de configurar un túnel de CloudBridge Connector, compruebe que se han completado las siguientes tareas:

1. Implemente y configure un dispositivo Citrix ADC en cada uno de los dos centros de datos.
2. Asegúrese de que las direcciones IP de punto final del túnel CloudBridge Connector sean accesibles entre sí.

Procedimiento de configuración

Para configurar un túnel de CloudBridge Connector entre un dispositivo Citrix ADC que reside en un centro de datos y otro dispositivo Citrix ADC que reside en el otro centro de datos, utilice la GUI o la interfaz de línea de comandos de uno de los dispositivos Citrix ADC.

Cuando se utiliza la GUI, la configuración del túnel de CloudBridge Connector creada en el primer dispositivo Citrix ADC se envía automáticamente al otro extremo (el otro dispositivo Citrix ADC) del túnel de CloudBridge Connector. Por lo tanto, no es necesario acceder a la GUI del otro dispositivo Citrix ADC para crear la configuración de túnel de CloudBridge Connector correspondiente en él.

La configuración del túnel de CloudBridge Connector en cada uno de los dispositivos Citrix ADC consta de las siguientes entidades:

- **Perfil IPSec**: Una entidad de perfil IPSec especifica los parámetros del protocolo IPSec, como la versión IKE, el algoritmo de cifrado, el algoritmo hash y PSK, que utilizará el protocolo IPSec en el túnel de CloudBridge Connector.
- **Túnel GRE**: Un túnel IP especifica la dirección IP local (una dirección SNIP pública configurada en el dispositivo Citrix ADC local), la dirección IP remota (una dirección SNIP pública configurada en el dispositivo Citrix ADC remoto), el protocolo (GRE) utilizado para configurar el túnel CloudBridge Connector y un IPSec entidad de perfil.
- **Cree una regla PBR y asocie el túnel IP a ella**: Una entidad PBR especifica un conjunto de condiciones y una entidad de túnel IP. El intervalo de direcciones IP de origen y el intervalo IP de destino son las condiciones para la entidad PBR. Debe establecer el intervalo de direcciones IP de origen y el intervalo de direcciones IP de destino para especificar la subred cuyo tráfico va a atravesar el túnel del conector de CloudBridge. Por ejemplo, considere un paquete de solicitud que se origina en un cliente de la subred del primer centro de datos y está destinado a un servidor de la subred del segundo centro de datos. Si este paquete coincide con el intervalo de direcciones IP de origen y destino de la entidad PBR en el dispositivo Citrix ADC en el primer centro de datos, se envía a través del túnel CloudBridge Connector asociado a la entidad PBR.

Para crear un perfil IPSEC mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

- `add ipsec profile <name> [-ikeVersion ( V1 | V2 )] [-encAlgo ( AES | 3 DES )...] [-hashAlgo <hashAlgo\> ...] [-lifetime <positive_integer>] (-psk | (-publickey<string> -privatekey <string>-peerPublicKey <string >))[-livenessCheckInterval <positive_intege>][-replayWindowSize \<`

positive_integer>] [-ikeRetryInterval <positive_integer>] [-retransmissiontime <positive_integer>]

- show ipsec profile <name>

Para crear un túnel IP y enlazar el perfil IPSEC mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

- add ipTunnel <name> <remote><remoteSubnetMask> <local> [-protocol <protocol>] [-ipsecProfileName <string>]
- show ipTunnel <name>

Para crear una regla PBR y enlazar el túnel IPSEC con ella mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

- add ns pbr <pbr_name> ALLOW -srcIP = <local_subnet_range> -destIP = <remote_subnet_range> -ipTunnel <tunnel_name>
- apply ns pbrs
- show ns pbr <pbr_name>

Ejemplo

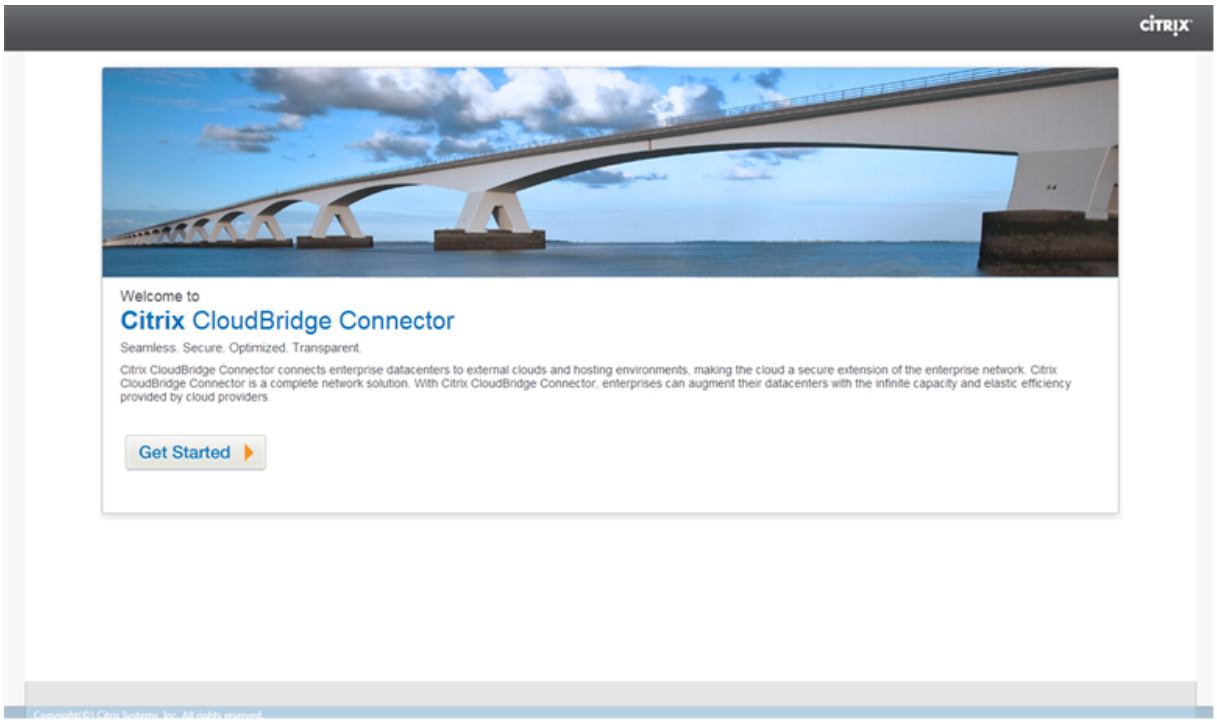
```
1  add ipsec profile Cloud_Connector_DC1-DC2  -encAlgo AES -hashAlgo
       HMAC_SHA1
2      Done
3      > add ipTunnel Cloud_Connector_DC1-DC2 203.0.113.133
          255.255.255.255 198.51.100.15 -protocol GRE -ipsecProfileName
          Cloud_Connector_DC1-DC2
4
5      Done
6      > add ns pbr PBR-DC1-DC2 ALLOW -srcIP 198.51.100.15 -destIP
          203.0.113.133 ipTunnel Cloud_Connector_DC1-DC2
7
8      Done
9      > apply ns pbrs
10
11     Done
12 <!--NeedCopy-->
```

Para configurar un túnel de CloudBridge Connector en un dispositivo Citrix ADC mediante la interfaz gráfica de usuario

1. Escriba la dirección NSIP de un dispositivo Citrix ADC en la línea de direcciones de un explorador web.

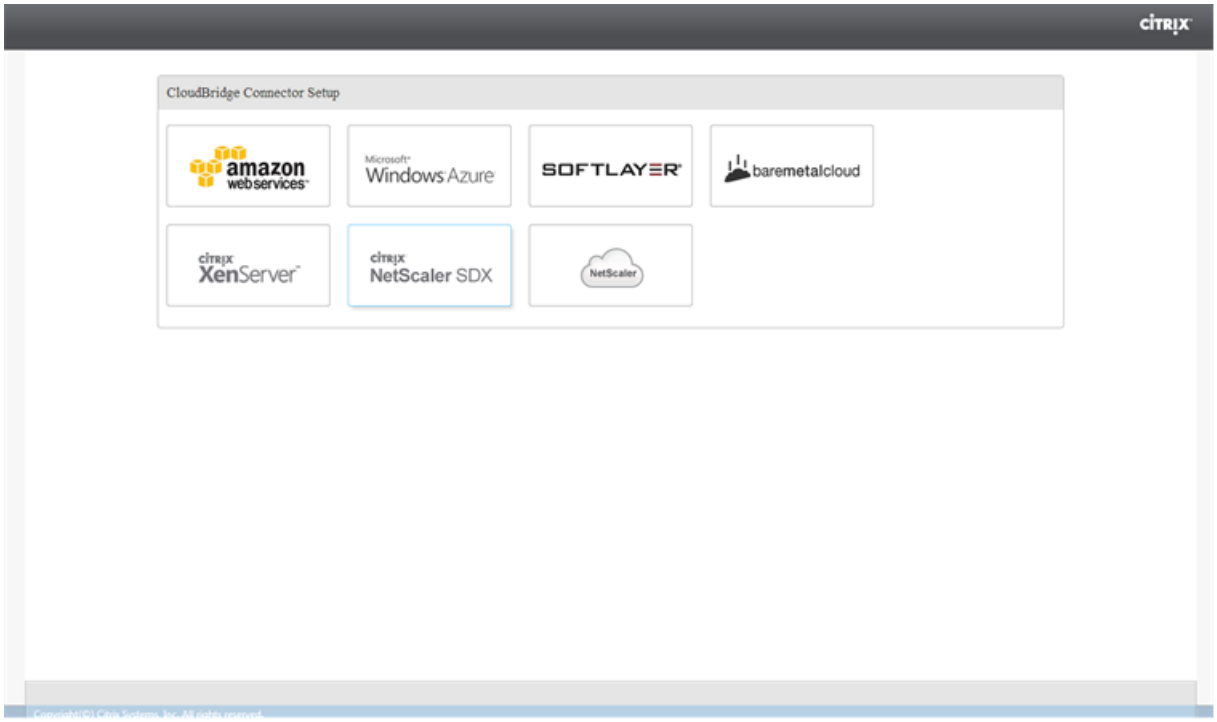
2. Inicie sesión en la GUI del dispositivo Citrix ADC mediante las credenciales de cuenta del dispositivo.
3. Vaya a **Sistema** > **Conector de CloudBridge**.
4. En el panel derecho, en **Introducción**, haga clic en **Crear/Supervisar CloudBridge**.

   La primera vez que configure un túnel de CloudBridge Connector en el dispositivo, aparece una pantalla de **bienvenida**.
5. En la **pantalla de bienvenida**, haga clic en **Introducción**.



> **Nota**:
>
> Si ya tiene configurado un túnel de CloudBridge Connector en el dispositivo Citrix ADC, la pantalla de bienvenida no aparece, por lo que no hace clic en Comenzar.

1. En el panel **Configuración de CloudBridge Connector**, haga clic en **Citrix ADC**.



1. En el panel ADC de Citrix, proporcione las credenciales de cuenta para el dispositivo Citrix ADC remoto. Haga clic en **Continuar**.
2. En el panel **Configuración del conector de CloudBridge**, establezca el siguiente parámetro:
   - **CloudBridge Connector Name**: Nombre para la configuración de CloudBridge Connector en el dispositivo local. Debe comenzar con un carácter alfabético ASCII o de subrayado (_) y debe contener solo caracteres alfanuméricos ASCII, guión bajo, hash (#), punto (.), espacio, dos puntos (:), en (@), igual (=) y guión (-). No se puede cambiar después de crear la configuración de CloudBridge Connector.
3. En **Configuración local**, establezca el siguiente parámetro:
   - **IP de subred**: Dirección IP del extremo local del túnel de CloudBridge Connector.
4. En **Configuración remota**, establezca el siguiente parámetro:
   - **IP de subred**: Dirección IP del punto final del mismo nivel del túnel de CloudBridge Connector.
5. En Configuración de **PBR**, defina los siguientes parámetros:
   - **Operación**: El igual (=) o no es igual a (! =) operador lógico.
   - **IP de origen bajo**: La dirección IP de origen más baja para que coincida con la dirección IP de origen de un paquete IPv4 saliente.
   - **IP de origen alto**: La dirección IP de origen más alta que debe coincidir con la dirección IP de origen de un paquete IPv4 saliente.
   - **Operación**: El igual (=) o no es igual a (! =) operador lógico.

- IP de destino Low*: La dirección IP de destino más baja para que coincida con la dirección IP de destino de un paquete IPv4 saliente.
- Dirección**IP de destino alta**: La dirección IP de destino más alta que debe coincidir con la dirección IP de destino de un paquete IPv4 saliente.

6. (Opcional) En **Configuración de seguridad**, establezca los siguientes parámetros de protocolo IPSec para el túnel de CloudBridge Connector:

   - **Algoritmo**de cifrado: Algoritmo de cifrado que utilizará el protocolo IPSec en el túnel de CloudBridge.
   - **Algoritmo hash**: Algoritmo hash que utilizará el protocolo IPSec en el túnel CloudBridge.
   - **Clave**: Seleccione uno de los siguientes métodos de autenticación IPSec que los dos pares utilizarán para autenticarse mutuamente.
     - **Generación automática de clave**: Autenticación basada en una cadena de texto, denominada clave previamente compartida (PSK), generada automáticamente por el dispositivo local. Las claves PSK de los pares se comparan entre sí para la autenticación.
     - **Clave específica**: Autenticación basada en un PSK introducido manualmente. Los PSK de los pares se comparan entre sí para la autenticación.
       * Clave de seguridad precompartida: la cadena de texto introducida para la autenticación basada en clave previamente compartida.
     - **Cargar certificados**: Autenticación basada en certificados digitales.
       * **Clave pública**: Certificado digital local que se utilizará para autenticar el dispositivo Citrix ADC local en el mismo nivel antes de establecer asociaciones de seguridad IPSec. El mismo certificado debe estar presente y configurado para el parámetro Peer Public Key en el peer.
       * **Clave privada**: Clave privada del certificado digital local.
       * **Clave pública del mismo nivel**: Certificado digital del mismo nivel. Se utiliza para autenticar el par en el punto final local antes de establecer asociaciones de seguridad IPSec. El mismo certificado debe estar presente y configurado para el parámetro de clave pública en el par.

7. Haga clic en **Done**.

La nueva configuración del túnel de CloudBridge Connector en ambos dispositivos Citrix ADC aparece en la ficha Inicio de la interfaz gráfica de usuario correspondiente. El estado actual del túnel del conector de CloudBridge se indica en el panel Connectors configurados de CloudBridge. Un punto verde indica que el túnel está arriba. Un punto rojo indica que el túnel está caído.

Supervisión del túnel de CloudBridge Connector

Puede supervisar el rendimiento de los túneles de CloudBridge Connector en un dispositivo Citrix ADC mediante contadores estadísticos del túnel de CloudBridge Connector. Para obtener más información sobre cómo mostrar estadísticas de túnel de CloudBridge Connector en un dispositivo Citrix ADC, consulte Supervisión de túneles de CloudBridge Connector.

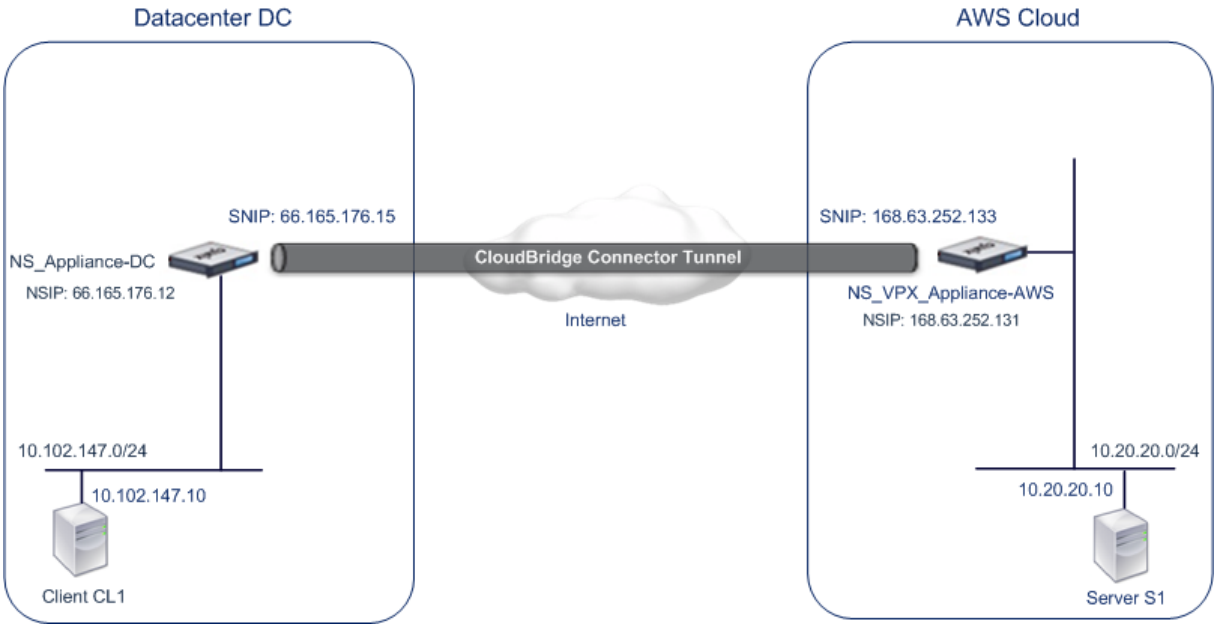
Configuración de CloudBridge Connector entre el centro de datos y la nube de AWS

August 20, 2021

Puede configurar un túnel de CloudBridge Connector entre un centro de datos y la nube de AWS para aprovechar la infraestructura y las capacidades informáticas del centro de datos y la nube de AWS. Con AWS, puede ampliar su red sin inversión inicial de capital ni el coste de mantener la infraestructura de red ampliada. Puede escalar su infraestructura hacia arriba o hacia abajo, según sea necesario. Por ejemplo, puede arrendar más capacidades de servidor cuando aumente la demanda.

Para conectar un centro de datos a la nube de AWS, configure un túnel de CloudBridge Connector entre un dispositivo Citrix ADC que reside en el centro de datos y un dispositivo virtual Citrix ADC (VPX) que reside en la nube de AWS.

Como ilustración de un túnel de CloudBridge Connector entre un centro de datos y la nube de Amazon AWS, considere un ejemplo en el que se configura un túnel de CloudBridge Connector entre el dispositivo Citrix ADC NS_Appliance-DC, en el centro de datos DC y Citrix ADC virtual appliance (VPX) NS_VPX_Appliance-AWS.



Ambos NS_Appliance-DC y NS_VPX_Appliance-AWS funcionan en modo L3. Permiten la comunicación entre redes privadas en el centro de datos DC y la nube de AWS. NS_Appliance-DC y NS_VPX_Appliance-AWS permiten la comunicación entre el cliente CL1 en el DC del centro de datos y el servidor S1 en la nube de AWS a través del túnel CloudBridge Connector. El cliente CL1 y el servidor S1 están en diferentes redes privadas.

> **Nota**:
>
> AWS no admite el modo L2, por lo que es necesario tener solo el modo L3 habilitado en ambos extremos.

Para una comunicación adecuada entre CL1 y S1, el modo L3 está habilitado en NS_Appliance-DC y NS_VPX_Appliance-AWS y las rutas se actualizan como tales:

- CL1 tiene una ruta a NS_Appliance-DC para llegar a S1.
- NS_Appliance-DC tiene una ruta a NS_VPX_Appliance-AWS para llegar a S1.
- S1 debería tener una ruta a NS_VPX_Appliance-AWS para llegar a CL1.
- NS_VPX_Appliance-AWS tiene una ruta a NS_Appliance-DC para llegar a CL1.

En la tabla siguiente se enumeran las opciones de configuración del dispositivo Citrix ADC NS_Appliance-DC en el centro de datos DC.

Entidad	Nombre	Detalles
La dirección NSIP		66.165.176.12
Dirección SNIP		66.165.176.15

Entidad	Nombre	Detalles
Túnel del conector CloudBridge	CC_Tunnel_DC-AWS	Dirección IP del extremo local del túnel del conector de CloudBridge: 66.165.176.15, Dirección IP del extremo remoto del túnel del conector de CloudBridge: 168.63.252.133, Detalles del túnel GRE: Nombre= CC_Tunnel_DC-AWS

En la siguiente tabla se enumeran las configuraciones de Citrix ADC VPX NS_VPX_Appliance-AWS en la nube de AWS.

Entidad	Nombre	Detalles
Dirección NSIP		10.102.25.30
Dirección EIP pública asignada a la dirección NSIP		168.63.252.131
Dirección SNIP		10.102.29.30
Dirección EIP pública asignada a la dirección SNIP		168.63.252.133
Túnel del conector CloudBridge	CC_Tunnel_DC-AWS	Dirección IP del extremo local del túnel del conector de CloudBridge:168.63.252.133, Dirección IP del extremo remoto del túnel del conector de CloudBridge: 66.165.176.15; **Detalles del túnel GRE** Nombre= CC_Tunnel_DC-AWS, Detalles del perfil de IPSec, Nombre= CC_Tunnel_DC-AWS, algoritmo de cifrado = AES, algoritmo de hash = HMAC SHA1

Requisitos previos

Antes de configurar un túnel de CloudBridge Connector, compruebe que se han completado las siguientes tareas:

1. Instale, configure e inicie una instancia de Citrix ADC Virtual Appliance (VPX) en la nube de AWS. Para obtener instrucciones sobre la instalación de Citrix ADC VPX en AWS, consulte Implementación de una instancia Citrix ADC VPX en AWS.
2. Implementar y configurar un dispositivo físico Citrix ADC, o Provisioning y configurar un dispositivo virtual Citrix ADC (VPX) en una plataforma de virtualización en el centro de datos.
3. Asegúrese de que las direcciones IP de punto final del túnel CloudBridge Connector sean accesibles entre sí.

Licencia Citrix ADC VPX

Después del lanzamiento inicial de la instancia, Citrix ADC VPX for AWS requiere una licencia. Si va a traer su propia licencia (BYOL), consulte la Guía de licencias de VPX en: http://support.citrix.com/article/CTX122426.

Es necesario que:

1. Utilice el portal de licencias del sitio web de Citrix para generar una licencia válida.
2. Cargue la licencia en la instancia.

Si se trata de una instancia de mercado de **pago**, no es necesario instalar licencia. El conjunto de funciones y el rendimiento correctos se activarán automáticamente.

Pasos de configuración

Para configurar un túnel de CloudBridge Connector entre un dispositivo Citrix ADC que reside en un centro de datos y un dispositivo virtual Citrix ADC (VPX) que reside en la nube de AWS, utilice la GUI del dispositivo Citrix ADC.

Cuando se utiliza la GUI, la configuración del túnel de CloudBridge Connector creada en el dispositivo Citrix ADC se envía automáticamente al otro punto final o par (Citrix ADC VPX en AWS) del túnel de CloudBridge Connector. Por lo tanto, no es necesario acceder a la GUI (GUI) de Citrix ADC VPX en AWS para crear la configuración de túnel de CloudBridge Connector correspondiente en él.

La configuración del túnel de CloudBridge Connector en ambos pares (el dispositivo Citrix ADC que reside en el centro de datos y el dispositivo virtual Citrix ADC (VPX) que reside en la nube de AWS) consta de las siguientes entidades:

- **Perfil IPSec**: Una entidad de perfil IPSec especifica los parámetros del protocolo IPSec, como la versión IKE, el algoritmo de cifrado, el algoritmo hash y PSK, que utilizará el protocolo IPSec en ambos pares del túnel de CloudBridge Connector.

- **Túnel GRE**: Un túnel IP especifica una dirección IP local (una dirección SNIP pública configurada en el par local), una dirección IP remota (una dirección SNIP pública configurada en el par remoto), un protocolo (GRE) utilizado para configurar el túnel CloudBridge Connector y una entidad de perfil IPSec.
- **Cree una regla PBR y asocie el túnel IP a ella**: Una entidad PBR especifica un conjunto de condiciones y una entidad de túnel IP. El intervalo de direcciones IP de origen y el intervalo IP de destino son las condiciones para la entidad PBR. Debe establecer el intervalo de direcciones IP de origen y el intervalo de direcciones IP de destino para especificar la subred cuyo tráfico va a atravesar el túnel del conector de CloudBridge. Por ejemplo, considere un paquete de solicitud que se origina en un cliente de la subred del centro de datos y está destinado a un servidor de la subred en la nube de AWS. Si este paquete coincide con el intervalo de direcciones IP de origen y destino de la entidad PBR en el dispositivo Citrix ADC en el centro de datos, se envía a través del túnel CloudBridge Connector asociado a la entidad PBR.

Para crear un perfil IPSEC mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

- `add ipsec profile <name> [-**ikeVersion** (V1 | V2)] [-**encAlgo** (AES | 3DES)...] [-**hashAlgo** <hashAlgo> ...] [-**lifetime** <positive_integer>] (-**psk** | (-**publickey** <string> -**privatekey** <string> -**peerPublicKey** <string>))[-**livenessCheckInterval** <positive_integer>] [-**replayWindowSize** <positive_integer>] [-**ikeRetryInterval** <positive_integer>] [-**retransmissiontime** <positive_integer>]`
- `**show ipsec profile** <name>`

Para crear un túnel IP y enlazar el perfil IPSEC mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

- `add ipTunnel <name> <remote><remoteSubnetMask> <local> [-protocol <protocol>] [-ipsecProfileName <string>]`
- `show ipTunnel <name>`

Para crear una regla PBR y enlazar el túnel IPSEC con ella mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

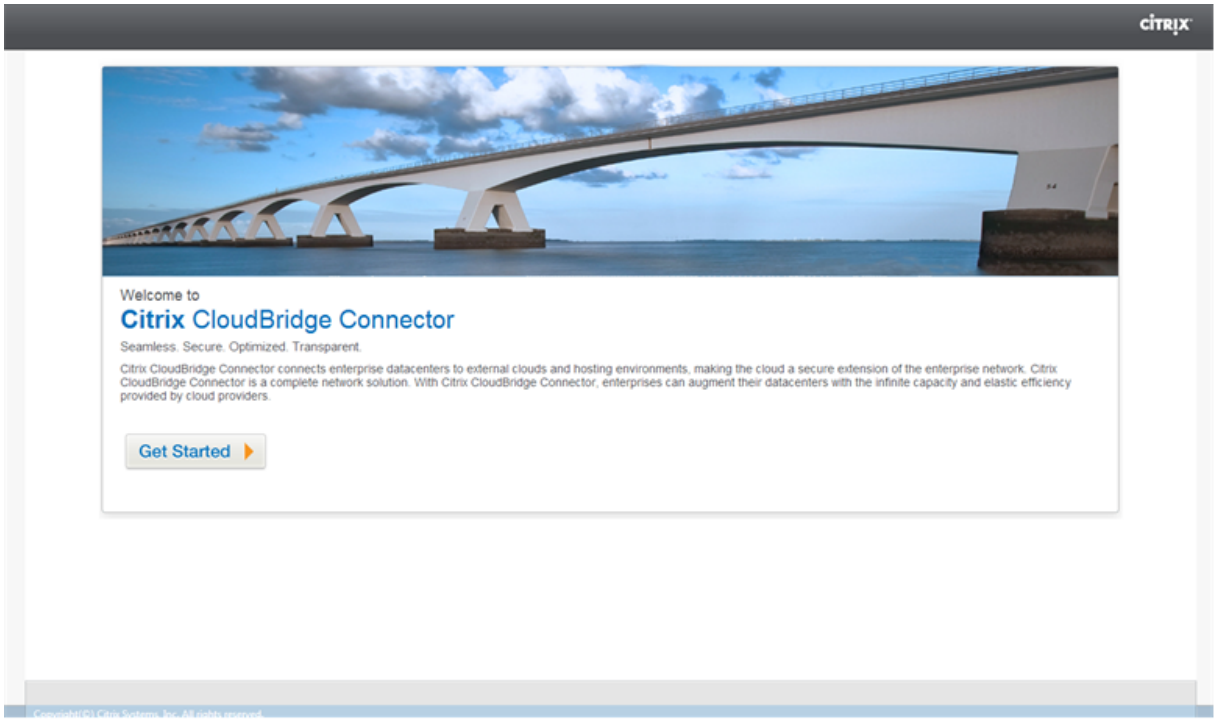
- `add ns pbr <pbr_name> ALLOW -srcIP = <local_subnet_range> -destIP = <remote_subnet_range> -ipTunnel <tunnel_name>`
- `apply ns pbrs`
- `show ns pbr <pbr_name>`

Ejemplo


```
1      > add ipsec profile CC_Tunnel_DC-AWS -encAlgo AES -hashAlgo
          HMAC_SHA1
2
3      Done
4      > add ipTunnel CC_Tunnel_DC-AWS 168.63.252.133 255.255.255.0
          66.165.176.15  - protocol GRE -ipsecProfileName CC_Tunnel_DC-AWS
5
6      Done
7      > add ns pbr PBR-DC-AWS ALLOW  - srcIP 66.165.176.15  - destIP
          168.63.252.133 ipTunnel CC_Tunnel_DC-AWS
8
9      Done
10     > apply ns pbrs
11
12     Done
13 <!--NeedCopy-->
```

Para configurar un túnel de CloudBridge Connector en un dispositivo Citrix ADC mediante la interfaz gráfica de usuario

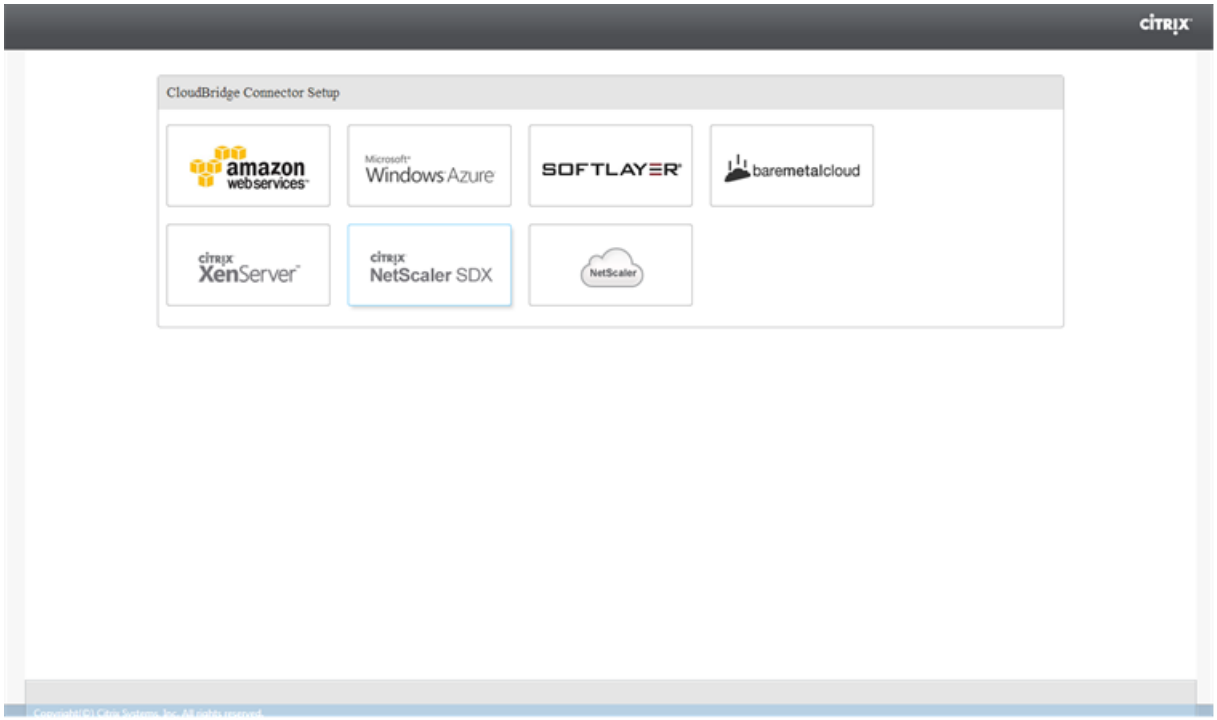
1. Escriba la dirección NSIP de un dispositivo Citrix ADC en la línea de direcciones de un explorador web.
2. Inicie sesión en la GUI del dispositivo Citrix ADC mediante las credenciales de cuenta del dispositivo.
3. Vaya a **Sistema** > **Conector de CloudBridge**.
4. En el panel derecho, en **Introducción**, haga clic en **Crear/Supervisar CloudBridge**.
5. La primera vez que configure un túnel de CloudBridge Connector en el dispositivo, aparece una pantalla de **bienvenida**.
6. En la **pantalla de bienvenida**, haga clic en **Introducción**.



Nota:

Si ya tiene configurado un túnel de CloudBridge Connector en el dispositivo Citrix ADC, la pantalla de bienvenida no aparece, por lo que no hace clic en Comenzar.

1. En el panel **Configuración de CloudBridge Connector**, haga clic en **amazon web services**



1. En el panel **Amazon**, proporcione las credenciales de su cuenta de AWS: ID de clave de acceso de AWS y clave de acceso secreta de AWS. Puede obtener estas claves de acceso desde la consola GUI de AWS. Haga clic en **Continuar**.

> **Nota**
>
> Anteriormente, el asistente de configuración siempre se conecta a la misma región de AWS incluso cuando se selecciona otra región. Como resultado, la configuración del túnel de CloudBridge Connector en un dispositivo Citrix ADC VPX que se ejecuta en la región de AWS seleccionada solía fallar. Este problema se ha solucionado ahora.

1. En el panel **Citrix ADC**, seleccione la dirección NSIP del dispositivo virtual Citrix ADC que se ejecuta en AWS. A continuación, proporcione las credenciales de su cuenta para el dispositivo virtual Citrix ADC. Haga clic en **Continuar**.
2. En el panel **Configuración del conector de CloudBridge**, establezca el siguiente parámetro:
   - **CloudBridge Connector Name**: Nombre para la configuración de CloudBridge Connector en el dispositivo local. Debe comenzar con un carácter alfabético ASCII o de subrayado (_) y debe contener solo caracteres alfanuméricos ASCII, guión bajo, hash (#), punto (.), espacio, dos puntos (:), en (@), igual (=) y guión (-). No se puede cambiar después de crear la configuración de CloudBridge Connector.
3. En **Configuración local**, establezca el siguiente parámetro:
   - **IP de subred**: Dirección IP del extremo local del túnel de CloudBridge Connector. Debe ser una dirección IP pública del tipo SNIP.
4. En **Configuración remota**, establezca el siguiente parámetro:
   - **IP de subred**: Dirección IP del punto final del túnel de CloudBridge Connector en el lado de AWS. Debe ser una dirección IP del tipo SNIP en la instancia de Citrix ADC VPX en AWS.
   - **NAT**: Dirección IP pública (EIP) en AWS que se asigna al SNIP configurado en la instancia de Citrix ADC VPX en AWS.
5. En **Configuración de PBR**, establezca los siguientes parámetros:
   - **Operación**: El igual (=) o no es igual a (! =) operador lógico.
   - **IP de origen bajo**: La dirección IP de origen más baja para que coincida con la dirección IP de origen de un paquete IPv4 saliente.
   - **IP de origen alto**: La dirección IP de origen más alta que debe coincidir con la dirección IP de origen de un paquete IPv4 saliente.
   - **Operación**: El igual (=) o no es igual a (! =) operador lógico.
   - Dirección**IP de destino baja**: La dirección IP de destino más baja para que coincida con la dirección IP de destino de un paquete IPv4 saliente.
   - Dirección**IP de destino alta**: La dirección IP de destino más alta que debe coincidir con la dirección IP de destino de un paquete IPv4 saliente.

6. (Opcional) En **Configuración de seguridad**, establezca los siguientes parámetros de protocolo IPSec para el túnel de CloudBridge Connector:
    - **Algoritmo**de cifrado: Algoritmo de cifrado que utilizará el protocolo IPSec en el túnel de CloudBridge.
    - **Algoritmo hash**: Algoritmo hash que utilizará el protocolo IPSec en el túnel CloudBridge.
    - **Clave**: Seleccione uno de los siguientes métodos de autenticación IPSec que los dos pares utilizarán para autenticarse mutuamente.
        - **Generación automática de clave**: Autenticación basada en una cadena de texto, denominada clave previamente compartida (PSK), generada automáticamente por el dispositivo local. Las claves PSK de los pares se comparan entre sí para la autenticación.
        - **Clave específica**: Autenticación basada en un PSK introducido manualmente. Los PSK de los pares se comparan entre sí para la autenticación.
            * **Clave de seguridad precompartida**: la cadena de texto introducida para la autenticación basada en clave previamente compartida.
        - **Cargar certificados**: Autenticación basada en certificados digitales.
            * **Clave pública**: Certificado digital local que se utilizará para autenticar el peer local al peer remoto antes de establecer asociaciones de seguridad IPSec. El mismo certificado debe estar presente y configurado para el parámetro Peer Public Key en el peer.
            * **Clave privada**: Clave privada del certificado digital local.
            * **Clave pública del mismo nivel**: Certificado digital del mismo nivel. Se utiliza para autenticar el par en el punto final local antes de establecer asociaciones de seguridad IPSec. El mismo certificado debe estar presente y configurado para el parámetro de clave pública en el par.
7. Haga clic en **Done**.

La nueva configuración del túnel de CloudBridge Connector en el dispositivo Citrix ADC en el centro de datos aparece en la ficha Inicio de la GUI. La nueva configuración de túnel de CloudBridge Connector correspondiente en el dispositivo Citrix ADC VPX en la nube de AWS aparece en la GUI. El estado actual del túnel del conector de CloudBridge se indica en el panel Configurado de CloudBridge. Un punto verde indica que el túnel está arriba. Un punto rojo indica que el túnel está caído.

Supervisión del túnel de CloudBridge Connector

Puede supervisar el rendimiento de los túneles de CloudBridge Connector en un dispositivo Citrix ADC mediante contadores estadísticos del túnel de CloudBridge Connector. Para obtener más información sobre cómo mostrar estadísticas de túnel de CloudBridge Connector en un dispositivo Citrix ADC, consulte Supervisión de túneles de CloudBridge Connector.

Configuración de un túnel de CloudBridge Connector entre un dispositivo Citrix ADC y una Gateway privada virtual en AWS

October 5, 2021

Para conectar un centro de datos a Amazon Web Services (AWS), puede configurar un túnel de CloudBridge Connector entre un dispositivo Citrix ADC en el centro de datos y una Gateway privada virtual en AWS. El dispositivo Citrix ADC y la Gateway privada virtual forman los extremos del túnel CloudBridge Connector y se denominan pares.

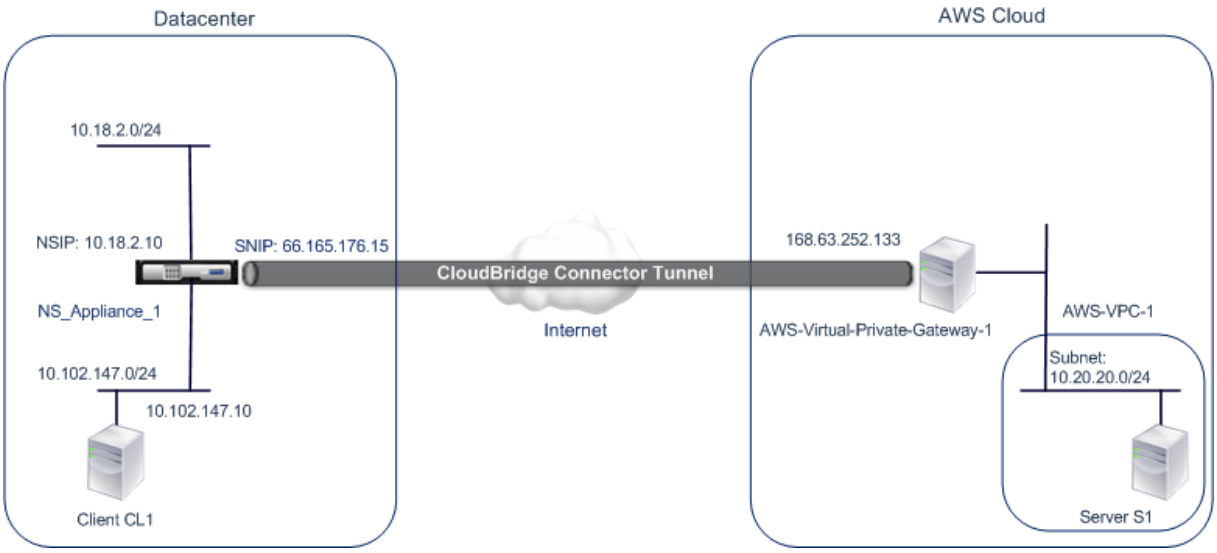
> **Nota:**
>
> También puede configurar un túnel de CloudBridge Connector entre un dispositivo Citrix ADC en un centro de datos y una instancia de Citrix ADC VPX (en lugar de una Gateway privada virtual) en AWS. Para obtener más información, consulte Configuración de CloudBridge Connector entre el centro de datos y la nube de AWS.

Las puertas de enlace privadas virtuales de AWS admiten la siguiente configuración de IPSec para un túnel de CloudBridge Connector. Por lo tanto, debe especificar la misma configuración de IPSec al configurar el dispositivo Citrix ADC para el túnel de CloudBridge Connector.

Propiedades IPSec	Configuración
Modo IPSec	Modo túnel
Versión de IKE	Versión 1
Método de autenticación IKE	Clave previamente compartida
Algoritmo de cifrado	AES
Algoritmo hash	HMAC SHA1

Ejemplo de configuración del túnel de CloudBridge Connector y flujo de datos

Como ejemplo del flujo de tráfico en un túnel de CloudBridge Connector, considere un ejemplo en el que se configura un túnel de CloudBridge Connector entre el dispositivo Citrix ADC NS_Appliance-1 en un centro de datos y la Gateway privada virtual AWS-Virtual-Private-Gateway-1 en la nube de AWS.



NS_Appliance-1 también funciona como enrutador L3, lo que permite que una red privada del centro de datos llegue a una red privada en la nube de AWS a través del túnel CloudBridge Connector. Como router, NS_Appliance-1 permite la comunicación entre el cliente CL1 en el centro de datos y el servidor S1 en la nube de AWS a través del túnel CloudBridge Connector. El cliente CL1 y el servidor S1 están en diferentes redes privadas.

En NS_Appliance-1, la configuración del túnel de CloudBridge Connector incluye una entidad de perfil IPSec denominada NS_AWS_IPSEC_Profile, una entidad de túnel de CloudBridge Connector denominada NS_AWS_Tunnel y una entidad de redirección basada en directivas (PBR) denominada NS_AWS_PBR.

La entidad de perfil IPSec NS_AWS_IPSEC_PROFILE especifica los parámetros del protocolo IPSec, como la versión IKE, el algoritmo de cifrado y el algoritmo hash, que utilizará el protocolo IPSec en el túnel del conector de CloudBridge. NS_AWS_IPSEC_Profile está enlazado a la entidad de túnel IP NS_AWS_Tunnel.

La entidad de túnel del conector de CloudBridge NS_AWS_Tunnel especifica la dirección IP local (una dirección IP pública —SNIP configurada en el dispositivo Citrix ADC), la dirección IP remota (la dirección IP del AWS-Virtual-Private-gateway-1) y el protocolo (IPSec) utilizado para configurar el túnel del conector de CloudBridge. NS_AWS_Tunnel está enlazado a la entidad de redirección basada en directivas (PBR) NS_AWS_PBR.

La entidad PBR NS_AWS_PBR especifica un conjunto de condiciones y una entidad de túnel CloudBridge Connector (NS_AWS_Tunnel). El intervalo de direcciones IP de origen y el intervalo de direcciones IP de destino son las condiciones para NS_AWS_PBR. El intervalo de direcciones IP de origen y el intervalo de direcciones IP de destino se especifican como una subred en el centro de datos y una subred en la nube de AWS, respectivamente. Cualquier paquete de solicitud procedente de un cliente de la subred del centro de datos y destinado a un servidor de la subred de la nube de AWS coincide con las condiciones de NS_AWS_PBR. Este paquete se considera entonces para el procesamiento

de CloudBridge Connector y se envía a través del túnel de CloudBridge Connector (NS_AWS_Tunnel) vinculado a la entidad PBR.

En la tabla siguiente se enumeran los parámetros utilizados en este ejemplo.

Dirección IP del punto final del túnel de CloudBridge Connector (NS_Appliance-1) en el lado del centro de datos	66.165.176.15
Dirección IP del punto final del túnel de CloudBridge Connector (AWS-Virtual-Private-Gateway-1) en AWS	168.63.252.133
Subred del centro de datos, cuyo tráfico debe atravesar el túnel del conector de CloudBridge	10.102.147.0/24
Subred de AWS, cuyo tráfico es atravesar el túnel de CloudBridge Connector	10.20.20.0/24

Configuración de Amazon AWS

		Redirección = estática, dirección IP = dirección IP del extremo del túnel del conector CloudBridge Routable a través de Internet en el lado Citrix ADC = 66.165.176.15
Puerta de enlace del cliente	AWS-Customer-Gateway-1	
Puerta de enlace privada virtual	AWS-Virtual-Private-Gateway-1	VPC asociada = AWS-VPC-1
Conexión VPN	AWS-VPN-Connection-1	Puerta de enlace del cliente = AWS-Customer-gateway-1, Puerta de enlace privada virtual= Puerta de enlace virtual-privada-1, Opciones de redirección: Tipo = Prefijos de IP estáticos y estáticos = Subredes en el lado Citrix ADC = 10.102.147.0/24

Configuración del dispositivo Citrix ADC NS_Appliance-1 en Datacenter-1:

Dispositivo	Parámetros	
SNIP1 (solo para fines de referencia)	66.165.176.15	
IPSec profile	NS_AWS_IPSec_Profile	IKE version = v1, Encryption algorithm = AES, Hash algorithm = HMAC SHA1
CloudBridge Connector tunnel	NS_AWS_Tunnel	Remote IP = 168.63.252.133, Local IP= 66.165.176.15, Tunnel protocol = IPSec, IPSec profile= NS_AWS_IPSec_Profile
Policy based route	NS_AWS_Pbr	Source IP range = Subnet in the datacenter =10.102.147.0-10.102.147.255, Destination IP range =Subnet in AWS =10.20.20.0-10.20.20.255, IP Tunnel = NS_AWS_Tunnel

Puntos a tener en cuenta para una configuración de túnel de CloudBridge Connector

Antes de configurar un túnel de CloudBridge Connector entre un dispositivo Citrix ADC y una Gateway de AWS, tenga en cuenta los siguientes puntos:

1. AWS admite la siguiente configuración de IPSec para un túnel de CloudBridge Connector. Por lo tanto, debe especificar la misma configuración de IPSec al configurar el dispositivo Citrix ADC para el túnel de CloudBridge Connector.
    - Versión IKE = v1
    - Algoritmo de cifrado = AES
    - Algoritmo hash = HMAC SHA1
2. Debe configurar el firewall en el extremo Citrix ADC para permitir lo siguiente.
    - Cualquier paquete UDP para el puerto 500
    - Cualquier paquete UDP para el puerto 4500
    - Cualquier paquete ESP (protocolo IP número 50)
3. Debe configurar Amazon AWS antes de especificar la configuración del túnel en Citrix ADC, ya que la dirección IP pública del extremo de AWS (Gateway) del túnel y el PSK se generan automáti-

camente al configurar la configuración del túnel en AWS. Necesita esta información para especificar la configuración del túnel en el dispositivo Citrix ADC.

4. AWS Gateway admite rutas estáticas y el protocolo BGP para las actualizaciones de rutas. El dispositivo Citrix ADC no admite el protocolo BGP en un túnel de CloudBridge Connector a la Gateway de AWS. Por lo tanto, se deben utilizar rutas estáticas adecuadas a ambos lados del túnel CloudBridge Connector para enrutar correctamente el tráfico a través del túnel.

Configuración de Amazon AWS para el túnel de CloudBridge Connector

Para crear una configuración de túnel de CloudBridge Connector en Amazon AWS, utilice Amazon AWS Management Console, que es una interfaz gráfica basada en web para crear y administrar recursos en Amazon AWS.

Antes de comenzar la configuración del túnel de CloudBridge Connector en la nube de AWS, asegúrese de que:

- Tiene una cuenta de usuario para la nube de Amazon AWS.
- Tiene una nube privada virtual cuyas redes quiere conectarse a las redes del lado Citrix ADC a través del túnel CloudBridge Connector.
- Está familiarizado con Amazon AWS Management Console.

> **Nota**:
>
> Los procedimientos para configurar Amazon AWS para un túnel de CloudBridge Connector pueden cambiar con el tiempo, dependiendo del ciclo de lanzamiento de Amazon AWS. Citrix recomienda que consulte la documentación de Amazon AWS para obtener los procedimientos más recientes.

Para configurar un túnel de conector de CloudBridge entre un dispositivo Citrix ADC y una Gateway de AWS, realice las siguientes tareas en AWS Management Console:

- **Cree una puerta de enlace de clientes**. Una Gateway del cliente es una entidad de AWS que representa un extremo de túnel de CloudBridge Connector. Para un túnel de CloudBridge Connector entre un dispositivo Citrix ADC y una Gateway de AWS, la Gateway del cliente representa el dispositivo Citrix ADC en AWS. La Gateway del cliente especifica un nombre, el tipo de redirección (estático o BGP) utilizado en el túnel y la dirección IP del extremo del túnel de CloudBridge Connector en el lado Citrix ADC. La dirección IP puede ser una dirección IP de subred (SNIP) propiedad de Citrix ADC enrutable por Internet o, si el dispositivo Citrix ADC está detrás de un dispositivo NAT, una dirección IP NAT enrutable por Internet que represente la dirección SNIP.
- **Cree una puerta de enlace privada virtual y adjúntela a una VPC**. Una Gateway privada virtual es un extremo de túnel de CloudBridge Connector en el lado de AWS. Cuando crea una Gateway privada virtual, le ha asignado un nombre o permite que AWS le asigne el nombre. A continuación, asocie la Gateway privada virtual con una VPC. Esta asociación permite que las

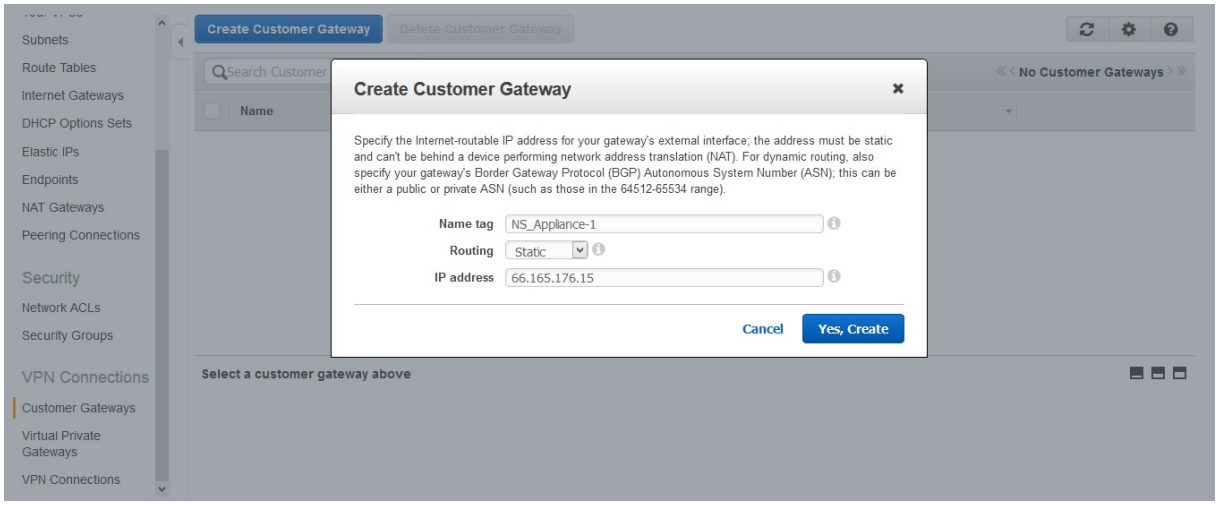
subredes de la VPC se conecten a las subredes del lado Citrix ADC a través del túnel CloudBridge Connector.

- **Cree una conexión VPN**. Una conexión VPN especifica una Gateway de cliente y una Gateway privada virtual entre la que se va a crear un túnel de CloudBridge Connector. También especifica un prefijo IP para las redes en el lado Citrix ADC. Solo los prefijos IP conocidos por la puerta de enlace privada virtual (mediante la entrada de ruta estática) pueden recibir tráfico de la VPC a través del túnel. Además, la Gateway privada virtual no enruta ningún tráfico no destinado a los prefijos IP especificados a través del túnel. Después de configurar una conexión VPN, es posible que tenga que esperar unos minutos para que se cree.
- **Configurar las opciones de redirección**. Para que la red de la VPC llegue a las redes del lado Citrix ADC a través del túnel de CloudBridge Connector, debe configurar la tabla de redirección de la VPC para que incluya rutas para las redes en el lado Citrix ADC y señale esas rutas a la Gateway privada virtual. Puede incluir rutas en la tabla de redirección de una VPC de una de las siguientes maneras:
  - **Habilite la propagación de rutas**. Puede habilitar la propagación de rutas para la tabla de redirección, de modo que las rutas se propaguen automáticamente a la tabla. Los prefijos IP estáticos que especifique para la configuración VPN se propagan a la tabla de redirección después de crear la conexión VPN.
  - **Introduzca manualmente rutas estáticas**. Si no habilita la propagación de rutas, debe introducir manualmente las rutas estáticas para las redes en el lado Citrix ADC.
- **Configuración de descarga**. Una vez creada la configuración del túnel de CloudBridge Connector (conexión VPN) en AWS, descargue el archivo de configuración de la conexión VPN en su sistema local. Es posible que necesite la información del archivo de configuración para configurar el túnel de CloudBridge Connector en el dispositivo Citrix ADC.

Para crear una Gateway de cliente

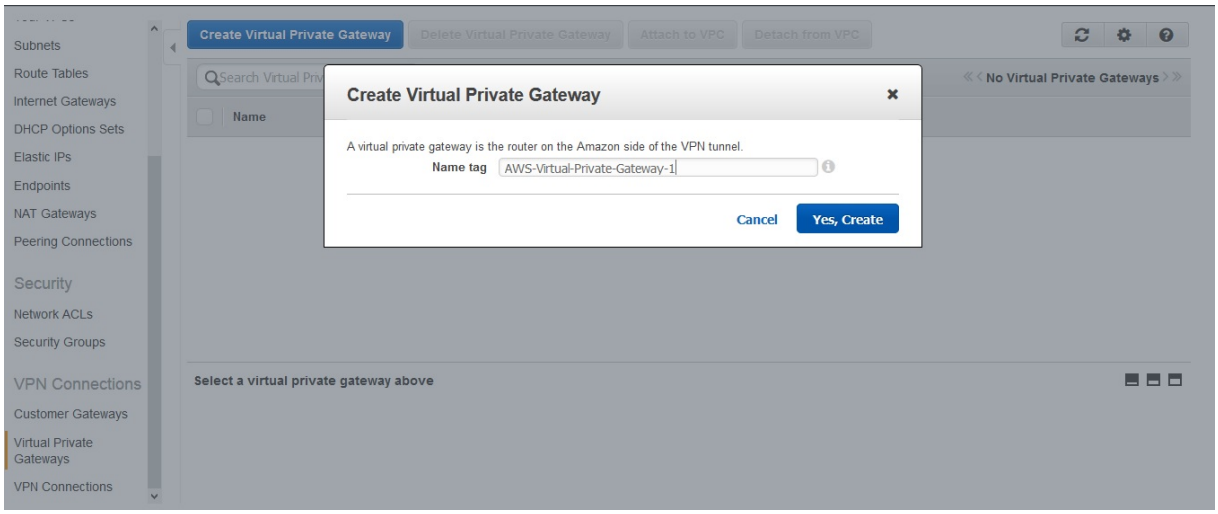
1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. Vaya a **Conexiones VPN** > **Puertas de enlace del cliente** y haga clic en **Crear puerta de enlace del cliente**.
3. En el cuadro de diálogo **Crear puerta de enlace de cliente**, establezca los parámetros siguientes y, a continuación, haga clic en **Sí, crear**:
   - **Etiqueta de nombre**. Un nombre para la Gateway del cliente.
   - **Lista de rutas**. Tipo de redirección entre el dispositivo Citrix ADC y la Gateway privada virtual de AWS para las rutas publicitarias entre sí a través del túnel CloudBridge Connector. Seleccione **Redirección estática** en la lista **Redirección**. **Nota**: El dispositivo Citrix ADC no admite el protocolo BGP en un túnel de CloudBridge Connector a AWS Gateway. Por lo tanto, se deben utilizar rutas estáticas adecuadas a ambos lados del túnel CloudBridge Connector para enrutar correctamente el tráfico a través del túnel.
   - **Dirección IP**. Dirección IP del extremo del túnel de CloudBridge Connector enrutable a Internet en el lado Citrix ADC. La dirección IP puede ser una dirección IP de subred (SNIP)

propiedad de Citrix ADC enrutable por Internet o, si el dispositivo Citrix ADC está detrás de un dispositivo NAT, una dirección IP NAT enrutable por Internet que represente la dirección SNIP.

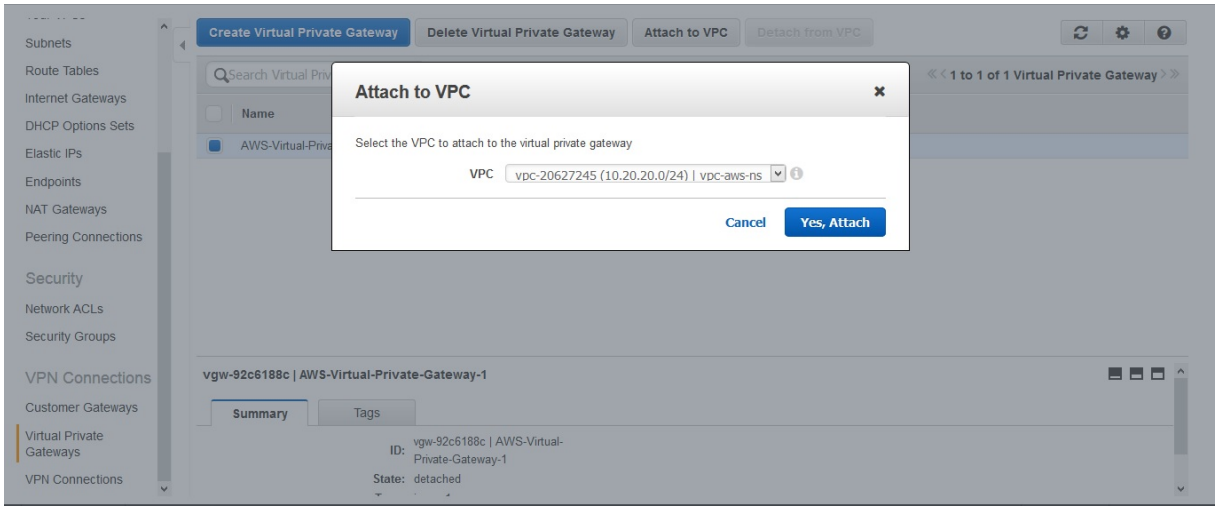


Para crear una Gateway privada virtual y adjuntarla a una VPC

1. Vaya a **Conexiones VPN** > **Puertas de enlace privadas virtuales** y, a continuación, haga clic en Crear puerta de enlace privada virtual.
2. Escriba un nombre para la Gateway privada virtual y, a continuación, haga clic en Sí, Crear.

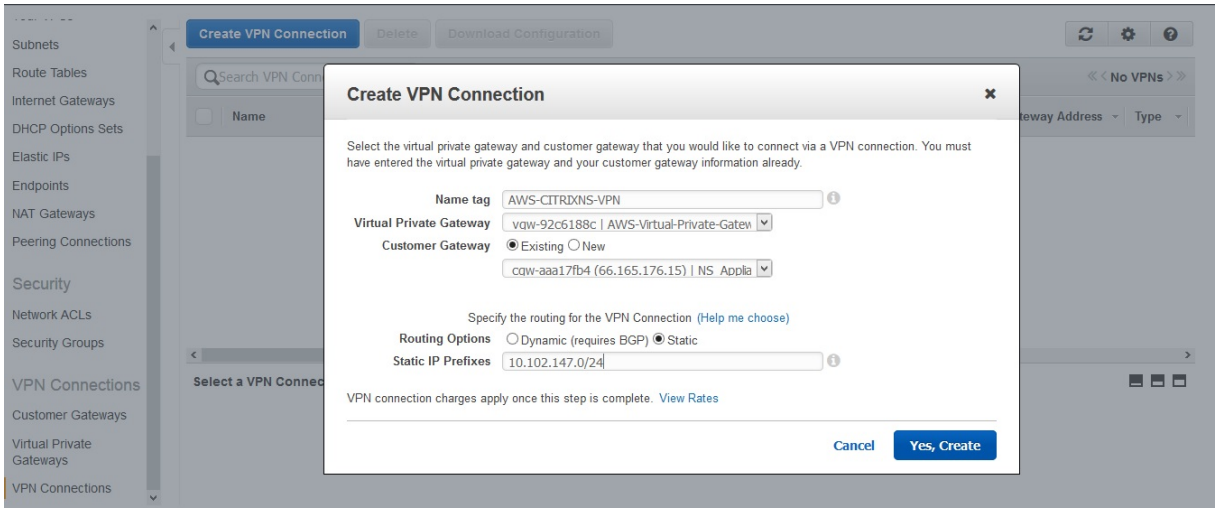


1. Seleccione la Gateway privada virtual que creó y, a continuación, haga clic en Adjuntar a VPC.
2. En el cuadro de diálogo Adjuntar a VPC, seleccione la VPC de la lista y, a continuación, elija Sí, Adjuntar.



Para crear una conexión VPN:

1. Vaya a Conexiones VPN > Conexiones VPN y, a continuación, haga clic en Crear conexión VPN.
2. En el cuadro de diálogo Crear conexión VPN, establezca los siguientes parámetros y, a continuación, elija Sí, Crear:
   - **Etiqueta de nombre**. Nombre para la conexión VPN.
   - Puerta de**enlace privada virtual**. Seleccione la Gateway privada virtual que creó anteriormente.
   - **Puerta de enlace del cliente**. Seleccione Existente. A continuación, en la lista desplegable, seleccione la Gateway del cliente que creó anteriormente.
   - **Opciones de redirección**. Tipo de redirección entre la Gateway privada virtual y la Gateway del cliente (dispositivo Citrix ADC). Seleccione Estático. En el campo Prefijos de IP estáticos, especifique los prefijos IP para la subred en el lado Citrix ADC, separados por comas.



Para habilitar la propagación de rutas:

1. Desplácese hasta **Tablas de ruta** y seleccione la tabla de redirección asociada a la subred cuyo tráfico va a atravesar el túnel de CloudBridge Connector.

> **Nota**
>
> De forma predeterminada, esta es la tabla de redirección principal para la VPC.

1. En la ficha **Propagación de rutas** del panel de detalles, elija **Modificar**, seleccione la puerta de enlace privada virtual y, a continuación, elija **Guardar**.

Para introducir manualmente rutas estáticas:

1. Desplácese hasta **Tablas de redirección** y seleccione la tabla de redirección.
2. En la ficha **Rutas**, haga clic en **Modificar**.
3. En el campo **Destino**, introduzca la ruta estática utilizada por el túnel del conector de CloudBridge (conexión VPN).
4. Seleccione el ID de Gateway privada virtual en la lista **Destino** y, a continuación, haga clic en **Guardar**.

Para descargar el archivo de configuración:

1. Vaya a **Conexión VPN**, seleccione una conexión VPN y, a continuación, haga clic en **Descargar configuración**.
2. En el cuadro de diálogo **Configuración de descarga**, establezca los parámetros siguientes y, a continuación, haga clic en **Sí, descargar**.
   - **Vendedor**. Seleccione **Genérico**.
   - **Plataforma**. Seleccione **Genérico**.
   - **Software**. Seleccione **el proveedor independiente**.

Configuración del dispositivo Citrix ADC para el túnel de CloudBridge Connector

Para configurar un túnel de CloudBridge Connector entre un dispositivo Citrix ADC y una Gateway privada virtual en la nube de AWS, realice las siguientes tareas en el dispositivo Citrix ADC.
Puede utilizar la línea de comandos Citrix ADC o la GUI.

- **Cree un perfil IPSec**. Una entidad de perfil IPSec especifica los parámetros del protocolo IPSec, como la versión IKE, el algoritmo de cifrado, el algoritmo hash y PSK que utilizará el protocolo IPSec en el túnel de CloudBridge Connector.
- **Cree un túnel IP que utilice el protocolo IPSec y asocie el perfil IPSec con él**. Un túnel IP especifica la dirección IP local (una dirección SNIP configurada en el dispositivo Citrix ADC), la dirección IP remota (la dirección IP pública de la Gateway privada virtual en AWS), el protocolo (IPSec) utilizado para configurar el túnel CloudBridge Connector y una entidad de perfil IPSec. La entidad de túnel IP creada también se denomina entidad de túnel CloudBridge Connector.

- **Cree una regla PBR y asociarla con el túnel IP**. Una entidad PBR especifica un conjunto de reglas y una entidad de túnel IP (túnel CloudBridge Connector). El intervalo de direcciones IP de origen y el intervalo de direcciones IP de destino son las condiciones para la entidad PBR. Establezca el intervalo de direcciones IP de origen para especificar la subred del lado de Citrix ADC cuyo tráfico va a atravesar el túnel y establezca el intervalo de direcciones IP de destino para especificar la subred de AWS VPC cuyo tráfico va a atravesar el túnel de CloudBridge Connector. Cualquier paquete de solicitud que se origina en un cliente de la subred del lado Citrix ADC y esté destinado a un servidor de la subred de la nube de AWS y que coincida con el rango IP de origen y destino de la entidad PBR, se envía a través del túnel de CloudBridge Connector asociado a la entidad PBR.

Para crear un perfil IPSEC mediante la línea de comandos de Citrix ADC

En el símbolo del sistema, escriba:

- `add ipsec profile <name> -psk <string> -**ikeVersion** v1`
- `show ipsec profile** <name>`

Para crear un túnel IPSEC y enlazar el perfil IPSEC con él mediante la línea de comandos de Citrix ADC

En el símbolo del sistema, escriba:

- `add ipTunnel <name> <remote> <remoteSubnetMask> <local> -protocol IPSEC -ipsecProfileName <string>`
- `show ipTunnel <name>`

Para crear una regla PBR y enlazar el túnel IPSEC con ella mediante la línea de comandos de Citrix ADC

En el símbolo del sistema, escriba:

- `add pbr <pbrName> ALLOW -srcIP <subnet-range> -destIP** <subnet-range> -*ipTunnel <tunnelName>`
- `apply pbrs`
- `show pbr <pbrName>`

Los siguientes comandos crean toda la configuración del dispositivo Citrix ADC NS_Appliance-1 utilizado en “Ejemplo de configuración y flujo de datos de CloudBridge Connector.”

```
1     > add ipsec profile NS_AWS_IPSec_Profile -psk
          DkiMgMdcbqvYREEuIvxsbKkW0Foyabcd -ikeVersion v1 - lifetime
          31536000
2     Done
3     > add iptunnel NS_AWS_Tunnel 168.63.252.133 255.255.255.255
          66.165.176.15 - protocol IPSEC - ipsecProfileName
          NS_AWS_IPSec_Profile
4
```



```
5      Done
6      > add pbr NS_AWS_Pbr -srcIP 10.102.147.0-10.102.147.255 - destIP
           10.20.0.0-10.20.255.255 - ipTunnel NS_AWS_Tunnel
7      Done
8
9      > apply pbrs
10
11     Done
12 <!--NeedCopy-->
```

Para crear un perfil IPSEC mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **Conector de CloudBridge** > **Perfil IPSec**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En el cuadro de diálogo **Agregar perfil IPSec**, defina los siguientes parámetros:
   - Nombre
   - Algoritmo de cifrado
   - Algoritmo hash
   - Versión del protocolo IKE (seleccione V1)
4. Seleccione el método de **autenticación de clave previamente compartida** y establezca el parámetro **Claves previamente compartidas**.
5. Haga clic en **Crear** y, a continuación, en **Cerrar**.

Para crear un túnel IP y enlazar el perfil IPSEC con él mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **Conector de CloudBridge** > **Túneles IP**.
2. En la ficha **Túneles IPv4**, haga clic en Agregar.
3. En el cuadro de diálogo **Agregar túnel IP**, establezca los siguientes parámetros:
   - Nombre
   - IP remota
   - Máscara remota
   - Tipo de IP local (en la lista desplegable Tipo de IP local, seleccione IP de subred).
   - IP local (todas las direcciones IP configuradas del tipo IP seleccionado se encuentran en la lista desplegable de IP local. Seleccione la IP deseada de la lista.)
   - Protocolo
   - Perfil IPSec
4. Haga clic en **Crear** y, a continuación, en **Cerrar**.

Para crear una regla PBR y enlazar el túnel IPSEC con ella mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **Red** > **PBR**.

2. En la ficha **PBR**, haga clic en **Agregar**.
3. En el cuadro de diálogo **Crear PBR**, defina los parámetros siguientes:
    - Nombre
    - Action
    - Tipo de salto siguiente (Seleccionar túnel IP)
    - Nombre del túnel IP
    - IP de origen bajo
    - IP de origen alto
    - IP de destino bajo
    - IP de destino alto
4. Haga clic en **Crear** y, a continuación, en **Cerrar**.

La nueva configuración de túnel de CloudBridge Connector correspondiente en el dispositivo Citrix ADC aparece en la GUI.

El estado actual del túnel del conector de CloudBridge se muestra en el panel Connector configurado de CloudBridge. Un punto verde indica que el túnel está arriba. Un punto rojo indica que el túnel está caído.

Supervisión del túnel de CloudBridge Connector

Puede supervisar el rendimiento de los túneles de CloudBridge Connector en un dispositivo Citrix ADC mediante contadores estadísticos del túnel de CloudBridge Connector.
Para obtener más información sobre cómo mostrar estadísticas de túnel de CloudBridge Connector en un dispositivo Citrix ADC, consulte Supervisión de túneles de CloudBridge Connector.

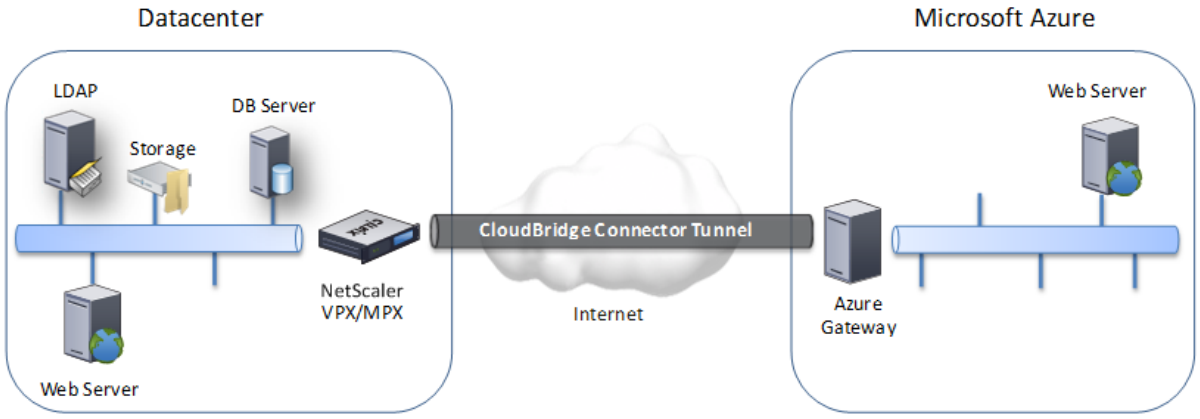
Configuración de un túnel de CloudBridge Connector entre un centro de datos y la nube de Azure

June 2, 2022

El dispositivo Citrix ADC proporciona conectividad entre los centros de datos empresariales y el proveedor de alojamiento en la nube de Microsoft, Azure, lo que convierte a Azure en una extensión perfecta de la red empresarial. Citrix ADC cifra la conexión entre el centro de datos empresarial y la nube de Azure para que todos los datos transferidos entre ambos sean seguros.

Cómo funciona el túnel de CloudBridge Connector

Para conectar un centro de datos a la nube de Azure, configure un túnel de CloudBridge Connector entre un dispositivo Citrix ADC que reside en el centro de datos y una Gateway que reside en la nube de Azure. El dispositivo Citrix ADC en el centro de datos y la Gateway en la nube de Azure son los puntos finales del túnel de CloudBridge Connector y se denominan pares del túnel de CloudBridge Connector.



Un túnel de CloudBridge Connector entre un centro de datos y la nube de Azure utiliza el conjunto de protocolos de seguridad de protocolo Internet (IPSec) de estándar abierto, en modo túnel, para proteger las comunicaciones entre pares en el túnel de CloudBridge Connector. En un túnel de CloudBridge Connector, IPSec garantiza:

- Integridad de los datos
- Autenticación de origen de datos
- Confidencialidad de los datos (cifrado)
- Protección contra ataques de repetición

IPSec utiliza el modo de túnel en el que se cifra y, a continuación, se encapsula el paquete IP completo. El cifrado utiliza el protocolo Encapsulating Security Payload (ESP), que garantiza la integridad del paquete mediante una función hash HMAC y garantiza la confidencialidad mediante un algoritmo de cifrado. El protocolo ESP, después de cifrar la carga útil y calcular el HMAC, genera un encabezado ESP y lo inserta antes del paquete IP cifrado. El protocolo ESP también genera un remolque ESP y lo inserta al final del paquete.

A continuación, el protocolo IPSec encapsula el paquete resultante agregando un encabezado IP antes del encabezado ESP. En el encabezado IP, la dirección IP de destino se establece en la dirección IP del par CloudBridge Connecter.

Los pares del túnel de CloudBridge Connector utilizan el protocolo de intercambio de claves de Internet versión 1 (IKEv1) (parte del conjunto de protocolos IPSec) para negociar la comunicación segura, como se indica a continuación:

1. Los dos pares se autentican mutuamente, mediante la autenticación de clave previamente com-

partida, en la que los pares intercambian una cadena de texto denominada clave previamente compartida (PSK). Las claves previamente compartidas se comparan entre sí para la autenticación. Por lo tanto, para que la autenticación sea correcta, debe configurar la misma clave previamente compartida en cada uno de los pares.

2. A continuación, los pares negocian para llegar a un acuerdo sobre:

   - Un algoritmo de cifrado
   - Claves criptográficas para cifrar datos en un par y descifrarlos en el otro.

   Este acuerdo sobre el protocolo de seguridad, el algoritmo de cifrado y las claves criptográficas se denomina Asociación de Seguridad (SA). Las SA son unidireccionales (simplex). Por ejemplo, cuando se configura un túnel de CloudBridge Connector entre un dispositivo Citrix ADC en un centro de datos y una Gateway en una nube de Azure, tanto el dispositivo del centro de datos como la Gateway de Azure tienen dos SA. Una SA se utiliza para procesar paquetes de salida y la otra SA se utiliza para procesar paquetes de entrada. Las SA caducan después de un intervalo de tiempo especificado, que se denomina duración.

Ejemplo de configuración del túnel de CloudBridge Connector y flujo de datos

Como ilustración de CloudBridge Connector Tunnel, considere un ejemplo en el que se configura un túnel de CloudBridge Connector entre el dispositivo CB_Appliance-1 de Citrix ADC en un centro de datos y una Gateway Azure_Gateway-1 en la nube de Azure.

CB_Appliance-1 también funciona como un enrutador L3, lo que permite que una red privada en el centro de datos llegue a una red privada en la nube de Azure a través del túnel CloudBridge Connector. Como enrutador, CB_Appliance-1 permite la comunicación entre el cliente CL1 en el centro de datos y el servidor S1 en la nube de Azure a través del túnel CloudBridge Connector. El cliente CL1 y el servidor S1 están en diferentes redes privadas.

En CB_Appliance-1, la configuración del túnel de CloudBridge Connector incluye una entidad de perfil IPSec denominada CB_Azure_IPSEC_Profile, una entidad de túnel de CloudBridge Connector denominada CB_Azure_Tunnel y una entidad de redirección basada en directivas (PBR) denominada CB_Azure_PBR.

La entidad de perfil IPSec CB_Azure_IPSec_Profile especifica los parámetros del protocolo IPSec, como la versión IKE, el algoritmo de cifrado y el algoritmo hash, que utilizará el protocolo IPSec en el túnel del conector de CloudBridge. CB_Azure_IPSec_Profile está enlazado a la entidad de túnel IP CB_Azure_tunnel.

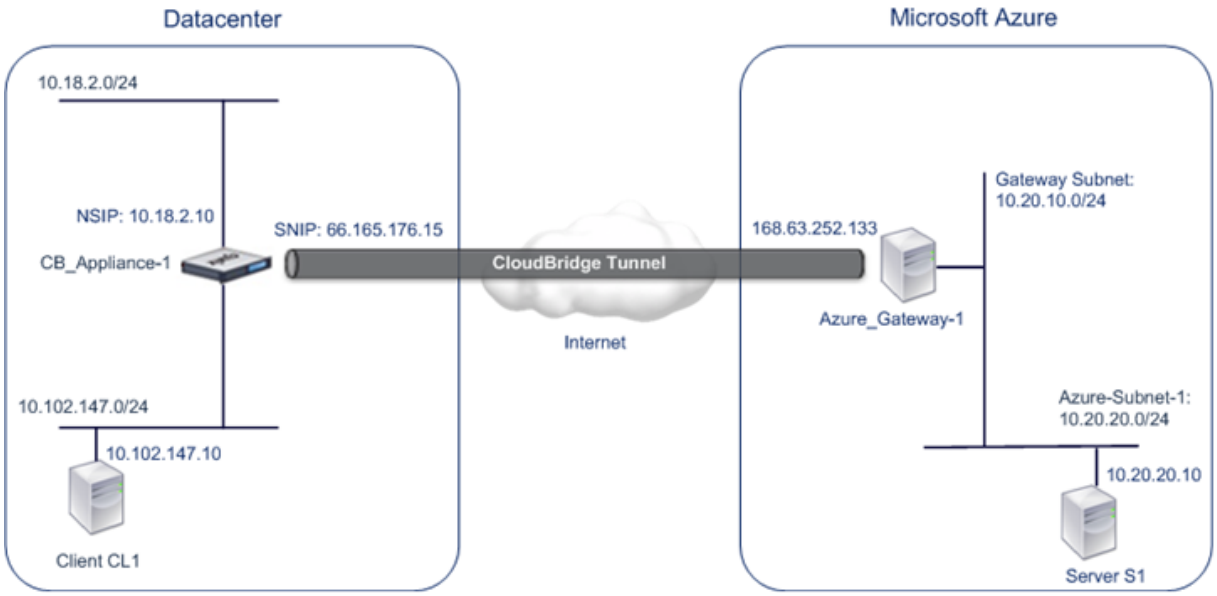
La entidad de túnel del conector de CloudBridge CB_Azure_tunnel especifica la dirección IP local (una dirección IP pública (SNIP) configurada en el dispositivo Citrix ADC), la dirección IP remota (la dirección IP de Azure_Gateway-1) y el protocolo (IPSec) utilizado para configurar el túnel del conector de CloudBridge. CB_Azure_tunnel está enlazado a la entidad PBR CB_Azure_PBR.

La entidad PBR CB_Azure_PBR especifica un conjunto de condiciones y una entidad de túnel CloudBridge Connector (CB_Azure_Tunnel). El intervalo de direcciones IP de origen y el intervalo de direcciones IP de destino son las condiciones para CB_Azure_PBR. El intervalo de direcciones IP de origen y el intervalo de direcciones IP de destino se especifican como una subred en el centro de datos y una subred en la nube de Azure, respectivamente. Cualquier paquete de solicitud procedente de un cliente de la subred del centro de datos y destinado a un servidor de la subred de la nube de Azure coincide con las condiciones de CB_Azure_PBR. A continuación, este paquete se considera para el procesamiento de CloudBridge y se envía a través del túnel de CloudBridge Connector (CB_Azure_Tunnel) vinculado a la entidad PBR.

En Microsoft Azure, la configuración del túnel de CloudBridge Connector incluye una entidad de red local denominada My-Datacenter-Network, una entidad de red virtual denominada Azure-Network-for-CloudBridge-Tunnel y una Gateway denominada Azure_Gateway-1.

La entidad de red local (local de Azure) My-Datacenter-Network especifica la dirección IP del dispositivo Citrix ADC en el lado del centro de datos y la subred del centro de datos cuyo tráfico va a atravesar el túnel de CloudBridge Connector. La entidad de red virtual Azure-Network-for-CloudBridge-Tunnel define una subred privada denominada Azure-Subnet-1 en Azure. El tráfico de la subred atraviesa el túnel CloudBridge Connector. El servidor S1 se aprovisiona en esta subred.

La entidad de red local My-Datacenter-Network está asociada a la entidad de red virtual Azure-Network-for-CloudBridge-Tunnel. Esta asociación define los detalles de red local y remota de la configuración del túnel de CloudBridge Connector en Azure. Gateway Azure_Gateway-1 se creó para que esta asociación se convirtiera en el punto final de CloudBridge en el extremo de Azure del túnel de CloudBridge Connector.



Para obtener más información sobre la configuración, consulte el pdf Configuración del túnel de CloudBridge Connector .

Puntos a tener en cuenta para una configuración de túnel de CloudBridge Connector

Antes de configurar un túnel de CloudBridge Connector entre un dispositivo Citrix ADC en el centro de datos y Microsoft Azure, tenga en cuenta los siguientes puntos:

1. El dispositivo Citrix ADC debe tener una dirección IPv4 pública (tipo SNIP) para utilizarla como dirección de punto final del túnel para el túnel CloudBridge Connector. Además, el dispositivo Citrix ADC no debe estar detrás de un dispositivo NAT.
2. Azure admite la siguiente configuración de IPSec para un túnel de CloudBridge Connector. Por lo tanto, debe especificar la misma configuración de IPSec al configurar Citrix ADC para el túnel de CloudBridge Connector.
    - Versión IKE = v1
    - Algoritmo de cifrado = AES
    - Algoritmo hash = HMAC SHA1
3. Debe configurar el firewall en el borde del centro de datos para permitir lo siguiente.
    - Cualquier paquete UDP para el puerto 500
    - Cualquier paquete UDP para el puerto 4500
    - Cualquier paquete ESP (protocolo IP número 50)
4. No se admite la reconversión de claves IKE, que es la renegociación de nuevas claves criptográficas entre los puntos finales del túnel de CloudBridge Connector para establecer nuevas SA. Cuando caducan las asociaciones de seguridad (SA), el túnel pasa al estado DOWN. Por lo tanto, debe establecer un valor muy grande para las vidas de las SA.
5. Debe configurar Microsoft Azure antes de especificar la configuración del túnel en Citrix ADC, porque la dirección IP pública del extremo (Gateway) de Azure del túnel y el PSK se generan automáticamente al configurar la configuración del túnel en Azure. Necesita esta información para especificar la configuración del túnel en Citrix ADC.

Configuración del túnel de CloudBridge Connector

Para configurar un túnel de CloudBridge Connector entre el centro de datos y Azure, debe instalar CloudBridge VPX/MPX en el centro de datos, configurar Microsoft Azure para el túnel de CloudBridge Connector y, a continuación, configurar el dispositivo Citrix ADC en el centro de datos para el túnel de CloudBridge Connector.

La configuración de un túnel de CloudBridge Connector entre un dispositivo Citrix ADC en el centro de datos y Microsoft Azure consiste en las siguientes tareas:

1. **Configuración del dispositivo Citrix ADC en el centro de datos**. Esta tarea implica la implementación y configuración de un dispositivo físico Citrix ADC (MPX) o el Provisioning y configuración de un dispositivo virtual Citrix ADC (VPX) en una plataforma de virtualización del centro de datos.
2. **Configuración de Microsoft Azure para el túnel de CloudBridge Connector**. Esta tarea im-

plica la creación de entidades de red local, red virtual y Gateway en Azure. La entidad de red local especifica la dirección IP del punto final del túnel de CloudBridge Connector (el dispositivo Citrix ADC) en el lado del centro de datos y la subred del centro de datos cuyo tráfico va a atravesar el túnel de CloudBridge Connector. La red virtual define una red en Azure. La creación de la red virtual incluye la definición de una subred cuyo tráfico es atravesar el túnel de CloudBridge Connector que se va a formar. A continuación, asocie la red local con la red virtual. Por último, se crea una Gateway que se convierte en el punto final en el extremo de Azure del túnel de CloudBridge Connector.

3. **Configuración del dispositivo Citrix ADC en el centro de datos para el túnel de CloudBridge Connector**. Esta tarea implica la creación de un perfil IPSec, una entidad de túnel IP y una entidad PBR en el dispositivo Citrix ADC en el centro de datos. La entidad de perfil IPSec especifica los parámetros del protocolo IPSec, como la versión IKE, el algoritmo de cifrado, el algoritmo hash y PSK, que se utilizarán en el túnel de CloudBridge Connector. El túnel IP especifica la dirección IP de los puntos finales del túnel de CloudBridge Connector (el dispositivo Citrix ADC en el centro de datos y la Gateway en Azure) y el protocolo que se utilizará en el túnel de CloudBridge Connector. A continuación, asocie la entidad de perfil IPSec con la entidad de túnel IP. La entidad PBR especifica las dos subredes, en el centro de datos y en la nube de Azure, que deben comunicarse entre sí a través del túnel CloudBridge Connector. A continuación, asocie la entidad de túnel IP con la entidad PBR.

Configuración de Microsoft Azure para el túnel de CloudBridge Connector

Para crear una configuración de túnel de CloudBridge Connector en Microsoft Azure, utilice el Portal de administración de Microsoft Windows Azure, que es una interfaz gráfica basada en web para crear y administrar recursos en Microsoft Azure.

Antes de comenzar la configuración del túnel de CloudBridge Connector en la nube de Azure, asegúrese de que:

- Tiene una cuenta de usuario para Microsoft Azure.
- Tiene un conocimiento conceptual de Microsoft Azure.
- Está familiarizado con el Portal de administración de Microsoft Windows Azure.

Para configurar un túnel de CloudBridge Connector entre un centro de datos y una nube de Azure, realice las siguientes tareas en Microsoft Azure mediante el Portal de administración de Microsoft Windows Azure:

- **Cree una entidad de red local**. Cree una entidad de red local en Windows Azure para especificar los detalles de red del centro de datos. Una entidad de red local especifica la dirección IP del punto final del túnel de CloudBridge Connector (Citrix ADC) en el lado del centro de datos y la subred del centro de datos cuyo tráfico va a atravesar el túnel de CloudBridge Connector.
- **Crear una red virtual**. Cree una entidad de red virtual que defina una red en Azure. Esta tarea in-

cluye definir un espacio de direcciones privado, donde se proporciona un rango de direcciones privadas y subredes pertenecientes al rango especificado en el espacio de direcciones. El tráfico de las subredes atravesará el túnel CloudBridge Connector. A continuación, asociará una entidad de red local con la entidad de red virtual. Esta asociación permite a Azure crear una configuración para un túnel de CloudBridge Connector entre la red virtual y la red del centro de datos. Una Gateway (que se creará) en Azure para esta red virtual será el punto final de CloudBridge en el extremo de Azure del túnel de CloudBridge Connector. A continuación, defina una subred privada para la Gateway que se va a crear. Esta subred pertenece al intervalo especificado en el espacio de direcciones de la entidad de red virtual.

- **Cree una Gateway en Windows Azure**. Cree una Gateway que se convierta en el punto final en el extremo de Azure del túnel de CloudBridge Connector. Azure, desde su grupo de direcciones IP públicas, asigna una dirección IP a la Gateway creada.
- **Reúna la dirección IP pública de la Gateway y la clave previamente compartida.** Para una configuración de túnel de CloudBridge Connector en Azure, Azure genera automáticamente la dirección IP pública de la Gateway y la clave previamente compartida (PSK). Tome nota de esta información. Lo necesitará para configurar el túnel de CloudBridge Connector en el Citrix ADC en el centro de datos.

> **Nota:**
>
> Los procedimientos para configurar Microsoft Azure para un túnel de CloudBridge Connector pueden cambiar con el tiempo, dependiendo del ciclo de lanzamiento de Microsoft Azure. Para obtener los procedimientos más recientes, consulte la documentación de Microsoft Azure.

Configuración de Citrix ADC Appliance en el centro de datos para el túnel de CloudBridge Connector

Para configurar un túnel de CloudBridge Connector entre un centro de datos y una nube de Azure, realice las siguientes tareas en el Citrix ADC en el centro de datos. Puede usar la línea de comandos Citrix ADC o la GUI:

- **Cree un perfil IPSec**. Una entidad de perfil IPSec especifica los parámetros del protocolo IPSec, como la versión IKE, el algoritmo de cifrado, el algoritmo hash y PSK, que utilizará el protocolo IPSec en el túnel de CloudBridge Connector.
- **Cree un túnel IP con el protocolo IPSec y asocie el perfil IPSec a él**. Un túnel IP especifica la dirección IP local (una dirección SNIP pública configurada en el dispositivo Citrix ADC), la dirección IP remota (la dirección IP pública de la Gateway en Azure), el protocolo (IPSec) utilizado para configurar el túnel CloudBridge Connector y una entidad de perfil IPSec. La entidad de túnel IP creada también se denomina entidad de túnel CloudBridge Connector.
- **Cree una regla PBR y asocie el túnel IP a ella**. Una entidad PBR especifica un conjunto de condiciones y una entidad de túnel IP (túnel CloudBridge Connector). El intervalo de direcciones IP de origen y el intervalo IP de destino son las condiciones para la entidad PBR. Debe

establecer el intervalo de direcciones IP de origen para especificar la subred del centro de datos cuyo tráfico va a atravesar el túnel, y el intervalo de direcciones IP de destino para especificar la subred de Azure cuyo tráfico va a atravesar el túnel de CloudBridge Connector. Cualquier paquete de solicitud originado desde un cliente de la subred del centro de datos y destinado a un servidor de la subred de la nube de Azure coincide con el rango IP de origen y destino de la entidad PBR. Este paquete se considera entonces para el procesamiento del túnel de CloudBridge Connector y se envía a través del túnel de CloudBridge Connector asociado con la entidad PBR.

La interfaz gráfica de usuario combina todas estas tareas en un único asistente denominado asistente de CloudBridge Connector.
Para crear un perfil IPSEC mediante la línea de comandos de Citrix ADC:

En el símbolo del sistema, escriba:

```
add ipsec profile <name> -psk <string> -ikeVersion v1
```

Para crear un túnel IPSEC y enlazar el perfil IPSEC con él mediante la línea de comandos de Citrix ADC:

En el símbolo del sistema, escriba:

```
add ipTunnel <name> <remote> <remoteSubnetMask> <local> -protocol IPSEC -
ipsecProfileName <string>
```

Para crear una regla PBR y enlazar el túnel IPSEC con ella mediante la línea de comandos de Citrix ADC

```
add pbr <pbrName> ALLOW -srcIP <subnet-range> -destIP <subnet-range> ipTunnel
 <tunnelName> apply pbrs
```

Configuración de ejemplo

Los siguientes comandos crean toda la configuración del dispositivo Citrix ADC CB_Appliance-1 utilizado en “Ejemplo de configuración y flujo de datos de CloudBridge Connector”.

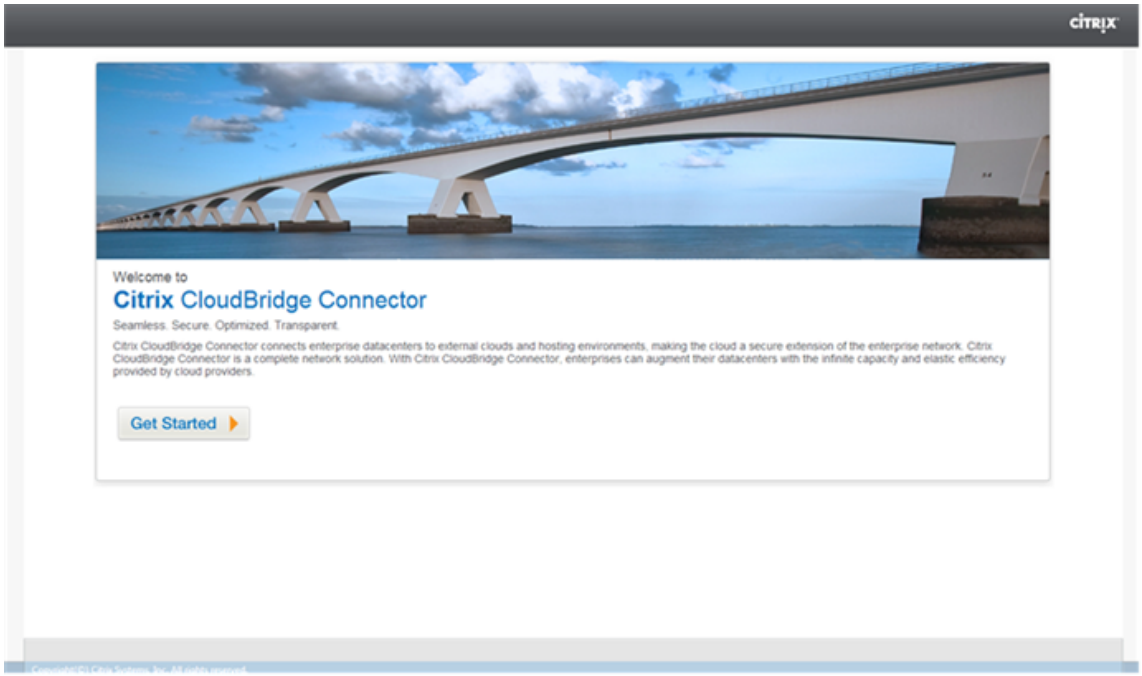
```
1  > add ipsec profile CB_Azure_IPSec_Profile -psk
       DkiMgMdcbqvYREEuIvxsbKkW0FOyDiLM  -ikeVersion v1  - lifetime 31536000
2  Done
3
4  >  add iptunnel CB_Azure_Tunnel 168.63.252.133 255.255.255.255
       66.165.176.15  - protocol IPSEC  - ipsecProfileName
       CB_Azure_IPSec_Profile
5  Done
6
7  > add pbr CB_Azure_Pbr -srcIP 10.102.147.0-10.102.147.255  - destIP
       10.20.0.0-10.20.255.255  - ipTunnelCB_Azure_Tunnel
8  Done
9
10 > apply pbrs
```



```
11 Done
12 <!--NeedCopy-->
```

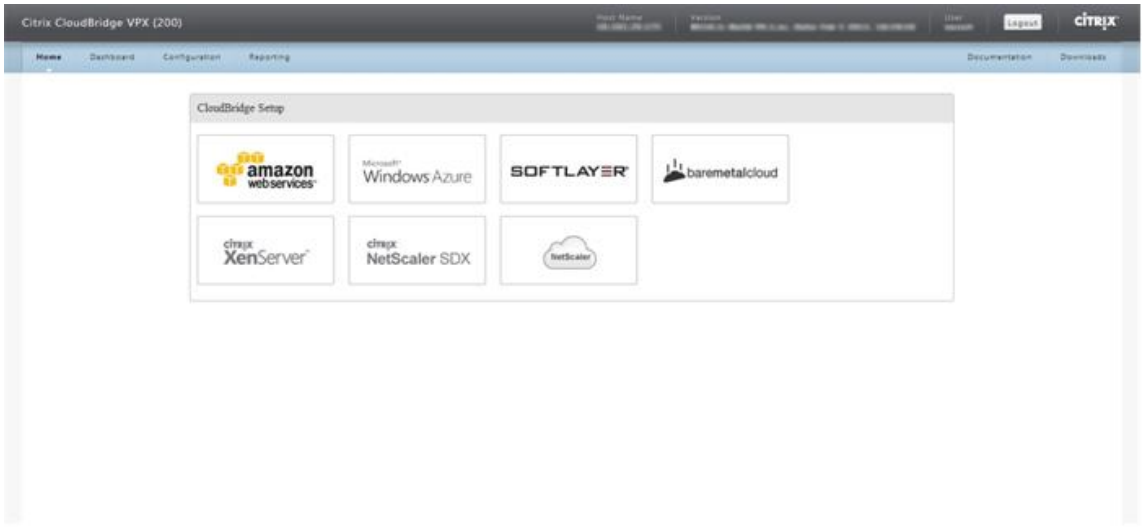
Para configurar un túnel de CloudBridge Connector en un dispositivo Citrix ADC mediante la interfaz gráfica de usuario

1. Acceda a la GUI mediante un explorador web para conectarse a la dirección IP del dispositivo Citrix ADC en el centro de datos.
2. Vaya a **Sistema** > **Conector de CloudBridge**.
3. En el panel derecho, en **Introducción**, haga clic en **Crear/Supervisar CloudBridge**.
4. Haga clic en **Get Started**.

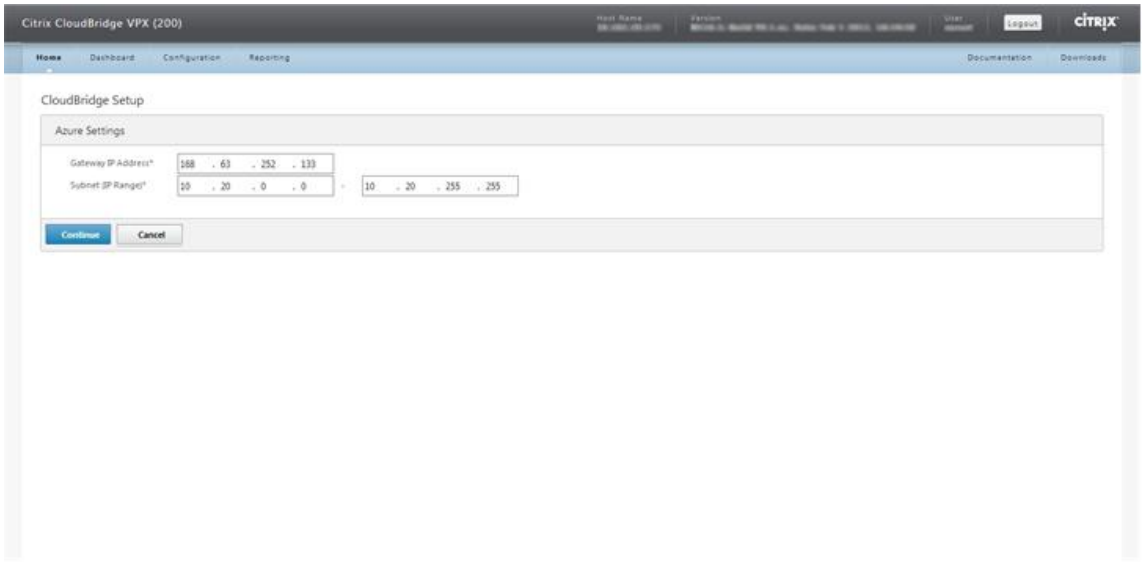


> **Nota**: Si ya tiene configurado un túnel de CloudBridge Connector en el dispositivo Citrix ADC, esta pantalla no aparece y se le lleva al panel Configuración de CloudBridge Connector.

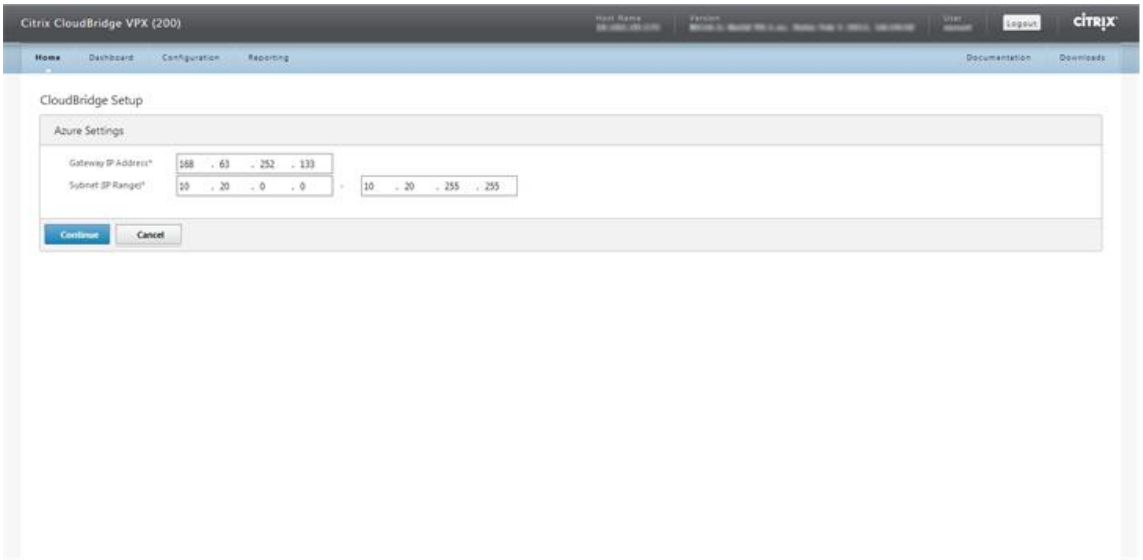
5. En el panel Configuración de CloudBridge, haga clic en **Microsoft Windows Azure**.



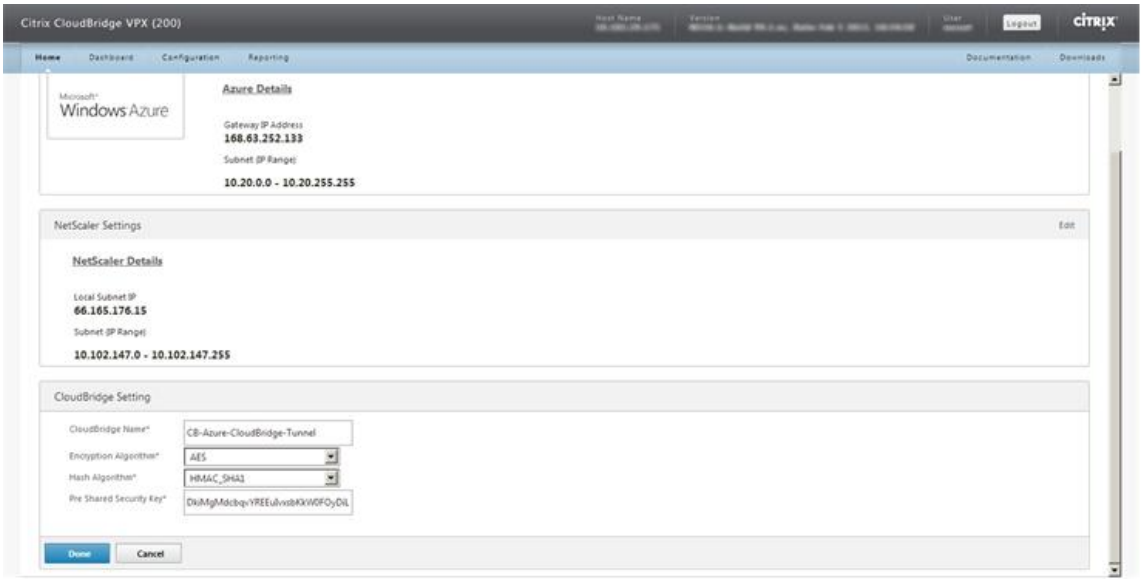
6. En el panel Configuración de Azure, en el campo **Dirección IP de puerta** de enlace, escriba la dirección IP de la puerta de enlace de Azure. A continuación, el túnel de CloudBridge Connector se configura entre el dispositivo Citrix ADC y la Gateway. En los cuadros de texto **Subred (Rango IP)**, especifique un rango de subred (en la nube de Azure) cuyo tráfico atraviesa el túnel de CloudBridge Connector. Haga clic en **Continuar**.



7. En el panel Configuración de Citrix ADC, en la lista desplegable **IP de subred local**, seleccione una dirección SNIP accesible públicamente configurada en el dispositivo Citrix ADC. En los cuadros de texto **Subred (Rango IP)**, especifique un rango de subred local cuyo tráfico atraviesa el túnel de CloudBridge Connector. Haga clic en **Continuar**.



8. En el panel **Configuración de CloudBridge**, en el cuadro de texto Nombre de CloudBridge, escriba un nombre para el CloudBridge que quiera crear.



9. En las listas desplegables Algoritmo de cifrado y Algoritmo hash, seleccione los algoritmos AES y HMAC_SHA1, respectivamente. En el cuadro de texto Clave de seguridad previamente compartida, escriba la clave de seguridad.
10. Haga clic en **Done**.

Supervisión del túnel de CloudBridge Connector

Puede ver estadísticas para supervisar el rendimiento de un túnel de CloudBridge Connector entre el dispositivo Citrix ADC en el centro de datos y Microsoft Azure. Para ver las estadísticas del túnel de CloudBridge Connector en el dispositivo Citrix ADC, utilice la línea de comandos GUI o Citrix ADC.

Para ver las estadísticas del túnel de CloudBridge Connector en Microsoft Azure, utilice el Portal de administración de Microsoft Windows Azure.

Visualización de estadísticas del túnel de CloudBridge Connector en el dispositivo Citrix ADC

Para obtener información sobre cómo mostrar estadísticas de túnel de CloudBridge Connector en un dispositivo Citrix ADC, consulte Supervisión de túneles de CloudBridge Connector.

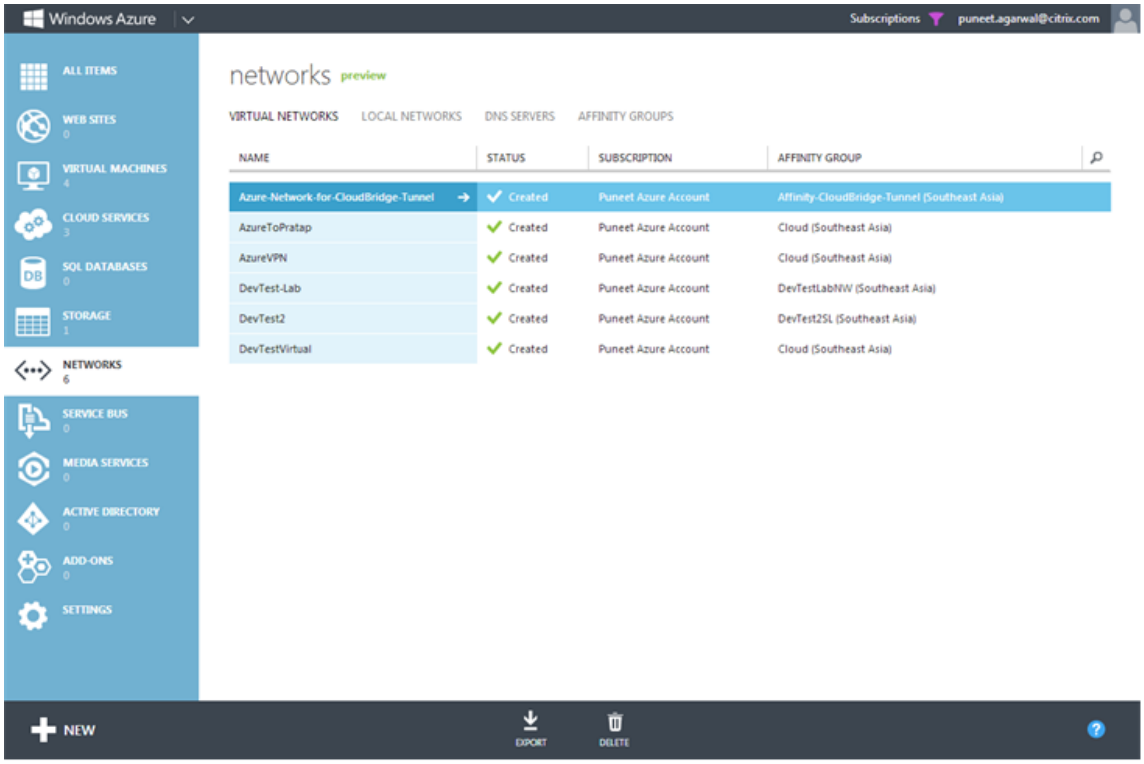
Visualización de estadísticas del túnel de CloudBridge Connector en Microsoft Azure

En la siguiente tabla se enumeran los contadores estadísticos disponibles para supervisar los túneles de CloudBridge Connector en Microsoft Azure.

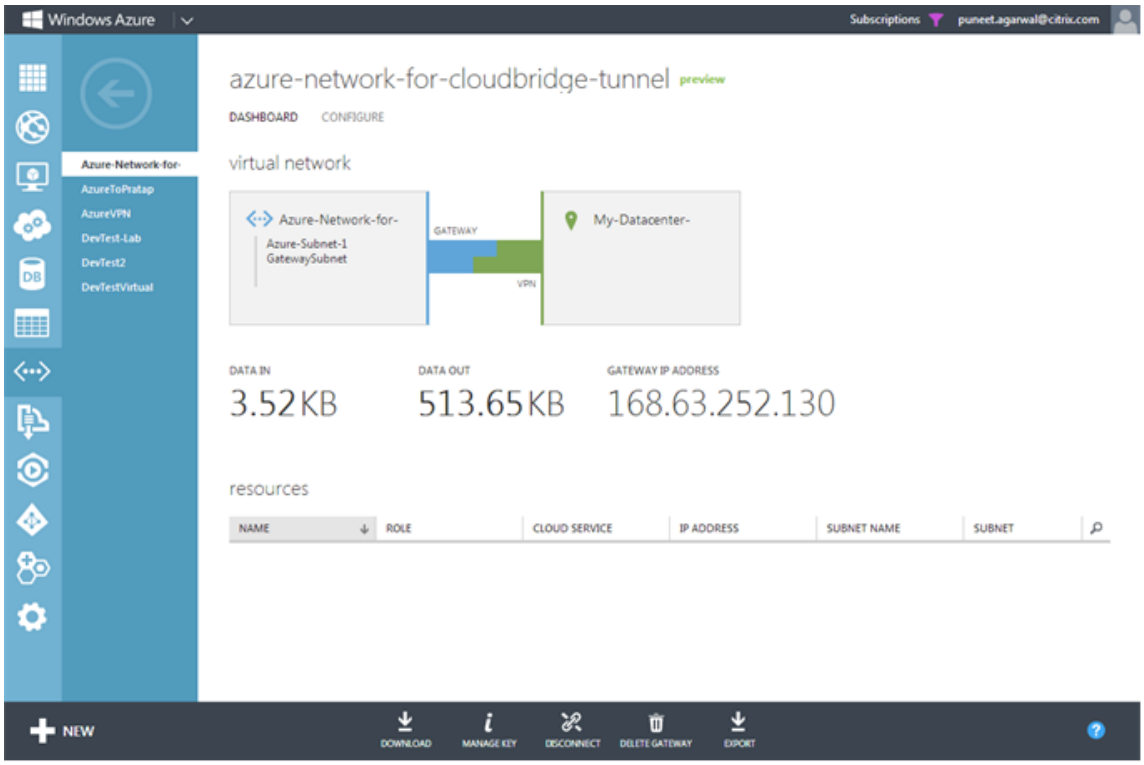
Contador estadístico	Especifica
DATOS EN	Número total de kilobytes recibidos por la Gateway de Azure a través del túnel de CloudBridge Connector desde que se creó la Gateway.
SALIDA DE DATOS	Número total de kilobytes enviados por la Gateway de Azure a través del túnel de CloudBridge Connector desde que se creó la Gateway.

Para mostrar las estadísticas del túnel de CloudBridge Connector mediante el Portal de administración de Microsoft Windows Azure

1. Inicie sesión en el portal de administración de Windows Azure mediante las credenciales de su cuenta de Microsoft Azure.
2. En el panel izquierdo, haga clic en **REDES**.
3. En la ficha **Red virtual**, en la columna Nombre, seleccione la entidad de red virtual asociada a un túnel de CloudBridge Connector cuyas estadísticas quiere mostrar.



4. En la página **DASHboard** de la red virtual, vea los contadores DATA IN y DATA OUT del túnel CloudBridge Connector.



Configuración del túnel de CloudBridge Connector entre el centro de datos y la nube empresarial de capa blanda

August 20, 2021

La GUI incluye un asistente que le ayuda a configurar fácilmente un túnel de CloudBridge Connector entre un dispositivo Citrix ADC en un centro de datos y las instancias de Citrix ADC VPX en la nube empresarial de SoftLayer.

Cuando utiliza el asistente del dispositivo Citrix ADC en el centro de datos, la configuración del túnel de CloudBridge Connector creada en el dispositivo Citrix ADC se envía automáticamente al otro punto final o par (Citrix ADC VPX en SoftLayer) del túnel de CloudBridge Connector.

Con el asistente del dispositivo Citrix ADC en el centro de datos, realice los siguientes pasos para configurar un túnel de CloudBridge Connector.

1. Conéctese a la nube empresarial de Softlayer proporcionando las credenciales de inicio de sesión del usuario.
2. Seleccione Citrix XenServer que ejecuta el dispositivo Citrix ADC VPX.
3. Seleccione el dispositivo Citrix ADC VPX.
4. Proporcione los parámetros del túnel de CloudBridge Connector para:
    - Configure un túnel GRE.
    - Configure IPSec en el túnel GRE.
    - Cree un netbridge, que es una representación lógica del conector CloudBridge, especificando un nombre.
    - Enlazar el túnel GRE al netbridge.

Para configurar un túnel de CloudBridge Connector mediante la interfaz gráfica de usuario

1. Inicie sesión en la GUI del dispositivo Citrix ADC en el centro de datos mediante las credenciales de cuenta del dispositivo.
2. Vaya a **Sistema** > **Conector** de **CloudBridge**.
3. En el panel derecho, en **Introducción**, haga clic en **Crear/Supervisar CloudBridge Connector**.
4. Haga clic en **Get Started**.

> **Nota**:
>
> Si ya tiene configurado un túnel de CloudBridge Connector en el dispositivo Citrix ADC, esta pantalla no aparece y se le lleva al panel Configuración de CloudBridge Connector.

1. En el panel Configuración del conector de CloudBridge, haga clic en Capa blanda y, a continuación, siga las instrucciones del asistente.

Supervisión del túnel de CloudBridge Connector

Puede supervisar el rendimiento de los túneles de CloudBridge Connector en un dispositivo Citrix ADC mediante contadores estadísticos del túnel de CloudBridge Connector. Para obtener más información sobre cómo mostrar estadísticas de túnel de CloudBridge Connector en un dispositivo Citrix ADC, consulte Supervisión de túneles de CloudBridge Connector.

Configuración de un túnel de CloudBridge Connector entre un dispositivo Citrix ADC y un dispositivo Cisco IOS

October 5, 2021

Puede configurar un túnel de CloudBridge Connector entre un dispositivo Citrix ADC y un dispositivo Cisco para conectar dos centros de datos o ampliar la red a un proveedor de Cloud. El dispositivo Citrix ADC y el dispositivo Cisco IOS forman los puntos finales del túnel CloudBridge Connector y se denominan pares.

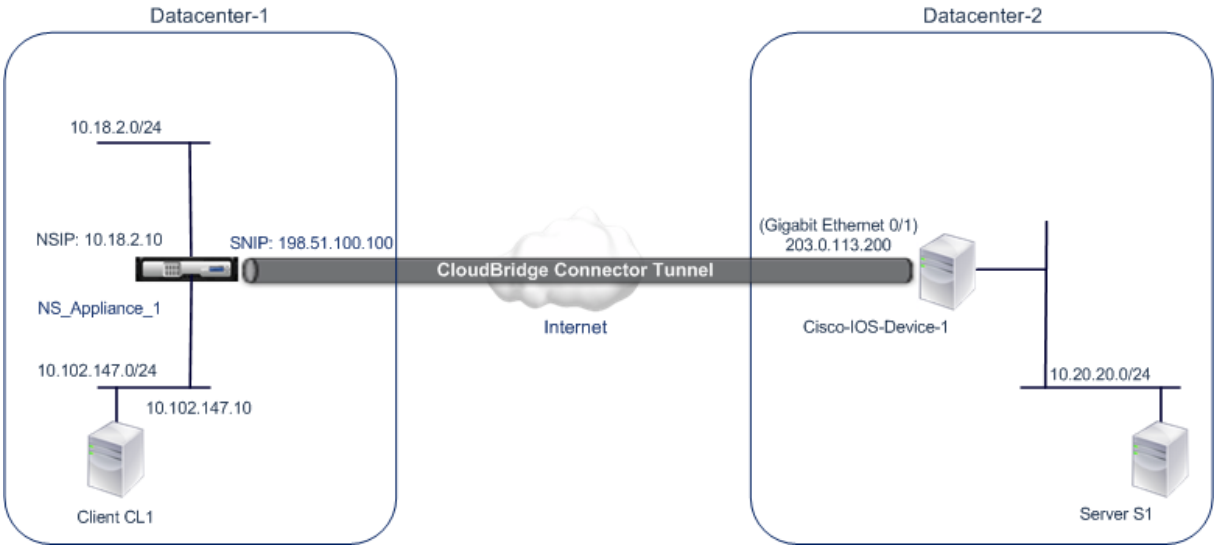
Ejemplo de configuración del túnel de CloudBridge Connector y flujo de datos

Como ilustración del flujo de tráfico en un túnel de CloudBridge Connector, considere un ejemplo en el que se configura un túnel de CloudBridge Connector entre los siguientes dispositivos:

- Dispositivo Citrix ADC NS_Appliance-1 en un centro de datos designado como Datacenter-1
- Dispositivo Cisco IOS CISCO-IOS-Device-1 en un centro de datos designado como Datacenter-2

NS_Appliance-1 y Cisco-IOS-Device-1 permiten la comunicación entre redes privadas en Datacenter-1 y Datacenter-2 a través del túnel CloudBridge Connector. En el ejemplo, NS_Appliance-1 y Cisco-IOS-Device-1 habilitan la comunicación entre el cliente CL1 en Datacenter-1 y el servidor S1 en Datacenter-2 a través del túnel CloudBridge Connector. El cliente CL1 y el servidor S1 están en diferentes redes privadas.

En NS_Appliance-1, la configuración del túnel de CloudBridge Connector incluye la entidad de perfil IPSec NS_CISCO_IPSEC_Profile, la entidad de túnel de CloudBridge Connector NS_CISCO_Tunnel y la entidad de redirección basada en directivas (PBR) NS_CISCO_PBR.



Para obtener más información, consulte el túnel CloudBridge Connector entre un dispositivo Citrix ADC y la configuración del dispositivo Cisco IOS pdf.

Puntos a tener en cuenta para una configuración de túnel de CloudBridge Connector

Antes de configurar un túnel de CloudBridge Connector entre un dispositivo Citrix ADC y un dispositivo Cisco IOS, tenga en cuenta los siguientes puntos:

- La siguiente configuración de IPSec se admite para un túnel de CloudBridge Connector entre un dispositivo Citrix ADC y un dispositivo Cisco IOS.

Propiedades IPSec	Configuración
Modo IPSec	Modo túnel
Versión de IKE	Versión 1
Grupo IKE DH	Grupo DH 2 (algoritmo MODP de 1024 bits)
Método de autenticación IKE	Clave previamente compartida
Algoritmo de cifrado IKE	AES, 3DES
Algoritmo hash IKE	HMAC SHA1, HMAC SHA256, HMAC SHA384, HMAC SHA512, HMAC MD5
Algoritmo de cifrado ESP	AES, 3DES
Algoritmo hash ESP	HMAC SHA1, HMAC SHA256, HMAC SHA256, HMAC SHA256, HMAC MD5

- Debe especificar la misma configuración IPSec en el dispositivo Citrix ADC y en el dispositivo

Cisco IOS en los dos extremos del conector CloudBridge.

- Citrix ADC proporciona un parámetro común (en perfiles IPSec) para especificar un algoritmo hash IKE y un algoritmo hash ESP. También proporciona otro parámetro común para especificar un algoritmo de cifrado IKE y un algoritmo de cifrado ESP. Por lo tanto, en el dispositivo Cisco, debe especificar el mismo algoritmo hash y el mismo algoritmo de cifrado para IKE (al crear la directiva IKE) y ESP (al crear el conjunto de transformaciones IPSec).
- Debe configurar el firewall en el extremo Citrix ADC y en el extremo del dispositivo Cisco para permitir lo siguiente.
  - Cualquier paquete UDP para el puerto 500
  - Cualquier paquete UDP para el puerto 4500
  - Cualquier paquete ESP (protocolo IP número 50)

Configuración del dispositivo Cisco IOS para el túnel CloudBridge Connector

Para configurar un túnel de CloudBridge Connector en un dispositivo Cisco IOS, utilice la interfaz de línea de comandos de Cisco IOS, que es la interfaz de usuario principal para configurar, supervisar y mantener dispositivos Cisco.

Antes de comenzar la configuración del túnel de CloudBridge Connector en un dispositivo Cisco IOS, asegúrese de que:

- Tiene una cuenta de usuario con credenciales de administrador en el dispositivo Cisco IOS.
- Está familiarizado con la interfaz de línea de comandos del IOS de Cisco.
- El dispositivo Cisco IOS está en funcionamiento, está conectado a Internet y también está conectado a las subredes privadas cuyo tráfico se va a proteger a través del túnel CloudBridge Connector.

> **Nota**:
>
> Los procedimientos para configurar el túnel de CloudBridge Connector en un dispositivo Cisco IOS pueden cambiar con el tiempo, dependiendo del ciclo de lanzamiento de Cisco. Citrix recomienda que siga la documentación oficial del producto de Cisco para obtener más información, consulte el tema Configuración de túneles VPN IPSec .

Para configurar un túnel de conector de CloudBridge entre un dispositivo Citrix ADC y un dispositivo Cisco IOS, realice las siguientes tareas en la línea de comandos IOS del dispositivo Cisco:

- Cree una directiva IKE.
- Configure una clave previamente compartida para la autenticación IKE.
- Defina un conjunto de transformaciones y configure IPSec en modo túnel.
- Crear una lista de acceso criptográfico
- Crear un mapa criptográfico

- Aplicar el mapa criptográfico a una interfaz

Los ejemplos de los siguientes procedimientos crean la configuración `Cisco IOS device Cisco-IOS-Device-1` mencionada en la sección “Ejemplo de configuración y flujo de datos de CloudBridge Connector. “

Para crear una directiva de IKE, consulte la directiva IKE pdf.

Para configurar una clave previamente compartida mediante la línea de comandos del IOS de Cisco:

En el símbolo del sistema del dispositivo Cisco IOS, escriba los siguientes comandos, comenzando en el modo de configuración global, en el orden mostrado:

Comando	Ejemplo	Descripción del comando
crypto isakmp identity address	Cisco-ios-device-1(config)# crypto isakmp identity address	Especifique la identidad ISAKMP (dirección) que debe utilizar el dispositivo Cisco IOS al comunicarse con el mismo nivel (dispositivo Citrix ADC) durante las negociaciones IKE. En este ejemplo se especifica la palabra clave address, que utiliza la dirección IP 203.0.113.200 (interfaz Gigabit Ethernet 0/1 de Cisco-IOS-Device-1) como identidad del dispositivo.

Comando	Ejemplo	Descripción del comando
crypto isakmp key keystringaddress peer-address	Cisco-ios-device-1 (config)# crypto isakmp key examplepresharedkey address 198.51.100.100	Especifique una clave previamente compartida para la autenticación IKE. En este ejemplo se configura la clave compartida examplepresharedkey para que se utilice con el dispositivo Citrix ADC NS_Appliance-1 (198.51.100.100). Se debe configurar la misma clave previamente compartida en el dispositivo Citrix ADC para que la autenticación IKE se realice correctamente entre el dispositivo Cisco IOS y el dispositivo Citrix ADC.

Para crear una lista de acceso criptográfico mediante la línea de comandos del IOS de Cisco:

En el símbolo del sistema del dispositivo Cisco IOS, escriba el siguiente comando en el modo de configuración global, en el orden mostrado:

Comando	Ejemplo	Descripción del comando
access-listaccess-list-number permit IPsource source-wildcard destination destination-wildcard	Cisco-ASA-appliance-1(config)# access-list 111 permit ip 10.20.20.0 0.0.0.255 10.102.14	Especifique las condiciones para determinar las subredes cuyo tráfico IP debe protegerse sobre el túnel de CloudBridge Connector. En este ejemplo se configura la lista de acceso 111 para proteger el tráfico de las subredes 10.20.20.0/24 (en el lado Cisco-IOS-Device-1) y 10.102.147.0/24 (en el lado NS_Appliance-1).

Para definir una transformación y configurar el modo de túnel IPSec mediante la línea de comandos del IOS de Cisco:

En el símbolo del sistema del dispositivo Cisco IOS, escriba los siguientes comandos, comenzando en el modo de configuración global, en el orden mostrado:
Comando	Ejemplo	Descripción del comando
–	–	–
crypto ipsec transform-setname ESP_Authentication_transform ESP_Encryption_transform Nota: ESP_Authentication_transform puede tomar los siguientes valores: esp-sha-hmac, esp-sha256-hmac, esp-sha384-hmac, esp-sha512-hmac, esp-md5-hmac. ESP_encryption_transform puede tomar los siguientes valores: esp-aes o esp-3des	Cisco-ios-device-1(config)# crypto ipsec transform-set NS-CISCO-TS esp-sha256-hmac esp-3des	Defina un conjunto de transformaciones y especifique el algoritmo hash ESP (para autenticación) y el algoritmo de cifrado ESP que se utilizará durante el intercambio de datos entre los pares del túnel de CloudBridge Connector. En este ejemplo se define el conjunto de transformaciones NS-CISCO-TS y se especifica el algoritmo de autenticación ESP como esp-sha256-hmac, y el algoritmo de cifrado ESP como esp-3des.
túnel modo	Túnel de modo # de Cisco-IOS-Device-1 (config-crypto-trans)	Establezca IPsec en modo túnel.
exit	Cisco-IOS-Device-1 (config-crypto-trans) # exit, cisco-ios-device-1 (config) #	Salga de nuevo al modo de configuración global.

Para crear un mapa criptográfico mediante la línea de comandos del IOS de Cisco:

En el símbolo del sistema del dispositivo Cisco IOS, escriba los siguientes comandos comenzando en el modo de configuración global, en el orden mostrado:

Comando	Ejemplo	Descripción del comando
criptomapa nombre-seq-num ipsec-isakmp	Cisco-iOS-device-1 (config) # mapa criptográfico NS-CISCO-CM 2 ipsec-isakmp	Introduzca el modo de configuración de mapa criptográfico, especifique un número de secuencia para el mapa criptográfico y configure el mapa criptográfico para usar IKE para establecer asociaciones de seguridad (SA). Este ejemplo configura el número de secuencia 2 e IKE para el mapa criptográfico NS-CISCO-CM.

Comando	Ejemplo	Descripción del comando
set peer ip-address	Cisco-ios-device-1 (config-crypto-map)# set peer 172.23.2.7	Especifique el par (dispositivo Citrix ADC) por su dirección IP. En este ejemplo se especifica 198.51.100.100, que es la dirección IP del extremo de CloudBridge Connector en el dispositivo Citrix ADC.
coincidir addressaccess-list-id	Cisco-ios-device-1 (config-crypto-map)# match address 111	Especifique una lista de acceso extendido. Esta lista de acceso especifica las condiciones para determinar las subredes cuyo tráfico IP debe protegerse sobre el túnel de CloudBridge Connector. En este ejemplo se especifica la lista de acceso 111.
establecer transform-set transform-set-nombre-set-	Cisco-ios-device-1 (config-crypto-map)# set transform-set NS-CISCO-TS	Especifique qué conjuntos de transformación se permiten para esta entrada de mapa criptográfico. En este ejemplo se especifica el conjunto de transformaciones NS-CISCO-TS.
exit	Cisco-ios-device-1 (config-crypto-map)# exit	
Cisco-ios-device-1 (config)#	Vuelve al modo de configuración global.	

Para aplicar un mapa criptográfico a una interfaz mediante la línea de comandos del IOS de Cisco:

En el símbolo del sistema del dispositivo Cisco IOS, escriba los siguientes comandos comenzando en el modo de configuración global, en el orden mostrado:

Comando	Ejemplo	Descripción del comando
Id. de interfaz	CISCO-IOS-Device-1 (config) # interfaz GigabitEthernet 0/1	Especifique una interfaz física a la que aplicar el mapa criptográfico y entre en el modo de configuración de interfaz. En este ejemplo se especifica la interfaz Gigabit Ethernet 0/1 del dispositivo Cisco Cisco-IOS-Device-1. La dirección IP 203.0.113.200 ya está configurada en esta interfaz.
nombre de mapa de mapa de cifrado	Cisco-IOS-Device-1 (config-if) # mapa criptográfico NS-CISCO-CM	Aplique el mapa criptográfico a la interfaz física. Este ejemplo aplica el mapa criptográfico NS-CISCO-CM.
exit	Cisco-iOS-device-1 (config-if) # exit, Cisco-iOS-device-1 (config) #	Salga de nuevo al modo de configuración global.

Configuración del dispositivo Citrix ADC para el túnel de CloudBridge Connector

Para configurar un túnel de CloudBridge Connector entre un dispositivo Citrix ADC y un dispositivo Cisco IOS, realice las siguientes tareas en el dispositivo Citrix ADC. Puede utilizar la línea de comandos de Citrix ADC o la interfaz gráfica de usuario (GUI) de Citrix ADC:

- Cree un perfil IPSec.
- Cree un túnel IP que utilice el protocolo IPSec y asocie el perfil IPSec con él.
- Cree una regla PBR y asociarla con el túnel IP.

Para crear un perfil IPSEC mediante la línea de comandos de Citrix ADC:

En el símbolo del sistema, escriba:

- `add ipsec profile <name> -psk <string> -ikeVersion v1`
- `show ipsec profile <name>`

Para crear un túnel IPSEC y enlazar el perfil IPSEC a él mediante la línea de comandos de Citrix ADC:

En el símbolo del sistema, escriba:

- `add ipTunnel <name> <remote> <remoteSubnetMask> <local> -protocol IPSEC -ipsecProfileName <string>`
- `add ipTunnel <name>`

Para crear una regla PBR y enlazar el túnel IPSEC a ella mediante la línea de comandos de Citrix ADC:

En el símbolo del sistema, escriba:

- `add pbr <pbrName> ALLOW -srcIP <subnet-range> -destIP <subnet-range> -ipTunnel <tunnelName>`
- `apply pbrs`
- `show pbrs <pbrName>`

Los siguientes comandos crean la configuración `Citrix ADC appliance NS_Appliance-1` mencionada en la sección **Ejemplo de configuración y flujo de datos de CloudBridge Connector**.

```
1      > add ipsec profile NS_Cisco_IPSec_Profile -psk
          examplepresharedkey -ikeVersion v1 - lifetime 315360 - encAlgo 3
          DES
2      Done
3      > add iptunnel NS_Cisco_Tunnel 203.0.113.200 255.255.255.255
          198.51.100.100 - protocol IPSEC - ipsecProfileName
          NS_Cisco_IPSec_Profile
4
5      Done
6      > add pbr NS_Cisco_Pbr -srcIP 10.102.147.0-10.102.147.255 - destIP
          10.20.0.0-10.20.255.255 - ipTunnel NS_Cisco_Tunnel
7
8      Done
9      > apply pbrs
10
11     Done
12 <!--NeedCopy-->
```

Para crear un perfil IPSEC mediante la GUI:

1. Vaya a **Sistema** > **Conector de CloudBridge** > **Perfil IPSec**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En el cuadro de diálogo **Agregar perfil IPSec**, defina los siguientes parámetros:
   - Nombre
   - Algoritmo de cifrado
   - Algoritmo hash
   - Versión del protocolo IKE

4. Configure el método de **autenticación IPSec** que utilizarán los dos pares de túnel de CloudBridge Connector para autenticarse mutuamente: seleccione el método de **autenticación de clave previamente compartida** y establezca el parámetro **Pre-Shared Key Exists**.
5. Haga clic en **Crear** y, a continuación, en **Cerrar**.

Para crear un túnel IP y enlazar el perfil IPSEC a él mediante la GUI:

1. Vaya a **Sistema** > **Conector de CloudBridge** > **Túneles IP**.
2. En la ficha **Túneles IPv4**, haga clic en **Agregar**.
3. En el cuadro de diálogo **Agregar túnel IP**, establezca los siguientes parámetros:
   - Nombre
   - IP remota
   - Máscara remota
   - Tipo de IP local (en la lista desplegable Tipo de IP local, seleccione IP de subred).
   - IP local (todas las direcciones IP configuradas del tipo IP seleccionado se encuentran en la lista desplegable de IP local. Seleccione la IP deseada de la lista.)
   - Protocolo
   - Perfil IPSec
4. Haga clic en **Crear** y, a continuación, en **Cerrar**.

Para crear una regla PBR y enlazar el túnel IPSEC con ella mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **Red** > **PBR**.
2. En la ficha **PBR**, haga clic en **Agregar**.
3. En el cuadro de diálogo **Crear PBR**, defina los parámetros siguientes:
   - Nombre
   - Action
   - Tipo de salto siguiente (Seleccionar túnel IP)
   - Nombre del túnel IP
   - IP de origen bajo
   - IP de origen alto
   - IP de destino bajo
   - IP de destino alto
4. Haga clic en **Crear** y, a continuación, en **Cerrar**.

Para aplicar un PBR mediante la GUI:

1. Vaya a **Sistema** > **Red** > **PBRs**.
2. En la ficha **PBRs**, seleccione el **PBR**, en la **lista Acción**, seleccione **Aplicar**.

La nueva configuración de túnel de CloudBridge Connector correspondiente en el dispositivo Citrix ADC aparece en la GUI. El estado actual del túnel del conector de CloudBridge se muestra en el panel Connector configurado de CloudBridge. Un punto verde indica que el túnel está arriba. Un punto rojo indica que el túnel está caído.

Supervisión del túnel de CloudBridge Connector

Puede supervisar el rendimiento de los túneles de CloudBridge Connector en un dispositivo Citrix ADC mediante contadores estadísticos del túnel de CloudBridge Connector. Para obtener más información sobre cómo mostrar estadísticas de túnel de CloudBridge Connector en un dispositivo Citrix ADC, consulte Supervisión de túneles de CloudBridge Connector.

Configuración de un túnel de CloudBridge Connector entre un dispositivo Citrix ADC y un dispositivo FortiGate fortinet

August 20, 2021

Puede configurar un túnel de CloudBridge Connector entre un dispositivo Citrix ADC y un dispositivo Fortinet FortiGate para conectar dos centros de datos o ampliar la red a un proveedor de nube. El dispositivo Citrix ADC y el dispositivo FortiGate forman los puntos finales del túnel CloudBridge Connector y se denominan pares.

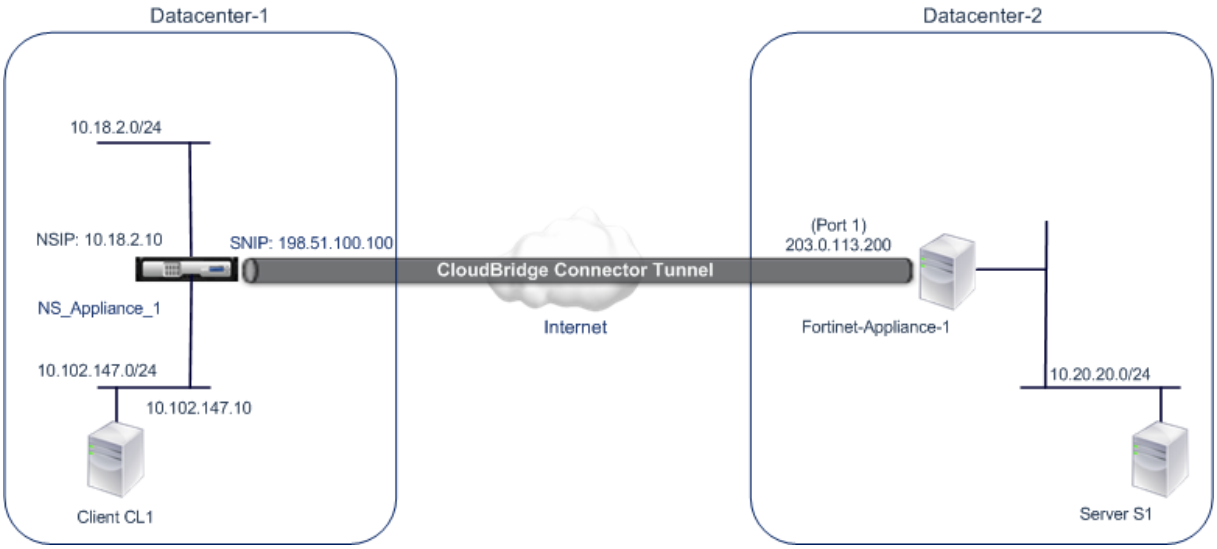
Ejemplo de configuración de túnel de CloudBridge Connector

Como ilustración del flujo de tráfico en un túnel de CloudBridge Connector, considere un ejemplo en el que se configura un túnel de CloudBridge Connector entre los siguientes dispositivos:

- Dispositivo Citrix ADC NS_Appliance-1 en un centro de datos designado como Datacenter-1
- Dispositivo FortiGate Fortigate-Appliance-1 en un centro de datos designado como Datacenter-2

NS_Appliance-1 y Fortigate-Appliance-1 permiten la comunicación entre redes privadas en Datacenter-1 y Datacenter-2 a través del túnel CloudBridge Connector. En el ejemplo, NS_Appliance-1 y Fortigate-Appliance-1 permiten la comunicación entre el cliente CL1 en Datacenter-1 y el servidor S1 en Datacenter-2 a través del túnel CloudBridge Connector. El cliente CL1 y el servidor S1 están en diferentes redes privadas.

En NS_Appliance-1, la configuración del túnel de CloudBridge Connector incluye la entidad de perfil IPSec NS_Fortinet_IPSEC_Profile, la entidad de túnel de CloudBridge Connector NS_Fortinet_Tunnel y la entidad de redirección basada en directivas (PBR) NS_Fortinet_PBR.



Para obtener más información, consulte Tabla de configuración de túneles de CloudBridge Connector pdf

Para obtener información sobre la configuración de Fortinet Fortigate-Appliance-1 en Datacenter-2, consulte la tabla.

Puntos a tener en cuenta para una configuración de túnel de CloudBridge Connector

Antes de configurar un túnel de CloudBridge Connector entre un dispositivo Citrix ADC y un dispositivo FortiGate, tenga en cuenta los siguientes puntos:

- La siguiente configuración de IPSec se admite para un túnel de CloudBridge Connector entre un dispositivo Citrix ADC y un dispositivo FortiGate.

Propiedades IPSec	Parámetros
Modo IPSec	Modo túnel
Versión de IKE	Versión 1
Grupo IKE DH	Grupo DH 2 (algoritmo MODP de 1024 bits)
Método de autenticación IKE	Clave previamente compartida
Algoritmo de cifrado IKE	AES
Algoritmo hash IKE	HMAC SHA1
Algoritmo de cifrado ESP	AES
Algoritmo hash ESP	HMAC SHA1

- Debe especificar la misma configuración de IPSec en el dispositivo Citrix ADC y en el dispositivo FortiGate en los dos extremos de CloudBridge Connector.
- Citrix ADC proporciona un parámetro común (en perfiles IPSec) para especificar un algoritmo hash IKE y un algoritmo hash ESP. También proporciona otro parámetro común para especificar un algoritmo de cifrado IKE y un algoritmo de cifrado ESP. Por lo tanto, en el dispositivo FortiGate, debe especificar el mismo algoritmo hash y el mismo algoritmo de cifrado en IKE (configuración de fase 1) y ESP (configuración de fase 2).
- Debe configurar el firewall en el extremo Citrix ADC y en el extremo FortiGate para permitir lo siguiente.
  - Cualquier paquete UDP para el puerto 500
  - Cualquier paquete UDP para el puerto 4500
  - Cualquier paquete ESP (protocolo IP número 50)
- El dispositivo FortiGate admite dos tipos de túneles VPN: Basados en directivas y basados en rutas. Solo se admite el túnel VPN basado en directivas entre un dispositivo FortiGate y un dispositivo Citrix ADC.

Configuración del dispositivo FortiGate para el túnel CloudBridge Connector

Para configurar un túnel de CloudBridge Connector en un dispositivo FortiGate, utilice el Administrador basado en web de Fortinet, que es la interfaz de usuario principal para configurar, supervisar y mantener los dispositivos FortiGate.

Antes de comenzar la configuración del túnel de CloudBridge Connector en un dispositivo FortiGate, asegúrese de que:

- Tiene una cuenta de usuario con credenciales de administrador en el dispositivo FortiGate.
- Está familiarizado con el Administrador basado en web de Fortinet.
- El dispositivo FortiGate está en funcionamiento, está conectado a Internet y también está conectado a las subredes privadas cuyo tráfico se va a proteger a través del túnel CloudBridge Connector.

> **Nota**
>
> Los procedimientos para configurar el túnel de CloudBridge Connector en un dispositivo FortiGate pueden cambiar con el tiempo, dependiendo del ciclo de lanzamiento de Fortinet. Citrix recomienda que siga la documentación oficial del producto de Fortinet para configurar túneles VPN IPSec.

Para configurar un túnel de conector CloudBridge entre un dispositivo Citrix ADC y un dispositivo FortiGate, realice las siguientes tareas en el dispositivo FortiGate mediante el administrador web de Fortinet:

- **Habilitar la función VPN IPSec basada**en directivas. Habilite esta función para crear túneles VPN basados en directivas en el dispositivo FortiGate. Solo se admite el tipo de túnel VPN basado en directivas entre un dispositivo FortiGate y un dispositivo Citrix ADC. Una configuración de túnel VPN basada en directivas en un dispositivo FortiGate incluye opciones de fase 1, configuración de fase 2 y una directiva de seguridad IPSec.
- **Defina los parámetros de fase 1.** El dispositivo FortiGate utiliza los parámetros de fase 1 para la autenticación IKE antes de formar un túnel seguro para el dispositivo Citrix ADC.
- **Defina los parámetros de fase 2**. El dispositivo FortiGate utiliza los parámetros de fase 2 para formar un túnel seguro para el dispositivo Citrix ADC mediante el establecimiento de asociaciones de seguridad IKE (SA).
- **Especifique subredes privadas**. Defina las subredes privadas de Fortigate y Citrix ADC cuyo tráfico IP se va a transportar a través del túnel.
- **Defina una directiva de seguridad IPSec para el túnel**. Una directiva de seguridad permite que el tráfico IP pase entre las interfaces de un dispositivo FortiGate. Una directiva de seguridad IPSec especifica la interfaz a la subred privada y la interfaz que conecta el dispositivo Citrix ADC a través del túnel.

Para habilitar la función VPN IPSec basada en directivas mediante el administrador web de Fortinet

1. Vaya a **Sistema** > **Config** > **Funciones**.
2. En la página **Configuración de funciones**, seleccione **Mostrar más** y active **VPN IPSec basada en directivas**.

Para definir parámetros de fase 1 mediante el administrador web de Fortinet

1. Vaya a **VPN** > **IPSec** > **Clave automática (IKE)** y haga clic en **Crear fase 1**.
2. En la página **Nueva fase 1**, establezca los siguientes parámetros:
    - Nombre: Introduzca un nombre para esta configuración de fase 1.
    - Puerta de enlace remota: Seleccione *Dirección IP estática.*
    - Modo: Seleccione *Principal (Protección de ID)*.
    - Método de autenticación: Seleccione la *clave previamente compartida*.
    - Clave previamente compartida: Introduzca una clave previamente compartida. La misma clave previamente compartida debe configurarse en el dispositivo Citrix ADC.
    - Opciones del mismo nivel: Defina los siguientes parámetros IKE para autenticar un dispositivo Citrix ADC.
        - Versión IKE: Seleccione *1*.
        - Configuración del modo: Desactive esta opción si está seleccionada.
        - IP de puerta de enlace local: Seleccione *IP de interfaz principal*.
        - Propuesta P1: Seleccione los algoritmos de cifrado y autenticación para la autenticación IKE antes de formar un túnel seguro para el dispositivo Citrix ADC.
            * 1: Cifrado: Seleccione *AES128*.
            * Autenticación: Seleccione *SHA1*.

        * Vida clave: Introduzca una cantidad de tiempo (en segundos) para la vida de la clave de fase 1.
        * Grupo DH: Seleccione 2.
      - X-Auth: Seleccione *Desactivar*.
      - Detección de pares de escritura: Seleccione esta opción.
3. Haga clic en **Aceptar**.

Para especificar subredes privadas mediante el administrador web de Fortinet

1. Vaya a **Objetos de firewall** > **Dirección** > **Direcciones** y seleccione **Crear nuevo**.
2. En la página **Nueva dirección**, establezca los siguientes parámetros:
   - Nombre: Introduzca un nombre para la subred Fortigate.
   - Tipo: Seleccione *Subred*.
   - Subred/ Rango IP: Introduzca la dirección de la subred Fortigate.
   - Interfaz: Seleccione la interfaz local para esta subred.
3. Haga clic en **Aceptar**.
4. Repita los pasos 1 a 3 para especificar la subred del lado de Citrix ADC.

Para definir parámetros de fase 2 mediante el administrador web de Fortinet

1. Vaya a **VPN** > **IPSec** > **Clave automática (IKE)** y haga clic en **Crear fase 2**.
2. En la página **Nueva fase 2**, establezca los siguientes parámetros:
   - Nombre: Introduzca un nombre para esta configuración de fase 2.
   - Fase 1: Seleccione la configuración de Fase 1 de la lista desplegable.
3. Haga clic en **Avanzadas** y defina los siguientes parámetros:
   - Propuesta de P2: Seleccione los algoritmos de cifrado y autenticación para formar un túnel seguro para el dispositivo Citrix ADC.
     - 1: Cifrado: Seleccione *AES128*.
     - Autenticación: Seleccione *SHA1*.
     - Activar detección de reproducción: Seleccione esta opción.
     - Habilitar el secreto directo perfecto (PFS): Seleccione esta opción.
     - Grupo DH: Seleccione *2*.
   - Vida clave: Introduzca una cantidad de tiempo (en segundos) para la vida de la clave de fase 2.
   - Autoclave Keep Alive: Seleccione esta opción.
   - Negociación automática: Seleccione esta opción.
   - Selector de modo rápido: Especifique las subredes privadas de Fortigate y Citrix ADC cuyo tráfico se recorra a través del túnel.
     - Dirección de origen: Seleccione la subred Fortigate de la lista desplegable.
     - Puerto de origen: Escriba *0*.
     - Dirección de destino: Seleccione la subred del lado de Citrix ADC en la lista desplegable.

- Puerto de destino: Escriba *0*.
- Protocolo: Escriba *0*.

4. Haga clic en **Aceptar**.

Para definir una directiva de seguridad IPSec mediante el administrador web de Fortinet

1. Vaya a **Directiva** > **Directiva** > **Directiva** y haga clic en **Crear nuevo**.
2. En la página **Modificar directiva**, establezca los siguientes parámetros:
   - Tipo de directiva: Seleccione *VPN*.
   - Subtipo de directiva: Seleccione *IPSec*.
   - Interfaz local: Seleccione la interfaz local a la red interna (privada).
   - Subred protegida local: Seleccione la subred Fortigate de la lista desplegable cuyo tráfico se recorra a través del túnel.
   - Interfaz VPN saliente: Seleccione la interfaz local para la red externa (pública).
   - Subred protegida remota: Seleccione la subred del lado de Citrix ADC de la lista desplegable cuyo tráfico se recorra a través del túnel.
   - Programar: Mantenga la configuración predeterminada (*siempre*) a menos que se necesiten cambios para cumplir requisitos específicos.
   - Servicio: Mantenga la configuración predeterminada (*CUALQUIERA*) a menos que se necesiten cambios para cumplir con sus requisitos específicos.
   - Túnel VPN: Seleccione *Usar existente* y seleccione el túnel en la lista desplegable.
   - Permitir que el tráfico se inicie desde el sitio remoto: Seleccione si el tráfico de la red remota podrá iniciar el túnel.
3. Haga clic en **Aceptar**.

Configuración del dispositivo Citrix ADC para el túnel de CloudBridge Connector

Para configurar un túnel de CloudBridge Connector entre un dispositivo Citrix ADC y un dispositivo FortiGate, realice las siguientes tareas en el dispositivo Citrix ADC. Puede utilizar la línea de comandos de Citrix ADC o la interfaz gráfica de usuario (GUI) de Citrix ADC:

- **Cree un perfil IPSec**. Una entidad de perfil IPSec especifica los parámetros del protocolo IPSec, como la versión IKE, el algoritmo de cifrado, el algoritmo hash y el método de autenticación que utilizará el protocolo IPSec en el túnel de CloudBridge Connector.
- **Cree un túnel IP que utilice el protocolo IPSec y asocie el perfil IPSec con él**. Un túnel IP especifica la dirección IP local (dirección IP de punto final del túnel de CloudBridge Connector (de tipo SNIP) configurada en el dispositivo Citrix ADC), la dirección IP remota (dirección IP del extremo del túnel de CloudBridge Connector configurada en el dispositivo FortiGate), el protocolo (IPSec) utilizado para configurar CloudBridge Túnel de conector y una entidad de perfil IPSec. La entidad de túnel IP creada también se denomina entidad de túnel CloudBridge Connector.
- **Cree una regla PBR y asociarla con el túnel IP**. Una entidad PBR especifica un conjunto de reglas y una entidad de túnel IP (túnel CloudBridge Connector). El intervalo de direcciones IP

de origen y el intervalo de direcciones IP de destino son las condiciones para la entidad PBR. Establezca el intervalo de direcciones IP de origen para especificar la subred del lado de Citrix ADC cuyo tráfico se va a proteger a través del túnel, y establezca el intervalo de direcciones IP de destino para especificar la subred del lado del dispositivo FortiGate cuyo tráfico se va a proteger a través del túnel.

Para crear un perfil IPSEC mediante la línea de comandos de Citrix ADC

En el símbolo del sistema, escriba:

- `add ipsec profile <name> -psk <string> -ikeVersion v1 -encAlgo AES -hashAlgo HMAC_SHA1 -perfectForwardSecrecy ENABLE`
- `show ipsec profile <name>`

Para crear un túnel IPSEC y enlazar el perfil IPSEC con él mediante la línea de comandos de Citrix ADC

En el símbolo del sistema, escriba:

- `add ipTunnel <name> <remote> <remoteSubnetMask> <local> -protocol IPSEC -ipsecProfileName** <string>`
- `show ipTunnel <name>`

Para crear una regla PBR y enlazar el túnel IPSEC con ella mediante la línea de comandos de Citrix ADC

En el símbolo del sistema, escriba:

- `add pbr <pbrName> ALLOW -srcIP <subnet-range> -destIP <subnet-range> -ipTunnel <tunnelName>`
- `apply pbrs`
- `show pbr <pbrName>`

Para crear un perfil IPSEC mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **Conector de CloudBridge** > **Perfil IPSec**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En la página **Agregar perfil IPSec**, establezca los siguientes parámetros:
   - Nombre
   - Algoritmo de cifrado
   - Algoritmo hash
   - Versión del protocolo IKE
   - Secreto directo perfecto (Habilitar este parámetro)
4. Configure el método de autenticación IPSec que utilizarán los dos pares de túnel de Cloud-Bridge Connector para autenticarse mutuamente: seleccione el método de autenticación de clave previamente compartida y establezca el parámetro Pre-Shared Key Exists.
5. Haga clic en **Crear** y, a continuación, en **Cerrar**.

Para crear un túnel IP y enlazar el perfil IPSEC con él mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **Conector de CloudBridge** > **Túneles IP**.
2. En la ficha **Túneles IPv4**, haga clic en **Agregar**.
3. En la página **Agregar túnel IP**, establezca los siguientes parámetros:
   - Nombre
   - IP remota
   - Máscara remota
   - Tipo de IP local (en la lista desplegable Tipo de IP local, seleccione *IP de subred*).
   - IP local (todas las direcciones IP configuradas del tipo IP seleccionado se encuentran en la lista desplegable de IP local. Seleccione la IP deseada de la lista.)
   - Protocolo
   - Perfil IPSec
4. Haga clic en **Crear** y, a continuación, en **Cerrar**.

Para crear una regla PBR y enlazar el túnel IPSEC con ella mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **Red** > **PBR**.
2. En la ficha **PBR**, haga clic en **Agregar**.
3. En la página **Crear PBR**, establezca los siguientes parámetros:
   - Nombre
   - Action
   - Tipo de salto siguiente (Seleccionar *túnel IP*)
   - Nombre del túnel IP
   - IP de origen bajo
   - IP de origen alto
   - IP de destino bajo
   - IP de destino alto
4. Haga clic en **Crear** y, a continuación, en **Cerrar**.

La nueva configuración de túnel de CloudBridge Connector correspondiente en el dispositivo Citrix ADC aparece en la GUI.

El estado actual del túnel del conector de CloudBridge se muestra en el panel Connector configurado de CloudBridge. Un punto verde indica que el túnel está arriba. Un punto rojo indica que el túnel está caído.

Los siguientes comandos crean la configuración del dispositivo Citrix ADC NS_Appliance-1 en “Ejemplo de una configuración de conector de CloudBridge.”

```
1      > add ipsec profile NS_Fortinet_IPSec_Profile -psk
         examplepresharedkey -ikeVersion v1 - encAlgo AES - hashalgo
         HMAC_SHA1 - lifetime 315360 -perfectForwardSecrecy ENABLE
2
3       Done
```



```
4       >  add iptunnel NS_Fortinet_Tunnel 203.0.113.200 255.255.255.255
           198.51.100.100  -protocol IPSEC  -ipsecProfileName
           NS_Fortinet_IPSec_Profile
5
6        Done
7       > add pbr NS_Fortinet_Pbr -srcIP 10.102.147.0-10.102.147.255  -
           destIP 10.20.0.0-10.20.255.255  -ipTunnel NS_Fortinet_Tunnel
8
9        Done
10      > apply pbrs
11
12       Done
13  <!--NeedCopy-->
```

Supervisión del túnel de CloudBridge Connector

Puede supervisar el rendimiento de los túneles de CloudBridge Connector en un dispositivo Citrix ADC mediante contadores estadísticos del túnel de CloudBridge Connector. Para obtener más información sobre cómo mostrar estadísticas de túnel de CloudBridge Connector en un dispositivo Citrix ADC, consulte Supervisión de túneles de CloudBridge Connector.

Diagnóstico y solución de problemas del túnel de CloudBridge Connector

August 20, 2021

Si tiene problemas con la configuración del túnel de CloudBridge Connector, asegúrese de que se han cumplido todos los requisitos previos antes de configurar el túnel. Si lo fueran, el problema podría deberse a las direcciones IP de punto final del túnel, una configuración NAT, la forma en que se configuró el túnel o con el tráfico de datos.

Solución de problemas de un túnel de CloudBridge Connector

Si el túnel de CloudBridge Connector no funciona correctamente, el problema podría deberse al establecimiento del túnel o al tráfico de datos. Si no está seguro del tipo de problema que tiene, busque un mensaje de error en el archivo de registro y vea si el mensaje de error está en la lista de problemas con el establecimiento de túneles. Si no encuentra su mensaje de error, compruebe la lista de posibles problemas relacionados con el tráfico de datos.

Cuestiones relacionadas con el establecimiento de túneles

Una vez que se cumplan los requisitos para configurar el túnel IPSec y se haya configurado el túnel CloudBridge Connector, si el estado del túnel no es UP, busque información de depuración en el archivo iked.log en uno o ambos dispositivos Citrix ADC configurados como los puntos finales del túnel.

En cualquiera de los dispositivos, escriba el comando siguiente en el símbolo del shell de Citrix ADC:

```
cat /tmp/iked.debug | tee /var/iked.log
```

El pdf de solución de problemas enumera algunos errores comunes y sus soluciones.

Problemas relacionados con el tráfico de datos

Si los datos del túnel CloudBridge Connector no se intercambian correctamente entre los puntos finales del túnel, haga lo siguiente.

- Para un túnel de CloudBridge Connector que utiliza protocolos GRE e IPSec:
  - Asegúrese de que el modo L2 está habilitado en ambos puntos finales del túnel de CloudBridge Connector. Para habilitar el modo L2, escriba el siguiente comando en la interfaz de línea de comandos de Citrix ADC:

    ```
    enable mode L2
    ```

    * Si uno de los puntos finales del túnel de CloudBridge Connector es un dispositivo virtual CloudBridge (VPX) y se aprovisiona en un Hypervisor VMware ESXi, asegúrese de que el modo promiscuo está configurado en Aceptar para el conmutador virtual asociado con el dispositivo CloudBridge VPX.
  - Si una VLAN se extiende a través de un túnel de CloudBridge Connector, verifique la asignación uno a uno en la entidad de VLAN extendida en cada uno de los puntos finales del túnel
  - Asegúrese de que la entidad de túnel IP está enlazada a la entidad netbridge correcta en cada uno de los puntos finales del túnel.
  - Compruebe que la entrada ARP para el punto final del túnel CloudBridge Connector del mismo nivel existe en el punto final del túnel local, escribiendo el siguiente comando en la interfaz de línea de comandos Citrix ADC:

    ```
    show arp
    ```
  - Si la salida muestra una entrada ARP incompleta, el tráfico bidireccional no fluye a través del túnel. Si el tráfico bidireccional fluye, la entrada ARP muestra el nombre de la interfaz del túnel para los dispositivos del otro lado del túnel.
  - Elimine las entidades de túnel IP de ambos puntos finales del túnel y agréguelas de nuevo con los mismos parámetros, pero con el perfil IPSec establecido en NONE, de modo que el túnel utilice solo el protocolo GRE.

Después de verificar lo siguiente en el túnel IP (que utiliza el protocolo GRE), configure el túnel con parámetros IPSec especificando un perfil IPSec válido para las entidades de túnel IP respectivas en cada uno de los puntos finales del túnel.
Flujo PING o TCP adecuado a través del túnel.Flujo
adecuado del tráfico de datos a través del túnel.
Después de que el túnel configurado (que utiliza los protocolos GRE e IPSec) esté en estado ACTIVO, si el tráfico de datos no fluye correctamente a través del túnel y si se ha implementado un dispositivo NAT delante de cualquiera o ambos puntos finales del túnel, analice los paquetes de entrada y salida en los dispositivos NAT.

- Si se utiliza un dispositivo Citrix ADC como enrutador o puerta de enlace.
  - Asegúrese de que el modo L3 está habilitado en el dispositivo Citrix ADC. Para habilitar el modo L3, ejecute el siguiente comando en la línea de comandos de CloudBridge.
  - modo de habilitar L3
  - Si las subredes están enlazadas a una entidad netbridge, asegúrese de que la entidad IP túnel correcta también está enlazada a la netbridge.
  - Ejecute el siguiente comando en la línea de comandos de Citrix ADC para ver dónde se descartan los paquetes (entrada y salida):
    ```
    stat ipsec counters
    ```
  - Asegúrese de que las rutas correctas estén configuradas en ambos puntos finales del túnel.
  - Si no se implementa ningún dispositivo NAT delante del dispositivo Citrix ADC, asegúrese de que los firewalls estén configurados para permitir paquetes ESP (protocolo IP número 50) y paquetes UDP para el puerto 4500.

Si ninguna de las medidas anteriores da como resultado un intercambio correcto de tráfico entre los puntos finales del túnel, póngase en contacto con el soporte técnico de Citrix.

Lista de comprobación antes de ponerse en contacto con el soporte técnico de Citrix

Para obtener una resolución rápida, asegúrese de tener los siguientes elementos listos antes de ponerse en contacto con el servicio de asistencia técnica de Citrix.

- Detalles de la implementación y la topología de red.
- Archivo de registro recopilado escribiendo el siguiente comando en el símbolo del shell de Citrix ADC.
  ```
  cat /tmp/iked.debug | tee /var/log/iked.log
  ```
- Paquete de soporte técnico capturado escribiendo el siguiente comando en la línea de comandos de Citrix ADC.
  ```
  show techsupport
  ```
- Rastreos de paquetes capturados en ambos puntos finales del túnel de CloudBridge Connector. Para iniciar un seguimiento de paquetes, escriba el siguiente comando en la línea de comandos

de Citrix ADC.

```
start nstrace -size 0
```

Para detener el seguimiento de paquetes, escriba el siguiente comando en la línea de comandos de Citrix ADC.

```
stop nstrace
```

- Salida del siguiente comando escrito en el símbolo del sistema de Citrix ADC.

```
show arp
```

Interoperabilidad del conector CloudBridge: StrongSwan

October 5, 2021

StrongSwan es una implementación IPSec de código abierto para plataformas Linux. Puede configurar un túnel de CloudBridge Connector entre un dispositivo Citrix ADC y un dispositivo StrongSwan para conectar dos centros de datos o ampliar la red a un proveedor de nube. El dispositivo Citrix ADC y el dispositivo StrongSwan forman los puntos finales del túnel CloudBridge Connector y se denominan pares.

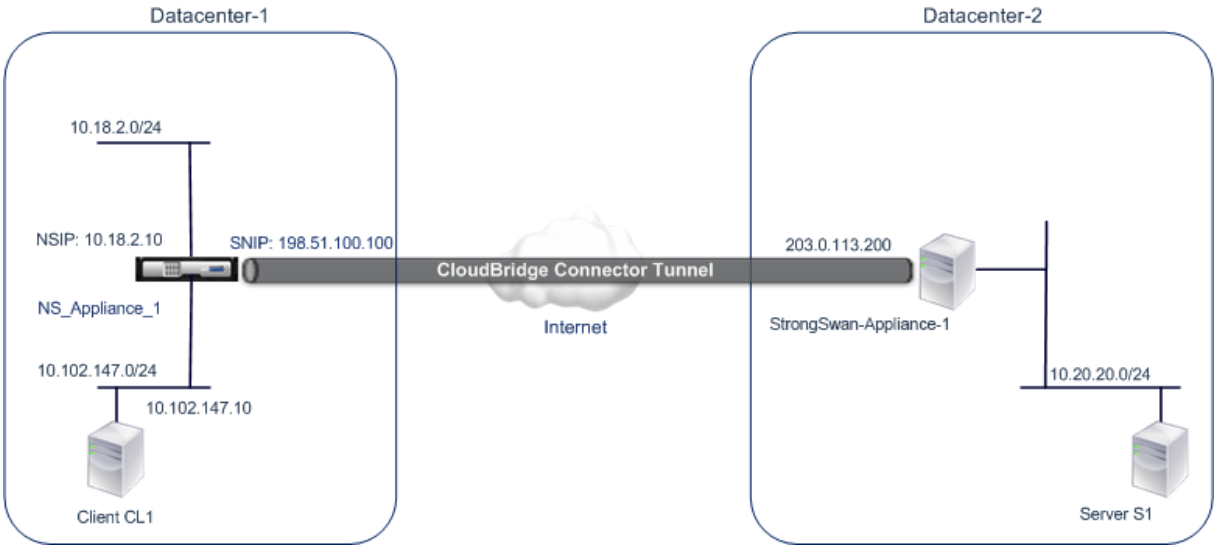
Ejemplo de configuración de túnel de CloudBridge Connector

Como ilustración del flujo de tráfico en un túnel de CloudBridge Connector, considere un ejemplo en el que se configura un túnel de CloudBridge Connector entre los siguientes dispositivos:

- Dispositivo Citrix ADC NS_Appliance-1 en un centro de datos designado como Datacenter-1
- Dispositivo StrongSwan StrongSwan-Appliance-1 en un centro de datos designado como Datacenter-2

NS_Appliance-1 y StrongSwan-Appliance-1 permiten la comunicación entre redes privadas en Datacenter-1 y Datacenter-2 a través del túnel CloudBridge Connector. En el ejemplo, NS_Appliance-1 y StrongSwan-Appliance-1 permiten la comunicación entre el cliente CL1 en Datacenter-1 y el servidor S1 en Datacenter-2 a través del túnel CloudBridge Connector. El cliente CL1 y el servidor S1 están en diferentes redes privadas.

En NS_Appliance-1, la configuración del túnel del conector de CloudBridge incluye la entidad de perfil IPSec NS_StrongSwan_IPSEC_Profile, la entidad del túnel del conector de CloudBridge NS_StrongSwan_Tunnel y la entidad de redirección basada en directivas (PBR) NS_StrongSwan_PBR.



En la tabla siguiente se enumeran los parámetros utilizados en este ejemplo.

Configuración principal de la configuración del túnel de CloudBridge Connector

Entidad	Detalles
Dirección IP del punto final del túnel CloudBridge Connector (NS_Appliance-1) en Datacenter-1	198.51.100.100
Dirección IP del punto final del túnel CloudBridge Connector (StrongSwan-Appliance-1) en Datacenter-2	203.0.113.200
Datacenter: Subred de 1 cuyo tráfico debe protegerse sobre el túnel de CloudBridge Connector	10.102.147.0/24
Datacenter: Subred de 2 cuyo tráfico debe protegerse sobre el túnel de CloudBridge Connector	10.20.20.0/24

Configuración del dispositivo Citrix ADC NS_Appliance-1 en Datacenter-1

SNIP1 (solo para fines de referencia)	198.51.100.100	
IPSec profile	NS_StrongSwan_IPSec_Profile	IKE version: V1, Encryption algorithm: AES, Hash algorithm: HMAC_SHA1

SNIP1 (solo para fines de referencia)	198.51.100.100	
psk = examplepresharedkey (Nota: Este es un ejemplo de una clave precompartida. Citrix no recomienda usar esta cadena en la configuración de su CloudBridge Connector.)		
CloudBridge Connector tunnel	NS_StrongSwan_Tunnel	Remote IP = 203.0.113.200, Local IP= 198.51.100.100, Tunnel protocol = IPSEC, IPSec profile= NS_StrongSwan_IPSec_Profile
Policy based route	NS_StrongSwan_Pbr	Source IP range = Subnet in the Datacenter-1=10.102.147.0-10.102.147.255, Destination IP range =Subnet in Datacenter-2=10.20.20.0-10.20.20.255, IP Tunnel = NS_StrongSwan_Tunnel

Puntos a tener en cuenta para una configuración de túnel de CloudBridge Connector

Antes de comenzar a configurar el túnel del conector de CloudBridge, asegúrese de que:

- Usted tiene un conocimiento básico sobre las configuraciones de Linux.
- Tiene conocimientos básicos sobre el conjunto de protocolos IPSec.
- El dispositivo StrongSwan está en funcionamiento, está conectado a Internet y también está conectado a las subredes privadas cuyo tráfico se va a proteger a través del túnel CloudBridge Connector.
- El dispositivo Citrix ADC está en funcionamiento, está conectado a Internet y también está conectado a las subredes privadas cuyo tráfico se va a proteger a través del túnel CloudBridge Connector.
- La siguiente configuración de IPSec se admite para un túnel de CloudBridge Connector entre un dispositivo Citrix ADC y un dispositivo StrongSwan.
  - Modo IPSec: Modo túnel
  - Versión IKE: Versión 1
  - Método de autenticación IKE: Clave previamente compartida

  - Algoritmo de cifrado IKE: AES
  - Algoritmo hash IKE: HMAC SHA1
  - Algoritmo de cifrado ESP: AES
  - Algoritmo hash ESP: HMAC SHA1
- Debe especificar la misma configuración IPSec en el dispositivo Citrix ADC y en el dispositivo StrongSwan en los dos extremos del túnel CloudBridge Connector.
- Citrix ADC proporciona un parámetro común (en perfiles IPSec) para especificar un algoritmo hash IKE y un algoritmo hash ESP. También proporciona otro parámetro común para especificar un algoritmo de cifrado IKE y un algoritmo de cifrado ESP. Por lo tanto, en el dispositivo StrongSwan, debe especificar el mismo algoritmo hash y el mismo algoritmo de cifrado en los parámetros IKE y ESP en el archivo IPsec.conf.
- Debe configurar el firewall en el extremo Citrix ADC y en el extremo StrongSwan para permitir lo siguiente.
  - Cualquier paquete UDP para el puerto 500
  - Cualquier paquete UDP para el puerto 4500
  - Cualquier paquete ESP (protocolo IP número 50)

Configurar StrongSwan para el túnel CloudBridge Connector

Para configurar un túnel de conector CloudBridge entre un dispositivo Citrix ADC y un dispositivo StrongSwan, realice las siguientes tareas en el dispositivo StrongSwan:

- **Especifique la información de conexión IPSec en el archivo ipsec.conf. El archivo**ipsec.conf define toda la información de control y configuración para las conexiones IPSec en el dispositivo StrongSwan.
- **Especifique clave previamente compartida en el archivo ipsec.secrets. El archivo**ipsec.secrets define secretos para la autenticación IKE/IPSec para conexiones IPSec en el dispositivo StrongSwan.

Los procedimientos para configurar IPSec VPN (túnel de conector de CloudBridge) en un dispositivo StrongSwan pueden cambiar con el tiempo, dependiendo del ciclo de lanzamiento de StrongSwan. Citrix recomienda que siga la documentación oficial de StrongSwan para configurar túneles VPN IPsec.

El siguiente extracto de ejemplo del archivo ipsec.conf especifica la información IPSec para configurar el túnel VPN IPSec, que se describe en el tema Ejemplo de una configuración de conector CloudBridge. Para obtener más información, consulte Configuración de CloudBridge Connector pdf.

El siguiente extracto de ejemplo del archivo ipsec.secrets especifica la clave previamente compartida de autenticación IKE para configurar el túnel VPN IPSec, que se describe en el tema Ejemplo de una configuración de conector de CloudBridge.

`/etc/ipsec.secrets` PSK 'examplepresharedkey' #pre -clave compartida para la autenticación IKE IPSec

Configuración del dispositivo Citrix ADC para el túnel de CloudBridge Connector

Para configurar un túnel de CloudBridge Connector entre un dispositivo Citrix ADC y un dispositivo StrongSwan, realice las siguientes tareas en el dispositivo Citrix ADC. Puede utilizar la línea de comandos de Citrix ADC o la interfaz gráfica de usuario (GUI) de Citrix ADC:

- **Cree un perfil IPSec**. Una entidad de perfil IPSec especifica los parámetros del protocolo IPSec, como la versión IKE, el algoritmo de cifrado, el algoritmo hash y el método de autenticación que utilizará el protocolo IPSec en el túnel de CloudBridge Connector.
- **Cree un túnel IP que utilice el protocolo IPSec y asocie el perfil IPSec con él**. Un túnel IP especifica la dirección IP local (dirección IP del extremo del túnel de CloudBridge Connector (de tipo SNIP) configurada en el dispositivo Citrix ADC), la dirección IP remota (dirección IP del extremo del túnel de CloudBridge Connector configurada en el dispositivo StrongSwan), el protocolo (IPSec) utilizado para configurar CloudBridge Túnel de conector y una entidad de perfil IPSec. La entidad de túnel IP creada también se denomina entidad de túnel CloudBridge Connector.
- **Cree una regla PBR y asociarla con el túnel IP**. Una entidad PBR especifica un conjunto de reglas y una entidad de túnel IP (túnel CloudBridge Connector). El intervalo de direcciones IP de origen y el intervalo de direcciones IP de destino son las condiciones para la entidad PBR. Establezca el rango de direcciones IP de origen para especificar la subred del lado de Citrix ADC cuyo tráfico se va a proteger sobre el túnel, y establezca el rango de direcciones IP de destino para especificar la subred del lado StrongSwan cuyo tráfico se va a proteger sobre el túnel.

Para crear un perfil IPSEC mediante la línea de comandos de Citrix ADC

En el símbolo del sistema, escriba:

- `add ipsec profile <name> -psk <string> -ikeVersion v1 -encAlgo AES -hashAlgo HMAC_SHA1`
- `show ipsec profile <name>`

Para crear un túnel IPSEC y enlazar el perfil IPSEC con él mediante la línea de comandos de Citrix ADC

En el símbolo del sistema, escriba:

- `add ipTunnel <name> <remote> <remoteSubnetMask> <local> -protocol IPSEC -ipsecProfileName <string>`
- `show ipTunnel <name>`

Para crear una regla PBR y enlazar el túnel IPSEC con ella mediante la línea de comandos de Citrix ADC

En el símbolo del sistema, escriba:

- `add pbr <pbrName> ALLOW -srcIP <subnet-range> -destIP <subnet-range> -ipTunnel <tunnelName>`
- `apply pbrs`
- `show pbr <pbrName>`

Para crear un perfil IPSEC mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **Conector** de **CloudBridge** > **PerfilIPSec**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En la página **Agregar perfil IPSec**, establezca los siguientes parámetros:
   - Nombre
   - Algoritmo de cifrado
   - Algoritmo hash
   - Versión del protocolo IKE
4. Configure el método de autenticación IPSec que utilizarán los dos pares de túnel de CloudBridge Connector para autenticarse mutuamente: Seleccione el **método de autenticación de clave previamente compartida** y establezca el parámetro La **clave precompartida existe** .
5. Haga clic en **Crear** y, a continuación, en **Cerrar**.

Para crear un túnel IP y enlazar el perfil IPSEC con él mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **Conector de CloudBridge** > **Túneles IP**.
2. En la ficha **Túneles IPv4**, haga clic en **Agregar**.
3. En la página Agregar túnel IP, establezca los siguientes parámetros:
   - Nombre
   - IP remota
   - Máscara remota
   - Tipo de IP local (en la lista desplegable Tipo de IP local, seleccione *IP de subred*).
   - IP local (todas las direcciones IP configuradas del tipo IP seleccionado se encuentran en la lista desplegable IP local. Seleccione la IP deseada de la lista.)
   - Protocolo
   - Perfil IPSec
4. Haga clic en **Crear** y, a continuación, en **Cerrar**.

Para crear una regla PBR y enlazar el túnel IPSEC con ella mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **Red** > **PBR**.
2. En la ficha **PBR**, haga clic en **Agregar**.
3. En la página **Crear PBR**, establezca los siguientes parámetros:
   - Nombre
   - Action
   - Tipo de salto siguiente (Seleccionar *túnel IP*)
   - Nombre del túnel IP
   - IP de origen bajo

- IP de origen alto
- IP de destino bajo
- IP de destino alto

4. Haga clic en **Crear** y, a continuación, en **Cerrar**.

La nueva configuración de túnel de CloudBridge Connector correspondiente en el dispositivo Citrix ADC aparece en la GUI. El estado actual del túnel del conector de CloudBridge se muestra en el panel Connector configurado de CloudBridge. Un punto verde indica que el túnel está arriba. Un punto rojo indica que el túnel está caído.
Los siguientes comandos crean la configuración del dispositivo Citrix ADC NS_Appliance-1 en "Ejemplo de una configuración de conector de CloudBridge:

```
1      > add ipsec profile NS_StrongSwan_IPSec_Profile -psk
           examplepresharedkey -ikeVersion v1 - encAlgo AES - hashalgo
           HMAC_SHA1
2
3
4      Done
5
6      > add iptunnel NS_StrongSwan_Tunnel 203.0.113.200 255.255.255.255
           198.51.100.100 - protocol IPSEC - ipsecProfileName
           NS_StrongSwan_IPSec_Profile
7
8
9      Done
10
11     > add pbr NS_StrongSwan_Pbr -srcIP 10.102.147.0-10.102.147.255 -
           destIP 10.20.0.0-10.20.255.255 - ipTunnel NS_StrongSwan_Tunnel
12
13
14     Done
15
16     > apply pbrs
17
18
19     Done
20 <!--NeedCopy-->
```

Supervisión del túnel de CloudBridge Connector

Puede supervisar el rendimiento de los túneles de CloudBridge Connector en un dispositivo Citrix ADC mediante contadores estadísticos del túnel de CloudBridge Connector. Para obtener más infor-

mación sobre cómo mostrar estadísticas de túnel de CloudBridge Connector en un dispositivo Citrix ADC, consulte Supervisión de túneles de CloudBridge Connector.

Interoperabilidad de CloudBridge Connector: F5 BIG-IP

August 20, 2021

Puede configurar un túnel de CloudBridge Connector entre un dispositivo Citrix ADC y un dispositivo F5 BIG-IP para conectar dos centros de datos o ampliar la red a un proveedor de nube. El dispositivo Citrix ADC y el dispositivo F5 BIG-IP forman los puntos finales del túnel de CloudBridge Connector y se denominan pares.

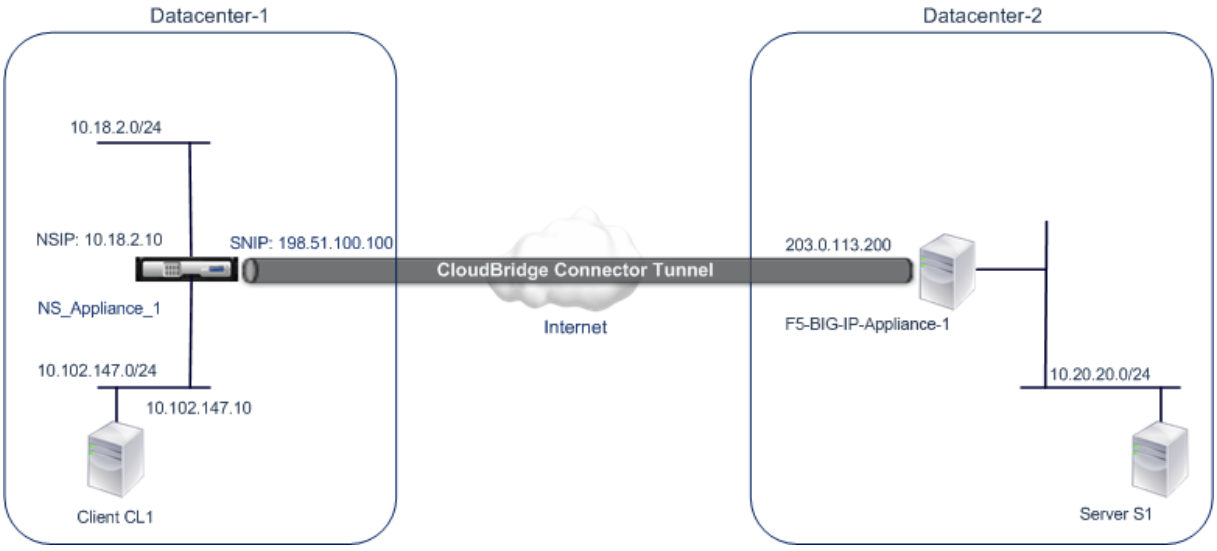
Ejemplo de configuración de túnel de CloudBridge Connector

Como ilustración del flujo de tráfico en un túnel de CloudBridge Connector, considere un ejemplo en el que se configura un túnel de CloudBridge Connector entre los siguientes dispositivos:

- Dispositivo Citrix ADC NS_Appliance-1 en un centro de datos designado como Datacenter-1
- Dispositivo F5 BIG-IP F5-BIG-IP-Spliance-1 en un centro de datos designado como Datacenter-2

NS_Appliance-1 y F5-Big-IP-Appliance-1 permiten la comunicación entre redes privadas en Datacenter-1 y Datacenter-2 a través del túnel CloudBridge Connector. En el ejemplo, NS_Appliance-1 y F5-Big-IP-Appliance-1 permiten la comunicación entre el cliente CL1 en Datacenter-1 y el servidor S1 en Datacenter-2 a través del túnel CloudBridge Connector. El cliente CL1 y el servidor S1 están en diferentes redes privadas.

En NS_Appliance-1, la configuración del túnel de CloudBridge Connector incluye la entidad de perfil IPSec NS_F5-Big-IP_IPSEC_Profile, la entidad de túnel del conector de CloudBridge NS_F5-Big-IP_Tunnel y la entidad de redirección basada en directivas (PBR) NS_F5-Big-IP_PBR.



Para obtener más información, consulte F5 big IP pdf.

Puntos a tener en cuenta para una configuración de túnel de CloudBridge Connector

- El dispositivo Citrix ADC está en funcionamiento, está conectado a Internet y también está conectado a las subredes privadas cuyo tráfico se va a proteger a través del túnel CloudBridge Connector.
- El dispositivo F5 BIG-IP está en funcionamiento, está conectado a Internet y también está conectado a las subredes privadas cuyo tráfico se va a proteger a través del túnel CloudBridge Connector.
- La siguiente configuración de IPSec se admite para un túnel de CloudBridge Connector entre un dispositivo Citrix ADC y un dispositivo F5 BIG-IP.
  - Modo IPSec: Modo túnel
  - Versión IKE: Versión 1
  - Método de autenticación IKE: Clave previamente compartida
  - Algoritmo de cifrado IKE: AES
  - Algoritmo hash IKE: HMAC SHA1
  - Algoritmo de cifrado ESP: AES
  - Algoritmo hash ESP: HMAC SHA1
- Debe especificar la misma configuración IPSec en el dispositivo Citrix ADC y en el dispositivo F5 BIG-IP en los dos extremos del túnel CloudBridge Connector.
- Citrix ADC proporciona un parámetro común (en perfiles IPSec) para especificar un algoritmo hash IKE y un algoritmo hash ESP. También proporciona otro parámetro común para especificar un algoritmo de cifrado IKE y un algoritmo de cifrado ESP. Por lo tanto, en el dispositivo F5 BIG-IP, debe especificar el mismo algoritmo hash y el mismo algoritmo de cifrado en IKE (configuración de fase 1) y ESP (configuración de fase 2).

- Debe configurar el firewall en el extremo Citrix ADC y el extremo F5 BIG-IP para permitir lo siguiente.
  - Cualquier paquete UDP para el puerto 500
  - Cualquier paquete UDP para el puerto 4500
  - Cualquier paquete ESP (protocolo IP número 50)

Configuración de F5 BIG-IP para el túnel CloudBridge Connector

Para configurar un túnel de conector CloudBridge entre un dispositivo Citrix ADC y un dispositivo F5 BIG-IP, realice las siguientes tareas en el dispositivo F5 BIG-IP:

- **Cree un servidor virtual de reenvío para IPSec**. Un servidor virtual de reenvío intercepta el tráfico IP para el túnel IPSec.
- **Cree un par IKE.** Un par IKE especifica los extremos del túnel IPSec locales y remotos. También especifica algoritmos y credenciales que se utilizarán para IPSec IKE fase 1.
- **Cree una directiva IPSec personalizada.** Una directiva especifica el protocolo IPSec (ESP) y el modo (túnel) que se utilizará para formar el túnel IPSec. También especifica los algoritmos y parámetros de seguridad que se utilizarán para IKE IPSec fase 2.
- **Cree un selector de tráfico IPSec bidireccional**. Un selector de tráfico especifica las subredes F5 BIG-IP y Citrix ADC lado cuyo tráfico IP debe atravesarse a través del túnel IPSec.

Los procedimientos para configurar IPSec VPN (túnel de conector de CloudBridge) en un dispositivo F5 BIG-IP pueden cambiar con el tiempo, dependiendo del ciclo de lanzamiento de F5. Citrix recomienda seguir la documentación oficial de F5 BIG-IP para configurar túneles VPN IPSec, en:

https://f5.com

Para crear un servidor virtual de reenvío para IPSec mediante la GUI F5 BIG-IP

1. En la ficha **Principal**, haga clic en **Tráfico local** > **Servidores virtuales** y, a continuación, haga clic en **Crear**.
2. En la pantalla **Nueva lista de servidores virtuales**, establezca los siguientes parámetros:
   - **Name**. Escriba un nombre único para el servidor virtual.
   - **Tipo**. Seleccione **Reenvío (IP)**.
   - **Dirección de destino**. Escriba una dirección de red comodín en formato CIDR, por ejemplo, 0.0.0.0/0 para IPv4 para aceptar cualquier tráfico.
   - **Puerto de servicio**. Seleccione **Todos los puertos** de la lista.
   - **Lista de protocolos**. Seleccione **Todos los protocolos** de la lista.
   - **VLAN y tráfico de túnel**. Conservar la selección predeterminada, **Todas las VLAN y túneles**.
3. Haga clic en **Finalizado**.

Para crear una directiva IPSec personalizada mediante la GUI F5 BIG-IP

1. En la ficha **Principal**, haga clic en **Red** > **IPSec** > **Directivas IPSec** y, a continuación, haga clic en **Crear**.
2. En la pantalla **Nueva directiva**, establezca los siguientes parámetros:
   - **Name**. Escriba un nombre único para la directiva.
   - **Protocolo IPSec**. Conservar la selección predeterminada, ESP.
   - **Modo**. Seleccione Túnel. La pantalla se actualiza para mostrar configuraciones adicionales relacionadas.
   - **Dirección local del túnel**. Escriba la dirección IP del extremo del túnel IPSec local (configurada en el dispositivo F5 BIG-IP).
   - **Dirección remota del túnel**. Escriba la dirección IP del extremo del túnel IPSec remoto (configurada en el dispositivo Citrix ADC).
3. Para los parámetros IKE Phase 2, conserve los valores predeterminados o seleccione las opciones adecuadas para su implementación.
4. Haga clic en **Finalizado**.

Para crear un selector de tráfico IPSec bidireccional mediante la GUI F5 BIG-IP

1. En la ficha **Principal**, haga clic en **Red** > **IPSec** > **Selectores de tráfico** y, a continuación, haga clic en **Crear**.
2. En la pantalla **New Traffic Selector**, establezca los siguientes parámetros:
   - **Name**. Escriba un nombre único para el selector de tráfico.
   - **Orden**. Conservar el valor predeterminado **(First)**. Esta configuración especifica el orden en que aparece el selector de tráfico en la pantalla Lista de selectores de tráfico.
3. En la lista **Configuración**, seleccione **Avanzadas** y defina los siguientes parámetros:
   - **Dirección IP de origen**. Haga clic en **Host** o **Red** y, en el campo **Dirección**, escriba la dirección de la subred lateral BIG-IP F5 cuyo tráfico se va a proteger sobre el túnel IPSec.
   - **Puerto de origen**. Seleccione *** Todos los puertos**.
   - **Dirección IP de destino**. Haga clic en **Host** y, en el campo **Dirección**, escriba la dirección de la subred del lado Citrix ADC cuyo tráfico debe protegerse a través del túnel IPSec.
   - **Puerto de destino**. Seleccione *** Todos los puertos**.
   - **Protocolo**. Seleccione *** Todos los protocolos**.
   - **Dirección**. Seleccione **Ambos**.
   - **Acción**. Seleccione **Proteger**. Aparece la configuración **Nombre de directiva IPSec**.
   - **Nombre de directiva IPSec**. Seleccione el nombre de la directiva IPSec personalizada que creó.
4. Haga clic en **Finalizado**.

Configuración del dispositivo Citrix ADC para el túnel de CloudBridge Connector

Para configurar un túnel de CloudBridge Connector entre un dispositivo Citrix ADC y un dispositivo F5 BIG-IP, realice las siguientes tareas en el dispositivo Citrix ADC. Puede utilizar la línea de comandos de

Citrix ADC o la interfaz gráfica de usuario (GUI) de Citrix ADC:

- **Cree un perfil IPSec**. Una entidad de perfil IPSec especifica los parámetros del protocolo IPSec, como la versión IKE, el algoritmo de cifrado, el algoritmo hash y el método de autenticación que utilizará el protocolo IPSec en el túnel de CloudBridge Connector.
- **Cree un túnel IP que utilice el protocolo IPSec y asocie el perfil IPSec con él**. Un túnel IP especifica la dirección IP local (dirección IP de punto final del túnel de CloudBridge Connector (de tipo SNIP) configurada en el dispositivo Citrix ADC), la dirección IP remota (dirección IP del extremo del túnel de CloudBridge Connector configurada en el dispositivo F5 BIG-IP), el protocolo (IPSec) utilizado para configurar CloudBridge Túnel de conector y una entidad de perfil IPSec. La entidad de túnel IP creada también se denomina entidad de túnel CloudBridge Connector.
- **Cree una regla PBR y asociarla con el túnel IP**. Una entidad PBR especifica un conjunto de reglas y una entidad de túnel IP (túnel CloudBridge Connector). El intervalo de direcciones IP de origen y el intervalo de direcciones IP de destino son las condiciones para la entidad PBR. Establezca el intervalo de direcciones IP de origen para especificar la subred del lado de Citrix ADC cuyo tráfico se va a proteger a través del túnel, y establezca el intervalo de direcciones IP de destino para especificar la subred del lado BIG-IP F5 cuyo tráfico se va a proteger a través del túnel.

Para crear un perfil IPSEC mediante la línea de comandos de Citrix ADC

En el símbolo del sistema, escriba:

- `add ipsec profile <name> -psk <string> -ikeVersion v1 -encAlgo AES -hashAlgo HMAC_SHA1 -perfectForwardSecrecyENABLE`
- `show ipsec profile** <name>`

Para crear un túnel IPSEC y enlazar el perfil IPSEC con él mediante la línea de comandos de Citrix ADC

En el símbolo del sistema, escriba:

- `add ipTunnel <name> <remote> <remoteSubnetMask> <local> -protocol IPSEC -ipsecProfileName <string>`
- `show ipTunnel <name>`

Para crear una regla PBR y enlazar el túnel IPSEC con ella mediante la línea de comandos de Citrix ADC

En el símbolo del sistema, escriba:

- `add pbr <pbrName> ALLOW -srcIP <subnet-range> -destIP <subnet-range> -ipTunnel <tunnelName>`
- `apply pbrs`
- `show pbr <pbrName>`

Para crear un perfil IPSEC mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **Conector de CloudBridge** > **Perfil IPSec**.

2. En el panel de detalles, haga clic en **Agregar**.
3. En la página **Agregar perfil IPSec**, establezca los siguientes parámetros:
    - Nombre
    - Algoritmo de cifrado
    - Algoritmo hash
    - Versión del protocolo IKE
4. Configure el método de autenticación IPSec que utilizarán los dos pares de túnel de CloudBridge Connector para autenticarse mutuamente: Seleccione el **método de autenticación de clave previamente compartida** y establezca el parámetro La **clave precompartida existe** .
5. Haga clic en **Crear** y, a continuación, en **Cerrar**.

Para crear un túnel IP y enlazar el perfil IPSEC con él mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **Conector de CloudBridge** > **Túneles IP**.
2. En la ficha **Túneles IPv4**, haga clic en **Agregar**.
3. En la página **Agregar túnel IP**, establezca los siguientes parámetros:
    - Nombre
    - IP remota
    - Máscara remota
    - Tipo de IP local (en la lista desplegable Tipo de IP local, seleccione *IP de subred*).
    - IP local (todas las direcciones IP configuradas del tipo IP seleccionado se encuentran en la lista desplegable de IP local. Seleccione la IP deseada de la lista.)
    - Protocolo
    - Perfil IPSec
4. Haga clic en **Crear** y, a continuación, en **Cerrar**.

Para crear una regla PBR y enlazar el túnel IPSEC con ella mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **Red** > **PBR**.
2. En la ficha **PBR**, haga clic en **Agregar**.
3. En la página **Crear PBR**, establezca los siguientes parámetros:
    - Nombre
    - Action
    - Tipo de salto siguiente (Seleccionar *túnel IP*)
    - Nombre del túnel IP
    - IP de origen bajo
    - IP de origen alto
    - IP de destino bajo
    - IP de destino alto
4. Haga clic en **Crear** y, a continuación, en **Cerrar**.

La nueva configuración de túnel de CloudBridge Connector correspondiente en el dispositivo Citrix ADC aparece en la GUI. El estado actual del túnel del conector de CloudBridge se muestra en el panel

Connector configurado de CloudBridge. Un punto verde indica que el túnel está arriba. Un punto rojo indica que el túnel está caído.

Los siguientes comandos crean la configuración del dispositivo Citrix ADC NS_Appliance-1 en “Ejemplo de una configuración de conector de CloudBridge. :

```
1      >  add ipsec profile NS_F5-BIG-IP_IPSec_Profile -psk
          examplepresharedkey -ikeVersion v1  - encAlgo AES  - hashalgo
          HMAC_SHA1  - lifetime 315360 -perfectForwardSecrecy ENABLE
2
3
4      Done
5
6      >  add iptunnel NS_F5-BIG-IP_Tunnel 203.0.113.200 255.255.255.255
          198.51.100.100  - protocol IPSEC  - ipsecProfileName NS_F5-BIG-
          IP_IPSec_Profile
7
8
9      Done
10
11     > add pbr NS_F5-BIG-IP_Pbr -srcIP 10.102.147.0-10.102.147.255  -
          destIP 10.20.0.0-10.20.255.255  - ipTunnel NS_F5-BIG-IP_Tunnel
12
13
14     Done
15
16     > apply pbrs
17
18
19     Done
20 <!--NeedCopy-->
```

Supervisión del túnel de CloudBridge Connector

Puede supervisar el rendimiento de los túneles de CloudBridge Connector en un dispositivo Citrix ADC mediante contadores estadísticos del túnel de CloudBridge Connector. Para obtener más información sobre cómo mostrar estadísticas de túnel de CloudBridge Connector en un dispositivo Citrix ADC, consulte Supervisión de túneles de CloudBridge Connector.

Interoperabilidad de CloudBridge Connector: Cisco ASA

August 20, 2021

Puede configurar un túnel de CloudBridge Connector entre un dispositivo Citrix ADC y un dispositivo Cisco ASA para conectar dos centros de datos o ampliar la red a un proveedor de nube. El dispositivo Citrix ADC y el dispositivo Cisco ASA forman los puntos finales del túnel de CloudBridge Connector y se denominan pares.

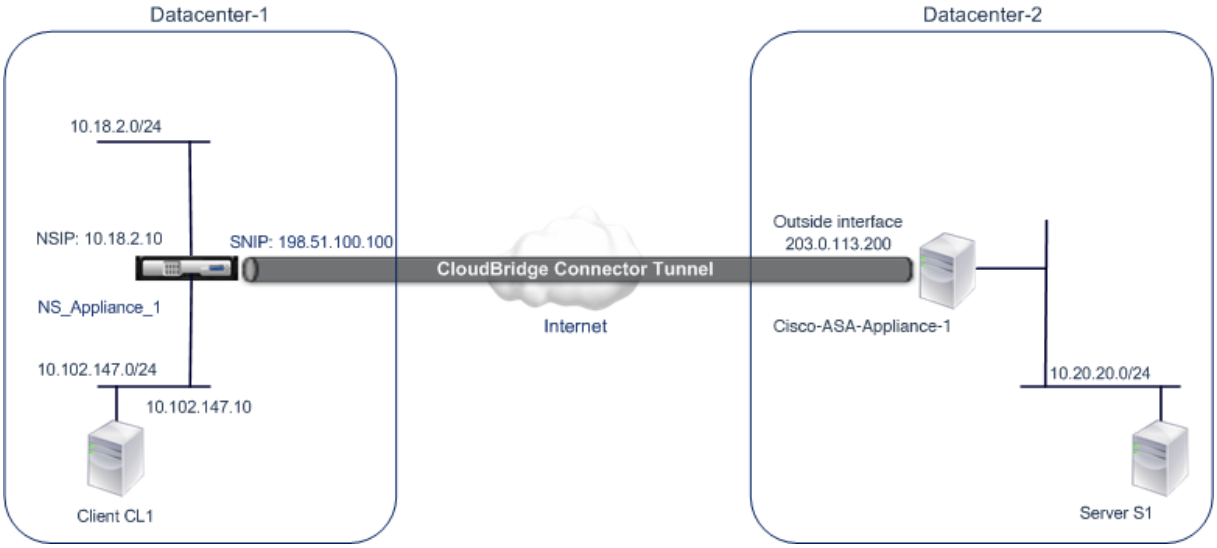
Ejemplo de configuración de túnel de CloudBridge Connector

Como ilustración del flujo de tráfico en un túnel de CloudBridge Connector, considere un ejemplo en el que se configura un túnel de CloudBridge Connector entre los siguientes dispositivos:

- Dispositivo Citrix ADC NS_Appliance-1 en un centro de datos designado como Datacenter-1
- Cisco ASA appliance CISCO-ASA-Appliance-1 en un centro de datos designado como Datacenter-2

NS_Appliance-1 y CISCO-ASA-Appliance-1 permiten la comunicación entre redes privadas en Datacenter-1 y Datacenter-2 a través del túnel CloudBridge Connector. En el ejemplo, NS_Appliance-1 y Cisco-ASA-Appliance-1 permiten la comunicación entre el cliente CL1 en Datacenter-1 y el servidor S1 en Datacenter-2 a través del túnel CloudBridge Connector. El cliente CL1 y el servidor S1 están en diferentes redes privadas.

En NS_Appliance-1, la configuración del túnel de CloudBridge Connector incluye la entidad de perfil IPSec NS_CISCO-ASA_IPSEC_Profile, la entidad de túnel de CloudBridge Connector NS_CISCO-ASA_Tunnel y la entidad de redirección basada en directivas (PBR) NS_CISCO-ASA_PBR.



Puntos a tener en cuenta para una configuración de túnel de CloudBridge Connector

Antes de comenzar a configurar el túnel del conector de CloudBridge, asegúrese de que:

- La siguiente configuración de IPSec se admite para un túnel de CloudBridge Connector entre un dispositivo Citrix ADC y un dispositivo Cisco ASA.

Propiedades IPSec	Parámetros
Modo IPSec	Modo túnel
Versión de IKE	Versión 1
Método de autenticación IKE	Clave previamente compartida
Algoritmo de cifrado IKE	AES, 3DES
Algoritmo hash IKE	HMAC SHA1, HMAC MD5
Algoritmo de cifrado ESP	AES, 3DES
Algoritmo hash ESP	HMAC SHA1, HMAC MD5

- Debe especificar la misma configuración IPSec en el dispositivo Citrix ADC y en el dispositivo Cisco ASA en los dos extremos del túnel CloudBridge Connector.
- Citrix ADC proporciona un parámetro común (en perfiles IPSec) para especificar un algoritmo hash IKE y un algoritmo hash ESP. También proporciona otro parámetro común para especificar un algoritmo de cifrado IKE y un algoritmo de cifrado ESP. Por lo tanto, en el dispositivo Cisco ASA, debe especificar el mismo algoritmo hash y el mismo algoritmo de cifrado en IKE (configuración de fase 1) y ESP (configuración de fase 2).
- Debe configurar el firewall en el extremo Citrix ADC y Cisco ASA para permitir lo siguiente.
  - Cualquier paquete UDP para el puerto 500
  - Cualquier paquete UDP para el puerto 4500
  - Cualquier paquete ESP (protocolo IP número 50)

Configuración de Cisco ASA para el túnel CloudBridge Connector

Para configurar un túnel de CloudBridge Connector en un dispositivo Cisco ASA, utilice la interfaz de línea de comandos ASA de Cisco, que es la interfaz de usuario principal para configurar, supervisar y mantener los dispositivos Cisco ASA.

Antes de comenzar la configuración del túnel de CloudBridge Connector en un dispositivo Cisco ASA, asegúrese de que:

- Tiene una cuenta de usuario con credenciales de administrador en el dispositivo ASA de Cisco.
- Está familiarizado con la interfaz de línea de comandos ASA de Cisco.

- El dispositivo Cisco ASA está en funcionamiento, está conectado a Internet y también está conectado a las subredes privadas cuyo tráfico se va a proteger a través del túnel CloudBridge Connector.

> **Nota**
>
> Los procedimientos para configurar el túnel de CloudBridge Connector en un dispositivo ASA de Cisco pueden cambiar con el tiempo, dependiendo del ciclo de lanzamiento de Cisco. Citrix recomienda que siga la documentación oficial del producto ASA de Cisco para Configurar túneles VPN IPSec, en:

- http://www.cisco.com

Para configurar un túnel de conector CloudBridge entre un dispositivo Citrix ADC y un dispositivo ASA de Cisco, realice las siguientes tareas en la línea de comandos del dispositivo ASA de Cisco:

- **Cree una directiva IKE**. Una directiva IKE define una combinación de parámetros de seguridad que se utilizarán durante la negociación IKE (fase 1). Por ejemplo, parámetros como el algoritmo hash, el algoritmo de cifrado y el método de autenticación que se utilizarán en la negociación IKE se establecen en esta tarea.
- **Habilite IKE en la interfaz externa**. Habilite IKE en la interfaz externa a través de la cual el tráfico del túnel fluirá al par del túnel.
- **Cree un grupo de túneles**. Un grupo de túneles especifica el tipo de túnel y la clave previamente compartida. El tipo de túnel debe establecerse en ipsec-l2l, que significa IPSec LAN a LAN. Una clave previamente compartida es una cadena de texto, que los pares de un túnel de CloudBridge Connector utilizan para autenticarse mutuamente entre sí. Las claves previamente compartidas se comparan entre sí para la autenticación IKE. Por lo tanto, para que la autenticación se realice correctamente, debe configurar la misma clave previamente compartida en el dispositivo Cisco ASA y en el dispositivo Citrix ADC.
- **Defina un conjunto de transformación**. Un conjunto de transformaciones define una combinación de parámetros de seguridad (fase 2) que se utilizarán en el intercambio de datos a través del túnel de CloudBridge Connector después de que la negociación IKE sea correcta.
- **Crear una lista de acceso**. Las listas de acceso criptográfico se utilizan para definir las subredes cuyo tráfico IP se protegerá sobre el túnel CloudBridge. Los parámetros de origen y destino de la lista de acceso especifican las subredes del lado del dispositivo Cisco y del lado del Citrix ADC que se van a proteger a través del túnel del conector de CloudBridge. La lista de acceso debe configurarse para permitir. Cualquier paquete de solicitud que se origina en un dispositivo de la subred del lado del dispositivo Cisco y esté destinado a un dispositivo de la subred del lado Citrix ADC y que coincida con los parámetros de origen y destino de la lista de acceso, se envía a través del túnel de CloudBridge Connector.
- **Crear un mapa criptográfico**. Los mapas criptográficos definen los parámetros IPSec para las asociaciones de seguridad (SA). Incluyen lo siguiente: Lista de acceso criptográfico para identificar las subredes cuyo tráfico se va a proteger a través del túnel CloudBridge, identificación

de pares (Citrix ADC) por dirección IP y transformación configurada para que coincidan con la configuración de seguridad del mismo nivel.

- **Aplique el mapa criptográfico a la interfaz externa**. En esta tarea, se aplica el mapa criptográfico a la interfaz externa a través de la cual el tráfico del túnel fluirá al par del túnel. Al aplicar el mapa criptográfico a una interfaz, se indica al dispositivo ASA de Cisco que evalúe todo el tráfico de interfaz en relación con el conjunto de mapas criptográficos y que utilice la directiva especificada durante las negociaciones de conexión o asociación de seguridad.

Los ejemplos de los procedimientos siguientes crean la configuración del dispositivo Cisco ASA Appliance-1 utilizado en Ejemplo de configuración del conector CloudBridge y flujo de datos.

Para crear una directiva IKE mediante la línea de comandos ASA de Cisco

En el símbolo del sistema del dispositivo ASA de Cisco, escriba los siguientes comandos, comenzando en el modo de configuración global, en el orden mostrado:

Comando	Ejemplo	Descripción del comando
crypto ikev1 policy priority	Cisco-ASA-appliance-1(config)# crypto ikev1 policy 1	Introduzca el modo de configuración de directivas IKE e identifique la directiva que quiere crear. (Cada directiva se identifica de forma única por el número de prioridad que asigne.) En este ejemplo se configura la directiva 1.
cifrado (3des | aes)	Cisco-ASA-Appliance-1 (config-ikev1-policy) # cifrado 3des	Especifique el algoritmo de cifrado. En este ejemplo se configura el algoritmo 3DES.
hash (sha | md5)	Cisco-ASA-Appliance-1 (config- ikev1-policy) # hash sha	Especifique el algoritmo hash. En este ejemplo se configura SHA.
authenticationpre-share	Cisco-ASA-Appliance-1 (config- ikev1-policy) # autenticación previa a la compartición	Especifique el método de autenticación previa al recurso compartido.
grupo 2	Cisco-ASA-Appliance-1 (config- ikev1-policy) # grupo 2	Especifique el identificador de grupo Diffie-Hellman de 1024 bits (2).

Comando	Ejemplo	Descripción del comando
segundos de vida	Cisco-ASA-Appliance-1 (config- ikev1-policy) # duración 28800	Especifique la duración de la asociación de seguridad en segundos. En este ejemplo se configuran 28800 segundos, que es el valor predeterminado de la vida útil de un dispositivo Citrix ADC.

Para habilitar IKE en la interfaz externa mediante la línea de comandos ASA de Cisco

En el símbolo del sistema del dispositivo ASA de Cisco, escriba los siguientes comandos, comenzando en el modo de configuración global, en el orden mostrado:

Comando	Ejemplo	Descripción del comando
crypto ikev1 enable outside	Cisco-ASA-appliance-1(config)# crypto ikev1 enable outside	Habilite IKEv1 en la interfaz a través de la cual el tráfico del túnel fluye hacia el par del túnel. En este ejemplo se habilita IKEv1 en la interfaz denominada outside.

Para crear un grupo de túnel mediante la línea de comandos Cisco ASA

En el símbolo del sistema del dispositivo Cisco ASA, escriba los siguientes comandos, comenzando en el modo de configuración global, como se muestra en el pdf Tunnel Group adjunto mediante la línea de comandos ASA de Cisco:

Para crear una lista de acceso criptográfico mediante la línea de comandos Cisco ASA

En el símbolo del sistema del dispositivo Cisco ASA, escriba el comando siguiente en el modo de configuración global, en el orden mostrado:

Comando	Ejemplo	Descripción del comando
lista de acceso a la lista de accesos-número permitir origen IP origen comodín destino destino comodín	Cisco-ASA-Appliance-1 (config) # lista de accesos 111 permiso ip 10.20.20.0 0.0.0.255 10.102.147.0 0.0.0.255	Especifique las condiciones para determinar las subredes cuyo tráfico IP debe protegerse sobre el túnel de CloudBridge Connector. En este ejemplo se configura la lista de acceso 111 para proteger el tráfico de las subredes 10.20.20.0/24 (en el lado Cisco-ASA-Appliance-1) y 10.102.147.0/24 (en el lado NS_Appliance-1).

Para definir un conjunto de transformaciones mediante la línea de comandos ASA de Cisco

En el símbolo del sistema del dispositivo ASA de Cisco, escriba los siguientes comandos, comenzando en el modo de configuración global. Consulte Conjunto de transformaciones mediante la tabla de línea de comandos ASA pdf.

Para crear un mapa criptográfico mediante la línea de comandos ASA de Cisco

En el símbolo del sistema del dispositivo ASA de Cisco, escriba los siguientes comandos comenzando en el modo de configuración global, en el orden mostrado:

Comando	Ejemplo	Descripción del comando
crypto map map-name seq-num match address access-list-name	Cisco-ASA-appliance-1 (config)# crypto map NS-CISCO-CM 1 match address 111	Cree un mapa criptográfico y especifique una lista de acceso a él. Este ejemplo configura el mapa criptográfico NS-CISCO-CM con el número de secuencia 1 y asigna la lista de acceso 111 a NS-CISCO-CM.

Comando	Ejemplo	Descripción del comando
crypto map map-name seq-num set peer ip-address	Cisco-ASA-Appliance-1 (config) # mapa criptográfico NS-CISCO-CM 1 conjunto par 198.51.100.100	Especifique el par (dispositivo Citrix ADC) por su dirección IP. En este ejemplo se especifica 198.51.100.100, que es la dirección IP del extremo del túnel en el dispositivo Citrix ADC.
crypto map map-name seq-num set ikev1 transform-set transform-set-name	Cisco-ASA-Appliance-1 (config) # mapa criptográfico NS-CISCO-CM 1 conjunto ikev1 transform-set NS-CISCO-TS	Especifique qué conjunto de transformaciones se permite para esta entrada de mapa criptográfico. En este ejemplo se especifica el conjunto de transformaciones NS-CISCO-TS.

Para aplicar un mapa criptográfico a una interfaz mediante la línea de comandos Cisco ASA

En el símbolo del sistema del dispositivo ASA de Cisco, escriba los siguientes comandos comenzando en el modo de configuración global, en el orden mostrado:

Comando	Ejemplo	Descripción del comando
crypto map map-nameinterface interface-name	Cisco-ASA-Appliance-1 (config) # mapa criptográfico NS-CISCO-CM interfaz fuera	Aplique el mapa de cifrado a la interfaz a través de la cual fluirá el tráfico del túnel de CloudBridge Connector. Este ejemplo aplica el mapa criptográfico NS-CISCO-CM a la interfaz externa.

Configuración del dispositivo Citrix ADC para el túnel de CloudBridge Connector

Para configurar un túnel de CloudBridge Connector entre un dispositivo Citrix ADC y un dispositivo Cisco ASA, realice las siguientes tareas en el dispositivo Citrix ADC. Puede utilizar la línea de comandos de Citrix ADC o la interfaz gráfica de usuario (GUI) de Citrix ADC:

- Cree un perfil IPSec.
- Cree un túnel IP que utilice el protocolo IPSec y asocie el perfil IPSec con él.

- Cree una regla PBR y asociarla con el túnel IP.

Para crear un perfil IPSEC mediante la línea de comandos de Citrix ADC:

En el símbolo del sistema, escriba:

- `add ipsec profile <name> -psk <string> -ikeVersion v1 -encAlgo AES -hashAlgo HMAC_SHA1 -perfectForwardSecrecy ENABLE`
- `show ipsec profile <name>`

Para crear un túnel IPSEC y enlazar el perfil IPSEC con él mediante la línea de comandos de Citrix ADC:

En el símbolo del sistema, escriba:

- `add ipTunnel <name> <remote> <remoteSubnetMask> <local> -protocol IPSEC -ipsecProfileName <string>`
- `show ipTunnel <name>`

Para crear una regla PBR y enlazar el túnel IPSEC a ella mediante la línea de comandos de Citrix ADC:

En el símbolo del sistema, escriba:

- `**add pbr** <pbrName> **ALLOW** -**srcIP** <subnet-range> -**destIP** <subnet-range>`
- `**ipTunnel** <tunnelName>`
- `**apply pbrs**`
- `**show pbr** <pbrName>`

Para crear un perfil IPSEC mediante la GUI:

1. Vaya a **Sistema** > **Conector de CloudBridge** > **Perfil IPSec**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En la página **Agregar perfil IPSec**, establezca los siguientes parámetros:
   - Nombre
   - Algoritmo de cifrado
   - Algoritmo hash
   - Versión del protocolo IKE
   - Secreto directo perfecto (Habilitar este parámetro)
4. Configure el método de autenticación IPSec que utilizarán los dos pares de túnel de CloudBridge Connector para autenticarse mutuamente: Seleccione el método de **autenticación de clave previamente compartida** y establezca el parámetro La **clave precompartida existe** .
5. Haga clic en **Crear** y, a continuación, en **Cerrar**.

Para crear un túnel IP y enlazar el perfil IPSEC a él mediante la GUI:

1. Vaya a **Sistema** > **Conector de CloudBridge** > **Túneles IP**.

2. En la **ficha Túneles IPv4**, haga clic en **Agregar**.
3. En la página **Agregar túnel IP**, establezca los siguientes parámetros:
   - Nombre
   - IP remota
   - Máscara remota
   - Tipo de IP local (en la lista desplegable Tipo de IP local, seleccione IP de subred).
   - IP local (todas las direcciones IP configuradas del tipo IP seleccionado se encuentran en la lista desplegable de IP local. Seleccione la IP deseada de la lista.)
   - Protocolo
   - Perfil IPSec
4. Haga clic en **Crear** y, a continuación, en **Cerrar**.

Para crear una regla PBR y enlazar el túnel IPSEC a ella mediante la GUI:

1. Vaya a **Sistema** > **Red** > **PBR**.
2. En la ficha **PBR**, haga clic en **Agregar**.
3. En la página **Crear PBR**, defina los siguientes parámetros:
   - Nombre
   - Action
   - Tipo de salto siguiente (Seleccionar túnel IP)
   - Nombre del túnel IP
   - IP de origen bajo
   - IP de origen alto
   - IP de destino bajo
   - IP de destino alto
4. Haga clic en **Crear** y, a continuación, en **Cerrar**.

La nueva configuración de túnel de CloudBridge Connector correspondiente en el dispositivo Citrix ADC aparece en la GUI. El estado actual del túnel del conector de CloudBridge se muestra en el panel Connector configurado de CloudBridge. Un punto verde indica que el túnel está arriba. Un punto rojo indica que el túnel está caído.

Los siguientes comandos crean la configuración del dispositivo Citrix ADC NS_Appliance-1 en “Ejemplo de una configuración de conector de CloudBridge.”:

```
1 >  add ipsec profile NS_Cisco-ASA_IPSec_Profile -psk
     examplepresharedkey -ikeVersion v1  - encAlgo AES  - hashalgo
     HMAC_SHA1  - lifetime 315360 -perfectForwardSecrecy ENABLE
2
3 Done
4
5 >  add iptunnel NS_Cisco-ASA_Tunnel 203.0.113.200 255.255.255.255
```



```
    198.51.100.100 -protocol IPSEC -ipsecProfileName NS_Cisco-
    ASA_IPSec_Profile
6
7
8 Done
9
10 > add pbr NS_Cisco-ASA_Pbr -srcIP 10.102.147.0-10.102.147.255 -destIP
    10.20.0.0-10.20.255.255 -ipTunnel NS_Cisco-ASA_Tunnel
11
12
13 Done
14
15 > apply pbrs
16
17 Done
18
19 <!--NeedCopy-->
```

Supervisión del túnel de CloudBridge Connector

Puede supervisar el rendimiento de los túneles de CloudBridge Connector en un dispositivo Citrix ADC mediante contadores estadísticos del túnel de CloudBridge Connector. Para obtener más información sobre cómo mostrar estadísticas de túnel de CloudBridge Connector en un dispositivo Citrix ADC, consulte Supervisión de túneles de CloudBridge Connector.

Alta disponibilidad

August 20, 2021

Una implementación de alta disponibilidad (HA) de dos dispositivos Citrix ADC puede proporcionar un funcionamiento ininterrumpido en cualquier transacción. Con un dispositivo configurado como nodo principal y el otro como nodo secundario, el nodo principal acepta conexiones y administra servidores, mientras que el nodo secundario supervisa el principal. Si, por cualquier motivo, el nodo principal no puede aceptar conexiones, el nodo secundario se hace cargo.

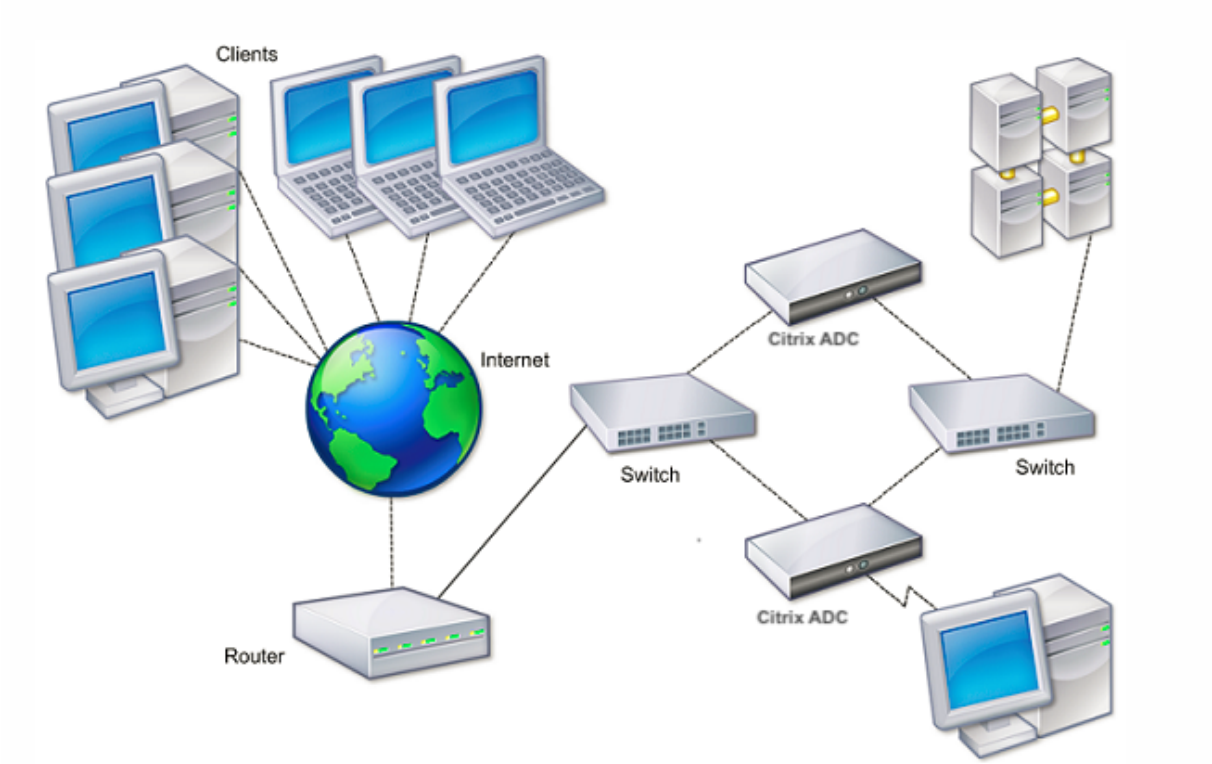
El nodo secundario supervisa el principal mediante el envío de mensajes periódicos (a menudo denominados mensajes de latido o comprobaciones de estado) para determinar si el nodo principal acepta conexiones. Si falla una comprobación de estado, el nodo secundario reintenta la conexión durante un período especificado, después del cual determina que el nodo principal no funciona normalmente. A continuación, el nodo secundario se hace cargo del principal (un proceso llamado failover).

Después de una conmutación por error, todos los clientes deben restablecer sus conexiones con los servidores administrados, pero las reglas de persistencia de sesión se mantienen como estaban antes de la conmutación por error.

Con la persistencia de registro del servidor web habilitada, no se pierden datos de registro debido a la conmutación por error. Para habilitar la persistencia de registros, la configuración del servidor de registros debe incluir entradas para ambos sistemas en el archivo log.conf.

La siguiente ilustración muestra una configuración de red con un par HA.

Ilustración 1. Dispositivos Citrix ADC en una configuración de alta disponibilidad



Para configurar HA, es posible que quiera comenzar por crear una configuración básica, con ambos nodos en la misma subred. A continuación, puede personalizar los intervalos en los que los nodos comunican información de comprobación de estado, el proceso mediante el cual los nodos mantienen la sincronización y la propagación de comandos del primario al secundario. Puede configurar el modo a prueba de fallos para evitar una situación en la que ninguno de los nodos sea primario. Si su entorno incluye dispositivos que no aceptan mensajes ARP gratuitos de Citrix ADC, debe configurar direcciones MAC virtuales. Cuando esté listo para una configuración más compleja, puede configurar nodos HA en diferentes subredes.

Para mejorar la fiabilidad de su configuración de alta disponibilidad, puede configurar monitores de ruta y crear vínculos redundantes. En algunas situaciones, como al solucionar problemas o realizar tareas de mantenimiento, es posible que quiera forzar a un nodo a conmutar por error (asignar el

estado principal al otro nodo), o que quiera forzar al nodo secundario a permanecer secundario o al nodo primario a permanecer primario.

Puntos a tener en cuenta para una configuración de alta disponibilidad

August 20, 2021

> **Nota**
>
> Los siguientes requisitos para configurar sistemas en una configuración de alta disponibilidad:

- En una configuración de alta disponibilidad, los dispositivos Citrix ADC primarios y secundarios deben ser del mismo modelo. Los diferentes modelos de Citrix ADC no se admiten en un par HA.
- En una configuración de alta disponibilidad, ambos nodos deben ejecutar la misma versión de Citrix ADC.
- Las entradas del archivo de configuración (ns.conf) en el sistema primario y secundario deben coincidir, con las siguientes excepciones:
  - Los sistemas primario y secundario deben configurarse cada uno con sus propias direcciones IP únicas (NSIP).
  - En un par HA, el ID de nodo y la dirección IP asociada de un nodo deben apuntar al otro nodo. Por ejemplo, si tiene nodos NS1 y NS2, debe configurar NS1 con un identificador de nodo único y la dirección IP de NS2, y debe configurar NS2 con un identificador de nodo único y la dirección IP de NS1.
- Si crea un archivo de configuración en cualquiera de los nodos mediante un método que no pasa directamente a través de la GUI o la CLI (por ejemplo, importar certificados SSL o cambiar a scripts de inicio), debe copiar el archivo de configuración en el otro nodo o crear un archivo idéntico en ese nodo.
- Inicialmente, todos los dispositivos Citrix ADC se configuran con la misma contraseña de nodo RPC. Los nodos RPC son entidades internas del sistema utilizadas para la comunicación de información de configuración y sesión de sistema a sistema. Por motivos de seguridad, debe cambiar las contraseñas de nodo RPC predeterminadas.

  Existe un nodo RPC en cada Citrix ADC. Este nodo almacena la contraseña, que se compara con la contraseña proporcionada por el sistema de contacto. Para comunicarse con otros sistemas, cada Citrix ADC requiere conocimiento de dichos sistemas, incluido el modo de autenticarse en dichos sistemas. Los nodos RPC mantienen esta información, que incluye las direcciones IP de los otros sistemas y las contraseñas que requieren para la autenticación.

Los nodos RPC se crean implícitamente al agregar un nodo o agregar un sitio Global Server Load Balancing (GSLB). No puede crear o eliminar nodos RPC manualmente.

> **Nota**:
>
> Si los dispositivos Citrix ADC en una configuración de alta disponibilidad están configurados en modo de un brazo, debe inhabilitar todas las interfaces del sistema excepto la conectada al switch o concentrador.

Para una configuración de alta disponibilidad IPv6, se aplican las siguientes consideraciones:

- Debe instalar la licencia IPv6pt en ambos dispositivos Citrix ADC.
- Después de instalar la licencia IPv6pt, habilite la función IPv6 mediante la interfaz GUI o la línea de comandos.
- Ambos dispositivos Citrix ADC requieren una dirección IPv6 NSIP global. Además, las entidades de red (por ejemplo, conmutadores y enrutadores) entre los dos nodos deben admitir IPv6.

Configuración de la alta disponibilidad

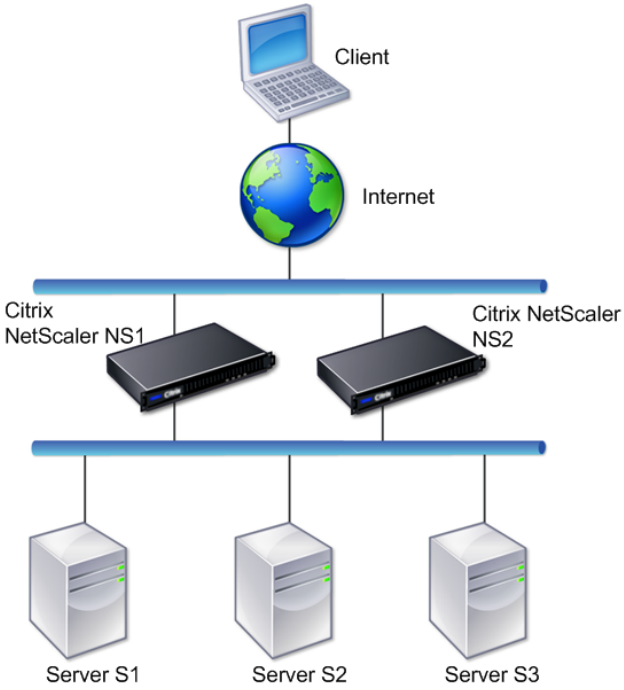
December 2, 2021

Para configurar una configuración de alta disponibilidad, se crean dos nodos, cada uno de los cuales define la dirección IP de Citrix ADC (NSIP) del otro como un nodo remoto. Comience por iniciar sesión en uno de los dos dispositivos Citrix ADC que quiere configurar para una alta disponibilidad y agregue un nodo. Especifique la dirección IP (NSIP) de Citrix ADC del otro dispositivo como la dirección del nuevo nodo. A continuación, inicie sesión en el otro dispositivo y agregue un nodo que tenga la dirección NSIP del primer dispositivo. Un algoritmo determina qué nodo pasa a ser primario y cuál se convierte en secundario.

> **Nota**:
>
> La GUI de Citrix ADC ofrece una opción que evita tener que iniciar sesión en el segundo dispositivo.

La siguiente ilustración muestra una configuración de HA simple, en la que ambos nodos están en la misma subred.

Ilustración 1. Dos dispositivos Citrix ADC conectados en una configuración de alta disponibilidad



Agregar un nodo remoto

Para agregar un dispositivo Citrix ADC remoto como nodo en una configuración de alta disponibilidad, debe especificar un identificador de nodo único y la dirección NSIP del dispositivo. Cuando se agrega un nodo HA, se debe inhabilitar el monitor HA para cada interfaz que no esté conectada o que no se esté usando para el tráfico. Para los usuarios de la CLI, este es un procedimiento independiente.

> **Nota**:
>
> Para garantizar que cada nodo de la configuración de alta disponibilidad tenga la misma configuración, debe sincronizar los certificados SSL, los scripts de inicio y otros archivos de configuración con los del nodo principal.

Para agregar un nodo mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

- `add ha node <id> <IPAddress>`
- `show ha node`

Ejemplo


```
> add ha node 10 203.0.113.32
<!--NeedCopy-->
```

Para inhabilitar un monitor de alta disponibilidad mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

- `set interface <ifNum> [-haMonitor ( ON | OFF )]`
- `show interface <ifNum>`

Ejemplo

```
> set interface 1/3 -haMonitor OFF
 Done
<!--NeedCopy-->
```

Para agregar un nodo remoto mediante la interfaz gráfica de usuario

Vaya a **Sistema** > **Alta disponibilidad** y, en la ficha **Nodos**, agregue un nuevo nodo remoto o modifique un nodo existente.

Desactivación o habilitación de un nodo

Solo puede inhabilitar o habilitar un nodo secundario. Cuando inhabilita un nodo secundario, deja de enviar mensajes de latidos al nodo principal y, por lo tanto, el nodo principal ya no puede comprobar el estado del secundario. Al habilitar un nodo, el nodo forma parte de la configuración de alta disponibilidad.

Para inhabilitar o habilitar un nodo mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba uno de los siguientes comandos:

- `set ha node -hastatus DISABLED`
- `set ha node -hastatus ENABLED`

Para inhabilitar o habilitar un nodo mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **Alta disponibilidad** y, en la ficha **Nodos**, abra el nodo.

2. En la lista **Estado de alta disponibilidad**, seleccione **HABILITADO (Participar activamente en HA)** o **DISCAPACITADO (no participar en HA)**.

Eliminación de un nodo

Si elimina un nodo, los nodos ya no están en una configuración de alta disponibilidad.

Para eliminar un nodo mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
rm ha node <id>
```

Ejemplo

```
1 > rm ha node 10
2   Done
3 <!--NeedCopy-->
```

Para eliminar un nodo mediante la interfaz gráfica de usuario

Vaya a **Sistema** > **Alta disponibilidad** y, en la ficha **Nodos**, elimine el nodo.

Configuración de los intervalos de comunicación

January 12, 2021

El intervalo de saludo es el intervalo en el que los mensajes de latido se envían al nodo del mismo nivel. El intervalo muerto es el intervalo de tiempo después del cual el nodo del mismo nivel se marca como DOWN si no se reciben paquetes de latido. Los mensajes de latido son paquetes UDP enviados al puerto 3003 del otro nodo en un par HA. El intervalo muerto debe establecerse como un múltiplo de intervalo de saludo.

Para establecer los intervalos hola y muertos mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

- `set HA node [-helloInterval <msecs>] [-deadInterval <secs>]`
- `show HA node <id>`

Para establecer los intervalos hola y muertos mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **Alta disponibilidad** y, en la ficha **Nodos**, abra el nodo.
2. Defina los siguientes parámetros:
   - Intervalo de saludo (msecs)
   - Intervalo muerto (segundos)

Configuración de la sincronización

January 12, 2021

La sincronización es un proceso de duplicación de la configuración del nodo primario en el nodo secundario. El propósito de la sincronización es garantizar que no haya pérdida de información de configuración entre los nodos primario y secundario, independientemente del número de conmutaciones por error que se produzcan. La sincronización utiliza el puerto 3010.

La sincronización se desencadena por cualquiera de las siguientes circunstancias:

- El nodo secundario en una configuración de alta disponibilidad aparece después de un reinicio.
- El nodo principal se convierte en secundario después de una conmutación por error.

La sincronización automática está habilitada de forma predeterminada. También puede forzar la sincronización.

Habilitar o inhabilitar la sincronización

La sincronización automática de alta disponibilidad está habilitada de forma predeterminada en cada nodo de un par de alta disponibilidad. Puede habilitarla o inhabilitarla en cualquiera de los nodos.

Para habilitar o inhabilitar la sincronización automática mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

- `set HA node -haSync DISABLED`
- `set HA node -haSync ENABLED`

Para habilitar o inhabilitar la sincronización mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **Alta disponibilidad**.
2. En Sincronización de alta disponibilidad, desactive o seleccione el nodo secundario obtendrá la configuración de la opción Principal.

Obligar al nodo secundario a sincronizar con el nodo principal

Además de la sincronización automática, Citrix ADC admite la sincronización forzada. Puede forzar la sincronización desde el nodo principal o secundario. Cuando se fuerza la sincronización desde el nodo secundario, éste comienza a sincronizar su configuración con el nodo principal.

Sin embargo, si la sincronización ya está en curso, la sincronización forzada falla y el sistema muestra una advertencia. La sincronización forzada también falla en cualquiera de las siguientes circunstancias:

- Forzar la sincronización en un sistema independiente.
- El nodo secundario está inhabilitado.
- La sincronización de HA está inhabilitada en el nodo secundario.

Para forzar la sincronización mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
force HA sync
```

Para forzar la sincronización mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **Alta disponibilidad**.
2. En la ficha **Nodos**, en la lista Acciones, haga clic en **Forzar sincronización**.

Sincronización de archivos de configuración en una configuración de alta disponibilidad

October 5, 2021

En una configuración de alta disponibilidad, todos los archivos de configuración se sincronizan automáticamente del nodo principal al nodo secundario en un intervalo de un minuto. La sincronización de los archivos de configuración se puede realizar manualmente mediante la interfaz de línea de comandos o la GUI del nodo principal o secundario.

Los archivos ubicados en el secundario que son específicos del secundario (no presentes en el principal) no se eliminan durante la sincronización.

Para sincronizar archivos en una configuración de alta disponibilidad mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

`sync HA files <mode>`

Ejemplo

```
> sync HA files all
 Done
<!--NeedCopy-->
```

```
> sync HA files ssl
 Done
<!--NeedCopy-->
```

Descripciones de parámetros (del comando incluido en el procedimiento CLI)

`sync ha files <mode>`

`mode`

Especifique uno de los siguientes modos de sincronización.

- **all** : sincronizar archivos relacionados con la configuración del sistema, los marcadores de Access Gateway, los certificados SSL, las listas CRL SSL y los objetos XML de Application Firewall.
- **bookmarks** : sincroniza todos los marcadores de Access Gateway.
- **ssl** : sincroniza todos los certificados, claves y CRL de la función SSL.
- **imports** - Sincroniza todos los objetos XML (por ejemplo, WSDL, esquemas, páginas de error) configurados para el firewall de aplicaciones.
- **misc** - Sincroniza todos los archivos de licencia y el archivo rc.conf.
- **all_plus_misc** : sincroniza archivos relacionados con la configuración del sistema, los marcadores de Access Gateway, los certificados SSL, las listas CRL SSL, los objetos XML del firewall de aplicaciones, las licencias y el archivo rc.conf.

Para sincronizar archivos en una configuración de alta disponibilidad mediante la interfaz gráfica de usuario

Vaya a **Sistema** > **Diagnóstico** y, en el grupo **Utilidades**, haga clic en **Iniciar sincronización de archivos HA**.

Configuración de la propagación de comandos

January 12, 2021

En una configuración de alta disponibilidad, cualquier comando emitido en el nodo principal se propaga automáticamente al secundario, y se ejecuta en él, antes de que se ejecute en el primario. Si la propagación del comando falla, o si la ejecución del comando falla en el secundario, el nodo principal ejecuta el comando y registra un error. La propagación de comandos utiliza el puerto 3010.

En una configuración de par HA, la propagación de comandos está habilitada de forma predeterminada en los nodos primario y secundario. Puede habilitar o inhabilitar la propagación de comandos en cualquiera de los nodos de un par HA. Si inhabilita la propagación de comandos en el nodo principal, los comandos no se propagan al nodo secundario. Si inhabilita la propagación de comandos en el nodo secundario, los comandos propagados desde el primario no se ejecutan en el nodo secundario.

> **Nota**
>
> Después de volver a habilitar la propagación, recuerde forzar la sincronización.

Si se produce la sincronización mientras se inhabilita la propagación, los cambios relacionados con la configuración que se realicen antes de que surta efecto la desactivación de la propagación se sincronizarán con el nodo secundario. Esto también es cierto para los casos en que la propagación está inhabilitada mientras la sincronización está en curso.

Para habilitar o inhabilitar la propagación de comandos mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

- establecer nodo HA -HAprop DISABLED
- establecer nodo HA -HAprop ENABLED

Para habilitar o inhabilitar la propagación de comandos mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **Alta disponibilidad** y, en la ficha **Nodos**, abra el nodo.
2. Desactive o seleccione el nodo primario propagará la configuración a la opción Secundaria.

Restringir el tráfico de sincronización de alta disponibilidad a una VLAN

August 20, 2021

En una implementación de alta disponibilidad (HA), el tráfico relacionado con el mantenimiento de la configuración de HA fluye entre los dos nodos de HA. Este tráfico es de los siguientes tipos:

- Sincronización de configuración
- Propagación de configuración
- Duplicación de conexión
- Sincronización de configuración de persistencia de equilibrio de carga
- Sincronización de sesión persistente
- Sincronización del estado de la sesión

El flujo adecuado de este tráfico relacionado con HA entre los dos nodos es fundamental para el funcionamiento de la implementación de HA. Normalmente, el tráfico relacionado con HA es pequeño en volumen, pero puede llegar a ser muy alto durante una conmutación por error. Se vuelve muy alto si la conmutación por error de conexión con estado está habilitada y el nodo que era principal antes de la conmutación por error manejaba un gran número de conexiones.

De forma predeterminada, el tráfico relacionado con HA fluye a través de las VLAN a las que está enlazada la dirección NSIP. Para acomodar un aumento potencial en este tráfico, puede separar el tráfico relacionado con HA del tráfico de administración y restringir su flujo a una VLAN separada. Esta VLAN se denomina HA SYNC VLAN.

Puntos a tener en cuenta antes de configurar una VLAN HA SYNC

- La configuración de una VLAN de HA SYNC no se propaga ni sincroniza. En otras palabras, la VLAN HA SYNC es específica del nodo y se configura de forma independiente en cada nodo.
- La configuración de HA SYNC VLAN se elimina cuando se borra la configuración solo en modo FULL.
- HA MON debe establecerse en OFF para las interfaces que forman parte de HA SYNC VLAN, para evitar una situación en la que ambos nodos funcionan como nodo principal.
- Las interfaces de administración (por ejemplo, 0/1 y 0/2) no deben formar parte de la VLAN SYNC de HA, de modo que el tráfico relacionado con HA no fluya a través de las interfaces de administración.
- Citrix recomienda inhabilitar los mensajes de latido de alta disponibilidad en las interfaces de administración y habilitar las interfaces VLAN de HA SYNC. Después de cumplir estas recomendaciones, los mensajes de latido de alta disponibilidad también se pueden habilitar en las interfaces de datos.

  Para obtener más información sobre la desactivación de los mensajes de latido de alta disponibilidad en las interfaces, consulte Administración de mensajes de latido de alta disponibilidad en un dispositivo Citrix ADC.

Para configurar una VLAN de HA SYNC en un nodo Citrix ADC, especifique una VLAN configurada con el parámetro HA SYNC VLAN de la entidad de nodo local.

Para configurar una VLAN HA SYNC en un nodo local mediante la línea de comandos:

En el símbolo del sistema, escriba:

- `set ha node -syncvlan <VLANID>`
- `show node`

Descripción del parámetro:

syncvlan (Sync VLAN): VLAN en la que se envía el tráfico relacionado con alta disponibilidad. Esto incluye el tráfico de sincronización, propagación, espejado de conexiones, persistencia del equilibrio de carga, sincronización de configuración, sincronización de sesiones persistente y sincronización del estado de la sesión. Sin embargo, los latidos del corazón de HA pueden usar cualquier interfaz.

Para configurar una VLAN HA SYNC en un nodo mediante la GUI:

1. Vaya a **Sistema** > **Alta disponibilidad**.
2. Establezca el parámetro **Sync VLAN** mientras modifica el nodo local.

Configuración del modo a prueba de fallos

January 12, 2021

En una configuración de alta disponibilidad, el modo a prueba de fallos garantiza que un nodo sea siempre primario cuando ambos nodos no cumplan la comprobación de estado. Esto es para garantizar que cuando un nodo solo está disponible parcialmente, los métodos de copia de seguridad estén habilitados para manejar el tráfico de la mejor manera posible. El modo de seguridad de alta disponibilidad se configura de forma independiente en cada nodo.

La siguiente tabla muestra algunos de los casos a prueba de fallos. El estado NOT_UP significa que el nodo ha fallado en la comprobación de estado, pero está parcialmente disponible. El estado ACTIVO significa que el nodo pasó la comprobación de estado.

Estado de salud del nodo A (primario)	Estado sanitario del nodo B (secundario)	Comportamiento de HA predeterminado	Comportamiento de HA habilitado a prueba de fallos	Descripción
NOT_UP (último error)	NOT_UP (error primero)	A (Secundaria), B (Secundaria)	A (Primaria), B (Secundaria)	Si ambos nodos fallan, uno tras otro, el nodo que fue el último primario permanece primario.
NOT_UP (error primero)	NOT_UP (último error)	A (Secundaria), B (Secundaria)	A (Secundaria), B (Primaria)	Si ambos nodos fallan, uno tras otro, el nodo que fue el último primario permanece primario.
ACTIVO	ACTIVO	A (Primaria), B (Secundaria)	A (Primaria), B (Secundaria)	Si ambos nodos pasan la comprobación de estado, no hay cambios en el comportamiento con la prueba de errores habilitada.
ACTIVO	NOT_UP	A (Primaria), B (Secundaria)	A (Primaria), B (Secundaria)	Si solo falla el nodo secundario, no hay cambios en el comportamiento con la prueba de fallos habilitada.

Estado de salud del nodo A (primario)	Estado sanitario del nodo B (secundario)	Comportamiento de HA predeterminado	Comportamiento de HA habilitado a prueba de fallos	Descripción
NOT_UP	ACTIVO	A (Secundaria), B (Primaria)	A (Secundaria), B (Primaria)	Si solo falla el primario, no hay cambios en el comportamiento con la seguridad habilitada.
NOT_UP	ACTIVO (STAY-SECONDARY)	A (Secundaria), B (Secundaria)	A (Primaria), B (Secundaria)	Si el secundario está configurado como STAYSE-CUNDARY, el primario permanece primario incluso si falla.

Para habilitar el modo a prueba de fallos mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
set HA node [-failSafe ( **ON** | **OFF** )]
```

Ejemplo

```
1 set ha node -failsafe ON
2 <!--NeedCopy-->
```

Para habilitar el modo a prueba de fallos mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **Alta disponibilidad** y, en la ficha **Nodos**, abra el nodo.
2. En **Modo a prueba de fallos**, seleccione la opción **Mantener un nodo principal**incluso cuando ambos nodos no estén en buen estado.

Configuración de direcciones MAC virtuales

January 19, 2021

Una dirección MAC virtual es una entidad flotante compartida por los nodos principal y secundario en una configuración de alta disponibilidad.

En una configuración de alta disponibilidad, el nodo principal posee todas las direcciones IP flotantes, como los MIP, los SNIP y los VIP. El nodo principal responde a las solicitudes de Protocolo de resolución de direcciones (ARP) para estas direcciones IP con su propia dirección MAC. Como resultado, la tabla ARP de un dispositivo externo (por ejemplo, un enrutador ascendente) se actualiza con la dirección IP flotante y la dirección MAC del nodo principal.

Cuando se produce una conmutación por error, el nodo secundario se hace cargo como el nuevo nodo principal. A continuación, utiliza ARP Gratuitous (GARP) para anunciar las direcciones IP flotantes que adquirió del primario. Sin embargo, la dirección MAC que anuncia la nueva principal es la dirección MAC de su propia interfaz.

Algunos dispositivos (especialmente algunos enrutadores) no aceptan los mensajes GARP generados por el dispositivo Citrix ADC. Como resultado, algunos dispositivos externos conservan la antigua asignación de IP a MAC anunciada por el nodo principal antiguo. Esto puede provocar que un sitio se vaya abajo.

Puede superar este problema configurando un MAC virtual en ambos nodos de un par HA. Ambos nodos poseen direcciones MAC idénticas. Por lo tanto, cuando se produce la conmutación por error, la dirección MAC del nodo secundario permanece sin cambios y no es necesario actualizar las tablas ARP en los dispositivos externos.

Para crear un MAC virtual, primero debe crear un ID de enrutador virtual (VRID) y vincularlo a una interfaz. (En una configuración de alta disponibilidad, debe vincular el VRID a las interfaces de ambos nodos). Una vez que el VRID está enlazado a una interfaz, el sistema genera un MAC virtual con el VRID como último octeto.

Esta sección incluye los siguientes detalles:

- Configuración de MAC virtuales IPv4
- Configuración de IPv6 virtual Mac6S

Configuración de MAC virtuales IPv4

Cuando crea una dirección MAC virtual IPv4 y la vincula a una interfaz, cualquier paquete IPv4 enviado desde la interfaz utiliza la dirección MAC virtual enlazada a la interfaz. Si no hay un MAC virtual IPv4 enlazado a una interfaz, se utiliza la dirección MAC física de la interfaz.

El MAC virtual genérico es de la forma`00:00:5e:00:01:<VRID>`. Por ejemplo, si crea un VRID con un valor de 60 y lo vincula a una interfaz, el MAC virtual resultante es 00:00:5 e: 00:01:3 c, donde 3c es la representación hexadecimal del VRID. Puede crear 255 VRID con valores de 1 a 255.

Creación o modificación de un MAC virtual IPv4

Crear un MAC virtual IPv4 asignándole un ID de enrutador virtual. A continuación, puede enlazar el MAC virtual a una interfaz. No puede enlazar varios VRID a la misma interfaz. Para verificar la configuración MAC virtual, debe mostrar y examinar los MAC virtuales y las interfaces enlazadas a los MAC virtuales.

Para agregar un MAC virtual mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

- `add vrID`
- `bind vrid <id> -ifnum <interface_name>`
- `show vrID`

Ejemplo

```
> add vrID 100
 Done
> bind vrid 100 -ifnum 1/1 1/2 1/3
 Done
<!--NeedCopy-->
```

Para desenlazar interfaces de un MAC virtual mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

- `unbind vrid <id> -ifnum <interface_name>`
- `show vrID`

Para configurar un MAC virtual mediante la interfaz gráfica de usuario

Vaya a **Sistema** > **Red** > **VMAC** y, en la ficha **VMAC**, agregue un nuevo MAC virtual o modifique un MAC virtual existente.

Eliminación de un MAC virtual IPv4

Para quitar un MAC virtual IPv4, elimine su ID de enrutador virtual.

Para eliminar un MAC virtual IPv4 mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
rm vrid <id>
```

Ejemplo

```
1 rm vrid 100s
2 <!--NeedCopy-->
```

Para eliminar un MAC virtual IPv4 mediante la interfaz gráfica de usuario

Vaya a **Sistema** > **Red** > **VMAC** y, en la ficha **VMAC**, elimine el MAC virtual IPv4.

Configuración de IPv6 virtual Mac6S

Citrix ADC admite paquetes virtuales MAC6 para IPv6. Puede enlazar cualquier interfaz a un MAC6 virtual, incluso si un MAC virtual IPv4 está enlazado a la interfaz. Cualquier paquete IPv6 enviado desde la interfaz utiliza el MAC6 virtual vinculado a esa interfaz. Si no hay un MAC6 virtual enlazado a una interfaz, un paquete IPv6 utiliza el MAC físico.

Creación o modificación de un MAC6 virtual

Crear un MAC virtual IPv6 asignándole un ID de enrutador virtual IPv6. A continuación, puede enlazar el MAC virtual a una interfaz. No se pueden enlazar varios VRID IPv6 a una interfaz. Para verificar la configuración virtual de MAC6, debe mostrar y examinar los mac6s virtuales y las interfaces enlazadas a los mac6s virtuales.

Para agregar un MAC6 virtual mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

- `add vrID6 <id>`
- `bind vrID6 <id> -ifnum <interface_name>`
- `show vrID6`

Ejemplo

```
1 > add vrID6 100
2 Done
```



```
3 > bind vrID6 100 -ifnum 1/1 1/2 1/3
4  Done
5 <!--NeedCopy-->
```

Para desenlazar interfaces de un MAC6 virtual mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

- `unbind vrID6 <id> -ifnum <interface_name>`
- `show vrID6`

Para configurar un MAC6 virtual mediante la interfaz gráfica de usuario

Vaya a **Sistema** > **Red** > **VMAC** y, en la ficha **VMAC6**, agregue un nuevo MAC6 virtual o modifique un MAC6 virtual existente.

Eliminación de un MAC6 virtual

Para quitar un MAC virtual IPv4, elimine su ID de enrutador virtual.

Para eliminar un MAC6 virtual mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

`rm vrid6 <id>`

Ejemplo

```
1 rm vrid6 100s
2 <!--NeedCopy-->
```

Para eliminar un MAC6 virtual mediante la interfaz gráfica de usuario

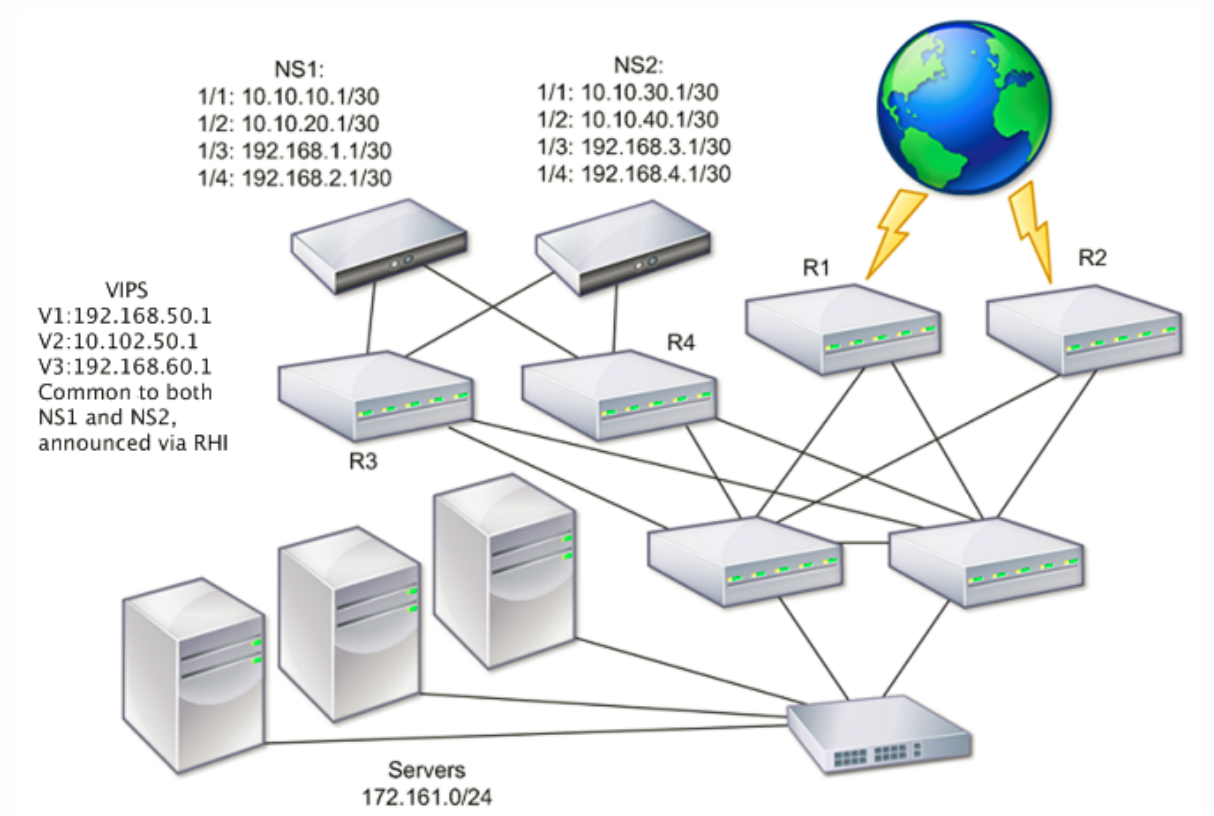
Vaya a **Sistema** > **Red** > **VMAC** y, en la ficha **VMAC6**, elimine el ID del enrutador virtual.

Configuración de nodos de alta disponibilidad en diferentes subredes

August 20, 2021

La siguiente ilustración muestra una implementación de alta disponibilidad con los dos sistemas ubicados en subredes diferentes:

Ilustración 1. Alta disponibilidad a través de una red enrutada



En la ilustración, los sistemas NS1 y NS2 están conectados a dos enrutadores separados, R3 y R4, en dos subredes diferentes. Los dispositivos Citrix ADC intercambian paquetes de latidos a través de los enrutadores. Esta configuración podría ampliarse para adaptarse a implementaciones que impliquen cualquier número de interfaces.

> **Nota**:
>
> Si utiliza redirección estática en la red, debe agregar rutas estáticas entre todos los sistemas para asegurarse de que los paquetes de latido se envían y reciben correctamente. (Si utiliza redirección dinámica en sus sistemas, las rutas estáticas son innecesarias).

Si los nodos de un par de alta disponibilidad residen en dos redes independientes, el nodo principal y secundario deben tener configuraciones de red independientes. Esto significa que los nodos de diferentes redes no pueden compartir entidades como la dirección de recorte, las VLAN y las rutas. Este tipo de configuración, donde los nodos de un par HA tienen diferentes parámetros configurables, se conoce como Configuración de red independiente (INC) o Configuración de red simétrica (SNC).

En la siguiente tabla se resumen las entidades y opciones configurables para un INC y se muestra cómo se deben establecer en cada nodo.

Entidades NetScaler	Opciones
IPs (NSIP/Recortes)	Específico de nodo. Activa solo en ese nodo.
VIP	Flotando.
VLAN	Específico de nodo. Activa solo en ese nodo.
Rutas	Específico de nodo. Activa solo en ese nodo. Las rutas de equilibrio de carga de enlace son flotantes.
ACL	Flotante (común). Activo en ambos nodos.
Redirección dinámica	Específico de nodo. Activa solo en ese nodo. El nodo secundario también debe ejecutar los protocolos de redirección y el par con enrutadores ascendentes.
Modo L2	Flotante (común). Activo en ambos nodos.
Modo L3	Flotante (común). Activo en ambos nodos.
NAT inversa (RNAT)	Configuración de RNAT con la dirección IP NAT establecida en una dirección IP del servidor virtual (VIP) porque la dirección VIP es flotante (común).

Al igual que en la configuración de nodos de alta disponibilidad en la misma subred, para configurar nodos de alta disponibilidad en diferentes subredes, inicie sesión en cada uno de los dos dispositivos Citrix ADC y agregue un nodo remoto que represente al otro dispositivo.

Agregar un nodo remoto

Cuando dos nodos de un par HA residen en subredes diferentes, cada nodo debe tener una configuración de red diferente. Por lo tanto, para configurar dos sistemas independientes para que funcionen como un par HA, debe especificar el modo INC durante el proceso de configuración.

Cuando se agrega un nodo HA, se debe inhabilitar el monitor HA para cada interfaz que no esté conectada o que no se esté mediante para el tráfico. Para los usuarios de CLI, este es un procedimiento independiente.

Para agregar un nodo mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

- `add ha node <id> <IPAddress> -inc ENABLED`
- `show ha node`

Ejemplo

```
> add ha node 3 10.102.29.170 -inc ENABLED
 Done
> add ha node 3 1000:0000:0000:0000:0005:0600:700a:888b
  Done
<!--NeedCopy-->
```

Para inhabilitar un monitor de alta disponibilidad mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

- `set interface <ifNum> [-haMonitor ( **ON** | **OFF** )]`
- `show interface <ifNum>`

Ejemplo

```
> set interface 1/3 -haMonitor OFF
 Done
<!--NeedCopy-->
```

Para agregar un nodo remoto mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **Alta disponibilidad** y, en la ficha **Nodos**, agregue un nuevo nodo remoto.
2. Asegúrese de seleccionar el modo Desactivar el monitor HA en interfaces/canales que están desactivados y Activar INC (Configuración de red independiente) en las opciones de modo auto.

Eliminación de un nodo

Si elimina un nodo, los nodos ya no están en configuración de alta disponibilidad.

Para eliminar un nodo mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

`rm ha node <id>`

Ejemplo


```
> rm ha node 2
  Done
<!--NeedCopy-->
```

Para eliminar un nodo mediante la interfaz gráfica de usuario

Vaya a **Sistema** > **Alta disponibilidad** y, en la ficha **Nodos**, elimine el nodo.

> **Nota**:
>
> Puede utilizar el Visualizador de red para ver los dispositivos Citrix ADC configurados como un par de alta disponibilidad (HA) y realizar tareas de configuración de alta disponibilidad.

Configuración de monitores de ruta

August 20, 2021

Puede utilizar monitores de ruta para hacer que el estado de HA dependa de la tabla de redirección interna, independientemente de que la tabla contenga o no rutas estáticas o aprendidas dinámicamente. En una configuración de alta disponibilidad, un monitor de ruta en cada nodo vigila la tabla de redirección interno para asegurarse de que una entrada de ruta para llegar a una red determinada esté siempre presente. Si la entrada de ruta no está presente, el estado del monitor de ruta cambia a DOWN.

Cuando un dispositivo Citrix ADC solo tiene rutas estáticas para llegar a una red y quiere crear un monitor de rutas para la red, debe habilitar las rutas estáticas supervisadas (MSR) para las rutas estáticas. MSR elimina rutas estáticas inalcanzables de la tabla de redirección interno. Si MSR está inhabilitado en rutas estáticas, una ruta estática inalcanzable puede permanecer en la tabla de redirección interno, lo que contradice el propósito de tener el monitor de ruta.

Los monitores de ruta son compatibles tanto en modo no INC como en modo INC.

Monitores de ruta en alta disponibilidad en modo no INC	Monitores de ruta en HA en modo INC
Los monitores de ruta se propagan por nodos y se intercambian durante la sincronización.	Los monitores de ruta no se propagan por nodos ni se intercambian durante la sincronización.
Los monitores de ruta solo están activos en el nodo principal actual.	Los monitores de ruta están activos tanto en el nodo primario como en el secundario.

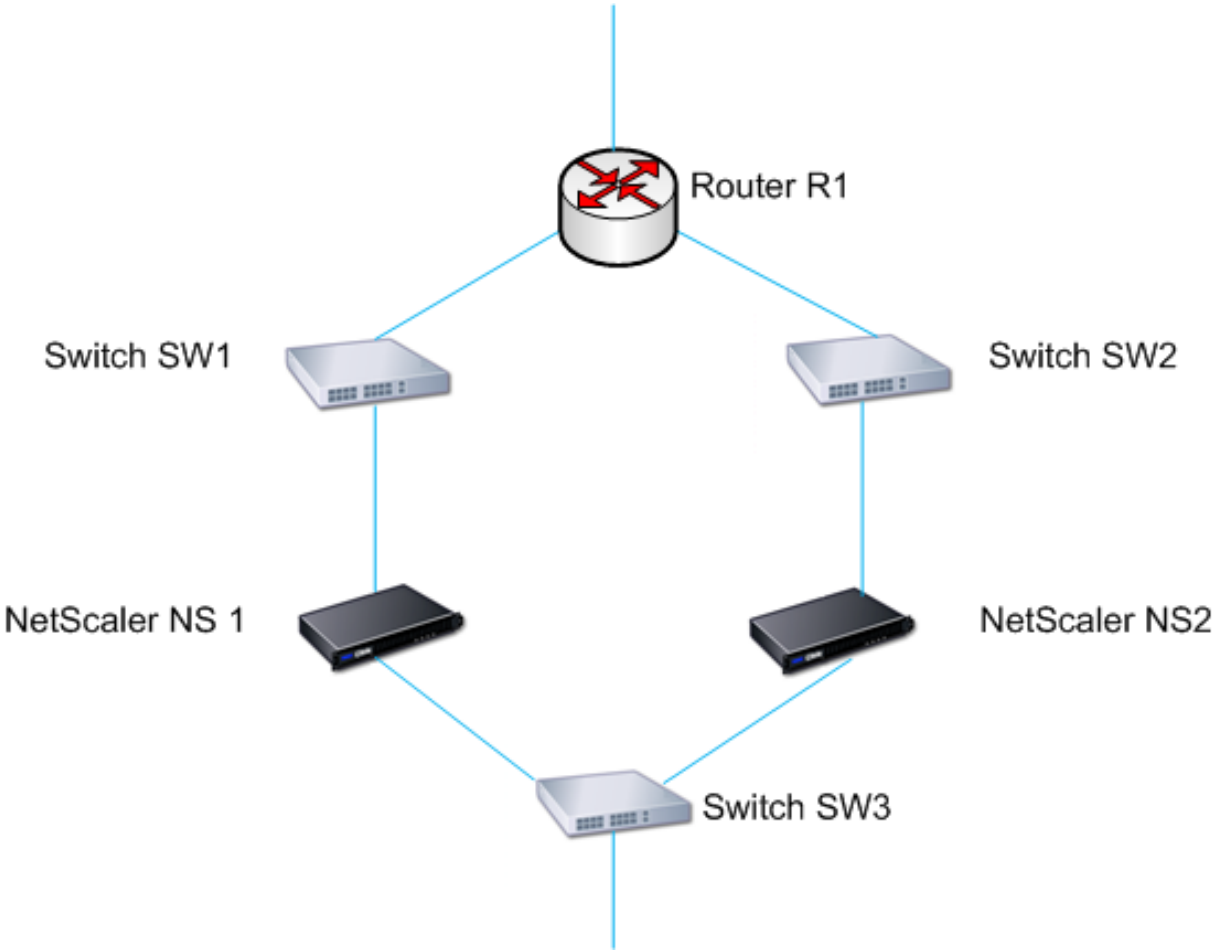
Monitores de ruta en alta disponibilidad en modo no INC	Monitores de ruta en HA en modo INC
El dispositivo Citrix ADC siempre muestra el estado de un monitor de ruta como UP, independientemente de si la entrada de ruta está presente o no en la tabla de redirección interno.	El dispositivo Citrix ADC muestra el estado del monitor de ruta como DOWN si la entrada de ruta correspondiente no está presente en la tabla de redirección interna.
Un monitor de rutas comienza a supervisar su ruta después de 180 segundos en los siguientes casos. [Esto se hace para permitir que se aprendan las rutas dinámicas, lo que puede tardar 180 segundos]: reinicio, failover, set route6 command for v6 route6, set route msr habilitar/disable comando para rutas v4, agregar un nuevo monitor de ruta.	-

Los monitores de ruta son útiles en una configuración de HA en modo no INC donde quiere que la no accesibilidad de una Gateway desde un nodo primario sea una de las condiciones para la conmutación por error de HA.

Considere un ejemplo de configuración de HA en modo no INC en una topología de dos brazos que tiene los dispositivos Citrix ADC NS1 y NS2 en la misma subred, con el router R1 y los conmutadores SW1, SW2 y SW3.

Dado que R1 es el único router en esta configuración, quiere que la configuración de HA se conmute por error siempre que R1 no sea accesible desde el nodo principal actual. Puede configurar un monitor de ruta (por ejemplo, RM1 y RM2, respectivamente) en cada uno de los nodos para supervisar la accesibilidad de R1 desde ese nodo.

Ilustración 1.



Con NS1 como nodo principal actual, el flujo de ejecución es el siguiente:

1. El monitor de ruta RM1 en NS1 monitorea la tabla de redirección interno de NS1 para detectar la presencia de una entrada de ruta para el enrutador R1. NS1 y NS2 intercambian mensajes de latidos a través del conmutador SW1 o SW3 a intervalos regulares.
2. Si el conmutador SW1 falla, el protocolo de redirección en NS1 detecta que R1 no es alcanzable y, por lo tanto, elimina la entrada de ruta para R1 de la tabla de redirección interno. NS1 y NS2 intercambian mensajes de latido a través del conmutador SW3 a intervalos regulares.
3. Al detectar que la entrada de ruta para R1 no está presente en la tabla de redirección interno, RM1 inicia una conmutación por error. Si la ruta a R1 está inactiva desde NS1 y NS2, la conmutación por error ocurre cada 180 segundos hasta que uno de los dispositivos pueda alcanzar R1 y restaurar la conectividad.

Agregar un monitor de ruta a un nodo de alta disponibilidad

Un único procedimiento crea un monitor de ruta y lo vincula a un nodo HA.

Para agregar un monitor de ruta mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

- `bind HA node <id> (-routeMonitor <ip_addr|ipv6_addr> [<netmask>])`
- `show HA node`

Ejemplo

```
> bind HA node 0 -routeMonitor 10.102.71.0 255.255.255.0
 Done
> bind HA node 0 -routeMonitor 1000:0000:0000:0000:0005:0600:700a:888b
 Done
<!--NeedCopy-->
```

Para agregar un monitor de ruta mediante la interfaz gráfica de usuario

Vaya a **Sistema** > **Alta disponibilidad** y, en la ficha **Monitores de ruta**, haga clic en **Configurar**.

Eliminación de monitores de ruta

Para quitar un monitor de ruta mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

- `unbind HA node <id> (-routeMonitor <ip_addr|ipv6_addr> [<netmask>])`
- show ha node

Ejemplo

```
unbind HA node 3 -routeMonitor 10.102.71.0 255.255.255.0
unbind HA node 3 -routeMonitor 1000:0000:0000:0000:0005:0600:700a:888b
<!--NeedCopy-->
```

Para quitar un monitor de ruta mediante la interfaz gráfica de usuario

Vaya a **Sistema** > **Alta disponibilidad** y, en la ficha **Monitores de ruta**, elimine el monitor de ruta.

Limitación de conmutaciones por error causadas por monitores de ruta en modo no INC

August 20, 2021

En una configuración de alta disponibilidad en modo no INC, si los monitores de ruta fallan en ambos nodos, la conmutación por error ocurre cada 180 segundos hasta que uno de los nodos pueda alcanzar todas las rutas supervisadas por los respectivos monitores de ruta.

Sin embargo, para un nodo, puede limitar el número de conmutaciones por error para un intervalo determinado estableciendo los parámetros Número máximo de volteos y Tiempo máximo de volteo en los nodos. Cuando se alcanza cualquiera de los límites, no se producen más conmutaciones y el nodo se asigna como primario (pero el estado del nodo es NOT UP) incluso si cualquier monitor de ruta falla en ese nodo. Esta combinación de estado HA como estado primario y estado de nodo como NO UP se denomina estado primario de palo.

Si el nodo puede llegar a todas las rutas supervisadas, el siguiente error del monitor desencadena el restablecimiento de los parámetros Número máximo de volteados y Tiempo máximo de volteo en el nodo e inicia la hora especificada en el parámetro Tiempo máximo de volteo.

Estos parámetros se establecen independientemente en cada nodo y, por lo tanto, no se propagan ni sincronizan.

Parámetros para limitar el número de conmutaciones por error

- **Número máximo de volteretas (MaxFlips)**

  Número máximo de conmutaciones por error permitido, dentro del intervalo de tiempo máximo de volteo, para el nodo en HA en modo no INC, si las conmutaciones por error son causadas por un error del monitor de ruta.

- **Tiempo máximo de volteo (MaxFlipTime)**

  Cantidad de tiempo, en segundos, durante el cual se permiten conmutaciones por error resultantes del error del monitor de ruta para el nodo en HA en modo no INC.

Para limitar el número de conmutaciones por error mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

- `set HA node [-maxFlips < positive_integer>] [-maxFlipTime <positive_integer >]`
- `show HA node [< id>]`

Para limitar el número de conmutaciones mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **Alta disponibilidad** y, en la ficha **Nodos**, abra el nodo local.

2. Defina los siguientes parámetros:

- Número máximo de volteretas
- Tiempo máximo de volteo

```
> set ha node -maxFlips 30 -maxFlipTime 60
Done
> sh ha node
1) Node ID: 0
IP: 10.102.169.82 (NS)
Node State: UP
Master State: Primary
Fail-Safe Mode: OFF
INC State: DISABLED
Sync State: ENABLED
Propagation: ENABLED
Enabled Interfaces : 1/1
Disabled Interfaces : None
HA MON ON Interfaces : 1/1
Interfaces on which heartbeats are not seen :None
Interfaces causing Partial Failure:None
SSL Card Status: NOT PRESENT
Hello Interval: 200 msecs
Dead Interval: 3 secs
Node in this Master State for: 0:4:24:1 (days:hrs:min:sec)

2) Node ID: 1
IP: 10.102.169.81
Node State: UP
Master State: Secondary
Fail-Safe Mode: OFF
INC State: DISABLED
Sync State: SUCCESS
Propagation: ENABLED
Enabled Interfaces : 1/1
Disabled Interfaces : None
HA MON ON Interfaces : 1/1
Interfaces on which heartbeats are not seen : None
Interfaces causing Partial Failure: None
SSL Card Status: NOT PRESENT

Local node information:
Configured/Completed Flips: 30/0
Configured Flip Time: 60
```



```
40     Critical Interfaces: 1/1
41
42     Done
43 <!--NeedCopy-->
```

Alarma SNMP para estado primario pegajoso

Habilite la alarma SNMP HA-STICKY-PRIMARY en un nodo con una configuración de alta disponibilidad si quiere recibir una alerta de que el nodo se convierta en primario pegajoso. Cuando el nodo se convierte en primario fijo, alerta generando un mensaje de captura (StickyPrimary (1.3.6.1.4.1.5951.1.1.0.138)) y lo envía a todos los destinos de captura SNMP configurados. Para obtener más información sobre cómo configurar alarmas SNMP y destinos de captura, consulte Configuración de Citrix ADC para generar capturas SNMPv1 y SNMPv2.

Preguntas frecuentes

Considere un ejemplo de configuración de alta disponibilidad de dos dispositivos Citrix ADC NS-1 y NS-2 en modo no INC. El número máximo de volteos y el tiempo máximo de volteo en ambos nodos se han establecido con los mismos valores.

En la tabla siguiente se enumeran los parámetros utilizados en este ejemplo:

Entidad	Detalles
Dirección IP de NS-1	10.102.173.211
Dirección IP de NS-2	10.102.173.212
Número máximo de volteretas	2
Tiempo máximo de volteo	200

Para obtener información sobre el número máximo de volteos y la configuración de tiempo de giro máximo, consulte el pdf.

Configuración del conjunto de interfaces de conmutación por error

August 20, 2021

Un conjunto de interfaces de conmutación por error (FIS) es un grupo lógico de interfaces. En una configuración de alta disponibilidad, el uso de un FIS es una forma de evitar la conmutación por er-

ror agrupando interfaces de modo que, cuando una interfaz falla, otras interfaces en funcionamiento sigan estando disponibles. También se puede configurar un FIS para los nodos de un clúster de Citrix ADC.

Las interfaces HA MON que no están enlazadas a un FIS se conocen como interfaces críticas (CI) porque si alguna de ellas falla, se activa la conmutación por error.

> **Nota**:
>
> Un FIS no crea una configuración activa y en espera. Tampoco impide la conexión de bucles en puente cuando se conecta a vínculos a la misma VLAN.

Creación o modificación de un FIS

Para agregar un FIS y enlazar interfaces a él mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

- `add fis <name>`
- `bind fis \<name\> \<ifnum\> ...`
- `show fis \<name\>`

Ejemplo

```
> add fis fis1
 Done
> bind fis fis1 1/3 1/5
 Done
<!--NeedCopy-->
```

Una interfaz independiente se convierte en una interfaz crítica (CI) si está habilitada y HA MON está activada.

Para desenlazar una interfaz de un FIS mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

- `unbind fis \<name\> \<ifnum\> ...`
- `show fis \<name\>`

Ejemplo

```
> unbind fis fis1 1/3
 Done
```



```
<!--NeedCopy-->
```

Para configurar un FIS mediante la interfaz gráfica de usuario

Vaya a Sistema > Alta disponibilidad y, en la ficha Juego de interfaces de conmutación por error, agregue un nuevo FIS o modifique un FIS existente.

Eliminación de un FIS

Cuando se elimina el FIS, sus interfaces se marcan como interfaces críticas.

Para eliminar un FIS mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
rm fis <name>
```

Ejemplo

```
> rm fis fis1
  Done
<!--NeedCopy-->
```

Para eliminar un FIS mediante la interfaz gráfica de usuario

Vaya a **Sistema** > **Alta disponibilidad** y, en la ficha **Juego de interfaces de conmutación por error**, elimine FIS.

Descripción de las causas de la conmutación por error

September 8, 2021

Los siguientes eventos pueden provocar la conmutación por error en una configuración de alta disponibilidad:

1. Si el nodo secundario no recibe un paquete de latidos del primario durante un período de tiempo que supera el intervalo muerto establecido en el secundario. (Consulte la nota 1.)
2. El nodo principal experimenta un fallo de hardware de su tarjeta SSL.
3. El nodo principal no recibe paquetes de latidos en sus interfaces de red durante tres segundos.

4. En el nodo principal, falla una interfaz de red que no forma parte de un conjunto de interfaces de conmutación por error (FIS) o de un canal de agregación de enlaces (LA) y tiene habilitado el Monitor de alta disponibilidad (HAMON). (Consulte la nota 2.)
5. En el nodo principal, fallan todas las interfaces de un FIS. (Consulte la nota 2.)
6. En el nodo principal, falla un canal LA con HAMON habilitado. (Consulte la nota 2.)
7. En el nodo principal, todas las interfaces fallan (consulte la nota 2). En este caso, la conmutación por error se produce independientemente de la configuración de HAMON.
8. En el nodo principal, todas las interfaces se inhabilitan manualmente. En este caso, la conmutación por error se produce independientemente de la configuración de HAMON.
9. Para forzar una conmutación por error, emite el comando force failover en cualquiera de los nodos.
10. Un monitor de ruta enlazado al nodo principal se desactiva.

> **Nota 1:**
>
> Para obtener más información sobre cómo configurar el intervalo muerto, consulte Configuración de los intervalos de comunicación. Entre las posibles causas de que un nodo no reciba paquetes de latidos de un nodo del mismo nivel se incluyen:
>
> - Un problema de configuración de red impide que los latidos atravesen la red entre los nodos de alta disponibilidad.
> - El nodo peer experimenta un fallo de hardware o software que hace que se congele (cuelgue), reinicie o detenga de otro modo el procesamiento y reenvío de paquetes de latidos cardíacos.
>
> **Nota 2:**
>
> En este caso, error significa que la interfaz está habilitada pero pasa al estado DOWN, como se puede ver en el comando show interface o desde la GUI. Las posibles causas para que una interfaz habilitada esté en estado DOWN son LINK DOWN y TXSTALL.

Obligar a un nodo a conmutar por error

August 20, 2021

Es posible que quiera forzar una conmutación por error si, por ejemplo, necesita reemplazar o actualizar el nodo principal. Puede forzar la conmutación por error desde el nodo principal o secundario. Una conmutación por error forzada no se propaga ni sincroniza. Para ver el estado de sincronización después de una conmutación por error forzada, puede ver el estado del nodo.

Una conmutación por error forzada falla en cualquiera de las siguientes circunstancias:

- Forzar la conmutación por error en un sistema independiente.

- El nodo secundario está inhabilitado.
- El nodo secundario está configurado para permanecer secundario.

El dispositivo Citrix ADC muestra un mensaje de advertencia si detecta un problema potencial al ejecutar el comando force failover. El mensaje incluye la información que activó la advertencia y solicita confirmación antes de continuar.

Puede forzar una conmutación por error en un nodo principal, nodo secundario y cuando los nodos están en modo de escucha.

- **Forzar conmutación por error en el nodo principal**.

  Si se fuerza la conmutación por error en el nodo principal, el primario se convierte en el secundario y el secundario en el primario. La conmutación por error forzada solo es posible cuando el nodo principal puede determinar que el nodo secundario está UP.

  Si el nodo secundario es DOWN, el comando force failover devuelve el siguiente mensaje de error: “Operation not possible due to invalid peer state. Rectificar y volver a intentarlo. “

  Si el sistema secundario está en estado de reclamación o está inactivo, devuelve el siguiente mensaje de error:

  ```
  Operation not possible now. Please wait for the system to stabilize
  before retrying.
  ```

- **Forzar conmutación por error en el nodo secundario**.

  Si ejecuta el comando force failover desde el nodo secundario, el nodo secundario se convierte en primario y el nodo primario se convierte en secundario. Una conmutación por error de fuerza solo puede producirse si el estado del nodo secundario es bueno y no está configurado para permanecer secundario.

  Si el nodo secundario no puede convertirse en el nodo principal o si el nodo secundario se ha configurado para permanecer secundario (mediante la opción STAYSECONDARY), el nodo muestra el siguiente mensaje de error:

  ```
  Operation not possible as my state is invalid. View the node for more
  information.
  ```

- **Forzar conmutación por error cuando los nodos están en modo de escucha**.

  Cuando los dos nodos de un par HA ejecutan versiones diferentes del software del sistema, el nodo que ejecuta la versión superior cambia al modo de escucha. En este modo, ni la propagación de comandos ni la sincronización funcionan.

  Antes de actualizar el software del sistema en ambos nodos, pruebe la nueva versión en uno de los nodos. Para ello, debe forzar una conmutación por error en el sistema que ya se ha actualizado. A continuación, el sistema actualizado toma el control como nodo principal, pero no se

produce ninguna propagación ni sincronización de comandos. Además, todas las conexiones deben restablecerse.

> **Importante.**
>
> Si fuerza una conmutación por error cuando se está realizando una operación de sincronización de alta disponibilidad, es posible que se pierdan algunas sesiones de datos activas en la configuración de alta disponibilidad. Por lo tanto, espere a que se complete la operación de sincronización de alta disponibilidad antes de realizar la operación de conmutación por error de fuerza.

Para forzar la conmutación por error en un nodo mediante la interfaz de línea de comandos:

En el símbolo del sistema, escriba:

```
force HA failover
```

Para forzar la conmutación por error en un nodo mediante la GUI:

Vaya a **Sistema** > **Alta disponibilidad** y, en la ficha **Nodos**, seleccione el nodo, en la lista Acciones, seleccione **Forzar conmutación por error**.

Obligar al nodo secundario a permanecer secundario

January 12, 2021

En una configuración de alta disponibilidad, el nodo secundario se puede obligar a permanecer secundario independientemente del estado del nodo primario.

Por ejemplo, supongamos que el nodo principal necesita ser actualizado y el proceso tomará unos segundos. Durante la actualización, el nodo principal puede bajar durante unos segundos, pero no quiere que el nodo secundario se haga cargo; quiere que siga siendo el nodo secundario aunque detecte un error en el nodo principal.

Cuando fuerce al nodo secundario a permanecer secundario, seguirá siendo secundario incluso si el nodo primario se desactiva. Además, cuando se fuerza el estado de un nodo en un par de HA para que permanezca secundario, no participa en transiciones de máquina de estado HA. El estado del nodo se muestra como STAYSECONDARY.

Obligar al nodo a permanecer secundario funciona tanto en nodos independientes como secundarios. En un nodo independiente, debe utilizar esta opción antes de poder agregar un nodo para crear un par HA. Al agregar el nuevo nodo, el nodo existente deja de procesar el tráfico y se convierte en el nodo secundario. El nuevo nodo se convierte en el nodo principal.

> **Nota**:
>
> Cuando se fuerza un sistema a permanecer secundario, el proceso de forzamiento no se propaga ni sincroniza. Solo afecta al nodo en el que se ejecuta el comando.

Para forzar al nodo secundario a permanecer secundario mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
set ha node -hastatus STAYSECONDARY
```

Para forzar al nodo secundario a permanecer secundario mediante el uso de la interfaz gráfica de usuario

Vaya a **Sistema** > **Alta disponibilidad**, en la ficha **Nodos**, abra el nodo local y seleccione **Permanezca SECUNDARIO**.

Obligar al nodo primario a permanecer primario

August 20, 2021

En una configuración de alta disponibilidad, puede forzar que un nodo principal en buen estado permanezca primario incluso después de una conmutación por error. Puede habilitar esta opción en un nodo principal de un par HA. Esta opción permite que el nodo principal esté en estado primario siempre que esté en buen estado.

En un nodo independiente, debe utilizar esta opción antes de poder agregar un nodo para crear un par HA. Cuando agrega el nuevo nodo, el nodo existente continúa funcionando como el nodo principal y el nuevo nodo se convierte en el nodo secundario.

Para forzar que el nodo principal permanezca primario mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
set ha node -hastatus STAYPRIMARY
```


Para forzar al nodo principal a permanecer primario mediante el uso de la interfaz gráfica de usuario

Vaya a **Sistema** > **Alta disponibilidad**, en la ficha **Nodos**, abra el nodo local y seleccione **Permanezca PRIMARIO**.

Comprender el cálculo de comprobación de estado de alta disponibilidad

January 12, 2021

En la siguiente tabla se resumen los factores examinados en un cálculo de comprobación de estado:

- Estado de los conjuntos de interfaces de conmutación por error
- Estado de las interfaces críticas
- Estado de los monitores de ruta

En la siguiente tabla se resume el cálculo de la comprobación de estado.

Conjuntos de interfaces de conmutación por error	Interfaces críticas	Monitor de ruta	Condición
N	S	N	Si el sistema tiene alguna interfaz crítica, todas esas interfaces críticas deben estar UP.
S	S	N	Si el sistema tiene conjuntos de interfaces de conmutación por error, todos esos conjuntos de interfaces de conmutación por error deben estar UP.

Conjuntos de interfaces de conmutación por error	Interfaces críticas	Monitor de ruta	Condición
S	S	S	Si el sistema tiene algún monitor de ruta configurado, todas las rutas supervisadas deben estar presentes en el conjunto de interfaz de conmutación por error.

Preguntas frecuentes sobre alta disponibilidad

August 20, 2021

1. ¿Cuáles son los diversos puertos utilizados para intercambiar información relacionada con HA entre los nodos en una configuración de HA?

   En una configuración de alta disponibilidad, ambos nodos utilizan los siguientes puertos para intercambiar información HareLated:

   - Puerto UDP 3003, para intercambiar paquetes de latidos.
   - Puerto 3010, para sincronización y propagación de comandos.

2. ¿Cuáles son las condiciones que desencadenan la sincronización?

   La sincronización se activa por cualquiera de las siguientes condiciones:

   - El número de encarnación del nodo primario, recibido por el secundario, no coincide con el del nodo secundario.
     Nota: Ambos nodos en una configuración de HA mantienen un contador llamado *número de encarnación*, que cuenta el número de configuraciones en el archivo de configuración del nodo. Cada nodo envía su número de encarnación entre sí nodo en los mensajes de latido. El número de encarnación no se incrementa para los siguientes comandos:
     a) Todos los comandos relacionados con la configuración de HA. Por ejemplo, agregue nodo ha, establezca nodo ha y enlace ha nodo.
     b) Todos los comandos relacionados con la interfaz. Por ejemplo, set interface y unset interface.

c) Todos los comandos relacionados con el canal. Por ejemplo, agregue canal, establezca canal y enlace canal.

- El nodo secundario aparece después de reiniciar.
- El nodo principal se convierte en secundario después de una conmutación por error.

3. ¿Qué configuraciones no se sincronizan o propagan en una configuración de alta disponibilidad en modo INC o no INC?

   Los siguientes comandos no se propagan ni sincronizan con el nodo secundario:

   - Todos los comandos de configuración de HA específicos del nodo. Por ejemplo, agregue nodo ha, establezca nodo ha y enlace ha nodo.
   - Todos los comandos de configuración relacionados con la interfaz. Por ejemplo, set interface y unset interface.
   - Todos los comandos de configuración relacionados con el canal. Por ejemplo, agregue canal, establezca canal y enlace canal.

   > **Nota:**
   >
   > Las siguientes configuraciones no se sincronizan ni se propagan solo en HA en modo INC. Cada nodo tiene su propio:
   >
   > ```
   > 1 - SNIP
   > ```
   >
   > - VLAN
   > - Rutas (excepto rutas LLB)
   > - Monitores de ruta
   > - Reglas RNAT (excepto cualquier regla RNAT con VIP como IP NAT)
   > - Configuraciones de redirección dinámica
   > - Perfiles de red

4. ¿Se sincroniza una configuración agregada al nodo secundario en el primario?

   No, una configuración agregada al nodo secundario no se sincroniza con el primario.

5. ¿Cuál podría ser la razón por la que ambos nodos afirman ser el principal en una configuración de alta disponibilidad?

   La razón más probable es que los nodos primario y secundario están en buen estado, pero el secundario no recibe los paquetes de latido del primario. El problema podría estar con la red entre los nodos.

6. ¿Una configuración de alta disponibilidad tiene algún problema si implementa los dos nodos con diferentes configuraciones de reloj del sistema?

Diferentes configuraciones de reloj del sistema en los dos nodos pueden causar los siguientes problemas:

- Las marcas de tiempo de las entradas del archivo de registro no coinciden. Esta situación hace que sea difícil analizar las entradas de registro para cualquier problema.
- Después de una conmutación por error, es posible que tenga problemas con cualquier tipo de persistencia basada en cookies para el equilibrio de carga. Una diferencia significativa entre los tiempos puede hacer que una cookie caduque antes de lo esperado, lo que resulta en la terminación de la sesión de persistencia.
- Consideraciones similares se aplican a cualquier decisión relacionada con el tiempo en los nodos.

7. ¿Cuáles son las condiciones para el fallo del comando *force HA sync* ?

   La sincronización forzada falla en cualquiera de las siguientes circunstancias:

   - Fuerza la sincronización cuando la sincronización ya está en curso.
   - Forzar la sincronización en un dispositivo Citrix ADC independiente.
   - El nodo secundario está inhabilitado.
   - La sincronización de HA está inhabilitada en el nodo secundario actual.
   - La propagación de HA está inhabilitada en el nodo principal actual y se fuerza la sincronización desde el primario.

8. ¿Cuáles son las condiciones para el fallo del comando *sync HA files* ?

   La sincronización de archivos de configuración falla en cualquiera de las siguientes circunstancias:

   - En un sistema independiente.
   - Con el nodo secundario inhabilitado.

9. En una configuración de alta disponibilidad, si el nodo secundario toma el control como primario, ¿cambia de nuevo al estado secundario si el primario original vuelve a conectarse?

   No. Después de que el nodo secundario toma el control como principal, permanece como primario incluso si el nodo primario original vuelve a conectarse de nuevo. Para intercambiar el estado primario y secundario de los nodos, ejecute el comando *force failover*.

10. ¿ Cuáles son las condiciones para el fallo del comando force failover ?

    Una conmutación por error forzada falla en cualquiera de las siguientes circunstancias:

    - Forzar la conmutación por error en un sistema independiente.
    - El nodo secundario está inhabilitado.
    - El nodo secundario está configurado para permanecer secundario.
    - El nodo principal está configurado para que siga siendo primario.
    - El estado del nodo del mismo nivel es desconocido.

Solución de problemas de alta disponibilidad

August 20, 2021

Los problemas de alta disponibilidad más comunes implican que la función de alta disponibilidad no funcione en absoluto o que funcione solo de forma intermitente. A continuación se presentan problemas comunes de alta disponibilidad, y causas probables y resoluciones.

- **Problema**
  Incapacidad de los dispositivos Citrix ADC para emparejar los dispositivos Citrix ADC en una configuración de alta disponibilidad.
  - **Causa**
    Conectividad de red
    Solución:
    Compruebe que los dispositivos estén conectados al conmutador y que las interfaces estén habilitadas.
  - **Causa**
    Falta de coincidencia en la contraseña de la cuenta de administrador predeterminada
    Solución:
    Compruebe que la contraseña de ambos dispositivos sea la misma.
  - **Causa**
    Conflicto de IP
    Solución:
    Compruebe que ambos dispositivos tienen una dirección IP de Citrix ADC (NSIP) única. Los dispositivos no deben tener la misma dirección NSIP.
  - **Causa**
    No coincide el ID de nodo
    Solución:
    Compruebe que la configuración de ID de nodo en ambos dispositivos es única. Los dispositivos no deben tener la misma configuración de ID de nodo. Además, debe asignar un valor para un ID de nodo entre 1 y 64.
  - **Causa**
    Falta de coincidencia en la contraseña del nodo RPC
    Solución:
    Compruebe que ambos nodos tienen la misma contraseña de nodo RPC.
  - **Causa**
    Un administrador ha inhabilitado el nodo remoto.
    Solución:
    Habilite el nodo remoto.
  - **Causa**

La aplicación Firewall ha bloqueado los paquetes de latido
Solución:

Compruebe que el puerto UDP 3003 está permitido.

- **Problema**
  Ambos dispositivos afirman ser el dispositivo principal.
  - **Causa**
    Paquetes de latido faltantes entre los dispositivos
    Solución:
    Compruebe que el puerto UDP 3003 no está bloqueado para la comunicación entre los dispositivos.
- **Problema**
  El dispositivo Citrix ADC no puede sincronizar la configuración.
  - **Causa**
    Una aplicación Firewall está bloqueando el puerto requerido.
    Solución:
    Compruebe que el puerto UDP 3010 (o el puerto UDP 3008 con sincronización segura) no está bloqueado para la comunicación entre los dispositivos.
  - **Causa**
    Un administrador ha inhabilitado la sincronización.
    Solución:
    Habilite la sincronización en el dispositivo que tiene el problema.
  - **Causa**
    Se instalan diferentes versiones o compilaciones de Citrix ADC en los dispositivos.
    Solución:
    Actualice los dispositivos a la misma versión o compilación de Citrix ADC.
- Error en la propagación del**comando**
  entre los dispositivos.
  - **Causa**
    Una aplicación Firewall está bloqueando el puerto.
    Solución:
    Compruebe que el puerto UDP 3011 (o el puerto UDP 3009 con propagación segura) no está bloqueado para la comunicación entre los dispositivos.
  - **Causa**
    Un administrador ha inhabilitado la propagación de comandos.
    Solución:
    Habilite la propagación de comandos en el dispositivo que tiene el problema.
  - **Causa**
    Se instalan diferentes versiones o compilaciones de Citrix ADC en los dispositivos.
    Solución:

Actualice los dispositivos a la misma versión o compilación de Citrix ADC.

- **Problema**
  Los dispositivos Citrix ADC del par de alta disponibilidad no pueden ejecutar el proceso de conmutación por error forzado.
  - **Causa**
    El nodo secundario está inhabilitado.
    Solución:
    Habilite el nodo secundario.
  - **Causa**
    El nodo Secundario está configurado para permanecer secundario.
    Solución:
    Establezca el estado secundario de alta disponibilidad del nodo secundario en Habilitar desde Permanencia secundaria.
- **Problema**
  El dispositivo secundario no recibe tráfico después del proceso de conmutación por error.
  - **Causa**
    El router ascendente no comprende los mensajes GARP del dispositivo Citrix ADC.
    Solución:
    Configure la dirección MAC virtual en el dispositivo secundario.

Administración de mensajes de latido de alta disponibilidad en un dispositivo Citrix ADC

January 12, 2021

Los dos nodos en una configuración de alta disponibilidad envían y reciben mensajes de latido entre sí en todas las interfaces habilitadas. Los mensajes de latido fluyen independientemente de la configuración HA MON en estas interfaces. Si NSVLAN o ambos (NSVLAN y SYNC) están configurados en un dispositivo, los mensajes de latido solo fluyen a través de las interfaces habilitadas que forman parte de NSVLAN y SYNCVLAN.

Si un nodo no recibe los mensajes de latido en una interfaz habilitada, envía alertas críticas a los administradores del Command Center y SNMP especificados. Estas alertas críticas proporcionan falsas alarmas y atraen la atención innecesaria de los administradores para las interfaces que no están configuradas como parte de las conexiones al nodo del mismo nivel.

Para resolver este problema, la opción HAHeartBeat para interfaces y canales se utiliza para habilitar o inhabilitar el flujo de mensajes de latido de HA en ellos.

Para administrar los mensajes de latido de alta disponibilidad en una interfaz mediante la interfaz de

línea de comandos

En el símbolo del sistema, escriba:

- `set interface <ID> [-HAHeartBeat ( ON | OFF )]`
- `show interface <ID>`

Para administrar los mensajes de latido de alta disponibilidad en un canal mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

- `set channel <ID> [-HAHeartBeat ( ON | OFF )]`
- `show channel <ID>`

Para administrar los mensajes de latido de alta disponibilidad para una interfaz mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **Red** > **Interfaces**.
2. Habilite o inhabilite el parámetro **HA Heart Beat**.

Para administrar los mensajes de latido de alta disponibilidad en un canal mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **Red** > **Canales**.
2. Habilite o inhabilite el parámetro **HA Heart Beat**.

Quitar y reemplazar un dispositivo Citrix ADC en una instalación de alta disponibilidad

August 20, 2021

Este tema le ayuda a abordar los reemplazos de RMA. Además, este tema contiene instrucciones sobre cómo realizar copias de seguridad de las configuraciones, actualizar o degradar la versión de software enviada y configurar la contraseña de RPC en ADC.

Puntos a considerar

Las siguientes configuraciones no se sincronizan ni propagan en una configuración de alta disponibilidad en modo INC (Configuración de red independiente) o no INC:

- Todos los comandos de configuración de HA específicos del nodo. Por ejemplo, agregue nodo ha, establezca nodo ha y enlace ha nodo.
- Todos los comandos de configuración relacionados con la interfaz. Por ejemplo, set interface y unset interface.

- Todos los comandos de configuración relacionados con el canal. Por ejemplo, agregue canal, establezca canal y enlace canal.
- Todos los comandos de configuración de Interface HA Monitoring.

Las siguientes configuraciones no se sincronizan ni propagan en una configuración de alta disponibilidad en modo INC (Configuración de red independiente):

- SNIP
- VLAN
- Rutas (excepto rutas LLB)
- Monitores de ruta
- Reglas RNAT (excepto cualquier regla RNAT con VIP como IP NAT)
- Configuraciones de redirección dinámica

Instrucciones

Complete los siguientes pasos para reemplazar un dispositivo Citrix ADC en una configuración de alta disponibilidad:

- Quitar un nodo secundario Active Citrix ADC
- Configurar nodo secundario de reemplazo
- Verificar y actualizar la compilación de software en ADC de reemplazo
- Establecer contraseña en Nuevo secundario a Coincidir principal
- Agregar licencias al ADC de reemplazo
- Creación de un par de HA entre el nodo primario y el nodo secundario nuevo

Quitar un nodo secundario activo

1. Inicie sesión en ambos ADC y ejecute el siguiente comando para confirmar qué nodo es primario y qué nodo es secundario:

```
1 show ha node
2 <!--NeedCopy-->
```

2. Inicie sesión en el ADC principal, realice una copia de seguridad de las configuraciones en el nodo principal y copie los archivos fuera del ADC antes de los cambios. Estos archivos se encuentran en el directorio “/var /ns_sys_backup/”.

   Los pasos son:

   a) Guarde las configuraciones que se ejecutan ADC en la memoria:


```
save ns config
<!--NeedCopy-->
```

b) Cree el paquete completo de archivos de copia de seguridad:

```
create system backup -level full
<!--NeedCopy-->
```

c) Cree el paquete básico de archivos de copia de seguridad:

```
create system backup -level basic
<!--NeedCopy-->
```

3. Después de que se hayan generado todos los archivos de copia de seguridad, asegúrese de copiarlos del dispositivo antes de continuar.

   Desde un terminal de Windows, abra un símbolo del sistema y copie los archivos de copia de seguridad del ADC y en el disco duro local. Esto se puede hacer mediante el siguiente comando:

```
pscp <username>@<NSIP>:<Target file source>  <Target file
   destination>
<!--NeedCopy-->
```

   Ejemplo:

```
pscp nsroot@10.125.245.78:/var/ns_sys_backup/backup_basic_10
   .125.245.78_2016_09_14_15_08.tgz c:\nsbackup\backup_basic_10
   .125.245.78_2016_09_14_15_08.tgz
<!--NeedCopy-->
```

   Cuando se le solicite, introduzca la contraseña de la cuenta de administrador especificada y, a continuación, pulse Intro. Repita estos pasos hasta que todos los paquetes de copia de seguridad se copien en el PC local antes de continuar.

4. SSH en el ADC secundario y establezca la unidad en el estado “STAYSECUNDARY”. Esto obligará a la unidad a no intentar asumir el rol principal en caso de que se detecte un error durante el intercambio. Confirme que está conectado al ADC secundario antes de ejecutar este paso


```
set ha node  -haStatus <state>
set ha node  -haStatus STAYSECONDARY
<!--NeedCopy-->
```

5. Una vez que el **estado del nodo** del ADC secundario muestra correctamente STAYSECONDARY, cambie al ADC principal y elimine el nodo secundario y ejecute el siguiente comando:

```
save ns config
<!--NeedCopy-->
```

Mientras haya iniciado sesión en el ADC principal, ejecute los siguientes comandos

a) Ejecute el siguiente comando para identificar qué valor numérico representa el nodo HA secundario:

```
show ha node
<!--NeedCopy-->
```

b) Ejecute el siguiente comando para eliminar el ADC secundario del par HA primario;

```
rm ha node <node ID>
<!--NeedCopy-->
```

c) Ejecute el siguiente comando para guardar la configuración:

```
save ns config
<!--NeedCopy-->
```

d) Con el ADC secundario ahora eliminado, apague, desconecte y quite el ADC secundario de la red.

Nota: Asegúrese de etiquetar todas las conexiones antes de desconectar.

Configurar nodo secundario de reemplazo

1. Con el ADC de reemplazo en su lugar, encienda el nuevo dispositivo. NO CONECTAR las conexiones de red en este punto.

2. Con el inicio completo, utilice el puerto de consola para conectarse al ADC y configure el NSIP que utilizará para conectarse a la unidad.
3. Cuando se le solicite, seleccione **4**.

   Nota: En este ejemplo, se utiliza otro NSIP para el ADC de reemplazo. Si quiere utilizar la IP de la unidad secundaria original, puede cambiarla en el reemplazo antes de vincular el nuevo ADC a la unidad HA primaria.
4. Ahora se debe arrancar el ADC. Ahora conecte la interfaz de red que se utilizará para el tráfico de administración y confirme que la dirección IP es accesible desde su red.

Verificar y actualizar la compilación de software en ADC de reemplazo

Antes de sincronizar la nueva unidad con el ADC principal, tenemos que asegurarnos de que ambos ADC están ejecutando la misma compilación.

1. Para verificar la versión en ADC, ejecute el siguiente comando:

```
1 show version
2 <!--NeedCopy-->
```

2. Mientras esté en el nuevo ADC secundario, cree una subcarpeta en **/var** que se utilizará para la actualización.
3. Vaya a Descargas de Citrix y descargue el paquete adecuado que coincida con la versión de compilación que se ejecuta en el ADC principal.
4. Descargue y extraiga el archivo.tgz:

```
1 tar -xvzf "file.tgz"
2 <!--NeedCopy-->
```

5. Copie los archivos extraídos en el ADC secundario. En su terminal de Windows, abra un "Símbolo del sistema" y navegue hasta el directorio que contiene el paquete de compilación.tgz extraído y ejecute el siguiente comando pscp:

```
1 pscp <Target file source>  <username>@<NSIP>:<Target file
     destination>
2 <!--NeedCopy-->
```


Ejemplo:

```
C:\inetpub>pscp c:\inetpub\build-12.1-47.14_nc.tgz nsroot@10
    .20.245.80:/var/NS_upg_12.1_47.14/build-12.1-47.14_nc.tgz
<!--NeedCopy-->
```

6. Una vez transferido el archivo, vuelva al ADC secundario y actualice. Para obtener instrucciones detalladas, consulte Actualización de un dispositivo independiente Citrix ADX.
7. Una vez que el nuevo secundario se haya reiniciado, SSH vuelva a la unidad y confirme que la actualización es correcta y que la compilación coincide con la del primario.

Establecer la contraseña en el nodo secundario de reemplazo para que coincida con el primario

Nota: Si en este momento quiere cambiar la dirección IP de administración (NSIP) del nuevo ADC secundario, puede hacerlo antes de avanzar.

Cambie la contraseña en el nuevo ADC secundario para que coincida con la contraseña que se encuentra actualmente en el ADC principal.

1. Asegúrese de que la contraseña predeterminada de la cuenta de administrador (nsroot) sea la misma que el ADC principal. Esto se logra mediante el siguiente comando mientras se inicia sesión a través de SSH en la nueva unidad secundaria:

```
set system user <user> <password>
<!--NeedCopy-->
```

   Este comando establece/restablece la contraseña del usuario especificado.

2. SSH en el ADC primario y nuevo secundario y confirmar que las contraseñas coinciden.

Agregar licencias al nodo secundario de reemplazo

Con el nuevo ADC actualizado y listo para el emparejamiento, descargue e instale la licencia adecuada para el nodo de reemplazo.

1. Vaya a https://www.citrix.com para solicitar y descargar licencias para la nueva unidad de reemplazo.
2. Una vez que haya descargado todas las licencias apropiadas, SSH en el nuevo ADC secundario y escriba el siguiente comando para ver el estado actual de la licencia:


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

3. Desde el símbolo del sistema del terminal de Windows, ahora debe cargar los archivos de licencia en el nuevo ADC secundario mediante el siguiente comando:

   Nota: Si tiene varias licencias, repita este paso hasta que se carguen todas las licencias.

```
pscp <Target file source>  <username>@<NSIP>:<Target file
   destination>
<!--NeedCopy-->
```

   Ejemplo:

```
C:\inetpub>pscp c:\inetpub\NS-VPX-3K-LIC-020030ad0024.lic
   nsroot@10.125.245.80:/nsconfig/license/NS-VPX-3K-LIC-020030
   ad0024.lic
<!--NeedCopy-->
```

4. SSH en el nuevo ADC secundario y realice un reinicio caliente mediante el siguiente comando:

```
reboot  -w
<!--NeedCopy-->
```

   Después de reiniciar la unidad, SSH en la unidad y ejecute el comando show license una vez más. En este punto, las licencias deben ser aplicadas.

Configuración de alta disponibilidad entre el nodo principal y el nodo secundario nuevo

En este punto, ahora estamos listos para unir las unidades Citrix ADC en un par de alta disponibilidad. Para obtener más información, consulte Configuración de alta disponibilidad.

Solicitar reintento

December 2, 2021

Cuando un dispositivo Citrix ADC recibe una solicitud HTTP pero tiene un error de conexión con un servidor back-end, el dispositivo utiliza una directiva de reintento. El reintento de la solicitud aborda los casos de error de conexión y permite que el dispositivo elija el siguiente servicio disponible y reenvíe la solicitud. Al hacer un reintento de solicitud, el cliente puede ahorrar tiempo de ida y vuelta (RTT).

La función de reintento de solicitud se aplica a los siguientes casos de error de conexión:

- Si un servidor back-end restablece una conexión TCP cuando se recibe una solicitud HTTP. Para obtener más información, consulta Solicitar reintento.
- Si un servidor back-end restablece una conexión TCP durante el establecimiento de la conexión. Para obtener más información, consulta Solicitar reintento.
- Si se agota el tiempo de espera de una respuesta de un servidor back-end (en función del valor de tiempo de espera configurado) cuando un dispositivo envía una solicitud HTTP. Para obtener más información, consulta Solicitar reintento.

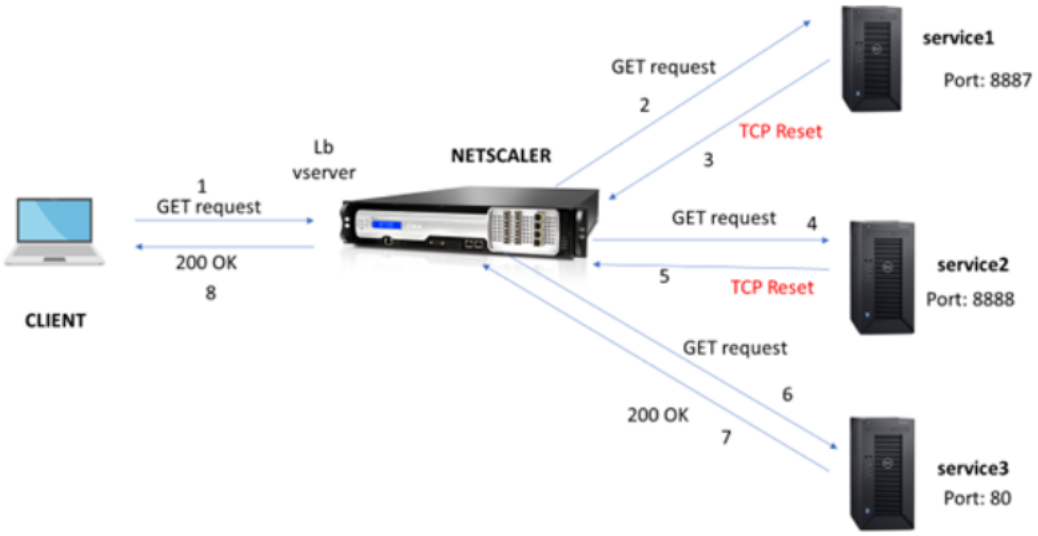
Solicitar reintento si el servidor back-end restablece la conexión TCP

August 20, 2021

Cuando un servidor back-end restablece una conexión TCP, la función de reintento de solicitud reenvía la solicitud al siguiente servidor disponible, en lugar de enviar el restablecimiento al cliente. Al realizar el equilibrio de recarga, el cliente guarda RTT cuando el dispositivo inicia la misma solicitud al siguiente servicio disponible.

Cómo funciona el reintento de solicitud cuando el servidor back-end restablece una conexión TCP

El siguiente diagrama muestra cómo interactúan los componentes entre sí.



1. El proceso comienza habilitando la función appqoe en el dispositivo.
2. Cuando el cliente envía una solicitud HTTP o HTTPS, el servidor virtual de equilibrio de carga envía la solicitud al servidor back-end.
3. Si el servicio solicitado no está disponible, el servidor back-end restablece la conexión TCP.
4. Si la configuración de appqoe tiene habilitado “reintentar” con el número deseado de intentos de reintento especificado, el servidor virtual de equilibrio de carga utiliza el algoritmo de equilibrio de carga configurado para reenviar la solicitud al siguiente servidor de aplicaciones disponible.
5. Después de que el servidor virtual de equilibrio de carga reciba la respuesta, el dispositivo reenvía la respuesta al cliente.
6. Si los servidores back-end disponibles son iguales o inferiores al recuento de reintentos y si todos los servidores envían restablecimiento, el dispositivo responderá a un error de 500 servidores internos. Considere un caso con cinco servidores disponibles y el recuento de reintentos establecido como seis. Si los cinco servidores restablecen la conexión, el dispositivo devuelve un error de servidor interno 500 al cliente.
7. Del mismo modo, si el número de servidores back-end es superior al recuento de reintentos y si los servidores back-end restablecen la conexión, el dispositivo reenvía el restablecimiento al cliente. Considere un caso con tres servidores back-end y el recuento de reintentos establecido como dos. Si los tres servidores restablecen la conexión, el dispositivo envía una respuesta de restablecimiento al cliente.

Configurar reintento de solicitud para el método GET

Para configurar la función de reintento para el método GET, debe completar los siguientes pasos.

1. Habilitar AppQoE
2. Agregar acción AppQoE
3. Agregar directiva AppQoE
4. Vincular la directiva AppQoE al servidor virtual de equilibrio de carga

Habilitar AppQoE

En el símbolo del sistema, escriba:

```
enable ns feature appqoe
```

Agregar acción AppQoE

Debe configurar una acción AppQoE para especificar si quiere que el dispositivo vuelva a intentarlo después de un restablecimiento de TCP y el número de intentos de reintento.

```
add appqoe action reset_action -retryOnReset ( YES | NO )-numretries <
positive_integer>]
```

Ejemplo:

```
add appqoe action reset_action -retryOnReset YES -numretries 5
```

Donde:
RetryOnReset. Habilite el reintento si el servidor back-end restablece una conexión TCP.
intentos numéricos. Reintentar contar.

Agregar directiva AppQoE

Para implementar AppQoE, debe configurar la directiva AppQoE para priorizar la solicitud HTTP o SSL entrante en una cola específica.

En el símbolo del sistema, escriba:

```
add appqoe policy <name> -rule <expression> -action <string>
```

Ejemplo:

```
add appqoe policy reset_policy -rule http.req.method.eq(get)-action reset_action
```

Vincular la directiva appqoe al servidor virtual de equilibrio de carga

Cuando un servidor back-end restablece una solicitud de paquete TCP y si quiere que el servidor virtual de equilibrio de carga reenvíe la solicitud al siguiente servicio disponible, debe enlazar el servidor virtual de equilibrio de carga a la directiva AppQoE.

En el símbolo del sistema, escriba:

```
bind lb vserver <name> ((<serviceName> (-policyName <string> [-priority <
positive_integer>] [-gotoPriorityExpression <expression>] [-type ( REQUEST
| RESPONSE )]
```

Ejemplo:

```
bind lb vserver v1 -policyName reset_policy -type REQUEST -priority 1
```

Configurar reintento de solicitud para solicitudes POST

Siempre debe tener precaución al volver a cargar las solicitudes de equilibrio que escriben datos en el servidor back-end. Para tales solicitudes, asegúrese de que la longitud del contenido sea corta. Si la longitud del contenido es larga, puede resultar en el consumo de recursos. Siga los pasos que se indican a continuación para configurar el equilibrio de recarga para las solicitudes POST.

1. Habilitar AppQoE
2. Agregar acción AppQoE
3. Agregar directiva AppQoE
4. Vincular la directiva AppQoE al servidor virtual de equilibrio de carga

Habilitar AppQoE

En el símbolo del sistema, escriba:

```
enable ns feature appqoe
```

Agregar acción Appqoe

Debe agregar una acción AppQoE para volver a intentarlo después de un restablecimiento de TCP y número de intentos de reintento.

```
add appqoe action reset_action -retryOnReset ( YES | NO )-numretries <
positive_integer>]
```

Ejemplo:

```
add appqoe action reset_action -retryOnReset YES -numretries 5
```

Agregar directiva Appqoe

Para implementar AppQoE debe configurar la directiva AppQoE para definir cómo poner en cola las conexiones en una cola específica.

En el símbolo del sistema, escriba:


```
add appqoe policy <name> -rule <expression> -action <string>
```

Ejemplo:

```
add appqoe policy reset_policy -rule HTTP.REQ.CONTENT_LENGTH.le(2000)-
action reset_action
```

> **Nota:**
>
> Puede utilizar esta configuración si prefiere restringir la función de reintento de solicitud para una longitud de contenido inferior a 2000.

Vincular el servidor virtual de equilibrio de carga a la directiva AppQoE

Cuando un servidor back-end restablece una solicitud de paquete TCP y si quiere que el servidor virtual de equilibrio de carga reenvíe la solicitud al siguiente servicio disponible a través de una cola específica, debe enlazar el servidor virtual de equilibrio de carga a la directiva AppQoE.

En el símbolo del sistema, escriba:

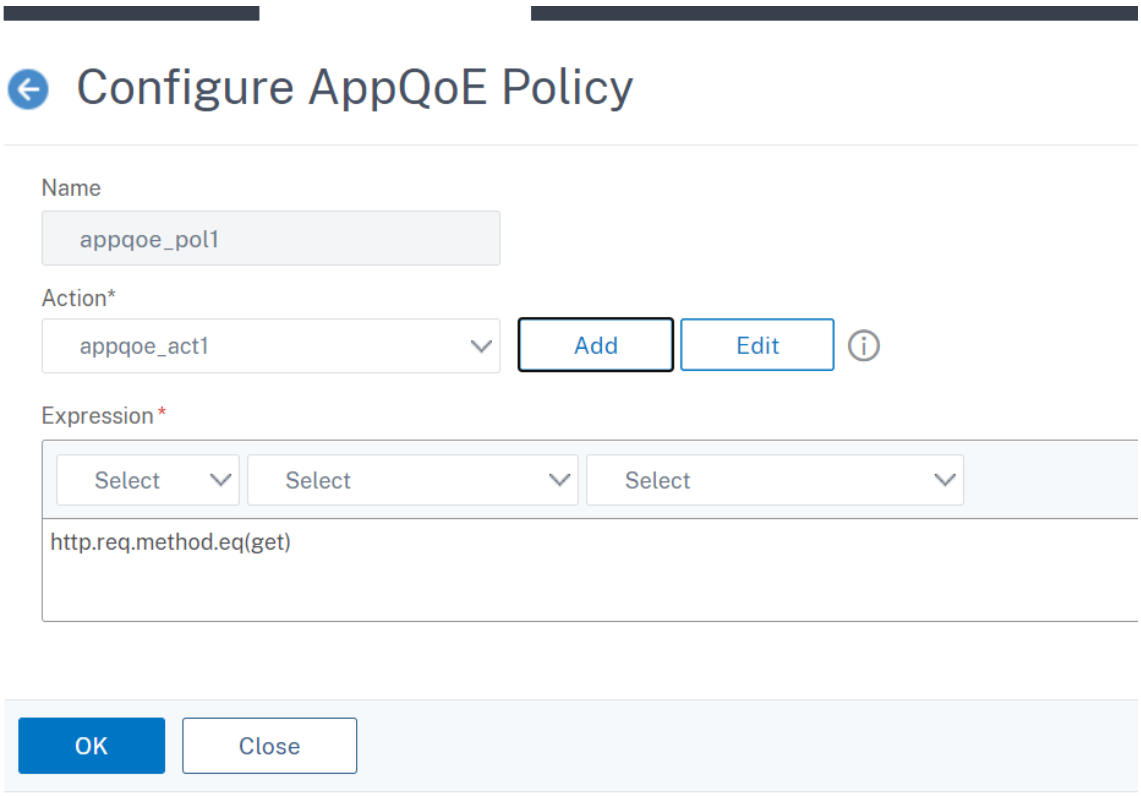
```
bind lb vserver <name> ((<serviceName> (-policyName <string> [-priority <
positive_integer>] [-gotoPriorityExpression <expression>] [-type ( REQUEST
| RESPONSE )]
```

Ejemplo:

```
bind lb vserver v1 -policyName reset_policy -type REQUEST -priority 1
```

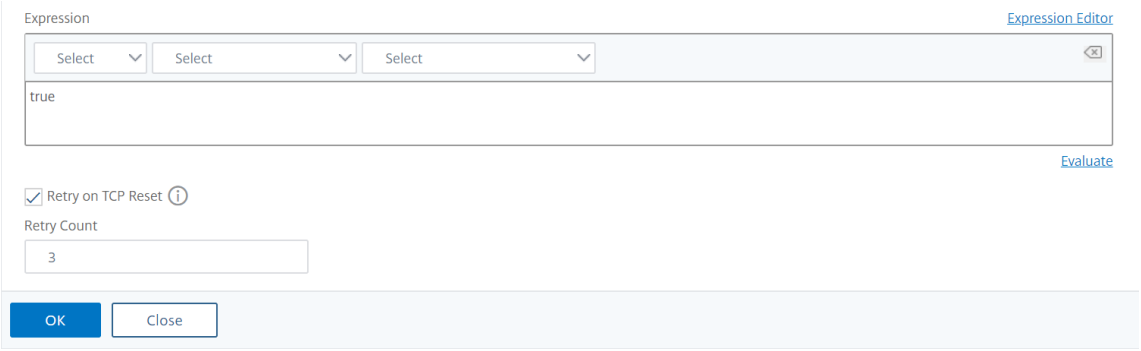
Configurar la directiva AppQoE para reintentar solicitudes mediante la GUI de Citrix ADC

1. Vaya a **AppExpert** > **AppQoE** > **Directivas**.
2. En la página **Directivas de AppQoE**, haga clic en **Agregar**.
3. En la página **Crear una directiva de AppQoE**, establezca los siguientes parámetros:
   a. nombre. Nombre de directiva AppQoE
   b. Acción. Agregar o modificar una acción. Para crear una acción, consulte la sección .
   c. expresión. Seleccione o escriba expresión`HTTP.REQ.CONTENT_LENGTH.le (2000)` de directiva.
4. Haga clic en **Crear** y **cerrar**.



Configurar la acción de AppQoE para el equilibrio de reintentos de solicitud mediante la GUI de Citrix ADC

1. Vaya a **AppExpert** > **AppQoE** > **Acción**.
2. En la página **Acciones de AppQoE**, haga clic en **Agregar**.
3. En la página **Crear acción de AppQoE**, establezca los siguientes parámetros para reintentar al restablecer TCP:
   a. Vuelva a intentar reiniciar TCP. Active la casilla de verificación para habilitar la acción de reintento para restablecer TCP.
   b. Reintentar recuento. Introduzca el recuento de reintentos.
4. Haga clic en **Crear** y **cerrar**.



Configurar el reintento de solicitud para el método GET cuando el servidor back-end se restablece en el establecimiento TCP SYN

La configuración de CLI y GUI es similar a los pasos seguidos para el método GET. Para obtener más información, consulte la sección Configurar solicitud de prueba para el método GET. cuando el servidor back-end restablece una sección de conexión.

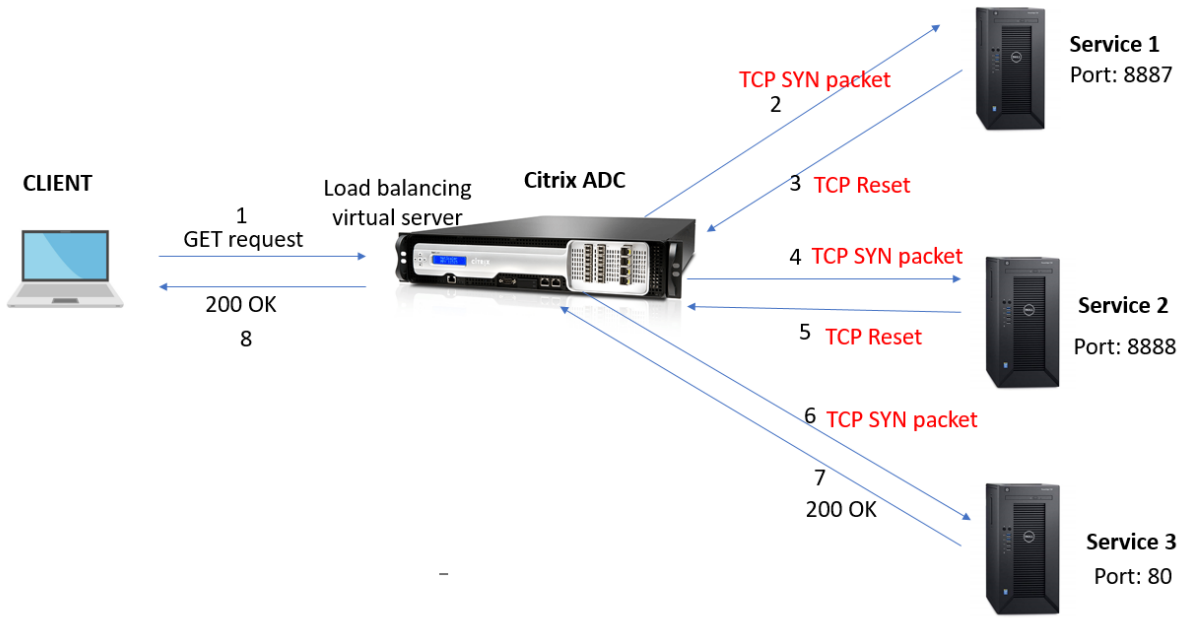
Solicitar reintento si el servidor back-end restablece la conexión TCP durante el establecimiento de la conexión

August 20, 2021

Cuando un servidor back-end restablece una conexión TCP durante el establecimiento de la conexión, la función de reintento de solicitud reenvía la solicitud al siguiente servidor disponible, en lugar de enviar el restablecimiento al cliente. Al realizar el equilibrio de recarga, el cliente guarda RTT cuando el dispositivo inicia la misma solicitud al siguiente servicio disponible.

Cómo funciona el reintento de solicitud cuando el servidor back-end restablece una conexión TCP en el establecimiento SYN

El siguiente diagrama muestra que los componentes interactúan entre sí:



1. El proceso comienza habilitando la función appqoe en el dispositivo.
2. Cuando el cliente envía una solicitud HTTP o HTTPS, el servidor virtual de equilibrio de carga inicia la conexión con el servidor back-end.
3. Si el servicio solicitado no está disponible en el establecimiento TCP SYN, el servidor back-end restablece la conexión TCP.
4. Si la configuración de appqoe tiene habilitado “reintentar” con el número deseado de intentos de reintento especificado, el servidor virtual de equilibrio de carga utiliza el algoritmo de equilibrio de carga configurado para reenviar la solicitud al siguiente servidor de aplicaciones disponible.
5. Después de que el servidor virtual de equilibrio de carga reciba la respuesta, el dispositivo reenvía la respuesta al cliente.
6. Si los servidores back-end disponibles son iguales o inferiores al recuento de reintentos y si todos los servidores envían restablecimiento, el dispositivo responderá a un error de 500 servidores internos. Considere un caso con cinco servidores disponibles y el recuento de reintentos establecido como seis. Si los cinco servidores restablecen la conexión, el dispositivo devuelve un error de servidor interno 500 al cliente.
7. Del mismo modo, si el número de servidores back-end es superior al recuento de reintentos y si los servidores back-end restablecen la conexión en el establecimiento TCP SYN, el dispositivo reenvía el restablecimiento al cliente. Considere un caso con tres servidores back-end y el recuento de reintentos establecido como dos. Si los tres servidores restablecen la conexión, el dispositivo envía un paquete de restablecimiento al cliente.

Configurar reintento de solicitud (método GET y POST) cuando el servidor back-end se restablece en el establecimiento TCP SYN

La configuración de CLI y GUI es similar a los pasos seguidos para el método GET y POST. Para obtener más información, consulte el tema Configurar el reintento de solicitud para el método GET, Configurar el reintento de solicitud para el método POST cuando el servidor back-end restablece una sección de conexión.

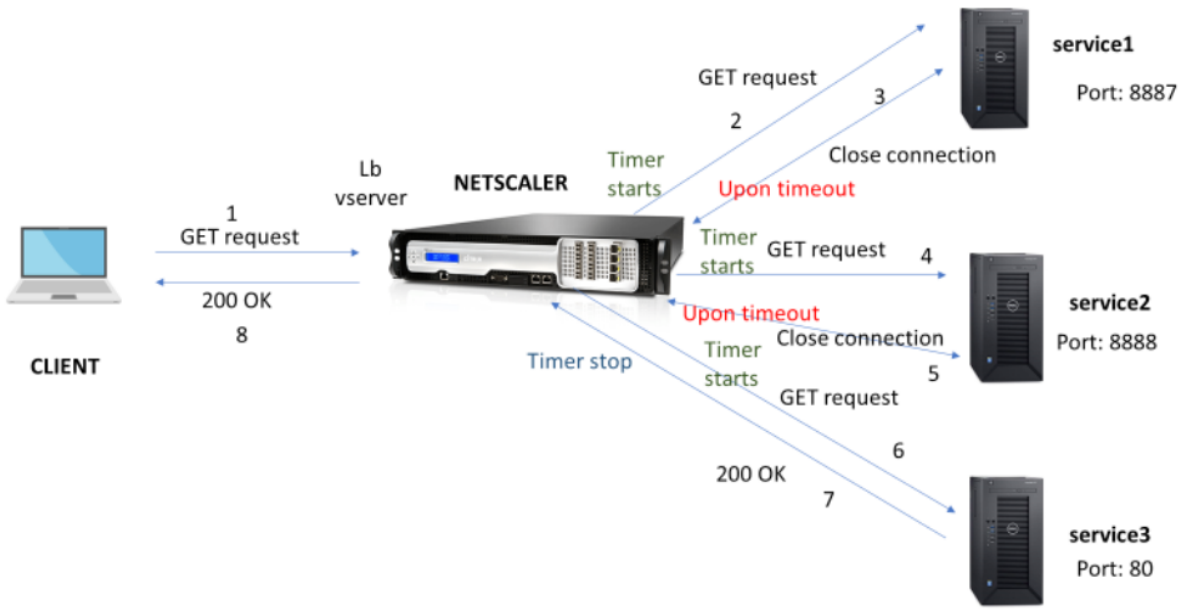
Solicitar reintento si la respuesta del servidor back-end se agota

August 20, 2021

El reintento de solicitud está disponible para otro caso en el que, si un servidor back-end tarda más tiempo en responder a las solicitudes, el dispositivo realiza el equilibrio de recarga al tiempo de espera y reenvía la solicitud al siguiente servidor disponible.

Cómo funciona el reintento de solicitud cuando se agota el tiempo de espera de respuesta del servidor back-end

El siguiente diagrama muestra que los componentes interactúan entre sí:



1. El proceso comienza habilitando la función appqoe en el dispositivo.
2. La configuración appqoe tiene el parámetro “RetryOnTimeout” en milisegundos.

3. Cuando el dispositivo envía una solicitud y si el servidor tarda más tiempo en responder, el dispositivo realiza un equilibrio de recarga basado en el valor de tiempo de espera configurado. El dispositivo restablece la conexión, elige otro servicio y reenvía la solicitud en lugar de esperar la respuesta del servidor.
4. Después de que el servidor virtual de equilibrio de carga reciba la respuesta, el dispositivo reenvía la respuesta al cliente. El uso de un parámetro de tiempo de espera impide que el dispositivo siga esperando la respuesta del servidor, lo que provoca un aumento de RTT.
5. Si los servidores back-end disponibles son iguales o inferiores al recuento de reintentos y si todos los servidores agotan el tiempo de espera para la solicitud, el dispositivo responderá a un error interno de 500 servidores. Considere un caso con cinco servidores disponibles y el recuento de reintentos establecido como seis. Si los cinco servidores agotan el tiempo de espera para la solicitud, el dispositivo devuelve un error de servidor interno 500 al cliente.
6. Del mismo modo, si el número de servidores back-end es superior al recuento de reintentos y si el servidor back-end agota el tiempo de espera tras una solicitud, el dispositivo sigue esperando el último servicio hasta que el servidor envíe una respuesta o se agote el tiempo de espera de la conexión inactiva del cliente. Considere un caso con tres servidores back-end y el recuento de reintentos establecido como dos. Si los tres servidores agotan el tiempo de espera tras la solicitud, el dispositivo sigue esperando al tercer servicio hasta que el servidor envíe una respuesta o el tiempo de espera de la conexión inactiva del cliente.

Configurar el reintento de solicitud (método GET y POST) cuando se agota el tiempo de espera de respuesta del servidor back-end

Para configurar el reintento de solicitud para el método GET en tiempo de espera, debe completar los siguientes pasos.

1. Activar appqoe
2. Configurar la acción appqoe
3. Agregar directiva appqoe
4. Vincular directiva de appqoe al servidor virtual de equilibrio de carga

> **Nota:**
>
> El caso de reintento de solicitud en tiempo de espera también es aplicable para el método POST.

Activar appqoe

En el símbolo del sistema, escriba:

```
enable ns feature appqoe
```


Agregar acción appqoe para el tiempo de espera

Debe configurar la acción appqoe para reintentarlo en el tiempo de espera y definir el número de intentos de reintento.

En el símbolo del sistema, escriba:

```
add appqoe action <name> -retryOnTimeout <msecs> -numRetries <positive_integer
>
```

Ejemplo:

```
add appqoe action appact1 -retryOnTimeout 35 -numRetries 5
```

Agregar directiva appqoe

Para implementar appqoe debe configurar la directiva appqoe para definir cómo poner en cola las conexiones.

En el símbolo del sistema, escriba:

```
add appqoe policy <name> -rule <rule> -action <name>
```

Ejemplo:

```
add appqoe policy timeout_policy -rule http.req.method.eq(get)-action
appact1
```

Vincular la directiva appqoe al servidor virtual de equilibrio de carga

Cuando un servidor back-end tarda mucho tiempo en responder y si quiere que el servidor virtual de equilibrio de carga reenvíe la solicitud al siguiente servicio disponible, debe vincular la directiva appqoe al servidor virtual de equilibrio.

En el símbolo del sistema, escriba:

```
bind lb vserver <name> ((<serviceName> (-policyName <string> [-priority <
positive_integer>] [-gotoPriorityExpression <expression>] [-type ( REQUEST
| RESPONSE )]
```

Ejemplo:

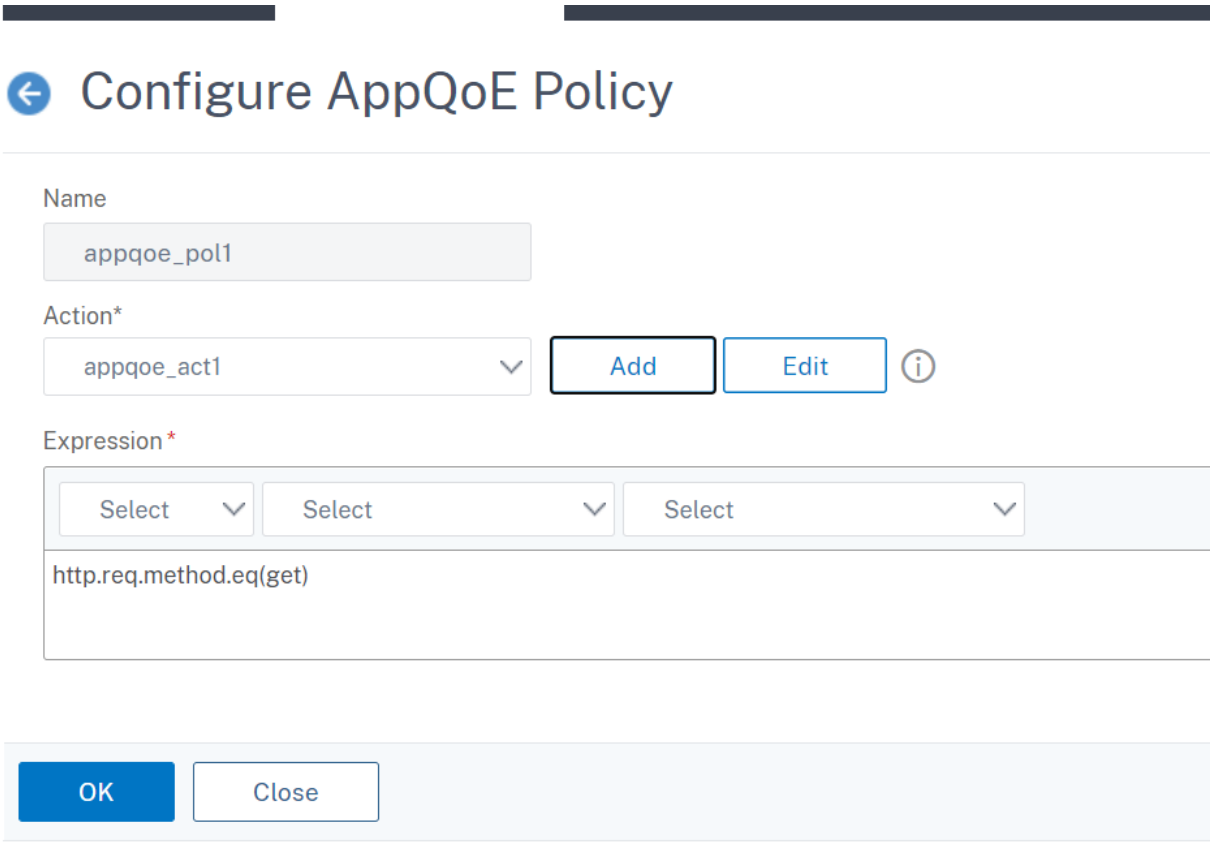
```
bind lb vserver v1 -policyName timeout_policy -type REQUEST -priority 1
```

Configurar la directiva AppQoE para volver a equilibrar la carga en el tiempo de espera mediante la GUI de Citrix ADC

1. Vaya a **AppExpert > AppQoE > Directivas**.

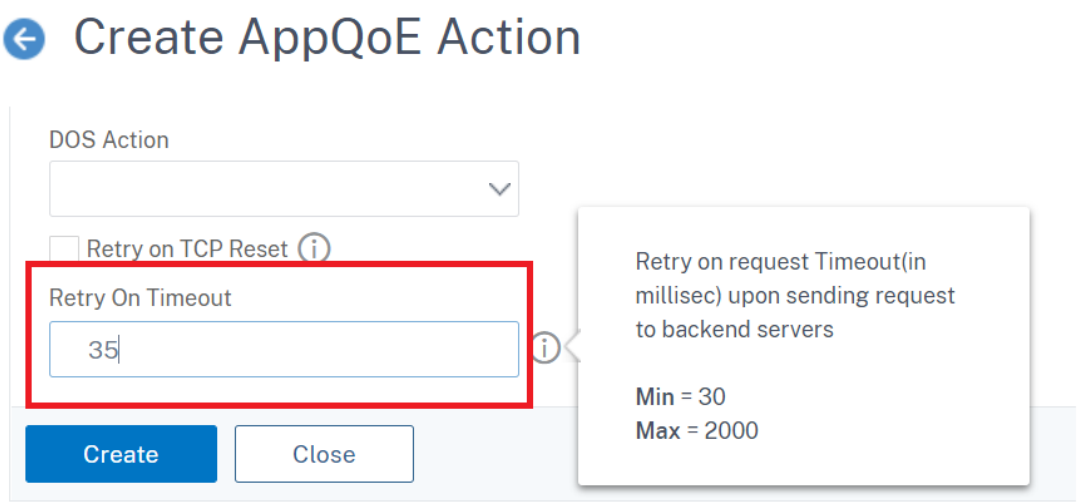
2. En la página **Directivas de AppQoE**, haga clic en **Agregar**.
3. En la página **Crear una directiva de AppQoE**, establezca los siguientes parámetros:

   a. nombre. Nombre de directiva AppQoE
   b. Acción. Agregar o modificar una acción. Para crear una acción nueva, consulte la sección Crear acción de AppQoE.
   c. expresión. Seleccione o introduzca la expresión de directiva “http.req.method.eq(get)”.
4. Haga clic en **Crear** y **cerrar**.



Configurar la acción AppQoE para el reintento de solicitud mediante la GUI de Citrix ADC

1. Vaya a **AppExpert > AppQoE > Acción**.
2. En la página **Acciones de AppQoE**, haga clic en **Agregar**.
3. En la página **Crear acción de AppQoE**, establezca el siguiente parámetro para reintentar en el tiempo de espera de respuesta del servidor back-end:
   a. Vuelva a intentar el tiempo de espera. Reintente el tiempo de espera de solicitud (en miliseg) al enviar la solicitud a los servidores back-end.
4. Haga clic en **Crear** y **cerrar**.



Optimización TCP

August 20, 2021

TCP utiliza las siguientes técnicas de optimización y estrategias de control de congestión (o algoritmos) para evitar la congestión de red en la transmisión de datos.

Estrategias de control de congestión

El TCP se ha utilizado durante mucho tiempo para establecer y administrar conexiones a Internet, manejar errores de transmisión y conectar sin problemas aplicaciones web con dispositivos cliente. Pero el tráfico de red se ha vuelto más difícil de controlar, porque la pérdida de paquetes no depende solo de la congestión en la red, y la congestión no necesariamente causa la pérdida de paquetes. Por lo tanto, para medir la congestión, un algoritmo TCP debe centrarse tanto en la pérdida de paquetes como en el ancho de banda.

Algoritmo de Recuperación de Tasa Proporcional (PRR)

Los mecanismos de recuperación rápida TCP reducen la latencia web causada por pérdidas de paquetes. El nuevo algoritmo de recuperación proporcional de velocidad (PRR) es un algoritmo de recuperación rápida que evalúa los datos TCP durante una recuperación de pérdidas. Se modela después de Rate-Halving, mediante el uso de la fracción que es apropiada para la ventana de destino elegida por el algoritmo de control de congestión. Minimiza el ajuste de la ventana y el tamaño real de la ventana al final de la recuperación está cerca del umbral de inicio lento (ssthresh).

Apertura rápida TCP (TFO)

TCP Fast Open (TFO) es un mecanismo TCP que permite el intercambio de datos rápido y seguro entre un cliente y un servidor durante el protocolo de enlace inicial de TCP. Esta función está disponible como opción TCP en el perfil TCP enlazado a un servidor virtual de un dispositivo Citrix ADC. TFO utiliza una cookie TCP Fast Open (una cookie de seguridad) que genera el dispositivo Citrix ADC para validar y autenticar al cliente que inicia una conexión TFO al servidor virtual. Mediante este mecanismo TFO, puede reducir la latencia de red de una aplicación en el tiempo necesario para un viaje completo de ida y vuelta, lo que reduce significativamente el retraso experimentado en las transferencias TCP cortas.

Cómo funciona el TFO

Cuando un cliente intenta establecer una conexión TFO, incluye una cookie TCP Fast Open con el segmento SYN inicial para autenticarse. Si la autenticación se realiza correctamente, el servidor virtual del dispositivo Citrix ADC puede incluir datos en el segmento SYN-ACK aunque no haya recibido el segmento ACK final del protocolo de enlace de tres vías. Esto ahorra hasta un viaje completo de ida y vuelta en comparación con una conexión TCP normal, que requiere un protocolo de enlace de tres vías antes de que se puedan intercambiar datos.

Un cliente y un servidor back-end realizan los siguientes pasos para establecer una conexión TFO e intercambiar datos de forma segura durante el enlace TCP inicial.

1. Si el cliente no tiene una cookie TCP Fast Open para autenticarse, envía una solicitud Fast Open Cookie en el paquete SYN al servidor virtual del dispositivo Citrix ADC.
2. Si la opción TFO está habilitada en el perfil TCP enlazado al servidor virtual, el dispositivo genera una cookie (cifrando la dirección IP del cliente bajo una clave secreta) y responde al cliente con un SYN-ACK que incluye la cookie de apertura rápida generada en un campo de opción TCP.
3. El cliente almacena en caché la cookie para futuras conexiones TFO al mismo servidor virtual del dispositivo.
4. Cuando el cliente intenta establecer una conexión TFO al mismo servidor virtual, envía SYN que incluye la cookie de apertura rápida en caché (como opción TCP) junto con los datos HTTP.
5. El dispositivo Citrix ADC valida la cookie y, si la autenticación es correcta, el servidor acepta los datos del paquete SYN y reconoce el evento con SYN-ACK, Cookie TFO y respuesta HTTP.

> **Nota:**
>
> Si falla la autenticación del cliente, el servidor quita los datos y reconoce el evento solo con un SYN que indica un tiempo de espera de la sesión.

1. En el lado del servidor, si la opción TFO está habilitada en un perfil TCP enlazado a un servicio, el dispositivo Citrix ADC determina si la cookie de apertura rápida TCP está presente en el servicio al que está intentando conectarse.

2. Si la cookie TCP Fast Open no está presente, el dispositivo envía una solicitud de cookie en el paquete SYN.
3. Cuando el servidor back-end envía la cookie, el dispositivo almacena la cookie en la caché de información del servidor.
4. Si el dispositivo ya tiene una cookie para el par IP de destino dado, reemplaza la cookie antigua por la nueva.
5. Si la cookie está disponible en la caché de información del servidor cuando el servidor virtual intenta volver a conectarse al mismo servidor back-end mediante la misma dirección SNIP, el dispositivo combina los datos del paquete SYN con la cookie y los envía al servidor back-end.
6. El servidor back-end reconoce el evento con datos y un SYN.

Nota: Si el servidor reconoce el evento con solo un segmento SYN, el dispositivo Citrix ADC reenvía inmediatamente el paquete de datos después de quitar el segmento SYN y las opciones TCP del paquete original.

Configuración de TCP fast open

Para utilizar la función TCP Fast Open (TFO), habilite la opción TCP Fast Open en el perfil TCP pertinente y establezca el parámetro TFO Cookie Timeout en un valor que se ajuste al requisito de seguridad para ese perfil.

Habilitar o inhabilitar TFO mediante la CLI

En el símbolo del sistema, escriba uno de los siguientes comandos para habilitar o inhabilitar TFO en un perfil nuevo o existente.

Nota: El valor predeterminado es DISABLED.

```
1     add tcpprofile <TCP Profile Name> - tcpFastOpen ENABLED | DISABLED
2     set tcpprofile <TCP Profile Name> - tcpFastOpen ENABLED | DISABLED
3     unset tcpprofile <TCP Profile Name> - tcpFastOpen
4     Examples
5     add tcpprofile Profile1 - tcpFastOpen
6     Set tcpprofile Profile1 - tcpFastOpen Enabled
7     unset tcpprofile Profile1 - tcpFastOpen
8 <!--NeedCopy-->
```

Para establecer el valor de tiempo de espera de la cookie de apertura rápida TCP mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:


```
    set tcpparam  - tcpfastOpenCookieTimeout <Timeout Value>
    Example
    set tcpprofile  - tcpfastOpenCookieTimeout 30secs
<!--NeedCopy-->
```

Para configurar el TCP Fast Open mediante la interfaz gráfica de usuario

1. Vaya a **Configuración** > **Sistema** > **Perfiles** > y, a continuación, haga clic en **Modificar** para modificar un perfil TCP.
2. En la página **Configurar perfil TCP**, active la casilla de verificación **Abrir rápido de TCP**.
3. Haga clic en **Aceptar** y, a continuación, **Listo**.

Para configurar el valor de tiempo de espera de TCP Fast Cookie mediante la interfaz gráfica de usuario

Vaya a **Configuración** > **Sistema** > **Configuración** > **Cambiar parámetros TCP** y, a continuación, **Configurar parámetros TCP** para establecer el valor de tiempo de espera TCP Fast Open Cookie.

TCP HyStart

Un nuevo parámetro de perfil TCP, HyStart, habilita el algoritmo HyStart, que es un algoritmo de inicio lento que determina dinámicamente un punto seguro en el que terminar (ssthresh). Permite una transición a evitar la congestión sin grandes pérdidas de paquetes. Este nuevo parámetro está inhabilitado de forma predeterminada.

Si se detecta congestión, HyStart entra en una fase de evitación de la congestión. Si lo habilita, obtendrá un mejor rendimiento en redes de alta velocidad con una alta pérdida de paquetes. Este algoritmo ayuda a mantener el ancho de banda cercano al máximo durante el procesamiento de transacciones. Por lo tanto, puede mejorar el rendimiento.

Configuración de TCP HyStart

Para utilizar la función HyStart, habilite la opción Cubic HyStart en el perfil TCP correspondiente.

Para configurar HyStart mediante la interfaz de línea de comandos (CLI)

En el símbolo del sistema, escriba uno de los siguientes comandos para habilitar o inhabilitar HyStart en un perfil TCP nuevo o existente.


```
add tcpprofile <profileName> -hystart ENABLED
set tcpprofile <profileName> -hystart ENABLED
unset tcprofile <profileName> -hystart
<!--NeedCopy-->
```

Ejemplos:

```
    add tcpprofile profile1 -hystart ENABLED
    set tcpprofile profile1 -hystart ENABLED
    unset tcprofile profile1 -hystart
<!--NeedCopy-->
```

Para configurar la compatibilidad con HyStart mediante la interfaz gráfica de usuario

1. Vaya a **Configuración** > **Sistema** > **Perfiles** > y haga clic en **Modificar** para modificar un perfil TCP.
2. En la página **Configurar perfil TCP**, active la casilla de verificación **Hystart cúbico**.
3. Haga clic en **Aceptar** y, a continuación, **Listo**.

Control de velocidad de ráfaga TCP

Se observa que los mecanismos de control TCP pueden conducir a un flujo de tráfico ráfaga en redes móviles de alta velocidad con un impacto negativo en la eficiencia general de la red. Debido a condiciones de la red móvil, como la congestión o la retransmisión de datos de capa 2, los acuse de recibo de TCP llegan agrupados al remitente y desencadenan una ráfaga de transmisión. Estos grupos de paquetes consecutivos enviados con una brecha corta entre paquetes se llama ráfaga de paquetes TCP. Para superar la ráfaga de tráfico, el dispositivo Citrix ADC utiliza una técnica TCP Burst Rate Control. Esta técnica distribuye de manera uniforme los datos en la red durante todo un tiempo de ida y vuelta para que los datos no se envíen a una ráfaga. Mediante esta técnica de control de velocidad de ráfaga, puede lograr un mejor rendimiento y menores tasas de caída de paquetes.

Cómo funciona el control de velocidad de ráfaga TCP

En un dispositivo Citrix ADC, esta técnica distribuye uniformemente la transmisión de un paquete a lo largo de toda la duración del tiempo de ida y vuelta (RTT). Esto se logra mediante una pila TCP y un programador de paquetes de red que identifica las diversas condiciones de red para generar paquetes para sesiones TCP en curso con el fin de reducir las ráfagas.

En el remitente, en lugar de transmitir paquetes inmediatamente después de recibir un acuse de recibo, el remitente puede retrasar la transmisión de paquetes para distribuirlos a la velocidad definida por el programador (Configuración dinámica) o por el perfil TCP (Configuración fija).

Configuración del control de velocidad de ráfaga TCP

Para utilizar la opción Control de velocidad de ráfaga TCP en el perfil TCP correspondiente y establecer los parámetros de control de velocidad de ráfaga.

Para establecer el control de velocidad de ráfaga TCP mediante la línea de comandos

En el símbolo del sistema, establezca uno de los siguientes comandos TCP Burst Rate Control se configuran en un perfil nuevo o existente.

Nota: El valor predeterminado es DESHABILITADO.

```
1 add tcpprofile <TCP Profile Name> -burstRateControl Disabled | Dynamic
     | Fixed
2
3 set tcpprofile <TCP Profile Name> -burstRateControl Disabled | Dynamic
     | Fixed
4
5 unset tcpprofile <TCP Profile Name> -burstRateControl Disabled |
     Dynamic | Fixed
6 <!--NeedCopy-->
```

Donde:

Desactivado: Si el control Burst rate está inhabilitado, un dispositivo Citrix ADC no realiza la administración de ráfagas excepto la configuración MaxBurst.

Corregido: Si el control de velocidad de ráfaga de TCP era Fijo, el dispositivo utiliza el valor de velocidad de envío de carga de conexión TCP mencionado en el perfil TCP.

Dinámico: Si el control de velocidad de ráfaga es “dinámico”, la conexión se está regulando en función de varias condiciones de red para reducir las ráfagas TCP. Este modo solo funciona cuando la conexión TCP está en modo ENDPOINT. Cuando el control Velocidad de ráfaga dinámica está habilitado, el parámetro MaxBurst del perfil TCP no está en vigor.

```
1 add tcpProfile  profile1 -burstRateControl Disabled
2
3 set tcpProfile profile1 -burstRateControl Dynamic
4
5 unset tcpProfile profile1 -burstRateControl Fixed
6 <!--NeedCopy-->
```


Para establecer los parámetros de control de velocidad de ráfaga TCP mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
set ns tcpprofile nstcp_default_profile -burstRateControl <type of burst rate control> -tcprate <TCP rate> -rateqmax <maximum bytes in queue>

T1300-10-2> show ns tcpprofile nstcp_default_profile
        Name: nstcp_default_profile
        Window Scaling status:  ENABLED
        Window Scaling factor: 8
        SACK status: ENABLED
        MSS: 1460
        MaxBurst setting: 30 MSS
        Initial cwnd setting: 16 MSS
        TCP Delayed-ACK Timer: 100 millisec
        Nagle's Algorithm: DISABLED
        Maximum out-of-order packets to queue: 15000
        Immediate ACK on PUSH packet: ENABLED
        Maximum packets per MSS: 0
        Maximum packets per retransmission: 1
        TCP minimum RTO in millisec: 1000
        TCP Slow start increment: 1
        TCP Buffer Size: 8000000 bytes
        TCP Send Buffer Size: 8000000 bytes
        TCP Syncookie: ENABLED
        Update Last activity on KA Probes: ENABLED
        TCP flavor: BIC
        TCP Dynamic Receive Buffering: DISABLED
        Keep-alive probes: ENABLED
        Connection idle time before starting keep-alive probes: 900 seconds
        Keep-alive probe interval: 75 seconds
        Maximum keep-alive probes to be missed before dropping connection: 3
        Establishing Client Connection: AUTOMATIC
        TCP Segmentation Offload: AUTOMATIC
        TCP Timestamp Option: DISABLED
        RST window attenuation (spoof protection): ENABLED
        Accept RST with last acknowledged sequence number: ENABLED
        SYN spoof protection: ENABLED
        TCP Explicit Congestion Notification: DISABLED
```



```
36                Multipath TCP: DISABLED
37                Multipath TCP drop data on pre-established subflow:
                      DISABLED
38                Multipath TCP fastopen: DISABLED
39                Multipath TCP session timeout: 0 seconds
40                DSACK: ENABLED
41                ACK Aggregation: DISABLED
42                FRTO: ENABLED
43                TCP Max CWND : 4000000 bytes
44                FACK: ENABLED
45                TCP Optimization mode: ENDPOINT
46                TCP Fastopen: DISABLED
47                HYSTART: DISABLED
48                TCP dupack threshold: 3
49                Burst Rate Control: Dynamic
50                TCP Rate: 0
51                TCP Rate Maximum Queue: 0
52  <!--NeedCopy-->
```

Para configurar el control de velocidad de ráfaga TCP mediante la interfaz gráfica de usuario

1. Vaya a **Configuración** > **Sistema** > **Perfiles** > y, a continuación, haga clic en **Modificar** para modificar un perfil TCP.
2. En la página **Configurar perfil TCP**, seleccione la opción **Control de ráfagas TCP** en la lista desplegable:
   a) Burstratecntrl
   b) Créditopor Teprms
   c) Tarifas por Teperms
   d) Tarifas de ChedulerQ
3. Haga clic en **Aceptar** y, a continuación, **Listo**.

Protección contra el algoritmo de secuencia envuelta (PAWS)

Si habilita la opción de marca de hora TCP en el perfil TCP predeterminado, el dispositivo Citrix ADC utiliza el algoritmo Protección contra Secuencia Envuelta (PAWS) para identificar y rechazar paquetes antiguos cuyos números de secuencia se encuentran dentro de la ventana de recepción de la conexión TCP actual porque la secuencia ha “envuelta” (alcanzó su valor máximo y se reinició desde 0).

Si la congestión de la red retrasa un paquete de datos no SYN y abre una nueva conexión antes de que llegue el paquete, el ajuste de número de secuencia podría provocar que la nueva conexión acepte el paquete como válido, lo que provocará daños en los datos. Pero si la opción de marca de tiempo TCP está habilitada, el paquete se descarta.

De forma predeterminada, la opción de marca de tiempo TCP está inhabilitada. Si lo habilita, el dispositivo compara la marca de tiempo TCP (seg.tsval) en el encabezado de un paquete con el valor de marca de tiempo reciente (ts.Recent). Si seg.tsval es igual o mayor que ts.Recent, el paquete se procesa. De lo contrario, el dispositivo elimina el paquete y envía un acuse de recibo correctivo.

Cómo funciona el PAWS

El algoritmo PAWS procesa todos los paquetes TCP entrantes de una conexión sincronizada de la siguiente manera:

1. Si `SEG.TSval` < `Ts.recent`: El paquete entrante no es aceptable. PAWS envía un acuse de recibo (como se especifica en RFC-793) y elimina el paquete. Nota: El envío de un segmento ACK es necesario para retener los mecanismos de TCP para detectar y recuperar de conexiones semiabiertas.
2. Si el paquete está fuera de la ventana: PAWS rechaza el paquete, como en el procesamiento TCP normal.
3. Si `SEG.TSval` > `Ts.recent`: `PAWS` acepta el paquete y lo procesa.
4. Si `SEG.TSval` <= `Last.ACK.sent`(segmento que llega satisface): PAWS debe copiar `SEG.TSval` el valor en `Ts.recent` (se copia en Ts. Campo reciente en el db?.
5. Si el paquete está en secuencia: PAWS acepta el paquete.
6. Si el paquete no está en secuencia: El paquete se trata como un segmento TCP normal dentro de ventana y fuera de secuencia. Por ejemplo, podría estar en cola para una entrega posterior.
7. Si el `Ts.recent` valor está inactivo durante más de 24 días: la validez de `Ts.recent` se comprueba si falla la comprobación de marca de tiempo de PAWS. Si se encuentra que el valor TS.Recent no es válido, se acepta el segmento y `PAWS rule` actualiza el `Ts.recent` con el valor TSVal del nuevo segmento.

Para habilitar o inhabilitar la marca de tiempo TCP mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
`set nstcpprofile nstcp_default_profile -TimeStamp (ENABLED | DISABLED)
    `
```

Para habilitar o inhabilitar la marca de tiempo TCP mediante la interfaz gráfica de usuario

Desplácese hasta **Sistema** > **Perfil** > **Perfil TCP**, seleccione el perfil TCP predeterminado, haga clic en **Modificar** y active o desactive la casilla de verificación **Marca de tiempo TCP**.

Técnicas de optimización

TCP utiliza las siguientes técnicas y métodos de optimización para controles de flujo optimizados.

Selección de perfil TCP basada en directivas

Hoy en día, el tráfico de red es más diverso y requiere mucho ancho de banda que nunca. Con el aumento del tráfico, el efecto que la calidad de servicio (QoS) tiene en el rendimiento TCP es significativo. Para mejorar la calidad de servicio, ahora puede configurar directivas de AppQoE con diferentes perfiles TCP para diferentes clases de tráfico de red. La directiva AppQoE clasifica el tráfico de un servidor virtual para asociar un perfil TCP optimizado para un tipo concreto de tráfico, como 3G, 4G, LAN o WAN.

Para utilizar esta función, cree una acción de directiva para cada perfil TCP, asocie una acción con directivas AppQoE y vincule las directivas a los servidores virtuales de equilibrio de carga.

Para obtener información sobre el uso de atributos de suscriptor para realizar la optimización TCP, consulte Perfil TCP basado en directivas.

Configuración de la selección de perfiles TCP basada en directivas

La configuración de la selección de perfiles TCP basada en directivas consta de las siguientes tareas:

- Activando AppQoE. Antes de configurar la función de perfil TCP, debe habilitar la función AppQoE.
- Agregar acción AppQoE. Después de habilitar la función AppQoE, configure una acción AppQoE con un perfil TCP.
- Configuración de la selección de perfiles TCP basada en AppQoE. Para implementar la selección de perfiles TCP para diferentes clases de tráfico, debe configurar directivas de AppQoE con las que Citrix ADC pueda distinguir las conexiones y vincular la acción de AppQoE correcta a cada directiva.
- Vinculación de la directiva AppQoE con el servidor virtual. Una vez que haya configurado las directivas de AppQoE, debe vincularlas a uno o más servidores virtuales de equilibrio de carga, conmutación de contenido o redirección de caché.

Configurar mediante la interfaz de línea de comandos

Para habilitar AppQoE mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba los siguientes comandos para habilitar la función y compruebe que está habilitada:

- `enable ns feature appqoe`
- `show ns feature`

Para enlazar un perfil TCP al crear una acción AppQoE mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba el siguiente comando de acción AppQoE con la `tcpprofiletobind` opción.

```
add appqoe action <name> [-priority <priority>] [-respondWith ( ACS | NS )
[<CustomFile>] [-altContentSvcName <string>] [-altContentPath <string>] [-
maxConn <positive_integer>] [-delay <usecs>]] [-polqDepth <positive_integer
>] [-priqDepth <positive_integer>] [-dosTrigExpression <expression>] [-
dosAction ( SimpleResponse |HICResponse )] [-tcpprofiletobind <string>]
show appqoe action
```

Para configurar una directiva AppQoE mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
add appqoe policy <name> -rule <expression> -action <string>
```

Para vincular una directiva de AppQoE al equilibrio de carga, la redirección de caché o la conmutación de contenido de servidores virtuales mediante la interfaz de línea de comandos

En el símbolo del sistema, escriba:

```
bind cs vserver cs1 -policyName <appqoe_policy_name> -priority <priority>
bind lb vserver <name> - policyName <appqoe_policy_name> -priority <priority
>
bind cr vserver <name> -policyName <appqoe_policy_name> -priority <priority
>
```

Ejemplo

```
1    add ns tcpProfile tcp1 -WS ENABLED -SACK ENABLED -WSVal 8 -nagle
        ENABLED -maxBurst 30 -initialCwnd 16 -oooQSize 15000 -minRTO 500
         -slowStartIncr 1 -bufferSize 4194304 -flavor BIC -KA ENABLED -
        sendBuffsize 4194304 -rstWindowAttenuate ENABLED -spoofSynDrop
        ENABLED -dsack enabled -frto ENABLED -maxcwnd 4000000 -fack
        ENABLED -tcpmode ENDPOINT
2    add appqoe action appact1 -priority HIGH -tcpprofile tcp1
3    add appqoe policy apppol1 -rule "client.ip.src.eq(10.102.71.31)" -
        action appact1
```



```
4     bind lb vserver lb2 -policyName apppol1 -priority 1 -
         gotoPriorityExpression END -type REQUEST
5     bind cs vserver cs1 -policyName apppol1 -priority 1 -
         gotoPriorityExpression END -type REQUEST
6  <!--NeedCopy-->
```

Configuración de perfiles TCP basados en directivas mediante la interfaz gráfica de usuario

Para habilitar AppQoE mediante la interfaz gráfica de usuario

1. Vaya a **Sistema** > **Configuración**.
2. En el panel de detalles, haga clic en **Configurar funciones avanzadas**.
3. En el cuadro de diálogo **Configurar funciones avanzadas**, active la casilla de verificación **AppQoE**.
4. Haga clic en **Aceptar**.

Para configurar la directiva AppQoE mediante la interfaz gráfica de usuario

1. Vaya a **App-Expert** > **AppQoE** > **Acciones**.
2. En el panel de detalles, realice una de las acciones siguientes:
3. Para crear una nueva acción, haga clic en **Agregar**.
4. Para modificar una acción existente, selecciónela y, a continuación, haga clic en **Modificar**.
5. En la pantalla **Crear acción AppQoE** o **Configurar acción AppQoE**, escriba o seleccione valores para los parámetros. El contenido del cuadro de diálogo corresponde a los parámetros descritos en “Parámetros para configurar la acción AppQoE” de la siguiente manera (asterisco indica un parámetro obligatorio):
   a) Nombre: Name
   b) Tipo de acción: RespondWith
   c) Prioridad: Priority
   d) Profundidad de cola de directivas: PolqDepth
   e) Profundidad de la cola: PriqDepth
   f) Acción de DOS: DosAction
6. Haga clic en **Crear**.

Para enlazar la directiva de AppQoE mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales**, seleccione un servidor y, a continuación, haga clic en **Modificar**.
2. En la sección **Directivas** y haga clic en (+) para enlazar una directiva de AppQoE.
3. En el control deslizante **Directivas**, haga lo siguiente:

a) Seleccione un tipo de directiva como AppQoE en la lista desplegable.
b) Seleccione un tipo de tráfico en la lista desplegable.

4. En la sección **Enlace de directivas**, haga lo siguiente:
   a) Haga clic en **Nuevo** para crear una nueva directiva de AppQoE.
   b) Haga clic en **Directiva existente** para seleccionar una directiva de AppQoE en la lista desplegable.
5. Establezca la prioridad de enlace y haga clic en **Vincular** a la directiva al servidor virtual.
6. Haga clic en **Done**.

Generación de bloques SACK

El rendimiento TCP se ralentiza cuando se pierden varios paquetes en una ventana de datos. En tal caso, un mecanismo de reconocimiento selectivo (SACK) combinado con una directiva de retransmisión selectiva de repeticiones supera esta limitación. Para cada paquete entrante fuera de pedido, debe generar un bloque SACK.

Si el paquete fuera de pedido encaja en el bloque de cola de reensamblaje, inserte la información del paquete en el bloque y establezca la información del bloque completa como SACK-0. Si un paquete fuera de orden no cabe en el bloque de reensamblaje, envíelo como SACK-0 y repita los bloques SACK anteriores. Si un paquete fuera de orden es un duplicado y la información del paquete se establece como SACK-0, entonces D-SACK el bloque.

Nota: Un paquete se considera como D-SACK si es un paquete reconocido, o un paquete fuera de servicio que ya se ha recibido.

Incumplimiento del cliente

Un dispositivo Citrix ADC puede manejar el renegamiento del cliente durante la recuperación basada en SACK.

Las comprobaciones de memoria para marcar end_point en la PCB no están considerando el total de la memoria disponible

En un dispositivo Citrix ADC, si el umbral de uso de memoria se establece en el 75% en lugar de utilizar la memoria total disponible, las nuevas conexiones TCP evitan la optimización TCP.

Retransmisiones innecesarias debido a la falta de bloques SACK

En un modo que no sea endpoint, cuando envía DUPACKS, si faltan bloques SACK para algunos paquetes fuera de orden, desencadena más retransmisiones desde el servidor.

SNMP para la optimización de conexiones omitidas debido a sobrecarga

Se han agregado los siguientes identificadores SNMP a un dispositivo Citrix ADC para realizar un seguimiento del número de conexiones omitidas optimizaciones TCP debido a una sobrecarga.

1. 1.3.6.1.4.1.5951.4.1.1.46.131 (TCPOptimizationEnabled). Para realizar un seguimiento del número total de conexiones habilitadas con la optimización TCP.
2. 1.3.6.1.4.1.5951.4.1.1.46.132 (tcpOptimizationBypassed). Para realizar un seguimiento del número total de conexiones que se omite TCP Optimization.

Buffer de recepción dinámica

Para maximizar el rendimiento TCP, un dispositivo Citrix ADC ahora puede ajustar dinámicamente el tamaño del búfer de recepción TCP.

Algoritmo de sonda de pérdida de cola

Un tiempo de espera de retransmisión (RTO) es una pérdida de segmentos en el extremo final de una transacción. Se produce un RTO si hay problemas de latencia de aplicaciones, especialmente en transacciones web cortas. Para recuperar la pérdida de segmentos al final de una transacción, TCP utiliza el algoritmo Tail Loss Probe (TLP).
TLP es un algoritmo de solo remitente. Si una conexión TCP no recibe ningún acuse de recibo durante un período determinado, TLP transmite el último paquete no reconocido (sonda de pérdida). En el caso de una pérdida de cola en la transmisión original, el reconocimiento de la sonda de pérdida desencadena una recuperación SACK o FACK.

Configuración de la sonda de pérdida de cola

Para utilizar el algoritmo Tail Loss Probe (TLP), debe habilitar la opción TLP en el perfil TCP y establecer el parámetro en un valor que se ajuste al requisito de seguridad para ese perfil.

Habilitar TLP mediante la línea de comandos

En el símbolo del sistema, escriba uno de los siguientes comandos para habilitar o inhabilitar TLP en un perfil nuevo o existente.

> **Nota**:
>
> El valor predeterminado es DISABLED.

```
add tcpprofile <TCP Profile Name> - taillossprobe ENABLED | DISABLED

set tcpprofile <TCP Profile Name> - taillossprobe ENABLED | DISABLED
```



```
unset tcpprofile <TCP Profile Name> - taillossprobe
```

Ejemplos:

```
add tcpprofile nstcp_default_profile - taillossprobe

set tcpprofile nstcp_default_profile -taillossprobe Enabled

unset tcpprofile nstcp_default_profile -taillossprobe
```

Configurar el algoritmo de sonda de pérdida de cola mediante la GUI de Citrix ADC

1. Vaya a **Configuración** > **Sistema** > **Perfiles** > y, a continuación, haga clic en **Modificar** para modificar un perfil TCP.
2. En la página **Configurar perfil TCP**, active la casilla de verificación **Sonda de pérdida de cola**.
3. Haga clic en **Aceptar** y, a continuación, **Listo**.

Soluciones de solución de problemas para Citrix ADC

January 12, 2021

En este tema se ofrecen algunas soluciones básicas de solución de problemas necesarias para resolver los problemas que se producen en el dispositivo. Le proporciona una comprensión del dispositivo NetScaler, cómo se integra con la red y qué problemas puede esperar en las funciones básicas del sistema.

Cómo registrar un seguimiento de paquetes en Citrix ADC

June 22, 2022

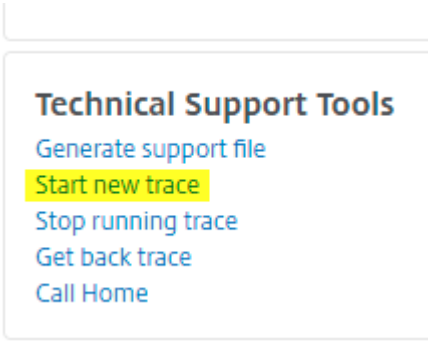
Este artículo de solución de problemas explica cómo un administrador puede registrar un seguimiento de paquetes de red mediante la GUI de Citrix ADC.

Puntos que tener en cuenta

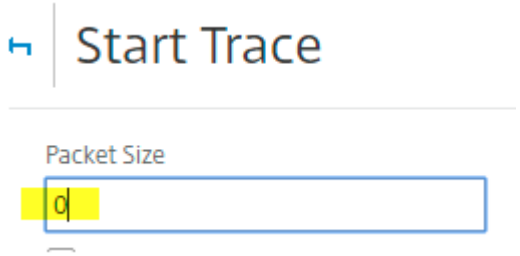
- Citrix recomienda utilizar la versión reciente de Wireshark de la "sección de compilación automatizada" disponible en la siguiente página web: http://www.wireshark.org/download/automated.
- En Citrix ADC versión 11.1 o posterior, para descifrar la captura y garantizar que los parámetros ECC (criptografía de curva elíptica), reutilización de sesiones y DH estén inhabilitados en el servidor virtual. Debe hacerlo antes de capturar un rastro.

Registrar el seguimiento de paquetes en NetScaler versión 11.1

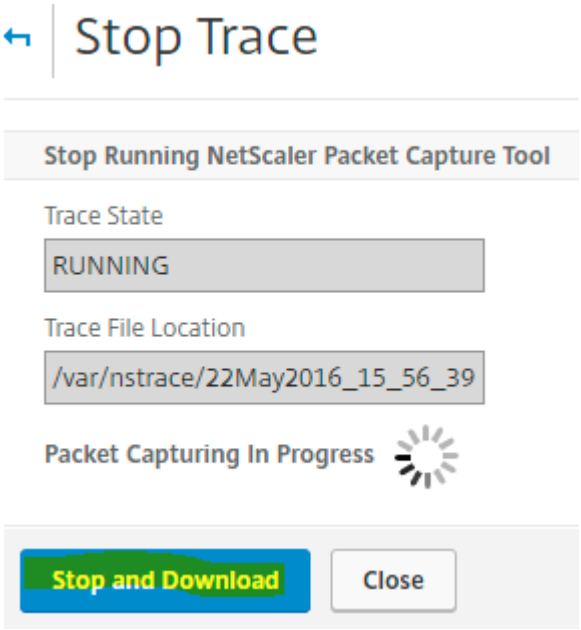
1. Vaya a la página **Sistema** > **Diagnóstico**.
2. haga clic en el enlace **Iniciar nuevo seguimiento** en la página **Diagnóstico**, como se muestra en la siguiente captura de pantalla.



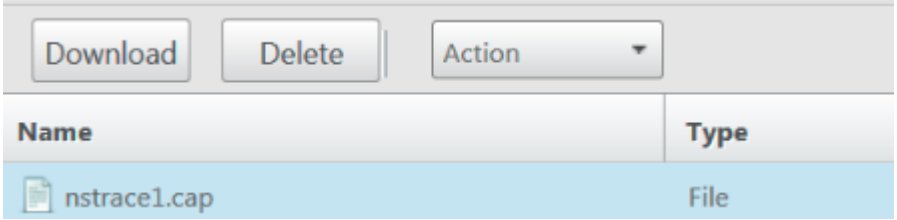
3. Actualice el tamaño del paquete a 0 en el campo **Tamaño del paquete**.



4. Haga clic en **Iniciar** para comenzar a registrar el seguimiento de paquetes de red.
5. Haga clic en **Detener y descargar** para detener el registro del seguimiento de paquetes de red una vez finalizada la prueba.

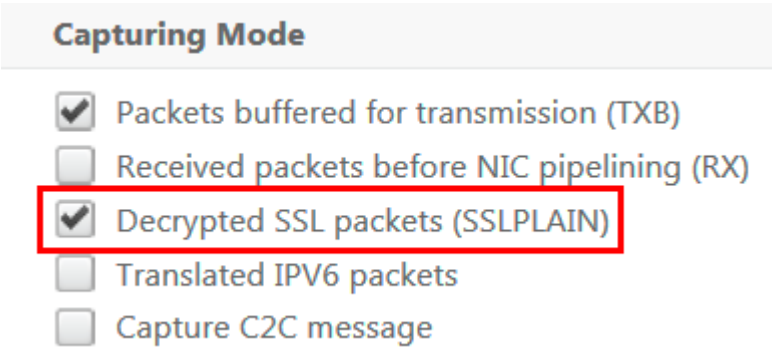


6. Seleccione el archivo deseado y haga clic en **Seleccionar** y, a continuación, en **Descargar**.



7. Abra el archivo de seguimiento de paquetes de red con la utilidad Wireshark para mostrar el contenido del archivo.

> **Nota**: Seleccione Paquetes SSL descifrados (SSLPLAIN) para descifrar el seguimiento del paquete sin la clave privada.



Capturar claves maestras SSL

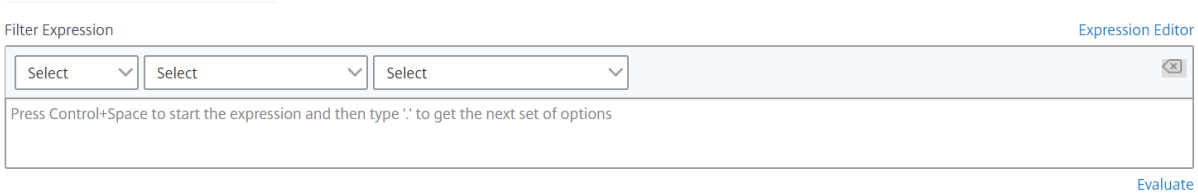
En las versiones 11.0, 11.1 y superiores, hay una opción para capturar las claves de sesión que es válida solo para esa sesión/nstrace en particular y esta opción se puede usar si no desea compartir la clave privada o usar el modo SSLPLAIN. Para obtener más información, consulte https://support.citrix.com/article/CTX135889.

Exportar claves de sesión sin compartir clave privada

En la mayoría de los casos, la clave privada no está disponible ni se comparte. En estos casos, podemos sugerir exportar las claves de **sesión SSL** en lugar de la clave privada. Consulte [Cómo exportar y utilizar claves de sesión SSL para descifrar rastros SSL sin compartir la clave privada SSL, consulte https://support.citrix.com/article/CTX135889.

Filtros

Además, siempre se recomienda agregar filtros basados en IP mientras se toman rastros. El proceso garantiza que solo capture el tráfico interesado, lo que facilita la solución de problemas. La adición de filtros también reduce la carga en el dispositivo mientras se realizan los seguimientos.



Los filtros simples basados en IP son suficientes para obtener las capturas correctas. Para obtener más información sobre filtros `nstrace` y ejemplos, consulte la página Documentación de Citrix.

Caso de uso para capturar un seguimiento de paquetes con filtro IP del servidor virtual (tanto front-end como back-end)

Mediante un filtro de la dirección IP del servidor virtual y la habilitación de la opción "—link" en la CLI o la selección de la opción "Rastrear tráfico de pares de conexión filtrada" en la GUI (disponible 10.1 y superior), puede capturar tanto el tráfico de front-end como el de back-end para la dirección IP.

```
1 start nstrace -size 0 -filter "CONNECTION.IP.EQ(1.1.1.1)" -link ENABLED
2
3 show nstrace
4         State:  RUNNING          Scope:  LOCAL            TraceLocation
              :  "/var/nstrace/24Mar2017_16_00_19/..." Nf:  24
                              Time:  3600              Size:  0
                            Mode:  TXB NEW_RX
5         Traceformat:  NSCAP      PerNIC:  DISABLED        FileName:  24
              Mar2017_16_00_19 Filter:  "CONNECTION.IP.EQ(1.1.1.1)" Link:
               ENABLED           Merge:  ONSTOP           Doruntimecleanup
              :  ENABLED
6         TraceBuffers:  5000      SkipRPC:  DISABLED       Capsslkeys:
              DISABLED    InMemoryTrace:  DISABLED
7 <!--NeedCopy-->
```

Captura de rastros cíclicos

Siempre es un desafío solucionar un problema intermitente. El seguimiento cíclico es el más adecuado para los problemas que son intermitentes. Los rastros se pueden ejecutar en un lapso de pocas

horas o días antes de que se produzca el problema. Además, puede usar un filtro específico y evaluar el tamaño de los archivos de seguimiento que se generan antes de ejecutarlo durante más tiempo.

Ejecute el siguiente comando desde la CLI:

```
start nstrace -nf 60 -time 30 -size 0
This particular trace will create 60 files each of them for 30 sec.
   This means the files will start getting overwritten after 60 trace
   files or 30 mins
Show nstrace à To check the status of the nstrace
Stop nstrace à To stop the nstrace.

<!--NeedCopy-->
```

Prácticas recomendadas

En una unidad que maneja GB de tráfico por segundo, la captura de tráfico es un proceso que requiere muchos recursos. El impacto en los recursos se debe principalmente a la CPU y al espacio en disco. El impacto del espacio en disco se puede reducir mediante el uso de expresiones de filtrado. Sin embargo, el impacto en la CPU se mantiene y, a veces, provoca un ligero aumento, ya que el dispositivo ahora necesita procesar los paquetes de acuerdo con el filtro antes de capturarlos.

La práctica recomendada para el rastreo es:

1. La duración durante la cual se ejecuta el seguimiento debe ser lo más limitada posible cuando se asegure de que se capturan los paquetes de interés.
2. Programe la actividad de rastreo para que se produzca en un momento en el que el número de usuarios (y, por lo tanto, el tráfico) se reduzca considerablemente, por ejemplo, fuera del horario laboral.

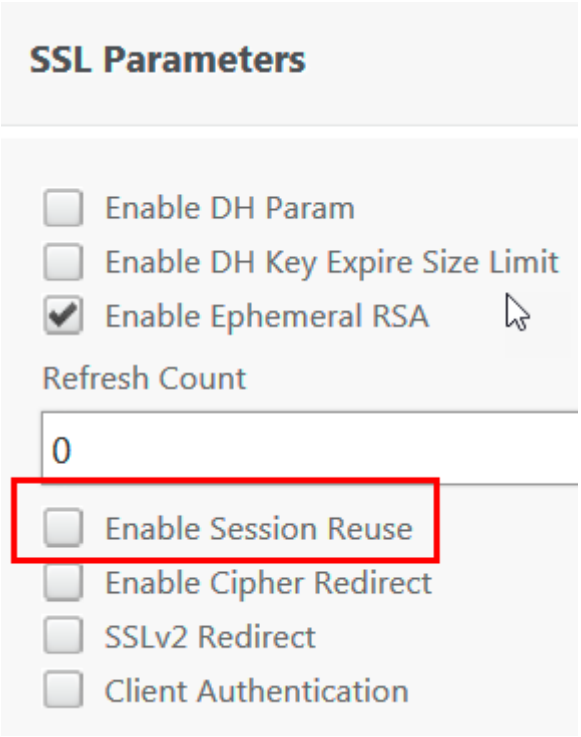
Más recursos

Inhabilitar la reutilización de sesiones en el servidor virtual desde la interfaz

La reutilización de sesiones se inhabilita cuando se captura un seguimiento para completar un protocolo de enlace SSL en el seguimiento. Cuando está habilitada, puede capturar un apretón de manos parcial en el seguimiento. Asegúrese de habilitar la opción después de la recopilación de trazas.
No inhabilites la reutilización de una sesión SSL cuando el método de persistencia es sslsession, ya que interrumpe la persistencia de las conexiones existentes. Para obtener más información, consulte https://support.citrix.com/article/CTX121925.

1. Abra el servidor virtual y vaya a Parámetros de SSL.

2. Desactive Activar reutilización de sesiones si está habilitada



Inhabilitar la reutilización de sesiones en el servidor virtual desde la CL

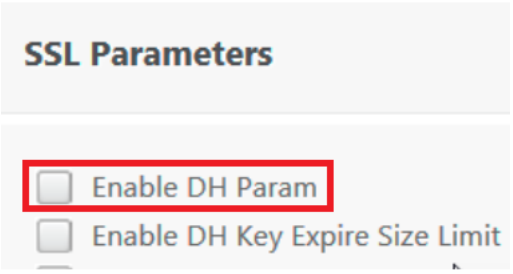
1. SSH a la consola del dispositivo.
2. Ejecute el siguiente comando para inhabilitar DH Param del servidor virtual:

```
set ssl vserver "vServer_Name"-sessReuse DISABLED
```

Inhabilitar el parámetro DH en el servidor virtual desde la GUI

Consulte https://support.citrix.com/article/CTX213335 Para comprender el parámetro DH.

1. Abra el servidor virtual y vaya a Parámetros de SSL.
2. Desactive DH Param si está habilitado.



Inhabilitar el parámetro DH en el servidor virtual desde la CLI

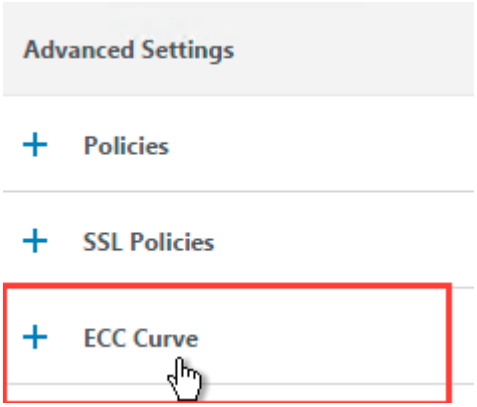
1. SSH a la consola del dispositivo.
2. Ejecute el siguiente comando para inhabilitar DH Param del servidor virtual:

```
set ssl vserver "vServer_Name"-dh DISABLED
```

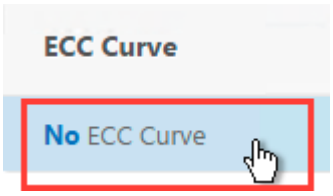
Inhabilitar la curva ECC en el servidor virtual desde la GUI

La curva ECC está inhabilitada para descifrar el seguimiento SSL capturado con clave privada. No debe inhabilitar las claves si se utilizan los cifrados SSL relacionados. Para obtener más información sobre la curva ECC, consulte https://support.citrix.com/article/CTX205289

1. Abra el servidor virtual y vaya a ECC Curve.



2. Si no hay ninguna curva de ECC enlazada al servidor virtual, no se requiere ninguna otra acción.



3. Si alguna curva ECC está enlazada al servidor virtual, haga clic en la curva ECC y desvincúlela del servidor virtual.

Inhabilitar la curva ECC en el servidor virtual desde la CLI

1. SSH a la consola del dispositivo.
2. Ejecute el siguiente comando para cada curva de ECC enlazada al servidor virtual:

```
unbind ssl vserver "vServer_Name"-eccCurveName "ECC_Curve_Name"
```


Cómo liberar espacio en el directorio VAR para problemas de registro con un dispositivo Citrix ADC

September 8, 2021

En el artículo siguiente se explica cómo un administrador puede liberar espacio del `/var` directorio de un dispositivo Citrix ADC. Puede seguir los pasos cuando no se puede acceder a la GUI de Citrix.

Cuando la cantidad de espacio en disco es baja en el directorio /var del dispositivo, es posible que no pueda iniciar sesión en la GUI de Citrix. En este caso, puede eliminar los archivos de registro antiguos para crear espacio libre en el directorio /var.

Puntos que tener en cuenta

- Asegúrese de realizar una copia de seguridad de los archivos antes de quitarlos del dispositivo.

Para liberar espacio en el `/var` directorio de un dispositivo Citrix ADC, realice el siguiente procedimiento:

1. Inicie sesión en la CLI de Citrix ADC mediante SSH. Para obtener más información para completar esta tarea, consulte la documentación de Citrix ADC.
2. Después de iniciar sesión en la CLI de Citrix ADC, cambie al símbolo del shell mediante el siguiente comando. `shell`
3. Ejecute el siguiente comando para ver la disponibilidad de espacio en el dispositivo Citrix ADC.
   `df -h`
4. Si la capacidad de memoria del `/var` directorio se llena hasta un 90 por ciento, debe eliminar algunos archivos de este directorio.
   - Ejecute los siguientes comandos para ver el contenido del directorio /var:
     ```
     cd /var
     ls -l
     ```

   Los directorios que suelen ser de interés son los siguientes:

```
1 /var/nstrace - This directory contains trace files.This is the
      most common reason for HDD being filled on the Citrix ADC
      appliance. This is due to an nstrace being left running for
      indefinite amount of time. All traces that are not of interest
      can and should be deleted. To stop an nstrace, go back to the
      CLI and issue stop nstrace command.
2
```



```
/var/log - This directory contains system specific log files.

/var/nslog - This directory contains Citrix ADC log files.

/var/tmp/support - This directory contains technical support files, also known as, support bundles. All files not of interest should be deleted.

/var/core - Core dumps are stored in this directory. There will be directories within this directory and they will be labeled with numbers starting with 1. These files can be quite large in size. Clear all files unless the core dumps are recent and investigation is required.

/var/crash - Crash files, such as process crashes are stored in this directory. Clear all files unless the crashes are recent and investigation is required.

/var/nsinstall -  Firmware is placed in this directory when upgrading. Clear all files, except the firmware that is currently being used.
```

- Verifique si alguno de los directorios consume más espacio:

```
du -hs *
44k     cache
2.0k    clusterd
2.0k    configdb
6.0k    core
989M    crash
4.0k    cron
2.0k    dev
6.0k    download
2.0k    gui
2.0k    install
2.0k    krb
2.0k    learnt_data
122M    log
366M    NetScaler
14k     ns_gui
86k     ns_sys_backup
631M    nsinstall
883M    nslog
```



```
32k    nsproflog
2.0k    nssynclog
16k    nstemplates
36k    nstmp
4.5G    nstrace
8.1M    opt
6.0k    pubkey
52k    run
28M    safenet
72M    tmp
2.0k    vmtools
14k    vpn
```

- Elimine los archivos que no son necesarios:

```
rm -r nstrace/*
```

For more help on deleting files see FreeBSD Man Pages.

- Delete the files which are not required.
  `rm -r nstrace/*`
  For more help on deleting files see FreeBSD Man Pages.
- If the log or `nslog` directory is using more space, then run the following commands to open the log directory and view its contents:

```
cd /var/log
ls -l
cd /var/nslog
ls -l
```

1. Asegúrese de que todos los archivos estén comprimidos. Esto se indica mediante la extensión de nombre de archivo.tar.gz.
2. Si utiliza Citrix ADM o Command Center, compruebe el directorio /var/ns_system_backup. Asegúrese de que Citrix ADM o Command Center borren los archivos de copia de seguridad que crea.

Más recursos

Para obtener información sobre cualquiera de los comandos mencionados en el procedimiento anterior, consulte - http://ss64.com/bash/

Cómo descargar archivos principales o bloqueados desde el dispositivo Citrix ADC

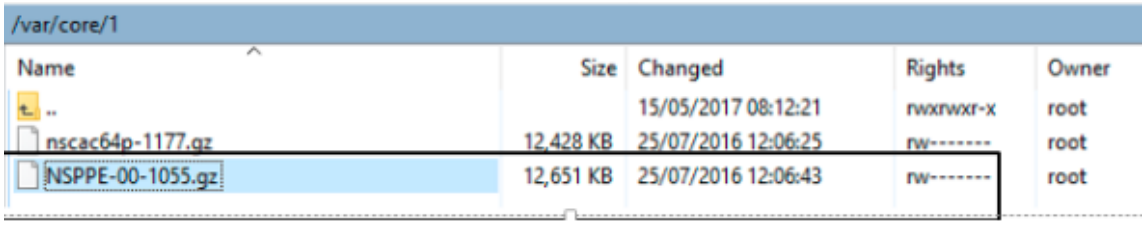
January 12, 2021

En este artículo de solución de problemas se explica cómo un administrador puede descargar archivos principales o bloqueados desde el dispositivo Citrix ADC.

Descargar archivos principales o de bloqueo desde el dispositivo Citrix ADC mediante el cliente SFTP

Para descargar los archivos principales o de bloqueo desde un dispositivo NetScaler, siga el procedimiento siguiente:

1. Abra WinSCP e inicie sesión en la dirección IP de NetScaler Management.
2. Vaya a `/var/core/1` para descargar los archivos.



> **Nota:**
>
> Para descargar el último archivo de bloqueo o núcleo, también puede utilizar la herramienta WinSCP a través de la interfaz de comandos. Los archivos se pueden ubicar en el directorio central o de bloqueo.

Cómo recopilar estadísticas de rendimiento y registros de eventos

January 12, 2021

Puede recopilar estadísticas de rendimiento de servidores virtuales y servicios asociados de un`newnslog` archivo archivado presente en el `/var/nslog` directorio. Los `newnslog` archivos se interpretan ejecutando `/netscaler/nsconmsg`.

Recopilar estadísticas de rendimiento y registros de eventos mediante la CLI

Puede ejecutar el `nsconmsg` comando desde el símbolo del shell de Citrix ADC para informar de eventos.

En el símbolo del sistema, escriba:

```
/netscaler/nsconmsg -K /var/nslog/newnslog -d event
```

```
1 Displaying event information
2 NetScaler V20 Performance Data
3 NetScaler NS10.5: Build 57.7.nc, Date: May 14 2015, 07:35:21
4 rtime: Relative time between two records in milliseconds
5 seqno rtime event-message                          event-time
6 11648 16310 PPE-0 MonServiceBinding_10.104.20.110:443_(tcp-default)
7 <!--NeedCopy-->
```

Ver el lapso de tiempo cubierto por un archivo "newnslog" dado

En el símbolo del sistema, escriba:

```
/netscaler/nsconmsg -K /var/nslog/newnslog -d setime
```

Los datos actuales se anexan al `/var/nslog/newnslog` archivo. NetScaler archiva el `newnslog` archivo automáticamente cada dos días de forma predeterminada. Para leer los datos archivados, debe extraer el archivo como se muestra en el siguiente ejemplo:

`cd /var/nslog`: Para ir a un directorio en particular desde NetScaler Shell Prompt.

`tar xvfz newnslog.100.tar.gz`: Para extraer el archivo tar.

`/netscaler/nsconmsg -K newnslog.100 -d setime`: Comando para comprobar el intervalo de tiempo cubierto por el archivo en particular, en este ejemplo`newnslog.100`.

`ls -l` Comando comprueba todos los archivos de registros y la marca de tiempo asociados con esos archivos.

```
root@NETSCALER## cd /var/nslog
root@NETSCALER## ls -l
```

```
1  wheel    461544 Aug  7  2014 newnslog.1.tar.gz
2 -rw-r--r--   1 root       wheel    191067 Aug  7  2014 newnslog.10.tar.
     gz
3 -rw-r--r--   1 root       wheel  11144873 Apr 26 22:04 newnslog.100.tar
     .gz
4 -rw-r--r--   1 root       wheel  11095053 Apr 28 22:04 newnslog.101.tar
     .gz
5 -rw-r--r--   1 root       wheel  11114284 Apr 30 22:04 newnslog.102.tar
     .gz
```



```
-rw-r--r--   1 root       wheel  11146418 May  2 22:04 newnslog.103.tar
    .gz
-rw-r--r--   1 root       wheel  11104227 May  4 22:04 newnslog.104.tar
    .gz
-rw-r--r--   1 root       wheel  11297419 May  6 22:04 newnslog.105.tar
    .gz
-rw-r--r--   1 root       wheel  11081212 May  8 22:04 newnslog.106.tar
    .gz
-rw-r--r--   1 root       wheel  11048542 May 10 22:04 newnslog.107.tar
    .gz
-rw-r--r--   1 root       wheel  11101869 May 12 22:04 newnslog.108.tar
    .gz
-rw-r--r--   1 root       wheel  11378787 May 14 22:04 newnslog.109.tar
    .gz
-rw-r--r--   1 root       wheel  44989298 Apr 11  2014 newnslog.11.gz
<!--NeedCopy-->
```

Mostrar el intervalo de tiempo dentro de un archivo

Utilice el `nsconmsg` comando para mostrar solo un lapso de tiempo dentro del archivo dado, como se muestra en el siguiente ejemplo:

```
/netscaler/nsconmsg -K /var/nslog/newnslog -s time=22Mar2007:20:00 -T 7 -s
ConLb=2 -d oldconmsg
```

Donde:

`s`: Time=22mar 2007:20:00:00 comienza el 22 de marzo de 2007 exactamente a las 20:00.

`T 7`: Muestra siete segundos de datos

`s`: Muestra el nivel de detalle de las estadísticas de equilibrio de carga.

`d`: Muestra información estadística.

> **Nota:**
>
> Desde la versión 12.1 de ADC también debe agregar en el “tiempo” segundos, es decir: 22Mar 2007:20:00:00

La información estadística proporcionada por el `-d oldconmsg` parámetro se registra cada siete segundos. A continuación se muestra un resultado de ejemplo.

```
VIP(10.128.58.149:80:UP:WEIGHTEDRR): Hits(38200495, 18/sec) Mbps(1.02)
    Pers(OFF) Err(0)
Pkt(186/sec, 610 bytes) actSvc(4) DefPol(NONE) override(0)
```



```
Conn: Clt(253, 1/sec, OE[252]) Svr(3)
S(10.128.49.40:80:UP) Hits(9443063, 4/sec, P[2602342, 0/sec]) ATr(5)
    Mbps(0.23) BWlmt(0 kbits) RspTime(112.58 ms)
Other: Pkt(36/sec, 712 bytes) Wt(10000) RHits(31555)
Conn: CSvr(42, 0/sec) MCSvr(20) OE(16) RP(11) SQ(0)
S(10.128.49.39:80:UP) Hits(9731048, 4/sec, P[2929279, 0/sec]) ATr(9)
    Mbps(0.27) BWlmt(0 kbits) RspTime(161.69 ms)
Other: Pkt(41/sec, 756 bytes) Wt(10000) RHits(31555)
Conn: CSvr(32, 0/sec) MCSvr(19) OE(13) RP(4) SQ(0)
S(10.128.49.38:80:UP) Hits(9341366, 5/sec, P[2700778, 0/sec]) ATr(4)
    Mbps(0.27) BWlmt(0 kbits) RspTime(120.50 ms)
Other: Pkt(42/sec, 720 bytes) Wt(10000) RHits(31556)
Conn: CSvr(37, 0/sec) MCSvr(19) OE(13) RP(9) SQ(0)
S(10.128.49.37:80:UP) Hits(9685018, 4/sec, P[2844418, 0/sec]) ATr(3)
    Mbps(0.23) BWlmt(0 kbits) RspTime(125.38 ms)
Other: Pkt(38/sec, 670 bytes) Wt(10000) RHits(31556)
Conn: CSvr(32, 0/sec) MCSvr(20) OE(10) RP(7) SQ(0)
<!--NeedCopy-->
```

> **Nota:**
>
> Los recuentos de conexiones de cliente de los servicios individuales no se suman al recuento de conexiones de cliente del servidor virtual. El motivo se debe a la reutilización de la sesión entre el dispositivo Citrix ADC y el servicio back-end.

Salida del servidor virtual

```
VIP(10.128.58.149:80:UP:WEIGHTEDRR): Hits(38200495, 18/sec)Mbps(1.02)Pers(
OFF)Err(0)Pkt(186/sec, 610 bytes)actSvc(4)DefPol(NONE)override(0)Conn: Clt
(253, 1/sec, OE[252])Svr(3)
```

La siguiente lista describe las estadísticas del servidor virtual:

1. `IP (IP address:port:state:Load balancing method)`. La dirección IP y el puerto de la dirección IP virtual tal como están configurados. El estado del servidor virtual o la dirección IP virtual es UP, DOWN o OUT OF SERVICE; Método de equilibrio de carga configurado para la dirección IP virtual.
2. `Hits (##)`. Número de solicitudes que llegaron al servidor virtual.
3. `Mbps (##)`. Volumen total de tráfico en el servidor virtual (Rx + Tx) convertido en Mbits/s
4. `Pers`: tipo de persistencia configurado.
5. `Err (##)`. Número de veces que el servidor virtual generó una página de error.
6. `Pkt (##/sec, ## bytes)`: Volumen de tráfico de red (como paquetes) que pasa a través del servidor virtual y el tamaño medio del paquete fluye a través del servidor virtual.
7. `actSvc(##)`. Número de servicios activos que están enlazados al servidor virtual.

8. `DefPol (RR)`. Indica si el método de equilibrio de carga predeterminado está activo. El método de equilibrio de carga predeterminado se utiliza para cierto número de solicitudes iniciales para suavizar el comportamiento de los otros métodos.
9. `Clt (##, ##/sec)`. Número de conexiones de cliente actuales a la velocidad del servidor virtual.
10. `OE [##]`. Número de conexiones de servidor desde el servidor virtual en estado abierto establecido.
11. `Svr (##)`. Número de conexiones de servidor actuales desde el servidor virtual.

En la salida anterior, `Svr(3)` indica que el comando recopila la muestra estadística. Hay tres conexiones activas para el servidor virtual con el servidor back-end, aunque hay cuatro servicios en total. Cuando un cliente establece una conexión con el servidor virtual, no es necesario que el cliente envíe o reciba tráfico cuando el comando recopila la información. Por lo tanto, es común ver el `Svr` contador más bajo que el `OE[]` número. El `Svr` contador representa el número de conexiones activas que están enviando o recibiendo datos activamente. La dirección IP asignada (MIP) o la dirección IP de subred (SNIP) está conectada al servidor back-end asociado. Además, Citrix ADC realiza un seguimiento del servidor virtual conectado al servidor back-end y calcula el contador.

Salida de servicio virtual

```
1 S(10.128.49.40:80:UP) Hits(9443063, 4/sec, P[2602342, 0/sec]) ATr(5)
     Mbps(0.23) BWlmt(0 kbits) RspTime(112.58 ms)
2 Other: Pkt(36/sec, 712 bytes) Wt(10000) RHits(31555)
3 Conn: CSvr(42, 0/sec) MCSvr(20) OE(16) RP(11) SQ(0)
4 <!--NeedCopy-->
```

La siguiente lista describe las estadísticas del servicio:

1. `S (IP address:port:state)`. Dirección IP, puerto y estado del servicio, como DOWN, UP o OUT OF SERVICE.
2. `Hits (##, P[##])`. Número de solicitudes dirigidas al servicio, Número de solicitudes dirigidas al servicio debido a la persistencia del servidor configurado.
3. `ATr (##)`. Número de conexiones activas al servicio.

> **Nota:**
>
> Las conexiones activas son aquellas que tienen la solicitud pendiente al servicio o que actualmente tienen actividad de tráfico.

1. `Mbps (##.####)`. Volumen total de tráfico en el servicio (Rx + Tx) convertido en Mbits/s
2. `BWlmt (## kbits)`: límite de ancho de banda definido.
3. `RspTime (## ms)`. Tiempo medio de respuesta del servicio en milisegundos.

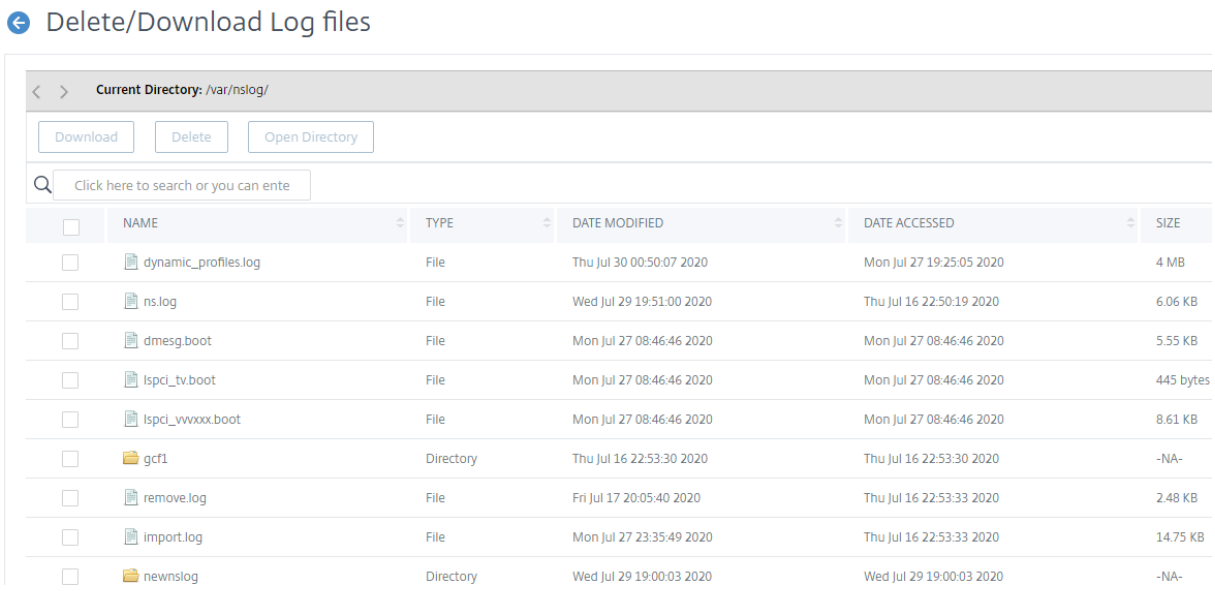
4. `Pkt(##/sec, ##bytes)`. Volumen de tráfico en términos de paquetes por segundo que van al servicio; Tamaño medio de los paquetes.
5. `Wt (##)`. Índice de peso, utilizado en el algoritmo de equilibrio de carga.

> **Nota:**
>
> Si divide este valor por 10.000, obtendrá el peso real configurado del servicio.

1. `RHits (##)`. Contador de solicitudes en ejecución utilizado en el algoritmo de equilibrio de carga de Round Robin.
2. `CSvr (##, ##/sec)`. Número de conexiones a la tasa de servicio.
3. `MCSvr (##)`. Número máximo de conexiones al servicio.
4. `OE (##)`. Número de conexiones al servicio en el estado establecido.
5. `RP (##)`. Número de conexiones al servicio que residen en el grupo de reutilización.
6. `SQ (##)`. Número de conexiones al servicio, esperando en la cola de sobretensión.

Recopilar estadísticas de rendimiento y registros de eventos mediante la GUI de Citrix ADC

1. Vaya a **Sistema > Diagnósticos > Mantenimiento > Eliminar o descargar archivos de registro**.
2. Seleccione un archivo y haga clic en **Descargar** para descargar el archivo.



Cómo configurar la rotación del archivo de registro

January 12, 2021

El dispositivo Citrix ADC genera registros en varios directorios y en varios formatos. Algunos de estos registros no se rotan de forma predeterminada y pueden crecer de tamaño consumiendo demasiado espacio en disco. Mediante el uso de las utilidades incluidas para la rotación de registros (`newsyslog`), puede administrar estos registros de forma coherente, manteniendo solo la información relevante para facilitar la administración y administración.

La `newsyslog` utilidad incluida en el firmware de Citrix ADC archiva los archivos de registro y gira los registros del sistema para que el registro actual esté vacío durante la rotación. El crontab del sistema ejecuta esta utilidad cada hora y lee el archivo de configuración que especifica los archivos a rotar y las condiciones. Los archivos archivados podrían estar comprimidos si es necesario.

La configuración existente se encuentra en `/etc/newsyslog.conf`. Sin embargo, dado que este archivo reside en el sistema de archivos de memoria, el administrador debe guardar las modificaciones en para `/nsconfig/newsyslog.conf` que la configuración sobreviva reiniciando NetScaler.

Las entradas contenidas en este archivo tienen el siguiente formato:

```
logfilename [owner:group] mode count size when flags [/pid_file] [sig_num]
```

> **Nota:**
>
> Los campos entre corchetes son opcionales y se pueden omitir.

Cada línea del archivo representa un archivo de registro y las condiciones en las que debe producirse la rotación.

En el ejemplo, el `size` campo indica que el tamaño de`ns.log` como 100 kilobytes. El `count` campo indica que el número de `ns.log` archivos archivados es 25. Un tamaño de 100 K y un recuento de 25 son los valores predeterminados de tamaño y recuento.

> **Nota:**
>
> Cuando el campo está configurado con un asterisco (*), lo que significa que el archivo ns.log no se gira en función del tiempo. Cada hora, un trabajo crontab ejecuta la `newsyslog` utilidad que comprueba si el tamaño de ns.log es mayor o igual al tamaño configurado en este archivo. En este ejemplo, si es mayor o igual que 100 K, rota ese archivo.

```
root@ns# cat /etc/newsyslog.conf
# Netscaler newsyslog.conf

# This file is present in the memory filesystem by default, and any
   changes
# to this file will be lost following a reboot. If changes to this file
# require persistence between reboots, copy this file to the /nsconfig
# directory and make the required changes to that file.
#
```



```
# logfilename [owner:group] mode count size when flags [/pid_file] [
    sig_num]
/var/log/cron 600 3 100 * Z
/var/log/amd.log 644 7 100 * Z
/var/log/auth.log 600 7 100 * Z
/var/log/ns.log 600 25 100 * Z
<!--NeedCopy-->
```

El`size` campo se puede cambiar para modificar el tamaño mínimo del`ns.log` archivo o el campo se puede cambiar para rotar el `ns.log` archivo en función de un tiempo determinado.

La especificación diaria, semanal y/o mensual se da como: `[Dhh]`, y `[Dhh [Mdd]]`, respectivamente. Los campos de hora del día, que son opcionales, por defecto son medianoche. Los rangos y significados de estas especificaciones son:

```
Hh hours, range 0 ... 23
w day of week, range 0 ... 6, 0 = Sunday
dd day of month, range 1 ... 31, or the letter L or l to specify the
    last day of the month.
<!--NeedCopy-->
```

Ejemplos:

Aquí hay algunos ejemplos con explicaciones para los registros que se rotan de forma predeterminada:

`/var/log/auth.log 600 7 100 * Z`

El registro de autenticación se rota cuando el archivo alcanza los 100 K, las últimas 7 copias del auth.log se archivan y comprimen con gzip (indicador Z), y a los archivos resultantes se les asignan los siguientes permisos —rw—.

`/var/log/all.log 600 7 * @T00 Z`

El registro de todo se gira 7 veces a medianoche cada noche (@T00) y se comprime con gzip. A los archivos resultantes se les asignan los siguientes permisos —rw-r—.

`/var/log/weekly.log 640 5 * $W6D0 Z`

El registro semanal se rota 5 veces a la medianoche todos los lunes. Los archivos resultantes se asignan con permisos.

Patrones de rotación comunes:

- `D0`. rotar todas las noches a medianoche
- `D23`. rotar todos los días a las 23:00

- `W0D23`. rotar cada semana el domingo a las 23:00
- `W5`. rotar todas las semanas el viernes a la medianoche
- `MLD6`. rotar el último día de cada mes a las 6:00
- `M5`. rotar cada quinto día del mes a medianoche

Si se da una especificación de intervalo y tiempo, se deben cumplir ambas condiciones. Es decir, el archivo debe ser tan antiguo o más antiguo que el intervalo especificado y la hora actual debe coincidir con la especificación de tiempo.

Puede controlar el tamaño mínimo del archivo, pero no hay límite en el tamaño del archivo antes de que la `newsyslog` utilidad obtenga su turno en la siguiente ranura de hora.

Depurar newsyslog:

Para depurar el comportamiento de la `newsyslog` utilidad, agregue el indicador detallado.

```
root@dj_ns# newsyslog -v
/var/log/cron <3Z>: size (Kb): 31 [100] --> skipping
/var/log/amd.log <7Z>: does not exist, skipped.
/var/log/auth.log <7Z>: size (Kb): 2 [100] --> skipping
/var/log/kerberos.log <7Z>: does not exist, skipped.
/var/log/lpd-errs <7Z>: size (Kb): 0 [100] --> skipping
/var/log/maillog <7Z>: --> will trim at Tue Mar 24 00:00:00 2009
/var/log/sendmail.st <10>: age (hr): 0 [168] --> skipping
/var/log/messages <5Z>: size (Kb): 7 [100] --> skipping
/var/log/all.log <7Z>: --> will trim at Tue Mar 24 00:00:00 2009
/var/log/slip.log <3Z>: size (Kb): 0 [100] --> skipping
/var/log/ppp.log <3Z>: does not exist, skipped.
/var/log/security <10Z>: size (Kb): 0 [100] --> skipping
/var/log/wtmp <3>: --> will trim at Wed Apr 1 04:00:00 2009
/var/log/daily.log <7Z>: does not exist, skipped.
/var/log/weekly.log <5Z>: does not exist, skipped.
/var/log/monthly.log <12Z>: does not exist, skipped.
/var/log/console.log <5Z>: does not exist, skipped.
/var/log/ns.log <5Z>: size (Kb): 18 [100] --> skipping
/var/log/nsvpn.log <5Z>: size (Kb): 0 [100] --> skipping
/var/log/httperror.log <5Z>: size (Kb): 1 [100] --> skipping
/var/log/httpaccess.log <5Z>: size (Kb): 1 [100] --> skipping
root@dj_ns#
<!--NeedCopy-->
```


Cómo liberar espacio en un directorio /flash en un dispositivo Citrix ADC

August 20, 2021

En este artículo de solución de problemas se explica cómo un administrador puede liberar espacio del directorio /flash de un dispositivo Citrix ADC.

Procedimiento para liberar espacio en el directorio /flash de un dispositivo Citrix ADC

1. Inicie sesión en la CLI de Citrix ADC mediante SSH.
2. Después de iniciar sesión en la CLI de Citrix ADC, cambie al símbolo del shell mediante el siguiente comando.`shell`.
3. Ejecute el `df -h` comando para ver la disponibilidad de espacio en el dispositivo Citrix ADC.
4. Si la capacidad del directorio /flash es superior al 90 por ciento o baja, debe eliminar algunos archivos de este directorio.
5. Ejecute los siguientes comandos para ver el contenido del directorio /flash:

```
cd /flash
ls -l
```

6. Es posible que encuentres varios archivos de varias versiones de la versión de software NetScaler. Asegúrese de que los archivos presentes en esta ubicación sean los aplicables a la versión actual del software NetScaler del dispositivo. Ejecute el siguiente comando para quitar cualquier otro archivo del dispositivo.

```
rm <filename>
```

> **Nota**
>
> Elimine solo las versiones anteriores del kernel. El directorio /flash debe contener los archivos que utiliza la versión o compilación actual de la versión de software de NetScaler y el archivo kernel.gz. Citrix recomienda no quitar estos archivos del directorio /flash.

Material de referencia

August 20, 2021

Utilice esta información de referencia para comprender en profundidad los siguientes componentes de Citrix ADC:

OID SNMP de Citrix ADC: Detalles de los OID SNMP que se pueden utilizar para obtener información de un dispositivo Citrix ADC.

Mensajes de syslog de Citrix ADC: Detalles de los mensajes de syslog proporcionados por el dispositivo Citrix ADC.

Comandos de la CLI de Citrix ADC: Detalles de los comandos que se pueden utilizar para configurar el dispositivo Citrix ADC a través de la CLI. También puede ver los detalles de cada comando en la CLI, mediante el comando “man <ns-command-name>”.

Referencia de API: Detalles de todas las operaciones que se pueden realizar en el dispositivo Citrix ADC mediante la API REST.

Citrix ADC Advanced Policy Expressions: Detalles de las expresiones que se pueden utilizar para definir directivas avanzadas.

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States